Agencija za civilno letalstvo Slovenija

Civil Aviation Agency Slovenia

Okviri regulative Izvedbene Uredbe Komisije (EU) 2023/203 PART-IS

Peter Čičerov

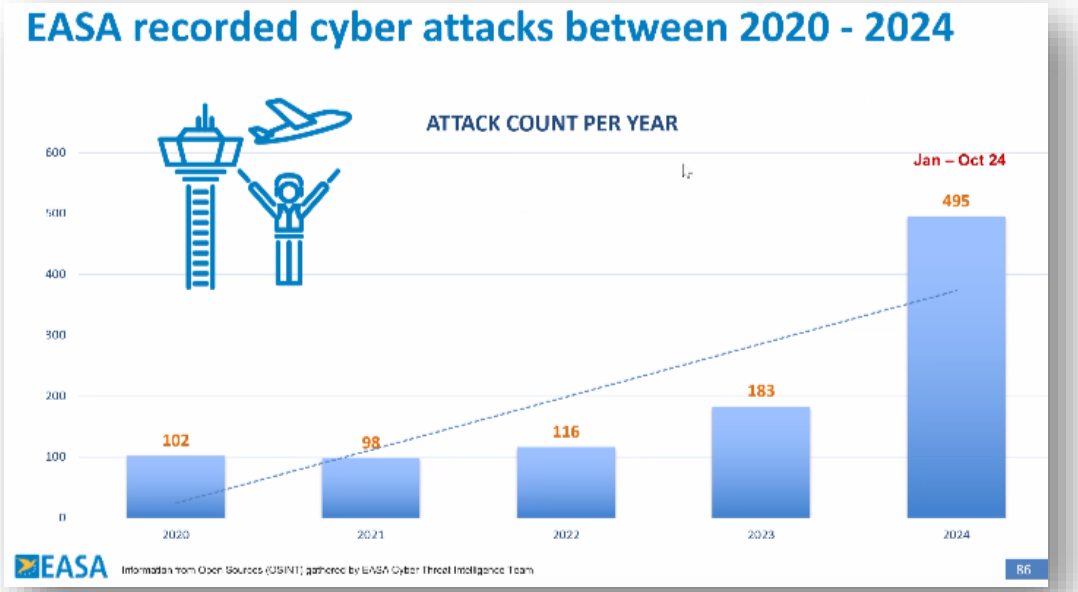
28.03.2025

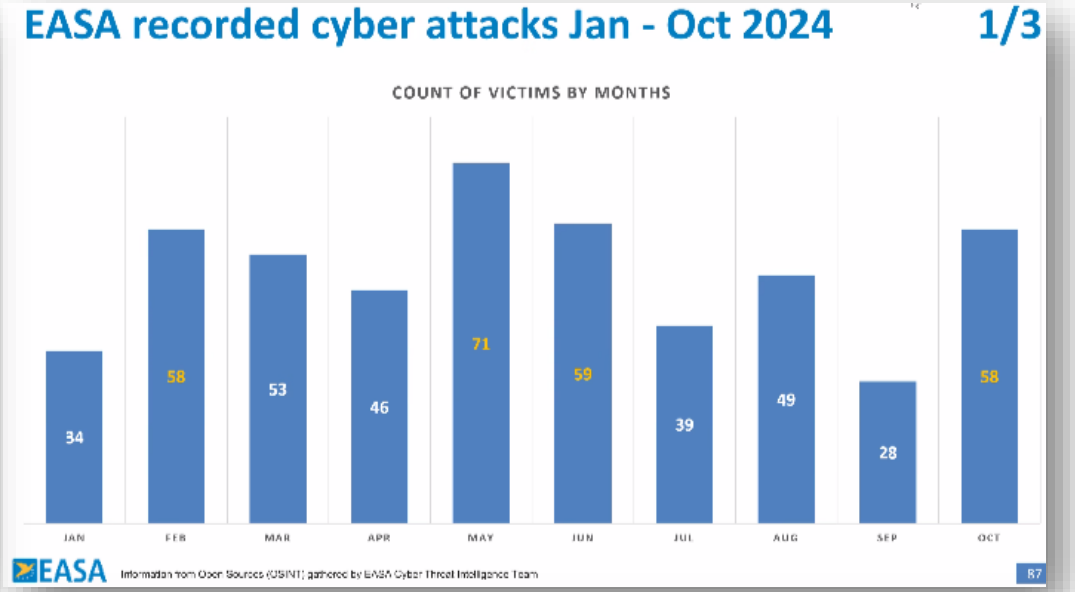
Letalstvo in izzivi informacijskih tveganj

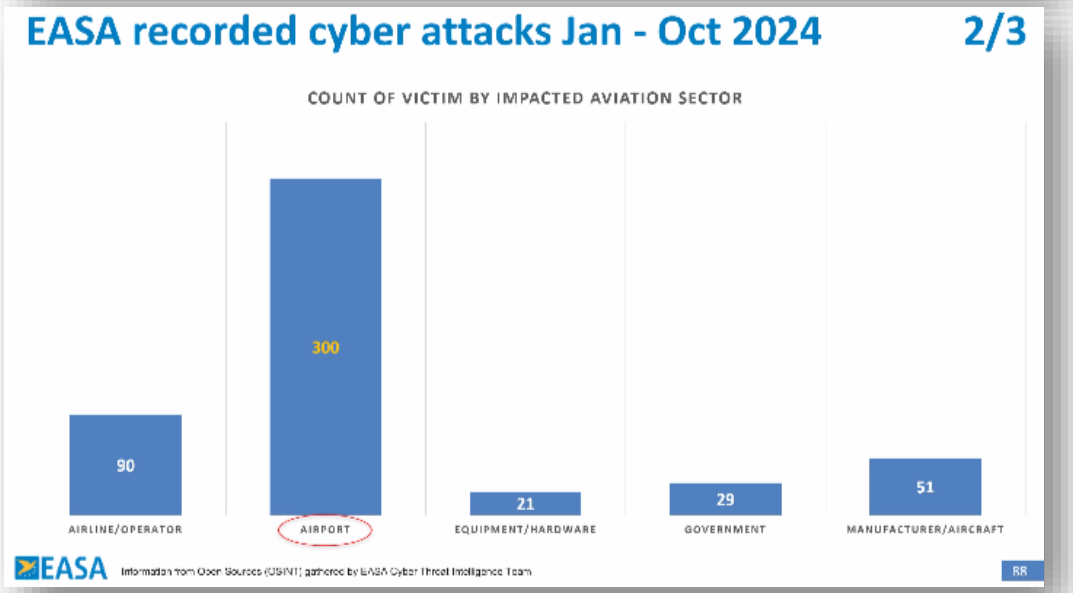
Cilji	**Zaščita letalskih sistemov pred informacijskimi tveganji, ki neposredno vplivajo na letalsko varnost**
Obseg	Sistemi informacijske in komunikacijske tehnologije ter podatki, ki jih uporabljajo pooblaščene organizacije in organi za namene civilnega letalstva
Aktivnosti	- prepoznati in obvladovati tveganja za informacijsko varnost v zvezi z informacijami, sistemi komunikacijske tehnologije in podatki, ki se uporabljajo za namene civilnega letalstva; - odkrivanje informacijsko varnostnih dogodkov z identifikacijo tistih, ki so upoštevani kot incidenti informacijske varnosti; in - odziv na zaznane incidente informacijske varnosti ter okrevanje po njih

