Warszawa, dnia 24 listopada 2015 r.

Poz. 64

WYTYCZNE Nr 11
PREZESA URZĘDU LOTNICTWA CYWILNEGO

z dnia 24 listopada 2015 r.

w sprawie wprowadzenia do stosowania wymagań ustanowionych przez Organizację Międzynarodowego Lotnictwa Cywilnego (ICAO) – Doc 9859

Na podstawie art. 21 ust. 2 pkt 16 oraz art. 23 ust. 2 pkt 2 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze (Dz. U. z 2013 r. poz. 1393, z późn. zm.[1)]) ogłasza się, co następuje:

§ 1. 1. W celu realizacji norm i zalecanych metod postępowania określonych w Załączniku 19 do Konwencji o międzynarodowym lotnictwie cywilnym, sporządzonej w Chicago dnia 7 grudnia 1944 r. (Dz. U. z 1959 r. Nr 35, poz. 212 i 214, z późn. zm.[2)]) zaleca się stosowanie wymagań ustanowionych przez Organizację Międzynarodowego Lotnictwa Cywilnego (ICAO) w Doc 9859 – „Podręcznik zarządzania bezpieczeństwem" (wydanie trzecie).

2. Wymagania, o których mowa w ust. 1, określa załącznik do wytycznych.

§ 2. Tracą moc wytyczne Nr 10 Prezesa Urzędu Lotnictwa Cywilnego z dnia 22 września 2011 r. w sprawie wprowadzenia do stosowania wymagań ustanowionych przez Organizację Międzynarodowego Lotnictwa Cywilnego (ICAO) – Doc 9859 (Dz. Urz. ULC z 2011 r. Nr 15, poz. 94).

§ 3. Wytyczne wchodzą w życie z dniem ogłoszenia.

Prezes Urzędu Lotnictwa Cywilnego

Piotr Ołowski

[1)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2014 r. poz. 768 oraz z 2015 r. poz. 978, 1221 i 1586.

[2)] Zmiany wymienionej umowy zostały ogłoszone w Dz. U. z 1963 r. Nr 24, poz. 137 i 138, z 1969 r. Nr 27, poz. 210 i 211, z 1976 r. Nr 21, poz. 130 i 131, Nr 32, poz. 188 i 189 i Nr 39, poz. 227 i 228, z 1984 r. Nr 39, poz. 199 i 200, z 2000 r. Nr 39, poz. 446 i 447, z 2002 r. Nr 58, poz. 527 i 528, z 2003 r. Nr 78, poz. 700 i 701 oraz z 2012 r. poz. 368, 369, 370 i 371.

Załącznik do wytycznych Nr 11

Prezesa Urzędu Lotnictwa Cywilnego

z dnia 24 listopada 2015 r.

Doc 9859
AN/474

PODRĘCZNIK ZARZĄDZANIA BEZPIECZEŃSTWEM (SMM)

Dokument zatwierdzony przez Sekretarza Generalnego ICAO

Wydanie trzecie — 2013

Organizacja Międzynarodowego Lotnictwa Cywilnego

ZMIANY

Zmiany są ogłaszane w suplementach do Katalogu Publikacji ICAO (Catalogue of ICAO Publications); katalog i jego suplementy są dostępne na stronie internetowej ICAO www.icao.int. Miejsce poniżej służy do ewidencji takich zmian.

REJESTR POPRAWEK I SPROSTOWAŃ

ZMIANY		
Nr	Data	Kto wprowadził

KOREKTY		
Nr	Data	Kto wprowadził

SPIS TREŚCI

SŁOWNIK POJĘĆ

Akronimy i skróty

AD	Airworthiness directive	Dyrektywa nt. zdatności do lotu samolotów
ADREP	Accident/incident data reporting (ICAO)	Zgłaszanie danych o wypadkach i zdarzeniach lotniczych (ICAO)
AIB	Accident investigation board	Organ ds. badania wypadków
AIR	Airworthiness	Zdatność do lotu
ALoSP	Acceptable level of safety performance	Akceptowalny poziom realizacji bezpieczeństwa
AMAN	Abrupt maneuvering	Manewrowanie gwałtowne
AME	Aircraft maintenance engineer	Mechanik obsługi samolotowej
AMO	Approved maintenance organization	Zatwierdzona organizacja obsługowa
AMS	Approved maintenance schedule	Zatwierdzony harmonogram obsługi
ANS	Air navigation service	Służba żeglugi powietrznej
AOC	Air operator certificate	Certyfikat przewoźnika lotniczego
AOG	Aircraft on ground	Samolot na ziemi
ASB	Alert service bulletin	Biuletyn alarmowy dla obsługi
ATC	Air traffic control	Kontrola ruchu lotniczego
ATM	Air traffic management	Zarządzanie ruchem lotniczym
ATS	Air traffic service(s)	Służby ruchu lotniczego
AMS	Approved maintenance schedule	Zatwierdzony harmonogram obsługi
ANS	Air navigation service	Służba żeglugi powietrznej
AOC	Air operator certificate	Certyfikat przewoźnika lotniczego
AOG	Aircraft on ground	Samolot na ziemi
ASB	Alert service bulletin	Biuletyn alarmowy dla obsługi
ATC	Air traffic control	Kontrola ruchu lotniczego
ATM	Air traffic management	Zarządzanie ruchem lotniczym
ATS	Air traffic service(s)	Służby ruchu lotniczego
CAA	Civil aviation authority	Organ lotnictwa cywilnego
CAN	Corrective action notice	Nota korygująca działanie
CBA	Cost-benefit analysis	Analiza kosztów i korzyści
CEO	Chief executive officer	Główna osoba wykonawcza szczebla dyrektorskiego
CFIT	Controlled flight into terrain	Zderzenie z ziemią w locie kontrolowanym
Cir	Circular	Okólnik
CM	Condition monitoring	Monitorowanie warunków
CMA	Continuous monitoring approach	Stosowanie monitorowania ciągłego
CMC	Crisis management center	Centrum zarządzania kryzysowego
CNS	Communications, navigation, and surveillance	Łączność, nawigacja i śledzenie
CP	Command post	Posterunek dowodzenia
CRM	Crew resource management	Zarządzanie zasobami ludzkimi (załogami)
CVR	Cockpit voice recorder	Rejestrator dźwięku w kabinie załogi
D&M	Design and manufacturing	Projekt i wykonawstwo
DGR	Dangerous goods regulation	Zarządzanie materiałami niebezpiecznymi
DMS	Document management system	System zarządzania dokumentami
DOA	Design organization approval	Zatwierdzanie organizacji projektowania
Doc	Document	Dokument
EAD	Emergency airworthiness directive	Awaryjna dyrektywa dotycząca lotności samolotu

EC	Escalation control	Kontrolowanie eskalacji [sytuacji]
ECCAIRS	European Coordination Centre for Accident and Incident Reporting Systems	Europejskie centrum koordynacji systemów zgłaszania wypadków i wydarzeń lotniczych
EDTO	Extended diversion time operation	Operowanie czasem zawrócenia samolotu w locie wydłużonym
EF	Escalation factor	Czynnik eskalacji [sytuacji]
EMC	Emergency management center	Centrum zarządzania awaryjnego
ERP	Emergency response plan	Plan reagowania awaryjnego
FDR	Flight data recorder	Rejestrator parametrów lotu
FH	Flying hours	Nalot
FIR	Flight information region	Rejon informacji powietrznej
FL	Flight level	Poziom lotu
FMS	Financial management system	System zarządzania finansowego
FRMS	Fatigue risk management systems	Systemy zarządzania ryzykiem związanym z przemęczeniem
FTL	Flight time limitation	Ograniczenia czasu trwania lotu
FTM	Fleet technical management	Techniczne zarządzanie flotą
GAQ	Gap analysis questionnaire	Kwestionariusz dotyczący analizy luk
H	Hazard	Zagrożenie
HF	Human factors	Czynniki ludzkie
HIRA	Hazard identification and risk assessment	Rozpoznawanie zagrożeń i ocena ryzyka
HIRM	Hazard identification and risk mitigation	Rozpoznawanie zagrożeń i łagodzenie ryzyka
IATA	International Air Transport Association	Międzynarodowe Zrzeszenie Przewoźników Lotniczych
ICAO	International Civil Aviation Organization	Organizacja Międzynarodowego Lotnictwa Cywilnego
IFSD	In-flight shutdown	Wyłączenie silnika w powietrzu
ILS	Instrument landing system	System lądowania według przyrządów
IMC	Instrument meteorological conditions	Warunki meteorologiczne dla lotów według przyrządów
ISO	International Organization for Standardization	Międzynarodowa Organizacja Normalizacyjna
iSTARS	Integrated Safety Trend and Reporting System	Scalony system trendów dotyczących bezpieczeństwa oraz ich zgłaszanie
ITM	Inventory technical management	Techniczne zarządzanie inwentarzem
kg	Kilogram(s)	Kilogram(y)
LEI	Lack of effective implementation	Brak skutecznego wdrożenia
LOC-I	Loss of control in flight	Utrata sterowności w powietrzu
LOFT	Line-oriented flight training	Szkolenie nastawione na potrzeby linii lotniczej
LOS	Loss of separation	Utrata separacji między samolotami
LOSA	Line operations safety audit	Audyt bezpieczeństwa operacji linii lotniczej
LRU	Line replaceable unit	Zespół wymienialny w obsłudze na płycie lotniska
LSI	Line station inspection	Inspekcje stacji obsługowej linii lotniczej
MCM	Maintenance control manual	Podręcznik przeprowadzania obsługi technicznej
MDR	Mandatory defect report	Wymagane zgłaszanie usterek
MEDA	Maintenance error decision aid	Pomoc decyzyjna dotycząca pomyłek w obsłudze technicznej
MEL	Minimum equipment list	Lista minimalnego wyposażenia
MFF	Mixed fleet flying	Latanie różnymi samolotami różnych przewoźników

MOR	Mandatory occurrence report	Obowiązkowy raport o zdarzeniu
MPD	Maintenance planning document	Dokument dotyczący planowania obsługi technicznej
MRM	Maintenance resource management	Zarządzanie zasobami ludzkimi (personel techniczny)
MRO	Maintenance repair organization	Organizacja dokonująca napraw
MSL	Mean sea level	Średni poziom morza
N/A	Not applicable	Nie dotyczy
OEM	Original equipment manufacturer	Producent części oryginalnych
OHSMS	Occupational Health & Safety management system	System zarządzania bezpieczeństwem i higieną pracy
OPS	Operations	Operacje [lotnicze]
ORP	Organization risk profile	Profil ryzyka danej organizacji
OSC	Organization safety culture	Kultura bezpieczeństwa w danej organizacji (przedsiębiorstwie)
OSHE	Occupational Safety, Health & Environment	Bezpieczeństwo zawodowe i higiena pracy
PC	Personal computer	Komputer osobisty
PMI	Principal maintenance inspector	Główny inspektor przeglądów i napraw
POA	Production organizational approval	Zatwierdzenie organizacji produkcji
POI	Principal operations inspector	Główny inspektor operacji lotniczych
QA	Quality assurance	Zapewnianie jakości
QC	Quality control	Kontrola jakości
QM	Quality management	Zarządzanie jakością
QMS	Quality management system	System zarządzania jakością
RAIO	Regional accident and incident investigation organization	Terenowy organ ds. badania wydarzeń lotniczych i wypadków
RM	Recovery measure	Środki służące odzyskiwaniu [sprzętu]
RSOO	Regional safety oversight organization	Terenowy organ ds. nadzorowania zachowywania bezpieczeństwa
SA	Safety assurance	Zapewnianie bezpieczeństwa
SAG	Safety action group	Grupa Reagowania W Sprawach Bezpieczeństwa
SARPs	Standards and Recommended Practices (ICAO)	Normy i zalecane metody postępowania (ICAO)
SB	Service bulletin	Biuletyn, wg którego musi być wykonywana obsługa techniczna
SCF-NP	System component failure – non-power plant	Usterka komponentu systemu – nie dotyczy zespołu napędowego
SD	Standard deviation	Odstępstwo od normy
SDCPS	Safety data collection and processing systems	Systemy zbierania i przetwarzania danych dotyczących bezpieczeństwa
SeMS	Security Management System	System zarządzania ochroną
SHEL	Software/Hardware/Environment/ Liveware	Oprogramowanie/Sprzęt komputerowy/Środowisko/ Człowiek
SM	Safety management	Zarządzanie bezpieczeństwem
SMM	Safety management manual	Podręcznik zarządzania bezpieczeństwem
SMP	Safety Management Panel	Panel zarządzania bezpieczeństwem
SMS	Safety management system(s)	System(y) zarządzania bezpieczeństwem
SOPs	Standard operating procedures	Standardowe, działające procedury
SPI	Safety performance indicator	Wskaźnik realizowania bezpieczeństwa
SRB	Safety review board	Komisja ds. przeglądu bezpieczeństwa

SRM	Safety risk management	Zarządzanie ryzykiem dotyczącym bezpieczeństwa
SSP	State Safety Programme	Krajowy Program Bezpieczeństwa
STDEVP	Population standard deviation	Odchylenie od norm ustalonych dla populacji
TBD	To be determinate	Należy określić/ustalić
TOR	Terms of reference	Parametry/warunki porównawcze
UC	Ultimate consequence	Ostateczne konsekwencje
UE	Unsafe event	Niebezpieczne wydarzenie
USOAP	Universal Safety Oversight Audit Programme (ICAO)	Globalny Program Kontroli Nadzoru nad Bezpieczeństwem (ICAO)
WIP	Work in progress	Praca w toku

Definicje

Uwaga. – Poniższe definicje były formułowane równocześnie z projektowaniem Załącznika 19 do Konwencji chicagowskiej (Zarządzanie bezpieczeństwem). Zaraz po rozpoczęciu stosowania Załącznika 19 do Konwencji chicagowskiej w listopadzie 2013, będzie on miał zwierzchność, jeśli w definicjach zdarzyłyby się jakieś różnice.

Akceptowalny poziom realizacji bezpieczeństwa (ALoSP) (Acceptable level of safety performance (ALoSP). Minimalny poziom realizacji bezpieczeństwa w lotnictwie cywilnym w danym Państwie definiowany w programie bezpieczeństwa danego Państwa lub programie firmy zapewniającej bezpieczeństwo, tak jak jest zdefiniowane w jej systemie zarządzania bezpieczeństwem, wyrażonym w parametrach celów realizacyjnych bezpieczeństwa i we wskaźnikach realizacji bezpieczeństwa.

Dyrektor odpowiedzialny (Accountable executive). Jest to jedna osoba odpowiedzialna za skuteczną i wydajną realizację krajowego programu bezpieczeństwa (SSP) lub podręcznika zarządzania bezpieczeństwem (SMS).

Zarządzanie zmianą (Change management). Jest to formalny proces zarządzania zmianami wewnątrz firmy, prowadzony w sposób systematyczny, tak aby zmiany, które mogą oddziaływać na rozpoznane zagrożenia i na strategie łagodzenia ryzyka były uwzględniane zanim zostaną wdrożone.

Działania obronne (Defences). Są to wprowadzane na miejscu konkretne działania łagodzące, prewencyjne kontrole bądź sposoby odzyskiwania, zapobiegające wystąpieniu zagrożenia bądź jego eskalacji w niepożądany skutek.

Błędy (Errors). Działanie lub brak działania osoby w pionie operacyjnym, które prowadzi do niezamierzonego odejścia od przepisów i procedur operacyjnych i organizacyjnych.

Wskaźniki wysokopoziomowe konsekwencji (High-consequence indicators). Wskaźniki realizacji bezpieczeństwa, należące do monitorowania i mierzenia wydarzeń o wysokopoziomowych konsekwencjach takich jak wypadki bądź poważne zdarzenia lotnicze.

Wskaźniki niskopoziomowe konsekwencji (Lower-consequence indicators). Wskaźniki realizacji bezpieczeństwa, należące do monitorowania i mierzenia nieprzewidzianych wydarzeń/okoliczności (occurrences) o niskopoziomowych konsekwencjach, wydarzeń (events) bądź działań takich jak incydenty, ustalenia istnienia niezgodności bądź odstępstw. Wskaźniki niskopoziomowych konsekwencji są czasami porównywane do wskaźników proaktywnych.

Łagodzenie ryzyka (Risk mitigation). Jest to proces obejmujący środki obronne lub działania zapobiegawcze, zastosowane dla obniżenia ostrości przewidywanych konsekwencji ryzyka i/lub jego prawdopodobieństwa.

System zarządzania bezpieczeństwem (Safety management system). Jest to systemowe podejście do zarządzania bezpieczeństwem, scalające niezbędne struktury organizacyjne, rozdysponowanie odpowiedzialności, strategiczne sposoby postępowania (policies) oraz procedury.

Działanie bezpieczeństwa (Safety performance). Oznacza osiągnięcie oczekiwanego poziomu bezpieczeństwa danego Państwa lub dostarczyciela usług, zdefiniowanego przez realizację celów i wskaźników działania bezpieczeństwa.

Wskaźnik działania bezpieczeństwa (Safety performance indicator). Parametr bezpieczeństwa, pobrany z bazy danych i stosowany do monitorowania i oceniania tego jak bezpieczeństwo jest realizowane.

Ryzyko dotyczące bezpieczeństwa (Safety risk). Przewidywane prawdopodobieństwo i dotkliwość konsekwencji lub wartości wynikowej zagrożenia.

Krajowy program bezpieczeństwa (State Safety Programme). Scalony komplet przepisów i działań nastawionych na poprawienie bezpieczeństwa.

Rozdział 1
OGLĄD PODRĘCZNIKA

1.1 INFORMACJE OGÓLNE

1.1.1. Niniejsze trzecie wydanie Podręcznika Zarządzania Bezpieczeństwem ICAO (SMM) (Doc 9859) zastępuje w całości drugie wydanie opublikowane w 2009 r. Niniejsze wydanie zastępuje również Podręcznik Zapobiegania Wypadkom ICAO (Doc 9422), który jest nieaktualny.

1.1.2. Przeznaczeniem niniejszego podręcznika jest dostarczenie Państwom wskazówek na temat opracowania i wdrożenia Krajowego Programu Bezpieczeństwa (SSP) zgodnie z normami i zalecanymi metodami postępowania (SARPs) zawartymi w Załącznikach do Konwencji chicagowskiej: Załączniku 1 — Licencjonowanie personelu, Załączniku 6 — Eksploatacja statków powietrznych, Załączniku 8 — Zdatność do lotu statków powietrznych, Załączniku 11 — Służby ruchu lotniczego, Załączniku 13 — Badanie wypadków i incydentów lotniczych i Załączniku 14 — Lotniska, Tom I – Projektowanie i eksploatacja lotnisk (wszystkie Załączniki do Konwencji chicagowskiej). Należy zauważyć, że zapisy dotyczące Krajowych programów bezpieczeństwa (SSP) będą włączone do Załącznika 19 do Konwencji chicagowskiej – Zarządzanie bezpieczeństwem, który był w trakcie opracowywania w momencie publikacji niniejszej wersji. Ten podręcznik zawiera również wskazówki dotyczące ustanowienia przez Państwa wymagań dla systemów zarządzania bezpieczeństwem (SMS), także dla opracowywania i wdrażania SMS przez dostawców usług i dostawców, których to obejmie.

1.1.3. Należy zauważyć, że niniejszy podręcznik jest przeznaczony do stosowania w połączeniu z innymi, właściwymi materiałami wytycznymi, które mogą być przydatne do uzupełnienia lub doprecyzowania koncepcji i wytycznych zawartych w niniejszym dokumencie.

Uwaga. – W kontekście zarządzania bezpieczeństwem, termin „dostawca usług" lub „dostawca i dostawca usług" odnosi się do każdej organizacji dostarczającej produkty lotnicze i/lub świadczącej usługi lotnicze. Termin obejmuje więc zatwierdzone organizacje szkoleniowe, które podczas świadczenia swoich usług są narażone na ryzyko dotyczące bezpieczeństwa, operatorów statków powietrznych, zatwierdzonych organizacji obsługi technicznej, organizacji odpowiedzialnych za projekt typu statków powietrznych i/lub produkcję, wszystkich służb zapewniających ruch lotniczy oraz lotnisk certyfikowanych.

1.2 CEL

Celem niniejszego podręcznika jest zapewnienie Państwom, dostawcom i dostawcom usług:

a) przeglądu podstaw zarządzania bezpieczeństwem;

b) streszczenia norm i zalecanych metod postępowania (SARPs) ICAO, które dotyczą zarządzania bezpieczeństwem, zawartych w Załącznikach do Konwencji chicagowskiej 1, 6, 8, 11, 13 i 14;

c) wskazówek jak opracować i wdrożyć SSP zgodnie z odnośnymi SARPs ICAO, w tym dostosowania ram prawnych nadzoru nad dostawcami i dostawcami usług posiadającymi SMS.

d) wytycznych dla dostawców i dostawców usług, dotyczące opracowania, wdrażania i prowadzenia SMS.

1.3 STRUKTURA

Rozdział 1 przedstawia ogląd podręcznika, podczas gdy Rozdział 2 omawia fundamentalne koncepcje zarządzania bezpieczeństwem. Rozdział 3 daje kompilację zawartych w Załącznikach do Konwencji chicagowskiej 1, 6, 8, 11, 13 i 14 SARPs-ów ICAO. Ostatecznie, Rozdziały 3 i 4 dają zarys stopniowego podejścia do opracowywania, wdrażania i utrzymywania SSP i SMS. Ostatnie dwa rozdziały zawierają także **Dodatki (appendices)**, które dostarczają praktycznych wskazówek i ilustracji. Natomiast **załączniki (attachment)** do podręcznika podają listę powiązanych z tematem materiałów wytycznych ICAO.

Uwaga. – Użycie rodzaju męskiego w niniejszym podręczniku należy rozumieć, iż obejmuje on osoby płci męskiej oraz płci żeńskiej.

Rozdział 2
FUNDAMENTY ZARZĄDZANIA BEZPIECZEŃSTWEM

Uwaga. – Niniejszy rozdział daje ogląd fundamentalnych koncepcji zarządzania bezpieczeństwem i praktyk dotyczących wdrażania krajowych programów bezpieczeństwa, także ogląd na to jak wdrażane i nadzorowane będą systemy zarządzania bezpieczeństwem u dostawców usług. Treść niniejszego rozdziału podajemy dla potrzeb początkowych; więcej szczegółów na te tematy można znaleźć w kolejnych rozdziałach podręcznika, gdzie są porozrzucane.

2.1. KONCEPCJA BEZPIECZEŃSTWA

2.1.1. W kontekście lotnictwa, bezpieczeństwo – to „stan, w którym możliwość uszkodzenia ciała lub mienia jest zredukowana i utrzymywana na akceptowalnym poziomie lub poniżej tego poziomu poprzez ciągły proces identyfikacji zagrożeń i zarządzania ryzykiem dotyczącym bezpieczeństwa".

2.1.2. Choć wyeliminowanie wypadków i/lub poważnych incydentów lotniczych pozostaje celem ostatecznym, uznaje się, że lotnictwo nie może być całkowicie wolne od zagrożeń i związanego z nimi ryzykiem. Nie można zagwarantować, że działalność ludzka i systemy zbudowane przez człowieka będą całkowicie wolne od błędów eksploatacyjnych i ich następstw. Dlatego bezpieczeństwo jest dynamiczną cechą systemów lotniczych, w których ryzyko dotyczące bezpieczeństwa musi być stale łagodzone. Należy zauważyć, że na akceptowalny poziom bezpieczeństwa mają często wpływ krajowe i międzynarodowe normy oraz czynniki kulturowe. Dopóki ryzyko dotyczące bezpieczeństwa utrzymuje się na odpowiednim poziomie, systemem tak otwartym i dynamicznym jak lotnictwo można nadal zarządzać tak, by utrzymywać właściwą równowagę między produkcją a ochroną.

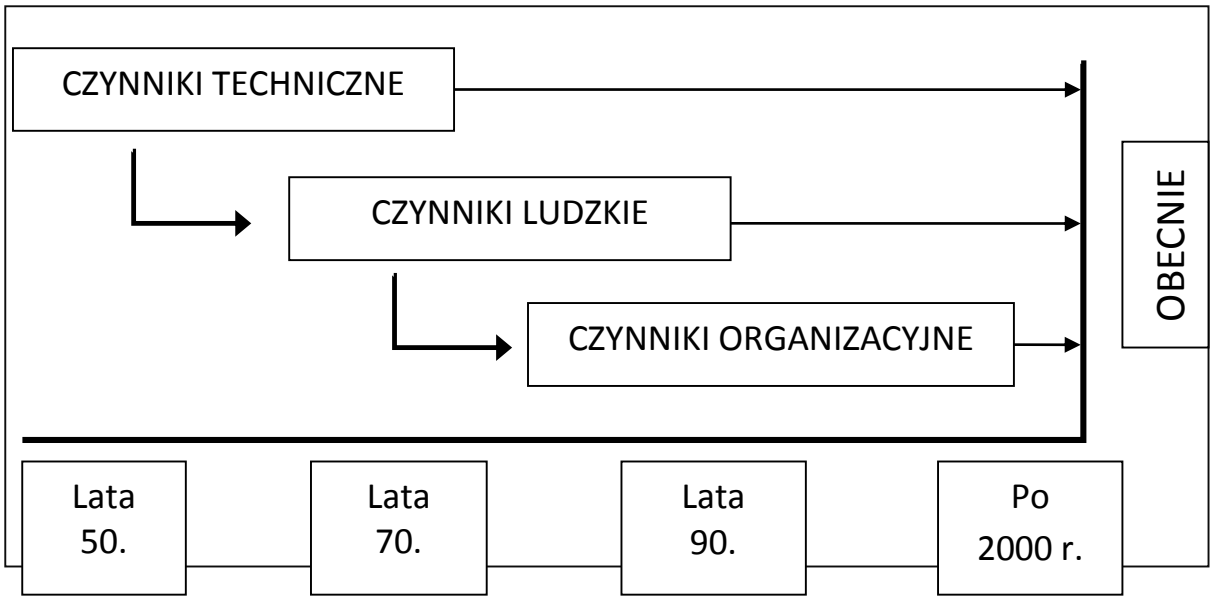
2.2. EWOLUCJA BEZPIECZEŃSTWA

Historia postępu w bezpieczeństwie lotniczym może być podzielona na trzy ery.

a) *Era techniczna – od wczesnych lat XX wieku do jego końcowych lat 60*. Lotnictwo pojawiło się jako forma transportu masowego, w której niedostatki w zakresie bezpieczeństwa były początkowo utożsamiane z czynnikami technicznymi i wadami technologicznymi. Głównym celem przedsięwzięć z zakresu bezpieczeństwa było więc skupienie się na badaniu i poprawie czynników technicznych. Do lat 50., postęp technologiczny doprowadził do stopniowego spadku częstotliwości wypadków, a zagadnienia bezpieczeństwa zostały poszerzone tak by objęły przestrzeganie procedur oraz przeoczenia.

b) *Era czynników ludzkich – od wczesnych lat 70. do końcowych lat 90.* We wczesnych latach 70., częstotliwość wypadków w lotnictwie zmniejszyła się znacząco dzięki poważnemu postępowi technologicznemu i doprecyzowaniu przepisów bezpieczeństwa. Lotnictwo stało się bezpieczniejszym rodzajem transportu a skupienie wysiłków na bezpieczeństwie zostało rozszerzone tak, by objąć także zagadnienia czynników ludzkich, w tym kontakt człowieka z maszyną. To prowadziło do poszukiwań informacji na temat bezpieczeństwa poza informacjami wygenerowanymi przez proces badania wypadków wcześniejszych. Pomimo zainwestowania środków w łagodzenie pomyłek, działania ludzkie były nadal cytowane jako czynnik powtarzający się w wypadkach (Rys. 2-1). Zastosowanie nauki o czynnikach ludzkich miało tendencję do skupiania się na samym człowieku, bez pełnego uwzględniania kontekstu operacyjnego i organizacyjnego. Dopiero we wczesnych latach 90. uwzględniono po raz pierwszy fakt, że ludzie działają w środowisku złożonym, obejmującym liczne czynniki mające potencjał oddziaływania na ludzkie postępowanie.

c) *Era organizacyjna – od połowy lat 90. do dziś*. Podczas ery organizacyjnej bezpieczeństwo zaczęto postrzegać z perspektywy systemowej, która miała oprócz czynników ludzkich i technicznych objąć także czynniki organizacyjne. W rezultacie wprowadzono pojęcie wypadku z przyczyn organizacyjnych (organizational accident), uwzględniające wpływ kultury firmy i zasad postępowania na efektywność kontroli ryzyka dotyczącego bezpieczeństwa. Dodatkowo, tradycyjne wysiłki w zakresie pozyskiwania i analizy danych, które wcześniej ograniczały się do korzystania z danych zebranych w trakcie badania wypadków i poważnych incydentów zostały rozszerzone o nowe, proaktywne podejście do bezpieczeństwa. To nowe podejście opiera się na rutynowym pozyskiwaniu i analizie danych z wykorzystaniem zarówno proaktywnych, jak i reaktywnych metodologii dla monitorowania znanego ryzyka i wykrywania pojawiających się w ich kontekście zagadnień dotyczących bezpieczeństwa. Wymienione doprecyzowania dały uzasadnienie dla przyjęcia podejścia zwanego zarządzaniem bezpieczeństwem.



Rys. 2-1. Ewolucja bezpieczeństwa

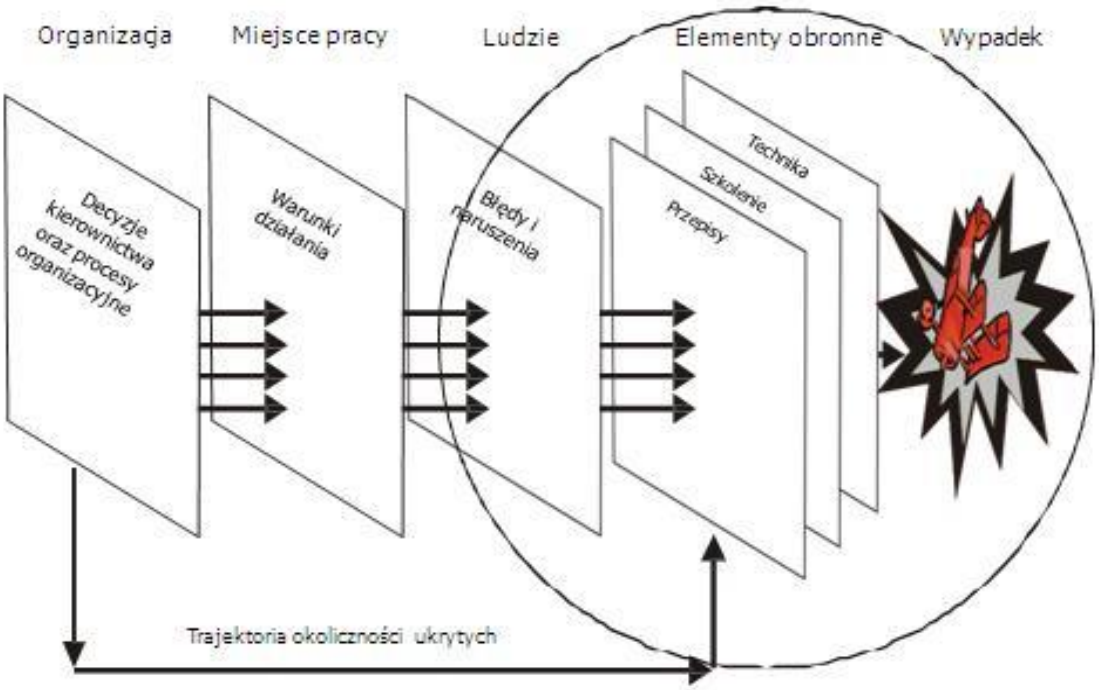
2.3. PRZYCZYNY WYPADKÓW

2.3.1. Model „sera szwajcarskiego", opracowany przez profesora Jamesa Reasona pokazuje, że wypadki związane są z kolejnymi naruszeniami różnorodnych elementów obronnych systemu. Takie naruszenia mogą zostać zainicjowane przez wiele czynników, takich jak awarie sprzętu lub błędy operacyjne. Ponieważ model „sera szwajcarskiego" zakłada, że tak skomplikowane systemy jak lotnictwo są szczególnie dobrze chronione przez poszczególne poziomy zabezpieczeń, stąd – w takich systemach - jednostkowe uchybienia rzadko powodują negatywne skutki. Naruszenia elementów obronnych w bezpieczeństwie mogą być opóźnioną konsekwencją decyzji podjętych na najwyższym szczeblu systemu, które mogą pozostawać uśpione aż do momentu, gdy ich skutki lub ich destrukcyjny potencjał uaktywni się w wyniku konkretnych okoliczności operacyjnych. W tych konkretnych okolicznościach, ludzkie niedoskonałości lub błędy w działaniu na szczeblu wykonawczym przyczyniają się do naruszania „wrodzonych" obronnych elementów systemu. W modelu nazwanym jego nazwiskiem, prof. Reason proponuje by wszystkie wypadki rozpatrywać jako kombinację czynników zarówno aktywnych, jak i uśpionych.

2.3.2. Uchybienia aktywne (active failures) to działania lub zaniechania, w tym błędy i naruszenia, które mają natychmiastowy skutek negatywny. Z korzystnej perspektywy czasu są one na ogół postrzegane jako działania niebezpieczne. Uchybienia aktywne są z reguły kojarzone z personelem z pierwszej linii (piloci, kontrolerzy ruchu lotniczego, mechanicy statków powietrznych itp.) i mogą prowadzić do szkodliwych następstw.

2.3.3. Stany uśpione *(latent conditions)* to takie, które występują w systemie lotniczym na długo zanim pojawi się ich szkodliwe następstwo. Konsekwencje stanów uśpionych mogą pozostawać w uśpieniu przez długi czas. Początkowo, takie uśpione stany nie są postrzegane jako szkodliwe, ale staną się dowodnie widoczne, gdy naruszone zostaną elementy obronne systemu. Takie stany są zazwyczaj tworzone przez ludzi, którym dane wydarzenie jest odległe w czasie i przestrzeni. Uśpione w systemie stany mogą obejmować stany takie, które powstają przez brak kultury w zakresie bezpieczeństwa, marny sprzęt czy wadliwą konstrukcję procedur, sprzeczne cele organizacyjne, wadliwe systemy organizacyjne lub błędne decyzje kierownicze. Poszukiwanie przyczyn będących podłożem wypadku z przyczyn organizacyjnych jest nakierowane na zidentyfikowanie i złagodzenie tych stanów uśpionych w podłożu całego systemu, a nie na podejmowanie lokalnych wysiłków nakierowanych na zminimalizowanie aktywnych uchybień poszczególnych osób.

2.3.4. Rysunek 2-2 pokazuje jak model „sera szwajcarskiego" pomaga w zrozumieniu wzajemnego oddziaływania czynników organizacyjnych i zarządczych na powodowanie wypadków. Rysunek jest ilustracją tego, że w system lotnictwa są wbudowane różne elementy obronne przed zmiennością ludzkich zachowań lub decyzji na wszystkich poziomach systemu. Choć te ochronne elementy działają zabezpieczająco przed zagrożeniami bezpieczeństwa, to jednak naruszenia, które penetrują wszystkie bariery obronne, mogą potencjalnie skutkować sytuacją katastrofalną. Model Reasona przedstawia to jak okoliczności uśpione są zawsze obecne w systemie jeszcze przed wypadkiem i że mogą się objawiać w wyniku lokalnych czynników aktywujących.



Rys. 2-2. Koncepcja przyczynowości wypadków

Wypadek z przyczyn organizacyjnych

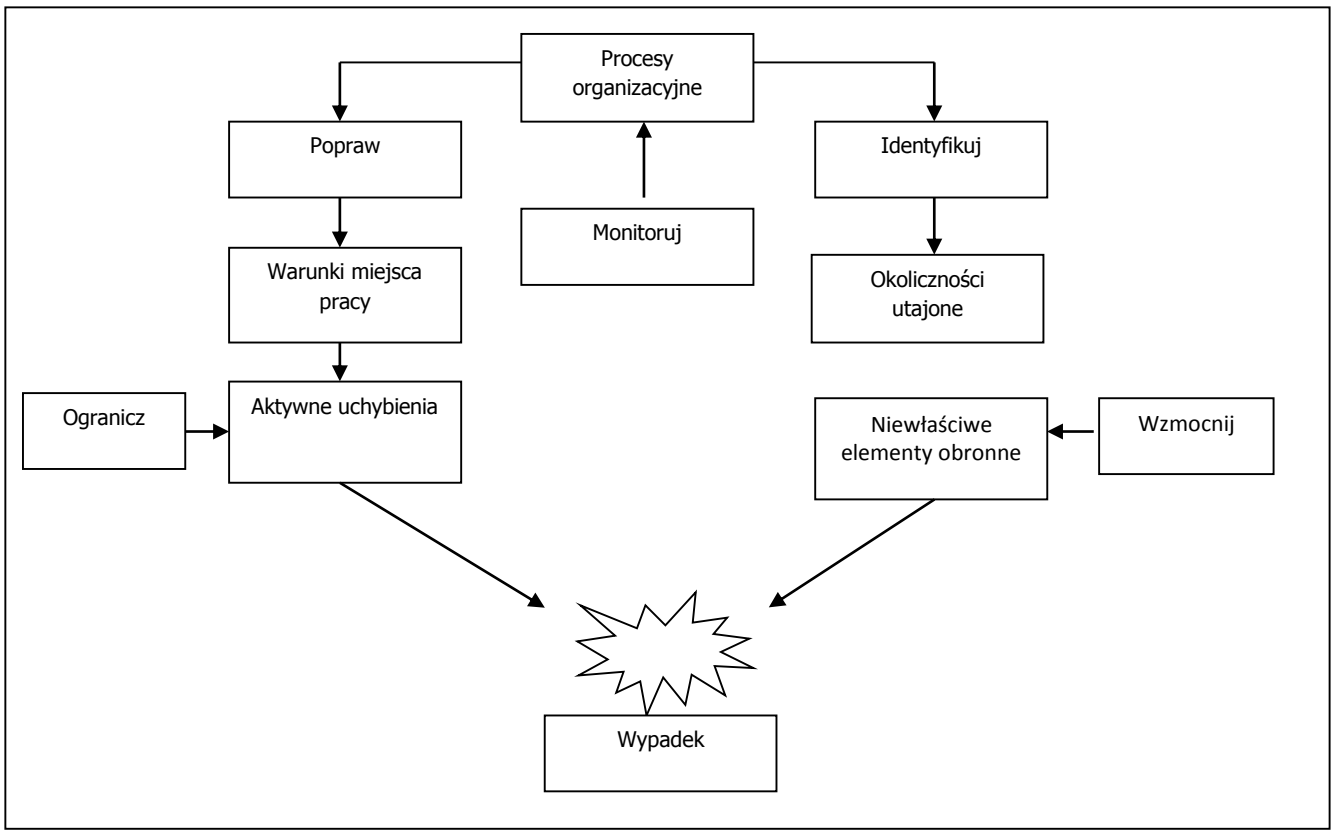
2.3.5. Pojęcie wypadku z przyczyn organizacyjnych, leżące u podłoża modelu Reasona, można najlepiej zrozumieć podchodząc do niego jak do budowania z klocków, przy czym klocków jest pięć (Rys. 2-3). Górny klocek reprezentuje procesy organizacyjne. Są to działania, które każda organizacja może bezpośrednio kontrolować w rozsądnym zakresie. Typowe przykłady obejmują: działania koncepcyjne, planowanie, komunikację, przydzielanie zasobów oraz nadzór. Nie ulega wątpliwości, że dwa podstawowe dla bezpieczeństwa procesy organizacyjne to alokacja zasobów i komunikacja. Potknięcia i niedostatki w tych procesach organizacyjnych są wylęgarniami dwukierunkowej ścieżki prowadzącej do niepowodzenia.

2.3.6. Jedna jest ścieżką stanów uśpionych. Przykłady stanów uśpionych mogą obejmować: niedostatki w projektach urządzeń, niekompletne/niewłaściwe standardowe procedury operacyjne i niedostatki szkolenia. W kategoriach ogólnych, warunki uśpione można zgrupować w dwa zbiory. Jeden zbiór to niewystarczająca identyfikacja zagrożeń i nieprawidłowe zarządzanie ryzykiem dotyczącym bezpieczeństwa, gdzie ryzyko dotyczące bezpieczeństwa, będące konsekwencją zagrożeń, nie są utrzymane pod kontrolą, lecz wędrują swobodnie po systemie by w końcu uaktywnić się pod wpływem czynników operacyjnych.

2.3.7. Drugi zbiór jest znany jako normalizacja odchyleń; pojęcie które, mówiąc prosto, wskazuje na konteksty operacyjne, gdzie wyjątki stają się regułami. Alokacja zasobów w tym przypadku jest ekstremalnie wadliwa. W konsekwencji braku zasobów, jedynym sposobem, którym bezpośrednio odpowiedzialny personel operacyjny może realizować działania operacyjne jest stałe „chodzenie na skróty", co wymaga stałego naruszania zasad i procedur.

2.3.8. Stany uśpione posiadają całkowity potencjał do przełamywania elementów obronnych systemu lotnictwa. Typowo, elementy obronne w lotnictwie można pogrupować w trzy duże kolumny: technika, szkolenie i przepisy. Elementy obronne są zwykle ostatnią siecią bezpieczeństwa, która wychwytuje stany uśpione, jak również konsekwencje uchybień ludzkich działań. Większość, jeśli nie wszystkie, strategii łagodzenia elementów ryzyka dotyczącego bezpieczeństwa bazuje na wzmacnianiu istniejących lub budowaniu nowych elementów obronnych.

2.3.9. Drugą ścieżką, wywodzącą się z procesów organizacyjnych, jest ścieżka warunków panujących na stanowisku pracy. Warunki stanowiska pracy są czynnikami, które bezpośrednio wpływają na sprawność ludzi na stanowiskach pracy w lotnictwie. Warunki panujące na stanowisku pracy są w dużej mierze odbierane intuicyjnie, przy czym pracownicy z doświadczeniem operacyjnym doświadczają ich w różnym stopniu; na dane warunki składają się: stabilność zatrudnienia, kwalifikacje i doświadczenie, morale, zaufanie do zarządzających oraz tradycyjne czynniki ergonomiczne, takie jak oświetlenie, ogrzewanie i chłodzenie.



Rys. 2-3 Wypadek z przyczyn organizacyjnych

2.3.10. Warunki pracy, gorsze od optymalnych, sprzyjają aktywnym uchybieniom personelu operacyjnego. Za aktywne uchybienia należy uznać zarówno błędy, jak i naruszenia. Różnicą między błędami a naruszeniami jest element motywacyjny. Osoba, która stara się robić wszystko co możliwe w celu wykonania zadania, przestrzegając przepisów i procedur zgodnych z odbytym szkoleniem, ale niepotrafiąca osiągnąć celu będącego w zasięgu ręki, popełnia błąd. Osoba, która podczas realizacji zadania chętnie odchodzi od przepisów, procedur lub zasad poznanych podczas szkolenia, popełnia naruszenie. Tak więc, zasadniczą różnicą między błędami a naruszeniami jest intencja.

2.3.11. Z perspektywy wypadku z przyczyn organizacyjnych, wysiłki na rzecz bezpieczeństwa powinny monitorować procesy organizacyjne po to by wykrywać stany uśpione i tym samym wzmacniać elementy obronne. Wysiłki na rzecz bezpieczeństwa powinny również poprawiać warunki stanowiska pracy w celu ograniczania aktywnych uchybień, ponieważ kombinacja tych wszystkich czynników powoduje załamywanie się bezpieczeństwa.

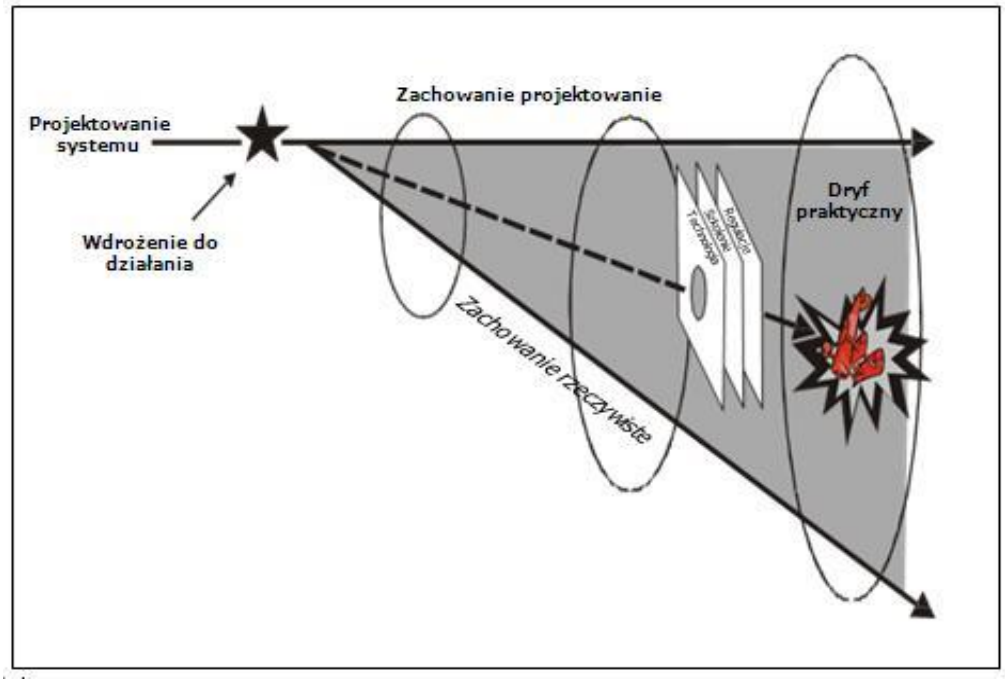
Dryf praktyczny

2.3.12. Teoria dryfu praktycznego Scotta A. Snooka jest używana jako podstawa do zrozumienia jak, w lotnictwie, działanie bazowe systemu „dryfuje", oddalając się od pierwotnego wzorca, w sytuacji gdy procesy i procedury firmy nie są w stanie przewidzieć wszystkich sytuacji, jakie mogą wystąpić w codziennych operacjach.

2.3.13. Podczas wczesnych etapów projektowania systemu (np. przestrzeni kontrolowanego ruchu lotniczego, wprowadzania konkretnych urządzeń, rozbudowywania schematu operacji lotniczych itd.) brane są pod uwagę współoddziaływania operacyjne pomiędzy ludźmi a techniką, jak również kontekst operacyjny, w celu identyfikacji spodziewanych ograniczeń w działaniu, jak również potencjalnych zagrożeń. Wstępne projektowanie systemu opiera się na trzech podstawowych założeniach: że dostępna jest technika potrzebna do osiągnięcia celów produkcyjnych, że ludzie są właściwie przeszkoleni do posługiwania się techniką i że przepisy i procedury będą dyktować działanie systemu i ludzi. Te przesłanki stanowią bazę działania systemu, który może być graficznie przedstawiony jako linia prosta od daty eksploatacyjnego uruchomienia systemu do wycofania go z eksploatacji (Rys. 2-4).

2.3.14. Po pełnym uruchomieniu eksploatacyjnym, system działa tak jak był zaprojektowany, działając przez większość czasu zgodnie ze swoją podstawą. Jednak w rzeczywistości, operacyjne działanie systemu jest inne niż projektowane, co jest konsekwencją jego działania w rzeczywistych warunkach eksploatacyjnych i otoczeniu legislacyjnym. Ponieważ dryf jest

konsekwencją codziennej praktyki, określa się go dryfem praktycznym (”practical drift”). Termin „dryf” jest użyty w tym kontekście jako stopniowe oddalanie się od zamierzonego kursu, spowodowane wpływami zewnętrznymi.



Rys. 2-4. Dryf praktyczny

2.3.15. Dryf praktyczny od zachowania projektowanego do zachowania operacyjnego jest przewidywany w każdym systemie, bez względu na to w jak przemyślany sposób i jak starannie został system zaplanowany. Niektóre z powodów dryfu praktycznego mogą obejmować: technikę, która nie zawsze działa tak jak to przewidziano; procedury, których w konkretnych warunkach operacyjnych nie można wykonać w sposób zaplanowany; przepisy, które nie mają zastosowania w ramach pewnych ograniczeń w danym kontekście; wprowadzenie zmian w systemie, w tym dodanie nowych komponentów; interakcje z innymi systemami i tak dalej. Faktem jednak pozostaje to, że pomimo wszystkich prowadzących do dryfu ograniczeń systemu, ludzie działający w praktycznym dryfie na co dzień, powodują iż system działa dzień w dzień, gdyż stosują miejscowe adaptacje i osobiste strategie „ponad to, co przewiduje podręcznik”.

2.3.16. Jak wyjaśniono na Rys. 2-4, uchwycenie i przeanalizowanie informacji o tym co dzieje się w praktycznym dryfie dostarcza bogatego materiału poznawczego na temat udanych adaptacji w zakresie bezpieczeństwa, więc przydatnego dla kontroli i łagodzenia ryzyka dotyczącego bezpieczeństwa. Im bliżej początku dryfu praktycznego, tym większa możliwość systematycznego przechwytywania informacji, oraz tym większą liczbę zagrożeń i niebezpieczeństw można przewidzieć i można się nimi zająć, doprowadzając do formalnych wniosków dla przeprojektowania lub poprawienia systemu. Jednakże niekontrolowane rozprzestrzenianie się lokalnych modyfikacji i indywidualnych strategii może prowadzić do tego, że system odejdzie zbyt daleko od spodziewanego zachowania podstawowego do takiego stopnia, że incydent lub wypadek staną się bardziej prawdopodobne.

2.4. LUDZIE, KONTEKST I BEZPIECZEŃSTWO

2.1. System lotniczy obejmuje dostawców produktów i dostawców usług oraz organizacje krajowe. Jest to skomplikowany system, który wymaga oceny wpływu czynnika ludzkiego na bezpieczeństwo i zrozumienia jak zachowania ludzkie mogą się zmieniać na skutek wielorakich i wzajemnie na siebie oddziałujących komponentów systemu.

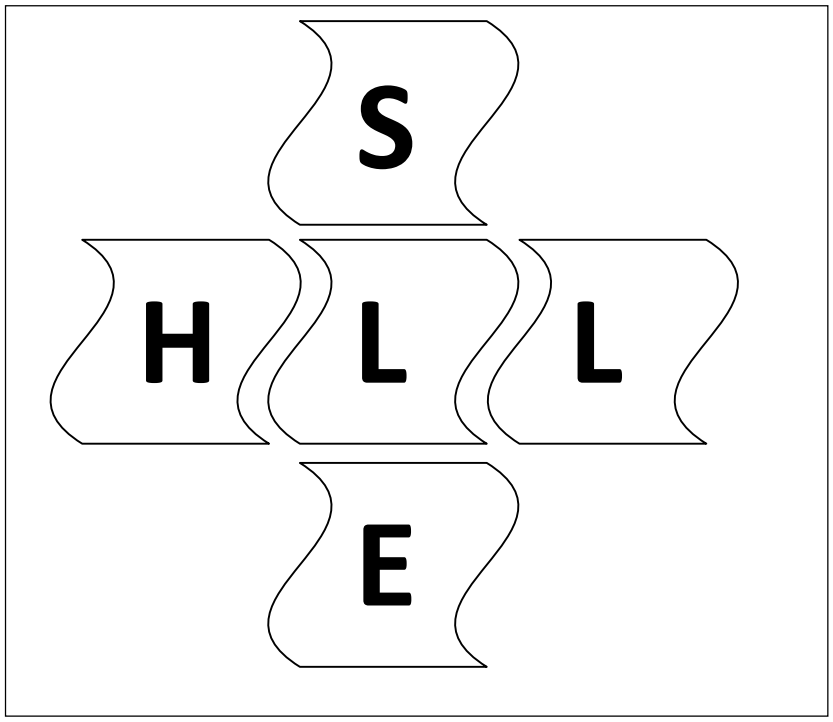
2.2. Model SHELL jest narzędziem koncepcyjnym wykorzystywanym do analizowania wzajemnego oddziaływania różnorodnych komponentów systemu. Rys. 2-5 przedstawia podstawowe relacje pomiędzy ludźmi i innymi komponentami stanowiska pracy. Model SHELL zawiera cztery następujące komponenty:

a) Oprogramowanie (S) [ang. „Software"] (procedury, szkolenie, wsparcie itp.);

b) Sprzęt (H) [ang. „Hardware"] (maszyny i wyposażenie);

c) Środowisko (E) [ang. „Environment"] (środowisko pracy, w którym reszta systemu L-H-S musi funkcjonować); i

d) Człowiek (L) [ang. „Liveware"] (ludzie w miejscu pracy).



Rys. 2-5. Model SHELL - komponenty i relacje

2.3. *Człowiek.* W centrum modelu SHELL znajdują się ludzie bezpośrednio zaangażowani w działania. Pomimo tego, że ludzie przystosowują się bardzo dobrze, wykazują jednak znaczne zróżnicowanie w swoich działaniach. Ludzie nie są znormalizowani w tym samym stopniu co sprzęt, więc krawędzie tego bloku nie są proste ani równe. Ludzie nie współdziałają też idealnie z różnymi składnikami środowiska, w którym pracują. Aby uniknąć napięć mogących wpłynąć negatywnie na działania ludzkie, należy zrozumieć skutki zakłóceń w relacjach między różnymi blokami SHELL i centralnym blokiem Liveware. Pozostałe komponenty systemu muszą być starannie dopasowane do ludzi, jeśli chce się uniknąć napięć w systemie. Model SHELL jest użyteczny w wizualizacji następujących relacji pomiędzy różnorodnymi komponentami systemu lotniczego:

a) *Człowiek-Sprzęt* (L-H). Styk L-H dotyczy relacji pomiędzy człowiekiem i fizycznymi cechami sprzętu, maszyn i obiektów. Relacje pomiędzy ludźmi i techniką są zwykle rozważane w odniesieniu do zachowań ludzkich w kontekście operacji lotniczych; istnieje naturalna ludzka tendencja przystosowywania się do rozbieżności między L a H. Niemniej jednak, ta tendencja może maskować poważne niedostatki, które stają się oczywiste dopiero po wystąpieniu jakiegoś zdarzenia;

b) *Człowiek-Oprogramowanie* (L-S). Interfejs L-S to relacja pomiędzy człowiekiem a systemami wspomagającymi w miejscu pracy, np. między przepisami, podręcznikami, listami kontrolnymi, publikacjami, standardowymi instrukcjami operacyjnymi (SOP) i oprogramowaniem komputerowym. Obejmuje ona takie sprawy jak aktualność doświadczeń, dokładność, format i sposób prezentacji, słownictwo, czytelność i symbole;

c) *Człowiek-Człowiek* (L-L). Interfejs L-L jest relacją pomiędzy osobami w środowisku pracy. Ponieważ załogi lotnicze, kontrolerzy ruchu, personel obsługi technicznej statków powietrznych i inny personel operacyjny funkcjonują w zespołach, ważne jest aby dostrzegać, że komunikacja i zdolności interpersonalne jak również dynamika grupy wpływają na ludzkie działanie. Pojawienie się zarządzania zasobami załogowymi (CRM) i objęcie nim także służb ruchu lotniczego (ATS) oraz obsługi technicznej spowodowało skupienie się na zarządzaniu błędami operacyjnymi w różnorodnych dziedzinach lotnictwa. Relacje między personelem a kierownictwem oraz ogólna kultura organizacyjna również należą do obszaru tej relacji;

d) *Człowiek-Środowisko* (L-E). Ten interfejs obejmuje relacje pomiędzy człowiekiem a środowiskiem wewnętrznym i zewnętrznym. Wewnętrzne środowisko miejsca pracy obejmuje takie warunki fizyczne jak temperaturę, otaczające

oświetlenie, hałas, wibrację i jakość powietrza. Środowisko zewnętrzne obejmuje aspekty operacyjne, takie jak czynniki pogodowe, infrastrukturę lotniczą i teren. Relacja dotyczy także zależności pomiędzy wewnętrznym środowiskiem człowieka i jego środowiskiem zewnętrznym. Potencjał psychologiczny i fizjologiczny, w tym choroby, zmęczenie, niepewność finansowa i relacje w pracy wraz z obawami o karierę mogą być albo wywołane przez wzajemne oddziaływania L-E albo mogą pochodzić z zewnętrznych źródeł wtórnych. Lotnicze środowisko pracy obejmuje zakłócenia normalnego rytmu biologicznego i harmonogramu snu. Dodatkowe czynniki środowiskowe mogą się wiązać z cechami danej organizacji, które mogą wpływać na procesy decyzyjne i wywoływać presję by korzystać z prowizorycznych rozwiązań lub drobnych odchyleń od standardowych procedur operacyjnych.

2.4. Zgodnie z modelem SHELL, niedopasowanie pomiędzy człowiekiem i czterema pozostałymi komponentami przyczynia się do błędów ludzkich. Dlatego też te interakcje muszą być oceniane i brane pod uwagę we wszystkich częściach systemu lotniczego.

2.5. BŁĘDY I NARUSZENIA

2.5.1. Efektywne wdrożenie SMS przez dostawcę produktu lub dostawcę usług, jak również efektywny nadzór Państwa nad SMS są uzależnione od wyraźnego, wzajemnego rozumienia błędów i naruszeń oraz rozróżniania jednych od drugich. Różnica pomiędzy pomyłkami a naruszeniami tkwi w intencji. Pomyłka jest niezamierzona, podczas gdy naruszenie jest celowym aktem lub zaniechaniem polegającym na odstąpieniu od ustanowionych procedur, protokołów, norm lub stosowanych praktyk

2.5.2. Pomyłki lub naruszenia mogą skutkować nieprzestrzeganiem przepisów lub przyjętych procedur operacyjnych. Brak innych rozwiązań niż środki dyscyplinarne podejmowane w odpowiedzi na przypadki nieprzestrzegania może prowadzić do spadku liczby zgłaszanych pomyłek. W związku z tym, przy ustalaniu właściwego środka dyscyplinarnego, Państwo i dostawca produktu lub dostawca usług muszą rozważyć czy przypadki nieprzestrzegania są wynikiem naruszeń czy nieumyślnych pomyłek, przy czym zwykle używanym kryterium jest to czy nieprzestrzeganie jest wynikiem winy umyślnej czy rażącego niedbalstwa.

Błędy

2.5.3. Jak wskazano wyżej, pomyłka jest definiowana jako: „działanie lub zaniechanie pracownika operacyjnego, prowadzące do odchodzenia od zamiaru lub oczekiwań własnych lub organizacji". W kontekście SMS zarówno Państwo, jak i dostawca produktu lub dostawca usług muszą zrozumieć i zakładać, że ludzie będą popełniać pomyłki bez względu na poziom zastosowanej techniki, poziom wyszkolenia oraz istnienie przepisów, procesów i procedur. Ważnym celem jest zatem ustanowienie i utrzymywanie elementów obronnych w celu redukowania prawdopodobieństwa występowania pomyłek i, co równie istotne, redukowania następstw pomyłek gdy już się zdarzą. Aby efektywnie realizować te założenia, pomyłki muszą zostać zidentyfikowane, zgłoszone i przeanalizowane, tak aby można zastosować właściwe środki zaradcze. Pomyłki można podzielić na dwie następujące kategorie:

a) *Pomyłki i uchybienia (Slips and failures).* Są to niepowodzenia w realizowaniu zamierzonej czynności. Pomyłki są działaniami, które nie idą zgodnie z planem, a uchybienia są wynikiem defektu pamięci. Przykładowo, użycie dźwigni klap, zamiast dźwigni podwozia, jest pomyłką. Zapomnienie o pozycji z listy kontrolnej jest uchybieniem;

b) *Błędy (Mistakes)* są wadami w planie działania. Nawet jeśli realizacja planu byłaby właściwa, to i tak osiągnięcie zamierzonego wyniku nie byłoby możliwe.

