

RZESZÓW, 02.09.2025

Part IS

Wymagania dla personelu



Civil
Aviation
Authority

WOJCIECH STUDZIŃSKI
DYREKTOR
DEPARTAMENT LOTNISK





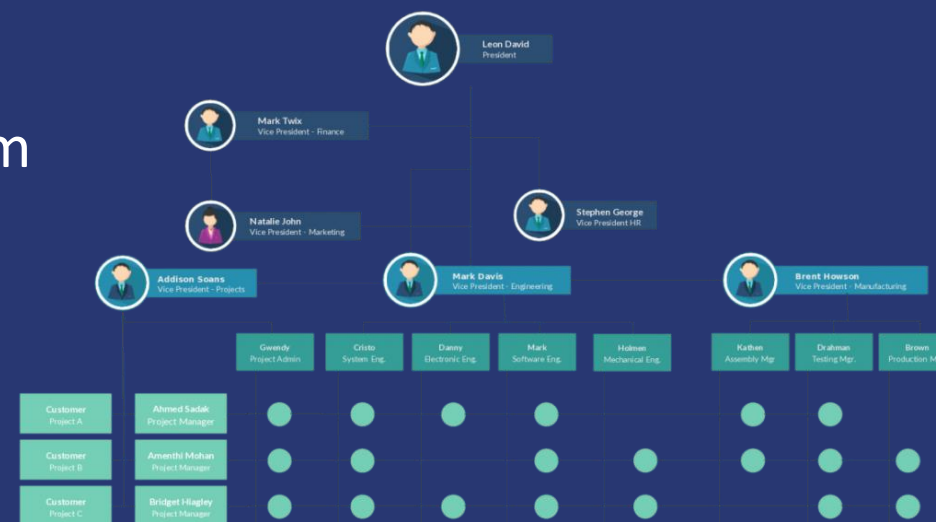
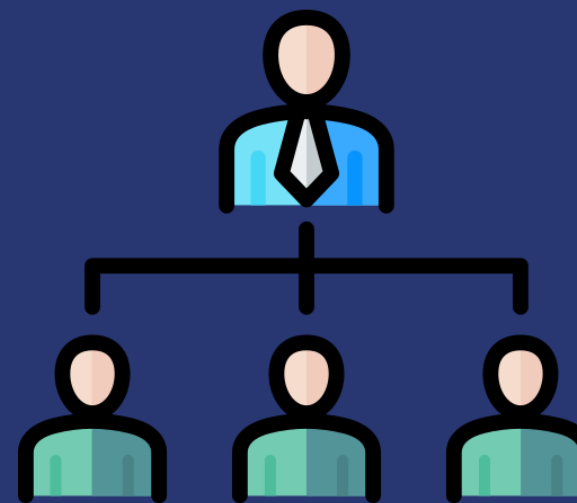
WYMAGANIA DOTYCZĄCE PERSONELU IS.AR.225 / IS.I.OR.240 / IS.D.OR.240

- Cel wdrożenia wymagań
- Wymagania, GM i AMC
- *The Accountable Manager* / Kierownik Odpowiedzialny
- *Common Responsible Person* / Wspólna Osoba Odpowiedzialna
- PART IS – Koordynacja w przypadku CRP
- Kompetencje i obowiązki
- Lista kontrolna dla IS.AR.225 / IS.I.OR.240 / IS.D.OR.240

CEL WDROŻENIA WYMAGAŃ

Celem wymogów (GM1 IS.I.OR.240) zawartych w rozporządzeniu jest:

- ✓ zapewnienie skutecznej struktury organizacyjnej w celu spełnienia wymogów niniejszego rozporządzenia;
- ✓ zapewnienie zaufania innym organizacjom, z którymi dzielone jest ryzyko



