



Part-IS Workshop



Workshop agenda

0915	Welcome and Introductions
0930	Topic: Part-IS explained Speaker - Gian Andrea Bandieri Section Manager – Cybersecurity in Aviation & Emerging Risks European Union Aviation Safety Agency Speaker - Cyrille Rosay EASA Senior Expert –Cybersecurity in Aviation
1100	Coffee
1130	Topic: Cybersecurity Regulation - a National Approach Speaker- Eleanor Travers, Aviation Security Manager Irish Aviation Authority
1200 - 1230	Questions and answers, Conclusions
1230	Workshop close

Part-IS explained

Gian Andrea Bandieri, Cyrille Rosay

EASA

15 September 2023

Your safety is our mission.

Aviation is a System-of-Systems

Satellite Communications
(SATCOM)

Cabin links accessible to passengers (Cabin Wifi, plugs on cabin seats, FAP, bluetooth...)

Aircraft - Ground links
(ACARS, HF, VHF, SATCOM ; GPS, ILS...)



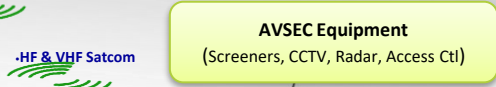
Air/Ground Links



AVSEC Equipment
(Screeners, CCTV, Radar, Access Ctl)

Outstation

Aircraft - Ground links
(Gatelink, GSM, Wifi, WiMax...)



Operations & Dispatch Centre

Supply chain
(Transit of Software from Supplier to OEMs...)

Maintenance & Industrial systems
(PMAT, Portable Data-Loader, troubleshooting equipment, USB keys, ITcards...)

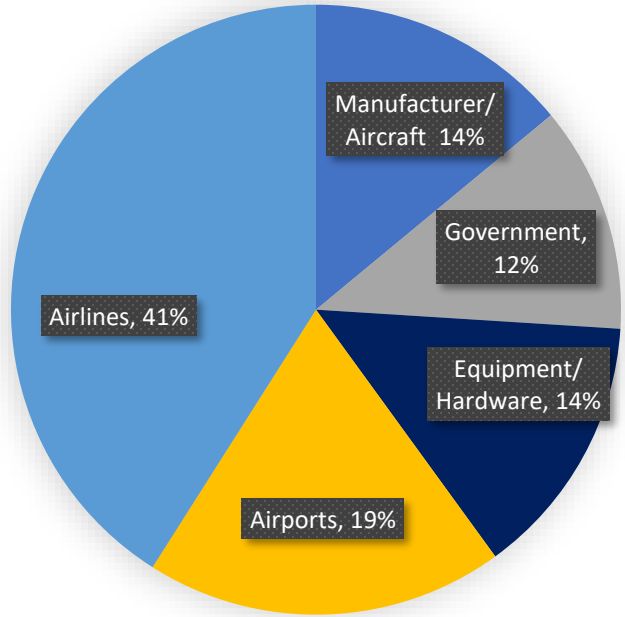
Maintenance & Engineering Centre

Aircraft data & parts suppliers

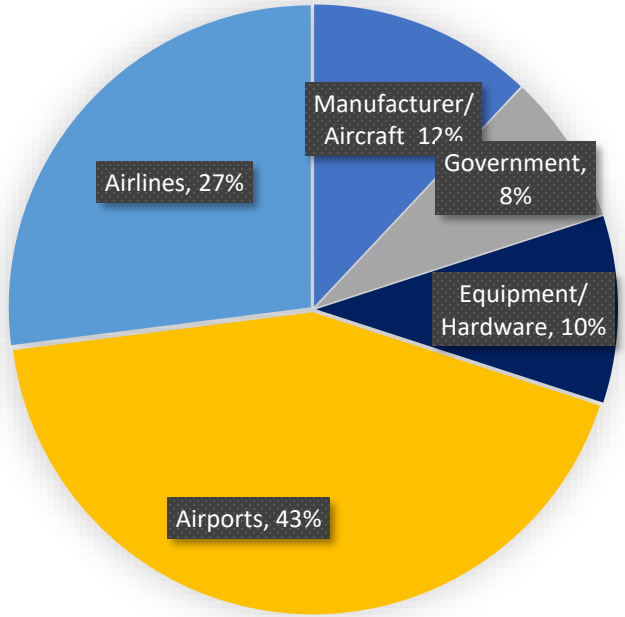


Cybersecurity risks matter to you

116 attacks by target organisation in 2022



49 attacks by target organisation JAN- APR 2023



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

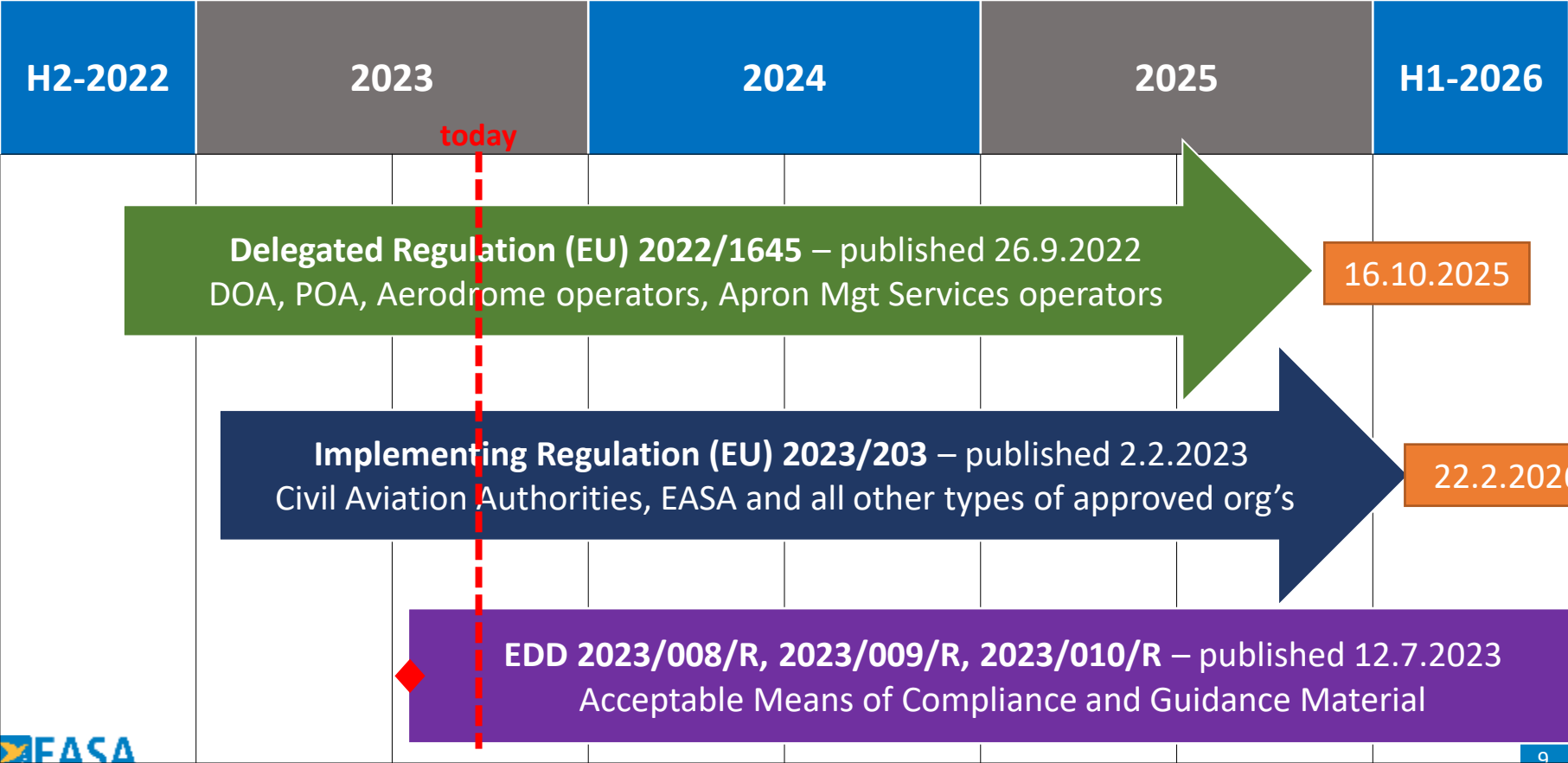
- To have competent and well aware workforce
- To monitor the current Threat Landscape
- To understand the future Threat Landscape



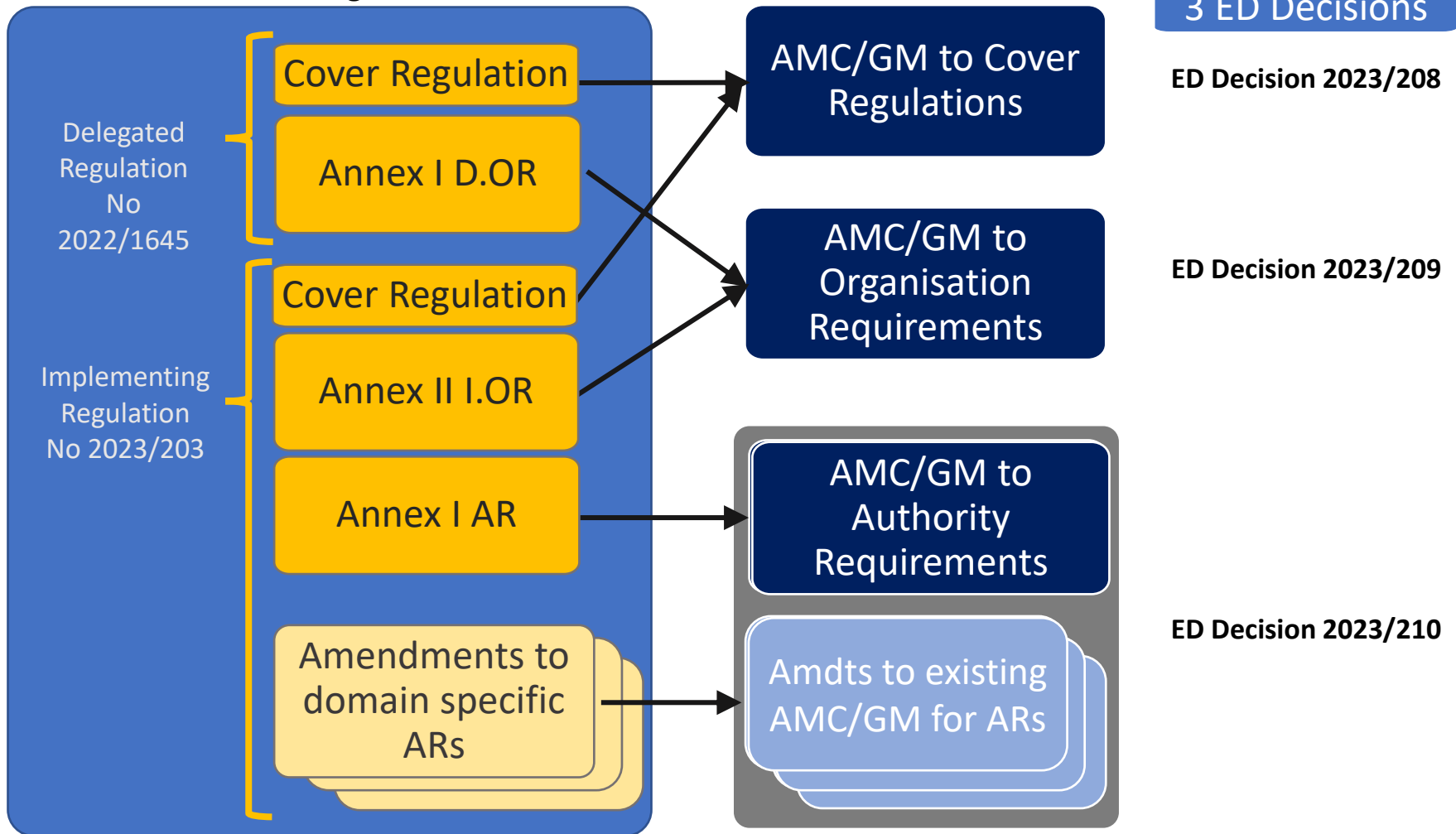
What we want to achieve with Part-IS

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

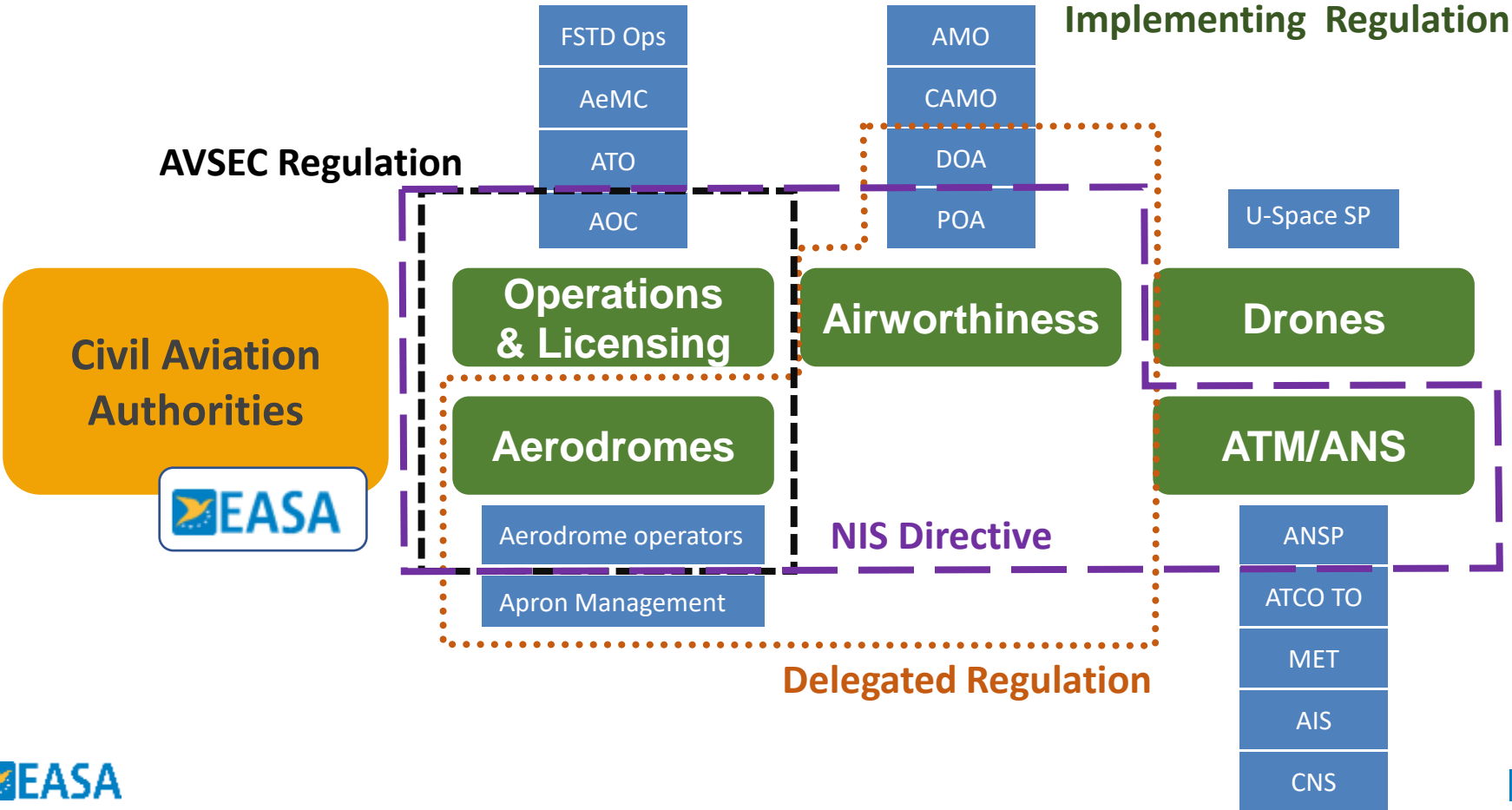
Part-IS implementation journey



Part-IS Regulations



Applicability of Part-IS



Part IS is not applicable to:

Production organisations not holding an approval

Part-147 maintenance training organisations.

