Part-IS w Organizacjach

Civil Aviation Authority

COS SPAŁA

03.04.2025

Spis treści

Part-IS w Organizacjach

Bezpieczeństwo Informacji - Wprowadzenie

Co to jest Bezpieczeństwo Informacji?

Ochrona poufności, integralności i dostępności informacji.
Zapewnienie, że informacje są dostępne tylko dla upoważnionych osób (**poufność**).
Gwarancja, że informacje są dokładne i kompletne (**integralność**).
Zapewnienie, że upoważnieni użytkownicy mają dostęp do informacji, kiedy jej potrzebują (**dostępność**).

Przykłady zagrożeń bezpieczeństwa informacji w lotnictwie

Ataki na systemy pokładowe

- Hakowanie systemów awioniki
- Zakłócenie GNSS

Zagrożenia dla systemów zarządzania ruchem lotniczym (ATM)

- Ataki na kontrolę ruchu lotniczego (ATC)
- Dezinformacja w ADS-B

2017 – testowe włamanie do Boeinga 757 – hakerzy z DHS (Department of Homeland Security) wykazali, że można przejąć kontrolę nad niektórymi funkcjami samolotu zdalnie.

Przykłady zagrożeń bezpieczeństwa informacji w lotnictwie

Ataki na linie lotnicze i pasażerów

- Kradzież danych pasażerów
- Podszywanie się pod linie lotnicze (phishing)

Zagrożenia w łańcuchu dostaw

- Fałszowanie oprogramowania pokładowego
- Nieautoryzowana ingerencja w części lotnicze

2018 – atak na British Airways – hakerzy ukradli dane kart płatniczych prawie 400 tys. pasażerów.

Przykłady zagrożeń bezpieczeństwa informacji w lotnictwie

Zagrożenia dla infrastruktury lotniskowej

Ataki ransomware

Ataki DDoS (Distributed Denial of Service)

2020 – atak ransomware na Garmin – firma dostarczająca systemy nawigacyjne dla lotnictwa ogólnego została sparaliżowana przez złośliwe oprogramowanie.

PART IS - CELE

Part-IS wprowadza wymagania dotyczące zarządzania ryzykiem bezpieczeństwa informacji, które mogą mieć wpływ na bezpieczeństwo lotnicze.

Ma na celu ochronę poufności, integralności, autentyczności i dostępności systemów i danych technologii informacyjnych i komunikacyjnych wykorzystywanych do celów lotnictwa cywilnego.

Przepisy te mają zastosowanie do różnych obszarów lotnictwa, podkreślając znaczenie bezpieczeństwa informacji w połączonym systemie lotniczym.

Part-IS jako kluczowy element kompleksowej strategii cyberbezpieczeństwa w lotnictwie.

Part-IS w Organizacjach

Rozporządzenia - wykaz

Rozporządzenia Part-IS

- Przepisy europejskie
  - Rozporządzenie 2022/1645 (Part IS dla organizacji POA, DOA dla ELA 2, operatorzy lotnisk i zarządzający płytą)
  - **Rozporządzenie 2023/203 (Part IS dla pozostałych organizacji, nadzoru)**
  - Rozporządzenie 2023/1769 (projektowaniem lub produkcją systemów i części składowych wykorzystywanych do zarządzania ruchem lotniczym/służb żeglugi powietrznej)
  - Rozporządzenie 2024/1109 (Bezzałogowe statki powietrzne)
- Wytyczne EASA
  - AMC
  - GM

Przepisy Rozporządzeń Part-IS

nakładają na podmioty oraz nadzory lotnicze

obowiązek stworzenia

Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)

Rozporządzenia Part-IS nakładają na Prezesa ULC (nowe)

obowiązki związane z zapewnieniem zgodności i

przestrzegania przepisów Rozporządzeń Part-IS przez

„podmioty lotnicze”.

