Ocena ryzyka związanego z bezpieczeństwem informacji

(IS.I.OR.205)

Urząd Lotnictwa Cywilnego

08.09.2025

Ocena ryzyka związanego z bezpieczeństwem informacji

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

a) Organizacja identyfikuje wszystkie swoje elementy, które mogą być narażone na ryzyko związane z bezpieczeństwem informacji.

a) REJESTR AKTYWÓW

b) Organizacja powinna zidentyfikować łączące ją z innymi organizacjami interfejsy, które mogą powodować wzajemne narażenie na ryzyko związane z bezpieczeństwem informacji.

b) INTERFEJSY

c) Jeżeli chodzi o elementy i interfejsy, o których mowa w lit. a) i b), organizacja identyfikuje ryzyko związane z bezpieczeństwem informacji, które może mieć potencjalny wpływ na bezpieczeństwo lotnicze.

c) WPŁYW NA SAFETY

d) Organizacja przeprowadza przegląd oceny ryzyka przeprowadzonej zgodnie z lit. a), b) i c) i aktualizuje ją.

d) PRZEGLĄD

e) Na zasadzie odstępstwa od lit. c) organizacje zobowiązane do przestrzegania podczęści C załącznika III (część ATM/ANS.OR) do rozporządzenia wykonawczego (UE) 2017/373 zastępują analizę wpływu na bezpieczeństwo lotnicze analizą wpływu na ich służby zgodnie z dodatkową oceną bezpieczeństwa wymaganą w pkt ATM/ANS.OR.C.005. Ta dodatkowa ocena bezpieczeństwa zostaje udostępniona instytucjom zapewniającym służby ruchu lotniczego, które obsługują, a te instytucje zapewniające służby ruchu lotniczego odpowiadają za ocenę wpływu na bezpieczeństwo lotnicze.

Ocena ryzyka związanego z bezpieczeństwem informacji

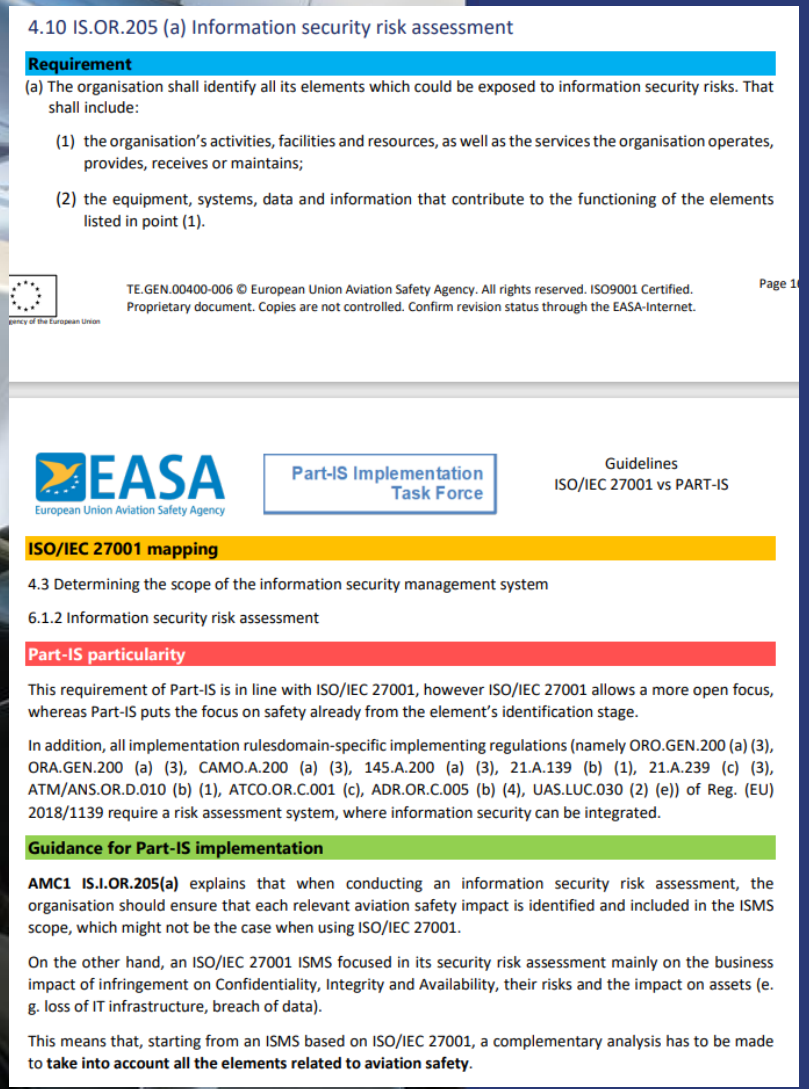
Part-IS nie wymaga stosowania żadnej konkretnej ramowej struktury do wdrożenia wymagań z zakresu bezpieczeństwa informacji.

Najważniejsze, aby system:

- był dostosowany do indywidualnych potrzeb / struktury i rodzaju działalności organizacji,
- spełniał wymogi przepisów,
- uwzględniał specyficzne potrzeby związane z bezpieczeństwem lotniczym.

Ogólne wytyczne dotyczące zarządzania ryzykiem, w tym oceny ryzyka, można znaleźć w normach ISO/IEC 27005 i ISO/IEC 31000, a także w NIST SP 800-30. Organizacje lotnicze mogą również rozważyć wytyczne dotyczące lotnictwa określone w rozdziale dotyczącym zarządzania ryzykiem w najnowszej wersji EUROCAE ED **(GM1 IS.I.OR.205).**

Ocena ryzyka związanego z bezpieczeństwem informacji



4.10 IS.OR.205 (a) Information security risk assessment

Requirement

(a) The organisation shall identify all its elements which could be exposed to information security risks. That shall include:

(1) the organisation's activities, facilities and resources, as well as the services the organisation operates, provides, receives or maintains;

(2) the equipment, systems, data and information that contribute to the functioning of the elements listed in point (1).

EASA European Union Aviation Safety Agency | Part-IS Implementation Task Force | Guidelines ISO/IEC 27001 vs PART-IS

ISO/IEC 27001 mapping

4.3 Determining the scope of the information security management system

6.1.2 Information security risk assessment

Part-IS particularity

This requirement of Part-IS is in line with ISO/IEC 27001, however ISO/IEC 27001 allows a more open focus, whereas Part-IS puts the focus on safety already from the element's identification stage.

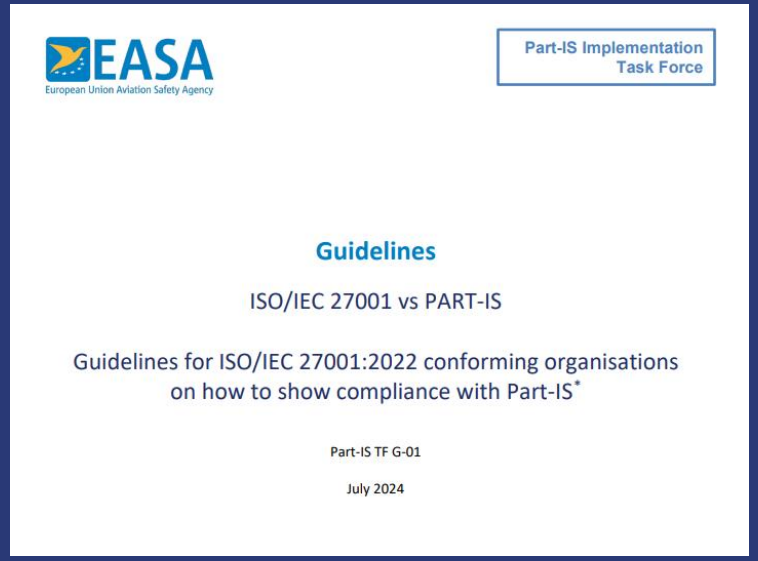
In addition, all implementation rulesdomain-specific implementing regulations (namely ORO.GEN.200 (a) (3), ORA.GEN.200 (a) (3), CAMO.A.200 (a) (3), 145.A.200 (a) (3), 21.A.139 (b) (1), 21.A.239 (c) (3), ATM/ANS.OR.D.010 (b) (1), ATCO.OR.C.001 (c), ADR.OR.C.005 (b) (4), UAS.LUC.030 (2) (e)) of Reg. (EU) 2018/1139 require a risk assessment system, where information security can be integrated.