Wymagania, GM i AMC

IR (EU) 2023/203 Annex II – IS.I.OR.240 Wymagania dotyczące personelu

Wymaganie	GM, AMC	Odniesienia
a) Kierownik odpowiedzialny (...), posiada uprawnienia służbowe w celu zapewnienia możliwości finansowania i prowadzenia wszystkich czynności wymaganych w niniejszym rozporządzeniu. Osoba ta:	GM1 IS.I.OR.240	
(1) zapewnia dostępność wszystkich zasobów niezbędnych do zapewnienia zgodności z wymaganiami niniejszego rozporządzenia;		
(2) ustanawia i promuje strategię bezpieczeństwa informacji, o której mowa w pkt IS.D.OR.200 lit. a) 1)	AMC1 IS.I.OR.240(a)(2)	
(3) jest w stanie wykazać się podstawową wiedzą na temat niniejszego rozporządzenia.	GM1 IS.I.OR.240(a)(3)	
b) Kierownik odpowiedzialny lub, w przypadku organizacji projektujących, dyrektor organizacji projektującej wyznacza osobę lub grupę osób odpowiedzialnych za utrzymanie zgodności organizacji z wymaganiami niniejszego rozporządzenia oraz określa zakres kompetencji tych osób. Taka osoba lub grupa osób odpowiada bezpośrednio przed kierownikiem odpowiedzialnym lub w przypadku organizacji projektujących dyrektorem organizacji projektującej oraz legitymuje się wiedzą, praktyką i doświadczeniem zawodowym odpowiednimi do powierzonego zakresu odpowiedzialności. W procedurach określa się, kto zastępuje daną osobę w przypadku jej długotrwałej nieobecności.	GM1 IS.I.OR.240(b) GM1 IS.I.OR.240(b) i (c) AMC1 IS.I.OR.240(b)	
c) Kierownik odpowiedzialny lub, w przypadku organizacji projektujących, dyrektor organizacji projektującej wyznacza osobę lub grupę osób odpowiedzialnych za zarządzanie funkcją monitorowania zgodności, o której mowa w pkt IS.D. OR.200 lit. a) ppkt 12.	GM1 IS.I.OR.240(b) i (c) GM1 IS.I.OR.240(c)	

Wymagania, GM i AMC

IR (EU) 2023/203 Annex II – IS.I.OR.240 Wymagania dotyczące personelu

Wymaganie	GM, AMC	Odniesienia
d) Jeżeli struktury organizacyjne, strategie, procesy i procedury w zakresie bezpieczeństwa informacji organizacji są wspólne z innymi organizacjami lub z obszarami własnej organizacji, które nie są objęte zatwierdzeniem ani oświadczeniem, kierownik odpowiedzialny lub, w przypadku organizacji projektujących, dyrektor organizacji projektującej mogą delegować swoje działania wspólnej osobie odpowiedzialnej. W takim przypadku wprowadza się środki koordynacji między kierownikiem odpowiedzialnym organizacji lub, w przypadku organizacji projektujących, dyrektorem organizacji projektującej a wspólną osobą odpowiedzialną w celu zapewnienia odpowiedniej integracji zarządzania bezpieczeństwem informacji w organizacji.	AMC1 IS.I.OR.240(c)	
e) Kierownik odpowiedzialny, lub dyrektor organizacji projektującej, lub wspólna osoba odpowiedzialna, o której mowa w lit. d), posiada uprawnienia służbowe do ustanowienia i utrzymania struktur organizacyjnych, strategii, procesów i procedur niezbędnych do wdrożenia pkt IS.D.OR.200.	GM1 IS.I.OR.240(e)	ENISA <u>European Cybersecurity Skills Framework</u> (ECSF)
f) Organizacja stosuje procedurę zapewniającą dysponowanie personelem dyżurującym wystarczającym do przeprowadzenia czynności objętych niniejszym załącznikiem.	GM1 IS.I.OR.240(f) AMC1 IS.I.OR.240(f)	

Wymagania, GM i AMC

IR (EU) 2023/203 Annex II – IS.I.OR.240 Wymagania dotyczące personelu

Wymaganie	GM, AMC	Odniesienia
g) Organizacja stosuje procedurę zapewniającą, aby personel, o którym mowa w lit. f), posiadał niezbędne kompetencje do realizacji powierzonych mu zadań.	GM1 IS.I.OR.240(g) AMC1 IS.I.OR.240(g)	NIST <u>Cybersecurity Skills Framework</u> (CSF); <u>National Initiative for Cybersecurity Education</u> (NICE)
h) Organizacja stosuje procedurę zapewniającą, aby personel przyjmował do wiadomości obowiązki związane z przydzielonymi funkcjami i zadaniami.	GM1 IS.I.OR.240(h) AMC1 IS.I.OR.240(h)	
i) Organizacja zapewnia, aby prawidłowo ustalono tożsamość i wiarygodność personelu mającego dostęp do systemów informatycznych i danych podlegających wymaganiom niniejszego rozporządzenia.	GM1 IS.I.OR.240(i) AMC1 IS.I.OR.240(i)	

