EASA

Agencja Unii Europejskiej
ds. Bezpieczeństwa Lotniczego

Narzędzie Oceny Systemu Zarządzania

Edycja 2.0
1 wrzesień 2023

Spis treści

Spis rewizji

Wydanie	Data wydania	Podsumowanie zmian
01	Wrzesień 2017	Wydanie pierwsze
02	Wrzesień 2023	Biorąc pod uwagę aktualizacje dokumentów, na których zbudowano pierwotną wersję dokumentu, grupa ekspertów UE opracowała nową edycję. Uwzględniono najnowsze dostępne wersje: Załącznika 19 ICAO[1], Podręcznika zarządzania bezpieczeństwem ICAO (dok. 9859)[2], ICAO SSPIA AREA PQ[3], narzędzie ewaluacji SMICG SMS[4] oraz Rozporządzenie (UE) 2018/1139[5]. Zakres wykorzystania Narzędzia został rozszerzony również na organizacje Part - CAMO, Part 145 i Part – 21. Informacje zwrotne i sugestie dotyczące ulepszeń przekazane przez właściwe organy UE i Branżę zostały wzięte pod uwagę, zgodnie z (zadaniem) MST.0026 EPAS[6].

Uwaga: Informacja zwrotna może być wysłana na adres safety.management@easa.europa.eu

[1] ICAO Załącznik 19, Edycja druga, czerwiec 2016, zawierająca Zmianę 1. Zmiana 2 procedowana w ramach sesji ANC (Air Navigation Commission) w 2023 r. została także uwzględniona (zob. AN.2022.WP.9611).
[2] Podręcznik Zarządzania Bezpieczeństwem ICAO (dok. 9859), Edycja czwarta, 2018. Wzięto pod uwagę również piątą edycję – przygotowywaną w zgodzie z drugą Zmianą do Załącznika 19.
[3] Zgodnie z publikacją ICAO z lutego 2022, w szczególności SSPIA.AREA.04/05/06/07/08.
[4] https://skybrary.aero/articles/sm-icg-sms-evaluation-tool (wersja 2)
[5] https://www.easa.europa.eu/en/regulations#regulations-basic-regulation
[6] https://www.easa.europa.eu/en/domains/safety-management/european-plan-aviation-safety - Edycja 2023-2025 została wzięta pod uwagę.

Wstęp

Niniejszy dokument zawiera metodologię oceny skupiającą się zarówno na zapewnieniu zgodności, jak i ciągłym doskonaleniu Systemu Zarządzania w organizacjach w systemie prawnym Unii Europejskiej (UE), mającą na celu ustandaryzowanie podejścia i wzmocnienie nadzoru właściwych organów państw członkowskich.

W ramach europejskiego porządku prawnego Narzędzie koncentruje się na dwóch elementach Systemu Zarządzania (Management System - MS):

- Systemie Zarządzania Bezpieczeństwem (SMS), odwołując się do Załącznika 19 zgodnie z ramami ICAO (zob. Sekcje 1 – 4, czyli cztery tradycyjne „filary" SMS: polityka bezpieczeństwa i jej cele; zarządzanie ryzykiem bezpieczeństwa; zapewnienie bezpieczeństwa; promowanie bezpieczeństwa);
- Systemie Monitorowania Zgodności, którego funkcją - jak opisano w systemie UE (zob. Sekcja 5) - jest sprawdzanie zgodności z odpowiednimi wymaganiami UE.

Narzędzie jest uzupełnione o ocenę zarządzania relacjami (interface management), które jest istotnym elementem bezpieczeństwa operacji lotniczych.

Uwaga 1: Odniesienia do norm i zalecanych praktyk (SARP) Załącznika 19 ICAO, jak również użytych w nim sformułowań, pozostały niezmienione. W większości przypadków zachowano odniesienie do „SMS", pozostając przy języku używanym przez ICAO dla określenia czterech filarów SMS. Zamienne stosowanie terminów [7] SMS i MS (System Zarządzania) w zależności od kontekstu nie powinno być dla użytkownika mylące.
Uwaga 2: W stosownych przypadkach zamieszczono odniesienia do Rozporządzenia (UE) nr 376/2014. Tam, gdzie było to właściwe język został również dostosowany do kontekstu UE. Przykładowo tam, gdzie ICAO używa terminu „Podmiot Lotniczy", w tym narzędziu użyto terminu „Organizacja".

Całościowe i przekrojowe podejście do oceny skuteczności Systemu Zarządzania wspiera właściwe organy w przejściu od tradycyjnego nadzoru opartego na zgodności do nadzoru opartego na wynikach/osiągach (performance-based oversight), zapewnia wspólny „mianownik" dla oceny efektywności Systemu Zarządzania i stwarza podstawę do wzajemnej akceptacji w następujących przypadkach:

- SMS-a w ramach umów międzynarodowych;
- wielu zatwierdzeń/certyfikatów (np. system zarządzania Part-CAMO zintegrowany z systemem zarządzania przewoźnika lotniczego/AOC) lub w przypadku zintegrowanego Systemu Zarządzania w przypadku organizacji posiadającej kilka certyfikatów wydanych i nadzorowanych przez różne właściwe organy; lub
- Harmonizacji Systemu Zarządzania Part-CAMO z systemem zarządzania operatora(-ów), w przypadku, gdy umowa z CAMO jest zawarta przez licencjonowanego(-ych) przewoźnika(-ów) lotniczego(-ych) stanowiącego(-ych) część grupy biznesowej przewoźnika lotniczego, gdy zaangażowane są różne właściwe organy (zob. Rozporządzenie (UE) 2022/410).

[7] Dalsze informacje na temat tego, „Czym jest System Zarządzania", zaproponowano w Załączniku 1 do tego dokumentu. Ponadto pomocne jest zrozumienie związku pomiędzy SMS i Systemem Zarządzania (MS).

Narzędzie Oceny Systemu Zarządzania jest przeznaczone do stosowania przez właściwe organy, ale może być również wykorzystywane przez organizacje w celu: oceny skuteczności ich własnych Systemów Zarządzania oraz w celu ciągłego doskonalenia lub „domknięcia" analizy luk przy wdrażaniu MS. Wynikowa ocena może być omówiona z właściwymi organami, w celu osiągnięcia konsensusu w zakresie skuteczności Systemu Zarządzania. Organizacje mogą również skorzystać z tego narzędzia do oceny relacji (interfejsów) w ramach Systemu Zarządzania z organizacjami - podwykonawcami, które powinny być zobowiązane do posiadania własnych, odpowiednio umiejscowionych Systemów Zarządzania.

Jak i kiedy narzędzie jest używane

Niniejsze narzędzie oceny Systemu Zarządzania może być wykorzystywane zarówno do wstępnej oceny Systemu Zarządzania organizacji (np. przed wstępną certyfikacją organizacji) jak i stałego nadzoru nad nią.

Uwaga: W niniejszym dokumencie używa się terminu „certyfikacja wstępna" (initial certification) w odniesieniu do zatwierdzonych organizacji, dla których wymagany jest System Zarządzania (MS); jednakże te same zasady mogą mieć zastosowanie do odpowiednich elementów systemu zarządzania w przypadku „organizacji zadeklarowanych" (declared organisations) w momencie rozpoczęcia przez nie działalności.

Certyfikacja wstępna/wstępna implementacja

Przed wstępną certyfikacją organizacji właściwy organ powinien upewnić się, że wszystkie procesy są „obecne" i „odpowiednie"[8], tak, aby wszystkie wymagane i umożliwiające działanie Systemu Zarządzania czynniki były dostępne w chwili rozpoczęcia operacji. W fazie wstępnej certyfikacji duża część oceny Systemu Zarządzania może zostać przeprowadzona poprzez przegląd odpowiedniej dokumentacji MS (tzw. desktop reviews). Jest zrozumiałe, że przed rozpoczęciem operacji nie wszystkimi elementami można się zająć (np. identyfikacją problemów bezpieczeństwa i wynikającymi z nich celami w zakresie bezpieczeństwa i wskaźnikami do monitorowania. Jednakże przeprowadzenie takiej oceny w siedzibie organizacji daje oceniającemu możliwość doradzania organizacji kierunku/ów w zakresie wdrażania Systemu Zarządzania oraz wspierania jego ustandaryzowanej implementacji; umożliwia również właściwemu organowi zadanie odpowiednich pytań:

- kluczowym kierownikom, w tym Kierownikowi Odpowiedzialnemu (Accountable Manager), odnośnie ich roli w systemie i funkcjonowania Systemu Zarządzania; oraz
- niektórym pracownikom na temat najważniejszych czynników wspierających zarządzanie bezpieczeństwem (key safety management enablers) tj. nt. znajomości i przestrzegania procedur, polityki bezpieczeństwa, pozytywnej kultury bezpieczeństwa, kultury sprawiedliwego traktowania i kultury zgłaszania (gdzie, jak, dlaczego…), roli komórki ds. bezpieczeństwa.

[8] Dalsze informacje na temat „skalowalności i odpowiedniości" znajdują się w Załączniku 2 do tego dokumentu.

Nadzór bieżący

Po rozpoczęciu działalności organizacja powinna od razu zacząć wykorzystywać procesy ustanowione w ramach Systemu Zarządzania. Właściwy organ jest z kolei zobowiązany zapewnić, że w pierwszym cyklu nadzoru bieżącego procesy te są „obecne" (P), „odpowiednie" (S) i „sprawne" (O). W niektórych elementach organizacja może posiadać „skuteczne" (E) procesy, co jest dowodem efektywnego MS. W celu sprawdzenia czy procesy MS rzeczywiście są „sprawne" i/lub „skutecznie", należy System Zarządzania regularnie poddawać ewaluacji, aby ocenić jak dobrze on działa (jak wysokie są jego osiągi). Taki przegląd powinien oceniać wszystkie elementy w ramach narzędzia oceny, czego można dokonać poprzez połączenie wizyt w organizacjach i przeglądów dokumentacji MS.

W miarę dojrzewania procesów Systemu Zarządzania w organizacji i przejścia do stanu „Sprawny" (O) i „Skuteczny" (E), może być wymagane ponowne sprawdzenie kryteriów „odpowiedniości". Zmiany w zatwierdzeniu organizacji mogą również wymagać ponownego rozważenia „odpowiedniości" procesów Systemu Zarządzania. W przypadku znaczących zmian właściwy organ może stwierdzić potrzebę przeglądu istniejącej oceny, aby upewnić się, że jest ona nadal odpowiednia.

Uznanie innych działań nadzorczych

Cenne informacje na temat efektywności Systemu Zarządzania można uzyskać z innych działań nadzorczych. Może to obejmować takie działania jak rutynowe audyty zgodności i inspekcje (zob. Sekcja 5), badania zdarzeń oraz spotkania z organizacją. Oceniający poprzez współpracę z innymi inspektorami zaangażowanymi w nadzór nad organizacją powinien to wziąć pod uwagę. Właściwy organ może również rozważyć przyznanie dodatkowych punktów, jeżeli organizacja otrzymała akredytację za spełnienie standardów branżowych.

Wydłużenie cyklu planowania nadzoru

W kontekście nadzoru opartego na osiągach (performance-based oversight), właściwy organ może wydłużyć cykl planowania inspekcji/audytu w przypadku niektórych organizacji (zob. np. ARO.GEN.305 (c)[9]) w przypadku, gdy:

(1.) organizacja zademonstrowała skuteczną identyfikację zagrożeń bezpieczeństwa lotniczego i zarządzanie towarzyszącymi im ryzykami;
(2.) organizacja stale wykazuje, że – zgodnie z ORO.GEN.130[10] – posiada pełną kontrolę nad wszystkimi zmianami w Systemie Zarządzania;
(3.) nie stwierdzono niezgodności poziomu 1; oraz

[9] https://www.easa.europa.eu/en/document-library/easy-access-rules/easy-access-rules-air-operations-regulation-eu-no-9652012 Rozporządzenie (UE) nr 965/2012 jest tu traktowane jako „odniesienie do przepisów", ale to samo podejście ma zastosowanie do każdego innego obszaru działalności.
[10] Zob. ORO.GEN.130 https://www.easa.europa.eu/en/document-library/easy-access-rules/easy-access-rules-aircrew-regulation-eu-no-11782011

(4.) wszystkie działania naprawcze zrealizowano w zaakceptowanym lub wydłużonym przez właściwy organ terminie zgodnie z ARO.GEN.350(d)(2).

Wymagania warunkujące wydłużenie cyklu nadzoru mogą być w całości zweryfikowane w oparciu o ocenę Systemu Zarządzania. W takim przypadku, właściwy organ powinien przynajmniej upewnić się, że wszystkie procesy są „sprawne" oraz że procesy identyfikacji zagrożeń, oceny i ograniczania ryzyk, zarządzanie zmianami oraz monitorowanie zgodności są „skuteczne".

Uwaga 3: Organizacja powinna mieć kontrolę nad wszystkimi zmianami i być w stanie wykazać, że każda zmiana mająca znaczący wpływ na bezpieczeństwo jest odpowiednio zarządzana.

Postępowanie w przypadku jednego lub wielu certyfikatów – zintegrowany System Zarządzania

System Zarządzania (MS) w różnych obszarach działalności lotniczej może wymagać wdrożenia określonych, specyficznych dla obszaru elementów, takich jak: plan skuteczności działania dla służb żeglugi powietrznej[11], Europejskie Forum Operatorów ds. Analizy Parametrów Lotu - EOFDM (European Operators Flight Data Monitoring[12] dla operatorów określonych typów statków powietrznych, integracja PART-CAMO w ramach przepisów OPS dla operacji CAT, próby w locie dla organizacji projektującej i/lub produkującej statki powietrzne (np. 21.A.143(a)13[13]), niezależna funkcja weryfikacji projektu produktów dla DOA (zob. 21.A.239 lit. d)2[14]), itp. Specyficzne cechy, o dużym stopniu szczegółowości, nie mogą być systematycznie i kompleksowo weryfikowane w ramach „podstawowego" narzędzia: może być konieczne dalsze „dostosowanie"[15] go do atrybutów w każdym z obszarów oraz najnowszych zmian właściwych przepisów (Domain Rules).

Jeżeli organizacja posiada wiele certyfikatów, a System Zarządzania jest zintegrowany dla kilku obszarów (np. PART-CAMO i Part-145 tj. CAMO.A.200(d) i (c) lub 145.A.200(c)[16]), korzystanie z Narzędzia Oceny Systemu Zarządzania (MSAT) powinno być zgodne z zasadą „jeden System Zarządzania = jedna ocena". Dlatego też, jeżeli jedna organizacja chce zintegrować kilka systemów zarządzania (MS) w jeden, w ocenie należy uwzględnić zintegrowany System Zarządzania w ujęciu całościowym.

[11] Zob. SKPI (Safety Key Performance Indicators) zgodnie z Rozporządzeniem wykonawczym Komisji (UE) 2019/317 ze zmianami https://www.easa.europa.eu/en/document-library/acceptable-means-of-compliance-and-guidance-materials/group/skpi-safety-key-performance-indicators; Zob. Plan skuteczności działania służb żeglugi powietrznej na lata 2025-2029 dla Polski https://ulc.gov.pl/zegluga-powietrzna/ses-jednolita-europejska-przestrzen-powietrzna/performance-scheme/plan-skutecznosci-dzialania-sluzb-zeglugi-powietrznej-na-lata-2025-2029

[12] Zob. https://www.easa.europa.eu/en/domains/safety-management/safety-promotion/european-operators-flight-data-monitoring-eofdm-forum

[13] Zob. Rozporządzenie (UE) nr 748/2012 (w:) https://www.easa.europa.eu/en/regulations/initial-airworthiness

[14] Zob. Rozporządzenie (UE) nr 748/2012 (w:) https://www.easa.europa.eu/en/regulations/initial-airworthiness

[15] Niektóre właściwe organy Państw UE uszczegółowiły Narzędzie Oceny Systemu Zarządzania EASA, aby uwzględnić specyfikę ich dziedzin zainteresowań lub profile ryzyk Podmiotów Lotniczych działających na ich terenie. Czasami te dostosowane wersje Narzędzia są dostępne na ich publicznych stronach internetowych.

[16] Zob. Rozporządzenie (UE) nr 1321/2014 (w:) https://www.easa.europa.eu/en/regulations/continuing-airworthiness

Poprzez uwzględnienie wszystkich obszarów działalności lotniczej oraz odniesień do regulacji/przepisów UE, a także wymagań Systemu Zarządzania dla każdego z nich, narzędzie to pozwala na uzgodnienie ogólnej oceny w przypadku kilku zatwierdzeń.

Może się również zdarzyć, że różne zespoły oceniających nadzorują ten sam System Zarządzania biorąc pod uwagę różne certyfikaty; wówczas pojedyncza ocena może być niepraktyczna ze względu na istotne cechy szczególne dla każdego z obszarów działalności lotniczej. W takim przypadku należy udostępnić oceny pozostałym zespołom oceniających, a właściwe organy powinny przekazać wspólne stanowisko. W razie potrzeby, gdy zaangażowane są różne właściwe organy, aby zapewnić spójne podejście, może być konieczne porozumienie i koordynacja między nimi. Dalsze wytyczne dotyczące „Systemu Zarządzania" i „zintegrowanego Systemu Zarządzania" ("integrated Management System") zostały zaproponowane w Załączniku 1 do niniejszego dokumentu.

Wytyczne dotyczące Narzędzia

Narzędzie ocenia zgodność oraz skuteczność Systemu Zarządzania przy użyciu szeregu składowych/funkcji w oparciu o Załącznik 19 ICAO oraz wymagania EASA dotyczące Systemu Zarządzania w organizacjach. Podzielono je w oparciu o 12 elementów struktury systemu SMS ICAO (zob. Załącznik 19 ICAO, Dodatek 2), uwzględniając też dodatkowe wymagania Systemu Zarządzania EASA w zawarte w przepisach UE, w tym obowiązki wynikające z Rozporządzenia (UE) nr 376/2014 dotyczące „zgłaszania zdarzeń" oraz niektórych kluczowych czynników umożliwiających rozwój „środowiska Kultury Sprawiedliwego Traktowania". Każda składowa (funkcja/cecha) powinna zostać sprawdzona w celu ustalenia, czy jest „Obecna" (P), „Odpowiednia" (S), „Sprawna" (O) i „Skuteczna" (E), przy użyciu definicji i wytycznych przedstawionych poniżej. Narzędzie to nie zajmuje się kompleksowo oceną „pozytywnej Kultury Bezpieczeństwa". Odbiorca tego dokumentu może w ramach dalszego wsparcia skorzystać z Narzędzia Ewaluacji Kultury Bezpieczeństwa w Przemyśle opracowanego przez SM-ICG (Industry Safety Culture Evaluation Tool, Safety Management International Collaboration Group)[17].

Narzędzie to jest wykorzystywane przez inspektora właściwego organu do oceny oraz może być użyte do udokumentowania tej oceny. Inną możliwością jest wykorzystanie przez organizację w celu dokonania samooceny, a następnie przez właściwy organ w celu weryfikacji i walidacji tej oceny wykonanej przez organizację.

Zastosowanie

Narzędzie oceny może być wykorzystane do oceny organizacji o dowolnej wielkości. Należy jednak wziąć pod uwagę jej wielkość, charakter i złożoność, aby ocenić czy dana cecha Systemu Zarządzania jest „Odpowiednia". Dalsze informacje na temat „skalowalności i odpowiedniości" znajdują się w Załączniku 2 do tego dokumentu. Oceniający powinni odnieść się do wszelkich istniejących przepisów UE definiujących jak System Zarządzania może wyglądać w przypadku organizacji typu non-complex (jeśli zostało to zdefiniowane w przepisach danego obszaru działalności lotniczej), gdy rozważa czy dana składowa jest „Odpowiednia". Właściwy organ powinien także rozważyć wszelkie mające zastosowanie Alternatywne Sposoby Spełnienia Wymagań w ramach oceny Systemu Zarządzania.

Narzędzie zostało zaprojektowane w celu ujęcia ogólnych wymagań dotyczących Systemu Zarządzania (MS). Ponieważ obecnie nie ma wspólnych wymogów Państw Członkowskich EASA we wszystkich obszarach działalności lotniczej, mogą obowiązywać dodatkowe wymagania specyficzne dla danego sektora, które należy uwzględnić w ramach oceny. Narzędzie jest zatem odpowiednie dla wszystkich obszarów działalności lotniczej, a jego dostosowanie do konkretnych sektorów jest „zalecane", jak wyjaśniono wcześniej w Narzędziu - w związku z posiadaniem kilku certyfikatów i/lub integracją Systemu Zarządzania.

[17] Industry Safety Culture Evaluation Tool and Guidance | SKYbrary Aviation Safety

Definicje użyte w narzędziu – poziomy dojrzałości

Obecny	Istnieją dowody na to, że przedmiot oceny jest udokumentowany w dokumentacji Systemu Zarządzania organizacji.
Odpowiedni[18]	Przedmiot oceny w sposób odpowiedni bazuje na wielkości, charakterze, złożoności organizacji oraz nieuniknionym ryzyku związanym z prowadzoną działalnością.
Sprawny	Istnieją dowody, że przedmiot oceny jest w użyciu oraz produkowany jest wynik.
Skuteczny	Istnieją dowody, że przedmiot oceny osiąga zamierzony cel i ma pozytywny wpływ na bezpieczeństwo.

Czego szukać

Ta kolumna w tabeli zawiera wskazówki dla inspektora/oceniającego, które powinien wziąć pod uwagę podczas sprawdzania poszczególnych pozycji, ale nie jest to lista kontrolna. Wymienione punkty oceny nie są specyficzne dla konkretnego poziomu PSOE, ale przypominają inspektorowi/oceniającemu, jakie obszary powinien rozważyć. Niektóre pozycje oceny w tej kolumnie mogą nie mieć zastosowania w zależności od typu lub charakteru danej organizacji.

Poziom szczegółowości dokumentacji

Ważne jest, aby inspektor/oceniający korzystający z Narzędzia udokumentował dowody oceny. Dowody obejmują dokumentację, raporty, zapisy rozmów i dyskusji. Na przykład dowodem istnienia (ocena „obecny”) danego przedmiotu oceny będzie jedynie dokumentacja, podczas gdy do wydania oceny „sprawny”, konieczne może być nie tylko ocenienie dokumentacji, ale również bezpośrednia rozmowa z personelem w organizacji.

Stwierdzanie niezgodności i obserwacji

Obecne definicje niezgodności (findings) w przepisach UE nie są spójne we wszystkich obszarach działalności lotniczej i niekoniecznie pasują do oceny Systemu Zarządzania, która wymaga większego skupienia się na efektywności procesów. Obserwacje powinny być wykorzystywane do identyfikacji obszarów dalszego doskonalenia oraz promowania pozytywnej Kultury Bezpieczeństwa.

W przypadku wstępnej certyfikacji lub w ramach przejścia do nowych wymagań Systemu Zarządzania dla obecnych posiadaczy certyfikatów, wszystkie procesy powinny być obecne i odpowiednie. Jeżeli którekolwiek z nich nie są, zatwierdzenie nie powinno być przyznane lub przejście nie powinno być zaakceptowane.

[18] Dalsze informacje na temat „skalowalności” i „odpowiedniości” znajdują się w Załączniku 2 do tego dokumentu.

Gdy System Zarządzania już rozpoczął działanie a okresy przejściowe wygasły, w przypadku stwierdzenia podczas oceny, że proces nie jest sprawny, należy wystawić niezgodność.

W przypadku stwierdzenia, że przedmiot oceny/funkcja nie jest „skuteczna", inspektorzy mogą rozważyć wpisanie/sformułowanie obserwacji w celu zapoczątkowania sugerowanych ulepszeń. Jednakże nie należy zgłaszać niezgodności, jeżeli proces jest „sprawny", ale nie jest „skuteczny", chyba, że organizacja wielokrotnie i strukturalnie ignoruje wskaźniki pokazujące, że System Zarządzania nie jest skuteczny lub nie są podejmowane żadne działania w celu zwiększenia jego efektywności.

Niezgodności zostaną stwierdzone w przypadku niekompletnego Systemu Zarządzania, poważnego ryzyka, którym się odpowiednio nie zajęto, braku zgodności, poważnego zastrzeżenia/obawy z zakresu bezpieczeństwa (wymagającego od organizacji podjęcia działania), poziomu wdrożenia MS poniżej lub daleko odbiegającego od oczekiwanego standardu. Natomiast obserwacje będą dotyczyć zidentyfikowanych obszarów do poprawy/doskonalenia, wzmacniając w ten sposób i wspierając stopniowe wdrażanie Systemu Zarządzania. Niezgodności można wystawiać wyłącznie w odniesieniu do przepisów, natomiast obserwacje mogą dotyczyć sekcji „Czego szukać", jeśli nie odnoszą się do konkretnych przepisów.

Przykłady „obserwacji"[19] mogą obejmować dowolne z następujących przypadków (ale nie ograniczać się do nich) niewymagających wystawienia niezgodności poziomu 1 lub 2:

a) jakikolwiek element podlegający ocenie, którego działanie/osiągnięty wynik (performance) zostało ocenione jako nieskuteczne;
b) gdy zidentyfikowano element podlegający ocenie potencjalnie mogący powodować niezgodność z przepisami;
c) gdy sugestie lub ulepszenia są w interesie ogólnego poziomu bezpieczeństwa organizacji.

Wartościowanie oceny Systemu Zarządzania

Głównym celem narzędzia oceny jest wsparcie właściwego organu w ocenie skuteczności Systemu Zarządzania w sposób spójny, a nie dostarczenie „wyniku" (punktacji). Uznaje się również, że plan skuteczności działania służb żeglugi powietrznej (ANS Performance scheme) może stanowić do pewnego stopnia odpowiednik oceny Systemu Zarządzania.

Jeżeli właściwy organ zdecyduje się punktować/wartościować ocenę Systemu Zarządzania nadzorowanych organizacji, musi wziąć pod uwagę następujące ważne kwestie:

- Punktacja nie powinna być liniowa, lecz wykładnicza, dzięki czemu uzyskiwany jest wyższy wynik za bycie „skutecznym", co zachęci organizacje do dążenia do osiągnięcia tego poziomu w swoich procesach.

[19] Dalsze wytyczne można znaleźć w przepisach dotyczących danego obszaru działalności lotniczej, np. w pkt. GM do 145.B.355 Rozporządzenia (UE) nr 1321/2014.

- Punktacja nie powinna być stosowana na zasadzie zaliczony/niezaliczony, ale jako pomoc w ocenie stopnia dojrzałości Systemu Zarządzania jako poziomu odniesienia w stosunku do innych organizacji oraz jako pomoc w ciągłym doskonaleniu.
- Punktacja może również powodować niewłaściwe zachowania w organizacjach, co może podważyć pozytywną Kulturę Bezpieczeństwa, dlatego należy ją bardzo ostrożnie stosować i monitorować pod kątem takiego ewentualnego wpływu.
- Osiągnięcie „skutecznego" poziomu lub wysokiego wyniku nie oznacza końca procesu, ponieważ wydajność w przeszłości nie gwarantuje wydajności w przyszłości. Środowisko z natury jest dynamiczne, występują bowiem zdarzenia lotnicze, zdarzenia zakłócające normalne operacje (disruptive events), kryzysy, pojawiające się nowe ryzyka, zmiany w Systemie Zarządzania itp. Wcześniejsze oceny ryzyka mogą z czasem utracić ważność, dlatego wymagają systematycznego przeglądu.

Podsumowanie oceny

Identyfikując poziomy dojrzałości różnych procesów i dostarczając organizacji szczegółowe komentarze z oceny, otrzyma ona pomoc w ciągłym doskonaleniu swojego Systemu Zarządzania.

W trakcie używania Narzędzia, oceniający powinien ocenić jak sprawnie organizacja działa i jak zarządza bezpieczeństwem z perspektywy globalnej (całościowej). W związku z tym podsumowanie oceny powinno być zorientowane na osiągane wyniki (performance). Każdy raport z działania Systemu Zarządzania powinien w szczególności uwzględniać:

- proaktywne zarządzanie ryzykami bezpieczeństwa;
- osiągany przez organizację poziom bezpieczeństwa (safety performance);
- zbieranie danych (data intelligence) i ich wykorzystanie;
- odporność i sprawność w reagowaniu na zdarzenia zakłócające normalne operacje lub stale zmieniające się, konkurencyjne środowisko; oraz
- ogólną dojrzałość organizacji w zakresie zarządzania bezpieczeństwem i inne jej działania mające wpływ na bezpieczeństwo.

Raport powinien dokumentować najskuteczniejsze procesy Systemu Zarządzania oraz obszary wymagające dalszego doskonalenia (np. nieskuteczna kontrola ryzyka, nowe lub pojawiające się ryzyka do rozważenia, niesprawne procesy, szanse doskonalenia). Ocena powinna również obejmować cele organizacji w zakresie bezpieczeństwa i stopień ich osiągnięcia, a także ich związek z celami na poziomie krajowym zawartymi w Krajowym Programie Bezpieczeństwa w Lotnictwie Cywilnym (KPBwLC)[20] oraz Krajowym Planie Bezpieczeństwa (KPB)[21] tam, gdzie to właściwe.

[20] https://ulc.gov.pl/zarzadzanie-bezpieczenstwem/program-bezpieczenstwa-w-lotnictwie-cywilnym/krajowy-program-bezpieczenstwa-w-lotnictwie-cywilnym-kpbwlc
[21] https://ulc.gov.pl/zarzadzanie-bezpieczenstwem/program-bezpieczenstwa-w-lotnictwie-cywilnym/krajowy-plan-bezpieczenstwa

Podsumowanie oceny Systemu Zarządzania powinno być przekazane organizacji wraz z raportem zawierającym niezgodności i obserwacje oraz harmonogramem ich usunięcia. Niezgodności i obserwacje powinny odzwierciedlać stopień pilności osiągnięcia celów bezpieczeństwa lub nakłaniać/motywować daną organizację do szybszych, lepszych osiągnięć i/lub ciągłego doskonalenia w zakresie bezpieczeństwa.

Podsumowanie może również podkreślić, jak chłonna (otwarta) jest organizacja na wdrażanie skutecznego Systemu Zarządzania oraz zwrócić uwagę na proces proaktywnego rozwijania zdolności zarządzania ryzykiem bezpieczeństwa i zapewniania poziomu bezpieczeństwa w miarę upływu czasu. Większość organizacji lubi wiedzieć, jak radzą sobie w porównaniu z innymi.

WAŻNE: jak używać wytycznych dotyczących narzędzia

Narzędzie służy zarówno do oceny zapewnienia zgodności jak i wydajności/osiągów. Obowiązkiem organizacji i oceniającego(-ych) jest dopilnowanie, by:

- właściwe elementy Systemu Zarządzania były obecne i odpowiednie do jego prawidłowego funkcjonowania (zorientowane na zgodność (compliance oriented));
- System Zarządzania był sprawny i świadczył usługi zgodnie z oczekiwaniami (zorientowany na wydajność/osiągi (performance-oriented)).

Obok bardziej tradycyjnych wymagań opartych na normach, ocena Systemu Zarządzania wymaga zrozumienia **oczekiwań opartych na osiąganych wynikach** (**performance-based expectations**). Rozumienie to dotyczy zarówno organizacji, jak i właściwego organu.

Oprócz „tradycyjnej zgodności" i uwzględnienia wielkości organizacji, a także złożoności/charakteru jej działań, ewaluacja Systemu Zarządzania powinna uwzględniać ogólną zdolność organizacji do skutecznego zarządzania bezpieczeństwem, wyznaczania celów bezpieczeństwa, ich monitorowania i osiągania.

W związku z tym, system *ocen „Obecny (P), Odpowiedni (S), Sprawny (O), Skuteczny (E)"* (PSOE) będzie raczej stosowany jako model dojrzałości, tak aby jego ocena była zorientowana na osiągane wyniki (wydajność) i obejmowała ewaluację tego, jak sprawnie organizacja działa, zarządza bezpieczeństwem oraz zapewnia bezpieczeństwo operacji w skali globalnej.

Ocena powinna w szczególności koncentrować się na poziomach dojrzałości i tym, czy:

- System Zarządzania, globalnie lub dla każdego elementu, jest udokumentowany i zdefiniowany – w pewnym stopniu nawiązuje do poziomu „Obecny" (P); lub
- Systemu Zarządzania jest zaprojektowany w taki sposób, że jest odpowiedni do działalności, jej charakteru i złożoności, relacji z innymi podmiotami (interfejsów) itp. – innymi słowy, MS jest „Odpowiedni" (S); lub
- System Zarządzania jest „skalowalny", „sprawny" i dostarcza oczekiwane usługi – istnieje dowód na to, że System Zarządzania działa zgodnie z założeniami; jednakże pożądany wynik nie został jeszcze osiągnięty i/lub więcej powinno zostać osiągnięte, jako że System Zarządzania nie osiągnął jeszcze oczekiwanego poziomu dojrzałości; lub
- Istnieją dowody na to, że System Zarządzania jest sprawny w skali globalnej i działa w „skuteczny" sposób, mając pozytywny wpływ na bezpieczeństwo i dążąc do ciągłego doskonalenia; pożądany efekt jest osiągany poprzez realizację celów bezpieczeństwa.

W żadnym wypadku narzędzia tego nie można używać jako listy kontrolnej w zakresie zgodności z przepisami w celu sprawdzenia, czy wszystkie poszczególne elementy Systemu Zarządzania są na swoim miejscu. Ocena Systemu nie jest zadaniem polegającym na zaznaczeniu wszystkich pól w części „Na co zwrócić uwagę" w każdej sekcji narzędzia. Obowiązkiem oceniającego jest odpowiednie wykorzystanie tego narzędzia **WYŁĄCZNIE jako przewodnika**

umożliwiającego przygotowanie się przed oceną; wybranie, jeśli to konieczne, tego, co istotne (w oparciu o wielkość, złożoność i charakter operacji); i zapewnienie ogólnej oceny Systemu Zarządzania pod kątem „dojrzałości" i „osiąganych wyników/wydajności" (performance).

„Bycie zgodnym z przepisami" niekoniecznie oznacza „bycie bezpiecznym". Zbyt literalne wykorzystanie tego narzędzia i ultra szczegółowa weryfikacja każdego procesu „krok po kroku" lub „słowo po słowie" stwarza ryzyko, że będzie ona zbyt wąska i powiedzie oceniającego błędną ścieżką prowadzącą tylko do oceny „zgodności"; spychając strukturę organizacji w kierunku nieodpowiedniej konfiguracji lub nadmiernie skomplikowanego Systemu Zarządzania, ostatecznie mijając się z najważniejszym celem: ocenieniem jak bezpieczne są operacje i upewnieniem się, że żadne większe ryzyko nie zostało przeoczone.