2.5.4. Aby kontrolować i eliminować błędy, należy wdrożyć strategie bezpieczeństwa. Strategie kontrolowania błędów wzmacniają podstawowe elementy obronne systemu lotniczego. Obejmują one:

a) Strategie redukcyjne *(reduction strategies)* przewidują bezpośrednią interwencję w celu redukcji lub eliminacji czynników przyczyniających się do błędu. Przykłady strategii redukcyjnych obejmują poprawę czynników ergonomicznych i zredukowanie zakłóceń środowiskowych;

b) Strategie wychwytujące *(capturing strategies)* zakładają, że błąd zostanie popełniony. Ich celem jest wychwycenie błędu zanim odczuwalne będą jakiekolwiek jego negatywne konsekwencje. Strategie wychwytujące różnią się od redukcyjnych tym, że wykorzystują listy kontrolne i inne działania proceduralne a nie eliminują błędów bezpośrednio;

c) Strategie tolerancyjne *(tolerance strategies)* dotyczą zdolności systemu do przyjęcia, że błąd będzie popełniony lecz bez następstw poważnych. Przykładami działań, które zwiększają tolerancję systemu na błędy jest wprowadzenie systemów nadmiarowych lub procesów wielokrotnie kontrolowanych.

2.5.5. Ponieważ na działanie personelu mają wpływ generalnie czynniki organizacyjne, regulacyjne i środowiskowe, zarządzanie ryzykiem dotyczącym bezpieczeństwa musi uwzględniać działania koncepcyjne, procesy i procedury dotyczące komunikacji, harmonogramu pracy personelu, alokacji zasobów i ograniczeń budżetowych, które mogą przyczynić się do wystąpienia błędu.

Naruszenia

2.5.6. Naruszenie jest definiowane następująco: „zamierzony akt umyślnego uchybienia lub zaniechania, skutkujący odejściem od ustalonych przepisów, procedur, norm lub pragmatyki". Niemniej jednak, nieprzestrzeganie niekoniecznie jest wynikiem naruszenia, gdyż odejście od wymogów stawianych przez przepisy lub procedury operacyjne może być wynikiem

błędu. Aby jeszcze bardziej skomplikować zagadnienie – uznając, że naruszenia są aktami świadomymi, uważa się jednak że nie zawsze są działaniami w złej wierze. Poszczególne osoby mogą świadomie odstępować od norm, wierząc że naruszenie ułatwia wykonanie zadania bez powodowania negatywnych konsekwencji. Naruszenia tego rodzaju są błędami w osądzie i nie mogą automatycznie skutkować postępowaniem dyscyplinarnym, zgodnie z przyjętą w tym zakresie polityką. Naruszenia tego typu można podzielić następująco:

a) Naruszenia sytuacyjne są popełniane w odpowiedzi na wystąpienie specyficznego kontekstu takich czynników, jak presja czasu lub duże obciążenie pracą;

b) Naruszenia rutynowe stają się normalnym sposobem wykonywania zadań w ramach grupy. Takie naruszenia popełniane są w odpowiedzi na sytuacje, w których przestrzeganie ustalonych procedur utrudnia wykonanie zadania. Może to być spowodowane względami praktycznymi/nakładem pracy, brakami w projekcie relacji człowiek-technika i innymi, które powodują, że ludzie zaczynają stosować uproszczenia, które w końcu stają się rutyną. Te odchylenia, określane słowem dryf, mogą trwać bez następstw, jednakże z czasem, mogą stać się częstsze i skutkować potencjalnie poważnymi konsekwencjami. W niektórych przypadkach, rutynowe naruszenia są uzasadnione i mogą skutkować włączeniem rutynowego naruszenia do przyjętych procedur - po dokonaniu właściwej oceny ryzyka, która wykaże, że bezpieczeństwo na tym nie ucierpi;

c) Naruszenia wymuszone organizacyjnie mogą być uznane za rozszerzenie naruszeń rutynowych. Ten typ naruszeń ma tendencję do pojawiania się, gdy organizacja usiłuje sprostać wymaganiom zwiększenia wydajności poprzez ignorowanie lub zbyt elastyczne traktowanie swoich elementów obronnych.

2.6. KULTURA BEZPIECZEŃSTWA

2.6.1. Kulturę określają przekonania, wartości, uprzedzenia i wynikające z nich zachowania, które są wspólne dla członków społeczności, grupy lub organizacji. W zarządzaniu bezpieczeństwem istotne znaczenie ma zrozumienie tych komponentów kulturowych oraz ich wzajemnych relacji. Najbardziej wpływowe są trzy komponenty kulturowe: organizacyjny, zawodowy i narodowy. Kluczowym komponentem tych różnych kultur jest kultura raportowania. Mieszanka komponentów kulturowych może się znacząco różnić w poszczególnych organizacjach i może negatywnie wpływać na raportowanie zagrożeń, wspólnie dokonywaną analizę pierwotnych przyczyn zdarzeń i zmniejszenie ryzyka do akceptowalnego poziomu. Ciągła poprawa w zapewnianiu bezpieczeństwa jest możliwa wtedy, gdy bezpieczeństwo staje się wartością dla organizacji, jak również priorytetem w wymiarze narodowym lub profesjonalnym.

2.6.2. Kultura bezpieczeństwa obejmuje powszechne odczucia i przekonania członków organizacji odnoszące się do bezpieczeństwa publicznego i może decydować o ich zachowaniach. Prawidłowo pojmowana/rozumiana kultura bezpieczeństwa opiera się na wysokim poziomie zaufania i szacunku pomiędzy pracownikami i kierownictwem i dlatego musi być kreowana i wspierana przez kierownictwo wyższego szczebla.

2.6.3. Prawidłowo pojmowana kultura bezpieczeństwa zakłada aktywne poszukiwanie usprawnień, zachowanie wrażliwości na zagrożenia, korzystanie z systemów i narzędzi do ciągłego monitorowania, analizowania i badania. Musi ona funkcjonować zarówno w państwowych organach lotniczych, jak i w organizacjach dostawców usług i dostawców produktów. Inne cechy charakterystyczne prawidłowo pojmowanej kultury to wspólne zaangażowanie się pracowników i kierownictwa w osobistą odpowiedzialność za bezpieczeństwo, zaufanie do systemu bezpieczeństwa i istnienie udokumentowanego zestawu reguł i zasad postępowania. Ostateczna odpowiedzialność za ustanowienie i przestrzeganie właściwych praktyk dotyczących bezpieczeństwa spoczywa na kierownictwie organizacji. Kultura bezpieczeństwa nie może być efektywna, jeśli nie jest osadzona w kulturze organizacyjnej.

2.6.4. Kultura organizacyjna odnosi się do cech charakterystycznych bezpieczeństwa i tego, jak jest postrzegana przez poszczególne osoby oddziałujące na siebie w obrębie konkretnego podmiotu. Stosowane w organizacjach systemy wartości zawierają zasady ustalania priorytetów czy też utrzymywania równowagi w takich obszarach jak: produktywność kontra jakość, bezpieczeństwo a efektywność, finanse a technika, zawodowy czy akademicki, działanie wymuszone czy korygujące.

2.6.5. Największe możliwości kreowania i utrzymywania skutecznej, samowystarczalnej kultury zarządzania bezpieczeństwem istnieją na poziomie organizacji. W głównej mierze, to organizacja determinuje o angażowaniu się podczas wykonywania działań kierowniczych lub operacyjnych, podczas realizowania lub nadzorowania działalności lotniczej. Kultura organizacyjna wyznacza granice dla akceptowalnych zachowań kierowniczych i operacyjnych poprzez ustanowienie norm i limitów. Zatem, kultura organizacyjna jest kamieniem węgielnym dla podejmowania decyzji przez kierownictwo i pracowników.

2.6.6. Kultura organizacyjna ma potencjał oddziaływania na:

a) interakcje między starszymi i młodszymi rangą członkami grupy;

b) interakcje między branżą a pracownikami organów regulacyjnych;

c) stopień wymiany informacji wewnątrz organizacji oraz z organami regulacyjnymi;

d) nadrzędność pracy zespołowej w organach regulacyjnych lub organizacji branży;

e) zachowania pracowników w trudnych okolicznościach operacyjnych;

f) akceptację konkretnych technologii i korzystanie z nich; oraz

g) tendencję do stosowania środków dyscyplinarnych za błędy w zakresie dostaw i usług oraz popełnionych przez organ regulacyjny.

2.6.7. Na kulturę organizacji wpływają takie czynniki jak:

a) biznesowe zasady działania i procedury;

b) zachowania i praktyki nadzorcze;

c) cele w zakresie poprawy bezpieczeństwa oraz minimalne poziomy tolerancji;

d) stosunek kierownictwa do zagadnień dotyczących jakości i bezpieczeństwa;

e) szkolenie i motywowanie pracowników;

f) relacje pomiędzy organami regulacyjnymi a dostawcami i dostawcami usług;

g) zasady zachowania równowagi między życiem prywatnym a zawodowym.

2.6.8. Dla podniesienia poziomu w zakresie kultury organizacyjnej kluczowy jest również sposób w jaki kierownictwo reaguje na co dzień na sprawy dotyczące bezpieczeństwa. Współpraca pomiędzy pracownikami pierwszej linii z ich odpowiednikami w dziedzinach bezpieczeństwo i jakość, jak również z reprezentantami organów regulacyjnych wskazuje na istnienie właściwej kultury organizacji. Relacje te powinny charakteryzować się zawodową uprzejmością, przy zachowaniu podziału kompetencji, niezbędnego do zapewnienia obiektywizmu i odpowiedzialności.

2.6.9. Efektywnym sposobem promowania działań bezpiecznych jest zapewnienie by organizacja zbudowała środowisko, w którym wszyscy pracownicy czują się odpowiedzialni za bezpieczeństwo. Staje się to widoczne, gdy pracownicy biorą pod uwagę swój wpływ na bezpieczeństwo we wszystkim co robią, gdy zgłaszają wszystkie zagrożenia, błędy i niebezpieczeństwa a także wspierają rozpoznawanie i usuwanie wszelkich zagrożeń towarzyszących ich działalności. Dodatkowo, kierownictwo musi budować środowisko, w którym pracownicy są świadomi istnienia ryzyka dotyczącego bezpieczeństwa, otrzymują systemy, którymi mogą się skutecznie ochronić oraz mają zapewnioną ochronę przy ujawnianiu informacji w ramach systemu raportowania bezpieczeństwa. Skuteczna kultura bezpieczeństwa w przedsiębiorstwie jest sposobem harmonizowania różnorodnych kultur narodowych i zawodowych.

2.6.10. *Kultura zawodowa* różnicuje cechy poszczególnych grup zawodowych (tj. charakterystycznych zachowań pilotów wobec typowych zachowań kontrolerów ruchu, pracowników władz lotnictwa cywilnego czy personelu obsługi technicznej). Poprzez selekcję personelu, kształcenie, szkolenie, nabieranie doświadczenia w trakcie pracy, poprzez nacisk pracowników na równorzędnych stanowiskach itd., fachowcy skłaniają się do przejmowania systemu wartości i wzorców zachowania swych równolatków i poprzedników. Skuteczna kultura zawodowa odzwierciedla zdolność grup zawodowych do odróżniania zachowań bezpiecznych od spraw kontraktowych czy branżowych. Właściwą kulturą zawodową można scharakteryzować jako zdolność wszystkich grup zawodowych w obrębie jednej organizacji do wspólnego działania na rzecz bezpieczeństwa.

2.6.11. *Kultura narodowa* rozróżnia cechy charakterystyczne poszczególnych narodów, w tym rolę jednostki w społeczeństwie, sposób podziału władzy, cele narodowe w odniesieniu do zasobów, odpowiedzialności, moralności, celów i różnych systemów prawnych. Z perspektywy zarządzania bezpieczeństwem, kultura narodowa odgrywa ogromną rolę w określaniu charakteru i zakresu polityki egzekwowania prawa, w tym określanie relacji między personelem organów nadzoru a personelem branży oraz zakresem ochrony informacji dotyczących bezpieczeństwa.

2.6.12. Kultura narodowa kształtuje wewnętrzny składnik osobistych przekonań, który określa indywidualne postrzeganie bezpieczeństwa przez daną osobę zanim zostanie ona członkiem organizacji. Z tego względu na kulturę organizacyjną znaczny wpływ mają kultury narodowe członków organizacji.

2.6.13. Realizując program zarządzania bezpieczeństwem, kierownicy powinni uważnie ocenić i wziąć pod uwagę różnice w kulturach narodowych zatrudnionych pracowników. Przykładowo, postrzeganie zagrożenia dla bezpieczeństwa może się różnić znacznie w różnych kulturach narodowych. Aspekty związane z bezpieczeństwem, w tym komunikacja i style przywództwa oraz interakcje między przełożonymi a podwładnymi mogą wymagać przystosowania ich do wielokulturowości w środowisku pracowniczym.

2.6.14. Kultura raportowania powstaje w oparciu o przekonania i stosunek personelu do korzyści i możliwych szkód związanych z systemami raportowania oraz o ostateczny wpływ tych czynników na ich akceptację i korzystanie z takich systemów. Duży wpływ na kulturę raportowania ma kultura organizacyjna, zawodowa i narodowa. Kultura raportowania jest jednym z kryteriów oceny skuteczności systemu bezpieczeństwa. Właściwa kultura raportowania dąży do zróżnicowania zamierzonych i niezamierzonych odchyleń i wyznaczenia najlepszego kierunku działań zarówno dla organizacji jako całości, jak i dla bezpośrednio zaangażowanych osób.

2.6.15. Sukces systemu raportowania zależy od nieustannego napływu informacji od personelu pierwszej linii. Działania koncepcyjne, w których rozróżnia się świadome czyny zabronione od niezamierzonych błędów, przewidywanie stosownych sankcji lub reagowanie bez karania, są istotne dla zapewnienia skutecznego raportowania niedoskonałości w systemie

bezpieczeństwa. Kultura „absolutnego braku winy" jest nieracjonalna a nawet niewykonalna. Choć kierownictwo uzyska wprawdzie informacje dotyczące bezpieczeństwa, ale system będzie nieskuteczny, jeżeli będzie kolidował z właściwymi działaniami dyscyplinarnymi. Odwrotnie zaś, kultura która nie rozróżnia niezamierzonych błędów/pomyłek od zamierzonych czynów zabronionych będzie hamować proces raportowania. Jeśli personel unika raportowania w obawie przed karą, kierownictwo nie pozyskuje istotnych informacji dotyczących bezpieczeństwa.

2.6.16. Generalnie, personel musi ufać, że znajdzie wsparcie w przypadku każdej decyzji podjętej w interesie bezpieczeństwa, ale musi także rozumieć, że celowe/umyślne naruszanie polityki bezpieczeństwa nie będzie tolerowane. Dlatego też dobrowolny system raportowania powinien być poufny i działać zgodnie z właściwymi zasadami bezsankcyjnymi. System powinien także dostarczać personelowi informacji zwrotnych na temat poprawy bezpieczeństwa osiągniętego w wyniku otrzymanych raportów. Cel ten wymaga bezpiecznego i łatwego dostępu do systemów raportowania o bezpieczeństwie, aktywnego pozyskiwania danych i proaktywnego traktowania danych przez kierownictwo.

2.6.17. Informacje dotyczące bezpieczeństwa powinny być pozyskiwane wyłącznie dla poprawy bezpieczeństwa lotniczego, a ochrona tych informacji jest niezbędna dla zapewnienia ich ciągłego dopływu. Można to osiągnąć poprzez zapewnienie/ustanowienie poufnego, dobrowolnego i bezsankcyjnego systemu raportowania. Korzyści będą dwojakie. Pracownicy często znajdują się najbliżej zagrożeń dotyczących bezpieczeństwa, więc system raportowania umożliwia im aktywną identyfikację tych zagrożeń. Jednocześnie, kierownictwo jest w stanie gromadzić istotne informacje o zagrożeniach dla bezpieczeństwa i budować zaufanie personelu.

2.6.18. Po zebraniu i zarchiwizowaniu danych, informacja musi zostać przetworzona w celu wdrożenia właściwych działań, o których należy we właściwym czasie poinformować pracowników pierwszej linii.

Ocena kultury bezpieczeństwa i jej promowanie

2.6.19. Skuteczność kultury bezpieczeństwa można mierzyć i monitorować za pomocą wymiernych wskaźników. W środowisku dojrzałej kultury bezpieczeństwa, można przewidzieć, że organizacje będą w stanie wprowadzić mechanizm wewnętrznej oceny kultury bezpieczeństwa (Organization Safety Culture - OSC). Ocena ta może być następnie wzbogacona poprzez bardziej zaawansowane technicznie czy też ukierunkowane profilowanie ryzyka organizacji (Organization Risk Profiling - ORP). Równocześnie, organizacje branży i/lub organizacje legislacyjne mogą rozważyć ustanowienie systemu nagradzania (np. nagrody za wysoki poziom kultury bezpieczeństwa) dla dostawców lub dostawców usług biorących dobrowolnie udział w ocenie OSC/ORP. Parametry, które należałoby ocenić w ramach realizacji OSC/ORP, to czynniki organizacyjne i wyniki wykraczające poza konwencjonalne wymagania ujęte w przepisach, niemniej wciąż odnoszące się do kultury bezpieczeństwa firmy i stąd mające wpływ na osiągany w niej poziom bezpieczeństwa. Taki jest główny cel ocen OSC/ORP. Służy on uzupełnieniu tradycyjnego nadzoru legislacyjnego, odnosząc się do czynników organizacyjnych (stanów uśpionych), normalnie będących poza zakresem przepisów. Lista kontrolna oceny OSC byłaby bardziej ogólna w treści, podczas gdy lista kontrolna w ORP byłaby w większym stopniu dostosowana do charakteru działań organizacji. Dodatek 1 jest ilustracją ewentualnej listy kontrolnej do oceny OSC/ORP, specyficznych dla danego sektora lotnictwa.

2.7. DYLEMAT ZARZĄDZANIA

2.7.1. Procesy zarządzania bezpieczeństwem identyfikują zagrożenia, które potencjalnie mogą niekorzystnie wpłynąć na bezpieczeństwo. Procesy te dostarczają również faktycznych i obiektywnych mechanizmów do oceny ryzyka stwarzanego przez zagrożenia, wdrażają sposoby eliminowania zagrożeń lub łagodzenia związanego z nimi ryzyka. Rezultatem tych procesów jest ułatwienie osiągania akceptowalnego poziomu bezpieczeństwa przy zachowaniu równowagi w podziale zasobów pomiędzy działalność zasadniczą (eksploatację, produkcję) i zabezpieczanie. Z perspektywy podziału zasobów, szczególnie użyteczna do opisu procesu osiągania równowagi jest koncepcja przestrzeni bezpieczeństwa.

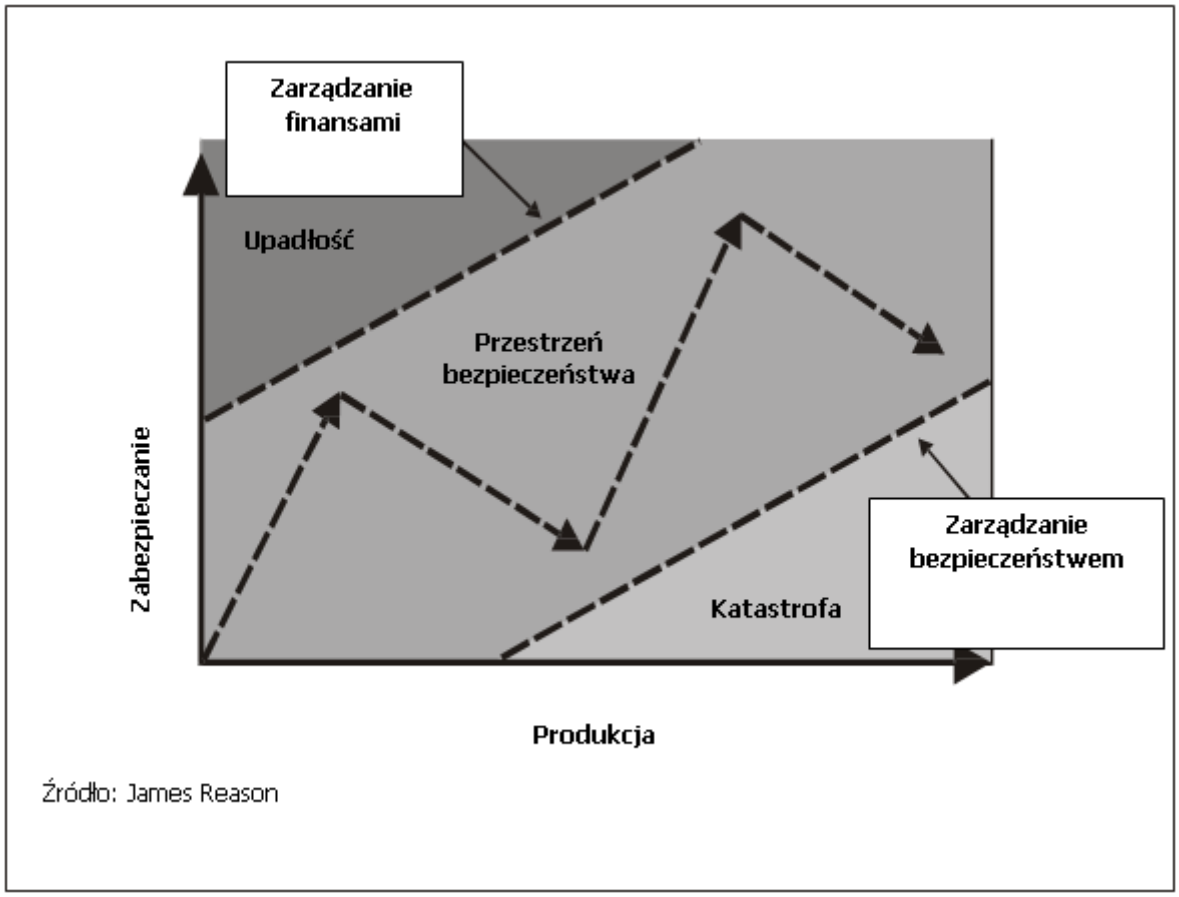
Przestrzeń bezpieczeństwa

2.7.2. W każdej organizacji zajmującej się świadczeniem usług, produkcja i ryzyko dotyczące bezpieczeństwa są ze sobą powiązane. W miarę wzrostu produkcji, może rosnąć ryzyko dotyczące bezpieczeństwa, jeśli niedostępne są niezbędne zasoby lub udoskonalenia procesów. Organizacja musi zdefiniować swoje cele produkcyjne oraz cele dotyczące bezpieczeństwa, poprzez osiągnięcie równowagi pomiędzy wynikami produkcyjnymi a akceptowalnym ryzykiem dotyczącym bezpieczeństwa. Także podczas definiowania celów produkcji, organizacja musi zdefiniować elementy obronne, które utrzymują pod kontrolą ryzyko dotyczące bezpieczeństwa. Dla dostawcy lub dostawcy usług, podstawowymi elementami obronnymi są: technika, szkolenie oraz wewnętrzne procesy i procedury. Dla państwa, podstawowe elementy obronne są podobne, tj.: szkolenie personelu, odpowiednie wykorzystanie techniki, skuteczny nadzór oraz wewnętrzne procesy i procedury wspomagające ten nadzór. Przestrzeń bezpieczeństwa jest strefą, w której organizacja równoważy pożądaną produkcję z jednoczesnym utrzymywaniem wymaganego zabezpieczania bezpieczeństwa poprzez kontrolne elementy ryzyka dla bezpieczeństwa. Przykładowo, producent lub dostarczyciel usług żeglugi powietrznej może chcieć wesprzeć planowany rozwój, inwestując w nowe technologie. Podejmowanie decyzji w takich przypadkach powinno obejmować zarówno ocenę wartości dodanej do produktu organizacji lub usługi danego dostawcy, jak i ocenę związanego z tym ryzyka dotyczącego bezpieczeństwa. Przydzielenie nadmiernych zasobów na chronienie przed ryzykiem i/lub ich kontrolowaniem może skutkować tym, że produkt lub usługa stają się nieopłacalne, co zagraża rentowności organizacji.

2.7.3. Z drugiej strony, przydzielenie nadmiernych zasobów na produkcję, kosztem zapewnienia bezpieczeństwa, może mieć wpływ na wskaźniki bezpieczeństwa produkcji lub usługi i może w ostateczności doprowadzić do wypadku. Dlatego, istotne jest by nakreślić granicę bezpieczeństwa, która dawałaby wczesny sygnał ostrzegający o tym, że ma miejsce przypadek

niezrównoważonego podziału zasobów. Dlatego to, granice przestrzeni bezpieczeństwa powinny być zdefiniowane przez kierownictwo organizacji i powinny być ustawicznie przeglądane by mieć pewność, że właściwie odzwierciedlają one aktualną sytuację właściwie. Patrz Rys. 2-6 ilustrujący granice przestrzeni bezpieczeństwa organizacji.

2.7.4. Potrzeba zachowania równowagi pomiędzy produkcją i zapewnieniem bezpieczeństwa stała się wymaganiem rozumianym i akceptowanym przez dostawców i dostawców usług. Równowaga ta ma również zastosowanie do zarządzania przez Państwo swoim SSP, biorąc pod uwagę wymóg zrównoważenia zasobów potrzebnych Państwu dla funkcji ochronnych, które obejmują certyfikowanie i śledzenie.



Rys. 2-6. Przestrzeń bezpieczeństwa

2.8. ZARZĄDZANIE ZMIANĄ

2.8.1. Organizacje lotnicze, łącznie z organami regulacyjnymi, doświadczają zmian spowodowanych rozwijaniem się bądź kurczeniem, a także zmianami w istniejących systemach, wyposażeniu, zasadach, programach, usługach i przepisach. Zagrożenia mogą być wprowadzone do systemu lotniczego nieumyślnie za każdym razem gdy zachodzi jakaś zmiana. Istniejące bazowe procesy łagodzenia ryzyka dotyczącego bezpieczeństwa też mogą zostać dotknięte. Istniejące praktyki zarządzania bezpieczeństwem wymagają, by systematycznie identyfikować wynikające ze zmian zagrożenia a także opracowywać, wdrażać i następnie oceniać strategie zarządzania ryzykiem dotyczącym bezpieczeństwa. Należyte zarządzanie ryzykiem dotyczącym bezpieczeństwa związanego ze zmianami jest krytycznym wymogiem SSP i SMS.

2.8.2. Zarządzanie ryzykiem dotyczącym bezpieczeństwa a wynikającym ze zmian powinno uwzględniać poniższe trzy kwestie:

a) *Krytyczne ocenianie systemów i czynności*. Krytyczność dotyczy potencjalnych konsekwencji ryzyka dla bezpieczeństwa czy to w procesie projektowania systemu czy w sytuacji związanej ze zmianą systemową. Zmiany w wyposażeniu i w czynnościach związanych z wyższym stopniem ryzyka dotyczącego bezpieczeństwa należy zbadać po to, by mieć pewność, że możliwe będzie podjęcie niezbędnych działań naprawczych w celu kontrolowania pojawiających się przypadków ryzyka dotyczącego bezpieczeństwa;

b) *Stabilność systemów i środowisk operacyjnych*. Zmiany mogą być zaplanowane i odbywać się pod bezpośrednią kontrolą organizacji. Planowane zmiany mogą wiązać się ze wzrostem lub kurczeniem się organizacji, jak również wprowadzeniem nowego wyposażenia, produktu lub usługi. Zmiany nieplanowane,

łącznie ze zmianami, które są operacyjne, polityczne lub ekonomiczne, mogą także stwarzać różne ryzyka które wymagają od organizacji reakcji łagodzącej. Przykłady, w których często zdarzają się zmiany systemowe lub środowiskowe wymagają by kierownicy uaktualniali proces zarządzania ryzykiem oraz przedmiotowe informacje częściej niż w sytuacjach bardziej stabilnych.

c) *Funkcjonowanie w przeszłości.* Dotychczasowe działanie krytycznych systemów może być wiarygodnym wskaźnikiem ich funkcjonowania w przyszłości. W procesie zapewniania bezpieczeństwa należy, dla śledzenia skuteczności zastosowanych środków zapewniania bezpieczeństwa na przestrzeni czasu, stosować analizy trendów, by następnie, w przypadku zmiany sytuacji, włączyć informacje uzyskane na potrzeby planowania przyszłych działań. Ponadto, gdy na skutek przeprowadzonych audytów, ocen, analiz danych, badań czy raportów nastąpi wykrycie i zaradzenie niedostatkom, istotnym będzie takie informacje uwzględnić po to, by zapewnić skuteczność działań naprawczych.

2.9. INTEGRACJA SYSTEMÓW ZARZĄDZANIA

2.9.1. Organizacje lotnicze znacznie różnią się pomiędzy sobą wielkością i złożonością. Każda organizacja posiada hierarchiczny system zarządzania, składający się z wielu podsystemów kierowanych poprzez jakiś rodzaj zarządzania. Organizacja powinna zintegrować swoje systemy zarządzania, które są przeznaczone do osiągania konkretnych celów, np. dostarczania produktów lub usług do klientów. Holistyczny system zarządzania organizacją jest często określany mianem zintegrowany system zarządzania lub po prostu „system zarządzania" organizacją.

2.9.2. Typowe systemy zarządzania wewnątrz organizacji lotniczej mogą obejmować:

a) system zarządzania jakością - *quality management system (QMS);*

b) system zarządzania bezpieczeństwem - *safety management system (SMS);*

c) system zarządzania ochroną - *security management system (SEMS);*

d) system zarządzania środowiskiem - *environmental management system (EMS);*

e) system zarządzania bezpieczeństwem i higieną pracy - *occupational health and safety management system (OHSMS);*

f) system zarządzania finansami - *financial management system (FMS);* oraz

g) system zarządzania dokumentacją - *documentation management system (DMS).*

2.9.3. Każdy system zarządzania jest monitorowany przez odpowiedzialnego przywódcę *(accountable leader).* Złożone organizacje dostawców lub dostawców usług mogą mieć ponad 30 systemów zarządzania, które muszą być zintegrowane w jednym przedsiębiorstwie. Przykłady takich systemów to:

a) system zarządzania dostawami;

b) system zarządzania marketingiem;

c) system zarządzania personelem;

d) system zarządzania obiektami;

e) system zarządzania sprzętem naziemnym;

f) system zarządzania produkcją;

g) system zarządzania szkoleniami;

h) system zarządzania operacjami lotniczymi;

i) system zarządzania przewozami towarów;

j) system zarządzania obsługą statków powietrznych;

k) system zarządzania spedycją;

l) system zarządzania ryzykiem wynikającym ze zmęczenia (FRMS).

2.9.4. W lotnictwie cywilnym rozwija się tendencja integrowania wszystkich wymienionych systemów zarządzania jako funkcjonalnych komponentów w jeden nadrzędny system zarządzania całym przedsiębiorstwem. Taka integracja przynosi wiele oczywistych korzyści:

a) ograniczenie dublowania działań, a więc obniżenie kosztów;

b) zmniejszenie ogólnego ryzyka organizacji oraz wzrost rentowności;

c) zrównoważenie celów potencjalnie sprzecznych; oraz

d) zlikwidowanie potencjalnie sprzecznych obowiązków i relacji.

2.9.5. Każda organizacja zintegruje te systemy opierając się na własnych specyficznych wymaganiach biznesowych. Procesy zarządzania ryzykiem są niezbędnymi cechami systemów SMS, QMS, EMS, FMS, OSHSMS i SeMS. Jeśli SMS miałby działać w izolacji od pozostałych systemów zarządzania, mogłaby wystąpić tendencja do skupienia się wyłącznie na ryzykach dotyczących bezpieczeństwa, bez zrozumienia istoty jakości, ochrony lub zagrożeń dla organizacji ze strony środowiska.

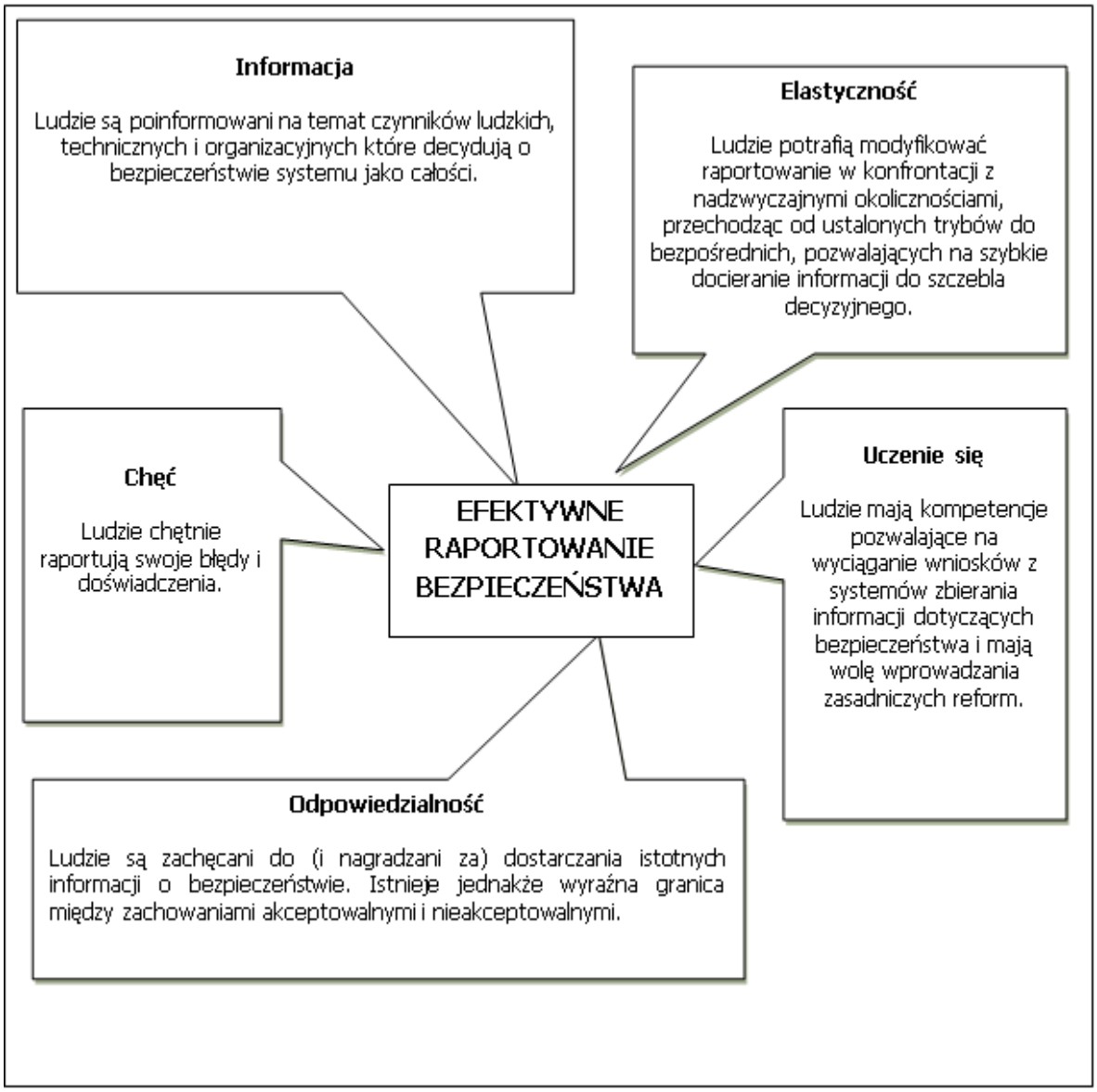
2.9.6. Pomimo że integracja systemów obecnie wykracza poza zakres zharmonizowanych SARPs ICAO i niniejszego podręcznika, liczne władze lotnictwa cywilnego oraz dostawcy i dostawcy usług dostrzegli zalety integracji i dopasowania wielu systemów zarządzania. Szczegóły na temat integracji SMS i QMS znajdują się w Rozdziale 5.

2.10. RAPORTOWANIE I DOCHODZENIA [POWYPADKOWE]

Skuteczne raportowanie dotyczące bezpieczeństwa

2.10.1. Precyzyjne i terminowe raportowanie istotnych informacji dotyczących zagrożeń, incydentów i wypadków jest w zarządzaniu bezpieczeństwem działaniem zasadniczym. Dane, stosowane w analizach bezpieczeństwa, pochodzą z wielu źródeł. Jednym z najlepszych źródeł danych jest bezpośrednie raportowanie przez personel pierwszej linii, ponieważ to oni widzą zagrożenia w codziennej pracy. Warunkiem wstępnym skutecznego systemu raportowania jest miejsce pracy, na którym pracownicy byli przeszkoleni i z którego są stale zachęcani do zgłaszania własnych błędów i doświadczeń, co jest warunkiem wstępnym skutecznego raportowania.

2.10.2. Istnieje pięć podstawowych cech powszechnie kojarzonych z systemami skutecznego raportowania o bezpieczeństwie (patrz Rys. 2-7). Skuteczne raportowanie zagrożeń jest kluczowym komponentem zarządzania bezpieczeństwem. Po zgłoszeniu, dane o zagrożeniach mogą zostać poddane analizom wraz z danymi z innych źródeł, na wsparcie procesów SRM i SA.



Rys. 2-7.Efektywne raportowanie bezpieczeństwa – pięć podstawowych cech

2.10.3. Innym źródłem danych używanych w SRM i SA są raporty z wydarzeń. Mogą one obejmować zdarzenia, od tych o największych konsekwencjach (wypadki, poważne incydenty) aż do zdarzeń o niewielkich konsekwencjach, takich jak incydenty operacyjne, awarie lub wady systemu/sprzętu itd. Przy czym, prawne wymogi obowiązkowego raportowania zdarzeń o dużych konsekwencjach (wypadki, poważne incydenty) są ogólnie znane a dojrzałe środowisko zarządzania bezpieczeństwem uwzględni też raportowanie zdarzeń o mniejszych konsekwencjach. Pozwoli to na ustanowienie niezbędnych mechanizmów monitorowania, ukierunkowanych na wszystkie potencjalne wydarzenia o dużych konsekwencjach. Częstość występowania wydarzeń o mniejszych konsekwencjach jest nieuniknioną zapowiedzią zaistnienia wydarzeń o większych konsekwencjach.

2.10.4. Dalszych wskazówek na temat systemów dobrowolnego i obowiązkowego raportowania przez Państwo incydentów do ICAO dostarczają Dodatki 2 i 3 do Rozdziału 4. Dalszych wskazówek na temat dobrowolnych systemów SMS raportowania dostarcza Dodatek 5 do Rozdziału 5.

Badanie wypadków i incydentów

2.10.5. Gdy zdarzy się wypadek lub poważny incydent uruchamiany jest proces jego badania w celu znalezienia przyczyn nieskuteczności działań dotyczących zarządzania bezpieczeństwem oraz wygenerowania środków zaradczych zapobiegających powtórzeniu się uchybienia. Tak więc, w środowisku zarządzania bezpieczeństwem badanie wypadku ma odrębny cel, będąc niezbędnym procesem, który jest uruchamiany w sytuacji, gdy elementy obronne bezpieczeństwa, bariery, kontrole i czynniki równoważące w systemie zawiodły.

2.10.6. Będąc istotnym, reaktywnym komponentem elementów zawartych w ramach SMS i SSP, badania wypadków przyczyniają się do ciągłej poprawy funkcjonowania systemu lotniczego poprzez wykrywanie pierwotnych przyczyn wypadków/incydentów oraz dostarczanie doświadczeń. Mogą wspomagać decyzje dotyczące opracowywania działań korygujących i towarzyszącą im odpowiednią alokację zasobów oraz mogą rozpoznawać to jakie ulepszenia są lotnictwu potrzebne, w tym SMS, SSP a także państwowy proces badania wypadków. Powszechnie jest tak, że obowiązkowe badania (na poziomie Państwa) ograniczają się do wypadków i poważnych incydentów, podczas gdy dojrzałe środowisko zarządzania bezpieczeństwem może zająć się także badaniem zdarzeń o mniejszych konsekwencjach.

2.10.7. Oprócz ustalania faktów i odkrywania pierwotnych przyczyn wypadków/incydentów, większość badań skutkuje także wykrywaniem zagrożeń/niebezpieczeństw. Skuteczny i całościowy proces badania uwzględnia różnicę między ostatecznym rezultatem niebezpiecznego wydarzenia a zagrożeniem/niebezpieczeństwem, które przyczyniło się do wypadku/incydentu. Taki proces może, w ramach całego systemu lotnictwa, obejmować czynniki systemowe, uśpione lub organizacyjne. W obecnym środowisku proaktywnego zarządzania bezpieczeństwem, konieczne i ważne jest integrowanie procesu badania wypadku/incydentu z procesem raportowania/identyfikacji zagrożeń w przedsiębiorstwie. Formularze raportów z badania powinny zawierać wyraźne postanowienie o dokumentowaniu wykrytych w trakcie badania zagrożeniach/niebezpieczeństwach, które wymagałyby dalszego działania w ramach procesu identyfikacji i łagodzenia zagrożeń w przedsiębiorstwie. Powszechną praktyką jest, że raporty z badań ograniczają swoje „Wnioski" i „Działania podjęte/zalecane" tylko do przyczyn najbliższych lub bezpośrednich. A zatem, wszystkie drugorzędne lub pośrednie zagrożenia/niebezpieczeństwa mogą być przeoczone o ile nie uzupełni się tej luki poprzez połączenie procesów badania wypadków/incydentów i procesów identyfikacji zagrożeń.

2.11. ZBIERANIE I ANALIZA DANYCH DOTYCZĄCYCH BEZPIECZEŃSTWA

Zbieranie danych dotyczących bezpieczeństwa oraz ich jakość

2.11.1. Podejmowanie decyzji w oparciu o dane jest jednym z najważniejszych aspektów każdego systemu zarządzania. Dane, które mają być zbierane mogą obejmować wypadki i incydenty, wydarzenia, niezgodności lub odchylenia oraz raporty dotyczące zagrożeń. Jakość danych, które wykorzystuje się do skutecznego podejmowania decyzji, musi być brana pod uwagę w całym procesie opracowywania i wdrażania SSP i SSM. Niestety, wielu bazom danych brakuje jakości jaka jest potrzebna do dostarczenia wiarygodnej podstawy do oceny priorytetów bezpieczeństwa i skuteczności łagodzenia ryzyka. Nieuwzględnienie ograniczeń jakimi obarczone są dane użyte do wsparcia procesu zarządzania ryzykiem dotyczącym bezpieczeństwa i funkcji zapewnienia bezpieczeństwa doprowadzi do wadliwych wyników analizy, co może prowadzić do błędnych decyzji i zdyskredytowania procesu zarządzania bezpieczeństwem.

2.11.2. Z uwagi na to jak ważna jest jakość danych, organizacje muszą oceniać dane, które są używane pomocniczo w zarządzaniu ryzykiem dotyczącym bezpieczeństwa i w procesach zapewniania bezpieczeństwa, stosując następujące kryteria:

a) *Trafność danych*. Czy zebrane dane są akceptowalne zgodnie z kryteriami ustalonymi dla ich planowanego wykorzystania?;

b) *Kompletność*. Czy nie brakuje jakichś istotnych danych?;

c) *Powtarzalność*. Czy zakres pomiaru danego parametru jest spójny, czy może zostać powtórzony i czy nie zawiera błędu?;

d) *Dostępność*. Czy dane są łatwo dostępne do analizowania?;

e) *Aktualność.* Czy dane odnoszą się do okresu pozostającego w sferze zainteresowania i czy są szybko dostępne?;

f) *Bezpieczeństwo*. Czy dane są chronione przed nieumyślną lub modyfikacją dokonaną w złej wierze?;

g) *Dokładność.* Czy dane są wolne od błędów?

Przez uwzględnienie tych siedmiu kryteriów dotyczących jakości danych, analizy danych dotyczących bezpieczeństwa wygenerują informacje możliwie najbardziej dokładne, do wykorzystania na wsparcie podejmowania decyzji strategicznych

Baza danych o bezpieczeństwie

2.11.3. W kontekście zbierania i analizy danych dotyczących bezpieczeństwa, określenie baza danych o bezpieczeństwie może obejmować następujące rodzaje danych lub informacji, które można wykorzystać na wsparcie analizy danych o bezpieczeństwie :

a) dane z badania wypadków;

b) dane z obowiązkowych badań incydentów;

c) dane z raportów dobrowolnych;

d) dane z ciągłego raportowania zdatności do lotu;

e) dane z monitorowania wyników operacyjnych;

f) dane z oceny ryzyka dotyczącego bezpieczeństwa;

g) dane z ustaleń audytów/raportów;

h) dane z badań nad bezpieczeństwem/z przeglądów bezpieczeństwa;

i) dane dotyczące bezpieczeństwa z innych Państw, regionalnych organizacji nadzorujących bezpieczeństwo (RSOO) lub z regionalnych organizacji do spraw badania wypadków i incydentów (EAIO) itp.

2.11.4. Termin *baza danych o bezpieczeństwie* może się odnosić do krajowych baz(y) danych związanych z SSP Państwa lub może się odnosić do baz(y) związanych z wewnętrznymi SMS-ami dostawcy usług, w zależności od kontekstu. Dobrowolne raporty mogą pochodzić od personelu operacyjnego (dostawców usług, pilotów itd.), ale także od pasażerów lub ogółu społeczeństwa.

2.11.5. Duża część danych w bazach bezpieczeństwa ma formę raportów związanych ze skomplikowanymi zdarzeniami, takimi jak wypadki i incydenty. Raporty w bazach danych tego typu udzielają, z reguły, odpowiedzi na serię pytań: Kto uczestniczył w zdarzeniu? Co się takiego zdarzyło, że spowodowało napisanie raportu? Kiedy zdarzenie miało miejsce? Gdzie zdarzenie miało miejsce? Dlaczego coś się wydarzyło? Inne rodzaje baz danych odnoszą się do relatywnie wąskich tematów, takich jak informacje o lotach, pogodzie i natężeniu ruchu. Te raporty zawierają proste fakty.

2.11.6. Bazy danych dotyczące bezpieczeństwa przechowuje się, z reguły, w różnych komórkach organizacyjnych danej organizacji. Wiele organizacji zapewnia dostęp do baz danych poprzez interfejs umożliwiający analitykom bezpieczeństwa skuteczne wyszukiwanie raportów, które ich interesują. Raporty mogą być przeglądane osobno lub łącznie. Narzędzia analityczne umożliwiają analitykom bezpieczeństwa na przeglądanie danych ściągniętych w różnych formatach. Przykłady: arkusze kalkulacyjne, mapy i rozmaite typy wykresów.

2.11.7. Dla zapewnienia zrozumiałości bazy danych i poprawności jej używania, informacje odnoszące się do samej bazy (metadane) muszą być dobrze udokumentowane i dostępne dla użytkowników. Rodzaje metadanych obejmują definicje dziedziny, zmiany dokonane w bazie na przestrzeni czasu, reguły użytkowania, formularz z zebrania danych i odnośniki do prawidłowych wartości.

2.11.8. Ogromna liczba baz danych dotyczących bezpieczeństwa została stworzona niezależnie przez wiele różnych organizacji mających specyficzne obszary odpowiedzialności i potrzeby analityczne. Aby dostarczyć analitykom zajmującym się bezpieczeństwem w lotnictwie szerszej perspektywy na zagadnienia bezpieczeństwa, należy zbudować programy wspomagające integrację informacji dotyczących bezpieczeństwa, które będą potrafiły pobierać informacje z mnogości źródeł, stosować powszechne dla baz standardy, łączyć metadane oraz ładować je na wspólną platformę usytuowaną w architekturze scentralizowanego przechowywania danych.

2.11.9. Po obróbce, dane dotyczące bezpieczeństwa udostępniane są analitykom poprzez wspólny interfejs i wspólny zestaw narzędzi analitycznych. Gdy analityk potrzebuje danych z różnorodnych baz, obsługa techniczna może je pozyskać z właściwych baz poprzez aplikację wspólnych standardów dla danych i skonstruować zupełnie nową bazę danych. Schematyczny wygląd krajowego systemu danych dotyczących bezpieczeństwa jest pokazany na Rys. 2-8, który pokazuje wejścia, procesy i wyjścia związane ze zbieraniem danych o bezpieczeństwie, analizą i wymianą.

Dane wprowadzane (Gromadzenie)	• raporty z wypadków i incydentów; • systemy dobrowolnego raportowania zdarzeń; • obowiązkowe systemy raportowania zdarzeń; • systemy zbierania danych operacyjnych (dostarczanych bezpośrednio przez dostawców usług); • systemy zbierania danych z nadzoru nad bezpieczeństwem.
Procesy (Analiza)	• narzędzia zbierania danych i systemy zarządzania danymi do zbierania i przechowywania danych pochodzących z: o systemów raportowania wypadków i incydentów; o systemów zbierania danych operacyjnych; o systemów zbierania danych z nadzoru nad bezpieczeństwem; o zaleceń z badań wypadków i poważnych incydentów; • metody analityczne do oceny znanego i nowego ryzyka wynikającego z wszelkich dostępnych danych; • wskaźniki poziomu bezpieczeństwa, poziomy docelowe i ostrzegawcze (poziom indywidualny lub połączony) do mierzenia stanu bezpieczeństwa i wykrywania niepożądanych trendów; • opracowywanie procesów nadzorowania opartych o ryzyko, łącznie z ustalaniem priorytetów inspekcji i audytów;

Dane wychodzące (Wymiana)	• zalecenia dotyczące bezpieczeństwa, wydawane przez • odpowiednie władze krajowe na podstawie analizy wszystkich danych wejściowych systemu bezpieczeństwa; • raporty dotyczące wskaźników bezpieczeństwa, celów i poziomów alarmowych (poziom państwa i dostawcy usług), wygenerowane poprzez analizy danych wejściowych, w tym: o analizy porównawcze (jako kryterium odniesienia); o analizy trendów historycznych; o korelacja; pomiędzy wskaźnikami proaktywnymi i wynikami bezpieczeństwa (wypadki i poważne incydenty); • przeglądy krajowych przepisów i procesów nadzoru, w tym ustalania priorytetów działań nadzorczych, według obszarów największego ryzyka; • działania administracyjne wymagane dla celów bezpieczeństwa; • wymiana informacji dotyczących bezpieczeństwa pomiędzy państwowymi organami regulacyjnymi i władzami prowadzącymi badania wypadków; • wymiana informacji dotyczących zagadnień bezpieczeństwa pomiędzy dostawcami usług, organami regulacyjnymi oraz organizacjami prowadzącymi badania wypadków, na poziomach krajowym, regionalnym i międzynarodowym.

Rys. 2-8 Schemat krajowego systemu danych dotyczących bezpieczeństwa

Analiza danych dotyczących bezpieczeństwa

2.11.10. Po zgromadzeniu z różnych źródeł danych o bezpieczeństwie, organizacje powinny dokonać analizy w celu zidentyfikowania zagrożeń i kontrolowania ich potencjalnych konsekwencji. Poza tym, analiza może być wykorzystana:

a) jako pomoc przy decydowaniu jakie dodatkowe fakty są potrzebne;

b) do ustalenia czy istnieją jakieś uśpione czynniki, leżące u podstaw niedostatków w sferze bezpieczeństwie;

c) jako pomoc w wyciąganiu przekonywujących wniosków;

d) do monitorowania i pomiaru trendów bezpieczeństwa lub ich poziomu.

2.11.11. Analiza bezpieczeństwa jest często powtarzalna i wymaga wielu cykli. Może być jakościowa lub ilościowa. Brak bazowych danych ilościowych może wymusić poleganie w większym stopniu na metodach analizy jakościowej.

2.11.12. Ocena ludzka może podlegać uprzedzeniom wynikającym z doświadczeń, co może mieć wpływ na interpretację wyników analizy lub weryfikację hipotez. Jedną z najczęstszych form błędu oceny jest skłonność do popełniania błędu konfirmacji *(confirmation bias).* Jest to tendencja poszukania i przyjmowania informacji, które potwierdzają to, co oceniający uważa za prawdziwe.

Metody i narzędzia analityczne

2.11.13. Można stosować poniższe metody analizy bezpieczeństwa:

a) *Analiza statystyczna*. Metody tej można użyć do oceny znaczenia dostrzeganych trendów w bezpieczeństwie, często ilustrowanych w graficznych prezentacjach wyników analizy. O ile analiza statystyczna może dostarczyć solidnej dawki informacji o tym jak znaczne są niektóre trendy to, aby uniknąć błędnych wniosków, należy starannie rozważyć poziom jakości danych i metod analitycznych.

b) *Analiza trendów.* Poprzez monitorowanie trendów w danych o bezpieczeństwie, można snuć przewidywania co do wydarzeń w przyszłości. Trendy mogą wskazywać na zagrożenia dopiero powstające.

c) *Porównania normatywne*. Dostępność danych może nie być wystarczająca by zapewnić faktograficzną podstawę do porównania okoliczności potencjalnych zdarzeń. W takich przypadkach, konieczne może być próbkowanie realiów w warunkach zbliżonych.

d) *Symulacje i testy*. W niektórych przypadkach, zagrożenia mogą się ujawnić podczas symulacji, jak również w testowaniu laboratoryjnym – przeprowadzanych dla uzasadnienia sugestii iż istnieją nowe typy operacji, sprzętu lub procedur.

e) *Panele ekspertów*. Opinie współpracowników i specjalistów mogą być użyteczne w ocenianiu zróżnicowanego charakteru zagrożeń kojarzonych z konkretną niebezpieczną okolicznością. Multidyscyplinarny zespół, powołany do oceny dowodów istnienia niebezpiecznej okoliczności, może pomóc ustalić najlepszy kierunek działań naprawczych.

f) *Analiza kosztów i zysków*. Zaakceptowanie zalecanych środków kontroli ryzyka dotyczącego bezpieczeństwa może zależeć od wiarygodności analizy kosztów i zysków. Koszt wdrożenia proponowanych środków trzeba wyważyć względem przyszłych korzyści. Analiza kosztów i zysków może sugerować, że da się tolerować konsekwencje ryzyka dotyczącego bezpieczeństwa, jeśli się weźmie pod uwagę czas, wysiłek i niezbędny koszt wdrożenia działania naprawczego.

Zarządzanie informacjami o bezpieczeństwie

2.11.14. Siłą napędową skutecznego zarządzania bezpieczeństwem są dane. Właściwe zarządzanie bazami danych organizacji jest fundamentalne dla zapewnienia skutecznej i niezawodnej analizy skonsolidowanych źródeł danych.

2.11.15. Zbudowanie i utrzymanie bazy danych dotyczących bezpieczeństwa dostarcza niezbędnego narzędzia personelowi monitorującemu zagadnienia bezpieczeństwa systemu. Na rynku dostępny jest szeroki asortyment stosunkowo niedrogich elektronicznych baz danych, które są w stanie spełnić wymagania dotyczące zarządzania danymi w organizacji.

2.11.16. W zależności od wielkości i złożoności organizacji, wymagania systemu mogą obejmować szereg umiejętności, niezbędnych dla skutecznego zarządzania danymi dotyczącymi bezpieczeństwa. Ogólnie, system powinien:

a) posiadać przyjazny dla użytkownika interfejs do wprowadzania danych i zapytań;

b) posiadać zdolność przetwarzania dużych ilości danych dotyczących bezpieczeństwa w użyteczne informacje, pomocne w podejmowaniu decyzji;

c) zredukować obciążenie pracą kierowników i personel zajmujący się bezpieczeństwem;

d) działać po relatywnie niskim koszcie.

2.11.17. Aby wykorzystać potencjalne możliwości baz danych, wymagane jest podstawowe rozumienie ich działania. O ile informacja, która została zgrupowana w sposób zorganizowany, może zostać uznana za bazę danych, o tyle analiza zapisów na papierze - przechowywanych w ramach prostego katalogu - wystarczy tylko do operacji prostych. Przechowywanie, rejestrowanie, zaglądanie do papierowych informacji i ich wyszukiwanie w systemach papierowych - to niewygodne zadanie. Dane dotyczące bezpieczeństwa powinny być raczej przechowywane w bazach elektronicznych, bo te umożliwiają zapytania o zapisy i generują analizy wyjściowe w asortymencie formatów.

2.11.18. Właściwości funkcjonalne i atrybuty różnych systemów zarządzania bazami danych różnią się pomiędzy sobą i należy je rozpatrywać pojedynczo przed podjęciem decyzji, która baza będzie najbardziej przydatna. Podstawowe funkcje powinny umożliwić użytkownikowi realizację zadań takich jak:

a) zapisywanie zdarzeń dotyczących bezpieczeństwa w różnych kategoriach;

b) linkowanie zdarzeń z właściwymi dokumentami (np. raportami lub fotografiami);

c) monitorowanie trendów;

d) zestawianie analiz, wykresów i raportów;

e) sprawdzanie zapisów historycznych;

f) dzielenie się danymi z innymi organizacjami;

g) monitorowanie procesu badania wypadków; oraz

h) monitorowanie wdrażania działań naprawczych.

Zabezpieczanie danych o bezpieczeństwie

2.11.19. Zakładając możliwość niewłaściwego użycia danych dotyczących bezpieczeństwa, które zostały skompilowane wyłącznie na rzecz postępu w bezpieczeństwie lotniczym, zarządzanie bazą danych musi obejmować także zabezpieczenie takich danych. Zarządzający bazą danych muszą równoważyć potrzebę ochrony danych z potrzebą jej udostępniania tym, którzy mogą zwiększyć bezpieczeństwo lotnicze. Zabezpieczanie obejmuje:

a) adekwatność przepisów dotyczących dostępu do informacji w stosunku do wymagań zarządzania bezpieczeństwem;

b) działania koncepcyjne i procedury organizacji w zakresie ochrony danych dotyczących bezpieczeństwa, które powinny umożliwiać dostęp do nich tylko osobom które „potrzebują wiedzieć”;

c) uniemożliwienie identyfikacji poprzez usunięcie wszystkich szczegółów, które mogą umożliwić stronie trzeciej odkrycie tożsamości osób (na przykład numery rejsów, daty/godziny, miejscowości i typy statków powietrznych);

d) bezpieczeństwo systemów informatycznych, przechowywania danych i sieci łączności;

e) zakaz nieuprawnionego użycia danych.

Dalsze informacje na temat ochrony danych dotyczących bezpieczeństwa znajdują się w Dodatku 5 do Rozdziału 4.

2.12. WSKAŹNIKI BEZPIECZEŃSTWA I MONITOROWANIE DZIAŁANIA

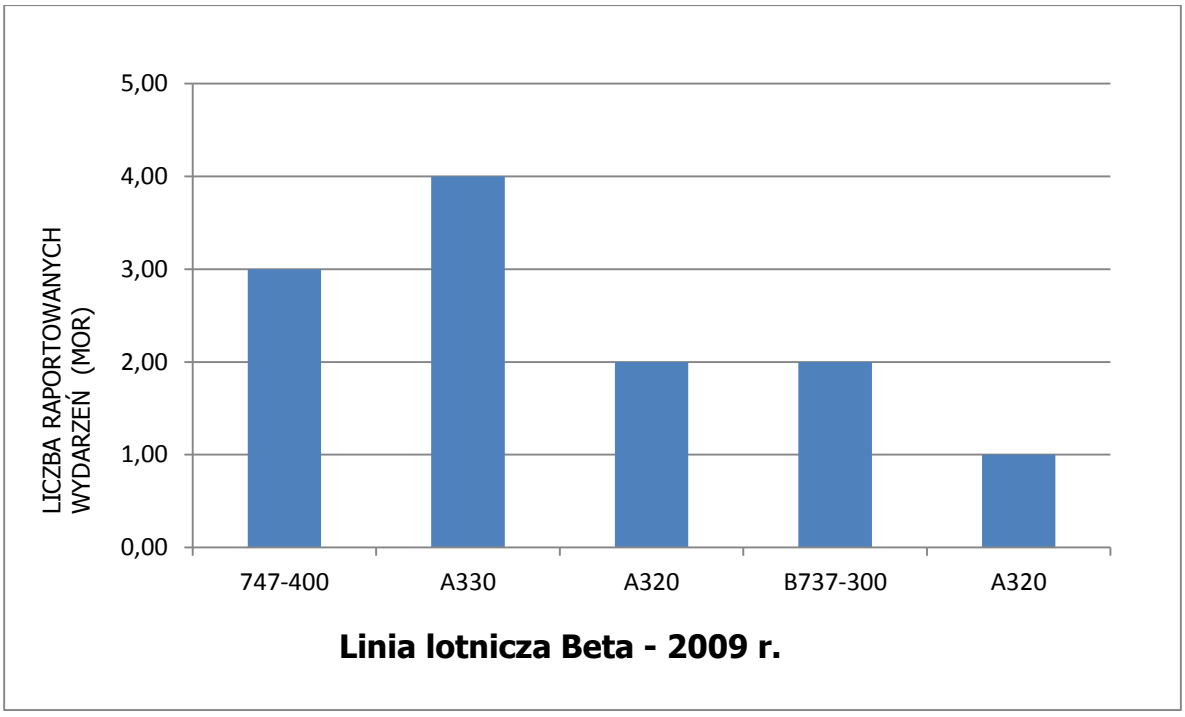
2.12.1. Dane wychodzące z systemu zbierania i analizy danych dotyczących bezpieczeństwa są zwykle przedstawiane w postaci tablic i wykresów. Typowo, takie tablice i wykresy, zazwyczaj wykorzystywane w konwencjonalnych systemach zarządzania typu jakość/niezawodność, pokazują zaledwie "migawkę" analizy danych z jednorazowego zapytania.

