IS.I.OR.200

System Zarządzania Bezpieczeństwem Informacji (SZBI/ISMS)

Urząd Lotnictwa Cywilnego

02.09.2025

Wprowadzenie

System Zarządzania Bezpieczeństwem Informacji - (I*SMS – Information Security Management System*) według EASA **-** kompleksowe podejście do ochrony informacji i procesów lotniczych. ISMS/SZBI jest kluczowym narzędziem, które umożliwia organizacjom lotniczym identyfikację zagrożeń związanych z bezpieczeństwem informacji, ocenę ryzyka oraz wdrażanie skutecznych mechanizmów kontroli.

W kontekście wymogów EASA, zaleca się, by ISMS/SZBI był zintegrowany z funkcjonującym systemem zarządzania, w tym SMS-em, tworząc spójne ramy zarządzania bezpieczeństwem zarówno na poziomie operacyjnym, jak i informacyjnym.

Zakres ISMS/SZBI według EASA

ISMS w ujęciu EASA wykracza poza ochronę jedynie danych. Obejmuje także zabezpieczenie wszystkich procesów, systemów informatycznych oraz zasobów, które mają bezpośredni lub pośredni wpływ na bezpieczeństwo operacji lotniczych. System ma za zadanie minimalizować ryzyko naruszeń poufności, integralności i dostępności informacji krytycznych dla bezpieczeństwa lotniczego.

Dostosowanie ISMS do kontekstu operacyjnego

EASA podkreśla znaczenie dostosowania ISMS/SZBI do specyfiki i charakteru działalności danego podmiotu lotniczego. Oznacza to, że polityka, procedury oraz środki bezpieczeństwa muszą być projektowane z uwzględnieniem realnych warunków operacyjnych, rodzaju prowadzonej działalności oraz wymagań regulacyjnych.

Etapy i zadania w procesie SZBI/ISMS

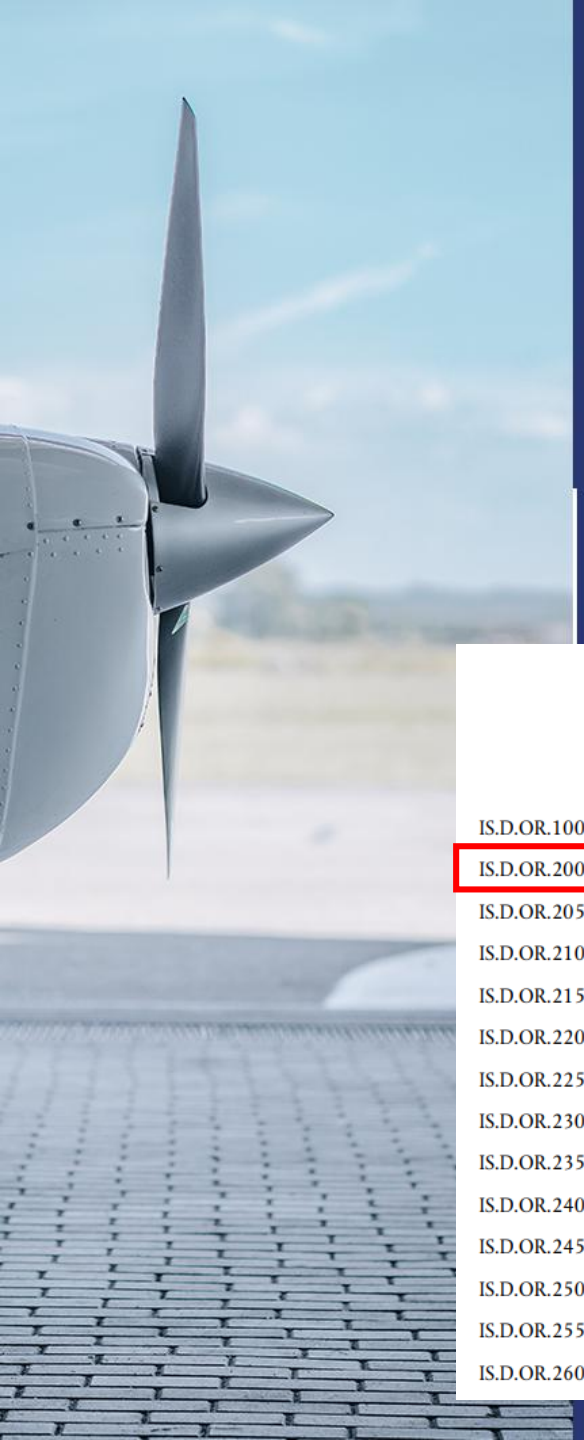
IMPLEMENT

- Define ISMS scope — OR.205
- Appoint responsible persons — OR.240
- Define ISMS policy — OR.200
- Adopt risk management framework — OR.205
- Establish incident management — OR.220
- Establish internal reporting scheme — OR.215
- Establish external reporting scheme — OR.230