ATOs providing only theoretical training.

Private operators of other than complex motor-powered aircraft.

Organisations dealing only with light aircraft:

- e.g. airplanes below 2000 kg MTOM, very light rotorcraft, sailplanes, balloons and airships.

Operators of UAS in the “open” and “specific” categories.

Organisation designing UAS in the “specific” category when not required to hold a DOA approval.

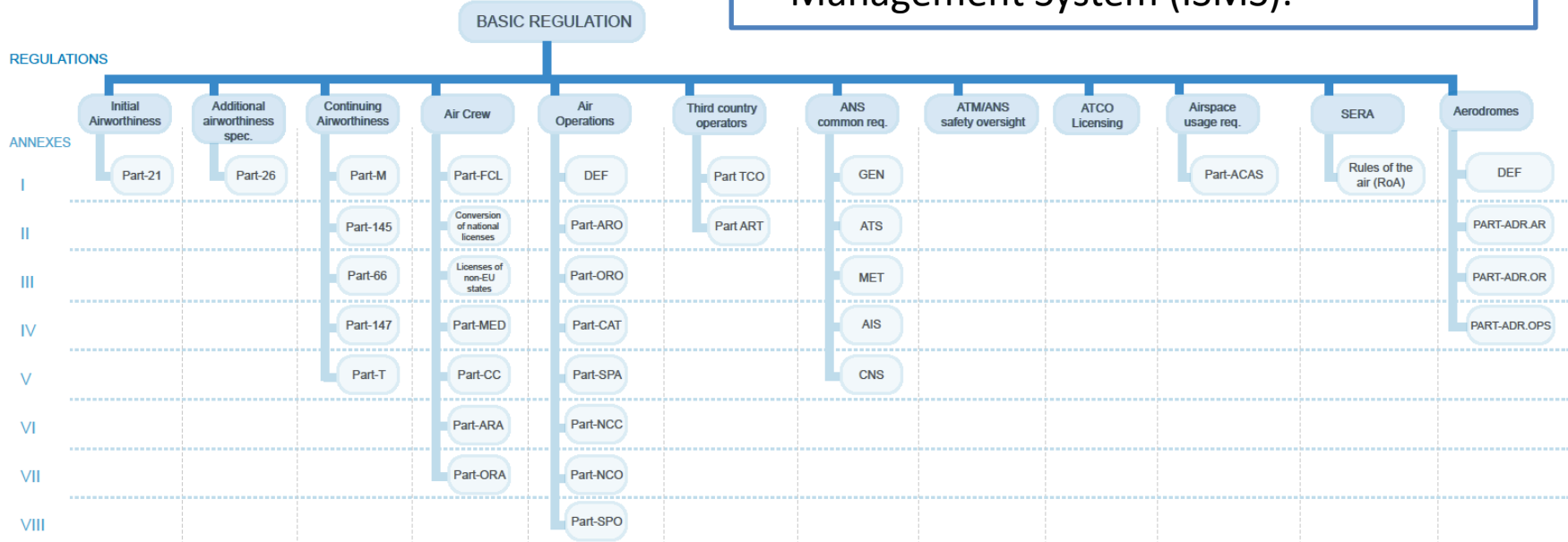
TCO operators

Regulated by ICAO Annex 6

Organisations approved under bilateral agreements

Main elements of Part-IS

Two “horizontal” regulations containing the provisions of the Information Security Management System (ISMS):



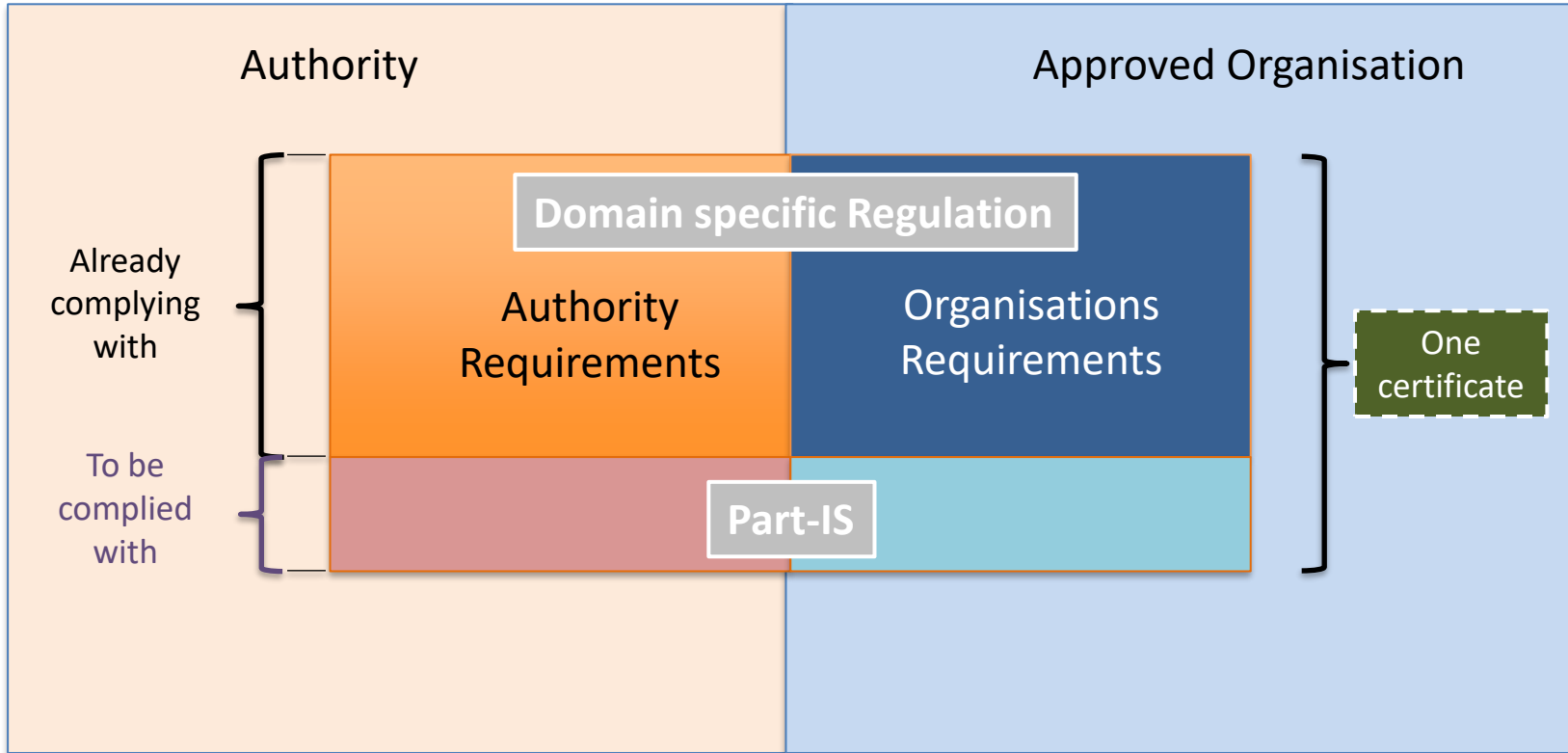
Authority Requirements: Part-IS.AR

Organisation Requirements: Part-IS.OR

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

Part-IS and existing approvals/regulations

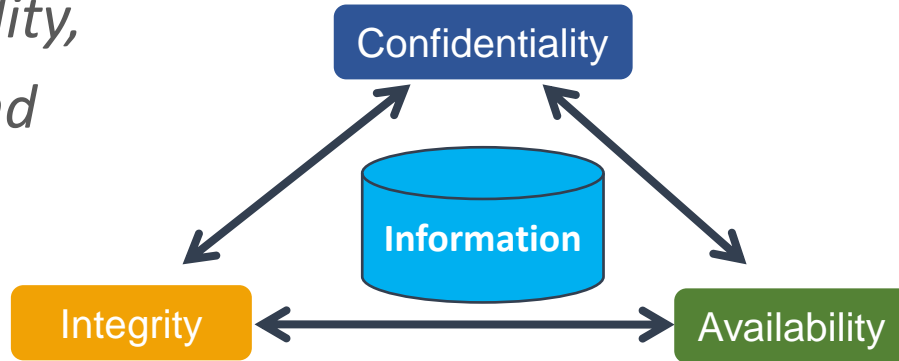


What is an ISMS?

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.

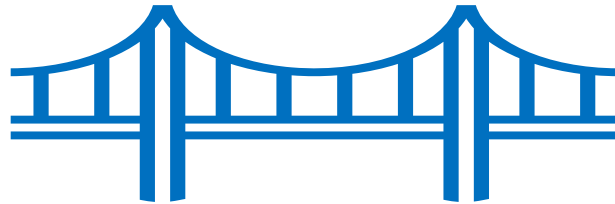
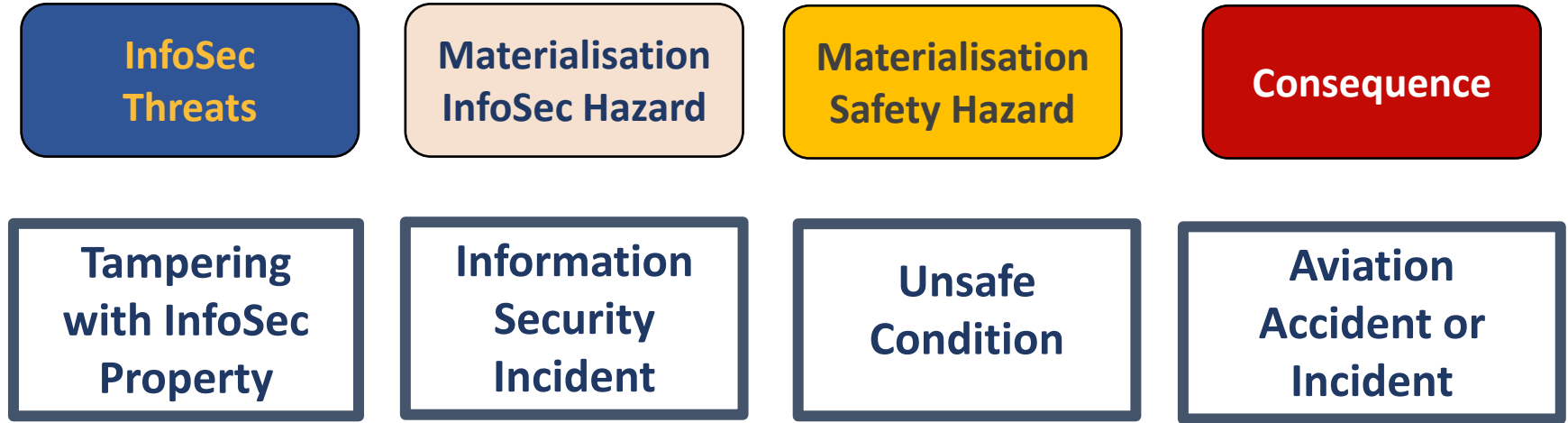
**business
risk**

Part-IS

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

**safety
risk**

Bridging Information Security and Safety



Transition of Notions

From a **Safety** Notion to a **Security-for-Safety** Notion

Reliable System*

A **Reliable System** does, what it is supposed to do.

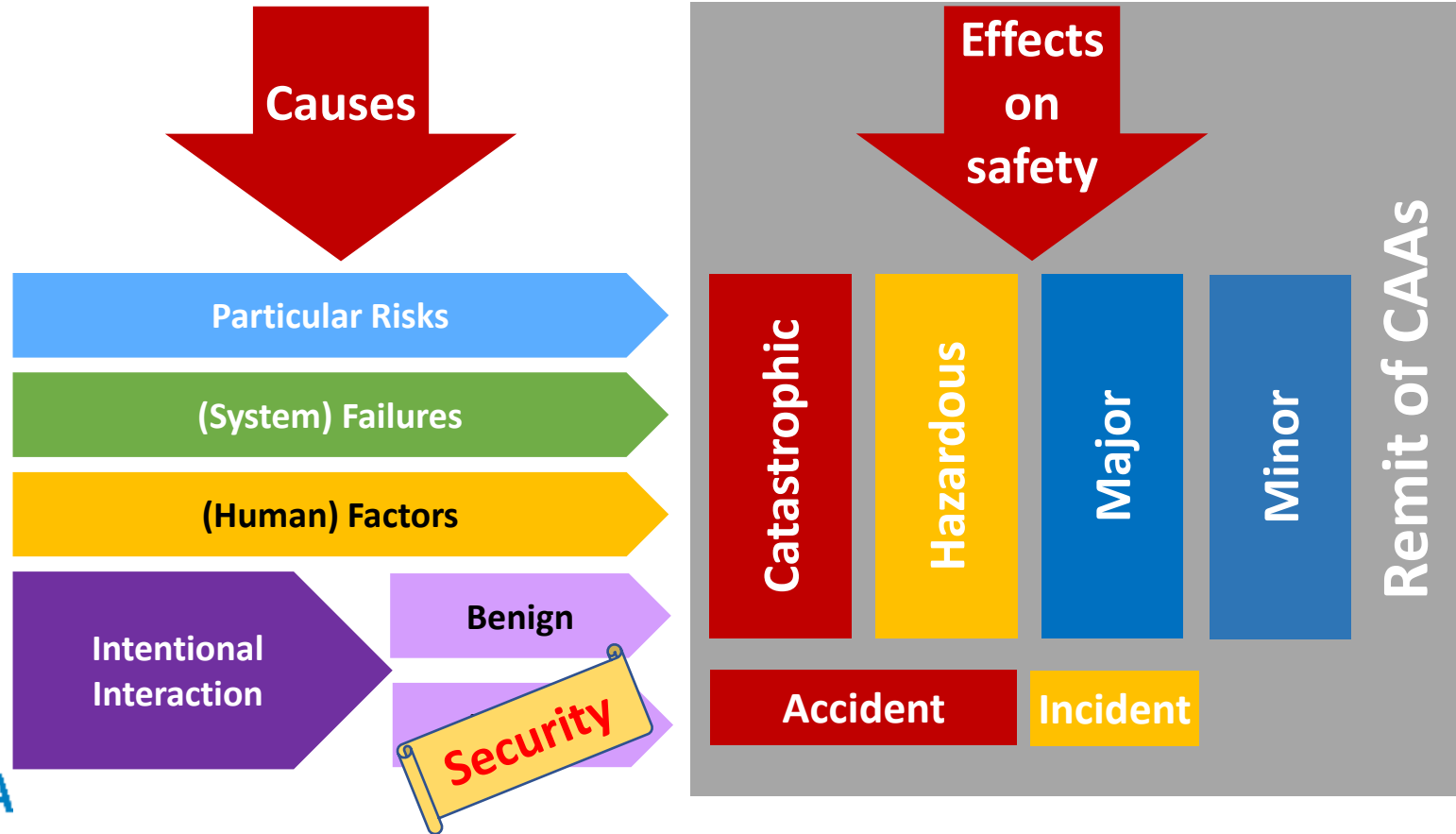
Secure System*

A **Secure System** does, what it is supposed to do.

