

Zrozumienie wymagań IS.I.OR.235 i perspektywy nadzoru (IS.AR.220)



Urząd
Lotnictwa
Cywilnego

02.09.2025



Odpowiedzialność Zawsze Pozostaje w Organizacji

Organizacja zlecająca (np. CAMO, Part-145) pozostaje w pełni odpowiedzialna za zgodność z przepisami Part-IS.

Działania firmy zewnętrznej są traktowane tak, jakby były wykonywane przez samą organizację.

Kierownik Odpowiedzialny (Accountable Manager) ponosi ostateczną odpowiedzialność





IS.I.OR.235 Zlecenie czynności w zakresie zarządzania bezpieczeństwem informacji

- a) Organizacja zapewnia, aby w przypadku zlecenia innym organizacjom realizacji dowolnej części czynności, o których mowa w pkt IS.I.OR.200, zlecane czynności były zgodne z wymaganiami określonymi w niniejszym rozporządzeniu, a organizacja przyjmująca zlecenie wykonywała prace pod jej nadzorem. Organizacja zapewnia odpowiednie zarządzanie ryzykiem związanym ze zlecanymi czynnościami.
- b) Na żądanie organizacja zapewnia właściwemu organowi możliwość dostępu do organizacji przyjmującej zlecenie w celu ustalenia stałego przestrzegania mających zastosowanie wymagań określonych w niniejszym rozporządzeniu.





Checklista – zlecanie czynności przez Organizację

- ✓ **Umowa:** Wszystkie zlecane czynności muszą być określone w formalnej umowie.
- ✓ **Kompetencje:** Organizacja musi się upewnić, że podwykonawca jest kompetentny i zdolny do wykonania powierzonych zadań.
- ✓ **Integracja z ISMS:** Zlecane działania muszą być zintegrowane z Systemem Zarządzania Bezpieczeństwem Informacji (ISMS) organizacji.
- ✓ **Nadzór:** Organizacja musi monitorować i oceniać działania podwykonawcy.
- ✓ **Dostęp dla Nadzoru:** Umowa musi gwarantować Właściwemu Organowi (ULC) dostęp do podwykonawcy w celu przeprowadzania audytów i inspekcji.



Przykład dla Organizacji 145

Scenariusz: Organizacja obsługowa zleca zewnętrznej firmie przeprowadzenie corocznych testów penetracyjnych swojej sieci IT.

- **Jak zastosować IS.I.OR.235?**

- **Umowa:** Precyzyjnie określa zakres testów (które systemy, jakie metody), harmonogram i format raportowania.

- **Kompetencje:** Organizacja Part-145 weryfikuje, czy firma posiada certyfikowanych specjalistów (np. OSCP, CEH) i doświadczenie w testowaniu systemów produkcyjnych. – Procedura oceny podwykonawcy w MOE

- **Integracja z ISMS:** Wyniki testu (znalezione luki) są formalnie rejestrowane w rejestrze ryzyka ISMS. Na ich podstawie tworzone są działania korygujące.

- **Dostęp dla Nadzoru:** W umowie znajduje się zapis o możliwości uczestnictwa audytora ULC w spotkaniach omawiających wyniki testów.



Perspektywa Nadzoru (IS.AR.220)

Czego Oczekuje ULC?

Nadzór musi być poinformowany o zleceniu przez organizację kluczowych czynności w zakresie bezpieczeństwa informacji.

Weryfikuje, czy organizacja spełnia wszystkie wymagania z IS.I.OR.235 (umowa, kompetencje, integracja, nadzór).

Musi mieć zapewniony bezpośredni dostęp do podwykonawcy i jego dokumentacji w celu przeprowadzania własnych audytów i inspekcji.

Cel: Zapewnienie, że zlecenie czynności nie obniża poziomu bezpieczeństwa i nie utrudnia skutecznego nadzoru.

Podsumowanie

3 Rzeczy do Zapamiętania:



Odpowiedzialność zostaje w Organizacji.

Zlecanie zadań $\neq$ pozbycie się odpowiedzialności.



Formalna umowa to podstawa.

Musi precyzyjnie określać zadania, obowiązki i zapewniać dostęp dla ULC.



To część Twojego systemu (ISMS).

Działania podwykonawcy muszą być w pełni zintegrowane z Twoimi procesami zarządzania ryzykiem i incydentami.



DZIĘKUJĘ ZA UWAGĘ

Aldona Spirzewska

LTT-2

(Specjalista, Tel: +48 734 118 963)