Wymagania, GM i AMC

Part IS główne zadanie	Rodzaj Aktywności	Odniesienie					
	Zarządzanie / Operacyjne	Part IS	NIST CSF Version 1.1		ISO/IEC 27001		
			Funkcja	Kategoria	Paragraf-Punkt	Załącznik A Kontrola	
						:2013	:2022
Stworzenie i utrzymywanie procesu zapewniającego wystarczającą liczbę pracowników do wykonywania wszystkich czynności związanych z zarządzaniem bezpieczeństwem informacji.	Zarządzanie	IS.D.OR.240(f)	Identyfikacja	ID.AM-5 ID.AM-6 ID.GV-2	7.1	A6.1.1	A5.2
Stworzenie i utrzymywanie procesu zapewniającego, że personel posiada niezbędne kompetencje do działań związanych z zarządzaniem bezpieczeństwem informacji.	Zarządzanie	IS.D.OR.240(g)	Identyfikacja	ID.AM-5 ID.AM-6	7.2	A7.2.2	A6.3
			Ochrona	PR.AT-1			
Stworzenie i utrzymywanie procesu zapewniającego, że personel przyjmuje do wiadomości obowiązki związane z przypisanymi rolami i zadaniami.	Zarządzanie	IS.D.OR.240(h)	Identyfikacja	ID.GV-2 ID.GV-3	7.3 7.4	A7.1.2	A6.2
Weryfikacja tożsamości i wiarygodności personelu mającego dostęp do systemów informatycznych.	Zarządzanie	IS.D.OR.240(i)	Ochrona	PR.AC-6 PR.IP-11	7.1	A7.1.1	A6.1

The Accountable Manager / Kierownik Odpowiedzialny

- ✓ Wykazuje się podstawową znajomością przepisów rozporządzenia (*GM1 IS.I.OR.240(a)(3)*) - **szkolenia**
- ✓ Posiada właściwe **uprawnienia** korporacyjne celem:
 - zapewnienia dostępności wszystkich niezbędnych zasobów;
 - ustanowienia i promowania polityki bezpieczeństwa;





The Accountable Manager / Kierownik Odpowiedzialny

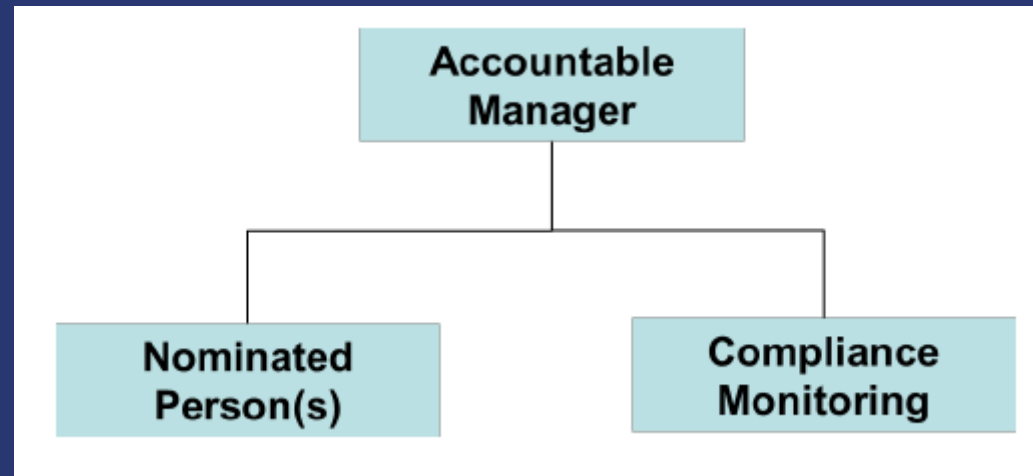
- ✓ Wyznacza (*GM1 IS.I.OR.240(b)*) **osobę** (lub grupę osób) w celu zapewnienia zgodności z wymogami.