And nothing else!

*) System = Totality of People, Processes, and Products

Relation between Causes and Effects



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

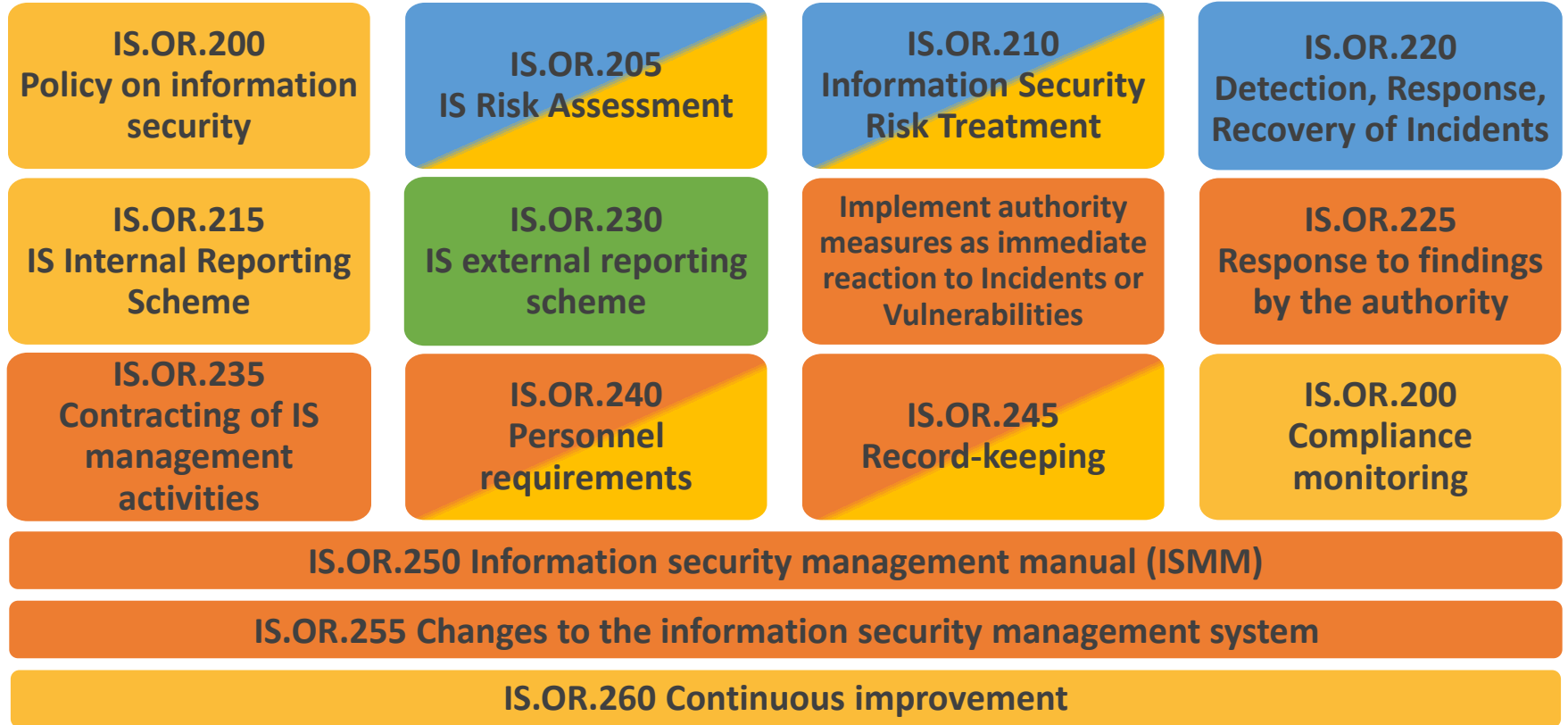
- Information Security Risk Treatment
- Information Security Incidents — Detection, Response, and Recovery



Reporting Regulation

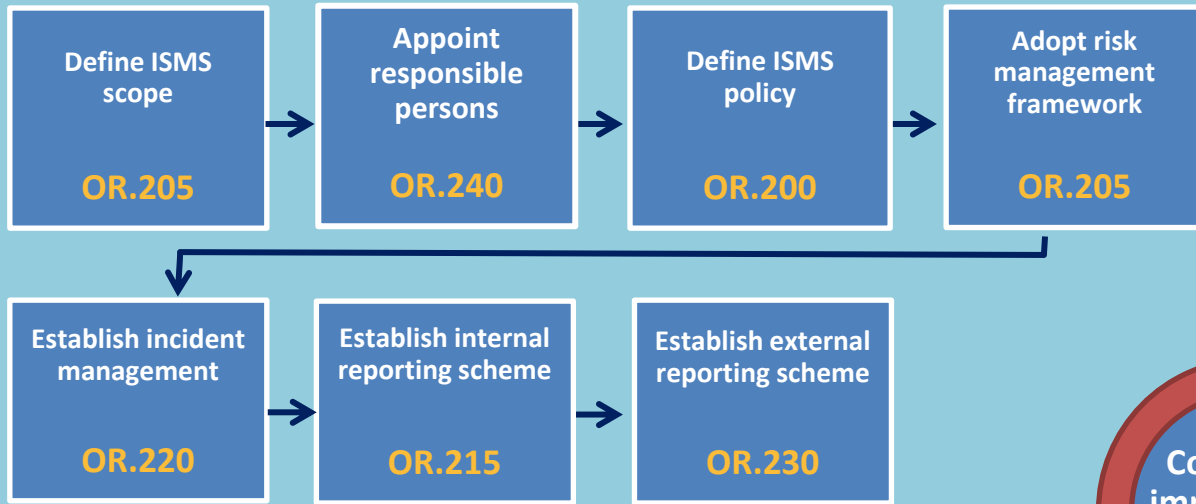
- Information Security External Reporting Scheme

The ISMS in Part-IS

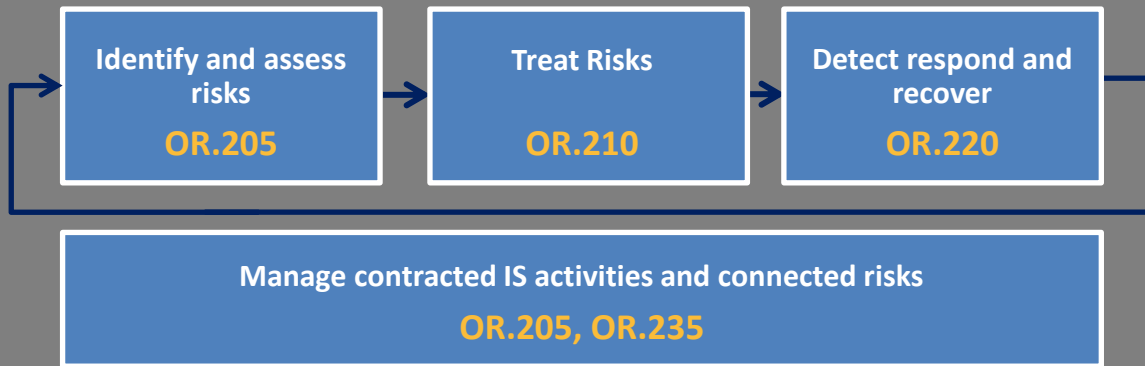


Colour code: NIST Framework ISO 2700x Basic Reg. Reporting Reg.