2.12.2. Rysunek 2-9 jest tablicą (skopiowanym ekranem) podstawowej analizy danych; pokazuje podlegającą obowiązkowemu raportowaniu (MOR) ostateczną liczbę incydentów u operatora w roku 2009, w rozbiciu na typ samolotów. Ta podstawowa tablica nie pokazuje liczby samolotów danego typu ani liczby wykonanych przez nie lotów. Dlatego, korzyść z tablic tego typu jest ograniczona. Taka tablica nie byłaby wystarczająca dla ciągłego wskazywania poziomu bezpieczeństwa.

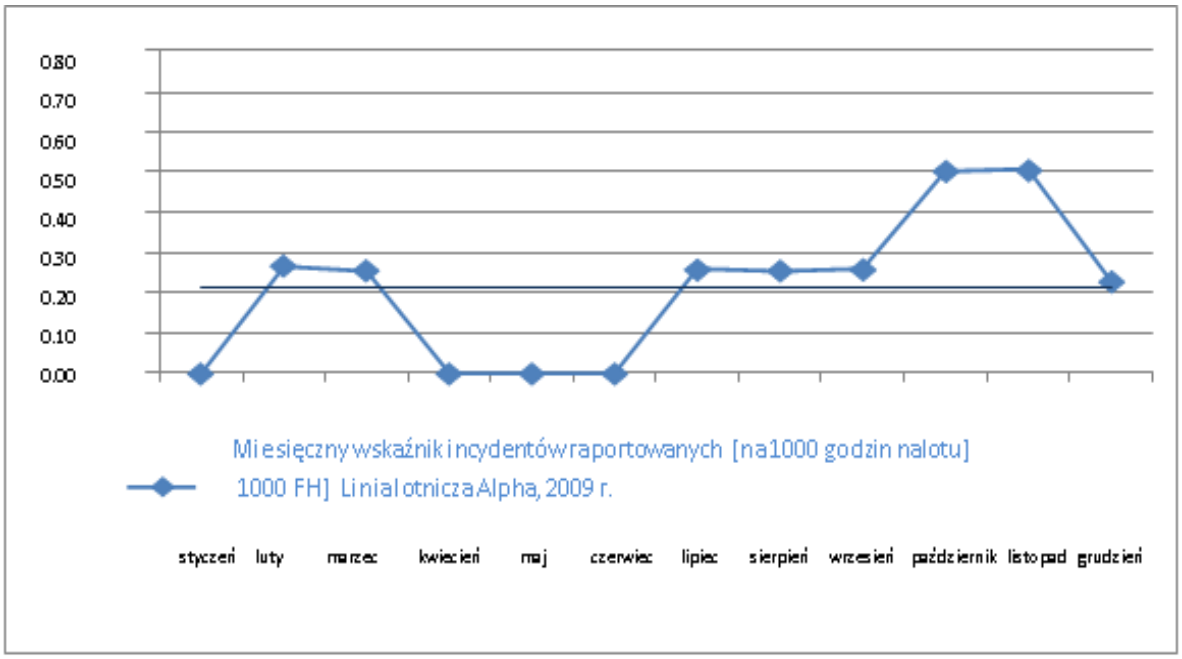
2.12.3. Analiza, wykorzystywana do ciągłego monitorowania bezpieczeństwa, miałaby postać danych okresowo wyodrębnionych w celu wygenerowania tablicy lub wykresu trendu aktualizowanego miesięcznie lub kwartalnie. Jego ilustracja jest pokazana na Rys. 2-10. Ta tablica danych podaje informacje o stopniu incydentalności, raportowanym comiesięcznie, dla całkowitej liczby godzin lotu (FH) floty danego operatora. Okresowe (miesięczne) uzupełnianie danych dotyczących stopnia incydentalności pozwoli wówczas wykorzystywać tablicę jako wskaźnik ciągłego monitorowania trendu. Gdy już taki ciągły wskaźnik monitorowania trendu znajdzie się na swym miejscu, następnym krokiem będzie przekształcenie go we wskaźnik pomiaru osiągów bezpieczeństwa, przez ustanowienie na tablicy poziomu docelowego i alarmowego. Te punkty danych historycznych (osiągi wcześniejsze) będą podstawą dla ustalenia lub zdefiniowania niedopuszczalnych poziomów alarmowych w trendach, jak również pożądanego docelowego poziomu poprawy jaki należy osiągnąć w konkretnym okresie. Dalszymi szczegółami na temat opracowywania wskaźników osiągów bezpieczeństwa i związanych z nimi ustawień celu i poziomu alarmowego znajdują się w Rozdziałach 4 (SSP) i 5 (SMS).

2.13. ZAGROŻENIA

2.13.1. Identyfikacja zagrożeń jest warunkiem wstępnym procesu zarządzania ryzykiem dotyczącym bezpieczeństwa. Każde błędne rozróżnienie pomiędzy zagrożeniem i ryzykiem dotyczącymi bezpieczeństwa może być źródłem chaosu. Wyraźne zrozumienie zagrożeń i związanych z nimi konsekwencji jest niezbędne dla wdrożenia właściwego zarządzania ryzykiem dotyczącym bezpieczeństwa.



Rys. 2-9. Prosty wykres (zrzut ekranu) analizy danych



Rys. 2-10. Wykres wskaźnika bezpieczeństwa ciągłego monitorowania

Zrozumienie zagrożeń i konsekwencji

2.13.2. Zagrożenie jest ogólnie zdefiniowane przez praktyków jako stan lub przedmiot posiadający możliwość spowodowania śmierci i obrażeń ludzi, uszkodzeń sprzętu lub konstrukcji, straty materialnej lub zmniejszenia zdolności do realizacji wyznaczonych zadań. Dla potrzeb zarządzania ryzykiem dotyczącym bezpieczeństwa w lotnictwie, pod pojęciem zagrożenie, należy skupiać te okoliczności, które mogą powodować lub przyczynić się do niebezpiecznej pod względem bezpieczeństwa eksploatacji samolotów, lotniczego sprzętu, produktu i usług. (Wskazówki na temat odróżniania zagrożeń bezpośrednio związanych z bezpieczeństwem lotniczym od innych ogólnych/przemysłowych zagrożeń znajdują się pod 2.13.12 oraz 2.13.13).

2.13.3. Rozważmy przykładowo wiatr o prędkości piętnastu węzłów, co nie jest koniecznie stanem zagrożenia. W istocie wiatr o prędkości piętnastu węzłów wiejący wzdłuż osi drogi startowej przyczynia się do polepszenia osiągów statku powietrznego podczas startu i lądowania. Jednakże wiatr o prędkości piętnastu węzłów wiejący pod kątem dziewięćdziesięciu stopni w stosunku do osi drogi startowej, na której ma się odbyć start lub lądowanie stwarza warunki wiatru bocznego, które mogą być zagrożeniem ze względu na możliwość przyczynienia się do zdarzenia w postaci bocznego wypadnięcia z drogi startowej.

2.13.4. Zagrożenia są nieodłączną częścią działalności lotniczej. Jednakże ich pojawieniu się i możliwym konsekwencjom można starać się zaradzić poprzez stosowanie rozmaitych strategii łagodzących, które zapanują nad potencjałem zagrożenia, które skutkowałoby niebezpieczeństwem dla działań statku powietrznego lub funkcjonowania sprzętu lotniczego.

2.13.5. Istnieje powszechna tendencja do mylenia zagrożeń z ich konsekwencjami lub skutkami. Konsekwencja to skutek, który mógł być wywołany przez zagrożenie. Na przykład, wypadnięcie poza koniec pasa drogi startowej, jest konsekwencją związaną z zagrożeniem w postaci zanieczyszczonego pasa. Poprzez wcześniejsze jasne zdefiniowanie zagrożenia można przewidywać określone konsekwencje lub skutki. Można zauważyć, że konsekwencje mogą być wielowarstwowe, takie jak pośrednie zdarzenie niebezpieczne, które poprzedzi ostateczną konsekwencję (wypadek). Więcej informacji w Dodatku 2, Tabela 2-A2-3.

2.13.6. W powyższym przykładzie z wiatrem bocznym, natychmiastowym skutkiem zagrożenia może być utrata sterowania poprzecznego, poprzedzająca wypadnięcie z drogi startowej. Ostateczną konsekwencją może być wypadek. Niszczący potencjał zagrożenia materializuje się w jednej lub wielu konsekwencjach. Dlatego też w ocenie bezpieczeństwa ważne jest, aby zawierała ona kompleksowe zestawienie wszystkich możliwych konsekwencji, które będą opisane dokładnie i w sposób praktyczny. Należy odróżnić najwyższą konsekwencję w postaci utraty życia, od innych, posiadających mniejszy potencjał, takich jak zwiększenie obciążenia pracą załogi lotniczej, dyskomfort pasażerów czy zmniejszenie marginesów bezpieczeństwa. Opis konsekwencji zgodnie z ich prawdopodobnymi skutkami ułatwi opracowanie i wdrożenie efektywnych strategii minimalizujących poprzez ustalenie priorytetów i przydział ograniczonych zasobów. Trafna identyfikacja zagrożeń prowadzi do odpowiedniej oceny ewentualnych skutków.

2.13.7. Zagrożenia należy odróżniać od błędów, zwykłego i nieuniknionego komponentu ludzkich działań, z którymi trzeba sobie radzić.

Identyfikacja zagrożenia i ustalanie priorytetów

2.13.8. Zagrożenia w przedsiębiorstwie istnieją na wszystkich poziomach i można je wykryć poprzez korzystanie z systemów raportowania, inspekcji czy audytów. Niefortunne przypadki mogą mieć miejsce gdy zagrożenie zbiegnie się z pewnymi czynnikami aktywującymi. W związku z tym, zagrożenia należy identyfikować zanim doprowadzą do wypadków, incydentów lub innych zdarzeń związanych z bezpieczeństwem. Ważnym mechanizmem proaktywnego identyfikowania zagrożeń jest system dobrowolnego zgłaszania zagrożeń/incydentów. Dalsze wskazówki na temat systemów dobrowolnego zgłaszania znajdują się w Dodatku 2 do Rozdziału 4, i w Dodatku 5 do Rozdziału 5. Informacje zebrane poprzez wymienione systemy zgłaszania mogą zostać uzupełnione obserwacjami lub ustaleniami zarejestrowanymi podczas rutynowych inspekcji obiektów lub audytów organizacji.

2.13.9. Zagrożenia mogą także być identyfikowane lub wyodrębniane z przeglądów raportów dotyczących badań powypadkowych. Uwzględniając przede wszystkim te, które są uznawane za pośrednie czynniki sprzyjające i które mogłyby nie być objęte właściwymi działaniami naprawczymi wynikającymi z procesu powypadkowego badania. Dlatego też, systematyczna procedura przeglądania raportów z badania wypadków/incydentów pod względem istniejących zagrożeń jest dobrym mechanizmem wzbogacenia systemu identyfikacji zagrożeń w organizacji. Jest to szczególnie istotne w organizacjach, w których kultura bezpieczeństwa nie jest jeszcze na tyle dojrzała, by utrzymać skuteczny system dobrowolnego zgłaszania zagrożeń.

2.13.10. Zagrożenia można dzielić ze względu na ich źródła lub lokalizację. Obiektywne ustalanie priorytetów zagrożeń może wymagać ich kategoryzacji pod względem dotkliwości/prawdopodobieństwa spodziewanych konsekwencji, co ułatwi ustalanie priorytetów strategii łagodzenia ryzyka tak by ograniczone zasoby były wykorzystane w sposób najbardziej efektywny. Przykład procedury ustalania priorytetów zagrożeń znajduje się w Dodatku 3 do niniejszego Rozdziału.

Metodologie identyfikacji zagrożeń

2.13.11. Trzy metodologie identyfikacji zagrożeń:

a) *Reaktywna (Reactive).* Ta metodologia obejmuje analizę przeszłych zdarzeń lub ich skutków. Zagrożenia są identyfikowane poprzez badanie zdarzeń dotyczących bezpieczeństwa. Incydenty i wypadki są czytelnymi wskazaniami niedostatków w systemie i dlatego mogą być użyte do określenia zagrożeń zarówno tych, które przyczyniły się do zdarzenia, jak i tych pozostających w uśpieniu;

b) *Proaktywna (Proactive).* Ta metodologia obejmuje analizę sytuacji aktualnych, która jest zadaniem pierwszorzędnym funkcji zapewniania bezpieczeństwa, wraz z jej audytami, ocenami, raportami pracowników oraz związanymi z tym analizami i procesami oceniania. Obejmuje ona aktywne poszukiwanie zagrożeń w ramach istniejących procesów;

c) *Przewidywalna (Predictive).* Ta metodologia obejmuje zbieranie danych w celu identyfikacji możliwych negatywnych skutków lub zdarzeń w przyszłości oraz analizowanie procesów i środowiska dla identyfikowania potencjalnych przyszłych zagrożeń i inicjowanie działań łagodzących.

Rozróżnianie między zagrożeniami dla lotnictwa a zagrożeniami dla pracowników, zdrowia i środowiska (polskie BHP)

2.13.12. Ustalenie tego czy zagrożenie odnosi się do lotnictwa czy BHP będzie zależało od jego potencjalnych lub przewidywalnych konsekwencji lub ryzyka. Każde zagrożenie, które może mieć wpływ (bezpośredni czy pośredni) na bezpieczeństwo operacyjne statku powietrznego lub bezpieczeństwo lotniczego sprzętu, produktu lub usługi związanej z bezpieczeństwem lotniczym powinno być uznane za mające związek z lotniczym SMS. Zagrożeniem skutkującym wyłącznie konsekwencjami dla BHP (tj. bez jakiegokolwiek wpływu na bezpieczeństwo lotnicze) należy się zająć oddzielnie w ramach systemu/procedury BHP, zgodnie z odnośnymi wymaganiami własnymi organizacji lub krajowymi. Zagrożenia dla BHP i ich konsekwencje, które nie mają wpływu na bezpieczeństwo lotnictwa nie są przedmiotem lotniczych SMS.

2.13.13. Ryzykiem dotyczącym bezpieczeństwa związanym ze złożonymi zagrożeniami, które jednocześnie mają wpływ na bezpieczeństwo lotnicze i BHP można zarządzać poprzez oddzielne (równoległe) procesy minimalizacji ryzyka po to, aby oddzielnie przeciwdziałać konsekwencjom dla lotnictwa i BHP. Alternatywnie, w przypadkach zagrożeń złożonych można stosować zintegrowany system minimalizacji ryzyka lotniczego i BHP. Przykładem zagrożenia złożonego jest „uderzenie pioruna w statek powietrzny" (w terminalu tranzytowym lotniska). Zagrożenie to może być uznane przez inspektora BHP za „zagrożenie w miejscu pracy" (personel naziemny/bezpieczeństwo miejsca pracy). Dla inspektora lotniczego SMS jest to jednocześnie zagrożenie lotnicze związane z ryzykiem uszkodzenia statku powietrznego i narażenia bezpieczeństwa pasażerów. Ponieważ konsekwencje takich złożonych zagrożeń dla BHP i dla bezpieczeństwa lotniczego nie są takie same, z należną uwagą powinny zostać poddane oddzielnie analizie. Cele i główny kierunek działań prewencyjnych w przypadku BHP i bezpieczeństwa lotniczego byłyby różne.

2.14. RYZYKO DOTYCZĄCE BEZPIECZEŃSTWA

2.14.1. Zarządzanie ryzykiem dotyczącym bezpieczeństwa jest kolejnym kluczowym składnikiem systemu zarządzania bezpieczeństwem. Użycie terminu zarządzanie ryzykiem dotyczącym bezpieczeństwa ma odróżnić tę funkcję od zarządzania

ryzykiem finansowym, prawnym, ekonomicznym i temu podobnymi. Niniejszy paragraf przedstawia podstawy zarządzania ryzykiem dotyczącym bezpieczeństwa i obejmuje następujące zagadnienia:

a) definicję ryzyka dotyczącego bezpieczeństwa;

b) prawdopodobieństwo ryzyka dotyczącego bezpieczeństwa;

c) dotkliwość ryzyka dotyczącego bezpieczeństwa;

d) możliwość tolerowania ryzyka dotyczącego bezpieczeństwa; oraz

e) zarządzanie ryzykiem dotyczącym bezpieczeństwa.

Definicja ryzyka dotyczącego bezpieczeństwa

2.14.2. Ryzyko dotyczące bezpieczeństwa to przewidywane prawdopodobieństwo i dotkliwość konsekwencji lub skutków istniejącego zagrożenia lub sytuacji. O ile skutkiem może być wypadek, to pośrednie konsekwencje wydarzenia/zdarzenia *(intermediate unsafe event/consequence)* może być określone jako „najbardziej wiarygodny skutek". Dostarczenie takich wielopoziomowych konsekwencji do identyfikacji wiąże się z reguły z posiadaniem bardziej skomplikowanego oprogramowania dla łagodzenia ryzyka. Przykład arkusza kalkulacyjnego łagodzenia ryzyka w Dodatku 2 do niniejszego rozdziału także spełnia to wymaganie.

Prawdopodobieństwo ryzyka dotyczącego bezpieczeństwa

2.14.3. Proces kontrolowania ryzyka dotyczącego bezpieczeństwa rozpoczyna się od oceny prawdopodobieństwa, że konsekwencje zagrożeń zmaterializują się podczas wykonywanych przez firmę działań lotniczych. Prawdopodobieństwo ryzyka dotyczącego bezpieczeństwa jest definiowane jako prawdopodobieństwo lub częstotliwość wystąpienia konsekwencji lub skutku dla bezpieczeństwa. Przy określaniu prawdopodobieństwa mogą być pomocne następujące pytania:

a) Czy w przeszłości wystąpiły zdarzenia podobne do rozważanego, czy też jest to przypadek odosobniony?

b) Jaki inny sprzęt lub części tego samego typu mogą mieć podobne defekty?

c) Ile osób przestrzega omawiane procedury lub jest do tego zobowiązana?

d) Przez jaki procent czasu jest w użyciu podejrzany sprzęt lub wątpliwa procedura?

e) W jakim stopniu implikacje organizacyjne, zarządcze lub regulacyjne mogą przenosić się na większe zagrożenia dla bezpieczeństwa publicznego?

2.14.4. Wszelkie czynniki, leżące u podstawy takich pytań, pomogą w ocenie prawdopodobieństwa zaistnienia zagrożenia, wziąwszy pod uwagę wszelkie potencjalnie możliwe scenariusze. Określenie prawdopodobieństwa może być wykorzystane jako pomoc przy określeniu prawdopodobieństwa ryzyka dotyczącego bezpieczeństwa.

2.14.5. Na Rys. 2-11 pokazano typową tabelę prawdopodobieństwa ryzyka dotyczącego bezpieczeństwa, w tym przypadku pięciopunktową. Tabela obejmuje pięć kategorii określających prawdopodobieństwo odnoszące się do niebezpiecznego wydarzenia lub okoliczności, opis każdej kategorii i przypisane do każdej kategorii wartości liczbowe.

2.14.6. Należy podkreślić, że jest to tylko przykład i że w celu osiągnięcia efektu współmiernego z konkretnymi potrzebami i stopniem skomplikowania różnych organizacji należy odpowiednio zaadaptować poziom szczegółowości i złożoności tabel i matryc. Należy także zauważyć, że organizacje mogą zamieścić zarówno kryteria jakościowe, jak i ilościowe, aż do piętnastu wartości.

Prawdopodobieństwo	*Znaczenie*	*Wartość liczbowa*
Częste	Prawdopodobnie wystąpi wiele razy (występowało często)	5
Sporadyczne	Prawdopodobnie wystąpi od czasu do czasu (występowało niezbyt często)	4
Dalekie	Prawdopodobnie nie wystąpi, ale jest to możliwe (występowało rzadko)	3
Nieprawdopodobne	Bardzo mało prawdopodobne, że wystąpi (przypadek wystąpienia nie jest znany)	2
Skrajnie nieprawdopodobne	Prawie niewyobrażalne, że kiedykolwiek może wystąpić	1

Rys. 2-11. Tabela prawdopodobieństwa ryzyka dotyczącego bezpieczeństwa

Dotkliwość ryzyka dotyczącego bezpieczeństwa

2.14.7. Po dokonaniu oceny prawdopodobieństwa wystąpienia ryzyka, w następnej kolejności ocenia się dotkliwość ryzyka, biorąc pod uwagę potencjalne konsekwencje związane z zagrożeniem. Dotkliwość ryzyka dotyczącego bezpieczeństwa definiuje się jako rozległość szkody jakiej można się normalnie spodziewać jako konsekwencji lub skutku zidentyfikowanego zagrożenia. Ocena dotkliwości może opierać się na:

a) *Ofiarach śmiertelnych/obrażeniach*: Ile może być ofiar śmiertelnych (pracowników, pasażerów, osób postronnych)?

b) *Szkodach:* jaki jest prawdopodobny stopień uszkodzeń statku powietrznego, sprzętu lub mienia?

2.14.8. Ocena dotkliwości powinna uwzględniać wszystkie możliwe konsekwencje związane z niebezpieczną okolicznością lub przedmiotem, zakładając najgorszy przewidywalny scenariusz. Rys. 2-12 przedstawia typową tabelę dotkliwości ryzyka dotyczącego bezpieczeństwa. Obejmuje ona pięć kategorii opisujących poziom dotkliwości, opis każdej kategorii i wartości liczbowe przypisane do każdej kategorii. Podobnie jak w przypadku tabeli prawdopodobieństwa ryzyka dotyczącego bezpieczeństwa, niniejsza tabela służy wyłącznie jako przykład:

Tolerancja ryzyka dotyczącego bezpieczeństwa

2.14.9. Proces oceniania prawdopodobieństwa i dotkliwości ryzyka dotyczącego bezpieczeństwa można wykorzystać do wyprowadzenia wskaźnika takiego ryzyka. Wskaźnik, utworzony według powyżej opisanej metodologii, składa się z alfanumerycznego oznacznika pokazującego połączone, szacunkowe wyniki prawdopodobieństwa i dotkliwości. Odpowiednie kombinacje dotkliwości/prawdopodobieństwa są przedstawione w matrycy oceny ryzyka dotyczącego bezpieczeństwa na Rys. 2-13.

2.14.10. Trzecim krokiem w tym procesie jest określenie tolerancji ryzyka. Po pierwsze, konieczne jest by w matrycy uzyskać oznaczniki oceny ryzyka dotyczącego bezpieczeństwa. Na przykład rozważmy sytuację, gdzie prawdopodobieństwo ryzyka dotyczącego bezpieczeństwa zostało ocenione jako sporadyczne (4), a dotkliwość ryzyka bezpieczeństwa - jako niebezpieczna (B). Połączenie prawdopodobieństwa i dotkliwości (4B) jest wskaźnikiem ryzyka dotyczącego bezpieczeństwa danej konsekwencji.

Dotkliwość	*Znaczenie*	*Wartość*
Katastrofalna	— Zniszczenie sprzętu — Wiele ofiar śmiertelnych	A
Niebezpieczna	— Duże obniżenie marginesu bezpieczeństwa, fizyczne dolegliwości lub obciążenie operatorów pracą w takim stopniu, że nie ma pewności, że będą wykonywali	B
Większa	— Znaczne zredukowanie marginesów bezpieczeństwa, osłabienie zdolności operatorów do radzenia sobie z niekorzystnymi warunkami na skutek wzrostu	C
Niewielka	— Uciążliwość — Ograniczenia operacyjne	D
Nieistotna	— Niewielkie konsekwencje	E

Rys. 2-12. Tabela dotkliwości ryzyka dotyczącego bezpieczeństwa

Prawdopodobieństwo ryzyka		Dotkliwość ryzyka				
		Katastrofalna A	Niebezpieczna B	Poważna C	Niewielka D	Nieistotna E
Częste	5	**5A**	**5B**	**5C**	**5D**	**5E**
Sporadyczne	4	**4A**	**4B**	**4C**	**4D**	**4E**
Odległe	3	**3A**	**3B**	**3C**	**3D**	**3E**
Nieprawdopodobne	2	**2A**	**2B**	**2C**	**2D**	**2E**
Skrajnie nieprawdopodobne	1	**1A**	**1B**	**1C**	**1D**	**1E**

Rys. 2-13. Matryca oceny ryzyka dotyczącego bezpieczeństwa

2.14.11. Znacznik, uzyskany z matrycy oceny ryzyka dotyczącego bezpieczeństwa należy następnie przenieść do matrycy tolerancji ryzyka dotyczącego bezpieczeństwa, która opisuje kryteria tolerancji w danej organizacji. Używając powyższego przykładu, kryterium oceny ryzyka na poziomie 4B zalicza się do kategorii „nietolerowane w istniejących warunkach". W tym przypadku oznacznik konsekwencji ryzyka dotyczącego bezpieczeństwa jest nie do zaakceptowania. Organizacja musi więc:

a) podjąć działania redukujące narażenie się na konkretne ryzyko, tj. musi w oznaczniku ryzyka zredukować składnik prawdopodobieństwa;

b) podjąć działania redukujące dotkliwość konsekwencji związanych z zagrożeniem, tj. musi w oznaczniku ryzyka zredukować składnik dotkliwości; lub

c) zaprzestać danej działalności, jeśli złagodzenie nie jest możliwe.

Uwaga. – Odwrócona piramida na Rys. 2-14 odzwierciedla stały wysiłek przesuwania znacznika ryzyka w kierunku odwróconego wierzchołka piramidy. Rys. 2-15 jest przykładem alternatywnej matrycy tolerowania ryzyka.

2.15. ZARZĄDZANIE RYZYKIEM DOTYCZĄCYM BEZPIECZEŃSTWA

2.15.1. Zarządzanie ryzykiem dotyczącym bezpieczeństwa obejmuje ocenę i łagodzenie skutków zagrożeń dla bezpieczeństwa. Celem zarządzania bezpieczeństwem jest ocena rodzajów ryzyka związanego ze zidentyfikowanymi zagrożeniami oraz stworzenie i wdrożenie skutecznych i właściwych środków łagodzących. Dlatego też zarządzanie ryzykiem jest kluczowym komponentem procesu zarządzania bezpieczeństwem zarówno na poziomie krajowym, jak i na poziomie dostawcy lub dostawcy usług.

2.15.2. Zagrożenia są ocenione pojęciowo jako akceptowalne, tolerowane lub nieakceptowalne. Spadek oceny ryzyka początkowo ocenionego jako nietolerowane jest nie do przyjęcia w żadnym wypadku. Prawdopodobieństwo nasilenia skutków

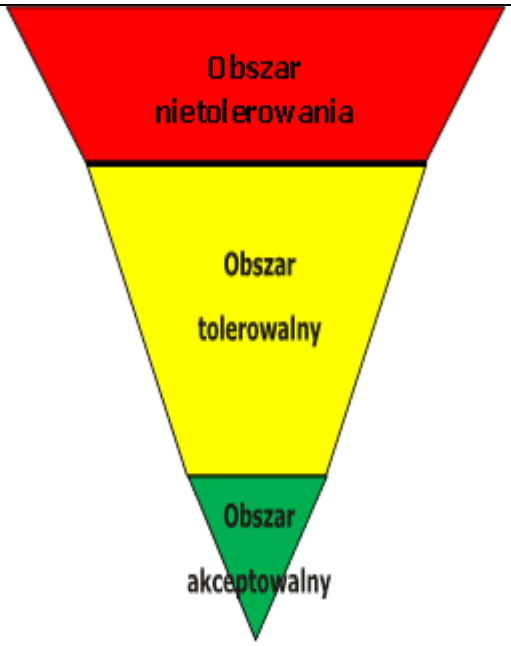
zagrożeń jest tak duże, a potencjał szkodliwości stwarza takie zagrożenie dla bezpieczeństwa, że jest wymagane natychmiastowe działanie łagodzące.

2.15.3. Ryzyko dotyczące bezpieczeństwa, których ocena mieści się w obszarze tolerowanym, są do zaakceptowania pod warunkiem wdrożenia przez organizację właściwych strategii łagodzących. Pojedyncze ryzyko dotyczące bezpieczeństwa, ocenione wstępnie jako nietolerowane może zostać złagodzone i następnie przejść do obszaru tolerowanego, pod warunkiem, że takie ryzyka będą kontrolowane przez odpowiednie strategie łagodzące. W obydwu przypadkach można przeprowadzić uzupełniającą analizę koszt-korzyść, jeśli uzna się to za stosowne. Dalsze szczegóły patrz pkt 2.15.7.

2.15.4. Ryzyko dotyczące bezpieczeństwa, ocenione początkowo jako podpadające pod obszar ryzyka akceptowalnych, stają się akceptowalne takimi jakimi aktualnie są i nie wymagają od organizacji żadnych działań dla podniesienia bądź utrzymania prawdopodobieństwa i/lub dotkliwości konsekwencji zagrożeń.

Dokumentacja/arkusz kalkulacyjny zarządzania ryzykiem

2.15.5. Każda próba łagodzenia ryzyka musi być udokumentowana zgodnie z wymaganiami. Można to zrobić na podstawowym arkuszu kalkulacyjnym lub tabeli łagodzenia ryzyka, obejmującej nieskomplikowane działania, procesy lub systemy. Dla identyfikacji zagrożeń i łagodzenia ryzyka w skomplikowanych procesach, systemach lub działaniach, dla ułatwienia procesu dokumentowania, konieczne może być wykorzystanie klientowi dedykowanego oprogramowania. Kompletna dokumentacja dotycząca łagodzenia ryzyka powinna zostać zatwierdzona przez odpowiedni szczebel kierownictwa. Przykład podstawowego arkusza dla łagodzenia ryzyka znajduje się w Dodatku 2.

Zakres tolerancji	Znacznik oceny ryzyka	Sugerowane kryteria
	**5A, 5B, 5C, 4A, 4B, 3A**	Nieakceptowalne w istniejących okolicznościach
	5D, 5E, 4C, 4D 4E, 3B, 3C, 3D 2A, 2B, 2C, 1A	Akceptowalne przy założonym łagodzeniu ryzyka. Może wymagać decyzji na poziomie kierowniczym.
	3E, 2D, 2E 1B, 1C, 1D, 1E	Akceptowalny

Rys. 2-14 Matryca tolerowania ryzyka bezpieczeństwa

Zakres znacznika ryzyka	Opis	Zalecane działanie
5A, 5B,5C, 4A,4B, 3A	Wysokie ryzyko	Przerwać lub zredukować operację natychmiast, jeśli konieczne. Przeprowadzić priorytetowe łagodzenie ryzyka, aby zapewnić wprowadzenie dodatkowych lub wzmocnionych środków zapobiegawczych w celu obniżenia znacznika ryzyka do zakres umiarkowanego lub niskiego poziomu.
5D, 5E,4C, 4D, 4E, 3B,3C, 3D, 2A, 2B,2C, 1A	Umiarkowane Ryzyko	Zaplanować wykonanie oceny bezpieczeństwa w celu obniżenia znacznika ryzyka do poziomu niskiego ryzyka, jeśli jest to wykonalne.
3E, 2D, 2E,1B, 1C,1D, 1E	Niskie Ryzyko	Akceptowalne, takie jakie jest. Nie ma potrzeby dalszego łagodzenia ryzyka.

Rys. 2-15 Alternatywna matryca tolerancji ryzyka dotyczącego bezpieczeństwa

Czynnik ludzki i zarządzanie ryzykiem

2.15.6. Założywszy, że celami dojrzałych SSP i SMS są zarówno czynniki ludzkie, jak i organizacyjne, elementem każdego dojrzałego, skutecznego systemu zarządzania ryzykiem jest określony proces analizy. W toku jakiegokolwiek działania identyfikującego zagrożenie bądź łagodzącego ryzyko z udziałem człowieka, niezbędne jest zapewnienie, by istniejące bądź zalecane elementy obronne uwzględniały czynnik ludzki *(human factor - HF)*. Tam gdzie konieczne, przeprowadzona może zostać uzupełniająca analiza czynnika ludzkiego dla wsparcia konkretnego działania/zespołu łagodzenia ryzyka. Analiza czynników ludzkich (HF) zapewnia zrozumienie wpływu błędu człowieka na sytuację i ostatecznie przyczynia się do opracowania bardziej wszechstronnych i efektywnych działań łagodząco/korygujących. Model błędu ludzkiego jest podstawą procesu analizy i definiuje związek pomiędzy działaniami i błędami oraz klasyfikuje błędy, pozwalając szybciej zidentyfikować i zrozumieć pierwotne zagrożenia. Takie zrozumienie zapewnia właściwe przeprowadzenie analizy pierwotnych przyczyn. Indywidualne działania i decyzje, rozpatrywane bez kontekstu, mogą praktycznie wyglądać na zdarzenia przypadkowe, umykające należnej uwadze. Zachowanie ludzkie natomiast niekoniecznie jest przypadkowe. Zazwyczaj jest zgodne z jakimś wzorcem i daje się analizować i odpowiednio zrozumieć. Ostatecznie, ta istotna perspektywa HF skutkuje bardziej wszechstronnym i pogłębionym procesem łagodzenia. Analiza czynnika ludzkiego zapewnia, że podczas procesu łagodzenia ryzyka w organizacji zostaną należycie rozważone czynniki ludzkie i związane z nimi okolicznościowe, nadzorcze i organizacyjne oddziaływania – przy okazji identyfikacji przyczyn pierwotnych i czynników sprzyjających lub eskalujących ryzyko.

Analiza kosztów i korzyści (CBA)

2.15.7. Analiza koszt-korzyść lub koszt-skutek jest procesem niezależnym od łagodzenia lub oceniania ryzyka dotyczącego bezpieczeństwa. Jest ona z reguły kojarzona z protokołem wyższego szczebla zarządzania, takim jak ocena wpływu przepisów, lub projektami rozszerzenia działalności gospodarczej. Ale możliwe są sytuacje, gdy ocena ryzyka może odbywać się na poziomie dostatecznie wysokim lub może mieć znaczący wpływ finansowy. W takich sytuacjach, na wsparcie oceny ryzyka może zostać zagwarantowany uzupełniający proces CBA lub proces skutecznego gospodarowania kosztami. Ma to zapewnić, by analiza koszt-efektywność kosztów, lub uzasadnienie dla zalecanych działań łagodzących lub kontroli prewencyjnych uwzględniało towarzyszące implikacje finansowe.

2.16. WYMAGANIA BAZUJĄCE NA NAKAZACH I OSIĄGACH

Zrozumienie wymagań opartych na osiągach

2.16.1. Wśród społeczności lotniczej istnieje wzrastające przekonanie, że skuteczne wdrożenie krajowych programów bezpieczeństwa (SSP) i systemów zarządzania bezpieczeństwem (SMS) wymaga, by istniejące nakazowe podejście do bezpieczeństwa uzupełnić o podejście oparte na wynikach. Podejście oparte na wynikach operacyjnych, wsparte zbieraniem i analizą istotnych danych, ma sens biznesowy, przy czym jednocześnie zapewnia odpowiedni poziom bezpieczeństwa.

2.16.2. Jednym z celów systemu zarządzania bezpieczeństwem jest to, by dla bardziej skutecznej kontroli ryzyka dotyczących bezpieczeństwa wprowadzić elementy uzupełniające, bazujące na wynikach. W środowisku konwencjonalnym, spolegliwym

wobec przepisów, podejście do zarządzania bezpieczeństwem jest względnie sztywne i nakazowe, gdzie to przepisy dotyczące bezpieczeństwa są stosowane jako narzędzia administracyjne. Dla zapewnienia przestrzegania przepisów, rama prawna jest uzupełniana inspekcjami i audytami.

2.16.3. W środowisku ulepszonego bezpieczeństwa bazującego na wynikach, wprowadza się do nakazowej ramy prawnej pewne elementy, które bazują na osiągach. To pozwala, by w aspekcie spolegliwości wobec przepisu znalazło się miejsce na osiągi bardziej elastyczne, oparte na ryzyku (i przez to bardziej dynamiczne). W rezultacie, niektóre elementy w ramach SMS i SSP mogą być zarządzane w sposób coraz bardziej bazujący na osiągach a nie na czystym nakazie. Bezpieczeństwo tych bazujących na osiągach elementów jest chronione niczym komponenty zarządzania ryzykiem dotyczącym bezpieczeństwa odnośnych ram.

2.16.4. Znajdujące się w ramach SMS/SSP elementy bazujące na osiągach obejmują proces monitorowania i mierzenia osiągów bezpieczeństwa zarówno na poziomie indywidualnego dostawcy lub dostawcy usług, jak i na poziomie Państwa. Element ten pozwala organizacji na wybór własnych wskaźników monitorowania bezpieczeństwa i nastawianie odpowiednich alarmów i celów odpowiednich dla własnego kontekstu, historii osiągów i oczekiwań. Nie ma sztywnych (obowiązkowych), nakazanych wskaźników bezpieczeństwa ani poziomów alarmowych czy nakazanych wartości, które wynikałyby z SMS/SSP.

Warunki wstępne dla wymagań bazujących na osiągach

2.16.5. Państwo powinno mieć SSP a jego dostawcy produktów i usług powinni mieć u siebie SSP i SMS. Na miejscu musi być interfejs, poprzez który organizacje legislacyjne będą z poszczególnymi dostawcami produktów i usług uzgadniać wskaźniki działania bezpieczeństwa ich SMS i związane z nimi cele, oczekiwane poziomy bezpieczeństwa oraz poziomy alarmowe. Wymagane jest by dostawca usług posiadał zdefiniowany proces ciągłego monitorowania wyników bezpieczeństwa u indywidualnych dostawców i dostawców usług. Nowe, dodatkowe procesy oparte na osiągach, wprowadzone i odpowiednio zaakceptowane/zaaprobowane przez organ regulacyjny, powinny posiadać właściwe wskaźniki wyników, opracowane do monitorowania właśnie takich procesów bazujących na osiągach. Takie wskaźniki, dedykowane dla procesów, można uważać za uzupełniające w stosunku do wskaźników SMS wyższego rzędu bezpieczeństwa.

Bazowy i równoważny poziom bezpieczeństwa

2.16.6. Wynik działania bezpieczeństwa, uzyskany z wprowadzenia do ramy SMS elementów bazujących na wynikach w ramie SMS lub będący uzupełnieniem SMS, nie powinien być gorszy niż wynik we wcześniej istniejącej, czysto nakazowej ramie prawnej. Aby ocenić lub monitorować czy istotnie występuje taka „równoważność", powinny istnieć wskaźniki bezpieczeństwa do monitorowania całościowego wyniku wydarzeń (przypadki nieprzestrzegania) w danym procesie/systemie, w którym będzie wprowadzony element oparty na osiągach. Jako przykład, wskaźnik średniej incydentów dla całego Planowania Lotów i Zarządzania Paliwem (FPFM) po wprowadzeniu postanowień, by bazować na osiągach nie powinien być gorszy niż wskaźnik incydentów sprzed wprowadzenia postanowień, by bazować na osiągach. Aby się przekonać czy jest utrzymywany „równoważny" poziom bezpieczeństwa można, poprzez taki proces porównawczy, zweryfikować osiągi bazowe sprzed wprowadzenia ww. elementów z osiągami po ich wprowadzeniu. Jeśli okaże się, że lepszy jest wynik późniejszy, będzie to oznaczać, że pojawił się „lepszy" poziom bezpieczeństwa. Tam gdzie jest degradacja osiągów w systemie, dostawca usług powinien wraz z organem regulacyjnym zweryfikować przyczyny takiego stanu i podjąć właściwe działania, które mogą obejmować konieczne modyfikacje samego wymogu by bazować na osiągach, lub jeśli to niezbędne, przywrócić zasadnicze wymagania nakazowe. Szczegóły dotyczące tego jak można zmierzyć osiągi systemu używając wskaźników osiągów bezpieczeństwa uwzględniono w pkt 2.16.7, a także Rozdział 4 i 5 niniejszego podręcznika.

Pomiar i monitorowanie oparte na wydajności

2.16.7. Monitorowanie i mierzenie procesu opartego na wydajności powinno być dokonywane poprzez stosowne wskaźniki wydajności, jakości lub bezpieczeństwa, które w sposób ciągły śledzą wydajność tego procesu. Parametrami dla śledzenia jego wydajności mogą być skutki przypadkowych zdarzeń, odchylenia lub wszelkie inne typy wydarzeń, które odzwierciedlają poziom bezpieczeństwa, jakość czy poziom ryzyka procesu. Do śledzenia takich skutków należy wykorzystać wykres trendu danych. Zwyczajowo, wydarzenia które są brzemienne w skutkach należy postrzegać bardziej w kategorii częstotliwości niż w wartościach bezwzględnych. Tam gdzie to ma zastosowanie, dla każdego wskaźnika powinny zostać ustalone poziomy alarmowe, jak również pożądane i docelowe poziomy poprawy. Docelowo mają one służyć jako znaczniki definiujące stopy odchyleń od normy/nieakceptowalności wydarzeń, jak również stopy pożądanej, docelowej poprawy wskaźnika. Ustawienie poziomu alarmowego skutecznie posłuży wskaźnikowi bezpieczeństwa, jako linia demarkacyjna między akceptowalnym obszarem trendu a obszarem nieakceptowalnym. Dopóki stopa częstotliwości wydarzenia nie ma w procesie tendencji do przekroczenia lub dokonania wyłomu w ustanowionych kryteriach poziomu alarmu, ilość takich wydarzeń uważa się za akceptowalną (a nie za nienormalną) dla danego okresu monitorowania. Z drugiej strony, docelowy poziom poprawy ma być osiągnięty w określonym punkcie czasu (kamień milowy) lub w okresie monitorowania. Przy tak zdefiniowanych nastawach celu i alarmu, staje się jasne, że jakościowe/ilościowe skutki można wyliczyć pod koniec dowolnego okresu monitorowania. Można to zrobić poprzez policzenie - dla poszczególnego wskaźnika i/lub pakietu wskaźników bezpieczeństwa - ilości przerw alarmowych i/lub liczby celów osiągniętych. Przykłady wskaźników działania bezpieczeństwa i metodologii ustalania celu/alarmu są omówione odpowiednio w Rozdziałach 4 i 5.

Ogląd wymagań bazujących na osiągach

2.16.8. Inaczej niż w przypadku audytu pojedynczych wymagań nakazowych, ocena procesu w oparciu o wyniki będzie wymagała, aby oceniający był świadom kontekstu procesu/elementu w ramach całej struktury, jak również złożoności

audytowanej organizacji. Może nie istnieć proste kryterium „tak” lub „nie” albo zdany/niezdany, które można zastosować. Przykładem mogłaby być akceptowalność systemu raportowania zagrożeń lub akceptowalność poziomów docelowych/alarmowych dla procesów opartych na wynikach. Może to obejmować więcej interaktywności, monitorowania, negocjacji i obiektywnego osądu audytora. Poziom lub stopień zgodności takich elementów bywają także różne w zależności od złożoności procesu lub działania podlegającego audytowi. Przykładem wyniku lub zgodności elementu, który zależy od złożoności organizacji lub procesu byłby proces łagodzenia ryzyka. Proces łagodzenia ryzyka może obejmować użycie jednostronicowego arkusza na potrzeby prostego, jednoosobowego działania w ramach zadania warsztatowego. Z drugiej strony łagodzenie ryzyka dla procesu wielodyscyplinarnego (np. operacji w przestrzeni powietrznej nad wulkanem) może wymagać użycia oprogramowania łagodzącego ryzyko w celu dokonania satysfakcjonującej wszechstronnej oceny bezpieczeństwa.

Dodatek 1 do Rozdziału 2

**LISTA KONTROLNA DO OCENY PROFILU RYZYKA W ORGANIZACJI (ORP)
I KULTURY BEZPIECZEŃSTWA W ORGANIZACJI (OSC)
(PRZYKŁAD DLA OPERATORA LOTNICZEGO)**

Uwaga. – Ta lista kontrolna OSC/ORP jest tylko koncepcyjna. Pokazanych trzydzieści siedem parametrów nie stanowią całości, ale mają zastosowanie do organizacji jaką jest operator lotniczy. Do oceny innych typów dostawców usług trzeba te parametry przystosować. Załączone wyniki mają charakter czysto ilustracyjny. Pokazana ocena OSC/ORP powinna być prowadzona na zasadzie dobrowolności uczestnictwa w związku z tym, że kultura organizacji/parametry profilu wykraczają poza zakres normalnych uregulowań prawnych. Po sugerowane zastosowania systemu oceny OSC/ORP patrz Rozdział 2 pkt 2.6.19.

Kolumna wyników: Z przewijanego menu wybierz "1" (L1), "2" (L2), "3" (L3) lub "N/A" (NIE DOTYCZY) według oceny POI/PMI/AOC ORP 12 marca

Nazwa organizacji:		Ocena dokonana przez/ Data:			
		POZIOM / PROFIL RYZYKA			*WYNIK (Poziom #)*
	Parametr ryzyka organizacji	*Poziom 3 (Najmniej pożądany)*	*Poziom 2 (Średni)*	*Poziom 1 (Najbardziej pożądany)*	
1	Kierownik Odpowiedzialny– pełnienie funkcji dotyczących bezpieczeństwa/jakości	Brak Kierownika Odpowiedzialny za pełnienie funkcji dotyczących bezpieczeństwa/jakości TOR	TOR Kierownika Odpowiedzialnego wspomina nieznacząco lub pomija funkcje dotyczące bezpieczeństwa/jakości	TOR Kierownika Odpowiedzialnego jasno określa ostateczną odpowiedzialność za bezpieczeństwo & sprawy jakości	3
2	Finansowa kondycja organizacji	DO USTALENIA	DO USTALENIA	DO USTALENIA	2
3	Średni wiek floty	> 12 lat	8 do 12 lat	< 8 lat	2
4	Wynik działania SMS	2011 r.: 65% do 75%	76% do 90%	> 90%	3
5	Program Identyfikacji Zagrożeń i Oceny Ryzyka (HIRA)	Brak programu HIRA	Wdrożono program HIRA. Ukończenie lub przegląd od 1 do 3 projektów oceniających ryzyko (na 100 pracowników operacyjnych) w ciągu ostatnich 12 miesięcy	Wdrożono program HIRA dla wszystkich głównych obszarów operacyjnych. Ukończenie lub przegląd > 3 projektów oceny ryzyka (na 100 pracowników operacyjnych) dla wszystkich obszarów operacyjnych w ciągu ostatnich 12 miesięcy	2
6	Wymagające grafików dyżurów lub rozkładów lotów (liczba incydentów na FTL?)	DO USTALENIA	DO USTALENIA	DO USTALENIA	2
7	Stosunek liczby osób zajmujących się bezpieczeństwem i kontrolą jakości do całkowitej liczby pracowników operacyjnych	1: > 20	1:15 - 20	1: < 15	3
8	Mieszane Floty [% pilotów objętych MFF – wyższy % mniej pożądany]	DO USTALENIA	DO USTALENIA	DO USTALENIA	1
9	Trasy ETOPS (% obsługiwanych sektorów ETOPS) [wyższy % mniej pożądany]	DO USTALENIA	DO USTALENIA	DO USTALENIA	2
10	Czas trwania ETOPS [wyższy czas trwania mniej pożądany]	DO USTALENIA	DO USTALENIA	DO USTALENIA	2

Nazwa organizacji:		Ocena dokonana przez/ Data:			
	Parametr ryzyka organizacji	*POZIOM / PROFIL RYZYKA*			*WYNIK (Poziom #)*
		Poziom 3 (Najmniej pożądany)	*Poziom 2 (Średni)*	*Poziom 1 (Najbardziej pożądany)*	
11	Doświadczenie firmy (lata działalności)	< 5 lat	5 do 10 lat	> 10 lat	3
12	Łączna fluktuacja na stanowiskach Odpowiedzialnego Kierownika, Kierownika ds. Bezpieczeństwa i Kierownika ds. Jakości przez ostatnie 36 miesięcy	3 lub więcej	2	1 lub zero	2
13	Doświadczenie i kwalifikacje Odpowiedzialnego Kierownika (na dzień dokonywania oceny)	Ma < niż 3 lata doświadczenia lotniczego oraz brak kwalifikacji technicznych	Ma > 3 lata doświadczenia lotniczego lub kwalifikacje techniczne	Ma > 3 lata doświadczenia lotniczego oraz kwalifikacje techniczne	3
14	Doświadczenie i kwalifikacje Kierownika ds. Bezpieczeństwa (SM)	Ma < 5 lat doświadczenia w lotnictwie cywilnym w dziedzinie bezpieczeństwa/jakości lub brak technicznych kwalifikacji lotniczych	Ma > 5 lat doświadczenia w lotnictwie cywilnym w dziedzinie bezpieczeństwa/jakości oraz techniczne kwalifikacje lotnicze	Ma > 15 lat doświadczenia w lotnictwie cywilnym w dziedzinie bezpieczeństwa/jakości oraz techniczne kwalifikacje lotnicze	2
15	Doświadczenie i kwalifikacje Kierownika ds. Jakości	Ma < 5 lat doświadczenia w lotnictwie cywilnym w dziedzinie QC/QA lub brak technicznych kwalifikacji w lotnictwie cywilnym.	Ma > 5 lat doświadczenia w lotnictwie cywilnym w dziedzinie kontroli jakości/zapewnianiu jakości oraz kwalifikacje techniczne w lotnictwie cywilnym.	Ma > 15 lat doświadczenia w lotnictwie cywilnym w dziedzinie QC/QA oraz kwalifikacje techniczne w lotnictwie cywilnym.	1
16	Wielorakie funkcje personelu związanego z zarządzaniem bezpieczeństwem/Jakością	Kierownik ds. Bezpieczeństwa lub Kierownik ds. Jakości zajmuje równocześnie inne kierownicze stanowiska w organizacji lub poza nią.	TOR SM lub QM obejmują inne, funkcje niezwiązane bezpośrednio z bezpieczeństwem/jakością, np. IT, administrację, szkolenie, itd.	SM lub QM nie zajmuje równocześnie żadnych innych kierowniczych stanowisk w organizacji lub poza nią a ich TOR nie obejmują innych funkcji niezwiązanych bezpośrednio bezpieczeństwem/jakością.	2
17	Wielość typów statków powietrznych	> 4 typy statków powietrznych	3 do 4 typów statków powietrznych	< 3 typy statków powietrznych	1
18	Połączony wskaźnik zdarzeń zgłaszanych obowiązkowo (na 1000FH) za ostatnie 24 miesiące	DO USTALENIA	DO USTALENIA	DO USTALENIA	2
19	Zarezerwowany				
20	Połączony IFSD silnika na 1000FH dla floty	DO USTALENIA	DO USTALENIA	DO USTALENIA	2
21	Średnia ilość zastosowania MEL dla floty (na 1000 FH)	> 30 zastosowań MEL na 1000 FH	10 do 30 zastosowań MEL na 1000 FH	< 10 zastosowań MEL na 1000 FH	2
22	Wewnętrzny wskaźnik odstępstw technicznych	> 3 odstępstwa na statek powietrzny na rok	> 1 odstępstwo na statek powietrzny na rok	< 1 odstępstwo na statek powietrzny na rok	2
23	Wskaźnik odstępstw technicznych CAA	> 1 odstępstwo na statek powietrzny na rok	> 0,5 odstępstwa na statek powietrzny na rok	< 0,5 odstępstwa na statek powietrzny na rok	2
24	Struktura odpowiedzialności za bezpieczeństwo	Funkcja zarządzania bezpieczeństwem/biuro/kierownik odpowiada przed lub podlega niektórym funkcjom operacyjnym.	Funkcja zarządzania bezpieczeństwem/biuro/kierownik odpowiada przed wyższym kierownictwem i nie jest zależny od żadnych funkcji operacyjnych	Funkcja zarządzania bezpieczeństwem/biuro/kierownik odpowiada i raportuje bezpośrednio do CEO	3

Nazwa organizacji:		Ocena dokonana przez/ Data:			
	Parametr ryzyka organizacji	*POZIOM / PROFIL RYZYKA*			*WYNIK (Poziom #)*
		Poziom 3 (Najmniej pożądany)	*Poziom 2 (Średni)*	*Poziom 1 (Najbardziej pożądany)*	
25	Struktura odpowiedzialności za jakość	Funkcja zarządzania jakością/biuro/kierownik odpowiada przed lub podlega niektórym funkcjom niezwiązanym z jakością/bezpieczeństwem.	Funkcja zarządzania jakością/biuro/kierownik odpowiada przed wyższym kierownictwem i nie jest zależny od żadnych funkcji operacyjnych	Funkcja zarządzania jakością/biuro/kierownik odpowiada i raportuje bezpośrednio do CEO	3
26	Oceny z audytu organizacji na certyfikat CAA AOC (Ustalenia tylko na poziomie 1 i 2, wykluczając obserwacje) za ostatnie 24 miesiące	Jakiekolwiek ustalenie na Poziomie 1 LUB > 5 ustaleń na audyt na statek powietrzny	>1 ustalenie na audyt na statek powietrzny	<1 ustalenie na audyt na statek powietrzny	2
27	Ustalenia inspektora CAA LSI (na Poziomie 1 i 2, wykluczając obserwacje) za ostatnie 24 miesiące	Jakiekolwiek ustalenie na Poziomie1 LUB > 3 ustaleń na audyt na bazę techniczną	> 0,5 ustalenia na audyt na bazę techniczną	< 0,5 ustalenia na audyt na bazę techniczną	2
28	Zasady ustalonej/CM/elastycznej eksploatacji (cyklu życia) komponentów (części wymienialnych) w obsłudze liniowej - ponad wymagania obowiązkowe lub MPD	Brak (sztywnych/elastycznych) zasad eksploatacji (cyklu życia) komponentów ponad wymagania obowiązkowe lub MPD	Zasady i procedury aktywnej kontroli eksploatacji komponentów (cykle życia). Co najmniej 5-10% wszystkich (wyszczególnionych w MPD/AMS) części wymienialnych systemów sterowania silnikiem i samolotem ma resursy sztywne lub elastyczne (wykraczające poza wymagania obowiązkowe i zaplanowane w MPD)	Zasady i procedury aktywnej kontroli eksploatacji komponentów (cykle życia). Więcej niż 5-10% wszystkich (wyszczególnionych w MPD/AMS) części wymienialnych systemów sterowania silnikiem i samolotem ma resursy sztywne lub elastyczne (wykraczające poza wymagania obowiązkowe i zaplanowane w MPD)	28
29	Zakres badania QA i procesu MEDA	Wewnętrzne badanie QA zastosowane tylko wobec obowiązkowo zgłaszanych incydentów.	Wewnętrzne badanie QA zastosowane wobec wszystkich raportowanych incydentów	Wewnętrzne badanie QA zastosowane wobec wszystkich raportowanych incydentów + dla procesów MEDA (lub równoważnych).	27
30	Dostępność programu Ochrony Środowiskowej	Nie istniejący.	Odizolowane uczestnictwo/program w Lotniczej Ochronie Środowiskowej.	Rutynowy program i regularne zaangażowanie oraz uczestnictwo w programie Lotniczej Ochrony Środowiska	3
31	Dostępność programu Specjalnej Inspekcji opartego na publikacjach nieobowiązkowej obsługi częściami OEM	Program Specjalnej Inspekcji tylko dla Biuletynów Obsługi spokrewnionych z AD.	Program Specjalnej Inspekcji tylko dla ADs i Ostrzegawczych Biuletynów Obsługi	Program Specjalnej Inspekcji tylko dla ADs, Ostrzegawczych SBs i rutynowych publikacji OEM	2
32	Kontrola Technicznego Zarządzania Flotą	Całkowicie zleca jakiejś organizacji zewnętrznej.(FTM + ITM)	Częściowo zleca jakiejś organizacji zewnętrznej	Wewnętrzne zarządzanie przez organizację AOC	2
33	Korzystanie z technicznych pracowników kontraktowych	> 15% pracowników kontraktowych (z innej organizacji) do wewnętrznych funkcji inżynierskich/technicznych	5 do 15% pracowników kontraktowych (z innej organizacji) do wewnętrznych funkcji inżynierskich/technicznych	<5 % pracowników kontraktowych (z innej organizacji) do wewnętrznych funkcji inżynierskich/technicznych	2
34	Certyfikuje inspekcję przesunięcia pilota, technika lub mechanika samolotowego (AME)	Praktykuje certyfikowanie inspekcji przesunięcia pilota w miejsce wykwalifikowanego mechanika/AME	Praktykuje certyfikowanie inspekcji przesunięcia technika (o ograniczonych uprawnieniach) w miejsce mechanika samolotowego (AME)	Praktykuje certyfikowanie inspekcji przesunięcia tylko AME (mechanik samolotowy z pełnymi uprawnieniami na typ samolotu)	3
35	Systemy raportowania zagrożeń	Nie ma	Jest system dobrowolnego raportowania zagrożeń	Jest system dobrowolnego raportowania zagrożeń. Także procedura identyfikująca zagrożenia w połączeniu z procesem badania incydentów	2

Nazwa organizacji:	Ocena dokonana przez/ Data:

	Parametr ryzyka organizacji	*POZIOM / PROFIL RYZYKA*			*WYNIK (Poziom #)*
		Poziom 3 (Najmniej pożądany)	*Poziom 2 (Średni)*	*Poziom 1 (Najbardziej pożądany)*	
36	Procedury raportowania incydentów, przeprowadzania działań dochodzeniowych i zaradczych	Brak udokumentowych procedur raportowania incydentów, dochodzeń i działań zaradczych	Udokumentowane procedury raportowania incydentów, dochodzeń i działań zaradczych	Udokumentowane i akceptowane przez CAA procedury raportowania incydentów, dochodzeń i działań zaradczych	2
37	Zapisy Techniczne, Magazyny Techniczne i Zarządzanie Planowaniem Floty	Pełne zlecanie firmie zewnętrznej prowadzenia Zapisów Technicznych, Magazynów Technicznych i zarządzania planowaniem floty	Zlecanie organizacji zewnętrznej Zapisów Technicznych, Magazynów Technicznych i Zarządzania Planowaniem Floty	Własne Zapisy Techniczne, Magazyny Techniczne i Zarządzanie Planowaniem Floty	3

	WYNIK CZĘŚCIOWY
A	11
POZIOM 2	21
POZIOM1	3
Nie dotyczy	0
Ogólna liczba pytań	37

Wynik oceny	
Suma punktów	Kategoria profile ryzyka operatora
78	D

Kategoryzacja ORP	
Łączny wynik	**Kategoria ORP**
35-49	A (Pożądany)
50-63	B
64-77	C
78-91	D
92-105	E (Najmniej pożądany)

Uwagi:

1. Opisy kryteriów poziomu ryzyka/liczby są jedynie ilustracją/; stosować pod warunkiem dostosowania do klienta i uwierzytelnienia liczb.
2. Listy kontrolne trzeba personalizować dla AMO i dla dostawców usług lotniskowych i dostawców usług ATS.
3. Punkty jakie należny przypisać każdemu ocenianemu parametrowi to 1, 2 lub 3 odpowiednio dla Poziomu 1, 2 i 3.
4. Oceny OSC/ORP poprzez listy kontrolne może dokonać wyznaczony inspektor według ustaleń (np. podczas audytu organizacji). Może on potrzebować nawiązać kontakt z dostawcą danej usługi w celu zebrania niektórych potrzebnych danych.
5. Niniejszy proces oceny OSC/ORP nie może być obowiązkowy z powodu parametrów, które wychodzą poza zwykły nadzór regulacyjny, np. wskaźnik rotacji pracowników itd. Może zostać zaaplikowany na zasadzie udziału dodatkowego/dobrowolnego.
6. Ogólna liczna osiągniętych punktów i odpowiadająca im Kategoria ORP (od A do E) powinny być skomentowane. Wyniki należy dostarczyć ocenianej organizacji.
7. Wyniki niniejszej oceny OSC/ORP mogą być korelowane z innymi ustaleniami wynikającymi z inspekcji/audytu określonego przepisami w celu zidentyfikowania obszarów (organizacji) wzbudzających więcej obaw lub o większych potrzebach zgodnie z wymaganiami pkt.3.3 SSP. W innych przypadkach, przekazanie wyników ORP tylko do każdej organizacji z osobna może służyć jako mechanizm zachęcający ją do zachowań (kultura bezpieczeństwa) zmierzających do uzyskania pożądanej kategorii.