Guidance for Part-IS implementation

AMC1 IS.I.OR.205(a) explains that when conducting an information security risk assessment, the organisation should ensure that each relevant aviation safety impact is identified and included in the ISMS scope, which might not be the case when using ISO/IEC 27001.

On the other hand, an ISO/IEC 27001 ISMS focused in its security risk assessment mainly on the business impact of infringement on Confidentiality, Integrity and Availability, their risks and the impact on assets (e. g. loss of IT infrastructure, breach of data).

This means that, starting from an ISMS based on ISO/IEC 27001, a complementary analysis has to be made to **take into account all the elements related to aviation safety**.



EASA European Union Aviation Safety Agency

Part-IS Implementation Task Force

Guidelines

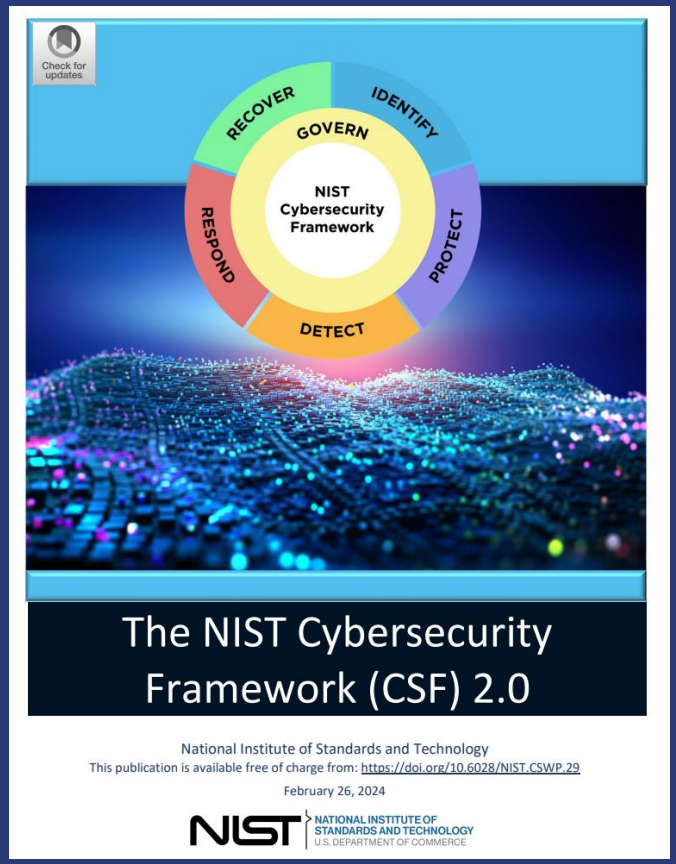
ISO/IEC 27001 vs PART-IS

Guidelines for ISO/IEC 27001:2022 conforming organisations on how to show compliance with Part-IS*

Part-IS TF G-01

July 2024

https://www.easa.europa.eu/community/sites/default/files/2024-07/Guidelines%20-%20ISO%2027001%20add-on.pdf



The NIST Cybersecurity Framework (CSF) 2.0

National Institute of Standards and Technology
This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.29
February 26, 2024

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

08.09.2025

Ocena ryzyka związanego z bezpieczeństwem informacji

AMC1 IS.I.OR.205(a) & AMC1 IS.D.OR.205(a) **a) REJESTR AKTYWÓW**

Organizacja identyfikuje wszystkie swoje elementy, które mogą być narażone na ryzyko związane z bezpieczeństwem informacji. Elementy te obejmują:

1) działalność, obiekty i zasoby organizacji, a także służby, które ta organizacja obsługuje, zapewnia, otrzymuje lub utrzymuje;

2) wyposażenie, układy, dane i informacje, które przyczyniają się do funkcjonowania elementów wymienionych w pkt 1.

Sposobem na spełnienie wymogu określonego w pkt IS.I.OR.205 lit. a) jest przeprowadzenie wstępnej oceny ryzyka **wysokiego poziomu** lub oceny skutków, przeprowadzonej zgodnie z udokumentowaną metodologią i zgodnie z precyzyjnymi kryteriami włączenia do zakresu SZIB / ISMS i wyłączenia z niego elementów wymienionych w IS.I.OR.205 lit. a).

Ocena ryzyka związanego z bezpieczeństwem informacji

GM1 IS.I.OR.205(a)

OKREŚLENIE ZAKRESU I GRANIC

Organizacja powinna opracować jasne kryteria dla swoich działań i usług lotniczych, powiązanych procesów i systemów informatycznych oraz odpowiednich przepływów danych i wymiany informacji, które określają zakres ISMS i granice oceny ryzyka.

Jasne i pełne zrozumienie swojej działalności lotniczej i świadczonych usług

Organizacje powinny:

- opracować odpowiednią dokumentację dotyczącą zasobów i zależności między nimi;
- określić, które mogą mieć wpływ na bezpieczeństwo informacji i bezpieczeństwo lotnicze (Safety);
- określić granice oceny ryzyka
- określić zakres oceny ryzyka

Ocena ryzyka związanego z bezpieczeństwem informacji

a) REJESTR AKTYWÓW

(a) Określenie operacyjnych danych wejściowych i wyjściowych istotnych dla funkcji, usług i zdolności organizacji; mogą one dotyczyć: — źródeł wewnętrznych lub zewnętrznych; — wewnętrznych lub zewnętrznych usług wynajmowanych lub zarządzanych, bądź innych zależności;

