IS.I.OR.255 Zmiany w systemie zarządzania bezpieczeństwem informacji

IS.I.OR.260 Ciągłe doskonalenie

Urząd Lotnictwa Cywilnego

02.09.2025

IS.I.OR.255 Zmiany w systemie zarządzania bezpieczeństwem informacji

“Jedyną stałą rzeczą w życiu jest zmiana”

Heraklit z Efezu

02.09.2025

IS.I.OR.255 Zmiany w systemie zarządzania bezpieczeństwem informacji

a) Zarządzanie zmianami w SZBI i powiadamianie o nich właściwego organu może przebiegać w ramach procedury opracowanej przez organizację. Procedurę tę zatwierdza właściwy organ.

b) Jeżeli chodzi o zmiany w SZBI nieobjęte procedurą, o której mowa w lit. a), organizacja ubiega się o zatwierdzenie wydawane przez właściwy organ i musi je uzyskać.

W odniesieniu do tych zmian:

1) wniosek składa się przed wprowadzeniem wszelkich zmian w celu umożliwienia właściwemu organowi stwierdzenia, czy zachowana zostanie zgodność z niniejszym rozporządzeniem, oraz – jeśli zajdzie taka potrzeba – zmiany certyfikatu organizacji i powiązanych warunków zatwierdzania dołączonych do certyfikatu;

2) organizacja przekazuje właściwemu organowi wszelkie informacje, których organ ten zażąda w celu dokonania oceny zmiany;

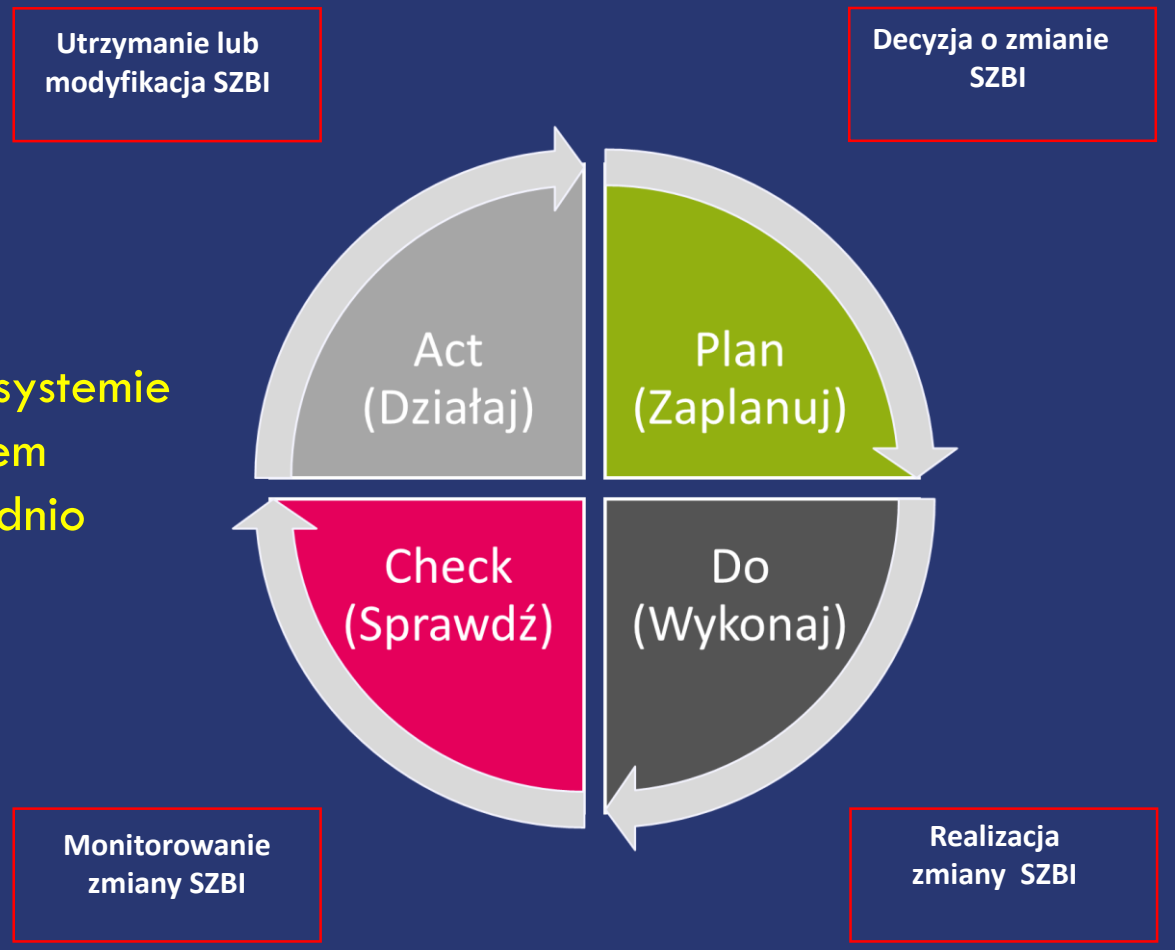
3) zmianę wprowadza się wyłącznie po otrzymaniu formalnego zatwierdzenia przez właściwy organ;

4) organizacja wprowadza tego typu zmiany zgodnie z warunkami określonymi przez właściwy organ.