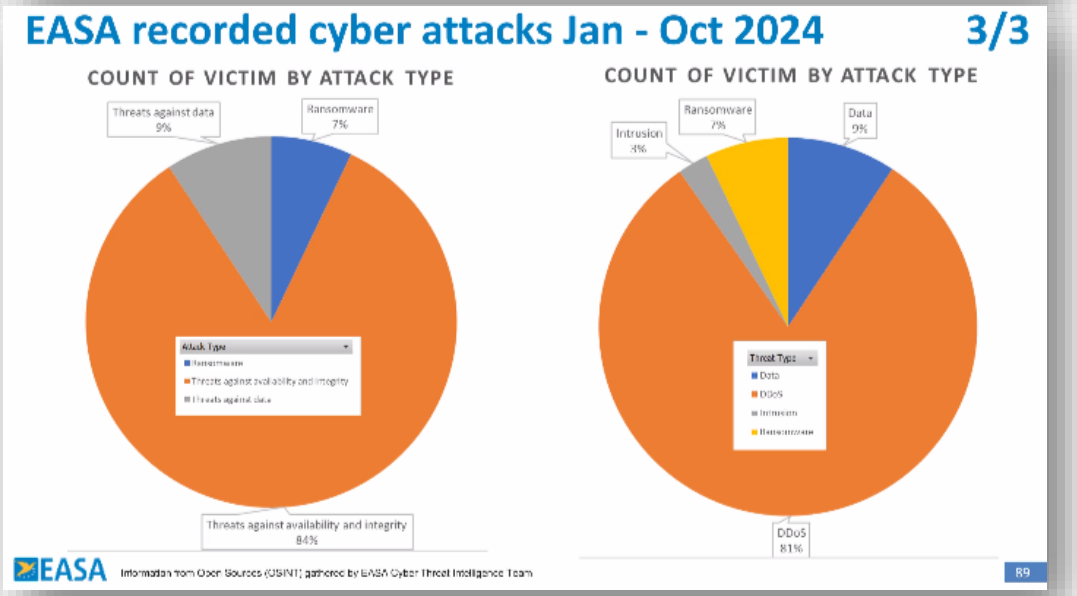
Sorazmerno z vplivom na varnost v letalstvu

Analiza kibernetskih napadov (vir:EASA)

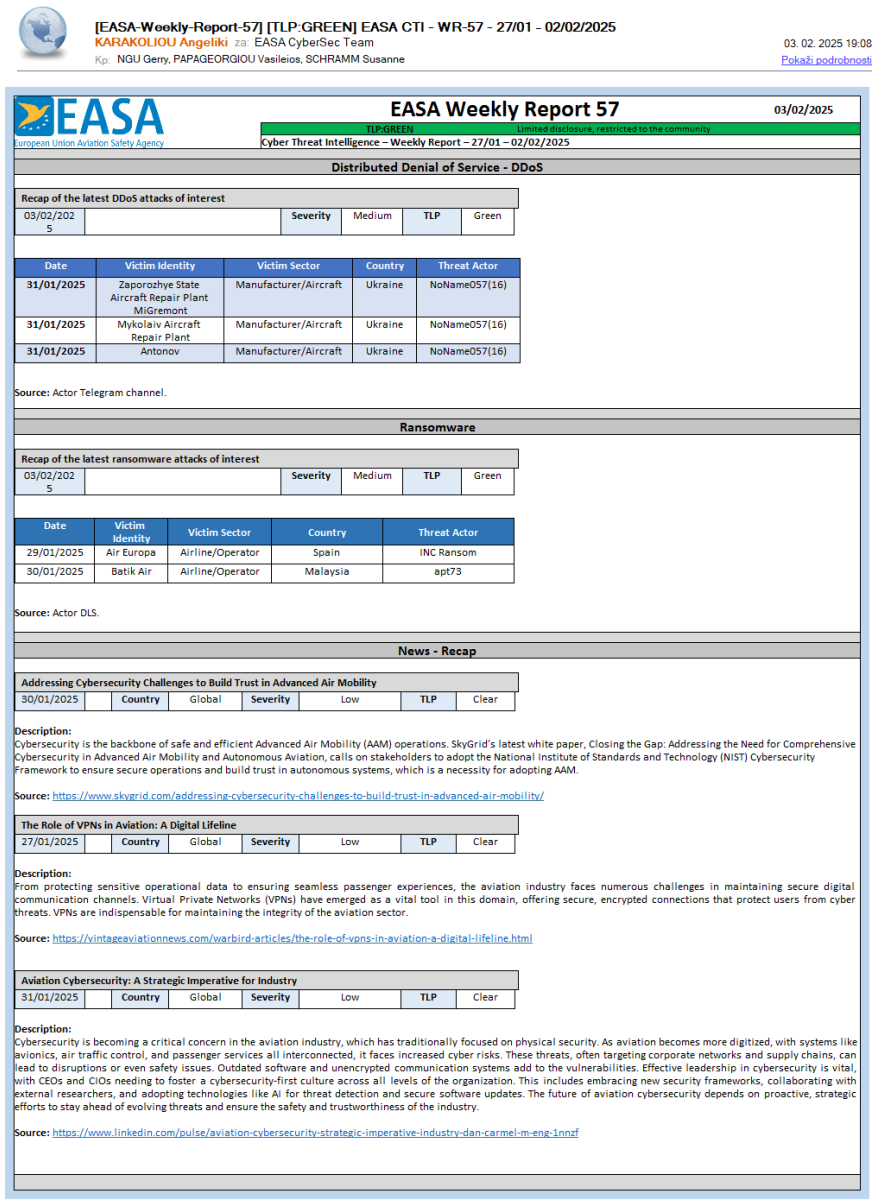








EASA redno tedensko poročilo o informacijskih varnostnih grožnjah



[EASA-Weekly-Report-57] [TLP:GREEN] EASA CTI - WR-57 - 27/01 - 02/02/2025
KARAKOLIOU Angeliki za: EASA CyberSec Team
Kp: NGU Gerry, PAPAGEORGIOU Vasileios, SCHRAMM Susanne
03. 02. 2025 19:08
Pokaži podrobnosti

EASA
European Union Aviation Safety Agency

EASA Weekly Report 57 03/02/2025

TLP:GREEN - Limited disclosure, restricted to the community

Cyber Threat Intelligence – Weekly Report – 27/01 – 02/02/2025

Distributed Denial of Service - DDoS

Recap of the latest DDoS attacks of interest					
03/02/2025		Severity	Medium	TLP	Green

Date	Victim Identity	Victim Sector	Country	Threat Actor
31/01/2025	Zaporozhye State Aircraft Repair Plant MiGremont	Manufacturer/Aircraft	Ukraine	NoName057(16)
31/01/2025	Mykolaiv Aircraft Repair Plant	Manufacturer/Aircraft	Ukraine	NoName057(16)
31/01/2025	Antonov	Manufacturer/Aircraft	Ukraine	NoName057(16)

Source: Actor Telegram channel.