OPERATE

- Identify and assess risks — OR.205
- Treat Risks — OR.210
- Detect respond and recover — OR.220
- Manage contracted IS activities and connected risks — OR.205, OR.235

Continuous improvement — OR.260



Co mówi przepis IS.I.OR.200 - Kluczowe elementy

Aby osiągnąć cele określone w Rozp. Delegowanym Komisji (UE) 2022/1645 i Rozp. Wykonawczym Komisji (UE) 2023/203, organizacja ustanawia, wdraża i utrzymuje system zarządzania bezpieczeństwem informacji (ISMS), w ramach którego realizuje poniższe działania:

- Ustanawia strategię/politykę bezpieczeństwa informacji (ang. *policy*) określającą ogólne zasady obowiązujące w danej organizacji w zakresie potencjalnego wpływu ryzyka związanego z bezpieczeństwem informacji na bezpieczeństwo lotnicze;

ZAŁĄCZNIK

BEZPIECZEŃSTWO INFORMACJI – WYMAGANIA DLA ORGANIZACJI

[Część IS.D.OR]

IS.D.OR.100	Zakres stosowania
IS.D.OR.200	System zarządzania bezpieczeństwem informacji
IS.D.OR.205	Ocena ryzyka związanego z bezpieczeństwem informacji
IS.D.OR.210	Zmniejszanie ryzyka związanego z bezpieczeństwem informacji
IS.D.OR.215	System wewnętrznego zgłaszania zdarzeń związanych z bezpieczeństwem informacji
IS.D.OR.220	Incydenty związane z bezpieczeństwem informacji – wykrywanie, reagowanie i działania naprawcze
IS.D.OR.225	Reagowanie na niezgodności, o których powiadomił właściwy organ
IS.D.OR.230	System zewnętrznego zgłaszania zdarzeń związanych z bezpieczeństwem informacji
IS.D.OR.235	Zlecanie czynności w zakresie zarządzania bezpieczeństwem informacji
IS.D.OR.240	Wymagania dotyczące personelu
IS.D.OR.245	Prowadzenie rejestrów
IS.D.OR.250	Podręcznik zarządzania bezpieczeństwem informacji
IS.D.OR.255	Zmiany w systemie zarządzania bezpieczeństwem informacji
IS.D.OR.260	Ciągłe doskonalenie

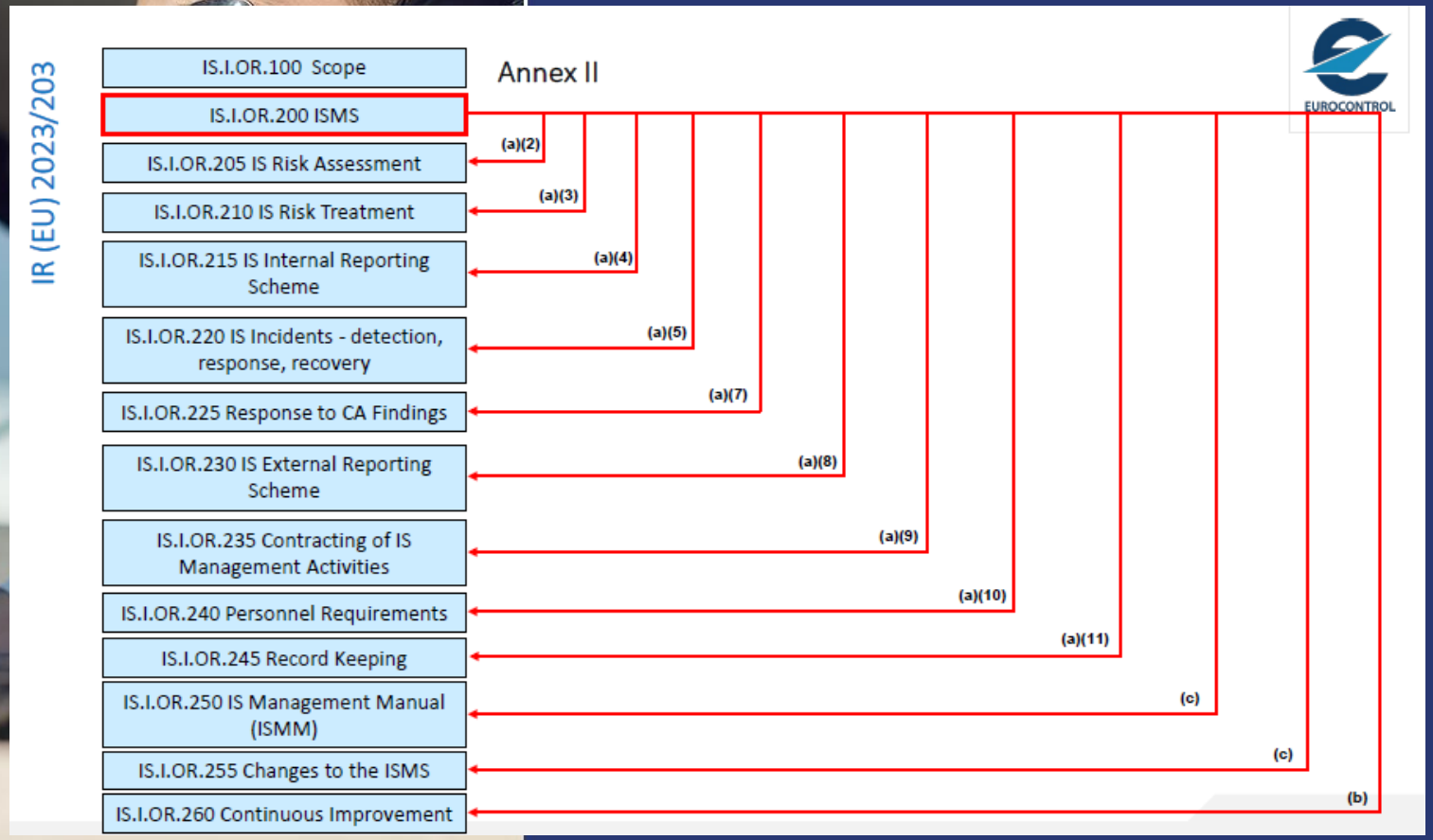
- Identyfikuje ryzyko/ryzyka związane z bezpieczeństwem informacji i dokonuje przeglądu takiego ryzyka zgodnie z pkt IS.I.OR.205;

