EASA
European Union Aviation Safety Agency

PART-IS regulation

Understanding specific provisions

Davide Martini

Senior Expert – Cybersecurity in Aviation

Cybersecurity in Aviation & Emerging Risks

AESA Workshop on Cybersecurity in Aviation, Madrid 07/05/2024

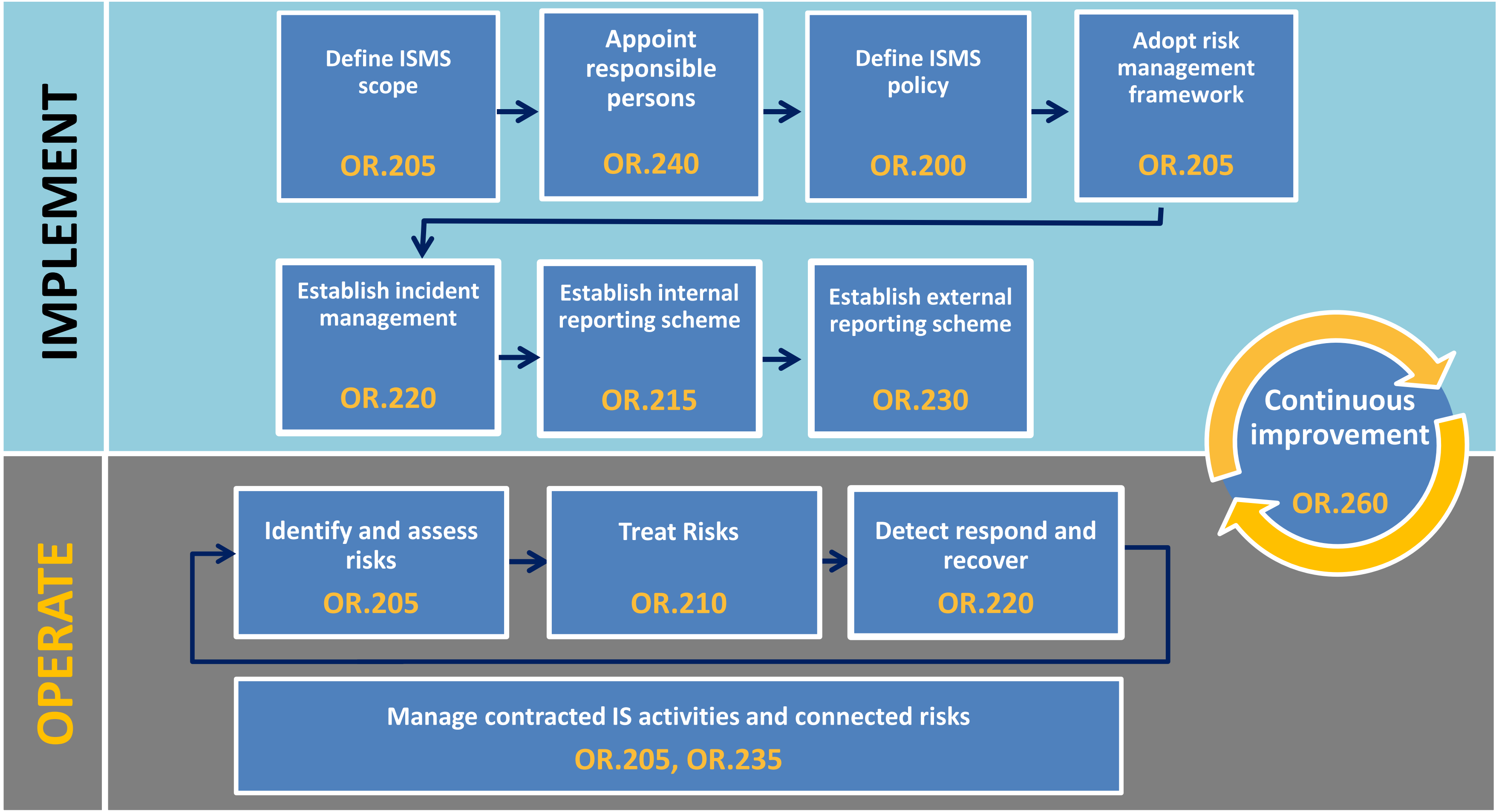
Your safety is our mission.