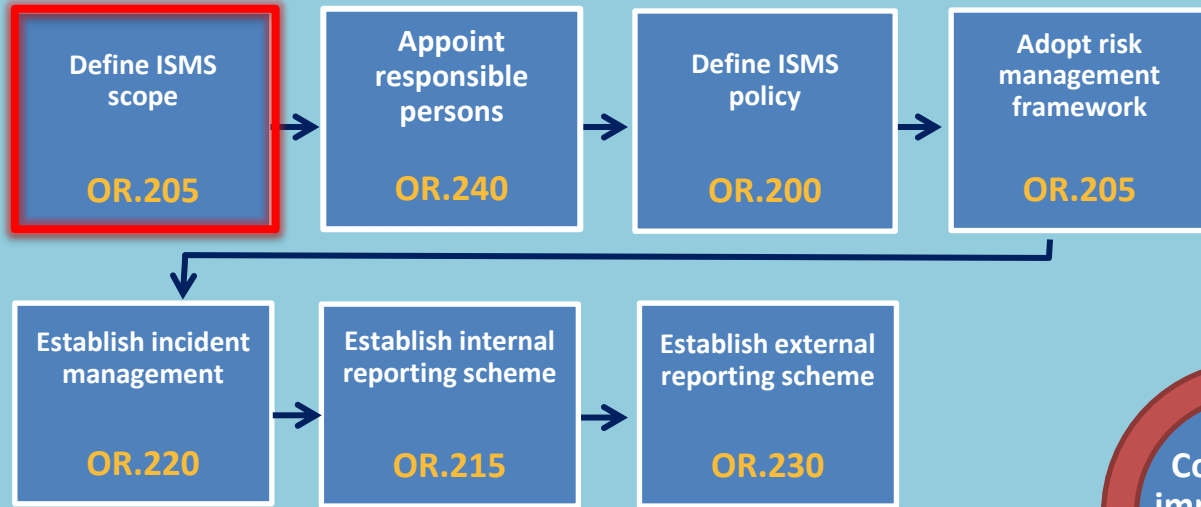
IMPLEMENT



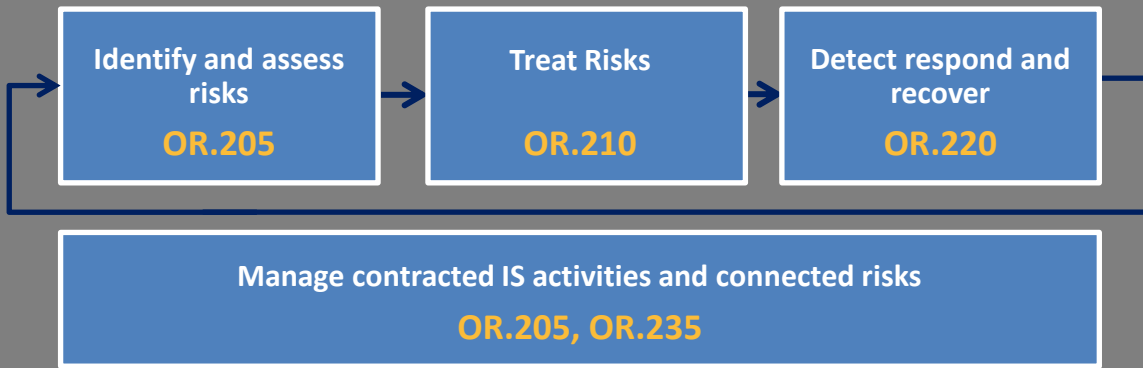
OPERATE



IMPLEMENT



OPERATE

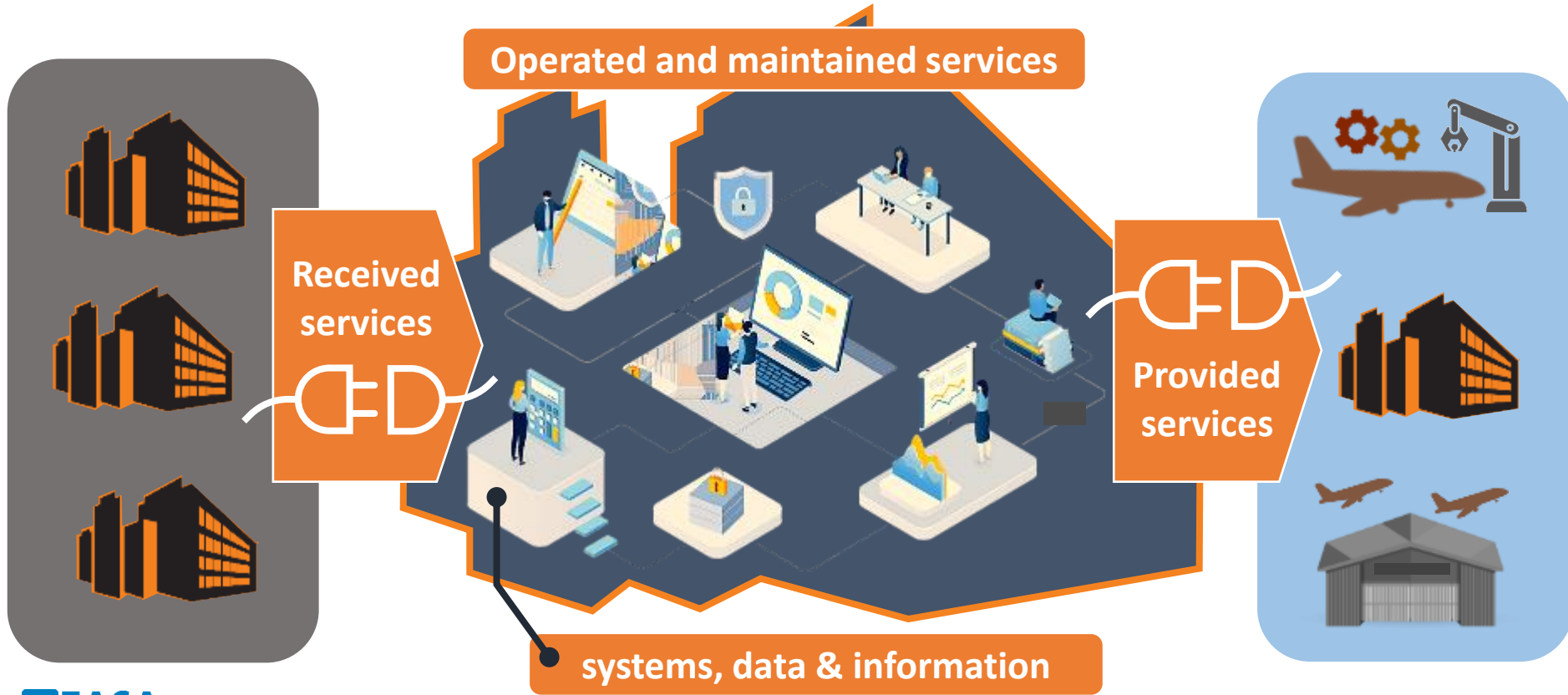


Creating Input for the ISMS Scope Definition

**AR/OR.205 (a) and (b):
Information Security Risk Assessment**

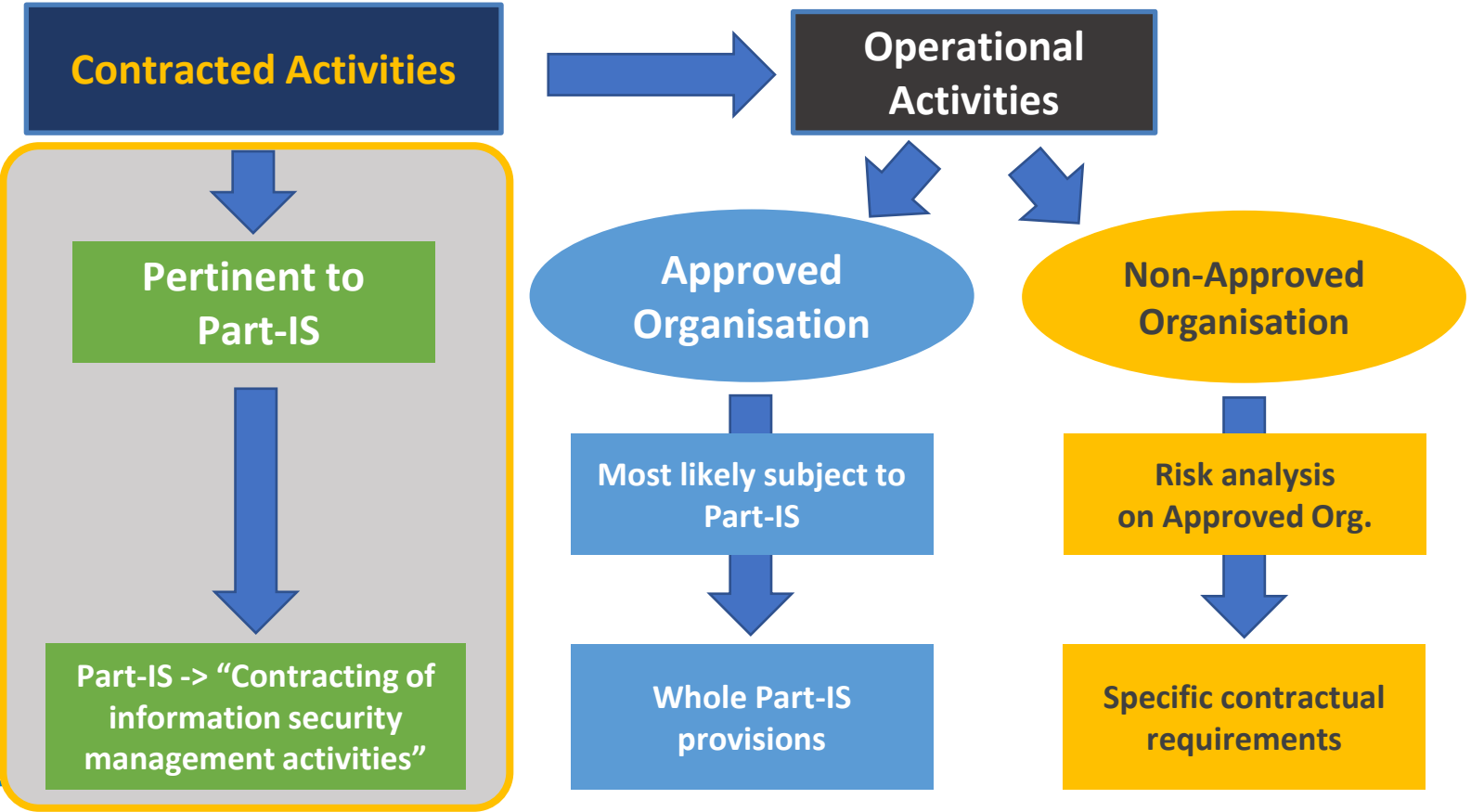
**AR/OR.205 (c)
...having a potential impact
on aviation safety**

Risk assessment - scope identification

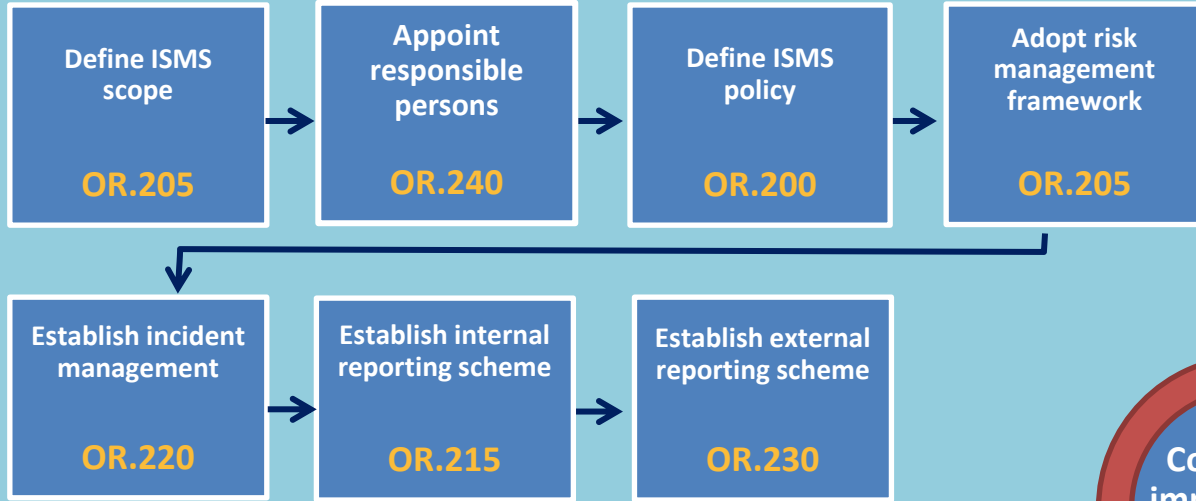


Suppliers are interfaced organisations

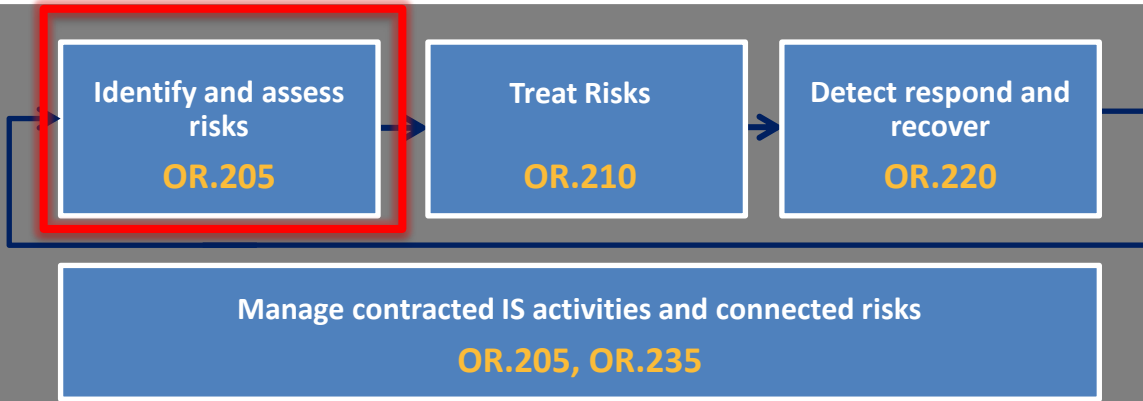
AMC&GM extract 1.1



IMPLEMENT



OPERATE



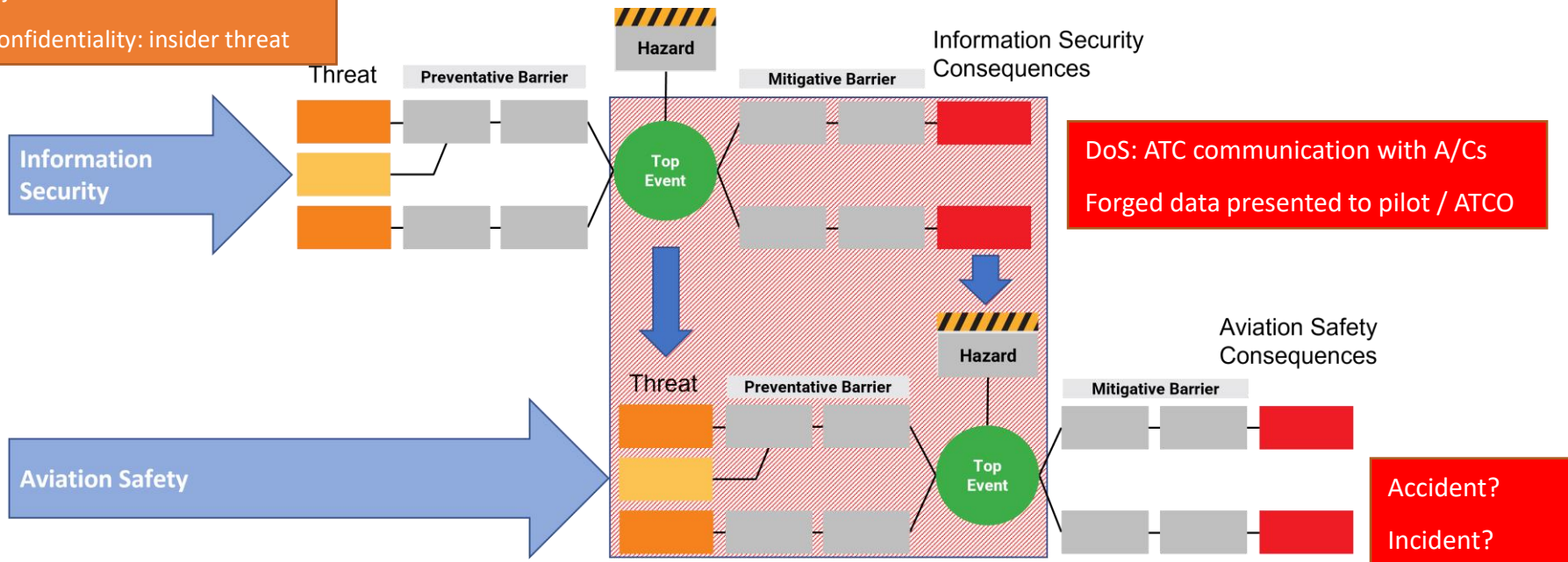
Risk acceptance

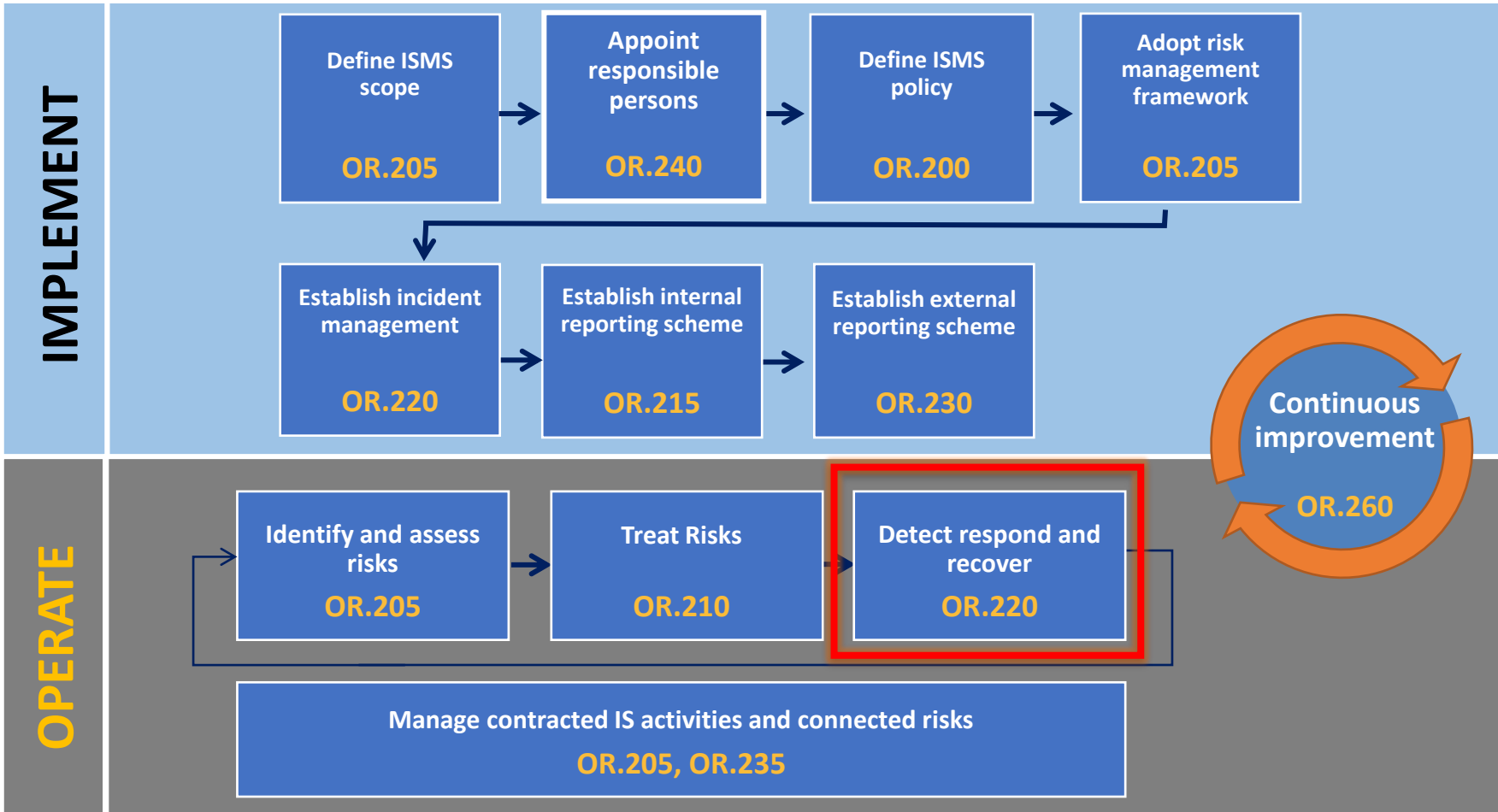
ICAO Annex 13 >	Negligible effect	Incident	Accident
Threat scenario — potential of occurrence	Low safety consequences	Moderate safety consequences	High safety consequences
High	Conditionally acceptable	Not acceptable	Not acceptable
Medium	Acceptable	Conditionally acceptable	Not acceptable
Low	Acceptable	Acceptable	Conditionally acceptable*

Figure 1: Risk acceptance matrix

Example 1

- Denial of Service
- Man in the middle
- Injection attacks
- Confidentiality: insider threat





Incident Response



→ A systematic and well-defined approach to managing and mitigating the impact of a cybersecurity incident.

