



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

EASA Part-IS Information event

for technical aviation organisations POA, MOA, CAMO

(EU)2022/1645 (EU)2023/203

**Management of information security risks in regard
to aviation safety**

Emmen/LU 15. November 2024



eRules

PART-IS
(IR/DR + AMC/GM)



Objectives of the event

The event's objectives are to...



- ✓ become aware of the rule regarding the management of information security
- ✓ profit from experiences of early Part-IS adopters
- ✓ engage organisations in starting the implementation journey
- ✓ foster networking in information security among aviation stakeholders

...make the aviation landscape more resilient against information security risks

Practical arrangements



In view of Switzerland's linguistic diversity, everyone is invited to speak in their own language (D / F / I) or E.



Participants are invited and encouraged to ask questions after each presentation and in the dedicated Q & A session.



FOCA will take pictures of the event by respecting your privacy. Please come to us, in case you have any objections.



Information about the event, including some images may be published on FOCA's website, and/or social media channels (e.g. LinkedIn)



The presentations will be sent to all participants as a PDF file among with a short survey in the aftermath of the event.

Agenda

Time	Title	Presenting Organisation
09:00 – 09:30	Check-In / Registration	
09:30 – 09:45	Opening – Introduction to the event	FOCA
09:45 – 10:30	Introduction and objectives of Part-IS	EASA
10:30 – 11:00	Information security risk management from a regulator's perspective	FOCA
11:00 – 11:30	Coffee break	
	ISMS / Part-IS implementation...	
11:30 – 12:15	... from an airport perspective	FZAG
12:15 – 13:00	... from a multiple approval holder perspective	Pilatus
13:00 – 14:00	Lunch break	
14:00 – 14:30	Panel discussion	EASA FOCA, FZAG and Pilatus
14:30 – 14:50	Q & A	all
14:50 – 15:00	Conclusion & Closing	FOCA

Speakers – Representatives of regulators



Davide Martini
Senior Expert –
Cybersecurity in Aviation

Davide Martini has been a Senior Cybersecurity Expert at EASA since 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.

He holds a Master degree in Aerospace Engineering from Politecnico di Milano.

Speakers – Representatives of regulators



Vasileios Papageorgiou
Junior Expert –
Cybersecurity

Vasileios Papageorgiou is a Junior Expert for Cybersecurity in Aviation. He is mainly involved in the Part-IS Implementation support activities as well as Cyber Threat Intelligence.

Prior to joining EASA, he worked as a Researcher in Cybersecurity & Counter Terrorism Research. He has completed his military service in the Hellenic Army Aviation and he has also served a 1-year traineeship at the Certification Directorate of EASA supporting the implementation activities on the UAS operations (Open & Specific).

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

Introduction and objectives of Part-IS

Vasileios Papageorgiou

Junior Expert – Cybersecurity in Aviation

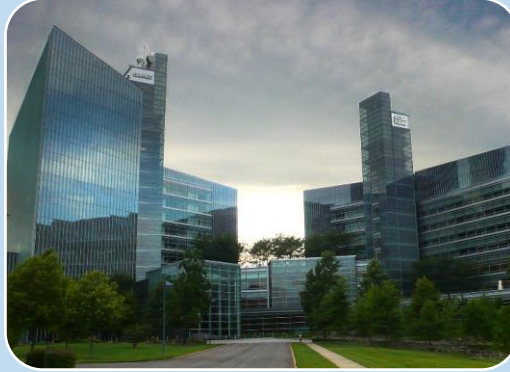
15th November 2024

Making EU aviation cyber resilient



Products (Aircrafts, Engines, ...)

- Transition from case by case approach to mandatory on all products now done.
- Positive change of mind set in industry: From defiance to full engagement.



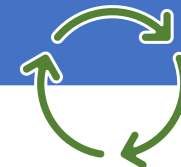
Organisations (People, Processes)

- **Part-IS** Regulations published in October 2022 and February 2023
- AMC/GM published on 12 July 2023



Information Sharing

- Create a community to
 - Share knowledge
 - Perform Analysis
 - Collaborate
 - Reinforce the system

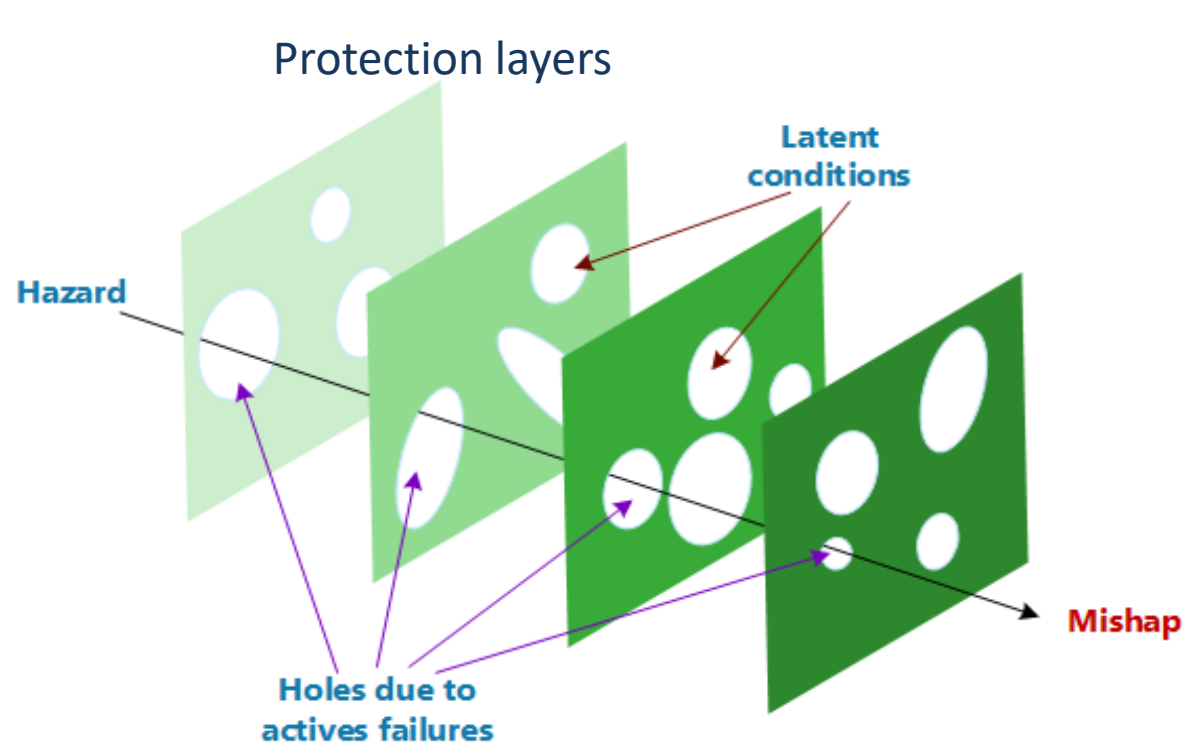


Capacity building & Research

- To have competent and well aware workforce
- To monitor the current Threat Landscape
- To understand the future Threat Landscape

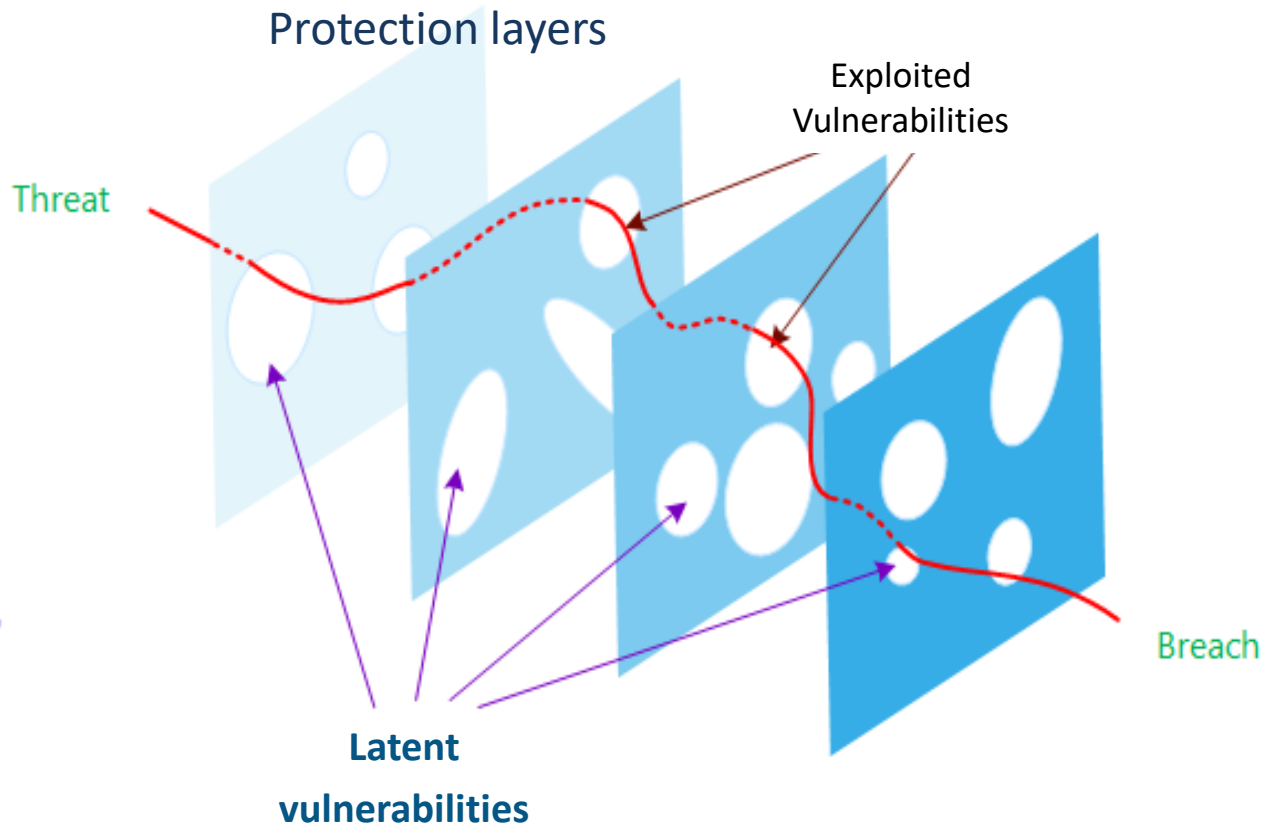


The cultural bias in aviation



Safety

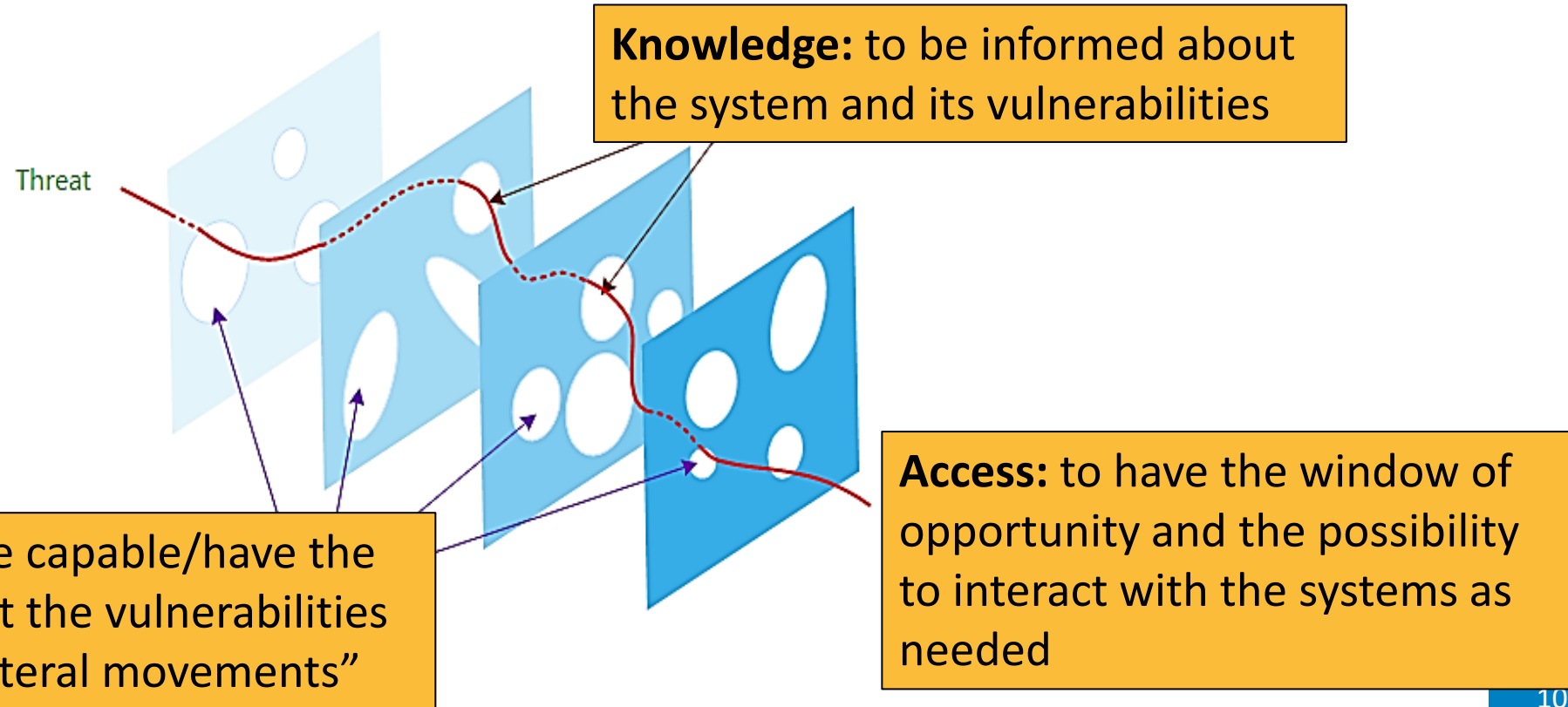
vs.