Ransomware

Recap of the latest ransomware attacks of interest					
03/02/2025		Severity	Medium	TLP	Green

Date	Victim Identity	Victim Sector	Country	Threat Actor
29/01/2025	Air Europa	Airline/Operator	Spain	INC Ransom
30/01/2025	Batik Air	Airline/Operator	Malaysia	apt73

Source: Actor DLS.

News - Recap

Addressing Cybersecurity Challenges to Build Trust in Advanced Air Mobility							
30/01/2025		Country	Global	Severity	Low	TLP	Clear

Description:
Cybersecurity is the backbone of safe and efficient Advanced Air Mobility (AAM) operations. SkyGrid's latest white paper, Closing the Gap: Addressing the Need for Comprehensive Cybersecurity in Advanced Air Mobility and Autonomous Aviation, calls on stakeholders to adopt the National Institute of Standards and Technology (NIST) Cybersecurity Framework to ensure secure operations and build trust in autonomous systems, which is a necessity for adopting AAM.

Source: https://www.skygrid.com/addressing-cybersecurity-challenges-to-build-trust-in-advanced-air-mobility/

The Role of VPNs in Aviation: A Digital Lifeline							
27/01/2025		Country	Global	Severity	Low	TLP	Clear

Description:
From protecting sensitive operational data to ensuring seamless passenger experiences, the aviation industry faces numerous challenges in maintaining secure digital communication channels. Virtual Private Networks (VPNs) have emerged as a vital tool in this domain, offering secure, encrypted connections that protect users from cyber threats. VPNs are indispensable for maintaining the integrity of the aviation sector.

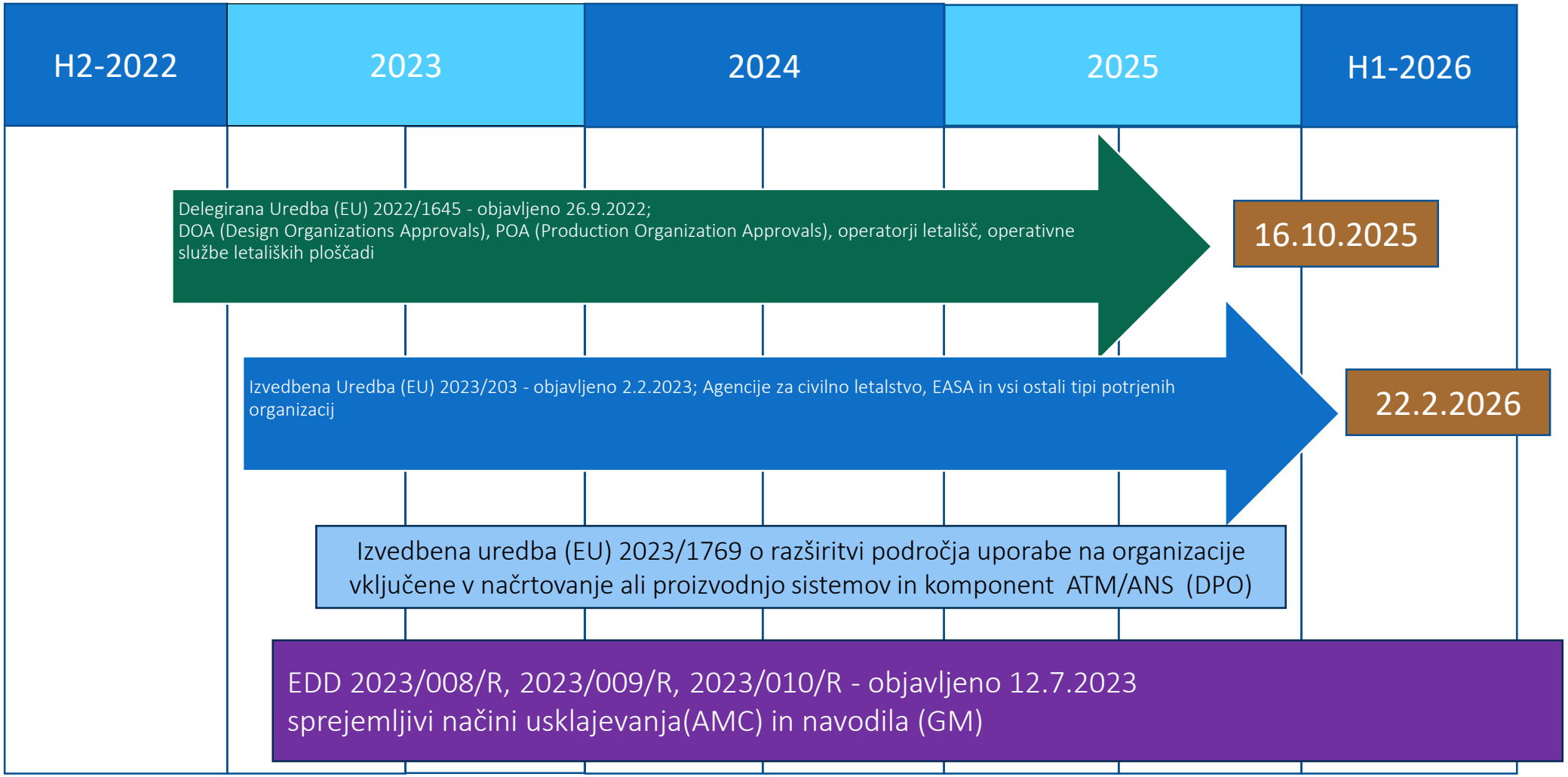
Source: https://vintageaviationnews.com/warbird-articles/the-role-of-vpns-in-aviation-a-digital-lifeline.html

Aviation Cybersecurity: A Strategic Imperative for Industry							
31/01/2025		Country	Global	Severity	Low	TLP	Clear

Description:
Cybersecurity is becoming a critical concern in the aviation industry, which has traditionally focused on physical security. As aviation becomes more digitized, with systems like avionics, air traffic control, and passenger services all interconnected, it faces increased cyber risks. These threats, often targeting corporate networks and supply chains, can lead to disruptions or even safety issues. Outdated software and unencrypted communication systems add to the vulnerabilities. Effective leadership in cybersecurity is vital, with CEOs and CIOs needing to foster a cybersecurity-first culture across all levels of the organization. This includes embracing new security frameworks, collaborating with external researchers, and adopting technologies like AI for threat detection and secure software updates. The future of aviation cybersecurity depends on proactive, strategic efforts to stay ahead of evolving threats and ensure the safety and trustworthiness of the industry.

