EASA
European Union Aviation Safety Agency

together
4safety

Summer 2023

No Compromise on Safety

Are you Ready, Resilient and Responsive enough for this summer's challenges?

EASA
European Union Aviation Safety Agency

together4safety

Summer 2023

Cybersecurity Session

2 June 2023

No Compromise on Safety

Are you Ready, Resilient and Responsive enough for this summer's challenges?

Theme: No Compromise on Safety

Are you Ready, Resilient and Responsive enough for this summer's challenges? Rules provide the baseline, identify and manage your risks and don't forget to look after your people.

Ready

Have enough competent people and the resources you need to manage risks effectively so that you can ensure safe and effective operations.

Resilient

You are prepared for any operational challenges and external threats and support your staff to perform to their best. You don't push the boundaries of the rules and are on guard for risk transfer.

Responsive

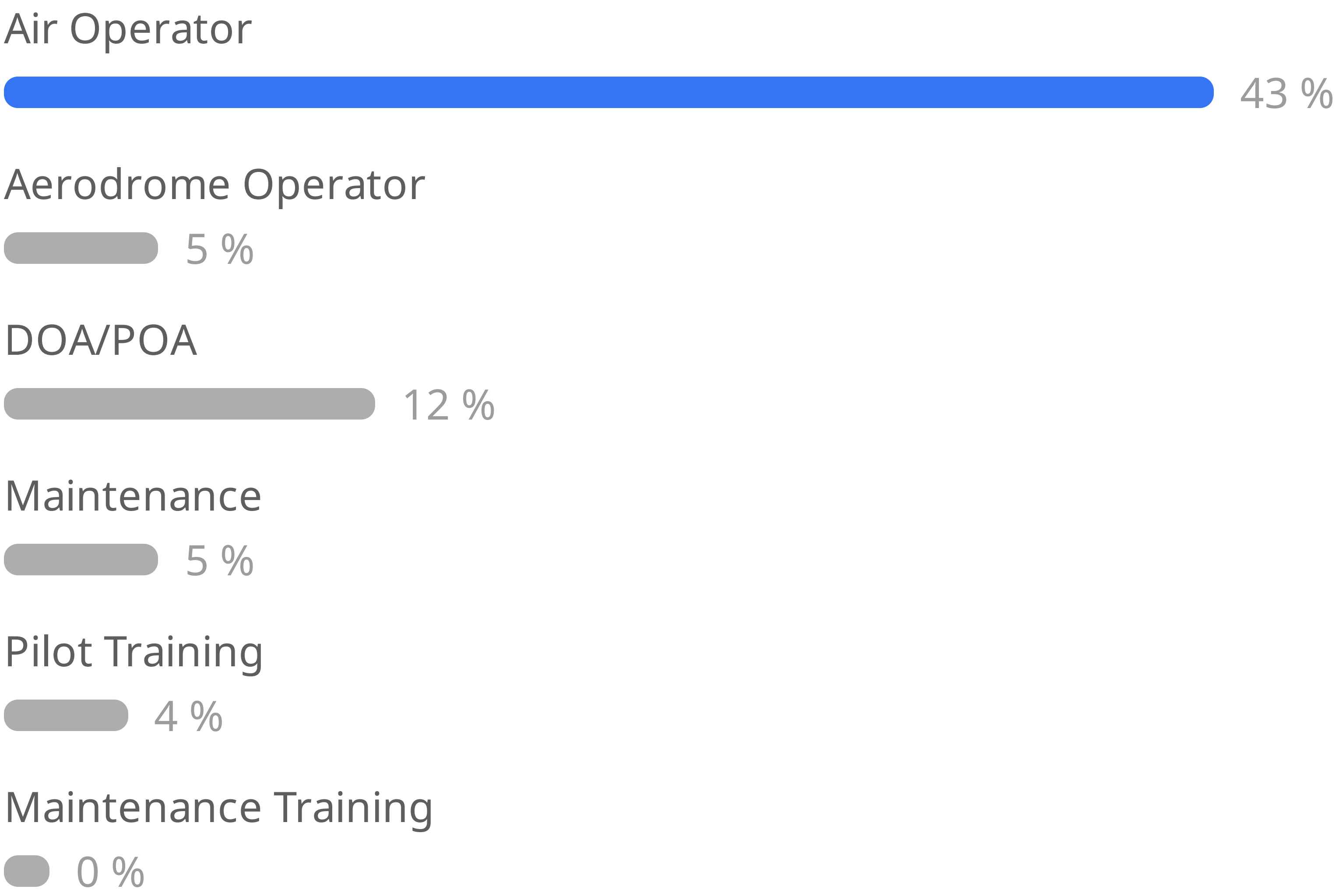
You have the mindset to promote safety reporting and encourage collaborative safety conversations. You react positively and quickly to challenges or changing situations and communicate effectively.

Multiple-choice poll

1. Which type of organisation are you working for?

(1/2)

1 3 3

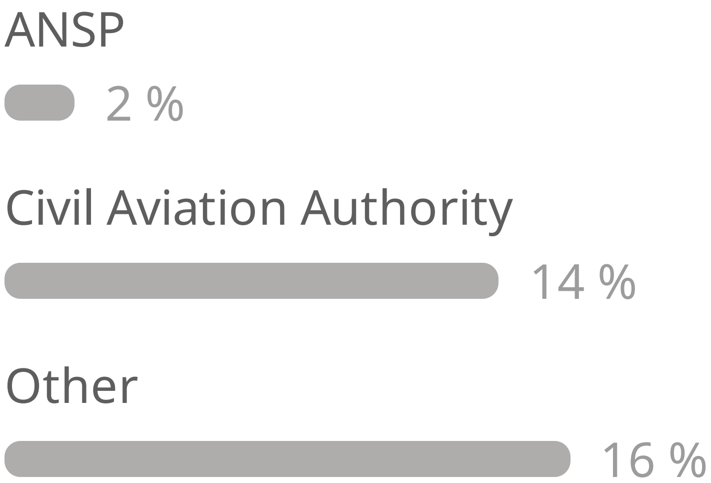


Multiple-choice poll

1. Which type of organisation are you working for?

(2/2)

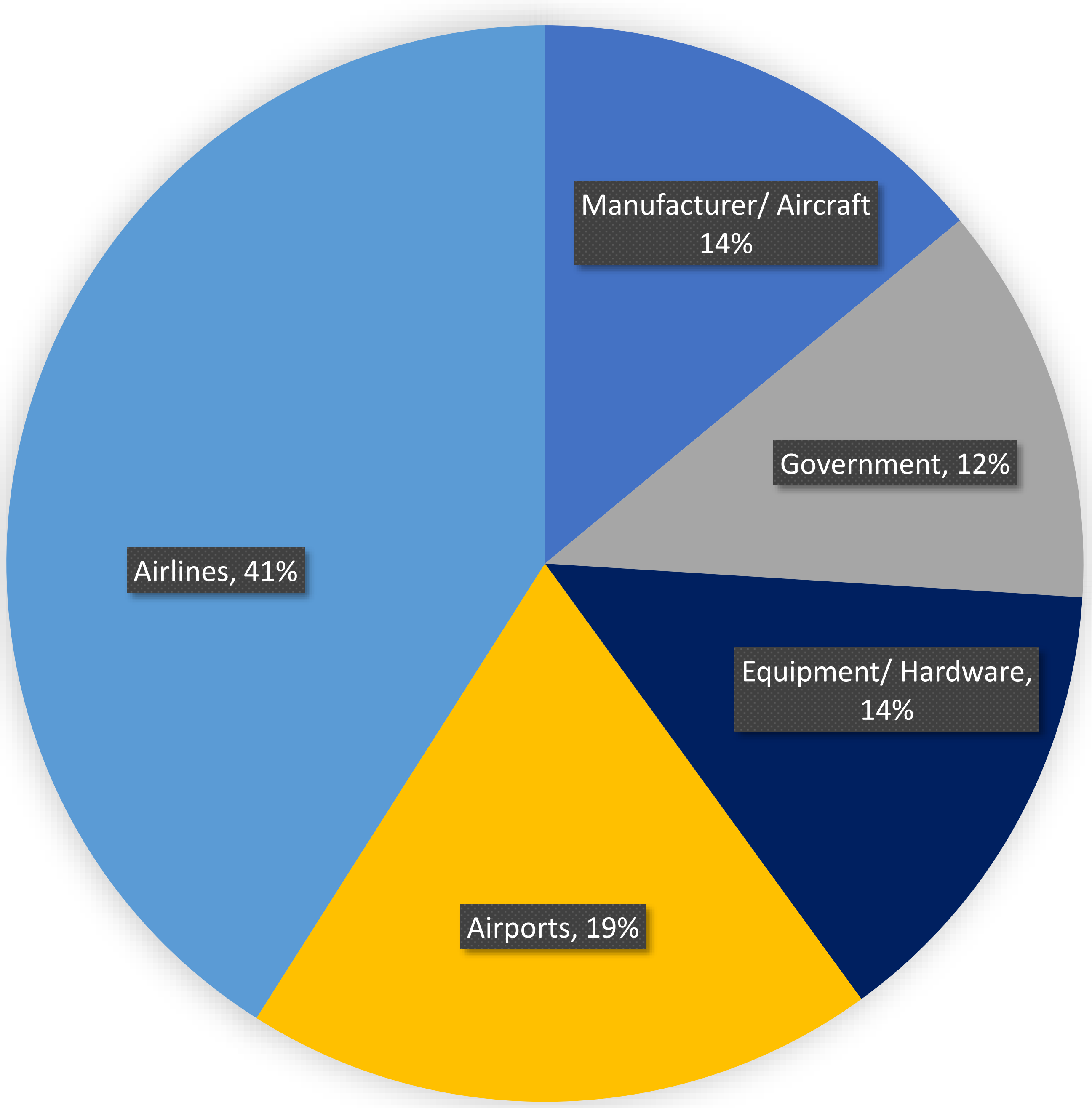
133



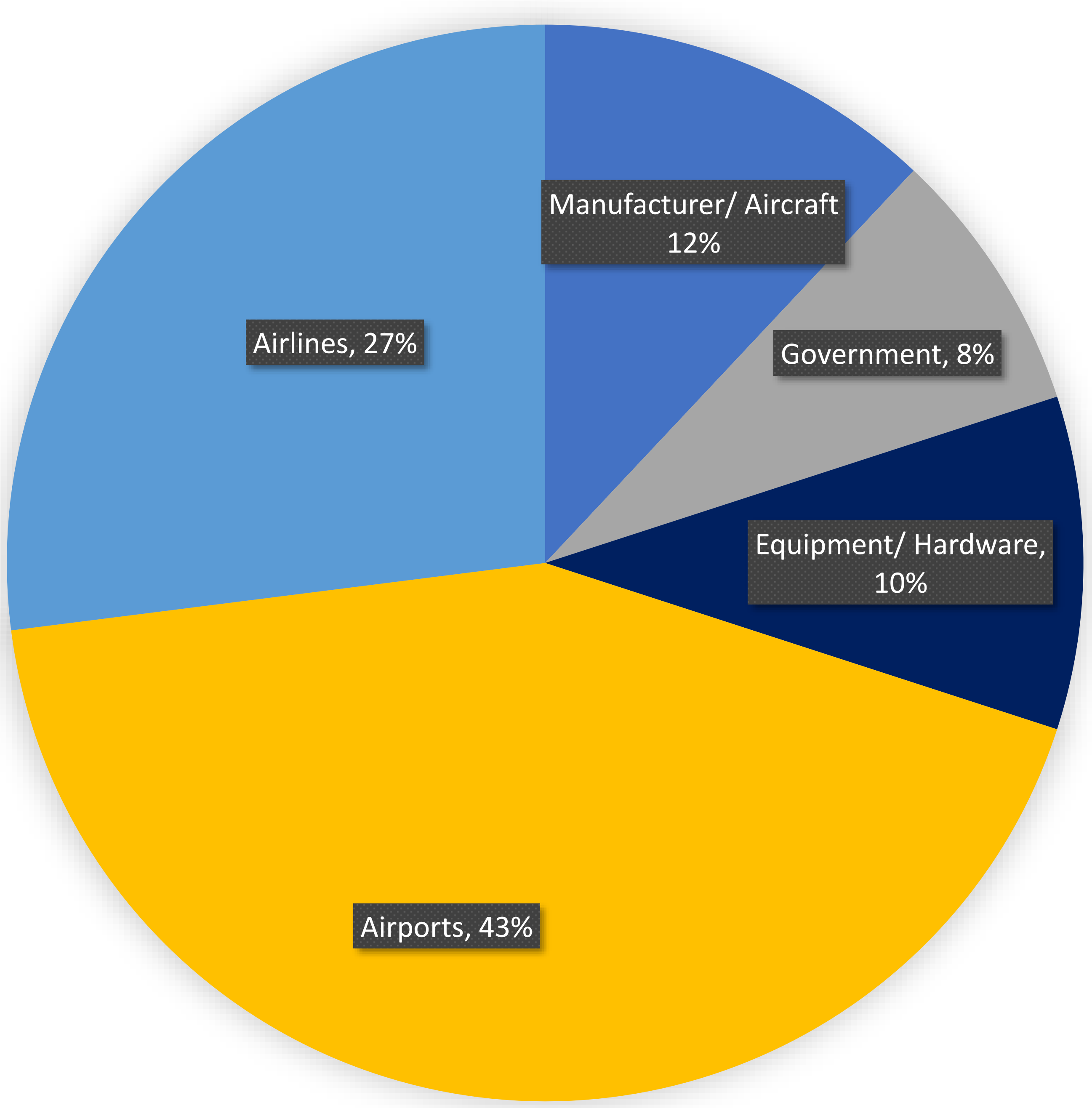
slido

Cybersecurity risks matters to you

116 attacks by target organisation in 2022



49 attacks by target organisation JAN- APR 2023



Theme: No Compromise on Safety

Are you Ready, Resilient and Responsive enough for this summer's challenges? Rules provide the baseline, identify and manag

don't forget to look after your people.

