Sudhara International
+48 32 724 35 86
info@sudharapolska.com
www.sudharapolska.com

ISMS – SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI W LOTNICTWIE. WYMAGANIA EASA PART-IS

PROGRAM SZKOLENIA

🎯 **Cel szkolenia:**

Celem szkolenia jest przygotowanie uczestników do skutecznego wdrożenia oraz nadzorowania wymagań Rozporządzenia (UE) 2022/1645, czyli PART-IS, w organizacjach lotniczych. Uczestnicy zdobędą wiedzę z zakresu zarządzania bezpieczeństwem informacji w środowisku lotniczym, poznają wymagania dotyczące systemu ISMS, procedury ochrony informacji krytycznych, a także sposoby reagowania na incydenty i przeprowadzania audytów wewnętrznych zgodnie z PART-IS i wytycznymi EASA.

Program szkolenia:

PRE-TEST

1. Kontekst regulacyjny i geneza PART-IS.
    - Rozporządzenie wykonawcze Komisji (UE) 2022/1645: ustanowienie obowiązków w zakresie bezpieczeństwa informacji dla organizacji objętych przepisami EASA.
    - Zakres zastosowania PART-IS – do kogo ma zastosowanie i w jakim zakresie.
    - Kluczowe definicje: information security, critical information, information asset, vulnerability, threat.
    - Podział odpowiedzialności – rola NAA (National Aviation Authority), EASA i organizacji lotniczych
    - **ĆWICZENIE: Analiza krótkiego studium przypadku.**
2. Przegląd struktury PART-IS, AMC i GM.
    - Podział PART-IS na sekcje: IS.GEN, IS.OPS, IS.MGT.
    - Wprowadzenie do dokumentów AMC (Acceptable Means of Compliance) – minimalne wymagania.
    - Wprowadzenie do GM (Guidance Material) – dobre praktyki i wytyczne interpretacyjne.
    - Przegląd relacji z ISO 27001 i innych regulacji (np. NIS2, RODO).
    - **ĆWICZENIE: Analiza wybranego przepisu PART-IS oraz jego interpretacji w AMC i GM.**
3. Kluczowe wymagania PART-IS i wdrażanie ISMS.
    - Wymóg wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji (ISMS).
    - Opracowanie polityki bezpieczeństwa informacji.

+48 32 724 35 86
info@sudharapolska.com
www.sudharapolska.com

- Zarządzanie personelem, dostępem do informacji i odpowiedzialnością.
- Ciągłe doskonalenie systemu (planowanie, ocena skuteczności, przeglądy, raportowanie).
- **ĆWICZENIE: Tworzenie elementów polityki bezpieczeństwa informacji dla organizacji lotniczej (warsztat grupowy).**

4. Ochrona informacji krytycznych.
   - Identyfikacja i klasyfikacja informacji istotnych z punktu widzenia bezpieczeństwa (Operational Security Data).
   - Kategorie informacji: dane lotów, dane maintenance, dane systemów komunikacji i zarządzania ruchem (ATM/ANS).
   - Środki techniczne i organizacyjne – kontrola dostępu, szyfrowanie, ochrona fizyczna, segmentacja sieci.
   - Wymagania w zakresie współpracy z podwykonawcami i dostawcami.
   - **ĆWICZENIE: Scenariusz – identyfikacja informacji krytycznych w wybranym procesie operacyjnym (CAMO, Part-145, ATM).**
5. Zarządzanie ryzykiem i reagowanie na incydenty.
   - Wymóg przeprowadzenia oceny ryzyka i utrzymywania jej aktualności.
   - Zarządzanie ryzykiem i identyfikacja zagrożeń zgodnie z Rozporządzeniem 2023/203 oraz ISO/IEC 27005:2025-01**.**
   - Identyfikacja zagrożeń – cyberatak, nieautoryzowany dostęp, modyfikacja danych.
   - Reagowanie na incydenty i system zgłaszania niezgodności (w tym zgodność z rozporządzeniem o zgłaszaniu zdarzeń w lotnictwie).
   - Zarządzanie naruszeniami ochrony informacji i dokumentowanie działań naprawczych.
   - **ĆWICZENIE: Symulacja: zgłoszenie i analiza incydentu informacyjnego zgodnie z wymaganiami PART-IS.**
6. Monitorowanie, audyty i działania doskonalące.
   - Planowanie i prowadzenie przeglądów ISMS zgodnie z PART-IS i AMC.
   - Audyty wewnętrzne oraz niezależna ocena skuteczności działań.
   - Integracja wymagań PART-IS z istniejącymi systemami zarządzania (np. Part-145, CAMO, ISO 9001, 27001).
   - Rola personelu odpowiedzialnego za nadzór.
   - **ĆWICZENIE: Przegląd przykładowego formularza audytu IS – identyfikacja luk i zaleceń.**

POST-TEST

+48 32 724 35 86
info@sudharapolska.com
www.sudharapolska.com

🧠 **Grupa odbiorcza:**

Szkolenie przeznaczone jest dla:

- Kierowników i specjalistów ds. bezpieczeństwa informacji w lotnictwie.
- Osób odpowiedzialnych za zgodność z przepisami EASA (Compliance Monitoring Managers).
- Menedżerów i inżynierów CAMO, Part-145 oraz ATM/ANS.
- Przedstawicieli działów IT, którzy współpracują z działami operacyjnymi w zakresie bezpieczeństwa danych.
- Auditorów wewnętrznych systemów zarządzania w organizacjach lotniczych.

🚀 **Korzyści po szkoleniu:**

Po ukończeniu szkolenia uczestnicy będą potrafili:

- Zrozumieć strukturę i wymagania regulacyjne PART-IS oraz ich powiązania z ISO 27001, NIS2, RODO.
- Wdrażać i doskonalić System Zarządzania Bezpieczeństwem Informacji (ISMS) w organizacjach objętych przepisami EASA.
- Identyfikować, klasyfikować i chronić informacje krytyczne dla bezpieczeństwa operacji lotniczych.
- Zarządzać ryzykiem informacyjnym i reagować na incydenty zgodnie z obowiązującymi procedurami.
- Współpracować z podwykonawcami i zapewniać zgodność bezpieczeństwa informacji w łańcuchu dostaw.
- Planować i realizować audyty zgodności z PART-IS oraz przygotować organizację na zewnętrzną kontrolę.

🧰 **Metodyka szkoleniowa:**

- Wprowadzenie teoretyczne z wykorzystaniem diagramów, modeli ISMS i przykładów dokumentacji.
- Warsztaty grupowe: opracowywanie polityki bezpieczeństwa informacji, identyfikacja zasobów i ryzyk.
- Studium przypadków: analiza naruszeń, błędów systemowych i reakcji organizacyjnych.
- Ćwiczenia praktyczne: formularze audytowe, raporty incydentów, dokumentacja ochrony informacji.
- Dyskusje moderowane – wymiana doświadczeń między uczestnikami z różnych obszarów branży.
- Pre-test i post-test umożliwiający ocenę postępu i przyswojenia wiedzy.
- Materiały szkoleniowe w formie elektronicznej oraz szablony dokumentów do wykorzystania wewnętrznie.

Czas trwania szkolenia – 2 dni