→ The incident response process typically involves four main stages

1 Prepare

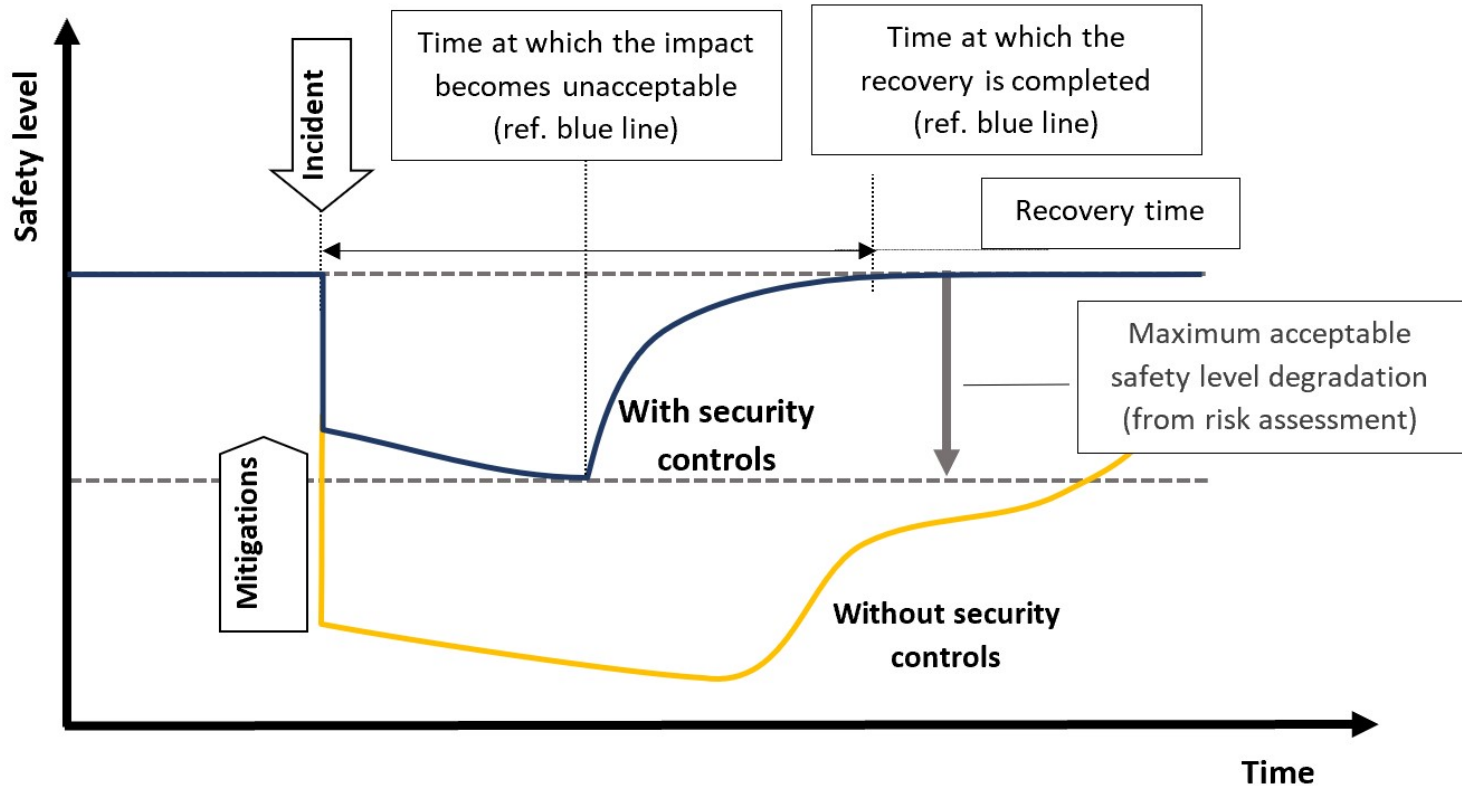
2 Detect

3 Contain

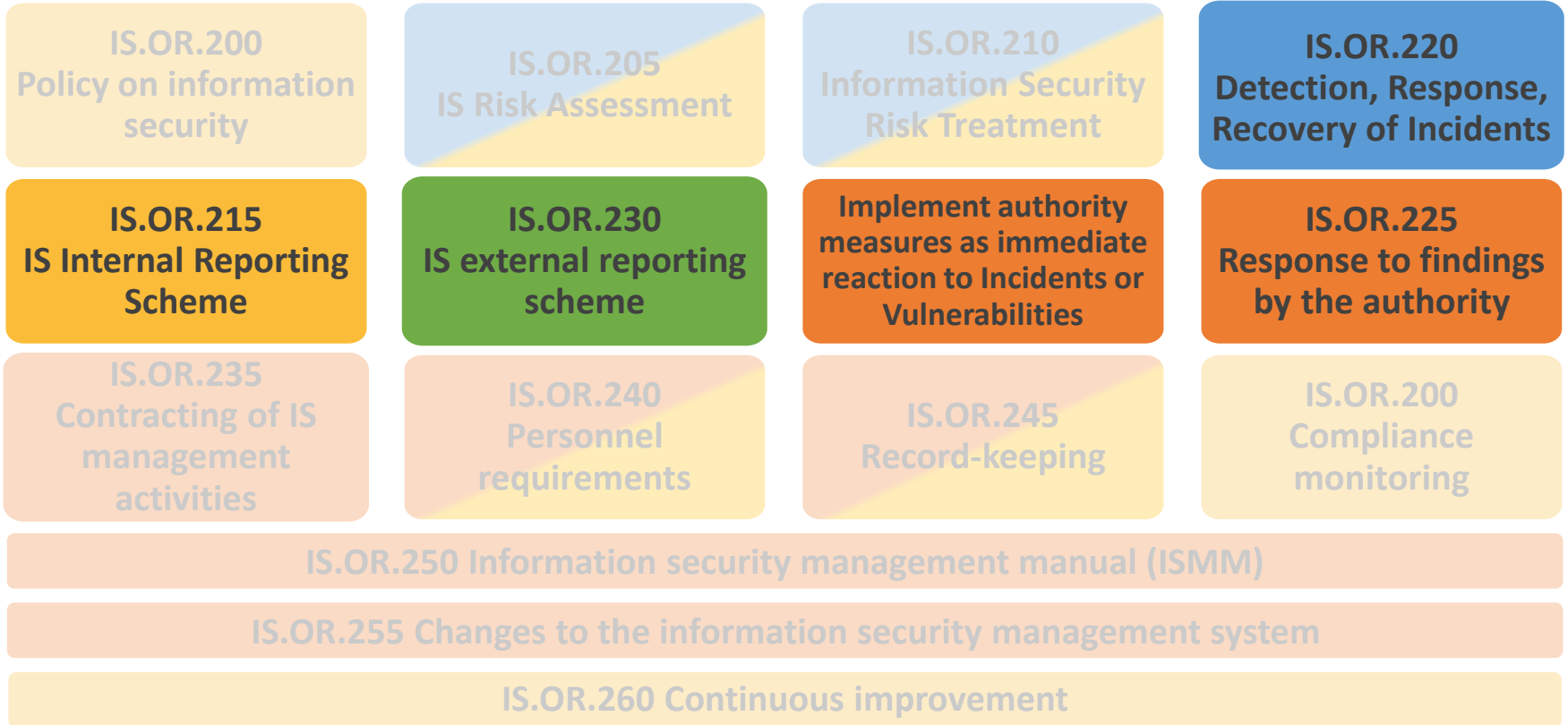
4 Recover

→ Following a incident response process, minimizes the impact of a cybersecurity incident and quickly resume normal operations.

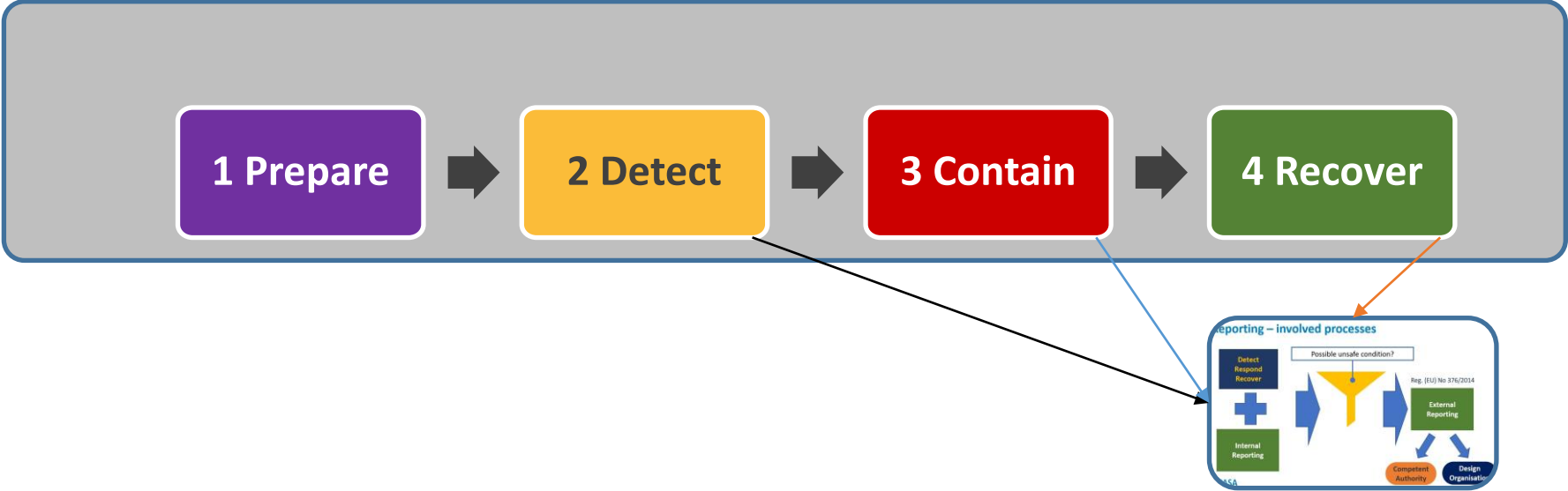
Response and recovery



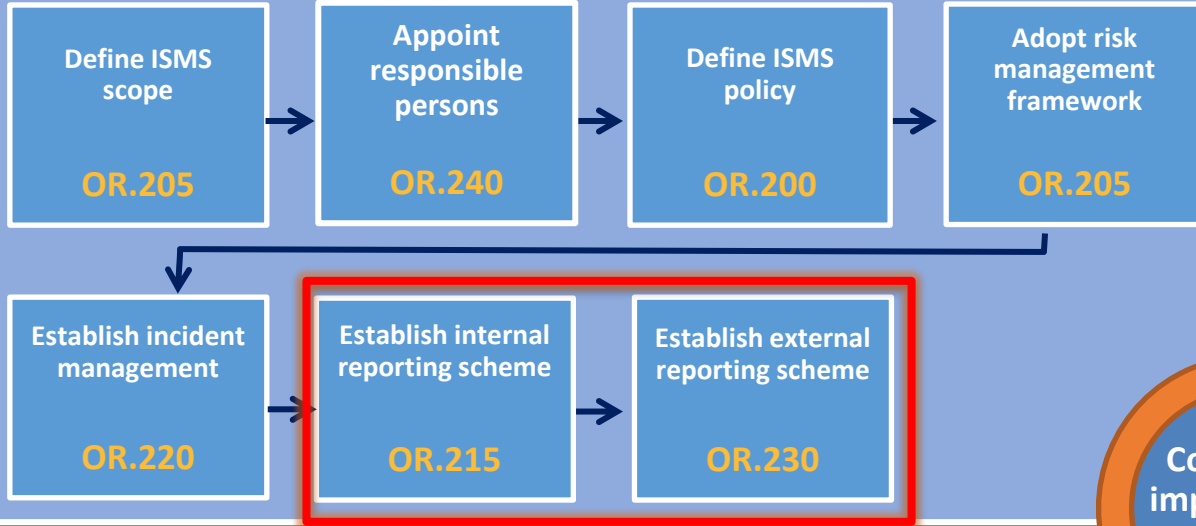
Incident Management in Part-IS



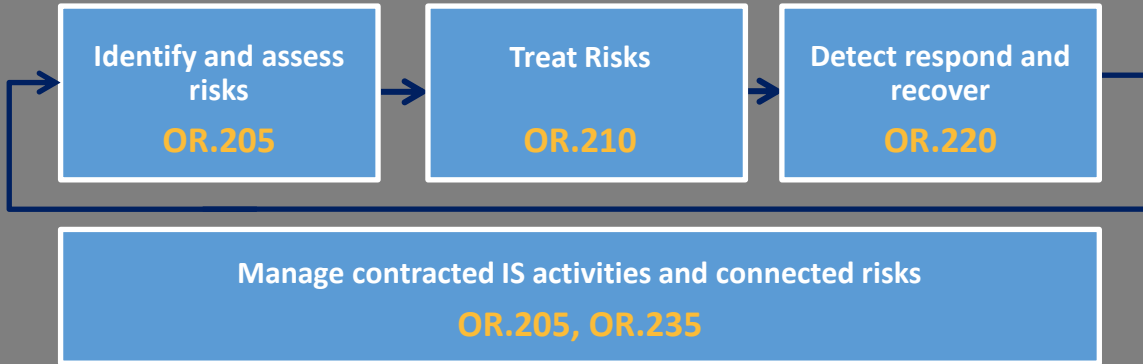
Incident Response and reporting



IMPLEMENT



OPERATE



PART-IS ANNEX I

Authority Requirements (AR)

IS.AR.200
ISMS

External Reporting

Organisations
subject to its
oversight &
information
received through
IS.I.OR.230



PART-IS ANNEX II

Organisations Requirements (OR)

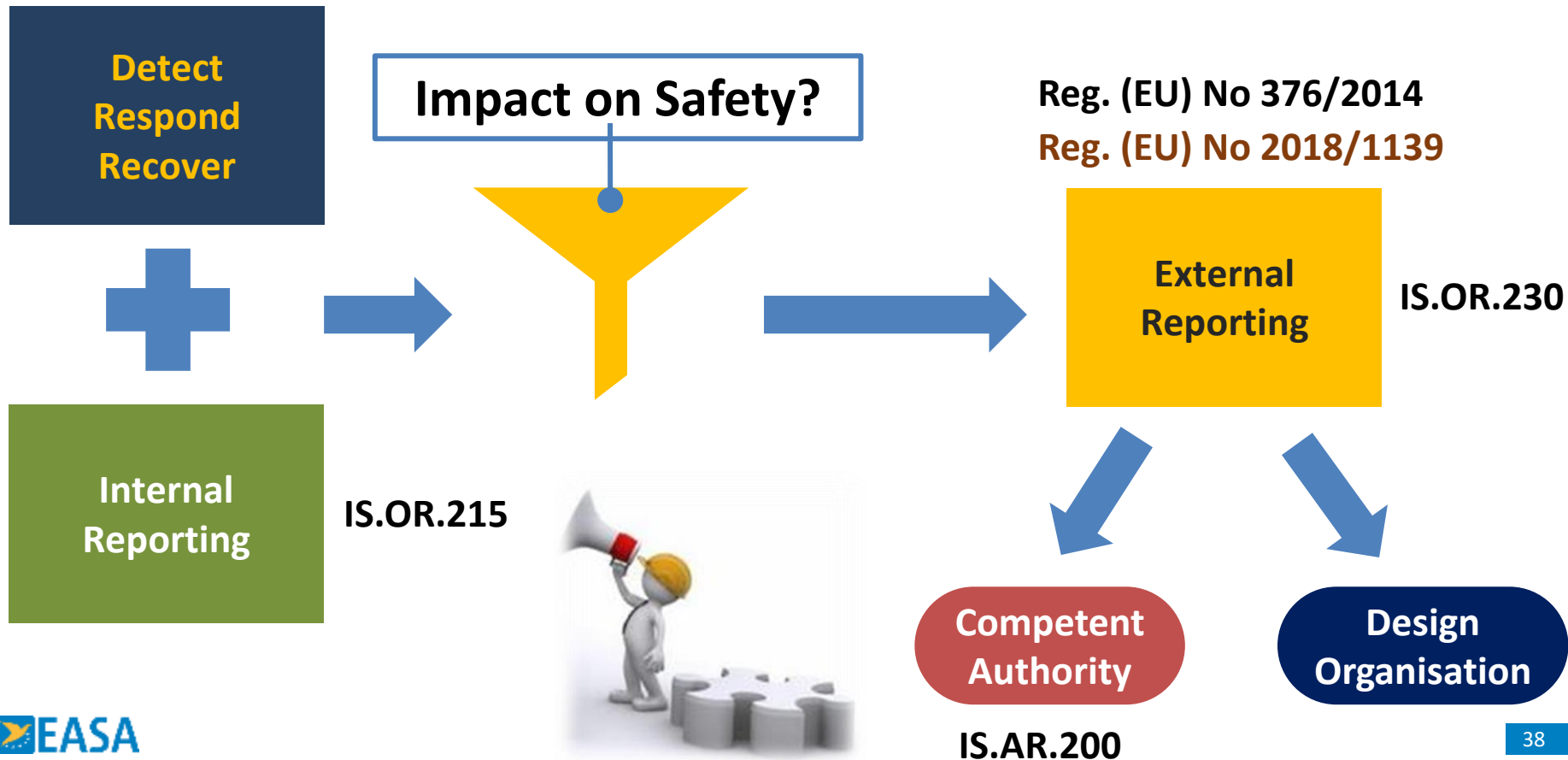
IS.OR.215
Internal Reporting

Internal Reporting
Cyber incidents
&
Vulnerabilities
with a potential
**impact on aviation
safety**