Ewaluacja „odpowiedniości" (suitability) i „skalowalności" (scalability)

„Odpowiedniość" Systemu Zarządzania jest specyficzna dla każdej organizacji i niemożliwa do zdefiniowania w taki sposób, by opisywała każdy typ aktywności i rozmiar organizacji. Niektóre organizacje mogą być „małe" w kategorii rozmiaru, ale wykonywać operacje krytyczne dla bezpieczeństwa współpracując z wieloma podmiotami zewnętrznymi. Czasami ramy prawne dedykowane danej dziedzinie działalności proponują pewne wytyczne dotyczące poszczególnych tematów, na przykład uwzględnienie zasobów ludzkich organizacji typu complex (complex organisation) vs non-complex (non-complex organisation). Nie zawsze tak jest, zatem rekomenduje się, by:

- przed oceną przeanalizować co jest odpowiednie dla danej struktury organizacyjnej;
- na koniec całościowej oceny Systemu Zarządzania ponownie rozważyć czy cały System Zarządzania i powiązane z nim procesy są współmierne do wielkości organizacji i złożoności/charakteru jej produktów lub świadczonych przez nią usług lotniczych.

Ani „odpowiedniość" ani „skalowalność" nie polegają na zastosowaniu określonych elementów Systemu Zarządzania ani też wybraniu uproszczonego lub złożonego Systemu Zarządzania: chodzi o dostosowanie Systemu Zarządzania wraz ze wszystkimi jego elementami do konkretnego kontekstu operacyjnego organizacji. Obowiązkiem organizacji jest określenie odpowiedniości i/lub skalowalności swojego Systemu Zarządzania i wykazanie właściwemu organowi, że system jest **prawidłowo zaprojektowany i odpowiedni** do skutecznego/efektywnego dostarczania usług zgodnie z oczekiwaniami, jak wyjaśniono w poprzedniej ramce.

W Załączniku 2 na końcu tego dokumentu zaproponowano dalsze wytyczne dotyczące „odpowiedniości" i „skalowalności".

Przeprowadzenie i sekwencjonowanie oceny Systemu Zarządzania

Nie ma szczególnych wymagań w zakresie kolejności korzystania z różnych sekcji narzędzia, decyzja o sposobie przeprowadzenia oceny Systemu Zarządzania pozostaje w gestii oceniającego:

- Czasami rozpoczęcie od sekcji 2 (Zarządzanie Ryzykiem Bezpieczeństwa), a następnie sekcji 3 (Zapewnianie bezpieczeństwa) Narzędzia może być bardziej odpowiednie - w zależności od dojrzałości organizacji. Na przykład najbardziej istotne mogą okazać się następujące pytania: „Jakie są główne ryzyka organizacji?", „Skąd organizacja o tym wie?", „W jaki sposób organizacja minimalizuje te ryzyka?" „Skąd organizacja wie, że środki łagodzące są skuteczne?", „Czy cele bezpieczeństwa są monitorowane i ostatecznie osiągane?", „W jaki sposób jest to przekazywane kierownictwu wyższego szczebla i pracownikom?" Itd./Itp.
- W niektórych przypadkach, np. wstępnego uruchomienia lub wdrożenia Systemu Bezpieczeństwa, korzystne może być najpierw zrozumienie postępów organizacji, wyzwań przed jakimi stanęła, a potem kolejnych etapów przed nią stojących (zanim osiągnie wyższy poziom dojrzałości). Nie ma wtedy szczególnego znaczenia kolejność stosowania sekcji narzędzia.
- Kolejnym sposobem jest wybranie konkretnego celu bezpieczeństwa, obszaru większego ryzyka lub Problemu Bezpieczeństwa, a następnie, przy wykorzystaniu wszystkich sekcji narzędzia jednocześnie (podejście oparte na celach, ryzyku i osiągach (objective-based, risk-based, and performance-based approach), zrozumienie w jaki sposób organizacja zarządza globalnie danym tematem.
- Poprzez dopasowanie różnych elementów tego narzędzia można również monitorować ciągły przepływ informacji oraz uzyskiwać wyniki na poziomie krajowym prezentując dane z audytów w ramach bieżącego nadzoru; analizę zdarzeń; raporty dotyczące osiągów (performance reports, analiza FDM), zarządzanie paliwem, HUMS (Health and Usage Monitoring Systems), plan skuteczności działania służb żeglugi powietrznej (ATM performance scheme), zarządzanie zmianami; zatwierdzenie zmian w podręczniku procedur/charakterystyce organizacji (exposition manual); notatki ze spotkań Rady ds. Bezpieczeństwa (Safety Review Board) lub uczestnictwo w Komitetach Bezpieczeństwa Wysokiego Szczebla) itp.

Wymienione sposoby postępowania wpłyną na liczbę wykonywanych ocen i czas ich trwania, jednakże bez możliwości zalecenia konkretnego czasu czy liczby oceniających/audytorów potrzebnych do całkowitej/pełnej oceny Systemu Zarządzania w ramach cyklu nadzoru. Zależy to bowiem od „wielkości", „złożoności", „charakteru operacji" i „liczby/istotności ryzyk".

We wszystkich przypadkach ostatecznie liczy się to, aby oceniający na koniec cyklu nadzoru był w stanie ocenić ogólny/całkowity poziom dojrzałości organizacji i jej zdolność do efektywnego zarządzania bezpieczeństwem wykraczającą poza samo przestrzeganie przepisów.

Opinia na temat korzystania z narzędzia

Zgodnie z MST.0026 w EPAS[22], właściwe organy państw UE korzystające z tego narzędzia, niezależnie od tego, czy zostało ono dostosowane, czy nie, mają obowiązek przekazywania EASA wniosków z jego stosowania na adres safety.management@easa.europa.eu oraz w razie potrzeby, sugerowania ulepszeń. Każdy inny użytkownik (w tym z organizacji) jest również zaproszony do wniesienia swojego wkładu.

Szkolenie w zakresie korzystania z Narzędzia Oceny Systemu Zarządzania

Ważne jest, aby oceniający byli kompetentni w zakresie prawidłowego korzystania z narzędzia. Ocena Systemu Zarządzania różni się od tradycyjnego podejścia opartego na zgodności z przepisami (compliance-based approach). Oceniający powinni:

- być zaznajomieni z podstawami Systemu Zarządzania, w tym z koncepcjami ocen opartych na ryzyku (risk-based) i na osiągach (performance-based);
- potrafić zrozumieć zasady dotyczące „odpowiedniości", „skalowalności" i „efektywności" Systemu Zarządzania (MS);
- być przeszkoleni w zakresie stosowania tego Narzędzia Oceny Systemu Zarządzania i innych technik przeprowadzania oceny MS;
- zachowywać się zgodnie z zasadami pozytywnej Kultury Bezpieczeństwa;
- być kompetentni w korzystaniu z tego narzędzia – należy rozważyć potrzebę szkolenia w miejscu pracy - OJT (On-the-Job Training) przed uznaniem ich za wykwalifikowanych;
- regularnie aktualizować informacje na temat stosowania tego narzędzia i dobrych praktyk w zakresie oceniania SMS – szczególnie ważne jest, aby dzielić się swoimi doświadczeniami i wspierać spójne podejście wśród oceniających.

[22] https://www.easa.europa.eu/domains/safety-management/european-plan-aviation-safety

1 POLITYKA BEZPIECZEŃSTWA I JEJ CELE

1.1 ZAANGAŻOWANIE KIEROWNICTWA

1.1.1 Polityka bezpieczeństwa, zatwierdzanie i przegląd okresowy

Odniesienia i tekst Załącznika 19

1.1.1 Podmiot lotniczy definiuje swoją politykę bezpieczeństwa zgodnie z wymogami międzynarodowymi i krajowymi.

Polityka bezpieczeństwa:

e) jest podpisana przez Dyrektora Odpowiedzialnego (Accountable Executive) organizacji
Uwaga: w kontekście UE Dyrektor Odpowiedzialny jest wyznaczony jako Kierownik Odpowiedzialny (Accountable Manager).

g) jest okresowo analizowana, aby zapewnić, że pozostaje aktualna i odpowiednia dla podmiotu lotniczego

Obecny	Odpowiedni	Sprawny	Skuteczny
Istnieje polityka bezpieczeństwa, zatwierdzona przez Kierownika Odpowiedzialnego, która zawiera zobowiązanie do ciągłego doskonalenia; zawiera wszystkie obowiązujące wymagania i standardy prawne, a także uwzględnia najlepsze praktyki.	Polityka bezpieczeństwa jest łatwa do odczytania.Treść jest dostosowana do organizacji.	Polityka bezpieczeństwa poddawana jest okresowym przeglądom, aby zapewnić, że pozostaje odpowiednia dla organizacji.	Kierownik Odpowiedzialny doskonale rozumie politykę bezpieczeństwa i jest w pełni zaangażowany w jej wdrażanie.
Wyniki oceny			

Czego szukać

- Przeprowadzić wywiad z Kierownikiem Odpowiedzialnym, aby ocenić jej/jego wiedzę i zrozumienie polityki bezpieczeństwa.
- Sprawdzić dowody potwierdzające, że Kierownik Odpowiedzialny podejmuje świadome decyzje zgodnie z polityką bezpieczeństwa.
- Potwierdzić, czy polityka bezpieczeństwa jest właściwa i spełnia obowiązujące przepisy UE.
- Sprawdzić, czy „bezpieczeństwo" jest kluczowe dla polityki i pozostaje najwyższym priorytetem.
- Przeprowadzić wywiad z personelem, aby ustalić, w jakim stopniu znane są wartości i cele polityki bezpieczeństwa oraz na ile są one czytelne i zrozumiałe.
- Znaleźć dowody potwierdzające, że wszyscy pracownicy i kluczowi interesariusze przyczyniają się do bezpiecznego funkcjonowania systemu zgodnie z polityką bezpieczeństwa.
- Sprawdzić, czy polityka bezpieczeństwa jest okresowo sprawdzana pod kątem treści i aktualności.
- Sprawdzić, czy polityka bezpieczeństwa zawiera zobowiązanie do ciągłego doskonalenia, przestrzega wszystkich obowiązujących wymagań i standardów prawnych oraz bierze pod uwagę najlepsze praktyki.

Odpowiednie odniesienia do przepisów UE/EASA				
Operacje lotnicze	**Załoga lotnicza**	**Lotniska**	**ATM/ANS**	**Organizacja szkolenia ATC**
ORO.GEN.200 "System zarządzania" punkt (a)(2) i (a)(6) AMC1 ORO.GEN.200 (a)(2) "System zarządzania" – (operatorzy typu complex) AMC1 ORO.GEN.200(a) (1)(2)(3)(5) "System zarządzania" punkt (e) – (operatorzy typu non-complex)	ORA.GEN.200 „System zarządzania" punkt (a)(2) i (a)(6) AMC1 ORA.GEN.200(a)(2) „System zarządzania" – (organizacje typu complex) AMC1 ORA.GEN.200(a)(1)(2) (3)(5) „System zarządzania" punkt (e) – (organizacje typu non-complex)	ADR.OR.D.005 „System zarządzania" punkt (b)(2) AMC1 ADR.OR.D.005 „System zarządzania" punkt (b)(2)	ATS.OR.200 "System zarządzania" punkt (1) AMC1 ATS.OR.200(1) (i) „System zarządzania bezpieczeństwem; polityka bezpieczeństwa" – (podmioty ATS typu complex) AMC1 ATS.OR.200(1); (2); (3) „System zarządzania bezpieczeństwem" OGÓLNE (podmioty ATS typu non-complex)	ATCO.OR.C.001 „System zarządzania organizacji szkoleniowych" punkt (b) AMC1 ATCO.OR.C.001(b) „Polityka bezpieczeństwa systemu zarządzania organizacji szkoleniowych"
CAMO	**PART 145**	**Organizacje produkujące/POA**	**Organizacje projektujące/DOA**	**Zarezerwowane**
CAMO.A.200 "System zarządzania" punkt (a)(2) i (a)(6) AMC1 CAMO. A. 200 (a) (2) GM CAMO.A.200(a)(2) CAMO.A.300(a)(2) „Charakterystyka zarządzania ciągłą zdatnością do lotu (CAME)"	145.A.200 „System zarządzania" punkt (a) (2) i (a) (6) 145.A.30 „Wymagania dotyczące personelu" (a)(2) AMC1 145.A.200(a)(2) „Polityka bezpieczeństwa i jej cele" GM 145.A.200(a)(2) „Polityka bezpieczeństwa" 145.A.70 punkt (a)(2) „Charakterystyka organizacji obsługowej (MOE)" AMC1 145.A.70 „Charakterystyka organizacji obsługowej (MOE)"	21.A.139(c)(1) „System zarządzania produkcją" AMC1 21.A.139 (c)(1) „Polityka bezpieczeństwa i jej cele" GM1 21.A.139(c)(1) „Polityka bezpieczeństwa"	21.A.239 „System zarządzania projektowaniem" (c)(1) AMC1 21.A.239 (c)(1) „Polityka bezpieczeństwa i jej cele" GM1 21.A.239(c)(1) „Polityka bezpieczeństwa"	

1.1.2 Polityka bezpieczeństwa i zasoby

Odniesienia i tekst Załącznika 19

1.1.1 Polityka bezpieczeństwa:

b) zawiera jednoznaczne oświadczenie o zapewnieniu zasobów niezbędnych do wdrożenia polityki bezpieczeństwa.

Obecny	Odpowiedni	Sprawny	Skuteczny
Polityka bezpieczeństwa zawiera oświadczenie o zapewnieniu odpowiednich zasobów.	Istnieje proces oceny zasobów i eliminowania wszelkich braków; potrzeby są omawiane na właściwym szczeblu kierownictwa. Wielkość i znaczenie zleconych działań (do i od) są odpowiednio uwzględniane przy określaniu zasobów niezbędnych do zapewnienia bezpiecznych operacji. W przypadku wielu zatwierdzeń przydzielane są odpowiednie zasoby, biorąc pod uwagę złożoność operacji.	Organizacja ocenia zapewnione zasoby w celu świadczenia bezpiecznych usług i podejmuje działania w celu usunięcia wszelkich braków.	Organizacja dokonuje przeglądu i podejmuje działania w celu usunięcia wszelkich prognozowanych niedoborów w zasobach. Przewiduje się i prognozuje potrzeby, w szczególności wykorzystując zasady „zarządzania zmianami”.
Wyniki oceny			

Czego szukać

Uwaga 1: nacisk położony jest tutaj na „zasoby” umożliwiające osiągnięcie celów bezpieczeństwa i prawidłowe zarządzanie kluczowymi ryzykami bezpieczeństwa. Wiedząc, że zasoby nie są nieograniczone, należy dokonać przeglądu tej kwestii w kontekście wyników w zakresie bezpieczeństwa, zwłaszcza pod kątem dostępności zasobów przeznaczonych do realizacji najważniejszych działań związanych z bezpieczeństwem. Zarządzanie ryzykiem bezpieczeństwa (Safety risk management) to podejmowanie decyzji mających na celu zrównoważenie/zbalansowanie poprawy bezpieczeństwa, dostępnych zasobów do jego rozwoju i zoptymalizowanych sposobów pracy.
Uwaga 2: „zasoby” w tym przypadku nie ograniczają się do „zasobów ludzkich”, ponieważ mogą również obejmować zasoby finansowe, narzędzia, dokumentację i procesy itp.
Uwaga 3: polityka bezpieczeństwa powinna zawierać jasne stwierdzenie dotyczące zapewnienia niezbędnych zasobów. Jej szczegółową realizację można znaleźć w innym dokumencie.

- Przejrzeć dostępne, odpowiednie zasoby, w tym: personelu, sprzętu i finansów.
- W jaki sposób organizacja zarządza zasobami, przewidując i eliminując wszelkie braki?
- Czy jest wystarczająca liczba kompetentnych pracowników? Jak organizacja to ocenia?
- Przejrzeć zapotrzebowanie (targeted resources) w porównaniu z rzeczywistymi zasobami.
- Sprawdzić, czy zasoby są omawiane odpowiednio z kierownikiem odpowiedzialnym lub podczas posiedzenia Rady ds. Bezpieczeństwa - SRB (Safety Review Board) (lub jej odpowiednika).
- Zagwarantować, by strategia nie została zdefiniowana tylko w oparciu o bieżące zasoby, ale także, by opierała się na potrzebnych zasobach i sposobach pracy, aby odpowiednio złagodzić kluczowe ryzyka bezpieczeństwa.
- Sprawdzić, czy zgłasza się jakiekolwiek problemy ze zmęczeniem, brak zasobów, słabe strony wydolności człowieka, zwłaszcza w ramach wewnętrznego systemu zgłaszania kwestii związanych z bezpieczeństwem.

- Rozważyć system organizacji czasu pracy a także, w stosownych przypadkach, wdrożenie Dyrektywy 2003/88/WE. W stosownych przypadkach sprawdzić wdrożenie FRMS (Fatigue Risk Management System), FTL (Flight Time Limitations) itp.
- Sprawdzić, czy stosowane są zasady „zarządzania zmianami" w celu przewidywania ograniczenia/braku zasobów w przypadku zmian.
- Ocenić sytuację, gdy organizacja posiada wiele zatwierdzeń.
- Sprawdzić potrzebę powołania Grup(y) ds. działań w zakresie bezpieczeństwa (Safety Action Group(s)) do pomocy lub działania w imieniu Kierownika ds. bezpieczeństwa (Safety Manager) lub SRB.
- Jeżeli kilku operatorów tworzących część jednej grupy biznesowej przewoźnika lotniczego korzysta z tego samego CAMO do zarządzania ciągłą zdatnością do lotu wszystkich eksploatowanych przez siebie statków powietrznych, należy sprawdzić, czy zasoby przydzielone przez CAMO odpowiadają potrzebom różnych zaangażowanych operatorów i (zasoby) są odpowiednie do zapewnienia zarządzania ciągłą zdatnością do lotu wszystkich obsługiwanych statków powietrznych (zob. M.A.201(ea) oraz CAMO.A.200(e)).

Odpowiednie odniesienia do przepisów UE/EASA				
Operacje lotnicze	**Załoga lotnicza**	**Lotniska**	**ATM/ANS**	**Organizacja szkolenia ATC**
AMC1 ORO.GEN.200(a)(2) "System zarządzania" – (operatorzy typu complex) AMC1 ORO.GEN.200(a) (1)(2)(3)(5) "System zarządzania" punkt (e) – (operatorzy typu non-complex)	AMC1 ORA.GEN.200(a)(2) „System zarządzania" – (organizacje typu complex) AMC1 ORA.GEN.200(a)(1)(2)(3)(5) „System zarządzania" punkt (e) – (organizacje typu non-complex)	AMC1 ADR.OR.D.005 „System zarządzania" punkt (b)(2)	ATS.OR.200 "System zarządzania" Punkt (1) oraz powiązane AMC/GM	ATCO.OR.C.001 „System zarządzania organizacji szkoleniowych" punkt (b) oraz powiązane AMC/GM
CAMO	**PART 145**	**Organizacje produkujące/POA**	**Organizacje projektujące/DOA**	**Zarezerwowane**
AMC1 CAMO.A.200(a)(1) "System zarządzania" punkt (c) AMC1 CAMO.A.200(a)(2) "System zarządzania" punkt (b)(2) CAMO.A.300(a)(4) „Charakterystyka zarządzania ciągłą zdatnością do lotu (CAME)" CAMO.A.305 (a)(5) „Wymagania w stosunku do personelu" GM1 CAMO.A.305 (a)(5) „Kierownik ds. bezpieczeństwa" CAMO.A.305(d) i AMC1	145.A.200 „System zarządzania" punkt (a)(2) 145.A.30 „Wymagania w stosunku do personelu" punkty (a)(1); (b); (ca) 145.A.70 „Charakterystyka organizacji obsługowej (MOE)" punkt (a)(2) AMC1 145.A.200(a)(2) „Polityka bezpieczeństwa i jej cele" GM 145.A.200(a)(2) „Polityka bezpieczeństwa" AMC1 145.A.70 „Charakterystyka organizacji obsługowej (MOE)" AMC1 145.A.30(b) „Struktura zarządzania obsługi technicznej"	21.A.139 „System zarządzania produkcją" punkt (c)(1) i (c)(2) AMC1 21.A.139 (c)(1) „Polityka bezpieczeństwa i jej cele" punkt (b)2 21.A.145(a) „Zasoby" całość AMC i GM powiązane z 21.A.145(a) „Zasoby"	21.A.239 „System zarządzania projektowaniem" punkt (c)(1) i (c)(2) AMC1 21.A.239 (c)(1) „Polityka bezpieczeństwa i jej cele" punkt (b)2 21.A.245 (a) i (e) „Zasoby" AMC1 21.A.245(a) i AMC1 21.A.245(e) „Zasoby"	

CAMO.A.305(d) „Wystarczająca liczba personelu” M.A.201(ea) i CAMO.A.200(e) „System zarządzania” punkt (e) – powiązane AMC i GM	AMC1 145.A.30(d) „Wymagania dotyczące personelu” AMC1 145.A.30(c);(ca) „Zarządzanie bezpieczeństwem i funkcja monitorowania zgodności” - powiązane GM1 145.A.30(ca) AMC1 145.A.200(a)(1) „Organizacja i odpowiedzialność – powiązane z GM1 145.A.200(a)(1)			

1.1.3 Komunikowanie polityki bezpieczeństwa

Odniesienia i tekst Załącznika 19

1.1.1 Polityka bezpieczeństwa:

f) jest upowszechniona oraz widoczna w całej organizacji

Zob. 2.1.2 odnośnie c) zawierać procedury zgłaszania informacji bezpieczeństwa (safety reporting procedures)

Obecny	Odpowiedni	Sprawny	Skuteczny
Istnieją środki umożliwiające komunikowanie polityki bezpieczeństwa i związanych z nią celów. Zaangażowanie kierownictwa w bezpieczeństwo jest udokumentowane w polityce bezpieczeństwa.	Polityka bezpieczeństwa i związane z nią cele są wyraźnie widoczne (lub osiągalne) dla całego personelu (np. uwzględniają mnogość stron, państw). Polityka bezpieczeństwa jest zrozumiała (należy wziąć pod uwagę mnogość języków).	Polityka bezpieczeństwa i powiązane z nią cele są przekazywane całemu personelowi (w tym odpowiedniemu personelowi kontraktowemu i organizacjom współpracującym). Kierownik Odpowiedzialny i kadra kierownicza wyższego szczebla promują swoje zaangażowanie w politykę bezpieczeństwa poprzez aktywne i widoczne uczestnictwo w systemie zarządzania bezpieczeństwem.	Osoby w całej organizacji znają politykę bezpieczeństwa i powiązane z nią cele oraz potrafią opisać swoje obowiązki w odniesieniu do polityki bezpieczeństwa i wewnętrznego systemu zgłaszania kwestii związanych z bezpieczeństwem.
Wyniki oceny			

Czego szukać

Uwaga: Polityka bezpieczeństwa powinna określać cele bezpieczeństwa, które należy uwzględnić w ocenie (zob. część „cele bezpieczeństwa”).

- Przejrzeć sposób komunikowania/rozpowszechniania polityki bezpieczeństwa.
- Polityka bezpieczeństwa jest wyraźnie widoczna (lub osiągalna, w zależności od struktury i wielkości organizacji) dla całego personelu, w tym odpowiedniego personelu kontraktowego i organizacji współpracujących.
- Zapytać kierowników i pracowników o wiedzę na temat polityki bezpieczeństwa i powiązanych z nią celów.
- Wszyscy kierownicy są zaznajomieni z kluczowymi elementami polityki bezpieczeństwa i związanymi z nią celami.
- Dowiedzieć się, czy kadra kierownicza wyższego szczebla (senior management) zaangażowana w działania związane z bezpieczeństwem uczestniczy w spotkaniach, szkoleniach, konferencjach itp. dotyczących bezpieczeństwa.
- Sprawdzić, w jaki sposób promowana jest pozytywna kultura bezpieczeństwa (positive safety culture) i jak wpływa ona na ogólną skuteczność, szczególnie w odniesieniu do systemu raportowania na temat bezpieczeństwa (zgłaszania informacji dot. bezpieczeństwa) i jego działań.

Odpowiednie odniesienia do przepisów UE/EASA				
Operacje lotnicze	**Załoga lotnicza**	**Lotniska**	**ATM/ANS**	**Organizacja szkolenia ATC**
AMC1 ORO.GEN.200(a)(2) "System zarządzania" – (operatorzy typu complex) Nie dotyczy operatorów typu non-complex.	AMC1 ORA.GEN.200(a)(2) „System zarządzania" – (organizacje typu complex) Nie dotyczy organizacji typu non-complex	AMC1 ADR.OR.D.005 „System zarządzania" punkt (b)(2) AMC1 ADR.OR.D.005(b)(2) „System zarządzania" punkt (a)(4)	ATS.OR.200 "System zarządzania" (1)(i) AMC1 ATS.OR.200(1)(i) System zarządzania bezpieczeństwem POLITYKA BAZPIECZEŃSTWA – (podmioty ATS typu complex) AMC1 ATS.OR.200 (1); (2); (3) „System zarządzania bezpieczeństwem" WYMAGANIA OGÓLNE (podmioty ATS typu non-complex)	AMC1 ATCO.OR.C.001(b) „System zarządzania organizacji szkoleniowych" punkt (d)
CAMO	**PART 145**	**Organizacje produkujące/POA**	**Organizacje projektujące/DOA**	**Zarezerwowane**
AMC1 CAMO.A.200(a)(2) "System zarządzania" – punkt (a)(5) CAMO.A.200(a)(5) oraz GM1 CAMO.A.200(a)(5) CAMO.A.202 „Wewnętrzny system zgłaszania kwestii związanych z bezpieczeństwem/informacji bezpieczeństwa" i AMC1 CAMO.A.202	145.A.200 „System Zarządzania" punkt (a)(2) i (a)(5) AMC 1 145.A.200(a)(2) „Polityka bezpieczeństwa i jej cele" punkt (c) i (d)	AMC1 21.A.139 (c)(1) „Polityka bezpieczeństwa i jej cele" punkt (a)1	AMC1 21.A.239 (c)(1) „Polityka bezpieczeństwa i jej cele" punkt (a)1	

1.1.4 Polityka bezpieczeństwa, zaangażowanie i pozytywna kultura bezpieczeństwa (positive safety culture)

Odniesienia i tekst Załącznika 19

1.1.1 Polityka bezpieczeństwa:

a) odzwierciedla zaangażowanie organizacji w zakresie bezpieczeństwa, w tym promowanie pozytywnej kultury bezpieczeństwa

Zob. Rozporządzenie (EU) 376/2014 Art. 16

Obecny	Odpowiedni	Sprawny	Skuteczny
Polityka bezpieczeństwa jest udokumentowana, włączając w to promocję pozytywnej kultury bezpieczeństwa. Polityka bezpieczeństwa podkreśla podstawową odpowiedzialność za bezpieczeństwo wszystkich pracowników by proaktywnie zarządzać ryzykiem. Polityka bezpieczeństwa zawiera główne atrybuty pozytywnej kultury bezpieczeństwa, w tym zaangażowanie w przywództwo związane z bezpieczeństwem (safety leadership) i Just Culture w całej organizacji.	Polityka bezpieczeństwa opisuje zaangażowanie całego właściwego personelu w działania związane z bezpieczeństwem. „Kodeks etyki" lub zachowań pożądanych jest udokumentowany i odpowiedni do rodzaju działań związanych z bezpieczeństwem.	Polityka bezpieczeństwa i związana z nią pozytywna kultura bezpieczeństwa są wdrażane operacyjnie i promowane na poziomie pracowniczym przez Kierownika Odpowiedzialnego i kluczowych menedżerów zaangażowanych w działania związane z bezpieczeństwem.	Polityka bezpieczeństwa, jej wdrażanie są regularnie przeglądane przez Kierownika Odpowiedzialnego i kadrę kierowniczą wyższego szczebla. Zaangażowanie organizacji w bezpieczeństwo dotyczy interakcji z kluczowymi interesariuszami zewnętrznymi. Wewnętrzny system zgłaszania kwestii związanych z bezpieczeństwem/informacji bezpieczeństwa jest powszechnie znany i stosowany bez obawy przed negatywnymi konsekwencjami.
Wyniki oceny			

Czego szukać
– Kierownicy zaangażowani w działania związane z bezpieczeństwem znają kluczowe elementy polityki bezpieczeństwa i związanych z nią celów, w tym pozytywną kulturę bezpieczeństwa. – Kierownictwo wyższego szczebla zaangażowane w działania związane z bezpieczeństwem jest aktywne w obszarze systemu zarządzania (bezpieczeństwem), proaktywnego zarządzania polityką bezpieczeństwa, budowania pozytywnej kultury bezpieczeństwa i procesach ustanowionych przez organizację w celu proaktywnego zarządzania ryzykiem. – Udział kadry kierowniczej wyższego szczebla w spotkaniach, szkoleniach, konferencjach itp. dotyczących bezpieczeństwa, podczas których promowana jest pozytywna kultura bezpieczeństwa, powinien być udowodniony. – Należy znaleźć dowody na proaktywne zachowania kierowników zaangażowanych w działania związane z bezpieczeństwem oraz wykazać ich realne przywództwo i ciągłe doskonalenie. – Budowanie relacji z właściwymi organami i innymi kluczowymi stronami zainteresowanymi (interesariuszami) jest osiągane poprzez np. informacje zwrotne, zaufanie, wymianę informacji. – Informacje zwrotne z ankiet dotyczących bezpieczeństwa, które obejmują konkretne aspekty Just Culture potwierdza, że wewnętrzny system zgłaszania kwestii związanych z bezpieczeństwem (informacji bezpieczeństwa) jest znany i stosowany bez obawy przed negatywnymi konsekwencjami. – Zaobserwować, jak promuje się pozytywną kulturę bezpieczeństwa i Just Culture. – Dowieść, że pracownicy nie boją się zgłaszać w ramach wewnętrznego systemu zgłaszania informacji bezpieczeństwa/systemu zgłaszania zdarzeń. *Uwaga: SMICG proponuje narzędzie oceny kultury bezpieczeństwa w przemyśle lotniczym[23].*

Odpowiednie odniesienia do przepisów UE/EASA				
Operacje lotnicze	**Załoga lotnicza**	**Lotniska**	**ATM/ANS**	**Organizacja szkolenia ATC**
AMC1 ORO.GEN.200(a)(2) "System zarządzania" – (operatorzy typu complex) AMC1 ORO.GEN.200(a) (1)(2)(3)(5) "System zarządzania" punkt (e) – (operatorzy typu non-complex)	AMC1 ORA.GEN.200(a)(2) „System zarządzania" – punkt (a)(2) - (organizacje typu complex) AMC1 ORA.GEN.200(a)(1)(2)(3)(5) „System zarządzania" punkt (e) – (organizacje typu non-complex)	ADR.OR.D.005 „System zarządzania" punkt (b)(2) AMC1 ADR.OR.D.005 „System zarządzania" punkt (a)(3)	ATM/ANS.OR.B.015(a)(2) GM3 ATM/ANS.OR.B.005(a)(2) „System zarządzania; kultura bezpieczeństwa" ATS.OR.200 „System zarządzania bezpieczeństwem" (1)(i) AMC1 ATS.OR.200 (1)(i) „System zarządzania bezpieczeństwem"	AMC1 ATCO.OR.C.001(b) „System zarządzania organizacji szkoleniowych" punkt (c), (e) i (f)

[23] https://skybrary.aero/articles/industry-safety-culture-evaluation-tool-and-guidance

CAMO	PART 145	Organizacje produkujące/POA	Organizacje projektujące/DOA	Zarezerwowane
AMC1 CAMO.A.200(a)(2) „System zarządzania" punkt (a)(1) CAMO.A.202 „Wewnętrzny system zgłaszania kwestii związanych z bezpieczeństwem" oraz AMC/GM CAMO.A.300 „Charakterystyka zarządzania ciągłą zdatnością do lotu (CAME)" punkt (a) (10)	145.A.200 „System zarządzania" punkt (a)(2) AMC 1 145.A.200(a)(2) „Polityka bezpieczeństwa i jej cele" punkt (b) – powiązany z GM1 145.A.200(a)(2) punkt (b) i (c)145.A.202 „Wewnętrzny system zgłaszania kwestii związanych z bezpieczeństwem/informacji bezpieczeństwa" oraz AMC/GM	21.A.139 „System zarządzania produkcją" (c)(1) AMC1 21.A.139 (c)(1) „Polityka bezpieczeństwa i jej cele" punkt (a)(b)(c) GM1 21.A.139 (c)(1) „Polityka bezpieczeństwa"	21.A.239 'System zarządzania projektowaniem" (c)(1) AMC1 21.A.239 (c)(1) „Polityka bezpieczeństwa i jej cele" punkt (a)(b)(c) GM1 21.A.239 (c)(1) „Polityka bezpieczeństwa"	

1.1.5 Polityka bezpieczeństwa i kultura sprawiedliwego traktowania (Just Culture)

Odniesienia i tekst Załącznika 19

1.1.1 Polityka bezpieczeństwa:

d) jednoznacznie wskazuje, które rodzaje zachowań są nieakceptowalne w odniesieniu do działalności lotniczej podmiotu lotniczego oraz określa sytuacje, w których działania dyscyplinarne nie będą miały zastosowania.

Zob. Rozporządzenie (EU) 376/2014 Art. 16

Obecny	Odpowiedni	Sprawny	Skuteczny
Polityka i zasady Just Culture zostały zdefiniowane.	Polityka (przepisy) Just Culture (lub jakikolwiek inny powiązany dokument) jasno określają akceptowalne i niedopuszczalne zachowania. Zasady zapewniają, że przepisy mogą być stosowane spójnie w całej organizacji. Polityka i zasady Just Culture są zrozumiałe i wyraźnie widoczne (lub osiągalne). Proces decyzyjny związany z implementacją Just Culture jest dopasowany do wielkości organizacji (np. zaangażowania przedstawicieli personelu, związków zawodowych itp.)	Istnieją dowody na stosowanie i promowanie wśród personelu polityki Just Culture oraz wspierających ją zasad.	Polityka Just Culture jest stosowana w sposób uczciwy i konsekwentny, a ludzie obdarzają system zaufaniem. Istnieją dowody na to, że granica pomiędzy akceptowalnym, a niedopuszczalnym zachowaniem została określona w porozumieniu z przedstawicielami personelu.
Wyniki oceny			

Czego szukać

- Sprawdzić czy opracowano wytyczne i wdrożono nadzór dotyczący stosowania polityki Just Culture.
- Dowieść, kiedy po zdarzeniu zastosowano zasady Just Culture.
- Dowieść, że przy dochodzeniach dotyczących bezpieczeństwa szukano przyczyn systemowych/organizacyjnych, a nie skupiano się wyłącznie na jednostce.
- Sprawdzić, jak organizacja monitoruje wskaźniki dobrowolnego zgłaszania (voluntary reporting rates) i przejrzeć liczbę raportów bezpieczeństwa (czy jest adekwatna do skali działalności).
- Raporty/zgłoszenia uwzględniają własne błędy zgłaszającego oraz zdarzenia, w które jest on zaangażowany (zdarzenia, w których nie było „świadków").
- Przejrzeć informacje zwrotne (feedback) na temat sposobu stosowania polityki Just Culture i jej postrzegania przez pracowników.
- Przeprowadzić wywiady z przedstawicielami personelu, aby potwierdzić, że zgadzają się z polityką i zasadami kultury sprawiedliwego traktowania.
- Sprawdzić, czy pracownicy są świadomi istnienia polityki bezpieczeństwa i zasad Just Culture.
- Ew. sprawdzić zgodność z (niewiążącą prawnie) Deklaracją kultury bezpieczeństwa w lotnictwie (European Corporate Just culture declaration) i jej wdrożeniem (zob. Załącznik 3 do tego dokumentu).