Dodatek 2 do Rozdziału 2
PRZYKŁAD ROBOCZEGO ARKUSZA ŁAGODZENIA RYZYKA DOTYCZĄCEGO BEZPIECZEŃSTWA

Uwaga. – dla łatwiejszego operowania arkuszem zaleca się używać osobnych kart dla poszczególnych: Zagrożeń>niebezpiecznych wydarzeń> kombinacji ostatecznych skutków.

Tabela 2-A2-1. Zagrożenie i Konsekwencja

Operacja/proces:	Opisz proces/operację/sprzęt/system będący przedmiotem tego ćwiczenia HIRM.
Zagrożenie [H]:	Jeśli operacji/procesowi przypisano więcej niż jedno zagrożenie użyj oddzielnych arkuszy dla każdego zagrożenia.
Niebezpieczne wydarzenie [UE]:	Jeśli zagrożeniu odpowiada więcej niż jedno UE użyj oddzielnych arkuszy dla każdej kombinacji UE-UC.
Ostateczna konsekwencja [UC]:	Jeśli zagrożeniu odpowiada więcej niż jedna UC użyj oddzielnych arkuszy dla każdej UC.

Tabela 2-A2-2. Indeks ryzyka i tolerowania konsekwencji / UE (patrz Dodatek 1):

	Tolerowanie bieżącego ryzyka (wzięcie pod uwagę wszelkich				*Indeks wypadkowy ryzyka i tolerowanie (wzięcie pod uwagę wszelkich nowych PC/RM/EC)*		
	Dotkliwość	Prawdo-podobieństwo	Tolerancja		Dotkliwość	Prawdo-podobieństwo	Tolerancja
Niebezpieczne wydarzenie							
Ostateczna konsekwencja							

Tabela 2-A2-3. Łagodzenie ryzyka

Zagrożenie [H]	Środek Zapobiegawczy [PC]	Czynnik Eskalujący [EF]	Środek Zapobiegający Eskalacji [EC]		Środek Naprawczy [RM]	Czynnik Eskalujący [EF]	Środek Zapobiegający Eskalacji [EC]	
H	PC1 *(istniejący)*	EF *(istniejący)*	EC1 *(istniejący)*	NIEBEZPIECZNE WYDARZENIE [UE]	RM1	EF (do RM1)	EC (do EF)	OSTATECZNA KONSEKWENCJA [UC]
			EC2 *(nowy)*					
	PC2 *(istniejący)*	EF1 *(nowy)*	EC *(nowy)*		RM2	EF (do RM2)	EC (do EF)	
		EF2 *(nowy)*	EC *(nowy)*					
	PC3 *(nowy)*	EF *(nowy)*	EC *(nowy)*		RM3	EF (do RM3)	EC (do EF)	

Notatki objaśniające:

1. *Operacja/Proces (Tabela 2-A2-1).* Opis operacji lub procesu, który jest przedmiotem niniejszej czynności łagodzenie zagrożenia/ryzyka dotyczącego bezpieczeństwa.

2. *Zagrożenie (H – Hazard*). Niepożądana okoliczność lub sytuacja, która może prowadzić do Niebezpiecznego Wydarzenia (wydarzeń) lub zdarzenia (zdarzeń). Czasami używa się określenia „niebezpieczeństwo" (np. TEM) zamiennie z „zagrożeniem".

3. *Niebezpieczne wydarzenie (UE – Unsafe event).* Możliwe niebezpieczne wydarzenie (UE), pośrednie przed ostateczną konsekwencją, wypadkiem lub najbardziej prawdopodobnym skutkiem. Identyfikacja niebezpiecznego wydarzenia ma zastosowanie tylko wtedy, gdy zachodzi potrzeba rozróżnienia i ustanowienia działań łagodzących przed i po zaistnieniu takiego pośredniego wydarzenia (przed ostateczną konsekwencją/wypadkiem, np. "wydarzenie zwiększona temperatura" przed "awarią silnika"). Jeśli ten pośredni stan UE nie dotyczy określonej operacji, wtedy może on zostać wykluczony.

4. *Ostateczna konsekwencja (UC – Ultimate Consequence).* Najbardziej wiarygodny skutek, ostateczne wydarzenie lub wypadek.

5. *Środek zapobiegawczy (PC – Preventive Control).* Minimalizujące działanie/mechanizm/element obronny mający na celu blokowanie lub zapobieganie przekształcaniu się zagrożenia/niebezpieczeństwa w niebezpieczne wydarzenie lub ostateczną konsekwencję.

6. *Czynnik eskalujący (EF – Escalation factor).* Prawdopodobna okoliczność/czynnik uśpiony, który może osłabiać skuteczność środka zapobiegawczego (lub środka naprawczego). Stosować tylko we właściwych przypadkach. Czynnik eskalujący może być czasem określany terminem „threat" (zagrożenie)".

7. *Środek panowania nad eskalacją (EC – Escalation control).* Łagodzące działanie/mechanizm, mające na celu blokowanie lub zapobieganie naruszeniu lub osłabieniu czynnika zapobiegawczego (lub środka naprawczego) przez czynnik eskalujący. Stosować tylko we właściwych przypadkach.

8. *Bieżący indeks ryzyka i tolerancji (Current risk index and tolerability*). Akcja mająca na celu złagodzenie ryzyka (Tabela 2-A2-3), stosowana zawsze gdy w Tabeli 2-A2-2 zostanie zidentyfikowany nieakceptowalny bieżący poziom tolerancji w wydarzeniu niebezpiecznym lub w ostatecznej konsekwencji. Indeks aktualnego ryzyka i tolerowania powinien uwzględniać, istniejące środki zapobiegawcze, o ile są dostępne.

9. *Wypadkowy indeks ryzyka i tolerancji (Resultant risk index and tolerability*). Wskaźnik wypadkowego ryzyka i tolerowanie bazują się na aktualnych środkach zapobiegawczych (jeśli istnieją) połączonych z nowymi środkami zapobiegawczymi/środkami panowania nad eskalacją/i środkami naprawczymi, wdrożonymi w wyniku zakończenia czynności łagodzenia ryzyka.

Załącznik do Dodatku nr 2

Przykłady dotkliwości, prawdopodobieństwo, indeksu ryzyka i tabel Tolerancji

Tabela Att-1. Tabela Dotkliwości (podstawowa)

Poziom	*Oznacznik*	*Opis dotkliwości (dostosować zgodnie z charakterem działalności dostawcy lub dostawcy usług)*
1	Nieznaczny	Bez znaczenia dla bezpieczeństwa operacyjnego związanego ze statkiem powietrznym.
2	Niewielki	Obniża lub wpływa na normalne procedury operacyjne lub osiągi statku powietrznego.
3	Umiarkowany	Częściowe zniszczenie znaczących/głównych systemów statku powietrznego, lub skutkuje zastosowaniem procedur odbiegających od normy lotniczych procedur operacyjnych.
4	Poważny	Całkowita awaria znaczących/głównych systemów statku powietrznego lub skutkuje zastosowaniem procedur awaryjnych lotniczych procedur operacyjnych.
5	Katastrofalny	Zniszczenie statku powietrznego lub utrata życia.

Tabela Att-2. Tabela dotkliwości (alternatywna)

Poziom	*Opis*	*Opis dotkliwości (dostosować zgodnie z charakterem działalności dostawcy lub dostawcy usług)*					
		Bezpieczeństwo statku powietrznego	*Obrażenia osób*	*Szkody materialne*	*Potencjalne straty dochodów*	*Szkody dla środowiska*	*Uszczerbek w reputacji firmy*
1	*Nieznaczna*	*Bez znaczenia dla bezpieczeństwa operacyjnego związanego ze statkiem powietrznym*	*Brak obrażeń*	*Brak szkód*	*Bez utraty dochodu*	*Bez szkód*	*Bez implikacji*
2	*Niewielka*	*Obniża lub wpływa na normalne procedury operacyjne lub osiągi statku powietrznego*	*Niewielkie obrażenia*	*Niewielka szkoda<$__*	*Niewielka strata< $*	*Niewielkie szkody*	*Ograniczone lokalne implikacje*
3	*Umiarkowana*	*Częściowe zniszczenie znaczących/głównych systemów statku powietrznego lub skutkuje nienormalnym działaniem procedury F/Ops*	*Poważne obrażenia*	*Istotna szkoda<$__*	*Istotna strata<$*	*Ograniczone szkody*	*Regionalne implikacje*
4	*Poważna*	*Całkowita awaria znaczących/ głównych systemów statku powietrznego lub skutkuje zastosowaniem procedury awaryjnej j F/Ops*	*Pojedyncza ofiara*	*Znaczna szkoda<$__*	*Znaczna strata<$__*	*Znaczne szkody*	*Krajowe implikacje*
5	*Katastrofalna*	*Zniszczenie statku powietrznego/kadłuba*	*Wiele ofiar*	*Katastrofalna szkoda >$__*	*Rozległe straty>$__*	*Rozległe szkody*	*Międzynarodowe implikacje*

Uwaga.– Aby otrzymać indeks ryzyka w tabeli matrycy indeksu ryzyka użyj najwyższego uzyskanego stopnia dotkliwości .

Tabela Att-3. Tabela prawdopodobieństwa

Poziom	*Słowa opisujące*	*Opis prawdopodobieństwa*
A	Pewny/częsty	Oczekuje się, że wystąpi w większości sytuacji.
B	Prawdopodobny/sporadyczny	Prawdopodobnie kiedyś wystąpi.
C	Możliwy/odległy w czasie	Może kiedyś wystąpić.
D	Nieprawdopodobny	Mógłby kiedyś wystąpić.
E	Na zasadzie wyjątku	Może wystąpić tylko w wyjątkowych okolicznościach.

Tabela Att-4. Matryca indeksu ryzyka (dotkliwość x prawdopodobieństwo)

Prawdopodobieństwo	*Dotkliwość*				
	1. Nieznaczna	*2. Niewielka*	*3. Umiarkowana*	*4. Poważna*	*5. Katastrofalna*
A. pewny/częsty	**Umiarkowane (1A)**	**Umiarkowane (2A)**	**Wysokie (3A)**	**Ekstremalne (4A)**	**Ekstremalne (5A)**
B. prawdopodobny/ sporadyczny	**Niskie (1B)**	**Umiarkowane (2B)**	**Umiarkowane (3B)**	**Wysokie (4B)**	**Ekstremalne (5B)**
C. możliwy/odległy w czasie	**Niskie (1C)**	**Niskie (2C)**	**Umiarkowane (3C)**	**Umiarkowane (4C)**	**Wysokie (5C)**
D. prawie niemożliwy/ nieprawdopodobny	**Nieistotne (1D)**	**Niskie (2D)**	**Niskie (3D)**	**Umiarkowane (4D)**	**Umiarkowane (5D)**
E. wyjątkowy	**Nieistotne (1E)**	**Nieistotne (2E)**	**Niskie (3E)**	**Niskie (4E)**	**Umiarkowane (5E)**

Tabela Att-5 Tabela akceptowalności (tolerowania) ryzyka

Indeks ryzyka	*Tolerowanie*	*Wymagane działanie (przystosować do klienta)*
5A, 5B, 4A	Ekstremalne ryzyko	Natychmiast wstrzymaj działanie lub proces. Nieakceptowane w istniejących okolicznościach. Nie zezwalaj na żadne działanie do czasu wdrożenia wystarczających środków kontrolnych dla zredukowania ryzyka do akceptowalnego poziomu. Wymagana zgoda najwyższego kierownictwa.
5C, 4B, 3A	Wysokie ryzyko	Ostrożnie. Upewnij się, że ocena ryzyka została dokonana prawidłowo i że zadeklarowane środki zapobiegawcze zostały zastosowane. Wymagana akceptacja oceny ryzyka przez wyższe kierownictwo przed rozpoczęciem operacji lub procesu.
1A, 2A, 2B, 3B, 3C, 4C, 4D,5D, 5E	Umiarkowane ryzyko	Wykonaj lub sprawdź łagodzenie ryzyka zgodnie z potrzebami. Wymagana akceptacja oceny ryzyka w ramach departamentu/działu.
1B, 1C, 2C, 2D, 3D, 3E, 4E	Niskie ryzyko	Opcjonalne łagodzenie lub sprawdzenie ryzyka.
1D, 1E, 2E	Nieistotne ryzyko	Akceptowalne na istniejącym poziomie. Nie wymaga złagodzenia ryzyka.

Dodatek 3 do Rozdziału 2
Ilustracja procedury ustalania priorytetów zagrożeń

<table>
<tr><th></th><th>OPCJA 1 (podstawowa)</th><th>OPCJA 2 (zaawansowana)</th></tr>
<tr><td>Kryteria</td><td>Priorytetyzacja kategorii najgorszej możliwej konsekwencji (dotkliwość incydentu) zagrożenia</td><td>Priorytetyzacja kategorii indeksu ryzyka (dotkliwość i prawdopodobieństwo) najgorszej możliwej konsekwencji zagrożeń.</td></tr>
<tr><td>Metodologia</td><td>a) Przewidzieć najgorszą możliwą konsekwencję

b) przewidzieć klasyfikację prawdopodobieństwa tej konsekwencji, tj. czy będzie uznana za wypadek, poważny incydent, czy incydent?

c) zamknąć wnioskiem, że priorytetyzacja zagrożenia jest taka:
<table><tr><th>Przewidywane konsekwencje</th><th>Poziom zagrożenia</th></tr><tr><td>Wypadek
Poważny incydent
Incydent</td><td>Poziom 1
Poziom 2
Poziom 3</td></tr></table></td><td>a) Przewidzieć wielkość indeksu ryzyka (w oparciu o stosowną matrycę dotkliwości i prawdopodobieństwa) najgorszej możliwej konsekwencji zagrożenia (patrz Rys. 2-13 w tym rozdziale);

b) dla pokrewnej matrycy tolerancji ustalić kategorię tolerancji indeksu ryzyka (tj. nietolerowana, tolerowana lub akceptowalna) lub terminologię/kategoryzację równoważną

c) zamknąć wnioskiem, że priorytetyzacja zagrożenia jest taka:
<table><tr><th>Przewidywany wskaźnik/indeks ryzyka</th><th>Poziom zagrożenia</th></tr><tr><td>Nietolerowane
Tolerowane
Akceptowalne</td><td>Poziom 1
Poziom 2
Poziom 3</td></tr></table></td></tr>
<tr><td>Uwagi</td><td>Niniejsza opcja 1 uwzględnia tylko dotkliwość przewidywanej konsekwencji zagrożenia</td><td>Niniejsza opcja 2 uwzględnia dotkliwość i prawdopodobieństwo przewidywanej konsekwencji zagrożenia - bardziej wszechstronne kryterium niż opcja nr 1</td></tr>
</table>

Uwaga. – Z praktycznego punktu widzenia, dla uproszczenia systemu priorytetyzacji, opcja 1 byłaby łatwiejsza do realizacji niż opcja 2. Celem takiego systemu jest ułatwienie sortowania i priorytetyzacji zagrożeń dla działań łagodzenia ryzyka.

Po tym jak każdemu zagrożeniu zostanie nadany określony priorytet, stanie się jasnym, że może ono zostać posortowane jako zagrożenia na poziomie 1, 2 lub 3. Wówczas można będzie przypisać im priorytetowość lub baczenie według ich poziomu 1, 2 lub 3.

Rozdział 3
MIĘDZYNARODOWE NORMY I ZALECANE METODY POSTĘPOWANIA (SARPs) ICAO Z ZAKRESU ZARZĄDZANIA BEZPIECZEŃSTWEM

3.1. WSTĘP

3.1.1. Niniejszy Rozdział prezentuje przegląd międzynarodowych norm i zalecanych metod postępowania (SARPs) odnoszących się do zarządzania bezpieczeństwem, które początkowo były przyjęte w Załącznikach do Konwencji chicagowskiej: Załączniku 1 — Licencjonowanie personelu, Załączniku 6 — Eksploatacja statków powietrznych, Załączniku 8 — Zdatność do lotu statków powietrznych, Załączniku 11 — Służby ruchu lotniczego, Załączniku 13 — Badanie wypadków i incydentów statków powietrznych i Załączniku 14 — Lotniska. Niniejszy rozdział zawiera również informacje o nowym Załączniku 19 do Konwencji chicagowskiej, który się zajmuje odpowiedzialnościami w zakresie zarządzania bezpieczeństwem i jego procesami oraz konsoliduje nadrzędne zapisy dotyczące zarządzania bezpieczeństwem.

3.1.2. SARPs ICAO, dotyczące zarządzania bezpieczeństwem, zawierają wymagania wysokiego poziomu, które Państwa muszą wdrożyć by wypełnić swe obowiązki dotyczące zarządzania bezpieczeństwem, bezpośrednio związane z bezpieczną eksploatacją statków powietrznych lub ją wspierające. Postanowienia te skierowane są do dwu grup odbiorców: Państw i dostawców usług. W kontekście zarządzania bezpieczeństwem, termin „dostawca usług" odnosi się do każdej organizacji, od której wymaga się wdrożenia systemu zarządzania bezpieczeństwem (SMS), zgodnego ze strukturą SMS opracowaną przez ICAO. Dlatego też w niniejszym kontekście, termin *„safety prioviders"* (tj. organizacje zapewniające bezpieczeństwo) obejmuje:

a) zatwierdzone organizacje szkoleniowe, które są narażone na ryzyko dotyczące bezpieczeństwa podczas świadczenia swoich usług;

b) operatorów statków powietrznych (samolotów i śmigłowców) upoważnionych do prowadzenia międzynarodowego komercyjnego transportu lotniczego;

c) zatwierdzone organizacje obsługi technicznej świadczące usługi operatorom samolotów lub śmigłowców, uczestniczącym w międzynarodowym komercyjnym transporcie lotniczym;

d) organizacje odpowiedzialne za projekt typu i/lub produkcję statków powietrznych;

e) organizacje zapewniające służby ruchu lotniczego; oraz

f) operatorów certyfikowanych lotnisk.

3.1.3. Międzynarodowe normy i zalecane metody postępowania SARPs ICAO dotyczące zarządzania bezpieczeństwem wymagają także, by Państwa ustanowiły akceptowalny poziom bezpieczeństwa, zdefiniowany przez ich cele w zakresie bezpieczeństwa i wskaźniki jego wykonawstwa. Dalsze szczegóły dotyczące tych dwóch tematów zawarte są, odpowiednio, w Rozdziałach 4 i 5.

3.2. WYMAGANIA DOTYCZĄCE ZARZĄDZANIA BEZPIECZEŃSTWEM PRZEZ PAŃSTWO

3.2.1. Wymagania dotyczące zarządzania bezpieczeństwem przez Państwo zawierają specyfikacje dotyczące działania, personelu i procesów, będące bezpośrednią odpowiedzialnością Państw a niezbędne dla bezpieczeństwa transportu lotniczego. Wymagania te obejmują wprowadzenie i utrzymywanie Krajowego Programu Bezpieczeństwa (SSP) [w lotnictwie cywilnym]; zbieranie, analizę i wymianę danych dotyczących bezpieczeństwa oraz ochronę informacji dotyczących bezpieczeństwa.

3.2.2. SSP wymaga, by pewne funkcje były sprawowane przez Państwa, w tym wydawanie ustaw, przepisów, zasad i wytycznych mających na celu wspieranie bezpiecznego i skutecznego dostarczania podlegających ich nadzorowi produktów i usług lotniczych. Do celów tworzenia i utrzymywania programów SSP, ICAO opracowała ramę, która zawiera co najmniej cztery następujące komponenty a każdy z nich po jedenaście podstawowych elementów:

a) polityka i cele Państwa w zakresie bezpieczeństwa;

b) krajowe zarządzanie ryzykiem dotyczącym bezpieczeństwa;

c) zapewnienie bezpieczeństwa przez Państwo;

d) promowanie bezpieczeństwa przez Państwo.

Tabela 3-1 dostarcza streszczenie odnośników do krajowych wymogów w sferze bezpieczeństwa i ramę SSP, która była przyjęta w Załącznikach do Konwencji, dotyczące Międzynarodowego Lotnictwa Cywilnego. Dalsze wskazówki dotyczące wymogów programu SSP, jego ramy i akceptowalnego poziomu bezpieczeństwa są zamieszczone w Rozdziale nr 4.

3.3. WYMAGANIA DOTYCZĄCE ZARZĄDZANIA BEZPIECZEŃSTWEM PRZEZ DOSTAWCÓW USŁUG

3.3.1. SARPs ICAO obejmują również wymagania dotyczące wdrożenia SMS przez dostawców usług i operatorów lotnictwa ogólnego, jako elementu programu SSP każdego Państwa. SMS zapewnia środki do identyfikowania zagrożeń dotyczących bezpieczeństwa, wdrażania działań redukujących ryzyka w sferze bezpieczeństwa, monitorowania poziomu bezpieczeństwa i osiągania ciągłej poprawy działania bezpieczeństwa.

3.3.2. Rama SMS wymaga konkretnych działań i procesów, które muszą być realizowane przez dostawców usług lotniczych. Opracowana przez ICAO rama SMS zawiera cztery następujące komponenty, jak również dwanaście elementów leżących u podstawy tej ramy:

a) polityka bezpieczeństwa i jej cele;

b) zarządzanie ryzykiem w sferze bezpieczeństwa;

c) zapewnienie bezpieczeństwa; oraz

d) promocja bezpieczeństwa.

3.3.3. Międzynarodowi operatorzy lotnictwa ogólnego, używający dużych lub turboodrzutowych samolotów opisanych w Załączniku 6 do Konwencji chicagowskiej (Część II, Rozdział III), ustanowią i będą utrzymywać SMS, który jest odpowiedni do wielkości i złożoności działalności i który powinien, jako minimum, obejmować:

a) proces identyfikowania rzeczywistych i potencjalnych zagrożeń dotyczących bezpieczeństwa i oceniania ryzyka z nimi związanych;

b) proces opracowania i wdrożenia działań naprawczych niezbędnych do utrzymania akceptowalnego poziomu bezpieczeństwa; oraz

c) zapisy dotyczące ciągłego monitorowania i systematycznej oceny adekwatności i skuteczności działań w zarządzaniu bezpieczeństwem.

3.3.4. Tabela 3-2 zawiera podsumowanie odnośników do wymagań dotyczących zarządzania bezpieczeństwem przez dostawców usług i operatorów lotnictwa ogólnego, w tym do ramy SMS, pierwotnie przyjętej w Załącznikach do Konwencji o międzynarodowym lotnictwie cywilnym. Dalsze wskazówki dotyczące wymagań wobec dostawców usług i ramy SMS są zamieszczone w Rozdziale 5.

Tabela 3-1. Podsumowanie odnośników do wymagań dotyczących zarządzania bezpieczeństwem przez Państwo i do ramy SSP, wstępnie przyjętych w Załącznikach do Konwencji chicagowskiej

Źródło		Temat
Załączniki do Konwencji chicagowskiej	Zapis	
Załącznik 1 Załącznik 6, Część I, II i III	Definicje	Krajowy Program Bezpieczeństwa (SSP)
Załącznik 6, Część I	3.3.1 i 8.7.3.1	Ustanowienie SSP
Załącznik 6, Część III	1.3.1	
Załącznik 8	5.1	
Załącznik 11	2.27.1	
Załącznik 13	3.2	
Załącznik 14	1.5.1	
Załącznik 6, Część I	3.3.2 i 8.7.3.2	Akceptowalny poziom koncepcji działania bezpieczeństwa
Załącznik 6, Część III	1.3.2	
Załącznik 8	5.2	
Załącznik 11	2.27.2	
Załącznik 14	1.5.2	
Załącznik 13	5.12	Ochrona zapisów z wypadków i incydentów
Załącznik 13	8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.9	Zbieranie, analiza i wymiana danych dotyczących bezpieczeństwa
Załącznik 1	załącznik C	Rama SSP - komponenty i elementy
Załącznik 6, Część I	załącznik I	
Załącznik 6, Część III	załącznik I	
Załącznik 8	załącznik do Części II	
Załącznik 11	załącznik D	
Załącznik 13	załącznik F	
Załącznik 14	załącznik C	
Załącznik 13	załącznik E	Wskazówki prawne dotyczące zabezpieczania informacji pobieranych z systemów gromadzenia i przetwarzania danych

Tabela 3-2. Podsumowanie odnośników do wymagań dotyczących zarządzania bezpieczeństwem przez dostawców usług i operatorów lotnictwa ogólnego, w tym do ramy SMS, wstępnie przyjętej w Załącznikach do Konwencji chicagowskiej

Źródło		*Temat*
Załączniki do Konwencji chicagowskiej	*Zapis*	
Załącznik 1 Załącznik 6, Część I, II i III	Definicja	System zarządzania bezpieczeństwem
Załącznik 11 Załącznik 13		
Załącznik 14, Tom I		
Załącznik 1	Załączniki 2, 4.1 i 4.2	Wymagania SMS dla zaaprobowanych organizacji szkoleniowych
Załącznik 6, Część I	3.3.3, 3.3.4, 8.7.3.3 i 8.7.3.4	Wymagania SMS wobec operatorów statków powietrznych i organizacji obsługi technicznej
Załącznik 6, Część II, Sekcja 3	3.3.2.1 i 3.3.2.2	Wymagania SMS wobec samolotów międzynarodowego lotnictwa ogólnego
Załącznik 6, Część III	1.3.3 i 1.3.4	Wymagania SMS wobec operatorów śmigłowców
Załącznik 8	5.3 i 5.4	Wymagania SMS wobec organizacji odpowiedzialnych za projekt typu i produkcję statku powietrznego (stosuje się od 14 listopada 2013)
Załącznik 11	2.27.3 i 2.27.4	Wymagania SMS wobec organizacji zapewniających służby ruchu lotniczego
Załącznik 14, Tom I	1.5.3 i 1.5.4	Wymagania SMS wobec operatorów certyfikowanych lotnisk
Załącznik 1	Dodatek 4	Rama SMS
Załącznik 6, Część I	Dodatek 7	
Załącznik 6, Część III	Dodatek 4	
Załącznik 11	Dodatek 6	
Załącznik 14, Tom I	Dodatek 7	

3.4. Nowy Załącznik 19 do Konwencji chicagowskiej ZARZĄDZANIE BEZPIECZEŃSTWEM

3.4.1. Potrzeba stworzenia jednostkowego Załącznika, dedykowanemu odpowiedzialnościami za zarządzanie bezpieczeństwem, była zarekomendowana podczas Konferencji Dyrektorów Generalnych Lotnictwa Cywilnego dotyczącej Globalnej Strategii Bezpieczeństwa Lotniczego, która odbyła się w Montrealu w dniach 20-22 marca 2006 r. (DGCA/06) i Konferencji Bezpieczeństwa Wysokiego Szczebla, która również odbyła się w Montrealu w dniach 29 marca-1 kwietnia 2010 r. (HLSC/2010).

3.4.2. Zgodnie z mandatem Konferencji, Komisja Żeglugi Powietrznej (ANC) zgodziła się powołać Panel Zarządzania Bezpieczeństwem (Safety Management Panel - SMP) w celu wydania zaleceń do opracowania nowego Załącznika, dedykowanego odpowiedzialnościom za zarządzanie bezpieczeństwem i za procesy.

3.4.3. W lutym 2012 r. SMP zalecił przeniesienie przepisów zarządzania bezpieczeństwem z Załączników 1; 6, Część I, II, i III, także 8; 11; 13 i 14, Tom I (patrz Tabele 3-1 i 3-2) do nowego Załącznika 19 do Konwencji chicagowskiej. Większość tych wymagań została zmodyfikowana dla zachowania spójności i jasności przy jednoczesnym zachowaniu oryginalnych wymagań, dla których zostały one przyjęte.

3.4.4. Intencją postanowień Załącznika 19 do Konwencji chicagowskiej, zaproponowanych przez SMP, jest zharmonizować i wdrożyć zalecaną pragmatykę w zakresie zarządzania bezpieczeństwem przez Państwa i przez organizacje uczestniczące w działalności lotniczej. Konsekwentnie, Załącznik 19 do Konwencji chicagowskiej zawiera wymagania dotyczące zarządzania bezpieczeństwem przez Państwo, dostawców produktów i usług lotniczych, jak również operatorów samolotów używanych w międzynarodowych operacjach lotnictwa ogólnego. Wybrane, specyficzne dla danego sektora wymagania, dotyczące

bezpieczeństwa, pozostają w Załączniku dotyczącym dziedziny lub działalności każdego konkretnego dostawcy usług (np. wymagania wobec operatorów lotniczych co do programów analizowania danych o lotach pozostają zachowane w Części I Załącznika 6 do Konwencji chicagowskiej).

3.4.5. Gdy już Załącznik 19 do Konwencji chicagowskiej zostanie przyjęty, wpłynie on na wiele Załączników do Konwencji ICAO o międzynarodowym lotnictwie cywilnym. Dlatego też wprowadzone będą konsekwentne zmiany w Załącznikach do Konwencji chicagowskiej: 1 — *Licencjonowanie personelu*, 6 — *Eksploatacja statków powietrznych*, 8 — *Zdatność do lotu statków powietrznych*, 11 — *Służby ruchu lotniczego*, 13 — *Badanie wypadków i incydentów statków powietrznych* i 14 — *Lotniska*, wynikające z przyjęcia Załącznika 19 do Konwencji chicagowskiej, po to by uniknąć powtarzania wymagań.

3.4.6. Dostępność danych Załącznika 19 do Konwencji chicagowskiej jest niezależna od dat wprowadzenia istniejących przepisów o zarządzaniu bezpieczeństwem. A zatem, data wprowadzenie Załącznika 19 do Konwencji chicagowskiej nie ma wpływu na aktualne stosowanie programów SARPs dotyczących zarządzania bezpieczeństwem, które są zawarte w innych Załącznikach.

Rozdział 4
KRAJOWY PROGRAM BEZPIECZEŃSTWA (SSP)

4.1. WSTĘP

4.1.1. Niniejszy rozdział wprowadza cele i ramy dla wdrożenia Krajowego Programu Bezpieczeństwa (SSP). Omawia również znaczenie rozpoczęcia procesów dla utrzymania i oceny skuteczności samego programu SSP.

4.1.2. SSP jest systemem zarządzania pozwalającym Państwu na regulowanie bezpieczeństwa i administrowanie nim. Wdrażane SSP jest współmierne do wielkości i złożoności Krajowego systemu lotnictwa cywilnego i wymaga koordynacji ze strony wielu organów odpowiedzialnych za funkcje lotnicze w danym Państwie. Oto cele SSP:

a) zapewnienie posiadania przez Państwo minimalnych wymaganych ram prawnych;

b) zapewnienie harmonizacji pomiędzy krajowymi organami ustawodawczymi a organami administracyjnymi w zakresie ról pełnionych w zarządzaniu ryzykiem w obszarze bezpieczeństwa;

c) ułatwienie monitorowania i mierzenia zsumowanego poziomu bezpieczeństwa w branży lotniczej Państwa;

d) koordynowanie i stałe usprawnianie funkcji zarządzania bezpieczeństwem przez Państwo;

e) wspieranie skutecznego wdrażania SMS i interakcji z programem SMS dostawcy usług.

4.1.3. Zasady zarządzania bezpieczeństwem dają platformę do równoległego opracowania SSP przez Państwo a SMS - przez dostawców usług. Poprzez opracowanie ram legislacyjnych dla sfery bezpieczeństwa, Państwo obwieszcza wymogi programu SMS, wymagając od dostawców usług, by uruchomili własne umiejętności zarządzania bezpieczeństwem, co pozwoli na skuteczną identyfikację słabości systemowych w sferze bezpieczeństwa i na rozwiązywanie problemów bezpieczeństwa.

4.1.4. SMS dostawcy usług wymaga skutecznego nadzoru prawnego. Ponadto, SMS jest w znacznym stopniu systemem opartym na osiągach operacyjnych, wymagającym odpowiedniej wymiany informacji o bezpieczeństwie pomiędzy wewnętrznymi i zewnętrznymi stronami. Poprzez swoje funkcje w SSP, Państwo zapewnia zarówno nadzór nad funkcjami, jak i ułatwia wdrażanie scalania stosownych danych oraz ułatwia dzielenie się informacjami.

4.2. RAMA KRAJOWEGO PROGRAMU BEZPIECZEŃSTWA (SSP)

4.2.1. Są cztery komponenty, które tworzą fundamenty SSP. Każdy komponent podzielony jest na elementy, które składają się na procesy lub działania podejmowane przez Państwo w sferze zarządzania bezpieczeństwem. Tych jedenaście elementów łączy w sobie podejście nakazowe oraz podejście oparte na osiągach operacyjnych, wspomagając wdrożenie SMS przez dostawców usług. Tymi czterema komponentami i jedenastoma elementami ramy SSP są:

1. Polityka i cele Państwa w sferze bezpieczeństwa
   - 1.1. Krajowe ramy legislacyjne dla bezpieczeństwa
   - 1.2. Odpowiedzialność Państwa i jego funkcjonariuszy za bezpieczeństwo
   - 1.3. Badanie wypadków i incydentów
   - 1.4. Polityka zapewniania przestrzegania przepisów
2. Zarządzanie ryzykiem dotyczącym bezpieczeństwa przez Państwo
   - 2.1. Krajowe wymagania wobec systemu SMS dostawcy usług
   - 2.2. Zgoda na realizowanie bezpieczeństwa przez dostawcę usług
3. Zapewnianie bezpieczeństwa przez Państwo
   - 3.1. Nadzór nad bezpieczeństwem
   - 3.2. Zbieranie, analizowanie i wymiana danych dotyczących bezpieczeństwa
   - 3.3. Ukierunkowanie nadzoru na obszary największych potrzeb i wymagających szczególnej uwagi, poprzez użycie danych
4. Promowanie bezpieczeństwa przez Państwo
   - 4.1. Szkolenia wewnętrzne, komunikacja i upowszechnianie informacji dotyczących bezpieczeństwa
   - 4.2. Szkolenia zewnętrzne, komunikacja i upowszechnianie informacji dotyczących bezpieczeństwa.

4.2.2. Oto krótki opis komponentów i elementów ramy programu SSP:

Komponent nr 1 systemu SSP. Polityka i cele państwa w zakresie bezpieczeństwa

4.2.3. Komponent polityki bezpieczeństwa Państwa i jej celów definiuje to jak Państwo będzie zarządzać bezpieczeństwem w całym swoim systemie lotniczym. Obejmuje on określenie obowiązków i odpowiedzialności różnych państwowych instytucji związanych z SSP, jak również szeroko pojmowanych celów, które trzeba osiągnąć poprzez SSP.

4.2.4. Polityka bezpieczeństwa Państwa i jej cele wyposażają kierownictwo i personel w wyraźnie postawione działania koncepcyjne, kierunki, procedury, środki zarządzania, dokumentację i procesy realizacji działań naprawczych, które utrzymują wysiłki państwowych organów lotnictwa cywilnego i innych państwowych organizacji na kursie. To pozwala Państwu zapewnić sobie przewodnictwo w sferze bezpieczeństwa w coraz bardziej złożonym i ciągle zmieniającym się systemie transportu powietrznego. Wytyczne dla opracowania expose w zakresie polityki bezpieczeństwa Państwa znajduje się w Dodatku 1 do niniejszego Rozdziału.

Element 1.1 programu SSP
Krajowe ramy legislacyjne bezpieczeństwa

Państwo ogłosiło krajowe ramy legislacyjne bezpieczeństwa i szczegółowe przepisy, zgodne z międzynarodowymi i krajowymi normami, które definiują, jak Państwo będzie prowadzić zarządzanie bezpieczeństwem. Ramy te obejmują udział krajowych organizacji lotniczych w konkretnych działaniach związanych z zarządzaniem bezpieczeństwem oraz ustanowienie ról, odpowiedzialności i powiązań pomiędzy tymi organizacjami. Państwo prowadzi okresowe przeglądy ram legislacyjnych bezpieczeństwa i szczegółowych przepisów, w celu zapewnienia czy są nadal aktualne i przydatne dla Państwa.

4.2.5. Krajowe ramy legislacyjne bezpieczeństwa muszą być ustanowione i aktualizowane w miarę potrzeb. Takie ramy obejmują wszystkie sektory lotnictwa i przynależne Państwu funkcje administracyjne i są zgodne ze standardami międzynarodowymi. Prawo wyraźnie definiuje role i odpowiedzialność każdej krajowej instytucji, która pełni funkcję ustawodawczą lub administracyjną. Jest możliwe, że niektóre ramy prawne mogą składać się z prawodawstw oddzielnych dla różnych ministerstw i że takie prawodawstwa mogły być opracowane niezależnie od siebie. Na przykład, ramy legislacyjne dla odpowiedzialności Państwa za bezpośrednią administrację i funkcjonowanie lądowisk i służb ATS mogła być opracowywana osobno na przestrzeni lat. Takie prawodawstwo może skupiać się na tych dwu sektorach z konsekwentnym naciskiem na elementy operacyjne i techniczne zapewniania takich usług. Ramy legislacyjne, przychylne działalności operacyjnej, mogą w sposób niewystarczający zajmować się koordynacją działań w sferze zarządzania bezpieczeństwem we wszystkich odnośnych instytucjach państwowych.

4.2.6. Mechanizm dla okresowego całościowego przeglądu krajowej ramy legislacyjnej zapewni stałe polepszanie prawodawstwa i korelacji między prawodawstwem Państwa i prawnymi wymaganiami operacyjnymi. Choć przegląd konkretnych wymagań operacyjnych będzie w zakresie odnośnych instytucji ustawodawczych, to niezbędną integracją i spójnością ustawodawstwa wyższego szczebla być może będzie musiała zająć się platforma koordynacyjna na poziomie krajowym, szczególnie tam gdzie dotyczy to wielu instytucji i ministerstw.

Element 1.2 programu SSP
Zakresy odpowiedzialności za bezpieczeństwo Państwa i rozliczanie się z nich

Odnośnie utworzenia i utrzymywania SSP, Państwo identyfikuje, definiuje i dokumentuje wymagania, zakresy obowiązków i ich rozliczanie. Tym zakresem są objęte dyrektywy jak planować, organizować, rozwijać, utrzymywać, kontrolować i stale usprawniać SSP w sposób spełniający krajowe cele w sferze bezpieczeństwa. Ten zakres zawiera również jasne obwieszczenie o zapewnieniu zasobów jakie są konieczne dla wdrażania SSP.

4.2.7. Początkowym obowiązkiem Państwa we wdrażaniu SSP jest wyznaczyć kogoś na dyrektora odpowiedzialnego za SSP *(accountable executive)* oraz jakąś instytucję państwową – dla administrowania programem SSP i koordynowania jego wdrożeniem i działaniem. Ten podmiot jest w tym dokumencie także nazywany organizacją lokowania programu SSP (*placeholder organization*).

4.2.8. W Państwach, w których w SSP jest zaangażowanych wiele instytucji legislacyjnych i administracyjnych, może trzeba będzie powołać też stosowny zespół ogólnokrajowy, w którym takie instytucje będą reprezentowane; taki zespół miałby służyć jako państwowa platforma do koordynowania SSP na bieżąco.

4.2.9. Osoba powołana na dyrektora odpowiedzialnego za SSP (*accountable executive*) oraz organizacja lokowania programu SSP (*placeholder organization*) zainicjują proces wdrażania SSP poprzez wyznaczenie zespołu ds. jego wdrożenia.

4.2.10. Proces wdrożenia, a następnie utrzymania ciągłej zdatności operacyjnej SSP, będzie musiał zostać zdefiniowany i udokumentowany. W systemie dokumentacji SSP powinien się znaleźć najważniejszy dokument SSP, który definiuje/opisuje SSP, a także powinny być inne dokumenty, formularze, SOP itp. dotyczące jego wdrożenia i działania.

4.2.11. Równocześnie z definicją odpowiedzialności za system zarządzania bezpieczeństwem i rozliczanie za jego realizację, występuje skoordynowany rozwój krajowej polityki w sferze bezpieczeństwa i jej obwieszczenie po całej krajowej ramie legislacyjnej i administracyjnej. Podobnie, rozległe cele krajowego systemu bezpieczeństwa są częścią tej misji bezpieczeństwa, kierowanych do istotnych instytucji Państwa. Ważne założenia dotyczące bezpieczeństwa mogą być następnie wsparte odpowiednimi wskaźnikami poziomu bezpieczeństwa odpowiednio ułatwiającymi ich ocenę lub pomiar.

Element 1.3 programu SSP
Badanie wypadków i zdarzeń

Państwo stworzyło niezależny proces badania wypadków i incydentów, którego wyłącznym celem jest zapobieganie wypadkom i incydentom, a nie przypisywanie winy lub odpowiedzialności. Takie badania stanowią wsparcie dla zarządzania systemem bezpieczeństwa w Państwie. W czasie funkcjonowania SSP, Państwo utrzymuje niezależność instytucji badającej wypadki i incydenty od innych krajowych instytucji lotniczych.

4.2.12. Z perspektywy programu SSP, funkcja badania wypadków i incydentów jest zorientowana na administrowaniu nim na poziomie Państwa. Instytucja lub podmiot badający musi być funkcjonalnie niezależny od wszelkich innych instytucji, szczególnie od krajowej władzy lotnictwa cywilnego, której interesy mogą być sprzeczne z zadaniami powierzonymi instytucji prowadzącej dochodzenie. Fundamentalnym uzasadnieniem za niezależnością tej funkcji od funkcji innych instytucji jest to, że przyczyny wypadków mogą być powiązane z czynnikami legislacyjnymi lub z programem SSP.

4.2.13th Niektóre Państwa mogą nie dysponować niezbędnymi środkami by wywiązywać się ze swych obowiązków w obszarze dochodzeniowym. Dla takich Państw, przystąpienie do regionalnej instytucji badania wypadków i zdarzeń (*Regional Accident and Investigation Organization* (RAIO)) byłoby odpowiednim rozwiązaniem pozwalającym na spełnienie założenia niezależnego procesu dochodzeniowego. W związku z tym, zwraca się uwagę na Podręcznik Regionalnej Organizacji ds. Badania Wypadków i Incydentów *Manual on Regional Accident and Incident Investigation Organization* (ICAO, Doc 9946).

Element 1.4 programu SSP
Polityka egzekwowania przepisów

Polityka zapewniania przestrzegania przepisów – państwo ogłosiło politykę zapewniania przestrzegania przepisów, określając warunki i okoliczności, w których podmiotom prowadzącym działalność lotniczą, w ramach SMS danego podmiotu i za aprobatą właściwej władzy krajowej, zezwala się na prowadzenie wewnętrznego postępowania przy zdarzeniach związanych z niektórymi naruszeniami. Polityka ta określa również warunki i okoliczności, w jakich naruszenia podlegają określonej procedurze egzekucyjnej.

4.2.14. Tak jak w przypadku każdej innej narodowej legislacji, można oczekiwać, że rama legislacji lotniczej może zawrzeć podstawowy zapis o wymuszaniu działań. Podstawowy zapis prawny sprowadzałby się zapewne tylko do omówienia zakresu kar za naruszenia. W zamierzeniu, w środowisku SSP-SMS, działania wymuszające i procedury, czy to u pojedynczego dostawcy usług czy na poziomie Państwa (CAA), powinny zostać ulepszone tak by zawierały zapisy, które łagodzą charakter i zakres działań egzekucyjnych lub dyscyplinarnych, stosownie do faktycznych warunków i okoliczności otaczających naruszenie lub akt niezgodnego działania. Zamierzeniem takiego ulepszenia jest zapewnienie niezbędnego rozróżnienia pomiędzy celowym/poważnym naruszeniem a niezamierzoną pomyłką/ błędem.

4.2.15. Aby takie ulepszenie mogło zaistnieć, Państwo wskaże taki zamiar poprzez swą politykę zapewniania przestrzegania przepisów i procedur. Równocześnie, Państwo może potrzebować sformalizować wymóg by jego dostawcy usług posiadali swoje wewnętrzne procedury dyscyplinarne zawierające ulepszenia równorzędne. To może implikować, że po dostawcach usług oczekuje się iż już mają własny, akceptowalny proces rutynowego zarządzania bezpieczeństwem/jakością poprzez stosowanie wewnętrznej polityki dyscyplinarnej i procedur. Państwo wskazałoby, że w pewnych warunkach i okolicznościach można się spodziewać interwencji legislacyjnej poprzez którą krajowy organ CAA zajmie się procesem badania konkretnego naruszenia lub niezgodnego działania.

Komponent nr 2 programu SSP. Krajowe zarządzanie ryzykiem

4.2.16. Komponent zarządzania ryzykiem bezpieczeństwa krajowego obejmuje opracowanie wymagań SMS zapewniające, że każdy podmiot lotniczy państwa wdroży niezbędne procesy identyfikacji zagrożenia i zarządzania ryzykiem. Część tych wymagań uwzględnia mechanizm uzgadniania z pojedynczymi podmiotami lotniczymi akceptowalnych poziomów bezpieczeństwa, które mają osiągnąć poprzez swój SMS.

4.2.17. Poza upewnieniem się, że dostawcy usług są zaangażowani w skuteczną identyfikację zagrożeń i zarządzanie ryzykiem poprzez realizację wymagań SMS, Państwo może również wprowadzić do swych własnych działań w sferze przepisów i programu SSP zasady zarządzania ryzykiem dotyczącym bezpieczeństwa. Tworzenie, między innymi, przepisów, wybór wskaźników poziomu bezpieczeństwa SSP i ich celu oraz poziomów alarmowych, jak również priorytetyzacja programu śledzenia, to procesy, które można dopracować przez przyjęcie podejścia bazującego na ryzyku i pozyskanych danych.

4.2.18. Znaczne ryzyka, które stają się widoczne poprzez analizę wewnętrznie generowanych danych dotyczących bezpieczeństwa i powiązanych wskaźników poziomu bezpieczeństwa u pojedynczego dostawcy usług, mogą wymagać skoordynowania lub uzgodnienia z krajowym organem stanowiącym przepisy lotnicze co do podjęcia stosownej akcji łagodzącej, szczególnie tam gdzie takie ryzyka mogą uderzyć w innych dostawców usług lub innych zainteresowanych.

Element 2.1 programu SSP
Wymagania bezpieczeństwa dotyczące SMS dostawców usług

Państwo ustanawia środki decydowania o tym jak dostawcy usług będą identyfikować zagrożenia i zarządzać ryzykiem. Obejmują one wymagania, szczegółowe przepisy operacyjne i politykę wdrażania SMS u dostawcy usług. Takie wymagania, szczegółowe przepisy operacyjne i polityka wdrażania są przeglądane okresowo dla pewności, że pozostają dla dostawcy usług istotnymi i odpowiednimi.

4.2.19. Państwo ustanawia wymagania bezpieczeństwa dla SMS dostawców usług poprzez obwieszczenie przepisów, które definiują wymagane komponenty i elementy ramy programu SMS. W ramach tej ramy, skuteczne wdrożenie komponentu zarządzania ryzykiem (SRM) zapewni to, że dostawcy usług będą identyfikować zagrożenia i będą zarządzać pokrewnym ryzykiem. Szczegóły procedur każdego dostawcy usług dotyczące identyfikacji zagrożenia i zarządzania ryzykiem będą współmierne do złożoności każdej organizacji i będą odpowiednio odzwierciedlane w jego dokumentacji SMS. Od organizacji nie objętych uregulowaniami kontraktu, takich jak podwykonawcy, organizacja o zatwierdzonym programie SMS może zażądać uruchomienia procesów identyfikacji zagrożenia i zarządzania ryzykiem, tam gdzie będzie miało to zastosowanie. Jeżeli podwykonawca ma zaakceptowany SMS konieczne będzie uzgodnienie niezbędnej integracji.

4.2.20. Wymagania prawne krajowego programu SMS i związane z nimi materiały zawierające wytyczne podlegają okresowemu przeglądowi po to, by uwzględnić informacje zwrotne z organizacji pracujących na rzecz lotnictwa, jak również aktualny status, stosowalność programów ICAO SMS SARPs oraz materiały zawierające wytyczne.

Element 2.2 programu SSP.
Uzgadnianie poziomu bezpieczeństwa podmiotu lotniczego

Państwo uzgadnia z poszczególnymi dostawcami usług działanie ich programów SMS. Uzgodnione działanie SMS-a poszczególnych dostawców usług jest przeglądane okresowo, by upewnić się, iż jego SMS pozostaje istotnym i odpowiednim dla dostawców usług.

4.2.21. Jako część procesu akceptowania SMS, proponowane przez dostawcę usług wskaźniki działania bezpieczeństwa (SPI) i ich cele oraz alarmy są przeglądane i podlegają akceptacji odpowiedniej instytucji legislacyjnej Państwa. Istnieje również możliwość, by plan wdrożenia SMS był akceptowany przez Państwo, dopuszczając by zaakceptowanie wskaźników SPI dostawcy usług było w którejś późniejszej fazie procesu wdrażania jego SMS. W każdym razie, pełna akceptacja SMS wymaga by instytucja regulująca uznała, że proponowane wskaźniki SPI są odpowiednie i stosowne do indywidualnych czynności lotniczych dostawcy usług.

4.2.22. Istnieje możliwość, że ten proces uzgadniania działania bezpieczeństwa będzie mógł uwzględniać przeprowadzenie przez dostawcę usług ocen bezpieczeństwa lub działań łagodzących ryzyko. Taka możliwość może powstać jako skutek ujawnienia konkretnego ryzyka ze źródeł takich, jak dostawców usług, przemysłu, Państwa lub z danych światowych.

4.2.23. Należy dokonać okresowego przeglądu wskaźników SPI każdego dostawcy usług i powiązanych z nimi celów i ustawień alarmowych. Taki przegląd powinien obejmować działanie i skuteczność każdego SPI i powiązanego z nim celu oraz ustawień alarmowych. Wszelkie konieczne przystosowywania do wcześniej uzgodnionych SPI, także celu i ustawień alarmowych muszą być uzasadniane odpowiednimi danymi bezpieczeństwa i muszą być odpowiednio dokumentowane.

Komponent nr 3 programu SSP. Zapewnianie bezpieczeństwa przez państwo

4.2.24. Państwo zapewnia bezpieczeństwo poprzez nadzorowanie i śledzenie dostawców usług oraz przez wewnętrzny przegląd swych procesów legislacyjnych i administracyjnych. Zajmuje się także ważną rolą danych dotyczących bezpieczeństwa, ich zbieraniem, analizą i dzieleniem się nimi. Krajowe programy śledzenia powinny się opierać na pozyskiwanych danych, tak aby zasoby Państwa można skupiać i kierować priorytetowo na obszary największego ryzyka lub trosk.

Element 3.1 programu SSP
Nadzorowanie bezpieczeństwa

Państwo ustanawia mechanizmy zapewniania skutecznego monitorowania ośmiu krytycznych elementów funkcji doglądania bezpieczeństwa. Państwo ustanawia również mechanizmy zapewniania, by identyfikacja zagrożeń i zarządzanie ryzykiem dotyczącym bezpieczeństwa przez dostawców usług trzymały się ustaleń prawnych (wymagań, szczegółowych przepisów operacyjnych i polityki wdrożeniowej). Mechanizmy te obejmują inspekcje, audyty i pomiary mające zapewnić, by prawne narzędzia kontroli ryzyka dotyczące bezpieczeństwa były właściwie wpisane w SMS dostawcy usług oraz żeby były tak używane jak je zaprojektowano oraz żeby takie narzędzia prawne oddziaływały na ryzyko dotyczące bezpieczeństwa w sposób zamierzony.

4.2.25th Wdrożenie ICAO SARPs kładzie podwaliny krajowej strategii bezpieczeństwa w lotnictwie. Element 3.1 krajowego programu bezpieczeństwa (SSP) dotyczy metod stosowanych przez Państwo dla skutecznego monitorowania tego jak jest tworzony i wdrażany krajowy system nadzorowania bezpieczeństwa. Szczegółami omówienia elementów krytycznych krajowego systemu nadzorowania bezpieczeństwa zajmuje się ICAO Doc 9734. AN/959 Podręcznik nadzoru nad bezpieczeństwem. Wydanie drugie – 2006, Część A, Utworzenie i zarządzanie systemem nadzoru bezpieczeństwa danego państwa (Safety Oversight Manual. Second Edition — 2006. Part A. The Establishment and Management of a State's Safety Oversight System).

4.2.26. Krajowy system nadzorowania bezpieczeństwa obejmuje zobowiązania związane z pierwszym zatwierdzeniem i ciągłym śledzeniem swych dostawców usług lotniczych w celu zapewnienia zgodności z krajowymi przepisami, opracowanymi zgodnie z ICAO SARPs.

Uwaga. – Proces wstępnego zatwierdzenia obejmuje państwową autoryzację, certyfikację lub wyznaczenie dostawców usług.

4.2.27. Proces wstępnego zatwierdzenia obejmuje państwową autoryzację, certyfikację lub wyznaczenie dostawców usług, proces pierwszego zatwierdzenia, upoważnienia, certyfikacji lub wyznaczenia dostawcy usług przez Państwo obejmuje zaakceptowanie planu wdrożenia SMS tej organizacji. Pewne elementy planu wdrożenia SMS-a dostawcy usług już u niego będą w momencie wstępnego zatwierdzania organizacji, podczas gdy inne elementy będą wdrożone po opisanej w Rozdziale 5 realizacji fazowej.

4.2.28. Zobowiązania Państwa do śledzenia są wykonywane poprzez audyty i inspekcje i mają na celu zapewnić utrzymywanie przez swych dostawców usług odpowiedniego poziomu zgodności z przepisami oraz tego by ich działania związane z lotnictwem były wykonywane bezpiecznie. Zobowiązania Państwa do śledzenia obejmują również akceptowanie systemu SMS, wdrożonego przez każdego swego aktualnego dostawcę usług oraz okresową ocenę działania programu SMS.

4.2.29. Tam gdzie konieczne, dla potrzeb oceny i decydowania/rozwiązywania problemów, działania Państwa w monitorowaniu i przeglądaniu, w tym zalecane odnośne akcje są koordynowane na platformie koordynacyjnej krajowego SSP.

Element 3.2 programu SSP
Zbieranie, analizowanie i wymienianie się danymi dotyczącymi bezpieczeństwa

Państwo ustanawia mechanizmy chwytania i składowania danych o zagrożeniach i ryzykach, zarówno na poziomie indywidualnym jak i na krajowym poziomie scalania. Państwo ustanawia również mechanizmy budowania informacji z danych które ma na składzie; ma też mechanizmy dla aktywnej wymiany informacji z dostawcami usług i/lub innymi Państwami.

4.2.30. Poprzez składanie obowiązkowych i dobrowolnych zgłoszeń Państwo stworzyło system zbierania danych dotyczących bezpieczeństwa i ich przetwarzania (SDCPS), aby zapewnić wykrywanie, przechowywanie i scalanie w jednym miejscu danych dotyczących wypadków, zdarzeń i zagrożeń. Po to by dostawcy usług raportowali wypadki, poważne incydenty i wszelkie inne incydenty, które Państwo uznało za podlegające zgłoszeniu, system powinien być przez Państwo wsparty wymaganiami wobec dostawców usług. Należy stosownie rozgraniczać zgłoszenia na wypadki, zdarzenia i zagrożenia. Podobnie, istnieje różnica między systemami obowiązkowego (wymóg ustawowy zgłaszania) i dobrowolnego zgłaszania, w tym wymóg odpowiedniej poufności w systemie dobrowolnym. Dodatek 2 zawiera wytyczne dotyczące krajowego, dobrowolnego systemu zgłaszania, a Dodatek 3 – dla przykładu krajowej procedury zgłaszania obowiązkowego.

4.2.31. Wykrywanie danych o wypadkach i incydentach podlegających zgłoszeniu powinno być dokumentowane odpowiednimi raportami. Przychodzące dobrowolne raporty mogą wymagać procesu dalszej oceny ryzyka i procesu łagodzenia, odpowiednio, na poziomie dostawcy usług lub krajowego CAA. Różne typy danych o bezpieczeństwie mogą być konsolidowane, odpowiednio, w obrębie scentralizowanego SDCPS, lub mogą być gromadzone i archiwizowane w obrębie zintegrowanych modułów rozparcelowanej sieci SDCPS.

4.2.32. Państwo ustanowiło również procedury dla budowania i przetwarzania informacji ze scalonych, składowanych danych i dla wymiany informacji dotyczących bezpieczeństwa z dostawcami usług i/lub innym Państwami. Dostępność tych źródłowych

danych o bezpieczeństwie dla Państwa pozwala na opracowanie wskaźników bezpieczeństwa dla SSP, takich jak wielkości wypadków i incydentów. Określone wskaźniki bezpieczeństwa razem z ich celem i nastawami alarmowymi będą służyć jako krajowy mechanizm mierzenia i monitorowania (ALoSP). Dalsze szczegóły dotyczące tworzenia wskaźników bezpieczeństwa są od 4.3.5.1 do 4.3.5.12 i Dodatek 4 do niniejszego Rozdziału.

4.2.33. Dla zapewnienia stałego dostępu do danych bezpieczeństwa, szczególnie z systemów dobrowolnego powiadamiania, SDCPS powinien zapewnić odpowiednią ochronę informacji dotyczącej bezpieczeństwa. Dodatek 5 podaje wytyczne dla ochrony informacji o bezpieczeństwie.

4.2.34. Jeśli chodzi o Państwa, w których wiele jest władz/organów odpowiedzialnych za regulowanie bezpieczeństwa, to powinna być ustanowiona odpowiednia koordynacja, integracja i dostępność do tych ich baz, które są pokrewne programowi SSP. Dotyczy to również Państw, w których proces badania wypadków jest realizowany przez organ niezależny od krajowej władzy lotniczej (CAA). Może trzeba będzie rozpatrzeć czy nie dać podobnych prerogatyw Państwom, w których pewne funkcje zarządzania bezpieczeństwem (włącznie z przetwarzaniem danych związanych z SSP) są realizowane w imieniu Państwa przez Regionalną Organizację Nadzorowania Bezpieczeństwa (RSOO) lub Regionalną Organizację Badania Wypadków i Incydentów.

