

PART-IS regulation

Understanding specific provisions

Davide Martini

Senior Expert – Cybersecurity in Aviation

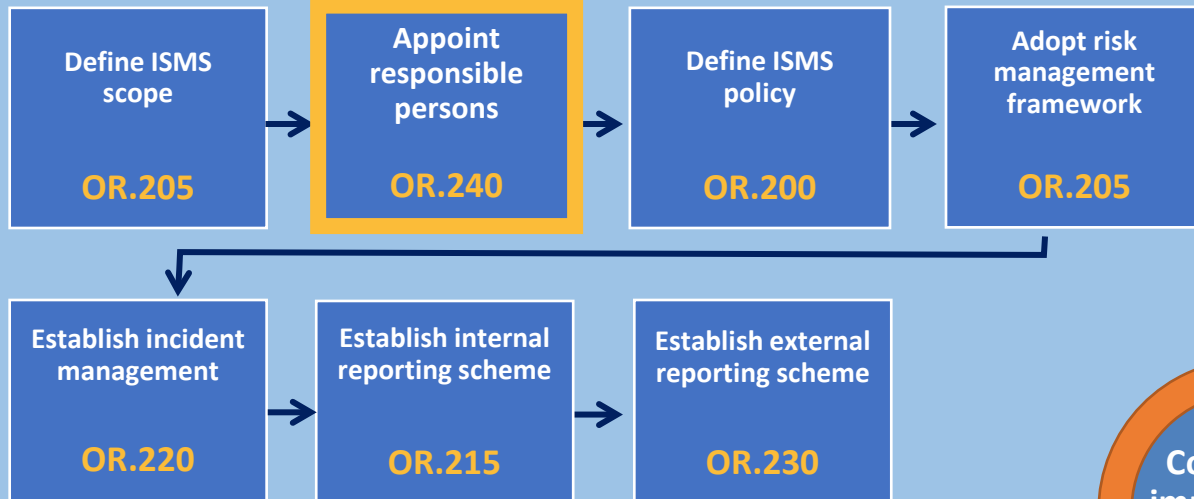
Cybersecurity in Aviation & Emerging Risks

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

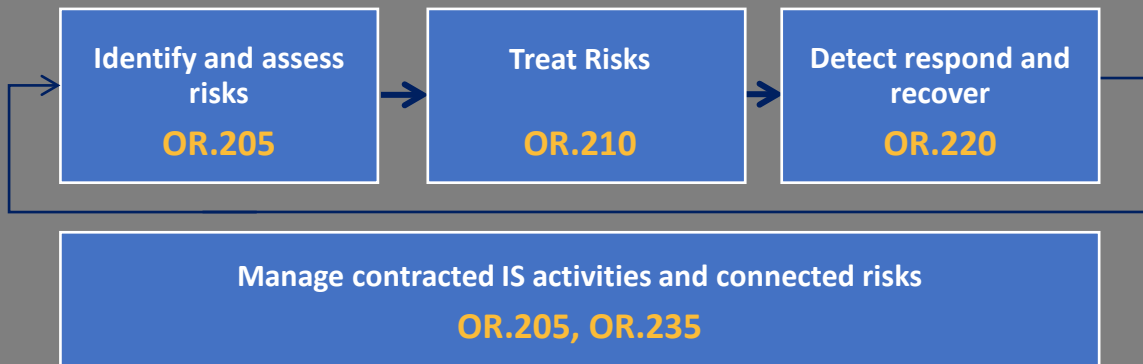
Your safety is our mission.

