Zmniejszanie ryzyka związanego z bezpieczeństwem informacji

(IS.I.OR.210)

Urząd Lotnictwa Cywilnego

08.09.2025

Zmniejszanie ryzyka związanego z bezpieczeństwem informacji

Co mówi przepis IS.D.OR.205 / IS.I.OR.210?

a) Organizacja opracowuje środki służące wyeliminowaniu niedopuszczalnego ryzyka zidentyfikowanego zgodnie z pkt IS.I.OR.205, terminowo wdraża te środki i kontroluje ich ciągłą skuteczność. Środki te umożliwiają organizacji:

Środki

1) kontrolowanie okoliczności, które przyczyniają się do faktycznego wystąpienia scenariusza zagrożenia;
2) ograniczenie skutków dla bezpieczeństwa lotniczego urzeczywistnienia się scenariusza zagrożenia;
3) uniknięcie ryzyka.

Cele

Środki te nie mogą stwarzać jakiegokolwiek nowego potencjalnego niedopuszczalnego ryzyka dla bezpieczeństwa lotniczego.

ISMS/SZBI → **SMS**

Zmniejszanie ryzyka związanego z bezpieczeństwem informacji

Co mówi przepis IS.D.OR.205 / IS.I.OR.210?

b) Osobę, o której mowa w pkt IS.I.OR.240 lit. a) i b), oraz innych narażonych członków personelu organizacji należy powiadomić o wyniku oceny ryzyka przeprowadzonej zgodnie z pkt IS.I.OR.205 oraz o powiązanych scenariuszach zagrożenia i wprowadzanych środkach.

Kierownik odpowiedzialny w organizacji wyznaczony, odpowiednio, zgodnie z rozporządzeniami wykonawczymi

Osoba lub grupa osób odpowiedzialnych za zapewnienie zgodności organizacji z wymaganiami Part-IS

Organizacja informuje również organizacje, z którymi jest połączona interfejsem zgodnie z pkt IS.I.OR.205 lit. b), o każdym rodzaju ryzyka wspólnym dla obu organizacji.

Właściciele

Zmniejszanie ryzyka związanego z bezpieczeństwem informacji

AMC1 IS.I.OR.210(a)

a) Proces postępowania z ryzykiem powinien osiągać co najmniej jeden z celów wymienionych w IS.I.OR.210(a).

b) Ustalając zgodność z celami określonymi w punktach IS.I.OR.210(a)(1) i IS.I.OR.210(a)(2), organizacja powinna uwzględnić, że:

- środki opracowane w ramach tych punktów powinny być wdrażane zgodnie z planem postępowania z ryzykiem, z określonymi priorytetami opartymi na ryzyku, celami, uzgodnionymi harmonogramami i właścicielami;
- należy zidentyfikować i powiązać względy dotyczące cyklu życia aktywów/elementów, aby zapewnić ciągłą skuteczność środków bezpieczeństwa informacji, w tym wymianę danych z innymi podmiotami;
- zgodnie z IS.I.OR.205(d) należy dokonać przeglądu i aktualizacji oceny ryzyka, aby ocenić, czy opracowane środki nie wprowadzają nowych, niedopuszczalnych ryzyk lub nie modyfikują istniejących ryzyk w taki sposób, że stają się one niedopuszczalne / nieakceptowalne.

c) Postępowanie z ryzykiem powinno być udokumentowane i zarejestrowane, na przykład w rejestrze ryzyka, nawet jeśli ryzyko zostało uniknięte.

Zmniejszanie ryzyka związanego z bezpieczeństwem informacji

AMC1 IS.I.OR.210(a)

- Plan zarządzania ryzykiem
  - Priorytety
  - Cele
  - Terminy i właściciele
- Uwzględnienie cyklu życia aktywów
- Przegląd i aktualizacja oceny ryzyka zgodnie z IS.I.OR.205(d)
- Zapis i udokumentowanie procesu zmniejszania/ograniczania ryzyka

Zmniejszanie ryzyka związanego z bezpieczeństwem informacji

GM1 IS.I.OR.210

1. Wymóg zarządzania niedopuszczalnym ryzykiem

Każde ryzyko zidentyfikowane jako niedopuszczalne (zgodnie z IS.I.OR.205) musi zostać objęte formalnym procesem zarządzania ryzykiem. Celem jest:

- redukcja ryzyka do poziomu akceptowalnego,
- wdrożenie i utrzymanie środków bezpieczeństwa informacji (kontroli),
- zapewnienie ciągłości działań poprzez monitorowanie i reakcję na zmiany.