- Wdraża środki zmniejszające ryzyko związane z bezpieczeństwem informacji zgodnie z pkt IS.I.OR.210;

- Wdraża wewnętrzny system zgłaszania zdarzeń związanych z bezpieczeństwem informacji zgodnie z pkt IS.I.OR.215;

IS.I.OR.200 - Kluczowe elementy

- Definiuje i wdraża, zgodnie z pkt IS.I.OR.220, środki konieczne do wykrywania zdarzeń związanych z bezpieczeństwem informacji, identyfikuje zdarzenia o potencjalnym wpływie na bezpieczeństwo lotnicze oraz reaguje na te incydenty i przywraca system do stanu sprzed takich incydentów;



- Wdraża odpowiednie środki w reakcji na powiadomienie przez właściwy organ, które nastąpiło w ramach natychmiastowej reakcji na incydent związany z bezpieczeństwem informacji lub identyfikację podatności mającej wpływ na bezpieczeństwo lotnicze;

- Podejmuje odpowiednie działania, zgodnie z pkt IS.I.OR.225, w celu wyeliminowania niezgodności stwierdzonych przez właściwy organ;

IS.I.OR.200 System Zarządzania Bezpieczeństwem Informacji (SZBI/ISMS)

- Ustanawia zewnętrzny system zgłaszania zdarzeń zgodnie z pkt IS.I.OR.230, umożliwiający właściwemu organowi podjęcie odpowiednich działań;

- Przestrzega wymagań zawartych w pkt IS.I.OR.235 w przypadku zlecenia jakiejkolwiek czynności, o których mowa w pkt IS.I.OR.200, innym organizacjom;

- Przestrzega wymagań dotyczących personelu, określonych w pkt IS.I.OR.240;

- Przestrzega wymagań dotyczących prowadzenia rejestrów określonych w pkt IS.I.OR.245;

- Monitoruje przestrzeganie przez organizację wymagań określonych w rozporządzeniach dot. Part-IS oraz udziela informacji zwrotnych dotyczących niezgodności kierownikowi odpowiedzialnemu (AM) w celu zapewnienia skutecznego wdrożenia działań naprawczych;

- Chroni, bez uszczerbku dla mających zastosowanie wymagań dotyczących zgłaszania incydentów, poufności wszelkich informacji, które organizacja mogła otrzymać od innych organizacji, zgodnie z poziomem ich wrażliwości.

Aby zapewnić stałe przestrzeganie wymagań organizacja powinna:

- wdrożyć proces ciągłego doskonalenia zgodnie z pkt IS.I.OR.260;

- dokumentować, zgodnie z pkt IS.I.OR.250, wszystkie najważniejsze procesy, procedury, funkcje i obowiązki konieczne do zapewnienia zgodności z pkt IS.I.OR.200 lit. a) oraz ustanowić tryb zmiany tej dokumentacji;

- zarządzać zmianami procesów, procedur, funkcji i obowiązków utworzonych przez organizację w celu zapewnienia zgodności z pkt. IS.I.OR.200 lit. a) odpowiadają charakterowi i złożoności działalności tej organizacji, na podstawie oceny właściwego dla tej działalności ryzyka związanego z bezpieczeństwem informacji, oraz mogą zostać włączone do innych systemów zarządzania już wdrożonych przez tę organizację.