Cyber version

Ready

Your cybersecurity risks are known, assessed and mitigated; detection measures are in place.

Resilient

Following a cyberattack, you have processes ensuring continuation of safety critical activities and, possibly, full recovery.

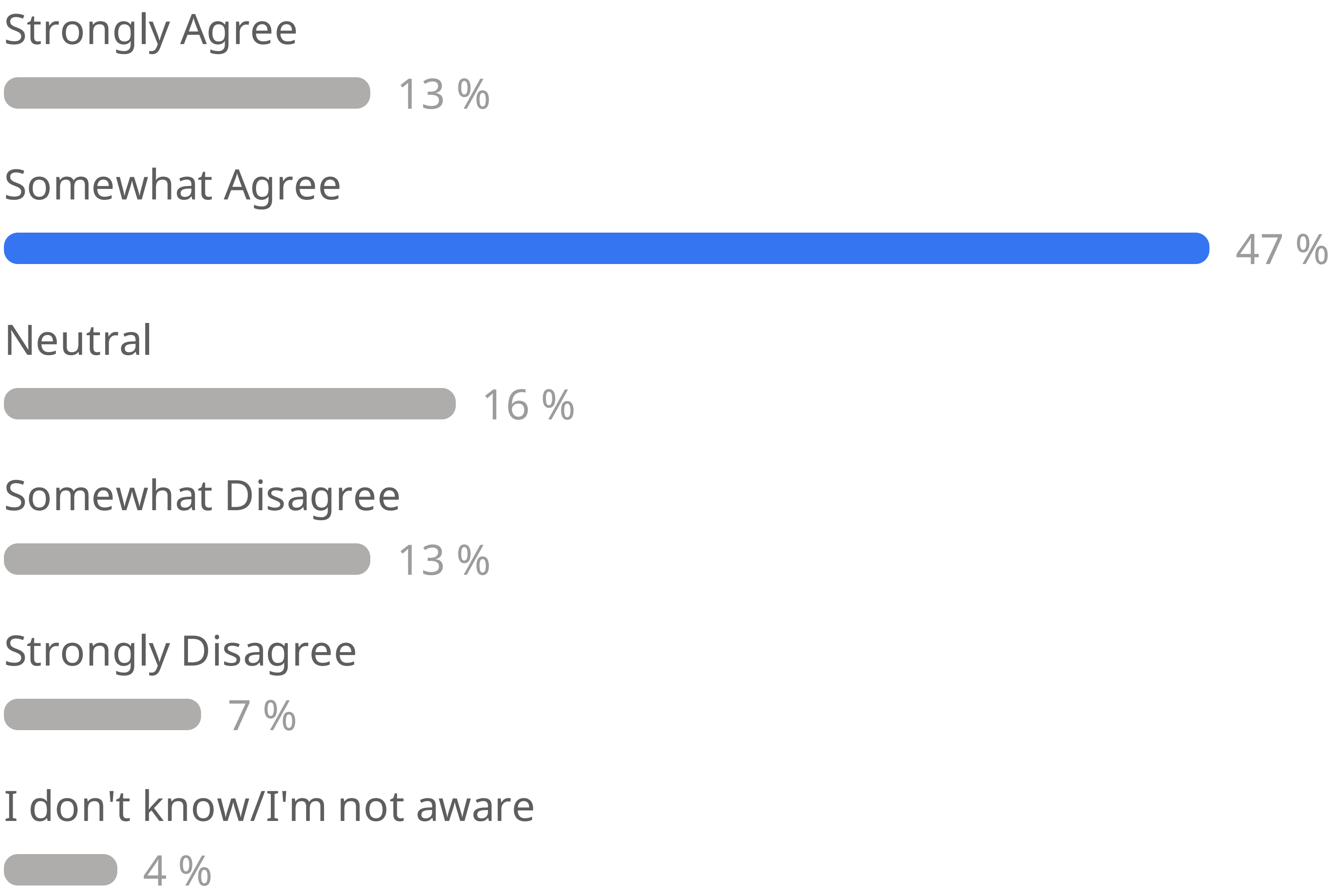
Responsive

Following a cyberattack, you have processes allowing removal of causes and adequate reporting