ORGANISATIONAL STRUCTURE AND PERSONNEL COMPETENCES

IMPLEMENT



OPERATE



OR.240

IR

- The accountable manager (AM) is also accountable for Part-IS
- The AM shall appoint a group of competent persons to comply with Part-IS
- The AM may delegate its activities to a common responsible person (CRP)
- Sufficient and competent personnel shall be available
- Personnel shall be trustworthy

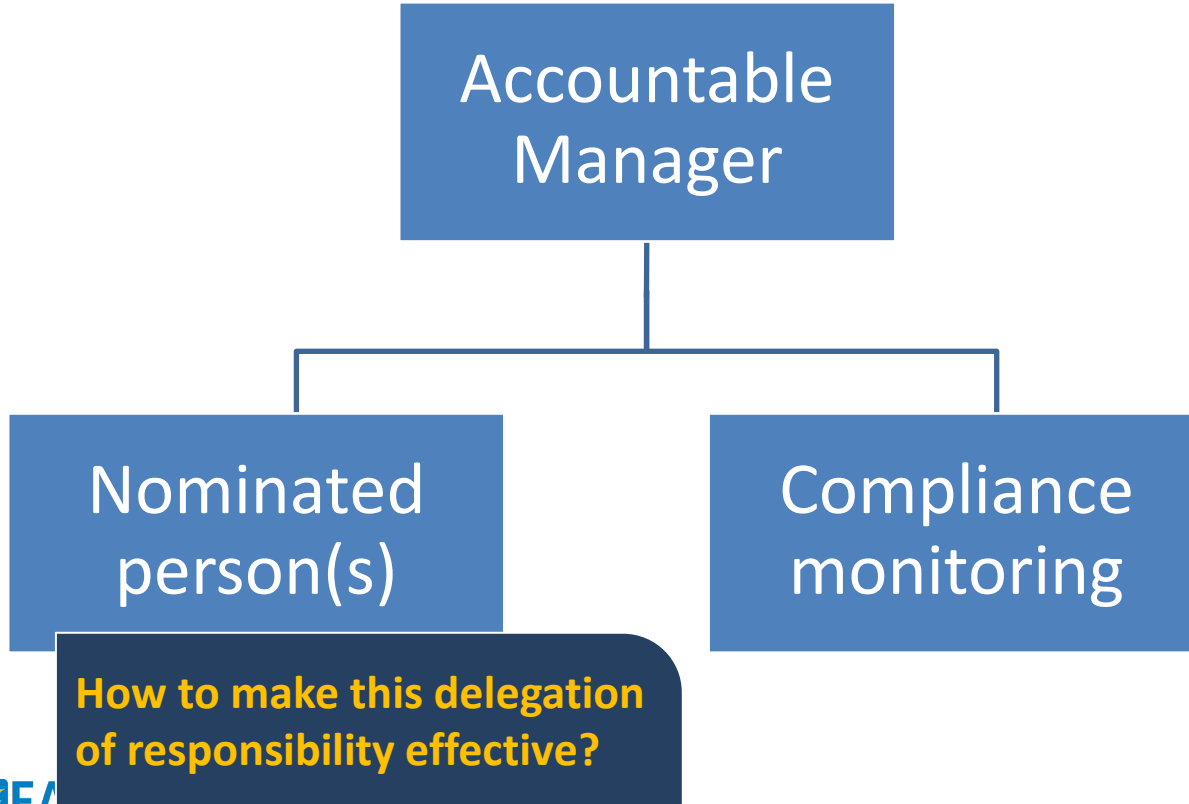
AMC

- Person or group of persons directly responsible to the AM
- CRP coordinates with the AM and boundaries are well defined
- Sufficiency decided considering org. structure, interfaces and level of risk
- Competence to be evaluated on the basis of the personnel role and tasks
- Trustworthiness initially established by means of vetting