GM3 IS.I.OR.235

Przykłady działań z zakresu zarządzania bezpieczeństwem informacji, które mogą być zlecone

Warunki uzyskania odstępstwa (derogacji)

Właściwy organ może zezwolić organizacji na niewdrożenie wymagań określonych w punktach IS.I.OR.200 lit. a) ppkt 13 oraz IS.I.OR.205–IS.I.OR.260, pod warunkiem że organizacja wykaże, iż jej działalność, obiekty, zasoby oraz świadczone, zapewniane, otrzymywane lub utrzymywane usługi nie generują ryzyka dla bezpieczeństwa informacji, które mogłoby wpłynąć na bezpieczeństwo lotnicze.

Warunkiem uzyskania takiego zezwolenia jest przedłożenie udokumentowanej oceny ryzyka bezpieczeństwa informacji, przeprowadzonej przez organizację lub stronę trzecią zgodnie z pkt. IS.I.OR.205. Ocena ta musi zostać zweryfikowana i zatwierdzona przez właściwy organ.

Niezależnie od przyznanego zezwolenia, organizacja pozostaje zobowiązana do przestrzegania wymagań dotyczących zgłaszania zdarzeń zgodnie z rozporządzeniem (UE) nr 376/2014.

Właściwy organ będzie regularnie weryfikował ważność zezwolenia w ramach nadzoru bieżącego oraz przy każdej zmianie w zakresie działalności organizacji, zapewniając ciągłą zgodność z wymogami bezpieczeństwa.

Part-IS – AMC & GM

Ta tabela przedstawia powiązania między głównymi zadaniami z zakresu bezpieczeństwa informacji (zgodnie z Part-IS – np. IS.I.OR.200), a ich odpowiednimi odniesieniami w ramach standardów:

- **EU e-CF** (*European e-Competence Framework*)
- **NIST CSF 2.0** (*National Institute of Standards and Technology Cybersecurity Framework*)

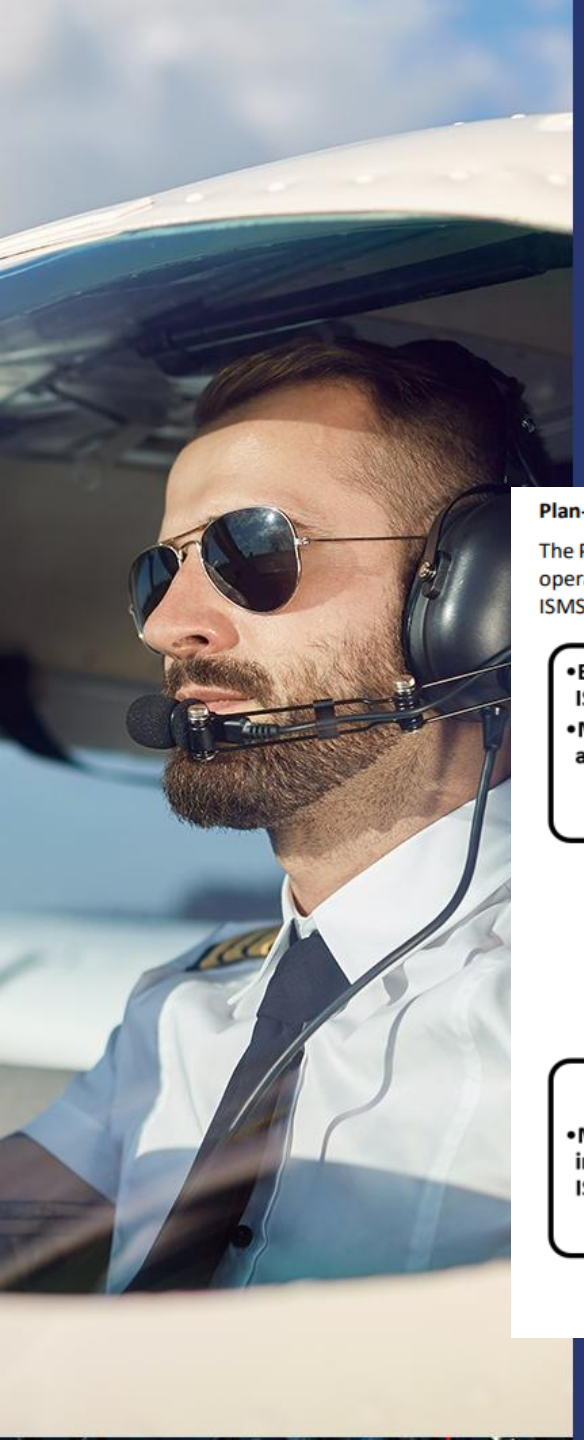
Tabela pochodzi z AMC & GM do części IS.I.OR – wydanie 1, załącznik II (dla IR (UE) 2023/203 załącznik II)

Podobne tabele mapowania znajdują się w: AMC & GM do Part-IS.AR – wydanie 1, załącznik II (dla IR (UE) 2023/203 załącznik I)

& AMC & GM do Part-IS.D.OR – wydanie, załącznik II (dla DR (UE) 2022/1645)

Załącznik II - Tabela zgodności między głównymi zadaniami wymaganymi na mocy Part-IS a EU e-CF oraz NIST CSF