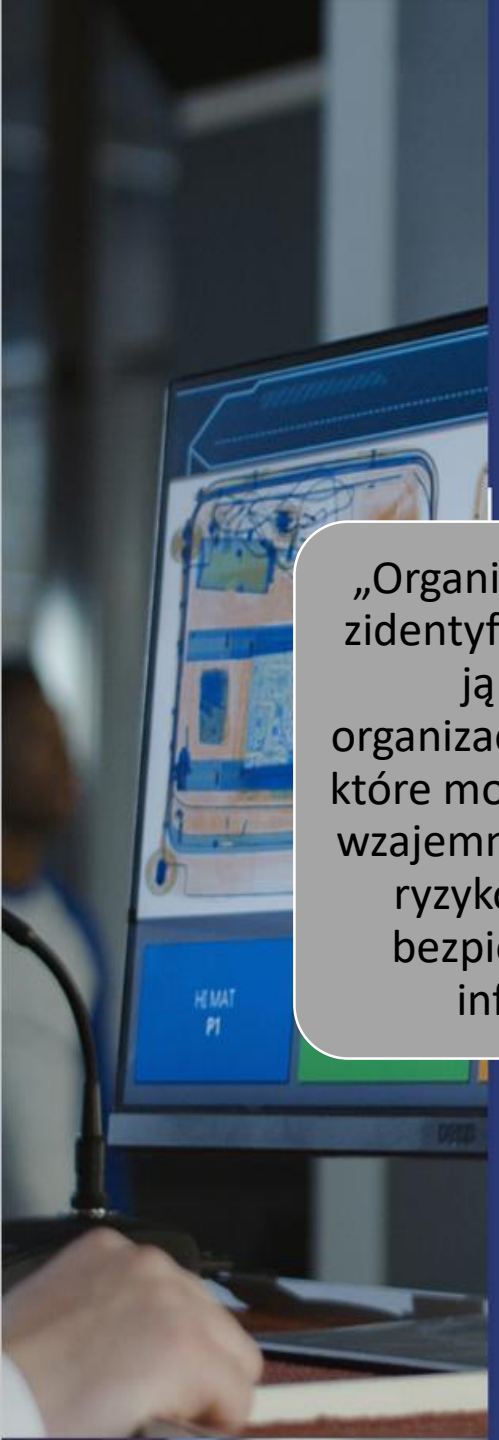
(b) Identyfikacja wszystkich istotnych aktywów (tj. sprzętu, oprogramowania, zasobów sieciowych i obliczeniowych) wykorzystywanych do tworzenia, przetwarzania, przesyłania, przechowywania lub odbioru wspomnianych operacyjnych danych wejściowych i wyjściowych;

(c) Określenie środowisk operacyjnych (np. biuro, obszar publicznego dostępu, pomieszczenie z kontrolowanym dostępem itp.) oraz lokalizacji dla wszystkich istotnych aktywów;

(d) Dla każdego aktywu objętego zakresem, określenie konkretnych metod, procesów i zasobów, które będą wykorzystywane do zarządzania, eksploatacji i utrzymania każdego aktywu przez cały jego cykl życia, w tym: — zasoby wewnętrzne lub kontraktowe; — firmy kontraktowe zdalnie zarządzające aktywami (tj. dostawcy usług zarządzanych).

Ocena ryzyka związanego z bezpieczeństwem informacji

b) INTERFEJSY AMC1 IS.I.OR.205(b) & AMC1 IS.D.OR.205(b)



„Organizacja powinna zidentyfikować łączące ją z innymi organizacjami interfejsy, które mogą powodować wzajemne narażenie na ryzyko związane z bezpieczeństwem informacji”

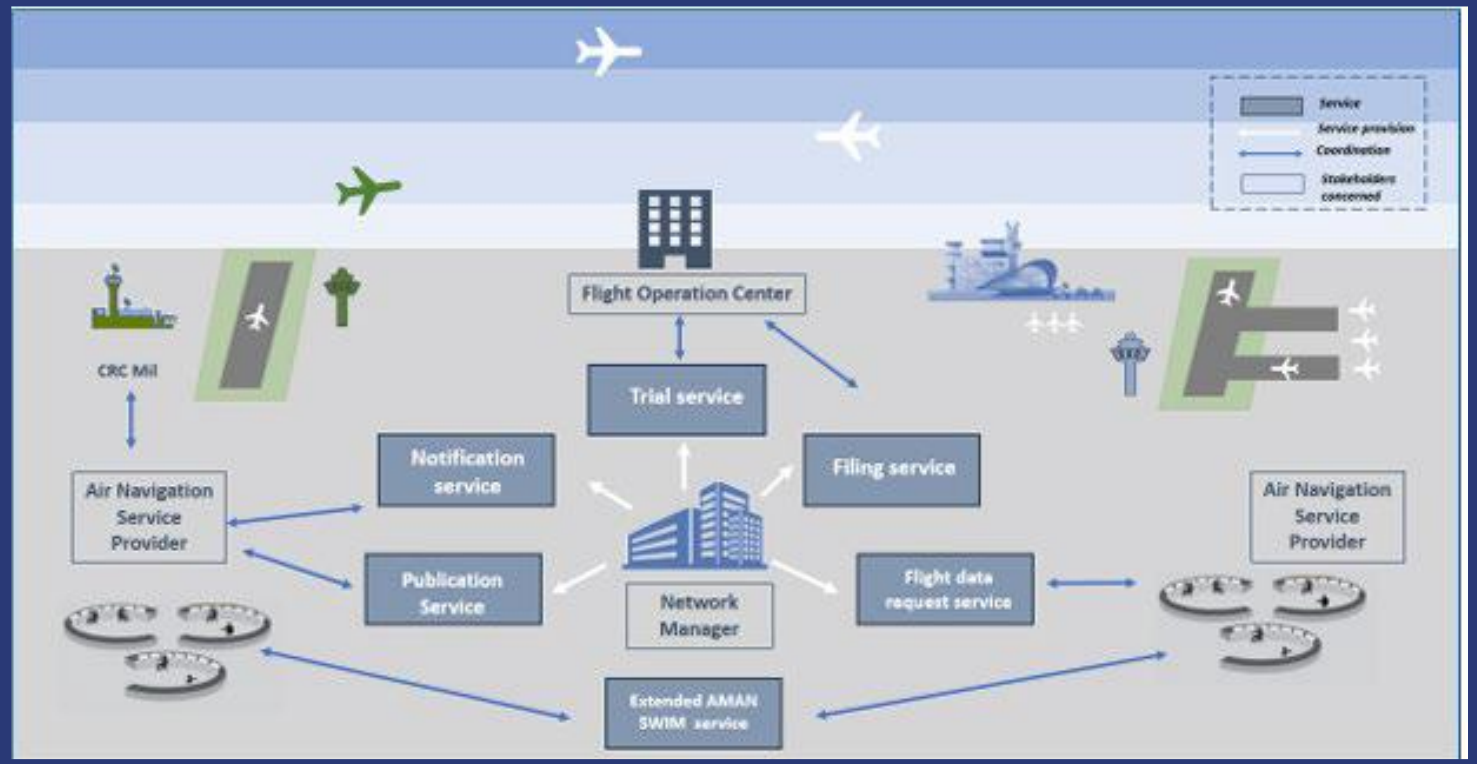
Strony, takie jak dostawcy usług, kontrahenci w łańcuchu dostaw i inne strony trzecie

Zwiększone ryzyko związane z bezpieczeństwem lotniczym dla innych stron i organizacji!