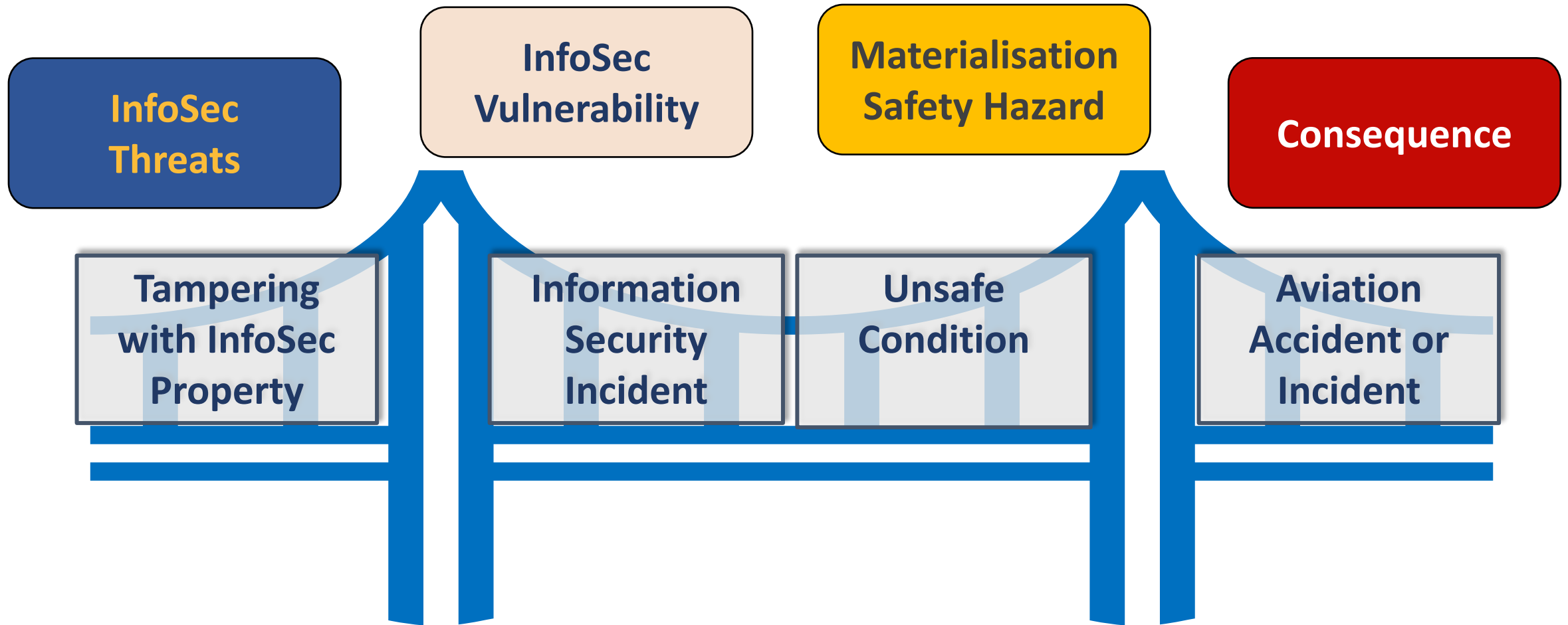
Security

A different approach to risk assessment

Risk assessment in cybersecurity is based on capability, knowledge and access



Bridging between Information Security and Safety



What we want to achieve with Part-IS

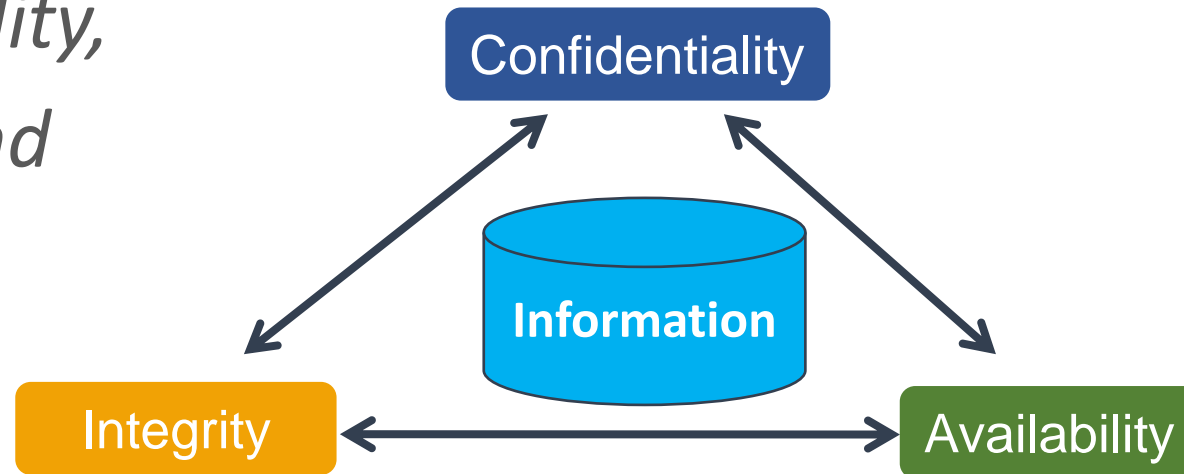
Objective	Protect the aviation system from information security risks with potential impact on aviation safety
Scope	Information and communication technology systems and data used by Approved Organisations and Authorities for civil aviation purposes
Activity	<ul style="list-style-type: none">- identify and manage information security risks related to information and communication technology systems and data used for civil aviation purposes;- detect information security events, identifying those which are considered information security incidents; and- respond to, and recover from, those information security incidents

What is an ISMS?

What is Information Security Management?

➤ ISO 27000 states that *Information Security Management* is a top-down, business driven approach to the management of an organization's physical and electronic information assets in order to preserve their

- Confidentiality,
- Integrity, and
- Availability.



What is an ISMS?

ISO 27001

An ISMS is the means by which management monitors and controls information security, minimizing the residual **business risk** and ensuring that information security continues to fulfill corporate, customer and legal requirements.

**business
risk**

Part-IS

An ISMS is the means by which management monitors and controls information security, minimizing the residual **business** **safety risk** and ensuring that information security continues to fulfill ~~corporate, customer and~~ legal requirements **and societal expectations**.

**safety
risk**

What are the Key Ingredients for Part-IS?

Basic Regulation

- Acceptable Safety Risks
- Record-keeping
- Personnel Requirements

ISO 2700x

- Information Security Management System (ISMS)
- Information Security Risk Assessment
- Continuous Improvement

NIST Cyber Security Framework

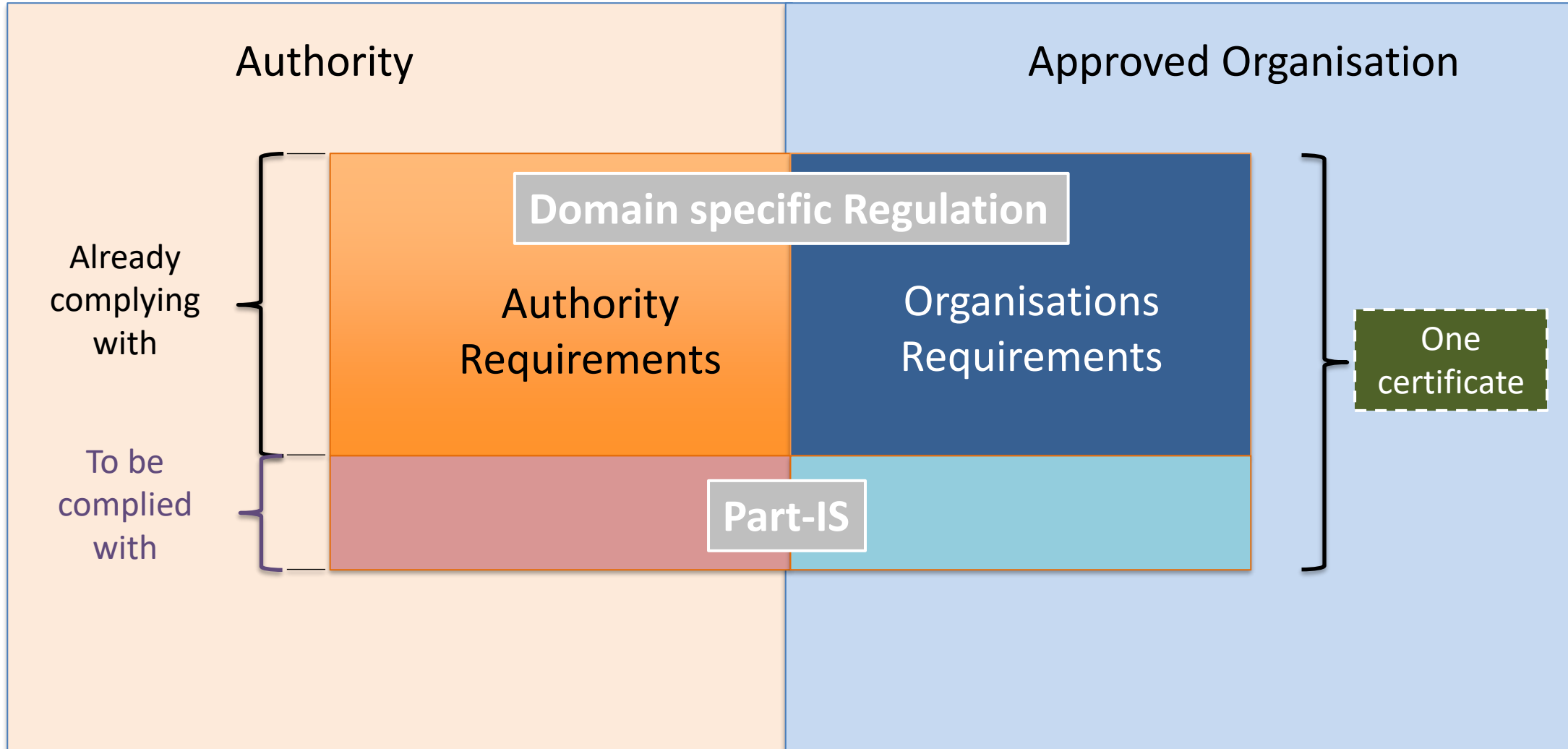
- Information Security Risk Treatment
- Information Security Incidents — Detection, Response, and Recovery