Organizacje objęte Part IS

Zarządzający lotniskami i płytą postojową

Koncesjonowani przewoźnicy lotniczy (ORO)

Zatwierdzone organizacje szkoleniowe (ATO)

Operatorzy szkolnych urządzeń symulacji lotu

Organizacje podlegające załącznikowi III do Rozporządzenia 2017/373 (AMT/ANS)

Instytucje świadczące usługi U-Space

Organizacje obsługi technicznej 145 i zarządzania ciągłą zdatnością do lotu CAMO

Organizacje DOA i POA (projektujące i produkujące)

Bezzałogowe statki powietrzne

Organizacje szkolące i centra medycyny lotniczej kontrolerów ruchu lotniczego

Centra medycyny lotniczej dla załóg lotniczych

Part-IS w Organizacjach

Zastosowanie i zakres

Szerokie zastosowanie do wielu typów organizacji

Czy Organizacja podlega wg przepisu pod Rozporządzenie – PART IS

Kogo dotyczy PART IS?- przykład

Artykuł 2

Zakres stosowania

1. Niniejsze rozporządzenie ma zastosowanie do następujących organizacji:

a) organizacji obsługi technicznej podlegających sekcji A załącznika II (część 145) do rozporządzenia (UE) nr 1321/2014, z wyjątkiem organizacji zaangażowanych wyłącznie w obsługę techniczną statków powietrznych zgodnie z załącznikiem Vb (część ML) do rozporządzenia (UE) nr 1321/2014;

b) organizacji zarządzania ciągłą zdatnością do lotu (CAMO) podlegających sekcji A załącznika Vc (część CAMO) do rozporządzenia (UE) nr 1321/2014, z wyjątkiem organizacji zaangażowanych wyłącznie w zarządzanie ciągłą zdatnością do lotu statków powietrznych zgodnie z załącznikiem Vb (część ML) do rozporządzenia (UE) nr 1321/2014;

„statek powietrzny ELA1” oznacza załogowy europejski lekki statek powietrzny:

(i) samolot o maksymalnej masie startowej (MTOM) nie większej niż 1 200 kg, który nie jest sklasyfikowany jako skomplikowany statek powietrzny z napędem silnikowym;
(ii) szybowiec lub szybowiec z napędem o maksymalnej masie startowej (MTOM) nie większej niż 1 200 kg;
(iii) balon o maksymalnej nominalnej objętości gazu wznoszącego lub ogrzanego powietrza nie większej niż 3 400 m3 w przypadku balonów na ogrzane powietrze, 1 050 m3 w przypadku balonów gazowych, 300 m3 w przypadku balonów gazowych na uwięzi;
(iv) sterowiec zaprojektowany dla nie więcej niż czterech osób i o maksymalnej nominalnej ilości gazu wznoszącego lub ogrzanego powietrza nie większej niż 3 400 m3 w przypadku sterowców na ogrzane powietrze i 1 000 m3 w przypadku sterowców gazowych;

ka) „statek powietrzny ELA2” oznacza załogowy europejski lekki statek powietrzny:
(i) samolot o maksymalnej masie startowej (MTOM) nie większej niż 2 000 kg, który nie jest sklasyfikowany jako skomplikowany statek powietrzny z napędem silnikowym;
(ii) szybowiec lub szybowiec z napędem o maksymalnej masie startowej (MTOM) nie większej niż 2 000 kg;
(iii) balon;
(iv) sterowiec na ogrzane powietrze;
(v) sterowiec gazowy (…);
(vi) bardzo lekki wiropłat;