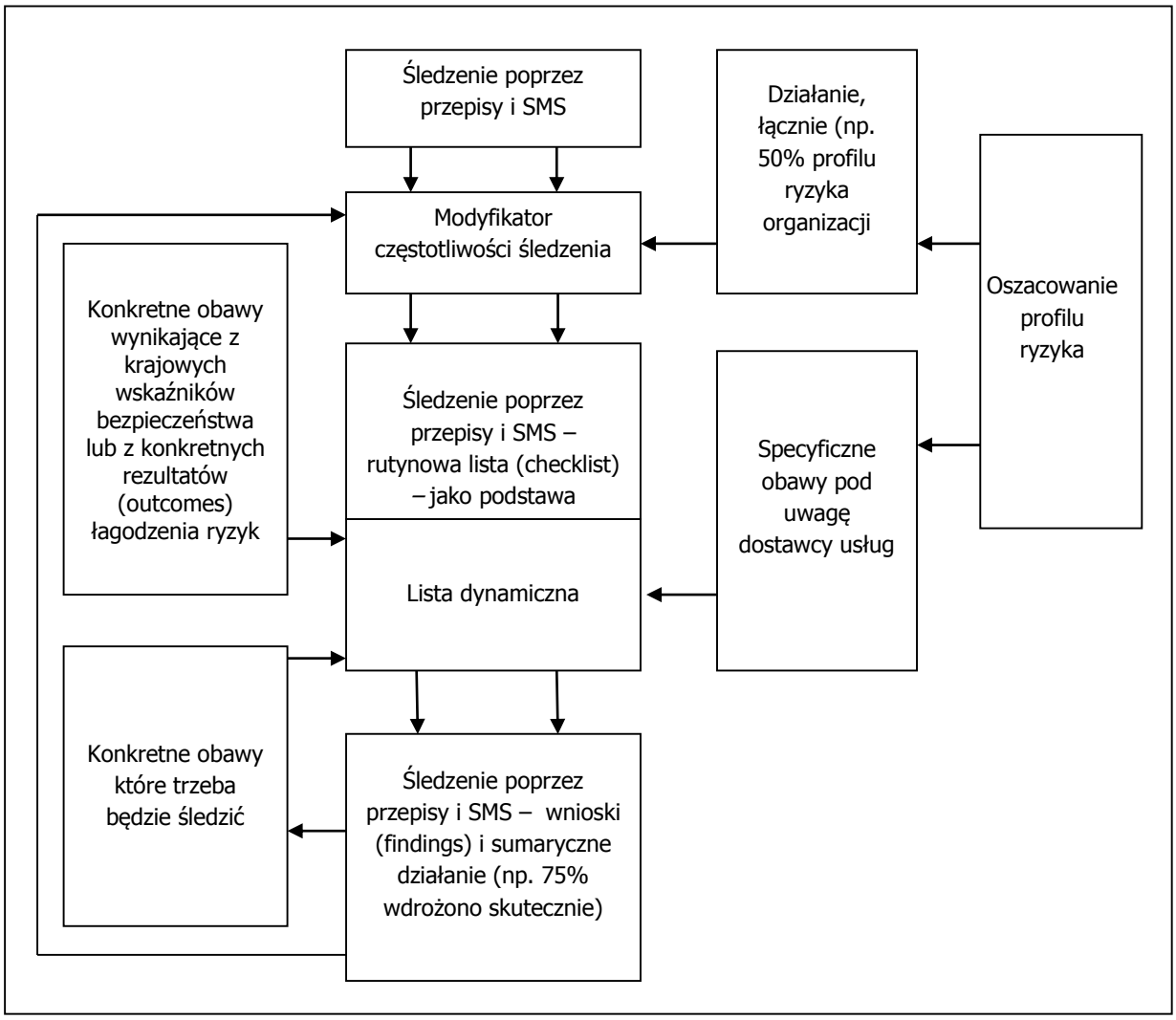
4.2.35. Krajowy SDCPS powinien zawierać procedury składania do ICAO raportów z badań wypadków i incydentów, co ułatwi zbieranie i wymianę informacji o bezpieczeństwie na skalę światową. Wytyczne dotyczące zawiadamiania o wypadkach i incydentach wg wymagań Załącznika 13 ICAO do Konwencji chicagowskiej można znaleźć w Załączniku 6 do Konwencji chicagowskiej, do niniejszego rozdziału.

Element 3.3 programu SSP
Ukierunkowanie nadzorowania – opartego na danych o bezpieczeństwie – na obszary wymagające większej troski lub mające większe potrzeby

Państwo ustanawia procedury na faworyzowanie programów inspekcji, audytów oraz badań na rzecz obszarów wymagających większej troski lub mających większe potrzeby - zidentyfikowane poprzez analizę danych o zagrożeniach, ich konsekwencjach operacyjnych i oszacowanym ryzyku.

4.2.36. Typowe programy nadzoru, dozoru lub inspekcji są ciągle i niezmiennie stosowane wobec podmiotów lotniczych, bez mechanizmów dopasowania częstotliwości lub zakresu czynności nadzoru. Środowisko zarządzania bezpieczeństwem pozwala na bardziej dynamiczną ocenę poziomu bezpieczeństwa. W ramach SSP, wymagane programy nadzoru powinny uwzględniać mechanizmy pozwalające na dopasowanie zakresu lub częstotliwości nadzoru do aktualnego poziomu bezpieczeństwa. Ustalenie priorytetów nadzoru w oparciu o ryzyko ułatwi przydzielenie zasobów w odniesieniu do obszarów o większym ryzyku, zagrożeniu lub potrzebie. Dane użyte dla dostosowania nadzoru mogą obejmować wskaźniki poziomu bezpieczeństwa powiązane z konkretnymi sektorami działalności lotniczej, ale także wyniki z poprzednich inspekcji lub audytów u pojedynczych podmiotów lotniczych. W tym celu konieczne byłoby ustalenie kryteriów dla obliczenia wyników (np. % skutecznej zgodności) każdego ukończonego audytu.

4.2.37. Bardziej wszechstronna koncepcja nadzoru oparta na ryzyku może uwzględniać zewnętrzne dane wejściowe ryzyka dotyczącego bezpieczeństwa, spoza samego programu nadzoru. Wkład dla dodatkowej częstotliwości nadzoru/modyfikatora zakresu danych wejściowych może pochodzić z (np.) programu oceny profilu ryzyka organizacji (ORP). (Patrz Rozdział 2, Dodatek 1 w sprawie informacji o koncepcji oceny profilu ryzyka organizacji). Dodatkowy wkład/zawartość mogą pochodzić z krajowego SDCPS lub wskaźników poziomu bezpieczeństwa. Przed wdrożeniem zmian w nadzorze należy podjąć odpowiednie współdziałanie z podmiotem lotniczym. Struktura rozszerzonego nadzoru opartego na danych bezpieczeństwa i koncepcji nadzoru opartego na ocenie ryzyka przedstawiona jest na Rys. 4-1.



Rys. 4-1. Dane o bezpieczeństwie i koncepcja śledzenia w oparciu o ryzyko

Komponent nr 4 programu SSP. Promowanie bezpieczeństwa przez Państwo

4.2.38. Promowanie bezpieczeństwa obejmuje ustanowienie przez Państwo wewnętrznych i zewnętrznych procesów dla zapewnienia lub ułatwienia przeprowadzania szkoleń z zakresu bezpieczeństwa, komunikacji i upowszechniania informacji dotyczących bezpieczeństwa.

Element 4.1 programu SSP
Szkolenia wewnętrzne, komunikacja i upowszechnianie informacji dotyczących bezpieczeństwa

Państwo zapewnia szkolenia i sprzyja świadomości bezpieczeństwa oraz utrzymuje dwustronną wymianę informacji istotnych z punktu widzenia bezpieczeństwa, wspierającą rozwój kultury korporacyjnej, która sprzyja skutecznemu i wydajnemu SSP.

4.2.39. Krajowe instytucje legislacyjne, odpowiedzialne za różne sektory lotnictwa, jak i inne niezależne podmioty administracyjne, takie jak komisja badania wypadków, powinny mieć do swych odnośnych ról podejście zintegrowane. Dlatego, jest rzeczą ważną zapewnić istnienie kanału dedykowanego komunikacji w sprawach bezpieczeństwa między ww. i, szczególnie, z instytucją w której jest SSP ma miejsce. Dokument SSP i związane z nim bezpieczeństwo Państwa i polityka egzekucyjne są fundamentalne dla integracji szkolenia, komunikacji i upowszechniania odnośnej informacji. Wszystkie inne późniejsze strategie operacyjne SSP, w tym harmonizowane wymagania SMS i nadzorowanie odnośnych dostawców usług,

organizacje powinny sobie przekazywać wiedzę, informować się o nich i je koordynować. Takie podejście pozwoli na uniknięcie tworzenia sprzecznych wymagań dla SMS lub kryteriów nadzoru/akceptacji dotyczących różnych sektorów lotnictwa.

4.2.40. Wewnętrzne programy szkolenia w zakresie bezpieczeństwa dla personelu realizującego różne obowiązki związane z SMS powinny być skoordynowane pomiędzy różnymi instytucjami krajowymi. W pierwszej kolejności szkoleniem z zakresu SSP i SMS powinien być objęty personel zajmujący się wdrożeniem lub nadzorowaniem tych programów, szczególnie inspektorzy operacyjni terenowi, którzy będą się zajmować ustalaniem kryteriów akceptowania programów SMS i innymi sprawami działania bezpieczeństwa. Zakres materiałów zapoznawczych z programami SSP i SMS i szkoleniowych będzie ewoluować tak, aby odzwierciedlać aktualne procesy SSP danego Państwa do chwili ich pełnego wdrożenia. Pierwsze szkolenia SSP i SMS można ograniczyć do podstawowych elementów ramy SSP/SMS i materiałów wiodących, takich jak w kursach szkoleniowych ICAO SSP/SMS.

Element 4.2 programu SSP
Szkolenia zewnętrzne, komunikacja i upowszechnianie informacji dot. bezpieczeństwa

Państwo zapewnia szkolenia, promuje świadomość zagrożeń dla bezpieczeństwa oraz dwustronną komunikację w zakresie informacji dotyczących bezpieczeństwa, po to, by wśród dostawców usług wspierać rozwój kultury korporacyjnej, co sprzyja skuteczności i wydajności SMS.

4.2.41. Państwo powinno mieć odpowiednią platformę komunikacji, lub medium, aby ułatwić wdrożenia SMS. Może to być medium zintegrowane dla dostawców usług wszystkich sektorów lotnictwa danego Państwa lub dedykowany im przez odpowiednią organizację legislacyjną kanał pozostający ściśle pod jej jurysdykcją. Zasadniczymi treściami dla takiego zewnętrznego SMS i komunikacji dotyczącej bezpieczeństwa są wymogi SMS i materiałów wiodących. Dostawcom usług należy także udostępnić dokumentację krajowego SSP i związaną z nim politykę bezpieczeństwa oraz politykę egzekwowania. Takie zewnętrzne kanały komunikacji też można ulepszyć tak, aby objęły inne zagadnienia związane z bezpieczeństwem. Zaleca się stworzenie komunikacji dwukierunkowej pozwalającej na otrzymywanie informacji zwrotnych z branży.

4.2.42. Tam gdzie jest to możliwe lub odpowiednie, Państwo powinno także ułatwić dostawcom usług naukę lub szkolenie z zakresu SMS.

4.3. PLANOWANIE WDROŻENIA PROGRAMU SSP

4.3.1. Informacje ogólne

Krajowy SSP musi odpowiadać wielkością i złożonością systemowi lotnictwa i może wymagać koordynacji ze strony wielu lotniczych organizacji legislacyjnych, odpowiedzialnych za poszczególne sektory. Wdrożenie jakiegoś SSP nie zmienia ról organizacji lotniczych Państwa ani normalnej współpracy pomiędzy nimi. Wręcz przeciwnie, to ulepsza ich kolektywne funkcje prawne/administracyjne i możliwości działania na rzecz Państwa. Większość Państw ma już istniejące procesy, które spełniają oczekiwania niektórych elementów SSP.

Zadaniem jest skonsolidowanie i ulepszenie tych istniejących procesów z dodatkowymi elementami działania systemu i elementami opartymi na ryzyku, by stworzyć ramę zintegrowanego zarządzania bezpieczeństwem. Taka rama SSP umożliwi również branży/przemysłowi skutecznie wdrożyć SMS u siebie i go doglądać. Niniejszy paragraf podkreśla niektóre ważne względy za wdrożeniem SSP.

4.3.2. Opis systemu prawnego

Przegląd systemu prawnego jest częścią procesu planowania wdrożenia SSP.

Taki przegląd powinien zawierać opis tego, co następuje:

a) ramę istniejącego w lotnictwie porządku prawnego, od poziomu Ministerstwa do różnych organizacji prawnych lub administracyjnych;

b) role i odpowiedzialności różnych organizacji w odniesieniu do zarządzania bezpieczeństwem;

c) platformę lub mechanizm koordynowania programem SSP wśród ww. organizacji;

d) mechanizm wewnętrznego przeglądu bezpieczeństwa/jakości na poziomie Państwa i w każdej organizacji.

W dokumencie SSP należy zamieścić strukturę organizacyjną /tablicę krajowej instytucji legislacyjnej i administracyjnej.

4.3.3. Analiza luk

Przed opracowaniem planu wdrożenia SSP potrzebna jest analiza luk w istniejących strukturach krajowych i procesach; potrzeba porównania z ramą ICAO SSP dla dokonania oceny żywotności i dojrzałości odnośnych elementów SSP. Elementy

lub procesy zidentyfikowane w analizie luk jako wymagające podjęcia działań stanowią podstawę planu wdrożenia SSP. Dalsze wytyczne dotyczące procesu analizy luk SSP można znaleźć w Dodatku 7 do niniejszego Rozdziału.

4.3.4. Plan wdrożenia SSP

Tak jak w przypadku wdrożenia każdego większego projektu, wdrożenie SSP wymaga wykonania wielu zadań i podzadań w określonej ramie czasowej. Liczba zadań, jak i zakres każdego z nich, uzależniona jest od aktualnej dojrzałości krajowego systemu nadzoru bezpieczeństwa. Celem procesu wdrożenia jest sukcesywne ulepszanie istniejących procesów zarządzania bezpieczeństwem, administrowania i nadzorowania. Faworyzowane są właściwe zadania i są one dokumentowane w format odpowiedni dla stopniowego wdrożenia. Plan implementacji SSP, razem z opracowaniem dokumentu SSP najwyższej rangi, stanowią fundament pozwalający Państwu na stopniowe ulepszanie swych procesów zarządzania bezpieczeństwem, administrowania i doglądania. Te dwa kluczowe dokumenty muszą być łatwo dostępne dla całego odnośnego personelu w organizacji, aby zwiększyć świadomość znaczenia SSP i postępu jego wdrażania. Dalsze wytyczne dotyczące postępów w planie wdrożenia SSP zawarte są w pkt 4.4 oraz w Dodatku 7 do niniejszego Rozdziału.

4.3.5. Wskaźniki bezpieczeństwa

Akceptowalny poziom realizacji bezpieczeństwa

4.3.5.1. Koncepcja akceptowalnego poziomu realizacji bezpieczeństwa uzupełnia tradycyjne podejście do doglądania bezpieczeństwa, które skupia się przede wszystkim na zachowaniu nakazanej przepisami zgodności z podejściem opartym na realizacji bezpieczeństwa, która definiuje faktyczne poziomy realizowania bezpieczeństwa w ramach nakazanego SSP.

Dla celów niniejszego podręcznika przyjmuje się, że ALoSP jest akceptowalnym poziomem realizowania bezpieczeństwa Państwa, zdefiniowanym przez wskaźniki poziomu bezpieczeństwa krajowego SSP i przez powiązane z nimi poziomy docelowe i alarmowe. Krajowy ALoSP powinien być zgodny z celami i założeniami polityki bezpieczeństwa Państwa.

4.3.5.2. Kryteria krajowego ALoSP mogą się różnić w zależności od konkretnego kontekstu systemu lotniczego danego Państwa i dojrzałości jego systemu doglądania bezpieczeństwa. Celem priorytetowym jest osiągnięcie zgodności z wymaganiami ICAO i zredukowanie liczby brzemiennych w skutki wydarzeń tam, gdzie się pojawiają. Ten cel będzie pozostawał priorytetem dopóki Państwo będzie troszczyło się o ciągłe polepszanie poziomu bezpieczeństwa. Akceptowalny poziom bezpieczeństwa dla danego SSP, po jego opracowaniu, stanowi manifestację tego, co Państwo uznaje za odpowiednie w ramach kontekstu swego, własnego systemu lotnictwa. Krajowy ALoSP również wyraża minimalne, akceptowane dla władzy doglądającej cele dotyczące bezpieczeństwa, jakie muszą być osiągnięte przez ogół dostawców usług nadzorowanych przez tę władzę.

4.3.5.3. Dla celów SSP, akceptowalny poziom bezpieczeństwa jest rozpoznawalny i ustanawiany przez ogół wskaźników poziomu bezpieczeństwa danego Państwa. Stosowane w tym celu krajowe wskaźniki bezpieczeństwa to te, w które – tam gdzie ma to zastosowanie – zostały wprowadzone ustawienia obiektywnych celów i alarmów. Akceptowalny poziom bezpieczeństwa jest koncepcją pomostową, a wskaźniki bezpieczeństwa z odnoszącymi się do nich poziomami alarmowymi i docelowymi (graniczne ustawienia możliwości) są rzeczywistymi miernikami ALoSP. Zakresem, w jakim zostały osiągnięte cele wskaźników bezpieczeństwa, jest pomiar ich wydajności. Przykłady ilustrujące rozwój wskaźników ALoSP znajdują się w Dodatku 4.

4.3.5.4. W pełni rozwinięty proces monitorowania i mierzenia ALoSP będzie na bieżąco:

a) rozpoznawać wszystkie sektory krytyczne dla bezpieczeństwa oraz wskaźniki bezpieczeństwa, które definiują poziom bezpieczeństwa w tych obszarach;

b) rozpoznawać cele, które definiują poziom jaki ma być utrzymany, lub będzie rozpoznawał pożądane ulepszenie, które mają być osiągnięte przez odnośne wskaźniki w każdym sektorze z założeniem, że nadrzędnym celem jest ciągłe ulepszanie całego systemu lotniczego;

c) rozpoznawał alarmy, które będą wskazywać faktyczny lub powstający problem związany z wydajnością bezpieczeństwa w konkretnym wskaźniku lub sektorze poziomu bezpieczeństwa;

d) analizować wydajność programu bezpieczeństwa (SSP) w celu określenia czy, dla uzyskania ciągłego usprawniania, potrzebne są modyfikacje lub uzupełnienia do istniejących wskaźników, celów bądź alarmów.

4.3.5.5. Ustanowienie dla SSP wskaźników bezpieczeństwa, celów i alarmów z ALoSP nie zastąpi/nie zmieni konieczności wdrożenia przez Państwo wszystkich odnośnych programów SARPs ani nie zwolni Państw ze swych obowiązków wynikających z Konwencji o międzynarodowym lotnictwie cywilnym i związanych z nią postanowień.

Ustalanie poziomów alarmów i celów

4.3.5.6. Wskaźniki bezpieczeństwa są narzędziami taktycznego monitorowania i mierzenia działania bezpieczeństwa w Państwie. Podczas wstępnego opracowywania i wdrażania SSP, poziom działania bezpieczeństwa jest normalnie reprezentowany przez wskaźniki bezpieczeństwa związane z wynikami wysokich konsekwencji (takich jak liczba wypadków i poważnych incydentów) i wynikami szacunkowymi z górnych systemów (takich jak skuteczne wdrożenie programów SARPs

ICAO). W miarę jak SSP dojrzewa, poziom działania bezpieczeństwa może być uzupełniony o wskaźniki reprezentujące wyniki systemów przewidzianych dla mniejszych konsekwencji lub dla wydarzeń dewiacyjnych. Wskaźniki działania bezpieczeństwa są na ogół monitorowane przy użyciu narzędzi monitorujących podstawowe dane ilościowe trendów, które generują wykresy lub plansze uwzględniające poziomy alarmów i cele, powszechnie stosowane w technicznych i jakościowych systemach kontroli lub systemach wiarygodności.

4.3.5.7. Cele definiują długoterminowe założenia SSP dotyczące działania bezpieczeństwa. Wyrażane są w wartościach liczbowych i muszą być konkretne, mierzalne, akceptowalne, wiarygodne i sensowne. Cele muszą także zawierać daty ukończenia; daty poszczególnych faz – jeżeli cel ma być osiągnięty w fazach lub w dłuższym okresie. Cele zapewniają mierzalny sposób zapewnienia i zademonstrowania skuteczności SSP. Określając cel (ilościowo) należy uwzględnić takie czynniki, jak dający się zastosować poziom ryzyka, koszty i korzyści związane z usprawnieniami systemu lotniczego oraz oczekiwania związane z bezpieczeństwem przemysłu lotniczego danego Państwa. Oczekiwane cele odnośnie poprawy należy określić po rozważeniu co faktycznie można osiągnąć w określonym sektorze lotnictwa. Rozważania powinny uwzględniać bieżące i historyczne działanie konkretnego wskaźnika poziomu bezpieczeństwa, jeżeli dostępne są dane historyczne trendów.

4.3.5.8. Poziom alarmu jest tożsamy z każdym wskaźnikiem działania bezpieczeństwa, określającym ilościowo próg nieakceptowanego działania bezpieczeństwa (nienormalny współczynnik zdarzenia) podczas konkretnego okresu monitorowania. Stosowanie, dla ustawienia poziomów alarmowych, kryteriów opartych na danych obiektywnych jest istotne dla ułatwienia stałego analizowania trendów lub dokonywania porównań. Ustawienie poziomu alarmowego separuje na planszy wskaźnika bezpieczeństwa obszary z akceptowalnym i nieakceptowalnym jego działaniem, i jest podstawowym sygnałem (przestroga/dzwonek alarmowy) dla podjęcia działań naprawczych związanych z konkretnym wskaźnikiem bezpieczeństwa. Naruszenie poziomu alarmowego gwarantuje to, że podjęte będzie dochodzenie dla znalezienia przyczyny alarmu i, w konsekwencji, podjęcie czynności naprawczych lub łagodzących, tam gdzie konieczne. Dla rozpoznania przyczyn źródłowych, zagrożeń i związanych z nimi ryzykiem, czynności dochodzeniowe będą wymagać koordynacji z dostawcami usług, których dotyczą.

4.3.5.9. Tak jak w ogólnych metodach pomiaru wskaźników bezpieczeństwa, zastosowanie odchylenia standardowego populacji (STDEVP) zapewnia podstawy obiektywizmu przy sposobie wyznaczania kryteriów do oznaczenia poziomów alarmowych. Zgodnie z tą metodą wyznaczenie wartości odchylenia standardowego opiera się na poprzednich (historycznych) wskaźnikach bezpieczeństwa. Ta wartość odchylenia standardowego oraz średnia wartość zebranych danych historycznych wyznaczają podstawowe wartości uznawane za alarmowe dla kolejnego okresu monitorowania. Zgodnie z zasadą odchylenia standardowego (podstawowa funkcja programu MS Excel) ustala się kryteria dla wyznaczenia poziomów alarmowych opartych na rzeczywistych danych/wynikach historycznych dotyczących danego wskaźnika (zbioru danych) włączając w to ich zmienność (fluktuacje danych punktowych). Wyższe wartości danych historycznych będą generować wyższe (bardziej liczne) poziomy wartości alarmowych dla następnego okresu monitorowania. Materiały doradcze dotyczące ustalania poziomu alarmowego z wykorzystaniem kryteriów związanych z odchyleniem standardowym jest w Dodatku 4.

4.3.5.10. Podstawowe wskaźniki bezpieczeństwa dla danego Państwa (początkowy ALoSP) na ogół składają się ze wskaźników bezpieczeństwa wysokiego rzędu konsekwencji, takich jak współczynniki poważnych incydentów dla każdego sektora. Ważne jest by takie dane były podawane w formie współczynnika zamiast w bezwzględnych liczbach incydentów. Następnie, w dojrzałym stadium ALoSP, można opracować wskaźniki dla konsekwencji niższego rzędu, w celu uzupełnienia istniejącego pakietu ALoSP (wskaźniki konsekwencji niższego rzędu są czasem określane jako wskaźniki proaktywne/wyprzedzające).

4.3.5.11. Po zdefiniowaniu krajowego pakietu wskaźników poziomu bezpieczeństwa, celów i poziomów alarmowych ALoSP, istnieje możliwość regularnego kompilowania podsumowania wyników działania każdego wskaźnika poziomu bezpieczeństwa. Następnie, można sprawdzić wartość docelową i poziom alarmowy dla każdego wskaźnika czy odpowiadają swym statusom osiągów. Następnie należy dokonać skonsolidowanego podsumowania całościowego celu/wyniku działania zestawu wskaźników alarmowych poziomu bezpieczeństwa ALoSP dla konkretnego roku lub okresu monitorowania. Jeżeli istnieje taka konieczność, można przydzielić wartość liczbową dla każdego „osiągniętego celu" i każdego „nieprzekroczonego poziomu alarmowego" (punkty dodatnie). To umożliwi pomiar liczbowy/procentowy działania ALoSP. Działanie ALoSP dla danego roku lub okresu monitorowania można porównać z dotychczasowym lub przyszłym działaniem. Państwa mają wolną rękę w rozwijaniu tych podstawowych kryteriów pomiaru działania ALoSP uzupełniając je o dodatkowe czynniki lub procesy uznane za konieczne.

4.3.5.12. Aby dopilnować, by wszystkie wskaźniki poziomu bezpieczeństwa ALoSP pozostawały skuteczne i odpowiednie wraz z upływem czasu muszą być okresowo przeglądane w celu sprawdzenia czy nie zachodzi konieczność wprowadzenia modyfikacji lub uzupełnień do istniejących wskaźników, celów i alarmów. Okresowym przeglądem ALoSP i wszelkimi wynikającymi z tego zmianami można się zająć, tam gdzie warto, na poziomie koordynacji platformy SSP. Dodatkowe informacje dotyczące opracowywania wskaźników poziomu bezpieczeństwa, ustalenia celów i poziomów alarmowych znajdują się w Dodatku 4 do niniejszego rozdziału. Analogiczne wytyczne dla wskaźników poziomu bezpieczeństwa SMS można znaleźć w Rozdziale 2 i 5.

4.4. WDROŻENIE PROGRAMU SSP – PODEJŚCIE FAZOWE

4.4.1. Wdrożenie SSP zostaje ułatwione przez zidentyfikowanie procesów związanych z każdym z czterech komponentów i odnośnych elementów ramy SSP. Progresywne lub fazowe wdrażanie SSP skutecznie sobie radzi z obciążeniem pracą i oczekiwaniami w realistycznym przedziale czasowym. Praktyczne ustalanie kolejności zadań lub wg ich priorytetów związanych z wdrożeniem różnych elementów SSP jest różne w różnych Państwach. Podejście fazowe, opisane w niniejszym rozdziale,

zakłada że wszystkie 11 elementów SSP wymaga pewnego stopnia wdrożeń dodatkowych. Tam gdzie niektóre elementy lub procesy są już na miejscu, można je zintegrować lub przyłączyć do ramy SSP.

4.4.2. Niniejsza sekcja omawia podejście etapowe przy wdrażaniu SSP. Takie podejście wymaga przeorganizowania 11 elementów w ramach czterech faz. Uzasadnieniem zastosowania struktury etapowej jest ułatwienie wdrożenia elementów i procesów w sposób progresywny. Przegląd czterech etapów i włączonych do nich elementów przedstawiono w Tabeli 4-1.

FAZA 1

4.4.3. Zakresy odpowiedzialności Państwa i osób za bezpieczeństwo – Element 1.2 (i):

a) Zidentyfikować jaka organizacja jest gospodarzem (*placeholder*) SSP i kto jest dyrektorem odpowiedzialnym. Dyrektor odpowiedzialny krajowego SSP powinien, jako minimum:

1. posiadać władzę i ponosić osobistą odpowiedzialność, w imieniu Państwa, za wdrożenie i utrzymanie SSP w całym systemie lotniczym Państwa, z wyłączeniem Państwowej Komisji Badania Wypadków;

2. posiadać władzę w zakresie zagadnień związanych z zasobami ludzkimi w organizacji gospodarza SSP;

3. posiadać władzę w zakresie większych zagadnień finansowych w organizacji gospodarza SSP;

4. posiadać władzę w zakresie certyfikacji dostawców usług i doglądania bezpieczeństwa przez organizację gospodarza SSP;

5. być odpowiedzialnym za koordynację wszystkich spraw Państwa, związanych z SSP.

b) Powołać zespół ds. wdrożenia SSP. Zespół powinien się składać z przedstawicieli odnośnych krajowych instytucji legislacyjnych i administracyjnych. Rolą zespołu jest napędzać wdrażanie SSP od etapu planowania do zakończenia. Organizacja/gospodarz SSP, wraz z departamentem/ biurem odpowiedzialnym za administrowanie SSP powinny - po jego wdrożeniu - przejąć SSP od zespołu wdrażającego. Inne funkcje zespołu wdrożeniowego powinny obejmować, ale nie tylko:

1. koordynowanie procesu analizy luk;

2. opracowanie planu wdrożenia SSP;

3. zapewnienie odpowiedniego szkolenia w zakresie SSP i wiedzy technicznej zespołu po to by ustanowić skuteczne wdrożenie elementów SSP i procesów pokrewnych;

4. monitorowanie i raportowanie o postępach we wdrażaniu SSP, raportując o regularnych uaktualnieniach, o koordynacji z dyrektorem odpowiedzialnym za SSP i o dopilnowywaniu by działania w każdej fazie były kończone w określonym przedziale czasowym.

Aby zapewnić prawidłową realizację planu wdrożenia, szczególnie w Państwach z wieloma instytucjami/organizacjami, dyrektor odpowiedzialny powinien dopilnować by zespół wdrożeniowy dostał stosowne upoważnienia i wsparcie w zarządzaniu.

c) Przeprowadź analizę luk SSP. W celu opracowania planu wdrożenia SSP, należy przeprowadzić w istniejącej strukturze i procesach analizę luk i porównać z ramą SSP ICAO. Pozwoli to Państwu na ocenę istnienia i dojrzałości elementów swego SSP. Po zakończeniu analizy luk i jej udokumentowaniu, zidentyfikowane brakujące lub niepełne komponenty/elementy/procesy stworzą z tymi już istniejącymi podstawę dla przygotowania planu wdrożenia SSP. Przykład analizy luk dla SSP przedstawiony jest w Dodatku 7 do niniejszego Rozdziału.

d) Opracuj plan wdrożenia SSP. Plan będzie służył jako przewodnik dla zbudowania SSP i zintegrowania go z czynnościami zarządzania bezpieczeństwem przez Państwo. Plan powinien:

1. jednoznacznie określić czynności (elementy/procesy), które będą opracowywane lub zakończone zgodnie z odnoszącymi się do nich terminami pośrednimi lub fazami. Czynności te zależą od wyników analizy luk,

2. określić realistyczny przedział czasu, z uwzględnieniem terminów pośrednich, dla realizacji każdej czynności lub fazy. W zależności od złożoności krajowego SSP, plan wdrożenia SSP może być skompilowany jako prosta tabela w Word/Excel, lub, jeżeli konieczne, przy zastosowaniu narzędzia zarządczego takiego jak tablica Gantta. Przykład prostego formatu dla planu wdrożenia SSP znajduje się w Dodatku 7 do niniejszego Rozdziału.

e) Powołaj państwową platformę ds. koordynacji bezpieczeństwa lotniczego. Jeżeli jeszcze nie istnieje, zainicjuj stworzenie mechanizmu koordynowania SSP, przy udziale wszystkich krajowych, legislacyjnych, organizacji lotniczych. Mechanizm ten może mieć kształt rady lub zespołu/komisji itp. Jej zadaniem jest koordynowanie wdrażania a następnie administrowanie SSP w różnych krajowych, legislacyjnych i administracyjnych instytucjach i organizacjach lotniczych. To

zapewni, że rozwój, okresowe przeglądy i decyzje oraz kształtowanie polityki dotyczące działań SSP, takich jak polityka bezpieczeństwa, wskaźniki bezpieczeństwa, polityka przestrzegania prawa, ochrona i wymiana danych o bezpieczeństwie, tworzenia przepisów dla SSP, przeprowadzania wewnętrznych przeglądów SSP i dokonywanie ustaleń itp. będą realizowane są w sposób zintegrowany i skoordynowany. W tej stałej platformie SSP uczestniczyć powinno kierownictwo wysokiego szczebla różnych organizacji, przy czym koordynatorem powinien być dyrektor odpowiedzialny SSP.

f) Załóż dokumentację SSP. Proces tworzenia projektu dokumentu SSP należy rozpocząć z chwilą rozpoczęcia wdrażania SSP. Wraz z postępującym określaniem/definiowaniem komponentów i elementów SSP można do tego najważniejszego dokumentu sukcesywnie wpisywać opis każdego elementu i powiązane z nim procesy. Patrz Appendix 8, gdzie przedstawiono strukturę, jaką można nadać dokumentowi SSP i jego zawartości. Załóż u dostawcy usług - gospodarza SSP, system dokumentacji SSP (biblioteka/szafa/teczka), który będzie służyć jako centralna składnica takich rzeczy, jak dokument tego SSP i pokrewnych programów SOP, druków, protokołów z posiedzeń oraz zapisów związanych z wdrożeniem SSP i jego ciągłym działaniem. Dokumenty te służyć będą jako zapisy i dowody faktycznie wykonanych działań i ciągłego działania poszczególnych elementów SSP. Istnieje możliwość, że niektóre zapisy, takie jak poufne sprawozdania i raporty ze zdarzeń będą przechowywane w osobnym systemie komputerowym lub że będą tkwiły w innej krajowej, legislacyjnej lub administracyjnej organizacji. W takich przypadkach, próbki/wzory lub wyciągi będą mogły być przechowywane w odnośnej bibliotece. Główny spis dokumentacji SSP powinien pomóc w poruszaniu się po całej przedmiotowej dokumentacji. Tak jak w każdym innym systemie, System skonsolidowanej dokumentacji ułatwi śledzenie, aktualizację, docieranie do odnośników oraz wewnętrzne/zewnętrzne audytowanie systemu.

Tabela 4-1. Przykład czterech faz wdrażania SSP

Faza 1 (12 miesięcy)	*Faza 2 (12 miesięcy)*	*Faza 3 (24 miesiące)*	*Faza 4 (24 miesiące)*
1. SSP element 1.2 (i): a) ustalić organizację/ instytucję-gospodarza i kto będzie dyrektorem odpowiedzialnym; b)powołać zespół ds. wdrożenia SSP; c) przeprowadź analizę luk SSP; d) opracować plan wdrożenia SSP; e) ustanowić mechanizm koordynacji SSP; f) stworzyć wymaganą dokumentację SSP włącznie z ramą krajowego SSP, jego podzespołami i elementami.	1. SSP element 1.1: Ustanowić ramę legislacyjną dla bezpieczeństwa narodowego 2. SSP element 1.2 (ii): a) ustalić jakie mają być obowiązki w zarządzaniu bezpieczeństwem, zdefiniować je i udokumentować oraz ustalić odpowiedzialność osobistą; b) zdefiniować i udokumentować politykę bezpieczeństwa Państwa i cele. 3. SSP element 1.3: uruchomić proces badania wypadków i poważnych incydentów. 4. SSP element 1.4 (i): ustanowić podstawowe prawodawstwo dla egzekwowania prawa (kary). 5. SSP element 3.1 (i): zapewnić Państwu skuteczne śledzenie i nadzorowanie działań dostawców usług. 6. SSP element 2.1 (i): ułatwiać edukację dot. SMS i promować ją wśród dostawców usług.	1. SSP element 1.4 (ii): obwieścić politykę egzekwowania prawa/prawodawstwo, które mają zawierać: a) postanowienia dla dostawców usług działających w oparciu o SMS, pozwalające na podejmowanie i wewnętrznego rozwiązywanie odstępstw od bezpieczeństwa i jakości; b) warunki i okoliczności, w których Państwo może interweniować w przypadku odstępstw od bezpieczeństwa; c) postanowienia zapobiegające ujawnianiu i korzystaniu z danych o bezpieczeństwie dla celów innych niż poprawienie bezpieczeństwa. d) postanowienia do ochrony źródła informacji pozyskanych z dobrowolnego/poufnego systemy raportowania 2. SSP element 2.1 (ii): stworzyć zharmonizowane przepisy nakazujące wdrażanie SMS 3. SSP element 3.2 (i): a) ustanowić systemy zbierania i wymiany danych o bezpieczeństwie; b) ustanowić krajowe wysokopoziomowe wskaźniki bezpieczeństwa oraz ich poziomy alarmowe.	1. SSP element 2.2: przejrzeć i uzgodnić wskaźniki bezpieczeństwa u dostawcy usług. 2. SSP element 3.1 (ii): wprowadzić SMS dostawcy usług i wskaźniki działania bezpieczeństwa do rutynowego programu śledzenia. 3. SSP element 3.2 (ii): a) wdrożyć systemy dobrowolnego/poufnego powiadamiania o bezpieczeństwie; b) ustanowić niskopoziomowe wskaźniki bezpieczeństwa i ich poziomy alarmowe z możliwością ich monitorowania; c) promować wymianę informacji o bezpieczeństwie z i wśród dostawców usług i innych Państw. 4. SSP element 3.3: gdzie możliwe, dawać pierwszeństwo inspekcjom i audytom opartym o analizę ryzyka dotyczącego bezpieczeństwa lub danych o jakości. 5. SSP element 3.1 (iii): ustanowić wewnętrzny mechanizm przeglądu SSP dla zapewnienia ciągłej skuteczności i usprawniania.
Uwaga 1.– Elementy 4.1 i 4.2 systemu SSP (wewnętrzne szkolenie SSP i SMS; promocja szkolenia zewnętrznego SMS; wewnętrzna i zewnętrzna komunikacja oraz upowszechnianie informacji związanej z bezpieczeństwem) są progresywnie wdrażane w fazach 1 do 4. *Uwaga 2.– Rama czasowa każdej fazy (np. 12 miesięcy dla Fazy nr 1) jest tylko okresem w przybliżeniu. Faktyczny okres wdrażania będzie zależeć od zakresu/złożoności systemu lotniczego danego Państwa, od faktycznych luk w każdym elemencie i od struktury organizacyjnej.*			

FAZA 2

4.4.4. Rama prawna bezpieczeństwa Państwa – Element 1.1

a) Dokonaj przeglądu, opracowuj i obwieszczaj, tam gdzie to konieczne, ramę prawną bezpieczeństwa narodowego i konkretne przepisy, zgodnie ze standardami międzynarodowymi i krajowymi, które definiują to jak Państwo będzie zarządzać bezpieczeństwem i regulować bezpieczeństwo lotnictwa na całym swym obszarze.

b) Załóż ramę czasową dla okresowego przeglądu przepisów bezpieczeństwa i konkretnych przepisów operacyjnych w celu zapewnienia, iż pozostają one dla Państwa istotnymi i odpowiednimi.

4.4.5. Określenie zakresów odpowiedzialności Państwa i osób za bezpieczeństwo – Element 1.2 (ii)

a) Zdefiniuj oraz ustal obowiązki i odpowiedzialność odnośnych organizacji legislacyjnych i ich osób za zarządzanie bezpieczeństwem. W dokumencie SSP należy umieścić opis lub ilustrację istniejącej struktury organizacyjnej oraz zintegrowanie różnych instytucji oraz organizacji legislacyjnych i administracyjnych. Stamtąd będzie można dawać odsyłacze do dokumentacji drugorzędnej, gdzie znaleźć można szczegółowe wykazy obowiązków i odpowiedzialność za bezpieczeństwo odnośnych organizacji.

b) Opracuj i wykonaj wdrożenie polityki bezpieczeństwa Państwa oraz niezbędnych środków zapewniających, że taka polityka będzie zrozumiała i będzie przestrzegana na wszystkich poziomach w krajowych instytucjach/organizacjach lotniczych. Wytyczne dotyczące przygotowania polityki bezpieczeństwa Państwa są nakreślone w Dodatku 1 do niniejszego rozdziału.

c) Opracuj lub włącz szerokie cele bezpieczeństwa Państwa, te które przystają do polityki bezpieczeństwa Państwa. Takie cele bezpieczeństwa mogą być celami osobnymi lub być częścią całościowego oświadczenia dotyczącego misji, zależnie od złożoności i ról organizacji.

4.4.6. Badanie wypadków i incydentów – Element 1.3

Państwo powinno:

a) zapewnić by jego rama prawna zawierała postanowienia dla uruchomienia niezależnego procesu badania wypadków i incydentów, administrowanego przez jakąś niezależną organizację, biuro, komisję lub inne ciało;

b) powołać organizację, biuro, komisję lub inne ciało do badania wypadków i zdarzeń - niezależne od wszystkich innych krajowych organizacji. W Państwach, w których powołanie stałego podmiotu dla badania wypadków byłoby niepraktyczne, można każdorazowo wyznaczać kompetentną komisję lub zespół do zbadania każdego wypadku. Ewentualnie, takie Państwa mogą rozważyć skorzystanie z usług regionalnej organizacji badania wypadków i zdarzeń (RAIO, patrz Doc 9946);

c) utwórz mechanizmy zapewniające, że jedynym celem procesu badania wypadków i incydentów jest zapobieganie wypadkom i incydentom, na wsparcie zarządzania bezpieczeństwem w Państwie, a nie przypisywanie winy lub odpowiedzialności.

4.4.7. Polityka egzekwowania przepisów – Element 1.4 (i)

Państwo powinno zagwarantować lub stworzyć podstawowe przepisy prawne dla czynności egzekucyjnych (kary), włącznie z zawieszeniem lub cofnięciem certyfikatów.

4.4.8. Nadzorowanie bezpieczeństwa – Element 3.1 (i)

Państwo powinno zapewnić lub stworzyć podstawowy program doglądania bezpieczeństwa u dostawców usług. Powinien on zawierać program śledzenia, zapewniający, że dostawcy usług będą stosować się do przepisów podczas rutynowych operacji, ale niekonieczne ograniczonych do:

a) inspekcjonowania miejsca, bazy lub produktu; oraz

b) audytowania organizacji lub systemu.

4.4.9. Wymagania bezpieczeństwa wobec SMS dostawców usług – Element 2.1 (i)

a) Tam gdzie jest stosowne w fazie szkolenia i promowania wdrażania SMS, Państwo powinno przygotować dostawców usług i zainteresowane podmioty lotnicze do wymogów dotyczących wdrażania SMS poprzez szkolenia i działania promujące SMS, takie jak fora SMS, seminaria, odprawy instruktażowe lub warsztaty.

b) W oczekiwaniu na opracowanie przepisów dla SMS, lub równocześnie z ich opracowywaniem, opracuj odpowiednie dla dostawców usług materiały doradcze dotyczące SMS. Po przykład regulacji prawnej z krajowego SMS - patrz Dodatek 9 do niniejszego rozdziału.

FAZA 3

4.4.10. Polityka egzekwowania prawa – Element 1.4 (ii)

Polityka i procedury Państwa dotyczące egzekwowania powinny ustanowić, co następuje:

a) w kontekście należących do dostawców usług systemów zarządzania bezpieczeństwem (SMS) i za aprobatą właściwej władzy krajowej, zezwala się dostawcom usług na zajmowanie się i wewnętrznym rozwiązywaniem wydarzeń, w których zaistniały jakieś odstępstwa od bezpieczeństwa;

b) warunki i okoliczności, w których odstępstwa od bezpieczeństwa podlegają ustanowionej określonej procedurze egzekwowania prawa;

c) procedury dla zagwarantowania, że w SMS nie będzie się wykorzystywać dla potrzeb egzekwowania prawa żadnych informacji pozyskanych z dobrowolnych/poufnych systemów raportowania ani z równoważnych, zastrzeżonych systemów monitorowania danych operacyjnych;

d) proces dla ochrony źródeł informacji pozyskanych z dobrowolnych/poufnych systemów raportowania.

Próbka polityki egzekwowania prawa przez Państwo jest nakreślona w Dodatku 10 a próbka jego procedur jest nakreślona w Dodatku 11 do Rozdziału 4.

4.4.11. Wymagania SMS wobec dostawców usług – Element 2.1(ii)

a) Ustanów dla wszystkich dostawców usług, których to dotyczy, przepisy SMS, materiały pomocnicze i wymagania związane z wdrożeniem by dopilnować, aby rama prawna SMS była zharmonizowana we wszystkich sektorach lotnictwa i aby przystawała do ramy SMS ICAO. Przyjęcie zharmonizowanej ramy SMS ICAO ułatwi wzajemne ich uznawanie pośród Państw.

b) Uruchom proces przyjęcia SMS poszczególnego dostawcy usług by się upewnić, że rama jego SMS przystaje do ramy prawnej Państwa. Taki początkowy przegląd i akceptację można okazać poprzez parafowanie lub przyjęcie podręcznika SMS danej organizacji. W Państwie, które podeszło fazowo do wdrożenia SMS, taki proces akceptacji można też realizować fazowo, gdy warto. Po przykład listy kontrolnej przepisów przyjęcia/akceptacji SMS patrz Dodatek 12.

Uwaga.– Zaleca się akceptowanie lub honorowanie SMS obcej organizacji (np. obcego AMO), gdy taki SMS został stosownie zaakceptowany przez władzę lotniczą danej organizacji, a struktura SMS jest zgodna ze strukturą SMS ICAO.

4.4.12. Zbieranie, analizowanie i wymiana danych związanych z bezpieczeństwem – Element 3.2 (i) Państwo powinno:

a) Ustanowić mechanizmy i procedury dla zbierania i analizowania wydarzeń obowiązkowych/okoliczności podlegających zbiorowemu zgłaszaniu na poziomie Państwa. To by wymagało od Państwa:

1. ustanowienia - dla certyfikowanych/zatwierdzonych dostawców usług dla każdego sektora - procedury na raportowanie (obowiązkowe) wypadków i poważnych incydentów. Tam gdzie możliwe, procedura powinna obejmować zgłaszanie defektów poważnych lub zgłaszanych obowiązkowo (MDR). Patrz Dodatek 3 zawierający wytyczne dla procedury raportowania obowiązkowego;

2. ustanowienia wymagań wobec dostawców usług by posiadali wewnętrzny proces badania i rozwiązywania wydarzeń, dokumentujący wyniki dochodzeń i udostępniający raporty organizacjom legislacyjnym swych Państw;

3. zapewnienia stosownej integracji, konsolidacji i scalania danych zbieranych z różnych sektorów lotnictwa na poziomie SSP. Dane dotyczące bezpieczeństwa nie powinny istnieć jako niezależne lub samodzielne zbiory tylko na poziomie pojedynczego sektora. Ten aspekt integracyjny powinien także dotyczyć odnośnych baz danych krajowej władzy lotniczej (CAA) i bazy danych niezależnych komisji badania wypadków, włącznie z bazami Państw, w których pewne funkcje zarządzania bezpieczeństwem są wykonywane w imieniu Państwa przez RSOO lub RAIO.

b) Ustanowienia podstawowych wysokopoziomowych wskaźników bezpieczeństwa (początkowo ALoSP) oraz powiązanych z nimi ustanowionych celów i poziomów alarmowych. Przykładami wysokopoziomowych wskaźników są: liczba wypadków, poważnych incydentów oraz monitoring skutków tych zdarzeń pod względem wysokiego ryzyka, przepisów, niezgodności (np. ustalenia audytu ICAO). Opracowanie wskaźników bezpieczeństwa i ich selekcja powinny przystawać do krajowych celów w sferze i polityce bezpieczeństwa. Powinny być stosowne i odpowiadać zakresowi i złożoności działań Państwa w sferze

bezpieczeństwa lotnictwa. Wyborem wskaźników niskopoziomowych konsekwencji dla bezpieczeństwa można się zająć na późniejszym etapie. Należy przeprowadzać okresowe monitorowanie wskaźników poziomu bezpieczeństwa pod kątem niepożądanych trendów, naruszeń poziomów alarmowych i uzyskiwania wartości docelowych. Patrz Dodatek 4 dla wytycznych dotyczących opracowania wskaźników poziomu bezpieczeństwa i monitorowania.

FAZA 4

4.4.13. Zgoda na działania dostawców usług w sferze bezpieczeństwa – Element 2.2

Państwo powinno ustanowić procedurę dla łączności z dostawcami usług w ich opracowywaniu kompletu wskaźników realnego działania bezpieczeństwa (SPI), celów i alarmów, tam gdzie możliwe w zależności od wielkości i złożoności organizacji. Wskaźniki bezpieczeństwa, wartości docelowych i poziomów alarmowych powinny być:

a) kombinacją SPI dla konsekwencji dużych i mniejszych, zależnie od potrzeb;

b) adekwatne do działalności lotniczych dostawców usług;

c) kompatybilne dla innych dostawców usług w tym samym sektorze/kategorii;

d) przystające do całości wskaźników bezpieczeństwa krajowego SSP dla potrzeb sektora/kategorii dostawców usług.

Po opracowaniu wskaźników poziomu bezpieczeństwa, wartości docelowych i poziomów alarmowych, udokumentowane muszą zostać plany działań dostawców usług, dotyczące osiągania celów oraz plany działań dla ich naprawy w przypadku gdy zaistnieje poziom alarmowy. Krajowy proces okresowego przeglądu poziomu bezpieczeństwa u dostawcy usług powinien być dla dostawców usług przejrzysty przy wypracowywaniu wymagań dotyczących działania.

4.4.14. Nadzorowanie bezpieczeństwa – Element 3.1 (ii)

Państwo wdroży nadzór nad SMS dostawców usług jako część stałego programu nadzoru, który uwzględniać będzie:

a) ustalanie z dostawcami usług okresowych przeglądów wymagań SMS i odnośnych materiałów pomocniczych, by upewnić się, że są dla nich nadal istotne i odpowiednie;

b) mierzenie jak działa bezpieczeństwo w SMS poszczególnego dostawcy usług, poprzez okresowe przeglądy uzgodnionego poziomu bezpieczeństwa i sprawdzając czy wskaźniki SPI oraz ustawienia docelowe i alarmowe pozostają istotne dla dostawcy usług;

c) upewnianie się czy procesy identyfikacji zagrożeń i zarządzania ryzykiem bezpieczeństwa przez dostawcę usług podążają za ustalonymi przez prawodawcę wymaganiami i czy mechanizmy kontrolowania ryzyka dotyczącego bezpieczeństwa są odpowiednio wprowadzone do SMS dostawcy usług.

4.4.15. Nadzorowanie bezpieczeństwa – Element 3.1(iii)

Państwo powinno zbudować wewnętrzny mechanizm przeglądu lub oceny SSP i jego polityki bezpieczeństwa po to, by zapewnić ciągłe jego ulepszanie i podporządkowywanie. Tak jak w każdym skutecznym wewnętrznym mechanizmie przeglądu, tak i w tym procesie przeglądania powinien istnieć odpowiedni poziom niezależności oraz osobista odpowiedzialność za przestrzeganie ustaleń w swym działaniu.

4.4.16. Zbieranie, analizowanie i wymiana danych związanych z bezpieczeństwem – Element 3.2 (ii)

Państwo powinno:

a) ustanowić krajowy system dobrowolnego powiadamiania, uwzględniający postanowienia ochrony informacji dotyczących bezpieczeństwa. Zajrzyj do Dodatku 5 po wytyczne dla ochrony informacji o bezpieczeństwie. System dobrowolnego powiadamiania powinien stanowić część systemu zbierania i przetwarzania danych o bezpieczeństwie, w programie SSP. Baza danych dobrowolnego systemu powiadamiania powinna być częścią SSP SDCPS i być dostępna dla krajowej władzy lotniczej (CAA) jak również dla państwowego organu badania wypadków. Zajrzyj do Dodatku 2 po wytyczne nt. krajowego, dobrowolnego systemu raportowania;
b) ustanowić wskaźniki niskopoziomowych konsekwencji dla bezpieczeństwa i/lub wskaźniki jakości z odpowiednim monitorowaniem celów i alarmów (dojrzały ALoSP). Opracowanie i selekcja wskaźników bezpieczeństwa powinna przystawać do celów bezpieczeństwa Państwa i polityki bezpieczeństwa Państwa oraz powinny być właściwe i odpowiednie dla zakresu i złożoności działań lotniczych Państwa. Należy przeprowadzać okresowe monitorowanie wskaźników bezpieczeństwa pod kątem niepożądanych trendów, naruszenia poziomów alarmowych i osiągania celów. Zajrzyj do Dodatku 4 po wytyczne dotyczące opracowania wskaźników bezpieczeństwa i monitorowania;
c) promować wymianę i dzielenie się informacjami dotyczącymi bezpieczeństwa pomiędzy instytucjami legislacyjnymi i administracyjnymi Państwa a dostawcami usług, jak również przedsiębiorstwami przemysłowymi innych Państw.

4.4.17. Ukierunkowanie (bazujące na danych o bezpieczeństwie) nadzorowania na obszary wymagające większej troski lub potrzeb – Element 3.3

Państwo powinno przeglądać istniejące programy śledzenia i audytowania po to, by wprowadzać klauzulę dotyczącą kalibracji śledzenia lub częstotliwości i zakresu audytowania poszczególnego dostawcy usług w oparciu o adekwatne dane wyjściowe i wejściowe działania bezpieczeństwa. Po wskazówki dotyczące koncepcji śledzenia opartego na danych z bazy danych o bezpieczeństwie, zajrzyj do pkt 4.2, SSP Element 3.3, 4.2.36 oraz 4.2.37.

4.4.18. Szkolenie wewnętrzne, komunikacja i rozpowszechnianie informacji o bezpieczeństwie – Element 4.1 (Fazy 1 do 4)

Państwo powinno:

a) opracować politykę wewnętrznego szkolenia oraz procedury;

b) opracować program szkolenia odnośnego personelu na SSP i SMS. Pierwszeństwo szkolenia się należy dać personelowi wdrażającemu SSP-SMS i inspektorom operacyjnym/terenowym zajmującymi się systemem SMS dostawcy usług;

c) włączyć w szkolenie powdrożeniowe i w materiały szkoleniowe sobie specyficzne procesy SSP i ich odniesienia do ogólnych elementów ramy ICAO;

d) opracować system przekazywania informacji dotyczącej bezpieczeństwa pomiędzy wszystkimi krajowymi i administracyjnymi instytucjami/organizacjami w państwie, włącznie z państwową dokumentacją SSP, polityką bezpieczeństwa i przestrzegania prawa oraz procedurami korzystając z takich narzędzi jak ulotki, biuletyny lub sieć.

4.4.19. Szkolenie zewnętrzne, komunikacja i upowszechnianie informacji o bezpieczeństwie – Element 4.2 (Fazy 1 do 4)
Państwo powinno:

a) ustanowić proces dla przekazywania usługodawcom informacji o przepisach, programie SSP i systemie SMS;

b) opracować materiały pomocnicze dla dostawców usług, na temat wdrażania SMS;

c) opracować środki do przekazywania na zewnątrz aktualnych spraw dotyczących bezpieczeństwa, w tym działań koncepcyjnych i procedur, poprzez takie mechanizmy jak biuletyny branżowe, inne biuletyny i strony internetowe;

d) promować wymianę informacji o bezpieczeństwie pomiędzy dostawcami usług i innymi Państwami.

e) tam gdzie jest to odpowiednie, umożliwiać dostawcom usług szkolenie w zakresie SMS i zapoznawanie się z nim.

Uwaga.– Elementy zawarte w 4.4.18 i 4.4.19 są rozwijane progresywnie i wdrażane we wszystkich fazach

Dodatek 1 do Rozdziału 4
OŚWIADCZENIE W SPRAWIE POLITYKI BEZPIECZEŃSTWA PAŃSTWA

1. OGÓLNIE

1.1. Ogłoszenie przez Państwo polityki bezpieczeństwa powinno uwzględniać, ale nie musi być ograniczone do poniższych zobowiązań:

a) stworzenie i wdrożenie strategii i procesów zapewniających, że wszystkie działania lotnicze i operacje osiągną najwyższy, stały poziom bezpieczeństwa;

b) opracowanie i ogłoszenie krajowej ramy porządku prawnego i odnośnych przepisów operacyjnych pozwalających na zarządzanie bezpieczeństwem w Państwie, opartego na całościowej analizie lotniczego systemu Państwa i zgodnego z międzynarodowymi wymaganiami i standardami bezpieczeństwa - a tam gdzie możliwe, powyżej nich.

c) konsultowanie z segmentami branży lotniczej spraw bieżących, związanych z rozwojem przepisów;

d) przyznanie niezbędnych zasobów krajowym organizacjom lotniczym, aby była pewność, że ich personel będzie odpowiednio przeszkolony i będzie mógł wykonywać swe zakresy odpowiedzialności;

e) wspieranie zarządzaniem bezpieczeństwem poprzez promowanie systemów dobrowolnego i poufnego raportowania tak na poziomie dostawcy usług, jak i Państwa;

f) wykonywanie priorytetowych czynności nadzorowania, ponaglanych przez napływ danych o ryzyku i nastawionych na doglądanie tego czy przepisy są przestrzegane oraz dopilnowanie by te czynności legislacyjne i administracyjne były prowadzone zgodnie z międzynarodowymi standardami i najlepszymi praktykami;

g) promowanie koncepcji i zasad zarządzania bezpieczeństwem oraz edukowanie sektora lotniczego w tym zakresie, a także nadzorowanie wdrażania i działania SMS u krajowych dostawców usług;

h) dokonanie zapisów dla ochrony systemów zbierania i przetwarzania danych po to, by zachęcić personel i organizacje do dostarczania istotnych danych dotyczących bezpieczeństwa i utrzymywania między Państwem a dostawcami usług ciągłego przepływu i wymiany informacji o zarządzaniu bezpieczeństwem;

i) utrzymywanie skutecznej interakcji z dostawcami usług przy rozwiązywaniu problemów związanych z bezpieczeństwem;

j) prowadzenie polityki egzekwowania przestrzegania prawa i procedur, która uzupełnia ochronę informacji pochodzących z systemów zbierania danych o bezpieczeństwie i ich przetwarzania;

k) ustanowienia mechanizmów dla monitorowania i mierzenia wydolności SSP przy użyciu wskaźników bezpieczeństwa i ich odnośnych ustalonych celów i poziomów alarmowych;

l) promowania przyjmowania najlepszych praktyk i pozytywnej kultury bezpieczeństwa w firmach usługowych.

1.2. Orędzie dotyczące polityki bezpieczeństwa Państwa powinno być podpisane przez dyrektora odpowiedzialnego SSP lub przedstawiciela odpowiedniego szczebla odnośnego rządu, odpowiedzialnego za doglądanie legislacyjnych i administracyjnych organizacji tego Państwa.

2. PRZYKŁAD ILUSTRUJĄCY PODSTAWOWE SFORMUŁOWANIA POLITYKI BEZPIECZEŃSTWA

Poniżej wzór podstawowego oświadczenia w sprawie polityki bezpieczeństwa

[Nazwa krajowej organizacji legislacyjnej] promuje i reguluje bezpieczeństwo lotnictwa w [nazwa Państwa]. Zobowiązujemy się do rozwijania i wdrażania skutecznych strategii, ram prawnych i procesów zapewniających, że nadzorowana przez nas działalność lotnicza realizowana będzie na najwyższym możliwym poziomie bezpieczeństwa.

W tym celu:

1) ustanowimy krajowe standardy zgodne ze standardami, rekomendowanymi praktykami i procedurami Organizacji Międzynarodowego Lotnictwa Cywilnego;

2) tam gdzie jest możliwe, do regulowania bezpieczeństwa i nadzorowania działań branży lotniczej przyjmiemy podejście opierające się na danych i działaniu bezpieczeństwa;

3) aby się zająć obszarami o większym zagrożeniu lub potrzebie, będziemy identyfikować trendy bezpieczeństwa, panujące w branży lotniczej i przyjmujemy podejście oparte na zarządzaniu ryzykiem;

4) stale będziemy monitorować i mierzyć osiągi bezpieczeństwa w naszym systemie lotniczym przy użyciu krajowych wskaźników bezpieczeństwa oraz wskaźników dostawców usług;

5) zobowiązujemy się współpracować i konsultować z przemysłem lotniczym w zagadnieniach związanych z bezpieczeństwem i w sprawie ciągłego podnoszenia poziomu bezpieczeństwa;

6) będziemy promować dobre praktyki bezpieczeństwa i pozytywną kulturę bezpieczeństwa w całym przemyśle - oparte na zdrowych zasadach zarządzania bezpieczeństwem;

7) będziemy zachęcać do zbierania, analizowania i wymiany informacji o bezpieczeństwie pomiędzy odpowiednimi organizacjami w przemyśle i dostawcami usług, z intencją by takie informacje były wykorzystywane tylko dla celów zarządzania bezpieczeństwem;

8) będziemy przydzielać wystarczające środki finansowe i pracowników dla kierowania i nadzorowania bezpieczeństwa;

9) wyposażymy pracowników w odpowiednie umiejętności i doświadczenie, aby móc im przekazać obowiązki nadzoru i zarządzania.

Podpisane _____

przez DGCA (dyrektora odpowiedzialnego
za SSP lub osobę odpowiedzialną
za lotnictwo cywilne na poziomie Państwa)

Dodatek 2 do Rozdziału 4
KRAJOWY SYSTEM DOBROWOLNEGO I POUFNEGO RAPORTOWANIA – WSKAZÓWKI

(Patrz Element 3.2 SSP oraz Rozdział 4, 4.4.16 a)

Krajowy system dobrowolnego i poufnego raportowania, jako minimum, powinien definiować:

a) cel systemu raportowania;

Przykład :

Kluczowym celem [krajowego] systemu dobrowolnego i poufnego raportowania jest poprawienie bezpieczeństwa lotniczego poprzez zbieranie raportów o faktycznych i potencjalnych słabościach w bezpieczeństwie, które w przeciwnym razie nie byłyby zgłoszone innymi kanałami. Takie raporty mogą obejmować zdarzenia, zagrożenia lub groźby dotyczące bezpieczeństwa lotniczego. System nie eliminuje wymogu obowiązkowego raportowania odpowiednim władzom o wypadkach i incydentach, który istnieje z racji obowiązujących przepisów lotniczych. Zgłaszający są zachęcani do korzystania z wewnętrznego, dobrowolnego systemu powiadamiania SMS w swoich organizacjach, gdy taki system u nich istnieje, chyba że nie mają dostępu do takiego systemu lub gdy zgłaszający uzna, że incydent lub zagrożenie wykracza poza zakres prawny organizacji.