IS.I.OR.255 Zmiany w systemie zarządzania bezpieczeństwem informacji

Celem tego wymagania jest:

- zapewnienie, że zmiany w systemie zarządzania bezpieczeństwem informacji (SZBI) są odpowiednio zarządzane



IS.I.OR.255 Zmiany w systemie zarządzania bezpieczeństwem informacji

Zmiany objęte procedurą

Procedura zarządzania zmianą – ważne czynniki

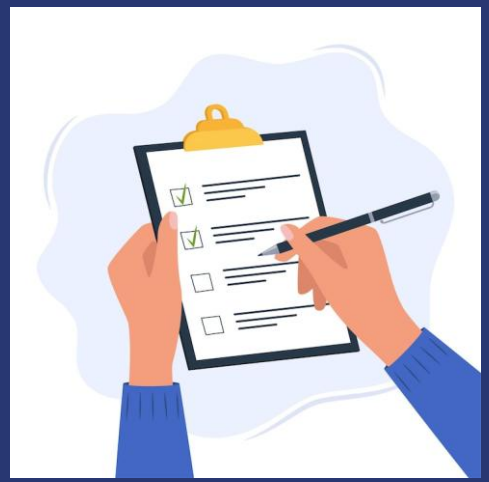
- Procedura powinna uwzględniać krytyczność zmiany.
- Szczególną uwagę należy zwrócić na zmiany, które mogą:
- mieć wpływ na utrzymanie lub osiągnięcie zgodności z rozporządzeniem lub
- prowadzić do niedopuszczalnego poziomu ryzyka.
- Zmiany w procedurze powinny podlegać zatwierdzeniu przez właściwy organ.

IS.I.OR.255 Zmiany w systemie zarządzania bezpieczeństwem informacji

Zmiany nie objęte procedurą - informacje

Gdy organizacja ubiega się o uprzednią zgodę właściwego organu na zmianę nieobjętą zatwierdzoną procedurą lub gdy taka zatwierdzona procedura nie istnieje, powinna ona przedstawić co najmniej następujące informacje:

— charakter i cel zmiany;
— plan wdrożenia zmiany;
— plan weryfikacji zmiany;
— potencjalny wpływ na bezpieczeństwo lotnicze wprowadzony przez zmianę.



Zmiany wynikające z procesu ciągłego doskonalenia ustanowionego przez organizację (patrz IS.I.OR.260) należy traktować jak każdą inną zmianę zgodnie z wytycznymi zawartymi w AMC1 IS.I.OR.255 i GM1 IS.I.OR.255

IS.I.OR.255 Zmiany w systemie zarządzania bezpieczeństwem informacji

Przykłady zmian mających wpływ na SZBI:

a) Zmiany zakresu SZBI, interfejsów lub powiązanych polityk:

— Organizacja rozszerza swoje funkcje biznesowe i integruje inną firmę w ramach swojej struktury organizacyjnej.
— Organizacja zidentyfikowała niezgodności wskazujące na nieprawidłowy zakres.
— Organizacja zmienia swoją politykę bezpieczeństwa informacji i/lub cele bezpieczeństwa informacji, co może mieć wpływ na bezpieczeństwo lotnicze.
— Zmiany w interfejsach organizacji wynikające np. z modyfikacji działań zleconych na zewnątrz

b) Zmiany w zakresie obowiązków i odpowiedzialności , a także w strukturze organizacyjnej związanej z wdrażaniem i ciągłym monitorowaniem zgodności z niniejszym rozporządzeniem:

— Kierownik odpowiedzialny delegował określone obowiązki wynikające z Części IS osobie lub grupie osób.
— Organizacja zleca działania z zakresu zarządzania bezpieczeństwem informacji zgodnie z IS.I.OR.235.

IS.I.OR.255 Zmiany w systemie zarządzania bezpieczeństwem informacji

Przykłady zmian mających wpływ na SZBI:

(c) Zmiany w metodologii stosowanej w zarządzaniu ryzykiem:

— Organizacja zmienia klasyfikację prawdopodobieństwa lub wpływu w swojej metodologii zarządzania ryzykiem, np. w celu uzyskania większej szczegółowości.

