Croatian Civil Aviation Agency

Informacije o Uredbi (EU) 2023/203

Part-IS
Informacijska sigurnost

Operatori, ATO-i

Sadržaj

0. Uvod

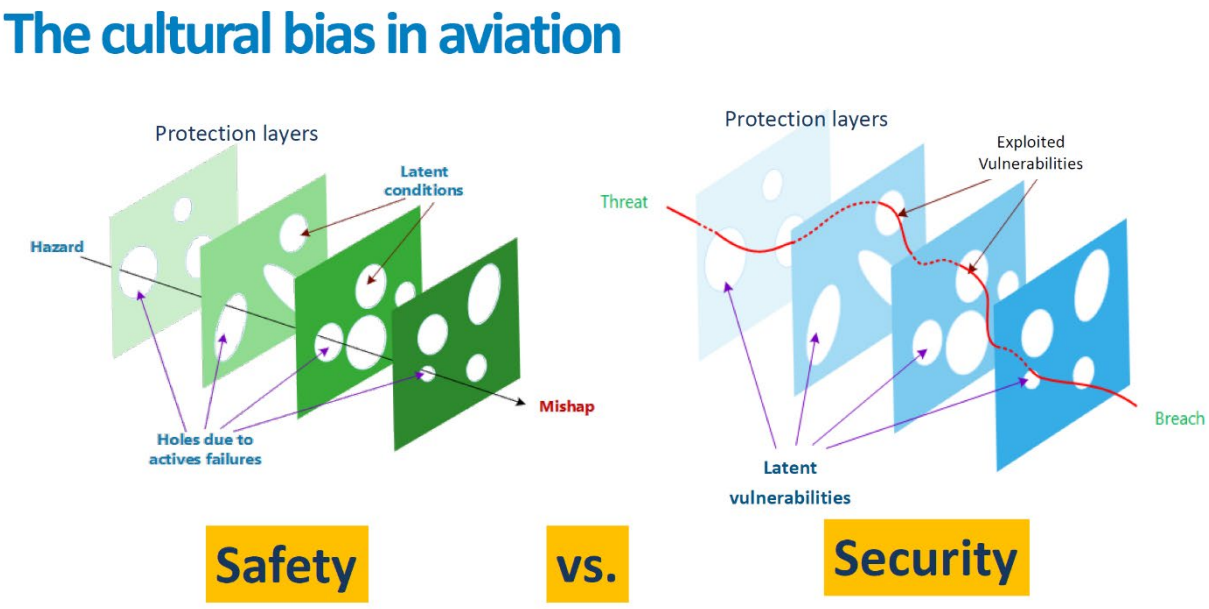
Svrha ovog dokumenta je pružiti operatorima i ATO-ima inicijalne informacije o Uredbi (EU) 2023/203 (Part IS – Informacijska sigurnost).

Informacije navedene u ovom dokumentu treba interpretirati u kontekstu svih izmjena i dopuna Osnovne Uredbe (EU) 2018/1139, Uredbe (EU) 965/2012 i Uredbe (EU) 1178/2011.

Informacije navedene u ovom dokumentu nikako ne mogu zamijeniti značenje odredbi Uredbe (EU) 2023/203 kako je izmijenjena i dopunjena.

1. Part IS - Informacijska sigurnost u civilnom zračnom prometu

Trenutno stanje u civilnom u zračnom prometu: *safety* vs. *security*



Cilj: povezivanje sigurnosti s zaštitom u civilnom zračnom prometu (u najširem kontekstu).

Ispunjavanjem Part IS zahtjeva se postiže sustavan pristup civilnom zračnom prometu, pri čemu se uzima u obzir postojanje interakcije između sigurnosti zračnog prometa i zaštite zračnog prometa (eng. *civil aviation security*), posebice informacijske sigurnosti (eng. ***i****nformation* ***s****ecurity* (IS)).
Ref. Vidi odredbe iz Osnovne Uredbe/ „Basic Regulation" (EU) 2018/1139, posebice: točka 12., točka 59., članak 4. stavak 1 d, članak 88., članak 89.

Po prvi put, europski regulator priznaje rizike informacijske sigurnosti koji utječu na sigurnost zračnog prometa. Part IS ima za cilj zauzeti holistički pristup informacijskoj sigurnosti u zrakoplovstvu, uzimajući u obzir sva povezana područja rizika informacijske sigurnosti određene organizacije (bez obzira na to izravno ili neizravno utječu na sigurnost zrakoplovstva), i provođenjem provedbe relevantnih kontrola kako bi se takvi rizici sveli na prihvatljivu razinu.

Nadalje, Part IS također zahtijeva od organizacija provedbu odgovarajućeg praćenja koje će im omogućiti ne samo otkrivanje događaja i incidenata vezanih uz informacijsku sigurnost, već i reagiranje i oporavak od incidenata unutar vremenskih okvira koji odražavaju percipiranu razinu utjecaja na sigurnost zračnog prometa.

Part IS je **„horizontalni propis“** koji određuje zahtjeve koji se odnose na informacijsku sigurnost (eng. *information security*) u civilnom zračnom prometu.

Radi se o primjeni informacijske sigurnosti u području zrakoplovstva.

Do nedavno informacijska sigurnost u području zrakoplovstva primjenjivala se samo na razini produkta, te nije obuhvaćala procese i ljudsku učinkovitost.
Međutim Part IS pristupa informacijskoj sigurnosti na sustavan način te obuhvaća organizacije, procese, ljudsku učinkovitost, produkte, sučelja iz zrakoplovnog okruženja.

Postoje razlike između primjene informacijske sigurnosti kod aerodroma ili primjene informacijske sigurnosti kod operatora/ aviokompanije ili primjene informacijske sigurnosti kod ATO-a, itd. Stoga se kod primjene informacijske sigurnosti uzima u obzir specifičnost svakog pojedinog podpodručja/ domene zrakoplovstva.

Zahtijeva se uspostava, provođenje i održavanje sustava upravljanja informacijskom sigurnošću (ISMS).

Zašto ISMS?

Radi se o tome da rizici sigurnosti civilnog zračnog prometa mogu proizlaziti iz raznih izvora.

Prijetnja za informacijsku sigurnost se može materijalizirati kao posljedica u sigurnosti zrakoplovstva.

Treba uzeti u obzir rizike sigurnosti civilnog zračnog prometa koji proizlaze iz prijetnji za informacijsku sigurnost kad postojeće nedostatke mogu iskorištavati pojedinci u zlonamjerne svrhe.

U kontekstu Part IS-a riječ je o novom riziku u avijaciji, i to u svim domenama avijacije – do sada se nismo bavili tim rizikom u avijaciji, barem ne na način koji se traži u Part IS-u, i smatra se da nismo zaštićeni na ispravan način od tog rizika.

Part IS adresira taj popularno nazvan „cyber“ rizik u području civilnog zračnog prometa.

Ti rizici za informacijsku sigurnost stalno se povećavaju u okruženju civilnog zračnog prometa kako postojeći informacijski sustavi postaju sve povezaniji, a sve češće i meta zlonamjernih aktera.