Source: https://www.linkedin.com/pulse/aviation-cybersecurity-strategic-imperative-industry-dan-carmel-m-eng-1nnzf

PART-IS implementacijska časovnica



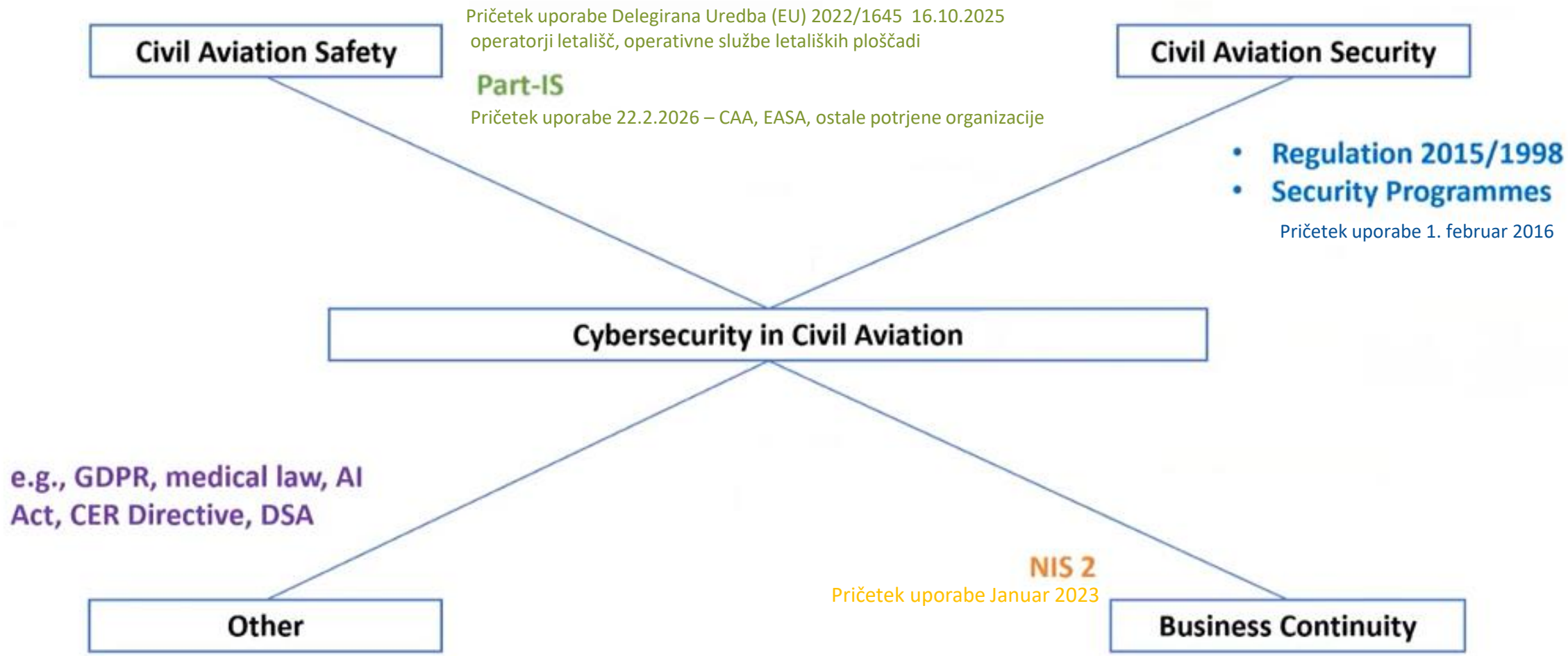
Spremembe obstoječih predpisov organizacije/ pristojni organi

Part / Area	ORA	21	ORO	ADR	ATCO	ATM/ANS	CAMO	145
ISMS	.GEN.200A	.A.139A .A.239A	.GEN.135A	.OR.D.005A .OR.D.007 .OR.F.045A	.OR.C.001A	.OR.B.005A .OR.D.010	.A.200A	.A.200A

Part / Area	ARA	21	ARO	ADR	ATCO	ATM/ANS	CAMO	145	66
ISMS	.GEN.200	.B.25	.GEN.200	.AR.B.005	.AR.B.001	.AR.B.001	.B.200	.B.200	.B.15
ISporočanje	.GEN.125 .GEN.135A	.B.15 .B.20A	.GEN.125 .GEN.135.A	.AR.A.025 .AR.A.030A	.AR.A.020 .AR.A.025A	.AR.A.020 .AR.A.025A	.B.125 .B.135A	.B.125 .B.135A	N/A
Nadzor	.GEN.300 .GEN.330A	.B.221 .B.240A .B.431 .B.435A	.GEN.300 .GEN.330A	.AR.C.005 .C.040A	.AR.C.001 .AR.E.010A	.AR.C.010 .AR.C.025A	.B.300 .B.330A	.B.300 .B.330A	N/A
Naloge	.GEN.205	.B.30	.GEN.205	.AR.B.010	.AR.B.005	.AR.B.005	.B.205	.B.205	N/A

PART-IS obstoječe odobritve / predpisi

Informacijska varnost v povezavi z različno zakonodajo (Vir: EASA)



Aplikabilnost v povezavi z različno zakonodajo (Vir: EASA)

Organisation	Certificate	Part-IS	NIS 2	AvSec	Remarks
Commercial air carriers	AOC	Y	Y	Y	only Large (> 250 employee) or Medium 50 to 249 employees*
Airports	ADR Management	Y	Y	Y	only Large (> 250 employee) or Medium 50 to 249 employees*
Air traffic control [ATC]	ANSP	Y	Y	(Y)	only Large (> 250 employee) or Medium 50 to 249 employees*
Aircraft Manufacturers	DOA, POA	Y	(Y)		To be determined by the Member State
Equipment Manufacturers	DOA, POA	Y	(Y)		To be determined by the Member State
Maintenance organisations	MOA	Y	(Y)	(Y)	To be determined by the Member State
Maintenance management	CAMO	Y	(Y)	(Y)	To be determined by the Member State
Pilot training organisations	ATO, TRTO	Y			Unlikely – it could be still theoretically possible if the MS decides so
ATCO Training Organisations	ATCO TO	Y			- // -
Simulators' operators	FSTD	Y			- // -
Aeromedical Centres	AeMC	Y			- // -