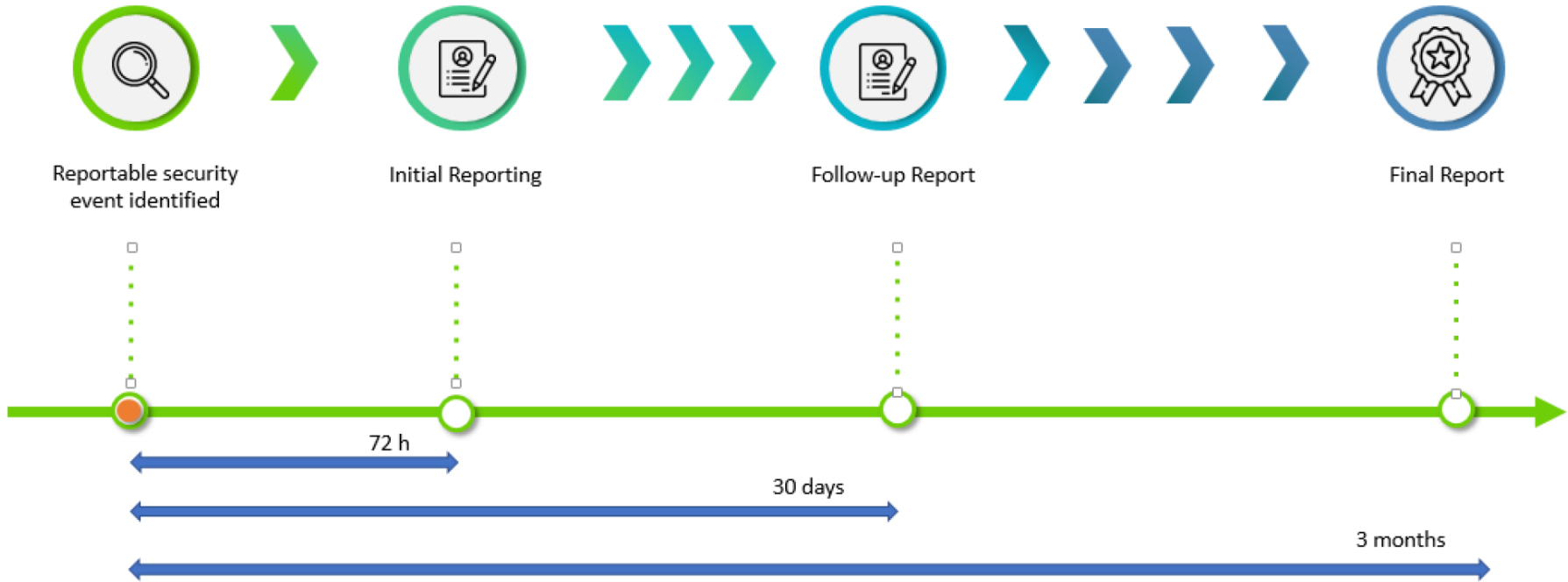
IS.OR.230
External Reporting

External Reporting
Reg (EU) 376/2014
Reg (EU) 2018/1139
Report to:
- Competent Authority
- Design Approval Holder
- Design of system/
constituent
- Not exceeding 72 h

PART-IS Reporting Aspects Overview



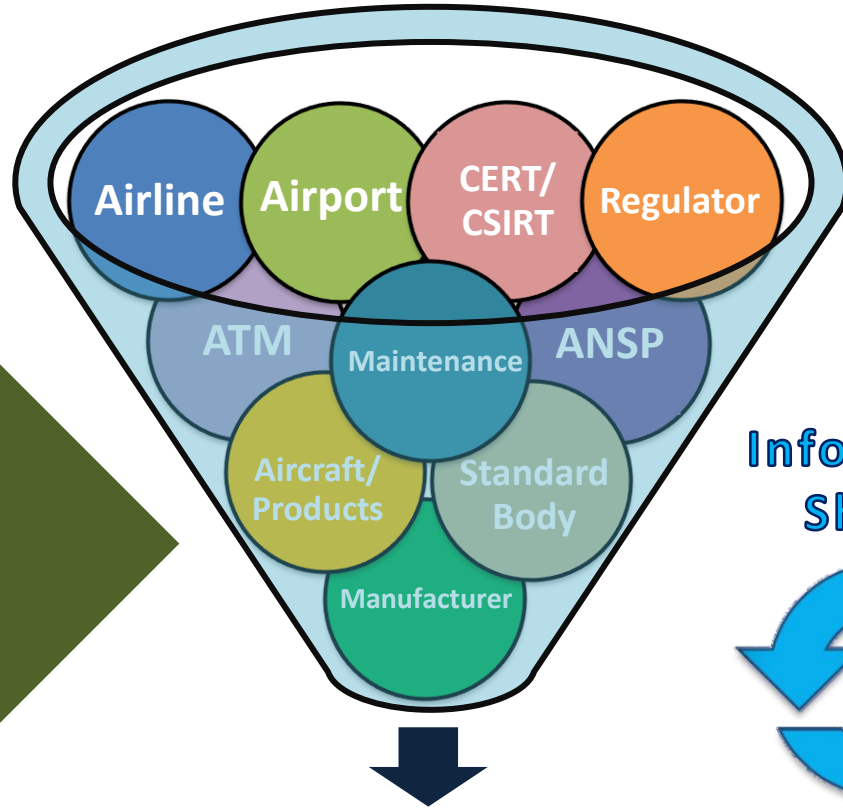
ED-206 6.4.2 Reporting Timeline example



Goal 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

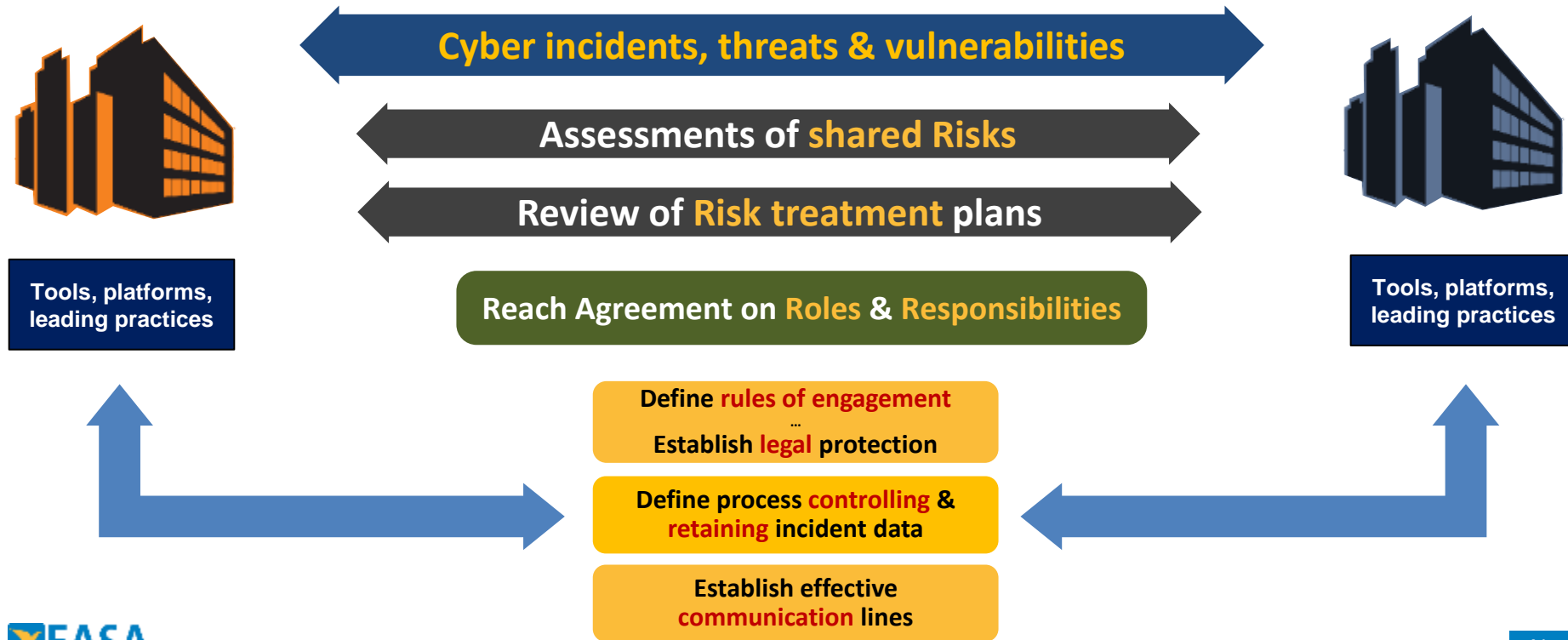


**Information
Sharing**

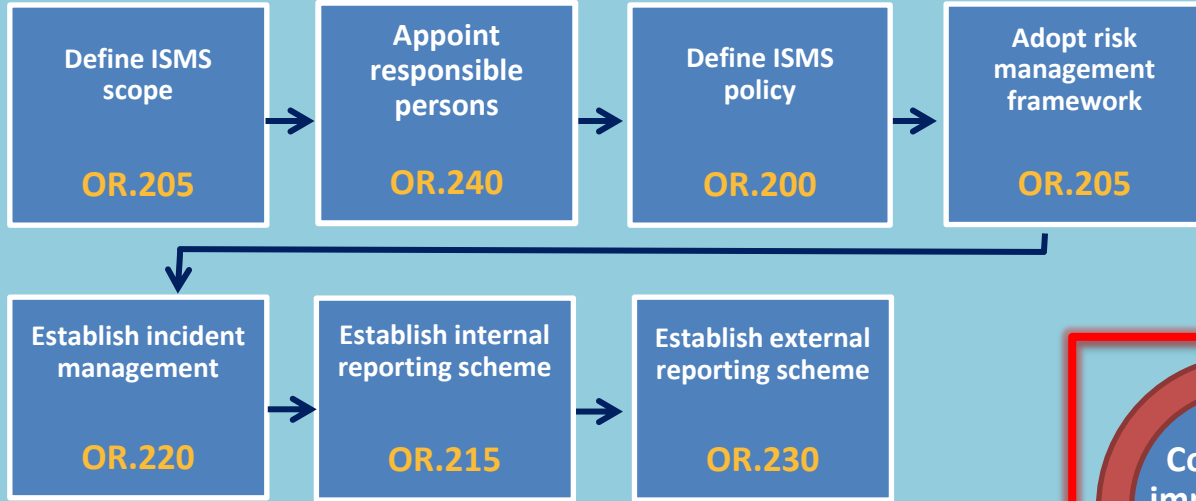


Resilience of the Aviation ECO-System

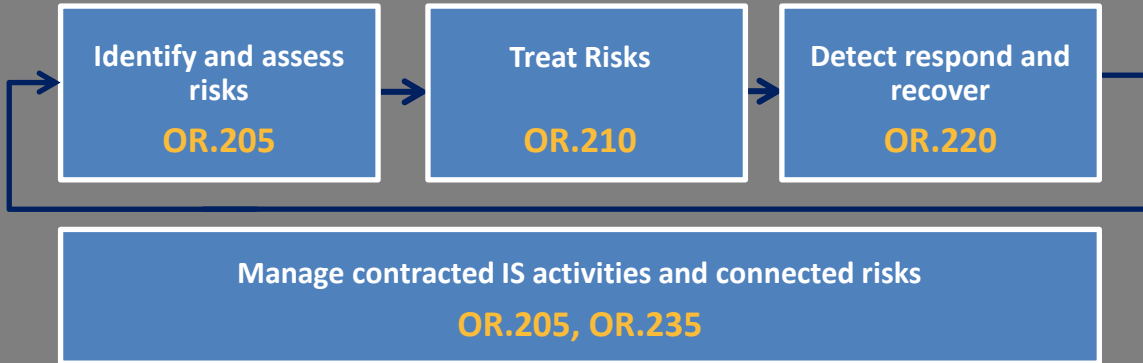
Sharing information between organisations