Rizici povezani s tim informacijskim sustavima nisu ograničeni na moguće napade na kiberprostor, nego obuhvaćaju i prijetnje koje mogu utjecati na procese i postupke te ljudsku učinkovitost.

Često se izraz informacijska sigurnost poistovjećuje s izrazom kibersigurnost – najviše radi popularnosti izraza, no radi se o tome da je kibersigurnost jedno od područja informacijske sigurnosti.
Područja informacijske sigurnosti kojima se upravlja:

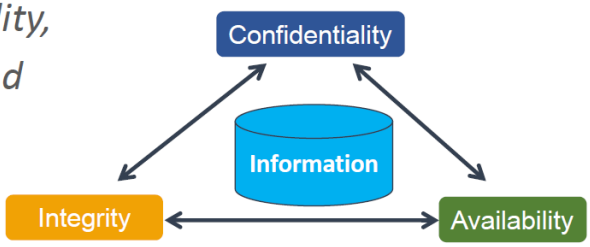
- sigurnosna provjera,
- fizička sigurnost,
- sigurnost podataka, eng. *cybersecurity*
- sigurnost informacijskog sustava, eng. *information system security*
- sigurnost poslovne suradnje.

Sustav upravljanja informacijskom sigurnošću (ISMS) čuva povjerljivost, cjelovitost i dostupnost informacija primjenom procesa upravljanja rizikom i daje povjerenje zainteresiranim stranama da se rizicima adekvatno upravlja.

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.*



Organizacije trebaju razvijati što veću *„cyber"* otpornost te
zaštititi informacijske sustave i komunikacijske tehnološke sustave i podatke koji se koriste u civilnom zračnom prometu od zlonamjernih napada.

Stoga je primjereno imati zahtjeve za upravljanje rizicima za informacijsku sigurnost koji bi mogli utjecati na sigurnost zračnog prometa.

Part IS zahtjeve moraju ispuniti **organizacije** (OR.IS zahtjevi) i **nadležna tijela** (AR.IS zahtjevi):

- kako bi identificirali i upravljali rizicima za informacijsku sigurnost koji bi mogli utjecati na sigurnost zračnog prometa, što bi moglo utjecati na sustave informacijske i komunikacijske tehnologije i podatke koji se upotrebljavaju u civilnom zrakoplovstvu,
- kako bi se otkrili događaji povezani s informacijskom sigurnošću i identificirali oni koji se smatraju incidentima povezanima s informacijskom sigurnošću koji bi mogli utjecati na sigurnost zračnog prometa,
- radi odgovora na te incidente i oporavka od njih.

Identificiraj i upravljaj rizicima informacijske sigurnosti koji bi mogli utjecati na sigurnost zračnog prometa

Otkrij događaje iz informacijske sigurnosti

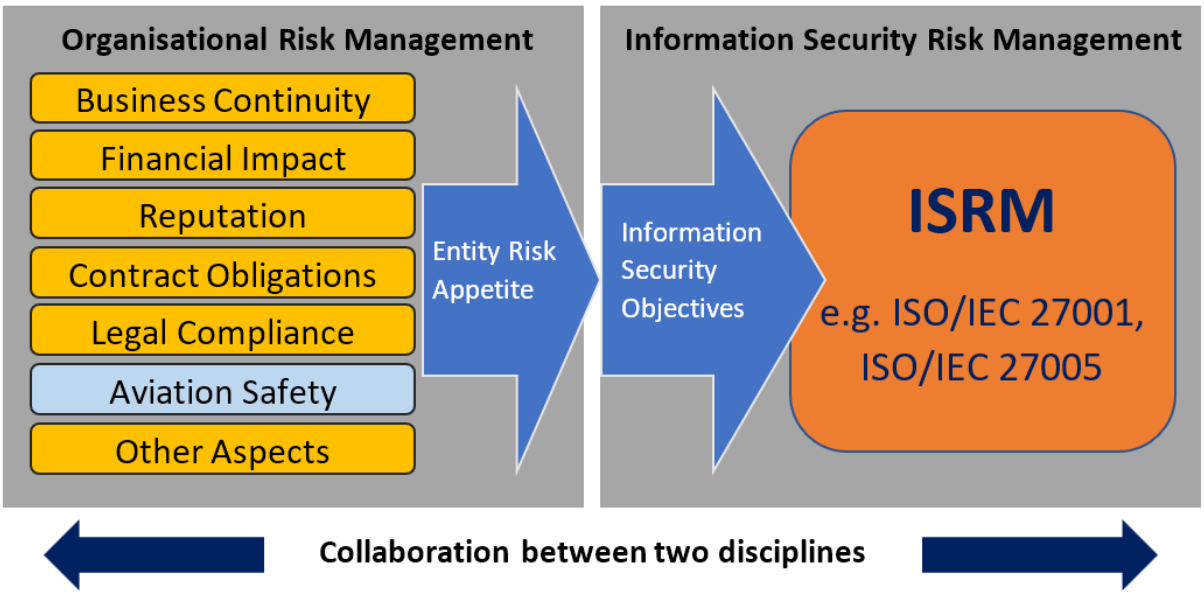
Identificiraj incidente, odgovori na njih i oporavi se od njih

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

EASA ***Proportionate to the impact on aviation safety*** 16

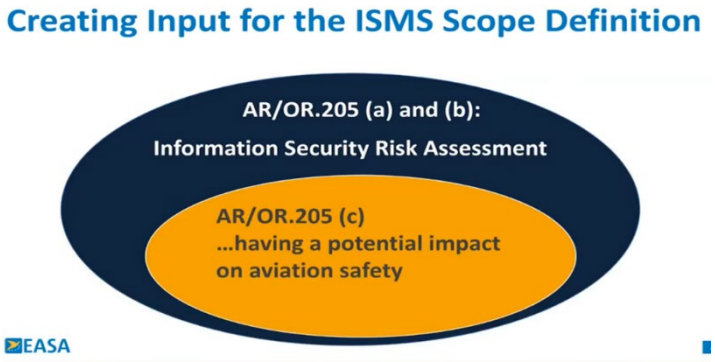
Potrebna je suradnja između dviju disciplina: između upravljanja rizika iz organizacije (npr. ISO 9001) i između rizika iz informacijske sigurnosti (npr. ISO 27001, 27002, 27005) koji bi mogli utjecati za sigurnost civilnog zračnog prometa (npr. ORA/ ORO.GEN.200a)3), itd.):