2. Środki zarządzania ryzykiem – zakres

Dla każdego ryzyka organizacja powinna określić i udokumentować środki obejmujące:

- **Redukcję ryzyka** – kontrole techniczne, proceduralne, organizacyjne.
- **Monitorowanie i utrzymanie aktywów** – cykliczne kontrole, testy, przeglądy.
- **Zarządzanie konfiguracją** – procedury aktualizacji, zgodność z politykami bezpieczeństwa.
- **Łańcuch dostaw** – wymagania bezpieczeństwa wobec dostawców, audyty.
- **Usługi kontraktowe** – kontrola i nadzór nad podmiotami zewnętrznymi.

Uwzględnia się cały **cykl życia aktywów**: od wdrożenia, przez eksploatację, po wycofanie.

Zmniejszanie ryzyka związanego z bezpieczeństwem informacji

GM1 IS.I.OR.210

3. Plan zarządzania ryzykiem, który powinien obejmować:

- **priorytetyzację ryzyk** (np. wg prawdopodobieństwa i skutków),
- **cele i środki zarządzania** przypisane do ryzyk,
- **harmonogram wdrożenia** – terminy uzgodnione z odpowiedzialnymi osobami,
- **akceptację kierownika** odpowiedzialnego lub osoby odpowiedzialnej,
- **procedurę dokumentowania opóźnień** wraz z przyczynami i uzasadnieniem.

W przypadku ryzyk, które mogą prowadzić do **stanu niebezpiecznego**, każde opóźnienie musi być:

- zaakceptowane,
- ewentualnie powiązane z zastosowaniem **środków kompensacyjnych** (monitoring, detekcja, szybka reakcja).

Zmniejszanie ryzyka związanego z bezpieczeństwem informacji

GM1 IS.I.OR.210

4. Reakcja i eskalacja

- W razie opóźnień lub ryzyka **materializacji zagrożenia** → informacja musi trafić do **właściwego organu**.
- Należy aktywować lub poinformować **zespół reagowania na incydenty**, aby był gotowy do szybkiego działania.

5. Komunikacja i współpraca

Plan zarządzania ryzykiem:

- **dokumentuje zgodność** i stanowi środek komunikacji z właściwymi organami,
- może być podstawą do **współpracy między organizacjami**, gdy istnieją ryzyka wspólne (np. w projektach partnerskich).

6. Regularny przegląd

Zgodnie z IS.I.OR.205(d) i IS.I.OR.210(a):

- regularne przeglądy oceny ryzyka są obowiązkowe,
- należy weryfikować aktualność i skuteczność środków zarządzania ryzykiem,
- jeśli wymagana jest korekta – wprowadza się dostosowania w planie i dokumentacji.

Zmniejszanie ryzyka związanego z bezpieczeństwem informacji

4T Risk Mitigation Method

Transfer
P[illegible]esienie
s[illegible]z
ube[illegible]ub
[illegible]
e[illegible]zycję
organizacji.

Tolerate
Akceptacja ryzyka, gdy jego wpływ lub prawdopodobieństwo jest niskie, a koszt działań zapobiegawczych przewyższa korzyści.

Terminate
Całkowite wyeliminowanie ryzyka poprzez zaprzestanie działalności lub procesu, który je wywołuje, jeśli jest to możliwe.

Treat
Wdrożenie środków kontroli lub działań mających na celu zmniejszenie prawdopodobieństwa lub skutków ryzyka, np. poprzez lepsze zabezpieczenia lub ulepszenia procesów.