NIS 2	Part-IS	AvSec
Needs to be transposed to the national law of the MS	Directly applicable to concerned organisations & authorities	Same as Part-IS
Size of entity is important for applicability	Size is not important – risk is	Same as Part-IS
Type of entity is important for applicability	Type of entity is how applicability is defined	Type of entity is how applicability is defined
Applicable to smaller entities under conditions*	N/A	N/A
Applicability defined by type of organisation (business units)	Applicability defined by approval (organisations = approval holders)	Applicability defined by type of organisation (business units)
Flexibility on transposition of the rule	Rule has to be applied as such	Rule has to be applied as such
As a Directive, requirements are of a higher level	As a Regulation, there are more granular requirements.	Requirements on cybersecurity are in general of a higher level than in Part-IS
ISMS is not necessary	An ISMS is needed	ISMS is not necessary

Kdo so zavezanci za skladnost z Uredbo Komisije (EU) 2023/203

Člen 2

Področje uporabe

1. Ta uredba se uporablja za naslednje organizacije:

(a) vzdrževalne organizacije, za katere velja Oddelek A Priloge II (del 145) k Uredbi (EU) št. 1321/2014, razen tistih, ki so vključen izključno v vzdrževanje zrakoplovov v skladu s Prilogo Vb (del ML) k Uredbi (EU) št. 1321/2014;

(b) organizacije za vodenje stalne plovnosti (CAMO), za katere velja Oddelek A Priloge Vc (del CAMO) k Uredbi (EU št. 1321/2014, razen tistih, ki so vključene izključno v vodenje stalne plovnosti zrakoplova v skladu s Prilogo Vb (del ML) Uredbi (EU) št. 1321/2014;

(c) letalske prevoznike, za katere velja Priloga III (del ORO) k Uredbi (EU) št. 965/2012, razen tistih, ki so vključeni izključno upravljanje katerega koli od naslednjih zrakoplovov:

(i) zrakoplov ELA2, kot je opredeljen v členu 1(2), točka (j), Uredbe (EU) št. 748/2012;

(ii) enomotorna propelerska letala z največjim operativnim številom potniških sedežev 5 ali manj, ki niso opredeljena kc kompleksni zrakoplovi na motorni pogon, kadar vzletajo in pristajajo na istem letališču ali območju delovanja ter obratujej v skladu s pravili vizualnega letenja (VFR) podnevi;

(iii) enomotorni helikopterji z največjim operativnim številom potniških sedežev 5 ali manj, ki niso opredeljeni kot kompleksn zrakoplovi na motorni pogon, kadar vzletajo in pristajajo na istem letališču ali območju delovanja ter obratujejo v skladu pravili VFR podnevi;

(d) odobrene organizacije za usposabljanje (ATO), za katere velja Priloga VII (del ORA) k Uredbi (EU) št. 1178/2011, razen tistih, k so vključene izključno v dejavnosti usposabljanja za zrakoplov ELA2, kot je opredeljen v členu 1(2), točka (j), Uredbe (EU št. 748/2012, ali so vključene izključno v teoretično usposabljanje;

(e) zdravstvene centre za letalsko osebje, za katere velja Priloga VII (del ORA) k Uredbi (EU) št. 1178/2011;

(f) operatorje naprav za simulacijo letenja (FSTD), za katere velja Priloga VII (del ORA) k Uredbi (EU) št. 1178/2011, razen tistih, k so vključeni izključno v upravljanje naprav FSTD za zrakoplov ELA2, kot je opredeljen v členu 1(2), točka (j), Uredbe (EU št. 748/2012;

(g) organizacije za usposabljanje kontrolorjev zračnega prometa (ATCO TO) in zdravstvene centre za letalsko osebje za kontrolorj zračnega prometa, za katere velja Priloga III (del ATCO.OR) k Uredbi (EU) 2015/340;

(h) organizacije, za katere velja Priloga III (del ATM/ANS.OR) k Izvedbeni uredbi (EU) 2017/373, razen naslednjih izvajalce storitev:

(i) izvajalci navigacijskih služb zračnega prometa, ki imajo omejen certifikat v skladu s točko ATM/ANS.OR.A.010 naveden priloge;

(ii) izvajalci služb informacij za letenje, ki dajo izjavo o svojih dejavnostih v skladu s točko ATM/ANS.OR.A.015 naveden priloge;

(i) izvajalce služb U-space in enotne izvajalce skupnih informacijskih služb, za katere velja Izvedbena uredba (EU) 2021/664.

2. Ta uredba se uporablja za pristojne organe, vključno z Agencijo Evropske unije za varnost v letalstvu (v nadaljnjem besedilu Agencija), iz člena 6 te uredbe in člena 5 Delegirane uredbe Komisije (EU) 2022/1645 ([14]).

3. Ta uredba se uporablja tudi za pristojni organ, odgovoren za izdajo, podaljšanje, spremembo, začasno ukinitev ali preklic licenc z vzdrževanje zrakoplova v skladu s Prilogo III (del 66) k Uredbi (EU) št. 1321/2014.

4. Ta uredba ne posega v zahteve glede informacijske in kibernetske varnosti iz točke 1.7 Priloge k Izvedbeni uredbi (EU) 2015/199 in člena 14 Direktive (EU) 2016/1148.

PART-IS NI APLIKABILNA v spodnjih primerih

Proizvodnje organizacije brez odobritev

Part-147 organizacije za vzdrževalno usposabljanje

ATO organizacije ki ponujajo izključno teoretično usposabljanje.

Zasebni operatorji, ki ne posedujejo kompleksnih motornih letal

Organizacije, ki se ukvarjajo z lahkimi letali :
katerih MTOM je pod 2000 kg, zelo lahki helikopterji, jadralna letala, baloni in zračne ladje

Operatorji sistemov brezpilotnih zrakoplovov v “odprti” ter “posebni” kategoriji.