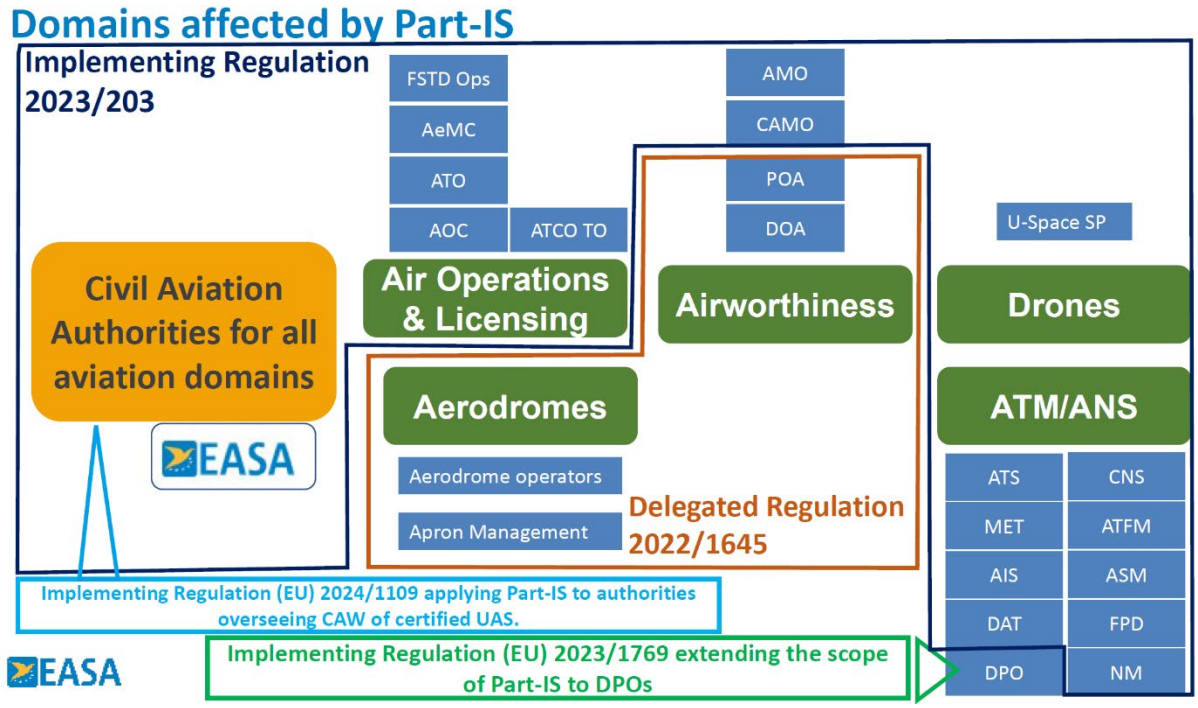
Ključno pitanje za organizacije:
-da li se u vašoj organizaciji rizici iz informacijske sigurnosti (vidi „controls“ iz ISO 27001:2022, Annex A „prelijevaju“, eng. spillover, na sigurnost civilnog zračnog prometa, odnosno na pojedino specifično područje/ domenu civilnog zračnog prometa?
-ako da, u kojoj mjeri se rizici iz informacijske sigurnosti (vidi „controls“ iz ISO 27001:2022, Annex A „prelijevaju“, eng. *spillover*; na sigurnost civilnog zračnog prometa, odnosno na pojedino specifično područje/ domenu civilnog zračnog prometa?

Kako bi se odredila politika informacijske sigurnosti potrebno je odrediti opseg ISMS-a preko dokumentirane procjene rizika iz informacijske sigurnosti i procjene njihovog mogućeg utjecaja na sigurnost zračnog prometa.


Risk assessment - scope identification
Operated and maintained services
Received services
Provided services
systems, data & information


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
EASA

2. Primjenjivost Part IS-a za operatore i ATO-e



*zelenom bojom označena su područja/ domene civilnog zračnog prometa
*plavom bojom označeni su certifikati organizacija iz pojedinih područja civilnog zračnog prometa na koje je primjenjiv Part IS
*narančastom bojom označena su nadležna tijela koja moraju ispuniti Part IS zahtjeve (npr. EASA, sve EU civilne zrakoplovne vlasti, uključujući i HACZ)

Part IS zahtjevi doneseni su:

- inicijalno kroz **delegiranu** Uredbu (EU) 2022/1645 (primjenjuje se na DOA, POA, aerodrome i pružatelje zemaljskih usluga); (IS.**D**.AR. ili IS.**D**.OR. zahtjevi) (**D- delegated**), te su dopunjavani i mijenjani sljedećim **provedbenim** Uredbama:

  -(EU) 2023/203 (primjenjuje se na CAMO, 145 organizacije, operatore, ATO-e, FSTD operatore, AeMC-ove, ATCTO, ATM/ ANS) i na nadležna tijela za sva ta područja/ domene; (IS.I.AR ili **IS.I.OR** zahtjevi), (**I**-implementing),

  -(EU) 2023/1769 (primjenjuje se za proizvođače ANS/ ATM opreme),

  -(EU) 2024/1107 (primjenjuje se na organizacije za plovidbenost bespilotnih zrakoplova),

  -(EU) 2024/1109 (primjenjuje se na nadležna tijela za bespilotne zrakoplove), i

  -(EU) 2024/1111 (primjenjuje se pri operacijama s VTOL / VCA zrakoplovima).

Provedbena Uredba (EU) 2023/203 (Part-IS) o informacijskoj sigurnosti se primjenjuje **od 22. veljače 2026. godine,** i na operatore i na ATO-e u skladu s člankom 2. „Područje primjene“.

Part-IS je primjenjiv za većinu operatora i ATO-a certificiranih u Republici Hrvatskoj od HACZ, stoga se pozivaju operatori i ATO-i da prema članku 2. Uredbe 2023/203 provjere je li Part IS primjenjiv na njih ili nije.

Ukoliko je Part IS primjenjiv, pozivaju se organizacije da se usklade s Part IS zahtjevima najkasnije do 22. veljače 2026. godine.

Članak 2. **Područje primjene**	*Article 2* **Scope**
1. Ova Uredba primjenjuje se na sljedeće organizacije: ……. (c) **operatore zrakoplova** podložne Prilogu III. (dio ORO) Uredbi (EU) br. 965/2012, osim onih koji su isključivo uključeni u rad bilo koje od sljedećih vrsta zrakoplova: i. zrakoplova ELA 2 kako je definiran u članku 1. stavku 2. točki (j) Uredbe (EU) br. 748/2012; ii. aviona uzgonjenih jednim elisnim motorom s konfiguracijom najvećeg operativnog broja putničkih sjedala od pet ili manje koji nisu klasificirani kao složeni zrakoplovi na motorni pogon, koji polijeću i slijeću na isti aerodrom ili operativnu površinu i kojima se upravlja po danu prema pravilima vizualnog letenja (VFR); iii. jednomotornih helikoptera s konfiguracijom najvećeg operativnog broja putničkih sjedala od pet ili manje koji nisu klasificirani kao složeni zrakoplovi na motorni pogon, koji polijeću i slijeću na isti aerodrom ili operativnu površinu i kojima se upravlja po danu prema VFR-u; (d) **odobrene organizacije za osposobljavanje (ATO-ovi)** podložne Prilogu VII. (dio ORA) Uredbi (EU) br. 1178/2011, osim onih koje su isključivo uključene u osposobljavanje za zrakoplove ELA 2 kako su definirani u članku 1. stavku 2. točki (j) Uredbe (EU) br. 748/2012 ili koje su isključivo uključene u teorijsko osposobljavanje; ….	1. This Regulation applies to the following organisations: ……. (c) **air operators** subject to Annex III (Part-ORO) to Regulation (EU) No 965/2012, except those solely involved in the operation of any of the following: (i) an ELA 2 aircraft as defined in Article 1(2), point (j) of Regulation (EU) No 748/2012; (ii) single-engine propeller-driven aeroplanes with a Maximum Operational Passenger Seating Configuration of 5 or less that are not classified as complex motor-powered aircraft, when taking off and landing at the same aerodrome or operating site and operating under Visual Flight Rules (VFR) by day rules; (iii) single-engine helicopters with a Maximum Operational Passenger Seating Configuration of 5 or less that are not classified as complex motor-powered aircraft, when taking off and landing at the same aerodrome or operating site and operating under VFR by day rules. (d) **approved training organisations (ATOs)** subject to Annex VII (Part-ORA) to Regulation (EU) No 1178/2011, except those solely involved in training activities of ELA2 aircraft as defined in Article 1(2), point (j) of Regulation (EU) No 748/2012, or solely involved in theoretical training; ….