Zmniejszanie ryzyka związanego z bezpieczeństwem informacji

Wymóg	Mapowanie z ISO/IEC 27001	Wytyczne dla Part-IS
IS.OR.210 (a) *Organizacja opracowuje środki służące wyeliminowaniu niedopuszczalnego ryzyka zidentyfikowanego zgodnie z pkt IS.I.OR.205, terminowo wdraża te środki i kontroluje ich ciągłą skuteczność.* *1) …* *2) …* *3) …*	6.1.3 Postępowanie z ryzykiem bezpieczeństwa informacji 8.3 Wdrażanie planu postępowania z ryzykiem	ISO/IEC 27001 6.1.3 dotyczy definicji planu postępowania z ryzykiem, natomiast 8.3 – jego wdrożenia. Załącznik A ISO/IEC 27001 zawiera listę możliwych kontroli bezpieczeństwa informacji, które mogą być stosowane w celu ograniczenia ryzyk wpływających na bezpieczeństwo. IS.I.OR.210(a) wymaga, aby środki w planie zmniejszały skutki dla bezpieczeństwa lotniczego wynikające z materializacji zagrożenia. Środki te nie mogą wprowadzać nowych nieakceptowalnych ryzyk dla bezpieczeństwa lotniczego, co dotyczy tzw. efektów ubocznych wprowadzania środków do systemu (np. fizyczne zabezpieczenia lub kontrola dostępu mogą powodować niezamierzone skutki uboczne). Postępowanie z ryzykiem powinno integrować bezpieczeństwo informacji i bezpieczeństwo operacyjne.

Zmniejszanie ryzyka związanego z bezpieczeństwem informacji

Wymóg	Mapowanie z ISO/IEC 27001	Wytyczne dla Part-IS
IS.OR.210 (b) *Osobę, o której mowa w pkt IS.I.OR.240 lit. a) i b), oraz innych narażonych członków personelu organizacji należy powiadomić o wyniku oceny ryzyka przeprowadzonej zgodnie z pkt IS.I.OR.205 oraz o powiązanych scenariuszach zagrożenia i wprowadzanych środkach.*	**6.1.3.f** Postępowanie z ryzykiem bezpieczeństwa informacji **7.3** Świadomość **9.3** Przegląd zarządzania **A5.19** Bezpieczeństwo informacji w relacjach z dostawcami **A5.21** Zarządzanie bezpieczeństwem informacji w łańcuchu dostaw ICT	Poza zatwierdzeniem planu przez właściciela ryzyka, organizacja musi: • Poinformować kierownika odpowiedzialnego o planie (przegląd zarządzania). • Poinformować podmioty powiązane o ryzykach współdzielonych (zgodnie z wytycznymi GM1 IS.I.OR.205(b) i ED-201A).

Zmniejszanie ryzyka związanego z bezpieczeństwem informacji

Jak poinformować kierownika odpowiedzialnego?

- Szczegółowy raport zawierający scenariusze zagrożeń
- Lista kluczowych niezgodności/podatności
- Propozycje działań ograniczających ryzyko wraz z analizą kosztów i korzyści
- Plan wdrożenia działań zawierający „kamienie milowe”

Zmniejszanie ryzyka związanego z bezpieczeństwem informacji

Przykłady zakontraktowanych działań dla środków zmniejszania ryzyka:

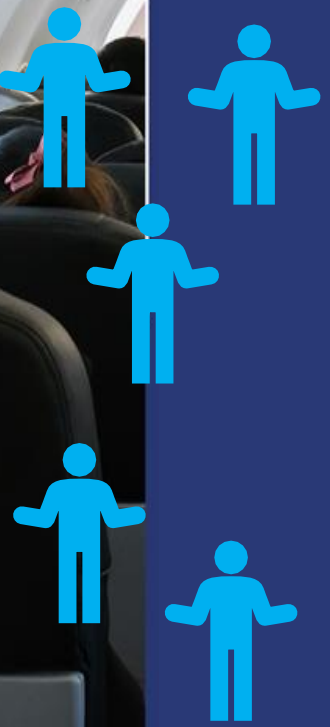
- Weryfikacja początkowej i ciągłej skuteczności wdrożonych środków
- Ćwiczenia typu red-team/blue-team
- Testy penetracyjne
- Skanowanie podatności

Komunikacja z zaangażowanymi interesariuszami wyników oceny ryzyka oraz ich obowiązków w ramach procesu leczenia ryzyka.