Odpowiednie odniesienia do przepisów UE/EASA				
Operacje lotnicze	**Załoga lotnicza**	**Lotniska**	**ATM/ANS**	**Organizacja szkolenia ATC**
Rozp. 376/2014 Art. 16(11) AMC1 ORO.GEN.200(a)(2) "System zarządzania" – punkt (a)(4) „zasady zgłaszania zdarzeń związanych z bezpieczeństwem" – (organizacje typu complex)	Rozp. 376/2014 Art. 16(11) AMC1 ORO.GEN.200(a)(2) "System zarządzania" – punkt (a)(4) „zasady zgłaszania zdarzeń związanych z bezpieczeństwem" – (organizacje typu complex)	Rozp. 376/2014 Art. 16(11) AMC1 ORO.GEN.200(a)(2) "System zarządzania" – punkt (a)(4) „zasady zgłaszania zdarzeń związanych z bezpieczeństwem" – (organizacje typu complex)	Rozp. 376/2014 Art. 16(11) ATS.OR.200 „System zarządzania bezpieczeństwem" (1)(i) AMC1 ATS.OR.200(1)(i) „System zarządzania bezpieczeństwem" POLITYKA BAZPIECZEŃSTWA – (podmioty ATS typu complex) ATM/ANS.OR.A.065	Rozp. 376/2014 Art. 16(11) AMC1 ATCO.OR.C.001(b) „System zarządzania organizacji szkoleniowych"
CAMO	**PART 145**	**Organizacje produkujące/POA**	**Organizacje projektujące/DOA**	**Zarezerwowane**
Rozp. 376/2014 Art. 16(11) AMC1 CAMO.A.200(a)(2) „System zarządzania" punkt (b)(5) CAMO.A.202 „Wewnętrzny system zgłaszania kwestii związanych z bezpieczeństwem" oraz AMC/GM CAMO.A.300 „Charakterystyka zarządzania ciągłą zdatnością do lotu (CAME)" punkt (a) (10)	Rozp. 376/2014 Art. 16(11) 145.A.200 „System zarządzania" punkt (a)(2) AMC 1 145.A.200(a)(2) „Polityka bezpieczeństwa i jej cele" punkt (b) – powiązany z GM1 145.A.200(a)(2) punkt (b) i (c) 145.A.202 „Wewnętrzny system zgłaszania kwestii związanych z bezpieczeństwem" oraz AMC1 145.A.202	GM1 21.A.3A „System raportowania" łącznie z Rozp. 376/2014 Art. 16(11) AMC1 21.A.139 (c)(1) „Polityka bezpieczeństwa i jej cele" punkt (b) (c) GM1 21.A.139 (c)(1) „Polityka bezpieczeństwa" GM2 21.A.3A(a)(1) i (b)(1) „Wewnętrzny system zgłaszania kwestii związanych z bezpieczeństwem"	GM1 21.A.3A „System raportowania" łącznie z Rozp. 376/2014 Art. 16(11) AMC1 21.A.139 (c)(1) „Polityka bezpieczeństwa i jej cele" punkt (b) (c) GM1 21.A.139 (c)(1) „Polityka bezpieczeństwa" GM2 21.A.3A(a)(1) i (b)(1) „Wewnętrzny system zgłaszania kwestii związanych z bezpieczeństwem"	

1.1.6 Cele bezpieczeństwa

Odniesienia i tekst Załącznika 19

1.1.2 Biorąc pod uwagę swoją politykę bezpieczeństwa, podmiot lotniczy określa następujące cele bezpieczeństwa, które:

a) stanowią podstawę monitorowania i pomiaru poziomu bezpieczeństwa zgodnie z wymaganiami, o których mowa w pkt 3.1.2;
b) odzwierciedlają zaangażowanie podmiotu lotniczego w utrzymywanie lub ciągłe podnoszenie skuteczności systemu zarządzania bezpieczeństwem;
c) są upowszechnione w całej organizacji; oraz
d) są okresowo analizowane, aby zapewnić, że pozostają aktualne i odpowiednie dla podmiotu lotniczego.

Obecny	Odpowiedni	Sprawny	Skuteczny
Ustalono cele bezpieczeństwa, które są spójne z polityką bezpieczeństwa i upowszechnione/komunikowane w całej organizacji.	Cele bezpieczeństwa są istotne (i adekwatne) dla organizacji i jej działań. Monitoruje je odpowiedni poziom (wyższego) kierownictwa. Cele bezpieczeństwa są zrozumiałe i wyraźnie widoczne. Cele bezpieczeństwa są zgodne z KPBwLC i KPB, jeśli ma to zastosowanie.	Cele bezpieczeństwa są mierzone i regularnie przeglądane, są istotne (i adekwatne) oraz komunikowane w całej organizacji. Są one monitorowane przez Radę ds. Bezpieczeństwa (Safety Review Board) lub jej odpowiednik i dostosowywane w razie potrzeby.	Osiąganie celów bezpieczeństwa jest monitorowane przez wyższą kadrę kierowniczą i podejmowane są działania mające na celu zapewnienie ich osiągnięcia. Istnieją powiązane z tym procesem wskaźniki jakościowe i ilościowe. Cele bezpieczeństwa są nie tylko zgodne z KPBwLC i/lub KPB, ale są również porównywalne z celami z obszarów zagrożeń na poziomie europejskim (EPAS Vol. III[24]). Są one aktualizowane w oparciu o najnowsze dostępne informacje dotyczące bezpieczeństwa. Organizacja angażuje się w prace nad KPB. Ciągła poprawa bezpieczeństwa jest skutecznie mierzona.

[24] https://www.easa.europa.eu/en/document-library/general-publications/european-plan-aviation-safety-epas-2025

Wyniki oceny			

Czego szukać

- Ocenić, czy cele bezpieczeństwa są odpowiednie i istotne.
- Sprawdzić czy cele dotyczące bezpieczeństwa i ich realizacja są monitorowane mierzone za pomocą wskaźników jakościowych i ilościowych, takich jak SMART SPI (Safety Performance Indicator) i SPT (Safety Performance Target). Sprawdzić, czy cele bezpieczeństwa dotyczą przynajmniej „ciągłego doskonalenia".
- Sprawdzić protokoły/notatki ze spotkań Rady ds. Bezpieczeństwa (Safety Review Board) lub jej odpowiednika pod kątem sposobu monitorowania celów bezpieczeństwa.
- Określono cele, które doprowadzą do poprawy procesów, wyników i rozwoju pozytywnej kultury bezpieczeństwa.
- Ocenić, w jaki sposób cele bezpieczeństwa są komunikowane w całej organizacji. Sprawdzić, w jaki sposób te cele bezpieczeństwa, a także powiązane z nimi wskaźniki są widoczne (i osiągalne) dla wszystkich pracowników zaangażowanych w działania związane z bezpieczeństwem.
- Ocenić, czy cele bezpieczeństwa odnoszą się do odpowiedniej dokumentacji, tak jak obszary zagrożeń (profile ryzyka) sektora lotniczego, obszary zagrożeń (profile ryzyka) państwa, cele bezpieczeństwa państwa w KPBwLC i/lub KPB i/lub EPAS Tom II, zob. Sekcja 4.2 i Tom III (zob. Art. 7 lub 8 Rozporządzenia (UE) 2018/1139).
- Rozważyć cele bezpieczeństwa określone zgodnie z Art. 76 ust. 6 Rozporządzenia (UE) 2018/1139, jeśli występują.
- Ocenić, czy/w jaki sposób wynik audytu wewnętrznego i zewnętrznego wpływa na ustalenie i monitorowanie celów bezpieczeństwa.

Odpowiednie odniesienia do przepisów UE/EASA

Operacje lotnicze	Załoga lotnicza	Lotniska	ATM/ANS	Organizacja szkolenia ATC
AMC1 ORO.GEN.200(a)(2) "System zarządzania" punkt (c)(3) – (operatorzy typu complex) AMC1 ORO.GEN.200(a)(3) "System zarządzania" punkt (d)(1) – (operatorzy typu complex) AMC2 ORO.GEN.200(a)(5) „System zarządzania" punkt (a) – (operatorzy typu complex)	AMC1 ORA.GEN.200(a)(2) „System zarządzania" – punkt (c)(3) - (organizacje typu complex) AMC1 ORA.GEN.200(a)(3) „System zarządzania" punkt (d)(1) – (organizacje typu complex) AMC2 ORA.GEN.200(a)(5) „System zarządzania" punkt (a) – (organizacje typu complex)	AMC1 ADR.OR.D.005(b)(2) „System zarządzania" punkt (c)(3)	ATM/ANS.OR.B.005(a)(3) "System zarządzania" AMC2 ATM/ANS.OR.B.005(a)(3) "System zarządzania" AMC1 ATS.OR.200(1)(i) "System zarządzania bezpieczeństwem" POLITYKA BEZPIECZEŃSTWA punkt (b)(3) –podmioty ATS typu complex)	ATCO.OR.C.001 „System zarządzania organizacji szkoleniowych" AMC1 ATCO.OR.C.001(b) „System zarządzania organizacji szkoleniowych" POLITYKA BEZPIECZEŃSTWA

CAMO	PART 145	Organizacje produkujące/POA	Organizacje projektujące/DOA	Zarezerwowane
CAMO.A.200(a)(2) AMC1 CAMO.A.200(a)(2) „System zarządzania” CAMO.A.200(a)(5) i GM1 AMC1 CAMO.A.200(a)(3) „System zarządzania” Punkt (d) i (f)	145.A.200 „System zarządzania” Punkt (a) 2 AMC1 145.A.200(a)(2) „Polityka bezpieczeństwa i jej cele” punkt (d) AMC1 145.A.200(a)(3) „Kluczowe procesy zarządzania bezpieczeństwem” punkt (d) GM1 145.A.200(a)(4) „Promocja Bezpieczeństwa” punkt (b) GM1 145.A.200(a)(5) „System Zarządzania Dokumentacją” punkt (a) 145.A.70(a)(2)	21.A.139 „System zarządzania produkcją” punkt (c)(1) AMC1 21.A.139 (c)(1) „Polityka bezpieczeństwa i jej cele” punkt (d)	21.A.239 „System zarządzania projektowaniem” punkt (c)(1) AMC1 21.A.239 (c)(1) „Polityka bezpieczeństwa i jej cele” punkt (d)	

PODSUMOWANIE KOMENTARZY do 1.1. „ZAANGAŻOWANIE KIEROWNICTWA”

1.2. ODPOWIEDZIALNOŚĆ W ZAKRESIE BEZPIECZEŃSTWA (Załącznik 19, podpunkt 1.2)

1.2.1 Wyznaczenie kierownika odpowiedzialnego

Odniesienia i tekst Załącznika 19

1.2.1 Podmiot lotniczy:

a) wyznacza dyrektora odpowiedzialnego (accountable executive), który niezależnie od innych pełnionych funkcji, ma w imieniu organizacji wyłączny obowiązek i odpowiedzialność (accountability) za wdrożenie i prowadzenie skutecznego SMS.

Uwaga: w kontekście UE Dyrektor Odpowiedzialny jest określony jako Kierownik Odpowiedzialny lub w przypadku zatwierdzenia organizacji projektującej DOA (Design Organisation Approval), Szef organizacji projektującej (Head of Design Organisation).

Obecny	Odpowiedni	Sprawny	Skuteczny
Wyznaczono Kierownika Odpowiedzialnego, który ma pełen zakres odpowiedzialności (full responsibility) i ponosi ostateczną odpowiedzialność (ultimate accountability) za SMS.	Kierownik Odpowiedzialny ma kontrolę nad zasobami. W przypadku kilku zatwierdzeń wyznaczenie „Kierownika Odpowiedzialnego" będzie odzwierciedlać strukturę nadzoru bieżącego, tj. różne SMS-y w każdym z obszarów działalności lotniczej (z interfejsami) lub jeden SMS dla całej organizacji.	Kierownik Odpowiedzialny gwarantuje, że SMS jest odpowiednio wyposażony, wdrożony i utrzymywany oraz ma uprawnienia do wstrzymania operacji, jeśli wynik oceny ryzyka bezpieczeństwa jest na poziomie nieakceptowalnym. Kierownik Odpowiedzialny jest w pełni świadomy swojej roli i obowiązków w ramach SMS. Kierownik Odpowiedzialny jest dostępny dla personelu organizacji.	Kierownik Odpowiedzialny dba o to, aby działanie i wyniki SMS (SMS performance) było monitorowane, sprawdzane i ulepszane. Poza swoimi rolami i obowiązkami w SMS, Kierownik Odpowiedzialny stale promuje politykę bezpieczeństwa, standardy bezpieczeństwa i kulturę bezpieczeństwa organizacji.
Wyniki oceny			

Czego szukać

- Dowieść, że Kierownik Odpowiedzialny ma uprawnienia do zapewnienia wystarczających zasobów w celu poprawy bezpieczeństwa.
- Dowieść, że Kierownik Odpowiedzialny jest w pełni świadomy swoich ról i obowiązków w SMS.
- Sprawdzić proces podejmowania decyzji dotyczących akceptowalności (poziomów) ryzyka.
- Sprawdzić, czy działania SMS są przeprowadzane terminowo i czy SMS posiada wystarczające zasoby do sprawnego funkcjonowania.
- Dowieść przypadków wstrzymanych działań ze względu na niedopuszczalny poziom ryzyka bezpieczeństwa.
- Poszukać dowodów na to, że działania Kierownika Odpowiedzialnego są spójne z aktywnym promowaniem pozytywnej kultury bezpieczeństwa w organizacji.

Odpowiednie odniesienia do przepisów UE/EASA				
Operacje lotnicze	**Załoga lotnicza**	**Lotniska**	**ATM/ANS**	**Organizacja szkolenia ATC**
ORO.GEN.200 "System zarządzania" punkt (a)(1) ORO.GEN.210 „Wymagania dotyczące personelu" punkt (a)	ORA.GEN.200 „System zarządzania" – punkt (a)(1) ORA.GEN.210 „Wymagania odnoszące się do personelu" punkt (a)	ADR.OR.D.015 „Wymagania dotyczące personelu" punkt (a)	ATS.OR.200 „System zarządzania bezpieczeństwem" punkt (1)(ii)(iii) AMC1 ATS.OR.200(1)(ii);(iii) „System zarządzania bezpieczeństwem"	ATCO.OR.C.001 „System zarządzania organizacji szkoleniowych" punkt (a) ATCO.OR.C.010 „Wymagania odnoszące się do personelu" punkt (a)
CAMO	**PART 145**	**Organizacje produkujące/POA**	**Organizacje projektujące/DOA**	**Zarezerwowane**
CAMO.A.200(a)(1) „System zarządzania" CAMO.A.305 „Wymagania w stosunku do personelu" CAMO.A.305 „Kierownik Odpowiedzialny"	145.A.200 „System zarządzania" punkt (a)(1) 145.A.30 „Wymagania dotyczące personelu" punkt (a) (b)(ca)(cb) AMC1 145.A.30 (a) „Kierownik Odpowiedzialny"	21.A.139 „System zarządzania produkcją" punkt (b)2 and (c)(2) 21.A.145 „Zasoby" punkt (c)(1) AMC1 21.A.145(c)(1) „Kierownik Odpowiedzialny" GM1 21.A.145(c)(1) „Kierownik Odpowiedzialny"	21.A.239 „System zarządzania projektowaniem" punkt (c)(2) 21.A.245 „Zasoby" punkt (b) i (d) AMC1 21.A.245(c)(1) „Kierownik Odpowiedzialny" GM1 21.A.245(c)(1) „Kierownik Odpowiedzialny"	

1.2.2 Odpowiedzialność i obowiązki w zakresie bezpieczeństwa (Accountabilities and responsibilities)

Odniesienia i tekst Załącznika 19

1.2.2 Podmiot lotniczy:

b) wyraźnie określa zakresy odpowiedzialności (accountability) za bezpieczeństwo w całej organizacji, włącznie z bezpośrednią odpowiedzialnością za bezpieczeństwo ponoszoną przez członków kierownictwa wyższego szczebla organizacji;

c) określa obowiązki (responsibilities) wszystkich członków kierownictwa, niezależnie od innych pełnionych funkcji, oraz pracowników w odniesieniu do Poziomu Bezpieczeństwa osiąganego w ramach organizacji;

d) dokumentuje i komunikuje całej organizacji zakresy odpowiedzialności (accountability), obowiązki (responsibilities) oraz uprawnienia dotyczące bezpieczeństwa; oraz

e) określa poziomy odpowiedzialności personelu zarządzającego, posiadającego uprawnienia do podejmowania decyzji dotyczących poziomu tolerancji ryzyka bezpieczeństwa.

Uwaga (z Załącznika 19 ICAO, Dodatku 2): W kontekście niniejszego dodatku w odniesieniu do podmiotów lotniczych „odpowiedzialność" (accountability) odnosi się do „obowiązku" (obligation), którego nie można delegować, a „obowiązki" (responsibilities) odnoszą się do funkcji i działań, które mogą być delegowane.

Obecny	Odpowiedni	Sprawny	Skuteczny
Odpowiedzialność za bezpieczeństwo, uprawnienia i obowiązki są jasno określone i udokumentowane.	Zidentyfikowano kluczowe role w zakresie bezpieczeństwa w kontekście odpowiedzialności, uprawnień i obowiązków (na przykład poprzez opis stanowiska pracy, opis grupy stanowisk lub schematy organizacyjne).	Wyznaczono osoby do pełnienia kluczowych ról związanych z bezpieczeństwem; osoby te są świadome i wypełniają swoje obowiązki w zakresie bezpieczeństwa, są świadome nadanych uprawnień i odpowiedzialności oraz są zachęcane do wnoszenia wkładu w SMS.	Kierownik odpowiedzialny i kierownictwo wyższego szczebla są świadomi istotnych/znaczących ryzyk, na jakie narażona jest organizacja, a w całej organizacji wdrożone są procedury SMS, dzięki czemu bezpieczeństwo jest jednym z najwyższych priorytetów w organizacji.
Wyniki oceny			

Czego szukać

- Zadać pytania kierownikom i pracownikom o ich role i wykaz obowiązków.
- Potwierdzić świadomość kierownictwa wyższego szczebla w zakresie poziomu bezpieczeństwa (safety performance), najważniejszych ryzyk oraz celów bezpieczeństwa organizacji.
- Udowodnić, że kierownicy mają postawione cele w zakresie bezpieczeństwa (safety related performance targets).
- Poszukać aktywnego udziału kadry zarządzającej w SMS.
- Dowieść odpowiedniego łagodzenia, reagowania i własności ryzyk.
- Zdefiniowano i zastosowano poziomy zarządzania ze wskazanym upoważnieniem do podejmowania decyzji o akceptacji ryzyka.
- Akceptacja ryzyka jest powiązana z uprawnieniami (poziomem zarządzania).
- Sprawdzić, czy nie występują konflikty interesów oraz czy zostały one zidentyfikowane i są zarządzane.

Odpowiednie odniesienia do przepisów UE/EASA				
Operacje lotnicze	**Załoga lotnicza**	**Lotniska**	**ATM/ANS**	**Organizacja szkolenia ATC**
ORO.GEN.200 „System zarządzania” punkt (a)(1)	ORA.GEN.200 „System zarządzania” punkt (a)(1)	ADR.OR.D.005 „System zarządzania ” punkt (b)(1)	ATM/ANS.OR.B.005(a)(1) i (b) ATS.OR.200 „System zarządzania bezpieczeństwem” (1)(ii)	ATCO.OR.C.001 „System zarządzania organizacji szkoleniowych” punkt (a)
ORA.GEN.200 “System zarządzania” punkt (a)(1) ORO.GEN.210 „Wymagania dotyczące personelu” punkt (a) i (b)	ORA.GEN.200 „System zarządzania” punkt (a)(1) ORA.GEN.210 „Wymagania dotyczące personelu” punkt (a) i (b)	ADR.OR.D.005 „System zarządzania ” punkt (b)(1) i ADR.OR.D.015 „Wymagania dotyczące personelu” punkt (a); (b)	ATM/ANS.OR.B.005(a)(1) i ATS.OR.200(1)(ii)	ATCO.OR.C.001 „System zarządzania organizacji szkoleniowych” punkt (b) ATCO.OR.C.010 „Wymagania odnoszące się do personelu” punkt (a) i (b)
ORO.GEN.200 “System zarządzania” punkt (a)(5) AMC1 ORO.GEN.200(a)(5) AMC2 ORO.GEN.200(a)(5) (operatorzy typu complex)	ORA.GEN.200 “System zarządzania” punkt (a)(5) AMC1 ORA.GEN.200(a)(5) AMC1 ORA.GEN.200(a)(5) (organizacje typu complex)	ADR.OR.D.005 „System zarządzania ” punkt (c) AMC1 ADR.OR.D.005(c) „System zarządzania ” AMC2 ADR.OR.D.005(c) „System zarządzania ”	ATM/ANS.OR.B.005(a)(1) ATS.OR.200 „System zarządzania bezpieczeństwem” (1)(ii)	ATCO.OR.C.001 „System zarządzania organizacji szkoleniowych” punkt (e)
AMC1 ORO.GEN.200(a)(3) “System zarządzania” punkt (b)(2) – (operatorzy typu complex) AMC1 ORO.GEN.200(a) (1)(2)(3)(5) “System zarządzania” punkt (d) – (operatorzy typu non-complex)	AMC1 ORO.GEN.200(a)(3) “System zarządzania” punkt (b)(2) – (operatorzy typu complex) AMC1 ORO.GEN.200(a) (1)(2)(3)(5) “System zarządzania” punkt (d) – (organizacje typu non-complex)	AMC1 ADR.OR.D.005(b)(4) „System zarządzania ”	ATM/ANS.OR.B.005(a)(1) ATS.OR.200 „System zarządzania bezpieczeństwem” (1)(ii)	ATCO.OR.C.001 „System zarządzania organizacji szkoleniowych” punkt (a)

CAMO	PART 145	Organizacje produkujące/POA	Organizacje projektujące/DOA	Zarezerwowane
CAMO.A.200 „System zarządzania” punkt (a)(1) i (3) AMC1 CAMO.A.200 (a)(3) „System zarządzania” punkt (b)(2) CAMO.A.300 i AMC/GM CAMO.A.305 „Wymagania w stosunku do personelu” punkt (a)(5) AMC1 CAMO.A.305 „Kierownik odpowiedzialny” AMC1 CAMO.A.305(a)(4); (a)(5)	145.A.200 „System zarządzania” punkt (a)(1) AMC1 145.A.200(a)(1) „Organizacja i odpowiedzialność” 145.A.30 „Wymagania dotyczące personelu” punkt (b) (c) (ca) (cb) AMC1 145.A.30(b) „Struktura zarządzania obsługi technicznej” i GM1 AMC1 145.A.30(c) (ca) „Zarządzanie bezpieczeństwem i funkcja monitorowania zgodności” GM1 145.A.30(ca) „Kierownik ds. bezpieczeństwa” GM1 145.A.30 (cb) „Obowiązki osób nominowanych wobec Kierownika odpowiedzialnego” 145.A.70(a) punkt (3)(4) i (5)	21.A.139 „System zarządzania produkcją” punkt (c)(2) GM1 21.A.139(c) „Element zarządzania bezpieczeństwem” AMC1 21.A.139 (c)(2) „Organizacja i odpowiedzialność” Punkt GM1 21.A.139 (c)(2) „Grupa ds. działań w zakresie bezpieczeństwa (SAG)” AMC1 21.A.139(c)(3) i (4) „Kluczowe procesy zarządzania bezpieczeństwem” punkt (b) 21.A.145 „Zasoby” punkt (c) AMC1 21.A.145(c)(2) „Nominowani kierownicy”	21.A.239 „System zarządzania projektowaniem” punkt (c)(2) GM1 21.A.239(c) „Element zarządzania bezpieczeństwem” AMC1 21.A.239 (c)(2) „Organizacja i odpowiedzialność” GM1 21.A.239 (c)(2) „Grupa ds. działań w zakresie bezpieczeństwa (SAG)” AMC1 21.A.239(c)(3) i (4) „Kluczowe procesy zarządzania bezpieczeństwem” punkt (b) 21.A.245 „Zasoby” punkt (b) i (c) AMC1 21.A.245(b) „Nominowani kierownicy”	

PODSUMOWANIE KOMENTARZY do 1.2. „ODPOWIEDZIALNOŚĆ I OBOWIĄZKI W ZAKRESIE BEZPIECZEŃSTWA”

1.3.1 Wyznaczenie kluczowego personelu

Odniesienia i tekst Załącznika 19

1.3.1 Podmiot lotniczy wyznacza pełnomocnika ds. zarządzania bezpieczeństwa (safety manager) odpowiedzialnego (responsible) za wdrożenie i prowadzenie SMS.

Uwaga – W zależności od wielkości podmiotu lotniczego oraz złożoności jego produktów lub usług lotniczych, obowiązki (responsibilities) związane z wdrożeniem i prowadzeniem systemu zarządzania bezpieczeństwem mogą być przypisane jednej lub kilku osobom pełniącym rolę kierownika ds. bezpieczeństwa, jako jedyna pełniona przez nie funkcja lub w połączeniu z innymi zadaniami, pod warunkiem, że nie powodują one konfliktu interesów.

Obecny	Odpowiedni	Sprawny	Skuteczny
Wyznaczono kierownika ds. bezpieczeństwa odpowiedzialnego za wdrożenie i utrzymanie SMS, bezpośrednio podlegającego Kierownikowi Odpowiedzialnemu.	Kierownik ds. bezpieczeństwa jest kompetentny. Na utrzymanie SMS poświęcono wystarczającą ilość czasu i zasobów, ale bez ograniczenia się do kompetentnego personelu zajmującego się analizami bezpieczeństwa, audytami i promocją bezpieczeństwa. *Zob. uwaga powyżej dot. Zał. 19.* *Zob. Sekcja 1.3.2*	Kierownik ds. bezpieczeństwa wdrożył i utrzymuje SMS. Kierownik ds. bezpieczeństwa (Safety Manager) regularnie kontaktuje się z Kierownikiem Odpowiedzialnym (Accountable Manager) i - jeśli to odpowiednie - eskaluje kwestie dotyczące bezpieczeństwa. Kierownik ds. bezpieczeństwa jest dostępny dla personelu organizacji.	Kierownik ds. bezpieczeństwa posiada kompetencje do zarządzania systemem SMS oraz identyfikuje we właściwym czasie możliwe ulepszenia. Istnieje ścisły związek zawodowy pomiędzy Kierownikiem Odpowiedzialnym, a Kierownikiem ds. bezpieczeństwa – w celu terminowego i regularnego składania raportów na temat kwestii związanych z bezpieczeństwem.
Wyniki oceny			

Czego szukać

- Rozważyć, czy odpowiedzialność za wdrożenie i utrzymanie SMS powinna zostać powierzona jednej osobie zatrudnionej na pełen etat, czy kierownikowi ds. bezpieczeństwa wspieranemu przez zespół, posiadającym wystarczające uprawnienia, aby opowiadać się za bezpieczeństwem w przypadku konfliktu interesów.
- Sprawdzić dostępność kierownika ds. bezpieczeństwa (i personelu pomocniczego, jeśli to konieczne), aby zweryfikować, czy ma wystarczającą ilość czasu na wdrożenie i utrzymanie SMS.
- Sprawdzić, czy nie występują konflikty interesów oraz czy zostały one zidentyfikowane i są zarządzane.
- Dokonać przeglądu roli kierownika ds. bezpieczeństwa, w tym wiarygodności, kompetencji i statusu.
- Dokonać przeglądu szkolenia, które przeszedł kierownik ds. bezpieczeństwa.
- Dowieść utrzymywania kompetencji.
- Sprawdzić, w jaki sposób kierownik ds. bezpieczeństwa uzyskuje dostęp do wewnętrznych i zewnętrznych informacji dotyczących bezpieczeństwa.
- Przejrzeć sposoby, w jakie kierownik ds. bezpieczeństwa komunikuje się i współpracuje z personelem operacyjnym i wyższą kadrą kierowniczą.
- Przejrzeć obciążenie pracą kierownika ds. bezpieczeństwa/przydzielony czas na pełnienie roli.

- Sprawdzić, czy w odpowiednim czasie dostępne są wystarczające zasoby do działań w ramach SMS, takich jak: badania i ankiety dotyczące bezpieczeństwa, analizy, oceny, udział w spotkaniach dotyczących bezpieczeństwa, spójność wdrożenia SMS (zwłaszcza w zakresie oceny ryzyka i środków łagodzących), okresowe raporty na temat poziomu bezpieczeństwa, procesy komunikacji obejmujące identyfikację i rozpowszechnianie informacji związanych z bezpieczeństwem (wewnętrznie i zewnętrznie) oraz promocja bezpieczeństwa.
- W przypadku organizacji posiadających wiele certyfikatów kierownik odpowiedzialny może wyznaczyć jeden punkt kontaktowy (focal point), tj. „kierownika ds. bezpieczeństwa".
- Przejrzeć działania po analizie bezpieczeństwa (safety report action) i terminy realizacji tych działań.
- Przeprowadzić wywiad z Kierownikiem Odpowiedzialnym i Kierownikiem ds. bezpieczeństwa.

Odpowiednie odniesienia do przepisów UE/EASA				
Operacje lotnicze	**Załoga lotnicza**	**Lotniska**	**ATM/ANS**	**Organizacja szkolenia ATC**
ORO.GEN.210 „Wymagania dotyczące personelu" punkt (b) AMC1 ORO.GEN.200(a)(1) "System zarządzania" punkt (a)(1) – (operatorzy typu complex) AMC1 ORO.GEN.200(a)(1);(2);(3);(5) "System zarządzania" punkt (c) – (operatorzy typu non-complex) AMC1 ORO.AOC.130 „Monitorowanie parametrów lotu - samoloty" punkt (a)	ORO.GEN.210 „Wymagania dotyczące personelu" punkt (b) AMC1 ORA.GEN.200(a)(1) "System zarządzania" punkt (a)(1) – (organizacje typu complex) AMC1 ORA.GEN.200(a) (1)(2)(3)(5) "System zarządzania" punkt (c) – (organizacje typu non-complex)	ADR.OR.D.015 „Wymagania wobec personelu" punkt (c) AMC1 ADR.OR.D.015 „Wymagania wobec personelu"	ATS.OR.200(1)(iii)	ATCO.OR.C.010 „Wymagania odnoszące się do personelu"
CAMO	**PART 145**	**Organizacje produkujące/POA**	**Organizacje projektujące/DOA**	**Zarezerwowane**
AMC1 CAMO.A.200(a)(1) „Organizacja i odpowiedzialność" CAMO.A.300 „Charakterystyka zarządzania ciągłą zdatnością do lotu (CAME)" punkt (a)(5) CAMO.A.305 „Wymagania w stosunku do personelu" punkt (a)(4) i (5) AMC1 CAMO.A.305 (a)(4); (a)(5) „Zarządzanie bezpieczeństwem" i „Kierownik ds. bezpieczeństwa" punkt (a) GM1 CAMO.A.305 „Kierownik ds. bezpieczeństwa" GM3 CAMO.A.305(g) „Kompetencje kierownika ds. bezpieczeństwa" AMC1 CAMO.A.200(a)(1) „Organizacja i odpowiedzialność"	145.A.2'0 „System zarządzania" punkt (a)(1) AMC1 145.A.200(a)(1) „Organizacja i odpowiedzialność" 145.A.'0 „Wymagania dotyczące personelu" punkt (b), (ca), (cb) i (cc) AMC1 145.A.30(c);(ca) „Zarządzanie bezpieczeństwem i funkcja monitorowania zgodności" GM1 145.A.30(ca) „Kierownik ds. bezpieczeństwa" GM4 145.A.30(e) „Kompetencje Kierownika ds. Bezpieczeństwa"	21.A.139 „System zarządzania produkcją" punkt (c)(2) 21.A.145 „Zasoby" punkt (c) AMC1 21.A.145 (c)(2) „Nominowani kierownicy" punkt (j) i (k) AMC2 21.A.145 (c)(2) „Kompetencje personelu zarządzającego" punkt (d)	21.A.239 „System zarządzania projektowaniem" punkt (c)(2) 21.A.245 „Zasoby" AMC1 21.A.245 (b) „Nominowani kierownicy" punkt (g) AMC1 21.A.245 (d) „Kompetencje personelu zarządzającego" punkt (e)	

1.3.2 Wyznaczenie kluczowego personelu dla organizacji typu complex

Odniesienia i tekst Załącznika 19

1.3.2 System zarządzania w organizacjach typu complex (zob. odniesienia do przepisów poniżej)

Obecny	Odpowiedni	Sprawny	Skuteczny
Organizacja powołała odpowiedni(e) komitet(y) ds. bezpieczeństwa (np. SRB – Safety Review Board)	Struktura oraz częstotliwość spotkań komitetu(-ów) ds. bezpieczeństwa wspierają funkcje SMS w całej organizacji. Zakres kompetencji komitetów ds. bezpieczeństwa obejmuje zarówno zagrożenia bezpieczeństwa, jak i kwestie zgodności. W skład komitetu ds. bezpieczeństwa najwyższego szczebla wchodzi co najmniej Kierownik Odpowiedzialny i kierownicy obszarów funkcjonalnych.	Istnieją dowody spotkań zawierające szczegółowe dane na temat uczestnictwa, dyskusji i działań. Komitet(y) ds. bezpieczeństwa monitoruje (-ją) skuteczność funkcji monitorowania zgodności SMS poprzez sprawdzenie czy zasoby są wystarczalne. Działania są monitorowane. Ustanowiono środki jakościowe/ilościowe do pomiaru i monitorowania ustalonych celów w zakresie bezpieczeństwa.	W skład komitetu(ów) ds. bezpieczeństwa wchodzą kluczowi interesariusze. Wyniki spotkań są dokumentowane i komunikowane, a wszystkie działania są uzgadniane, podejmowane i monitorowane (followed up) w odpowiednim czasie. Wyniki (wydajność) i cele w zakresie bezpieczeństwa są poddawane przeglądom i podejmowane są odpowiednie działania.
Wyniki oceny			

Czego szukać

- Sprawdzić komitet ds. bezpieczeństwa i strukturę spotkań oraz zasady funkcjonowania dla każdego komitetu/spotkania.
- Sprawdzić poziom frekwencji na spotkaniach.
- Przejrzeć zapis spotkań i działań.
- Wyniki są komunikowane reszcie organizacji.
- Dowody dotyczące celów bezpieczeństwa, poziomu bezpieczeństwa i zgodności są przeglądane i omawiane na spotkaniach.
- Uczestnicy kwestionują to, co jest przedstawiane, gdy istnieją ograniczone dowody.
- Kierownictwo wyższego szczebla jest świadome najważniejszych ryzyk stojących przed organizacją i ogólnego poziomu bezpieczeństwa (safety performance) organizacji.
- System Zarządzania może być zintegrowany dla organizacji posiadających wiele certyfikatów.