Multiple-choice poll

2. My organisation is Ready

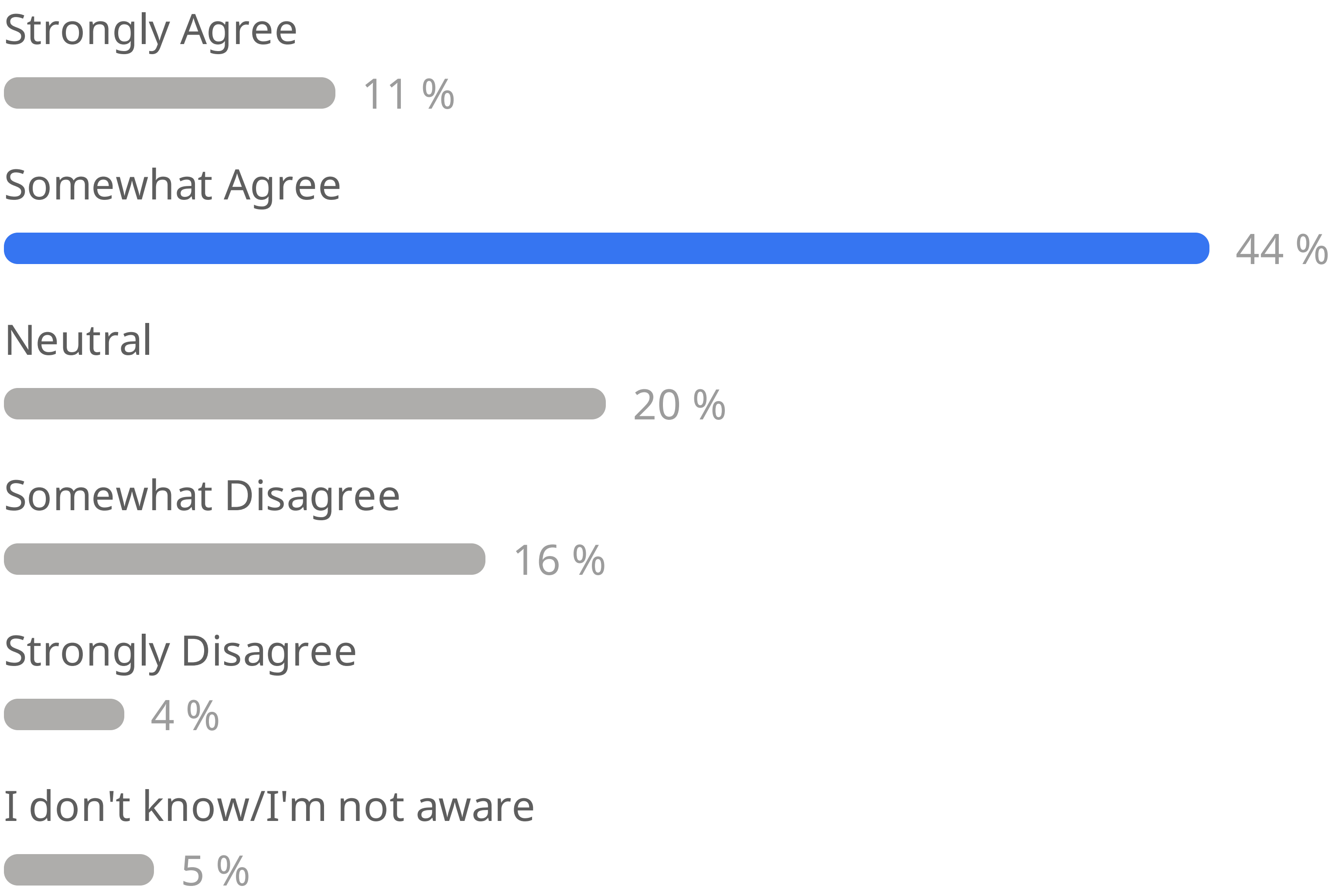
142



Multiple-choice poll

3. My organisation is Resilient

125

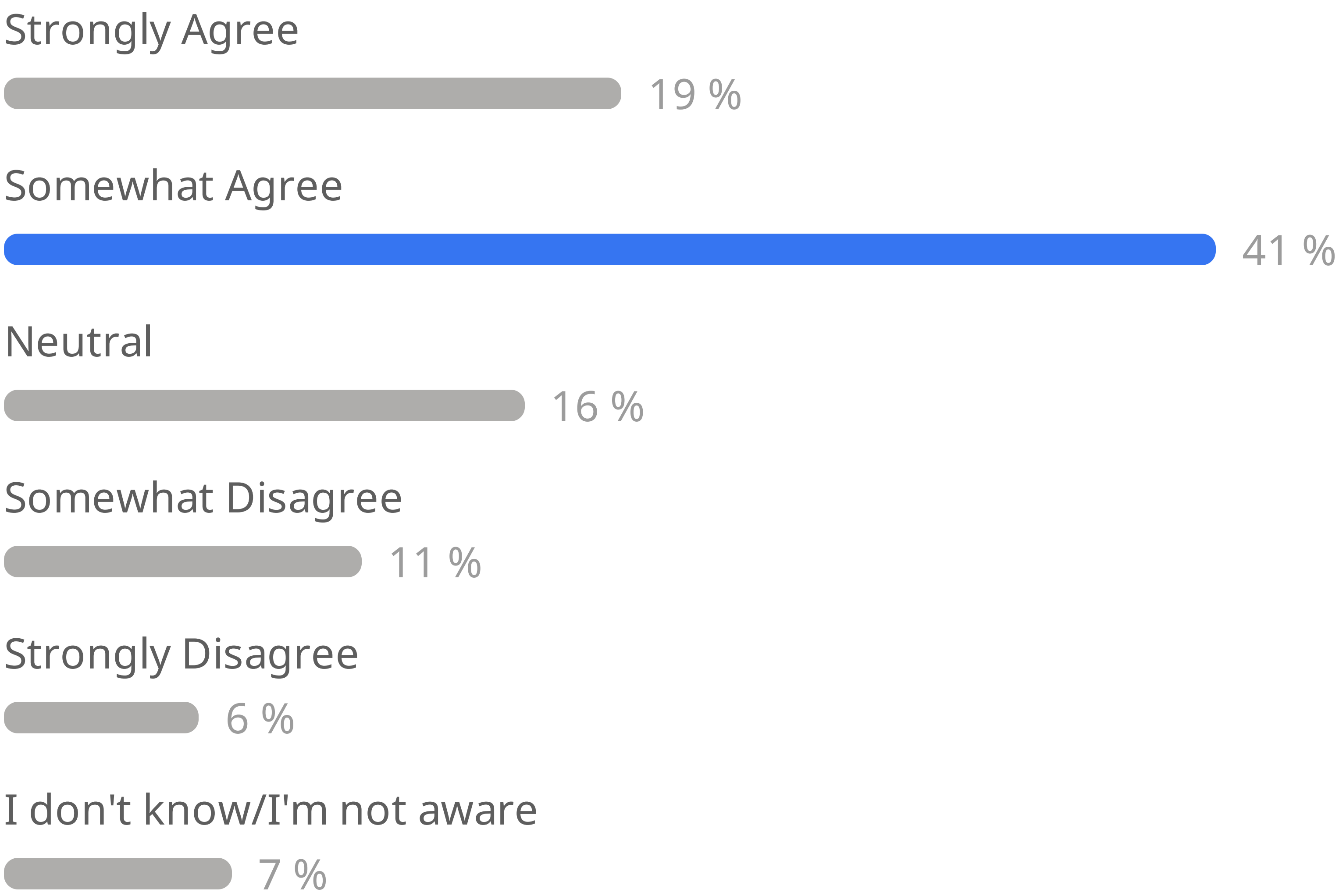


slido

Multiple-choice poll

4. My organisation is Responsive

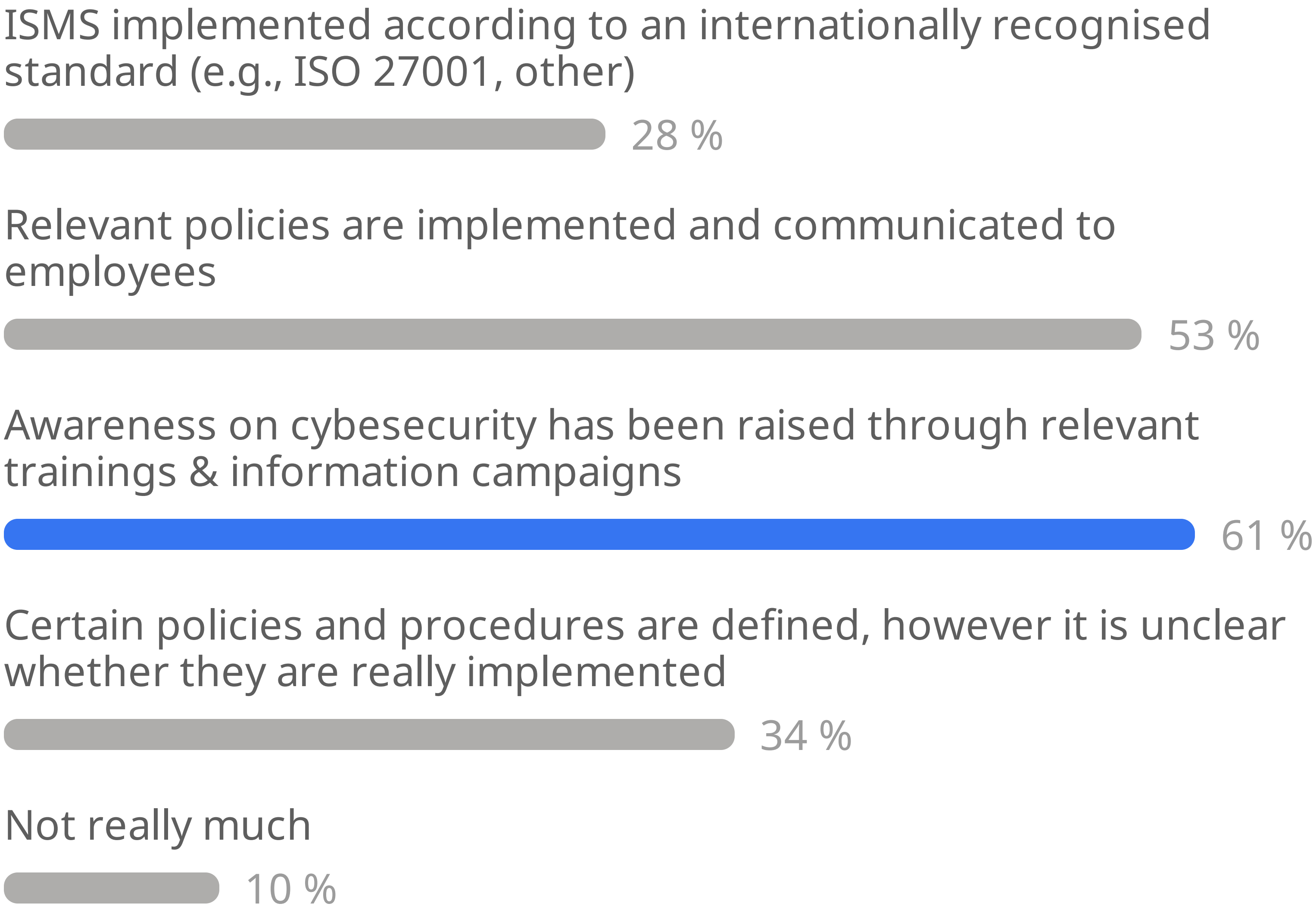
125



Multiple-choice poll (Multiple answers)

5. What have you done so far to achieve that status?

127



ISMS implemented according to an internationally recognised standard (e.g., ISO 27001, other)

28 %

Relevant policies are implemented and communicated to employees

53 %

Awareness on cybesecurity has been raised through relevant trainings & information campaigns

61 %

Certain policies and procedures are defined, however it is unclear whether they are really implemented

34 %

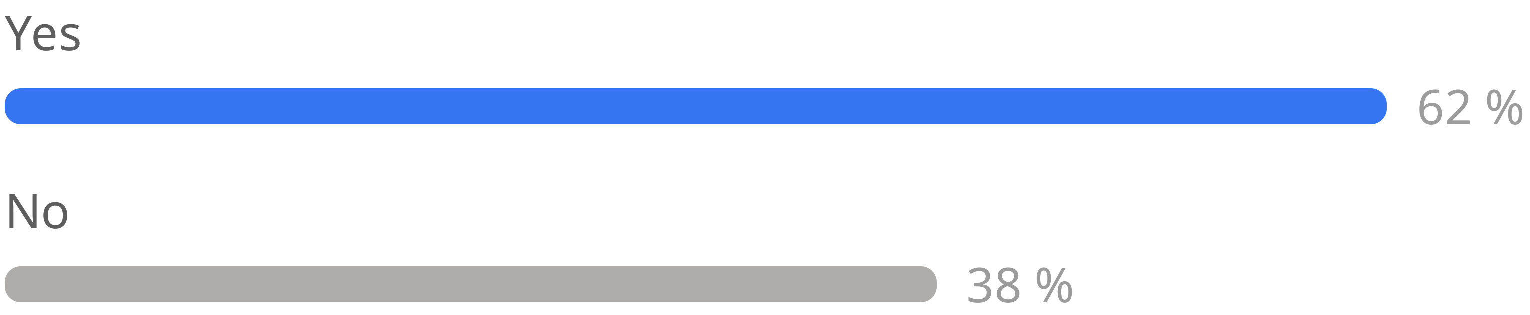
Not really much

10 %

Multiple-choice poll

6. Do you know what Part-IS is about?

140



EASA
European Union Aviation Safety Agency

Introduction to Part-IS

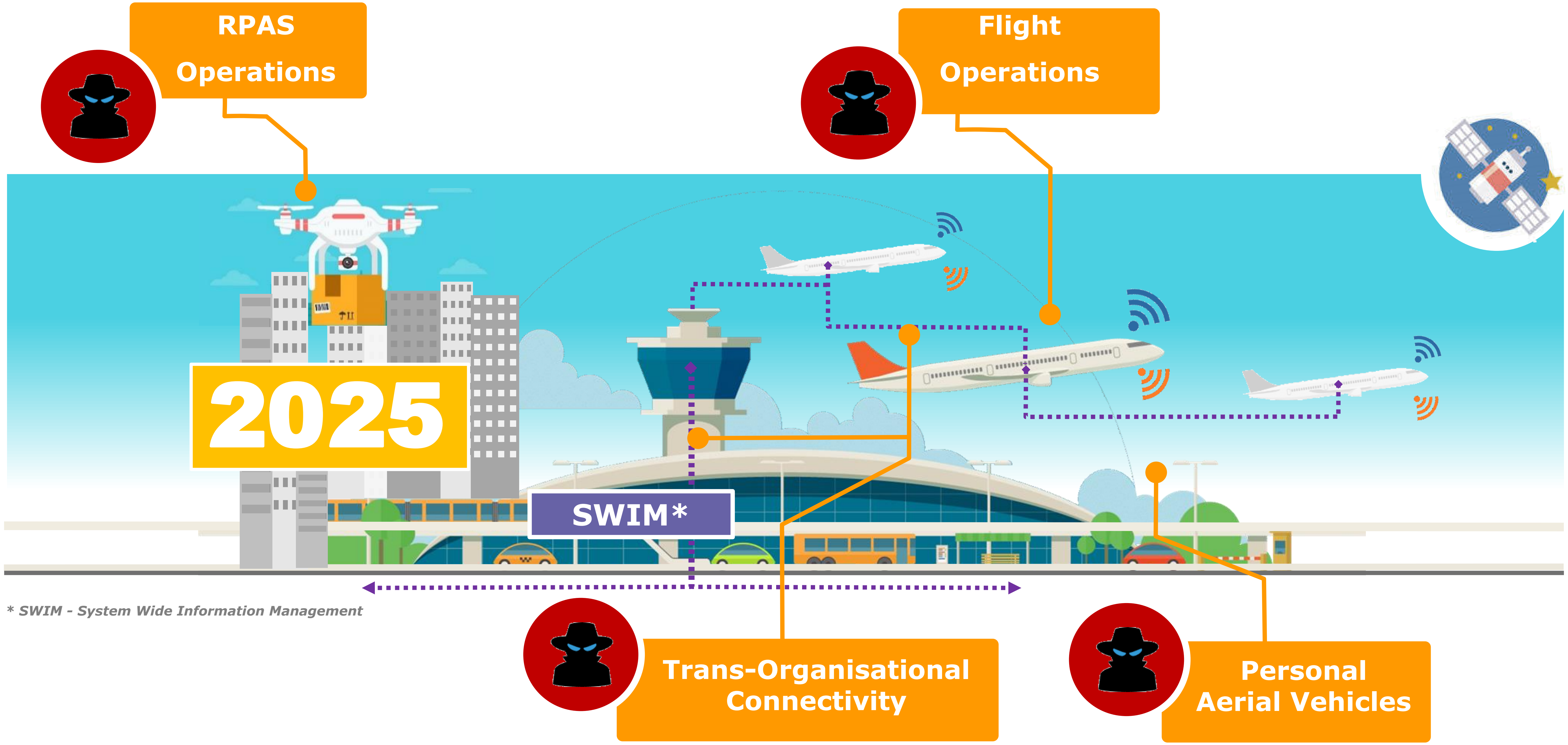
Gian Andrea Bandieri

Section Manager Cybersecurity in Aviation and Emerging Risks

2 June 2023

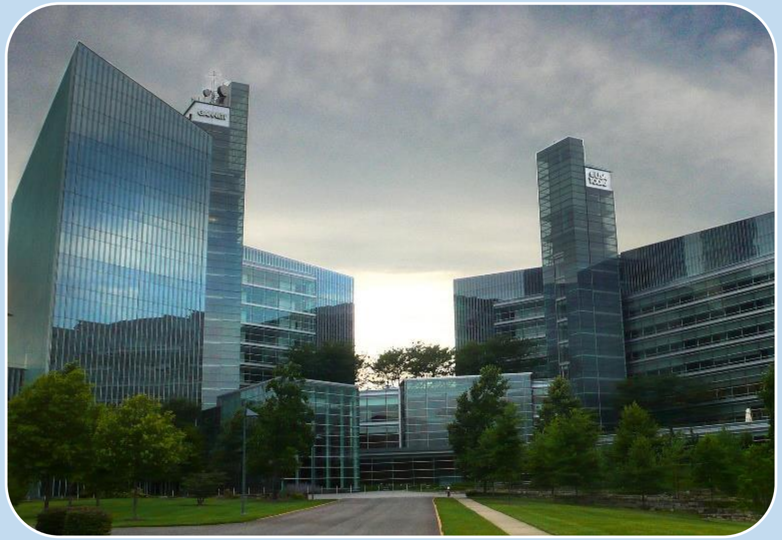
An Agency of the European Union

Aviation changes and so does the Risk



** SWIM - System Wide Information Management*

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)

- EASA proposal for a rule (**Part-IS**) published in June 2021
- Regulation(s) published in February 2023.
- AMC/GM under development

In progress

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

↻

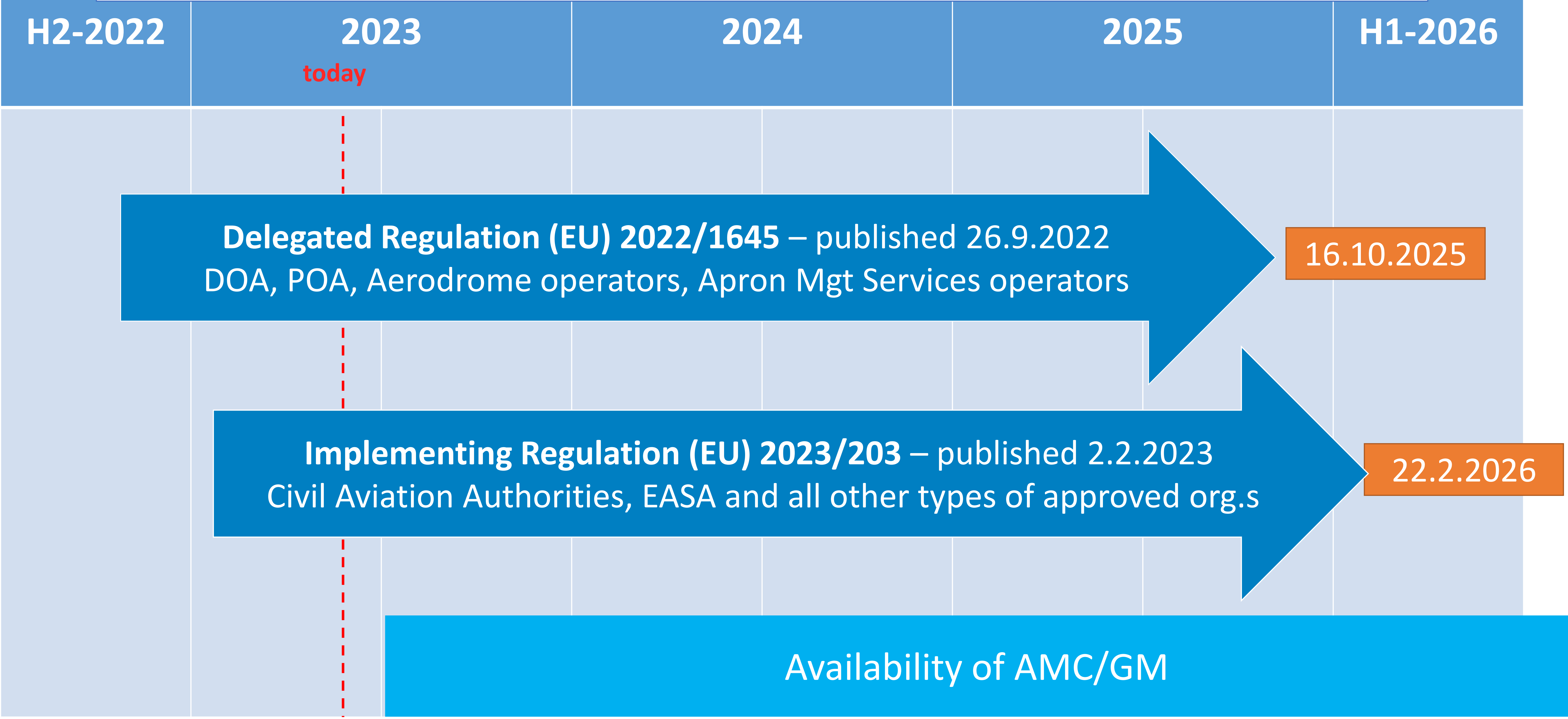
What we want to achieve with Part-IS

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	- **identify and manage** information security risks related to information and communication technology systems and data used for civil aviation purposes; - **detect** information security events, identifying those which are considered information security incidents; and - **respond** to, and **recover** from, those information security incidents