An Agency of the European Union

ISMS EVALUATION

AND

CONTINUOUS IMPROVEMNT



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

AR.235/OR.260

IR	- Identify adequate performance indicators - Assess effectiveness and maturity of the ISMS - Ensure risks remain at an acceptable level - Take necessary improvement measures, if needed
AMC	- Continuously improve the effectiveness, suitability and adequacy of ISMS - Assess ISMS proactively and systematically, including its maturity - Consider outcomes/conclusions of other information security and assurance processes
GM	- Assurance processes for ISMS are equivalent to safety assurance (Doc 9859) - Include performance monitoring & measurement, management of change and continuous improvement - ISMS needs to be continuously monitored and improved

One input is Compliance Monitoring

- Internal audits, at planned, regular intervals

- Include a feedback of audit findings to the accountable manager for assurance
- Triggers corrective actions, as necessary
- Includes the execution of independent Audits

Continuous Improvement – Two Reasons

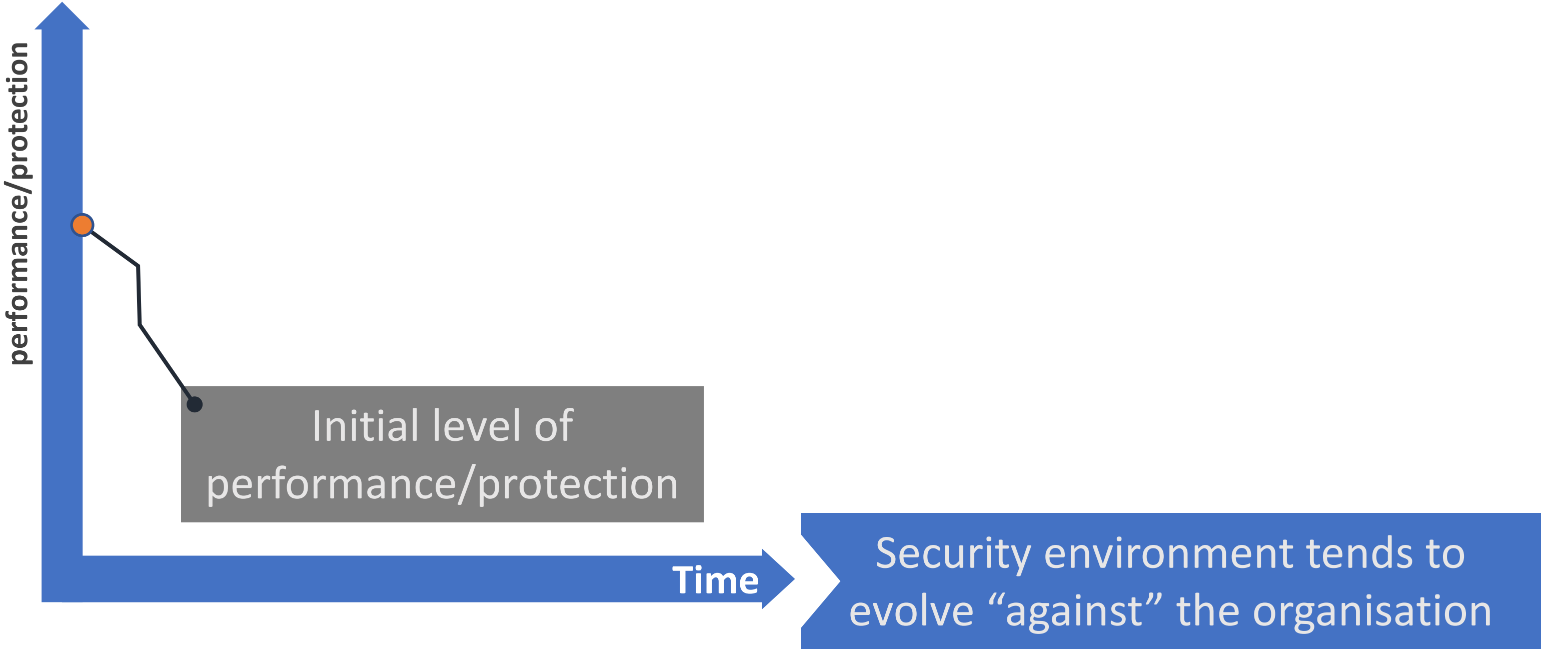
Organisation

Dynamic adaptation to the evolution and change of the objectives, architectures, organisational structures and processes of an entity, which are reducing the level of compliance

Security Environment

Dynamic adaptation to constantly emerging discovery of vulnerabilities, threat actors, tools and methods, which are reducing effectiveness of controls

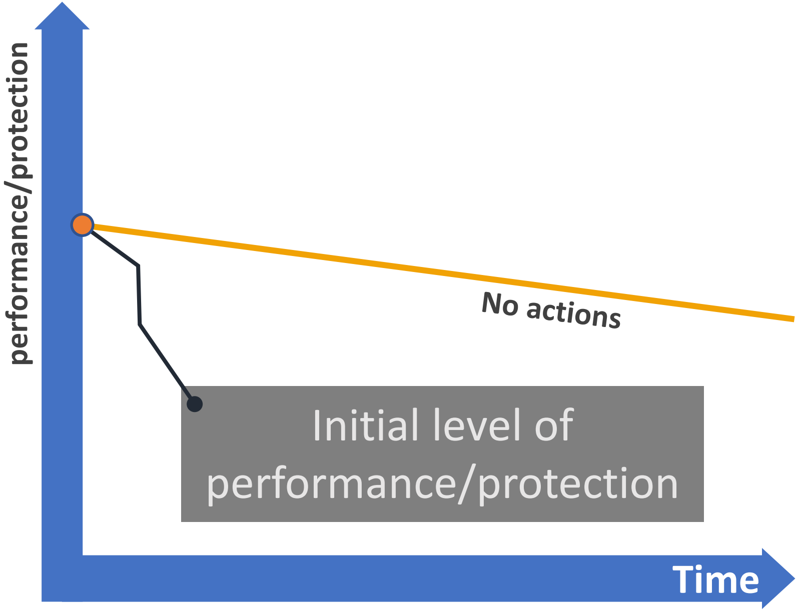
Continuous improvement



Initial level of performance/protection

Security environment tends to evolve “against” the organisation

Continuous improvement



Initial level of performance/protection

Opportunities for threats arise from new vulnerabilities and attack tools

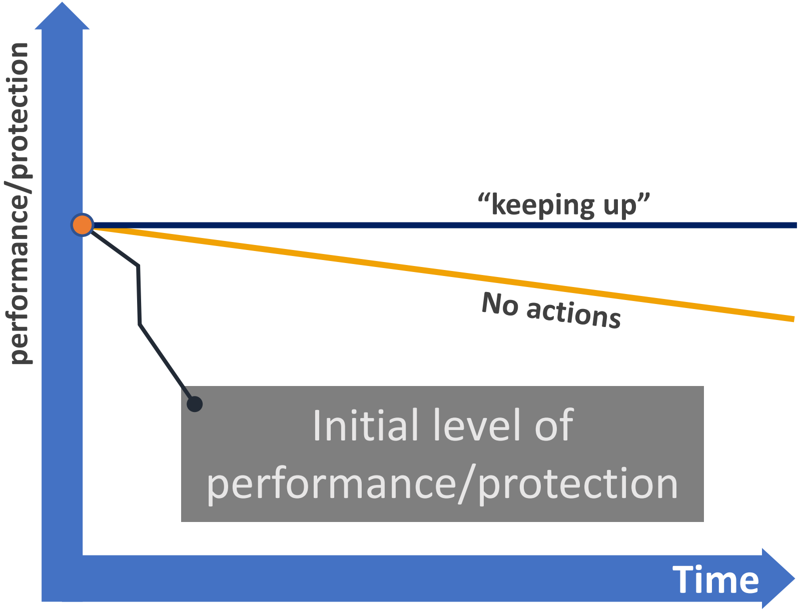
Security environment tends to evolve “against” the organisation