— Organizacja wdraża zmiany w swojej metodologii postępowania z ryzykiem.

— Organizacja integruje zarządzanie ryzykiem bezpieczeństwa informacji z istniejącymi systemami zarządzania.

(d) Zmiany w procesie zarządzania zdarzeniami bezpieczeństwa:

— Organizacja podejmuje decyzję o zleceniu działań z zakresu zarządzania zdarzeniami bezpieczeństwa.

— Organizacja zmienia proces powiadamiania o zdarzeniach bezpieczeństwa oraz kryteria eskalacji do kierownictwa wyższego szczebla w celu szybszego rozwiązania.

— Organizacja zmienia swoją politykę ograniczania podatności .

— Organizacja zmienia swoją procedurę przywracania po incydencie.

IS.I.OR.255 Zmiany w systemie zarządzania bezpieczeństwem informacji

Przykłady zmian nie mających wpływ na SZBI:

— Po pomyślnym wykryciu zdarzenia związanego z bezpieczeństwem, które mogło łatwo przekształcić się w incydent, organizacja decyduje się na wdrożenie szeroko zakrojonej kampanii uświadamiającej w zakresie cyberbezpieczeństwa dla wszystkich pracowników.

— Aktualizacja programu szkoleń personelu i/lub treści szkoleń w wyniku procesów ciągłego doskonalenia wdrożonych w organizacji.

— Organizacja zastępuje narzędzie programowe używane do szyfrowania poufnych plików innym rozwiązaniem programowym.

— Organizacja zdecydowała się na wewnętrzną restrukturyzację z przyczyn biznesowych, zmieniając nazwy działów lub sekcji, bez wprowadzania żadnych zmian w zakresie obowiązków i odpowiedzialności (np. kierownika odpowiedzialnego) w ramach SZBI organizacji.

— Organizacja decyduje się na aktualizację istniejącego środka ochrony, np. poprzez skonfigurowanie nowej zapory sieciowej w sieci wewnętrznej

IS.I.OR.260 Ciągłe doskonalenie

IS.I.OR.260 Ciągłe doskonalenie

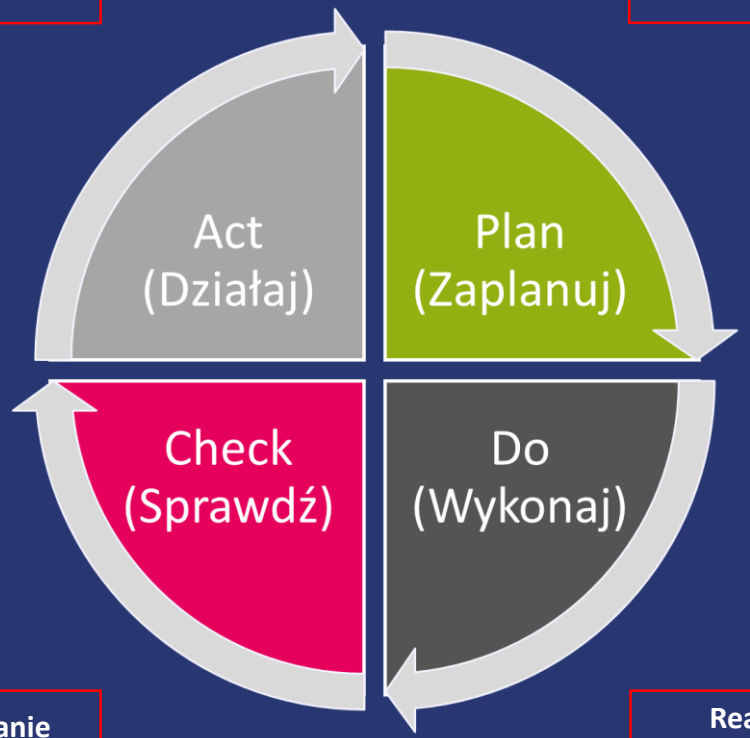
a) *Stosując odpowiednie wskaźniki skuteczności działania, organizacja dokonuje oceny skuteczności i stopnia zaawansowania SZBI. Oceny tej dokonuje się według kalendarza wcześniej ustalonego przez organizację lub po wystąpieniu incydentu związanego z bezpieczeństwem informacji.*

b) *Jeżeli w toku oceny przeprowadzonej zgodnie z lit. a) zostają wykryte uchybienia, organizacja podejmuje niezbędne środki poprawy w celu utrzymania zgodności systemu SZBI z mającymi zastosowanie wymaganiami i umożliwienia utrzymania dopuszczalnego poziomu ryzyka związanego z bezpieczeństwem informacji. Ponadto organizacja ponownie ocenia elementy SZBI, na które przyjęte środki wpływają.*