Part IS nije primjenjiv na sljedeće organizacije:

3. Part IS zahtjevi

Operatori i ATO-i, uz postojeći sustav upravljanja, trebaju:
-uspostaviti, provoditi i održavati **sustav upravljanja informacijskom sigurnošću (ISMS).**

Za operatore vidi:
Prilog V Uredbe (EU) 2023/203:

"Annexes II (Part-ARO) and III (Part-ORO) to Regulation (EU) No 965/2012 are amended as follows:

(2) Annex III (Part-ORO) is amended as follows:
The following point ORO.GEN.200A is inserted after point ORO.GEN.200:

'**ORO.GEN.200A** Information security management system
In addition to the management system referred to in point ORO.GEN.200, the operator shall establish, implement and maintain an **information security management system** in accordance with Implementing Regulation (EU) 2023/203 in order to ensure the proper management of information security risks which may have an impact on aviation safety.'."

Za ATO-e vidi:
Prilog III Uredbe (EU) 2023/203:

"Annexes VI (Part-ARA) and VII (Part-ORA) to Regulation (EU) No 1178/2011 are amended as follows:
……..
(2) Annex VII (Part-ORA) is amended as follows:
The following point ORA.GEN.200A is inserted after point ORA.GEN.200:

'**ORA.GEN.200A** Information security management system
In addition to the management system referred to in point ORA.GEN.200, the organisation shall establish, implement and maintain an **information security management system** in accordance with Implementing Regulation (EU) 2023/203 in order to ensure the proper management of information security risks which may have an impact on aviation safety.'.
…"

Operatori i ATO-i, moraju uspostaviti, provoditi i održavati sustav upravljanja informacijskom sigurnošću (ISMS) u skladu s zahtjevima iz Uredbe (EU) 2023/203, konkretnije, u skladu s:

-zahtjevima propisanima u Dijelu IS.I.OR - Prilog II Uredbe (EU) 2023/203,

-EASA Odlukom ED Decision 2023/009/R i AMC & GM za Prilog II (Part IS.I.OR) Uredbe (EU) 2023/203.

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

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.

13

What is an ISMS?

ISO 27001	Part-IS
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.	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.

business risk

safety risk

EASA

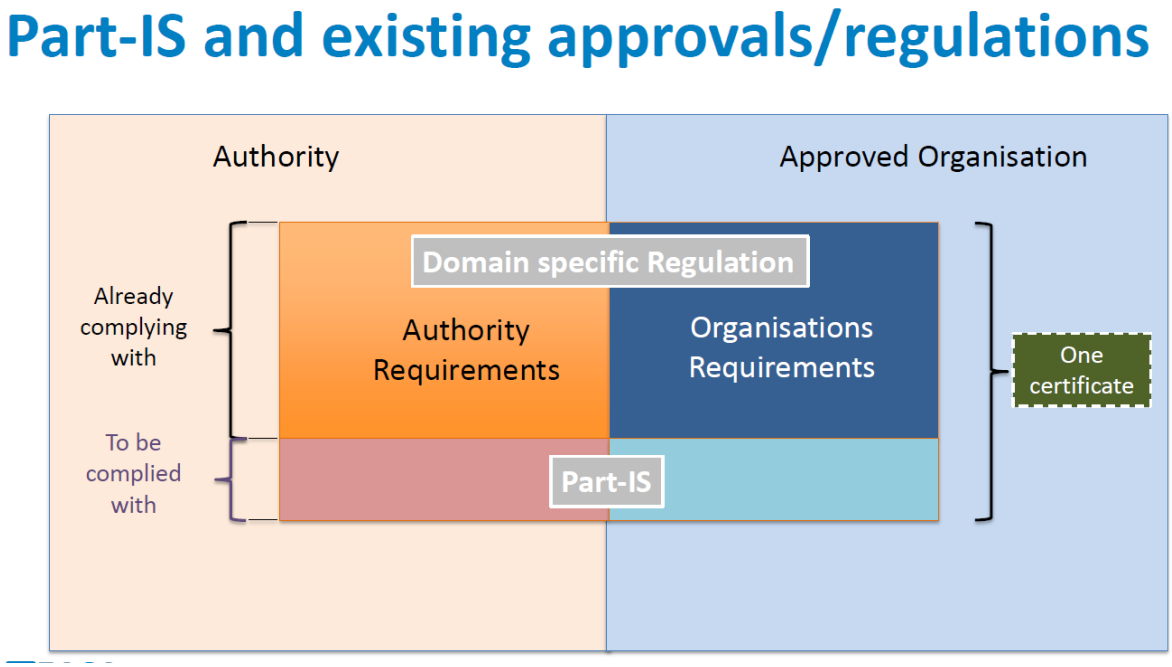
18

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

4. Okvir procesa dokazivanja početne razine usklađenosti s Part IS zahtjevima

Part IS ne zahtjeva izdavanje novog certifikata organizaciji, nego traži da se svaka organizacija koja ima određeni certifikat iz pojedinog područja zrakoplovstva (npr. certifikat da je operator, ATO certifikat, certifikat da je CAMO, certifikat da je 145 organizacija, itd.) uskladi dodatno s Part IS zahtjevima.



Za organizacije koje posjeduju jedan ili više certifikata iz područja civilnog zrakoplovstva, usklađivanje s Part IS zahtjevima će predstavljati značajnu **promjenu koja zahtjeva prethodno odobrenje.**

Organizacija **treba ishoditi odobrenje promjene koja se odnosi na usklađivanje s Part IS zahtjevima prije 26.02.2026. godine.**

Ukoliko se organizacija koja ima neki od certifikata ne uskladi s zahtjevima iz Part IS-a do 26.02.2026. godine, nadležno tijelo (HACZ) je u obavezi poduzeti odgovarajuće mjere (npr. pisano ispostaviti nesukladnosti organizaciji s rokom za otklanjanje, privremeno oduzeti certifikat/-e dok organizacija ne dokaže usklađenost s Part IS zahtjevima, itd.).