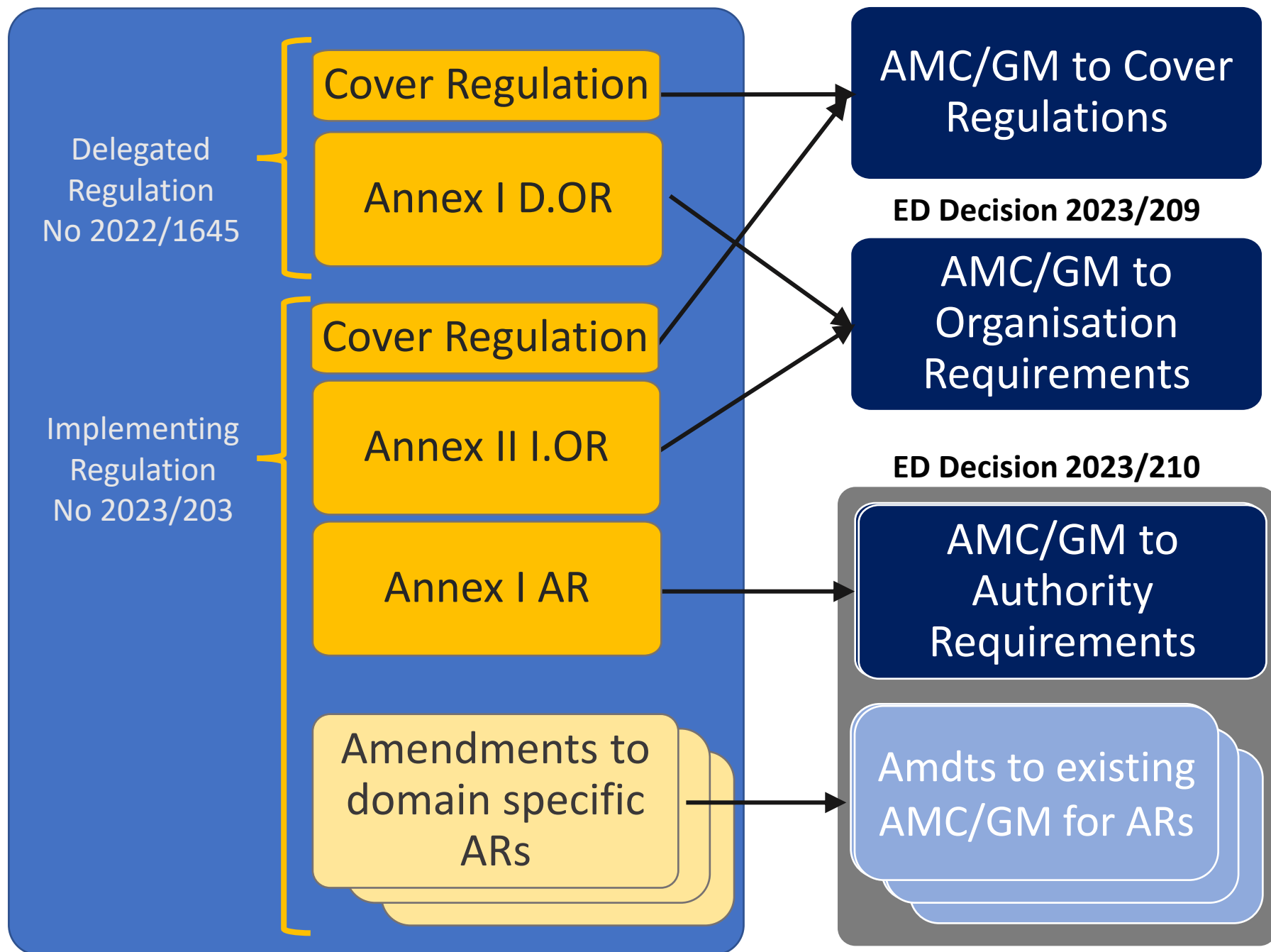
Reporting Regulation

- Information Security External Reporting Scheme

Part-IS and existing approvals/regulations



Part-IS Regulations



3 ED Decisions



Easy Access Rules
available [here](#)

Domains affected by Part-IS

Implementing Regulation
2023/203

FSTD Ops	
AeMC	
ATO	
AOC	ATCO TO

AMO
CAMO
POA
DOA

Civil Aviation
Authorities for all
aviation domains



Air Operations
& Licensing

Airworthiness

Drones

U-Space SP

Aerodromes

Aerodrome operators
Apron Management

ATM/ANS

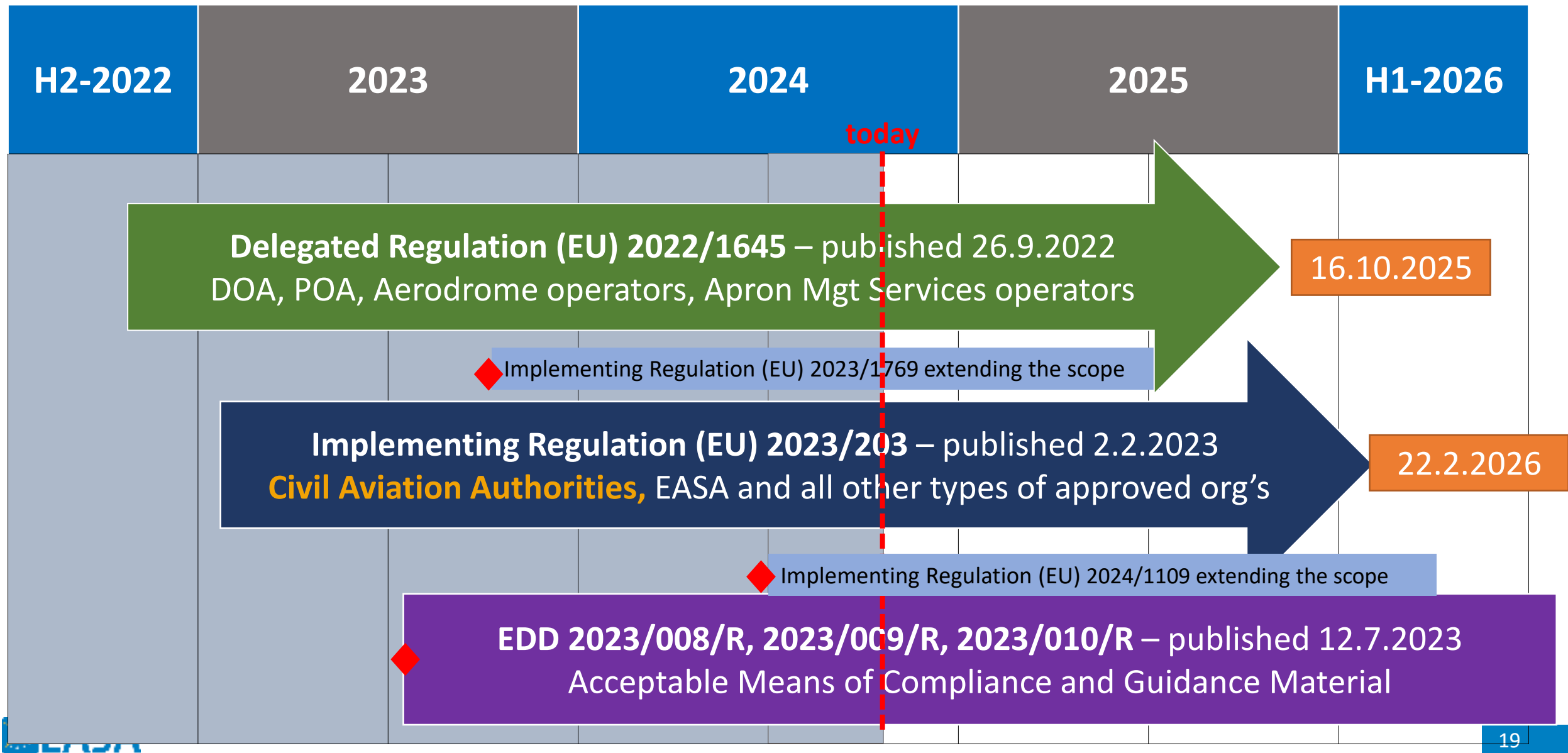
ATS	CNS
MET	ATFM
AIS	ASM
DAT	FPD
DPO	NM

Delegated Regulation
2022/1645

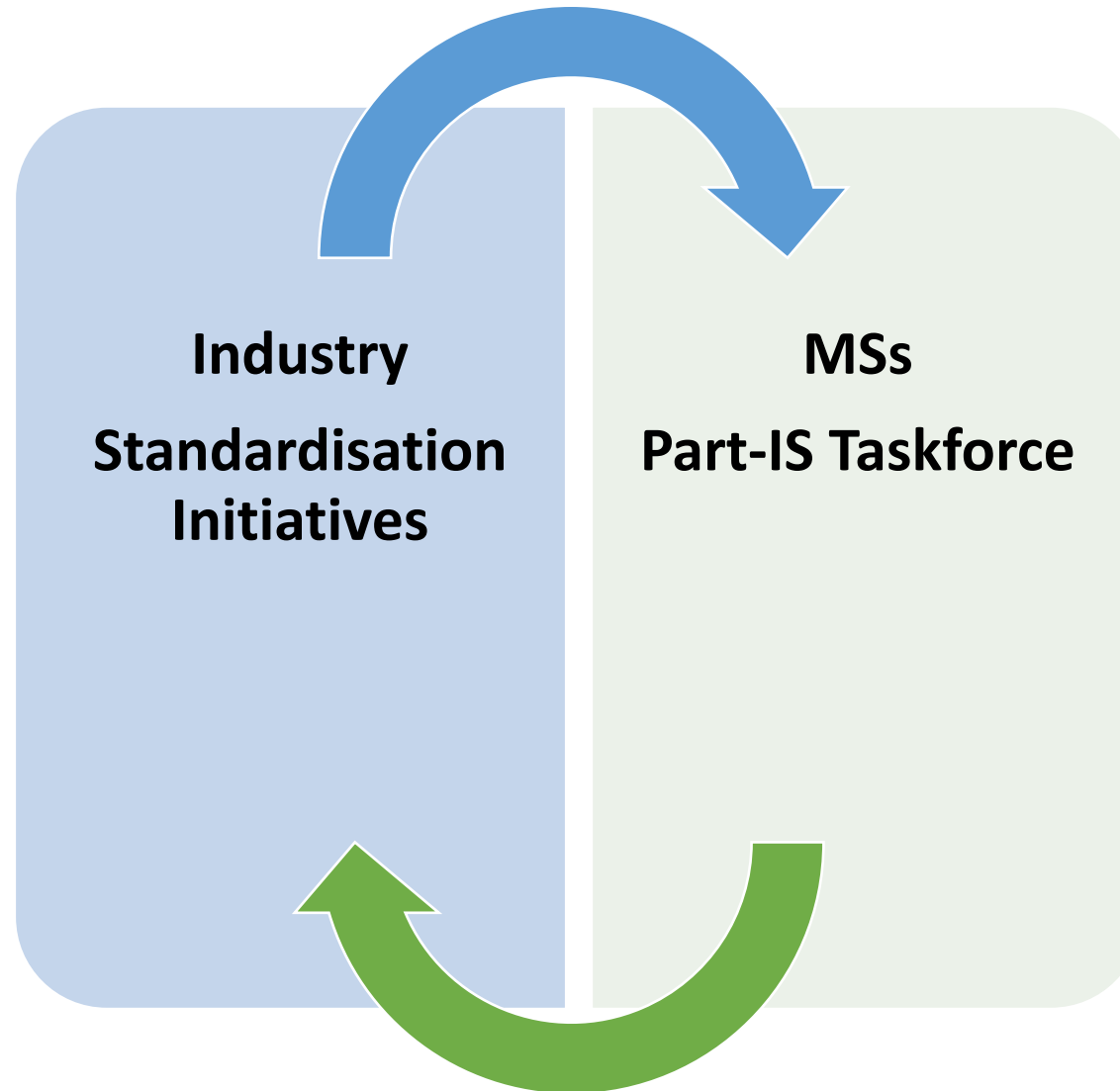
Implementing Regulation (EU) 2024/1109 applying Part-IS to authorities
overseeing CAW of certified UAS.