Proportionate to the impact on aviation safety

Part-IS implementation journey

Compliance is not protection - Protection is the objective



H2-2022 | 2023 | 2024 | 2025 | H1-2026

Delegated Regulation (EU) 2022/1645 – published 26.9.2022
DOA, POA, Aerodrome operators, Apron Mgt Services operators

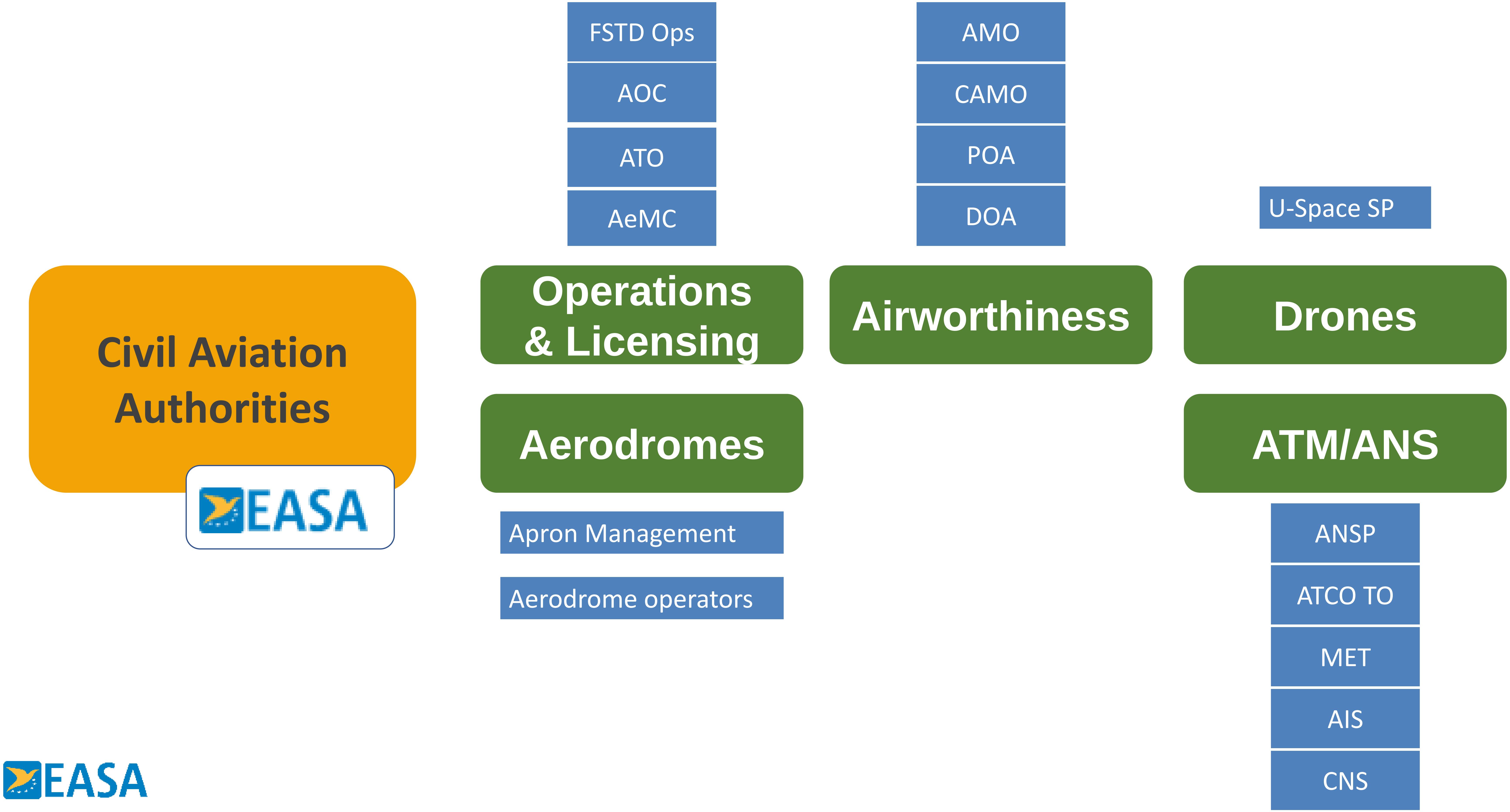
16.10.2025

Implementing Regulation (EU) 2023/203 – published 2.2.2023
Civil Aviation Authorities, EASA and all other types of approved org.s

22.2.2026

Availability of AMC/GM

Applicability of Part-IS



Civil Aviation Authorities

EASA

Operations & Licensing
- FSTD Ops
- AOC
- ATO
- AeMC

Airworthiness
- AMO
- CAMO
- POA
- DOA

Drones
- U-Space SP

Aerodromes
- Apron Management
- Aerodrome operators

ATM/ANS
- ANSP
- ATCO TO
- MET
- AIS
- CNS

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

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

Main Elements for Part-IS

Basic Regulation

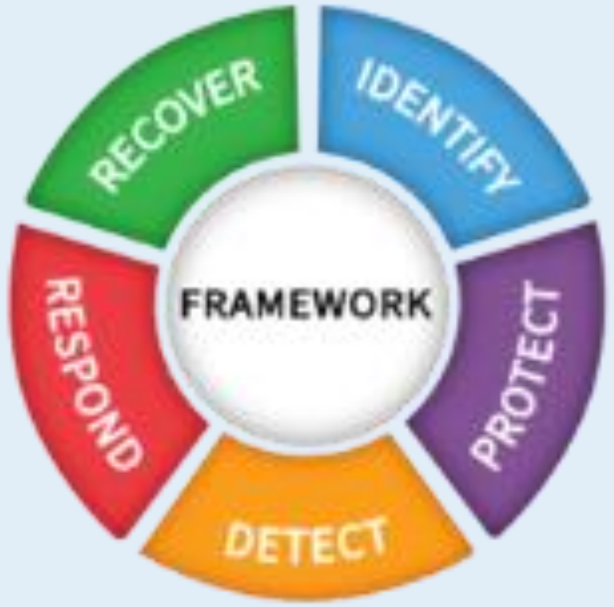
- Acceptable Safety Risks
- Record-keeping
- Personnel Requirements

ISO 2700x

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

NIST Cyber Security Framework

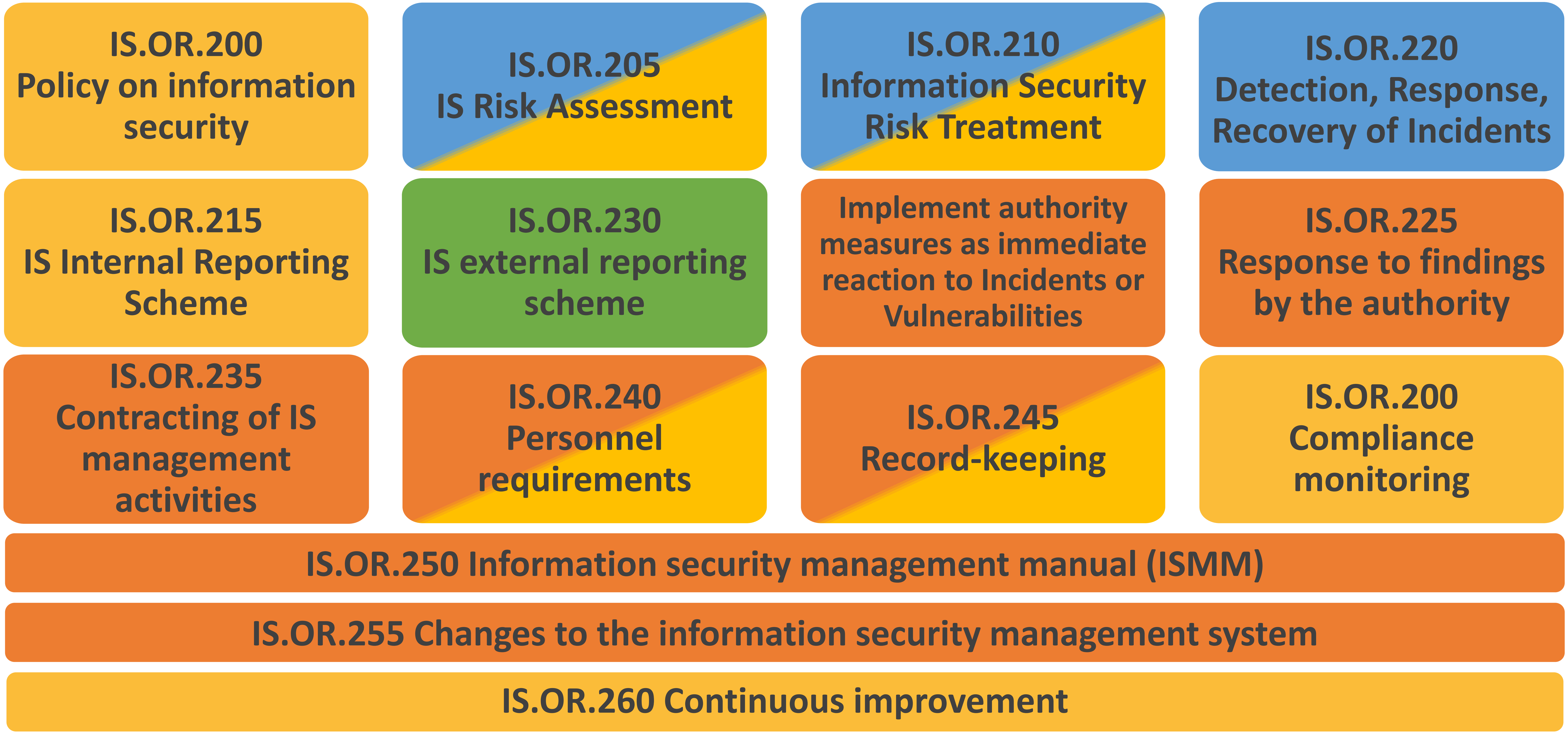
- Information Security Risk Treatment
- Information Security Incidents — Detection, Response, and Recovery



Reporting Regulation

- Information Security External Reporting Scheme

The ISMS in Part-IS



IS.OR.200 Policy on information security

IS.OR.205 IS Risk Assessment

IS.OR.210 Information Security Risk Treatment

IS.OR.220 Detection, Response, Recovery of Incidents

IS.OR.215 IS Internal Reporting Scheme

IS.OR.230 IS external reporting scheme

Implement authority measures as immediate reaction to Incidents or Vulnerabilities

IS.OR.225 Response to findings by the authority

IS.OR.235 Contracting of IS management activities

IS.OR.240 Personnel requirements

IS.OR.245 Record-keeping

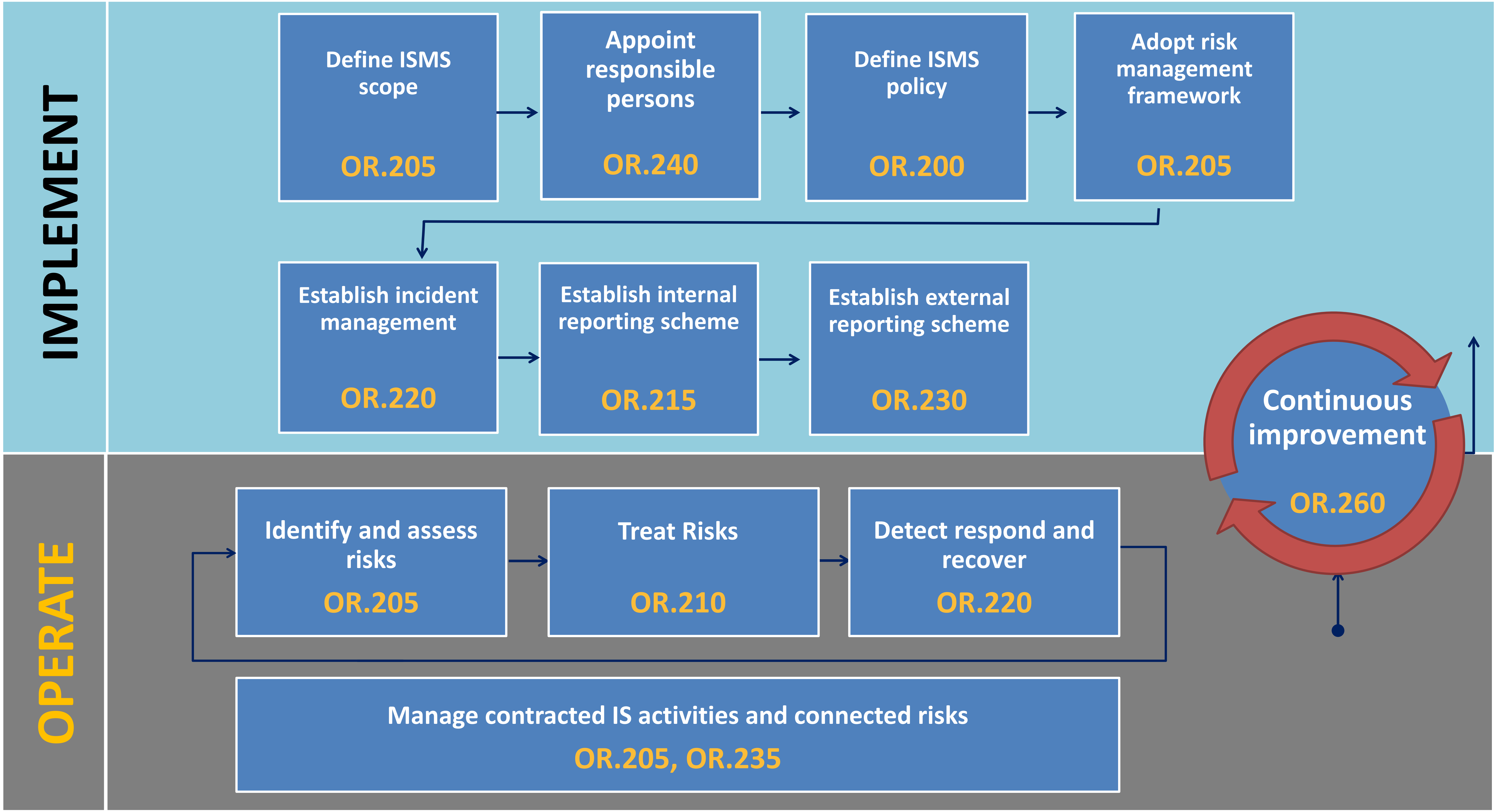
IS.OR.200 Compliance monitoring

IS.OR.250 Information security management manual (ISMM)

IS.OR.255 Changes to the information security management system

IS.OR.260 Continuous improvement

Colour code: NIST Framework | ISO 2700x | Basic Reg. | Reporting Reg.