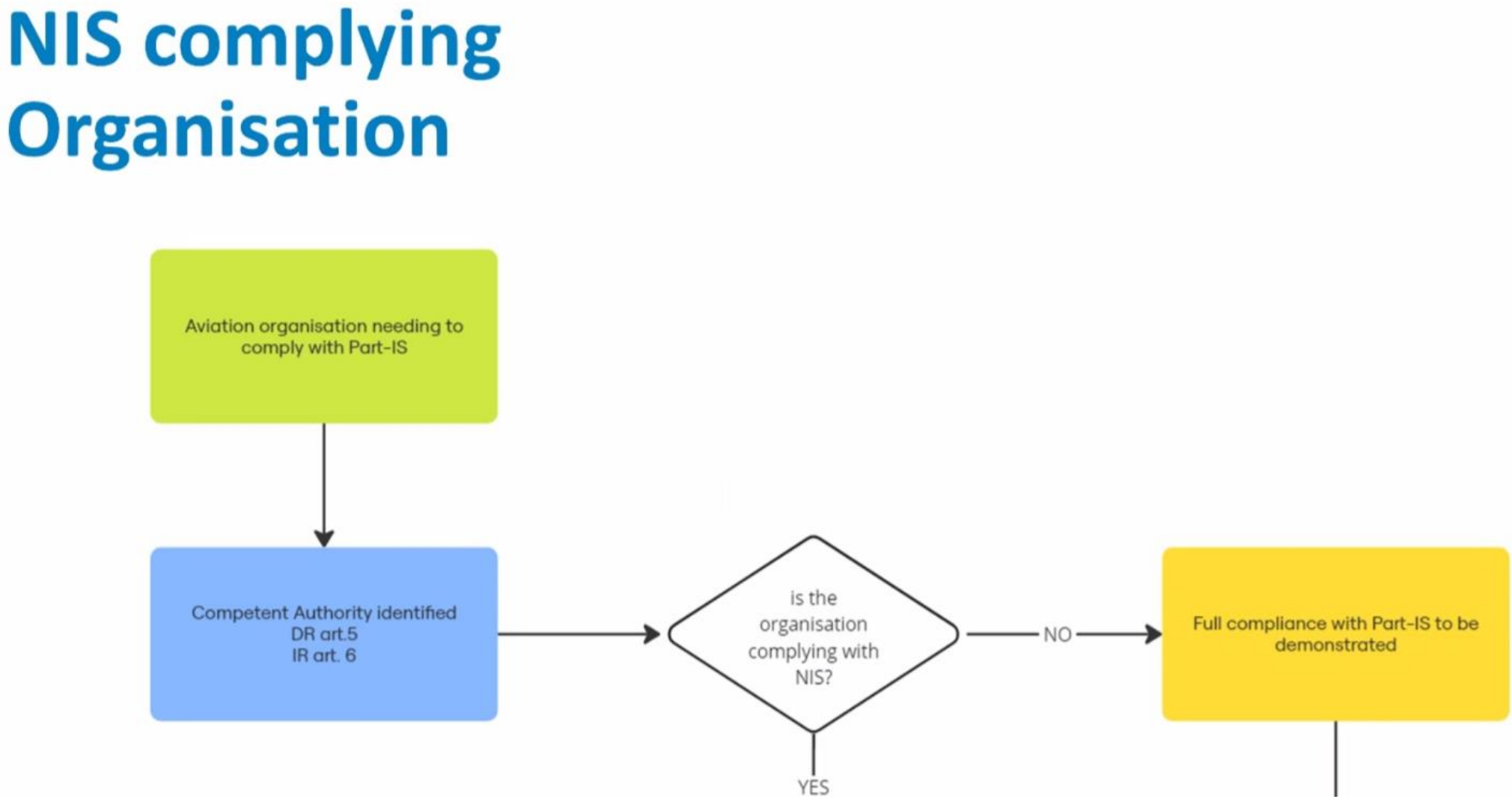
Organizacije, ki razvijajo sistem brezpilotnega zrakoplova za “posebno kategorijo”, kjer ni zahtevana DOA odobritev

TCO operatorji

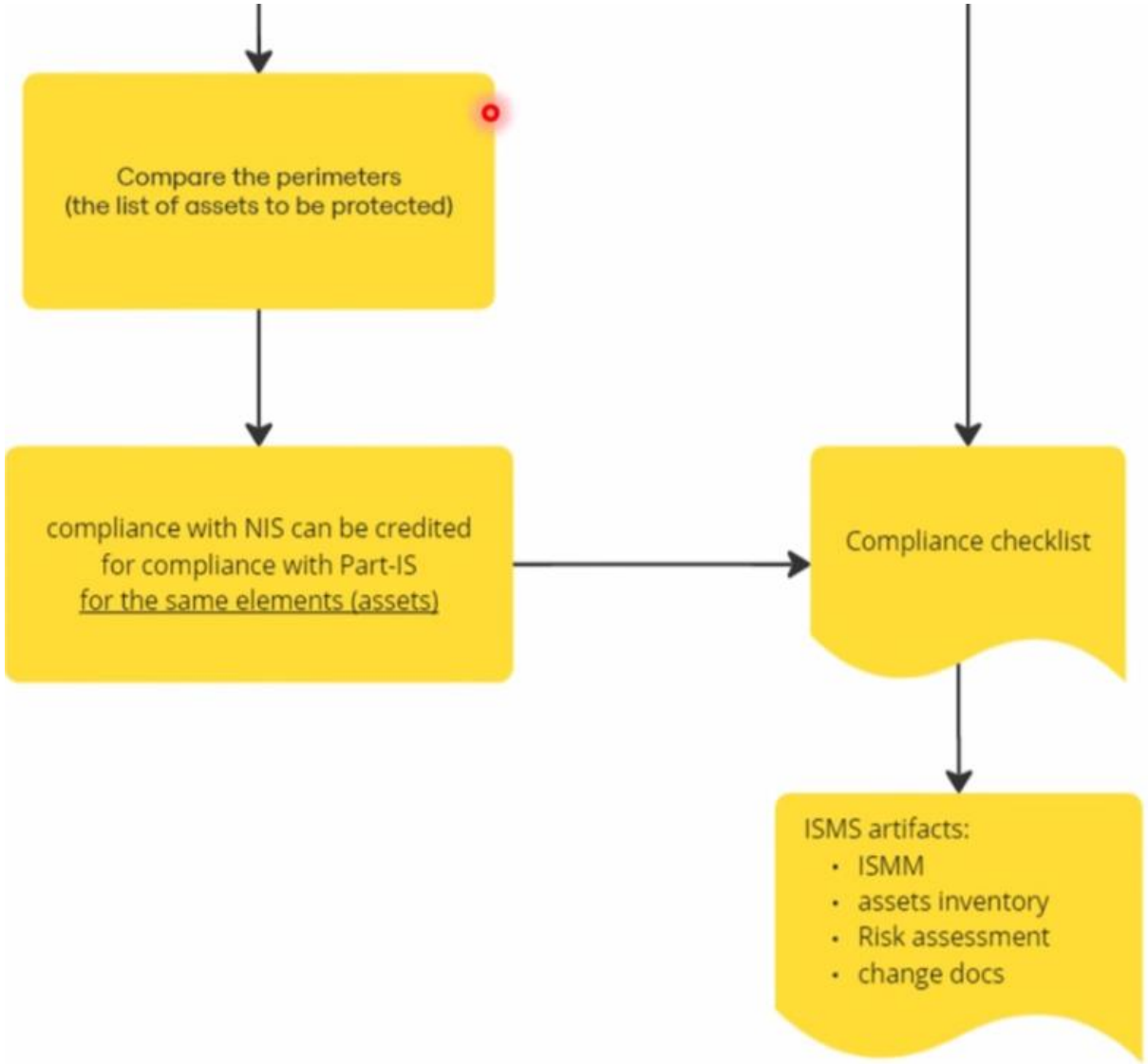
Regulirano z ICAO Annex 6

Organizacije potrjene v bilateralnih sporazumih.