Implementing Regulation (EU) 2023/1769 extending the scope
of Part-IS to DPOs

Part-IS implementation journey



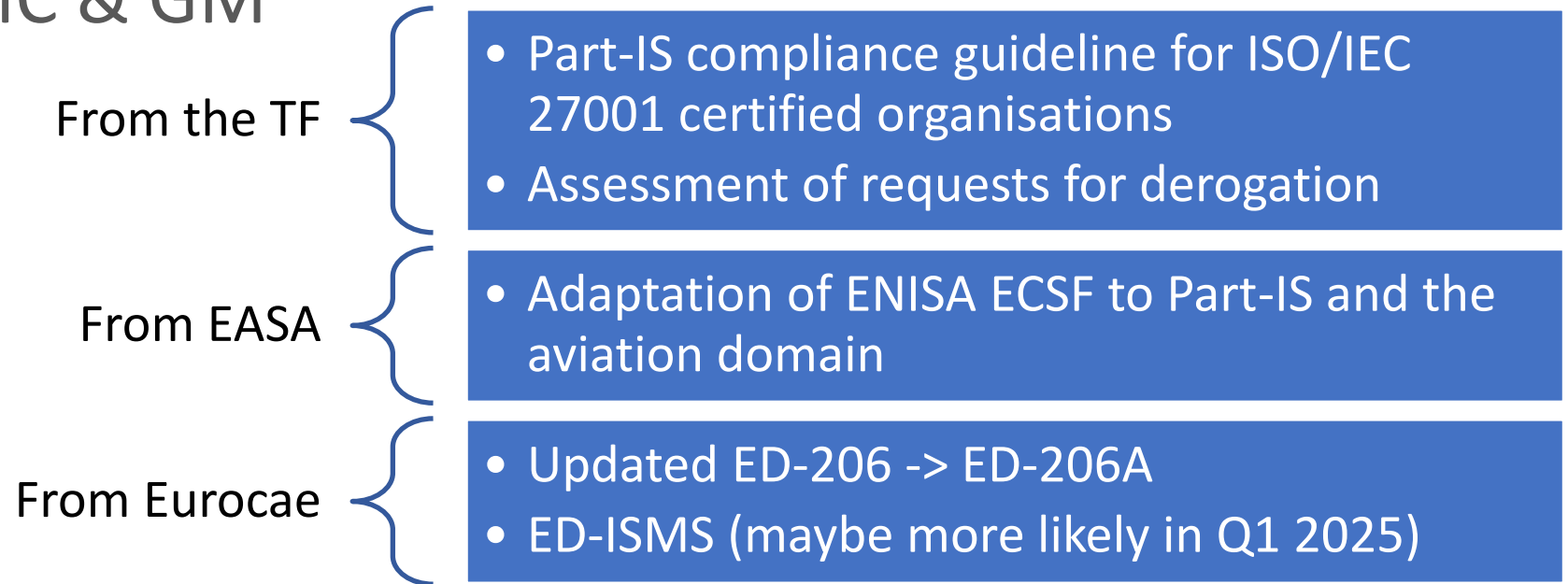
Other initiatives supporting Part-IS implementation



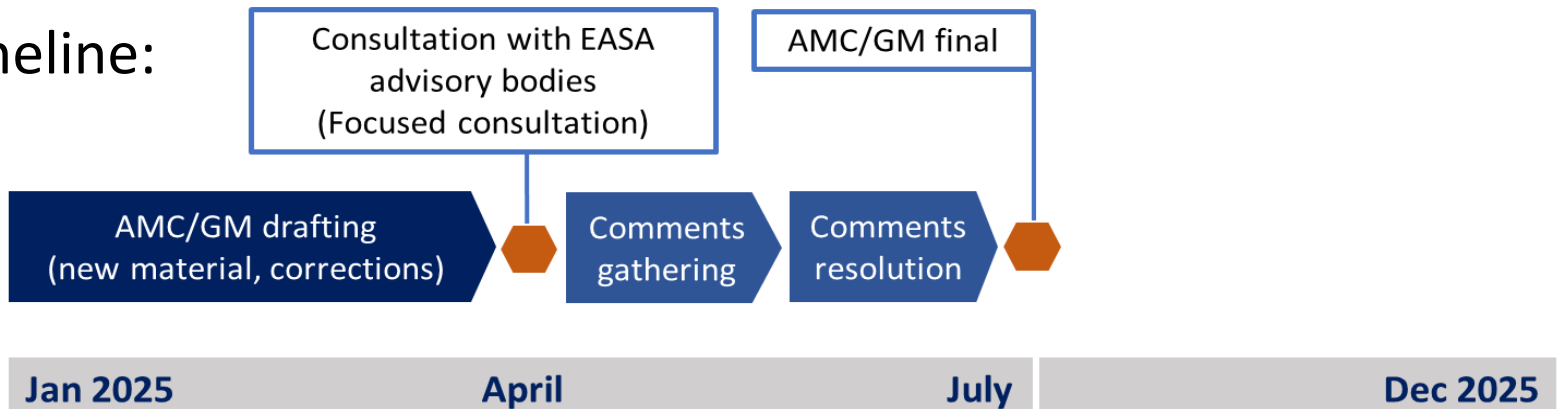
AMC & GM update before Part-IS applicability

→ New guidance material has been/is being developed since the publication of AMC & GM

→ Some examples:



Tentative timeline:

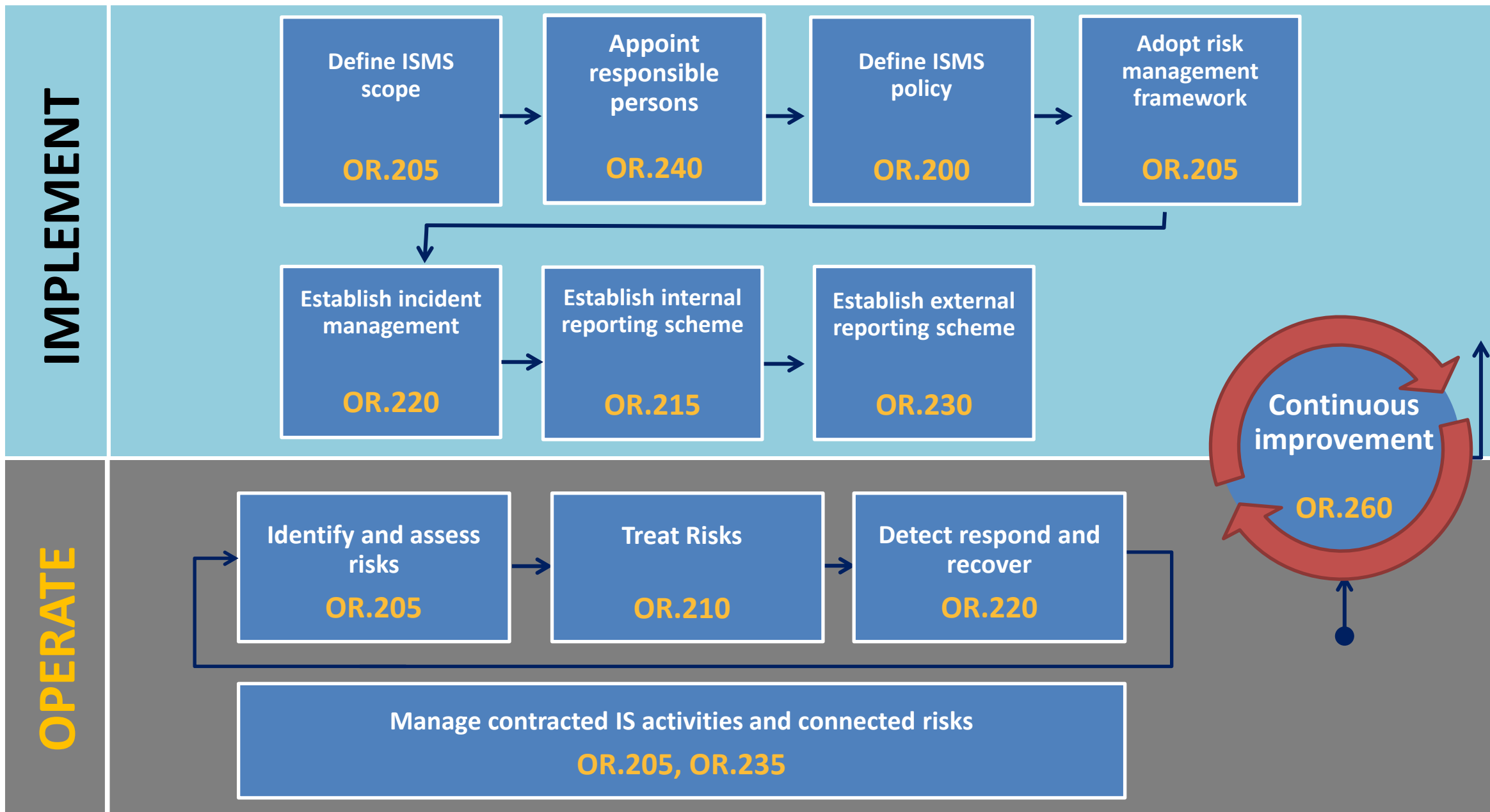


Overview of Part IS requirements: Organisation vs Authority

ORGANISATION	Description	AUTHORITY
IS.I.OR.100	Scope	IS.AR.100
IS.I.OR.200	Information security management system (ISMS)	IS.AR.200
IS.I.OR.205	Information security risk assessment	IS.AR.205
IS.I.OR.210	Information security risk treatment	IS.AR.210
IS.I.OR.215		
IS.I.OR.220	Information security incidents — detection, response, and recovery	IS.AR.215
IS.I.OR.225		
IS.I.OR.230	Information security external reporting scheme	✓
IS.I.OR.235	Contracting of information security management activities	IS.AR.220
IS.I.OR.240	Personnel requirements	IS.AR.225
IS.I.OR.245	Record-keeping	IS.AR.230
IS.I.OR.250		
IS.I.OR.255		
IS.I.OR.260	Continuous improvement	IS.AR.235

Overview of Part IS requirements: Organisation vs Authority

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



Thank you for your attention!

Join our Community:



easa.europa.eu/connect



Contact us at:
cybersec@easa.europa.eu

Your safety is our mission.

An Agency of the European Union 

Speakers – Representatives of regulators



Federal Office Of Civil Aviation,
FOCA



Camille Kunzi
Inspector Information
Security

Camille Kunzi has been working in the aviation industry for 10+ years in various positions as a innovation and project manager and recently joined FOCA.

At Airbus Defence & Space she worked as a program manager for industrial cyber security and led a multi-functional team to improve cyber resilience in aircraft & spacecraft production environment.

She holds a Master's degree in material engineering.

Speakers – Representatives of regulators



Federal Office Of Civil Aviation,
FOCA



Christoph Schnyder's role Cyber Security Coordinator, responsible for implementing EASA Part-IS at FOCA. He represents the office in various national and international bodies in regard to information security.

He has 20+ years professional experience and has held various roles as a software and security engineer and as an expert in product cyber security.

Christoph Schnyder

Cyber Security Coordinator / Program Lead



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 Management from a regulator perspective