Należy dodatkowo zapewnić, że:

- znane są zasady raportowania do Kierownika Odpowiedzialnego
- znany jest zakres uprawnień osoby / poszczególnych osób
- personel wykazuje się znajomością przepisów, a także odpowiednim doświadczeniem i wiedzą
- ustalony jest system zastępstw w przypadku nieobecności kluczowego personelu

The Accountable Manager / Kierownik Odpowiedzialny

- ✓ Wyznacza osobę (lub grupę osób) do zarządzania funkcją monitorowania zgodności (*GM1 IS.I.OR.240(c)*)





Common Responsible Person / Wspólna Osoba Odpowiedzialna

Jeśli kierownik odpowiedzialny lub kierownik organizacji projektującej deleguje wspólną osobę odpowiedzialną (CRP) do działań objętych rozporządzeniem, osoba ta powinna również otrzymać odpowiednie uprawnienia niezbędne do wdrożenia postanowień IS.D.OR.200, w tym uprawnienia i środki finansowe do mobilizowania i kontrolowania zasobów w zaangażowanych organizacjach lub częściach organizacji. Delegowanie to może również obejmować wyznaczenie osoby lub grupy osób, o których mowa w IS.D.OR.240 lit. b) i c), oraz, ogólnie rzecz biorąc, CRP może być wspomagany w wykonywaniu swoich obowiązków przez dodatkowy personel.

Common Responsible Person / Wspólna Osoba Odpowiedzialna

Możliwość delegowania CRP ma zastosowanie do organizacji, która dzieli struktury organizacyjne, polityki, procesy i procedury w zakresie bezpieczeństwa informacji z innymi organizacjami lub z częściami własnej organizacji, które nie są objęte upoważnieniem lub oświadczeniem, a zatem oczekuje się, że CRP będzie miał obowiązki i kompetencje w zakresie bezpieczeństwa informacji.





CRP - Koordynacja

- ✓ Kryteria służące ustanowieniu koordynacji zapewniającej odpowiednią integrację SZBI w ramach organizacji (AMC1 IS.I.OR.240(d)):
 - zakres i granice organizacji zostały ustalone i przekazane do CRP;
 - wymogi rozporządzenia zostały przekazane i udostępnione CRP;
 - CRP ma bezpośredni dostęp do Kierownika Odpowiedzialnego;
 - ustanowiono system proaktywnego zarządzania, a wszelkie wczesne sygnały wskazujące na niezgodności są dokumentowane i podejmowane są odpowiednie działania



PART IS – Kompetencje i obowiązki

Organizacja musi wdrożyć procedury zapewniające:

- ✓ wystarczającą ilość personelu do wykonywania niezbędnych działań;
- ✓ personel posiada niezbędne kompetencje do wykonywania swoich zadań;
- ✓ personel potwierdza swoją odpowiedzialność związaną z przypisanymi rolami i zadaniami

Organizacja powinna zapewnić, że tożsamość i wiarygodność personelu (mającego dostęp do systemów informatycznych i danych podlegających wymogom rozporządzenia) są odpowiednio potwierdzone (AMC1 IS.I.OR.240(i), GM1 IS.I.OR.240(i)).