Główne zadanie Part-IS	Rodzaj aktywności	Odniesienie do Part-IS	EU-eCF	NIST CSF 2.0
Ustanowienie i prowadzenie systemu zarządzania bezpieczeństwem informacji (ISMS)	Zarządzanie	IS.I.OR.200(a)	ISM (E.08)	GV.OP – Zarządzanie bezpieczeństwem informacji
Ustalenie zakresu ISMS zgodnie z wymaganiami Part-IS	Zarządzanie	IS.I.OR.205(a)	ISM (E.08)	GV.RM – Zarządzanie ryzykiem
Wdrażanie i utrzymywanie polityki bezpieczeństwa informacji	Zarządzanie	IS.I.OR.200(a)(1)	ISM (E.08)	GV.OP – Zarządzanie bezpieczeństwem informacji
Identyfikacja i przegląd ryzyk bezpieczeństwa informacji	Zarządzanie	IS.I.OR.200(a)(2), IS.I.OR.205	ISM (E.08), Zarządzanie ryzykiem (E.02)	ID.RA – Ocena ryzyka
Wdrażanie środków zarządzania ryzykiem w zakresie bezpieczeństwa informacji	Zarządzanie	IS.I.OR.200(a)(3), IS.I.OR.210	ISM (E.08), Zarządzanie ryzykiem (E.02)	PR.IP – Procesy ochrony informacji
Wdrażanie środków wykrywania incydentów bezpieczeństwa i identyfikacja tych związanych z bezpieczeństwem lotniczym	Zarządzanie	IS.I.OR.200(a)(5), IS.I.OR.220	ISM (E.08), Zarządzanie ryzykiem (E.02)	DE.AE – Anomalie i zdarzenia
Wdrażanie środków wskazanych przez właściwy organ	Operacyjne	IS.I.OR.200(a)(5), IS.I.OR.220	-	-
Podejmowanie odpowiednich działań naprawczych wobec ustaleń zgłoszonych przez organ (niezgodności)	Zarządzanie + Operacyjne	IS.I.OR.200(a)(7), IS.I.OR.225	-	-
Wdrożenie zewnętrznego systemu raportowania incydentów bezpieczeństwa informacji	Zarządzanie	IS.I.OR.200(a)(7), IS.I.OR.225	Zarządzanie incydentami (C.04)	RS.CO – Komunikacja
Monitorowanie zgodności z niniejszym rozporządzeniem i raportowanie do najwyższego kierownictwa	Operacyjne	IS.I.OR.200(a)(7), IS.I.OR.225	Zgodność (E.09)	GV.RM – Zarządzanie ryzykiem



ISMS - Cykl ciągłego doskonalenia

W materiałach doradczych (GM) dotyczących ISMS/SZBI, EASA rekomenduje zastosowanie podejścia opartego na Cyklu Deminga, znanego również pod nazwą PDCA (*Plan-Do-Check-Act*). Ten model stanowi fundamentalny schemat zarządzania, który ilustruje zasadę ciągłego doskonalenia procesów oraz systemów.

Plan-Do-Check-Act approach

The Plan-Do-Check-Act (PDCA) refers to a process approach that is often used to establish, implement, operate, monitor, review and improve management systems. Figure 3 depicts the PDCA applied to an ISMS.

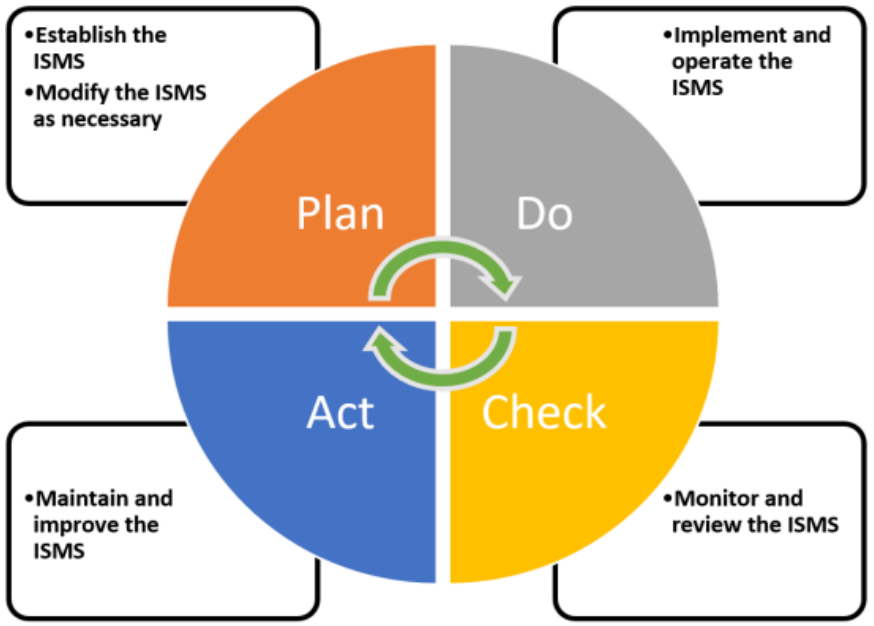


Figure 3: Plan-Do-Check-Act approach applied to an ISMS

GM1.IS.I.0R.200

PLANUJ (*Plan*): Zidentyfikuj obszar do poprawy, przeanalizuj obecne procesy i opracuj szczegółowy plan wprowadzenia nowych, bardziej efektywnych rozwiązań.