IMPLEMENT

Define ISMS scope
OR.205

Appoint responsible persons
OR.240

Define ISMS policy
OR.200

Adopt risk management framework
OR.205

Establish incident management
OR.220

Establish internal reporting scheme
OR.215

Establish external reporting scheme
OR.230

Continuous improvement
OR.260

OPERATE

Identify and assess risks
OR.205

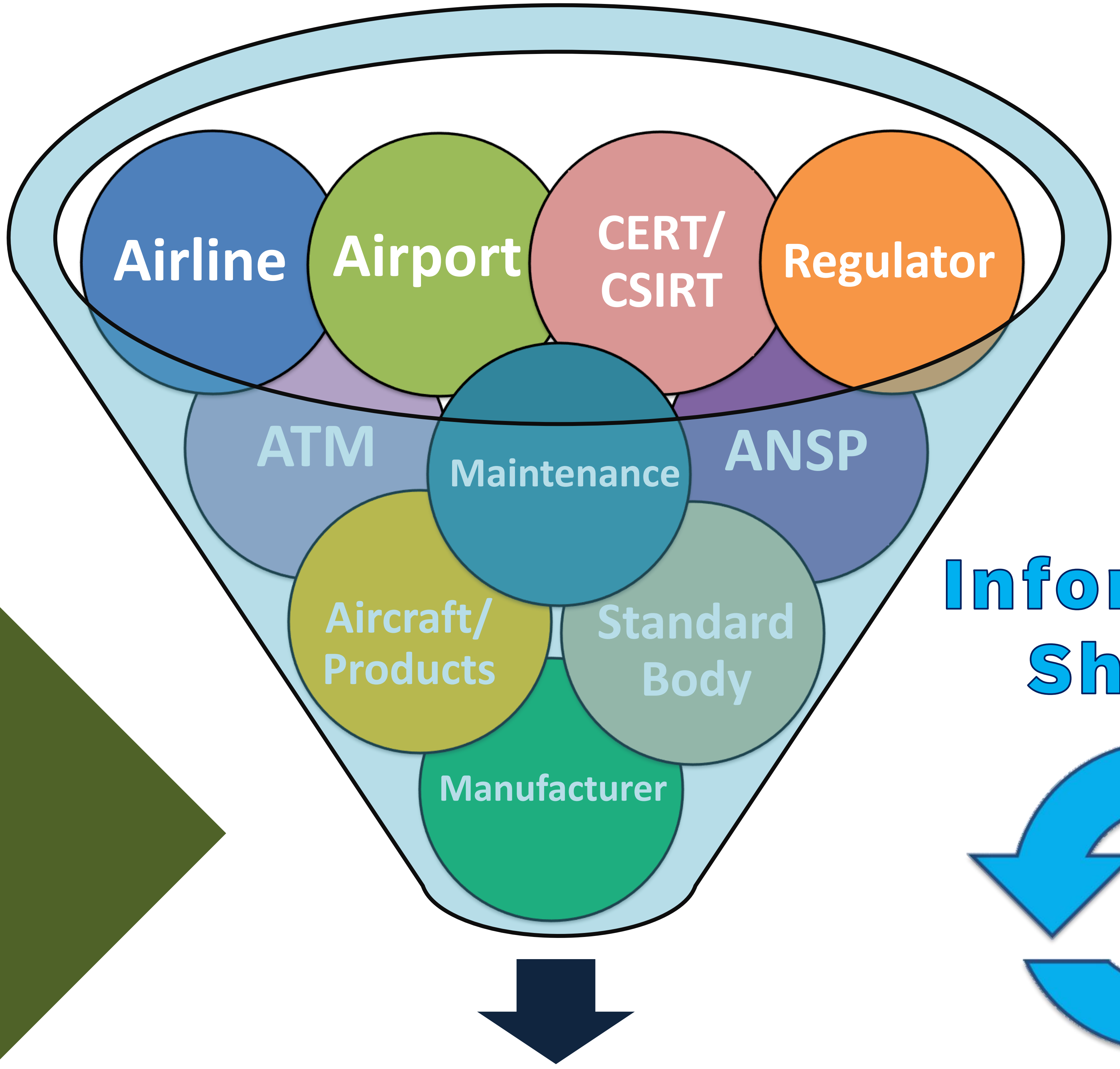
Treat Risks
OR.210

Detect respond and recover
OR.220

Manage contracted IS activities and connected risks
OR.205, OR.235

Information sharing

The cyber threat landscape is constantly shifting in the aviation sector…
It is important to share in a timely & rapid manner
cybersecurity related information

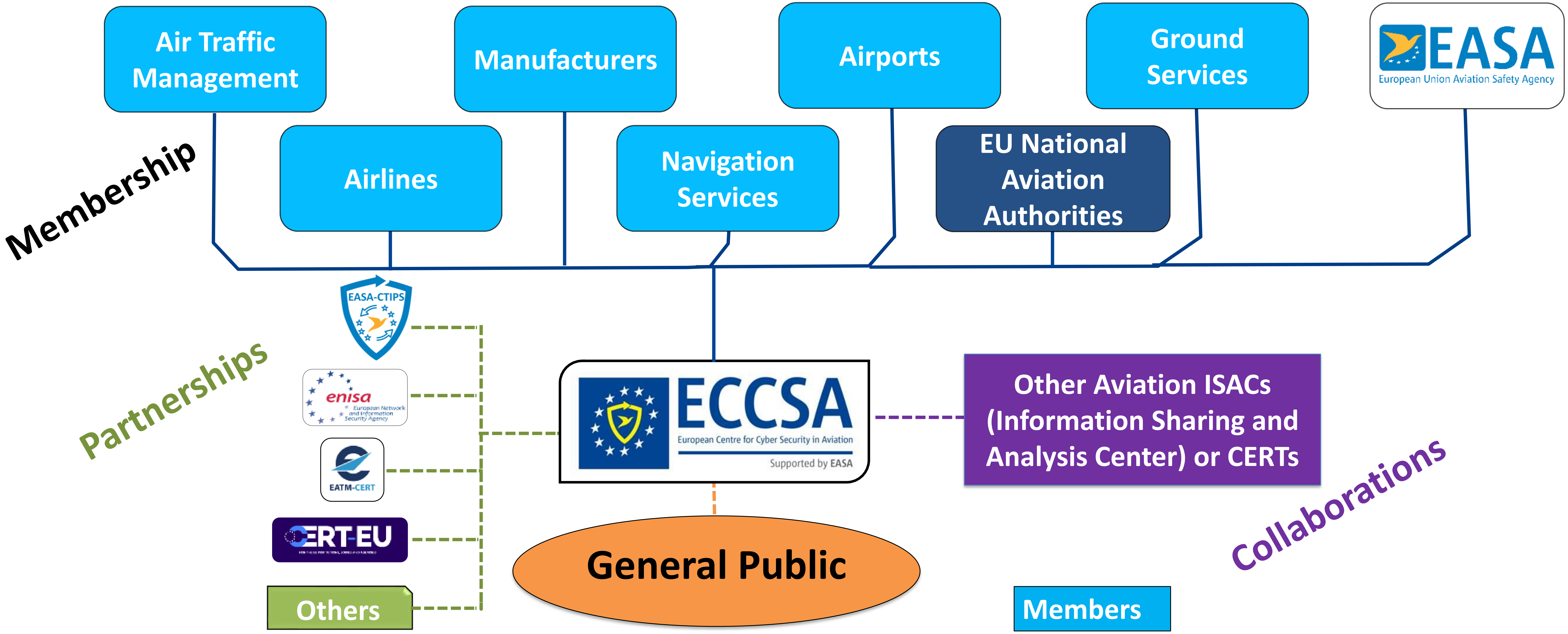


Information Sharing

Resilience of the Aviation ECO-System

EASA

ECCSA (European Center for Cybersecurity in Aviation)


Membership
Air Traffic Management
Manufacturers
Airports
Ground Services
EASA
European Union Aviation Safety Agency
Airlines
Navigation Services
EU National Aviation Authorities
Partnerships
EASA-CTIPS
enisa
European Network and Information Security Agency
EATM-CERT
CERT-EU
Others
ECCSA
European Centre for Cyber Security in Aviation
Supported by EASA
Other Aviation ISACs (Information Sharing and Analysis Center) or CERTs
Collaborations
General Public
Members

Since 2017 Members: 13 + 24	Non profit & free of charges	Fully voluntary initiative	Aviation Industry & NAAs	Vulnerability Disclosure Process

EASA
European Union Aviation Safety Agency

Thank you for your attention !

YEARS

Contact us at:

cybersec@easa.europa.eu

Join our Community:
https://www.easa.europa.eu/community/cybersecurity

easa.europa.eu/connect

Your safety is our mission.

An Agency of the European Union

Alidaunia

SINCE 1976

EASA SAFETY WEEK 2023
DAY 4 - CYBER/SECURITY

02-06-2023

LEONARDO PRATT & WHITNEY DART AEROSPACE SKYTRAC TRONAIR ROBINSON HELICOPTER COMPANY LAVERSAB GOODYEAR START PAC IS-BAO

Member of CISQ Federation
RINA
CERTIFIED MANAGEMENT SYSTEM
ISO 9001 - ISO 14001
ISO 45001 ISO 22301

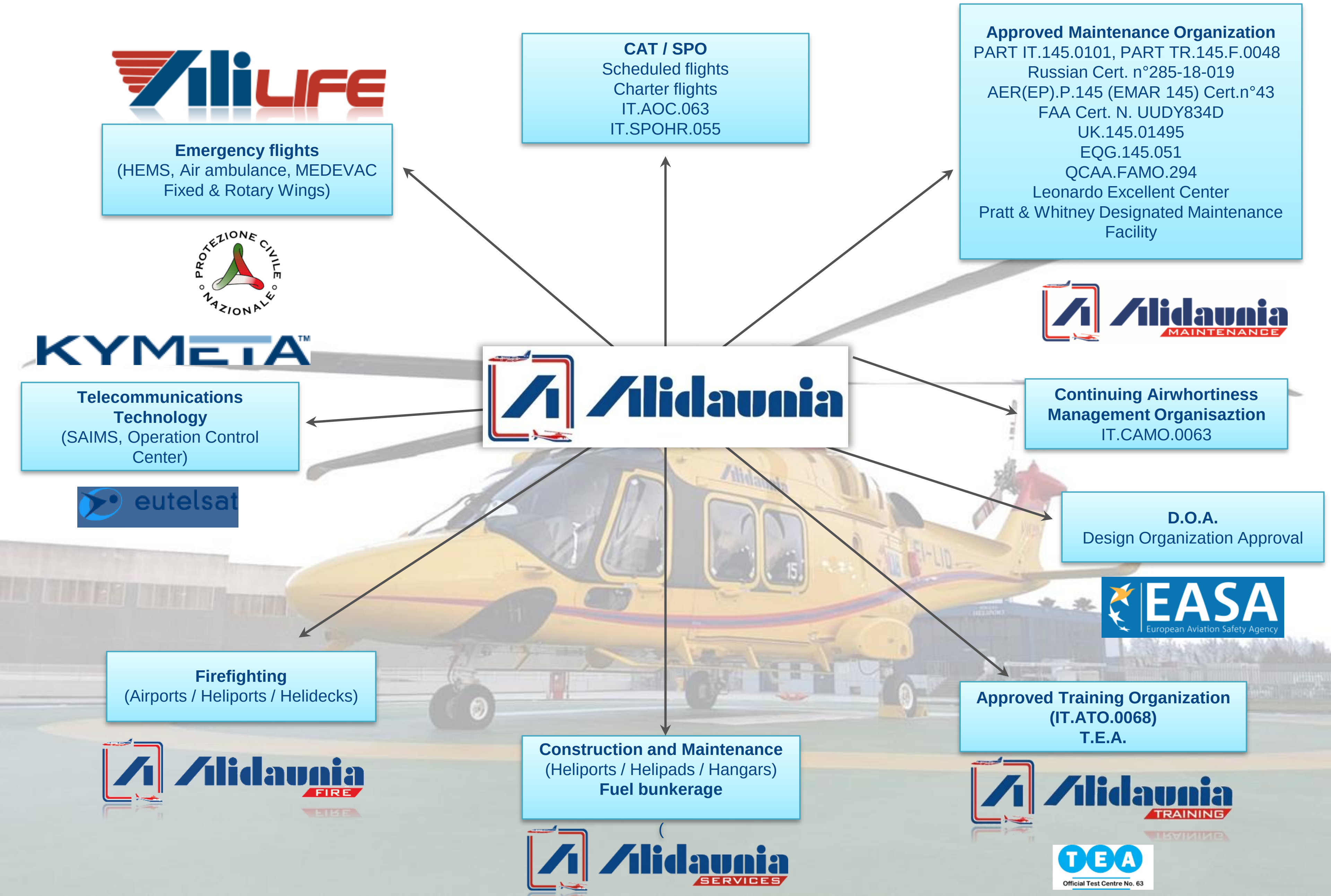
AGENDA

- ALIDAUNIA - Company Overview
- Mission first; Safety and Security always!
- How to be Ready
- How to be Resilient
- How to be Responsive
- Next Steps
- Advice for friends

ALIDAUNIA - Company Overview

- Established in Foggia on the 1st March 1976 as fixed wing operator of aerial work.
- In 1984 began helicopters era.
- Since 1986 is the only Italian company operating line scheduled flights with helicopters.
- Since 2002 Alidaunia is Agusta Westland (today LHD) Authorized Service Center. In 2017 became one of six companies worldwide to be awarded the title of LHD Excellence Service Center
- LHD exclusive fleet.
- In December 2019 officially recognized as DMF Designated Maintenance Facility for Pratt & Whitney engines.