System [podać nazwę] jest systemem dobrowolnego, niepodlegającego karaniu, poufnego powiadamiania, ustanowiony przez [nazwa organu legislacyjnego/ administracyjnego]. System zapewnia kanał dla dobrowolnego raportowania o zdarzeniach lotniczych lub zagrożeniach, jednocześnie chroniąc tożsamość zgłaszającego.

b) zakres sektorów lotnictwa/obszarów objętych systemem;

Przykład :

[Nazwa systemu] obejmuje następujące obszary:

a) Operacje lotnicze:
   i. odlot/przelot/zbliżanie i lądowanie,
   ii. operacje w kabinie statku powietrznego,
   iii. wydarzenia związane z bliskością samolotu względem jakiegoś obiektu,
   iv. masa, wyważenie i osiągi.

b) Operacje na lotnisku:
   i. naziemne operacje statku powietrznego,
   ii. ruch na lotnisku,
   iii. operacja tankowania,
   iv. warunki lotniskowe lub usługi,
   v. ładowania do bagażników.

c) Zarządzanie ruchem lotniczym:
   i. Operacje ATC,
   ii. Wyposażenie ATC i pomoce nawigacyjne,
   iii. Komunikacja pomiędzy załogą a ATC.

d) Techniczna obsługa statku powietrznego:
   i. obsługa statku powietrznego/silników/podzespołów oraz naprawy.

e) Projektowanie i produkcja:

i. projektowanie statku powietrznego/silników/podzespołów oraz produkcja.

f) Zatwierdzone organizacje szkoleniowe:

i. szkolenia obejmujące operacje lotnicze.

g) Różne:

i. mające związek z bezpieczeństwem obsługi pasażerów,

ii. itp.

c) kto może złożyć dobrowolny raport;

Przykład :

Jeżeli należysz do którejś z tych grup, możesz się przyczynić do ulepszenia bezpieczeństwa lotniczego zgłaszając zdarzenia, zagrożenia lub groźby poprzez system [podać nazwę].

a) członkowie załogi lotniczej i pokładowej;

b) kontrolerzy ruchu lotniczego;

c) licencjonowani inżynierowie, technicy lub mechanicy samolotowi;

d) pracownicy organizacji obsługi technicznej, firm projektowych i produkcyjnych;

e) personel naziemny operatorów lotniczych;

f) pracownicy lotniska;

g) personel lotnictwa ogólnego;

h) itp.

d) kiedy napisać taki raport;

Przykład :

Raport należy napisać, gdy:

a) chcesz, aby inni nauczyli się i skorzystali z raportu dotyczącego zdarzenia lub zagrożenia, ale obawiasz się braku ochrony swej tożsamości;

b) nie ma innego odpowiedniego kanału lub procedury powiadamiania;

c) już próbowałeś innej procedury lub kanału powiadamiania, ale nie podjęto żadnych działań w odniesieniu do zagadnienia.

e) jak raporty są załatwiane;

Przykład :

Przy przetwarzaniu raportów, system [nazwa systemu] przywiązuje szczególną uwagę do konieczności chronienia tożsamości zgłaszającego. Każdy raport będzie przeczytany przez administratora i będzie mu nadany bieg. Administrator może skontaktować się ze zgłaszającym, żeby upewnić się, że rozumie charakter i okoliczności zgłoszonego zdarzenia/zagrożenia i/lub w celu uzyskania niezbędnych dodatkowych informacji i objaśnień.
Gdy administrator uzna, że uzyskana informacja jest kompletna i spójna, rozpracuje informację i wprowadzi jej dane do bazy systemu [nazwa systemu]. Gdyby ewentualnie zaszła potrzeba poszukiwania informacji u jakiejś strony trzeciej, użyte będą tylko dane rozpracowane.

Formularz systemu [podać nazwę systemu], z odnotowaną datą zwrotu, zostanie zwrócony do zgłaszającego. Jeżeli nie są potrzebne informacje dodatkowe, administrator dołoży starań, aby cały proces załatwiania zakończyć w ciągu dziesięciu (10) dni roboczych. W przypadkach, gdy administrator potrzebuje przedyskutować zagadnienie ze zgłaszającym lub skonsultować się z jakąś stroną trzecią, więcej czasu może być potrzebne.

Jeżeli administrator jest nieobecny w pracy przez dłuższy okres, inny administrator przeanalizuje raport. Zgłaszający mogą być spokojni o to, że każdy raport do systemu [nazwa systemu] będzie przeczytany i dalej będzie się nim zajmował administrator lub inny administrator.

Informacja zwrotna dla społeczności lotniczej

Raportami istotnymi, pozbawionymi cech identyfikacyjnych, oraz wyciągami można się dzielić ze środowiskiem lotniczym przez ich okresowe opublikowanie, tak aby wszyscy uczyli się z doświadczeń. Odnośne władze i strony mogą również dokonywać przeglądów swojej polityki i zaplanować usprawnienia.

Jeżeli treść raportu/zgłoszenia do [nazwa systemu] sugeruje sytuację lub stan, który stanowi natychmiastowe lub pilne zagrożenia dla bezpieczeństwa lotniczego, raport zostanie przeanalizowany w trybie pilnym i przekazany, po usunięciu cech identyfikacyjnych, organizacjom których dotyczy, tak szybko jak to będzie możliwe, żeby mogły podjąć niezbędne działania bezpieczeństwa.

f) jak się kontaktować z administratorem [nazwa systemu].

Przykład :

Zachęcamy do zatelefonowania do [nazwa organu legislacyjnej administracji] i zapytać o nazwę [nazwa systemu] lub poprosić o wstępną rozmowę z administratorem [nazwa systemu] przed złożeniem raportu/zgłoszenia. Z administratorem i z administratorem alternatywnym można się kontaktować w godzinach pracy od poniedziałku do piątku pod numerami telefonicznymi:

Administrator [nazwa systemu]	Administrator alternatywny
Pan	Pan .....
Tel:	Tel: .....

Dodatek 3 do Rozdziału 4
PRZYKŁAD KRAJOWEJ PROCEDURY OBOWIĄZKOWEGO RAPORTOWANIA

Poniżej podany jest przykład krajowej procedury obowiązkowego raportowania, która obejmuje wszystkie systemy obowiązkowego raportowania o zdarzeniach lotniczych. Procedura odnosi się do terminowego, obowiązkowego powiadamiania o wypadkach, poważnych incydentach i innych zdarzeniach, które podlegają zgłoszeniu przez zainteresowane strony/osoby, które w nich uczestniczyły. W zależności od przepisów obowiązujących w danym Państwie, takimi zainteresowanymi stronami mogą być certyfikowane/zatwierdzone organizacje lotnicze, niezależny licencjonowany/upoważniony personel (np. piloci, personel pokładowy, kontrolerzy ruchu lotniczego, personel obsługi technicznej) oraz przedstawicieli społeczeństwa.

Uwaga 1.– Jeżeli taka jest wola Państwa, obowiązkowe raportowanie o wypadkach i poważnych incydentach oraz awariach/usterkach/niesprawnościach/innych kłopotach obsługowych itp. może zostać objęte osobnymi procedurami; ewentualnie własną obowiązkową procedurą raportowania (jak w tym przykładzie).

Uwaga 2.– W niektórych przypadkach, „Uwaga" została podana w kwadratowych nawiasach [ ]. Jest to wskazówka administracyjna do rozważenia przez Państwo w trakcie opracowywania własnej obowiązkowej procedury raportowania.

1. RAPORTOWANIE OBOWIĄZKOWE

1.1. Na mocy [podać przepis] [nazwa zgłaszającego] jest obowiązany raportować [podać nazwę władzy/agencji i departamentu] o wypadkach lotniczych, poważnych incydentach, incydentach i innych zdarzeniach związanych z bezpieczeństwem (włącznie z awariami/usterkami/niesprawnościami/kłopotami obsługowymi).

1.2. Wykaz zdarzeń podlegających raportowaniu (poza wypadkami) i przedziały czasowe na raportowanie znajdują się w załączniku A do niniejszej procedury. [Uwaga: Choć załącznik A zawiera głównie przykłady poważnych incydentów, to jednak zachęca się Państwa do włączenia do obowiązkowego system raportowania także inne zdarzenia, które dane Państwo uzna za podlegające zgłoszeniu].

1.3. Obowiązkowe raportowanie zdarzeń odbywa się na formularzu Mandatory Report [Raport Obowiązkowy] (formularz XYZ). Tam gdzie podpisywanie jest stosowane, wszystkie obowiązkowe raporty są podpisywane przez upoważnionego sygnatariusza zatwierdzonej/certyfikowanej organizacji. [Uwaga: Należy również opracować procedurę dla zgłoszeń ustnych/telefonicznych].

1.4 Odnośnie wypadków i poważnych incydentów, trzeba uruchomić natychmiastową koordynację z [podać nazwę państwowej instytucji ds. badania wypadków] z chwilą otrzymania takiego zawiadomienia, po to by ustalić czy trzeba uruchomić proces niezależny. [Uwaga: Faktyczny proces zawiadomienia władzy lotniczej danego Państwa i/lub instytucji ds. badania wypadków będzie zależeć od natury wymagań Państwa co do raportowania i od uzgodnień. Specyficzne szczegóły powinny znaleźć odzwierciedlenie w tej sekcji/odcinku procedury].

2. ZAŁATWIANIE RAPORTÓW OBOWIĄZKOWYCH

2.1. Z chwilą otrzymania obowiązkowego raportu, musi on zostać uprawomocniony, by zapewnić, że zgłaszający dostarczył wszystkie istotne informacje.

2.2. Następnie, zgłoszenie musi zostać sklasyfikowane wg następujących kategorii:

a) wypadek;

b) poważny incydent;

c) incydent;

d) inne zdarzenie.

2.3. Po zaklasyfikowaniu, raport zostanie wprowadzony do odpowiedniej bazy danych z przypisanym mu numerem referencyjnym.

2.4. Status każdego raportu będzie kategoryzowany i uaktualniany następująco:

a) Zawiadomienie wstępne: Do oceny/zbierać dalsze informacje, wg adnotacji.

b) W trakcie badania: W trakcie badania prowadzonego przez [nazwa instytucji odpowiedzialnej za badanie wypadków/dostawca usług], wg adnotacji.

c) Badanie zakończone: Wyniki badania/dane otrzymano i wprowadzono do bazy.

d) Zamknięte: Żadne dalsze działania nie jest wymagane.

Uwaga.– Za zawiadomienie i przedłożenie raportu z wypadku i poważnego incydentu do ICAO odpowiada [nazwa instytucji odpowiedzialnej za badanie wypadków].

[Uwaga: Państwa, w których jest kilka instytucji odpowiedzialnych za regulację bezpieczeństwa powinny ustalić odpowiednią koordynację i opracować dostęp do bazy danych (np. CAA, instytucja odpowiedzialna za badanie wypadków)].

3. KLASYFIKACJA WYPADKU / POWAŻNEGO INCYDENTU/ INCYDENTU

3.1. Klasyfikacja wypadku, poważnego incydentu i innego incydentu będzie oparta na definicjach Załącznika 13 ICAO do Konwencji chicagowskiej.

3.2. Zdarzenia, które są klasyfikowane jako wypadki lub poważne incydenty mogą wymagać przeprowadzenia niezależnych badań przez [nazwa instytucji odpowiedzialnej za badanie wypadków]. W takich przypadkach, przydzielony przedstawiciel CAA śledzi wyniki niezależnego procesu badania i wprowadza uaktualnienia [nazwa bazy danych CAA].

3.3. W odniesieniu do incydentów i innych zdarzeń (włącznie z awariami/ usterkami/ niesprawnościami/ kłopotami obsługowymi), które nie są podmiotem procesu badawczego, który jest niezależny od Państwa, przydzielony przedstawiciel CAA będzie współpracować z odnośną stroną w celu prowadzenia dalszego dochodzenia i przedłożenia raportu, zależnie od tego czy jest to praktykowane.

4. DALSZE DOCHODZENIE

4.1. Przy zdarzeniach, które wymagają od wewnętrznego systemu jakości/bezpieczeństwa dostawcy usług dodatkowego działania lub badania, odpowiedni przedstawiciel CAA będzie współpracować z upoważnionym, odpowiedzialnym za jakość/bezpieczeństwo przedstawicielem dostawcy usług by dopilnować procesu badania i terminowość jego zamknięcia, zależnie co trzeba będzie.

4.2. Przydzielony przedstawiciel CAA monitoruje i określa czy interwencja CAA jest potrzebna przed, w trakcie lub po zamknięciu przez dostawcę usług wewnętrznego badania zdarzenia dotyczącego bezpieczeństwa i procesu, który miał się zakończyć jakimś postanowieniem.

4.3. Z chwilą skompletowania i otrzymania raportu z dalszego badania, przedstawiciel krajowego CAA wprowadza wszystkie otrzymane przedmiotowe informacje do odpowiedniej bazy danych. W przypadku, gdy raport z badania jest wystawiony przez [nazwa instytucji odpowiedzialnej za badanie wypadków] przedstawiciel krajowego CAA współdziała z tą instytucją w celu koniecznego wprowadzenia takich danych do bazy danych.

4.4. Działania administracyjne podejmowane na podstawie wniosków wynikających z raportów badania zdarzenia, tam gdzie uzna się za konieczne, to takie zalecenia są przekazywane przez odpowiedniego inspektora do DGCA, celem zatwierdzenia zgodnie z procedurą (nr referencyjny…) krajowego CAA egzekwowania przepisów. W przypadku raportów z badania wydanych przez (nazwa Organu ds. badania wypadków) należy starannie się przyjrzeć celowi badania, wskazanemu w Załączniku 13 do Konwencji chicagowskiej.

Załącznik A
Część I. RAMY CZASOWE NA RAPORTOWANIE (PRZYKŁAD):

	*Zawiadamianie CAA i/lub instytucji odpowiedzialnej za badanie wypadków**	*Przedłożenie Obowiązkowego Raportu agenci CAA i/lub instytucji odpowiedzialnej za badanie wypadków ***	*Raport z badania –do CAA****
Wypadek	Natychmiast/najszybciej jak to możliwe	W ciągu 24 godzin	90 dni
Poważny incydent	Natychmiast/najszybciej jak to możliwe	W ciągu 48 godzin	60 dni
Incydent	Nie dotyczy	W ciągu 72 godzin	30 dni (tam gdzie wymagane

* Telefon, fax lub email w większości przypadków stanowić będzie najbardziej odpowiedni i najszybszy środek przekazania zawiadomienia.
** Kolumna nie dotyczy społeczeństwa.
*** Kolumna nie dotyczy raportów z badania wypadków od państwowej instytucji odpowiedzialnej za badanie wypadków.

CZĘŚĆ II. PRZYKŁADY WYDARZEŃ, KTÓRE PODLEGAJĄ RAPORTOWANIU

Uwaga.– Poniższy wykaz nie jest wyczerpujący i nie obejmuje wypadków.

Operator lotniczy

- sytuacje bliskie zderzeniu, wymagające manewru w celu uniknięcia zderzenia lub sytuacji niebezpiecznej, lub sytuacja, w której zastosowanie unikowego byłoby właściwe;
- minimalne uniknięcie zderzenia z ziemią w locie kontrolowanym;
- przerwane starty z zamkniętej lub zajętej drogi startowej, z drogi kołowania[1] lub nieprzydzielonej drogi startowej;
- starty z zamkniętej lub zajętej drogi startowej, z drogi kołowania1 lub nieprzydzielonej drogi startowej;
- lądowania lub próby lądowań na zamkniętej lub zajętej drodze startowej, na drodze kołowania1 lub nieprzydzielonej drodze startowej;
- rażące błędy dotyczące osiągnięcia przewidzianych osiągów podczas startu lub początkowego wznoszenia;
- nieklasyfikowane jako wypadek pożary i dym w kabinie pasażerskiej lub w przedziałach towarowych cargo, lub pożar silników, nawet jeżeli zostały ugaszone z wykorzystaniem środków gaśniczych;
- wydarzenia wymagające awaryjnego użycia tlenu przez załogę lotniczą;
- usterki w konstrukcji statku powietrznego lub wypadnięcia części silnika/turbiny poza samolot, które nie są klasyfikowane jako wypadek;
- wiele niesprawności jednego lub większej liczby systemów statku powietrznego, poważnie wpływające na jego użytkowanie;
- utrata zdolności do wykonywania czynności w locie przez załogę lotniczą;
- ilość paliwa wymagająca zgłoszenia przez pilota sytuacji awaryjnej;
- wtargnięcia na drogi startowe, klasyfikowane jako zagrożenia „A". Podręcznik dotyczący zapobiegania wtargnięciom na drogę startową (Doc 9870) The Manual on the Prevention of Runway Incursions zawiera informacje na temat klasyfikacji zagrożeń;
- incydenty podczas startu lub lądowania, takie jak niedolot, przelecenie, wypadnięcie z drogi startowej;
- awarie systemów, zjawiska atmosferyczne, przekroczenia ograniczeń parametrów lotu lub inne zdarzenia, które mogły spowodować utrudnienia w sterowaniu statku powietrznego;

[1] Z wyjątkiem uprawnionych operacji śmigłowcami

- awaria więcej niż jednego systemu w systemie nadmiarowym, niezbędnym do sterowania i nawigacji statku powietrznego;

- *[Uwaga: Każde inne incydenty lub zdarzenia, które Państwo uzna za wymagające zgłoszenia na mocy niniejszego obowiązkowego systemu raportowania].*

Obsługa techniczna

- wszelkie awarie/nieprawidłowe działanie, uszkodzenie płatowca, silnika, śmigła, podzespołu lub systemu, stwierdzone podczas planowej lub nieplanowej obsługi statku powietrznego /płatowca/silników/podzespołów, które mogłoby ewentualnie doprowadzić do wypadku operacyjnego statku powietrznego lub do poważnego zdarzenia (jeżeli nie zostały naprawione niezwłocznie);

- *[Uwaga: wszelkie inne incydenty lub zdarzenia które Państwo uzna za wymagające zgłoszenia na mocy niniejszego obowiązkowego systemu raportowania].*

Organizacje projektowe i produkcyjne

- każde niedociągnięcie/awaria/nieprawidłowe działanie, uszkodzenie produktu lub obsługi wykryte przez lub, na które zwrócono uwagę organizacji projektowej/produkcyjnej, które może wymagać ewentualnego wydania Awaryjnej Dyrektywy Zdatności (EAD), Dyrektywy Zdatności (AD) lub Alarmowego Biuletynu Serwisowego (ASB);

- *[Uwaga: każde inne zdarzenie lub incydent, które Państwo uzna, że należy zgłosić zgodnie z niniejszym obowiązkowym systemem powiadamiania].*

Operator lotniska

- wtargnięcia na drogę startową (bez udziału ATC);

- wypadnięcie z drogi startowej/wyjechanie poza jej długości (bez udziału ATC);

- awaria lub poważne nieprawidłowe działanie świateł lotniska;

- uszkodzenie statku powietrznego lub silnika, wynikające z kontaktu z/lub zassaniem obcych przedmiotów lub szczątków metalowych na drodze startowej lub drodze kołowania;

- incydenty w granicach lotniska, obejmujące uszkodzenie statku powietrznego lub ewentualne skutki na bezpieczeństwo statków powietrznych przemieszczających się po ziemi;

- *[Uwaga: każde inne zdarzenie lub incydent, które Państwo uzna, że należy zgłosić zgodnie z niniejszym obowiązkowym systemem powiadamiania].*

Podmiot świadczący usługi ANS/CNS

- każda awaria/nieprawidłowe działanie, uszkodzenie sprzętu lub systemu związanego z ANS/CNS, wykryte podczas działania lub obsługi sprzętu, które mogłoby doprowadzić do wypadku statku powietrznego podczas operacji lotniczej, lub do poważnego incydentu;

- naruszenie przestrzeni powietrznej;

- bliska utrata kontroli w locie sterowanym samolotu CFIT;

- znaczące nieutrzymanie poziomu lotu (level bust);

- utrata separacji;

- wtargnięcia na drogę startową (z udziałem łączności ATC);

- wypadnięcie/wyjechanie z drogi startowej (z udziałem łączności ATC);

- wszystkie inne zgłoszone (i zweryfikowane przez operatora ANS/CNS) niedociągnięcia/ defekty/nieprawidłowe działania, które uważa się za mające wpływ na bezpieczeństwo żeglugi powietrznej.

- *[Uwaga.- Każde inne zdarzenie lub incydent, które Państwo uzna, że należy zgłosić zgodnie z obowiązkowym systemem zgłaszania].*

Uwaga.– W Państwie, w którym występują inne specyficzne dla sektora lub podmiotu lotniczego obowiązkowe (przymusowe) systemy raportowania, zgodne z Załącznikiem 8 do Konwencji chicagowskiej, Część II, 4.2.3(f) i 4.2.4 [stała informacja o zdatności samolotu do lotu], może zaistnieć potrzeba skorelowania lub zintegrowania ich z ogólnokrajową, państwową, obowiązkową procedurą raportowania.

Dodatek 4 do Rozdziału 4
WSKAŹNIKI WYDOLNOŚCI BEZPIECZEŃSTWA KRAJOWEGO SSP

1. Tabele 4-A4-1 do 4-A4-4 (przykłady wskaźników bezpieczeństwa) dostarczają przykładów zebranych wskaźników działania bezpieczeństwa (SPI) Państwa i odpowiadających im kryteriów ustawiania poziomów alarmowych i docelowych. Podane po prawej stronie tablic, wskaźniki (SPI) systemu SMS są przedstawione dla pokazania niezbędnej korelacji pomiędzy wskaźnikami bezpieczeństwa SSP i SMS. Taka tablica może być przygotowana przez Państwo i odpowiednio wypełniona możliwie największą ilością wszelkich istniejących lub realnych wskaźników bezpieczeństwa. Wskaźniki SPI systemu SMS będą musiały być opracowane przez dostawców usług, stosownie do oczekiwań wynikających ze wskaźników bezpieczeństwa krajowego SSP. Aby zapewnić by wskaźniki SSP i SMS przystawały do siebie, Państwo będzie musiało czynnie zaangażować dostawców usług w opracowanie swych (krajowych) SPI SMS. Można się spodziewać, że SPI SMS będą znacznie pełniejsze niż wskaźniki bezpieczeństwa SSP. Z takiego banku wskaźników, Państwo będzie mogło wówczas wyselekcjonować odpowiedni pakiet wskaźników w celu monitorowania i mierzenia w swym SSP ALoSP. Jest możliwe, by niektóre wskaźniki bezpieczeństwa/jakości utrzymywane były (przez Państwo lub dostawców usług) dla celów dodatkowych, dlatego nie muszą być włączone dla monitorowania i mierzenia poziomów w SSP (lub SMS). Bo one będą w przedsiębiorstwie zazwyczaj wskaźnikami niskopoziomowymi lub wskaźnikami dla szczególnych procesów w organizacji.

2. Tabela 4-A4-5 (przykład wykresu wskaźników bezpieczeństwa SSP) jest przykładem tego jak może wyglądać wykres wskaźnika SSP dużych konsekwencji dla bezpieczeństwa. W tym przypadku jest to suma incydentów zgłoszonych/także obowiązkowo przez dostawców usług w Państwie. Wykres po lewej stronie przedstawia wynik roku poprzedniego, podczas gdy po prawej stronie widać postępujący trend tegoroczny. Poziom ustawienia alarmu bazuje na kryteriach odstępstw od podstawowej, standardowej miary bezpieczeństwa. Wzór w arkuszu Excel, to „=STDEVP". Dla potrzeb ręcznego obliczenia odstępstwa od standardu, formuła jest taka:

$$\sigma = \sqrt{\frac{\sum(x \ -\mu)^2}{N}}$$

gdzie „X" stanowi wartość każdego punktu danych; „N" to ilość punktów danych, a „U" to średnia wartość wszystkich punktów danych.

3. Nastawa docelowa jest pożądanym polepszeniem w procentach (w tym przypadku 5%) w stosunku do średniej punktów z roku poprzedniego. Należy zauważyć, że dla zapewnienia wiarygodności wskaźnika bezpieczeństwa, faktyczny interwał między punktami danych jak i wyznacznik ilości zdarzeń trzeba będzie określić w oparciu o właściwości każdego zestawu danych. Dla wydarzeń występujących bardzo rzadko, interwał między punktami danych może, przykładowo, będzie musiał być aktualizowany rocznie a nie kwartalnie. Podobnie, wyznacznik ilości zdarzeń może być, przykładowo, co 100 000 operacji powietrznych zamiast co 1000 operacji powietrznych. Wykres jest generowany przez arkusz danych pokazanych w tabeli 4-A4-6.

4. Arkusz danych w tabeli 4-A6 (arkusz danych dla przykładowego wykresu wskaźnika bezpieczeństwa) stosuje się do dla generowania wykresu wskaźnika bezpieczeństwa, jak pokazano w tabeli 4-A4-5. Ten arkusz można też wykorzystać dla wygenerowania wykresu każdego innego wskaźnika bezpieczeństwa, wprowadzając odpowiednie dane i dostosowując wskaźnik bezpieczeństwa do cech klienta. Trzy linie wykreślające poziomy alarmów i linia wartości docelowej są generowane automatycznie w oparciu o swe odnośne ustawienia w tym arkuszu danych.

5. Tabela 4-A4-7 (przykład podsumowania osiągów SSP ALoSP) jest podsumowaniem wszystkich wskaźników bezpieczeństwa krajowego SSP, z adnotacją o wynikach ich odpowiednich poziomów alarmowych i docelowych. Takiego podsumowania można dokonać na koniec każdego okresu monitorowania, w celu przygotowania przeglądu osiągów SSP ALoSP. Jeżeli pożądane jest bardziej ilościowe podsumowanie osiągów, każdej odpowiedzi na TAK/NIE można przydzielić odpowiednią ilość punktów za każde osiągnięcie dotyczące celu i alarmu. Na przykład:

Wskaźniki wysokopoziomowych konsekwencji:	
Nie przekroczono poziomu alarmowego?	[Tak (4), Nie (0)]
Osiągnięto cel?	[Tak (3), Nie (0)]
Wskaźniki niskopoziomowych konsekwencji:	
Nie przekroczono poziomu alarmowego?	[Tak (2), Nie (0)]
Osiągnięto cel?	[Tak (1), Nie (0)]

Może to pozwolić na uzyskanie cyfrowego wyniku sumarycznego (lub procentowego) by pokazać całościowe działanie wskaźników bezpieczeństwa ALoSP na koniec danego okresu monitorowania.

Tabela 4-A4-1. Wskaźniki działania bezpieczeństwa, dotyczące operatorów lotniczych

Wskaźniki bezpieczeństwa SSP (Ogółem Państwo)						*Wskaźniki wyników bezpieczeństwa SMS (indywidualny podmiot lotniczy)*					
Wskaźniki wysokopoziomowe konsekwencji (oparte na zdarzeniach/wynikach)			*Wskaźniki niskopoziomowe konsekwencji (oparte na zdarzeniach/działaniach)*			*Wskaźniki wysokopoziomowe konsekwencji (oparte na zdarzeniach/wynikach)*			*Wskaźniki niskopoziomowe konsekwencji (oparte na zdarzeniach/działaniach)*		
Wskaźnik bezpieczeństwa	*Kryteria poziomów alarmowych*	*Kryteria poziomów docelowych*	*Wskaźnik bezpieczeństwa*	*Kryteria poziomów alarmowych*	*Kryteria poziomów docelowych*	*Wskaźnik bezpieczeństwa*	*Kryteria poziomów alarmowych*	*Kryteria poziomów docelowych*	*Wskaźnik bezpieczeństwa*	*Kryteria poziomów alarmowych*	*Kryteria poziomów docelowych*
Operatorzy lotniczy (tylko operatorzy danego Państwa)											
CAA: Łączna liczba wypadków/poważnych incydentów operatorów lotniczych(np. na 1.000FH) - miesięcznie/ kwartalnie	Średnia +1/2/3 SD (ustawienie roczne / dwuletnie)	__% (np. 5) poprawy pomiędzy każdą roczną średnią	CAA: łącznie, %LEI lub liczba ustaleń [niezgodności] w corocznym audycie śledzenia operatora lotniczego	Rozważane	Rozważane	Liczba poważnych incydentów we flocie poszczególnego operatora lotniczego, miesięcznie (np. na 1.000 FH)	Średnia +1/2/3 SD (ustawienie roczne lub dwuletnie)	__%(np. 5%) poprawy pomiędzy każdą roczną średnią	Liczba incydentów we flocie połączonej operatora lotniczego, miesięcznie, (np. na 1.000FH)	Średnia +1/2/3 SD (ustawienie roczne lub dwuletnie)	__% (np.5%) poprawy pomiędzy każdą roczną średnią
CAA: Łączna liczba incydentów zgaśnięcia silnika w locie (IFSD) u operatorów lotniczych (np. na 1.000FH) - miesięcznie/ kwartalnie	Średnia +1/2/3 SD. (ustawienie roczne/ dwuletnie)	__% (np. 5) poprawy pomiędzy każdą roczną średnią	CAA: zbiorczo, % LEI lub liczba odkryć niezgodności przez roczne inspekcje w bazie obsługi liniowej operatora lotniczego	Rozważane	Rozważane	Liczba poważnych incydentów we flocie połączonej operatora lotniczego, miesięcznie (np. na 1.000FH)	Średnia +1/2/3 SD (ustawienie roczne lub dwuletnie)	__%(np. 5%) poprawy pomiędzy każdą roczną średnią	% LEI lub liczba odkryć niezgodności przez wewnętrzne roczne audyty QMS/SMS (liczba niezgodności per audyt)	Rozważane	Rozważane
			CAA: Średnia procentowa LEI z rocznych inspekcji RAMP obcych przewoźników (dla każdego obcego przewoźnika)	Rozważane	Rozważane	Liczba incydentów zgaśnięcia silnika w locie (IFSD) u operatorów lotniczych (np. na 1.000FH)	Średnia +1/2/3 SD (ustawienie roczne lub dwuletnie)	__%(np. 5%) poprawy pomiędzy każdą roczną średnią	Liczba zagrożeń zgłoszonych dobrowolnie przez przewoźnika (np. na 1000 FH)	Rozważane	Rozważane
			CAA: Liczba zdarzeń DGR na przewoźnika (np. 1000 FH), łącznie	Średnia +1/2/3 SD. (ustawienie roczne lub dwu letnie)	__% (np. 5) poprawy pomiędzy każdą roczną średnią				Liczba zgłoszonych przez przewoźnika incydentów DGR	Średnia +1/2/3 SD (ustawienie roczne lub dwuletnie)	__% (np. 5%) poprawy pomiędzy każdą roczną średnią
Itd.											

Tabela 4-A4-2. Wskaźniki działania bezpieczeństwa dotyczące operatorów lotnisk

Wskaźniki bezpieczeństwa SSP (Ogółem Państwo)						Wskaźniki wyników bezpieczeństwa SMS (indywidualny podmiot lotniczy)					
Wskaźniki wysokopoziomowe konsekwencji (oparte na zdarzeniach/wynikach			*Wskaźniki niskopoziomowe konsekwencji (oparte na zdarzeniach/ działaniach)*			*Wskaźniki wysokopoziomowe konsekwencji (oparte na zdarzeniach/wynikach)*			*Wskaźniki niskopoziomowe konsekwencji (oparte na zdarzeniach/działaniach)*		
Wskaźnik bezpieczeństwa	*Kryteria poziomów alarmowych*	*Kryteria poziomów docelowych*	*Wskaźnik bezpieczeństwa*	*Kryteria poziomów alarmowych*	*Kryteria poziomów docelowych*	*Wskaźnik bezpieczeństwa*	*Kryteria poziomów alarmowych*	*Kryteria poziomów docelowych*	*Wskaźnik bezpieczeństwa*	*Kryteria poziomów alarmowych*	*Kryteria poziomów docelowych*
Operatorzy lotnisk											
CAA: Łączna liczba miesięczna/ kwartalna wypadków/ poważnych incydentów na ziemi z udziałem dowolnego samolotu (np. na 10.000 ruchów naziemnych)	Średnia +1/2/3 SD (ustawienie roczne lub dwuletnie)	__% (np. 5%) poprawy pomiędzy każdą roczną średnią	CAA: % LEI lub liczba [niezgodności] wychwyconych przez roczny audyt śledzenia operatora lotniczego, łącznie	Rozważane	Rozważane	Liczba naziemnych wypadków/ poważnych incydentów operatora lotniska z udziałem dowolnych samolotów (np. na 10000 ruchów na ziemi), kwartalnie	Średnia +1/2/3 SD (ustawienie roczne lub dwuletnie)	-% (np. 5%) poprawy pomiędzy każdą roczną średnią	% LEI lub liczba niezgodności odkrytych przez wewnętrzne roczne audyty QMS/SMS operatora lotniska (liczba odkryć per audyt)	Rozważane	Rozważane
CAA: Łączna liczba kwartalna incydentów wypadnięcia z drogi startowej , z udziałem dowolnego samolotu (np. na 10000 odlotów)	Średnia +1/2/3 SD (ustawienie roczne lub dwuletnie)	__% (np. 5%) poprawy pomiędzy każdą roczną średnią				Łączna liczba operatora lotniska incydentów wypadnięcia z drogi startowej , z udziałem dowolnego samolotu (np. na 10000 odlotów)	Średnia +1/2/3 SD (ustawienie roczne lub dwuletnie)	-% (np. 5%) poprawy pomiędzy każdą roczną średnią	Liczba, kwartalna, zgłaszanych przez operatora lotniska zagrożeń na drodze startowej („zguby", odpady) (np. na 10000 ruchów na ziemi)	Rozważane	Rozważane
CAA: Łączna liczba (miesięczna/ kwartalna) incydentów wtargnięcia na drogę startową, z udziałem dowolnego samolotu (np. na 10000 odlotów)	Średnia +1/2/3 SD (ustawienie roczne lub dwuletnie)	-% (np. 5%) poprawy pomiędzy każdą roczną średnią				Liczba incydentów wtargnięć na drogę startową, z udziałem dowolnego samolotu, u operatora lotniska (np. na 10000 odlotów)	Średnia +1/2/3 SD. (ustawienie roczne lub dwuletnie)	-% (np. 5%) poprawy pomiędzy każdą roczną średnią	Liczba dobrowolnych raportów operatora o zagrożeniach (kwartalnie)	Rozważane	Rozważane
CAA: Łączna liczba (miesięczna/ kwartalna) incydentów wtargnięcia na drogę startową, z udziałem dowolnego samolotu (np. na 10000 odlotów)	Średnia +1/2/3 SD (ustawienie roczne lub dwuletnie)	-% (np. 5%) poprawy pomiędzy każdą roczną średnią							Liczba, kwartalna, zgłaszanych przez operatora lotniska uszkodzeń samolotów na drodze startowej przez „zguby", odpady (np. na 10000 ruchów na ziemi)	Średnia +1/2/3 SD. (ustawienie roczne lub dwuletnie)	__%(np.5%) poprawy pomiędzy każdą roczną średnią
Itd.											

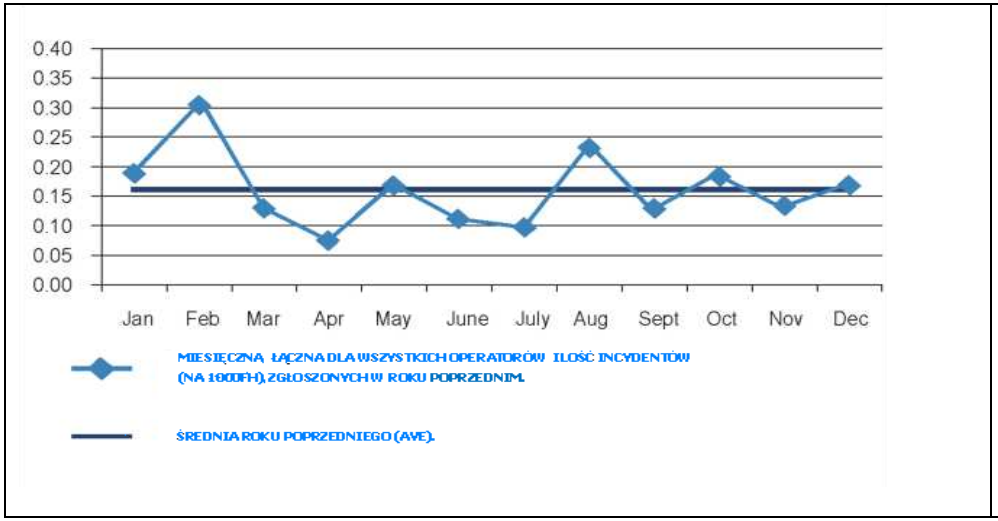
Tabela 4-A4-3. Wskaźniki działania bezpieczeństwa dotyczące operatorów ATS

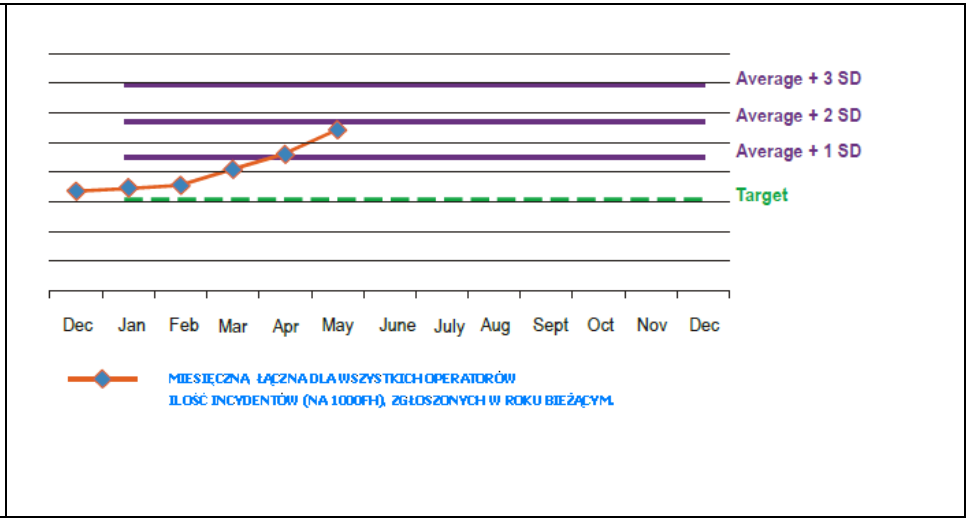
Wskaźniki bezpieczeństwa SSP (Ogółem Państwo)						Wskaźniki wyników bezpieczeństwa SMS (indywidualny podmiot lotniczy)					
Wskaźniki wysokopoziomowe konsekwencji (oparte na zdarzeniach/wynikach			*Wskaźniki niskopoziomowe konsekwencji (oparte na zdarzeniach/działaniach)*			*Wskaźniki wysokopoziomowe konsekwencji (oparte na zdarzeniach/wynikach)*			*Wskaźniki niskopoziomowe konsekwencji ((oparte na zdarzeniach/działaniach)*		
Wskaźnik bezpieczeństwa	*Kryteria poziomów alarmowych*	Kryteria poziomów docelowych	Wskaźnik bezpieczeństwa	*Kryteria poziomów alarmowych*	Kryteria poziomów docelowych	Wskaźnik działania bezpieczeństwa	*Kryteria poziomów alarmowych*	Kryteria poziomów docelowych	Wskaźnik bezpieczeństwa	*Kryteria poziomów alarmowych*	Kryteria poziomów docelowych
Operatorzy ATS											
CAA: Łączna liczba, kwartalnie, poważnych incydentów ATS w przestrzeni FIR – z udziałem dowolnych samolotów (np. na 100000 ruchów w locie)	Średnia +1/2/3 SD (ustawienie roczne lub dwuletnie)	__%(np.5) poprawy pomiędzy każdą roczną średnią	CAA: Łączna dla ATS liczba, incydentów TCAS RA w przestrzeni FIR – z udziałem dowolnych samolotów (np. na 100000 ruchów w locie) kwartalnie	Średnia + 1/2/3 SD (ustawienie roczne lub dwuletnie).	__%(np.5%) poprawy pomiędzy każdą roczną średnią	Łączna liczba, kwartalnie, poważnych incydentów u operatora ATS w FIR z udziałem dowolnych samolotów (np. na 100000 ruchów w locie)	Średnia + 1/2/3 SD (ustawienie roczne lub dwuletnie)	__%(np.5%) poprawy pomiędzy każdą roczną średnią	Liczba incydentów u operatora ATS, kwartalnie, FIR TCAS RA, z udziałem dowolnych samolotów (np. na 100000 ruchów w locie)	Średnia +1/2/3 SD (ustawienie roczne lub dwuletnie)	__% (np.5%) poprawy pomiędzy każdą roczną średnią
			CAA: Liczba, kwartalnie, incydentów nietrzymania poziomu/separacji (LOS) w FIR operatora ATS, z udziałem dowolnych samolotów (np. na 100000 ruchów w locie)	Średnia +1/2/3 SD (ustawienie roczne lub dwuletnie)	__% (np.5%) poprawy pomiędzy każdą roczną średnią	Liczba niebezpiecznych zbliżeń, kwartalnie /rocznie, u operatora ATS (np. na 100000 ruchów w locie)	Przyjąć, że historyczny m, średnioroczn ym jest 3, to ewentualny docelowy mogłaby być 5	Przyjąć, że historycznym, średnioroczny m jest 3, to ewentualny docelowy mogłaby być 2	Liczba incydentów nietrzymania poziomu/separacji (LOS) w FIR operatora ATS, kwartalnie (np. na 100000 ruchów w locie) z udziałem dowolnych samolotów	Średnia +1/2/3 SD (ustawienie roczne lub dwuletnie)	__%(np.5%) poprawy pomiędzy każdą roczną średnią
			CAA: % LEI lub liczba niezgodności odkrytych u operatora ATS w rocznym audycie (ilość odkryć na audyt)	Rozważane	Rozważane				% LEI lub liczba, niezgodności QMS/SMS, odkrytych w wewnętrznym rocznym audycie u operatora ATS (ilość odkryć na audyt)	Rozważane	Rozważane
Itd.											

Tabela 4-A4-4. Organizacje POA/DOA/MRO

Wskaźniki bezpieczeństwa SSP (Ogółem Państwo)						*Wskaźniki działania bezpieczeństwa SMS (indywidualny podmiot lotniczy)*					
Wskaźniki wysokopoziomowe dla konsekwencji (oparte na zdarzeniach/wynikach)			*Wskaźniki niskopoziomowe konsekwencji (oparte na zdarzeniach/działaniach)*			*Wskaźniki wysokopoziomowe konsekwencji (oparte na zdarzeniach/wynikach)*			*Wskaźniki niskopoziomowe konsekwencji (oparte na zdarzeniach/działaniach)*		
Wskaźnik bezpieczeństwa	*Kryteria poziomów alarmowych*	Kryteria poziomów docelowych	Wskaźnik bezpieczeństwa	*Kryteria poziomów alarmowych*	Kryteria poziomów docelowych	Wskaźnik bezpieczeństwa	*Kryteria poziomów alarmowych*	Kryteria poziomów docelowych	Wskaźnik bezpieczeństwa	*Kryteria poziomów alarmowych*	Kryteria poziomów docelowych
Organizacje POA/DOA/MRO											
CAA: Liczba obowiązkowych, kwartalnie, raportów MRO, Na temat usterek	Średnia +1/2/3 SD (ustawienie roczne lub dwuletnie)	__% (np.5%) poprawy pomiędzy każdą roczną średnią	CAA: % LEI lub liczba [niezgodności] wychwyconych przez roczny audyt śledzenia MRO/POA/DOA, zbiorczo,(ilość odkryć na audyt)	Rozważane	Rozważane	Liczba , kwartalnie, reklamacji komponentów z tyt. gwarancji technicznych MRO/POA	Średnia +1/2/3 SD (ustawienie roczne lub dwuletnie)	__% (np.5%) poprawy pomiędzy każdą roczną średnią	% LEI lub liczba, odkryć niezgodności QMS/SMS w wewnętrznym rocznym audycie u operatorów MRO/POA/DOA (ilość odkryć na audyt)	Rozważane	Rozważane
CAA: Liczba, zbiorczo, kwartalnie, produktów operacyjnych POA/DOA, podległych dyrektywom AD i ASB (wg linii produktu)	Rozważane	Rozważane				Liczba, kwartalnie, produktów operacyjnych POA/DOA, podległych dyrektywom AD i Biuletynom ASB (wg linii produktu)	Rozważane	Rozważane	Liczba odrzutów/ usterek, podczas testów/końcowej, kwartalnej inspekcji MRO/POA/DOA (z uwagi na wewnętrzne zagadnienia jakości)	Rozważane	Rozważane
						Liczba, kwartalnie, wymaganych od MRO/POA/DOA raportów o usterkach/większych defektach (zgodnie z wew. systemem jakości)	Rozważane	Rozważane	Liczba dobrowolnych zgłoszeń MRO/POA/DOA o zagrożeniach (personel operacyjny per kwartał)	Rozważane	Rozważane
Itd.											

Tabela 4-A4-5. Przykład wykresu wskaźnika działania bezpieczeństwa SSP (z ustalonymi poziomami alarmowym i docelowymi)





a) Ustawienie poziomu alarmowego:

Poziom alarmowy dla nowego okresu monitorowania (rok bieżący) bazuje na wyniku poprzedniego okresu (rok poprzedni), mianowicie, na średniej jego punktów danych i na odchyłce standardowej. Trzy linie alarmowe to średnia + 1SD, średnia + 2SD i średnia +3SD

b) Uruchomienie poziomu alarmowego:

Alarm (nietypowy/nieakceptowany trend) jest ukazywany, jeżeli spełniony jest którykolwiek z poniżej wymienionych warunków dla aktualnego okresu monitorowania (rok bieżący):

- gdy dowolny pojedynczy punkt jest powyżej linii 3SD
- gdy 2 kolejne punkty znajdują się powyżej linii 2SD
- gdy 3 kolejne punkty znajdują się powyżej linii 1SD

Gdy uruchomi się alarm (potencjalne duże ryzyko lub sytuacja poza kontrolą), oczekuje się podjęcia odpowiedniego dalszego działania, takiego jak dalsza analiza dla ustalenia źródła i pierwotnej przyczyny zbyt dużej liczby incydentów, oraz oczekuje się podjęcia niezbędnego działania dla powstrzymania nieakceptowanego trendu.

c) Ustalenie poziomu docelowego (planowane polepszenie):

Ustawienie wartości docelowej może być mniej złożone niż ustawienie poziomu alarmowego – np. ustawienie wartości docelowej dla nowego okresu monitorowania (rok bieżący), powiedzmy, o 5% niższej (lepszy) od średniej wartości poprzedniego.

d) Osiągnięcie wartości docelowej:

Pod koniec bieżącego roku, jeżeli średnia dla roku bieżącego jest przynajmniej mniejsza o 5%, lub więcej, w stosunku do średniej roku poprzedniego, to będzie się uważać, że został osiągnięty cel, ustawiony na polepszenie o 5%.

e) Poziomy alarmowe i wartość docelowa – okres ważności:

Poziomy alarmowe i docelowe należy przeglądać/ustawiać na nowo dla każdego nowego okresu monitorowania, bazując na średniej z tego samego okresu poprzedzającego i na SD.

Tabela 4-A4-6. Próbka arkusza danych, stosowanego do generowania wykresu wskaźnika bezpieczeństwa SSP (z kryteriami ustalania poziomów alarmowych i docelowych)

Rok poprzedni				
miesiąc	Łączna FH wszystkich operatorów	Incydenty wszystkich operatorów	Wielkość zdarzeń [2]	średnia
styczeń	51837	10.00	0.19	0.16
luty	48406	15.00	0.31	0.16
marzec	53354	7.00	0.13	0.16
kwiecień	52513	4.00	0.08	0.16
maj	54037	9.00	0.17	0.16
czerwiec	52673	6.00	0.11	0.16
lipiec	54086	5.00	0.09	0.16
sierpień	54043	13.00	0.24	0.16
wrzesień	52383	7.00	0.13	0.16
październik	53042	10.00	0.19	0.16
listopad	51353	7.00	0.14	0.16
grudzień	53006	9.00	0.17	0.16
		Średnia	0.16	
		SD	0.06	

Rok bieżący							
Miesiąc	Łączna FH wszystkich operatorów	Incydenty wszystkich operatorów	Wielkość zdarzeń *	Średnia roku poprzedniego +1SD	Średnia roku poprzedniego +2SD	Średnia roku poprzedniego +3SD	średnia docelowa na rok bież
styczeń	53006	9.00	0.17	0.23	0.29	0.36	0.16
luty	51635	9.00	0.17	0.23	0.29	0.36	0.15
marzec	44295	8.00	0.18	0.23	0.29	0.36	0.15
kwiecień	48232	10.00	0.21	0.23	0.29	0.36	0.15
maj	47176	11.00	0.23	0.23	0.29	0.36	0.15
czerwiec	47469	13.00	0.27	0.23	0.29	0.36	0.15
lipiec				0.23	0.29	0.36	0.15
sierpień				0.23	0.29	0.36	0.15
wrzesień				0.23	0.29	0.36	0.15
październik				0.23	0.29	0.36	0.15
listopad				0.23	0.29	0.36	0.15
grudzień				0.23	0.29	0.36	0.15
		Średnia					
		SD					

Średnia +1SD	Średnia +2SD	Średnia +3SD
0.23	0.29	0.35

Celem roku bieżącego jest, powiedzmy, polepszenie średniej o 5% w stosunku do średniej z roku poprzedniego, która stanowi	0.15

Kryteria ustalania poziomu alarmowego na rok bazują na roku poprzednim [średnia + 1/2/3 SD]

[2] Obliczenie wielkości (na 1000 FH)

Tabela 4-A4-7. Przykład podsumowania wyników SSP ALoSP Państwa „X" (przykładowo za rok 2010)

Wskaźniki niskopoziomowe konsekwencji dotyczących bezpieczeństwa					
Opis wskaźnika bezpieczeństwa SI		Kryteria poziomów alarmowych SI (dla 2010)	Czy przekroczono poziom alarmowy? [TAK/NIE]	Kryteria poziomu docelowego SI (dla 2010)	Czy osiągnięto cel? [TAK/NIE]
1	Liczba wypadków/ poważnych incydentów (zbiorczo miesięcznie) u przewoźników [na 1000FH]	Średnia roku 2009 +1/2/3 SD. (wyciągana coroczne)	Tak	Poprawa średniej 2010 o 5% wzgl. średniej z 2009	Nie
2	CAA Zbiorcza miesięczna liczba wypadków/poważnych incydentów samolotów na ziemi [na 1000 FH]	Średnia roku 2009 +1/2/3 SD. (wyciągana corocznie)	Tak	Poprawa średniej 2010 o 3% wzgl. średniej z 2009	Tak
3	CAA Miesięczna liczba poważnych incydentów wszystkich samolotów (na 100000 ruchów samolotów w powietrzu) w ATS w FIR	Średnia roku 2009 +1/2/3 SD. (wyciągana corocznie)	Nie	Poprawa średniej 2010 o 3% wzgl. średniej z 2009	Nie

Wskaźniki niskopoziomowe konsekwencji dotyczących bezpieczeństwa					
Opis wskaźnika bezpieczeństwa SI		Kryteria poziomów alarmowych SI (dla 2010)	Czy przekroczono poziom alarmowy? [TAK/NIE]	Kryteria poziomu docelowego SI (dla 2010)	Czy osiągnięto cel? [TAK/NIE]
1	Roczne wyniki zbiorcze śledzenia/audytów operatorów lotniczych	>25% średniej LEI lub każda niezgodność na poziomie 1 lub ponad 5 niezgodności na poziomie 2, na audyt	Tak	<10% średniej LEI lub <1 niezgodność na poziomie 2, na audyt	Nie
2	Roczna średnia LEI inspekcji CAA śledzenia bazy operatora lotniczego (osobno dla każdego przewoźnika)	>25% średniej LEI lub każda niezgodność na Poziomie 1 lub ponad 5 niezgodności na Poziomie 2, na audyt	Tak	<10% średniej LEI	Tak
3	Program corocznej wyrywkowej inspekcji RAMP u obcych przewoźników	>25% średniej LEI lub każda niezgodność na Poziomie 1 lub ponad 5 niezgodności na Poziomie 2, na audyt, lub <25% z inspekcjonowanych obcych przewoźników	Tak	Nie mniej niż 50% obcych przewoźników ma być poddanych inspekcji	Nie
4	Zbiorcze wyniki CAA z dla corocznego śledzenia/ audytu operatorów lotniskowych	>25% średniej LEI lub każda niezgodność na Poziomie 1 lub >5 niezgodności na Poz. 2, na audyt	Nie	<10% średniej LEI oraz <1 niezgodność na Poziomie 2	Nie

Wskaźniki niskopoziomowe konsekwencji dotyczących bezpieczeństwa					
Opis wskaźnika bezpieczeństwa SI		Kryteria poziomów alarmowych SI (dla 2010)	Czy przekroczono poziom alarmowy? [TAK/NIE]	Kryteria poziomu docelowego SI (dla 2010)	Czy osiągnięto cel? [TAK/NIE]
1	Zbiorcze roczne wyniki CAA śledzenia/ audytów u operatorów ATS	>25% średniej LEI; lub każda niezgodność na Poziomie 1 lub >5 niezgodności na Poziomie 2, na audyt	Tak	<10% średniej LEI oraz <1 niezgodności na Poziomie 2	Tak
2	Zbiorcze kwartalne wielkości incydentów w FIR TCAS RA – z udziałem samolotów [na 100.000 ruchów w powietrzu]	Średnia roku 2009 +1/2/3 SD (wyciągana corocznie)	Tak	Polepszenie o 5% średniej 2010 wobec średniej z 2009	Nie
3	Zbiorcze roczne wyniki CAA śledzenia /audytowania DiM/MRO	>25% średniej LEI lub każda niezgodność na Poziomie 1 lub > 5 niezgodności na Poziomie 2, na audyt	Tak	<10% średniej LEI lub <1 niezgodności na Poziomie 2	Tak
4	CAA - zbiorcze kwartalne ilości reklamacji u AMO(MRO z powodu (poważnych) defektów podzespołów	Średnia roku 2009 +1/2/3 SD (wyciągana corocznie)	Nie	Polepszenie o 5% średniej roku 2010 wobec średniej z 2009	Nie

Uwaga 1. – Inne wskaźniki procesu. Poza wyżej wymienionymi wskaźnikami poziomu bezpieczeństwa SSP, w każdym obszarze operacyjnym mogą być inne wskaźniki poziomu bezpieczeństwa systemów. Przykładami mogą być szczególne wskaźniki monitorowania procesu lub systemu w AIR, OPS, AGA lub wskaźniki powiązane z programami opartymi na działaniu, takimi jak zarządzanie ryzykiem zużycia [komponentów, zmęczenia ludzi] lub zarządzanie paliwem. Takie szczególne wskaźniki monitorowania procesu lub systemu muszą być prawidłowo administrowane jako część systemu lub procesu, którego dotyczą. Mogą być postrzegane jako wskaźniki poziomu dla konkretnego systemu lub procesu, które podwiązują się pod wskaźniki dużych konsekwencji dla bezpieczeństwa SSP. Należy je omówić w podręczniku odnośnych systemów lub procesów/SOP swoich systemów. Niezależnie od tego, kryteria nastawiania poziomów alarmowych lub wartości docelowych dla takich wskaźników, najlepiej jest zgrać z kryteriami wskaźników poziomu bezpieczeństwa SSP, tam gdzie to da się zrobić.

Uwaga 2. – Wybór wskaźników i poziomów Kombinacja (lub zestaw) wskaźników wysokopoziomowych i niskopoziomowych konsekwencji dotyczących bezpieczeństwa ma być wybrana przez Państwo zgodnie z zakresem jego systemu lotniczego. Dla tych wskaźników, gdzie sugerowane kryteria nastawiania poziomów alarmowych lub docelowych nie mają zastosowania, Państwo może uznać za właściwe każde inne kryterium. Ogólne wytyczne są takie: ustalić alarmy i wartości docelowe tak, by uwzględniały osiągi niedawne i bieżące.

Dodatek 5 do Rozdziału 4
OCHRONA INFORMACJI O BEZPIECZEŃSTWIE

1.1. Nieopublikowanie dokumentu o bezpieczeństwie międzynarodowego lotnictwa cywilnego jest wynikiem, między innymi, jednego kluczowego czynnika: ciągłego procesu nauczania opartego na powiększaniu informacji i dobrowolnej ich wymianie. Już dawno stwierdzono, że usiłowania skierowane na poprawienie bezpieczeństwa we współczesnym lotnictwie cywilnym muszą być budowane na obiektywnych danych. Jest kilka źródeł takich danych dostępnych dla lotnictwa cywilnego. Po ich połączeniu, dają podstawę dla solidnego zrozumienia mocnych i słabych stron operacji lotniczych.

1.2. Historycznie, informacje pochodzące z badania wypadków i incydentów stanowiły kościec działań nakierowanych na polepszenie projektowania sprzętu, procedur obsługowych, szkolenia załóg lotniczych, systemów kontroli ruchu lotniczego, projektowania lotnisk i ich funkcji, usług meteorologicznych i innych aspektów krytycznych dla systemu bezpieczeństw transportu lotniczego. W ostatnich latach, dostępność środków technicznych doprowadziła do przyspieszonego zbierania danych o bezpieczeństwie i rozbudowy systemów ich przetwarzania (SDCPS).

1.3. SCDPS umożliwił społeczności lotnictwa cywilnego uzyskanie głębszego rozumienia błędów operacyjnych: dlaczego się zdarzają, co można zrobić by zminimalizować ich występowanie i jak ograniczać ich negatywny wpływ na bezpieczeństwo. Nie podlega dyskusji, że zagrożenia prowadzą do błędów operacyjnych w lotnictwie, z których większość jest nieumyślna. Błędy popełniają ludzie dobrze wyszkoleni i z dobrymi intencjami, podczas obsługi technicznej, podczas używania dobrze zaprojektowanego sprzętu i sterowania nim. Dla tych rzadkich przypadków uznanych, zgodnie z prawem, za czyny, które mają być dokonane z zamiarem spowodowania uszkodzenia lub ze świadomością, że uszkodzenie może być skutkiem równoznacznym z lekkomyślnym postępowaniem, rażącym niedbalstwem, umyślnym występkiem, miejscowe systemy egzekwowania prawa zapewniają, by nie został przerwany łańcuch odpowiedzialności osobistej. Takie podwójne podejście, łączące lepsze rozumienie nieumyślnych błędów operacyjnych z odpowiednim egzekwowaniem prawa przez odnośną władzę, tam gdzie to ma miejsce, dobrze służy lotnictwu cywilnemu, jeśli chodzi o bezpieczeństwo i jednocześnie zapewnia, że dla osób naruszających prawo nie ma miejsca.

1.4. Jednak ostatnie lata pokazują trend w lotnictwie cywilnym, polegający na tym, że informacje z SDCPS są wykorzystywane dla celów dyscyplinarnych i egzekucyjnych. W niektórych przypadkach, takie informacje są dopuszczane jako dowód w postępowaniach sądowych, skutkując postawieniem oskarżeń przeciw osobom uczestniczącym w takich zdarzeniach. Stawianie oskarżeń kryminalnych w zdarzeniach lotniczych będących skutkiem nieumyślnych błędów operacyjnych może utrudnić skuteczne raportowanie o takich wydarzeniach, tym samym nie dopuszczać do tak istotnego dla poprawiania bezpieczeństwa lotniczego przyrostu informacji o bezpieczeństwie i dzielenia się.

1.5. Szereg inicjatyw w środowisku międzynarodowego lotnictwa cywilnego usiłuje zająć się sprawą chronienia SDCPS. Biorąc jednak pod uwagę delikatność aktualnego zagadnienia, istotną dla tego zagadnienia jest rama, która zapewni jedność i spójność wysiłków środowiska lotniczego. Wysiłki dla zapewnienia ochrony informacji dotyczących bezpieczeństwa muszą wyznaczyć delikatną równowagę między potrzebami: ochrona informacji o bezpieczeństwie, istnienie kontroli jakości, zarządzanie ryzykiem dotyczącym bezpieczeństwa i prawidłowe stosowanie prawa. Mając powyższe na względzie, należy przyjąć podejście ostrożne po to, by uniknąć składania propozycji, które mogą nie przystawać do praw podlegających egzekwowaniu w Umawiających się Państwach.