Testy penetracyjne (ang. penetration testing, często nazywane pentesting) to kontrolowane symulacje ataków na systemy informatyczne, sieci, aplikacje lub infrastrukturę organizacji w celu zidentyfikowania i zweryfikowania podatności (słabości) w zabezpieczeniach. Ich celem jest sprawdzenie, jak dobrze systemy są chronione przed rzeczywistymi atakami hakerskimi oraz wskazanie obszarów wymagających poprawy.

Zmniejszanie ryzyka związanego z bezpieczeństwem informacji

Ćwiczenia typu red team/blue team to symulacje bezpieczeństwa stosowane głównie w cyberbezpieczeństwie, ale także w innych dziedzinach, takich jak bezpieczeństwo fizyczne czy zarządzanie ryzykiem. Polegają one na podziale uczestników na dwa zespoły: red team (zespół czerwony) i blue team (zespół niebieski), które odgrywają przeciwstawne role w celu przetestowania i doskonalenia zabezpieczeń organizacji.



Zespół Niebieski ***d****ziała jako "obrońcy" organizacji.*

- *Jego zadaniem jest wykrywanie, zapobieganie i reagowanie na działania red teamu, aby chronić systemy i dane.*
- *Odpowiada za monitorowanie, analizę logów, wdrażanie zabezpieczeń i reagowanie na incydenty.*
- *Przykłady działań: analiza ruchu sieciowego, aktualizacja zapór sieciowych, reagowanie na wykryte zagrożenia.*

Zespół Czerwony ***d****ziała jako "atakujący" lub symulowany przeciwnik.*

- *Jego celem jest identyfikacja słabości w systemach, procesach lub infrastrukturze organizacji poprzez próby ich naruszenia (np. symulowane ataki hakerskie, socjotechnika, testy penetracyjne).*
- *Używa realistycznych scenariuszy, aby naśladować działania prawdziwych cyberprzestępców lub innych zagrożeń.*
- *Przykłady działań: próby włamania do systemów IT, testowanie zabezpieczeń fizycznych, wykorzystanie podatności /luk.*

Zmniejszanie ryzyka związanego z bezpieczeństwem informacji

Podsumowanie – do zapamiętania!

IS.OR.210(a):
Organizacja powinna opracować i wdrożyć środki ograniczające niedopuszczalne (nieakceptowalne) ryzyka bezpieczeństwa informacji, które: kontrolują wystąpienie zagrożenia, zmniejszają skutki dla bezpieczeństwa lotniczego, unikają ryzyk.

Środki nie mogą wprowadzać nowych niedopuszczalnych ryzyk. Planowanie i wdrożenie powinno uwzględniać integrację SZBI/ISMS i bezpieczeństwa operacyjnego (SAFETY).

IS.OR.210(b):
Kluczowy personel oraz podmioty powiązane muszą być poinformowane o ryzykach, scenariuszach zagrożeń i wdrażanych środkach. Informacje te są wymagane do przeglądu zarządzania i do współpracy międzyorganizacyjnej przy ryzykach współdzielonych.

DZIĘKUJĘ ZA UWAGĘ

Dorota KOWALSKA

Naczelnik Wydziału Analiz Bezpieczeństwa Lotniczego
Departament Zarządzania Bezpieczeństwem w Lotnictwie Cywilnym
tel. +48 (22) 520 73 37, tel. kom. +48 538 550 691
e-mail: dkowalska@ulc.gov.pl

SUPPORTING EUROPEAN AVIATION

Prezentacja przygotowana z wykorzystaniem wybranych materiałów EUROCONTROL

08.09.2025