„wzajemne narażenie na ryzyko”

Ocena ryzyka związanego z bezpieczeństwem informacji

https://www.eurocontrol.int



Należy jasno określić wszystkie aktywa / zasoby
Należy określić wszystkie funkcje, działania i procesy tworzące tzw. łańcuchy funkcjonalne

Jedna strona współpracująca pełni rolę inicjatora lub odbiorcy

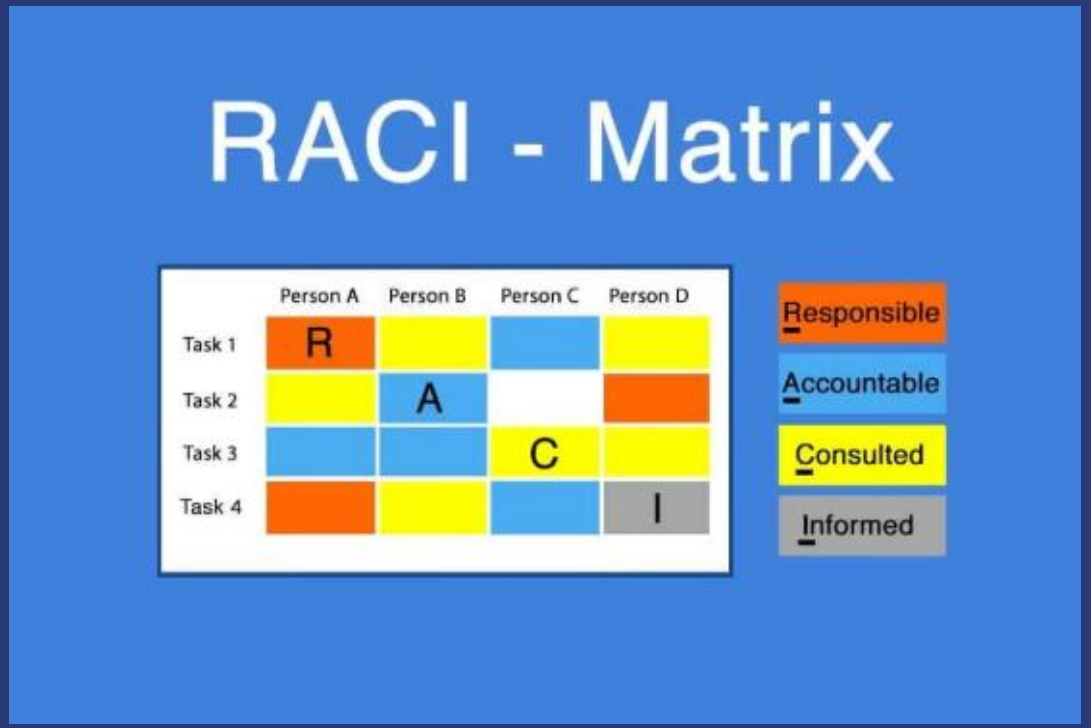
Ocena ryzyka związanego z bezpieczeństwem informacji

GM1 IS.I.OR.205(b) & GM1 IS.D.OR.205(b)

EUROCAE ED-201A

Appendix B
B.1 External Agreement Template
B.2 External Agreement Template - contractual
B.3 SRA sharing Template

Appendix C
C.1 Example for case study
C.2 Example RASCI



https://t2informatik.de/en/smartpedia/raci-matrix/

RASCI: Responsible, Accountable, Support, Consulted, Informed
RACI-VS: Responsible, Accountable, Consulted, Informed, Verify, Signatory

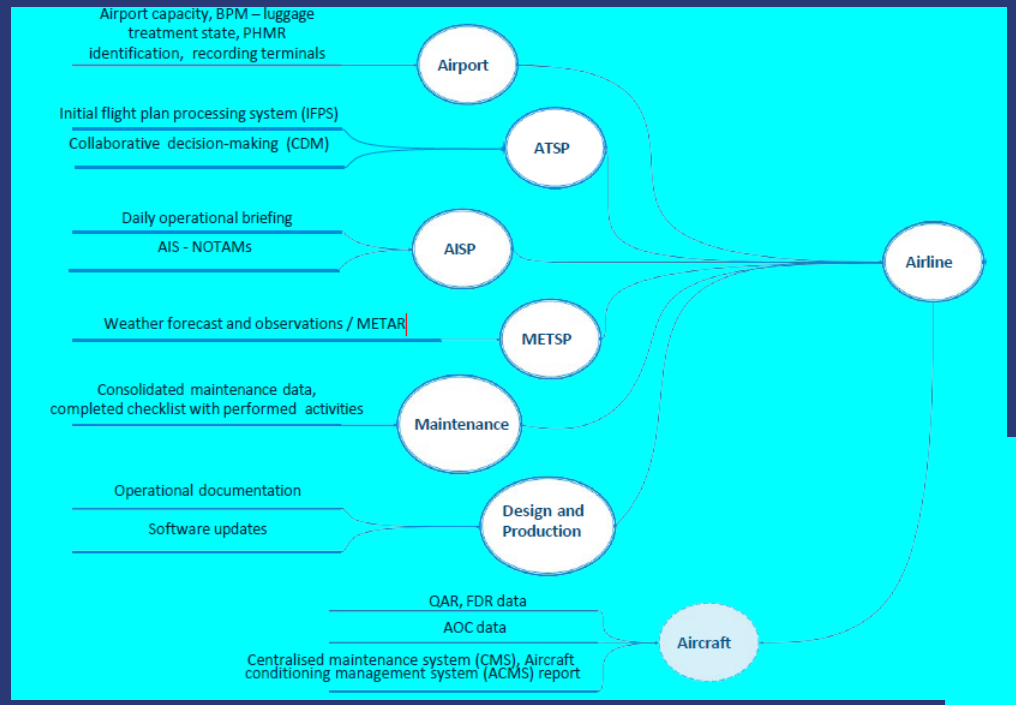
Ocena ryzyka związanego z bezpieczeństwem informacji

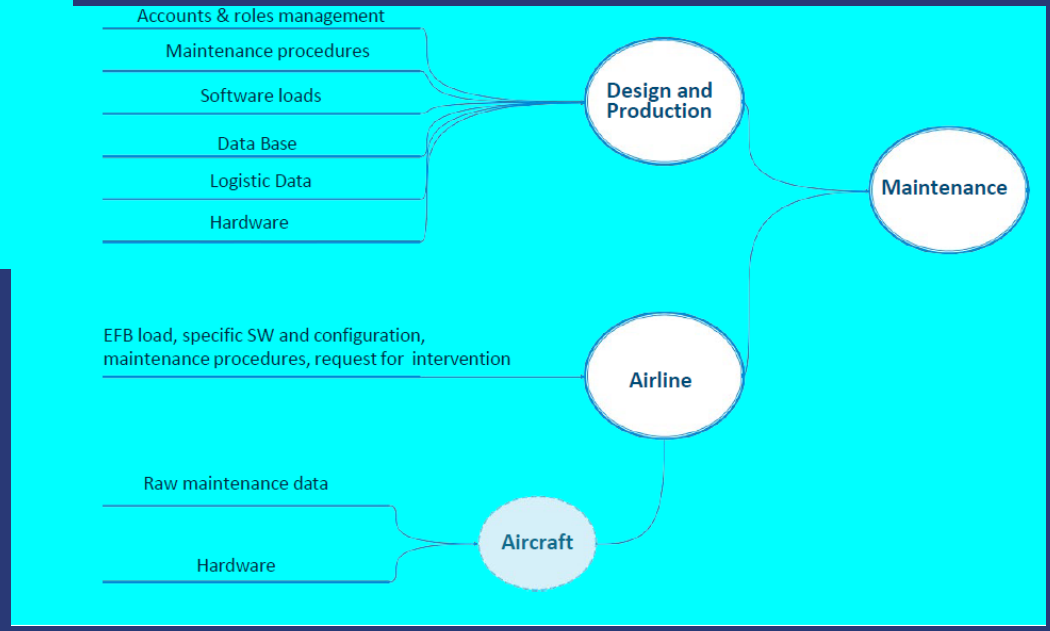
GM1 IS.I.OR.205(b) & GM1 IS.D.OR.205(b) Załącznik III
Przykłady usług lotniczych i interfejsów