Napomena: Organizacije koje su u postupku ishođenja nekog od certifikata (inicijalna certifikacija) moraju dokazati i usklađenost s Part IS zahtjevima, za slučajeve kad se taj (inicijalni) certifikat izdaje iza 26.02.2026. godine.

5. Okvir dokazivanja početne razine usklađenosti s Part IS zahtjevima

Okvir dokazivanja početne razine usklađenosti s Part IS zahtjevima uključuje, do najkasnije 22.02.2026.,:

- dostavu dokumentirane procjene rizika iz informacijske sigurnosti s procjenom mogućeg utjecaja na sigurnost zračnog prometa,
- dokumentiranje svih procesa sustava upravljanja informacijskom sigurnošću (ISMS) koje Part IS zahtijeva i njihovu usklađenost s Part IS zahtjevima i s relevantnim AMC/ GM materijalima
  -vidi IS.I.OR.250 d): organizacija može integrirati ISMM s drugim priručnicima za upravljanje ili priručnicima koje ima, pod uvjetom da postoji jasno unakrsno upućivanje koje pokazuje koji dijelovi priručnika za upravljanje odgovaraju različitim zahtjevima sadržanima u Dijelu IS.I.OR.

Vidi dokument koji je pripremila EASA:
"EASA Guidelines ISO/IEC 27001 vs PART-IS
-Guidelines for ISO/IEC 27001:2022 conforming organisations on how to show compliance with Part-IS" (July 2024)
(u naslovu dokumenta navodi se da je riječ o smjernicama za organizacije koje su usklađene s ISO/IEC 27001:2022, no isto tako obzirom da ističe specifičnosti primjene informacijske sigurnosti u zrakoplovstvu vrlo je koristan za razumijevanje Part IS odredbi)

Za varijantu ishođenja "privremenog odobrenja derogacije" u skladu s odredbom OR.I.200(e), za slučajeve kad organizacija ne predstavlja rizike informacijske sigurnosti koji potencijalno utječu na sigurnost zračnog prometa ni za svoju organizaciju ni za druge organizacije, **okvir** dokazivanja usklađenosti radi ishođenja odobrenja „privremenog odobrenja derogacije" do najkasnije 22.02.2026., uključuje:

- dostavu dokumentirane procjene rizika iz informacijske sigurnosti
  kojom se treba dokazati da organizacija ne predstavlja rizike informacijske sigurnosti koji potencijalno utječu na sigurnost zračnog prometa ni za svoju organizaciju ni za druge organizacije
- dopunu postojećih priručnika organizacije s procesom koji se suštinski odnosi na:
  -upravljanje "privremenim odobrenjem derogacije" u skladu s odredbom OR.I.200(e), uključujući i
  -uspostavu i održavanje dokumentirane procjene rizika iz informacijske sigurnosti.

Vidi dokument koji je pripremila EASA:
"EASA Guidelines - Implementation guidelines for Part-IS - IS.I/D.OR.200 (e)" (July 2024.)

6. Popis zadataka provedbe ISMS-a

Part-IS main task	Activity type	Reference					
	Management, Operational	Part-IS	NIST CSF Version 1.1		ISO/IEC 27001		
			Function	Category	Paragraph Clause	Annex A Control :2013	Annex A Control :2022
Establish and operate an information security management system (ISMS)	Management	IS.I.OR.200(a)	IDENTIFY	ID.RM	4 6.1.1		
Establish the scope of the ISMS according to Part-IS requirements	Management	IS.I.OR.205(a)	IDENTIFY	ID.BE-2 ID.BE-4 ID.AM-5	4.3		
Implement and maintain an information security policy	Management	IS.I.OR.200(a)(1)	IDENTIFY	ID.GV-1	5.2	A5.1	A5.1
Identify and review information security risks	Management	IS.I.OR.200(a)(2) IS.I.OR.205	IDENTIFY	ID.GV-4 ID.RA	6.1.2 8.1 8.2		
Implement information security risk treatment measures	Management	IS.I.OR.200(a)(3) IS.I.OR.210	PROTECT	PR.PT	6.1.3 8.1 8.3		
Implement measures to detect information security events and identify those related to aviation safety	Management	IS.I.OR.200(a)(5) IS.I.OR.220	DETECT	DE.AE-3 DE.CM-1 DE.CM-2 DE.CM-3		A11.1.2 A12.4.1 A12.4.3 A16.1.7	A7.2 A8.15 A5.28
Implement measures that have been notified by the competent authority	Operational	IS.I.OR.200(a)(6)			10.1	A6.1.3	A5.5
Take appropriate remedial actions to address findings notified by the competent authority (non-compliances)	Both	IS.I.OR.200(a)(7) IS.I.OR.225			10.1	A6.1.3	A5.5
Implement an external information security reporting scheme	Management	IS.I.OR.200(a)(8) IS.I.OR.230	RESPOND	RS.CO-2 RS.CO-3 RS.CO-4 RS.CO-5	7.4	A6.1.3 A16.1.2 A16.1.3	A5.5 A6.8

Part-IS main task	Activity type	Reference					
	Management, Operational	Part-IS	NIST CSF Version 1.1		ISO/IEC 27001		
			Function	Category	Paragraph Clause	Annex A Control :2013	Annex A Control :2022
Monitor compliance with this Regulation and report findings to top management	Operational	IS.I.OR.200(a)(12)	IDENTIFY	ID.GV-3	9.2	A18.2.1 A18.2.2	A5.35 A5.36
Protect confidentiality of exchanged information	Operational	IS.I.OR.200(a)(13)	PROTECT	PR.DS-1 PR.DS-2		A8.2.2 A13.2	A5.13 A5.14
Implement and maintain a continuous improvement process to measure the effectiveness and maturity of the ISMS and strive to improve it	Management	IS.I.OR.200(b) IS.I.OR.260	IDENTIFY	ID.RA-6 ID.SC-4	4.4 9.1 9.3 10.1 10.2	A5.1.2 A16.1.7 A17.1.3 A18.2.1	A5.1 A5.28 A5.29 A5.35
			PROTECT	PR.IP-7 PR.IP-10			
			DETECT	DE.DP-5			
			RESPOND	RS.MI-3 RS.IM-2			
			RECOVER	RC.IM-2			
Document and maintain all key processes, procedures, roles and responsibilities	Management	IS.I.OR.200(c)	IDENTIFY	ID.AM-6 ID.GV-4 ID.RM-1 ID.SC-1 ID.SC-2	4.2 5.2 5.3	A5.1 A6.1.1	A5.1 A5.2
			PROTECT	PR.AT-2 PR.AT-4 PR.AT-5 PR.IP-12			
			DETECT	DE.DP-1			
			RESPOND	RS.CO-1 RS.AN-5			
Identify all elements which could be exposed to information security risks	Management	IS.I.OR.205(a)	IDENTIFY	ID.AM-1 ID.AM-2 ID.AM-4 ID.AM-5	4.3	A8.1.1	A5.9
Identify the interfaces with other organisations which could result in exposure to information security risks	Management	IS.I.OR.205(b)	IDENTIFY	ID.BE-1 ID.BE-2 ID.BE-4 ID.BE-5	4.3		
Identify information security risks and assign a risk level	Management	IS.I.OR.205(c)	IDENTIFY	ID.RA-1 ID.RA-2 ID.RA-3 ID.RA-4 ID.RA-5	6.1.2		