IMPLEMENT



OPERATE



Continuous Improvement – Two Reasons

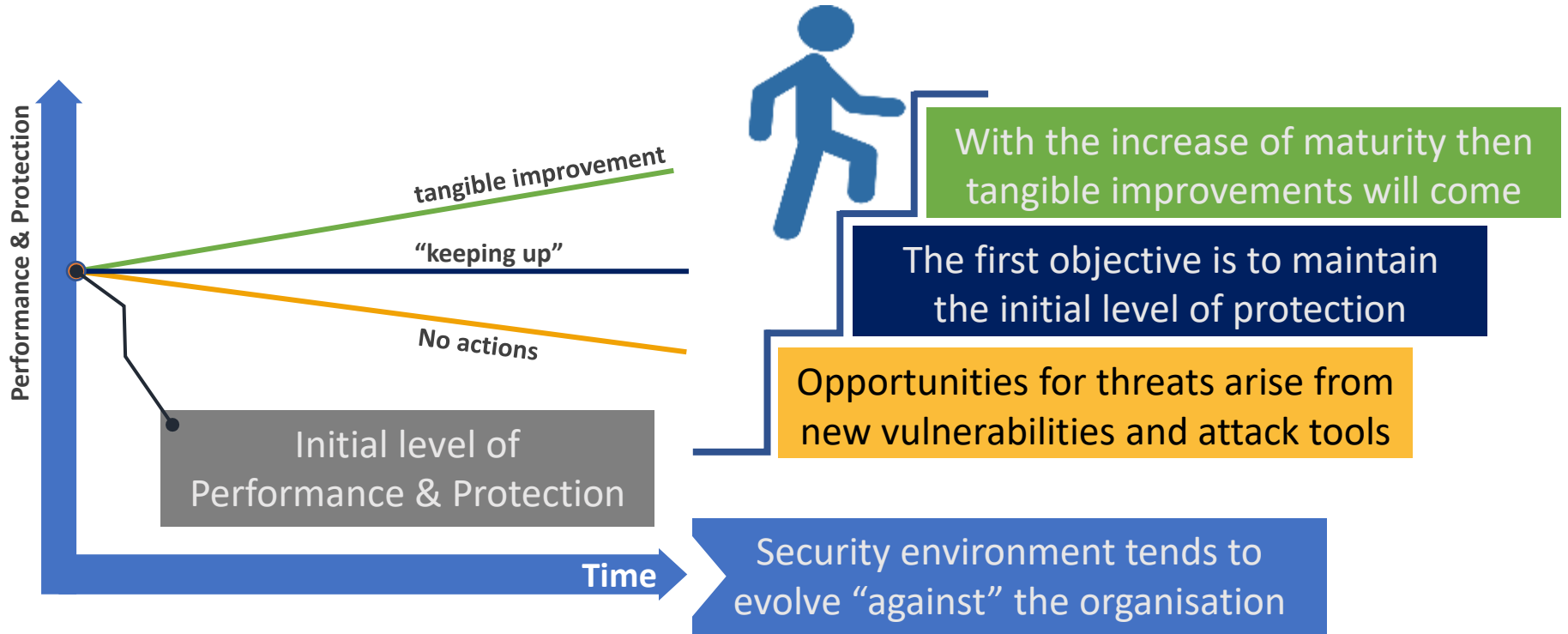
Organisation

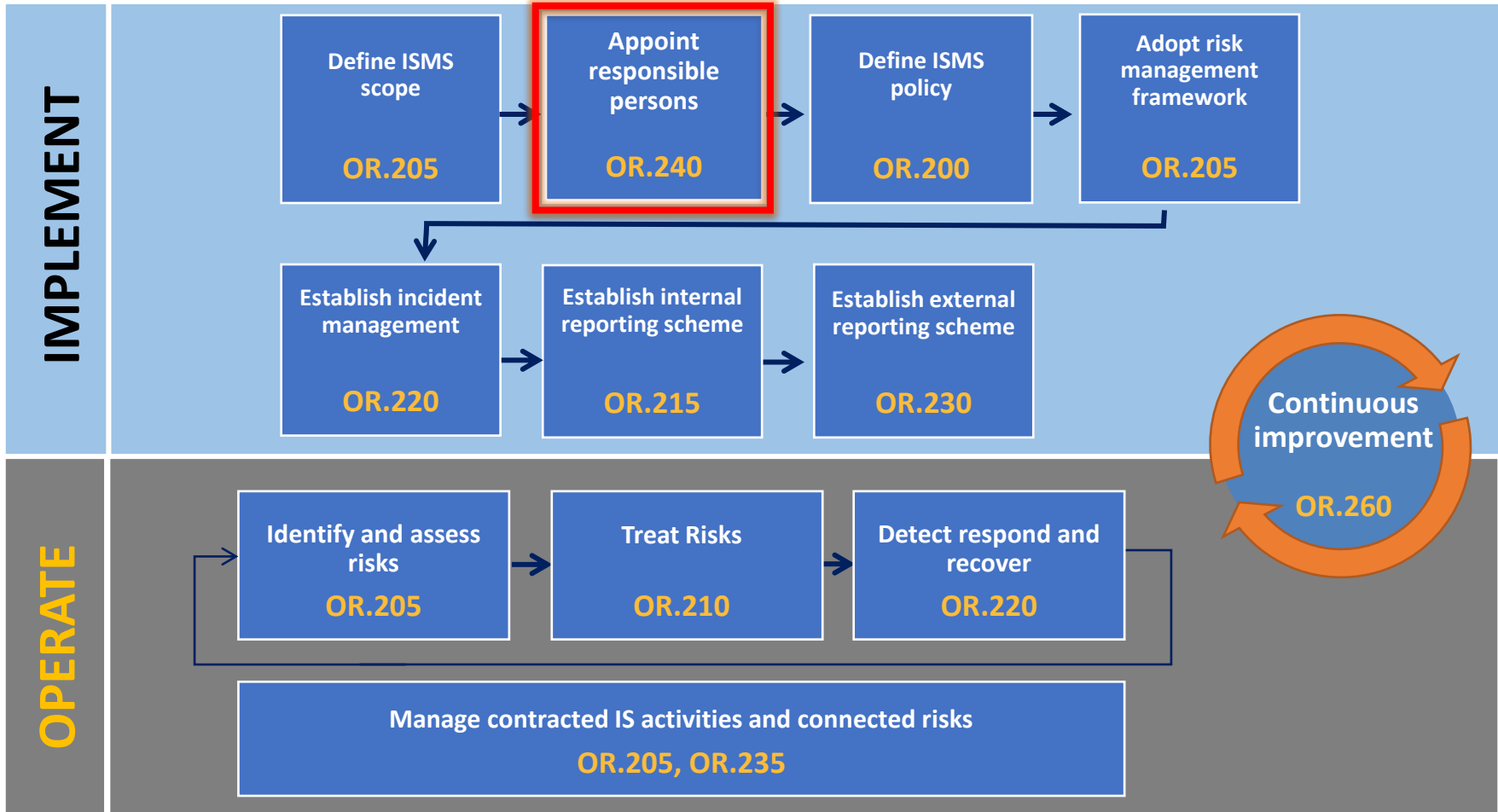
Dynamic adaptation to the evolution and change of the objectives, architectures, organisational structures and processes of an entity, which are reducing the level of compliance

Security Environment

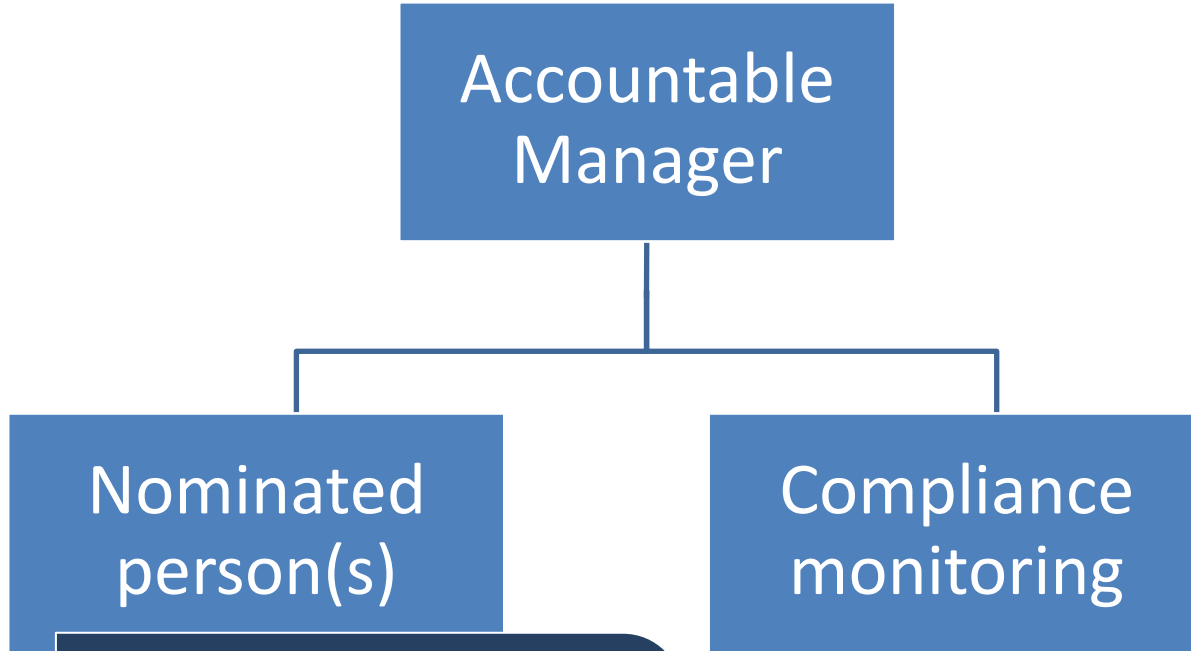
Dynamic adaptation to constantly emerging discovery of vulnerabilities, threat actors, tools and methods, which are reducing effectiveness of controls

Continuous improvement – Security Environment



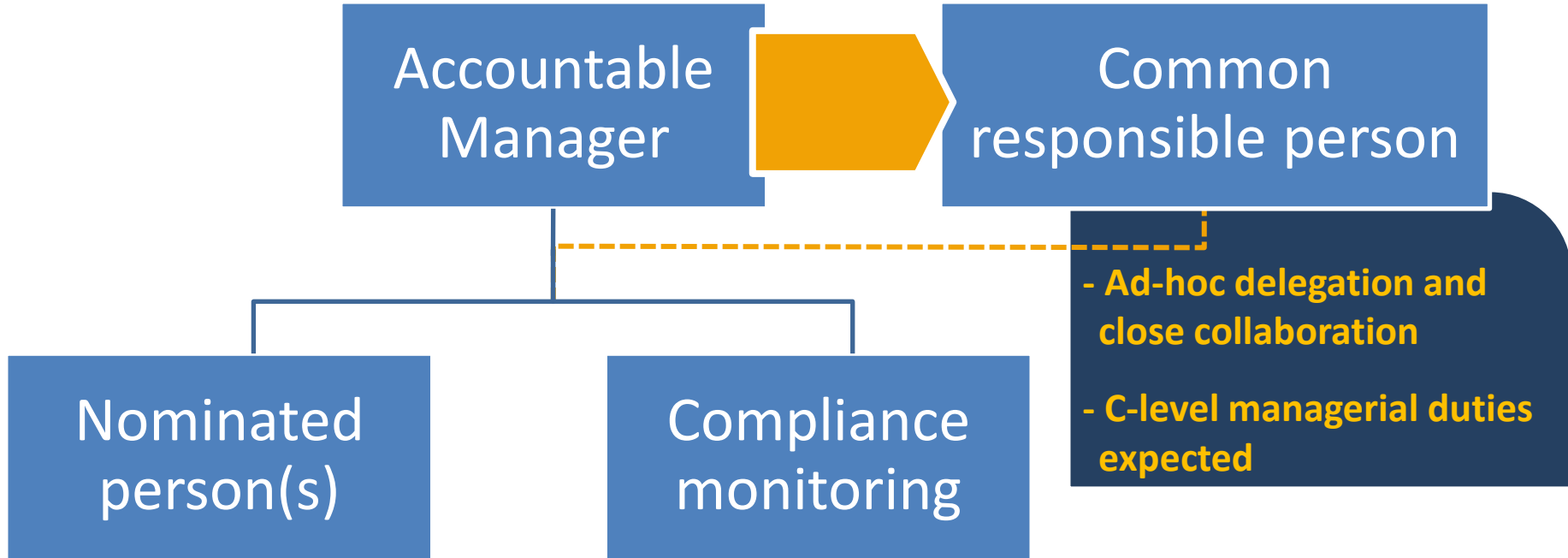


Organisational structure

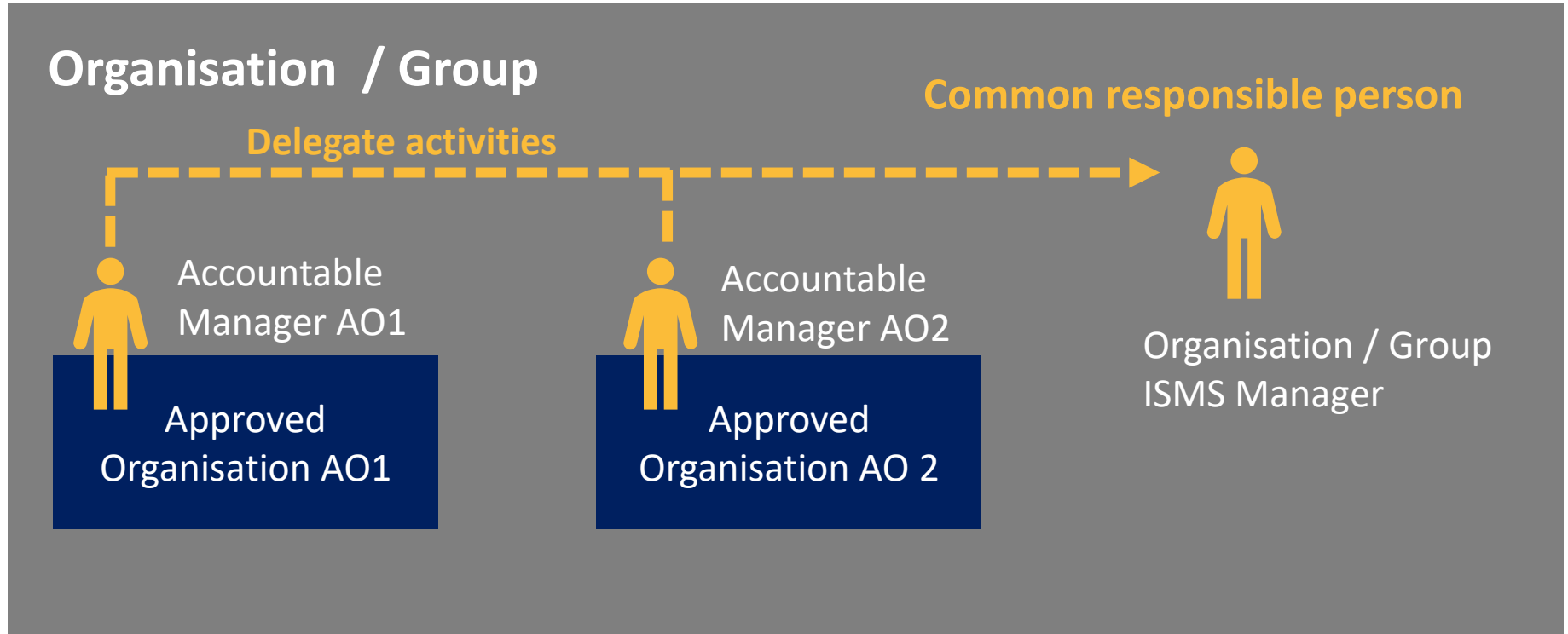


How to make this delegation of responsibility effective?

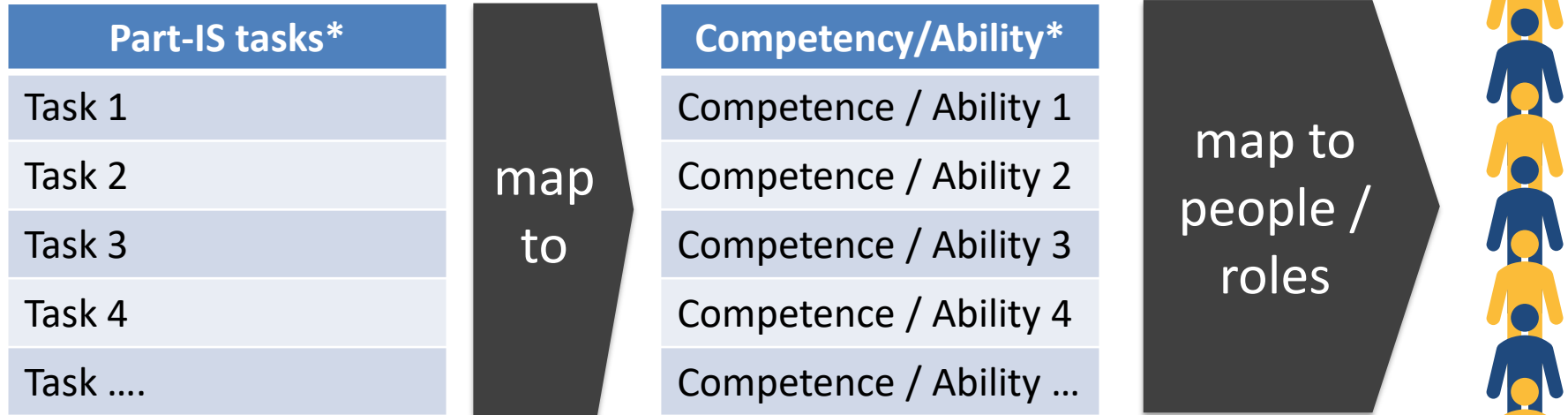
Organisational structure



Common responsible person



Personnel Competence



* Appendix II provides a mapping between Part-IS Tasks and NIST CSF v1.1

ENISA Cybersecurity Skills Framework

European Cybersecurity Skills Conference 2023

ENISA is pleased to announce the 2nd edition of the annual European Cybersecurity Skills Conference. This year the conference will focus on sharing and discussing progress linked to the promotion and endorsement of the ENISA Cybersecurity Skills Framework (ECSF). The conference will also address ENISA's role as part of the European Commission initiative: The Cybersecurity Skills Academy.