- aerodrome & ATM-MET service providers
- aeronautical digital mapping services
- aeronautical information management (AIM) – external, national, regional
- airports
- air traffic control (ATC) – external, superior
- air traffic management (ATM)
- approach (APP) & area control (ACC) Services – ER ACC, APP ACC
- cargo and passenger loading
- civil & state airspace user (AU) operations centres
- communication infrastructure
- flight information & traffic information services (FIS/TIS) data integrator
- fuel calculation
- navigation infrastructure – ground-based, satellite-based
- non-ATM meteorological (MET) service providers
- mass & balance calculation
- non-aviation users (external)
- regional & sub-regional airspace management (ASM) and air traffic flow & capacity management (ATFCM)
- static aeronautical data services
- sub-regional demand & capacity balancing (DCB) common service providers
- surveillance infrastructure –airport, en-route, terminal manoeuvringarea (TMA)
- route planning
- time reference services (external)
- tower (TWR) services

Ocena ryzyka związanego z bezpieczeństwem informacji

Przykłady „ecosystem data exchange” w EUROCAE ED-201A





Ocena ryzyka związanego z bezpieczeństwem informacji

AMC1 IS.I.OR.205(c) & AMC1 IS.D.OR.205(c) **c) WPŁYW NA SAFETY**

Określono ZAKRES I GRANICE (elementy/aktywa)
Określono INTERFEJSY i WYMIANĘ INFORMACJI o ryzyku

Organizacja identyfikuje ryzyko związane z bezpieczeństwem informacji, które może mieć potencjalny wpływ na bezpieczeństwo lotnicze.

https://aspectmr.com/flawed-research-methodology/

RISK ASSESSMENT

Ocena ryzyka związanego z bezpieczeństwem informacji

GM1 IS.D.OR.205(c)

Kompleksowa struktura zarządzania ryzykiem zazwyczaj obejmuje następujące aspekty i procesy:

- powtarzalną i odtwarzalną (udokumentowaną) ocenę ryzyka;
- dokładny przegląd ryzyk, które mają być warunkowo akceptowalne, przeprowadzany przez osobę (osoby) upoważnioną (upoważnione);
- środki / działania zaradcze ograniczające / obniżające poziom ryzyka i harmonogram ich wdrożenia;
- ścisłe monitorowanie kluczowych wskaźników ryzyka;
- istnienie planu reagowania na incydenty, obejmującego środki reaktywne uruchamiane przez mechanizmy wykrywania incydentów w celu natychmiastowego ograniczenia skutków, w szczególności w przypadku scenariuszy ryzyka o wysokim poziomie dotkliwości.

Ocena ryzyka związanego z bezpieczeństwem informacji

GM1 IS.D.OR.205(c)

Organizacja powinna określić i udokumentować stosowane, specyficzne dla organizacji poziomy klasyfikacji ryzyka – przyjętą metodologię oceny ryzyka.

Np. EUROCAE ED-203A i EUROCAE ED-202A, które zostały pierwotnie opracowane na potrzeby oceny ryzyka związanego z bezpieczeństwem informacji w lotnictwie, ale ogólne zasady zawarte w tych dokumentach mogą zostać dostosowane do innych ram, jeśli organizacja uzna to za przydatne.

Organizacje powinny klasyfikować ryzyko wystąpienia scenariuszy zagrożeń na wysokie, średnie lub niskie na podstawie prawdopodobieństwa, wykonalności i historycznych danych, zgodnie z EUROCAE ED-203A. Ocena obejmuje aspekty ochrony (np. zabezpieczenia, wykrywanie ataków), redukcji ekspozycji (np. ograniczenia dostępu, zarządzanie podatnościami) oraz zdolności atakujących. Skutki dla bezpieczeństwa dzieli się na wysoką, średnią i niską dotkliwość, w zależności od wpływu na operacje lotnicze. Ryzyko klasyfikuje się jako niedopuszczalne, warunkowo dopuszczalne lub dopuszczalne, przy czym warunkowa akceptacja wymaga planu redukcji ryzyka i solidnego systemu zarządzania ryzykiem. Szczegółowe wytyczne znajdują się w EUROCAE ED-201A

Ocena ryzyka związanego z bezpieczeństwem informacji

GM1 IS.D.OR.205(c)

Kryteria akceptacji ryzyka

- są kluczowe i powinny być opracowane, określone oraz udokumentowane;
- mogą definiować różne progi, z pożądanym docelowym poziomem ryzyka, ale także umożliwiać osobom upoważnionym, akceptację ryzyka powyżej tego poziomu w określonych okolicznościach i warunkach;
- powinny uwzględniać czas trwania ryzyka (tymczasowe lub krótkotrwałe narażenie).

Macierz akceptacji ryzyka (ICAO, Zał. 13)

ICAO Annex 13 >	Negligible effect	Incident	Accident
Threat scenario — potential of occurrence	**Low safety consequences**	**Moderate safety consequences**	**High safety consequences**
High	Conditionally acceptable	**Not acceptable**	**Not acceptable**
Medium	Acceptable	Conditionally acceptable	**Not acceptable**
Low	Acceptable	Acceptable	Conditionally acceptable*

Aby ułatwić wzajemną porównywalność ocen ryzyka między współpracującymi podmiotami, organizacja powinna klasyfikować ryzyko w następujących kategoriach:

— Ryzyko nieakceptowalne;
— Ryzyko warunkowo akceptowalne;
— Ryzyko akceptowalne.

Ocena ryzyka związanego z bezpieczeństwem informacji

GM1 IS.D.OR.205(c)

Ryzyko powinno być warunkowo akceptowane tylko w przypadku, gdy organizacja wykaże istnienie kompleksowej struktury zarządzania ryzykiem, która obejmuje procesy oceny ryzyka, ograniczania ryzyka i monitorowania ryzyka.

Zarządzanie ryzykiem powinno uwzględniać zmienność prawdopodobieństwa zagrożeń, podatności, istniejących zabezpieczeń, zależności zewnętrznych oraz wpływu na bezpieczeństwo lotnicze.