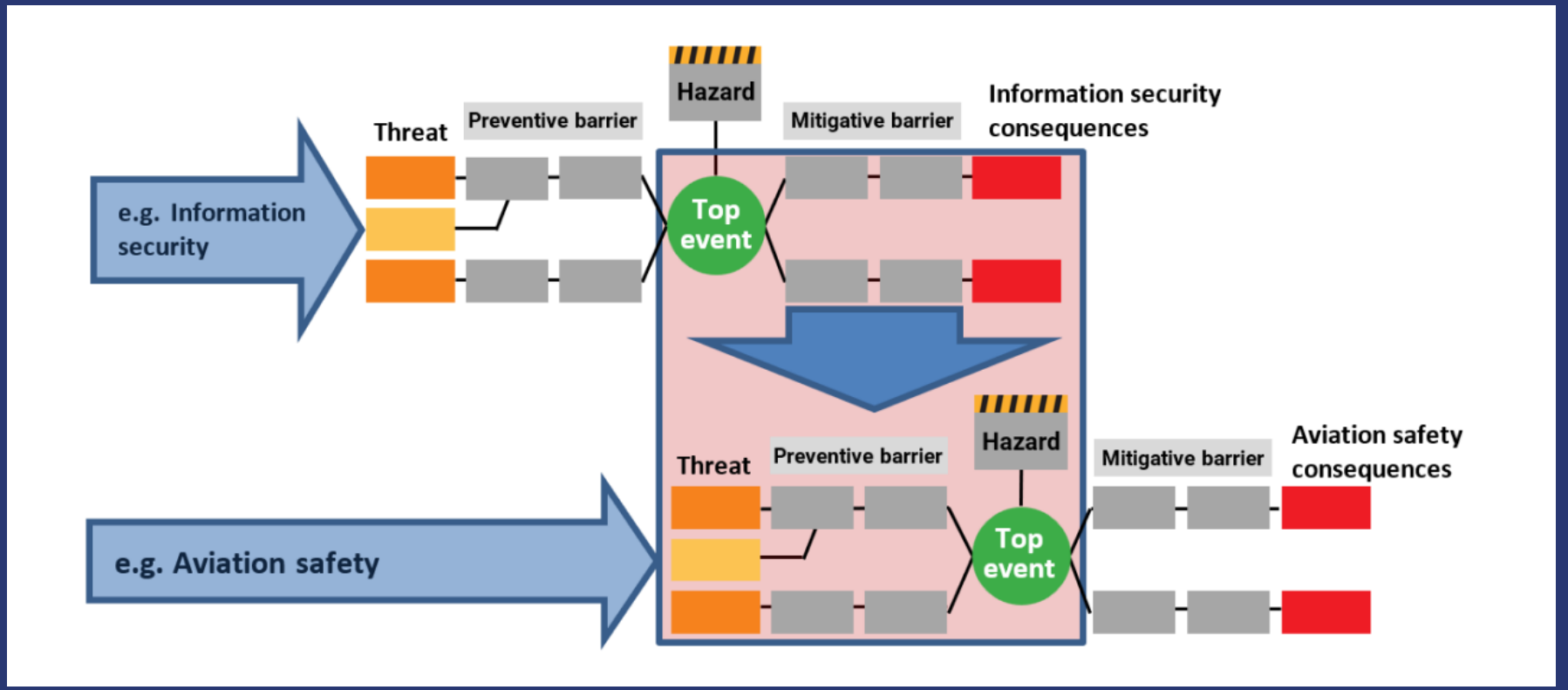
Part-IS w Organizacjach

Elementy Systemu Zarządzania Bezpieczeństwem Informacji (SZBI, ISMS):

1. Strategia zarządzania bezpieczeństwem informacji
2. Zarządzanie ryzykiem związanym z bezpieczeństwem informacji
3. Obsługa incydentów związanych z bezpieczeństwem informacji
4. Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji (wewnętrzny i zewnętrzny system zgłaszania)

Part-IS w Organizacjach

Różnice między IS a SMS



Główne wymagania dla organizacji:

1. Ustanowienie systemu zarządzania bezpieczeństwem informacji (ISMS).
2. Identyfikowanie i przeglądanie zagrożeń bezpieczeństwa informacji.
3. Definiowanie i wdrażanie środków postępowania z ryzykiem.
4. Wdrożenie wewnętrznego schematu raportowania bezpieczeństwa informacji.
5. Wdrożenie środków wykrywania zdarzeń i incydentów związanych z bezpieczeństwem informacji.
6. Reagowanie na incydenty związane z bezpieczeństwem informacji i odzyskiwanie po nich. Wdrożenie środków zgłoszonych przez właściwy organ.
7. Podejmowanie działań w celu rozwiązania ustaleń zgłoszonych przez właściwy organ.
8. Wdrożenie zewnętrznego schematu raportowania.
9. Przestrzeganie wymogów kontraktowych.
10. Przestrzeganie wymogów kadrowych.
11. Przestrzeganie wymogów dotyczących przechowywania dokumentacji.
12. Monitorowanie zgodności i przekazywanie informacji zwrotnych.
13. Ochrona poufności informacji.
14. Wdrożenie procesu ciągłego doskonalenia.
15. Udokumentowanie kluczowych procesów i procedur.