Security Risk Acceptability Matrix

Risk Level	Threat Condition Severity of Effect				
Level of Threat	No Effect	Minor	Major	Hazardous	Catastrophic
Very High	🟩	🟨	🟥 Unacceptable	🟥	🟥
High	🟩	🟩	🟥	🟥	🟥
Moderate	🟩	🟩	🟨	🟥	🟥
Low	🟩	🟩	🟩	🟨	🟥
Extremely Low	🟩	🟩	🟩	🟩 ✡	🟨

This is a non-normative example

Continuous improvement



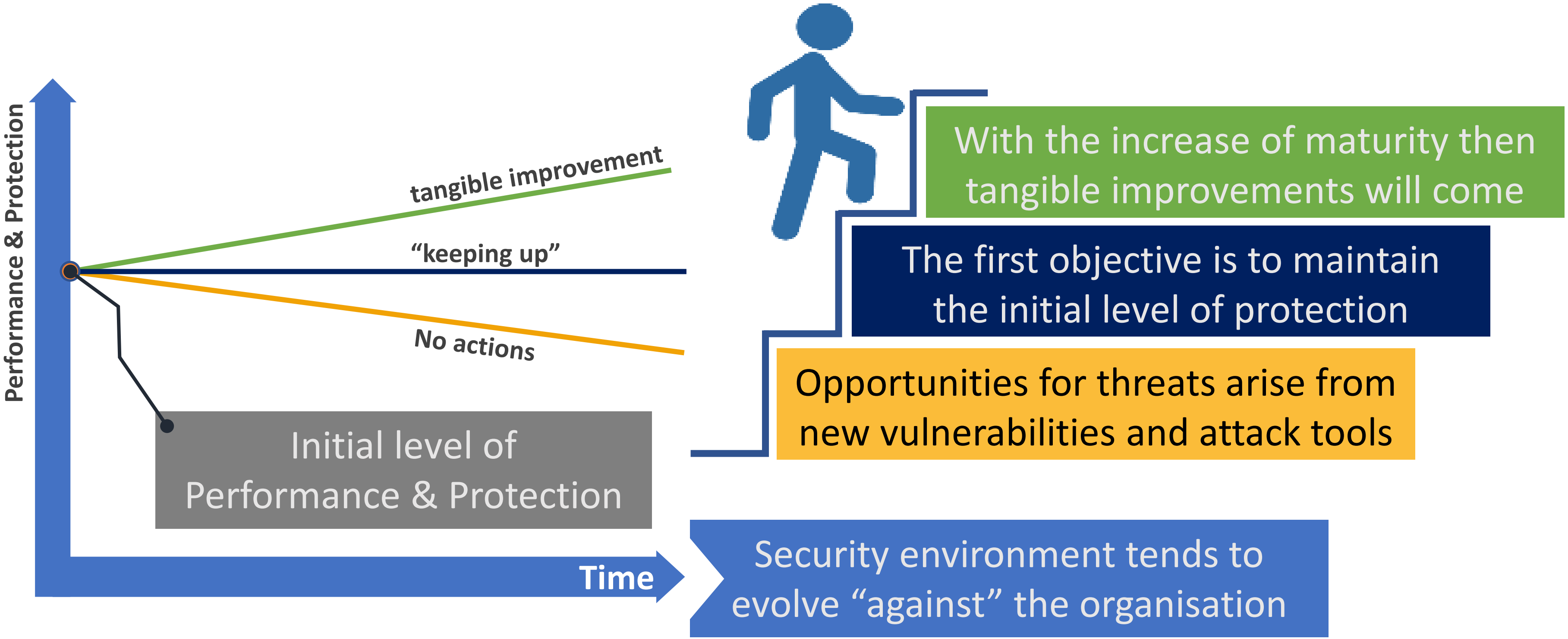
Initial level of performance/protection