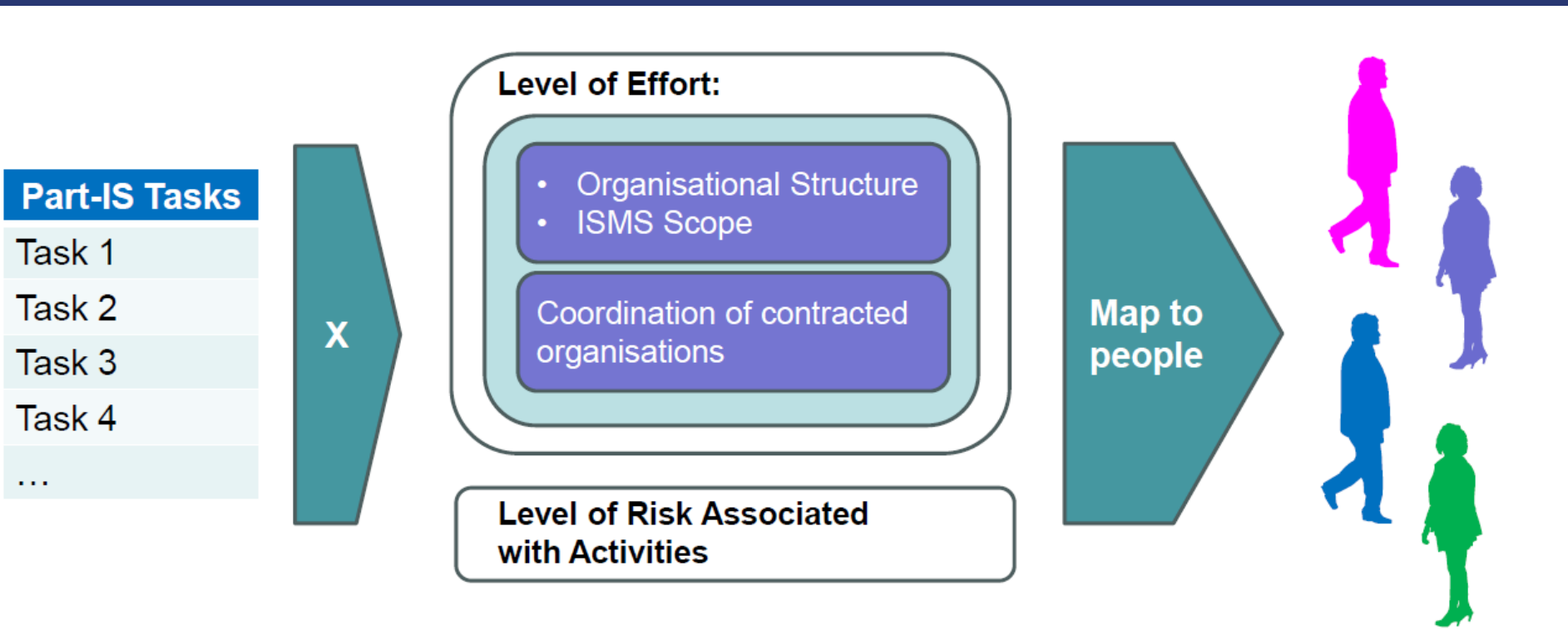


PART IS – Kompetencje i obowiązki

Personel odnosi się do kombinacji osób bezpośrednio zatrudnionych przez organizację, jak również osób zakontraktowanych, zgodnie z IS.D.OR.235.

Działania zgłoszone w Dodatku II, dotyczące głównych zadań wynikających z wdrożenia Part IS, należy uwzględnić przy ustalaniu struktury organizacyjnej niezbędnej do spełnienia wymogów niniejszego rozporządzenia.

PART IS – Kompetencje i obowiązki



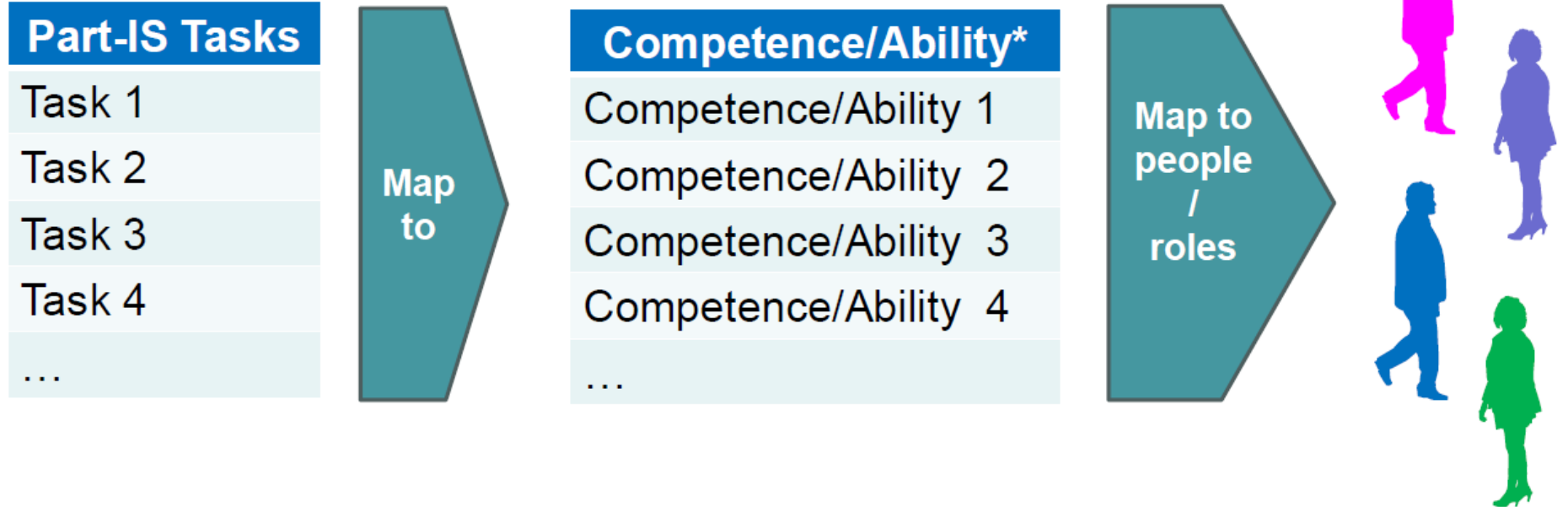


PART IS – Kompetencje i obowiązki

Aby określić kompetencje wymagane od personelu wykonującego czynności, należy wziąć pod uwagę następujące elementy:

- 1) role zawodowe i związane z nimi zadania;
- 2) wymagana wiedza, umiejętności i zdolności.