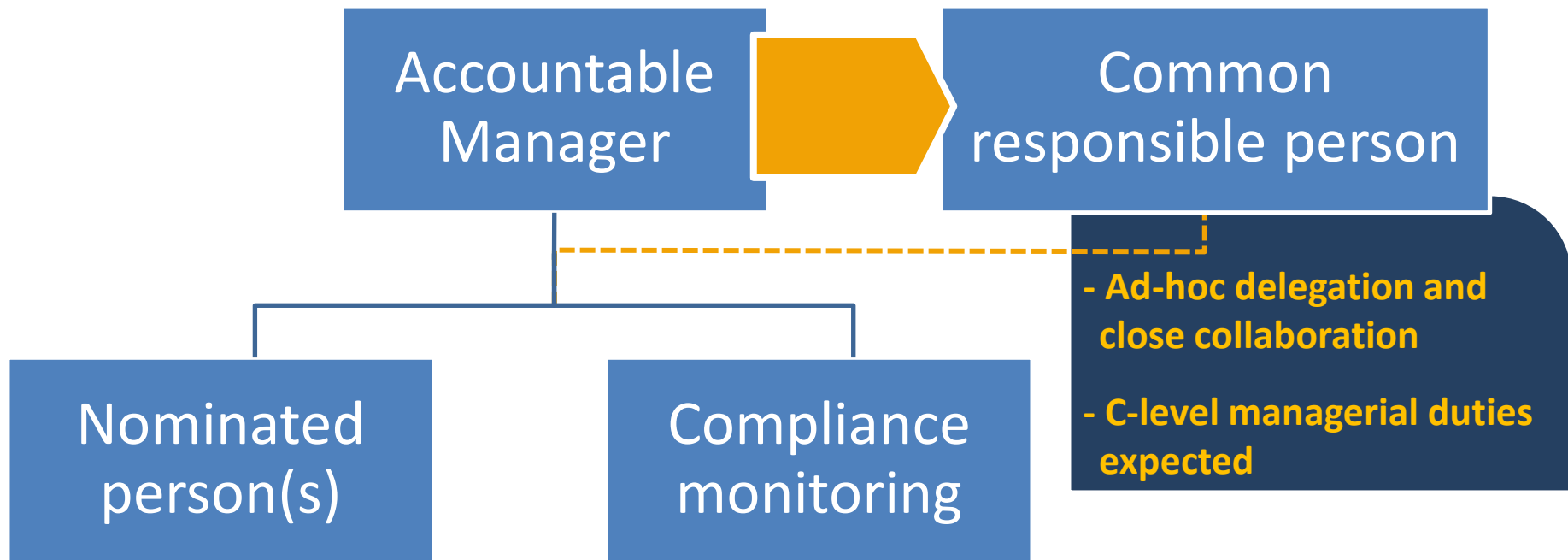
GM

- Profile of common responsible person
- Appendix II
 - Main task stemming from Part-IS
 - Link between tasks and competencies in NIST CF v1.1.