Przykłady zagrożeń i ich mitygacja

Zagrożenie	Opis	Przykłady łagodzenia ryzyka
Nieautoryzowany dostęp	Dostęp do systemów lub danych przez osoby nieupoważnione.	* Silne uwierzytelnianie (np. uwierzytelnianie wieloskładnikowe) * Listy kontroli dostępu * Zasada minimalnych uprawnień
Naruszenia danych	Ujawnienie wrażliwych informacji.	* Szyfrowanie danych podczas przesyłania i przechowywania * Środki zapobiegania utracie danych (DLP)
Ataki złośliwego oprogramowania	Wprowadzenie złośliwego oprogramowania (np. wirusów, oprogramowania ransomware) do systemów.	* Oprogramowanie antywirusowe * Regularne aktualizacje i łatanie oprogramowania * sandboxing
Ataki typu „odmowa usługi” (DoS)	Przeciążenie systemów, aby uczynić je niedostępnymi.	* Zapory ogniowe (firewalls) * Systemy wykrywania włamań (IDS) * Sieci dostarczania treści (CDN)
Ataki typu „człowiek pośrodku”	Przechwytywanie i manipulowanie danymi podczas przesyłania.	* Szyfrowanie (np. TLS/SSL) * Bezpieczne protokoły sieciowe
Zagrożenia wewnętrzne	Zagrożenia pochodzące z wewnątrz organizacji (np. niezadowoleni pracownicy).	* Sprawdzanie przeszłości pracowników * Monitorowanie aktywności pracowników * Zasada minimalnych uprawnień
Ataki na łańcuch dostaw	Kompromitacja systemu poprzez lukę w produkcie lub usłudze dostawcy.	* Ocena ryzyka dostawców * Bezpieczne praktyki rozwoju oprogramowania * Sprawdzanie integralności oprogramowania

Part-IS w Organizacjach

Proces dla Organizacji ubiegającej się o zwolnienie (Derogację)

1. Zrozumienie przepisów i określenie potrzeby derogacji.
2. Przygotowanie wniosku o derogację. Wstępna ocena wniosku przez ULC
3. Przeprowadzenie i udokumentowanie Oceny Ryzyka.
4. Złożenie wniosku i dokumentacji do Nadzoru.
5. Udzielanie dodatkowych informacji (jeśli wymagane).
6. Powiadamianie o zmianach.

Derogacji może podlegać większość wymagań, wyjątkiem jest: IS.I.OR.200 (a)(13) dot. Ochrona poufności informacji od innych organizacji , IS.I.OR.205 Ocena ryzyka, IS.I.OR.240 Personel

Przykłady organizacji, które mogą rozważyć wystąpienie o odstępstwo

• Przewoźnik lotniczy, który wykonuje operacje handlowe specjalistyczne niskiego ryzyka (SPO) nieskomplikowanymi statkami powietrznymi, jeżeli charakter operacji uzasadnia podstawy do odstępstwa.

• Przewoźnik lotniczy, który operują na statkach powietrznych ELA2 zdefiniowane w art. 1 ust. 2 lit. j) rozporządzenia (UE) nr 748/2012, z wyjątkiem statku powietrznego, który jest eksploatowany w określonych warunkach operacyjnych lub z pewnymi ograniczeniami operacyjnymi.

• Organizacja obsługi technicznej zatwierdzona na podstawie Part-145, zajmująca się wyłącznie obsługą techniczną komponentów lub czynnościami obsługi technicznej, które nie przyczyniają się do zapewnienia integralności strukturalnej statku powietrznego ani żadnych głównych funkcji związanych z bezpieczeństwem — na przykład wykonywanie czynności takich jak mycie, usuwanie powłok, malowanie itp.