**EASA Part-IS Information event for technical organisations
(POA, CAMO, Part-145)**

Emmen 15. November 2024

FOCA – Camille Kunzi & Christoph Schnyder



Voices from you, the industry

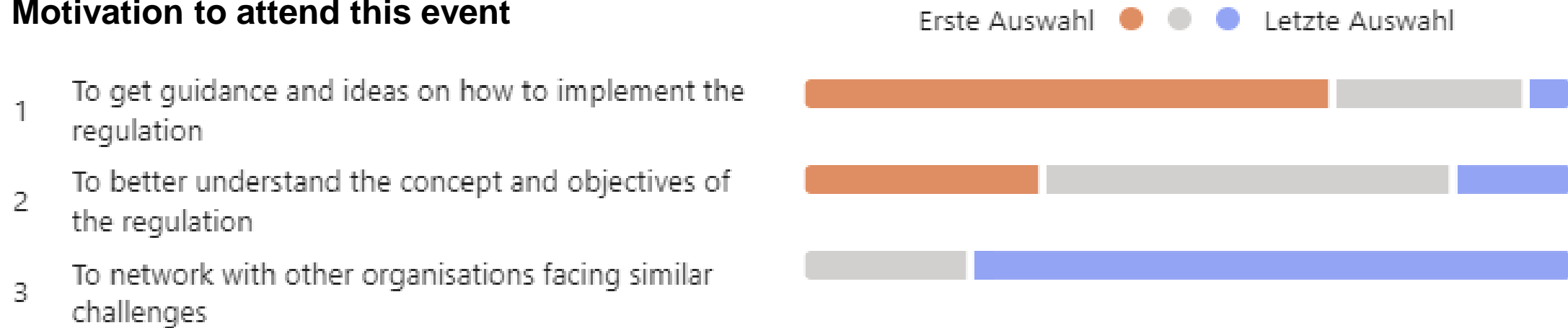




Voices from you, the industry

Number of responses as per 14.11.2024 17:30: **55**

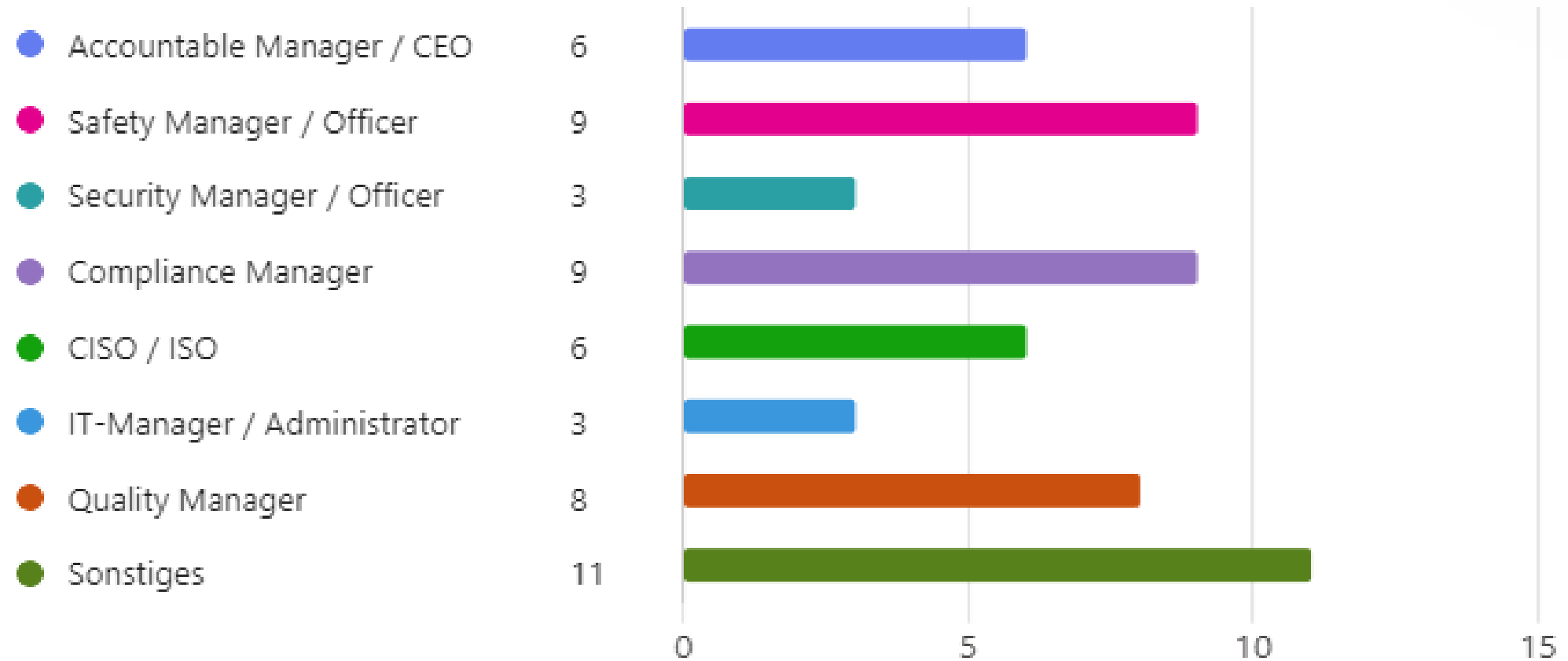
Motivation to attend this event





Voices from you, the industry

Position of participants

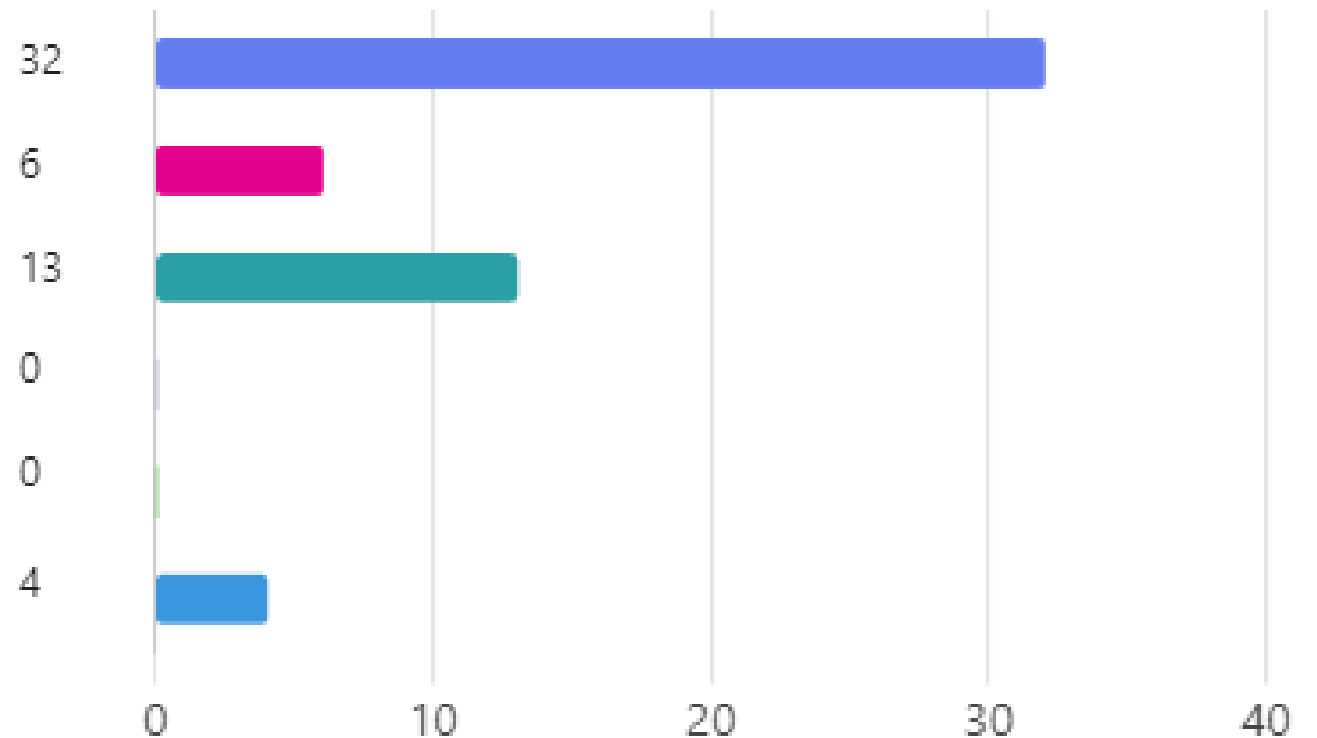




Voices from you, the industry

Implementation progress

- We have not started yet
- We have identified some gaps
- Implementation is in progress
- We are almost done
- Implementation is complete
- Our organisation is considering to obtain an approval for derogation as per IS.OR.200(e)



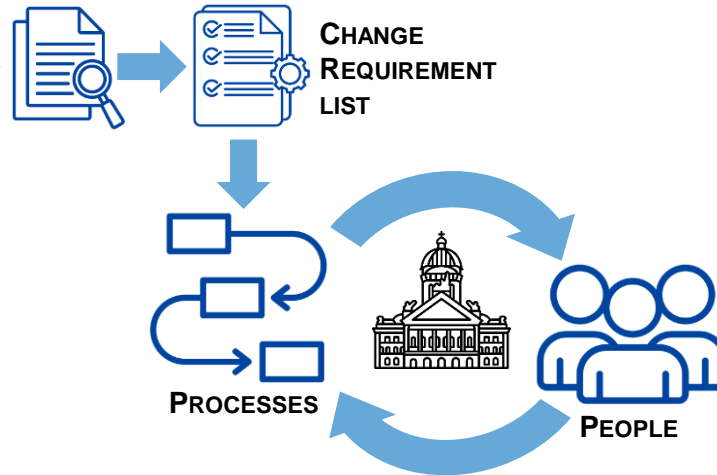


Part IS Project - Mission

COORDINATION WITH REGULATORS



COORDINATION WITHIN BAZL



INFORMATION TO SWISS AVIATION INDUSTRY





Implementation objectives

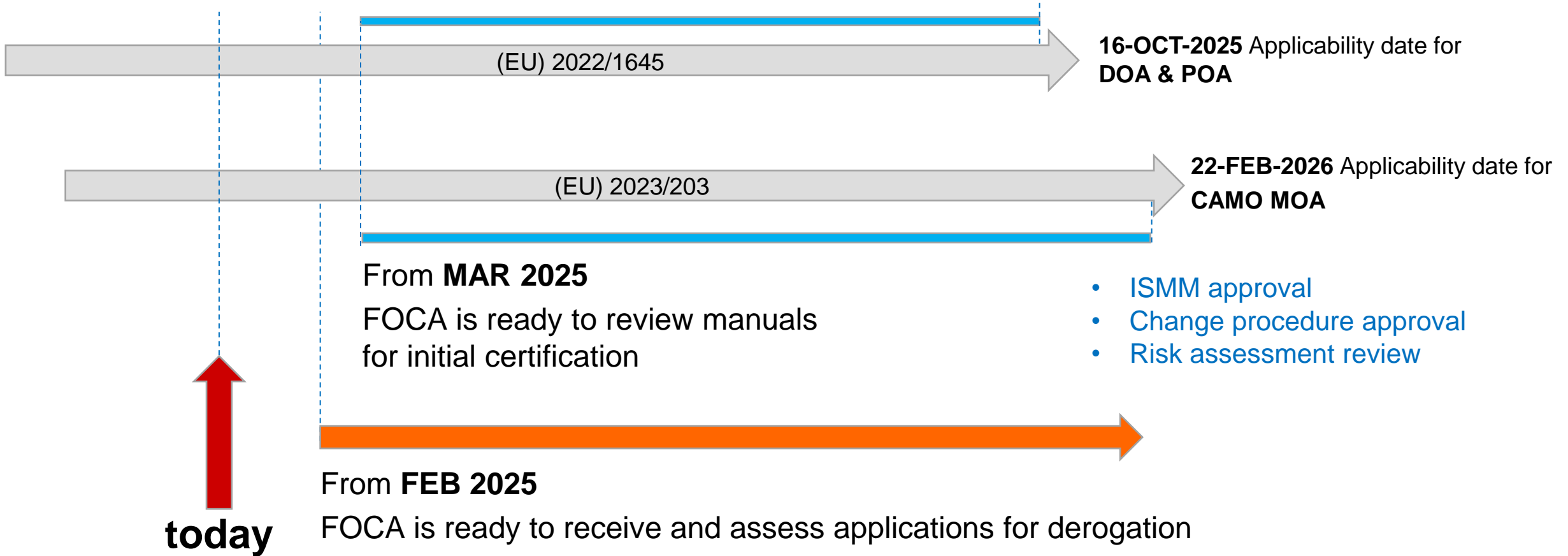
- FOCA aims to integrate Part-IS into joint oversight activities of safety management systems where applicable.
- FOCA internally coordinates oversight activities for organisations holding multiple approvals to avoid redundant audits.
- FOCA will acquire dedicated resources with specific information security know-how which serve all safety departments and sections.
- FOCA will perform risk- and performance based oversight (RBO/PBO) with adequate application of the aspect of proportionality (IS.I/D.OR.200 (d))
- FOCA aims to create a standardised and easy process to handle derogation requests from eligible organisations (IS.I/D.OR.200 (e))



Part-IS Timeline

From **MAR 2025**

FOCA is ready to review manuals for initial certification





Expectation at applicability date

- The organisation should be able to demonstrate a consistent and comprehensible approach in the management of information security.
- FOCA does not expect perfection at initial compliance stage
- An integration of the ISMS into existing MS is possible and beneficial



Expectation at applicability date

PRESENT – **SUITABLE** – OPERATING - EFFECTIVE

Appoint
responsible
persons

OR.240

Define ISMS
scope

OR.205

Define ISMS
policy

OR.200



Organisational structure

Non conclusive

- Has the structure been updated to account for ISMS? (e.g., appointment of an information security manager, reporting structure).
- Are roles and responsibilities defined and assigned?



Security policy

- Is the purpose and scope defined?
- Are the information security objectives defined?
- Is aviation safety an integral part and reflected in the policy?
- Are there references to a data classification scheme of the organisation?