1.6. Aby zająć się tym aktualnym tematem, ICAO opracowało załącznik E do Załącznika 13 do Konwencji chicagowskiej, który zawiera wskazówki prawne by pomóc państwom w uchwalaniu praw krajowych i przepisów dla ochrony informacji zbieranych od SDCPS, i jednocześnie daje możliwość prawidłowego stosowanie prawa. Celem jest niedopuszczenie do nieprawidłowego wykorzystania informacji zebranych wyłącznie dla celów poprawiania bezpieczeństwa lotniczego. Z uwagi na to, że Państwom powinno się dawać swobodę pisania projektów ustaw zgodnie z własną polityką krajową i praktykami, takie prawne wskazówki mają formę serii zasad, które mogą być zaadaptowane dla spełnienia konkretnych potrzeb Państwa uchwalającego prawa i przepisy dla ochrony informacji bezpieczeństwa.

1.7. Wskazówki prawne zawierają ogólne zasady, które stanowią, że:

a) jedynym sposobem chronienia informacji dotyczących bezpieczeństwa przed niewłaściwym wykorzystaniem jest stała jej dostępność po to, by możliwe było terminowe podejmowanie właściwych działań prewencyjnych oraz polepszających bezpieczeństwo lotnicze;

b) celem chronienia informacji dotyczących bezpieczeństwa nie jest zakłócanie właściwego wymierzania sprawiedliwości w Państwach;

c) krajowe ustawy i przepisy chroniące informacje dotyczące bezpieczeństwa powinny zapewniać równowagę pomiędzy potrzebą ochrony informacji dotyczących bezpieczeństwa w celu zwiększenia bezpieczeństwa lotniczego, a potrzebą właściwego funkcjonowania wymiaru sprawiedliwości;

d) krajowe prawa i przepisy chroniące informacje dotyczące bezpieczeństwa powinny zapobiegać niewłaściwemu ich wykorzystywaniu; przy czym

e) zapewnianie ochrony niejawnych informacji dotyczących bezpieczeństwa w określonych warunkach jest częścią obowiązków Państwa w zakresie bezpieczeństwa.

1.8. Ww. wskazówki zawierają następujące zasady ochrony:

a) informacje dotyczące bezpieczeństwa powinny nadawać się do ochrony przed niewłaściwym ich wykorzystaniem, zgodnie z określonymi warunkami, które powinny uwzględniać, ale niekoniecznie ograniczać się do tego, że zbieranie informacji było wyraźnie dla celów bezpieczeństwa, a ujawnienie informacji utrudniłoby ciągłość ich dostępności;

b) sposób ochrony powinien być właściwy dla każdego SDCPS, bazujący na charakterze zawartych w nim informacji dotyczących bezpieczeństwa;

c) należy ustanowić formalną procedurę zapewniania ochrony niejawnych informacji dotyczących bezpieczeństwa, zgodnie z określonymi warunkami;

d) informacje dotyczące bezpieczeństwa nie powinny być wykorzystywane w sposób odbiegający od celów, dla których były zbierane; i

e) wykorzystanie informacji dotyczących bezpieczeństwa - w postępowaniu dyscyplinarnym, cywilnym, administracyjnym lub karnym - powinno się odbywać wyłącznie z zachowaniem odpowiednich zabezpieczeń.

1.9. Zalecamy przyjąć, że w poniższych okolicznościach, informacje dotyczące bezpieczeństwa mogą nie kwalifikować się do objęcia ich ochroną:

a) gdy istnieje dowód/y, że zdarzenie było spowodowane poprzez czyn, który w świetle prawa uważa się za postępowanie z intencją wyrządzenia szkody lub ze świadomością, że w jego wyniku powstanie zapewne szkoda, co jest równoznaczne z zachowaniem lekkomyślnym, rażącym zaniedbaniem, lub umyślnym złym postępowaniem;

b) gdy właściwy organ uważa, że istnieją uzasadnione okoliczności wskazujące, iż zdarzenie mogło być spowodowane przez postępowanie z intencją wyrządzenia szkody, lub ze świadomością, że w jego wyniku powstanie zapewne szkoda, co jest równoznaczne z zachowaniem lekkomyślnym, rażącym zaniedbaniem, lub umyślnym złym postępowaniem;

c) gdy dokonany przez odpowiednią władzę przegląd ustali, że ujawnienie informacji dotyczącej bezpieczeństwa jest konieczne dla prawidłowego wymierzenia sprawiedliwości oraz, że jej ujawnienie przeważa krajowe i międzynarodowe negatywne skutki jakie odnośne ujawnienie może mieć w przyszłości na dostępność informacji dotyczących bezpieczeństwa.

1.10. Ww. wskazówki również dotyczą zagadnień związanych z publicznym ujawnieniem, proponując by pod warunkiem zachowania zasad ochrony i wyjątków omówionych powyżej, każda osoba wnosząca o opublikowanie informacji o bezpieczeństwie powinna takie ujawnienie uzasadnić. Odnośnie ujawniania informacji o bezpieczeństwie, należy ustalić formalne kryteria, które będą zawierać, ale niekoniecznie ograniczać się do następujących kryteriów:

a) ujawnianie informacji dotyczących bezpieczeństwa jest konieczne do skorygowania warunków kosztem bezpieczeństwa i/lub zmiany zasad i przepisów;

b) ujawnienie informacji dotyczącej bezpieczeństwa nie ograniczy dostępności do niej w przyszłości do celów poprawienia bezpieczeństwa;

c) ujawnienie istotnej informacji personalnej, zawartej w informacjach dotyczących bezpieczeństwa, gdy jest to zgodne z obowiązującymi przepisami o ochronie prywatności; i

d) ujawnianie informacji dotyczącej bezpieczeństwa jest dokonywane w formie odpersonalizowanej, streszczonej lub zbiorczej.

1.11. Ww. wskazówki omawiają odpowiedzialność osoby przechowującej informację o bezpieczeństwie, proponując by każdy SDCPS miał przydzielonego depozytariusza. Odpowiedzialnością depozytariusza informacji bezpieczeństwa jest stosowanie wszelkich możliwych zabezpieczeń przed ujawnieniem, chyba że:

a) depozytariusz informacji bezpieczeństwa ma zgodę autora informacji na jej ujawnienie; lub

b) depozytariusz informacji bezpieczeństwa jest przekonany, że ujawnienie informacji dotyczących bezpieczeństwa jest zgodne z zasadami odstępstw.

1.12. Na koniec, te wskazówki wprowadzają (a) ochronę informacji zanotowanej i uwzględniając to, że prawem wymagane nagrania z otoczenia stanowiska pracy, jak na rejestratorach głosów w kabinie (CVR), mogą być postrzegane jako naruszające prywatność personelu operacyjnego, na co inne zawody nie są narażone, i (b) zalecają, co następuje:

a) by, przestrzegając ww. zasad ochrony i odstępstw, krajowe ustawy i przepisy powinny traktować prawem wymagane nagrania z otoczenia stanowiska jako uprzywilejowane informacje chronione, tj. informacje zasługujące na zwiększoną ochronę; oraz

b) by krajowe ustawy i przepisy i dawały konkretne środki ochrony takich zapisów w zakresie ich poufności i publicznego do nich dostępu. Takie konkretne środki ochrony prawem wymaganych zapisów tła pracy mogą obejmować wydawanie zakazów podawania takich zapisów do publicznej wiadomości.

1.13. Choć wskazówki dla ochrony SDCPS zostały przyjęte 3 marca 2006 jako załącznik do Załącznika 13 do Konwencji chicagowskiej, społeczność lotnicza zaleca, by ICAO kontynuowała działania dotyczące ochrony danych o bezpieczeństwie i informacji o bezpieczeństwie, po to by zapewnić ich dostępność dla poprawiania bezpieczeństwa. Dlatego, podczas swej 37 Sesji, Zgromadzenie wydało instrukcję do Rady by rozważyła dopracowanie postanowień o ochronie informacji dotyczących bezpieczeństwa. 7-go grudnia 2010, Komisja Żeglugi Powietrznej zatwierdziła powołanie Grupy Zadaniowej Ochrony Informacji Bezpieczeństwa (SIP TF), która rozpoczęła swoją działalność 5-go maja 2011 r. z zaleceniem opracowania nowych lub dopracowania postanowień i materiałów pomocniczych, związanych z ochroną informacji dotyczących bezpieczeństwa.

Dodatek 6 do Rozdziału 4
WSKAZÓWKI DOTYCZĄCE RAPORTOWANIA I ZAWIADAMIANIA O WYPADKACH I ZDARZENIACH

1. WPROWADZENIE

1.1. Zgodnie z Załącznikiem 13 - Badanie wypadków i incydentów statków powietrznych, wymaga się od Państw, by przekazywały do ICAO informacje o wszystkich wypadkach samolotów turboodrzutowych lub statków powietrznych o maksymalnej certyfikowanej masie startowej powyżej 2250 kg. ICAO również zbiera informacje o incydentach z udziałem statków powietrznych, uważanych za ważne dla bezpieczeństwa i zapobiegania wypadkom. Dla ułatwienia wyszukiwania, termin „*occurence*" (zdarzenie) dotyczy zarówno wypadków, jak i incydentów.

1.2. Standardy Załącznika 13 zostały przytoczone w wytycznych na szarym tle.

2. WYPADKI I INCYDENTY - RAPORTOWANIE I ZAWIADAMIANIE

2.1. Ogólnie

2.1.1. System ICAO przekazywania danych dotyczących wypadków i zdarzeń (ADREP), zbiera dane od Państw w celu wzmocnienia bezpieczeństwa poprzez analizę, bądź przez uprawomocnianie znanych, aktualnych zagadnień, bądź przez rozpoznawanie powstających trendów w bezpieczeństwie, prowadzących do opracowania zaleceń dla potrzeb zapobiegania wypadkom.

2.1.2. Są cztery różne etapy, na których wysyłane są do ICAO informacje po zdarzeniu. Są to:

a) zawiadomienie;

b) raport wstępny (ADREP);

c) raport końcowy; oraz

d) raport danych (ADREP).

Te cztery etapy są szerzej omówione w punktach 2.2 do 2.5, a Tabela 4-A6-1 pokazuje w streszczeniu kolejność zawiadamiania i listę kontrolną raportowania, zgodnie z Załącznikiem 13 do Konwencji chicagowskiej, załącznik B.

2.1.3. Dla ułatwienia raportowania, Państwa mogą teraz, dla zawiadamiania i przekazywania raportów ADREP, korzystać z bezpiecznego portalu internetowego ICAO i składać zawiadomienia oraz raporty ADREP na formularzu internetowym lub za pomocą formatu kompatybilnego z systemem ADREP (np. ECCAIRS). Dalsze wskazówki dotyczące internetowych druków ICAO znajdują się w punkcie 3.

2.2. Zawiadamianie

Zawiadamianie stosuje się dla natychmiastowego upowszechnienia informacji o wypadku/incydencie. Według Załącznika 13 do Konwencji chicagowskiej, Rozdział 4, do ICAO muszą być wysłane informacje następujące:

4.1 Państwo, w którym doszło do zdarzenia wysyła zawiadomienie o wypadku lub poważnym incydencie, możliwie z małą zwłoką, najbardziej przydatnym i najszybszym, dostępnym środkiem, do:

a) Państwa Rejestracji;

b) Państwa Operatora;

c) Państwa Konstruktora;

d) Państwa Producenta; oraz

e) Organizacji Międzynarodowego Lotnictwa Cywilnego (ICAO), gdy maksymalna masa przedmiotowego statku powietrznego przekracza 2250 kg lub gdy jest to samolot z napędem turboodrzutowym.

Jednakże, gdy Państwo miejsca zdarzenia nie wie o żadnym poważnym incydencie, to, w zależności od sytuacji, Państwo Rejestracji lub Państwo Operatora przekieruje zawiadomienie o takim incydencie do Państwa Konstruktora, Państwa Producenta i Państwa miejsca zdarzenia.

…

4.2 Zawiadomienie ma być formułowane prostym językiem i ma zawierać tyle informacji spośród niżej wymienionych, ile jest dostępnych bezpośrednio, lecz ich wysyłka nie może być opóźniona z powodu braku pełnych informacji:

a) dla wypadków, akronimem identyfikującym jest ACCID, a dla poważnych incydentów - INCID;

b) producent, typ, przynależność państwowa i znaki rozpoznawcze oraz numer seryjny statku powietrznego;

c) nazwa właściciela, operatora i najemcy statku powietrznego - jeśli występuje;

d) kwalifikacje dowódcy statku powietrznego oraz narodowość członków załogi i pasażerów;

e) data i godzina (wg czasu miejscowego lub UTC) wypadku lub poważnego incydentu;

f) miejsce ostatniego odlotu i miejsce zamierzonego lądowania statku powietrznego;

g) pozycja statku powietrznego w odniesieniu do łatwego do określenia punktu geograficznego oraz szerokość i długość geograficzna;

h) liczba członków załogi i pasażerów; na pokładzie, ofiar śmiertelnych i ciężko rannych; innych ofiar i ciężko rannych;

i) opis wypadku lub poważnego incydentu oraz stopień uszkodzenia statku powietrznego, na tyle na ile jest znany;

j) wskazanie w jakim zakresie będzie badanie prowadzone, lub propozycja przekazania go przez Państwo miejsca zdarzenia;

k) fizyczna charakterystyka obszaru, w którym zaistniał wypadek lub poważny incydent, jak również wskazanie trudności w dostępie do tego miejsca, lub wskazanie szczególnych wymagań związanych z dostępem do miejsca zdarzenia;

l) identyfikacja organu wysyłającego zawiadomienie oraz sposób kontaktu w dowolnym czasie z Przewodniczącym zespołu badawczego i z organem ds. badania wypadków Państwa miejsca zdarzenia; oraz

m) obecność oraz opis materiałów niebezpiecznych na pokładzie statku powietrznego.

2.3. Raport wstępny

2.3.1. Raport wstępny jest formą pilnego rozpowszechnienia danych uzyskanych na wczesnych etapach badania. Jest to raport przejściowy, zawierający dodatkowe informacje, których było brak lub były niedostępne w chwili wysyłania zawiadomienia. Raporty Wstępne nie są obowiązkowe dla zdarzeń. Informacje, które trzeba wysłać do Raportu Wstępnego można znaleźć na http://www.icao.int/Safety/reporting.

2.3.2. Załącznik 13 do Konwencji chicagowskiej, Rozdziały 7.1 oraz 7.2 stanowią, że:

Wypadki statków powietrznych o masie większej niż 2250 kg

7.1 Gdy masa całkowita biorącego udział w wypadku statku powietrznego jest większa niż 2250 kg, Państwo prowadzące badanie wysyła Raport Wstępny do:

a) Państwa Rejestracji lub do Państwa miejsca zdarzenia, stosownie od okoliczności;

b) Państwa Operatora;

c) Państwa Konstruktora;

d) Państwa Producenta;

e) każdego Państwa, które udostępniło istotne informacje, ważne urządzenia/obiekty lub ekspertów; i

f) Organizacji Międzynarodowego Lotnictwa Cywilnego.

Wypadki statków powietrznych o masie 2250 kg lub mniejszej

7.2 W przypadku zaistnienia wypadku statku powietrznego niespełniającego warunków punktu 7.1 i gdy okoliczności dotyczą problemów zdatności do lotu lub takich, którymi mogą być zainteresowane inne przedmiotowe Państwa, Państwo prowadzące badanie kieruje Raport Wstępny do:

a) Państwa Rejestracji lub Państwa miejsca zdarzenia, stosownie do okoliczności;

b) Państwa Operatora;

c) Państwa Konstruktora;

d) Państwa Producenta; oraz

e) każdego Państwa, które udostępniło istotne informacje, ważne urządzenia/obiekty lub ekspertów.

2.3.3. Załącznik 13 do Konwencji chicagowskiej, Rozdział 7.4 stanowi, że:

Wysyłanie

7.4 Raport Wstępny wysyła się za pomocą telefaksu, e-maila lub pocztą lotniczą w ciągu trzydziestu dni od daty zaistnienia wypadku, chyba że przed tym terminem wysłany był Raport Informacyjny o wypadku/incydencie. W przypadku problemów bezpośrednio dotyczących bezpieczeństwa, wysyła się Raport Wstępny natychmiast po uzyskaniu informacji, za pomocą najbardziej odpowiedniego i najszybszego dostępnego środka.

2.4. Raport końcowy

2.4.1. Załącznik 13 do Konwencji chicagowskiej, Rozdziały 6.5 do 6.7 zawierają poniższe standardy, które dotyczą Raportu Końcowego:

Publikacja raportu końcowego

6.5 W interesie zapobiegania wypadkom, Państwo prowadzące badanie wypadku lub incydentu udostępnia Raport Końcowy do wiadomości publicznej w możliwie krótkim czasie, a jeśli to możliwe, to w ciągu dwunastu miesięcy.

. . .

6.6 Jeżeli nie jest możliwe podanie raportu do publicznej wiadomości w ciągu dwunastu miesięcy, Państwo prowadzące badanie wydaje publiczne oświadczenie przejściowe w każdą rocznicę zdarzenia, informując szczegółowo o postępie w badaniu i o wszelkich, poruszonych kwestiach bezpieczeństwa.

6.7 Jeżeli Państwo, które przeprowadziło badanie wypadku lub incydentu statku powietrznego o masie maksymalnej powyżej 5700 kg, ujawniło Raport Końcowy, to wysyła jego kopię do Organizacji Międzynarodowego Lotnictwa Cywilnego.

2.4.2. Szczegółowe wskazówki co do formatu, treści i przedkładania Raportu Końcowego znajdują się w Podręczniku Badania Wypadków Statków Powietrznych i Zdarzeń, Doc 9756 (Część IV Raportowanie).

2.5. Zgłaszanie danych

2.5.1. Po zakończeniu dochodzenia i zatwierdzeniu Raportu Końcowego, należy wypełnić Raport Danych o Wypadku lub Zdarzeniu. Jeżeli dochodzenie jest ponownie otwarte, informacje poprzednio zgłoszone powinny zostać odpowiednio poprawione/uzupełnione. Celem Raportu Danych jest dostarczyć dokładnych i kompletnych informacji w formacie standardowym.

2.5.2. Informacje potrzebne do wypełnienia Raportu Danych można znaleźć na http://www.icao.int/Safety/reporting.

2.5.3. Ponadto, Załącznik 13 do Konwencji chicagowskiej, Rozdz. 7.5 wymaga, co następuje:

Wypadki statków powietrznych o masie większej niż 2250 kg

7.5 W przypadku zaistnienia wypadku statku powietrznego, którego maksymalna masa jest większa niż 2250 kg, Państwo prowadzące badanie wysyła do Organizacji Międzynarodowego Lotnictwa Cywilnego, tak szybko jak to możliwe po zakończeniu badania, Raport Informacyjny o wypadku.

3. OGÓLNA INSTRUKCJA KOMPILOWANIA RAPORTÓW

3.1. Opcje raportowania zdarzeń do ICAO

Zdarzenia można raportować do ICAO korzystając z jednej spośród następujących opcji:

a) ICAO Occurence Report Manager, opcja jest dostępna na bezpiecznym portalu pod: iSTARS: http://www.icao.int/Safety;

b) raportem z bazy danych, który jest kompatybilny z bazą danych systemu ADREP (np. ECCAIRS);

c) jako raport papierowy, na adres ICAO.

3.2. Program raportowania zdarzeń (Occurence Report Manager)

Formularze zawiadamiania o zdarzeniach i formularze Wstępnych Raportów ADREP można teraz wypełniać elektronicznie poprzez program raportowania zdarzeń, dostępny na bezpiecznym portalu iSTARS. Członkowie iSTARS mogą uzyskiwać dostęp do formularzy Raportowania Zdarzeń odwiedzając iSTARS a następnie, podążając linkiem do instrukcji raportowania o zdarzeniu. Noworejestrujący się na bezpiecznym portalu iSTARS mogą prosić o dostęp do formularza albo online przez iSTARS lub emailem na adres adrep@icao.int.

3.3. Podstawowe zasady (Basic rules)

Okres ważności informacji dotyczących bezpieczeństwa, dostarczanych Państwom przez ICAO, zależy od szczegółowości i staranności z jaką zdarzenia są raportowane. Tak więc, w interesie wszystkich Państw jest dokładne i pełne raportowanie wszystkich danych, zgodnie z Załącznikiem 13 do Konwencji chicagowskiej i wskazówką podaną w tym podręczniku. Oto kilka podstawowych zasad dotyczących wypełniania internetowego formularza ICAO Accident and Incident Reporting Form lub formatu kompatybilnego z systemem ADREP (np. ECCAIRS):

a) Określ prawidłową klasyfikację i kategorię zdarzenia, tzn. czy to jest wypadek, incydent czy poważny incydent, czy incydent, bazując na poziomie obrażeń, uszkodzeniach statku powietrznego i innych dostępnych informacjach.

b) Uzupełnij podstawowe dane takie jak data, czas, Państwo i miejsce zdarzenia, lotnisko, dotkliwość zdarzenia, typ statku powietrznego, operator, typ operacji i faza lotu.

c) Wybierz odpowiednie jednostki przed wpisaniem wartości w rubryki, np. stopy, a dla ciśnienia/wysokości - MSL lub FL.

d) Jeżeli w zdarzeniu uczestniczył więcej niż jeden statek powietrzny, podaj informacje o drugim statku powietrznym. Przy wpisywaniu typu zdarzenia dla więcej niż jednego statku powietrznego sprawdź czy wybrałeś odpowiedni statek powietrzny (1 lub 2). Wszystkie zdarzenia muszą być podane w kolejności chronologicznej i należy zadbać by nie przeoczyć istotnych zdarzeń.

e) Dopasuj zdarzenie do kategorii zdarzenia.

f) Wpisz „nieznane" tylko, jeżeli ustalono po badaniu, że nie znaleziono żadnej informacji.

g) Pozostaw 'puste' miejsca by podkreślić, że dochodzenie jest w toku dla wykrycia informacji, które w tej chwili są niedostępne.

3.4. Powiadomienia

3.4.1. W przypadku składania zawiadomienia za pomocą systemu iSTARS Occurence Report Manager, wszystkie informacje, wymagane zgodnie z wymaganiem Rozdziału 4.2 w Załączniku 13 do Konwencji chicagowskiej, znajdują się w formularzach elektronicznego zawiadamiania, teraz dostępnych online, które należy wypełnić zgodnie z podaną instrukcją na formularzu.

3.4.2. Pewne rubryki na formularzach zawiadamiania są kluczowymi identyfikatorami, które pozwolą ICAO zidentyfikować zgłoszenie w bazie danych. Dlatego, w przypadku elektronicznego składania zawiadomienia, te rubryki są obowiązkowe i muszą być wypełnione po to by przedłożyć pierwsze zawiadomienie. Te pola to:

a) Państwo raportujące;

b) Numer pliku Państwa;

c) Organizacja zgłaszająca;

d) Klasa zdarzenia, oraz

e) Data zdarzenia.

3.4.3. Przy wpisywaniu podstawowych danych zdarzenia, takich jak poziom okaleczeń i uszkodzeń statku powietrznego, należy zadbać by zgrać takie wybory z klasą zdarzenia. Np., jeżeli zdarzenie zostało sklasyfikowane jako 'wypadek', to poziom okaleczeń musi być poważny, śmiertelny lub nieznany, a statek powietrzny musi być znacznie uszkodzony, zniszczony, lub w stopniu nieznanym.

3.5. Klasyfikacja ADREP

Klasyfikacja ADREP została opracowana przez ICAO i zawiera definicje i terminologię dla systemów raportowania o wypadkach i incydentach lotniczych. Dokumenty taksonomii dostępne są na stronie http://www.icao.int/Safety/reporting. Należy odwoływać się do tych dokumentów zawsze, gdy pojawią się wątpliwości co do terminologii zawiadomienia i formularzy raportów.

3.6. Wysyłanie raportów

3.6.1. Gdy informacja dotycząca zdarzenia jest dostępna w formacie kompatybilnym z ADREP (np. format ECCAIRS), kopię pliku elektronicznego należy dołączyć do zawiadamiającego e-maila i wysłać do adrep@icao.int.

3.6.2. Formularze raportów wysyłanych online przez bezpieczny portal iSTARS (Integrated Safety Trend and Reporting System), docierają bezpośrednio do ICAO. Raporty które się wypełnia na papierze wysyła się do ICAO na adres adrep@icao.int lub na adres poniższy:

International Civil Aviation Organization
999 University Street
Montréal, Quebec H3C 5H7
Canada
Fax: + 1 (514) 954-6077

3.6.3. Zawiadomienia i raporty należy pisać prostym językiem i, tam gdzie możliwe, bez zbędnej zwłoki, w jednym z roboczych języków ICAO, uwzględniając język/i odbiorców.

4. SPECJALNE INSTRUKCJE WYPEŁNIANIA RAPORTÓW

4.1. Kodowanie kategorii zdarzeń

4.1.1. Taksonomia kategoryzacji zdarzeń ADREP stanowi część systemu zawiadamiania ICAO o wypadkach i incydentach. Kategorie zdarzeń stanowią komplet terminów stosowanych przez ICAO dla kategoryzowania wypadków i incydentów w celu prowadzenia analizy trendów bezpieczeństwa. Celem takiej analizy jest podjęcie działań wyprzedzających, dla zapobieżenia wystąpieniu podobnych wypadków lub incydentów w przyszłości.

4.1.2. Większość wypadków i incydentów składa się z wielu wydarzeń. Dlatego, precyzyjne zakodowanie wypadku lub incydentu do pojedynczej kategorii może być trudne. Na przykład, gwałtowne manewrowanie (AMAN) może również skutkować utratą sterowności w locie (LOC-I). W takim przypadku, zdarzenie koduje się w obu kategoriach: AMAN i LOC-I. Filozofia ICAO dla kategorii kodowania zdarzeń pozwala zgłaszającemu kodować pojedynczy wypadek lub incydent w wielu kategoriach, po to by ICAO mogła rozważać lub analizować wszystkie wydarzenia wypadki lub incydenty, które prowadziły do wypadku lub incydentu. Szczegółowe definicje kategorii zdarzeń oraz wskazówki dotyczące kodowania w różnych kategoriach można znaleźć pod adresem http://www.icao.int/Safety/reporting.

4.2. Kodowanie typów zdarzeń

4.2.1. Aby ustalić dlaczego wypadek lub incydent miał miejsce, trzeba koniecznie przestudiować czynniki prowadzące do zdarzenia, występujące w trakcie i po nim. Dlatego, sprawą bardzo istotną jest dokładne podanie w raporcie wszystkich aktualnie znanych danych o zdarzeniu.

4.2.2. Aby rozszerzyć opis wydarzenia, dla każdego wydarzenia można wprowadzić „czynniki opisowe". Czynniki opisowe objaśniają w szczegółach – podając ich spis - co się stało podczas wydarzenia. Jeżeli możliwe, czynniki opisowe powinny być kodowane chronologicznie pod każdym typem wydarzenia.

4.2.3. Aby zdarzenie wyjaśnić, można dla każdego czynnika opisowego wprowadzić „czynniki objaśniające". W kodowaniu wydarzenia, te czynniki objaśniają dlaczego zdarzenie zaistniało, oraz zawierają aspekty czynników ludzkich. Są one stosowane do ustalenia tego jakie działanie prewencyjne może być wymagane. Komplet typów zdarzeń, czynników opisowych i wyjaśniających, razem z ich szczegółowymi opisami można znaleźć na stronie ADREP ICAO.

4.2.4. Co zamieszczać w raportach ze zdarzeń:

a) *Bądź konkretny na ile jest to możliwe, bez spekulowania co do szczegółów*. Na przykład, jeżeli przednie podwozie nie wysunęło się, zdarzenie to określ tak: "Zdarzenie dotyczące podwozia przedniego/tylnego", a nie „Zdarzenie dotyczące podwozia".

b) *Połącz kategorie zdarzeń z wydarzeniami*. Na przykład, jeśli kategorią zdarzenia jest SCF-NP, to oznacza, że zdarzeniem jest usterka systemu/komponentu innego niż zespół napędowy.

c) *Połącz zdarzenia z czynnikami opisowymi*: Zdarzenia i czynniki opisowe opisują co było nie tak, co nie działało, co było nietypowe i co przyczyniło się do zdarzenia. Np. zdarzenie „zdarzenie dotyczące centralnego systemu ostrzegania" można użyć dla zdarzeń jakimi jest złe działanie systemu, a czynnik opisowy „Komputery centralne" - dla doprecyzowania zdarzenia.

d) *Ustaw wydarzenia chronologicznie*: Zdarzenie należy opisać w sposób jak jest zakodowane. W swojej istocie kodowanie powinno zapewnić pojedynczy obraz kolejności zdarzenia, jak przedstawiono w części opisowej.

4.3. Narracje

4.3.1. Narracja dostarcza krótkiego opisu zdarzenia, łącznie z sytuacjami awaryjnymi, istotnymi faktami i innymi odnośnymi informacjami. Narracja nie może być przedstawiona większą ilością słów niż 200. Ważne jest, aby wydarzenia były opisane w porządku chronologicznym (czas), krótko i konkretnie.

4.3.2. Badanie i analiza kolejności wydarzeń, które doprowadziły do zdarzenia może pomóc lepiej zrozumieć charakter zdarzenia. Dlatego, narracje powinny zawierać zwięzłe streszczenie wszystkich wydarzeń w celu dostarczenia informacji dotyczących wydarzeń, które doprowadziły do zdarzenia. Informacje, dostarczone w części narracyjnej Raportu Wstępnego nie muszą być powtarzane w Raporcie Danych. Jednakże, wszelkie nowe informacje uzyskane po złożeniu Raportu Wstępnego muszą być włączone do Raportu Danych. Zestawienie obu narracji powinno dać pełną historię lotu oraz wnioski z badania.

4.3.3. Jeżeli Raportu Wstępnego nie przedłożono (albo w przypadku incydentu lub gdy badanie wypadku ukończono w ciągu 30 dni), narracja w Raporcie Danych musi zawierać historię lotu i opis oraz analizę powodu i przyczyny zdarzenia, wnioski z badania, co wykryto oraz prawdopodobną przyczynę. W takich przypadkach, idealną ilością słów przedłożonego Raportu Danych może być 400.

4.4. Zalecenia dotyczące bezpieczeństwa

Tam gdzie ma to zastosowanie, zgłaszający powinien skorelować zalecenia dotyczące bezpieczeństwa, lub działania, z odnośnymi odkryciami. Rubryki w Raporcie Danych, znajdujące się pod zaleceniem dotyczącym bezpieczeństwa, powinny zawierać każde działanie naprawcze, podjęte lub rozważane. Jeżeli możliwe, rekomendacja powinna wyszczególnić to jak dane działanie naprawcze rozwiąże zidentyfikowany problem bezpieczeństwa. Zamieść streszczenie każdego już podjętego działania naprawczego.

Tabela 4-A6-1. Zawiadamianie i lista kontrolna dla raportów.

Poniższe terminy mają w tej liście kontrolnej takie znaczenia:

Wydarzenia międzynarodowe. Wypadki i poważne incydenty statków powietrznych zarejestrowanych w jednym Umawiającym się Państwie, lecz zaistniałych na terytorium innego Umawiającego się Państwa.

Wydarzenia krajowe. Wypadki i poważne incydenty, które zaistniały na terytorium Państwa Rejestracji.

Inne zdarzenia. Wypadki i poważne zdarzenia, które zaistniały na terytorium Państwa nie będącego Umawiającym się Państwem, lub poza terytorium jakiegokolwiek Państwa.

Zawiadamianie o wypadkach i poważnych incydentach

Nadawca	Rodzaj zgłoszenia	Adresat	Dotyczy	Data ostateczna
Państwo miejsca Zdarzenia	Zawiadomienie	Państwo Rejestracji Państwo Operatora Państwo Skonstruowania Państwo Producenta	Zdarzenia międzynarodowe: Wszystkie statki powietrzne	Z minimalnym opóźnieniem
		ICAO	Statki powietrzne o masie większej niż 2250 kg lub samoloty z napędem turboodrzutowym	
Państwo Rejestracji	Zawiadomienie	Państwo Operatora Państwo Skonstruowania Państwo Producenta	Zdarzenia krajowe i inne	
		ICAO	Statki powietrzne o masie większej niż 2250 kg lub samoloty z napędem turboodrzutowym	

Raport Wstępny ADREP

Zgłaszający	Kategoria wydarzenia	Rodzaj zgłoszenia	Adresat	Dotyczy	Data ostateczna
Państwo prowadzące badanie	Wypadek	Raport Wstępny	Państwo Rejestracji Państwo Zdarzenia Państwo Operatora Państwo Producenta Państwo Projektu	Statki powietrzne o masie większej niż 2250 kg	30 dni*
			Każde Państwa dostarczające informacji, ważnych urządzeń/obiektów lub ekspertów.		
			ICAO		
			Jak powyżej, ale bez ICAO	Wypadki statków powietrznych o masie 2250 kg lub mniejszej, jeżeli dotyczy to zdatności do lotu lub zagadnień będących przedmiotem zainteresowania	
	Incydent	Wstępny	Nie jest wymagane		
*Jeżeli Raport Danych był opracowany i wysłany do ICAO w ciągu 30 dni, nie jest wymagany Raport Wstępny.					

Raport końcowy – Wypadki i incydenty gdziekolwiek by się nie zdarzyły

Zgłaszający	*Kategoria wydarzenia*	*Rodzaj zgłoszenia*	*Dotyczy*	*Data ostateczna*
Państwo prowadzące dochodzenie	Raport Końcowy	Państwo, które otworzyło badanie Państwo Rejestracji Państwo Operatora Państwo Projektu Państwo Producenta Państwo zainteresowane w związku z ofiarami śmiertelnymi	Wszystkie statki powietrzne	Z minimalnym opóźnieniem
		Państwa zapewniające informacje, ważne urządzenia/obiekty lub ekspertów		
		ICAO	Statki powietrzne o masie większej niż 5700 kg	

Raport danych ADREP

Od	*Kategoria*	*Zgłoszenie*	*Do*	*Dotyczy*	*W terminie*
Państwo prowadzące dochodzenie	Wypadek	Dane	ICAO	Statki powietrzne o masie większej niż 2250 kg	Po zakończeniu badania
Państwo prowadzące dochodzenie	Incydent	Dane	ICAO	Statki powietrzne o masie większej niż 5700 kg	Po zakończeniu badania

Dodatek 7 do Rozdziału 4
LISTA KONTROLNA ANALIZOWANIA LUK KRAJOWEGO PROGRAMU BEZPIECZEŃSTWA (SSP GAP) ORAZ PLAN WDROŻENIOWY

1. POCZĄTKOWA LISTA KONTROLNA ANALIZY LUK (TABELE 4-A7-1)

1.1. Początkowa lista kontrolna analizy luk, w Tabeli 4-A7-1, może być użyta jako matryca dla wykonania pierwszego kroku w analizie luk w SSP. Taki format z ogólnymi odpowiedziami „TAK/NIE/CZĘŚCIOWO" dostarczy początkowego wskazania co do tego jak szeroki jest zakres luk, a więc jakiego obciążenia pracą można się spodziewać. Ta początkowa informacja będzie bardzo przydatna dla wyższego kierownictwa przy określaniu przewidywanej skali wysiłków dla wdrożenia SSP, a więc i zasobów jakie trzeba będzie dostarczyć. Za tą początkową listą kontrolną musi podążać odpowiedni plan wdrożeniowy, wg Tabeli 4-A7-2 oraz 4-A7-3).

1.2. Odpowiedź „TAK" wskazuje, że Państwo spełnia lub wykracza poza oczekiwanie odpowiedniego pytania. Odpowiedź „NIE" wskazuje na znaczącą lukę w istniejącym systemie wobec oczekiwanej odpowiedzi. Odpowiedź „CZĘŚCIOWO" wskazuje na konieczność dalszego ulepszania lub pracy w rozbudowie istniejącego procesu w celu spełnienia oczekiwań wynikających z pytania.

Uwaga. – Odnośniki SMM, znajdujące się w nawiasach kwadratowych [ ] odnoszą się do materiałów pomocniczych dotyczących pytania zawartego w analizie luk.

Tabela 4-A7-1. – Lista kontrolna Analizy Luk

Nr	*Aspekt do przeanalizowania lub pytanie wymagające odpowiedzi*	*Odpowiedź*	*Stan wdrożenia*
Komponent 1 – POLITYKA BEZPIECZEŃSTWA PAŃSTWA I CELE			
Element 1.1 – Rama legislacyjna bezpieczeństwa Państwa			
1.1-1	Czy [Państwo] obwieściło ramę legislacyjną bezpieczeństwa narodowego i odpowiednie przepisy, które definiują zarządzanie bezpieczeństwem w Państwie? [4.2.1, Element 1]	□ Tak □ Nie □ Częściowo	
1.1-2	Czy [Państwo] obwieściło ramę legislacyjną bezpieczeństwa narodowego i odpowiednie przepisy, które definiują zarządzanie bezpieczeństwem w Państwie? [4.2.1, Element 1]	□ Tak □ Nie □ Częściowo	
Element 1.2 – Odpowiedzialność Państwa i osób za bezpieczeństwo			
1.2-1	Czy [Państwo] wskazało instytucję/organizację na gospodarza SSP i czy powołało dyrektora odpowiedzialnego personalnie za wdrożenie i koordynację SSP? [4.2.1, Element 1.2; 4.4.3 a)]	□ Tak □ Nie □ Częściowo	
1.2-2	Czy [Państwo] powołało zespół do wdrożenia SSP? [4.2.1, Element 1.2; 4.4.3 b)]	□ Tak □ Nie □ Częściowo	
1.2-3	Czy [Państwo] określiło i zdefiniowało swe wymagania, zakresy odpowiedzialności oraz odpowiedzialności personalne za uruchomienie i utrzymywanie SSP? [4.2.1, Element 1.2; 4.4.3]	□ Tak □ Nie □ Częściowo	
1.2-4	Czy Państwo posiada gotowy plan wdrożenia SSP, który zawiera ramę czasową na wdrażanie działań i na luki rozpoznane poprzez analizę luk? [4.3; 4.4.3 d)]	□ Tak □ Nie □ Częściowo	
1.2-5	Czy istnieje udokumentowane oświadczenie o zapewnieniu odpowiednich środków na wdrożenie i utrzymywanie SSP? [4.2.1, Element 1.2; Rozdział 4, Dodatek 1, Część 1, 1.1 d)]	□ Tak □ Nie □ Częściowo	
1.2-6	Czy Dyrektor Odpowiedzialny za SSP w [Państwie] ma kontrolę nad zasobami wymaganymi dla wdrażanie SSP? [4.3.3 a)]	□ Tak □ Nie □ Częściowo	
1.2-7	Czy [Państwo] określiło konkretne działania i personalne odpowiedzialności związane z zarządzaniem bezpieczeństwem w Państwie, za co jest odpowiedzialna każda instytucja/organizacja działająca w ramach SSP? [4.4.5 a)]	□ Tak □ Nie □ Częściowo	

Nr	*Aspekt do przeanalizowania lub pytanie wymagające odpowiedzi*	*Odpowiedź*	*Stan wdrożenia*
1.2-8	Czy [Państwo] ma mechanizm lub platformę dla koordynowania wdrażania SSP, jak i późniejszych czynności stałego monitorowania SSP, angażujących wszystkie legislacyjne instytucje/organizacje Państwa? [4.4.3 e)]	□ Tak □ Nie □ Częściowo	
1.2-9	Czy Dyrektor Odpowiedzialny za SSP [Państwa] koordynuje działania różnych organizacji krajowych w ramach SSP? [4.2.1, Element 1.2; 4.4.3 a)]	□ Tak □ Nie □ Częściowo	
1.2-10	Czy [Państwo] ustanowiło jakąś politykę bezpieczeństwa? [4.2.1, Element 1.2; 4.4.5 b)]	□ Tak □ Nie □ Częściowo	
1.2-11	Czy polityka bezpieczeństwa[Państwa] jest sygnowana przez Dyrektora Odpowiedzialnego za SSP w [Państwie] czy przez odpowiednią instytucję/organizację w [Państwie]? [Roz.4, Dodatek 1]	□ Tak □ Nie □ Częściowo	
1.2-12	Czy polityka bezpieczeństwa [Państwa] jest przeglądana okresowo? [4.4.15]	□ Tak □ Nie □ Częściowo	
1.2-13	Czy polityka bezpieczeństwa [Państwa] jest komunikowana wszystkim instytucjom/organizacjom lotniczym [Państwa] po to, by ich uświadomić o ich personalnej odpowiedzialności za bezpieczeństwo? [4.4.5 b)]	□ Tak □ Nie □ Częściowo	
1.2-14	Czy dla opisania komponentów i elementów ramy SSP, [Państwo] zainicjowało przygotowanie ujednoliconego dokumentu SSP jako części planu jego wdrożenia? [4.2.1, Element 1.2; 4.4.3 f), Dodatek 8], w tym związki pomiędzy poszczególnymi elementami?	□ Tak □ Nie □ Częściowo	
1.2-15	Czy dokument SSP został skompletowany, zatwierdzony i podpisany przez Dyrektora Odpowiedzialnego za SSP i czy został zakomunikowany/udostępniony wszystkim zainteresowanym z chwilą pełnego wdrożenia? [4.4.3 f)]	□ Tak □ Nie □ Częściowo	
1.2-16	Czy [Państwo] posiada system dokumentacji zapewniający odpowiednie przechowywanie, archiwizowanie, ochronę i wyszukiwanie wszystkich dokumentów dotyczących działania SSP? [4.2.1, Element 1.2; 4.4.3 f)]	□ Tak □ Nie □ Częściowo	
1.2-17	Czy [Państwo] ma mechanizm wewnętrznego, okresowego przeglądania dla zapewnienia ciągłości usprawniania i skuteczności swego SSP? [4.2.1, Element 3.1; 4.4.15]	□ Tak □ Nie □ Częściowo	
Element 1.3 – Badanie wypadków i incydentów			
1.3-1	Czy [Państwo] ustanowiło niezależny proces badania wypadków i incydentów, którego jedynym celem jest zapobieganie wypadkom i incydentom, a nie obarczanie winą i odpowiedzialnością karną? [4.2.1, Element 1-3; 4.4.6]	□ Tak □ Nie □ Częściowo	
1.3-2	Czy organizacja/zespół ds. badania wypadków i incydentów działa niezależnie (Patrz *Podręcznik badanie wypadków i incydentów* (Doc 9756, część 1, pkt 2.1)? [4.4.6 b)]	□ Tak □ Nie □ Częściowo	
Element 1.4 – Polityka zapewnienia przestrzegania przepisów			
1.4-1	Czy [Państwo] obwieściło politykę zapewnienia przestrzegania przepisów? [4.2.1, Element 1.4; 4.4.10; Dodatki 10 i 11]	□ Tak □ Nie □ Częściowo	
1.4-2	Czy krajowy porządek prawny Państwa zapewnia przestrzeganie odpowiedniej legislacji i przepisów? [4.4.7]	□ Tak □ Nie □ Częściowo	
1.4-3	Czy polityka egzekwowania bierze pod uwagę to, że normalnie dopuszcza się by dostawcy usług w ramach swych zatwierdzonych procedur SMS/QMS zajmowali się i rozwiązywali wewnętrznie sprawy rutynowych odstępstw od bezpieczeństwa i jakości? [4.4.10 a)]	□ Tak □ Nie □ Częściowo	
1.4-4	Czy polityka egzekwowania przepisów określa warunki i okoliczności, w których Państwo może bezpośrednio zajmować się odstępstwami od bezpieczeństwa, poprzez swe procedury ustanowione dla badania i egzekwowania prawa? [4.2.1, Element 1.4; 4.4.10 b)]	□ Tak □ Nie □ Częściowo	

Nr	*Aspekt do przeanalizowania lub pytanie wymagające odpowiedzi*	*Odpowiedź*	*Stan wdrożenia*
1.4-5	Czy polityka egzekwowania w SSP ma zapisy zapobiegające użyciu lub ujawnieniu danych dotyczących bezpieczeństwa dla celów innych niż polepszenie bezpieczeństwa? [4.2.1, Element 1.4; 4.4.10 c)]	□ Tak □ Nie □ Częściowo	
1.4-6	Czy polityka egzekwowania ma w SSP zapisy chroniące źródła informacji pozyskanych z systemów dobrowolnego raportowania zdarzeń? [4.4.10 d); Dodatki 2 i 10]	□ Tak □ Nie □ Częściowo	
Komponent 2 – KRAJOWE ZARZĄDZANIE RYZYKIEM			
Element 2.1 – Wymagania bezpieczeństwa stawiane systemowi SMS dostawcy usług			
2.1-1	Czy Państwo obwieściło zharmonizowane przepisy nakładające obowiązek wdrożenia SMS przez dostawców usług? [4.2.1, Element 2.1, 4.4.9; Dodatek 9]	□ Tak □ Nie □ Częściowo	
2.1-2	Czy wymagania tego SMS i pokrewne materiały pomocnicze są okresowo przeglądane dla upewnienia się, że są nadal istotne i odpowiednie dla dostawców usług? [4.2.1, Element 2.1, 4.4.14 a)]	□ Tak □ Nie □ Częściowo	
Element 2.2 – Zgoda na osiągi bezpieczeństwa u dostawcy usług			
2.2-1	Czy [Państwo] uzgodniło z poszczególnym dostawcą usług lub zaakceptowało jego wskaźniki działania bezpieczeństwa i ich alarmowe i docelowe poziomy? [4.2.1, Element 2.2,; 4.4.13?	□ Tak □ Nie □ Częściowo	
2.2-2	Czy uzgodnione/zaakceptowane wskaźniki działania bezpieczeństwa są współmierne do zakresu/złożoności specyficznego kontekstu operacyjnego poszczególnego dostawcy usług? [4.4.13]	□ Tak □ Nie □ Częściowo	
2.2-3	Czy uzgodnione wskaźniki działania bezpieczeństwa są okresowo przeglądane przez [Państwo] dla upewnienia się, że są nadal istotne i odpowiednie dla dostawcy usług? [4.4.14 b)]	□ Tak □ Nie □ Częściowo	
Komponent 3 – ZAPEWNIANIE BEZPIECZEŃSTWA PRZEZ PAŃSTWO			
Element 3.1 – Nadzorowanie bezpieczeństwa			
3.1-1	Czy [Państwo] ustanowiło formalny program śledzenia by zapewnić zadawalające przestrzeganie krajowych przepisów i wymagań przez dostawców usług? [4.2.1, Element 3.1]	□ Tak □ Nie □ Częściowo	
3.1-2	Czy Państwo ustanowiło proces dla wstępnego przeglądu SMS poszczególnego dostawcy usług i jego zaakceptowania? [4.2.1, Element 2.2; 4.4.11 b)]	□ Tak □ Nie □ Częściowo	
3.1-3	Czy Państwo ustanowiło procedury dla przeglądu działania wskaźników działania bezpieczeństwa i ich odnośnych poziomów alarmowych/ docelowych u poszczególnego dostawcy usług? [4.2.1, Element 2.2; 4.4.13]	□ Tak □ Nie □ Częściowo	
3.1-4	Czy krajowy program nadzorowania bezpieczeństwa obejmuje okresową ocenę SMS poszczególnego dostawcy usług? [4.2.1, Element 3.1; 4.4.14]	□ Tak □ Nie □ Częściowo	
3.1-5	Czy krajowy program okresowego śledzenia SMS obejmuje ocenę procesów rozpoznawania zagrożeń przez dostawcę usług i procesów zarządzania ryzykiem dotyczącym bezpieczeństwa? [4.4.14 c)]	□ Tak □ Nie □ Częściowo	
3.1-6	Czy krajowy program okresowego śledzenia SMS obejmuje ocenę działania własnych wskaźników bezpieczeństwa dostawcy usług i ich odnośnych poziomów alarmowych i docelowych? [4.4.14 b)]	□ Tak □ Nie □ Częściowo	
3.1-7	Czy Państwo ma wewnętrzny mechanizm dla okresowego upewniania się o skutecznym podporządkowaniu SSP i spokrewnionych z nim funkcji doglądania bezpieczeństwa? [4.4.15]	□ Tak □ Nie □ Częściowo	
Element 3.2 – Zbieranie, analizowanie i wymiana danych dotyczących bezpieczeństwa			

Nr	*Aspekt do przeanalizowania lub pytanie wymagające odpowiedzi*	*Odpowiedź*	*Stan wdrożenia*
3.2-1	Czy [Państwo] ustanowiło, na scalonym poziomie Państwa, mechanizmy zapewniające obowiązkowe raportowanie, ocenianie i przetwarzanie danych z wypadków i poważnych incydentów? [4.2.1, Element 3.2; 4.4.12]	□ Tak □ Nie □ Częściowo	
3.2-2	Czy Państwo ustanowiło system dobrowolnego raportowania, by ułatwić zbieranie danych dotyczących zagrożeń i związanego z tym ryzyka dotyczącego bezpieczeństwa, które mogą nie zostać wykryte przez system obowiązkowego raportowania o zdarzeniach? [4.4.16 a)]	□ Tak □ Nie □ Częściowo	
3.2-3	Czy [Państwo] ustanowiło mechanizmy opracowywania informacji z przechowywanych danych oraz promowania wymiany danych dotyczących bezpieczeństwa z dostawcami usług i/lub innymi Państwami? [4.2.1, Element 3.2; 4.4.16]	□ Tak □ Nie □ Częściowo	
3.2-4	Czy [Państwo] ustanowiło akceptowalny poziom działania bezpieczeństwa (AloSP), zdefiniowany przez wybrane wskaźniki bezpieczeństwa z korespondującymi poziomami alarmowymi i docelowymi? [4.4.12 b); 4.4.16 b)]	□ Tak □ Nie □ Częściowo	
3.2-5	Czy wskaźniki bezpieczeństwa (AloSP) są odpowiednie i wystarczające dla zakresu i złożoności działań lotniczych? [4.4.12 b); 4.4.16 b)]	□ Tak □ Nie □ Częściowo	
3.2-6	Czy Państwo ma mechanizm dla okresowego monitorowania wskaźników bezpieczeństwa SSP po to, by się upewnić, że są podejmowane i kontynuowane działania naprawcze wobec wszelkich niepożądanych trendów, naruszeń poziomów alarmowych lub braku osiągnięć na rzecz polepszania celów? [4.4.12 b); 4.4.16 b)]	□ Tak □ Nie □ Częściowo	
Element 3.3 – Ukierunkowanie doglądania na obszary większych potrzeb lub wymagających większej troski, motywowane danymi o bezpieczeństwie			
3.3-1	Czy [Państwo] opracowało procedury dawania pierwszeństwa inspekcjom, audytom i badaniom pomiarowym nakierowanym na obszary o większych potrzebach w sferze bezpieczeństwa, lub wymagających więcej troski? [4.2.1, Element 3.3; 4.4.17]	□ Tak □ Nie □ Częściowo	
3.3-2	Czy dawanie pierwszeństwa inspekcjom i audytom jest związane z analizą odnośnych wewnętrznych/zewnętrznych danych o bezpieczeństwie? [4.2.1, Element 3.3; 4.4.17]	□ Tak □ Nie □ Częściowo	
Komponent 4 – PROMOWANIE BEZPIECZEŃSTWA PRZEZ PAŃSTWO			
Element 4.1 – Wewnętrzne szkolenia, komunikacja i upowszechnianie informacji o bezpieczeństwie			
4.1-1	Czy istnieje proces identyfikowania wymagań szkoleniowych dotyczących zarządzania bezpieczeństwem, włącznie ze szkoleniem SSP i SMS dla odnośnego personelu krajowych organizacji legislacyjnych lub administracyjnych? [4.4.18]	□ Tak □ Nie □ Częściowo	
4.1-2	Czy są zapisy dokumentujące, że personel zaangażowany we wdrożenie i działanie SSP został odpowiednio przeszkolony lub zapoznany z SSP/SMS? [4.2.1, Element 4.1; 4.4.18]	□ Tak □ Nie □ Częściowo	
4.1-3	Czy [Państwo] utrzymuje mechanizm dla konsolidacji, komunikacji i wymiany informacji o bezpieczeństwie pomiędzy krajowymi organizacjami administracyjnymi zaangażowanymi w SSP? [4.4.18 d)]	□ Tak □ Nie □ Częściowo	
4.1-4	Czy wewnętrzna wymiana danych/informacji dotyczących bezpieczeństwa obejmuje raporty ze zdarzeń, badań i zagrożeń z wszystkich sektorów lotnictwa Państwa? [4.4.16 c)]	□ Tak □ Nie □ Częściowo	
Element 4.2 – Zewnętrzne szkolenia, komunikacja i upowszechnianie informacji dotyczących bezpieczeństwa			
4.2-1	Czy Państwo ułatwia ciągłe nauczania, komunikację i wymianę informacji o bezpieczeństwie pomiędzy swymi dostawcami usług? [4.2.1, Element 4.2; 4.4.19]	□ Tak □ Nie □ Częściowo	
4.2-2	Czy krajowe organizacje/instytucje legislacyjne uczestniczą w regionalnej i światowej wymianie informacji o bezpieczeństwie i czy umożliwiają taki udział swoim podmiotom lotniczym? [4.4.19 d)]	□ Tak □ Nie □ Częściowo	

Nr	*Aspekt do przeanalizowania lub pytanie wymagające odpowiedzi*	*Odpowiedź*	*Stan wdrożenia*
4.2-3	Czy istnieje formalny proces dla zewnętrznego rozprowadzania przepisów oraz informacji do dostawców usług i czy istnieje środek dla zapewnienia efektywności tego procesu? [4.4.19 a)]	□ Tak □ Nie □ Częściowo	
4.2-4	Czy krajowy dokument SSP i powiązana z nim polityka bezpieczeństwa, polityka egzekwowania prawa i zebrane wskaźniki bezpieczeństwa zostały włączone przez Państwo do swego procesu przekazywania i wymiany informacji o bezpieczeństwie? [4.4.19 a)]	□ Tak □ Nie □ Częściowo	

2. SZCZEGÓŁOWA ANALIZA LUK ORAZ ZADANIA WDROŻENIOWE (TABELA 4-A7-2)

Należy postępować według podanej w Tabeli 4-A7-1 listy kontrolnej dla wstępnej analizy luk, posługując się szczegółowym planem Analiza luk i plan identyfikowania zadań wdrożeniowych, podanym w Tabeli 4-A7-2. Po zakończeniu ww. listy kontrolnej, tabela powinna zapewnić dalszą analizę szczegółów dotyczących luk oraz pomóc je przełożyć na zadania i podzadania rzeczywiście wymagane w konkretnym kontekście środowiska, procesów i terminologii Państwa. Każde zadanie będzie przydzielone odpowiednim osobom lub grupom. Jest ważne, by w Tabeli 4-A7-2 została zapewniona korelacja realizacji pojedynczego elementu/zadania z opisanymi w dokumencie SSP gospodarzami, po to by szybko uruchomić progresywne uaktualnianie projektu dokumentu SSP równocześnie z wdrażaniem lub ulepszaniem każdego elementu (pierwsze wpisy elementu w dokumencie SSP są bardziej życzeniowe niż deklaratywne).

3. HARMONOGRAM DZIAŁAŃ/ZADAŃ WDROŻENIOWYCH (TABELA 4-A7-3)

Tabela 4-A7-3 pokaże „kamienie milowe" (daty rozpoczęcia/zakończenia) każdego zadania/działania. Przy fazowym podejściu do wdrażania te zadania/działania trzeba będzie posortować wg tego, do której fazy zostały przydzielone elementy z nimi spokrewnione. Po szczegóły - patrz pkt 4.4 tego rozdziału. Tabela 4-A7-3 może być osobnym skonsolidowaniem wszystkich niezałatwionych działań/zadań lub, jeśli wolisz, kontynuacją Tabeli 4-A7-2 w formie arkusza.

Tabela 4-A7-2. Przykład analizy luk i rozpoznawania zadań planu wdrożeniowych

Odnośnik GAQ	*Pytania z analizy luk*	*Odpowiedź: TAK/ NIE/ CZĘŚCIOWO*	*Opis luki*	*Zadanie/działanie, wymagane dla wypełnienia luki*	*Grupa/ Osoba, przydzielona do wykonania zadania*	*Odnośnik do dokumentu w SSP*	*Stan działania/zadania (otwarte/w toku/ zamknięte)*
1.1-1	Czy [Państwo] obwieściło krajową ramę legislacyjną bezpieczeństwa i przepisy, które definiują zarządzanie bezpieczeństwem w Państwie?	Częściowo	Brak wyraźnej definicji lub przydziału ról w istniejących organizacjach legislacyjnych, do zarządzania bezpieczeństwem.	Zadanie # 1 – Departament Prawny ma przejrzeć ramę legislacyjną	Grupa zadaniowa A	Rozdział 2, Sekcja 1	Praca w toku
1.1-2	Czy rama legislacyjna i konkretne regulacje są okresowo weryfikowane, aby pozostawały aktualne i odpowiednie dla Państwa?	Częściowo	Przegląd tylko doraźny lub fragmentaryczny. Brak SOP dla procesu okresowego przeglądu	Zadanie # 3 – Opracować SOP dla procesu okresowego przeglądu wszystkich przepisów operacyjnych	Grupa zadaniowa B	Rozdział 2, Sekcja 3	Otwarte
itp.							

Uwaga. – W tę tabelę można wstawiać wszelkie pytania dotyczące analizy luk lub tylko pytania dla odpowiedzi na „Nie/Częściowo”

Tabela 4-A7-3. Przykład harmonogramu działań/zadań wdrożeniowych

Działanie / zadanie potrzebne dla wypełnienia luki	*Odnośnik GAQ*	*Przydzielona Grupa Zadaniowa / Osoba*	*Stan działania / zadania*	*Harmonogram/przedział czasowy (początek – koniec)*												
				1Q10	2Q10	3Q10	4Q10	1Q11	2Q11	3Q11	4Q11	1Q12	2Q12	3Q12	4Q12	itd.
Zadanie # 1 – Departament Prawny ma przejrzeć ramę legislacyjną	1.1-1	Grupa Zadaniowa A	Praca w toku													
Zadanie # 2 – Zdefiniować zakres SMS		Grupa 3														
Itd.																

Uwaga. – Tabela 4-A7-3 może być, wedle życzenia, albo osobną konsolidacją albo kontynuacją Tabeli 4-A7-2 (rozkładówka) albo kontynuacją Tabeli 4-A7-2 w formie rozkładówki. Tam gdzie konieczne jest ustawienie priorytetów zadań wdrożeniowych, patrz Sekcja 4.4 niniejszego Rozdziału

Dodatek 8 do Rozdziału 4
PRZYKŁADOWY SPIS TREŚCI DOKUMENTU SSP

SPIS TREŚCI

Strona

Dodatek 9 do Rozdziału 4
PRZYKŁAD PRZEPISU PRAWNEGO Z KRAJOWEGO SMS

1. PODSTAWA USTAWOWA

SMS powinien być obwieszczony przez krajowy organ statutowy ds. lotnictwa cywilnego

2. ZAKRES PRZEPISÓW DOTYCZĄCYCH SMS

2.1. Przepis wyszczególnia wymóg, by dostawcy usług wdrożyli system zarządzania bezpieczeństwem (SMS), działający wg Załącznika 1 do Konwencji chicagowskiej - Licencjonowanie personelu; Załącznika 6 do Konwencji chicagowskiej - Eksploatacja statków powietrznych; Załącznika 8 do Konwencji chicagowskiej – Zdatność do lotu statków powietrznych; Załącznika 11 do Konwencji chicagowskiej - Służby ruchu lotniczego i Załącznika 14 ICAO do Konwencji chicagowskiej - Lotniska, w tomie I - Projektowanie i eksploatacja lotnisk.