Inne kluczowe wymagania

b) Organizacja powinna zidentyfikować łączące ją z innymi organizacjami interfejsy, które mogą powodować wzajemne narażenie na ryzyko związane z bezpieczeństwem informacji.

GM1 IS.I.OR.205(b) Information security risk assessment

Oznacza to, że nawet jeśli Organizacja A nie ma w pełni wdrożonego ISMS, nadal ma obowiązki dotyczące ryzyka związanego z bezpieczeństwem informacji, gdy współpracuje z Organizacją B.
Organizacja B może nałożyć na Organizację A wymagania dotyczące zarządzania ryzykiem wynikającym z ich interfejsu.

Personel- Kierownik Odpowiedzialny

- ma uprawnienia do zapewnienia, że wszystkie działania wymagane niniejszym rozporządzeniem mogą być finansowane i realizowane.
- zapewnia, że wszystkie niezbędne zasoby są dostępne do spełnienia wymogów niniejszego rozporządzenia;
- ustanawia i promuje politykę bezpieczeństwa informacji.
- wykazuje się podstawową znajomością niniejszego rozporządzenia.
- wyznacza osobę lub grupę osób, które zapewnią, że organizacja spełnia wymogi niniejszego rozporządzenia, i określić zakres ich uprawnień – raportują bezpośrednio do Kierownika Odpowiedzialnego
- wyznacza osobę lub grupę osób odpowiedzialnych za zarządzanie funkcją monitorowania zgodności.