Odpowiednie odniesienia do przepisów UE/EASA

Operacje lotnicze	Załoga lotnicza	Lotniska	ATM/ANS	Organizacja szkolenia ATC
AMC1 ORO.GEN.200(a)(1) „System zarządzania” punkt (b)(c) i (d)	AMC1 ORA.GEN.200(a)(1) „System zarządzania” punkt (b)(c) i (d)	AMC1 ADR.OR.D.005(b)(1) „System zarządzania”	Uwaga: podmiot zapewniający służby ruchu lotniczego należy uważać za complex, chyba że kwalifikuje się do ubiegania się o certyfikat o ograniczonym zakresie i spełnia kryteria określone w	Nie dotyczy

			ATM/ANS.OR.A.010(a). AMC1 ATS.OR.200(1)(i) „System zarządzania bezpieczeństwem” AMC1 ATS.OR.200(1)(ii) „System zarządzania bezpieczeństwem ODPOWIEDZIALNOŚĆ” – (podmioty ATS typu complex) AMC2 ATS.OR.200(1)(ii);(iii) „System zarządzania bezpieczeństwem” ORGANIZACJA I ODPOWIEDZIALNOŚĆ – (podmioty ATS typu complex)	
CAMO	**PART 145**	**Organizacje produkujące/POA**	**Organizacje projektujące/DOA**	**Zarezerwowane**
Koncepcja „organizacji typu complex” nie ma zastosowania dla części CAMO; ale odpowiedniość (suitability) jest definiowana przez: CAMO.A.200 (b) CAMO.A.200 „System zarządzania ” i AMC/GM AMC1 CAMO.A.200(a)(1) dotyczy również GM1 CAMO.A.200(a)(1)	Koncepcja „organizacji typu complex” nie ma zastosowania dla Part – 145; Zob. 145.A.200 „System zarządzania” punkt (b) AMC1 145.A.200(a)(1) ma zastosowanie również GM1 145.A.200(a)(1)	Koncepcja „organizacji typu complex” nie ma zastosowania dla Part-21; Zob. 21.A.139 „System zarządzania produkcją” punkt b) 1 GM1 21.A.139(c)(2) „Grupa ds. działań w zakresie Bezpieczeństwa (SAG)”	Koncepcja „organizacji typu complex” nie ma zastosowania dla Part-21; Zob. 21.A.239 „System zarządzania projektowaniem” punkt (b) GM 21.A.239(c)(2) „Grupa ds. działań w zakresie Bezpieczeństwa (SAG)”	

PODSUMOWANIE KOMENTARZY do 1.3. „WYZNACZENIE PERSONELU KLUCZOWEGO”

1.4 Koordynacja planowania reagowania awaryjnego (ERP)

Odniesienia i tekst Załącznika 19

1.4.1 Podmiot lotniczy zobowiązany jest do ustanowienia i zapewnienia funkcjonowania planu reagowania kryzysowego/awaryjnego dotyczącego przypadków zaistnienia wypadków i incydentów w operacjach statków powietrznych i innych lotniczych sytuacjach kryzysowych/awaryjnych oraz zapewnia prawidłową koordynację planu reagowania kryzysowego/awaryjnego z planami reagowania kryzysowego/awaryjnego tych organizacji, z którymi musi współpracować podczas dostarczania swoich produktów i usług.

Obecny	Odpowiedni	Sprawny	Skuteczny
Opracowano i rozpowszechniono odpowiedni, skoordynowany ERP, który definiuje procedury, role, obowiązki i działania różnych organizacji i kluczowego personelu.	Kluczowy personel ma przez cały czas łatwy dostęp do odpowiednich części ERP. ERP definiuje procedury, role, obowiązki i działania różnych organizacji i personelu kluczowego. Określono częstotliwość i metody testowania ERP są zdefiniowane, w tym koordynacja z innymi organizacjami (w tym organizacjami nielotniczymi).	System ERP jest sprawdzany i testowany, aby zapewnić jego aktualność i adekwatność. Stosowane są różne scenariusze oraz podejmowane są działania mające na celu poprawę efektywności procedur ERP.	Istnieją dowody na koordynację z innymi organizacjami poprzez regularne symulacje zagrożeń lub ćwiczenia kryzysowe, które są analizowane pod kątem dalszej poprawy.
Wyniki oceny			

Czego szukać

Uwaga: Zgodnie z przepisami EASA, ERP jest wymagany tylko dla operatorów lotniczych, Służb ANS/ATS i Lotnisk; należy jednakże odpowiednio rozważyć koordynację ich ERP w relacjach (interfejsach) z innymi.

- Sprawdzić, czy podmiot lotniczy jest zobowiązany do posiadania ERP lub do koordynowania działania z systemem ERP innej organizacji, w zależności od obszaru działalności.
- Przejrzeć plan reagowania kryzysowego oraz sposób, w jaki zdefiniowano procedury, role, obowiązki i działania różnych organizacji. Przejrzeć, jak planowana jest koordynacja z innymi organizacjami (w tym organizacjami nielotniczymi).
- Sprawdzić jak plan reagowania kryzysowego jest dystrybuowany i gdzie przechowywane są kopie.
- Przeprowadzić wywiad z personelem kluczowym i sprawdzić, czy ma on dostęp do odpowiednich części ERP.
- Sprawdzić, czy wzięto pod uwagę różne rodzaje przewidywalnych sytuacji awaryjnych.
- Sprawdzić jak zdefiniowano częstotliwość i metody ćwiczenia ERP.
- Sprawdzić, kiedy plan był ostatnio przeglądany, ćwiczony oraz kiedy podjęto działania.
- Zweryfikować, czy regularnie rozważane są różne scenariusze mające na celu sprawdzenie niezawodności istniejącego ERP.

Odpowiednie odniesienia do przepisów UE/EASA				
Operacje lotnicze	**Załoga lotnicza**	**Lotniska**	**ATM/ANS**	**Organizacja szkolenia ATC**
ORO.GEN.200 „System zarządzania” punkt (a)(3) AMC1 ORO.GEN.200(a)(3) „System zarządzania” punkt (g) – (operatorzy typu complex) AMC1 ORO.GEN.200(a) (1)(2)(3)(5) „System zarządzania” punkt (f) – (operatorzy typu non - complex)	ORA.GEN.200 „System zarządzania” punkt (a)(3) AMC1.ORA.GEN.200(a)(3) „System zarządzania” punkt (g) – (organizacje typu complex) AMC1 ORA.GEN.200(a) (1)(2)(3)(5) „System zarządzania” punkt (f) – (organizacje typu non-complex)	ADR.OR.D.005 „System zarządzania” punkt (b)(10) AMC1 ADR.OR.D.005(b)(10) „System zarządzania”	ATS.OR.200(1)(iv) AMC1 ATS.OR.200(1)(iv) „System zarządzania bezpieczeństwem” AMC1 ATS.OR.200(1)(iv) „System zarządzania bezpieczeństwem KOORDYNACJA PLANOWANIA REAGOWANIA AWARYJNEGO DLA PODMIOTÓW ATS” – (podmioty ATS typu complex)	Nie dotyczy (obowiązują regulacje ANSP ERP)
CAMO	**PART 145**	**Organizacje produkujące/POA**	**Organizacje projektujące/DOA**	**Zarezerwowane**
AMC1 CAMO.A.200(a)(3) punkt (g) „Natychmiastowe działanie w zakresie bezpieczeństwa i koordynacja z planem reagowania awaryjnego (ERP) podmiotu”	145.A.155 „Natychmiastowa reakcja na problem z obszaru bezpieczeństwa” AMC1 145.A.200(a)(3) „Kluczowe procesy zarządzania bezpieczeństwem” punkt (g)	Koncepcja ERP nie ma zastosowania do Part21	Koncepcja ERP nie ma zastosowania do Part21; 21.A.3 „System raportowania” punkt (d) AMC1 21.A.3A(a)(3), 21.A.3A(b)(3), 21.A.3A(d)	

PODSUMOWANIE KOMENTARZY do 1.4. „KOORDYNACJA PLANOWANIA REAGOWANIA AWARYJNEGO”

1.5.1 Dokumentacja SMS

Odniesienia i tekst Załącznika 19

1.5.1 Podmiot lotniczy opracowuje i prowadzi podręcznik systemu zarządzania bezpieczeństwem, który opisuje:

a) politykę i cele bezpieczeństwa;
b) wymagania dotyczące SMS;
c) procesy i procedury SMS; oraz
d) odpowiedzialność (accountability), obowiązki (responsibilities) oraz uprawnienia decyzyjne w zakresie procesów i procedur SMS.

Obecny	Odpowiedni	Sprawny	Skuteczny
Dokumentacja SMS zawiera zasady i procesy opisujące SMS i procesy organizacji.	Zakres działań w ramach SMS jest jasno określony. Dokumentacja SMS jest zrozumiała. Dokumentacja SMS jest spójna z innymi wewnętrznymi systemami zarządzania i oddaje aktualność stosowanych procesów. Sposób i format dokumentacji SMS jest odpowiedni dla organizacji i łatwo dostępny dla całego odpowiedniego personelu. *Zob. Załącznik 19 Uwaga: W zależności od wielkości podmiotu lotniczego i złożoności jego produktów lub usług lotniczych, podręcznik SMS i dokumentacja operacyjna SMS mogą mieć formę samodzielnych dokumentów lub mogą być zintegrowane z innymi dokumentami organizacyjnymi (lub dokumentacją) prowadzonymi przez podmiot lotniczy.*	Prowadzone są zmiany w dokumentacji SMS. Kluczowy personel zaangażowany we wdrażanie SMS zna i przestrzega odpowiednich części dokumentacji SMS, natomiast pracownicy znają treść dokumentacji SMS odpowiednią do ich zakresu zadań.	Dokumentacja SMS jest proaktywnie sprawdzana pod kątem ciągłego udoskonalania.
Wyniki oceny			

Czego szukać
– Przejrzeć dokumentację SMS i procedury zmian. – Sprawdzić sposób i format dokumentacji SMS, w zależności od wielkości, struktury organizacji, jej modelu biznesowego, takiego jak wielkość i znaczenie zleconych działań (od i do). – Sprawdzić, czy nie ma odniesień do innych dokumentów i procedur. – Sprawdzić dostępność dokumentacji SMS dla wszystkich pracowników. – Sprawdzić, czy pracownicy wiedzą z kim się kontaktować (w razie potrzeby) lub gdzie znaleźć dokumentację związaną z bezpieczeństwem, w tym procedury odpowiednie do ich roli w systemie. – Przejrzeć dokumentację uzupełniającą SMS (rejestry zagrożeń, protokoły/notatki ze spotkań, raporty dotyczące poziomu bezpieczeństwa, oceny ryzyka itp.). – W przypadku gdy kilku operatorów tworzących część jednej grupy biznesowej przewoźnika lotniczego korzysta z tego samego CAMO w celu zapewnienia ciągłej zdatności do lotu wszystkich obsługiwanych przez siebie statków powietrznych (AMC3 CAMO.A.300) należy sprawdzić, w jaki sposób wdrażane są potencjalne, szczegółowe wymagania i procedury dla różnych operatorów.

Odpowiednie odniesienia do przepisów UE/EASA				
Operacje lotnicze	**Załoga lotnicza**	**Lotniska**	**ATM/ANS**	**Organizacja szkolenia ATC**
AMC1 ORO.GEN.200(a)(5) „System zarządzania” punkt (a) AMC2 ORO.GEN.200(a)(5) –(operatorzy typu complex)	ORA.GEN.200 „System zarządzania” punkt (a)(5) AMC1 ORA.GEN.200(a)(5) „System zarządzania” punkt (a) AMC1 ORA.GEN.200(a)(5) – (organizacje typu complex)	ADR.OR.D.005 „System zarządzania” punkt (c) AMC1 ADR.OR.D.005(c) „System zarządzania” AMC2 ADR.OR.D.005(c) „System zarządzania”	ATM/ANS.OR.B.005(b) AMC1 ATM/ANS.OR.B.005(b) „System zarządzania” i Zał. IV ATS.OR.200(1)(v) AMC1 ATS.OR.200(1)(v) „System zarządzania bezpieczeństwem”	AMC1 ATCO.OR.C.001(e) „System zarządzania organizacji szkoleniowych” punkt (e)(8)

CAMO	PART 145	Organizacje produkujące/POA	Organizacje projektujące/DOA	Zarezerwowane
CAMO.A.200(a)(5) „System zarządzania” GM1 CAMO.A.200(a)(5) „Dokumentacja systemu zarządzania” CAMO.A.300 ‘CAME’ i AMC1 CAMO.A.300 CAMO.A.200(a)(5) i GM1 CAMO.A.200(a)(5) „Dokumentacja systemu zarządzania” AMC3 CAMO.A.300 w przypadku kilku operatorów tworzących część jednej grupy biznesowej przewoźnika lotniczego korzystających z tego samego CAMO w celu zapewnienia ciągłej zdatności do lotu wszystkich obsługiwanych przez siebie statków powietrznych.	145.A.200 „System zarządzania” punkt (a)(5) GM1 145.A.200(a)(5) „Dokumentacja systemu zarządzania” 145.A.70 „Charakterystyka organizacji obsługowej (MOE)” AMC 1 145.A.70 „Charakterystyka organizacji obsługowej (MOE)”	21.A.143 „Charakterystyka organizacji produkującej (POE)” GM1 21.A.143 „POE” AMC1 21.A.143 (a)(1) „Zawartość POE”	21.A.243 Podręcznik AMC1 21.A.243(a) Podręcznik AMC2 21.A.243(a) „Typowa treść podręcznika…/…”	

PODSUMOWANIE KOMENTARZY do 1.5. „DOKUMENTACJA SMS”

1.5.2 Dokumentacja operacyjna SMS

Odniesienia i tekst Załącznika 19

1.5.2 Podmiot lotniczy opracowuje i prowadzi dokumentację operacyjną SMS stanowiącą część dokumentacji SMS

Uwaga: W zależności od wielkości podmiotu lotniczego oraz złożoności jego produktów lub usług lotniczych, podręcznik i dokumentacja operacyjna SMS mogą być opracowane w formie samodzielnych dokumentów lub mogą być zintegrowane z innymi dokumentami (lub dokumentacją) organizacji prowadzonymi przez podmiot lotniczy.

Obecny	Odpowiedni	Sprawny	Skuteczny
Dokumentacja SMS definiuje dane wyjściowe SMS (SMS outputs) oraz dokumentację działalności operacyjnej SMS (records of SMS activities), które będą przechowywane. Określono dokumentację, która ma być przechowywana, okres przechowywania i lokalizację.	Określono zasady ochrony oraz poufność danych.	Działalność SMS (SMS activities) jest odpowiednio gromadzona i uznana za kompletną oraz zgodną z właściwymi zasadami ochrony danych i kontroli poufności.	Dokumentacja operacyjna SMS jest rutynowo wykorzystywana jako dane wejściowe (inputs) dla zadań związanych z zarządzaniem bezpieczeństwem i ciągłym doskonaleniem SMS. Dokumentacja SMS, w tym powiązana dokumentacja operacyjna SMS, jest regularnie przeglądana i aktualizowana przy zastosowaniu odpowiedniej kontroli wersji.
Wyniki oceny			

Czego szukać

- Sprawdzić jak przechowywane są dane dotyczące bezpieczeństwa i jak kontrolowana jest ich aktualność/wersja.
- Zasady ochrony danych i poufności zostały zdefiniowane i są konsekwentnie stosowane.
- Sprawdzić, czy odpowiedni personel jest świadomy procesów i procedur kontroli dokumentacji.
- Sprawdzić, czy przechowywana dokumentacja operacyjna SMS zawiera decyzje podjęte przez Radę ds. Bezpieczeństwa (Safety Review Board) lub jakąkolwiek inną komisję ds. bezpieczeństwa wysokiego szczebla i jest to poparte dowodami.

Odpowiednie odniesienia do przepisów UE/EASA				
Operacje lotnicze	**Załoga lotnicza**	**Lotniska**	**ATM/ANS**	**Organizacja szkolenia ATC**
ORO.GEN.220 „Prowadzenie dokumentacji” AMC1 ORO.GEN.220(b) „Prowadzenie dokumentacji” AMC1 ORO.AOC.130 „Monitorowanie parametrów lotu - samoloty” punkt (k)	ORA.GEN.220 „Prowadzenie dokumentacji” AMC1 ORA.GEN.220(b) „Prowadzenie dokumentacji”	ADR.OR.D.035 „Prowadzenie dokumentacji” AMC1 ADR.OR.D.035 „Prowadzenie dokumentacji” AMC2 ADR.OR.D.035 „Prowadzenie dokumentacji”	ATM/ANS.OR.B.030 „Prowadzenie dokumentacji” ATS.OR.200(1)(v) AMC2 ATS.OR.200(1)(v) „System zarządzania bezpieczeństwem”	ATCO.OR.C.020 „Prowadzenie dokumentacji” AMC1 ATCO.OR.C.020(a);(b) „Prowadzenie dokumentacji”
CAMO	**PART 145**	**Organizacje produkujące/POA**	**Organizacje projektujące/DOA**	**Zarezerwowane**
CAMO.A.220 „Prowadzenie dokumentacji” punkt (b) AMC1 CAMO.A.220 „Przechowywanie dokumentacji - ogólne wytyczne”	145.A.55 „Prowadzenie dokumentacji” punkt (c) AMC1 145.A.55 „Przechowywanie dokumentacji – ogólne wytyczne”			

PODSUMOWANIE KOMENTARZY do „DOKUMENTACJA OPERACYJNA SMS”

2 OCENA RYZYKA BEZPIECZEŃSTWA

2.1.1 Identyfikacja zagrożeń

2.1.1 Podmiot lotniczy opracowuje i zapewnia funkcjonowanie procesu identyfikacji zagrożeń występujących w związku z oferowanymi produktami lub usługami lotniczymi.

Identyfikacja zagrożeń opiera się na kombinacji metod reaktywnych i proaktywnych.

Obecny	Odpowiedni	Sprawny	Skuteczny
Istnieje proces określający, w jaki sposób zagrożenia są identyfikowane metodami reaktywnymi i proaktywnymi, z wykorzystaniem wielu źródeł. Metodologia definiowania kryteriów badania (zdarzeń) bezpieczeństwa jest udokumentowana. Proces obejmuje zarządzanie zmianą organizacyjną, gdy ma ona wpływ na bezpieczeństwo (zob.3.2).	Rozważa się i poddaje przeglądowi wiele źródeł zagrożeń (wewnętrznych i zewnętrznych), stosownie do potrzeb danej dziedziny (lotnictwa). Powiązania (interfejsy) są odpowiednio wskazane. Zagrożenia są dokumentowane w łatwej do zrozumienia formie. Zasady formalnego zakańczania badań (zdarzeń) bezpieczeństwa są określone i dopasowane do poziomu ryzyka. W stosownych przypadkach zagrożenia bezpieczeństwa na poziomie organizacji są zgodne z zagrożeniami zidentyfikowanymi na poziomie władzy.	Zagrożenia są identyfikowane i dokumentowane. Rozważane są zagrożenia powiązane z czynnikami technicznymi, ludzkimi i organizacyjnymi. Zidentyfikowano i zastosowano kryteria badań (zdarzeń) bezpieczeństwa. Prowadzane i rejestrowane są badania (zdarzeń) bezpieczeństwa.	Organizacja posiada procesy i środki identyfikujące zagrożenia (związane z czynnikami technicznymi, środowiskowymi, ludzkimi i organizacyjnymi), które są utrzymywane i przeglądane w celu zapewnienia ich aktualności. Organizacja bezustannie i proaktywnie identyfikuje zagrożenia (związane z czynnikami technicznymi, środowiskowymi, ludzkimi i organizacyjnymi) związane z jej działalnością i środowiskiem operacyjnym, angażując cały kluczowy personel i odpowiednich interesariuszy. Zagrożenia są oceniane w sposób systematyczny i terminowy. Personel wyraża zaufanie do polityki i procesów raportowania organizacji. Kryteria badania (zdarzeń) bezpieczeństwa są stale aktualizowane, aby w razie potrzeby uwzględnić źródła wewnętrzne i zewnętrzne.
Wyniki oceny			

Czego szukać

- Przejrzeć, w jaki sposób zagrożenia są identyfikowane, analizowane, jak się nimi zajęto i jak są rejestrowane.
- Przejrzeć strukturę i układ rejestru zagrożeń.
- Rozważyć zagrożenia związane z:
  - możliwymi scenariuszami wypadków lub poważnych incydentów,

- czynnikami technicznymi oraz czynnikami ludzkimi i organizacyjnymi (np. zagrożenia związane z wydolnością człowieka i wydajnością organizacji w ramach zarządzania ryzykiem systemowym – proszę wziąć pod uwagę Doc. ICAO 10151 „Podręcznik dotyczący wydolności człowieka dla organów regulacyjnych” (Manual on Human Performance for Regulators)),
- decyzjami i procesami biznesowymi,
- organizacjami zewnętrznymi (tzw. trzecimi stronami).

– Sprawdzić, jakie wewnętrzne i zewnętrzne źródła informacji o zagrożeniach są brane pod uwagę -np: raporty bezpieczeństwa/automatyczne gromadzenie danych (takie jak monitorowanie parametrów lotu – FDM/FDA, ATS/ANS, system monitorowania stanu zdrowia), audyty, ankiety i/lub opracowania/analizy bezpieczeństwa, badania zdarzeń, inspekcje, burze mózgów, działania w ramach zarządzania zmianą, ochrona, cyberbezpieczeństwo, kryzysy sanitarne, wpływy środowiskowe, handlowe i inne; analizy monitorowania zgodności z przepisami; profil ryzyk sektorowych itp.
– Sprawdzić, czy identyfikacja zagrożeń bezpieczeństwa uwzględnia te zidentyfikowane na poziomie Władzy Lotniczej np. relacje (interfejsy) KPBwLC/SMS i KPB zgodnie z art. 7 i 8 Rozporządzenia (UE) 2018/1139, ryzyka bezpieczeństwa określone na poziomie państwa lub obszary zagrożeń (profile ryzyk) państwa (np. portfolio Problemów Bezpieczeństwa określonych na poziomie państwa), w EPAS, w Rocznym Przeglądzie Bezpieczeństwa EASA (Annual Safety Review) i Sprawozdaniu o stanie bezpieczeństwa w Lotnictwie Cywilnym), Rocznym Przeglądzie Zaleceń Bezpieczeństwa EASA (https://www.easa.europa.eu/en/document-library/general-publications/annual-safety-recommendations-review-2024) czy określonych w ASR uznanych organizacji międzynarodowych (tj. IATA, CANSO - Civil Air Navigation Services Organisation); czy w ramach celów bezpieczeństwa określonych zgodnie z art. 76.6 Rozporządzenia (UE) 2018/1139), w SIB;
– Badania zdarzeń w zakresie bezpieczeństwa ustalają czynniki przyczynowe/czynniki sprzyjające zajściu zdarzenia (dlaczego tak się stało, a nie tylko co się wydarzyło) oraz identyfikują sprzyjające czynniki ludzkie i organizacyjne.
– Ocenić, w jakim stopniu proces nie ogranicza się do części reaktywnej (tj. zdarzeń), ale uwzględnia także podejście proaktywne (jak zaproponowano powyżej).
– Sprawdzić w jaki sposób zagrożenia zidentyfikowane w ramach analizy zdarzeń są przetwarzane zgodnie z art. 4 i 5 Rozporządzenia (UE) 376/2014 (zob. następną część).
– Czy zachęca się pracowników do zgłaszania błędów lub sytuacji potencjalnie wypadkowych (near misses) za pośrednictwem systemu zgłaszania zapewniającego odpowiednią ochronę zgłaszającego?
– Czy ustanowiony został mechanizm dokumentowania rejestru zagrożeń w sposób umożliwiający jego ewolucję z upływem czasu? Czy rejestr zagrożeń jest poddawany okresowym przeglądom?

Odpowiednie odniesienia do przepisów UE/EASA				
Operacje lotnicze	**Załoga lotnicza**	**Lotniska**	**ATM/ANS**	**Organizacja szkolenia ATC**
ORO.GEN.200 „System zarządzania” punkt (a)(3) AMC1 ORO.GEN.200(a)(3) “System zarządzania” punkt (a)(1) – (operatorzy typu complex) AMC1 ORO.GEN.200(a) (1);(2);(3);(5) “System zarządzania” punkt (a), (b) i (d) – (operatorzy typu non-complex) AMC1 ORO.AOC.130 „Monitorowanie parametrów lotu - samoloty” punkt (b)	ORA.GEN.200 „System zarządzania” punkt (a)(3) AMC1 ORA.GEN.200(a)(3) “System zarządzania” punkt (a)(1) – (organizacje typu complex) AMC1 ORA.GEN.200(a) (1);(2);(3);(5) „”System zarządzania” punkt (a), (b) i (d) – (organizacje typu non-complex)	ADR.OR.D.005 „System zarządzania” punkt (b)(3) AMC1 ADR.OR.D.005(b)(3) „System zarządzania”	ATM/ANS.OR.B.005(a)(5) „System zarządzania” ATS.OR.200(2)(i) „System zarządzania bezpieczeństwem” AMC1 ATS.OR.205(b)(1) „Ocena bezpieczeństwa i zapewnienie zmian w systemie funkcjonalnym KOMPLETNOŚĆ IDENTYFIKACJI ZAGROŻEŃ” AMC2 ATS.OR.205(b)(1) „Ocena bezpieczeństwa i zapewnienie zmian w systemie funkcjonalnym ZAGROŻENIA DO ZIDENTYFIKOWANIA”	ATM/ANS.OR.B.005(a)(5) „System zarządzania” ATS.OR.200(2)(i) „System zarządzania bezpieczeństwem” AMC1 ATS.OR.205(b)(1) „Ocena bezpieczeństwa i zapewnienie zmian w systemie funkcjonalnym KOMPLETNOŚĆ IDENTYFIKACJI ZAGROŻEŃ” AMC2 ATS.OR.205(b)(1) „Ocena bezpieczeństwa i zapewnienie zmian w systemie funkcjonalnym ZAGROŻENIA DO ZIDENTYFIKOWANIA”

CAMO	PART 145	Organizacje produkujące/POA	Organizacje projektujące/DOA	Zarezerwowane
CAMO.A.160 „Zgłaszanie zdarzeń” CAMO.A.200 „System zarządzania” punkt (a)(3) GM1 CAMO.A.200 „System zarządzania” AMC1 CAMO.A.200(a)(3) GM1 CAMO.A.200(a)(3) „System zarządzania – Zarządzanie ryzykiem bezpieczeństwa – współpraca (interfejsy) między organizacjami” GM2 CAMO.A.200(a)(3) „System zarządzania” CAMO.A.202 „Wewnętrzny system zgłaszania kwestii związanych z bezpieczeństwem” oraz AMC/GM CAMO.A.300 „Charakterystyka zarządzania ciągłą zdatnością do lotu (CAME)” punkt (a)(10)	145.A.200 „System zarządzania” punkt (a)(3) AMC1 145.A.200(a)(3) „Kluczowe procesy zarządzania bezpieczeństwem” GM1 145.A.200(a)(3) „Zarządzanie ryzykiem bezpieczeństwa – współpraca (interfejsy) między organizacjami” 145.A.60 „Zgłaszanie zdarzeń” 145.A.202 „Wewnętrzny system zgłaszania kwestii związanych z bezpieczeństwem” AMC1/GM1 145.A.202 145.A.205 „Umowy i podwykonawstwo” GM1 145.A.205 „Odpowiedzialność przy zamawianiu czynności lub zleceniu podwykonawstwa zadań obsługowych”	21.A.139 „System zarządzania produkcją” punkt (c)(3) GM1 21.A.139(c) „System zarządzania bezpieczeństwem” AMC1 21.A.139(c)(3) i (4) „Kluczowe procesy zarządzania bezpieczeństwem” 21.A.3A „System zgłaszania” punkt (b) GM1 21.A.3A „Związek pomiędzy punktem 21.A.3A a Rozporządzeniem (UE) nr 376/2014” GM1 21.A.3A(a) i 21.A.3A(b) „Ogólnie – system zgłaszania” GM1 21.A.3A(a)(1) i (b)(1) „Dobrowolne zgłaszanie zdarzeń organizacji” GM2 21.A.3A(a)(1) i (b)(1) „Wewnętrzny system zgłaszania kwestii związanych z bezpieczeństwem”	21.A.239 „System zarządzania projektowaniem” punkt (c)(3) GM1 21.A.239(c) „System zarządzania bezpieczeństwem” AMC1 21.A.239(c)(3) i (4) „Kluczowe procesy zarządzania bezpieczeństwem” 21.A.243 (a)(4) „Próby w locie” 21.A.3A System zgłaszania” punkt (a) GM1 21.A.3A „Związek pomiędzy punktem 21.A.3A a Rozporządzeniem (UE) nr 376/2014” GM1 21.A.3A(a) i 21.A.3A(b) „Ogólnie – system zgłaszania” GM1 21.A.3A(a)(1) i (b)(1) „Dobrowolne zgłaszanie zdarzeń organizacji” GM2 21.A.3A(a)(1) i (b)(1) „Wewnętrzny system zgłaszania kwestii związanych z bezpieczeństwem”	

2.1.2 Zgłaszanie zdarzeń zgodnie z Rozporządzeniem (UE) nr 376/2014

Procedury zgłaszania zdarzeń dotyczące bezpieczeństwa określone w Załączniku 19, które stanowią część Polityki bezpieczeństwa zgodnie z 1.1.1 (c)

Rozporządzenie 376/2014 również ma tu zastosowanie.

Obecny	Odpowiedni	Sprawny	Skuteczny
Istnieje system poufnego zgłaszania zdarzeń obejmujący obowiązkowe oraz dobrowolne zgłoszenia przechowywany w bazie danych, zawierający system informacji zwrotnych. Zakres obowiązków został określony zgodnie z wymogami Rozporządzenia (UE) nr 376/2014. Proces określa w jaki sposób zgłoszenia są przekładane na działania oraz w jaki sposób określany jest ich harmonogram czasowy.	System zgłaszania jest dostępny i łatwy w użyciu dla personelu zaangażowanego w działania związane z bezpieczeństwem organizacji. Istnieją odpowiednie środki do identyfikowania problemów stron trzecich (partnerów, dostawców, wykonawców).	System zgłaszania zdarzeń jest łatwy w użyciu, jest wykorzystywany i dostępny dla wszystkich pracowników. Istnieje system informacji zwrotnych przekazywanych osobie zgłaszającej na temat wszelkich podjętych (lub niepodjętych) działań oraz w stosownych przypadkach, pozostałej części organizacji. Zgłoszenia są oceniane, przetwarzane, analizowane i przechowywane. Badania zdarzeń bezpieczeństwa przeprowadzane są przez odpowiednio przeszkolony personel w celu zidentyfikowania ich pierwotnych przyczyn (dlaczego tak się stało, a nie tylko co się stało). Ludzie są świadomi i wywiązują się ze swoich obowiązków w zakresie systemu raportowania. Zgłoszenia są przetwarzane w określonych ramach czasowych. Zapewniona jest łączność z tematami omawianymi podczas posiedzeń Rady ds. Bezpieczeństwa (SRB) lub komitetów ds. bezpieczeństwa (safety commitees).	Personel wyraża zaufanie do polityki i procesu zgłaszania zdarzeń organizacji. System zgłaszania jest wykorzystywany do wpływania na decyzje zarządcze i ciągłe doskonalenie. System zgłaszania zdarzeń oparty na trafności otrzymanych zgłoszeń jest w dobrej kondycji. Działania wynikające z analiz zgłoszeń bezpieczeństwa są realizowane terminowo. System zgłaszania przyczynia się do ciągłego doskonalenia osiągów organizacji.
Wyniki oceny			

Czego szukać
– Sprawdzić, czy obowiązki wymagane przez Rozporządzenie (UE) nr 376/2014 zostały zdefiniowane i sformułowane w opisach stanowisk. – Dokonać przeglądu systemu zgłaszania pod kątem dostępu i łatwości użytkowania (odpowiedniość systemów zgłaszania). W zależności od wielkości i złożoności, odpowiedniość systemu raportowania może obejmować zarówno proste, zabezpieczone skrzynki jak i system cyfrowy, obejmujący aplikacje do zainstalowania na urządzeniach mobilnych. – Sprawdzić, czy pracownicy ufają systemowi zgłaszania zdarzeń, znają go i wiedzą, co należy zgłaszać. – Zebrać dowody, że ludzie nie boją się zgłaszać w ramach wewnętrznego systemu zgłaszania bezpieczeństwa. – Sprawdzić, w jaki sposób zapewnia się ochronę i poufność danych. – Zebrać dowody przekazywania informacji zwrotnej zgłaszającym (lub pętli informacji zwrotnych dotyczących agregacji zgłoszeń wraz z ich analizami, w zależności od liczby zdarzeń). – Ocenić ilość i jakość zgłoszeń, w tym zgłoszeń własnych (self-reporting). – Przejrzeć wskaźniki zamykania zgłoszeń. – Sprawdzić dostępność zgłaszania dla zakontraktowanych organizacji i klientów. – Sprawdzić przeszkolenie personelu prowadzącego badania zdarzeń. – Sprawdzić, czy taksonomia jest zdefiniowana i stosowana. – Badania zdarzeń prowadzone są w celu zidentyfikowania ich pierwotnych przyczyn (dlaczego tak się stało, a nie tylko, co się stało). Sprawdzić jakość analiz. – System wspiera analizy, działania następcze i zgłaszanie do odpowiedniego właściwego organu zgodnie z art. 13 Rozporządzenia (UE) nr 376/2014. Istnieje proces analizowania danych i informacji bezpieczeństwa w celu identyfikowania trendów i uzyskiwania przydatnych pod kątem zarządzania informacji. – Potwierdzić, że obowiązki w zakresie analizy zdarzeń, przechowywania i działań następczych są jasno określone. – Sprawdzić, czy odpowiedni personel jest świadomy, które zdarzenia powinny być obowiązkowe. Sprawdzić, w jaki sposób załączniki do Rozporządzenia (UE) nr 2015/1018 są wdrożone i znane pracownikom. – Ocenić, w jaki sposób menedżerowie/kierownicy operacyjni i kadra kierownicza wyższego szczebla wykorzystują wyniki systemu zgłaszania.