WYKONAJ (*Do*): Wprowadź zaplanowane procedury i realizuj przyjęte działania.

SPRAWDŹ (*Check*): Przeprowadź ocenę wyników, porównując dane przed i po zmianach, aby zweryfikować skuteczność nowych metod oraz zidentyfikować ewentualne problemy – monitorowanie, audyty, ocena skuteczności.

POPRAW (*Act*): Jeśli nowy sposób działania przynosi lepsze rezultaty, uznaj go za normę (obowiązującą procedurę), zestandaryzuj i ustal nowe standardy operacyjne do dalszego monitorowania.

From AMC & GM to Part-IS.I.OR – Issue 1

Związek Part-IS z normą ISO/IEC 27001

Międzynarodowa norma ISO/IEC 27001 jest powszechnie stosowaną normą dotyczącą bezpieczeństwa informacji, która określa ogólne wymagania dotyczące ustanowienia, wdrożenia, utrzymania i ciągłego doskonalenia ISMS/SZBI. Obejmuje również wymagania dotyczące oceny i postępowania z ryzykiem związanym z bezpieczeństwem informacji. Wymagania te można zastosować do wszystkich podmiotów, niezależnie od ich rodzaju, wielkości lub charakteru.

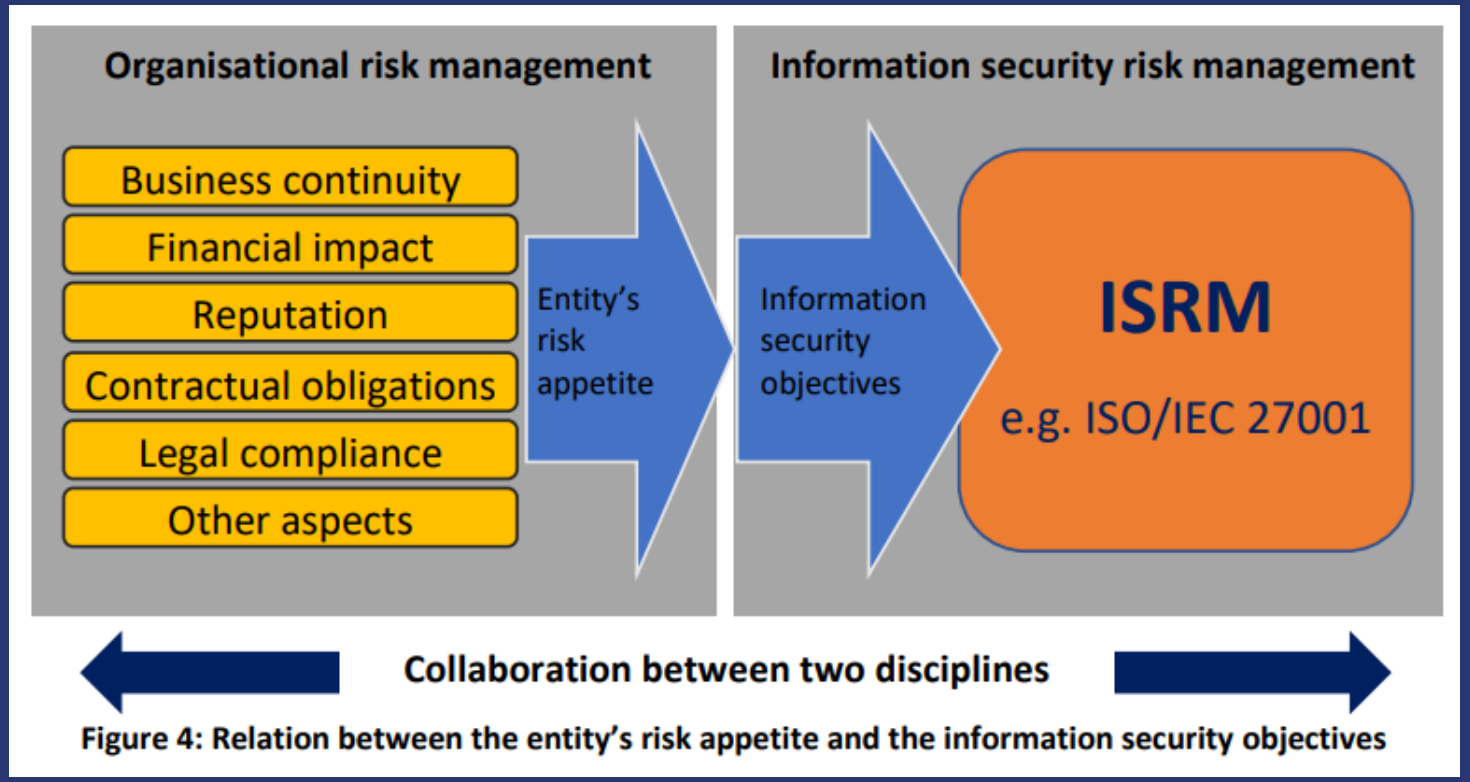


Figure 4: Relation between the entity's risk appetite and the information security objectives