The first objective is to maintain the initial level of protection

Opportunities for threats arise from new vulnerabilities and attack tools

Security environment tends to evolve “against” the organisation

Continuous improvement – Security Environment



Initial level of Performance & Protection

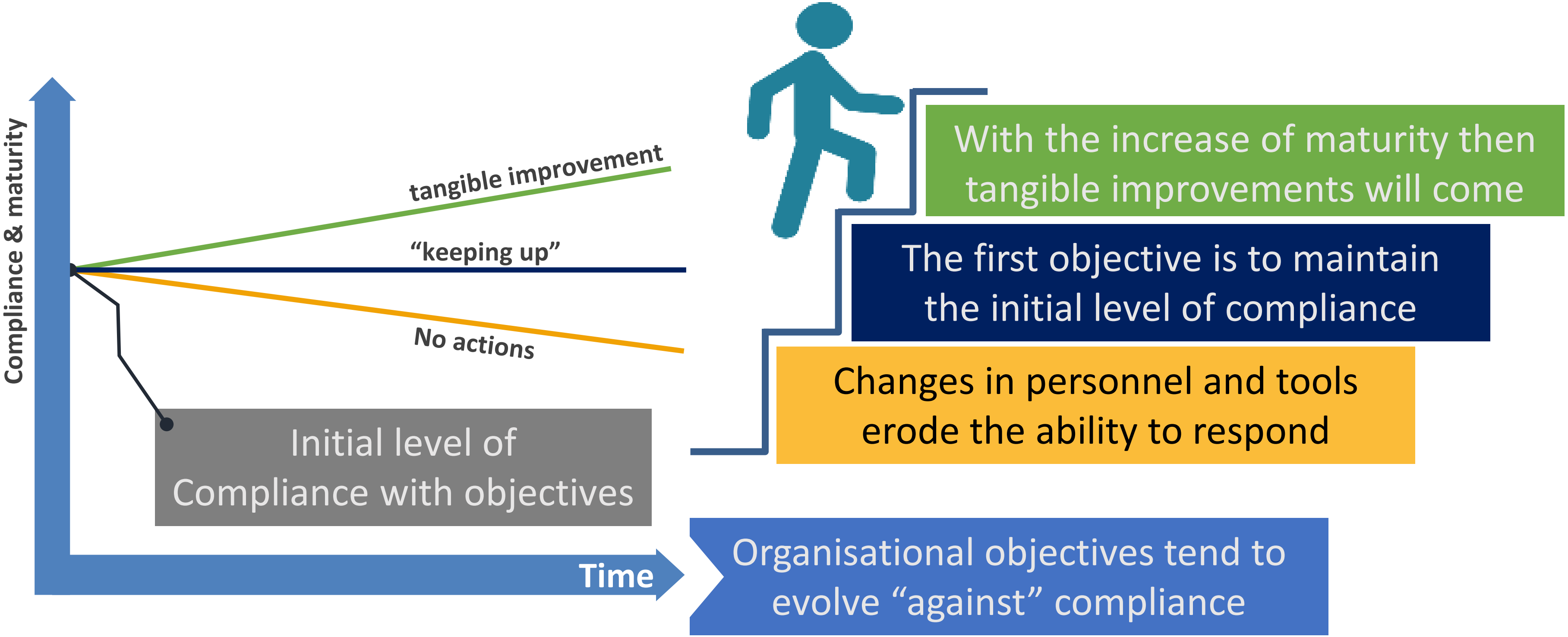
With the increase of maturity then tangible improvements will come