Odpowiednie odniesienia do przepisów UE/EASA				
Operacje lotnicze	**Załoga lotnicza**	**Lotniska**	**ATM/ANS**	**Organizacja szkolenia ATC**
Rozporządzenie (UE) nr 376/2014 Artykuł 4 „Obowiązkowe zgłaszanie zdarzeń”, Artykuł 5 „Dobrowolne zgłaszanie zdarzeń”, Artykuł 13 „Analiza zdarzeń i działania następcze na poziomie krajowym”, Artykuł 16 „Ochrona źródła informacji”.				

CAMO	PART 145	Organizacje produkujące/POA	Organizacje projektujące/DOA	Zarezerwowane
CAMO.A.160 „Zgłaszanie zdarzeń” oraz AMC/GM CAMO.A.202 „Wewnętrzny system zgłaszania kwestii związanych z bezpieczeństwem” oraz AMC/GM CAMO.A.300 „Charakterystyka zarządzania ciągłą zdatnością (CAME)” punkt (a)(10)	145.A.60 „Zgłaszanie zdarzeń” AMC2 145.A.60 AMC1 145.A.60 „Ogólne” GM1 145.A.60 „Obowiązkowe zgłaszanie zdarzeń - ogólne” 145.A.202 „Wewnętrzny system zgłaszania kwestii związanych z bezpieczeństwem” oraz	21.A.3A „System zgłaszania” GM1 21.A.3A „Związek pomiędzy punktem 21.A.3A a Rozporządzeniem (UE) nr 376/2014” W stosownych przypadkach wszystkie AMC i GM opracowane dla 21.A.3A	21.A.3A „System zgłaszania” GM1 21.A.3A „Związek pomiędzy punktem 21.A.3A a Rozporządzeniem (UE) nr 376/2014” W stosownych przypadkach wszystkie AMC i GM opracowane dla 21.A.3A	

	AMC1 GM1 145.A.202 „Ogólne" 145.A.70 „Charakterystyka organizacji obsługowej (MOE)" AMC1 145.A.70(a) 'MOE' Punkt 2.18 i 3.2	AMC1 21.A.143 (a)(1) „Zakres organizacji produkującej POE"	AMC1 21.A.243(a) „Podręcznik"	
Rozporządzenie (UE) nr 376/2014 Artykuł 4 „Obowiązkowe zgłaszanie zdarzeń", Artykuł 5 „Dobrowolne zgłaszanie zdarzeń", Artykuł 13 „Analiza zdarzeń i działania następcze na poziomie krajowym", Artykuł 16 „Ochrona źródła informacji".				

PODSUMOWANIE KOMENTARZY do 2.1. „IDENTYFIKACJA ZAGROŻEŃ"

2.2 Ocena i obniżanie poziomu ryzyka bezpieczeństwa

Odniesienia i tekst Załącznika 19

2.2.1 Podmiot lotniczy opracowuje i gwarantuje funkcjonowanie procesu zapewniającego analizowanie, ocenę i kontrolę ryzyk bezpieczeństwa związanych ze zidentyfikowanymi zagrożeniami.

Uwaga – Proces może obejmować predykcyjne metody analizy danych bezpieczeństwa.

Obecny	Odpowiedni	Sprawny	Skuteczny
Istnieje proces analizy i oceny ryzyk bezpieczeństwa.	Metodologia oceny ryzyka, w tym nadające się do użytku kryteria „dotkliwości" i „prawdopodobieństwa", są zdefiniowane i dopasowane do rzeczywistego otoczenia podmiotu lotniczego, z uwzględnieniem oceny eksperckiej, gdy dane nie są dostępne. Zastosowane definicje są wystarczająco jednoznaczne oraz szczegółowe. Właściwy poziom uprawnień (odpowiedzialności) na poszczególnych szczeblach organizacji we współpracy z interesariuszami jest jasno określony do akceptacji danego poziomu ryzyka.	Analizy i oceny ryzyk prowadzone są w spójny sposób w oparciu o zdefiniowany proces. Stosowane są odpowiednie mechanizmy kontroli ryzyk w celu sprowadzenia ryzyk bezpieczeństwa do akceptowalnego poziomu, w tym harmonogramy i podział obowiązków uzgodniony z zainteresowanymi stronami. Czynniki operacyjne, techniczne, ludzkie i organizacyjne są uwzględniane w ramach opracowywania środków kontrolowania ryzyk. Kierownictwo wyższego szczebla jest aktywnie zaangażowane przy średnich i wysokich ryzykach oraz ich ograniczaniu i kontrolowaniu. Zrozumienie zewnętrznych czynników wejściowych i wyników zarządzania ryzykami bezpieczeństwa, którymi należy się zająć.	Analizy i oceny ryzyk są poddawane przeglądowi pod kątem spójności i identyfikacji ulepszeń w procesach. Oceny ryzyk są regularnie przeglądane, by zapewnić ich aktualność. Kryteria akceptowalności ryzyk są stosowane rutynowo, konsekwentnie wykorzystywane w procesach podejmowania decyzji zarządczych i podlegają regularnym przeglądom.
Wyniki oceny			

Czego szukać

- Przejrzeć schemat i procedury klasyfikacji ryzyk.
- Sprawdzić metodologię stosowaną do oceny ryzyk; w jaki sposób jest dokumentowana, dokładnie zdefiniowana i wykorzystywana; sprawdzić, jak szkolona jest kadra stosująca tę metodologię.
- Sprawdzić wszelkie przyjęte założenia i czy są one weryfikowane.
- Sprawdzić, czy proces określa, kto może zaakceptować jaki poziom ryzyka.
- Sprawdzić, czy określono poziom ryzyka, który organizacja jest skłonna zaakceptować.

- Definicje oraz kryteria dotkliwości i prawdopodobieństwa są wystarczająco zdefiniowane (lub alternatywna metodologia została opisana) i zaadaptowane do charakteru prowadzonej działalności. Została także opisana dotkliwość „do czego mogłoby dojść" („najgorszy możliwy scenariusz" i konsekwencje). Różnica pomiędzy „prawdopodobieństwem" a „częstością" jest rozumiana.
- Sprawdzić, czy oceny ryzyka są prowadzone konsekwentnie i spójnie w całej organizacji (np. rozważenie różnych perspektyw i poglądów dotyczących bezpieczeństwa w celu podjęcia odpowiedniej decyzji).
- Przejrzeć klasyfikację problemów, jeśli nie ma wystarczających danych ilościowych. W przypadku korzystania z oceny eksperckiej stosuje się proces wspólnej oceny ryzyka (np. różne oceny eksperckie w dziedzinach przekrojowych, takich jak: Operacje Lotnicze, Projektowanie, Produkcja, eksperci ds. Wydolności Człowieka), biorąc pod uwagę różne perspektywy i poglądy w zakresie bezpieczeństwa w celu podjęcia odpowiedniej decyzji, aby zapewnić powtarzalność oceny.
- Rozważyć, w jaki sposób oceniana jest wydolność człowieka w ramach procesu zarządzania ryzykiem bezpieczeństwa i jego łagodzenia (zob. Podręcznik ICAO 10151).
- Sprawdzić, czy wyniki działania systemu zgłaszania zdarzeń bezpieczeństwa, w tym obowiązkowych i dobrowolnych systemów zgłaszania zdarzeń, są wykorzystywane do testowania solidności ocen ryzyk, w tym w przypadkach wykorzystania opinii eksperckich (zob. Sekcja 3.1). Czy sieć zainteresowanych stron jest zaangażowana w gromadzenie danych i informacji bezpieczeństwa, które stanowią podstawę do oceny ryzyk, szczególnie w odniesieniu do ryzyk w relacjach z podmiotami zewnętrznymi (interfejsy)? (zob. Sekcja 5.1).
- Sprawdzić, czy oceny ryzyk są aktualizowane, gdy dostępne są nowe dane z systemu zgłaszania zdarzeń bezpieczeństwa. Sprawdzić, co uruchamia ocenę ryzyka i jej przegląd w określonym czasie. Sprawdzić, czy rejestr ryzyk jest poddawany przeglądowi i monitorowany przez odpowiedni(-e) komitet(-y) ds. bezpieczeństwa, jeśli ma to zastosowanie. Sprawdzić, w jaki sposób doświadczenie, opinie/informacje zwrotne i monitorowanie ostatnio opublikowanych informacji bezpieczeństwa służą tej regularnej aktualizacji.
- Przejrzeć układ rejestru ryzyk, np. wstępna ocena, ryzyko pozostałe (rezydualne), działania łagodzące, kto jest właścicielem, powiązane osiągi w zakresie poziomu bezpieczeństwa i działania następcze.
- Skontrolować wyrywkowo zidentyfikowane zagrożenia oraz sposoby ich przetwarzania i dokumentowania.
- Sprawdzić, które komitety ds. bezpieczeństwa lub osoby odpowiedzialne nadzorują „akceptowalność". Sprawdzić dostępność instrukcji dotyczących wdrożenia poziomu „tak niskiego, jak to rozsądnie praktyczne" (As Low As Reasonably Practical - ALARP). Sprawdzić odpowiedni poziom uprawnień do podejmowania decyzji.
- Znaleźć dowody na stosowanie w odpowiednich przypadkach przy podejmowaniu decyzji w oparciu o dane redukcji ryzyk, ocen ryzyk pozostałych (rezydualnych) i akceptowalności ryzyk.
- Dowieść, że ryzyka, w tym te, które nie są generowane przez samą organizację, są analizowane i ograniczane bez dalszego ich przenoszenia do innych obszarów.
- Sprawdzić, jak trendy i pojawiające się problemy są identyfikowane i zarządzane.

Odpowiednie odniesienia do przepisów UE/EASA				
Operacje lotnicze	**Załoga lotnicza**	**Lotniska**	**ATM/ANS**	**Organizacja szkolenia ATC**
ORO.GEN.200 „System zarządzania" punkt (a)(3) AMC1 ORO.GEN.200(a)(3) „System zarządzania" punkt (b)(1) – (operatorzy typu complex) AMC1 ORO.GEN.200(a) (1);(2);(3);(5) „System zarządzania" punkt (a), (b) i (d) – (operatorzy typu non-complex)	ORO.GEN.200 „System zarządzania" punkt (a)(3) AMC1 ORA.GEN.200(a)(3) „System zarządzania" punkt (b)(1) – (organizacje typu complex) AMC1 ORA.GEN.200(a) (1);(2);(3);(5) „System zarządzania" punkt (a), (b) i (d) – (organizacje typu non-complex)	ADR.OR.D.005 „System zarządzania" punkt (b)(4) AMC1 ADR.OR.D.005 (b)(4) „System zarządzania"	ATS.OR.200(2)(i) „System zarządzania"	ATCO.OR.C.001 „System zarządzania organizacji szkoleniowych" punkt (c) AMC1 ATCO.OR.C.001(c) „System zarządzania organizacji szkoleniowych"

AMC1 ORO.AOC.130 „Monitorowanie parametrów lotu - samoloty” punkt (b)				
CAMO	**PART 145**	**Organizacje produkujące/POA**	**Organizacje projektujące/DOA**	**Zarezerwowane**
GM1 CAMO.A.200 „System zarządzania” CAMO.A.200 „System zarządzania” punkt (a)(3) AMC1 CAMO.A.200(a)(3) punkt (b)(1) AMC1 CAMO.A.200 point (a)(1) „Organizacja i obowiązki” GM1 CAMO.A.200(a)(1) w celu określenia komitetów ds. bezpieczeństwa odpowiedzialnych za „akceptowalność” CAMO.A.300 „Charakterystyka zarządzania ciągłą zdatnością (CAME)” punkt (a)(11)(i)	145.A.200 „System zarządzania” punkt (a)(3) AMC1 145.A.200(a)(3) „Kluczowe procesy zarządzania bezpieczeństwem” punkt (b) 145.A.48 „Wykonanie obsługi technicznej” AMC1/2/3 145.A.48(c)(2) „Wykonanie obsługi technicznej” AMC1 145.A.48(c)(3) „Wykonanie obsługi technicznej” oraz GM1 145.A.70 „Charakterystyka organizacji obsługowej (MOE)” AMC1 145.A.70(a) ‘MOE’ punkt 3.1 i 3.4	21.A.139 „System zarządzania produkcją” punkt (c)(3) GM1 21.A.139(c) „System zarządzania bezpieczeństwem” AMC1 21.A.139(c)(3) and (4) „Kluczowe procesy zarządzania bezpieczeństwem” GM1 21.A.139(c) (2) „Grupa ds. działań w zakresie bezpieczeństwa” 21.A.3A „System zgłaszania” punkt (b) GM1 21.A.3A „Związek pomiędzy punktem 21.A.3A a Rozporządzeniem (UE) nr 376/2014”	21.A.239 „System zarządzania projektowaniem” punkt (c)(3) GM1 21.A.239(c) „System zarządzania bezpieczeństwem” AMC1 21.A.239(c)(3) i (4) „Kluczowe procesy zarządzania bezpieczeństwem” GM1 21.A.239(c)(2) „Grupa ds. działań w zakresie bezpieczeństwa” 21.A.3A „System zgłaszania” punkt (a) GM1 21.A.3A „Związek pomiędzy punktem 21.A.3A a Rozporządzeniem (UE) nr 376/2014”	

Odniesienia i tekst Załącznika 19

Podmiot lotniczy opracowuje i utrzymuje proces, który zapewnia (analizę, ocenę i) **kontrolę** ryzyk bezpieczeństwa związanych ze zidentyfikowanymi zagrożeniami.

Obecny	Odpowiedni	Działający	Skuteczny
Organizacja posiada proces podejmowania decyzji i sposobów kontrolowania ryzyk.	Zdefiniowano obowiązki i harmonogramy do ustalenia i akceptowania sposobów kontrolowania ryzyk. Rozważane są odpowiednie strategie i perspektywy łagodzenia ryzyk.	Stosowane są odpowiednie sposoby kontrolowania ryzyk w celu ich ograniczenia do akceptowalnych poziomów, łącznie z harmonogramami i dzieleniem odpowiedzialności. Organizacja postępuje zgodnie z istniejącymi procesami, aby podejmować decyzje i stosować odpowiednie i skuteczne sposoby kontrolowania ryzyk. Wydolność człowieka jest brana pod uwagę jako część rozwoju sposobów kontrolowania ryzyk.	Sposoby kontrolowania ryzyk są praktyczne i trwałe, stosowane terminowo i nie stwarzają dodatkowych ryzyk. Skuteczność sposobów kontrolowania ryzyk jest monitorowana poprzez osiągany poziom bezpieczeństwa, przy użyciu środków jakościowych i/lub ilościowych. Sposoby kontrolowania ryzyk uwzględniają wydolność człowieka.
Wyniki oceny			

Czego szukać

- Sposoby kontrolowania ryzyk są jasno zidentyfikowane. Są dowody na podjęcie działań w zakresie kontrolowania ryzyk i związane z tym działania następcze.
- Do monitorowania skuteczności sposób kontrolowania ryzyk stosuje się środki ilościowe i/lub jakościowe, takie jak SMART SPIs, SPTs, poziomy alarmowe.
- Sprawdzić jak trendy są monitorowane i wykorzystywane.
- Rozważane jest ryzyko zagregowane/skumulowane.
- Sprawdzić, czy sposoby kontrolowania ryzyk zmniejszyły ryzyka pozostałe (rezydualne).
- Sprawdzić, czy nowe sposoby kontrolowania ryzyk nie stwarzają dodatkowych ryzyk.
- Sprawdzić, jak polityka uwzględnia zasadę ALARP – zweryfikować jej wdrożenie.
- Sprawdzić, w jaki sposób specyficzne dla danych obszarów działalności lotniczej ryzyka są odpowiednio kontrolowane, takie jak: Zarządzanie Ryzykiem Zmęczenia Załóg (Fatigue Risk Management), monitorowanie parametrów lotu – FDM/FDA, HUMS (Health and Usage Monitoring System), podwykonawstwo, interfejsy, itd.
- Sprawdzić, czy akceptowanie ryzyka jest dokonywane na właściwym szczeblu zarządzania.
- Kierownicy operacyjni i kadra kierownicza wyższego szczebla mają podgląd na ryzyka średniego i wysokiego poziomu, a także sposoby ich łagodzenia i kontrolowania.
- Dokonać przeglądu stosowania sposobów kontrolowania ryzyk, które opierają się wyłącznie na interwencji człowieka.
- Sposoby kontrolowania ryzyk uwzględniają wydolność ludzką i czynniki organizacyjne.
- Sprawdzić w jaki sposób zapewniona jest skuteczność barier ochronnych w przypadku istotnych ryzyk wynikających z relacji (interfejsów) (zob. Sekcja 5.1).

Odpowiednie odniesienia do przepisów UE/EASA				
Operacje lotnicze	**Załoga lotnicza**	**Lotniska**	**ATM/ANS**	**Organizacja szkolenia ATC**
AMC1 ORO.GEN.200(a)(3) “System zarządzania” punkt (b)	AMC1 ORA.GEN.200(a)(3) “System zarządzania” punkt (b)	AMC1 ADR.OR.D.005(b)(4) “System zarządzania”	ATS.OR.200(2)(i) „System zarządzania bezpieczeństwem”	ATCO.AR.B.001 „System zarządzania” punkt (a)(4); Ponadto, zastosowanie mają przepisy ATSP.
CAMO	**PART 145**	**Organizacje produkujące/POA**	**Organizacje projektujące/DOA**	**Zarezerwowane**
CAMO.A.200 „System zarządzania” punkt (a)(3) GM1 CAMO.A.200 „System zarządzania” AMC1 CAMO.A.200(a)(3) punkt (b) i (d) CAMO.A.300 „Charakterystyka zarządzania ciągłą zdatnością (CAME)” punkt (a)(11) (i)	145.A.200 „System zarządzania” punkt(a)(3) GM1 145.A.200 „System zarządzania” AMC1 145.A.200(a)(3) „Kluczowe procesy zarządzania bezpieczeństwem” punkt (a), (b) i (d) AMC1 145.A.70 ‘MOE’ punkt 3.1 i 3.4	21.A.139 (c) (3) „Element zarządzania produkcją” GM1 21.A.139(c) „System zarządzania bezpieczeństwem” AMC1 21.A.139(c)(3) and (4) „Kluczowe procesy zarządzania bezpieczeństwem” GM1 21.A.139(c) (2) „Grupa ds. działań w zakresie Bezpieczeństwa”	21.A.239 (c)(3) „Element zarządzania projektowaniem” GM1 21.A.239(c) „System zarządzania bezpieczeństwem” AMC1 21.A.239(c)(3) i (4) „Kluczowe procesy zarządzania bezpieczeństwem” GM1 21.A.239(c) (2) „Grupa ds. działań w zakresie Bezpieczeństwa”	

PODSUMOWANIE KOMENTARZY do 2.2. „OCENA I OBNIŻANIE POZIOMU RYZYKA”

3 ZAPEWNIANIE BEZPIECZEŃSTWA

3.1 Mierzenie i monitorowanie poziomu bezpieczeństwa (safety performance monitoring)

Odniesienia i tekst Załącznika 19

3.1.1 Podmiot lotniczy opracowuje i zapewnia funkcjonowanie sposobów weryfikowania Poziomu Bezpieczeństwa w organizacji (safety performance)[25] i potwierdzania skuteczności kontroli ryzyk bezpieczeństwa.

Uwaga: Proces audytu wewnętrznego jest jednym ze sposobów monitorowania zgodności z przepisami bezpieczeństwa, stanowiącymi podstawę do zbudowania systemu zarządzania bezpieczeństwem – SMS, oraz oceny skuteczności sposobów kontrolowania ryzyka bezpieczeństwa i SMS. Wytyczne dotyczące zakresu procesu audytu wewnętrznego znajdują się w Podręczniku Zarządzania Bezpieczeństwem (SMM) (Doc 9859).

Obecny	Odpowiedni	Sprawny	Skuteczny
Organizacja posiada udokumentowany program audytu wewnętrznego powiązany z procesem przeglądu zarządzania. Istnieje udokumentowany proces oceny, czy odpowiednie sposoby kontrolowania ryzyk są stosowane i skuteczne w zakresie kluczowych procesów SMS. Określono osobę lub grupę osób odpowiedzialnych za funkcję monitorowania, które mają bezpośredni dostęp do Kierownika Odpowiedzialnego (Accountable Executive).	Obowiązki, metody i ramy czasowe potrzebne do oceny sposobów kontrolowania ryzyk są odpowiednio zdefiniowane. Pomiar osiąganego poziomu bezpieczeństwa (safety performance measurement) skupia się na skuteczności środków łagodzących zastosowanych wobec kluczowych ryzyk, a co za tym idzie, celów bezpieczeństwa. Pomiar osiąganego poziomu bezpieczeństwa koncentruje się na tym, co jest istotne, a nie na tym, co jest łatwe do zmierzenia. Wkład organizacji zakontraktowanych należy uwzględnić w procesie zapewniania bezpieczeństwa, biorąc pod uwagę potencjalny efekt, jaki mogą one wywrzeć na poziom bezpieczeństwa w organizacji (safety performance of the organisation).	Informacje z systemu(ów) zgłaszania, zapewniania bezpieczeństwa, działań w zakresie monitorowania zgodności lub innych odpowiednich źródeł są wykorzystywane ponownie w procesie zarządzania ryzykami bezpieczeństwa. Odpowiednie mechanizmy/sposoby kontrolowania ryzyk są weryfikowane w celu oceny, czy są stosowane i skuteczne. Działania w ramach planów działań naprawczo-zapobiegawczych są dokumentowane i poddawane przeglądowi przez odpowiedni organ zarządzający systemem SMS (tj. posiadający odpowiedni poziom uprawnień w zależności od wielkości organizacji i złożoności prowadzonych przez nią operacji). Interfejsy (powiązania) pomiędzy audytami opartymi na zgodności a procesami zarządzania ryzykami bezpieczeństwa są zdefiniowane i używane.	Oceniane są odpowiednie mechanizmy/sposoby kontrolowania ryzyk i podejmowane są działania mające na celu zapewnienie ich skuteczności i bezpieczeństwa usługi. Badane są przyczyny nieefektywności mechanizmów/sposobów kontrolowaniaryzyk. Pod uwagę brana jest wydolność człowieka (human performance). W procesach Zarządzania ryzykiem bezpieczeństwa (Safety Risk Management) i zapewniania bezpieczeństwa (Safety Assurance) organizacji istnieje, stosownie do potrzeb, wszechstronna integracja zewnętrznych i wewnętrznych intefejsów. Wynik osiągnięty przez organizację w zakresie poziomu bezpieczeństwa uwzględnia i dostarcza informację zwrotną dla organu nadzorującego system SMS, jeśli ma to zastosowanie, w celu przeglądu i ostatecznie dla właściwego organu. Efektywność procesów SMS poddawana jest regularnemu przeglądowi.

[25] Uwaga EASA: W nadchodzącej poprawce do Załącznika 19 ICAO planuje dokonać przeglądu definicji „poziomu bezpieczeństwa (safety performance)" w następujący sposób: Poziom bezpieczeństwa: wymierny wpływ organizacji na bezpieczeństwo oceniany za pomocą SPIs, w razie potrzeby wspierany środkami jakościowymi. Podano także nową definicję SPIs: środki miernicze lub ilościowe stosowane do pomiaru i monitorowania postępów organizacji w drodze do osiągnięcia celów bezpieczeństwa (safety objectives). Planuje się zatem, że poprawiona Norma ICAO 3.1.2. będzie w większym stopniu skupiać się na postępie w osiąganiu celów bezpieczeństwa poprzez pomiar i monitorowanie wyników organizacji. Datą rozpoczęcia stosowania powinien być listopad 2026 r. (do potwierdzenia)

Wyniki oceny			

Czego szukać

Należy sprawdzić, czy istnieje mechanizm zapewniający, że organizacja korzysta ze wszystkich odpowiednich źródeł pozyskiwania danych, aby otrzymać prawdziwy obraz swoich ryzyk, ocenić swój poziom bezpieczeństwa (safety performance); a z czasem podjąć odpowiednie działania i sprawdzić ich skuteczność.

- Znaleźć dowody dotyczące odpowiedzialności, metod i harmonogramu w celu dokonania oceny czy sposoby kontrolowania ryzyk są stosowane i skuteczne: przejrzeć sposoby kontrolowania pod kątem ich oceniania i monitorowania w zakresie ich skuteczności (np. audyty, ankiety, przeglądy, jakościowe i/lub ilościowe środki do pomiaru i monitorowania osiągów poziomu bezpieczeństwa, np. Wskaźniki Poziomu Bezpieczeństwa - SPIs, SPTs, poziomy alarmowe, a w stosownych przypadkach - systemy zgłaszania).
- Znaleźć dowody na to, że procesy oceny ryzyka, w tym ryzyka pozostałego (rezydualnego), są poddawane regularnej ocenie.
- Zapewnienie bezpieczeństwa uwzględnia działania prowadzone na interfejsach (powiązaniach) zewnętrznych (tj. z interesariuszami/z zainteresowanymi stronami): znaleźć dowody stosowania środków kontrolowania ryzyk stosowanych przez zakontraktowane organizacje/strony trzecie, inne departamenty (czy są poddawane ocenie i nadzorowi, np. kontrola jakości, przeglądy i regularne spotkania).
- Informacje pochodzące z działań związanych z zapewnianiem bezpieczeństwa i monitorowaniem zgodności (zob. Sekcja 5.2.4) są wykorzystywane ponownie w procesie zarządzania ryzykami bezpieczeństwa (zob. Sekcja 2.2).
- Sprawdzić, gdzie w wyniku oceny zmieniono mechanizmy kontrolowania ryzyk.

Jakiego rodzaju informacje i źródła mogą wspierać pomiar osiąganego poziomu bezpieczeństwa?
Należy sprawdzić, w jakim stopniu organizacja zwraca uwagę na informacje wynikające ze zdarzeń wewnętrznych i zewnętrznych, rezultaty stosowania Rozporządzenia (UE) nr 376/2014 (w szczególności art. 13), cele bezpieczeństwa określone zgodnie z art. 76 ust. 6 rozporządzenia (UE) 2018/1139, raporty z badań zdarzeń; automatycznego zbierania danych (tj. monitorowania parametrów lotu – FDM/FDA dla operatorów lotniczych); spotkania bezpieczeństwa, warsztaty, seminaria, raporty o zagrożeniach, profile ryzyk sektorowych; audyty i statystyki w ramach funkcji monitorowania zgodności, analizy danych bezpieczeństwa, KPBwLC i/lub KPB, (branżowe i/lub wydane przez EASA), plany działania w zakresie bezpieczeństwa (safety roadmaps), EPAS (zwłaszcza Tom II, zob. Sekcja 4, w której proponuje się SPIs, które maja być monitorowane oraz Tom III), Roczny Raport/Przegląd Bezpieczeństwa (Annual Safety Report/Review - ASR) ICAO lub EASA, lub Państwa, lub ASR uznanych organizacji międzynarodowych (tj. IATA, CANSO); promowanie bezpieczeństwa przez Państwo, nadzór i akceptacja Wskaźników Poziomu Bezpieczeństwa/Celów Poziomu Bezpieczeństwa (SPIs/SPTs) przez Państwo zgodnie z Zaleceniem 3.3.2.2 Załącznika 19 itd.

Należy rozważyć, w jaki sposób wydolność człowieka (human performance) (dok. ICAO 10151) jest uwzględniana w osiągach poziomu bezpieczeństwa i zapewniania bezpieczeństwa.

Odpowiednie odniesienia do przepisów UE/EASA

Operacje lotnicze	Załoga lotnicza	Lotniska	ATM/ANS	Organizacja szkolenia ATC
ORO.GEN.200 “System zarządzania” punkt (a)(3) AMC1 ORO.GEN.200(a)(3) “System zarządzania” punkt (d)(1) – (operatorzy typu complex)	ORA.GEN.200 „System zarządzania” – punkt (a)(3) AMC1 ORA.GEN.200(a)(3) “System zarządzania” punkt (d)(1) – (organizacje typu complex)	ADR.OR.D.005 „System zarządzania” punkt (b)(5) AMC1 ADR.OR.D.005(b) (5) „System zarządzania”	ATS.OR.200 (3)(i) „System zrządzania bezpieczeństwem” Komisja wdrażająca Rozporządzenie (UE) 2019/317 lub najnowsza zmiana	Nie dotyczy, jednakże zastosowanie mają przepisy dotyczące instytucji zapewniającej służby ruchu lotniczego (ATS).

AMC1 ORO.AOC.130 „Monitorowanie parametrów lotu - samoloty” punkt (b)				
CAMO	**PART 145**	**Organizacje produkujące/POA**	**Organizacje projektujące/DOA**	**Zarezerwowane**
CAMO.A.200 „System zarządzania” punkt (a)(3) GM1 CAMO.A.200 „System zarządzania” AMC1 CAMO.A.200(a)(3) punkt (d) Zob. również CAMO.A.160 CAMO.A.300 „Charakterystyka zarządzania ciągłą zdatnością (CAME)” punkt (a)(11)(i)	145.A.200 „System zarządzania” punkt (a)(3) AMC1 145.A.200(a)(3) „Kluczowe procesy zarządzania bezpieczeństwem” punkt (d) 145.A.48 „Wykonanie obsługi technicznej” AMC1/2/3 145.A.48(c)(2) „Wykonanie obsługi technicznej” oraz GM1 AMC1 145.A.48(c)(3) „Wykonanie obsługi technicznej” oraz GM1 145.A.70 „Charakterystyka organizacji obsługowej (MOE)” AMC1 145.A.70 „MOE” punkt 3.4	21.A.139 „System zarządzania produkcją” punkt (c)(4)(i) GM1 21.A.139(c) „Element zarządzania bezpieczeństwem” AMC1 21.A.139(c)(3) i (4) „Kluczowe procesy zarządzania bezpieczeństwem” GM1 21.A.139(c)(2) „Grupa zadaniowa ds. bezpieczeństwa” 21.A.139 „System zarządzania produkcją” punkt (e) AMC1 21.A.139(e) i 21.A.139(d)(2)(xiv) „Funkcja niezależnego monitoringu”	21.A.239 „System zarządzania projektowaniem” punkt (c)(4)(i) GM1 21.A.239 (c) „Element zarządzania bezpieczeństwem” AMC1 21.A.239(c)(3) i (4) „Kluczowe procesy zarządzania bezpieczeństwem” GM1 21.A.239(c) (2) „Grupa ds. działań w zakresie bezpieczeństwa” 21.A.239 „System zarządzania projektowaniem” punkt (e) AMC1 21.A.239(e) „Funkcja niezależnego monitoringu”	

Odniesienia i tekst Załącznika 19

3.1.2 Poziom Bezpieczeństwa podmiotu lotniczego ma być weryfikowany w odniesieniu do **Wskaźników Poziomu Bezpieczeństwa** – SPIs i Celów Poziomu Bezpieczeństwa (safety performance targets - SPTs)[26] wyznaczonych w ramach SMS w celu wsparcia **celów bezpieczeństwa** organizacji.

Obecny	Odpowiedni	Sprawny	Skuteczny
Istnieje udokumentowany proces pomiaru poziomu bezpieczeństwa organizacji, obejmujący wszystkie odpowiednie obszary, w tym środki jakościowe i ilościowe powiązane z celami w zakresie bezpieczeństwa organizacji oraz pomiar skuteczności kontroli ryzyka bezpieczeństwa.	Środki ilościowe koncentrują się na tym, co ważne, a nie na tym, co łatwo zmierzyć. Wiarygodność źródeł danych jest brana pod uwagę przy projektowaniu środków jakościowych i/lub ilościowych, takich jak SPIs i SPTs. Środki jakościowe i ilościowe są powiązane ze zidentyfikowanym ryzykiem, skutecznością barier ochronnych i celami bezpieczeństwa. Zdefiniowano częstotliwość i odpowiedzialność za monitorowanie trendów środków jakościowych. Tam gdzie stosowne, postawiono realistyczne cele. W stosownych przypadkach brane są pod uwagę środki jakościowe i ilościowe związane z celami bezpieczeństwa Państwa z KPBwLC/KPB. Środki jakościowe i ilościowe uwzględniają kluczowe interfejsy wewnętrzne i zewnętrzne (lub ryzyko w relacjach), jeśli mają one znaczenie.	Poziom bezpieczeństwa mierzy się za pomocą środków jakościowych i ilościowych, które są stale monitorowane i analizowane pod kątem trendów tam, gdzie to konieczne. Skuteczność kontroli ryzyka bezpieczeństwa jest mierzona i wspiera proces podejmowania decyzji. Częstotliwość i odpowiedzialność za monitorowanie trendów środków jakościowych/ilościowych są odpowiednie i wiarygodne.	Środki jakościowe i ilościowe pokazują poziom bezpieczeństwa organizacji i skuteczność kontroli ryzyka w oparciu o wiarygodne dane. Dokonuje się przeglądu środków jakościowych i ilościowych oraz ich regularnej aktualizacji, aby zapewnić ich ważność/adekwatność. Przeglądy są następnie weryfikowane przez odpowiednią komórkę (organ) zarządzającą SMS i przyczyniają się do doskonalenia systemu. Jeżeli środki jakościowe i ilościowe wskazują, że kontrola ryzyka nie jest skuteczna, podejmowane są odpowiednie działania. Cele bezpieczeństwa z KPBwLC/KPB są odpowiednio uwzględniane, gdy ma to zastosowanie, a bieżący dialog z właściwym organem prowadzi do ciągłego doskonalenia procesów.