PART IS – Kompetencje i obowiązki





Lista kontrolna dla IS.AR.225 / IS.I.OR.240 / IS.D.OR.240

Czy Kierownik odpowiedzialny jest uprawniony do zapewnienia,
że wszystkie wymagane działania mogą zostać sfinansowane
i zrealizowane tj:

- ✓ dostępne są wszystkie niezbędne zasoby do spełnienia wymogów?
- ✓ polityka bezpieczeństwa jest ustanowiona i promowana?
- ✓ Kierownik odpowiedzialny wykazuje się podstawową znajomością Rozporządzenia?



Lista kontrolna dla IS.AR.225 / IS.I.OR.240 / IS.D.OR.240

Czy Kierownik odpowiedzialny wyznaczył osobę (lub grupę) do zapewnienia zgodności z wymogami rozporządzenia, a w szczególności:

- ✓ określił zakres jej (ich) uprawnień?
- ✓ zapewnił bezpośrednią poległość tej osoby / tych osób?
- ✓ osoba (lub grupa) posiada odpowiednią wiedzę, doświadczenie i wiedzę, aby wypełniać swoje obowiązki?
- ✓ został ustanowiony system zastępstw w przypadku dłuższej nieobecności Kierownika Odpowiedzialnego?

An abstract graphic on the left side of the slide, featuring a series of blue, curved, and overlapping lines that create a sense of depth and movement, resembling a stylized tunnel or a complex architectural structure.

Lista kontrolna dla IS.AR.225 / IS.I.OR.240 / IS.D.OR.240

- ✓ Czy Kierownik odpowiedzialny wyznaczył osobę (lub grupę) odpowiedzialną za zarządzanie funkcją monitorowania zgodności?
- ✓ Czy Kierownik Odpowiedzialny w przypadku, gdy organizacja współdzieli struktury organizacyjne, polityki, procesy i procedury (lub obszary własnej organizacji), deleguje swoje działania wspólnej osobie odpowiedzialnej?
- ✓ Czy ustanowiono środki koordynacji między Kierownikiem Odpowiedzialnym organizacji a Wspólną Osobą Odpowiedzialną celem zapewnienia odpowiedniej integracji?

An abstract graphic on the left side of the slide, featuring a series of blue, curved, and overlapping lines that create a sense of depth and movement, resembling a stylized architectural or mechanical structure.

Lista kontrolna dla IS.AR.225 / IS.I.OR.240 / IS.D.OR.240

- ✓ Czy Kierownik Odpowiedzialny lub Wspólna Osoba Odpowiedzialna ma uprawnienia korporacyjne do ustanawiania i utrzymywania struktur organizacyjnych, polityk, procesów i procedur niezbędnych do wdrożenia IS.I.OR.200?
- ✓ Czy organizacja wdrożyła procedury mające na celu zapewnienie odpowiedniej liczby personelu dyżurnego w celu wykonywania działań objętych rozporządzeniem?

An abstract graphic on the left side of the slide, featuring a series of blue, curved, and overlapping lines that create a sense of depth and movement, resembling a stylized tunnel or a complex architectural structure.

Lista kontrolna dla IS.AR.225 / IS.I.OR.240 / IS.D.OR.240

- ✓ Czy organizacja wdrożyła procedury zapewniające, że personel posiada niezbędne kompetencje do wykonywania swoich zadań?
- ✓ Czy organizacja wdrożyła procedury zapewniające, że personel uznaje obowiązki związane z przypisanymi rolami i zadaniami?
- ✓ Czy organizacja zapewniła, że tożsamość i wiarygodność personelu mającego dostęp do systemów informatycznych i danych są odpowiednio potwierdzone?



DZIĘKUJĘ ZA UWAGĘ!



Wojciech Studziński
DYREKTOR
DEPARTAMENT LOTNISK
wstudzinski@ulc.gov.pl
+48 519 528 625