Związek Part-IS z normą ISO/IEC 27001

- Jeśli ISMS/SZBI oparty na normie ISO/IEC 27001 jest już wykorzystywany przez podmiot w innym zakresie i kontekście, można go dostosować i rozszerzyć do zakresu i kontekstu w prosty sposób, w oparciu o analizę zakresu i luk.

- Bezpieczeństwo lotnicze musi być uwzględnione w ramach zarządzania ryzykiem organizacyjnym, a odpowiedni poziom akceptacji ryzyka musi zostać określony przez obowiązujące rozporządzenie.

- Konieczne jest rozróżnienie między ryzykiem związanym z bezpieczeństwem lotniczym a innymi rodzajami ryzyka organizacyjnego w ramach ISMS/SZBI. Może to mieć wpływ na decyzję o integracji ISMS/SZBI (lub jej braku).

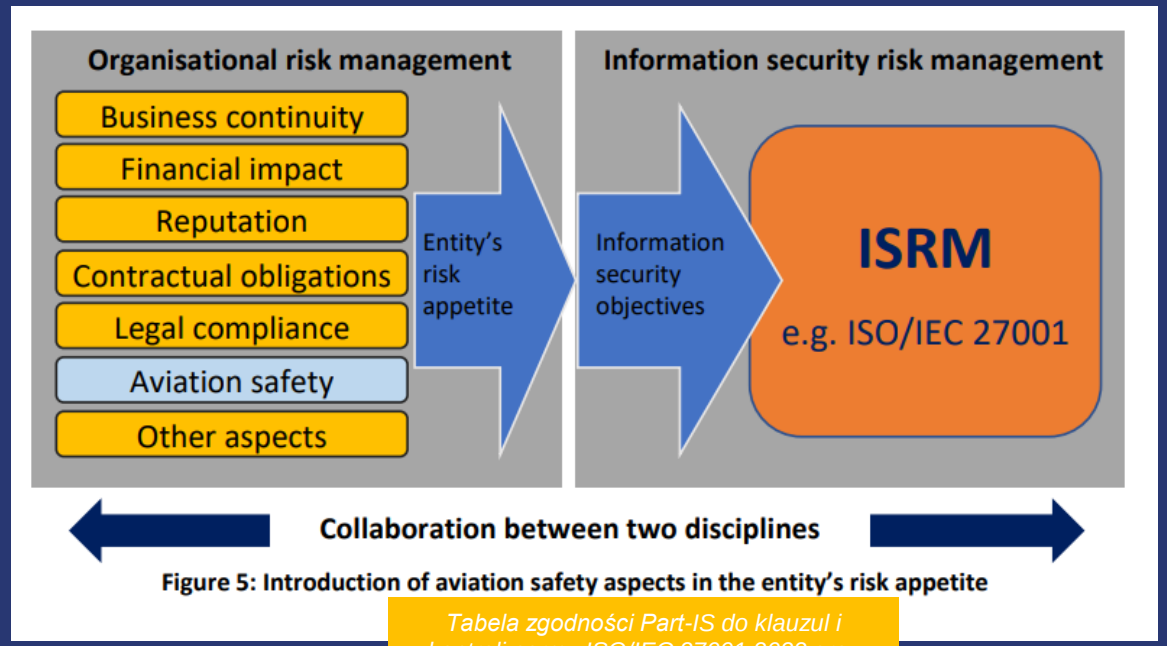


Figure 5: Introduction of aviation safety aspects in the entity's risk appetite

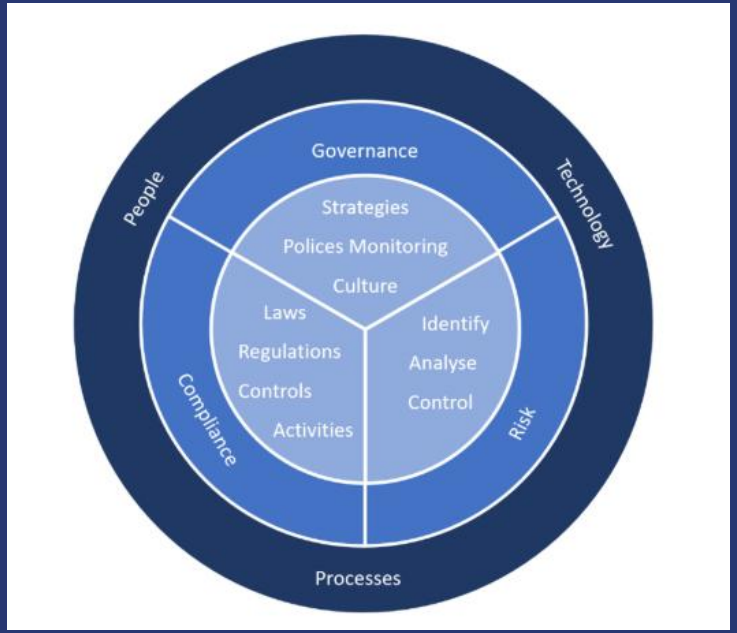
Tabela zgodności Part-IS do klauzul i kontroli normy ISO/IEC 27001:2022 oraz uwagi dotyczące różnic, patrz: Załącznik IV.