ALIDAUNIA GROUP



Emergency flights
(HEMS, Air ambulance, MEDEVAC
Fixed & Rotary Wings)

CAT / SPO
Scheduled flights
Charter flights
IT.AOC.063
IT.SPOHR.055

Approved Maintenance Organization
PART IT.145.0101, PART TR.145.F.0048
Russian Cert. n°285-18-019
AER(EP).P.145 (EMAR 145) Cert.n°43
FAA Cert. N. UUDY834D
UK.145.01495
EQG.145.051
QCAA.FAMO.294
Leonardo Excellent Center
Pratt & Whitney Designated Maintenance Facility

Telecommunications Technology
(SAIMS, Operation Control Center)

Continuing Airwhortiness Management Organisaztion
IT.CAMO.0063

D.O.A.
Design Organization Approval

Firefighting
(Airports / Heliports / Helidecks)

Construction and Maintenance
(Heliports / Helipads / Hangars)
Fuel bunkerage

(

Approved Training Organization
(IT.ATO.0068)
T.E.A.

There was a feeling, better to say a need

Ensure that our Air System (Air Platform + Ground Support System) is continuously:

- **Airworthy:** means safe for flight;
- **Resilient:** means that we are able to complete our tasks preventing, or responding to a threat notwithstanding the breach to our security perimeter and/ or degradation of system components;
- **Secure:** means it is free from those threat conditions that could impact our operations with unwanted consequences

BOUNDARIES

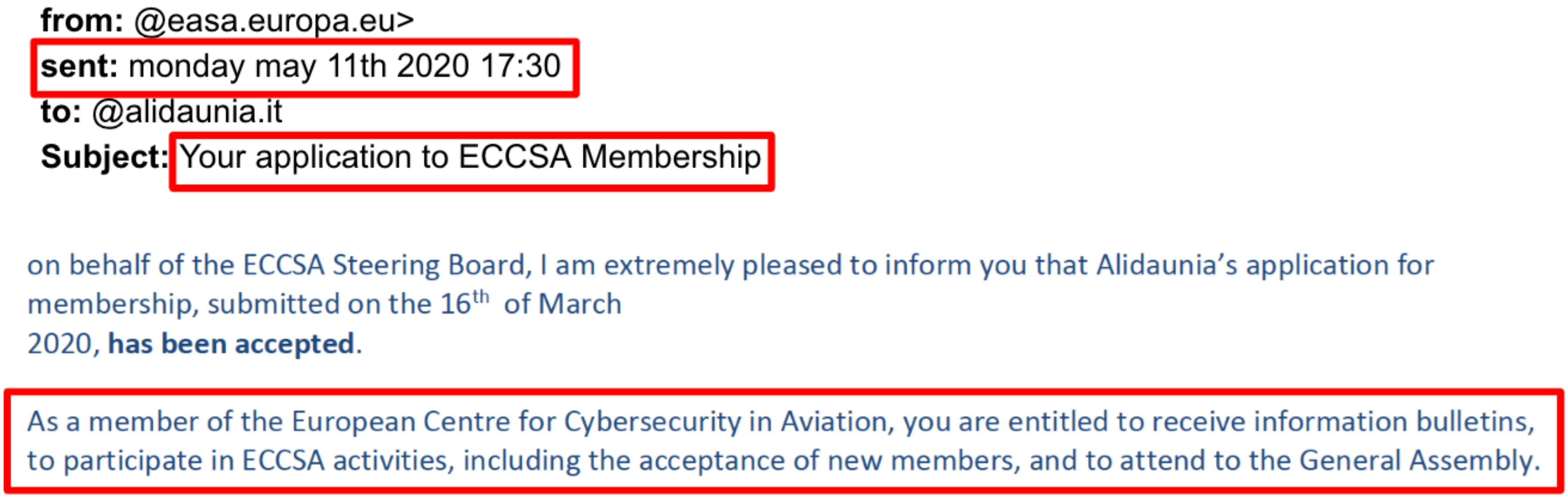
DEGRADED

EXCEEDED LIMITATIONS:

TECHNICAL - OPERATIONAL - ENVIRONMENTAL - PHISICAL

K.O.

And so….Call to action!



from: @easa.europa.eu>
sent: monday may 11th 2020 17:30
to: @alidaunia.it
Subject: Your application to ECCSA Membership

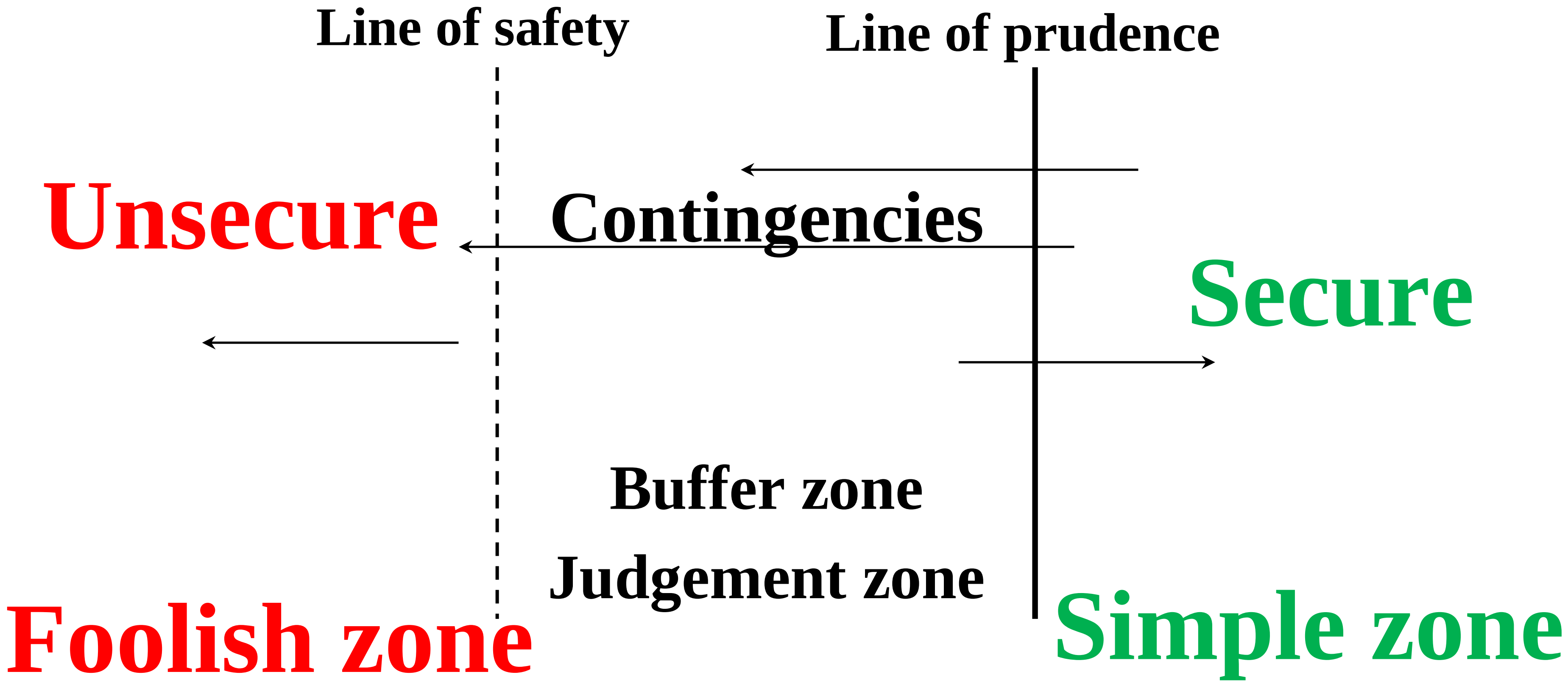
on behalf of the ECCSA Steering Board, I am extremely pleased to inform you that Alidaunia's application for membership, submitted on the 16th of March 2020, **has been accepted**.

As a member of the European Centre for Cybersecurity in Aviation, you are entitled to receive information bulletins, to participate in ECCSA activities, including the acceptance of new members, and to attend to the General Assembly.

ALIDAUNIA has clear the understanding that its competency is complementary and it can learn a lot from each other experience

How to be Ready

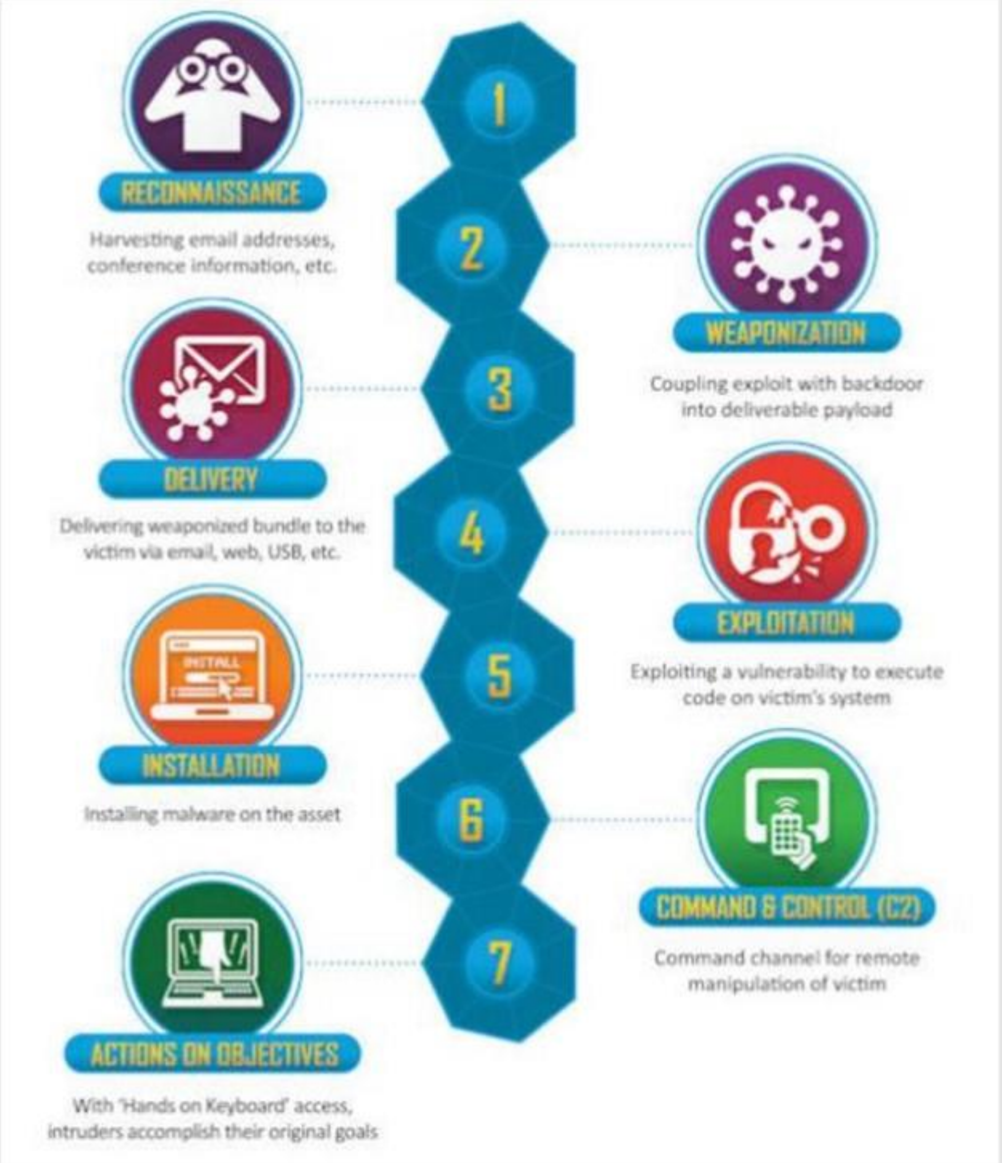
We applied the **“Know yourself!”** concept, in order to Know the strengths and weaknesses of our Organization



MAXIMISE OPERATIVE OUTPUT….