[26] Uwaga EASA: „poziom alarmowy" SPT, „wskaźniki wynikowe i wiodące" nie są wymagane przez EASA AMC. Jednakże są one obecnie wymienione w PQ ICAO AREA SSPIA (State Safety Programme Implementation Assessment). W nadchodzącej poprawce Załącznika 19, ICAO planuje dokonać przeglądu definicji „poziom bezpieczeństwa" w następujący sposób: Poziom bezpieczeństwa: wymierny wpływ organizacji na bezpieczeństwo oceniany za pomocą SPI, w razie potrzeby wspierany środkami jakościowymi. Podano także nową definicję SPI: środki metryczne lub ilościowe stosowane do pomiaru i monitorowania postępu organizacji dla osiągnięcia celów bezpieczeństwa [safety objectives]. Planuje się zatem, że poprawiona Norma ICAO 3.1.2. będzie w większym stopniu skupiać się na postępie w osiąganiu celów bezpieczeństwa poprzez pomiar i monitorowanie wyników organizacji. W stosownych przypadkach zastosowanie SPT i poziomów alarmowych będzie zależeć od uznania organizacji. Datą rozpoczęcia stosowania powinien być listopad 2026 r. (do potwierdzenia)

Wyniki oceny			

Czego szukać

- W jaki sposób monitoruje się i mierzy poziom bezpieczeństwa? Sprawdzić, czy zdefiniowano SPIs, SPTs, poziomy alarmowe i cele oraz czy są odpowiednie do działań organizacji i ryzyk.
- Sprawdzić, czy odpowiednio uwzględniono relacje (interfejsy) mające wpływ na działanie SMS (zob. Sekcja 5.1).
- W jaki sposób system zgłaszania zdarzeń skutecznie i terminowo umożliwia pomiar i ewaluację poziomu bezpieczeństwa organizacji? Działanie zgodnie z Rozporządzeniem (UE) nr 376/2014 w celu ciągłego doskonalenia SMS.
- W jaki sposób „monitorowanie zgodności" wspomaga monitorowanie i pomiar wyników poziomu bezpieczeństwa organizacji?
- Dowieść, że środki jakościowe lub ilościowe (takie jak SPIs, SPTs, poziomy alarmowe) opierają się na wszelkiego rodzaju wiarygodnych źródłach danych, informujących o wynikach organizacji i postępie w osiąganiu celów bezpieczeństwa.
- Sprawdzić, kiedy ostatni raz dokonano przeglądu środków/wskaźników jakościowych i ilościowych.
- Czy wskaźniki jakościowe skupiają się na tym, co ważne, a nie na tym, co łatwo zmierzyć. SPIs skupiają się na celach bezpieczeństwa i skuteczności barier, zwłaszcza zapobiegawczych: sprawdzić, czy pozwalają one na ciągłą poprawę wyników organizacji w czasie.
- Dowieść, czy środki jakościowe i ilościowe organizacji są zrównoważone (wiodące i wynikowe, na poziomie państwa/wytworzone samodzielnie/reprezentatywne dla celów bezpieczeństwa) i dokładnie odzwierciedlają obraz ryzyka organizacji i mogą służyć jako narzędzie do monitorowania jej poziomów bezpieczeństwa.
- Znaleźć dowód, że po osiągnięciu poziomów alarmowych organizacja podejmuje odpowiednie działania i w stosownych przypadkach, składa raport na wyższym szczeblu (SRB, komitety ds. bezpieczeństwa itp.).
- Uwzględnienie celów bezpieczeństwa pana poziomie krajowym (wynikających z KPBwLC i/lub KPB) zgodnie z Rozporządzeniem (UE) 2018/1139, art. 7 i 8;
- Rozważyć, czy jest brane pod uwagę monitorowanie celów bezpieczeństwa, w tym odpowiednich SPIs z EPAS, w szczególności tom II, zob. Sekcja 4.2 lub tom III, tam gdzie to konieczne (zob. Rozporządzenie (UE) 2018/1139, art. 6).
- Rozważyć każdy odpowiedni wskaźnik lub cel działania w zakresie bezpieczeństwa wynikający z rozporządzenia (UE) nr 376/2014, art. 13 i 14 lub ASR24 EASA[27] lub systemu zgłaszania zdarzeń (wewnętrzny, dobrowolny itp.), rocznego raportu/przeglądu bezpieczeństwa ICAO lub państwa (Sprawozdanie o stanie bezpieczeństwa w lotnictwie cywilnym) lub sprawozdań uznanych organizacji międzynarodowych (takich jak IATA, CANSO).
- Sprawdzić, czy podjęto jakiekolwiek działania, gdy monitorowanie poziomu bezpieczeństwa wskazuje na negatywny trend (odzwierciedlający nieskuteczną(-e) kontrolę(-e) ryzyka lub niewłaściwe środki jakościowe/ilościowe lub negatywny wpływ na wyniki organizacji).
- Sprawdzić, czy uwzględniono jakiekolwiek standardowe SPIs lub cele stosowane dla konkretnych obszarów zagrożeń lub w procesie monitorowania (np. programie monitorowania danych lotu dla operacji lotniczych; planie działania ANS) lub czy wzięto pod uwagę dobre praktyki/standardy branżowe.
- Znaleźć dowód na to, że wyniki monitorowania poziomu bezpieczeństwa są omawiane przez kierownictwo wyższego szczebla (przez SRB lub inny komitet ds. bezpieczeństwa lub inny, odpowiedni szczebel władzy w organizacji) i powiązane jest to z ciągłym doskonaleniem SMS (zob. Sekcja 3.3).
- Dowieść przekazywania informacji zwrotnej kierownikowi odpowiedzialnemu (accountable manager).
- Dowieść (tam, gdzie istotne) że po osiągnięciu poziomów alarmowych (związanych z SPTs) organizacja podejmuje odpowiednie działania i dokonuje przeglądu swoich celów bezpieczeństwa, gdy okaże się to konieczne.

[27] Począwszy od EASA ASR 2021, EASA planuje wydanie niektórych SPI w 2023 r. – w celu uzyskania dalszych informacji należy monitorować stronę internetową EASA

Odpowiednie odniesienia do przepisów UE/EASA				
Operacje lotnicze	**Załoga lotnicza**	**Lotniska**	**ATM/ANS**	**Organizacja szkolenia ATC**
ORO.GEN.200 „System zarządzania" punkt (a)(3) AMC1 ORO.GEN.200(a)(3) „System zarządzania" punkt (d)(1) – (operatorzy typu complex)	ORA.GEN.200 „System zarządzania" punkt (a)(3) AMC1 ORA.GEN.200(a)(3) „System zarządzania" punkt(d)(1) (organizacje typu complex)	ADR.OR.D.005 „System zarządzania" punkt (b)(5) AMC1 ADR.OR.D.005(b)(5) „System zarządzania"	ATM/ANS.OR.B.005(a)(3) AMC2 ATM/ANS.OR.B.005(a)(3) „System zarządzania" AMC1 ATS.OR.200(1)(v) „System zarządzania bezpieczeństwem" Rozporządzenie wykonawcze Komisji (UE) 2019/317 (i jego Załącznik I lub ostatnia zmiana	Nie dotyczy, jednakże zastosowanie mają przepisy dotyczące instytucji zapewniającej służby ruchu lotniczego.
CAMO	**PART 145**	**Organizacje produkujące/POA**	**Organizacje projektujące/DOA**	**Zarezerwowane**
GM1 CAMO.A.200 „System zarządzania" AMC1 CAMO.A.200(a)(1) „System zarządzania" punkt (b)(3)(i) CAMO.A.200 „System zarządzania" punkt (a)(3) AMC1 CAMO.A.200(a)(3) „System zarządzania" punkt (d) i (f)(5)	145.A.200 „System zarządzania" punkt (a)(3) AMC1 145.A.200(a)(3) „Kluczowe procesy zarządzania bezpieczeństwem" punkt (d) i (f)(5) 145.A.48 „Wykonanie obsługi technicznej" AMC1/2/3 145.A.48(c)(2) „Wykonanie obsługi technicznej" AMC1 145.A.48(c)(3) „Wykonanie obsługi technicznej" oraz GM1 145.A.70 „Charakterystyka organizacji obsługowej (MOE)" AMC1 145.A.70 „MOE" punkt 3.4	21.A.139 (c)(4)(i) „System zarządzanie produkcją" AMC1 21.A.139(c)(3) i (4) „Kluczowe procesy zarządzania bezpieczeństwem" punkt (e)	21.A.239 (c)(4)(i) „System zarządzanie produkcją" AMC1 21.A.239(c)(3) i (4) „Kluczowe procesy zarządzania bezpieczeństwem" punkt (e)	

PODSUMOWANIE KOMENTARZY do 3.1. „MIERZENIE I MONITOROWANIE POZIOMU BEZPIECZEŃSTWA”

3.2 Zarządzanie zmianą

Odniesienia i tekst Załącznika 19

3.2.1 Podmiot lotniczy opracowuje i zapewnia funkcjonowanie procesu mającego na celu **identyfikację zmian**, mogących mieć wpływ na poziom ryzyka bezpieczeństwa związanego z jego produktami lub usługami lotniczymi, oraz mający na celu identyfikację i **zarządzanie ryzykami, które mogą wynikać z tych zmian.**

Obecny	Odpowiedni	Sprawny	Skuteczny
Organizacja ustanowiła proces zarządzania zmianą w celu określenia, czy zmiany mają wpływ na bezpieczeństwo działań oraz w celu zarządzania znaczącymi, zidentyfikowanymi ryzykami zgodnie z istniejącymi procesami zarządzania ryzykiem bezpieczeństwa (zob. 2.2). W procesie definiowane są metody, obowiązki i ramy czasowe.	Zdefiniowano czynniki wpływające na proces zarządzania zmianami. Proces uwzględnia również zmiany związane z działalnością biznesową oraz powiązania z innymi organizacjami/działami, które mają wpływ na bezpieczeństwo.	Organizacja stosuje zdefiniowany proces zarządzania zmianami w celu określenia, czy istotne zmiany mają wpływ na bezpieczeństwo. Wszelkie zidentyfikowane ryzyka są zarządzane zgodnie z istniejącymi procesami zarządzania ryzykiem bezpieczeństwa i monitorowane poprzez zapewnienie bezpieczeństwa. W stosownych przypadkach brane są pod uwagę czynniki wewnętrzne i zewnętrzne, takie jak zagrożenia związane z czynnikami technicznymi, środowiskowymi, ludzkimi i organizacyjnymi.	Zarządzanie procesem zmian uwzględnia kumulację lub wpływ wielu zmian, a zmiany i wpływ na funkcje związane z bezpieczeństwem są komunikowane innym organizacjom, w tym wewnętrznym i zewnętrznym interesariuszom. Istnieje mechanizm umożliwiający dzielenie się informacjami dotyczącymi zarządzania wpływem zmian z zewnętrznymi interesariuszami (partnerami, dostawcami, wykonawcami itp.). Ryzyko związane z bezpieczeństwem jest zarządzane zgodnie z zakresem i harmonogramem zmian. Działania mające na celu ograniczenie ryzyka wynikające z zarządzania zmianami są częścią monitorowania wydajności SMS.
Wyniki oceny			

Czego szukać

- W proces zaangażowani są kluczowi interesariusze. Może to dotyczyć osób z innych działów organizacji i/lub organizacji zewnętrznych.
- Sprawdzić, co uruchamia proces „zarządzania zmianą”. Należy wziąć pod uwagę czynniki organizacyjne, finansowe, handlowe itp., a także wszelkie inne zmiany, które mogą mieć wpływ na bezpieczeństwo (np. cyberbezpieczeństwo, środowisko, kryzys sanitarny, choroba lub przechodzenie pracowników na emeryturę i przekazywanie wiedzy).
- Przejrzeć najnowsze zmiany, które przeszły proces oceny ryzyka.
- Sprawdzić, czy zmiana została podpisana przez odpowiednio upoważnioną osobę.

- Ryzyka przejściowe (transitional risks) są identyfikowane i zarządzane.
- Przejrzeć działania następcze, takie jak sprawdzenie, czy jakiekolwiek przyjęte założenia zostały pozytywnie zweryfikowane.
- Sprawdzić, czy istnieje wpływ na poprzednie oceny ryzyka i istniejące zagrożenia.
- Sprawdzić, czy uwzględniono skumulowany efekt (przy zaistnieniu) wielu zmian.
- Sprawdzić, czy zmiany związane z biznesem uwzględniają ryzyko bezpieczeństwa (restrukturyzacja organizacyjna, zwiększenie lub zmniejszenie zatrudnienia, projekty informatyczne itp.).
- Znaleźć dowód na rozwiązywanie problemów związanych z wydajnością człowieka (HP - human performance) podczas zmian.
- Ocenić, czy działania mające na celu ograniczenie ryzyka wynikające z tych zmian są oczywiste i zgodne z pozytywnymi trendami w monitorowaniu wydajności.
- Przejrzeć wpływ zmian na szkolenia i kompetencje.
- Przejrzeć poprzednie (w pełni wprowadzone) zmiany, aby upewnić się, że pozostają pod kontrolą.
- Rozważyć, w jaki sposób komunikowane są przyczyny tych zmian oraz w jaki sposób zmiany są planowane i komunikowane osobom, których zmiana dotyczy zewnętrznie i wewnętrznie. Zastanowić się, w jaki sposób strony (inne działy, partnerzy, dostawcy, kontrahenci, właściwe organy) dotknięte zmianami są zaangażowane w proces.
- Sprawdzić, czy standardowe ustalenia umowne dotyczą „zarządzania zmianami" po obu stronach umowy. Sprawdzić dowody wdrożenia.

Odpowiednie odniesienia do przepisów UE/EASA				
Operacje lotnicze	**Załoga lotnicza**	**Lotniska**	**ATM/ANS**	**Organizacja szkolenia ATC**
ORO.GEN.200 „System zarządzania" punkt (a)(3) AMC1 ORO.GEN.200(a)(3) „System zarządzania" punkt (e) – (operatorzy typu complex) AMC1 ORO.GEN.200(a)(1);(2);(3);(5) „System zarządzania" punkt (b) – {operatorzy typu non-complex)	ORA.GEN.200 „System zarządzania" punkt (a)(3) AMC1 ORA.GEN.200(a)(3) „System zarządzania" punkt (e) – (organizacje typu complex) AMC1 ORA.GEN.200(a)(1);(2);(3);(5) „System zarządzania" punkt (b) – (organizacje typu non-complex)	ADR.OR.D.005 „System zarządzania" punkt (b)(6) AMC1 ADR.OR.D.005(b)(6) „System zarządzania" ADR.OR.B.040 „Zmiany" w szczególności punkt (f)"	ATM/ANS.OR.A.040 „Zmiany – wymagania ogólne" ATM/ANS.OR.A.045 „Zmiany w systemie funkcjonalnym" ATM/ANS.OR.B.005(a)(4) ATM/ANS.OR.B.010 „Zmiany – wymagania ogólne" ATS.OR.205 „Ocena bezpieczeństwa i zapewnianie bezpieczeństwa w odniesieniu do zmian w systemie funkcjonalnym" ATS.OR.210 „Kryteria bezpieczeństwa"	AMC1 ATCO.OR.C.001(e) „System zarządzania organizacji szkoleniowych" punkt (c)
CAMO	**PART 145**	**Organizacje produkujące/POA**	**Organizacje projektujące/DOA**	**Zarezerwowane**
CAMO.A.130 „Zmiany" AMC2 CAMO.A.130 GM1 CAMO.A.200(a)(1) „System zarządzania" punkt (d)(3)	145.A.85 „Zmiany w organizacji" AMC2 145.A.85 „Zarządzanie zmianami"	21.A.139 „System zarządzania produkcją" punkt (c)(4)(ii) AMC1 21.A.139(c)(3) i (4) „Kluczowe procesy zarządzania bezpieczeństwem" punkt (f)	21.A.239 „System zarządzania projektowaniem" punkt (c)(4)(i) AMC1 21.A.239(c)(3) i (4) „Kluczowe procesy zarządzania bezpieczeństwem" punkt (f)	

CAMO.A.200 „System zarządzania” punkt (a)(3) AMC1 CAMO.A.200 (a)(3) „Zarządzanie zmianą” punkt (e) GM2 CAMO.A.200 (a)(3) „Zarządzanie zmianą” CAMO.A.300(a)(11) i (c)	GM1 145.A.200 „System zarządzania – wymagania ogólne” AMC1 145.A.200(a) (3) „Kluczowe procesy zarządzania bezpieczeństwem” punkt (e) 145.A.70 „Charakterystyka organizacji obsługowej (MOE)” punkt (a)(10) i (c) AMC1 145.A.70 „MOE” punkt 3.5	21.A.147 „Zmiany w zatwierdzonej organizacji produkującej” AMC1 21.A.147 „Wniosek o zatwierdzenie istotnych zmian lub różnic w zakresie lub warunkach POA” GM1 21.A.147 „Istotne zmiany” 21.A.143 „Charakterystyka organizacji produkującej (POE)” punkt (c) GM1 21.A.143 „Charakterystyka organizacji produkującej (POE)” AMC1 21.A.143 (a)(1) „Charakterystyka organizacji produkującej (POE)”	21.A.247 „Zmiany w systemie zarządzania organizacji projektującej” AMC1 21.A.247 „Wniosek o zatwierdzenie istotnych zmian lub różnic w zakresie lub warunkach DOA” GM1 21.A.247 „Istotne zmiany w systemie zarządzania organizacji projektującej” 21.A.243 „Podręcznik” punkt (c) 21.A.265 „Obowiązki posiadacza” punkt (a) AMC1 21.A.265(a) „Administracja podręcznika”	

PODSUMOWANIE KOMENTARZY do 3.2. „ZARZĄDZANIE ZMIANĄ”

3.3 Ciągłe doskonalenie SMS

Odniesienia i tekst Załącznika 19

3.3.1 Podmiot lotniczy monitoruje i ocenia procesy w ramach swojego SMS w celu utrzymania lub ciągłego podnoszenia całościowej efektywności SMS.

Obecny	Odpowiedni	Sprawny	Skuteczny
Istnieje udokumentowany proces monitorowania i sprawdzania efektywności/skuteczności SMS przy użyciu dostępnych danych i informacji.	Cały system, w tym działania związane z zapewnieniem bezpieczeństwa, generuje dane/informacje SMS, które są okresowo przeglądane przez organizację w celu poprawy wdrażania SMS. Informacje zewnętrzne są również brane pod uwagę. Właściwi kierownicy wyższego szczebla są szczególnie zaangażowani (w przypadkach, gdy zaangażowane są różne działy w organizacji). Podejmowanie decyzji odbywa się na podstawie danych.	Istnieją dowody na to, że SMS jest poddawany okresowym przeglądom w celu wsparcia oceny jego skuteczności oraz, że podejmowane są odpowiednie działania. SMS jest okresowo przeglądany przez kadrę kierowniczą wyższego szczebla w celu wsparcia oceny jego skuteczności i podejmowane są odpowiednie działania. Organizacja wykorzystuje SMS i dane dotyczące bezpieczeństwa do opracowywania i oceny skuteczności SPIs w celu poprawy bezpieczeństwa i ciągłego doskonalenia procesów SMS.	Ocena skuteczności SMS wykorzystuje wiele źródeł informacji, w tym analizę danych dotyczących bezpieczeństwa, która wspiera decyzje dotyczące ciągłego doskonalenia. Pomiar poziomu bezpieczeństwa (safety performance) uwzględnia ciągłe doskonalenie SMS w sposób proaktywny, a także cele bezpieczeństwa, które są regularnie aktualizowane. Uwzględnia się wkład SMS i danych dotyczących bezpieczeństwa w relacjach z kluczowymi zewnętrznymi organizacjami (key external interface organisations). Opracowano rzetelny i kompleksowy zestaw danych dotyczących SMS i bezpieczeństwa (baza danych SMS z zarządzaniem danymi), który wspiera wykorzystanie analizy danych predykcyjnych. Organizacja dzieli się najlepszymi praktykami i doświadczeniami jako światowy lider w dziedzinie SMS.
Wyniki oceny			

Czego szukać

- Jakiego rodzaju informacje i źródła wspierają ciągłe doskonalenie SMS? Należy sprawdzić, w jakim stopniu organizacja zwraca uwagę na informacje pochodzące ze źródeł wewnętrznych i zewnętrznych, wyniki rozporządzenia (UE) nr 376/2014 (w szczególności art. 13), raporty z badań zdarzeń; automatyczne gromadzenie danych (takie jak monitorowanie danych lotniczych dla operatorów lotniczych); spotkania dotyczące bezpieczeństwa, warsztaty, seminaria, raporty dotyczące zagrożeń, profil ryzyka sektora; audyty i statystyki z funkcji monitorowania zgodności, analizy danych dotyczących bezpieczeństwa, KPBwLC i/lub KPB, plany działania w zakresie bezpieczeństwa opracowane przez branżę i EASA, np. dla śmigłowców, EPAS (w szczególności zob. Sekcja 4, w której proponuje się SPI do monitorowania), roczny przegląd bezpieczeństwa (ASR) ICAO lub EASA lub krajowe Sprawozdania o stanie bezpieczeństwa lotnictwa cywilnego - Urząd Lotnictwa Cywilnego lub ASR uznanych organizacji międzynarodowych (takich jak IATA, CANSO); Promocja bezpieczeństwa przez państwo, właściwy organ i akceptacja SPI/SPT zgodnie z zaleceniem 3.3.2.2 załącznika 19 itp.
- Przegląd informacji i danych dotyczących bezpieczeństwa wykorzystywanych do podejmowania decyzji zarządczych w celu ciągłego doskonalenia.
- Dowody:
  - Wykorzystanie zdobytych doświadczeń w SMS i procesach operacyjnych.

- Poszukiwanie i stosowanie najlepszych praktyk.
- Przeprowadzanie badań i ocen kultury organizacyjnej oraz podejmowanie odpowiednich działań.
- Analizowanie danych i przekazywanie wyników komitetom ds. bezpieczeństwa.
- Dowody podjęcia działań następczych.

– W jaki sposób pomiar wyników usługodawcy w zakresie bezpieczeństwa jest powiązany z celami bezpieczeństwa? W jaki sposób takie procesy są aktualizowane? Sprawdzić, czy stosowana jest metodologia, dzięki której cele bezpieczeństwa są wyrażane i opracowywane, a powiązane wskaźniki SPIs są SMART, ulepszane i zrównoważone (wynikowe/wiodące, na poziomie krajowym/generowane samodzielnie), dokładnie odzwierciedlają obraz ryzyka i służą monitorowaniu i ciągłemu doskonaleniu wyników w zakresie bezpieczeństwa. Sprawdzić, czy SPTs powiązane z celami bezpieczeństwa organizacji są monitorowane pod kątem ciągłego doskonalenia w czasie (jako minimum), zgodnie z rozporządzeniem (UE) 1139/2018.
Ocenić zaangażowanie i przywództwo kierownictwa wyższego szczebla w zakresie ciągłego doskonalenia SMS, biorąc pod uwagę poniesione koszty i zwrot z inwestycji.

Odpowiednie odniesienia do przepisów UE/EASA				
Operacje lotnicze	**Załoga lotnicza**	**Lotniska**	**ATM/ANS**	**Organizacja szkolenia ATC**
Rozporządzenie 216/2008-Zasadnicze wymagania dotyczące operacji lotniczych, punkt 8.a.4 ORO.GEN.200 “System zarządzania” punkt (a)(3) i (a)(6) AMC1 ORO.GEN.200(a)(3) “System zarządzania” punkt (f) – (operatorzy typu complex) AMC1 ORO.GEN.200(a)(1)(2)(3) (5) “System zarządzania” punkt (e) – (operatorzy typu non-complex)	Rozporządzenie 216/2008-Zasadnicze wymagania dotyczące licencjonowania pilotów, punkt 3.a.1(ii) dla ATO i 4.c.1(ii) dla AMC (Aero-Medical Centre)(Centrum Medycyny Lotniczej - CML) ORA.GEN.200 „System zarządzania” – punkt (a)(3) i (a)(6) AMC1 ORA.GEN.200(a)(3) “System zarządzania” punkt (f) – (organizacje typu complex) AMC1 ORA.GEN.200(a)(1);(2);(3);(5) “System zarządzania” punkt (e) – (organizacje typu non-complex)	ADR.OR.D.005 „System zarządzania” punkt (b)(7) AMC1 ADR.OR.D.005(b)(7) „System zarządzania”	ATS.OR.200(2)(iii) „System zarządzania bezpieczeństwem” Rozporządzenie wykonawcze Komisji (UE) 2019/317 lub ostatnia zmiana)	AMC1 ATCO.OR.C.001(e) „System zarządzania organizacji szkoleniowych” punkt (b)

CAMO	PART 145	Organizacje produkujące/POA	Organizacje projektujące/DOA	Zarezerwowane
CAMO.A.200 „System zarządzania” punkt (a)(3) i (a)(6) AMC1 CAMO.A.200(a)(3) „Ciągłe doskonalenie” punkt (d) i (f) AMC and GM to CAMO.A.200(a)(6) „Monitorowanie zgodności”	145.A.200 „System zarządzania” punkt (a)(3)i (c)(6) AMC1 145.A.200(a)(3) „Kluczowe procesy zarządzania bezpieczeństwem” punkt (f) AMC and GM to 145.A.200(a)(6) „Monitorowanie zgodności” 145.A.48 „Wykonanie obsługi technicznej” AMC1 145.A.70 „MOE” punkt 2.23	21.A.139 „System zarządzania produkcją” punkt (c)(4)(ii) i (c)(6) GM1 21.A.139(c) „System zarządzania bezpieczeństwem” AMC1 21.A.139(c)(3) i (4) „Kluczowe procesy zarządzania bezpieczeństwem” punkt (g) 21.A.3A „System raportowania” GM1 21.A.3A „Związek pomiędzy punktem 21.A.3A a Rozporządzeniem (UE) nr 376/2014”	21.A.239 „System zarządzania projektowaniem” punkt (c)(4)(iii) i (c)(6) GM1 21.A.239(c) „System zarządzania bezpieczeństwem” AMC1 21.A.239(c)(3) i (4) „Kluczowe procesy zarządzania bezpieczeństwem” punkt (g) 21.A.3A „System raportowania” GM1 21.A.3A „Związek pomiędzy punktem 21.A.3A, a Rozporządzeniem (UE) nr 376/2014”	

PODSUMOWANIE KOMENTARZY do 3.3. „CIĄGŁE DOSKONALENIE SMS”

4 PROMOWANIE BEZPIECZEŃSTWA

4.1 Szkolenie i kształcenie

Odniesienia i tekst Załącznika 19

4.1.1 Podmiot lotniczy opracowuje i zapewnia funkcjonowanie programu szkolenia z zakresu bezpieczeństwa gwarantującego, że personel jest przeszkolony i ma odpowiednie kompetencje do wykonywania swoich obowiązków związanych z SMS.

Zakres programu szkolenia z zagadnień dotyczących bezpieczeństwa ma być proporcjonalny do udziału danej osoby w SMS.

Obecny	Odpowiedni	Sprawny	Skuteczny
Istnieje program szkoleń SMS, który obejmuje szkolenia wstępne i okresowe.	Szkolenie obejmuje indywidualne obowiązki z zakresu bezpieczeństwa (safety duties) (w tym role, obowiązki i odpowiedzialność) oraz sposób działania SMS organizacji. Materiały i metodologia szkoleń są dostosowane do odbiorców oraz, jeśli to konieczne, uwzględniają wydajność człowieka. Zidentyfikowano cały personel wymagający szkolenia.	Program szkoleniowy SMS zapewnia odpowiednie szkolenia różnym pracownikom organizacji i jest prowadzony przez kompetentny personel.	Szkolenie SMS jest oceniane pod kątem wszystkich aspektów (cele nauczania, treść, metody i style nauczania, testy) i jest powiązane z oceną kompetencji. Szkolenia są rutynowo poddawane przeglądom w celu uwzględnienia informacji zwrotnych z różnych źródeł.
Wyniki oceny			

Czego szukać

- Przejrzeć program szkoleń SMS, w tym treść kursu i metodę jego realizacji.
- Sprawdzić, czy szkolenia obejmują indywidualne obowiązki w zakresie bezpieczeństwa (safety duties) (w tym role, obowiązki i odpowiedzialność) oraz sposób działania SMS organizacji.
- Czy szkolenie uwzględnia informacje zwrotne ze zdarzeń zewnętrznych, raporty z badania zdarzeń, spotkania dotyczące bezpieczeństwa, raporty o zagrożeniach, wyniki audytów, analizę danych dotyczących bezpieczeństwa, oceny szkolenia itp.?
- Sprawdzić, czy szkolenia obejmują czynnik ludzkie i organizacyjny, kulturę i umiejętności nietechniczne, mając na celu zmniejszenie ryzyka organizacyjnego, które może prowadzić do błędów ludzkich.
- Porównać dokumentację ze szkoleń z programem szkolenia.
- Sprawdzić, w jaki sposób oceniane i utrzymywane są kompetencje szkolących.
- Sprawdzić, czy istnieje proces pomiaru efektywności szkoleń i podjęcia odpowiednich działań w celu ich poprawy. Jak oceniana jest efektywność/skuteczność szkolenia?
- Sprawdzić w jaki sposób ocenia się szkolenia dla nowych pracowników i w przypadkach zmiany stanowisk.
- Przejrzeć wybraną ocenę szkolenia.
- Zapytać pracowników o ich własne rozumienie swoich obowiązków w zakresie bezpieczeństwa (safety duties) w SMS organizacji.
- Sprawdzić, czy przypomina się całemu personelowi o konieczności przestrzegania procedur SMS.

- W jaki sposób ciągłe doskonalenie SMS a także monitorowanie i pomiar poziomu bezpieczeństwa (safety performance) podmiotu lotniczego uwzględniane są w okresowych szkoleniach w obszarze bezpieczeństwa (recurrent safety training)?
- Jeżeli kilku operatorów tworzących część jednej grupy biznesowej przewoźnika lotniczego korzysta z tego samego CAMO do zarządzania ciągłą zdatnością do lotu wszystkich eksploatowanych przez siebie statków powietrznych, należy sprawdzić, czy szkolenie prowadzone przez CAMO spełnia potrzeby różnych zaangażowanych operatorów, uwzględnia ich różne polityki i procedury (operacyjne), obowiązki i sposoby komunikacji, obszary relacji (interfejsów) (zob. M.A.201(ea) oraz CAMO.A.200(e)).

Odpowiednie odniesienia do przepisów UE/EASA				
Operacje lotnicze	**Załoga lotnicza**	**Lotniska**	**ATM/ANS**	**Organizacja szkolenia ATC**
ORO.GEN.200 “System zarządzania” punkt (a)(4) AMC1 ORO.GEN.200(a)(4) “System zarządzania” punkt (a)	ORA.GEN.200 „System zarządzania” – punkt (a)(4) AMC1 ORA.GEN.200(a)(4) “System zarządzania” punkt (a)	ADR.OR.D.005 „System zarządzania” (b)(8) AMC1 ADR.OR.D.005(b)(8)	ATM/ANS.OR.B.005 (a)(6) Załącznik IV ATS.OR.200 “System Zarządzania bezpieczeństwem” punkt (4)(i)	ATCO.OR.C.001 „System zarządzania organizacji szkoleniowych” punkt (d)
CAMO	**PART 145**	**Organizacje produkujące/POA**	**Organizacje projektujące/DOA**	**Zarezerwowane**
GM1 CAMO.A.200 „System zarządzania” punkt (a)(4) CAMO.A.200 „System zarządzania” punkt (a)(4) i GM1 AMC1 CAMO.A.200(a)(4) „System zarządzania” punkt (a) „Komunikowanie spraw dotyczących bezpieczeństwa” CAMO.A.305 „Wymagania dotyczące personelu” punkt (g) i AMC/GM, w szczególności AMC3 CAMO.A.305 (g) „Szkolenie z bezpieczeństwa (w tym czynnik ludzki)”, AMC 3 CAMO.A.305 (g) GM1 i 2 CAMO A.305(g) AMC1 CAMO.A.202 „Wewnętrzny system zgłaszania kwestii związanych z bezpieczeństwem” punkt (b)(5) i (c)(3) M.A.201(ea) a także CAMO.A.200 (e) – w połączeniu z AMC i GM AMC M.A.306(b) punkt (c)	145.A.30(e) i AMC3, AMC4, GM1. GM1 145.A.200 punkt (f) 145.A.200 „System zarządzania” punkt (a)(4) AMC1 145.A.200(a)(4) „Komunikowanie spraw dotyczących bezpieczeństwa” GM1 145.A.200(a)(4) „Promocja bezpieczeństwa” 145.A.48 „Wykonanie obsługi technicznej” AMC2 145.A.48(c)(2) punkt (b) (8) 145.A.70 „Charakterystyka organizacji obsługowej (MOE)” AMC1 145.A.70 „MOE” punkt 3.6 145.A.60 „Zgłaszanie zdarzeń” 145.A.202 „Wewnętrzny system zgłaszania kwestii związanych z bezpieczeństwem” AMC1 145.A.202 „Wewnętrzny system zgłaszania kwestii związanych z bezpieczeństwem” punkt (b)(5)	21.A.139 „System zarządzania produkcją” punkt (c)(5)(i) AMC1 21.A.139(c)(5)(i) „Szkolenia z zakresu bezpieczeństwa” GM1 21.A.139(c)(5)(i) „Szkolenia z zakresu bezpieczeństwa” AMC2 21.A.145(a) „Liczba i kompetencje personelu” punkt (g) i (h)	21.A.239 „System zarządzania projektowaniem” punkt (c)(5)(i) AMC1 21.A.239(c)(5)(i) „Szkolenia z zakresu bezpieczeństwa” GM1 21.A.139(c)(5)(i) „Szkolenia z zakresu bezpieczeństwa” AMC1 21.A.245(e) „Personel, zaplecze i koordynacja” punkt (e)	

4.1.2 Kompetencje (wymagania EASA)

Odniesienia i tekst Załącznika 19

Wymagania dotyczące utrzymywania personelu przeszkolonego i kompetentnego do wykonywania zadań związanych z bezpieczeństwem i zachowaniem zgodności:

- Istnieje proces, który ocenia kompetencje danej osoby i w razie potrzeby podejmuje odpowiednie działania zaradcze.
- Kompetencje szkolących są zdefiniowane i oceniane; w razie potrzeby podejmowane są odpowiednie działania zaradcze.

Obecny	Odpowiedni	Sprawny	Skuteczny
Określono ramy kompetencji dla personelu mającego wpływ na bezpieczeństwo, w tym dla osób prowadzących szkolenia.	Istnieje proces okresowej oceny rzeczywistych kompetencji w zakresie bezpieczeństwa w odniesieniu do przyjętych ram kompetencji.	Istnieją dowody na to, że proces oceny kompetencji jest stosowany i rejestrowany.	Program i proces oceny kompetencji są rutynowo przeglądane i doskonalone. W razie potrzeby, w ramach oceny kompetencji, podejmowane są odpowiednie działania zaradcze, które są uwzględniane w programie szkoleniowym.
Wyniki oceny			

Czego szukać

- Sprawdzić, w jaki sposób przeprowadzana jest ocena kompetencji podczas pierwszego zatrudnienia i w sposób cykliczny.
- Czy istnieje proces, który ocenia kompetencje danej osoby i w razie potrzeby podejmuje odpowiednie działania naprawcze? Czy uwzględnia on „wydajność człowieka”?
- Sprawdzić, czy ocena kompetencji obejmuje ocenę kompetencji w zakresie obowiązków i odpowiedzialności związanych z bezpieczeństwem, a także zarządzanie zgodnością.
- Czy kompetencje trenerów są zdefiniowane i oceniane?
- Czy w razie potrzeby podejmowane są odpowiednie działania naprawcze?
- W przypadku umów międzynarodowych sprawdzić, czy wszyscy odpowiedni pracownicy posiadają wystarczające umiejętności w zakresie wspólnego języka, takiego jak angielski, oraz w zakresie korzystania z dokumentacji.