Part-IS main task	Activity type	Reference					
	Management, Operational	Part-IS	NIST CSF Version 1.1		ISO/IEC 27001		
			Function	Category	Paragraph Clause	Annex A Control :2013	Annex A Control :2022
Review and update the risk assessment based on certain criteria	Operational	IS.I.OR.205(d)	IDENTIFY	ID.RM	8.2		A5.7
Organisations under Subpart C of Annex III (Part-ATM/ANS.OR) to Regulation (EU) 2017/373 share the safety support assessment	Operational	IS.I.OR.205(e)					
Develop and implement measures to address risks and verify their effectiveness	Operational	IS.I.OR.210(a)	PROTECT	PR.IP PR.PT	6.1.3 8.3		
Communicate the outcome of the risk assessment to management, other personnel and other organisations sharing an interface	Operational	IS.I.OR.210(b)	IDENTIFY	ID.AM-3 ID.BE-1 ID.BE-2 ID.BE-4 ID.RM-3 ID.SC-3	8.1		
			PROTECT	PR.IP-7			
Establish an internal information security reporting scheme to enable the collection and evaluation of information security events from personnel	Management	IS.I.OR.200(a)(4) IS.I.OR.215(a) IS.I.OR.215(e)	IDENTIFY	ID.AM-3	7.4	A16.1.1 A16.1.2	A5.28 A6.8
Ensure that contracted organisations report information security events	Management	IS.I.OR.215(c)	RESPOND	RS.CO-2 RS.CO-4	7.4	A15.1.1 A16.1.2	A5.19 A6.8
Analyse internally reported occurrences to identify information security events, incidents, and vulnerabilities	Operational	IS.I.OR.215(b)(1)-(b)(3)	IDENTIFY	ID.RA-1		A12.6.1 A16.1.1 A16.1.4	A8.8 A5.24 A5.25
			DETECT	DE.AE-2 DE.AE-3 DE.AE-5			

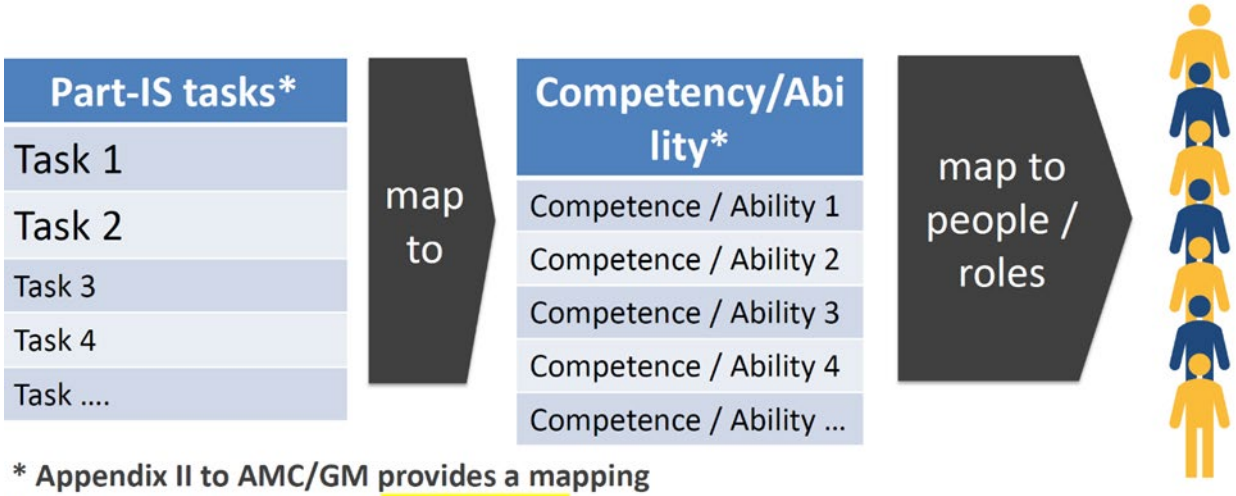
Part-IS main task	Activity type	Reference					
	Management, Operational	Part-IS	NIST CSF Version 1.1		ISO/IEC 27001		
			Function	Category	Paragraph Clause	Annex A Control :2013	Annex A Control :2022
Implement measures to detect in processes and operations information security events which may have a potential impact on aviation safety	Operational	IS.I.OR.220(a)	DETECT	DE.AE DE.CM DE.DP		A11.1.2 A12.4.1 A12.6.1 A16.1.1 A16.1.2 A16.1.3 A16.1.4 A16.1.5	A7.2 A8.8 A8.15 A8.16 A5.24 A5.25 A5.26 A6.8
			PROTECT	PR.PT-1			
Implement measures to respond to information security events that may cause an information security incident	Operational	IS.I.OR.220(b)	RESPOND	RS.RP RS.AN RS.MI		A16.1.5	A5.26
Cooperate on investigations with other organisations that contribute to the information security of its own activities	Management	IS.I.OR.215(d)	RESPOND	RS.AN-3 RS.AN-5		A15.1.2 A15.1.3 A16.1.7	A5.20 A5.21 A5.28
Implement measures to recover from information security incidents	Operational	IS.I.OR.220(c)	RECOVER	RC.RP-1 RC.IM-1		A16.1.5 A16.1.6	A5.26 A5.27
Manage risks associated with contracted activities with regard to the management of information security	Management	IS.I.OR.235	IDENTIFY	ID.SC-1 ID.SC-2		A15.1 A15.2	A5.19 A5.20 A5.21 A5.22
Create and maintain a process to ensure that there is sufficient personnel to perform all activities regarding information security management	Management	IS.I.OR.240(f)	IDENTIFY	ID.AM-5 ID.AM-6 ID.GV-2	7.1	A6.1.1	A5.2
Create and maintain a process to ensure that the personnel have the necessary competence for activities regarding information security management	Management	IS.I.OR.240(g)	IDENTIFY	ID.AM-5 ID.AM-6	7.2	A7.2.2	A6.3
			PROTECT	PR.AT-1			