IS.I.OR.260 Ciągłe doskonalenie

Celem tego wymagania jest:

- ciągłe podnoszenie skuteczności, przydatności i adekwatności SZBI



IS.I.OR.260 Ciągłe doskonalenie

Proces ciągłego doskonalenia (PCD) SZBI:

- proaktywna i systematyczna ocena SZBI oraz wszystkich jego elementów, włączając poziom dojrzałości systemu;
- uwzględnia wyniki i wnioski z innych procesów zapewniania bezpieczeństwa informacji, w tym audytów, przeglądów zarządzania, oceny zdolności, skuteczności i dojrzałości, a także wyniki podjętych działań korygujących i korekt;
- organizacja może zintegrować PCD SZIB z innym istniejącym PCD;
- może stosować metodę PDCA (Plan-Do-Check-Act) lub DMAIC (Define-Measure-Analyse-Improve-Control)

IS.I.OR.260 Ciągłe doskonalenie

Etapy procesu ciągłego doskonalenia powinny obejmować co najmniej:

a) Identyfikację możliwości usprawnień w oparciu o wyniki oceny SZBI
b) Ocenę zidentyfikowane możliwości w zakresie stosunku kosztów do korzyści, braku lub ograniczenia niepożądanych skutków oraz osiągnięcia założonych celów i zamierzonych rezultatów.
(c) Propozycję dla kierownictwa dotyczącą możliwości usprawnień oraz zalecenia dotyczące działań wspierających ich przegląd i podejmowanie decyzji.
(d) Planowanie, opracowywanie i wdrażanie działań oraz zmian w SZBI, jego procesach lub elementach w celu osiągnięcia usprawnień.
(e) Ocenę skuteczności wdrożonych działań i zmian w SZBI

IS.I.OR.260 Ciągłe doskonalenie

- Identyfikacja możliwości usprawnień
  - Propozycje usprawnień pochodzą ze źródeł takich jak:
    - wyniki regularnej analizy ryzyka i późniejszego postępowania z ryzykiem
    - wnioski z (kluczowych) wskaźników efektywności, ich pomiaru, analizy i ciągłego monitorowania
    - dojrzałość, w tym wyniki późniejszych korekt i działań korygujących
    - wnioski wyciągnięte z wykrywania incydentów bezpieczeństwa
    - wyniki (wewnętrznych) audytów itp.

IS.I.OR.260 Ciągłe doskonalenie

Ocena skuteczności SZBI i ocena dojrzałości SZBI

Kluczowe pytania do sprawdzenia:

- Kto ?
- Kiedy ?
- Jakie metody ?

Minimalne wymagania:

- Gromadzenie i przechowywanie metryk działań i dodatkowych informacji
- Analiza metryk w celu identyfikacji trendów i odchyleń

Ocena dojrzałości SZBI:

- Zdefiniowanie lub przyjęcie modelu dojrzałości
- Dla każdego ocenianego procesu lub zdolności, zdefiniowanie kryteriów, względem których oceniane są konkretne aspekty
- Określenie i pożądany docelowy poziom dojrzałości

IS.I.OR.260 Ciągłe doskonalenie

Przykładowe modele oceny dojrzałości

- Zestaw cech, atrybutów, wskaźników lub wzorców;
- Zapewnia punkt odniesienia, względem którego organizacja może ocenić aktualny poziom możliwości swoich praktyk, procesów i metod oraz wyznaczyć cele i priorytety doskonalenia;
- Modele dojrzałości zazwyczaj mają skalę definiującą poziomy dojrzałości;

Table 1: Mapping matrix of an existing MM to a hypothetical five-level MM

Mapping to a five-level MM	C2M2	Eurocontrol NM	ISO 21827	NIST CSF 1.1
Initial	MIL 0	Non-Existent	Performed Informally	
Defined	MIL 1 (Initial)	Partial	Planned & Tracked	Partial
Implemented	MIL 2 (Identified)	Defined	Well defined	Risk-Informed
Managed	MIL 3 (Managed)	Assured	Quantitatively Controlled	Repeatable
Improved		Adaptive	Continuously Improving	Adaptive

Urząd Lotnictwa Cywilnego

DZIĘKUJĘ ZA UWAGĘ

Karol Kaźmierczak

dane kontaktowe

(Naczelnik Inspektoratu CNS, tel. 22 520 72 25, e-mail: kkazmierczak@ulc.gov.pl)

02.09.2025