SAVE THE DATE

**2ND EUROPEAN
CYBERSECURITY
SKILLS CONFERENCE**

21-22
SEPTEMBER | Segovia, Spain
2023

**EUROPEAN
CYBERSECURITY
SKILLS FRAMEWORK**
Segovia

EASA

Logo row: EASA, Spanish Government, Portuguese Government, TR, INCIBE, ENISA, U23

Standard roles proposed by ENISA



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

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

Current and future standards for Part-IS

2018

NIST Cyber Security Framework v1.1

2022

ISO 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

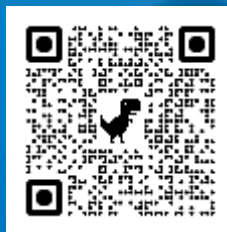
2024

ED-20X/Do-3xx – ISMS for aviation organisation

Thank you for your attention

Contact us at:
cybersec@easa.europa.eu

Join our Community:



easa.europa.eu/connect



Your safety is our mission.

An Agency of the European Union 



Cybersecurity

A National Approach

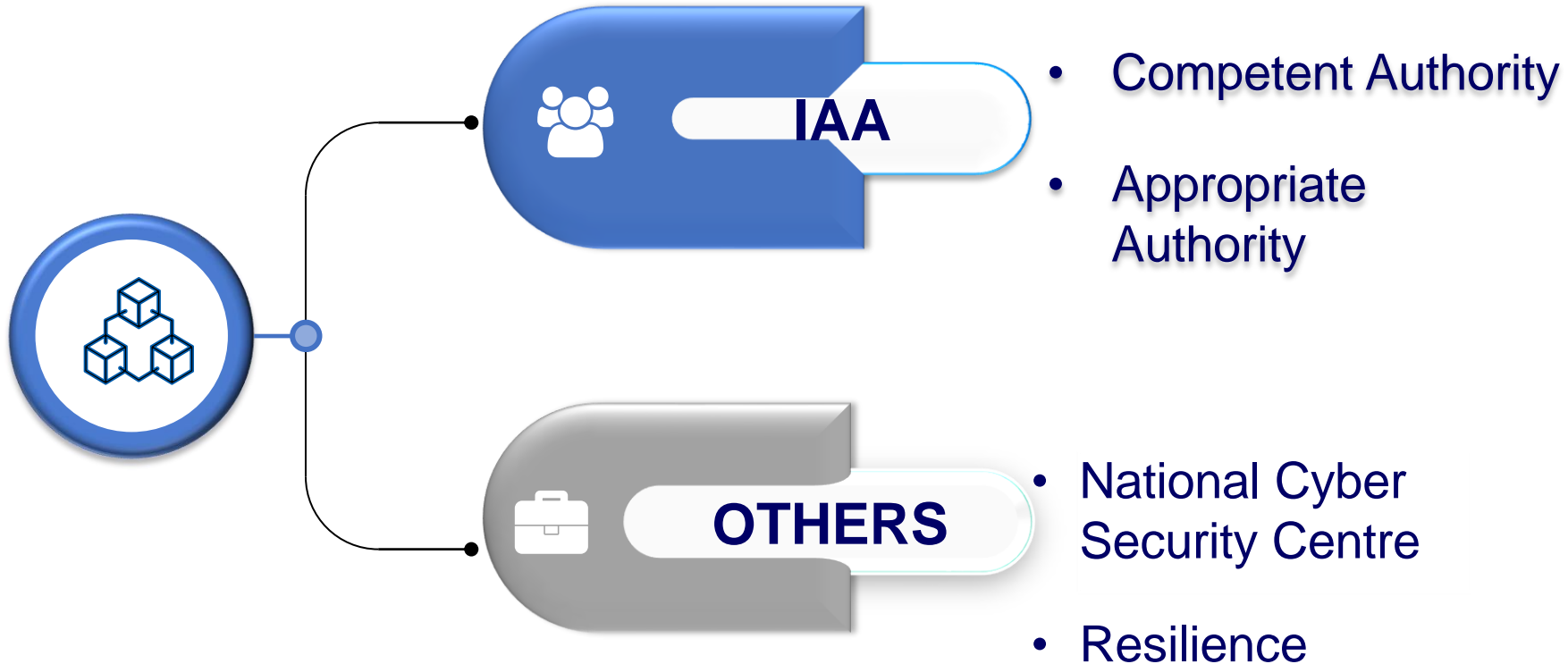


Overview

- Regulatory Roles
- Cybersecurity regulation
 - Process
 - Resources
 - Reporting
- Looking ahead
- Conclusions



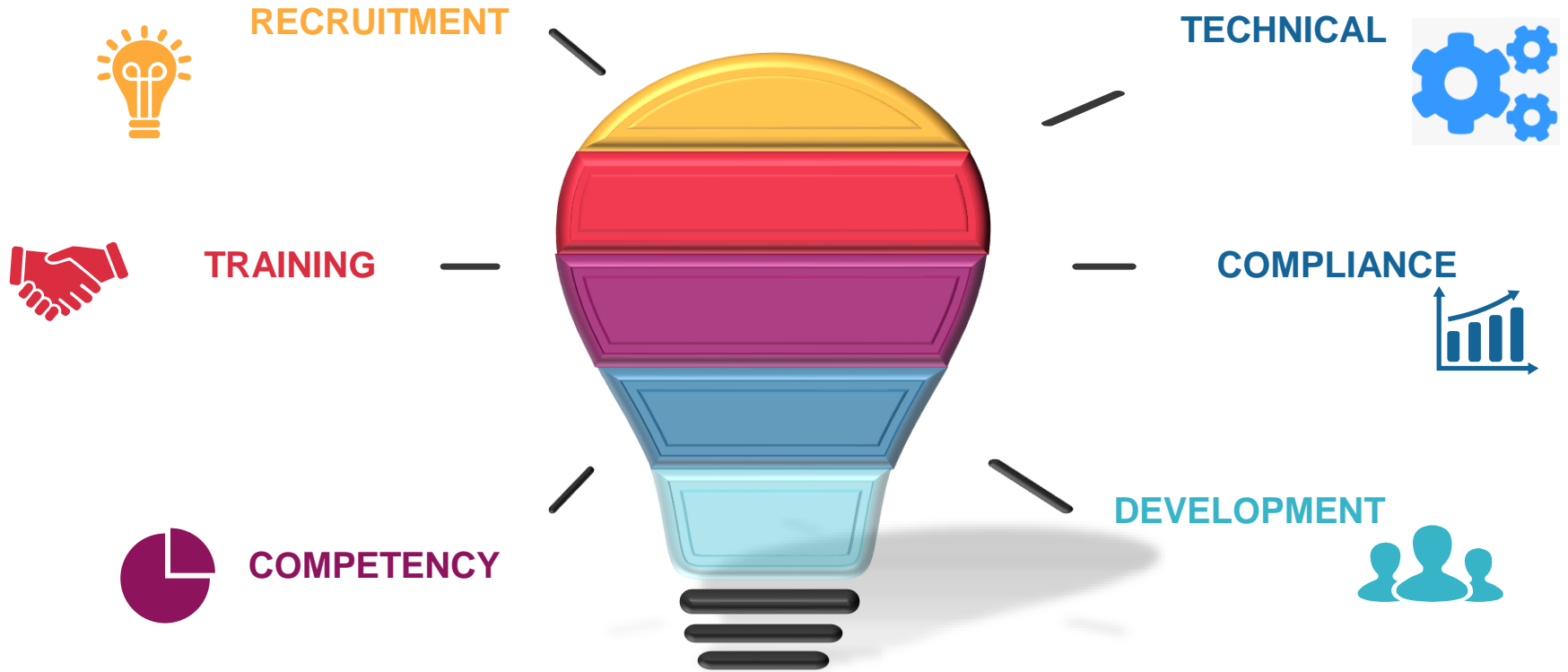
Regulatory Roles



Process



Resources



Reporting

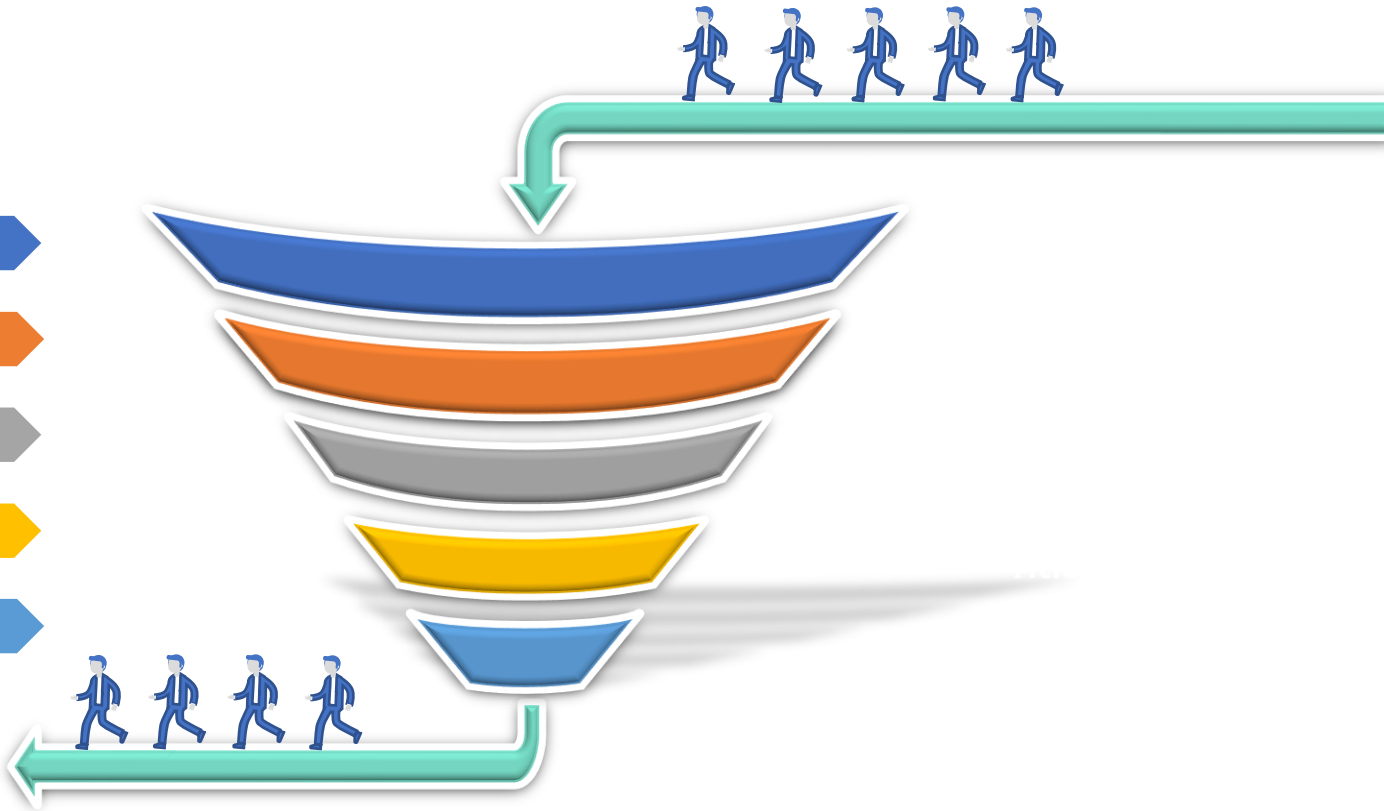
AVSEC

ECCAIRS

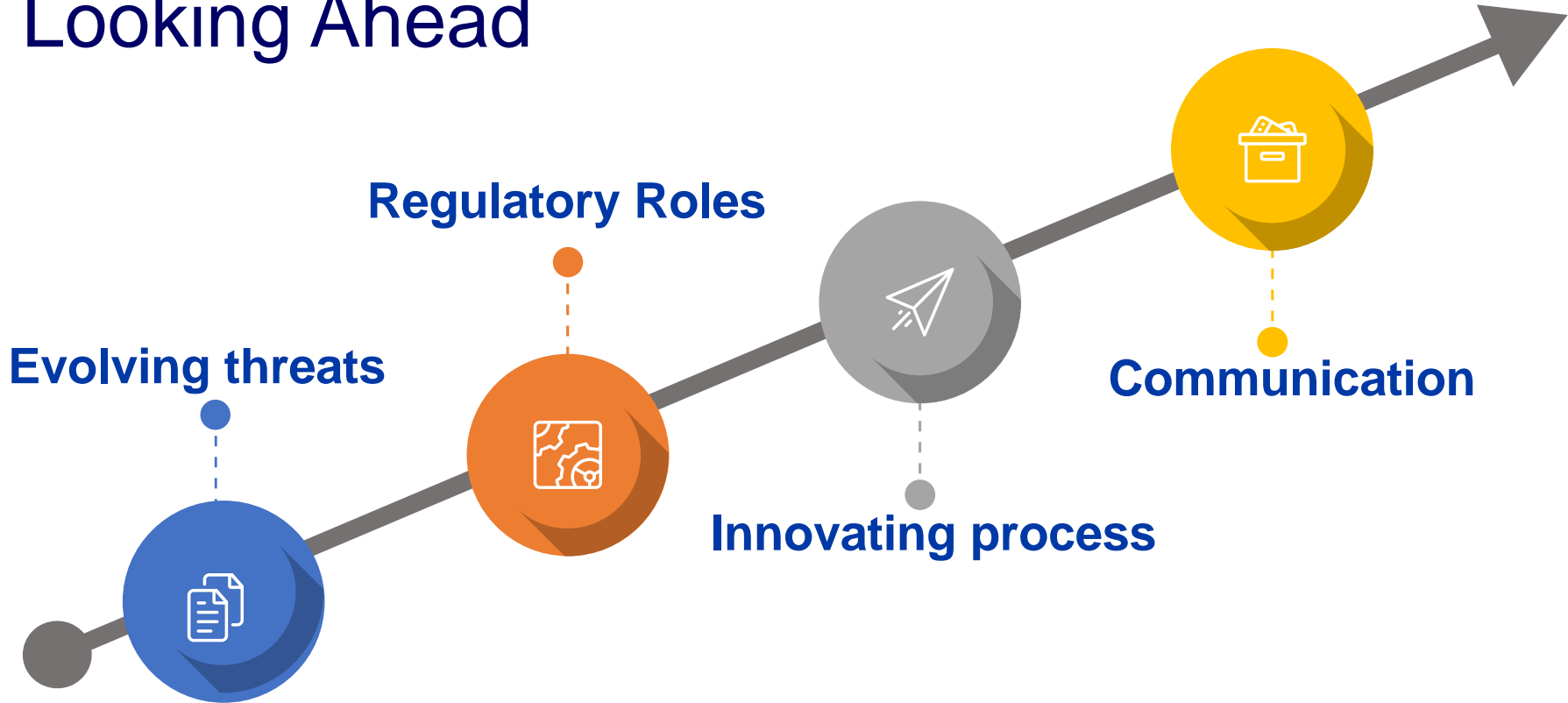
AGS

NCSC

International



Looking Ahead



Conclusions



Threat: Focus and mitigation



Effective management systems



Coordinated effort

Thank You