ED-203A:
Airworthiness Risk Acceptability Matrix

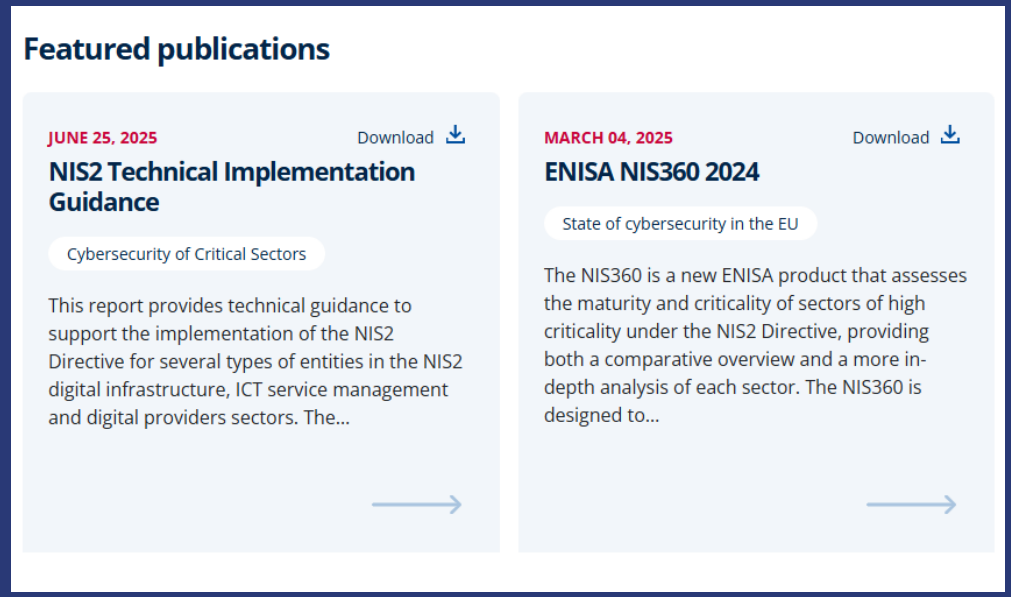
	Severity of the Threat Condition Effect				
Level of Threat	No Safety Effect	Minor	Major	Hazardous	Catastrophic
Very High	Acceptable	Acceptable	Unacceptable	Unacceptable	Unacceptable
High	Acceptable	Acceptable	Unacceptable	Unacceptable	Unacceptable
Moderate	Acceptable	Acceptable	Acceptable	Unacceptable	Unacceptable
Low	Acceptable	Acceptable	Acceptable	Acceptable	Unacceptable
Extremely Low	Acceptable	Acceptable	Acceptable	Acceptable	Acceptable*

ED-203A section 3.6

1. Protection Criteria section 3.6.2.1
2. Exposure Reduction Criteria section 3.6.2.2
3. Attack Attempt Criteria section 3.6.2.3
4. Risk Acceptance Criteria ED-203A section 2.7.2.3

Ocena ryzyka związanego z bezpieczeństwem informacji

Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA)



https://securitydelta.nl/media/com_hsd/report/690/document/ENISA-Threat-Landscape-2024.pdf

https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-union-agency-cybersecurity-enisa_pl

Ocena ryzyka związanego z bezpieczeństwem informacji

GM1 IS.D.OR.205(c) / Guidelines ISO/IEC 27001 vs PART-IS

Wytyczne dla organizacji, które są zobowiązane do stosowania SMS, w tym zarządzania ryzykiem bezpieczeństwa

W większości przypadków, gdy organizacja podlega szczegółowym przepisom wykonawczym dotyczącym SMS i stosuje ISMS (SZBI) w ramach dobrowolnej zgodności z normą ISO/IEC 27001, może ona stosować dwa systemy zarządzania ryzykiem, jeden dotyczący bezpieczeństwa pod nadzorem właściwego organu, a drugi dotyczący bezpieczeństwa informacji certyfikowany przez jednostkę akredytowaną zgodnie z normą ISO/IEC 27001.

SMS **ISMS/SZBI**

Każde potencjalne ryzyko zidentyfikowane przez ISMS powinno być systematycznie oceniane pod kątem jego potencjalnego wpływu na bezpieczeństwo (w ramach SMS).

Ocena ryzyka związanego z bezpieczeństwem informacji

GM1 IS.D.OR.205(c) / Guidelines ISO/IEC 27001 vs PART-IS

Ocena ryzyka bezpieczeństwa informacji powinna być w stanie dostarczyć kontekst i docelowe wartości prawdopodobieństwa dla akceptowalnych ryzyk ISMS. Kontekst obejmuje architekturę systemu, w tym bariery zapobiegawcze i łagodzące, ocenione zagrożenia oraz zidentyfikowane ryzyka bezpieczeństwa informacji, na podstawie których można przeprowadzić ocenę ryzyka bezpieczeństwa informacji.

Modyfikacje architektury systemu lub wszelkie modyfikacje właściwości barier zapobiegawczych lub łagodzących, a także osiągnięte wartości ryzyka bezpieczeństwa informacji muszą zostać uwzględnione w ramach ponownego procesu oceny ryzyka bezpieczeństwa lotniczego (Safety).

Na podstawie ww. informacji należy zaktualizować ocenę ryzyka bezpieczeństwa lotniczego czyli środki łagodzące wprowadzone w wyniku oceny ryzyka bezpieczeństwa informacji również powinny zostać uwzględnione w ramach SMS-a, ponieważ mogą one nie tylko łagodzić ryzyko, ale także potencjalnie wywierać negatywny wpływ na bezpieczeństwo.

Ocena ryzyka związanego z bezpieczeństwem informacji

GM1 IS.D.OR.205(c) / Guidelines ISO/IEC 27001 vs PART-IS

Jeżeli proces oceny bezpieczeństwa informacji identyfikuje nowe zagrożenie, które nie było wcześniej znane w ocenie ryzyka bezpieczeństwa lotniczego, należy przeprowadzić pełną ocenę zagrożeń wszystkich aspektów bezpieczeństwa, aby zapewnić, że ocena ryzyka bezpieczeństwa w ramach SMS zawiera „pełny obraz” nowo zidentyfikowanego zagrożenia.

Cykl wzajemnie oddziałujących ocen ryzyka bezpieczeństwa lotniczego i ryzyka bezpieczeństwa informacji należy powtarzać do momentu spełnienia wszystkich wymagań dotyczących akceptowalności wszystkich elementów.

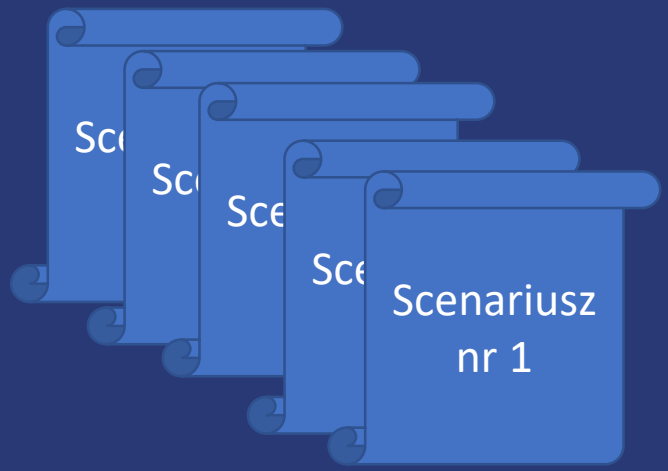
Ocena ryzyka związanego z bezpieczeństwem informacji

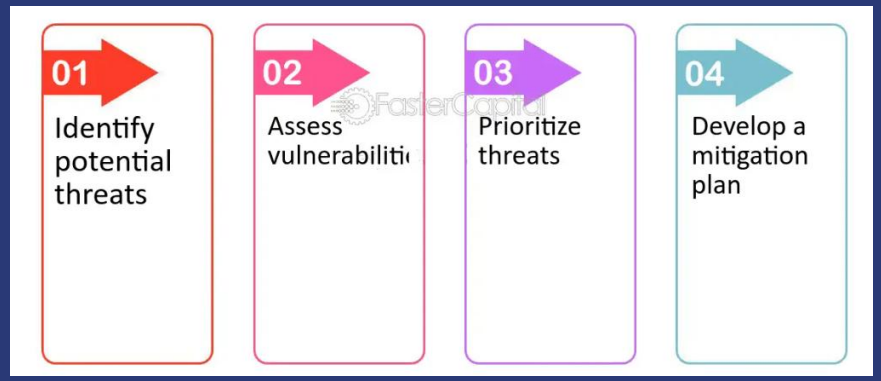
GM1 IS.D.OR.205(c)

SCENARIUSZE ZAGROŻEŃ

Scenariusz zagrożenia to jeden z możliwych sposobów, w jaki zagrożenie może się zmaterializować. Zazwyczaj scenariusz zagrożenia opisuje potencjalny atak wymierzony w jedną lub więcej słabych stron (podatności) zasobów i /lub procesów.