Wdrożenie i utrzymywanie ISMS w ramach GRC – kluczowe etapy

Wdrożenie ISMS wymaga ścisłej współpracy z elementami GRC (*Governance, Risk, and Compliance)*, aby zapewnić, że system jest zgodny z celami biznesowymi i regulacjami.

Wdrożenie i utrzymanie ISMS w ramach GRC to proces, który łączy strategiczne zarządzanie (*governance*), ocenę i zarządzanie ryzykiem (*risk management*) oraz zapewnienie zgodności (*compliance*).

- Perspektywa zarządzania koncentruje się na zapewnieniu przywództwa i zaangażowania kierownictwa w realizację celów organizacji.
- Perspektywa ryzyka, odnosi się do kluczowego aspektu ISMS w kontekście bezpieczeństwa lotniczego zgodnie z rozporządzeniem i służy jako podstawa przejrzystego podejmowania decyzji i ustalania priorytetów kontroli i opcji postępowania z ryzykiem.
- Perspektywa zgodności, odnosi się do zgodności z wymogami regulacyjnymi, prawnymi i umownymi.



Governance, Risk, & Compliance (GRC) Framework From Microsoft 365 Maturity Model

Proporcjonalność przy wdrożeniu ISMS

Przy wdrażaniu procesów i procedur oraz określaniu ról i odpowiedzialności wymaganych zgodnie z punktem IS.I.OR.200(d), organizacja powinna przede wszystkim brać pod uwagę ryzyko, jakie może stanowić dla innych organizacji, a także własne ryzyko, na które jest narażona.

Inne aspekty, które mogą być istotne, obejmują potrzeby i cele organizacji, wymagania dotyczące bezpieczeństwa informacji, własne procesy oraz wielkość, złożoność i strukturę organizacji, które mogą zmieniać się w czasie.

Złożoność organizacyjna jest kluczowym czynnikiem, który należy uwzględnić przy definiowaniu ISMS/SZBI.
Na wdrożenie ISM wpływ mają:

- Rola organizacji i interesariuszy, w tym współpracujących działów, poziomów hierarchii, lokalizacji zewnętrznych, spółek zależnych oraz powiązań między podmiotami zewnętrznymi
- Ogólne znaczenie i stopień złożoności organizacji, opisane w załączniku V.

GM1 IS.I.OR.200(d)

Więcej szczegółów na temat wpływu na proporcjonalne wdrożenie części IS w odniesieniu do każdego aspektu istotności bezpieczeństwa i złożoności organizacyjnej podano w Załączniku V.

Korzyści z ISMS

Korzyści z ISMS działającego w dynamicznym, niepewnym lub nieprzewidywalnym środowisku ryzyka są osiągane w perspektywie długoterminowej tylko wtedy, gdy organizacja ulepsza istniejące mechanizmy kontroli, procesy i rozwiązania w oparciu o ocenę ryzyka, wydajności i dojrzałości, a także na podstawie wniosków wyciągniętych z incydentów, audytów, niezgodności i ich przyczyn źródłowych.

Pomyślne wdrożenie i uruchomienie ISMS pozwala podmiotowi na:

- Zwiększenie pewności, że zasoby informacyjne są chronione przed zagrożeniami.
- Zwiększenie wiarygodności i rzetelności kierownictwa oraz zainteresowanych stron.
- Zwiększenie pewności, że ryzyko związane z systemami informatycznymi jest odpowiednio zarządzane
- Zwiększenie odporności całego systemu
- Terminowe wykrywanie słabych punktów

GM1.IS.I.0R.200

- Terminowa reakcja na zmiany:

- w środowisku zagrożeń,
- w architekturze systemu,
- związane z wdrażaniem nowych technologii

- Stanowi podstawę strategii bezpieczeństwa informacji dotyczącej:

- Transformacji cyfrowej
- Zwiększonej wzajemnej łączności systemów
- Pojawiających się nowych zagrożeń
- Wprowadzania nowych technologii

Natalia Najgebaor
Departament Zarządzania Bezpieczeństwem w Lotnictwie Cywilnym
Wydział Analiz Bezpieczeństwa Lotniczego
tel: (+ 48) 22 520 73 78
e-mail: nnajgebaor@ulc.gov.pl