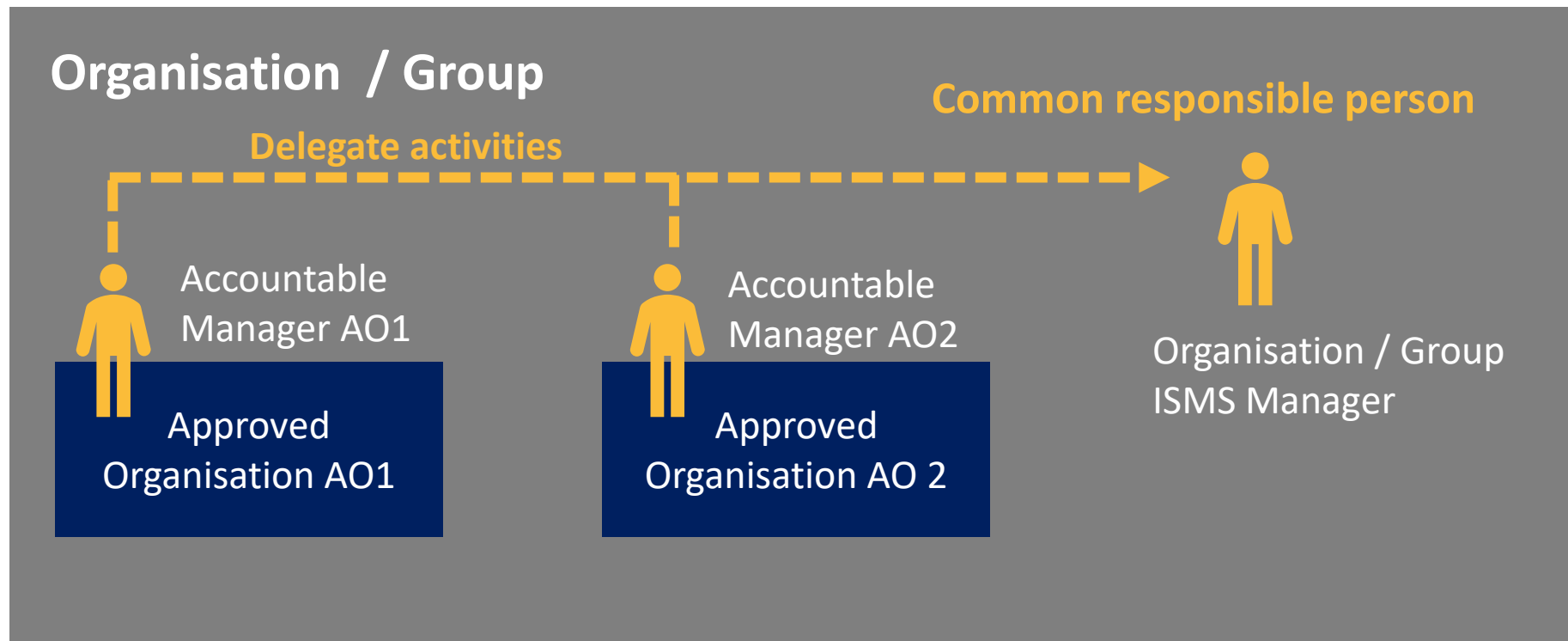
Organisational structure



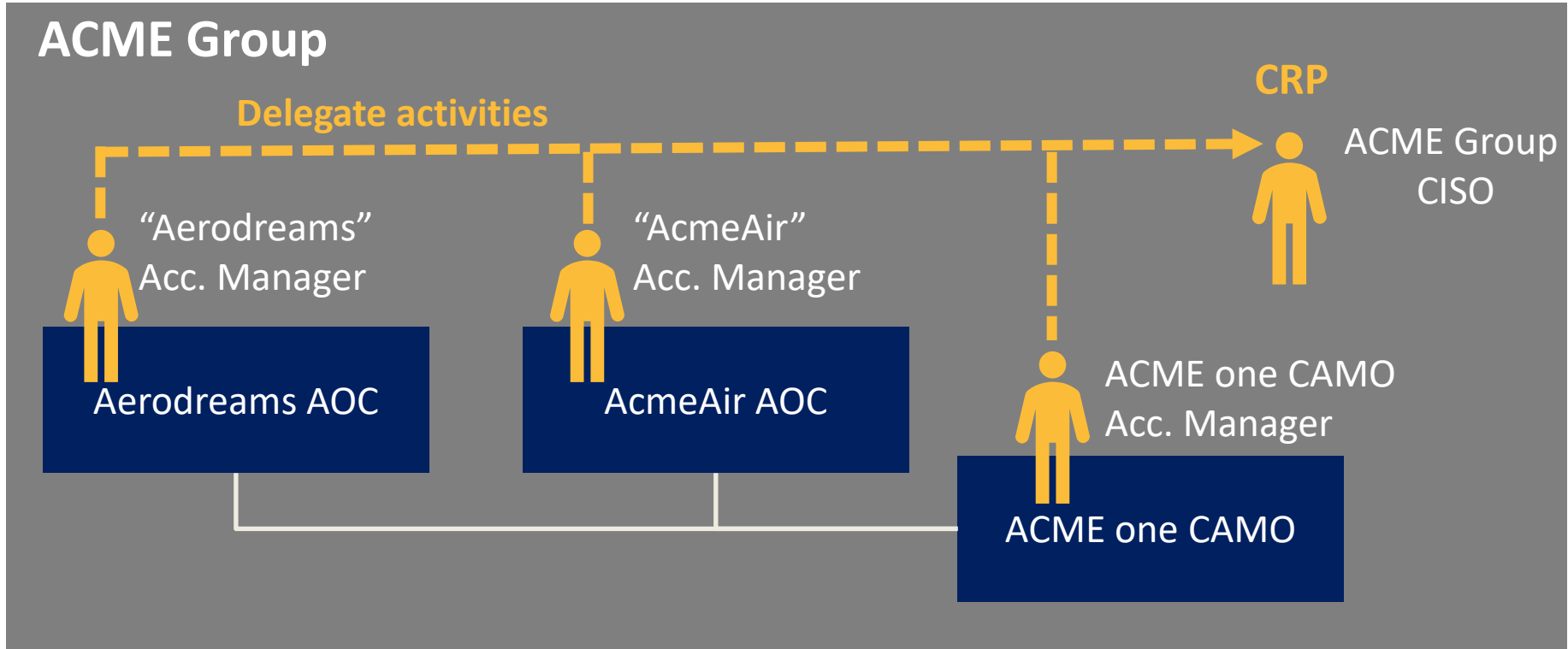
Organisational structure



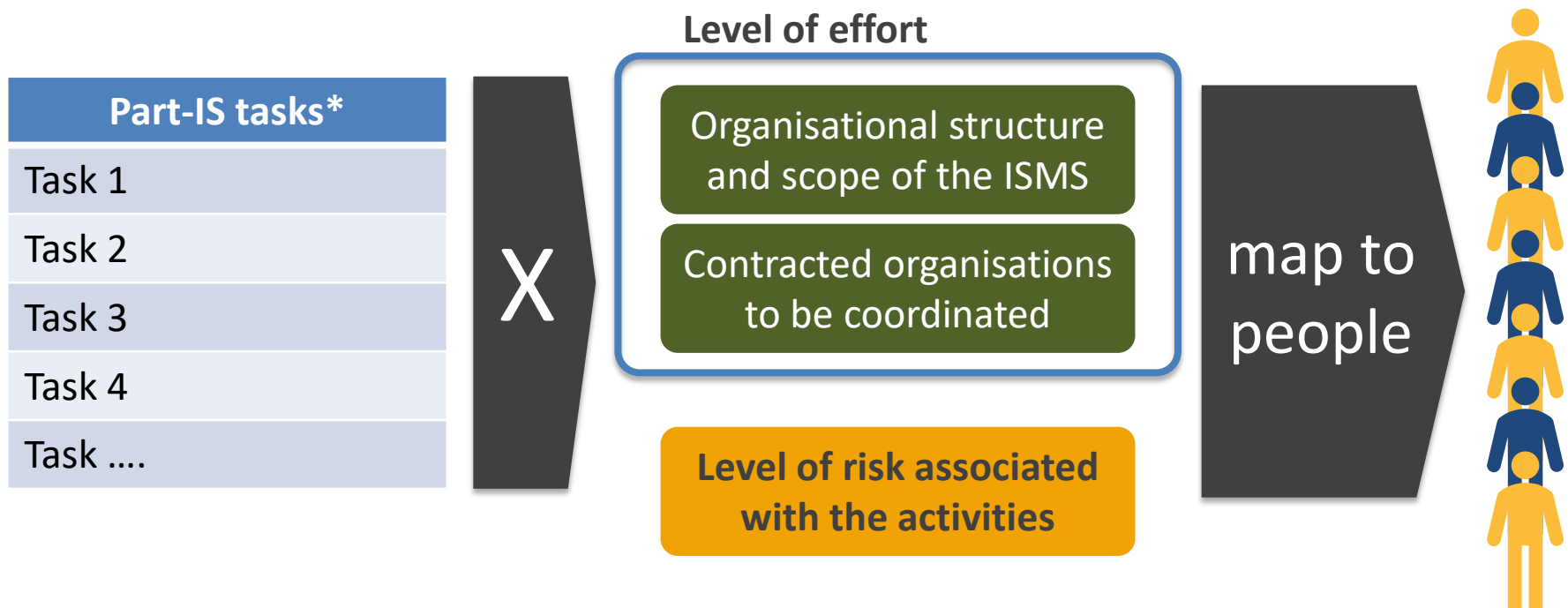
Common responsible person



Example – Group controlling multiple AOs

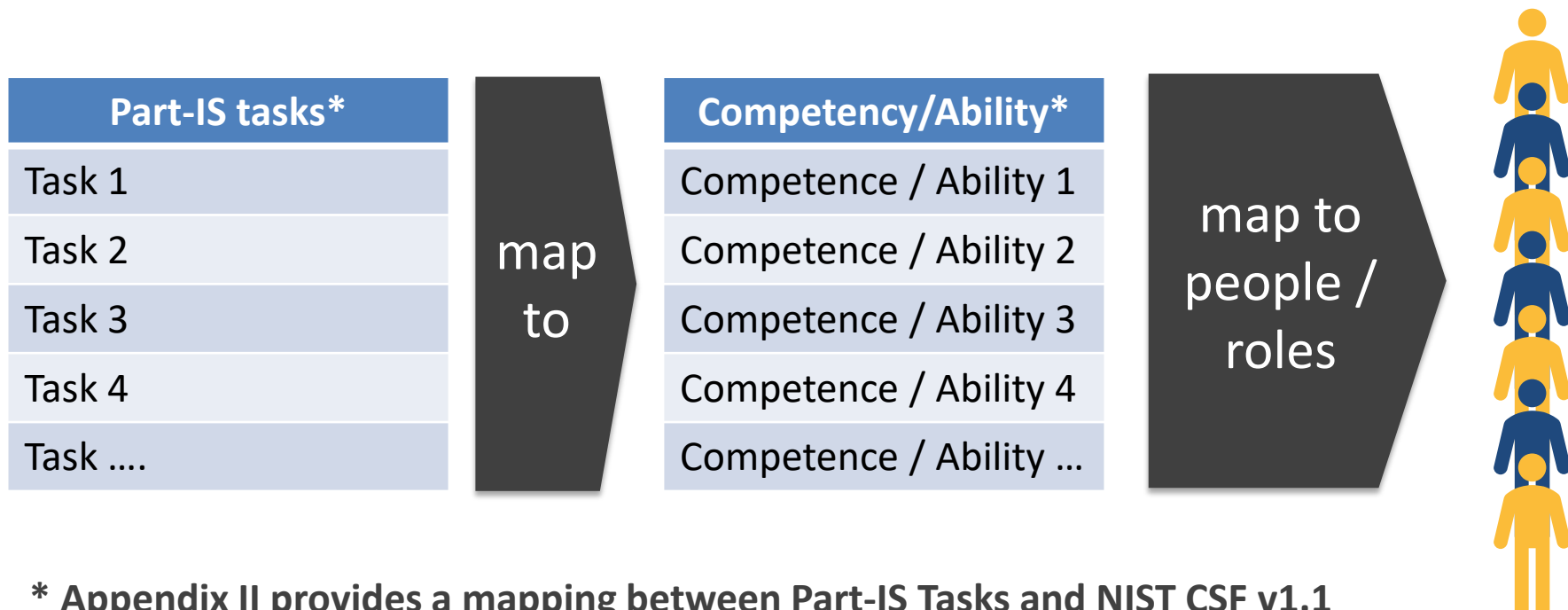


Determination of sufficiency



* Appendix II