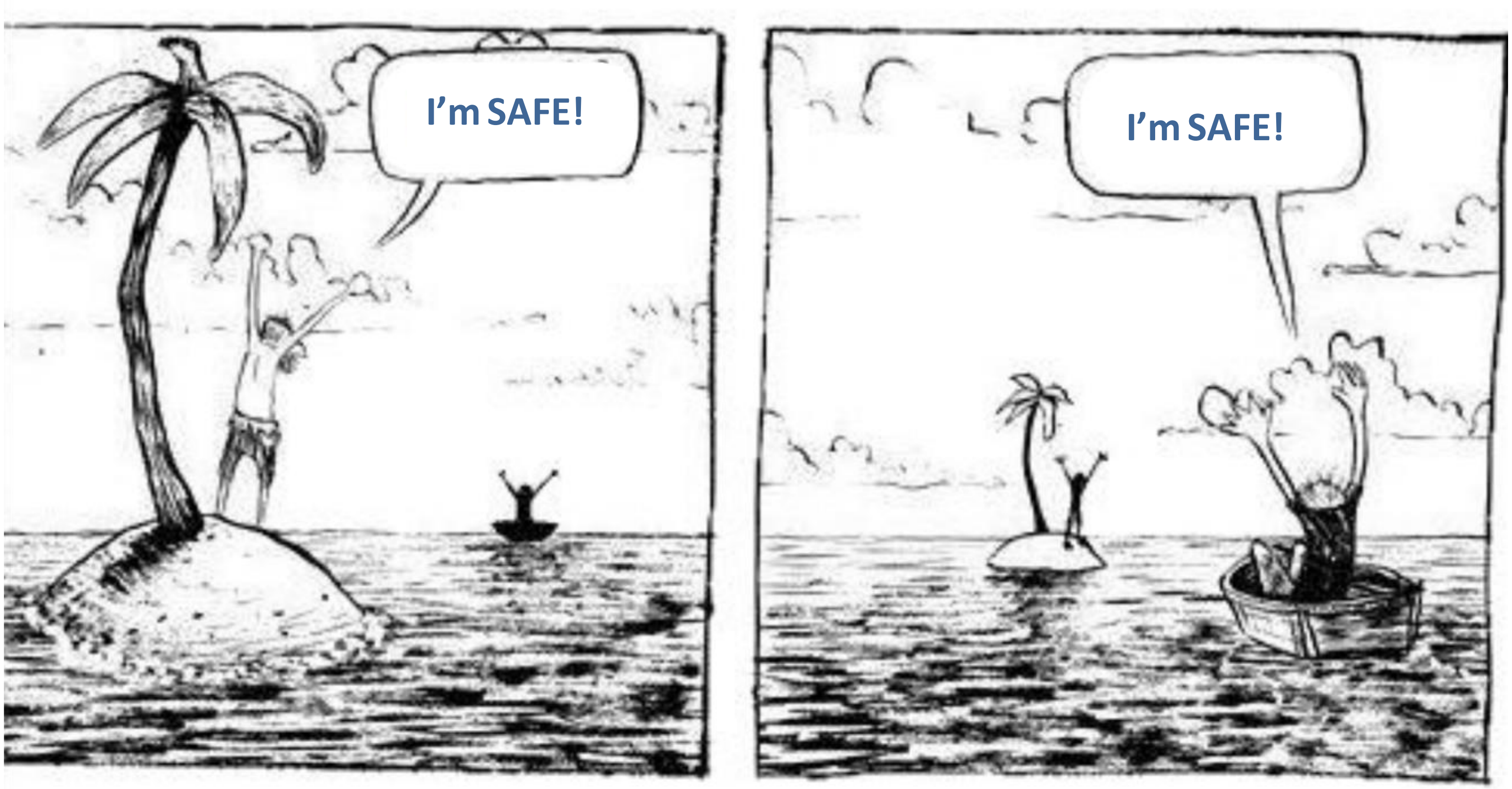
...WITHIN THE MAX LEVEL OF SECURITY & SAFETY

How to be Ready


1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALLATION
INSTALL
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

We believe that the first and most important milestone in cyber defense, as in other areas of life, is staff training. Disseminate to all workers and co - workers of the Company, information on the danger deriving from naive use of software and computers. Not only…

Resilience? A matter of….



….PERSPECTIVE AND PERCEPTION!

How to be Resilient

1st - Enhancement of a “NO BLAME CULTURE”: People must feel free to work without concern and feel safe reporting errors and mishaps!

2nd - Network separation

3rd - System log analysis in case of dashboard alerts

CYBER RESILIENCE
LEAP
TARGET
UNDERSTAND THE CONTEXT
ESTABLISH THE INITIAL CYBER RESILIENCY BASELINE

How to be Responsive

1st - CSIRT intervention

2nd - Thorough analysis of the situation

3rd - Isolate corrupt systems/ software

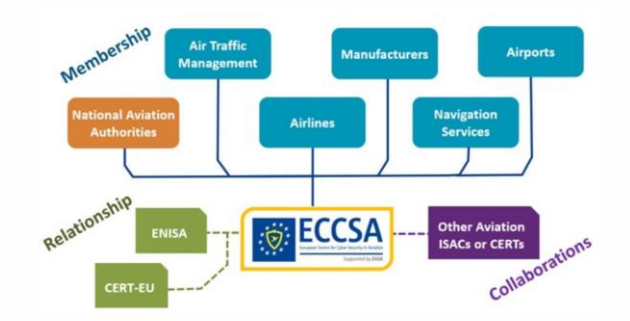
4th - Ensure vital functions by activating back-up systems

5th - Production of a detailed report containing improvement needs and areas of intervention

Next Steps

- Be prepared for future challenges
- Be ready to respond properly to changes in normative context
- Start to implement Part IS
- Stay tuned on potential threats
- Improve speed and precision of intervention in case of Cyber incident/accident
- Highlight area of improvement even if our strategies are working well in the present or performed well in the past

Advice for friends



- **Don't underestimate cyber threats**

- **Trust the network:** you can learn from other experiences without toll on finances or drain in morale!

- **Size doesn't matter:** being a small or a large operator makes no difference if we are all connected in the business, the effects can be equally serious for everyone

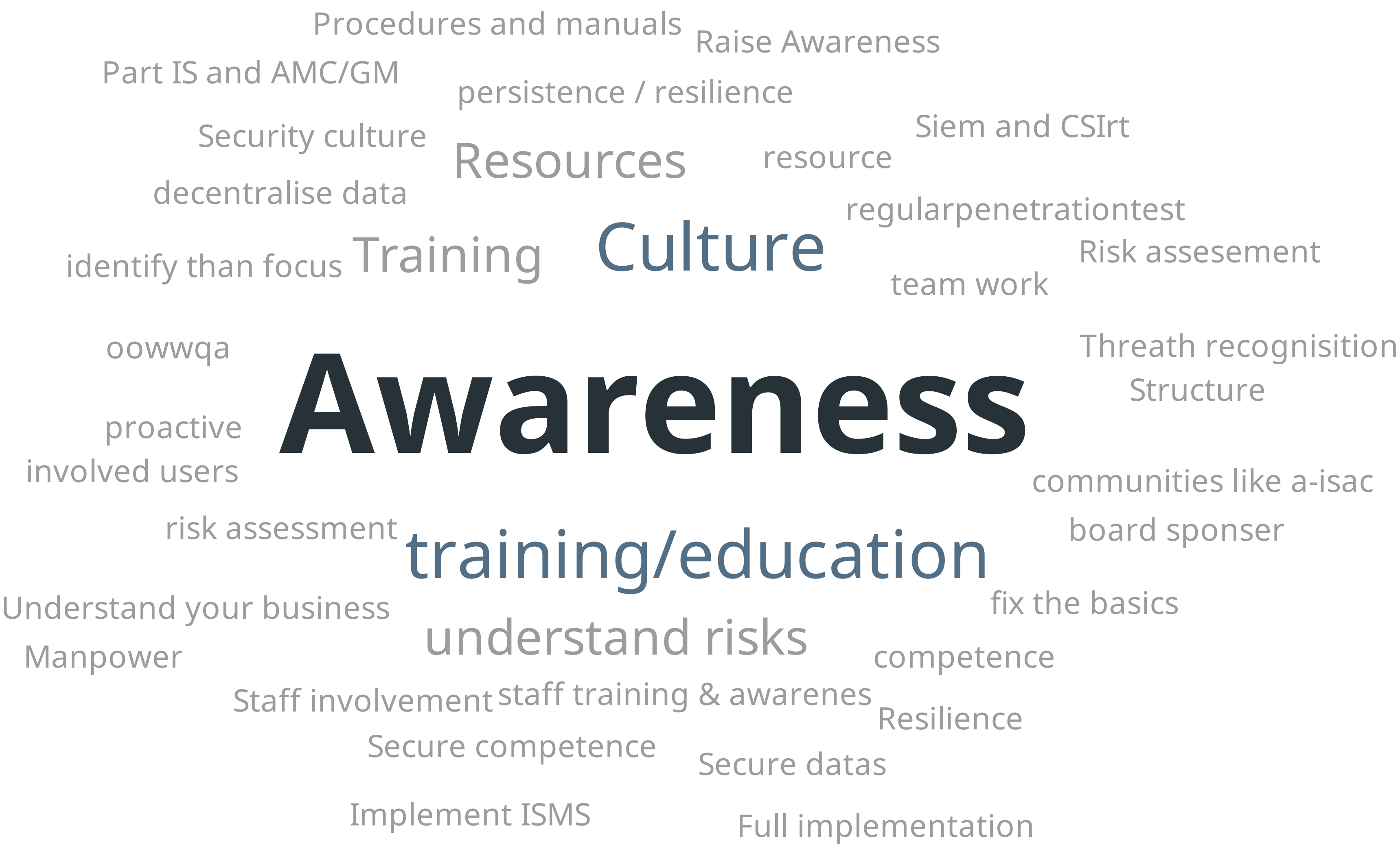
- **Join the ECCSA:** The main objective of ECCSA is to create a collaborative environment of organisations and of trusted cybersecurity professionals that can help each other to become more resilient with cyber-attacks.

THANK YOU FOR YOUR KIND ATTENTION

Wordcloud poll

7. In the case that you already have mitigation measures and processes in place, what advice would you give to an organisation starting tomorrow its journey to address cybersecurity risks?

071

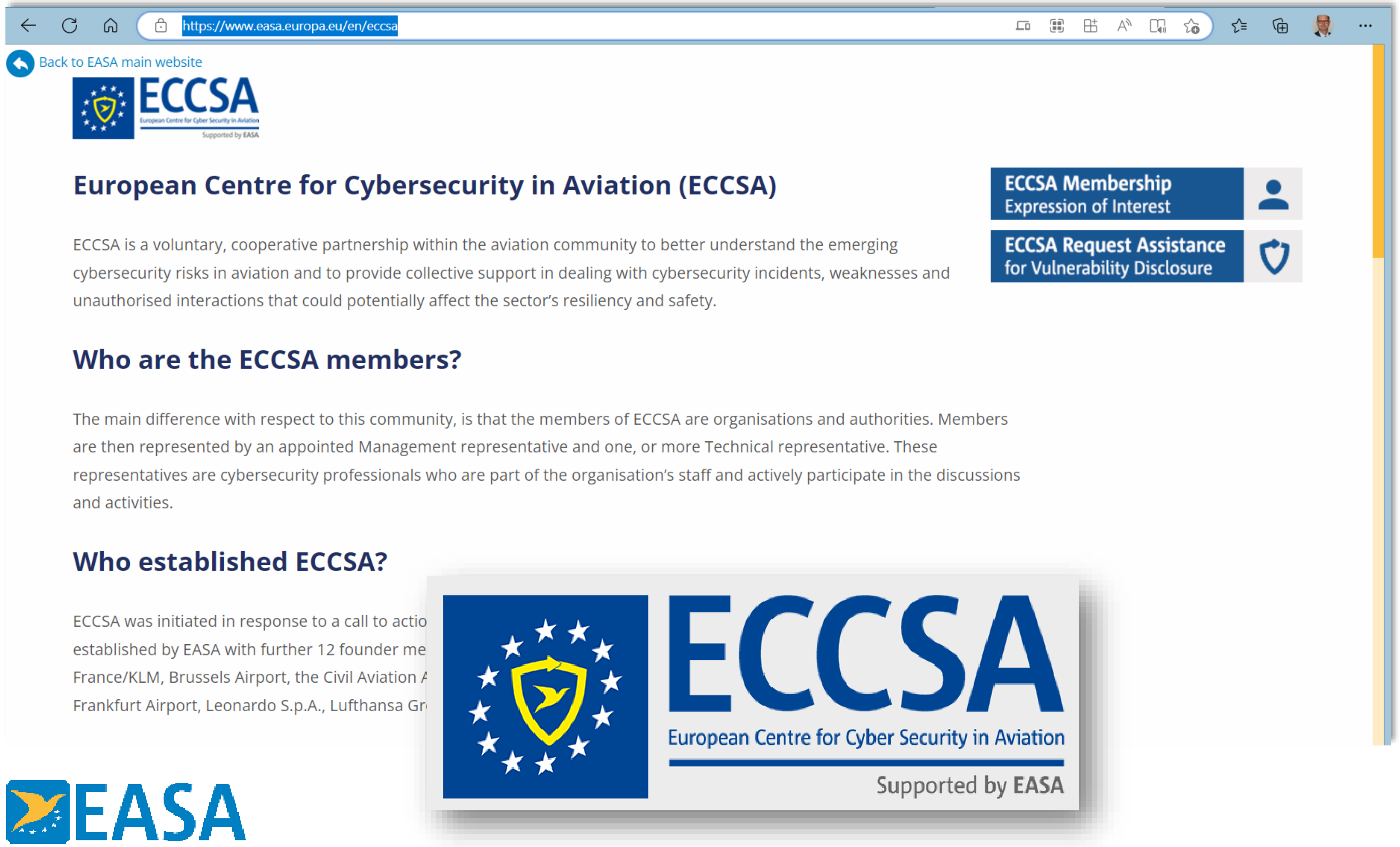


Procedures and manuals
Raise Awareness
Part IS and AMC/GM
persistence / resilience
Siem and CSIrt
Security culture
Resources
resource
decentralise data
regularpenetrationtest
identify than focus
Training
Culture
Risk assesement
team work
oowwqa
Threath recognisition
Awareness
Structure
proactive
involved users
communities like a-isac
risk assessment
board sponser
training/education
Understand your business
fix the basics
understand risks
Manpower
competence
Staff involvement
staff training & awarenes
Resilience
Secure competence
Secure datas
Implement ISMS
Full implementation

What can I do to mitigate cyber risks?