Expectation at applicability date

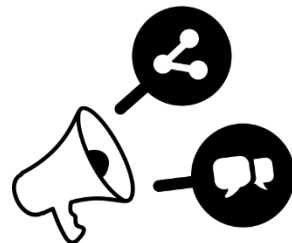
PRESENT – **SUITABLE** – OPERATING - EFFECTIVE



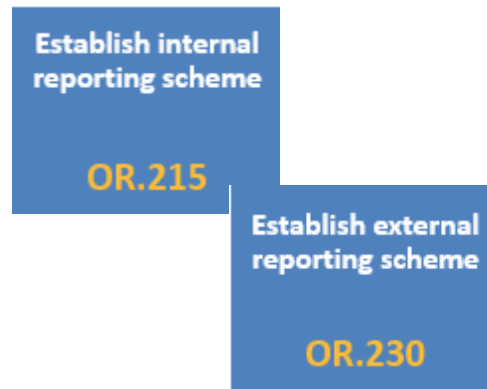
Risk management

Non conclusive

- Has the organisation established an asset inventory?
- Is there a formal process established?
 - Risk identification
 - Risk assessment
 - Risk treatment



Reporting



- Is there a scheme or process defined to internally and externally report security events and incidents?
- Identification of events and incidents which may have an impact on aviation safety



Applying for derogation

An organisation which does **not pose any information security risks** with a **potential impact on aviation safety** may be approved to not implement the requirements IS.OR.205 ... IS.OR.260

- No safety impact to the organisation itself and
 - No safety impact to other organisations
-
- An approved derogation will be assessed upon changes in the scope of work and during the regular oversight cycle.
 - There is no implementation «light»



Applying for derogation

Management process K-112
Ausnahmebewilligung nach Part-IS
IS.OR.200(e) bearbeiten

billable expenses

Pre-assessment phase

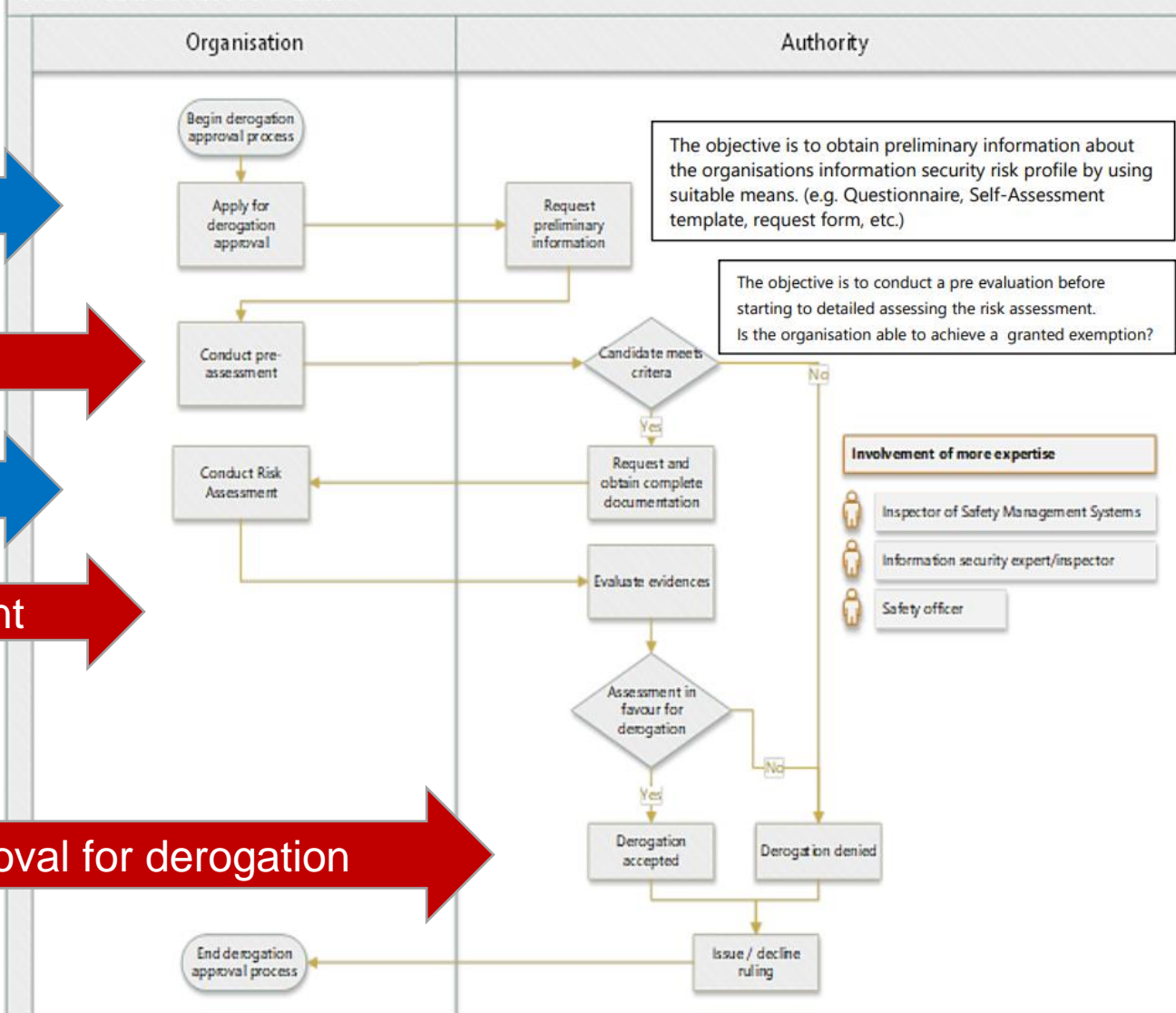
Verification of eligibility

Detailed Risk Assessment

Evaluate risk assessment

FOCA decides on approval for derogation

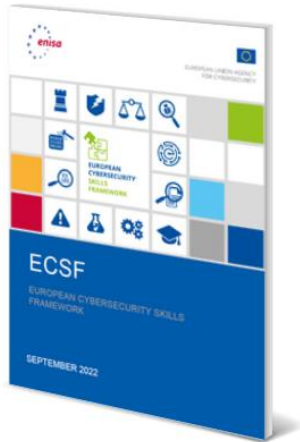
Cross Functional Flow chart



[Download extended guidance for derogation here](#)



Staff competencies



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

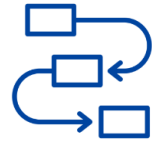
[European Cybersecurity Skills Framework Role Profiles Manual](#)

	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 \(NICE Framework\)](#)



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



































Qualifications of SME Group «Information Security»



SKILLS

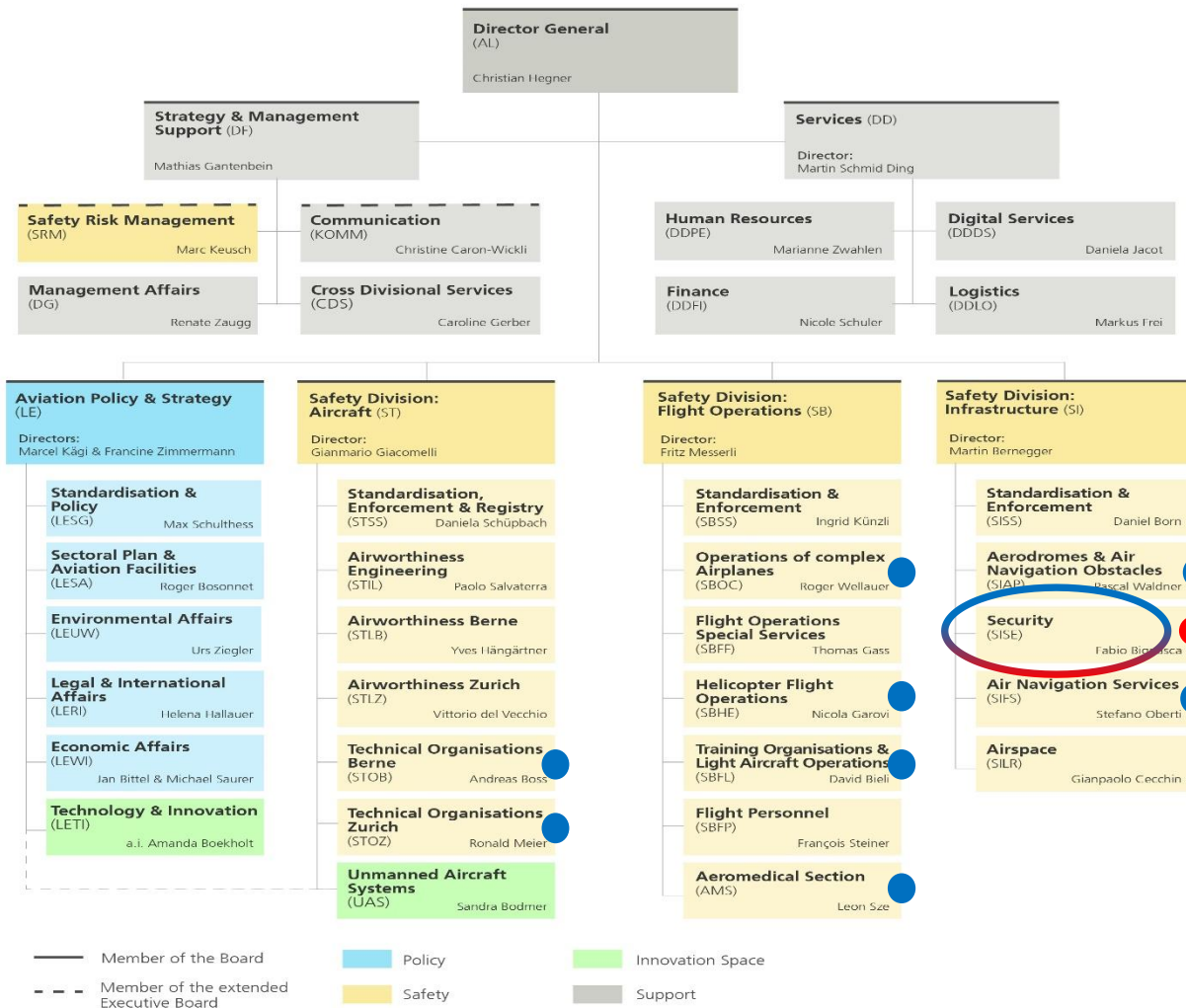
 available
 required

Product Safety and/or Security				
Enterprise Risk Management <ul style="list-style-type: none">GovernanceCyber				
Auditors / Compliance Management				
Cyber Experts / IT-Experts <ul style="list-style-type: none">Network Security and ArchitectureCloud Security, Endpoint Security, Encryption, IAM				
Project- and Change Management				
Expertise in communication <ul style="list-style-type: none">Training & e-learning				
Experts / Representatives of DOA, POA, MOA				
Quality assurance				

**NOW
HIRING!**



Organisation of Information Security at FOCA



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

01.10.2024

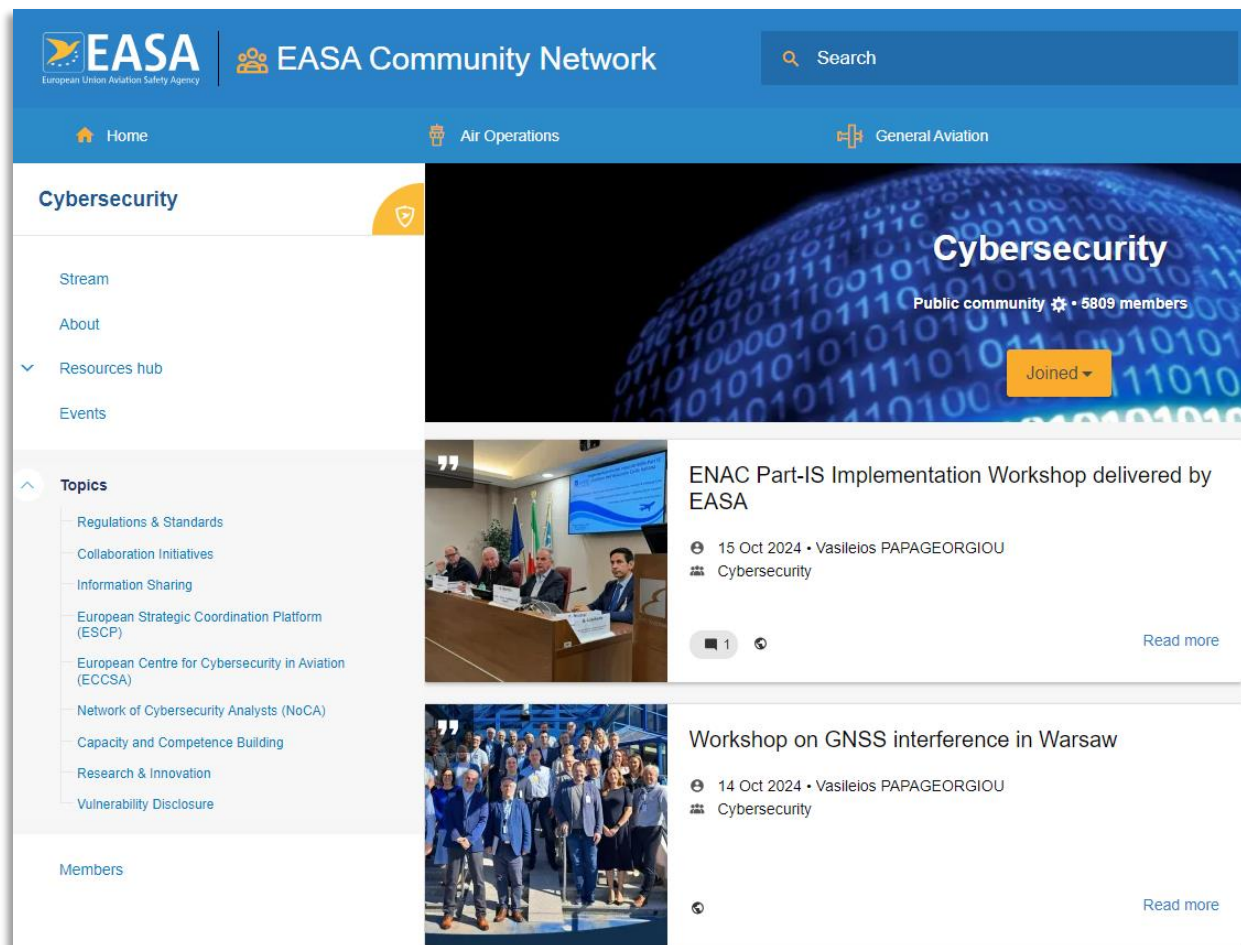


Where to find more guidance ?