Celem identyfikacji scenariuszy zagrożeń na mocy wymagań Part-IS jest opracowanie listy scenariuszy , które mogą prowadzić do zagrożenia bezpieczeństwa informacji mającego wpływ na bezpieczeństwo lotnicze.



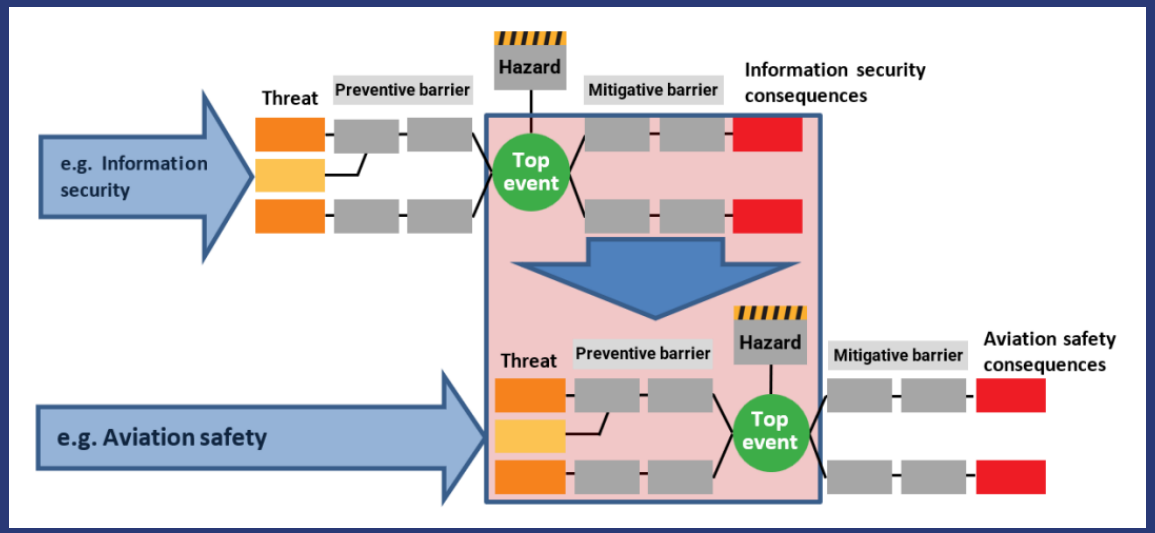


https://fastercapital.com/content/Juniorsecurity-Threat-Modeling--Anticipating-Potential-Risks.html

Ocena ryzyka związanego z bezpieczeństwem informacji

Scenariusz zagrożenia zazwyczaj zawiera:

- źródło zagrożenia / ataku na bezpieczeństwo informacji;
- wektor ataku i ścieżka przez organizację do konkretnego zasobu / elementu;
- środki kontroli bezpieczeństwa informacji, które mogłyby złagodzić skutki ataku;
- konsekwencje ataku, w tym aspekty bezpieczeństwa lotniczego, na które ma on wpływ.



Interakcje między bezpieczeństwem informacji a bezpieczeństwem lotniczym przedstawione za pomocą diagramu „bow-tie", który podkreśla powiązania między kontrolą ryzyka a podstawowym systemem zarządzania.

Ocena ryzyka związanego z bezpieczeństwem informacji

Appendix I — Examples of threat scenarios with a potential harmful impact on safety

ED Decision 2023/010/R

Example 1: Aircraft to ATC digital communications

- **Threat vector assets/domain**
  - ATC voice and ground automation systems
  - ground communications providers
  - air-ground/ground-air RF communications service providers
  - aircraft and the assets used for voice and datalink communications
- **Non-exhaustive summary of potential threats**
  - threat (availability): exceeding system performance, saturation of communication channel
  - threat (integrity): man-in-the-middle or injection attacks
  - threat (confidentiality): passive listening to communication, spying on hardware device
- **Summary of threats scenarios and their potential harmful impacts on safety**
  - Disruption of services prevents ATC communication with a single or multiple aircraft and/or ATC ground system.
  - Manipulation of data through a man-in-the-middle attack would present false information to the pilot and/or ATC system with the potential of creating a safety hazard or injection of data to the aircraft or ground systems to disrupt the service and capability.
  - There are no specific regulatory requirements for encryption of data or voice for datalink communications; however, for confidentiality purposes, the assets used to provide and deliver the services should be controlled and limited to only those resources that require access to ensure that the services cannot be disrupted and manipulated in any way.

Example 8: Aviation authority's airworthiness directive (AD) system and associated infrastructure

- **Threat vector assets/domain**
  - EASA AD system infrastructure and digital interface
  - supply chain for AD system maintenance and updates
  - EASA IT assets used for AD creation, distribution, and storage
- **Non-exhaustive summary of potential threats**
  - threat (availability): Disruption of the AD system or its access
  - threat (integrity): tampering with AD data or unauthorised AD creation
  - threat (confidentiality): unauthorised access to AD data
- **Summary of threats and their potential harmful impacts on safety**
  - Disruption to the AD system could prevent the dissemination of critical airworthiness information to aircraft operators and maintenance organisations, potentially leading to safety issues.
  - Tampering with AD data or unauthorised creation of ADs could lead to incorrect information being disseminated, potentially resulting in aircraft operators and maintenance organisations making decisions based on false or misleading data.
  - Unauthorised access to AD data could lead to information leakage, potentially revealing sensitive operational information.

Ocena ryzyka związanego z bezpieczeństwem informacji

d) PRZEGLĄD

Organizacja przeprowadza przegląd oceny ryzyka przeprowadzonej zgodnie z lit. a), b) i c) i aktualizuje ją we wszystkich następujących sytuacjach:

1) w przypadku zmiany elementów narażonych na ryzyko związane z bezpieczeństwem informacji;

2) w przypadku zmiany interfejsów między organizacją a innymi organizacjami lub ryzyka, o którym poinformowały pozostałe organizacje;

3) w przypadku zmiany informacji lub wiedzy wykorzystywanych do identyfikacji, analizy i klasyfikacji ryzyka;