Odpowiednie odniesienia do przepisów UE/EASA

Operacje lotnicze	Załoga lotnicza	Lotniska	ATM/ANS	Organizacja szkolenia ATC
ORO.GEN.200 „System zarządzania” punkt (a)(4) AMC1 ORO.GEN.200(a)(4) „System zarządzania” punkt (a)(4)	ORA.GEN.200 „System zarządzania” punkt (a)(4) AMC1 ORA.GEN.200(a)(4) „System zarządzania” punkt (a)	ADR.OR.D.005 „System zarządzania” punkt (b)(8) AMC1 ADR.OR.D.005(b)(8)	ATM/ANS.OR.B.005(a)(6) Załącznik IV ATS.OR.200 „System zarządzania bezpieczeństwem” punkt (4)(i)	AMC1 ATCO.OR.C.001(d) „System zarządzania organizacji szkoleniowych PERSONEL”

CAMO	PART 145	Organizacje produkujące/POA	Organizacje projektujące/DOA	Zarezerwowane
CAMO.A.200 „System zarządzania” punkt (a)(4) CAMO.A.305(g) „Wymagania dotyczące personelu” oraz AMC w zakresie „Kompetencje” GM1 CAMO.A.200 „System zarządzania” punkt (f) AMC1 CAMO.A.202 „Wewnętrzny system zgłaszania kwestii związanych z bezpieczeństwem” punkt (b)(5) GM1 CAMO.A.305(b) „Wymagania dotyczące personelu” AMC CAMO.A.305(g) punkt 8 „Wymagania w stosunku do personelu”	145.A.200 „System zarządzania” punkt (a)(4) 145.A.30 „Wymagania dotyczące personelu” AMC1 145.A.30(cc) „Wiedza, pochodzenie i doświadczenie osoby/osób nominowanej/nominowanych” AMC1 145.A.30(e) „Cele oceny kompetencji” AMC2 145.A.30(e) „Procedura oceny kompetencji” oraz GM2 145.A.30(e) AMC4 145.A.30(e) „Szkolenia z zakresu bezpieczeństwa (z włączeniem wydajności człowieka)” GM4 145.A.30(e) „Kompetencje kierownika ds. bezpieczeństwa” 145.A.35 „Personel poświadczający i personel wspomagający” oraz AMC	21.A.139 „System zarządzania produkcją” punkt (d)(2)(xi) 21.A.145 „Zasoby” punkt (c)2 i (d) AMC2 21.A.145(a) „Liczba i kompetencje personelu” punkt (g) AMC2 21.A.145(c)(2) „Kompetencje kadry kierowniczej”	21.A.245 „Zasoby” punkt (e) AMC1 21.A.245(e) „Personel, zaplecze i koordynacja” punkt (b) i (e) AMC1 21.A.245 (d) „Ścieżka zgłaszania i kompetencje kierownictwa” punkt b)	

PODSUMOWANIE KOMENTARZY do 4.1 „SZKOLENIE I KSZTAŁCENIE” ORAZ „KOMPETENCJE”

4.2 Komunikacja dotycząca bezpieczeństwa

Odniesienia i tekst Załącznika 19

4.2.1 Podmiot lotniczy opracowuje i zapewnia funkcjonowanie formalnych narzędzi służących do przekazywania informacji bezpieczeństwa, które:

a) zapewniają, że personel jest w pełni świadomy działania SMS, na poziomie odpowiednim do zajmowanego stanowiska;
b) przekazują informacje krytyczne dla bezpieczeństwa;
c) wyjaśniają dlaczego podejmowane są określone działania w celu poprawy bezpieczeństwa; oraz
d) wyjaśniają dlaczego są wprowadzane lub zmieniane procedury bezpieczeństwa.

Zob. także Rozporządzenie (UE) nr 376/2014 (Artykuł 13(3)).

Obecny	Odpowiedni	Sprawny	Skuteczny
Istnieje proces przekazywania informacji krytycznych dla bezpieczeństwa.	Proces określa co, kiedy i jak ma być przekazane (w zakresie informacji dotyczących bezpieczeństwa). W stosownych przypadkach proces obejmuje zakontraktowane organizacje i personel. Środki komunikacji dostosowane są do: - wielkości i złożoności organizacji; - odbiorcy informacji i znaczenia tego, co jest przekazywane.	Informacje krytyczne dla bezpieczeństwa są identyfikowane i przekazywane w organizacji całemu personelowi (w stosownych przypadkach) włącznie ze współpracującymi organizacjami i personelem kontraktowym (tam, gdzie to konieczne).	Organizacja skutecznie analizuje i przekazuje informacje krytyczne dla bezpieczeństwa za pomocą różnych metod, w zależności od przypadku, w celu łatwego ich zrozumienia. Ocenia się komunikację dotyczącą bezpieczeństwa w celu ustalenia, w jaki sposób jest ona wykorzystywana i rozumiana oraz (w stosownych przypadkach) w celu jej doskonalenia. Widoczna jest promocja polityki bezpieczeństwa i pozytywnej kultury bezpieczeństwa. Podejmowanie decyzji, działania i komunikacja odzwierciedlają pozytywną kulturę bezpieczeństwa i przywództwo w zakresie bezpieczeństwa, wykazujące zaangażowanie we wdrażanie polityki bezpieczeństwa.
Wyniki oceny			

Czego szukać
Uwaga 1: komunikacja jest niezbędna do budowania pozytywnej kultury bezpieczeństwa poprzez zgłaszanie zagrożeń lub wymianę informacji dotyczących bezpieczeństwa. – Przejrzeć źródła informacji wykorzystywane w ramach komunikacji dotyczącej bezpieczeństwa – Dokonać przeglądu metod stosowanych do przekazywania informacji dotyczących bezpieczeństwa (np. spotkania, prezentacje, odprawy, filmy, e-maile, strony internetowe, aktualności, ulotki, biuletyny, plakaty itp.). – Ocenić, czy środki komunikacji są odpowiednie, biorąc pod uwagę strukturę organizacji i odbiorców. Komunikat powinien być prosty i zwięzły, aby był łatwo zrozumiany. – Czy środki przekazu informacji dotyczących bezpieczeństwa są poddawane przeglądowi pod kątem ich skuteczności i czy materiały są wykorzystywane do aktualizacji odpowiedniego szkolenia? – Sprawdzić, czy przekazywane są wnioski wyciągnięte z badania/analizy istotnych zdarzeń i zmian w organizacji. – Sprawdzić, czy regularnie promowana jest pozytywna kultura bezpieczeństwa (positive safety culture), w tym kultura zgłaszania (gdzie, jak, kiedy itp.) oraz zasady kultury sprawiedliwego traktowania (just culture). – Sprawdzić dostępność informacji dotyczących bezpieczeństwa. – Zapytać personel o wszelkie najnowsze komunikaty dotyczące bezpieczeństwa. – Sprawdzić, czy informacje o zdarzeniach są terminowo przekazywane kluczowym interesariuszom (wewnętrznym i zewnętrznym) i czy zostały odpowiednio zanonimizowane. – Czy organizacja odpowiednio rozszerza komunikację dotyczącą bezpieczeństwa na zewnętrznych kluczowych interesariuszy (np. klientów, dostawców)? – Sprawdzić, czy personel wie, gdzie znaleźć cele bezpieczeństwa i powiązane wskaźniki służące monitorowaniu poziomu bezpieczeństwa. Sprawdzić, czy personel zna cele bezpieczeństwa w swojej dziedzinie kompetencji. Czy organizacja komunikuje stan osiągnięcia (lub wyników monitorowania) celów bezpieczeństwa?

Odpowiednie odniesienia do przepisów UE/EASA				
Operacje lotnicze	**Załoga lotnicza**	**Lotniska**	**ATM/ANS**	**Organizacja szkolenia ATC**
ORO.GEN.200 „System zarządzania” punkt (a)(4) ORO.GEN.200 „System zarządzania” punkt (a)(5) AMC1 ORO.GEN.200(a)(4) “System zarządzania” punkt (b)	ORA.GEN.200 „System zarządzania” – punkt (a)(4) ORA.GEN.200 „System zarządzania” – punkt (a)(5) AMC1 ORA.GEN.200(a)(4) „System zarządzania” punkt (b)	ADR.OR.D.005 „System zarządzania” punkt (b)(9) AMC1 ADR.OR.D.005(b)(9) „System zarządzania”	ATM/ANS.OR.B.005(a)(7) ATS.OR.200(4)(ii) AMC1 ATM/ANS.OR.B.005(a)(7) „System zarządzania”	Nie dotyczy, jednakże zastosowanie mają przepisy dotyczące instytucji zapewniającej służby ruchu lotniczego.

CAMO	PART 145	Organizacje produkujące/POA	Organizacje projektujące/DOA	Zarezerwowane
CAMO.A.200 „System zarządzania" punkt (a)(4) AMC1 CAMO.A.200(a)(4) „Komunikacja dotycząca bezpieczeństwa" GM1 CAMO.A.200 (a)(4) „Promocja bezpieczeństwa" CAMO.GEN.200 „System zarządzania" punkt (a)(5) oraz GM1	145.A.200 „System zarządzania" punkt (a)(4) AMC1 145.A.200(a)(4) „Komunikacja dotycząca bezpieczeństwa" GM1 145.A.200(a)(4) „Promocja bezpieczeństwa"	21.A.139 „System zarządzania produkcją" punkt (c)(5)(ii) AMC1 21.A.139(c)(5) „Komunikacja dotycząca bezpieczeństwa" GM1 21.A.139(c)(5) „Promocja bezpieczeństwa"	21.A.239 „System zarządzania projektowaniem" punkt (c)(5)(ii) AMC1 21.A.239(c)(5) „Komunikacja dotycząca bezpieczeństwa" GM1 21.A.239(c)(5) „Promocja bezpieczeństwa"	

PODSUMOWANIE KOMENTARZY do 4.2. „KOMUNIKACJA DOTYCZĄCA BEZPIECZEŃSTWA"

5 DODATKOWE ELEMENTY DO ROZWAŻENIA

5.1 Zarządzanie relacjami (interface management)

Odniesienia i tekst Załącznika 19

5.1.1 Dodatek 2 uwaga 2 – Relacje (interfejsy) podmiotu lotniczego z innymi organizacjami mogą znacząco przyczynić się do bezpieczeństwa jego produktów lub usług. Wytyczne dotyczące zarządzania interfejsem w odniesieniu do systemu zarządzania bezpieczeństwem znajdują się w Podręczniku Zarządzania Bezpieczeństwem (SMM) (Doc 9859).

Uwaga 1: Te dodatkowe elementy uwzględnione w ocenie odnoszą się do wymagań Systemu Zarządzania EASA lub nowych uwag w Wydaniu 2 Załącznika 19. Uważa się je za ważny element efektywnego SMS.

Obecny	Odpowiedni	Sprawny	Skuteczny
Organizacja zidentyfikowała i udokumentowała odpowiednie wewnętrzne i zewnętrzne relacje (interfejsy) oraz ich krytyczny charakter.	Sposób zarządzania relacjami (interfejsami) jest odpowiedni do ich krytycznego znaczenia dla bezpieczeństwa. Określono środki przekazywania informacji dotyczących bezpieczeństwa. W umowach odpowiednio uwzględniono krytyczne znaczenie relacji (interfejsów) dla bezpieczeństwa oraz konieczność odpowiedniego uwzględnienia identyfikacji zagrożeń i oceny ryzyka (HIRA), w tym środków ograniczających ryzyko.	Organizacja zarządza interfejsami poprzez identyfikację zagrożeń i zarządzanie ryzykiem. Prowadzona jest weryfikacja działań mająca na celu ocenę środków ograniczających ryzyko podejmowanych przez organizacje zewnętrzne.	Organizacja dobrze rozumie zarządzanie relacjami (interfejsami) i istnieją dowody na to, że ryzyko z nimi związane, mające kluczowe znaczenie dla bezpieczeństwa, jest identyfikowane i podejmowane są odpowiednie działania. Organizacje współpracujące dzielą się informacjami dotyczącymi bezpieczeństwa, zarządzają zmianami i podejmują działania w razie potrzeby. Dowody wskazują, że wśród współpracujących organizacji promowana jest pozytywna kultura bezpieczeństwa.
Wyniki oceny			

Czego szukać
– Przejrzeć w jaki sposób zidentyfikowano i udokumentowano relacje (powiązania) wewnętrzne (z innymi działami) i zewnętrzne (np. z wykonawcami, klientami, państwem). Przejrzeć opis systemowy interfejsów (jeśli jest to udokumentowane w podręczniku SMS lub innym równoważnym dokumencie). – Jeżeli kilku operatorów tworzących część jednej grupy biznesowej przewoźnika lotniczego korzysta z tego samego CAMO do zarządzania ciągłą zdatnością do lotu wszystkich eksploatowanych przez siebie statków powietrznych, należy sprawdzić, w jaki sposób odpowiednio uwzględniono interfejsy między tą grupą CAMO a wszystkimi różnymi zaangażowanymi operatorami (zob. M.A.201(ea) oraz CAMO.A.200(e)). W szczególności, czy umowy o zarządzanie ciągłą zdatnością do lotu opisują w jaki sposób indywidualne systemy zarządzania operatorów i CAMO są między sobą zharmonizowane. – Znaleźć dowód na to, czy: o Zidentyfikowano kwestie krytyczne dla bezpieczeństwa, obszary i związane z nimi zagrożenia; o Zgłaszane są zdarzenia związane z bezpieczeństwem i są one rozpatrywane/analizowane; o Stosowane są środki kontroli ryzyka i są one regularnie weryfikowane; o Interfejsy są poddawane okresowym przeglądom. – SMS organizacji obejmuje identyfikację zagrożeń dla zewnętrznych usług, działań i wewnętrznych relacji. – Organizowane są sesje szkoleniowe i promujące bezpieczeństwo z udziałem odpowiednich organizacji zewnętrznych. – Organizacje zewnętrzne uczestniczą w działaniach SMS i dzielą się informacjami dotyczącymi bezpieczeństwa. – Przeanalizować w jaki sposób promowana jest pozytywna kultura bezpieczeństwa w kontekście relacji. – Tam, gdzie jest to stosowne, system zgłaszania zdarzeń organizacji musi zostać rozszerzony na organizacje zewnętrzne. – Zarządzanie zmianami wpływającymi na bezpieczeństwo jest odpowiednio ujęte w umowach.

Odpowiednie odniesienia do przepisów UE/EASA				
Operacje lotnicze	**Załoga lotnicza**	**Lotniska**	**ATM/ANS**	**Organizacja szkolenia ATC**
Brak precyzyjnych zapisów Zob. ORO.GEN.205 „Działania zlecone” i powiązane GM1 & 2	Brak precyzyjnych zapisów Zob. ORA.GEN.205 „Zlecone czynności” i powiązane GM1 & 2	ADR.OR.D.010 „Zlecone czynności” ADR.OR.D.025 „Koordynacja działań z innymi organizacjami” Zob. powiązane AMC/GM	ATM/ANS.OR.B.005 „System zarządzania” punkt (f) GM1 ADR.OR.B.040(f) „Zmiany” punkt (b)(2) i (b)(3)	Brak precyzyjnych zapisów

CAMO	PART 145	Organizacje produkujące/POA	Organizacje projektujące/DOA	Zarezerwowane
CAMO.A.200(a)(3) i (c) GM1 CAMO.A.200(a)(3) „Zarządzanie ryzykiem bezpieczeństwa – relacje pomiędzy organizacjami” CAMO.A.200 (c) i (d) „System zarządzania” AMC1 CAMO.A.202 „Wewnętrzny system zgłaszania kwestii związanych z bezpieczeństwem” punkt (b)(6) CAMO.A.205 „Umowy i podwykonawstwo” M.A.201(ea) oraz CAMO.A.200(e) „System zarządzania” punkt (e) – powiązane AMC i GM	145.A.200 „System zarządzania” punkt (a)(3) i (c) GM1 145.A.200(a)(3) „Zarządzanie ryzykiem bezpieczeństwa – relacje pomiędzy organizacjami” 145.A.205 „Umowy i podwykonawstwo” GM1 145.A.205 „Odpowiedzialność przy zamawianiu czynności lub zleceniu podwykonawstwa zadań obsługowych” 145.A.60 „Zgłaszanie zdarzeń” 145.A.202 „Wewnętrzny system zgłaszania kwestii związanych z bezpieczeństwem” 145.A.70 „Charakterystyka organizacji obsługowej (MOE)” AMC1 145.A.70(a) „MOE” punkt 4.2	21.A.139 „System zarządzania produkcją” punkt (d)(2)(ii) GM1 21.A.139(d)(1) „Zgodność dostarczonych części i wyposażenia” GM2 21.A.139(d)(1) „Element systemu jakości – ustalenia z partnerami i podwykonawcami” AMC1 21.A.139 (d)(2)(ii) (b)(1)(ii) Ocena, audyt i kontrola dostawcy i podwykonawcy –POA, które korzysta z udokumentowanych ustaleń z innymi stronami w celu oceny i nadzoru dostawcy” AMC2 21.A.139 (d)(2)(ii) „Ocena dostawców i podwykonawców, audyt i kontrola – użytkownik POA, który korzysta z certyfikacji dostawców innych stron” 21.A.143 „Charakterystyka organizacji produkującej” punkt 12	21.A.239 „System zarządzania projektowaniem” punkt d) 3) AMC2 21.A.239 (d) „Element zapewniający bezpieczeństwo projektu w przypadku drobnych zmian w projekcie typu lub drobnych napraw wyrobów” GM1 21.A.239 (d)(3) „Element zapewniający bezpieczeństwo projektu – partner i podwykonawcy” GM2 21.A.239 (d)(3) „Element zapewniający bezpieczeństwo projektu – ustalenia z partnerami i podwykonawcami” GM2 21.A.239 (d)(3) „Element zapewniający bezpieczeństwo projektu – ustalenia z partnerami i podwykonawcami”punkty b), c) i d) odnośnie komunikacji	

PODSUMOWANIE KOMENTARZY do 5.1. „ZARZĄDZANIE RELACJAMI”

5.2 Obowiązek zapewnienia zgodności oraz funkcja monitorowania zgodności

5.2.1 Obowiązki i odpowiedzialność związane z zapewnieniem zgodności

5.2.1 Zdefiniowano obowiązki i odpowiedzialność za **zapewnienie** zgodności.

Obecny	Odpowiedni	Sprawny	Skuteczny
Odpowiednie wymagania są wyraźnie określone i prawidłowo zapisane w podręcznikach i procedurach organizacji. Obowiązki i odpowiedzialność za zgodność są zdefiniowane dla wszystkich pracowników zaangażowanych w działania związane z bezpieczeństwem.	Umowy z (lub wymagania przekazane) zewnętrznymi organizacjami, które mają znaczący wkład w bezpieczeństwo, również uwzględniają potrzebę zapewnienia zgodności z wymaganiami bezpieczeństwa; określono obowiązki i odpowiedzialność.	Podręczniki i procedury organizacji są regularnie przeglądane w świetle zmian w obowiązujących wymaganiach. Wszyscy pracownicy są świadomi swoich obowiązków i odpowiedzialności za zgodność oraz przestrzeganie procesów i procedur.	Udoskonalenia procesów i procedur są sugerowane przez pracowników i zarząd. Pracownicy proaktywnie identyfikują i zgłaszają potencjalne niezgodności.
Wyniki oceny			

Czego szukać

- Przejrzeć, w jaki sposób kierownictwo wyższego szczebla zapewnia, że organizacja pozostaje zgodna z wymaganiami.
- Sprawdzić, czy opisy stanowisk wyraźnie określają obowiązki związane z zapewnieniem zgodności.
- Upewnić się, że umowy z zewnętrznymi organizacjami, które mają znaczący wkład w bezpieczeństwo, odpowiednio uwzględniają potrzeby związane ze „zgodnością".
- Udowodnić, że kierownictwo wyższego szczebla podejmuje działania na podstawie wyników audytów wewnętrznych i zewnętrznych. Sprawdzić, czy w przypadku wykrycia niedociągnięć związanych ze znaczącymi ryzykami, identyfikowane są przyczyny źródłowe, które zasilają proces identyfikacji zagrożeń i oceny ryzyka (HIRA) (zob. Sekcja 2).
- Przejrzeć w jaki sposób osiągana jest niezależność funkcji audytu wewnętrznego.

Odpowiednie odniesienia do przepisów UE/EASA				
Operacje lotnicze	**Załoga lotnicza**	**Lotniska**	**ATM/ANS**	**Organizacja szkolenia ATC**
ORO.GEN.210 „Wymagania dotyczące personelu” punkt (b) Zob. powiązane AMC/GM	ORA.GEN.210 „Wymagania dotyczące personelu” punkt (b) Zob. powiązane AMC/GM	ADR.OR.D.005 „System zarządzania” punkt (b)(11) Zob. powiązane AMC/GM	ATM/ANS.OR.B.020 „Wymagania dotyczące personelu” Zob. powiązane AMC/GM	ATCO.OR.C.010 „Wymagania dotyczące personelu” punkt (b) Zob. powiązane AMC/GM
CAMO	**PART 145**	**Organizacje produkujące/POA**	**Organizacje projektujące/DOA**	**Zarezerwowane**
CAMO.A.200 „System zarządzania” punkt (a)(1)(a)(6) CAMO.A.300 „Charakterystyka zarządzania ciągłą zdatnością (CAME)” punkt (a)(6) i (7) CAMO.A.305 „Wymagania dotyczące personelu” punkt (a)(4) AMC1 CAMO.A.305 (a)(4) „Zarządzanie bezpieczeństwem i funkcja monitorowania zgodności” punkt (b)(c)	145.A.200 „System zarządzania” punkt (a)(1) i (a)(6) oraz AMC1 145.A.30 „Wymagania dotyczące personelu” GM1 145.A.30(b) „Odpowiedzialność za zapewnienie zgodności” AMC1 145.A.30 (c);(ca) „Zarządzanie bezpieczeństwem i funkcja monitorowania zgodności” punkt (b) GM1 145.A.30(cb) „Odpowiedzialność osób nominowanych wobec Kierownika Odpowiedzialnego” 145.A.70 „Charakterystyka organizacji obsługowej (MOE)” AMC1 145.A.70(a) ‘MOE’ punkt 1.4	21.A.139 „System zarządzania produkcją” punkt (e) AMC1 21.A.139(c)(2) „Organizacja i odpowiedzialność” punkt b) 4 AMC1 21.A.139(e) i 21.A.139(d)(2)(xiv) „Funkcja niezależnego monitoringu” 21.A.145 „Zasoby” punkty (c)(1) i (c)(2) AMC1 21.A.145(c)(2) „Kierownik nominowany” punkt b), c),(f),(g),(h),(i) AMC2 21.A.145(c)(2) „Kompetencje kierownictwa” punkt c)	21.A.239 „System zarządzania projektowaniem” punkt (d)(1) i (d)(2) oraz GM 21.A.239 „System zarządzania projektowaniem” punkt (e) AMC1 21.A.239(c)(2) „Organizacja i odpowiedzialność” punkt b) 4 AMC1 21.A.239(e) „Funkcja niezależnego monitoringu” AMC1 21.A.243(d) „Oświadczenie o kwalifikacjach i doświadczeniu” GM1 21.A.243(d) „Oświadczenie o kwalifikacjach i doświadczeniu” 21.A.245 „Zasoby” punkt (a) i (b)(2) AMC1 21.A.245 (b) „Kierownik nominowany” punkt d) f) AMC1 21.A.245 (d) „Ścieżka zgłaszania i kompetencje kierownictwa”	

5.2.2 Obowiązki i odpowiedzialność związane z monitorowaniem zgodności

5.2.2 Zdefiniowano obowiązki i odpowiedzialność za **monitorowanie** zgodności.

Obecny	Odpowiedni	Sprawny	Skuteczny
Udokumentowano, że istnieje osoba lub grupa osób odpowiedzialnych za monitorowanie zgodności, w tym osoba pełniąca funkcję kierownika ds. monitorowania zgodności, posiadająca bezpośredni dostęp do kierownika odpowiedzialnego. Odpowiedzialność i obowiązki kierownika odpowiedzialnego za monitorowanie zgodności są udokumentowane.	Osiągnięto niezależność funkcji audytu monitorowania zgodności.	Kierownik ds. monitorowania zgodności wdrożył i utrzymuje program monitorowania zgodności. Kierownik odpowiedzialny zapewnia wystarczające zasoby do monitorowania zgodności oraz utrzymanie niezależności funkcji audytu.	Organizacja ustanowiła metodę oceny efektywności i skuteczności działań w zakresie monitorowania zgodności z informacją zwrotną dla kierownika odpowiedzialnego. Kierownik odpowiedzialny i kierownictwo wyższego szczebla aktywnie poszukują informacji zwrotnych na temat stanu działań w zakresie monitorowania zgodności.
Wyniki oceny			

Czego szukać

- Jak kierownik ds. monitorowania zgodności współpracuje z:
  - wyższą kadrą kierowniczą,
  - kierownikami liniowymi,
  - personelem zarządzania bezpieczeństwem,
  - personelem organizacji zewnętrznych, mającymi znaczący wkład w bezpieczeństwo?
- Dowieść, czy kierownictwo wyższego szczebla działa w oparciu o wyniki monitorowania zgodności.
- Sprawdzić, czy liczba personelu zaangażowanego w monitorowanie zgodności jest odpowiednia.
- Sprawdzić, czy istnieją dowody bezpośredniego raportowania (dostępu) do kierownika odpowiedzialnego.
- Przejrzeć jak osiągana jest niezależność funkcji audytu.

Operacje lotnicze	**Załoga lotnicza**	**Lotniska**	**ATM/ANS**	**Organizacja szkolenia ATC**
AMC1 ORO.GEN.200(a)(6) „System zarządzania” punkt (c)	AMC1 ORA.GEN.200(a)(6) „System zarządzania” punkt (c)	AMC1 ADR.OR.D.005(b)(11) „System zarządzania” punkt (b) oraz AMC2 ADR.OR.D.005(b)(11) „System zarządzania”	AMC1 ATM/ANS.OR.B.005(c) „System zarządzania” MONITOROWANIE ZGODNOŚCI	AMC2 ATCO.OR.C.001(f) „System zarządzania organizacji szkoleniowych” MONITOROWANIE ZGODNOŚCI
CAMO	**PART 145**	**Organizacje produkujące/POA**	**Organizacje projektujące/DOA**	**Zarezerwowane**
CAMO.A.200 „System zarządzania” punkt (a)(1) i (a)(6) CAMO.A.305 „Wymagania dotyczące personelu” punkt (a)(4) AMC1 CAMO.A.305 (a)(4) „Zarządzanie bezpieczeństwem i funkcja monitorowania zgodności” punkt (b) i (c)	145.A.200 „Zarządzanie bezpieczeństwem” punkt (a)(1) i (a)(6) oraz GM1 145.A.30 „Wymagania dotyczące personelu” GM1 145.A.30(b) „Odpowiedzialność za zapewnianie zgodności” AMC1 145.A.30(c);(ca) „Funkcja zarządzania bezpieczeństwem i monitorowania zgodności” punkt (b) GM1 145.A.30(cb) „Obowiązki osób nominowanych wobec Kierownika odpowiedzialnego” 145.A.70 „Charakterystyka organizacji obsługowej (MOE)” AMC1 145.A.70(a) ‘MOE’ punkt 3.12	21.A.139 „System zarządzania produkcją” punkt (e) AMC1 21.A.139(e) i 21.A.139(d)(2)(xiv) „Funkcja niezależnego monitoringu” 21.A.145 „Zasoby” punkt (c)(1) i (c)(2 AMC1 21.A.145(c)(2) „Kierownik nominowany” punkt b), c), (h)(i)	21.A.239 „System zarządzania projektowaniem” punkt (e) AMC1 21.A.239(c)(2) „Organizacja i odpowiedzialność” punkt b)4 AMC1 21.A.239(e) „Funkcja niezależnego monitoringu” AMC1 21.A.243(d) „Oświadczenie o kwalifikacjach i doświadczeniu” GM1 21.A.243(d) „Oświadczenie o kwalifikacjach i doświadczeniu” 21.A.245 „Zasoby” punkt (a) i (b)(2) AMC1 21.A.245 (b) „Kierownicy nominowani” punt d) f) AMC1 21.A.245 (d) „Ścieżka zgłaszania i kompetencje kierownictwa”	

5.2.3 Program monitorowania zgodności

Odniesienia i tekst Załącznika 19

5.2.3 **Program** monitorowania zgodności

Obecny	Odpowiedni	Sprawny	Skuteczny
Organizacja posiada program monitorowania zgodności obejmujący szczegółowe informacje na temat harmonogramu działań monitorujących i procedur audytów, inspekcji, sprawozdawczości, działań następczych oraz przechowywania zapisów. Sposób osiągnięcia niezależności monitorowania zgodności jest udokumentowany.	Program audytów monitorowania zgodności obejmuje wszystkie obowiązujące przepisy i zawiera szczegółowy harmonogram audytów. Program monitorowania zgodności odpowiednio obejmuje organizacje zewnętrzne wspierające realizację usług, które mają istotny wkład w bezpieczeństwo.	Program monitorowania zgodności jest realizowany i regularnie poddawany przeglądom. Obejmuje to modyfikację programu w celu uwzględnienia zidentyfikowanych ryzyk lub zmian organizacyjnych i operacyjnych. Monitorowanie zgodności jest niezależne od działań operacyjnych i obejmuje działania zlecone na zewnątrz.	Organizacja regularnie dokonuje przeglądu programu monitorowania zgodności i procedur, zidentyfikować potrzebę zmian i zapewnić ich dalszą skuteczność. Skuteczność procesów SMS jest regularnie weryfikowana.
Wyniki oceny			

Czego szukać

- Ocenić zawartość programu w odniesieniu do wszelkich wymogów prawnych.
- Przejrzeć, w jaki sposób ryzyko i wyniki są wykorzystywane do określenia zakresu i częstotliwości działań monitorujących.
- Przeanalizować, jak osiągana jest niezależność.
- Ocenić, co powoduje/wyzwala zmianę w programie.
- Sprawdzić, czy nie ma potencjalnych konfliktów interesów.

Odpowiednie odniesienia do przepisów UE/EASA				
Operacje lotnicze	**Załoga lotnicza**	**Lotniska**	**ATM/ANS**	**Organizacja szkolenia ATC**
AMC1 ORO.GEN.200(a)(6) „System zarządzania" punkt (d)(2)(vi) GM2 ORO.GEN.200(a)(6) „System zarządzania" – (operatorzy typu complex) GM3 ORO.GEN.200(a)(6) „System zarządzania" – (operatorzy typu non-complex)	AMC1 ORA.GEN.200(a)(6) „System zarządzania" punkt (d)(2)(vi)	ADR.OR.D.005 „System zarządzania" punkt (b)11 (monitoring zgodności) oraz AMC, w szczególności AMC1 do ADR.OR.D.005 (b) (11) sekcja e)	AMC1 ATM/ANS.OR.B.005(c) „Monitoring zgodności systemu zarządzania"	GM1 ATCO.OR.C.001(f) „System zarządzania organizacji szkoleniowych" punkt (c)(2)(vi)
CAMO	**PART 145**	**Organizacje produkujące/POA**	**Organizacje projektujące/DOA**	**Zarezerwowane**
CAMO.A.200 „System zarządzania" punkt (a)(6) oraz AMC/GM CAMO.A.300 „Charakterystyka zarządzania ciągłą zdatnością (CAME)" punkt (a)(11)(i)	145.A.200 „System zarządzania" punkt (a)(6) AMC1 145.A.200(a)(6) „Monitoring zgodności - ogólne" AMC2 145.A.200(a)(6) „Monitoring zgodności – niezależny audyt" AMC3 145.A.200(a)(6) „Monitoring zgodności – zlecanie niezależnego audytu" GM2 145.A.200(a)(6) „Monitoring zgodności – plan audytu" 145.A.70 „Charakterystyka organizacji obsługowej (MOE)" AMC1 145.A.70(a) „MOE" punkt 3.12	21.A.139 „System zarządzania produkcją" punkt (e) AMC1 21.A.139(e) i 21.A.139(d)(2)(xiv) „Funkcja niezależnego monitoringu" AMC1 21.A.145(c)(2) „Kierownik nominowany" punkt (i)	21.A.239 „System zarządzania projektowaniem" punkt (e) AMC1 21.A.239(c)(2) „Organizacja i odpowiedzialność" punkt b)4 AMC1 21.A.239(e) „Funkcja niezależnego monitoringu" AMC1 21.A.245 (b) „Kierownicy nominowani" punkt (f)	

5.2.4 Wyniki monitorowania zgodności

5.2.4 Wyniki monitorowania zgodności m.in. wyniki audytu, w tym działania naprawcze i zapobiegawcze, działania następcze.