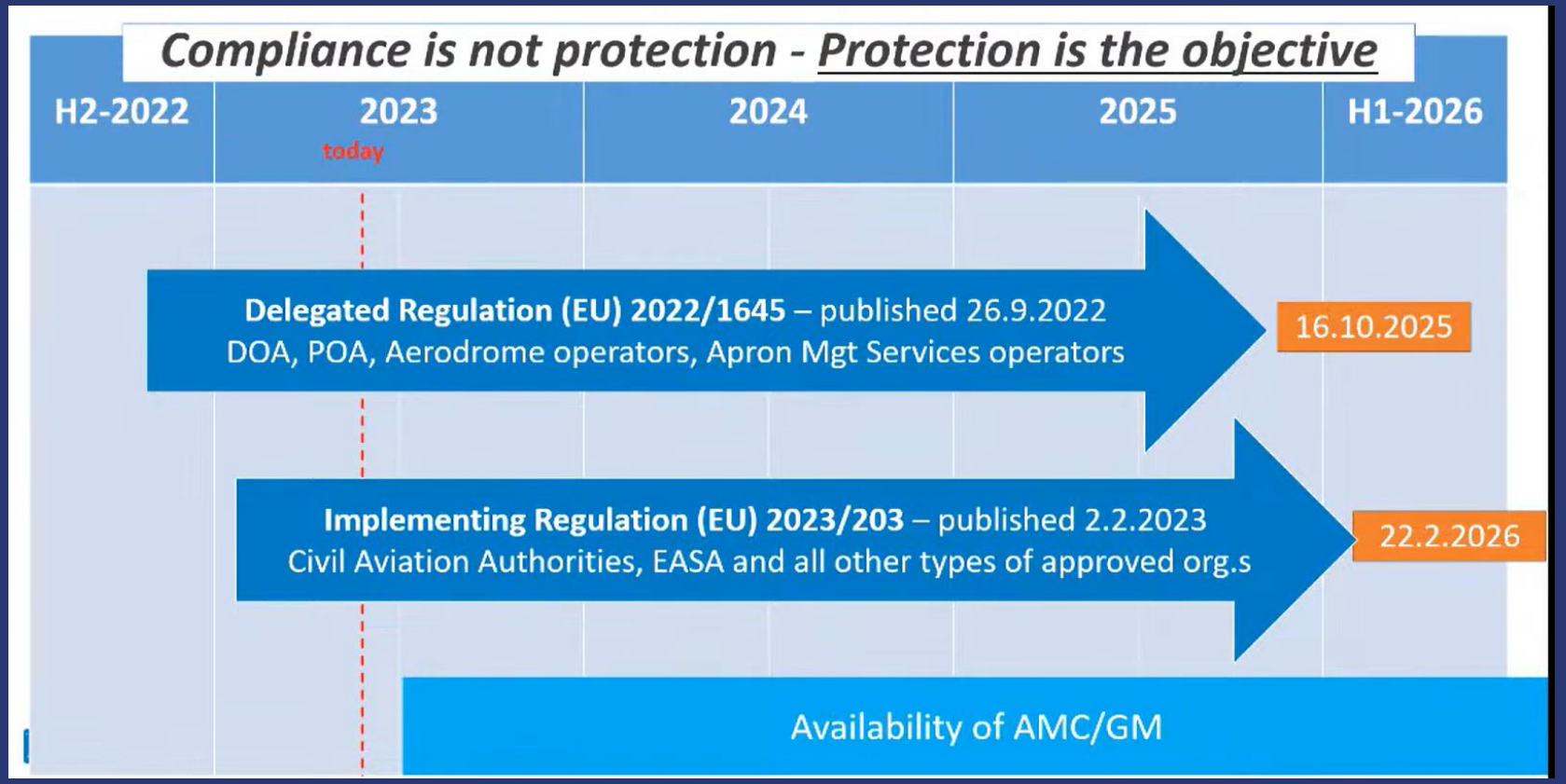
Personel – obowiązki Organizacji

Organizacja musi:

- posiadać proces zapewniający, że ma wystarczającą liczbę pracowników na służbie do wykonywania działań objętych niniejszym załącznikiem.
- posiadać proces zapewniający, że personel ma niezbędne kompetencje do wykonywania swoich zadań.
- posiadać proces zapewniający, że personel uznaje odpowiedzialność związaną z przypisanymi rolami i zadaniami.
- zapewnić, że tożsamość i wiarygodność personelu mającego dostęp do systemów informatycznych i danych podlegających wymogom niniejszego rozporządzenia zostaną odpowiednio ustalone.

Part-IS w Organizacjach

Implementacja



Rola EASA i Państw Członkowskich UE

- Komisja Europejska
- EASA
- EASA Task Force for Part-IS
- CAA/AA

1. pomoc we wdrażaniu wymogów Rozporządzenia
2. harmonizacja rozwiązań
3. nadzór
4. AMC, GM – publikacja zmian
5. Formularz do derogacji

ISO/IEC 27000 family

- **Zbiór norm:** Seria międzynarodowych standardów, które pomagają organizacjom zarządzać bezpieczeństwem aktywów informacyjnych.

- **ISO/IEC 27001:** Najważniejsza norma z rodziny, określa wymagania dla Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).

- **Inne normy:** Rodzina obejmuje również inne normy, które dostarczają wytycznych i najlepszych praktyk w różnych aspektach bezpieczeństwa informacji (np. zarządzanie ryzykiem, audytowanie, bezpieczeństwo sieci).

- **Podejście procesowe:** Normy z rodziny ISO 27000 promują podejście procesowe do zarządzania bezpieczeństwem informacji.

- **Zastosowanie:** Mogą być stosowane przez organizacje dowolnej wielkości i branży, w tym w lotnictwie.

Ponadto, mapowanie głównych zadań wymaganych w ramach Part-IS oraz klauzul i powiązanych kontroli w ISO/IEC 27001 znajduje się w Dodatku II opublikowanych Akceptowalnych Sposobów Zgodności i Materiałów Doradczych (AMC & GM) do Part-IS.

Materiały dodatkowe

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

https://www.easa.europa.eu/community/topics/part-implementation-task-force-deliverables

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

Urząd Lotnictwa Cywilnego

DZIĘKUJĘ ZA UWAGĘ

Aldona Spirzewska

LTT-2

(Specjalista, Tel: +48 734 118 963)

3.04.2025