The first objective is to maintain the initial level of protection

Opportunities for threats arise from new vulnerabilities and attack tools

Security environment tends to evolve “against” the organisation

Continuous Improvement – Organisation



Initial level of Compliance with objectives

Organisational objectives tend to evolve "against" compliance

Changes in personnel and tools erode the ability to respond

The first objective is to maintain the initial level of compliance

With the increase of maturity then tangible improvements will come

Current and future standards for Part-IS

2018	NIST Cyber Security Framework v1.1
2022	ISO/IEC 27001
2021	ED-201A/DO-391A - Aeronautical Information System Security Framework Guidance
2014	ED-202A/DO-326A - Airworthiness Security Process Specification
2022	ED-206 - Guidance on Security Event Management
2024	*ED-20X/Do-3xx – ISMS for aviation organisation*

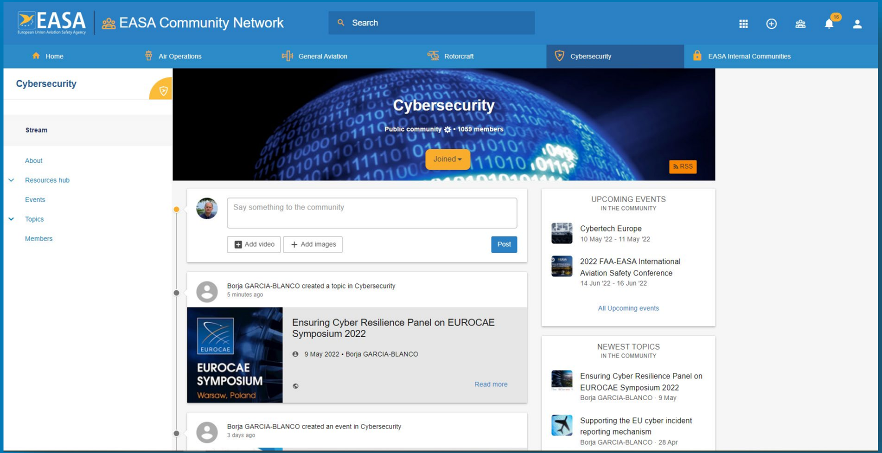
Current and future standards for Part-IS

2018	NIST Cyber Security Framework v1.1
2022	ISO/IEC 27001
2021	ED-201A/DO-391A - Aeronautical Information System Security Framework Guidance
2014	ED-202A/DO-326A - Airworthiness Security Process Specification
2022	ED-206 - Guidance on Security Event Management
2024	*ED-20X/Do-3xx – ISMS for aviation organisation*

EASA
European Union Aviation Safety Agency

Thank you!

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



Cybersecurity
Public community • 1059 members

Borja GARCIA-BLANCO created a topic in Cybersecurity
5 minutes ago

Ensuring Cyber Resilience Panel on EUROCAE Symposium 2022
9 May 2022 • Borja GARCIA-BLANCO

Borja GARCIA-BLANCO created an event in Cybersecurity
3 days ago

UPCOMING EVENTS
IN THE COMMUNITY

Cybertech Europe
10 May '22 - 11 May '22

2022 FAA-EASA International Aviation Safety Conference
14 Jun '22 - 16 Jun '22

NEWEST TOPICS
IN THE COMMUNITY

Ensuring Cyber Resilience Panel on EUROCAE Symposium 2022
Borja GARCIA-BLANCO · 9 May

Supporting the EU cyber incident reporting mechanism
Borja GARCIA-BLANCO · 28 Apr

Contact us at:
cybersec@easa.europa.eu

easa.europa.eu/connect

@

Your safety is our mission.

An Agency of the European Union