Obecny	Odpowiedni	Sprawny	Skuteczny
Organizacja posiada udokumentowane procedury identyfikacji i śledzenia działań korygujących oraz zapobiegawczych. Istnieje proces określający, jak wyniki audytów są przekazywane kierownikowi odpowiedzialnemu i kierownictwu wyższego szczebla. Opisano powiązania między monitorowaniem zgodności a procesami zarządzania ryzykiem bezpieczeństwa.	Zdefiniowano obowiązki i terminy określania, akceptacji oraz śledzenia działań korygujących i zapobiegawczych. Monitorowanie zgodności obejmuje działania zlecone na zewnątrz. Narzędzia do śledzenia działań korygujących i zapobiegawczych są dostosowane do wyników monitorowania zgodności i odpowiednio współdziałają z narzędziami SMS, gdy jest to konieczne. Metody stosowane do analizy przyczynowej są odpowiednie do wielkości organizacji oraz złożoności jej produktów i usług lotniczych.	Identyfikacja i śledzenie działań korygujących i zapobiegawczych są przeprowadzane zgodnie z procedurami, w tym analizą przyczynową w celu ustalenia przyczyn źródłowych. Status działań korygujących i zapobiegawczych jest regularnie przekazywany odpowiedniemu kierownictwu wyższego szczebla i personelowi.	Organizacja regularnie przegląda status działań korygujących i zapobiegawczych oraz ich skuteczność. Organizacja bada systemowe przyczyny i czynniki przyczyniające się, które dodatkowo łączą się z identyfikacją zagrożeń i oceną ryzyka (HIRA) oraz celami bezpieczeństwa. Znaczące ustalenia są wykorzystywane w wewnętrznych szkoleniach z zakresu bezpieczeństwa oraz w promocji bezpieczeństwa. Wyniki audytów, przyczyny źródłowe i czynniki przyczyniające się są analizowane i brane pod uwagę podczas przeglądu wewnętrznych polityk i procedur. Istnieje regularna komunikacja między personelem monitorowania zgodności a personelem zaangażowanym w inne działania SMS.
Wyniki oceny			

Czego szukać

- Przejrzeć metody stosowane do analizy przyczyn źródłowych.
- Czy metoda jest stosowana konsekwentnie i dostosowana do wielkości organizacji oraz jej złożoności działań?
- Dokonać przeglądu wszelkich powtarzających się sytuacji lub przypadków, w których działania nie zostały wdrożone lub są opóźnione.
- Sprawdzić terminowość realizacji działań.
- Świadomość kadry kierowniczej wyższego szczebla na temat statusu znaczących niezgodności i powiązanych działań korygujących i zapobiegawczych.
- Odpowiedni personel uczestniczy w ustalaniu przyczyn i czynników sprzyjających.
- Szukać spójności pomiędzy wynikami audytu wewnętrznego i wynikami audytu zewnętrznego.
- Sprawdzić, w jaki sposób identyfikacja przyczyn systemowych i czynników przyczyniających się do niezgodności łączą się z identyfikacją zagrożeń i oceną ryzyka, w tym z celami bezpieczeństwa i powiązanym z nimi pomiarem i monitorowaniem stanu bezpieczeństwa, jeśli ma to zastosowanie.
- Sprawdzić, jakiego rodzaju informacje należy zgłaszać kierownikowi odpowiedzialnemu (lub Radzie ds. bezpieczeństwa) lub odpowiednim komitetom bezpieczeństwa) w celu wsparcia HIRA i ustalenia celów bezpieczeństwa.

Odpowiednie odniesienia do przepisów UE/EASA				
Operacje lotnicze	**Załoga lotnicza**	**Lotniska**	**ATM/ANS**	**Organizacja szkolenia ATC**
ORO.GEN.200 „System zarządzania” punkt (a)(6) Zob. powiązane AMC/GM	ORA.GEN.200 „System zarządzania” punkt (a)(6) Zob. powiązane AMC/GM	AMC1 ADR.OR.D.005(b)(11) „System zarządzania” punkt (a)(1)(b) i (e)	AMC1 ATM/ANS.OR.B.005(c) „System zarządzania MONITORINGIEM ZGODNOŚCI”	ATCO.OR.C.001 „System zarządzania organizacji szkoleniowych” punkt (f) Zob. powiązane AMC/GM
CAMO	**PART 145**	**Organizacje produkujące/POA**	**Organizacje projektujące/DOA**	**Zarezerwowane**
CAMO.A.200 „System zarządzania” punkt (a)(6) oraz AMC/GM, w szczególności: AMC2 CAMO.A.200 (a)(6) AMC4 CAMO.A.200 (a)(6) CAMO.A.300 „Charakterystyka zarządzania ciągłą zdatnością (CAME)” punkt (a)(11)(i)	145.A.200 „System zarządzania” punkt (a)(6) AMC4 145.A.200(a)(6) „Monitoring zgodności – system informacji zwrotnych” 145.A.70 „Charakterystyka organizacji obsługowej (MOE)” AMC1 145.A.70(a) „MOE” punkt 3.8	21.A.139 „System zarządzania produkcją” punkt (e) AMC1 21.A.139(e) i 21.A.139(d)(2)(xiv) „Funkcja niezależnego monitoringu” AMC1 21.A.145(c)(2) „kierownik nominowany” punkt (i)	21.A.239 „System zarządzania projektowaniem” punkt (e) AMC1 21.A.239(c)(2) „Organizacja i odpowiedzialność” punkt b)4 AMC1 21.A.239(e) „Funkcja niezależnego monitoringu” AMC1 21.A.245(b) „Kierownicy nominowani” punkt (f)	

PODSUMOWANIE KOMENTARZY do 5.2. „OBOWIĄZEK ZAPEWNIENIA ZGODNOŚCI ORAZ FUNKCJA MONITOROWANIA ZGODNOŚCI”

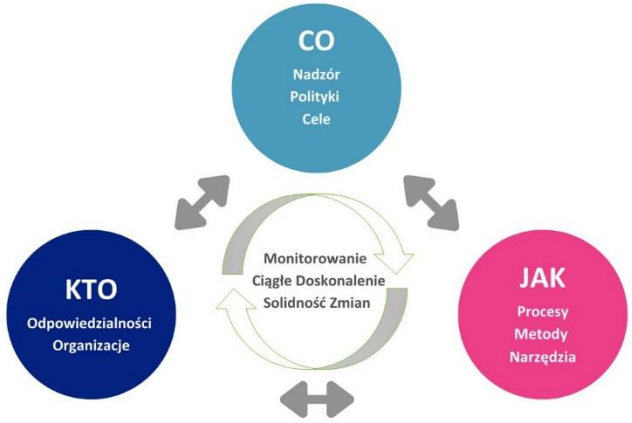
Załącznik 1: Czym jest System Zarządzania?

Ten załącznik ma na celu wyjaśnienie relacji pomiędzy SMS (Safety Management System) a Systemem Zarządzania (MS – Management System).

Większość organizacji posiada warstwowy system zarządzania, który składa się z wielu podsystemów koordynowanych przez jeden ośrodek decyzyjny – swoistego rodzaju *system nadzorujący* ISO 9000:2005 definiuje system zarządzania jako „zbiór powiązanych lub oddziałujących na siebie elementów służących do ustalania polityk i celów oraz osiągania tych celów".

System zarządzania to zbiór czterech kluczowych elementów (odpowiadających na cztery kluczowe pytania), dzięki którym organizacja może rozwijać:

1. „**Co**": Zasady i Nadzór:
   - które są wdrażane do procesów i zakresów odpowiedzialności w organizacji (powiązane z elementami „Kto" i „Jak")
   - które są dobrze rozumiane przez cały personel organizacji (powiązane z komponentem „Kto")
2. „**Jak**": Środki i Procesy do zastosowania przez organizację:
   - aby zapewnić, że sposób działania organizacji jest zgodny z zasadami i celami (powiązany z komponentem „Co")
   - aby zapewnić, że sposób działania organizacji jest opisany i przestrzegany przez personel organizacji (powiązany z komponentem „Kto")
3. „**Kto**": Odpowiedzialność, obowiązki i definicje powiązanych zadań:
   - aby zapewnić, że ludzie działają zgodnie z zasadami i politykami (powiązane z komponentem „Co")
   - aby zapewnić, że ludzie trzymają się procesów i sposobów pracy opisanych w organizacji/lub firmie (powiązane z komponentem „Jak")
4. „**Zapewnienie**": Monitorowanie i kontrola w celu zapewnienia prawidłowego działania trzech powyższych elementów: „Co", „Jak", „Kto" zgodnie z zasadami i celami ustalonymi przez organizację (podejście oparte na wynikach)



Typowe systemy zarządzania w organizacji lotniczej, które można integrować:

a) **System Jakości** – z Systemem Zarządzania Jakością (QMS – Quality Management System);
b) **Bezpieczeństwo lotów** – z Systemem Zarządzania Bezpieczeństwem (SMS – Safety Management System);
c) **Ochrona lotnictwa cywilnego przed aktami bezprawnej ingerencji (Security)** – z systemem zarządzania ochroną (SMS - Security Management System);
d) **Ochrona Środowiska** – z systemem zarządzania środowiskowego (EMS) - Environmental Management System);
e) **Bezpieczeństwo w środowisku pracy** – z systemem zarządzania bezpieczeństwem w środowisku pracy (OHSMS/BHP) - Occupational Health and Safety Management System/Bezpieczeństwo i Higiena Pracy);
f) **Finanse** – z systemem zarządzania finansami (FMS – Financial Management System);
g) **Systemy informacyjne** – z Systemem Zarządzania Bezpieczeństwem Informacji (ISMS – Information Security Management System), włącznie z aspektami cybersecurity.

W systemie Unii Europejskiej, zgodnie z zasadami obowiązującymi w każdym sektorze, System Zarządzania obejmuje SMS i funkcję monitorowania zgodności (podobnie do QMS); może również obejmować podsystemy/elementy istotne w danym obszarze takie jak System Zarządzania Ryzykiem Zmęczenia (Fatigue Risk Management System) w przypadku operacji lotniczych (Air OPS). Więcej informacji można znaleźć w GM1 do CAMO.A.20026[28].
W przyszłości planowane jest umieszczenie w Systemie Zarządzania kolejnych niezbędnych systemów takich jak ISMS. Takie całościowe podejście pozwala usprawnić procesy, zwiększyć efektywność relacji między różnymi systemami, wykorzystać synergię zasobów wymaganych przez różne certyfikaty lub zatwierdzenia oraz wspierać zintegrowane zarządzanie ryzykiem.

[28] https://www.easa.europa.eu/en/regulations/continuing-airworthiness

Załącznik 2: Przewodnik po „skalowalności” i „odpowiedniości”

Niniejszy załącznik ma na celu wyjaśnienie znaczenia następującego wymogu:

„System zarządzania powinien być dostosowany do wielkości organizacji oraz charakteru i złożoności jej działalności, z uwzględnieniem zagrożeń i związanych z nimi ryzyk nieodłącznie związanych z tą działalnością”.

1. Chociaż przepisy dotyczą głównych zagrożeń systemowych, nie są w stanie uwzględnić wszystkich rodzajów ryzyka. Zwłaszcza biorąc pod uwagę różnorodność organizacji, ich usług i produktów, a także szeroki wachlarz środowisk operacyjnych.
   - Organizacje powinny dążyć do wyjścia poza zwykłą zgodność z wymogami. System zarządzania (MS) powinien zatem zapewniać sposoby poszukiwania problemów związanych z bezpieczeństwem, które nie są odpowiednio uwzględnione w przepisach, w celu utrzymania lub poprawy bezpieczeństwa.
   - „Zgodność z przepisami (bycie zgodnym)” nie oznacza „bezpieczeństwa (bycia bezpiecznym)”. System zarządzania w każdej organizacji powinien pozostawać odporny, elastyczny i czujny w ciągle zmieniającym się kontekście (takim jak nowe modele biznesowe lub technologie, zmiana metod, pojawiające się zagrożenia, konkurencja, kryzys). Wreszcie, dobre wyniki w zakresie bezpieczeństwa i odporność przy braku negatywnych zdarzeń związanych z bezpieczeństwem w przeszłości nie gwarantują bezpiecznego funkcjonowania w przyszłości.
2. Wszystkie organizacje, niezależenie od ich wielkości są narażone na ryzyko. Niektóre z ryzyk mogą być potencjalnie znaczące, nawet w przypadku ograniczonego zakresu działalności. Oznacza to, że:
   - Wszystkie elementy Systemu Zarządzania powinny mieć zastosowanie;
   - Skuteczność Systemu Zarzadzania będzie zależała od tego, jak odpowiednio zaprojektowano, wdrożono i obsługiwano jego elementy.
3. Jednakże skuteczny system zarządzania ryzykiem nie musi być skomplikowany i kosztowny. System zarządzania ryzykiem może być skalowalny, jeśli nadal działa zgodnie z oczekiwaniami i zapewnia skuteczny sposób zarządzania wszystkimi kluczowymi rodzajami ryzyka operacyjnego. Opis systemu zarządzania ryzykiem powinien pomóc w identyfikacji różnych elementów i interfejsów, które należy uwzględnić przy projektowaniu i wdrażaniu systemu.
   - Skalowalność nie polega na stosowaniu określonych wybranych elementów Systemu Zarządzania lub uproszczonego SMS-a; skalowalność polega na dostosowaniu systemu zarządzania wraz ze wszystkimi jego elementami do konkretnego kontekstu operacyjnego organizacji.
   - Następujące aspekty mają kluczowe znaczenie dla każdej organizacji, aby zrozumieć kontekst, w jakim działa jej System Zarządzania, jaki powinien być jego cel oraz jakie są kluczowe ryzyka, którymi musi skutecznie zarządzać:
     1) wielkość organizacji:
        - liczba pracowników, liczba lokalizacji, w tym stałych i czasowych; wewnętrzne i zewnętrzne relacje; struktura organizacyjna;
        - rodzaj i różnorodność operacji (np. umowy leasingowe, organizacje z więcej niż jednym zatwierdzeniem/certyfikatem, ACMI);
        - typy i liczba statków powietrznych;
        - liczba przewożonych pasażerów – na każdy odcinek i rocznie; natężenia ruchu (ANSP); czy liczba pasów startowych (ADR);
     2) złożoność ryzyka, którym należy zarządzać:

- ryzyka związane ze środowiskiem operacyjnym (np. z górskie, mroźne warunki, operowanie na platformach na morzu, operacje zdalne bez bezpośredniego wsparcia, obszary polarne/arktyczne, obszary aktywnych wulkanów, operacje w pobliżu stref konfliktów); operacje specjalistyczne wymagające specjalnego zezwolenia (np. SPO)), konsekwencje dla bezpieczeństwa w przypadku awarii/braku produktów lub usług; potencjalne przestojami itd.
- ryzyka związane z modelem biznesowym (np. ze skalą zakontraktowanych wewnętrznych i zewnętrznych usług, usług o krótkim okresie realizacji lub operacji z „presją komercyjną”, zakresem zatwierdzania, działaniem jednej organizacji CAMO dla kilku AOC zgodnie z M.A.201 (ea)[29] i CAMO.A.200(e); umowami zerogodzinowymi dla pilotów ("zero-hour contract")
- zmian wymagających zatwierdzenia przed realizacją operacji;
- wyjątków i AltMoC przyznanych przez właściwy organ.

3) wpływu innych wewnętrznych i zewnętrznych czynników:
   - oczekiwań opinii publicznej,
   - otoczenia gospodarczego, handlowego i finansowego; konkurencji; stabilności działalności biznesowej w stosunku do potrzeb zmian;
   - doświadczenia w branży; adekwatności i solidności istniejących procedur itp.;
   - kultury bezpieczeństwa, kultury otwartego zgłaszania nieprawidłowości, kultury zapobiegania, kultury sprawiedliwego traktowania;
   - wyników w zakresie bezpieczeństwa na poziomie krajowym.

4. Ta wielowymiarowa złożoność powinna uwzględniona i odpowiednio wyważona. Poniżej zaproponowano kilka tematów do rozważenia:
   - Polityka bezpieczeństwa może być krótkim, ogólnym oświadczeniem kierownictwa o jego zaangażowaniu, popartym celami bezpieczeństwa, które dotyczą istotnych zagrożeń; powinna być bardziej szczegółowa w środowisku pełnym wyzwań; regularna aktualizacja celów bezpieczeństwa będzie konieczna w przypadku ciągłego rozwoju działalności/operacji (np. zmiany działań w obszarze operacyjnym, pojawiających się licznych niedociągnięć, kryzysu itp.); komunikacja tych celów bezpieczeństwa powinna być proporcjonalna do zasobów organizacji;
   - Polityka zgłaszania, polityka Just Culture oraz cele bezpieczeństwa mogą być połączone z polityką bezpieczeństwa w małych organizacjach;
   - W celu implementacji zasad kultury sprawiedliwego traktowania, wszelkie działania dyscyplinujące (w odpowiedzi na postepowanie niezgodne z prawem, zaniedbania czy umyślne uchybienia) byłyby przedkładane niezależnej komisji reprezentującej pracowników w dużej organizacji (np. komitet pracowniczy, przedstawiciele związków zawodowych), aby uniknąć pochopnych decyzji mogących zaszkodzić kulturze zgłaszania; w przypadku mniejszych organizacji przedstawiciele personelu powinni mieć wystarczające uprawnienia, aby zrównoważyć wszelkie jednostronne decyzje kierownictwa wyższego szczebla;
   - Znaczenie obszarów zwiększonego ryzyka (dotkliwość, prawdopodobieństwo, skuteczność środków ograniczających ryzyko) będzie miało ogromny wpływ na skuteczność procesów i monitorowanie barier bezpieczeństwa;
   - Dla organizacji o niższym poziomie ryzyka stosowany model oceny ryzyka może być bardzo prosty, jeśli zidentyfikowane zagrożenia są łatwe do złagodzenia,; ponadto organizacja będzie dążyć do klasyfikowania ryzyka w spójny sposób; ocena ekspercka może być wystarczająca do pomiaru

[29] https://www.easa.europa.eu/en/regulations/continuing-airworthiness

skuteczności barier bezpieczeństwa, zwłaszcza gdy ilość danych lub informacji dotyczących bezpieczeństwa nie pozwala na precyzyjne wsparcie oceny prawdopodobieństwa i dotkliwości skutków zagrożeń;

- Dane dotyczące bezpieczeństwa, które powinna gromadzić organizacja, muszą zależeć od rodzaju prowadzonej działalności, stopnia cyfryzacji (np. zautomatyzowane systemy zbierania danych). Przefiltrowane informacje będą wspierać ocenę ryzyka organizacji dysponujących dużymi zbiorami (data-rich organisations), natomiast organizacje nieposiadające takich danych będą w większym stopniu polegać na opinii ekspertów, ryzyku znanym w tym samym sektorze profilowania lub zbiorach danych (np. podejście oparte na współpracy, profilu ryzyka dla sektora). Organizacje dysponujące dużymi zbiorami danych będą skłonne do zakupu oprogramowania wspieranego przez rzetelną metodologię oceny ryzyka, aby klasyfikować ryzyko w sposób bardziej analityczny i spójny.
- Liczba zgłoszeń zdarzeń (dobrowolnych i obowiązkowych), a także środki i zasoby do zarządzania nimi będą zależały od kultury bezpieczeństwa, kultury otwartego zgłaszania, kultury sprawiedliwego traktowania, skali działalności i jej krytycznego znaczenia. Portfolia ryzyka publikowane przez EASA w tomie III EPAS[30] (European Plan for Aviation Safety), Rocznych Przeglądach Bezpieczeństwa (ASR – Annual Safety Review)[31] zgodnie z art. 13 Rozporządzenia (UE) 376/2014[32] lub wszelkie inne profile ryzyka sektorowego (udostępniane przez właściwe organy lub Branżę) mogą być wykorzystywane do identyfikacji konkretnych ryzyk w różnych rodzajach działalności w przypadku małej liczby (lub braku) zgłoszeń zdarzeń dla małych podmiotów; dodatkowo małe organizacje powinny w miarę możliwości uczestniczyć w warsztatach, konferencjach, wydarzeniach lub czytać literaturę (np. na temat profilowania ryzyka) w swojej dziedzinie działalności, aby wychwycić ryzyka, które mogły nie zostać prawidłowo zidentyfikowane przez ich SMS.
- Ilość zgromadzonych danych; bazy danych i sposób ich zarządzania będą się również różnić z zależności od organizacji; w związku z tym potrzebne będą narzędzia do analizy danych, dedykowane zasoby i kompetencje, a w przypadku dużej ilości i/lub złożoności zarządzania nimi mogą być potrzebni fachowi eksperci zajmujący się danymi lub analitycy zajmujący się ekstrakcją danych.
- Mechanizm i rodzaj informacji o bezpieczeństwie, które należy zgłaszać odpowiednim organom, będą zależeć od wielkości i struktury organizacji oraz procesu podejmowania decyzji (np. poziomu uprawnień). Analogicznie, odpowiednie zasoby zostaną przydzielone na potrzeby skutecznego systemu zarządzania (np. uzasadnienie pełnego etatu dla kierownika ds. bezpieczeństwa, komitety ds. bezpieczeństwa; częstotliwość spotkań Rady ds. Bezpieczeństwa, personel wyznaczony do monitorowania w czasie rzeczywistym);
- Przepływ, charakter i ilość informacji krążących w organizacji będą kształtować środki komunikacji, szkolenia i promocję bezpieczeństwa. Na przykład:
    a) formularz zgłoszenia zagrożenia bezpieczeństwa może mieć formę papierową dla organizacji o ograniczonych zasobach informatycznych lub formę elektroniczną dla tych, którzy mają możliwość wdrożenia takich rozwiązań (np. aplikacje zainstalowane na urządzeniach mobilnych);

[30] https://www.easa.europa.eu/en/domains/safety-management/european-plan-aviation-safety

[31] https://www.easa.europa.eu/en/document-library/general-publications?publication_type%5B%5D=144 – dla EASA – dla każdego państwa członkowskiego UE – informacja do zasięgnięcia z ich stron internetowych

[32] https://www.easa.europa.eu/en/regulations/occurrence-reporting

b) zalecenia i działania wynikające ze zgłoszeń dotyczących kwestii związanych z bezpieczeństwem mogą być publikowane w Internecie lub po prostu wywieszane na tablicach ogłoszeń;
c) w bardzo małych podmiotach, gdzie preferowana jest komunikacja werbalna z personelem, dokumentację dyskusji na temat bezpieczeństwa i jej wyników można ograniczyć do minimum;
d) Częstotliwość, treść i czas trwania szkoleń okresowych zostaną dostosowane do kultury bezpieczeństwa, liczby/znaczenia zidentyfikowanych problemów związanych z bezpieczeństwem;

- Terminowe przetwarzanie danych będzie zależało od ich znaczenia dla monitorowania w czasie rzeczywistym i podejmowania decyzji dotyczących zarządzania bezpieczeństwem przy wsparciu przez sztuczną inteligencję (np. zarządzanie ruchem lotniczym, pasy startowe w użyciu, inspekcje HUMS i planowe inspekcje obsługi technicznej, zarządzanie bezpieczeństwem w czasie rzeczywistym)
- Skupienie się na ryzyku na płaszczyznach styku będzie w znacznym stopniu zależeć od krytyczności znaczenia zadań zleconych podwykonawcom i wielkości łańcucha dostaw. Komunikowanie zmian i komunikacja na płaszczyznach styku z pewnością będzie bardziej wymagające w dużej organizacji lub w organizacji zlecającej wiele zadań.
- Dokumentacja systemu zarządzania; rejestr zagrożeń; udokumentowane oceny ryzyka; decyzje, działania, odpowiedzialność i monitorowanie itp. powinny być jasne, zwięzłe, ale wystarczająco szczegółowe, aby zapewnić odpowiednie zarządzanie ryzykiem. Powinny być spójne, kompletne, dostosowane do kontekstu i pod kontrolą. Jednak w małych podmiotach nie powinny generować nadmiernej biurokracji.
- „Wydajność człowieka" i „zasoby ludzkie" mogą mieć kluczowe znaczenie dla organizacji każdej wielkości, chociaż związane z tym kwestie mogą zależeć od kontekstu i wielkości: małe organizacje będą bardziej narażone na skutki odejść na emeryturę, transferu wiedzy, chorób i stresującego środowiska, podczas gdy dla dużych organizacji poważne wyzwanie mogą stanowić poważne zmiany lub znaczny wzrost;
- Stopień pilności osiągnięcia określonego poziomu bezpieczeństwa w oparciu o braki, informacje zwrotne z systemu monitorowania zgodności, aspekty kulturowe, zmiany w zakresie terminowego zarządzania lub wszelkie natychmiastowe/pilne kwestie związane z bezpieczeństwem mogą mieć wpływ na zasoby niezbędne do terminowego osiągnięcia celów w zakresie bezpieczeństwa.

5. Przy projektowaniu i funkcjonowaniu Systemu Zarządzania należy uwzględnić wdrożenie Standardów Branżowych lub Międzynarodowych Standarów bezpośrednio odnoszących się do działalności organizacji, takich jak System Zarządzania Jakością (np. ISO 91xx), SMS (Załącznik 19 ICAO), System Zarządzani Ryzykiem np. ISO 31000), System Zarządzania bezpieczeństwem Informacji (ISMS)System Zarządzania Środowiskowego (ISO 14001), system zarządzania bezpieczeństwem w środowisku pracy (OHSMS), System Zarządzania Finansami. W pełni rozwinięty system zarządzania może umożliwić usprawnienie procesów i osiągnięcie znacznych korzyści, gdy istnieją podobieństwa między różnymi elementami poszczególnych systemów (takie jak analiza niezgodności, system raportowania, ryzyka mające na siebie wpływ, spójna i zintegrowana metodologia oceny ryzyka, nadzór, zakresy odpowiedzialności, zasoby i kompetencje).
6. Wszystkie powyższe przykłady pokazują, że „nie ma jednego systemu, który pasowałby do wszystkich". Różnorodność organizacji, rodzajów działalności i ryzyk, którymi należy zarządzać, uzasadnia, dlaczego:
   - nie ma gotowego do użycia, czekającego „na półce" Systemu Zarządzania; oraz

- system zarządzania dotyczy wszystkich organizacji, niezależnie od tego, czy są małe, czy duże;
- nie oznacza to, że system musi być koniecznie złożony lub prosty (dla „małej organizacji").

7. Ciężar odpowiedzialności za wykazanie organowi nadzorującemu, że system zarządzania jest odpowiednio zaprojektowany i nadaje się do skutecznego działania zgodnie z oczekiwaniami, zgodnie z tym, co określono w dwóch pierwszych akapitach, spoczywa na organizacji. **SMS niekoniecznie musi być skomplikowany, czasochłonny i kosztowny, aby był skuteczny i wykazywał, że istotne ryzyka są pod kontrolą, a organizacja dysponuje odpowiednio dużym zapleczem danych dotyczących bezpieczeństwa, by podejmować właściwe decyzje.** Zamiast skupiać się na „wielkości" i „złożoności", organizacja i organ nadzorujący powinny skupić się na **skalowalności, odpowiedniości i skuteczności** danego systemu zarządzania.
8. Podczas korzystania z narzędzia oceny MS EASA oceniający ma obowiązek wybrać odpowiednie elementy i kryteria tego narzędzia, tak aby pytania zadawane podczas przeprowadzania oceny były adekwatne do specyfiki organizacji i nie zachęcały do tworzenia nadmiernie skomplikowanego systemu zarządzania.

Dostępne materiały w temacie „SMS w małych organizacjach":

- Zestawy materiałów edukacyjnych CASA SMS, Australia, w tym broszura nr 7 – SMS dla organizacji małych, typu non-complex;
- Wytyczne dla małych organizacji lotniczych – Implementacja Systemu Zarządzania Bezpieczeństwem, Nowa Zelandia;
- CAP1059 – System Zarządzania Bezpieczeństwem: Wytyczne dla organizacji małych, typu non-complex, Wielka Brytania;
- SMICG SMS dla małych organizacji;
- SM.0001 Część B i Załącznik 7 dotyczący „strategii implementacji SMS".

Załącznik 3: Europejska deklaracja kultury bezpieczeństwa w lotnictwie

EUROPEJSKA DEKLARACJA KULTURY BEZPIECZEŃSTWA W LOTNICTWIE[33]

Bezpieczeństwo ma ogromne znaczenie dla społeczeństwa, ale także dla branży lotniczej.

Bezpieczeństwo jest nie tylko wymogiem prawnym, ale także kluczowym czynnikiem wpływającym na zrównoważony rozwój działalności. Każdy podmiot działający w branży lotniczej ma zatem obowiązek utrzymywania i poprawiania bezpieczeństwa. Pracownicy branży lotniczej na wszystkich szczeblach ponoszą odpowiedzialność za bezpieczeństwo i odgrywają kluczową rolę w zapewnieniu bezpieczeństwa systemu.

Bezpieczny system lotniczy wymaga, aby zdarzenia mające lub mogące mieć wpływ na bezpieczeństwo lotnicze, były zgłaszane w sposób kompletny, swobodny i terminowy, zgodny z potrzebami, aby ułatwić ich badanie i wdrażanie wniosków z analizy.

Kultura Sprawiedliwego Traktowania (Just Culture) leży u podstaw skutecznego systemu zgłaszania, a taki system jest potrzebny we wszystkich organizacjach lotniczych w celu utrzymania i poprawy bezpieczeństwa w lotnictwie.

Niniejsza Deklaracja wspiera istniejące normy prawne, w szczególności Rozporządzenie (UE) nr 376/2014 w sprawie zgłaszania i analizy zdarzeń w lotnictwie cywilnym oraz podejmowanych w związku z nimi działań następczych i jest w pełni zgodna z obowiązującymi przepisami.

[33] ea938905-0ba0-43da-bae1-bedb7f070897_en
Niniejsza niewiążąca prawnie Deklaracja odnosi się wyłącznie do Kultury Sprawiedliwego Traktowania (Just Culture) w kontekście organizacji i nie dotyczy ani nie uchyla przepisów prawa ani zasad obowiązujących w poszczególnych państwach członkowskich.

Każda organizacja powinna, po konsultacji z przedstawicielami swoich pracowników, wdrożyć wewnętrzne zasady, które najlepiej odpowiadają jej wewnętrznej i zewnętrznej specyfice. Zasady[34] te powinny być wspierane przez udokumentowane procesy i stosowane w sposób spójny w całej organizacji.

Niniejsza Deklaracja stanowi zbiór kluczowych zasad, do których wdrażania każda organizacja jest zachęcana w kontekście swoich wewnętrznych zasad Just Culture.

My, sygnatariusze niniejszej Deklaracji, będziemy zachęcać naszych członków do wdrażania Just Culture w oparciu o następujące, kluczowe zasady, o których mowa w niniejszej Deklaracji. Sygnatariusze zgadzają się kontynuować współpracę w celu opracowania wytycznych i materiałów dotyczących najlepszych praktyk branżowych, aby pomóc we wdrażaniu Just Culture przez organizacje w różnych sektorach lotnictwa.

KLUCZOWE ZASADY KULTURY BEZPIECZEŃSTWA

1. Działanie w sposób bezpieczny jest najwyższym priorytetem.
2. Należy uznać, jako punkt wyjścia, że pracownicy wszystkich szczebli działają w interesie bezpieczeństwa, w sposób współmierny do wyszkolenia, doświadczenia i standardów zawodowych odpowiednich do ich stanowiska lub funkcji. Aby to osiągnąć, organizacje są odpowiedzialne za zapewnienie swoim pracownikom odpowiedniego środowiska, narzędzi, szkoleń i procedur.
3. Uznaje się, że w środowisku operacyjnym branży lotniczej jednostki, pomimo przeszkolenia, wiedzy fachowej, doświadczenia, umiejętności i dobrej woli, mogą mierzyć się z sytuacjami, w których ograniczenia ludzkich możliwości w połączeniu z niepożądanymi i nieprzewidywalnymi czynnikami systemowymi mogą doprowadzić do niepożądanych skutków.
4. Analiza zgłoszonych w ramach organizacji zdarzeń powinna przede wszystkim koncentrować się na wydajności systemu i czynnikach sprzyjających wystąpieniu zdarzenia, a nie na przypisywaniu winy i/lub skupianiu się na indywidualnej odpowiedzialności, z wyjątkiem przypadków przewidzianych w Rozporządzeniu (UE) nr 376/2014 i innych, mających zastosowanie przepisach.
5. Oceniając indywidualną odpowiedzialność, organizacje powinny skupić się na ustaleniu, czy podjęte działania, zaniedbania lub podjęte decyzje były współmierne do doświadczenia i przeszkolenia, a nie na wyniku zdarzenia.
6. Osoby zgłaszające informacje dotyczące bezpieczeństwa oraz wszelkie inne osoby wymienione w zgłoszeniu są chronione przed negatywnymi konsekwencjami zgodnie z Rozporządzeniem (UE) nr 376/2014.

[34] 33 Artykuł 16 pkt 11 Rozporządzenia (UE) nr 376/2014 przewiduje obecność „wewnętrznych zasad Just Culture", wspieranych przez wewnętrzne procesy, które muszą zostać przyjęte po konsultacji z przedstawicielami pracowników organizacji i wdrożone w europejskich organizacjach lotniczych.

7. Uznając, że zdarzenia niepożądane mogą często stanowić impuls do analizy, należy rejestrować i promować pozytywne zachowania i działania.
8. Organizacje powinny promować skuteczne wdrażanie zasad Just Culture w organizacji na wszystkich szczeblach i ze wszystkimi stronami, w tym wśród swoich przedstawicieli. Wszyscy powinni aktywnie wspierać wzajemne zaufanie i szacunek oraz promować wzajemne wsparcie i współpracę w celu budowania niezbędnego zaufania w całej organizacji. Personel powinien zostać przeszkolony w zakresie zasad Just Culture i mieć dostęp do dokumentacji z nią związanej.
9. Wewnętrzne zasady Just Culture powinny obejmować między innymi definicję procesu (w tym zaangażowanych podmiotów) służącego do określenia niedopuszczalnego zachowania zgodnie z jego opisem zawartym w Rozporządzeniu nr 376/2014.
10. Wewnętrzne zasady Just Culture powinny dokumentować, w jaki sposób dane dotyczące bezpieczeństwa są zarządzane, przechowywane, chronione i ujawniane. Powinny również zawierać informację w jakim zakresie organizacja zamierza udostępniać zanonimizowane dane w celach edukacyjnych dotyczących bezpieczeństwa.
11. Wsparcie udzielane przez organizacje w przypadkach, gdy pracownicy podlegają zewnętrznym procedurom w związku ze zdarzeniem, które zgłosili lub w którym uczestniczyli, wzmacnia wzajemne zaufanie niezbędne do zapewnienia skutecznej Kultury Sprawiedliwego Traktowania.
12. Spójne i skuteczne wdrożenie kultury sprawiedliwego traktowania wymaga czegoś więcej niż tylko opublikowania wewnętrznych zasad dotyczących Just Culture. Aby skutecznie wdrożyć Just Culture, pracownicy wszystkich szczebli, a także kierownictwo wyższego szczebla, powinni rozumieć i zaakceptować swoją odpowiedzialność w odniesieniu do zasad kultury sprawiedliwego traktowania oraz ich promowania.
13. Organizacje, we współpracy z zaangażowanymi stronami, w tym z właściwym organem, powinny określić, w jaki sposób zamierzają stale promować i wspierać wdrażanie zasad i praktyk Just Culture w całej organizacji.
14. Organizacje powinny regularnie dokonywać przeglądu i oceny dojrzałości swoich wewnętrznych zasad Just Culture i porównywać je z postrzeganiem Just Culture w organizacji. Korzystne może być również przeprowadzenie analizy porównawczej (Benchmarking).

W Polsce, w październiku 2017 r. Prezes ULC zainicjował Deklarację w sprawie kultury bezpieczeństwa, której sygnatariusze zobowiązują się wdrażać kulturę sprawiedliwego traktowania oraz propagować poprawę bezpieczeństwa transportu lotniczego.

Deklaracja jest otwarta do podpisu dla wszystkich organizacji działających w polskim sektorze lotniczym – niezależnie od wielkości i rodzaju świadczonych usług. Jedynym warunkiem jest traktowanie priorytetowo bezpieczeństwa. Więcej szczegółów można znaleźć na stronie internetowej ULC: Deklaracja w sprawie kultury bezpieczeństwa - Urząd Lotnictwa Cywilnego.