Part-IS main task	Activity type	Reference					
	Management, Operational	Part-IS	NIST CSF Version 1.1		ISO/IEC 27001		
			Function	Category	Paragraph Clause	Annex A Control :2013	Annex A Control :2022
Create and maintain a process to ensure that the personnel acknowledge the responsibilities associated with the assigned roles and tasks	Management	IS.I.OR.240(h)	IDENTIFY	ID.GV-2 ID.GV-3	7.3 7.4	A7.1.2	A6.2
Verify the identity and trustworthiness of personnel who have access to information systems	Management	IS.I.OR.240(i)	PROTECT	PR.AC-6 PR.IP-11	7.1	A7.1.1	A6.1
Archive, protect and retain records and ensure they are traceable for a specified time	Operational	IS.I.OR.245	IDENTIFY	ID.RA-4	7.5	A8.2.2 A8.2.3 A11.1.3 A11.1.4 A12.1.3 A12.3.1 A12.4.1 A12.4.2 A12.4.3	A5.10 A5.13 A7.3 A7.5 A8.6 A8.10 A8.13 A8.15
			PROTECT	PR.AC-2 PR.AC-3 PR.AC-4 PR.DS-1 PR.DS-4 PR.DS-5 PR.DS-6 PR.IP-4 PR.IP-6 PR.PT-1			
Correct non-compliance findings upon notification by the competent authority within the period agreed with the competent authority	Operational	IS.I.OR.225			10.1	A18.1.1 A18.2	A5.31 A5.35 A5.36
Implement an information security reporting system in accordance with Regulation (EU) No 376/2014	Management	IS.I.OR.230(a)					
Report information security incidents or vulnerabilities to the competent authority and, under certain conditions, to others	Operational	IS.I.OR.230(b) IS.I.OR.230(c)	DETECT	DE.DP-3	7.4	A16.1.1 A16.1.2 A16.1.3	A5.24 A6.8
			RESPOND	RS.CO-2 RS.CO-3 RS.CO-4 RS.CO-5			
			RECOVER	RC.CO-3			

Part-IS main task	Activity type	Reference					
	Management, Operational	Part-IS	NIST CSF Version 1.1		ISO/IEC 27001		
			Function	Category	Paragraph Clause	Annex A Control :2013	Annex A Control :2022
Regularly assess the effectiveness and maturity of the ISMS	Operational	IS.I.OR.260(a)			9	A5.1.2 A12.7.1 A16.1.6	A5.1 A5.27 A8.34
Take actions to improve the ISMS if required. Reassess the ISMS elements affected by the implemented measures.	Operational	IS.I.OR.260(b)			10	A5.1.2	A5.1
Ensure accessibility of the competent authority to the contracted organisation	Management	IS.I.OR.235(b)			9.3	A6.1.3 A15.1 A15.2	A5.5 A5.20 A5.22
Top management ensures that all necessary resources are available to comply with the Regulation	Management	IS.I.OR.240(a)(1)	IDENTIFY	ID.AM-5 ID.AM-6	7.1	A6.1.1	A5.2
Top management establishes and promotes the information security policy and demonstrates a basic understanding of the Regulation	Management	IS.I.OR.240(a)(2) &(a)(3)	IDENTIFY	ID.GV-1	5.1 5.2 7.4	A5.1.1 A7.2.1 A7.2.2	A5.1 A5.4 A6.3
			PROTECT	PR.AT-1 PR.AT-4			
Appoint a responsible person or a group of persons with appropriate knowledge to manage compliance with the Regulation	Management	IS.I.OR.240(b) IS.I.OR.240(c) IS.I.OR.240(d)	IDENTIFY	ID.AM-6 ID.GV-2	7.1 7.2	A6.1.1 A7.2.1 A7.2.2	A5.2 A5.4 A6.3
			PROTECT	PR.AT-1 PR.AT-4			
Create and maintain an information security management manual (ISMM)	Management	IS.I.OR.250			7.5.1	A6.1.3 A12.1.1	A5.5 A5.37
Develop a procedure on how to notify the competent authority upon changes to the ISMS	Management	IS.I.OR.255(a)	IDENTIFY	ID.AM-3	7.4 7.5.1	A6.1.3 A13.2.1 A13.2.2	A5.5 A5.14
Manage changes to the ISMS and notify the competent authority and/or request for approval of changes	Management	IS.I.OR.255(a) IS.I.OR.255(b)	IDENTIFY	ID.AM-3	7.4	A6.1.3 A13.2.1 A13.2.2	A5.5 A5.14

Organisational structure

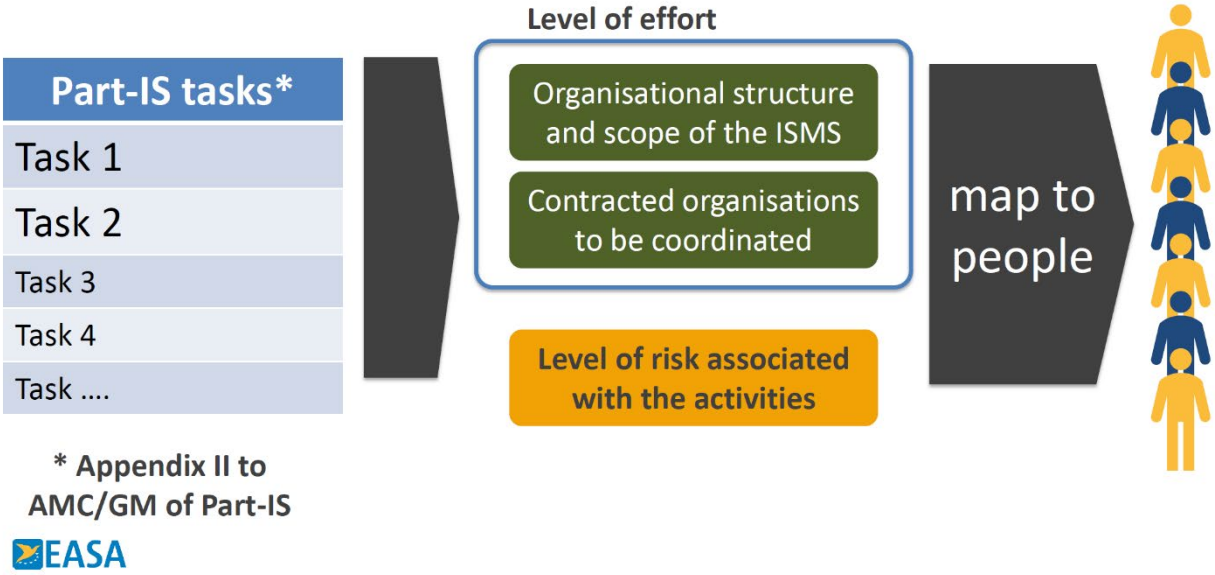
Personnel Competence



* Appendix II to AMC/GM provides a mapping between Part-IS Tasks and NICE CSF v1.1

EASA

Determination of sufficiency



7. Korisne poveznice i definicije

1. Easy access rules for Part IS (June 2024)

https://www.easa.europa.eu/en/document-library/easy-access-rules/easy-access-rules-information-security-regulations-eu-2023203

2. Poveznica na Uredbu (EU) 2023/203 i EASA Odluku EDD 2023/009/R
https://www.easa.europa.eu/en/newsroom-and-events/news/easa-published-first-easy-access-rules-information-security