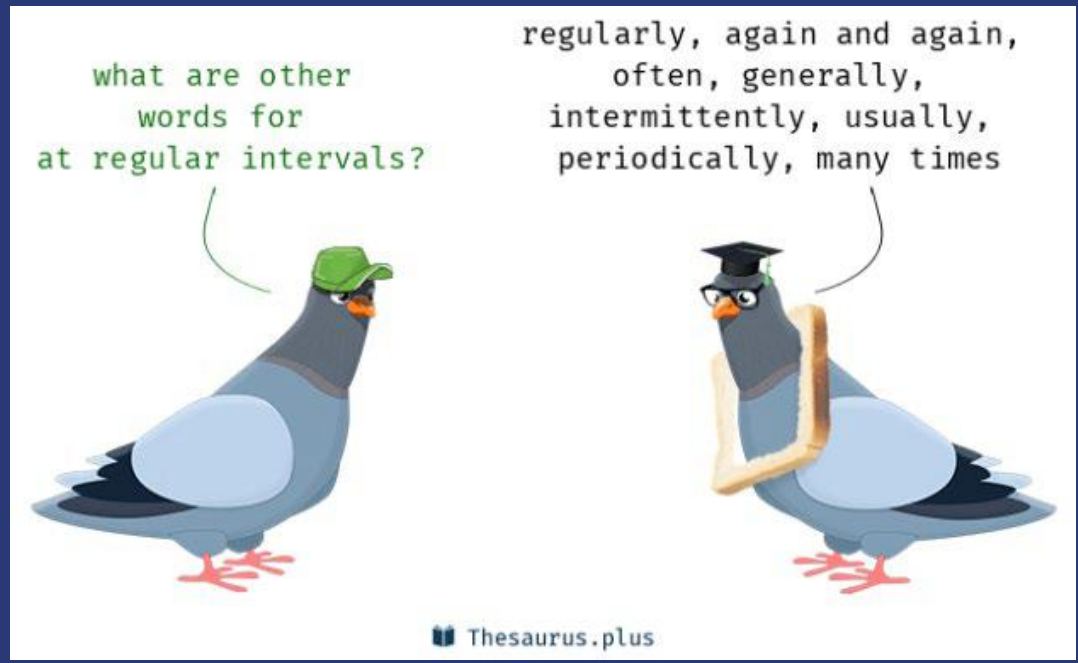
4) gdy dostępne są wnioski z analizy incydentów związanych z bezpieczeństwem informacji.

Ocena ryzyka związanego z bezpieczeństwem informacji

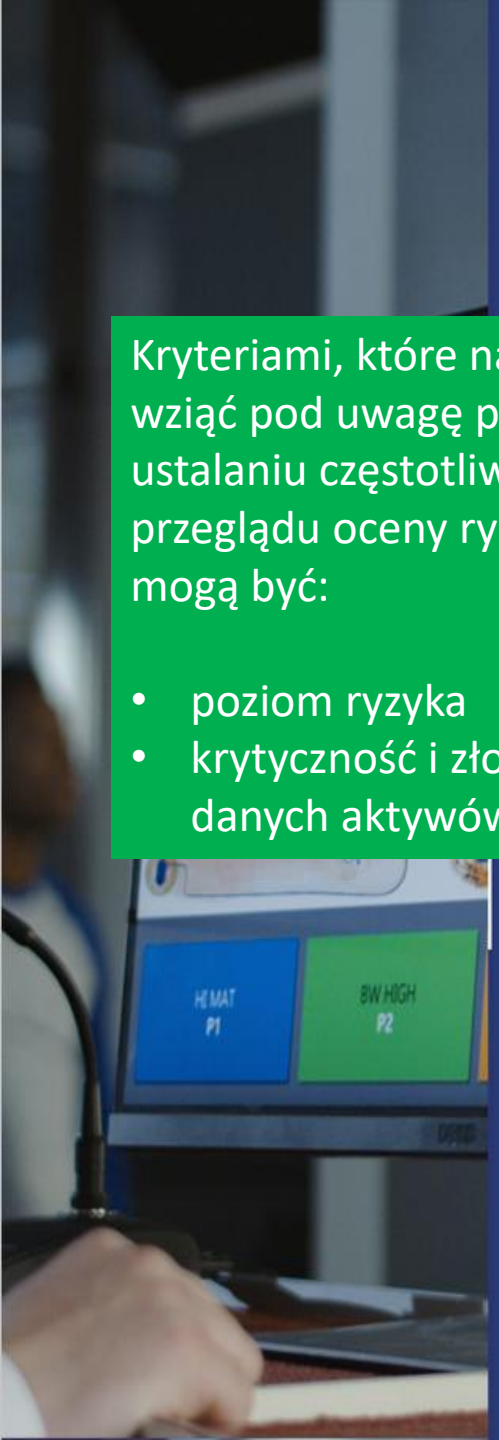
GM1 IS.D.OR.205(d) / Guidelines ISO/IEC 27001 vs PART-IS

Ten sam proces, który jest już stosowany w kontekście normy ISO/IEC 27001, może być wykorzystany do wdrożenia IS.OR.205 (d), pod warunkiem że proces ten został zaktualizowany w celu uwzględnienia oceny kryteriów dla zmian, które powodują nieplanowaną aktualizację oceny ryzyka.

Organizacje będą musiały wykazać się proaktywnością, aby częściej inicjować aktualizacje w sytuacjach wymienionych w 205(d) (1), (2), (3) i (4), które mogą mieć wpływ na bezpieczeństwo.



Ocena ryzyka związanego z bezpieczeństwem informacji



Kryteriami, które należy wziąć pod uwagę przy ustalaniu częstotliwości przeglądu oceny ryzyka, mogą być:

- poziom ryzyka
- krytyczność i złożoność danych aktywów

Celem przeglądu oceny ryzyka jest wywołanie ponownej oceny ryzyka, jego prawdopodobieństwa i wpływu w przypadku istotnych zmian. Jednym z możliwych sposobów jest zastosowanie wielopoziomowego podejścia do oceny ryzyka, przy czym do identyfikacji zmian stosuje się ocenę ryzyka wyższego poziomu. Ocena ryzyka wyższego poziomu może pozwolić na identyfikację szczegółowych rodzajów ryzyka, które powinny zostać poddane przeglądowi w kolejnym etapie.

Oceny ryzyka powinny podlegać regularnym przeglądom w celu:

(a) umożliwienia ciągłego doskonalenia jakości oceny ryzyka;
(b) zapewnienia skuteczności i efektywności kontroli ryzyka oraz środków ograniczających ryzyko;
(c) przeglądu planów i działań dotyczących postępowania z ryzykiem;
(d) zidentyfikowania wszelkich zmian organizacyjnych, które mogą wymagać przeglądu priorytetów, a także sposobu postępowania z ryzykiem;
(e) zachowania ogólnego obraz ryzyka;
(f) identyfikowania wszelkich nowo pojawiających się ryzyk.

GM1 IS.D.OR.205(d)

Ocena ryzyka związanego z bezpieczeństwem informacji

d) PRZEGLĄD

„Triggery” do przeglądu:

<u>zmiana w rejestrze aktywów/elementów:</u>
dodanie lub usunięcia elementów z zakresu
zmiany w projekcie lub konfiguracji
zmiany wartości

<u>zmiana interfejsów między użytkownikami / organizacjami:</u>
utworzenie nowych interfejsów
usunięcie istniejących interfejsów
zmiany istniejących interfejsów

<u>zmiana informacji lub wiedzy wykorzystywanej do identyfikacji:</u>

- zmiany zagrożeń i ich wartości, podatności, skutków lub konsekwencji, agregacji, ulepszeń, stosowanych kryteriów

<u>„lessons learned” / wyciągnięte wnioski</u>

- przegląd incydentów oraz przyczyn ich wystąpienia i przebiegu

Ocena ryzyka związanego z bezpieczeństwem informacji

Podsumowanie – do zapamiętania!

a) REJESTR AKTYWÓW

Fixed Asset Register

Serial Number	Location	Purchase Date	Supplier	Cost	Depreciation Method
hhjf8712	Accounts	17/05/2020	PC Computers	499	Straight
542ud2256	Accounts	17/05/2020	PC Computers	234	Straight
841144582	Support	01/02/2020	PC Computers	479	Straight
54712cd5584	Support	01/02/2020	PC Computers	234	Straight

b) INTERFEJSY

c) WPŁYW NA SAFETY

d) PRZEGLĄD

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