[EASA Cyber Security Community](#)

- **FAQ**
- **Resource hub with guidance**
- **Events and more**





For those of you who missed...



- [Part IS Implementation Workshop 2024 - Day 1](#)
- [Part IS Implementation Workshop 2024 - Day 2](#)



Take aways



Do not implement Part-IS for compliance reasons. Do it to protect the aviation sector



Don't wait until application date. Start now !



Do not aim for perfection at initial stage. Maturity will gradually increase over time



Consult third party providers if necessary, which can assist you with expert knowledge in information security

Coffee Break



11:00 – 11:30

Speakers – Representatives of the industry

Flughafen Zürich



Fabio Morandi

Information Security Officer
Head ICT Security Services

Fabio Morandi has a background in business informatics and has been working as an IT executive in various industries for more than two decades.

He has been working for Flughafen Zürich AG since March 2012. He took over as Head of ICT Security in May 2021. After the successful implementation and certification of an ISMS according to ISO/IEC 27001, he is responsible for the development, advancement and implementation of the new cyber and information security strategy.

He is leading this in a programme of 11 strategic projects. At the same time, he is setting up and expanding the ICT security organisation of Flughafen Zürich AG.

Speakers – Representatives of the industry

Flughafen Zürich



Simon Maurer
SQS Lead Auditor
ICT Security Services

Simon Maurer is a recognised expert in the field of cyber security with a decades-long management career in computer science and telecommunications. He has successfully supported numerous companies in the implementation of information security standards such as ISO/IEC 27001 as an independent auditor and consultant for over 10 years.

As a managing director and former CEO in the software and IT outsourcing industry, he has gained extensive experience in managing large projects and providing strategic advice. His consulting mandates range from Switzerland's critical infrastructure to the healthcare sector and public administration.

He has been working at Zurich Airport since 2021, where he supports Fabio Morandi in particular in the strategic development of cyber and information security.

EASA Part-IS Implementation @ Flughafen Zürich



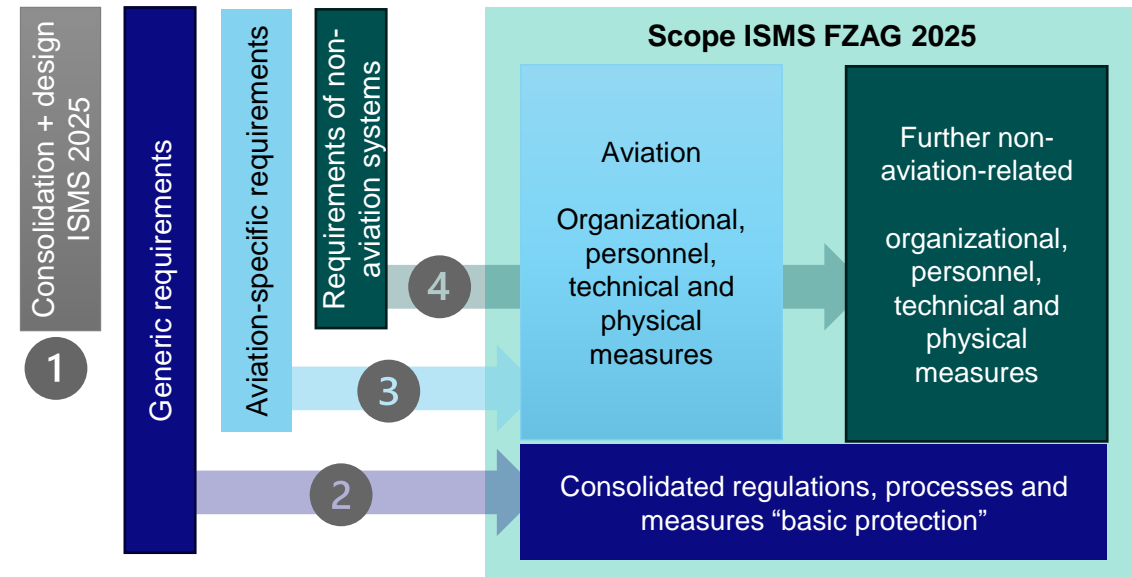
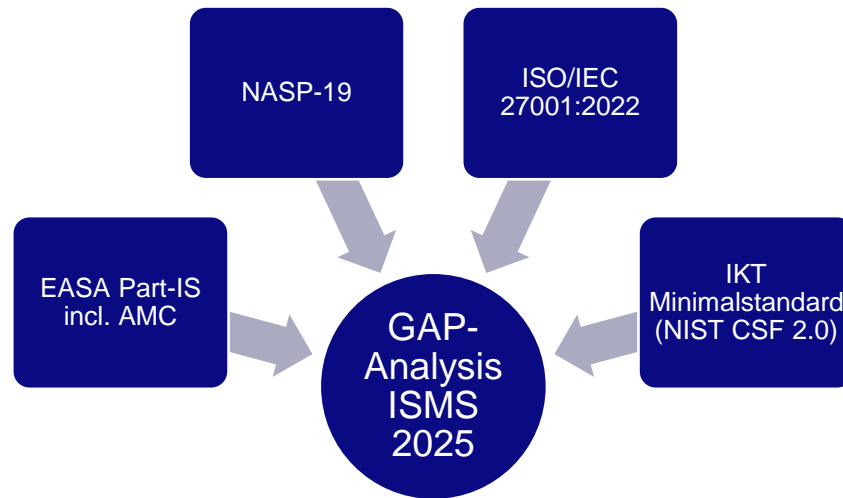
Fabio Morandi, Head ICT Security Services
November 2024

Flughafen Zürich

Where do we come from?

Year	Situation
2020	1 internal FTE ICT security and 3.5 FTE external consulting → Decision to build up internal competency and resources
2021	+2 internal resources → Reorganisation ICT security and ICT architecture
2022	ISO/IEC 27001:2013 certification of ISMS for ICT infrastructure → Start of »Cyber- and Information Security Strategy«
2023	Release of CIS23 Strategy in the board of Flughafen Zürich AG → Start of implementation of the project portfolio
2024	Final organisation: 15 internal FTE <ul style="list-style-type: none">• Cyber defence centre• ICT security architecture• ISMS & risk management• Identity & access management• IT service continuity management• 2 FTE longterm external consultants

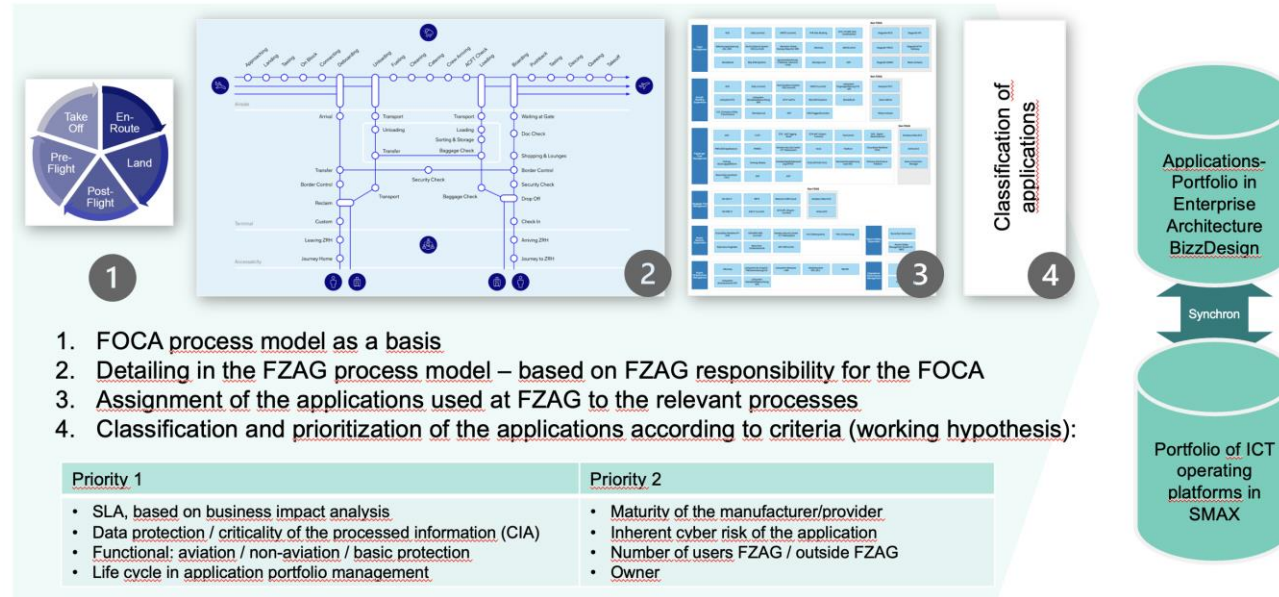
GAP-Analysis: The checklist consolidates 4 different frameworks



Sept. – Dec. 2024

Oct. 2024 – Oct. 2025

The asset scoping process has been set up and operationalized



- The application portfolio is to be continuously inventoried
- All applications are prioritized:
 - According to ICT SLA (mission-, business-critical, standard)
 - Data protection-relevant data
 - Life cycle of the application
 - Further criteria
- The operation of the process has been defined
 - Resource allocation
 - Iterative, annual implementation
 - Change management

Proof of rectification of the non-conformity 1 / November 2023:

The document of the asset scoping process and a list of the 200 identified applications including prioritization criteria were submitted by Fabio Morandi to FOCA on July 26th, 2024.

Systems chosen for GAP-Analysis ISMS 2025

System	Rationale	Interfaces	Stakeholder
Nova Alert NBK	Clear defined system-boundaries	Few	ICT
Netzeitsystem EVS_NLS	System in context OT	Few	OM and ICT
AOS	Large legacy system with a large number of business processes involved	Large number	ICT, large number of internal and external stakeholders

The aim of the GAP analysis:

1. Recognizing and addressing systemic deviations in relation to the consolidated requirements of:
 - EASA Part-IS (incl. AMC)
 - NASP-19
 - ISO/IEC 27001:2022
 - NIST CSF 2.0 (ICT minimum standard)
2. Definition of the design for the ISMS 2025

GAP-Analysis: Lessons learned

The working hypothesis was: We are looking for similarities between the applications so that we can define generic application-specific policies and fix the deviations step by step. Lessons learned:

1. Public procurement law – security is only one aspect of all evaluation criteria. Not every security requirement can be a deal breaker.
2. The technical heterogeneity of the applications and the OT is so great that individual security solutions must be found.

The ISMS Policy Framework will cover the generic ISMS requirements (in particular those of ICT operations) and thus the basic protection («Grundschutz»).

The information security of applications will follow the information security approach of the federal government.

Analogous to Hermes, we will define the security classification with a protection needs analysis («Schuban») and then the individual security solution with an ISDS concept. In doing so, “exceptions to policy” will have to be documented and approved.

Nächste Schritte und Zeitplanung der Umsetzung

<i>Development of a consolidated GAP checklist</i>	<i>Aug. 2024</i>
Conducting GAP analyses (systems: Nova Alert NBK, EVS_NLS network control system, AOS)	Sep.-Dec. 2024
End of ISMS 2025 Design	Dec. 2024
Implementation and certification of ISMS 2025 (Stage One Audit: July 2025)	Oct. 2025
FOCA execution notice for NASP-19 and EASA Part-IS	Oct. 16, 2025
Project end	Dec. 2025

A large commercial airplane, a Boeing 747-400, is being de-iced on a runway at dusk. The aircraft is white with a dark tail featuring the Star Alliance logo. The registration 'HB-LWO' is visible on the fuselage. Several ground support vehicles, including de-icing trucks, are positioned around the aircraft, spraying liquid onto its wings and fuselage. The runway is wet, reflecting the lights of the vehicles and the aircraft. The sky is a mix of blue and orange, indicating sunset or sunrise. The text 'Herzlichen Dank' is overlaid in the center of the image.

Herzlichen Dank

Kontakt

**Fabio Morandi**

Head ICT Security Services

Information, Communication and Technology

fabio.morandi@zurich-airport.com

+41 43 816 75 08

Speakers – Representatives of the industry



Veselin Monev
Information Security
Officer

Dr. Veselin Monev is a published author in information security, contributing several articles and co-authoring a textbook in the field.

He holds a Doctorate in Security Strategies and Policies and a Master's degree in Cybersecurity, along with professional certifications as a Certified Information Systems Auditor (CISA), CompTIA Security+, and ISO 27001 Lead Auditor.

In his current role as Information Security Officer at Pilatus Aircraft, he drives key security initiatives and provides advisement on security strategies across all organizational levels.