- Short term: join ECCSA
  - Access to Cyber Threats Information
  - Possibility of advance warnings

https://www.easa.europa.eu/en/eccsa


https://www.easa.europa.eu/en/eccsa
Back to EASA main website
ECCSA
European Centre for Cyber Security in Aviation
Supported by EASA
ECCSA Membership Expression of Interest
ECCSA Request Assistance for Vulnerability Disclosure

European Centre for Cybersecurity in Aviation (ECCSA)

ECCSA is a voluntary, cooperative partnership within the aviation community to better understand the emerging cybersecurity risks in aviation and to provide collective support in dealing with cybersecurity incidents, weaknesses and unauthorised interactions that could potentially affect the sector's resiliency and safety.

Who are the ECCSA members?

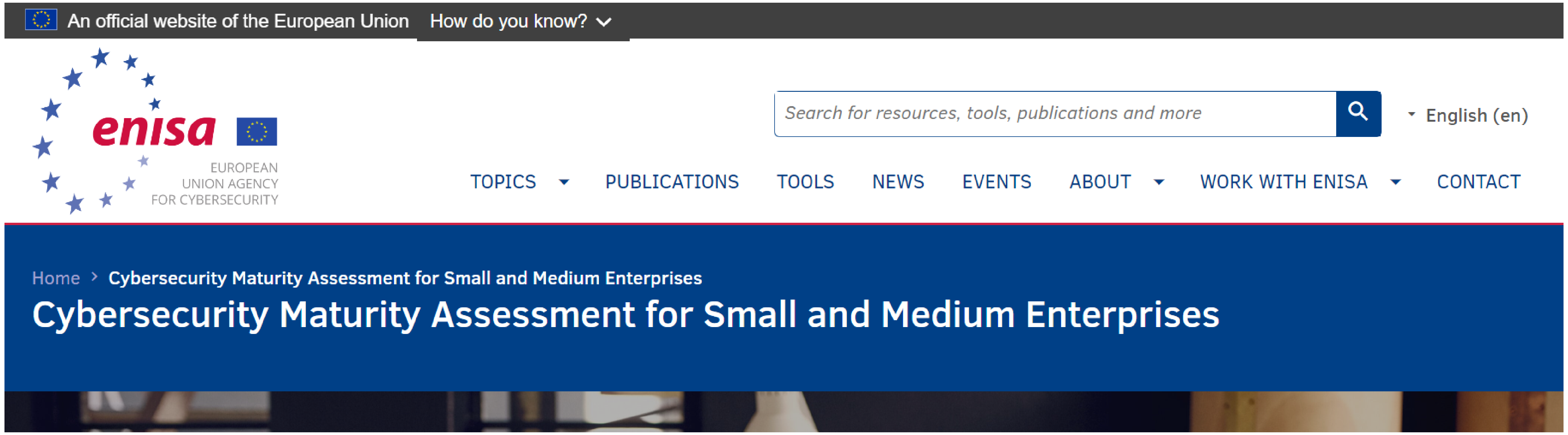
The main difference with respect to this community, is that the members of ECCSA are organisations and authorities. Members are then represented by an appointed Management representative and one, or more Technical representative. These representatives are cybersecurity professionals who are part of the organisation's staff and actively participate in the discussions and activities.

Who established ECCSA?

ECCSA was initiated in response to a call to actio
established by EASA with further 12 founder me
France/KLM, Brussels Airport, the Civil Aviation A
Frankfurt Airport, Leonardo S.p.A., Lufthansa Gr

- Medium term: start implementing Part-IS
  - Define scope
  - Perform risk assessment
  - Policies for Detection, Response and Recovery

Additional recommended readings



An official website of the European Union How do you know?

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

Search for resources, tools, publications and more

English (en)

TOPICS PUBLICATIONS TOOLS NEWS EVENTS ABOUT WORK WITH ENISA CONTACT

Home > Cybersecurity Maturity Assessment for Small and Medium Enterprises

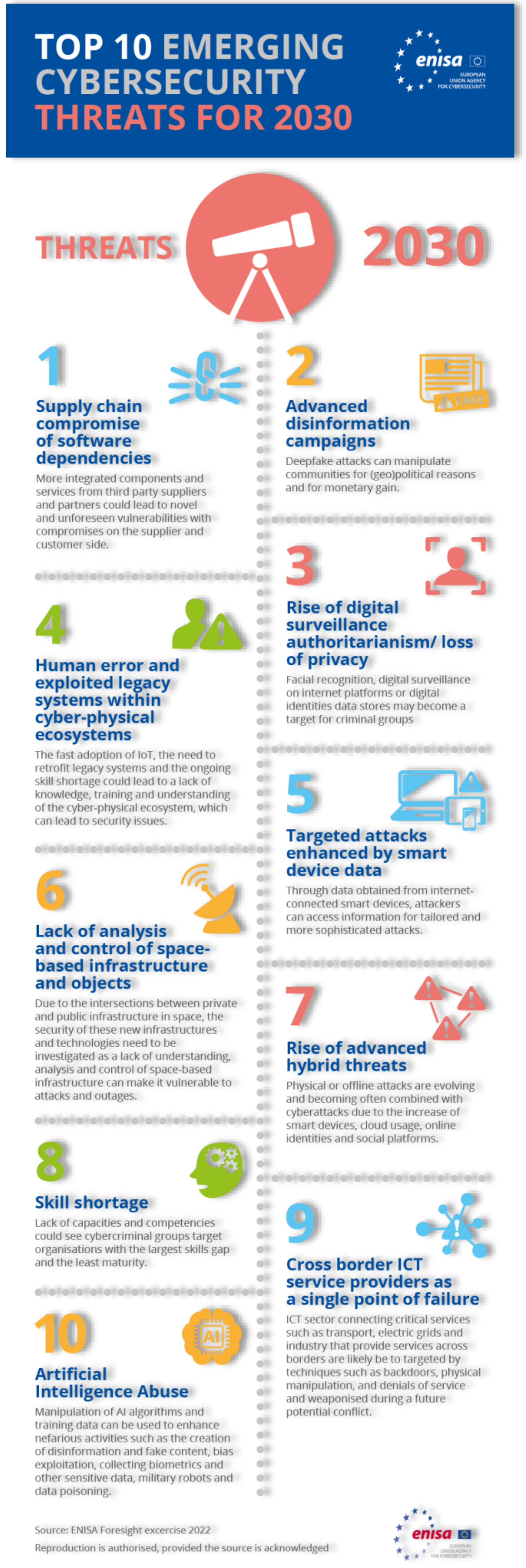
Cybersecurity Maturity Assessment for Small and Medium Enterprises

https://www.enisa.europa.eu/

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

Cybersecurity guide for SMEs

12 STEPS TO SECURING YOUR BUSINESS



TOP 10 EMERGING CYBERSECURITY THREATS FOR 2030

enisa

THREATS 2030

1 **Supply chain compromise of software dependencies**
More integrated components and services from third party suppliers and partners could lead to novel and unforeseen vulnerabilities with compromises on the supplier and customer side.

2 **Advanced disinformation campaigns**
Deepfake attacks can manipulate communities for (geo)political reasons and for monetary gain.

3 **Rise of digital surveillance authoritarianism/ loss of privacy**
Facial recognition, digital surveillance on internet platforms or digital identities data stores may become a target for criminal groups

4 **Human error and exploited legacy systems within cyber-physical ecosystems**
The fast adoption of IoT, the need to retrofit legacy systems and the ongoing skill shortage could lead to a lack of knowledge, training and understanding of the cyber-physical ecosystem, which can lead to security issues.

5 **Targeted attacks enhanced by smart device data**
Through data obtained from internet-connected smart devices, attackers can access information for tailored and more sophisticated attacks.

6 **Lack of analysis and control of space-based infrastructure and objects**
Due to the intersections between private and public infrastructure in space, the security of these new infrastructures and technologies need to be investigated as a lack of understanding, analysis and control of space-based infrastructure can make it vulnerable to attacks and outages.

7 **Rise of advanced hybrid threats**
Physical or offline attacks are evolving and becoming often combined with cyberattacks due to the increase of smart devices, cloud usage, online identities and social platforms.

8 **Skill shortage**
Lack of capacities and competencies could see cybercriminal groups target organisations with the largest skills gap and the least maturity.

9 **Cross border ICT service providers as a single point of failure**
ICT sector connecting critical services such as transport, electric grids and industry that provide services across borders are likely be to targeted by techniques such as backdoors, physical manipulation, and denials of service and weaponised during a future potential conflict.

10 **Artificial Intelligence Abuse**
Manipulation of AI algorithms and training data can be used to enhance nefarious activities such as the creation of disinformation and fake content, bias exploitation, collecting biometrics and other sensitive data, military robots and data poisoning.

Source: ENISA Foresight excercise 2022

Reproduction is authorised, provided the source is acknowledged

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

EASA
European Union Aviation Safety Agency

together
4safety

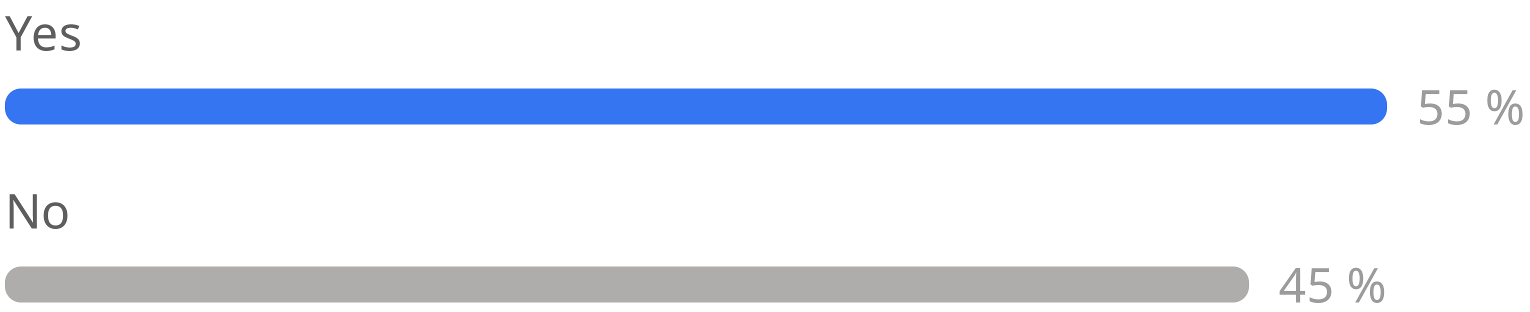
Summer 2023

Are you Ready, Resilient and Responsive enough for this summer's challenges?

Multiple-choice poll

8. Do you think your plans will change after today?

0 9 1



Open text poll

9. If you replied yes in the previous question, what do you plan to do next?

(1/3)

036

- clarify responsiblity
- Risk assessment
- Perform GAPT analysis between the PART-IS requirements and ISO 27001
- have a coffy
- Create resources
- spread the word
- Audit IT
- Plan a startup to see what our organization sees a threats regarding our operations and assignments
- additional GAP analysis?
- Share information through meetings
- ECCSA
- risk assessment
- Further align existing ISMS with Part-IS
- Share this content with the cyber/security experts and look the plans and internal processes.
- Raise Awarness
- Gap analysis
- join ECSSA, gap analysis
- I will internally organize who will join EASA groups in

Open text poll

9. If you replied yes in the previous question, what do you plan to do next?
(2/3)

0 3 6

the future to share information regarding implementation of Part-IS

- Analyze Part-IS in detail and see what can be done
- Join ECCSA
- Share the information with my colleagues
- ISO 27001, join ECCSA
- What do we have in place, how to improve it
- Raise awareness
- ECCSA
- Go through additional reading material suggested
- awareness with other dept
- Training
- Define who is responsible
- Collaborate with EASA and NAAs
- Proper risk assessment, setting responsibilities and procedures
- briefings
- explore the resources and legislation provided, including the organizations mentioned
- Perfom a gap analysis
- join ECCSA
- raise awareness
- Start Implementing IS

Open text poll

9. If you replied yes in the previous question, what do you plan to do next?

(3/3)

036

- Training

Questions answered after the session

- **ISMS pilot cases were kicked off by EASA in Q2/2022 with some selected organisations. However no EASA policy (clear objectives, roadmap, deliverables, expected outputs, ...) has been yet issued and shared with the selected organisations. When can we expect such policy to be issued?**
  - EASA Pilot projects were launched to test the implementation of Part-IS in selected organisations and to gain experience that could benefit other stakeholder. As such, each project is unique as deliverables and outputs need to fit the specific context of that organization. Therefore a common policy is not needed. Recently, also national authorities have been encouraged to launch their own pilot projects with organisations under their oversight. Also in these cases no common policy was deemed necessary

- **For an ATO with integrated ATPL and 1 Full flight simulator B737 level D, how should I see the implementation of part IS? It's in the scope, but isn't it over the top?**
  - Ref. IS.I/D.OR.205, the starting points should always be the definition of the scope, that is the assets you want to protect, including their interfaces with the external world. You will then assess the connected risks and decide on their appropriate treatment.

- **Does it make sense to combine all cyber regulations within the ISMM required by Part IS and EASA provide a cross reference table?**
  - In our opinion, yes it makes sense. However, attention should be paid to the different regulatory regimes and to what they ask for in terms of documenting the processes in place. To be noted that EASA does not plan at present to provide as cross-reference table to other Union legislation. Moreover, it’s responsibility of each organization to show compliance to applicable regulations and a cross-reference table is not alleviating such obligation.

KEEP
CALM
AND
IMPLEMENT PART-IS