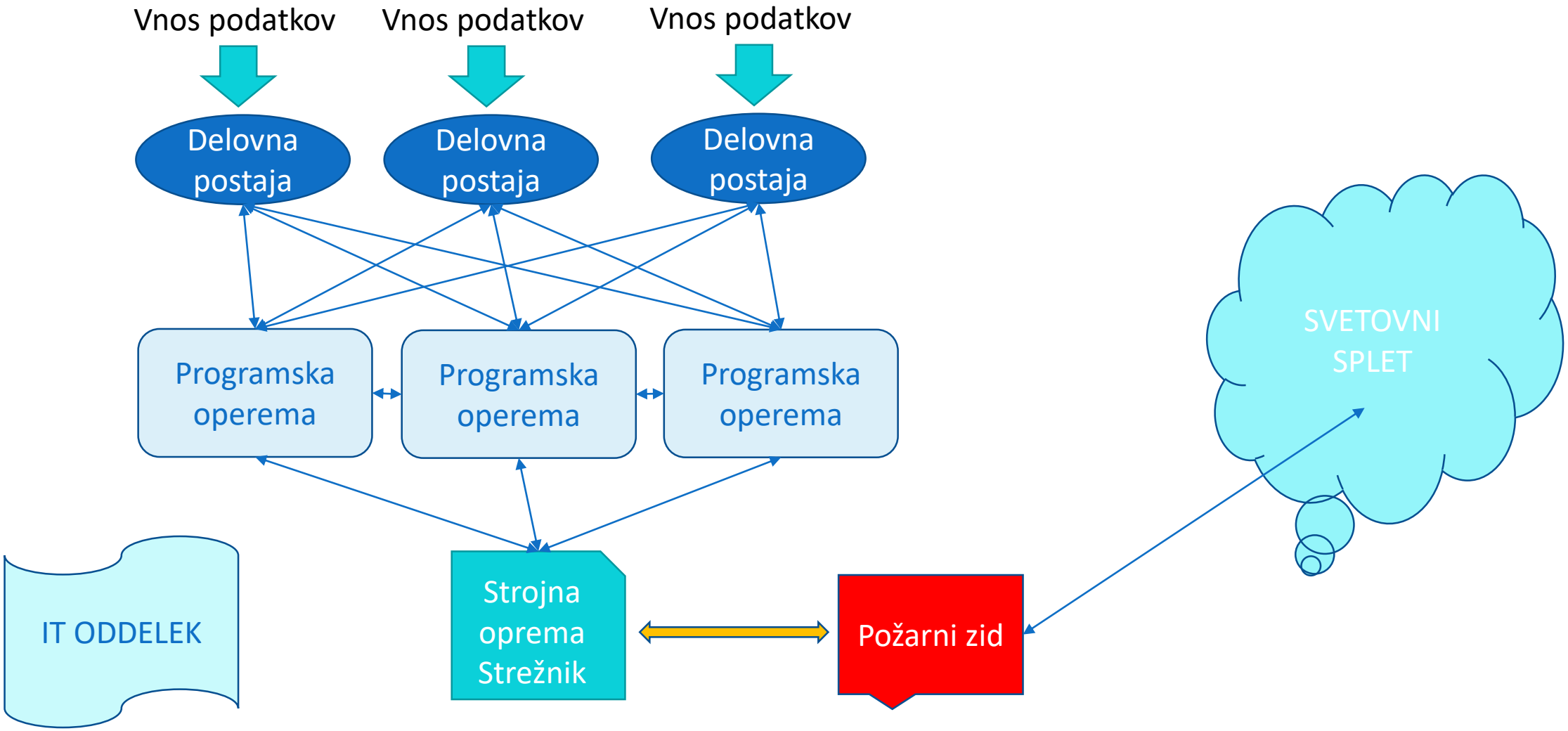
Aplikabilnost v povezavi z različno zakonodajo primer (Vir: EASA)



Aplikabilnost v povezavi z različno zakonodajo (Vir: EASA)



Ali znamo popisati trenutno stanje informacijskega sistema ?



Kaj je ISMS ?

Sistem upravljanja varnosti informacij (ISMS) je sistematičen pristop k vzpostavitvi, izvajanju, upravljanju, spremljanju, pregledovanju, vzdrževanju in nenehnem izboljševanju stanja varnostnih informacij organizacije.

Cilj je zaščititi informacijska sredstva, tako da je operativne in varnostne cilje organizacije mogoče doseči na razmeroma hiter in učinkovit način, ob zavedanju tveganj.

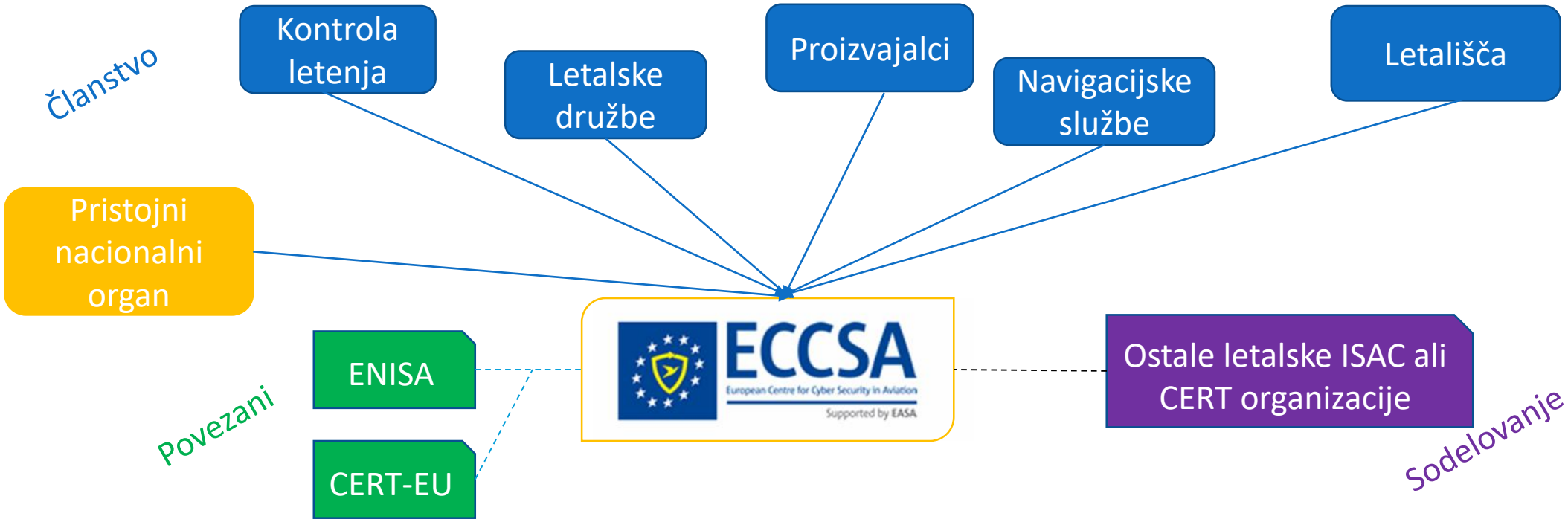
Na splošno ISMS vzpostavlja proces obvladovanja tveganja za varnost informacij, ki temelji na rezultatu analiz vpliva na informacijsko varnost, ki v osnovi določajo njen obseg. Če informacije o kršitvah varnosti lahko povzročijo ali prispevajo k posledicam za varnost v letalstvu, varnost informacij in zahteve morajo omejiti njihov vpliv na stopnje varnosti v letalstvu, ki veljajo za sprejemljive.