His responsibilities include implementing rigorous controls based on frameworks such as ISO 27001, ISO 27002, CIS Critical Security Controls, and NIST, and now leading the implementation of Part-IS.



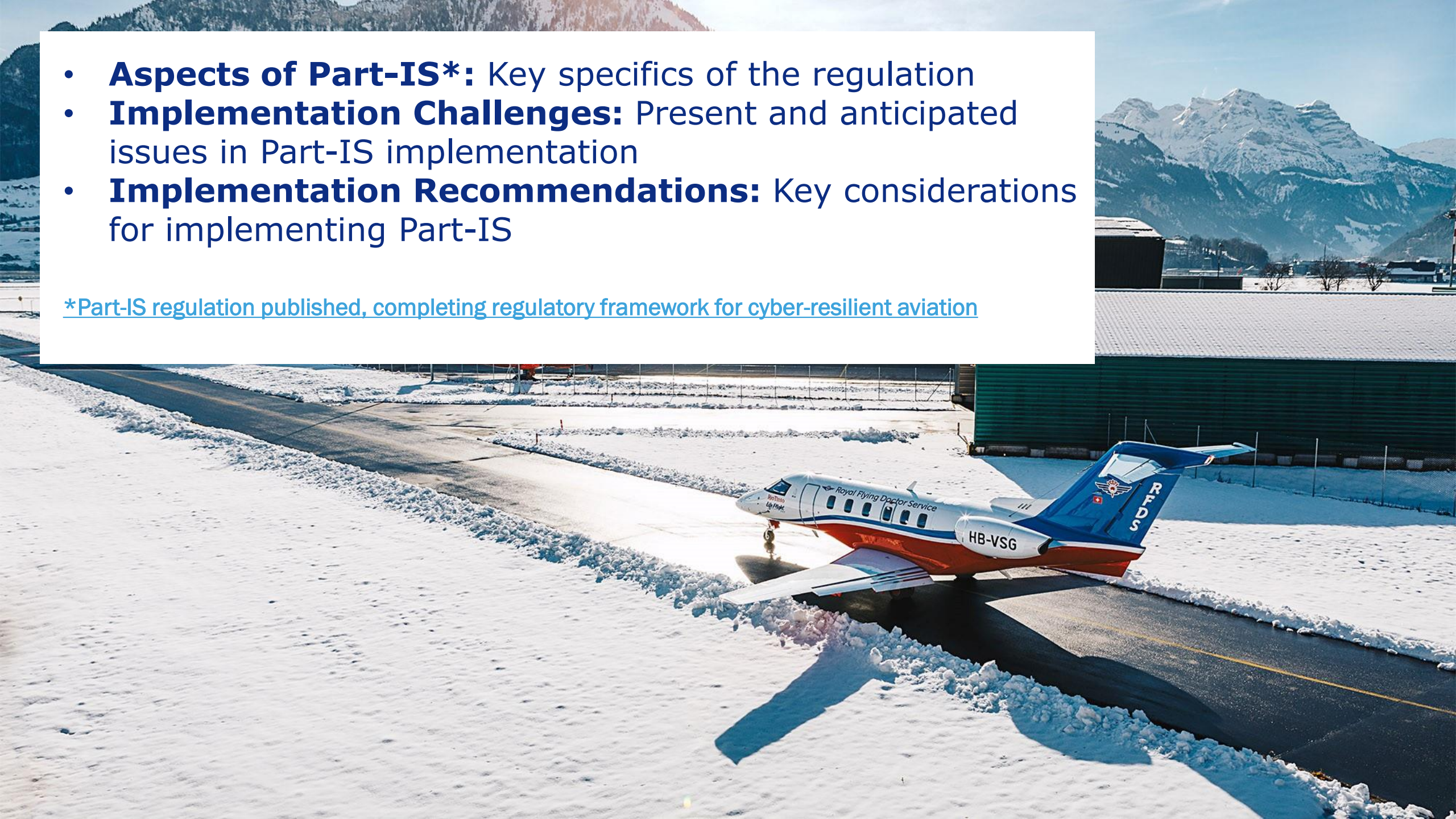
Aspects of Implementing Part-IS

Speaker: Dr. Veselin Monev



- **Aspects of Part-IS*:** Key specifics of the regulation
- **Implementation Challenges:** Present and anticipated issues in Part-IS implementation
- **Implementation Recommendations:** Key considerations for implementing Part-IS

[*Part-IS regulation published, completing regulatory framework for cyber-resilient aviation](#)



Aspects of Part-IS

Regulation and Guidance Publications

- **InfoSec dominant:** Mostly conventional InfoSec controls; InfoSec terminology.
- **EASA-style:** Some controls adjusted to EASA compliance practices (e.g. ISMM, reporting requirements).
- **Small:** Significantly fewer number of security controls compared to generic InfoSec frameworks (e.g. ISO 27001 and NIST SCF).
- **Complicated:** A heavy reading for the regulation(s) and guidance.
- **Target readers:** Interpretation primary by InfoSec specialists necessary.
- **Focal controls:** Risk Management, Security Incident Management, Vulnerability Management, Human Resource Security, Reporting.
- **Abstraction:** A mix of very abstract controls and some specific requirements.

Implementation Challenges (1)



- **Competences and team:** Teamwork of diverse specialists with ISMS, InfoSec, IT, OT, and aviation expertise.
- **Risk assessment and planning:** Initial ISMS-level of risk assessment to define specific security measures and an implementation plan.
- **Asset-oriented risk assessment:** Possible redesigning an existing risk management process.
- **Regulatory clarity:** Risk of potentially misaligned interpretation of requirements by EASA due to the lack of or different interpretation.
- **Collaboration:** Discovery and alignment with organizational entities.
- **Cultural change:** Potentially a significant cultural change.
- **Increased costs:** Ongoing operation resources for ISMS operation.

Implementation Challenges (2)



- **Revision of enterprise strategies and processes:** Adjustment or complete revision of InfoSec and non-InfoSec strategies and processes may be necessary.
- **Language:** Finding a common working and document language in a multinational setting.
- **Part-IS guidance limitations:**
 - Suitable for medium to large organizations only
 - No guidance for transforming/updating an existing ISMS
 - No guidance on supporting technical tools, e.g., a GRC tool
 - No methods, templates, and tools
 - InfoSec-expert level of interpretation necessary
 - High-abstraction degree of many guidelines

Implementation Recommendations (1)



- **Securing management buy-in and continuous leadership support.**
- Preliminary requirements analysis and ISMS implementation concept.
- **RFP and an evaluation scheme to select the right consultancy partner.**
- **A thorough project management plan with streams and work packages.**
- Stakeholder management.
- Roles and responsibilities.
- **Project schedule, issues, risks, and task management.**
- **SPOCs from all major organizational entities, and specific departments.**
- Resource availability planning.

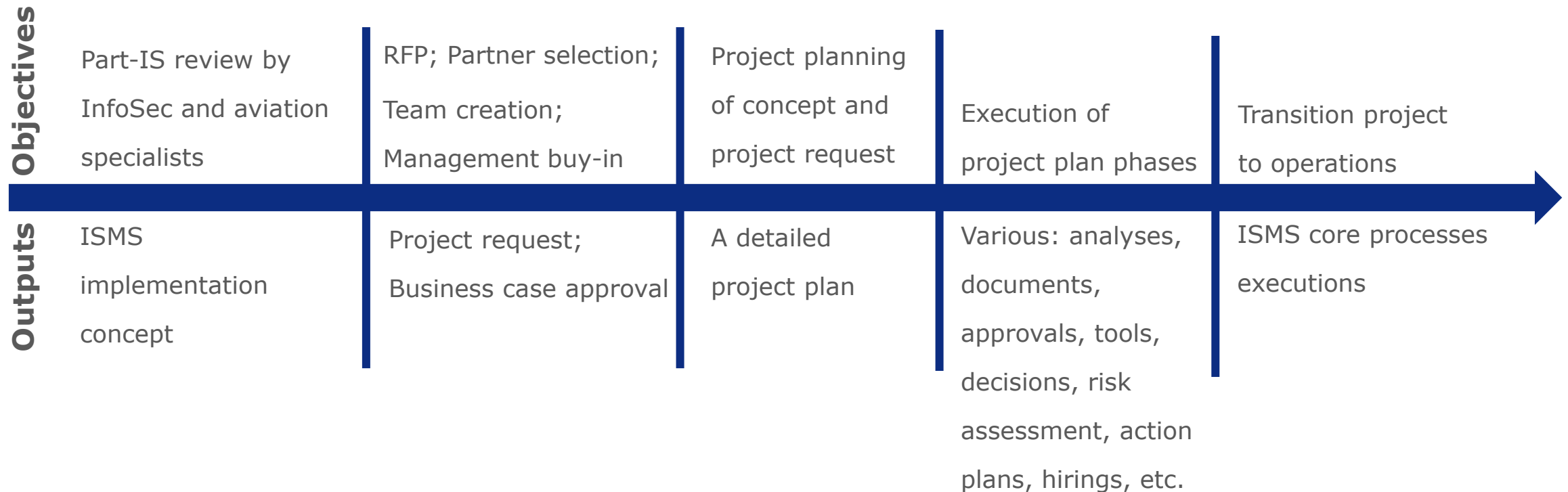
Implementation Recommendations (2)



- **A decision-making matrix, approved by the CEO / accountable manager.**
- GRC tool stream.
- Regular working, core team and steering meetings.
- **Initial risk assessment with asset discovery phase.**
- Project escalation processes.
- **Document discovery and review.**
- Subject-matter specialists and interviews.
- Review of existing tools.
- Definition of implemented security controls/requirements.

Implementation Recommendations (3)

Implementation milestones



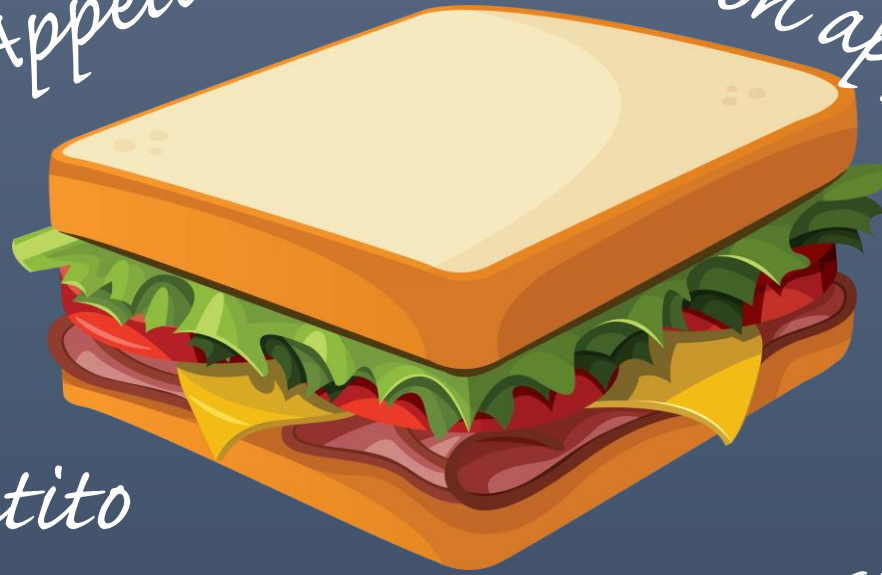
Questions and answers



Lunch Break

Guten Appetit

Bon appétit



Buon appetito

Enjoy your meal

13:00 – 14:00

Panel Discussion



1. What are the threat scenarios to get protected from?
2. ISMS vs. SMS What is the difference?

Participants choice:

- What competencies does our organisation need in order to meet the required criteria?

Questions & Answers



...because we care
the Swiss aviation industry is
cyber aware !

Conclusion

Implementing EASA Part-IS may not be as difficult as it seems for several reasons:



- ✓ **Clear Guidelines and Standards:** The Easy Access Rules of Part-IS provides well-defined guidelines specifically tailored for the aviation industry, simplifying compliance efforts.
- ✓ **Integration with Existing Compliance Frameworks:** Many aviation organisations already adhere to similar standards like ISO 27001 or other cybersecurity frameworks. These existing frameworks share foundational principles with Part-IS, allowing companies to adapt and build on current processes rather than start from scratch.
- ✓ **Availability of Support and Resources:** There is a lot of resources available on the internet which support organisations on an ISMS implementation. This, combined with the availability of consultants and third-party experts, can ease the transition by providing practical solutions and best practices.
- ✓ **Scalability:** An ISMS is scalable and suitable also for small organisations due to its adaptable, risk-based approach that can be tailored to the organisation's specific potential safety impact.



FOCA would like to thank all of you for your participation, contribution and attention to this event and wishes you a safe journey back home and a relaxing weekend.