Personnel Competence



Standard roles proposed by ECSF



Source: ENISA



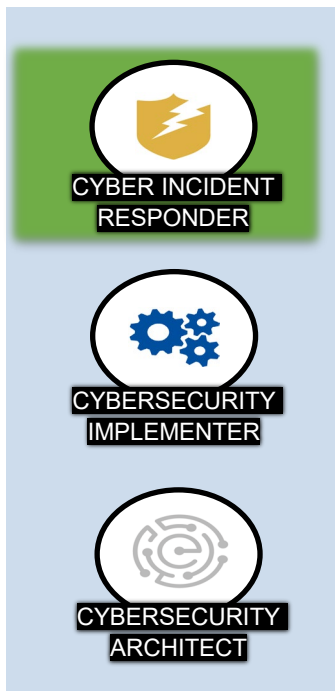
APPLICATION OF THE EUROPEAN CYBERSECURITY SKILLS FRAMEWORK TO AVIATION

Contents

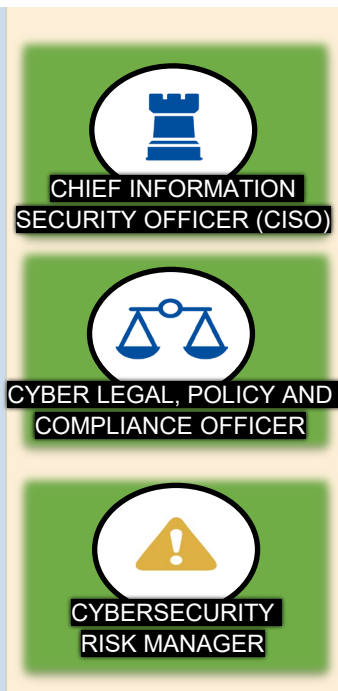
1. Introduction	2
2. Analysis of the situation and the target environment	3