Torej vse vloge, procesi ali informacijski sistemi, ki lahko povzročijo ali prispevajo k varnosti v letalstvu in posledice, spadajo v področje uporabe Uredbe (EU) 2023/203. ISMS zagotavlja sredstva za odločanja o potrebnih kontrolah varnosti informacij za vse arhitekturne plasti (upravljanje, poslovanje, aplikacija, tehnologija, podatki) in področja (organizacijska, človeška, fizična, tehnična). Še naprej omogoča upravljanje izbire, izvajanja in delovanja kontrol varnosti informacij.

Končno omogoča upravljanje upravljanja, obvladovanja tveganja in skladnosti (GRC) znotraj ISMS obsega.

Kibernetska varnost – prostovoljno kooperativno partnerstvo

ECCSA je prostovoljno kooperativno partnerstvo znotraj letalske skupnosti za boljše razumevanje nastajajočih tveganj kibernetske varnosti v letalstvu in za zagotavljanje skupne podpore pri obravnavi kibernetskih incidentov, slabosti in nepooblaščenih interakcij, ki bi lahko vplivale na odpornost in varnost sektorja. Del sistema ECCSA lahko postanejo vse zainteresirani v letalski skupnosti. Bljižnica do osnovne strani: https://www.easa.europa.eu/en/eccsa



EASA priporoča (PART-IS), sodelovanje, usposabljanje in ozaveščanje

- Sodelovanje in izmenjava informacij
- Skladnost s standardi in zakonodajo
- Analiza tveganja
- Robustna varnostna politika
- Usposabljanje za zavedanje kibernetskih groženj
- Upravljanje kibernetske varnosti
- Varna omrežna infrastruktura
- Varno razvita programska oprema
- Načrt odzivanja na incidente

- Upravljanje dobaviteljev
- Redni pregledi/revizije in ocene
- Stalno spremljanje

KIBERNETSKA VARNOST uporabne informacije

Urad vlade za informacijsko varnost (URSIV):
https://www.gov.si/drzavni-organi/vladne-sluzbe/urad-vlade-za-informacijsko-varnost/

Ocena kibernetskih tveganj:
https://www.gov.si/assets/vladne-sluzbe/URSIV/Datoteke/Dokumenti/Ocena_kibernetskih_tveganj_v1_0_Fina_P.pdf

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA JAVNO UPRAVO

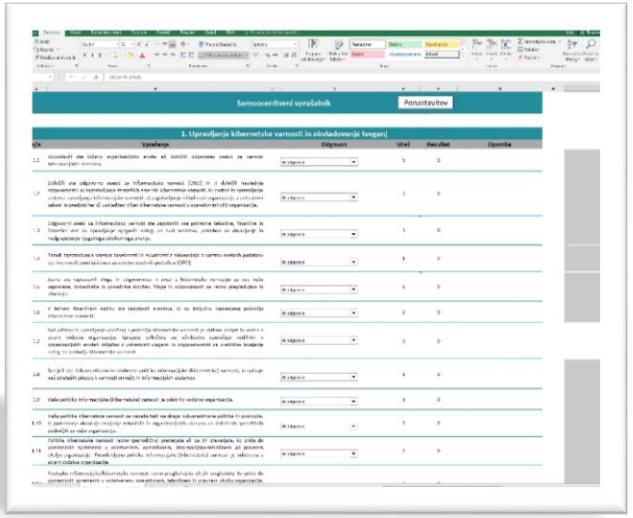
Številka: 842-2/2018/11
Datum: 26. 9. 2018

OCENA KIBERNETSKIH TVEGANJ

Verzija 1.0

	ORGAN	ODGOVORNA OSEBA
PRIPRAVILO IN SPREJELO	Ministrstvo za javno upravo	Rudi Medved Minister

Orodje za samooceno informacijske varnosti:
https://www.gov.si/assets/vladne-sluzbe/URSIV/Orodje-za-samooceno-informacijske-varnosti_ver-2.0_fixed.xlsm

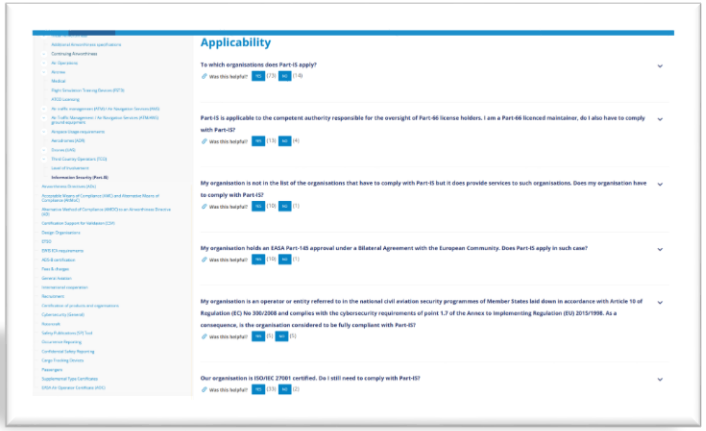

Samoocenjevalni vprašalnik

Pomantavitev

1. Upravljanje kibernetske varnosti in obvladovanje tveganj

KIBERNETSKA VARNOST uporabne informacije

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



EASA implementacijska delavnica 2024 PART-IS posnetek:

1.DAN:

https://www.youtube.com/watch?v=lBDL7B6eMzY&t=10205s

2.DAN

https://www.youtube.com/watch?v=ikrVJLRN4LE

Guidelines PART-IS oversight approach:
https://www.easa.europa.eu/community/system/files/2025-03/part-is-oversight-approach-guidelines_1.pdf