3. Poveznica na EASA Opinion 03/2021, NPA 2019-07
https://www.easa.europa.eu/en/document-library/opinions/opinion-032021#group-easa-downloads

4. FAQ EASA information security

https://www.easa.europa.eu/en/the-agency/faqs/information-security-part

5. Prijavite se na EASA community – "Cybersecurity in aviation community"
(tamo ćete naći dokumente/ guidelines koje je EASA pripremila i mnogo korisnih najnovijih informacija)

https://www.easa.europa.eu/community/go

6. EASA workshop: 7.-8. studeni 2024. na you tube kanalu

https://www.youtube.com/watch?v=IBDL7B6eMzY&list=PLTfS24aKkJn4SfagbAVp1K6PL-GDG_TA3&index=2

https://www.youtube.com/watch?v=ikrVJLRN4LE&list=PLTfS24aKkJn4SfagbAVp1K6PL-GDG_TA3

7. Definicija „zrakoplov ELA 2"

"(EU) No 748/2012, članak 1., 2.(j) ….. (j) **'ELA2 aircraft'** means the following manned European Light Aircraft: (i) an aeroplane with a Maximum Take-off Mass (MTOM) of 2 000 kg or less that is not classified as complex motor-powered aircraft; (ii) a sailplane or powered sailplane of 2 000 kg MTOM or less; (iii) a balloon; (iv) a hot air airship; (v) a gas airship complying with all of the following characteristics: — 3% maximum static heaviness, — Non-vectored thrust (except reverse thrust), — Conventional and simple design of: structure, control system and ballonet system, — Non-power assisted controls;	"Uredba 748/2012, članak 1. Područje primjene i definicije ….. 2. Za potrebe ove Uredbe primjenjuju se sljedeće definicije: ….. (j) **„zrakoplov ELA 2"** znači sljedeći europski laki zrakoplov s posadom: i.zrakoplov (čitaj avion) čija je najveća dopuštena masa pri uzlijetanju (MTOM) 2 000 kg ili manje, koji nije razvrstan kao složeni motorni zrakoplov; ii.jedrilica ili motorna jedrilica čiji je MTOM 2 000 kg ili manje; iii.balon; iv.zračni brod uzgonjen vrućim zrakom; v.zračni brod uzgonjen plinom koji je u skladu sa sljedećim karakteristikama: —3 % maksimalne statičke težine, —ne-vektorski potisak (osim povratnog potiska), —konvencionalan i jednostavan projekt konstrukcije, kontrolnog sustava i sustava baloneta,

(vi) a Very Light Rotorcraft."	—komande bez serva; vi.vrlo laki rotokopter."

8. Definicija „kompleksni zrakoplov na motorni pogon“

“Uredba 20181139, članak 140, 2. (b) Prijelazne odredbe …. 2. Najkasnije do 12. rujna 2023. provedbena pravila donesena na temelju uredaba (EZ) br. 216/2008 i (EZ) br. 552/2004 prilagođavaju se ovoj Uredbi. Do prilagodbe svako upućivanje u tim provedbenim pravilima na: (a)„komercijalnu djelatnost” smatra se upućivanjem na članak 3. točku (i) Uredbe (EZ) br. 216/2008; (b)„**kompleksni zrakoplov na motorni pogon”** smatra se upućivanjem na članak 3. točku (j) Uredbe (EZ) br. 216/2008; (c)„uređaje” smatra se upućivanjem na članak 3. točku 29. ove Uredbe; (d)„dozvolu rekreacijskog pilota” smatra se upućivanjem na dozvolu iz članka 7. stavka 7. Uredbe (EZ) br. 216/2008; ….	“Basic Regulation 2018/1139, article 140, 2.(b) ‘complex motor-powered aircraft’ shall be understood as a reference to point (j) of Article 3 of Regulation (EC) No 216/2008.
Uredba 216/2008, članak 3. Definicije	Article 3 j of Regulation (EC) No 216/2008:
(j)**„kompleksni zrakoplov na motorni pogon”** znači:	(j)**‘complex motor-powered aircraft’** shall mean:
i.zrakoplov / čitaj avion: —s najvećim certificiranom uzletnom masom koja prelazi 5 700 kg, ili —certificiran za najveći broj putničkih sjedala koji je veći od devetnaest, ili —certificiran za letenje s najmanjom posadom od barem dva pilota, ili —opremljen s turboreaktivnim motorom/motorima ili s više od jednog turboelisnog motora; ili	(i)an aeroplane: —with a maximum certificated take-off mass exceeding 5 700 kg, or —certificated for a maximum passenger seating configuration of more than nineteen, or —certificated for operation with a minimum crew of at least two pilots, or —equipped with (a) turbojet engine(s) or more than one turboprop engine, or
ii.certificirani helikopter: —za najveću uzletnu masu koja prelazi 3 175 kg, ili —za najveći broj putničkih sjedala koji je veći od devet, ili —za letenje s najmanjom posadom od barem dva pilota, ili	(ii)a helicopter certificated: —for a maximum take-off mass exceeding 3 175 kg, or —for a maximum passenger seating configuration of more than nine, or —for operation with a minimum crew of at least two pilots, or
iii.zrakoplov s nagibnim rotorom;”	(iii)a tilt rotor aircraft;”

9. Za potrebe Uredbe (EU) 2023/203 primjenjuju se sljedeće definicije:

(1) **„informacijska sigurnost"** znači očuvanje povjerljivosti, integriteta, autentičnosti i dostupnosti mrežnih i informacijskih sustava;

(2) **„događaj povezan s informacijskom sigurnošću"** znači identificirani događaj u stanju sustava, usluge ili mreže koji ukazuje na moguće narušavanje politike informacijske sigurnosti ili zakazivanje kontrola informacijske sigurnosti ili prethodno nepoznatu situaciju koja može biti relevantna za informacijsku sigurnost;

(3) **„incident"** znači svaki događaj koji ima stvaran negativni učinak na sigurnost mrežnih i informacijskih sustava, kako je definiran u članku 4. točki 7. Direktive (EU) 2016/1148;

(4) **„rizik za informacijsku sigurnost"** znači rizik za organizacijske operacije civilnog zrakoplovstva, imovinu, pojedince te druge organizacije zbog mogućeg događaja povezanog s informacijskom sigurnošću. Rizici za informacijsku sigurnost povezani su s mogućnošću prijetnje iskorištavanja ranjivosti informacijske imovine ili skupine informacijske imovine;

(5) **„prijetnja"** znači mogućnost povrede informacijske sigurnosti koja postoji kad postoji subjekt, okolnost, radnja ili događaj koji bi mogli prouzročiti štetu;

(6) **„ranjivost"** znači nedostatak ili slaba točka u imovini ili sustavu, postupcima, dizajnu, provedbi ili mjerama informacijske sigurnosti koja bi se mogla iskoristiti i koja dovede do kršenja politike informacijske sigurnosti.