3. Identification of specific objectives to be achieved	4
4. Selection of the appropriate ECSF components	4
5. Adapting the selected components according to specific needs	7
5.1 Chief Information Security Officer / Responsible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

The roles from aviation perspective

1ST LINE OF DEFENCE



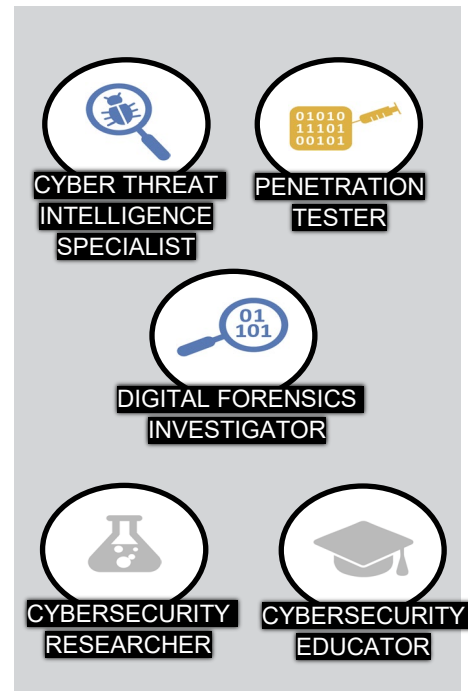
2ND LINE OF DEFENCE



3RD LINE OF DEFENCE



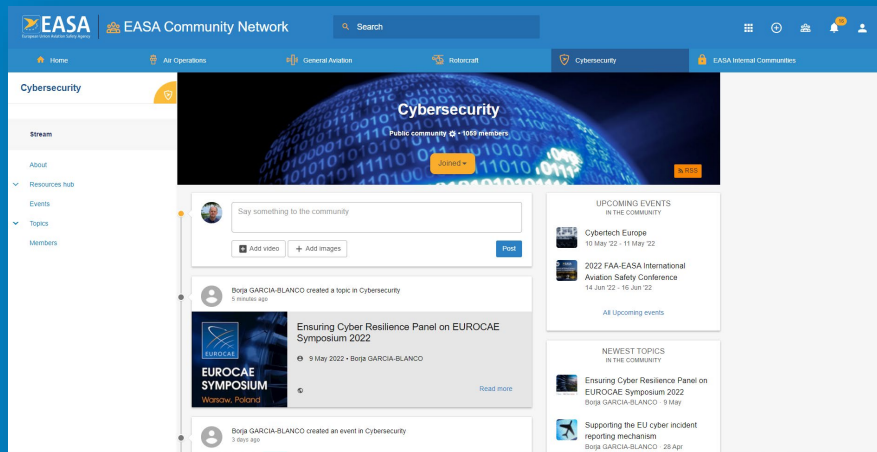
SUPPORTING



Thank you!

Join our Community:

<https://www.easa.europa.eu/community/cybersecurity>



Contact us at:

cybersec@easa.europa.eu

easa.europa.eu/connect



Your safety is our mission.

An Agency of the European Union 