2.2. W kontekście niniejszego przepisu, termin „service provider" (dostawca usług) odnosiłby się generalnie do zatwierdzonych/certyfikowanych organizacji świadczących usługi lotnicze. Tutaj, ten termin odnosi się do zatwierdzonych organizacji szkoleniowych, które są narażone na ryzyko operacyjne podczas świadczenia swych usług, do operatorów statków powietrznych, zatwierdzonych organizacji obsługi technicznej, organizacji odpowiedzialnych za projektowanie i/lub produkcję statków powietrznych, organizacji świadczących usługi ruchu lotniczego i do certyfikowanych lotnisk.

2.3. Ten przepis zajmuje się bardziej procesami związanymi z bezpieczeństwem lotniczym, procedurami i działaniami dostawcy usług niż bezpieczeństwem pracy, ochroną środowiska czy inną działalnością niezwiązaną z lotnictwem.

2.4. Ten przepis ustanawia minimalne wymagania dla ramy SMS. Dostawca usługi może ustanowić bardziej surowe wymagania wewnętrzne.

3. PRZYKŁAD UREGULOWANIA PRAWNEGO / KLAUZULI WYMAGALNOŚCI WOBEC SMS

3.1. Poczynając od [data] [rodzaj dostawcy usług] jest obowiązany posiadać na miejscu system zarządzania bezpieczeństwem (SMS), akceptowalny dla [CAA], który zajmując się czterema następującymi celami wysokiego poziomu bezpieczeństwa:

a) identyfikuje zagrożenia dotyczące bezpieczeństwa;

b) zapewnia wdrożenie takiego działania naprawczego jakie jest konieczne dla utrzymania uzgodnionych osiągów bezpieczeństwa;

c) zapewnia ciągłe monitorowanie i stałą ocenę osiągów bezpieczeństwa; oraz

d) ma na celu ciągłe polepszania całości działań systemu zarządzania bezpieczeństwem.

3.2. Rama niniejszego SMS musi, jako minimum, obejmować następujące komponenty i elementy:

1. Polityka bezpieczeństwa i jej cele
    - 1.1. Zaangażowanie się zarządu i odpowiedzialność
    - 1.2. Odpowiedzialność personalna za bezpieczeństwo
    - 1.3. Wyznaczenie personelu kluczowego dla systemu bezpieczeństwa
    - 1.4. Koordynacja planowania reakcji w sytuacji kryzysowej
    - 1.5. Dokumentacja SMS
2. Zarządzanie ryzykiem dotyczącym bezpieczeństwa
    - 2.1. Identyfikacja zagrożeń
    - 2.2. Ocena i łagodzenie ryzyka
3. Zapewnienie bezpieczeństwa
    - 3.1. Monitorowanie i mierzenie osiągów bezpieczeństwa
    - 3.2. Zarządzanie zmianami
    - 3.3. Ciągłe ulepszanie SMS

4. Promocja bezpieczeństwa

    4.1. Szkolenie i kształcenie

    4.2. Komunikacja w zakresie bezpieczeństwa

Uwaga. – Przepisowi dotyczącemu SMS powinno towarzyszyć dostarczenie przez Państwo wskazówek i materiałów-poradników. Takie materiały-poradniki powinny również zawierać zapis o fazowym podejściu do wdrożenia SMS. Proces zaakceptowania przez CAA systemu SMS poszczególnego dostawcy usług i uzgadniania proponowanych przez niego osiągów bezpieczeństwa powinien także być podany do wiadomości w takich wymaganiach lub w materiałach-wskazówkach.

Dodatek 10 do Rozdziału 4
PRÓBKA KRAJOWEJ POLITYKI EGZEKWOWANIA PRAWA

Politykę egzekwowania prawa obwieszcza krajowy organ statutowy ds. lotnictwa cywilnego [w zarządzeniu/zarządzeniach, poleceniach dotyczących żeglugi powietrznej lub w normach prawnych].

1. CEL

1.1. Prowadzona przez krajowego CAA polityka Państwa odnośnie egzekwowania prawa jest ukierunkowana na promowanie przestrzegania przepisów dotyczących bezpieczeństwa lotniczego i wymogów, poprzez funkcje egzekucyjne, realizowane w sposób sprawiedliwy.

1.2. Wdrażanie systemów zarządzania bezpieczeństwem (SMS) wymaga, by – dla wsparcia ramy SSP-SMS – podejście krajowego CAA do egzekwowania prawa cechowała sprawiedliwość i swoboda decyzji.

1.3. Polityka i procedury egzekwowania prawa przez krajową CAA dopuszczą do tego, by dostawcy usług załatwiali i rozwiązywali niektóre przypadki odstępstw od bezpieczeństwa we własnym zakresie, w kontekście swego SMS i za aprobatą ww. urzędu. Celowe naruszenia krajowej ustawy Prawo lotnicze i krajowych przepisów o lotnictwie cywilnym będą przedmiotem dochodzenia i mogą podlegać konwencjonalnej czynności egzekucyjnej tam gdzie taka jest praktyka. W ramie egzekwowania prawa powinny istnieć wyraźne zapisy nakazujące zajmować się takimi naruszeniami po to, by rozgraniczać między łamaniem prawa z premedytacją a niezamierzonymi błędami bądź odstępstwami.

1.4. Oświadczenie o polityce przestrzegania prawa i powiązanych procedurach egzekucyjnych ma zastosowanie do dostawców usług działających zgodnie z Załącznikami: *Załącznikiem 1 ICAO do Konwencji chicagowskiej - Licencjonowanie personelu; Załącznikiem 6 ICAO do Konwencji chicagowskiej - Eksploatacja statków powietrznych, Część I Międzynarodowy zarobkowy transport lotniczy - Samoloty i Część III - Operacje międzynarodowe – Śmigłowce; Załącznikiem 8 ICAO do Konwencji chicagowskiej - Zdatność do lotu statków powietrznych; Załącznikiem 11 ICAO do Konwencji chicagowskiej - Służby ruchu lotniczego; Załącznikiem 14 ICAO do Konwencji chicagowskiej - Lotniska , w tomie I – Projektowanie i eksploatacja lotnisk*.

2. POLITYKA

2.1. Wszyscy dostawcy usług, których to dotyczy, ustanowią i będą ściśle przestrzegać swego SMS, który ma być współmierny do rozmiaru, charakteru i złożoności operacji, do wykonywania których są upoważnieni z tytułu posiadania zatwierdzonego/certyfikowanego SMS.

2.2. Aby prowadzić taką politykę wspierania wdrażania SMS, inspektorzy krajowego CAA będą utrzymywać otwarty kanał komunikacji z dostawcami usług.

2.3. Żadnych informacji pochodzących z systemów zbierania i przetwarzania danych o bezpieczeństwie (stworzonych w oparciu o SMS), a dotyczących raportów zaklasyfikowanych jako poufne, dobrowolne lub równorzędnej kategorii, nie będą mogły być użyte jako podstawa dla postępowania egzekucyjnego.

2.4. Gdy dostawca usługi, działający na mocy SMS, nieumyślnie naruszy krajową ustawę Prawo lotnicze lub przepisy o lotnictwie cywilnym, zastosowane będą wobec danego dostawcy usług konkretne procedury przeglądu [jego postępowania]. Takie procedury dopuszczają, by inspektor CAA, odpowiedzialny za nadzorowanie dostawcy usług miał okazję zaangażować się w dialog z organizacją o zatwierdzonym SMS. Celem dialogu jest uzgodnić zaproponowane środki naprawcze i plan działania, który adekwatnie zajmie się niedociągnięciami, które doprowadziły do naruszeń oraz dać dostawcom usług rozsądny czas na wdrożenie działań naprawczych. Takie podejście ma na celu kultywowanie i utrzymywanie efektywnego raportowania o zdarzeniach, dzięki czemu pracownicy dostawców usług będą w stanie raportować niedociągnięcia w sferze bezpieczeństwa i zagrożeń, bez obawy o działania karne. Zatem, żeby włączyć środki naprawcze, które najlepiej pomogą nie dopuścić do powtórki niedociągnięć, dostawca usług będzie mógł, bez obwiniania kogokolwiek i bez strachu przed działaniem egzekucyjnym, przeanalizować zdarzenie oraz organizacyjne lub indywidualne czynniki, które być może doprowadziły do zdarzenia.

2.5. [Krajowy organ nadzoru lotniczego CAA], poprzez inspektora odpowiedzialnego za nadzorowanie dostawcy usług, oceni środki naprawcze zaproponowane przez dostawcę usług i/lub aktualnie istniejące systemy, w celu ustalenia zdarzenia leżącego u podstaw naruszenia. Jeżeli zaproponowane środki naprawcze (włącznie z odpowiednimi wewnętrznymi działania dyscyplinarnymi) zostaną uznane za zadowalające i rokujące zapobieżenie ponownemu wystąpieniu zdarzenia oraz sprzyjające przestrzeganiu przepisów w przyszłości, przegląd naruszenia powinien zostać zakończony bez żadnych sankcji ze strony podmiotu prawnego. W przypadkach, gdy bądź to środki naprawcze bądź istniejące systemy okażą się niewłaściwe, [krajowy CAA] będzie dalej kontaktował się z dostawcą usług, by znaleźć zadowalające rozwiązanie, które zapobiegnie zastosowaniu sankcji. Jednakże, w przypadkach, gdy dostawca usług odmówi podjęcia działań w związku ze zdarzeniem i przedstawienia skutecznych środków naprawczych [krajowy CAA] rozważy podjęcie sankcji lub innych działań administracyjnych, które uzna za właściwe.

2.6. Łamanie przepisów lotniczych może się zdarzać z wielu różnorodnych powodów, od autentycznego niezrozumienia przepisów po lekceważenie bezpieczeństwa w lotnictwie. [krajowy CAA] posiada pewien asortyment procedur do wymuszenia przestrzegania przepisów po to, by w różnych okolicznościach skutecznie załatwiać wynikające z odnośnej Ustawy zobowiązania dotyczące bezpieczeństwa. Procedury te mogą skutkować różnorodnością działań, takich jak:

a) doradztwo;

b) szkolenia korekcyjne;

c) zmiana wariantu upoważnienia, zawieszenie lub unieważnienie.

2.7. Na decyzje mające na celu zapewnienie przestrzegania przepisów nie może mieć wpływu:

a) konflikt o charakterze osobistym;

b) osobiste korzyści;

c) względy takie jak płeć, rasa, religia, poglądy lub powiązania polityczne; ani

d) wpływy osobiste, polityczne lub finansowe osób zainteresowanych.

3. PROPORCJONALNOŚĆ ŚRODKÓW REAGOWANIA

Decyzje dotyczące przestrzegania przepisów itp., u podstaw których są naruszenia i ryzyka dotyczącego bezpieczeństwa, muszą być proporcjonalne i muszą być oparte o trzy zasady:

a) [Krajowy CAA] podejmie działania przeciwko tym, którzy konsekwentnie i celowo operują poza przepisami obowiązującymi w lotnictwie cywilnym;

b) [Krajowy CAA] będzie starał się edukować i promować szkolenia lub objąć opieką mentorską tych, którzy wykazują zaangażowanie w rozwiązywanie niedostatków bezpieczeństwa.

c) [Krajowy CAA] dokona stosownego i uczciwego rozważenia, aby oddzielić pogwałcenie dokonane z premedytacją od niezamierzonych błędów lub odstępstw.

4. SPRAWIEDLIWOŚĆ NATURALNA I ODPOWIEDZIALNOŚĆ OSOBISTA

Decyzje mające na celu zapewnienie przestrzegania przepisów:

a) muszą być sprawiedliwe i podejmowane w należytym procesie;

b) muszą być przejrzyste dla zainteresowanych;

c) rozważając czy podjąć jakieś działanie, muszą wziąć pod uwagę okoliczności przypadku oraz postawę/czyny dostawcy usług lub osoby prywatnej;

d) muszą być działaniami/decyzjami konsekwentnymi względem takich samych/podobnych okoliczności; oraz

e) muszą podlegać odpowiedniemu przeglądowi wewnętrznemu i zewnętrznemu.

5. WYJĄTKI

5.1. Niniejsza polityka nie ma zastosowania w sytuacjach, gdy istnieją dowody na podjęcie umyślnego wysiłku dla zatajenia nieprzestrzegania przepisów.

5.2. Niniejsza polityka nie ma zastosowania w sytuacjach, gdy dostawca usług nie utrzymuje akceptowalnego SMS lub uzgodnionego stanu bezpieczeństwa.

5.3. Niniejsza polityka nie ma zastosowania, gdy Władza uznała dostawcę usług za recydywistę w naruszaniu przepisów.

5.4. W powyższych okolicznościach, Władza może zająć się takim nieprzestrzeganiem lub pogwałceniami zgodnie z ustanowionymi procedurami jakie uzna za właściwe.

(Podpisano) _____

Dyrektor Odpowiedzialny za SSP

Dodatek 11 do Rozdziału 4
WYTYCZNE DOTYCZĄCE KRAJOWYCH PROCEDUR EGZEKWOWANIA PRZEPISÓW W ŚRODOWISKU SSP-SMS

1. POSTANOWIENIA OGÓLNE

W ramach krajowego programu bezpieczeństwa (SSP), krajowy CAA odpowiada za nadzorowanie posiadaczy certyfikatów, którzy działają w środowisku SMS. Procedury egzekwowania przepisów dostarczają osobom odpowiedzialnym za nadzorowanie dostawców usług działających w środowisku SMS wskazówek dotyczących, jak reagować na błędy i pogwałcenia. Procedury te odgrywają w programie rolę pomocniczą. Ale ostateczna decyzja dotycząca egzekwowania każdego aktualnego zagadnienia SSP należy do Dyrektora Odpowiedzialnego w krajowym CAA.

2. ZASTOSOWANIA

2.1. Te procedury mają zastosowanie do naruszeń, które być może były popełnione przez osoby lub dostawców usług prowadzących działania w środowisku SSP-SMS.

2.2. Procedury wchodzą w życie z dniem [Data].

2.3. Procedury będą użyte wobec dostawców usług, którzy posiadają zaakceptowany przez krajowy CAA SMS lub którzy stosują się do „fazowego podejścia wdrażania SMS" z planem wdrożenia zaakceptowanym przez krajowy CAA.

2.4. Tam gdzie dostawcy usług lub osoby prywatne nie wykazały, że działają w środowisku SMS, działania wymuszające będą mogły być zastosowane bez korzyści wynikających z procedur opisanych w paragrafie 3.

3. PROCEDURY

3.1. W celu ustalenia czy proces badania lub egzekwowania powinien być prowadzony w otoczeniu egzekwującym SSP-SMS, konieczne będzie by panelowy ds. badań i egzekwowania ustalili jaki jest stan wdrożenia SMS danego dostawcy usług. Takiego ustalenia dokonuje się początkowo poprzez komunikację pomiędzy panelem a naczelnym inspektorem odpowiedzialnym za nadzorowanie działań dostawcy usług będącego przedmiotem dochodzenia oraz przez sprawdzenie czy ma certyfikat. Rozważania co do sankcji powinny zawsze być podejmowane przez panel osób urzędowych, wskazanych lub wyznaczonych, a nie przez pojedynczą osobę urzędową.

3.2. Naczelny inspektor ustali czy dany dostawca usług spełnia wyżej wymienione kryteria, ustalone dla procedur egzekwowania SMS. Dla ułatwienia dokonania początkowej oceny, krajowy CAA powinien mieć wykaz stanu wdrożenie SMS przez dostawców usług. Udostępnienie takiego wykazu personelowi dochodzeniowo/egzekucyjnemu pomoże im w podjęciu decyzji dotyczącej stosowalności procesu oceny badania dochodzenia/sankcji.

3.3. Przy „fazowym podejściu" do wdrażania SMS dostawcy usług, krajowy CAA może zastosować procedury wymuszające wdrożenia SMS wobec dostawców usług, którzy jeszcze nie w pełni wdrożyli lub przyjęli SMS, pod warunkiem spełnienia pewnych kryteriów.

3.4. Krajowy CAA będzie wymagać, jako minimum, by przed ewentualnym zastosowaniem procedur wymuszających SMS, spełnione były trzy następujące warunki:

a) dostawca usług posiada skuteczny, wewnętrzny proces raportowania zagrożeń i łagodzenia ryzyka;

b) dostawca usług posiada skuteczny proces dla badania zdarzeń i dla działań naprawczych, współmierny z rozmiarem i złożonością swych operacji i wystarczający do określenia czynników przyczynowych i opracowania środków naprawczych;

c) dane dotyczące bezpieczeństwa lub informacje dotyczące badanego zdarzenia są udostępniane panelowi badawczo/wymuszającemu, przy czym dostawca usług lub osoba prywatna zapewnia pełną współpracę z badawczo/wymuszającym panelem.

Wstępny raport o naruszeniu

3.5. Egzekwujący personel lotniczy powinien dokonać wstępnej analizy we wszystkich przypadkach, w których wykryto naruszenie lub co do których otrzymano informację o ewentualnym naruszeniu. Jeżeli naruszenie, o którym doniesiono, jest wynikiem oficjalnego raportu lub jest zaleceniem zeń wypływającym, panel wymuszający będzie musiał zadecydować czy raport o takim zdarzeniu jest wystarczającym wsparciem dla działania wymuszającego.

Ocena wstępna

3.6. W oparciu o otrzymane informacje należy rozważyć następujące kwestie:

a) Czy istnieją uzasadnione podstawy by wierzyć, że osoba lub organizacja prowadząca działalność w ramach SMS mogła popełnić naruszenie?

b) Czy zdarzenie jest tego rodzaju (np. poważne/powtarzające się nieprzestrzeganie), który uzasadnia podjęcie działania wymuszającego?

c) Czy są jakiekolwiek dalsze informacje lub dowody, takie jak stany uśpione, czynniki organizacyjne/ ludzkie, które powinny być zabezpieczone dla ułatwienia decyzji czy podjąć działanie wymuszające?

Gdy odpowiedzi na te pytania są twierdzące, należy zwrócić się do naczelnego inspektora o zgodę na kontynuowanie oceniania akcji wymuszania, tam gdzie to ma zastosowanie.

Ocena czy podjąć działanie wymuszające, oraz ewentualne zalecenie

3.7. Proces ustalania odpowiedniej, uczciwej i równocześnie skutecznej kary administracyjnej (lub finansowej) przez panel powołany do egzekwowania [przepisów] musi być oparty na obiektywnym procesie, który uwzględnia wszystkie znane okoliczności przyczynowe, środowiskowe i stany uśpione. Włączone powinny być czynniki organizacyjne, ludzkie i inne czynniki eskalacyjne, tam gdzie to ma zastosowanie. Inne czynniki, takie jak to czy postępowanie jest błędem niezamierzonym czy działaniem celowym powinny być wzięte pod uwagę.

3.8. Z chwilą podjęcia decyzji co do odpowiedniej akcji wymuszającej, panel powinien przygotować odpowiednie zalecenie do zatwierdzenia przez Dyrektora Odpowiedzialnego, a następnie zawiadamiać zainteresowane strony.

Dodatek 12 do Rozdziału 4
PRZYKŁAD LISTY KONTROLNEJ OCENY I AKCEPTACJI SMS NA ZGODNOŚĆ Z PRZEPISAMI

1. Tabela 4-A12-1 jest próbką (85 pytań) ustawowej listy kontrolnej oceny SMS, którą można wykorzystać do początkowej oceny i akceptacji SMS dostawcy usług. Dla każdego początkowego procesu akceptacji, pytania oceniające muszą być wyczerpujące po to, by móc adekwatnie zająć się wszystkimi elementami SMS danej organizacji. Da to pewność, iż wszystkie elementy i ich odnośne procesy są na miejscu w organizacji. Aspektami operacyjnymi SMS byłoby lepiej się zająć podczas kolejnych rutynowych/corocznych ocen SMS.

2. Przedstawiona procedura akceptowania osiągów minimalnych dostarcza minimalnych kryteriów akceptowania wyników w trzech etapach. Ta procedura może umożliwić ustawodawcy progresywne dokonywanie oceny procesu wdrażania SMS przez dostawcę usług, zamiast audytować dopiero po pełnym wdrożeniu SMS lub osiągnięciu stanu dojrzałego. Protokół z takiej progresywnej oceny również zapewni to, że ustawodawca będzie aktywnie zaangażowany w monitorowanie wdrażania branżowego SMS już od najwcześniejszych faz.

3. Tam gdzie przyjęto podejście, iż wdrożenie ma być fazowe, omówione w Rozdziale 5 niniejszego dokumentu, być może trzeba będzie w liście kontrolnej przekonfigurować (określone przez Państwo) już przyjęte pytania i zaadaptować je tak, by przystawały do konkretnego rozrzutu elementów po odnośnych fazach.

4. Ilustratywna procedura zawiadamiania o akcji naprawczej (CAN) jest podana pod koniec listy kontrolnej.

5. Tabela 4-A12-2 jest przykładem (39 pytań) ustawowej listy kontrolnej oceniania SMS, którą można wykorzystać przy kolejnym rutynowym ocenianiu SMS. Po tym jak SMS organizacji spełni wstępne wymagania prawodawcy i procesu akceptacji, na liście kontrolnej początkowej oceny pozostanie jeszcze wiele oceniających pytań, które nie będą już celowe ani niezbędne dla potrzeb oceny rutynowej. Lista kontrolna rutynowej oceny SMS musi się koncentrować tylko na aspektach operacyjnych SMS oraz na dowodach zadowalającego wdrożenia procesów ją wspomagających.

6. Rutynową ocenę SMS można przeprowadzić jako operację ustawodawcy, całkowicie samodzielną lub włączoną do rutynowego audytu organizacji/systemu jako jego część. W tym drugim przypadku, pytania rutynowej oceny SMS mogą być włączone w listę kontrolną audytowania organizacji, jako część składowa. Audytora wykonującego zintegrowany audyt QMS-SMS trzeba będzie odpowiednio przeszkolić pod kątem prowadzenia audytu SMS. Do rutynowej oceny SMS można również zastosować protokół ustawodawcy, normalnie stosowany do zawiadamiania o działaniach naprawczych (CAN).

Tabela 4-A12-1. Lista kontrolna oceny SMS – początkowa akceptacja SMS

Lista kontrolna oceny SMS – Akceptacja początkowa			Lista kontrolna rutynowego audytu SMS / 18 sierpnia 2011
Kolumna wpisywania: WPISZ „T" dla TAK, „N" dla NIE „ND" dla NIE DOTYCZY			
Nazwa organizacji:	Data oceny:	Ocenę przeprowadził Naczelny Inspektor (POI/PMI):	Znak:

Element SMS	**Poziom 1**	**Wpis**	**Nr dok./ Uwagi**	**Poziom 2**	**Wpis**	**Nr dok./ Uwagi**	**Poziom 3**	**Wpis**	**Nr dok./ Uwagi**
Zaangażowanie kierownictwa i odpowiedzialności [1.1]	**SMS Komponent nr 1. Polityka bezpieczeństwa i jej cele**								
	1.1/L1/1			1.1/L2/1			1.1/L3/1		
	Jest udokumentowane oświadczenie o polityce bezpieczeństwa.	T		Są dowody, że polityka bezpieczeństwa jest przekazywana wszystkim pracownikom z zamiarem uświadomienia im ich indywidualnych obowiązków związanych z bezpieczeństwem.	N		Jest okresowy przegląd polityki bezpieczeństwa przeprowadzony przez najwyższe kierownictwo lub komisję/zespół ds. bezpieczeństwa.	N	
	1.1/L1/2			1.1/L2/2			1.1/L3/2		
	Polityka bezpieczeństwa przystaje do bezpieczeństwa lotniczego.	T		Polityka bezpieczeństwa ma poparcie Dyrektora Odpowiedzialnego.	T		Zapis obowiązków Dyrektora Odpowiedzialnego wskazuje na jego całościową odpowiedzialność za wszystkie zagadnienia.	N	
	1.1/L1/3			1.1/L2/3					
	Polityka bezpieczeństwa jest odpowiednia do zakresu i złożoności operacji organizacji.	N		Polityka bezpieczeństwa zawiera zapis o zapewnieniu odpowiednich zasobów ludzkich i finansowych dla jej wdrożenia.	N		.___		
Zakresy odpowiedzialności bezpieczeństwa [1.2]	1.2/L1/1			1.2/L2/1					
	Jest udokumentowana w SMS odpowiedzialność personalna za bezpieczeństwo w organizacji, która się zaczyna się ona od kierownika odpowiedzialnego.	T		Zakres obowiązków kierownika odpowiedzialnego wskazuje na jego ostateczną odpowiedzialność za zarządzanie bezpieczeństwem w organizacji.	N		___		
	1.2/L1/2			1.2/L2/2					
	Dyrektor Odpowiedzialny ma władzę ostateczną nad wszystkimi działaniami lotniczymi organizacji.	N		Ostateczna władza nad działalnością lotniczą realizowaną w oparciu o certyfikat (y) organizacji jest zapisana w zakresie obowiązków Dyrektora Odpowiedzialnego.	N		___		
	1.2/L1/3			1.2/L2/3			1.2/L3/1		

Element SMS	Poziom 1	Wpis	Nr dok./ Uwagi	Poziom 2	Wpis	Nr dok./ Uwagi	Poziom 3	Wpis	Nr dok./ Uwagi
Zakresy odpowiedzialności bezpieczeństwa [1.2]	Jest komisja (lub zespół ekwiwalentny) ds. bezpieczeństwa, który dokonuje przeglądów SMS i działania bezpieczeństwa.	T		W dużej organizacji jest wydziałowa/sekcyjna grupa ds. działań dla bezpieczeństwa, współpracująca z komisją.	ND		Komisji (lub zespołowi przewodniczy kierownik odpowiedzialny lub w bardzo dużych organizacjach) stosownie wyznaczony zastępca, odpowiednio potwierdzony w podręczniku SMS.	T	
	1.2/L1/4			1.2/L2/4			1.2/L3/2		
	W komisji bezpieczeństwa są odnośni operacyjni lub wydziałowi naczelnicy	N		Jest w obrębie grupy akcji wyznaczony koordynator bezpieczeństwa (SMS).	ND		Grupom akcji bezpieczeństwa przewodniczy naczelnik wydziału lub sekcji	ND	
Wyznaczenie kluczowego personelu bezpieczeństwa [1.3]	1.3/L1/1			1.3/L2/1			1.3/L3/1		
	Jest kierownik z funkcją administrowania SMS.	T		Kierownik, odpowiedzialny za administrowanie SMS nie ma innych odpowiedzialności, które byłyby w konflikcie z SMS bądź osłabiałyby jego rolę jako kierownika SMS.	N		Kierownik SMS ma bezpośredni dostęp do kierownika odpowiedzialnego, lub raportowaniu mu wdrażania i działania SMS.	N	
	1.3/L1/2						1.3/L3/2		
	Kierownik, mający rolę w SMS, ma w zakresie obowiązków wpisane odpowiednie funkcje w SMS.	N		—			Kierownik SMS ma stanowisko wysokie, nie niższe ani nie podporządkowane stanowiskom operacyjnym lub produkcyjnym.	N	
Planowanie reagowania awaryjnego [1.4]	1.4/L1/1			1.4/L2/1			1.4/L3/1		
	Jest udokumentowany plan reagowania awaryjnego ERP lub równoważna, operacyjna procedura na taką ewentualność.	T		ERP zawiera procedury zapewniania ciągłej, bezpiecznej produkcji, dostaw lub zabezpieczania wsparcia dla produktów lotniczych lub usług podczas sytuacji awaryjnych lub podobnych ewentualności.	N		Tam gdzie to ma zastosowanie, ERP zajmuje się stosowną integracją z klientem zewnętrznym lub organizacji podwykonawczych.	N	
	1.4/L1/2			1.4/L2/2			1.4/L3/2		
	ERP jest odpowiedni dla wielkości, charakteru i złożoności organizacji	T		Jest plan ćwiczeń i praktyk w zakresie ERP.	T		Jest procedura dla okresowego przeglądu ERP dla zapewnienia jego stałej przydatności i skuteczności.	N	
	1.4/L1/3			1.4/L2/3					
	Plan awaryjny zajmuje się możliwymi lub prawdopodobnymi scenariuszami dla związanych z produkcją lotniczą lub z usługami sytuacjami awaryjnymi.	N		Ćwiczenia i praktyki ERP są realizowane zgodnie z planem, a wyniki przeprowadzonych ćwiczeń są dokumentowane.	N		—		
	1.5/L1/1			1.5/L2/1			1.5/L3/1		

Element SMS	Poziom 1	Wpis	Nr dok./ Uwagi	Poziom 2	Wpis	Nr dok./ Uwagi	Poziom 3	Wpis	Nr dok./ Uwagi
Dokumentacja SMS [1.5]	Jest dokument w SMS, lub dokument go prezentujący, zatwierdzony przez Dyrektora Odpowiedzialnego i zaakceptowany przez CAA.	T		Dokument SMS jest przyjęty lub parafowany przez krajową władzę lotniczą organizacji.	T		Procedury SMS odzwierciedlają odpowiednią integrację z innymi odnośnym systemami zarządzania wewnątrz organizacji, takimi jak QMS, OSHE, Ochrona.	N	
	1.5/L1/2			1.5/L2/2			1.5/L3/2		
	Dokument SMS zapewnia ogląd lub prezentację ramy i elementów SMS organizacji.	T		Zawarta w dokumencie SMS autoprezentacja każdego element obejmuje odsyłacze do procedur wsparcia i procedur pokrewnych, do podręczników lub systemów.	T		Procedury SMS odzwierciedlają odpowiednią koordynację lub integrację z zewnętrznymi organizacjami (organizacje klientów lub podwykonawców).	N	
	1.5/L1/3			1.5/L2/3			1.5/L3/3		
	Dokument SMS jest samodzielnym kontrolowanym dokumentem lub wyraźną częścią/sekcją dokumentu istniejącego i parafowanego /zaakceptowanego przez CAA.	T		Przechowywane są zapiski dotyczące protokołów ze spotkań Komisji Bezpieczeństwa/SAG (lub równoważnego).	T		Jest proces okresowego przeglądu charakterystyki SMS i dokumentacji wspierającej, dla zapewnienia ich ciągłej odpowiedniości.	N	
	1.5/L1/4			1.5/L2/4					
	Wszystkie komponenty i elementy ustawowych wymagań są w dokumencie SMS omówione.	T		Są dostępne zapisy należące do okresowego przeglądu istniejącego bezpieczeństwa / ryzyka, lub do specjalnego przeglądu związanego ze zmianami.	N		—		
	1.5/L1/5								
	Prowadzi się zapisy z przeprowadzonego procesu zarządzania ryzykiem.	T		—			—		
	1.5/L1/6								
	Prowadzi się zapisy dotyczące zidentyfikowanych lub zgłoszonych zagrożeń/ gróźb.	T		—			—		
Identyfikacja zagrożenia[2.1]	**SMS Komponent nr 2. Zarządzanie ryzykiem dotyczącym bezpieczeństwa**								
	2.1/L1/1			2.1/L2/1			2.1/L3/1		

Element SMS	Poziom 1	Wpis	Nr dok./ Uwagi	Poziom 2	Wpis	Nr dok./ Uwagi	Poziom 3	Wpis	Nr dok./ Uwagi
	Jest procedura dobrowolnego powiadamiania przez pracowników o zagrożeniach.	T		W systemie identyfikacji zagrożenia jest definicja i wyraźne rozróżnienie między zagrożeniami i konsekwencjami.	N		Jest procedura dobrowolnego powiadamiania przez pracowników o zagrożeniach.	T	
	2.1/L1/2			2.1/L2/2			2.1/L3/2		
	Jest procedura powiadamiania przez personel operacyjny i produkcyjny o incydentach/wypadkach.	T		System powiadamiania o zagrożeniu jest poufny i zawiera postanowienia dla ochrony danych zgłaszającego.	N		Jest procedura powiadamiania przez personel operacyjny i produkcyjny o incydentach/wypadkach.	T	
	2.1/L1/3			2.1/L2/3			2.1/L3/3		
	Jest badania zdarzeń/wypadków związanych z jakością lub bezpieczeństwem.	T		Wew. procedura organizacji badania i dyscypliny rozróżnia między świadomymi i umyślnymi a niezamierzonych błędami.	N		Jest procedura badania zdarzeń/wypadków związanych z jakością lub bezpieczeństwem.	T	
Ocena ryzyka bezpieczeństwa i ograniczenia [2.2]	2.2/L1/1			2.2/L2/1					
	Jest udokumentowana procedura (HIRM), uwzględniająca stosowanie narzędzi obiektywnej analizy ryzyka.	T		Protokoły procesu zarządzania ryzykiem są zatwierdzane przez dyrektorów oddziałów lub wyżej.	N		___		
	2.2/L1/2			2.2/L2/2					
	Jest procedura identyfikowania operacji, procesów, obiektów i sprzętu (uznanych przez organizację) jako dotyczących HIRM.	N		Zalecane działania łagodzące wymagające decyzji lub zatwierdzenia przez personel kierowniczy są uwzględnione i udokumentowane.	N		___		
	2.2/L1/3			2.2/L2/3			2.2/L3/1		
	Jest, zdefiniowany przez organizację, program progresywnego działania HIRA – dla wszystkich operacji, procesów, obiektów i sprzętu zidentyfikowanych przez organizację.	N		Jest procedura dla określenia priorytetów działania HIRA dla operacji /procesów/obiektów /wyposażenia o zidentyfikowanych lub znanych zagrożeniach krytycznych dla bezpieczeństwa.	N		Są dowody na stopniowe podporządkowywanie i i prowadzenie programu działania HIRA w organizacji.	N	
Monitorowanie poziomu bezpieczeństwa oraz [3.1]	**SMS Komponent nr 3. Zapewnianie bezpieczeństwa**								
	3.1/L1/1			3.1/L2/1			3.1/L3/1		

Element SMS	Poziom 1	Wpis	Nr dok./ Uwagi	Poziom 2	Wpis	Nr dok./ Uwagi	Poziom 3	Wpis	Nr dok./ Uwagi
	Są zidentyfikowane wskaźniki działania bezpieczeństwa, służące mierzeniu i monitorowaniu działania bezpieczeństwa w organizacji.	T		Są wskaźniki małych konsekwencji dla działania bezpieczeństwa (np. wydarzenia niespełniania, odchyleń od standardu).	N		Jest procedura podejmowania działań naprawczych lub kontrolnych w przypadku nie osiągnięcia celów i/lub przekroczenia poziomów alarmowych.	N	
	3.1/L1/2			3.1/L2/2			3.1/L3/2		
	Są wskaźniki, z bazy danych, dużych konsekwencji dla działania bezpieczeństwa (np. ilości wypadków i poważnych incydentów).	T		We wskaźnikach działania bezpieczeństwa są ustawienia poziomu alarmowego i/docelowego.	N		Wskaźniki poziomu bezpieczeństwa są przeglądane przez komisję ds. bezpieczeństwa - czy nie ma trendów, przekroczeń poziomów alarmowych i osiągnięć wielkości docelowych.	T	
Zarządzanie zmianą [3.2]	3.2/L1/1			3.2/L2/1			3.2/L3/1		
	Jest procedura przeglądania związanych z bezpieczeństwem lotniczym obiektów i sprzętu (w tym zapisów HIRA), zawsze gdy zachodzą w nich zmiany.	N		Jest procedura przeglądania – związanych z bezpieczeństwem lotniczym nowych obiektów i sprzętu - pod kątem zagrożeń, przed ich odbiorem od dostawcy.	N		Jest procedura dla przeglądania – związanych z bezpieczeństwem lotniczym – istniejących obiektów, sprzętu, operacji lub procesów (włącznie z zapisami HIRA) - zawsze gdy zachodzą zmiany poza organizacją/ przedsiębiorstwem, jak w przepisach, normach, uznanych praktykach lub technice.	N	
	3.2/L1/2			3.2/L2/2					
	Jest procedura przeglądania związanych z bezpieczeństwem lotniczym istniejących operacji i procesów (w tym zapisów HIRA), zawsze gdy zachodzą w nich zmiany.	N		Jest procedura – związanych z bezpieczeństwem lotniczym – nowych operacji i procesów pod kątem zagrożeń, przed ich odbiorem od dostawcy.	N		___		
Ciągłe doskonalenie SMS [3.3]	3.3/L1/1			3.3/L2/1			3.3/L3/1		
	Jest procedura wykonywania okresowych audytów wewnętrznych /dokonywania oceny SMS.	T		Jest procedura na działania naprawcze po audycie.	T		Audyt SMS/jego ocena została wykonana zgodnie z planem.	N	

Element SMS	Poziom 1	Wpis	Nr dok./ Uwagi	Poziom 2	Wpis	Nr dok./ Uwagi	Poziom 3	Wpis	Nr dok./ Uwagi
	3.3/L1/2			3.3/L2/2			3.3/L3/2		
	Jest aktualny plan wewnętrznego audytu SMS / jego oceny.	N		—			Jest proces przedkładania kierownikowi odpowiedzialnemu protokołów z audytów SMS/oceny (lub zwracania jego uwagi na główne punkty), gdy zachodzi potrzeba.	N	
	3.3/L1/3			3.3/L2/3			3.3/L3/3		
	Jest udokumentowana procedura dla prowadzenia wewnętrznego audytu/oceny SMS.	N		Plan audytu SMS obejmuje próbkowanie zakończonych ocen bezpieczeństwa.	N		Plan audytu SMS obejmuje role/wkłady dostawców w SMS, gdzie możliwe.	N	
Szkolenia I komunikacja [4.1, 4.2]	**SMS Komponent nr 4. Promocja bezpieczeństwa**								
	4.1/L1/1			4.1/L2/1			4.1/L3/1		
	Jest udokumentowana polityka szkolenia/zapoznawania personelu z SMS.	T		Personel zaangażowany w prowadzenie procesu zarządzania ryzykiem został odpowiednio w ryzykach przeszkolony lub zaznajomiony.	N		Są dowody na wysiłek włożony po całej organizacji na edukację i uświadamianie o SMS.	N	
	4.1/L1/2			4.1/L2/2			4.1/L3/2		
	Kierownik odpowiedzialny za administrowanie SMS przeszedł odpowiednio szkoleniowy kurs na SMS.	T		Personel bezpośrednio zaangażowany w SMS (członkowie Komisji Bezpieczeństwa/SAG) przeszli odpowiednie szkolenie SMS lub zostali odpowiednio zapoznani.	N		Są dowody opublikowania (SMS), okólników i że działają kanały komunikowania pracownikom zagadnień dotyczących bezpieczeństwa i SMS.	N	
	4.1/L1/3								
	Kierownik odpowiedzialny przeszedł odpowiednie zapoznanie z SMS, odprawę lub szkolenia,	T		—			—		

WYNIK CZĘŚCIOWY	Kategoria 1
T	23
N	11
ND	0
Liczba pytań na które odpowiedziano	34

Kategoria 2
6
21
2
29

Kategoria 3
2
19
1
22

WARTOŚĆ CAŁKOWITA*	
T	31
N	51
Nie dotyczy	3
Liczba pytań na które odpowiedziano	85

WYNIK OCENY (% TAK)
38,7%

PROCEDURA ZAWIADOMIENIA O [POTRZEBNYCH] DZIAŁANIACH NAPRAWCZYCH (CAN)

1) Minimalnie akceptowalne działanie całości (fazowe wdrożenie SMS):

1-szy rok/faza oceny (np. 2012) – 45%
2-gi rok /faza oceny (np. 2013) – 65%
3-ci rok / faza oceny (np. 2014), a w kolejnych – 85%
[Dziewięćdziesiąt (90) dni dla działania naprawczego po to, by uzyskać działanie całości nie mniejsze niż 45-procentowe.

2) Podstawowe działania (pytania z Poziomu nr 1) (w dowolnym roku/fazie oceny, następujących po wymaganej przez Państwo dacie zastosowanie wymagania SMS]:

Za pytania z Poziomu 1 z odpowiedzią na „NIE" (w każdym roku /fazie oceny), mają być wystawiane zawiadomienia o [potrzebie] akcji naprawczej (CAN).
Aby na odnośne pytanie/pytania uzyskać odpowiedź na „TAK", potrzeba sześćdziesięciu (60) dni na działania naprawcze.

Tabela 4-A12-2. Lista kontrolna oceny SMS – Rutynowa ocena SMS

Element SMS		*Pytanie oceniające*
Zaangażowanie się kierownictwa i ich obowiązki (1.1)	1	Polityka bezpieczeństwa jest odpowiednia do zakresu i złożoności operacji organizacji.
	2	Są dowody potwierdzające, że polityka bezpieczeństwa jest komunikowana wszystkim pracownikom z zamiarem uświadomienia ich o indywidualnych obowiązkach dotyczących bezpieczeństwa.
	3	Najwyższe kierownictwo lub komitet/zespół ds. bezpieczeństwa okresowo dokonuje przeglądu polityki bezpieczeństwa.
	4	Zakres obowiązków Dyrektora Odpowiedzialnego wskazuje na jego całościową odpowiedzialność za wszystkie zagadnienia związane z bezpieczeństwem.
Odpowiedzialność personalna za bezpieczeństwo (1.2)	1	Jest komisja/zespół ds. bezpieczeństwa (lub równoważny mechanizm), która dokonuje przeglądu SMS i jego osiągów w sferze bezpieczeństwa.
	2	Dyrektor Odpowiedzialny ma zapisaną w swoich obowiązkach ostateczną odpowiedzialność za wszystkie operacje prowadzone na podstawie certyfikatu(ów) organizacji.
Wyznaczenie personelu kluczowego dla bezpieczeństwa (1.3)	1	Kierownik pełniący taką rolę w SMS ma w swych obowiązkach wpisane odpowiednie funkcje.
	2	Dyrektor odpowiedzialny za administrowanie SMS nie ma innych obowiązków, które mogłyby być w konflikcie z jego rolą Dyrektora SMS lub ją utrudniać.
	3	Kierownik SMS ma bezpośredni dostęp do Dyrektora Odpowiedzialnego i jemu raportuje w sprawach dot. wdrożenia i działania SMS.
	4	Kierownik SMS zajmuje wyższe stanowisko kierownicze, nie niższe, lub takie samo jak inne stanowiska operacyjne lub produkcyjne.
Planowanie reagowania awaryjnego (1.4)	1	Plan reagowania awaryjnego zajmuje się możliwymi lub prawdopodobnymi scenariuszami dla sytuacji awaryjnych/kryzysowych, związanych z usługami lotniczymi świadczonymi przez organizację.
	2	ERP zawiera procedury zapewnienia ciągłej, bezpiecznej produkcji, dostaw lub wsparcia dla swoich produktów lotniczych lub usług w sytuacjach awaryjnych itp. okolicznościach.
	3	Ćwiczenia i praktyki ERP są realizowane zgodnie z planem, a wyniki przeprowadzonych ćwiczeń są dokumentowane.
	4	ERP zajmuje się stosowną integracją z klientem zewnętrznym lub podwykonawcą organizacji, jeśli takich ma.
	5	Obowiązuje procedura okresowego przeglądu ERP dla zapewnienia jego stałej przydatności i skuteczności.
Dokumentacja SMS (1.5)	1	Wszystkie komponenty i elementy SMS organizacji są w dokumencie SMS odpowiednio prezentowane.
	2	Udokumentowane komponenty i elementy SMS organizacji są zgodne z wymaganiami SMS władzy lotniczej.
	3	Są dowody odpowiedniej koordynacji lub integracji SMS z zewnętrznym klientem lub podwykonawcami organizacji, tam gdzie to ma zastosowanie.
	4	Są dowody na istnienie procedur dla okresowego przeglądu dokumentu SMS i dokumentacji wspierającej, dla zapewnienia ich ciągłej doniosłości.
	5	Dostępna jest dokumentacja dotycząca okresowego przeglądu istniejących procesu zarządzania ryzykiem.
Identyfikacja zagrożeń (2.1)	1	Liczba lub wielkość zarejestrowanych przez organizację lub zebranych raportów o zagrożeniu jest współmierna do wielkości i zakresu operacji wykonywanych przez tę organizację.
	2	System raportowania o zagrożeniach jest poufny i zawiera zapisy dla ochrony danych zgłaszającego.
	3	Są dowody potwierdzające, że zagrożenia/groźby, odkryte podczas badania incydentu/wypadku są rejestrowane w systemie HIRM.

Element SMS		*Pytanie oceniające*
	4	Są dowody na to, że zarejestrowane zagrożenia są systematycznie analizowane dla podjęcia działań łagodzących, gdzie ma to zastosowanie.
Proces zarządzania ryzykiem i łagodzenie (2.2)	1	Są dowody na to, że mające wpływ na bezpieczeństwo lotnicze operacje/procesy/obiekty/sprzęt są stopniowo poddawane procesowi HIRM w organizacji.
	2	Zamknięte protokoły procesu zarządzania ryzykiem są zatwierdzane przez kierownictwo odpowiedniego szczebla.
	3	Jest procedura okresowego przeglądu zamkniętych zapisów z łagodzenia ryzyka.
Monitorowanie i mierzenie poziomu bezpieczeństwa (3.1)	1	Wskaźniki działania bezpieczeństwa w SMS organizacji zostały uzgodnione z odnośną krajową władzą lotniczą.
	2	Są, oparte na bazie danych, wskaźniki dużych konsekwencji dla działania bezpieczeństwa (np. liczby wypadków i poważnych incydentów).
	3	Są, oparte na bazie danych, wskaźniki mniejszych konsekwencji dla działania bezpieczeństwa (np. nieprzestrzeganie, odchylenia).
	4	Tam gdzie ma to zastosowanie, we wskaźnikach działania bezpieczeństwa są poziomy alarmowe i/lub docelowe.
	5	Procedura zarządzania zmianami w organizacji obejmuje wymóg dokonania procesu zarządzania ryzykiem, zawsze gdy zaistnieje.
	6	Są dowody podejmowania działań naprawczych lub dalszych badań w przypadku nieosiągnięcia celów i/lub przekroczenia poziomów alarmowych.
Zarządzanie zmianami (3.2)	1	Są dowody na to, że odpowiednie procesy związane z bezpieczeństwem lotniczym i operacjami zostały podporządkowane procesowi HIRM organizacji.
	2	Procedura zarządzania zmianą w organizacji obejmuje wymóg dokonania procesu zarządzania ryzykiem, zawsze gdy wystąpi.
Ciągłe usprawnianie SMS (3.3)	1	Są dowody na to, że wewnętrzny audyt/ocena SMS /był zaplanowany i zrealizowany.
Szkolenie, edukacja i komunikacja (4.1, 4.2)	1	Są dowody na to, że personel zaangażowany w operacje SMS otrzymał odpowiednie szkolenie lub został odpowiednio zapoznany z SMS.
	2	Personel zaangażowany w prowadzenie oceny ryzyka otrzymuje odpowiednie przeszkolenie w zarządzaniu ryzykiem lub jest zapoznawany z zarządzaniem.
	3	Są dowody na istnienie publikacji (SMS) związanych z bezpieczeństwem, okólników oraz kanałów komunikowania pracownikom zagadnień związanych z bezpieczeństwem i SMS.

Rozdział 5
SYSTEM ZARZĄDZANIA BEZPIECZESTWEM (SMS)

5.1. WPROWADZENIE

5.1.1. SMS jest systemem zapewniania bezpieczeństwa operacji statków powietrznych poprzez efektywne zarządzanie ryzykiem dotyczącym bezpieczeństwa. System został zaprojektowany dla ciągłego ulepszania bezpieczeństwa poprzez rozpoznawanie zagrożeń, zbieranie i analizowanie danych oraz nieustanne prowadzenie procesu zarządzania ryzykiem. SMS dąży do proaktywnego opanowania, bądź łagodzenia ryzyka zanim któryś jego przypadek przeistoczy się w wypadki lub incydenty lotnicze. Jest to system współmierny do zobowiązań prawnych organizacji i jego celów w sferze bezpieczeństwa.

5.1.2. SMS jest dla organizacji lotniczej koniecznością, aby móc identyfikować zagrożenia i zarządzać ryzykiem, jakie istnieją dla bezpieczeństwa podczas dostarczania swych produktów i usług. SMS zawiera kluczowe elementy, bardzo istotne dla identyfikowania zagrożeń i dla zarządzania bezpieczeństwem, poprzez zapewnianie, że:

a) potrzebne informacje są dostępne;

b) odpowiednie narzędzia są dostępne dla organizacji;

c) narzędzia są odpowiednie dla danego zadania;

d) narzędzia są współmierne do istniejących w organizacji potrzeb i ograniczeń; oraz

e) decyzje są podejmowane w oparciu o pełne uwzględnienie ryzyka dotyczącego bezpieczeństwa.

5.2. ZAKRES

SMS zajmuje się działaniami lotniczymi dostarczyciela usług lotniczych, które mają związek z bezpiecznymi operacjami statków powietrznych. Zakres SMS może bezpośrednio obejmować inne działania tego dostawcy usług, wspomagających rozwój operacji i produktów, takie jak finanse, zasoby ludzkie, prawodawstwa. Istotne jest zatem przyciągnięcie tych wszystkich wewnętrznych i zewnętrznych uczestników systemu lotnictwa, którzy mają ewentualny wpływ na poziom bezpieczeństwa organizacji. Ponadto, wszelkie potencjalne, wprowadzane dane powinny być brane pod uwagę na wczesnym etapie wdrażania SMS, jak również przez cały czas przyszłych i wewnętrznych ewolucji. Takich danych mogą dostawcom usług dostarczać następujący uczestnicy, zależnie od ich potencjalnych wpływów na działanie bezpieczeństwa:

a) profesjonalni pracownicy lotnictwa;

b) władze ustawodawcze i administracyjne lotnictwa;

c) zrzeszenia branżowe;

d) stowarzyszenia i federacje zawodowe;

e) międzynarodowe organizacje lotnicze;

f) podwykonawcy lub kierownictwo dostawców usług; oraz

g) pasażerowie.

5.3. RAMA SMS

5.3.1. Ta sekcja przedstawia ramę dla wdrażania SMS przez istotnych dostawców usług lotniczych. Należy zauważyć, że wdrożenie tej ramy powinno być współmierne do wielkości organizacji i złożoności jego produktów i usług.

5.3.2. Rama obejmuje cztery komponenty i dwanaście elementów, reprezentujących minimalne wymogi dla wdrożenia SMS. Oto cztery komponenty systemu SMS:

a) polityka bezpieczeństwa i jej cele;

b) zarządzanie ryzykiem dotyczącym bezpieczeństwa;

c) zapewnianie bezpieczeństwa; oraz

d) promocja bezpieczeństwa.

5.3.3. Polityka bezpieczeństwa i jej cele tworzą warunki SMS. Celem komponentu zarządzania ryzykiem dotyczącym bezpieczeństwa jest identyfikować zagrożenia, oceniać zagrożenia pokrewne i rozwijać odpowiednie sposoby ich łagodzenia w kontekście dostaw produktów i usług. Zapewnianie bezpieczeństwa osiąga się poprzez stale trwające procesy, które monitorują zgodność z międzynarodowymi standardami i krajowymi przepisami. Ponadto, proces zapewniania bezpieczeństwa daje zaufanie, że SMS działa tak jak był zaprojektowany i że jest skuteczny. Promocja bezpieczeństwa zapewnia konieczną świadomość i szkolenie.

5.3.4. Cztery komponenty i dwanaście elementów, które składają się na ramę ICAO SMS, to:

1. Polityka bezpieczeństwa i jej cele

    1.1. Zaangażowanie się kierownictwa i zakresy obowiązków

    1.2. Odpowiedzialność personalna za bezpieczeństwo

    1.3. Powołanie personelu kluczowego dla bezpieczeństwa

    1.4. Koordynacja planów reagowania awaryjnego

    1.5. Dokumentacja SMS

2. Zarządzanie ryzykiem dotyczącym bezpieczeństwa

    2.1. Identyfikacja zagrożeń

    2.2. Proces zarządzania ryzykiem i łagodzenie ryzyka dotyczącego bezpieczeństwa

3. Zapewnianie bezpieczeństwa

    3.1. Monitorowanie realizacji założeń bezpieczeństwa i analiza

    3.2. Zarządzanie zmianami

    3.3. Stałe ulepszanie SMS

4. Promocja bezpieczeństwa

    4.1. Szkolenie i edukowanie

    4.2. Komunikacja dotycząca bezpieczeństwa.

5.3.5. Powyższe elementy i komponenty uzupełnione są o dodatkowe szczegóły. Sporządza się je, na wysokim poziomie, streszcza każdy z komponentów, po którym następuje tekst z ramy SMS, dotyczący każdego elementu. Następnie, dla każdego elementu, prezentowane są strategie ogólnego ukierunkowania i wdrażania.

Komponent nr 1 SMS. Polityka bezpieczeństwa i jej cele

5.3.6. Aby SMS organizacji osiągnął pożądane efekty bezpieczeństwa, polityka bezpieczeństwa nakreśla zasady, procesy i metody. Polityka ustanawia to jakie będzie zaangażowanie najwyższego kierownictwa w scalanie bezpieczeństwa i stałe jego ulepszanie we wszystkich aspektach działań kierownictwa. Najwyższe kierownictwo opracowuje osiągalne cele w całej organizacji.

Element 1.1 programu SMS.
Zaangażowanie się kierownictwa i ich odpowiedzialności

Dostawca usług musi zdefiniować swą politykę bezpieczeństwa zgodnie z wymogami międzynarodowymi i krajowymi. Polityka bezpieczeństwa musi:

a) odzwierciedlać zaangażowanie organizacji w bezpieczeństwo;

b) zawierać wyraźne oświadczenie o zapewnieniu zasobów potrzebnych dla wdrożenia polityki bezpieczeństwa;

c) zawierać procedury dla raportowania bezpieczeństwa;

d) wyraźnie wskazywać jakie typy zachowania są nieakceptowalne względem działalności lotniczej dostawców usług oraz obejmować okoliczności, w których działania dyscyplinarne nie mają zastosowania;

e) być podpisana przez Dyrektora Odpowiedzialnego organizacji;

f) być komunikowana w całej organizacji, przy czym jej potwierdzone poparcie musi być widoczne; oraz

g) być okresowo weryfikowana, w celu zapewnienia, że pozostaje dla dostawcy usług istotną i odpowiednią.

Wskazówki ogólne (General guidance)

5.3.7. W każdej organizacji kierownictwo zarządza pracą personelu i wykorzystaniem zasobów dla dostarczenia produktu lub usługi. Narażenie organizacji na zagrożenia bezpieczeństwa są konsekwencją pracy. Kierownictwo łagodzi związane z nimi ryzyko dotyczące bezpieczeństwa, poprzez:

a) określenie dla organizacji priorytetów i zadań;

b) przygotowanie procedur jak wykonywać działania i procesy;

c) zatrudnienie, szkolenie i nadzorowanie pracowników;

d) pozyskiwanie sprzętu wspierającego działania związane ze świadczeniem usług;

e) wykorzystywanie umiejętności własnego personelu; oraz

f) przydzielanie potrzebnych zasobów.

5.3.8. Kierownictwo powinno zapewnić, by:

a) dyrektywy bezpieczeństwa i środki kontrolne były zawarte w standardowych procedurach operacyjnych (SOP);

b) pracownicy ściśle przestrzegali standardowych procedur operacyjnych (SOP) i dyrektyw bezpieczeństwa; oraz

c) sprzęt pozostawał w stanie gotowym do użytku

5.3.9. Pierwszą odpowiedzialnością kierownictwa jest zapewnienie, by bezpieczna i skuteczna operacja była wykonywana poprzez ścisłe przestrzeganie programów SOP (przestrzeganie bezpieczeństwa) i utworzenie oraz utrzymywanie dedykowanego SMS, który ustanawia niezbędne środki kontrolowania ryzykiem dotyczącego bezpieczeństwa (działanie bezpieczeństwa).

Strategia wdrażania (Implementation strategy)

5.3.10. Naczelne kierownictwo opracowuje i wdroży politykę bezpieczeństwa, którą podpisuje Dyrektor Odpowiedzialny. (W sprawie dyskusji na temat elektronicznego podpisania polityki bezpieczeństwa i innych dokumentów powiązanych z SMS, zajrzyj do Dodatku 1.) Przykład oświadczenia dotyczącego polityki bezpieczeństwa jest na Rys. 5-1.

5.3.11. Kiedy już polityka bezpieczeństwa zostanie opracowana, naczelne kierownictwo powinno:

a) podpisać tę politykę w sposób widoczny;

b) zakomunikować tę politykę wszystkim pracownikom, których dotyczy;

c) określić docelowe poziomy bezpieczeństwa dla SMS i organizacji; oraz

d) określić założenia bezpieczeństwa, które identyfikują, co organizacja chce osiągnąć w rozumieniu zarządzania bezpieczeństwem.

5.3.12. Polityka bezpieczeństwa musi obejmować zaangażowanie się w:

a) osiąganie najwyższych standardów bezpieczeństwa;

b) przestrzeganie zgodności ze wszystkimi odpowiednimi wymogami prawnymi.

c) przestrzeganie standardów międzynarodowych;

d) przyjmowanie sprawdzonych, najlepszych praktyk, odpowiednich dla danego działania;

e) dostarczanie wszelkich potrzebnych zasobów;

f) dopilnowanie, by bezpieczeństwo było pierwszą odpowiedzialnością wszystkich kierowników;

g) działanie zgodne z polityką dyscyplinarną; oraz

h) dopilnowanie, by polityka bezpieczeństwa była rozumiana, wdrażana i utrzymywana na wszystkich poziomach.

5.3.13. Standardy bezpieczeństwa są wskaźnikiem zachowań organizacji a także miarą działania SMS. Ponadto, cele bezpieczeństwa i standardy działania bezpieczeństwa muszą być powiązane z:

a) wskaźnikami działania bezpieczeństwa;

b) celami działania bezpieczeństwa; oraz

c) działaniami SMS na rzecz łagodzenia.

OŚWIADCZENIE DOTYCZĄCE POLITYKI BEZPIECZEŃSTWA

Bezpieczeństwo jest jedną z naszych najbardziej istotnych funkcji biznesowych. Świadcząc usługi, jesteśmy oddani opracowywaniu, wdrażaniu, utrzymywaniu i ciągłemu ulepszaniu strategii i procesów, dla zapewnienia by wszystkie nasze działania lotnicze odbywały się w warunkach przydzielenia organizacji odpowiednich zasobów i były nastawione na osiąganie najwyższego poziomu działania bezpieczeństwa oraz spełniania wymogów prawnych.
Kierownictwo, na wszystkich poziomach, i wszyscy pracownicy są personalnie odpowiedzialni za uzyskanie najwyższego poziomu działania bezpieczeństwa, poczynając od Dyrektora Naczelnego (CEO).

Nasze zaangażowanie ma na celu:

- *wspomagać* (*support)* zarządzanie bezpieczeństwem poprzez dostarczanie wszystkich odpowiednich zasobów, które będą w organizacji skutkować kulturą, bo ona rozwija praktyki bezpieczeństwa, zachęca do skutecznego raportowania o bezpieczeństwie i do komunikacji, oraz aktywnie zarządza bezpieczeństwem, przywiązując taką samą uwagę do jego rezultatów jak do rezultatów innych systemów zarządzania bezpieczeństwem w organizacji;

- *dopilnowywać (ensure),* by zarządzanie bezpieczeństwem było priorytetem pośród obowiązków wszystkich kierowników i pracowników;

- *jasno zdefiniować* (*clearly define)* całemu personelowi, tak kierownikom jak i pracownikom, zakresy ich odpowiedzialności oraz odpowiedzialności personalne za realizowanie osiągów bezpieczeństwa organizacji, także za działanie systemu zarządzania bezpieczeństwem;

- *ustanowić i eksploatować* (*establish and operate)* procesy identyfikacji zagrożeń oraz zarządzania ryzykiem, w tym, systemem raportowania zagrożeń, w celu eliminacji lub łagodzenia ryzyka dotyczącego bezpieczeństwa, będące konsekwencjami zagrożeń wynikających z naszych operacji i działań; by osiągać stałą poprawę w naszym działaniu na rzecz bezpieczeństwa;

- *dopilnować (ensure),* by żadne działanie nie było podjęte przeciw któremukolwiek pracownikowi, który ujawni poprzez system raportowania zagrożeń jakieś zagrożenie lub wykaże troskę o bezpieczeństwo, o ile ujawnienie nie wskazuje, poza wszelką rozsądną wątpliwość, na rażące niedbalstwo lub na umyślne zaniedbanie dotyczące przepisów lub procedur;

- *przestrzegać* (*comply)*, a gdziekolwiek możliwe, przekraczać wymogi przepisów, prawodawstwa i standardów;

- *dopilnowywać (ensure),* by dostępne były zasoby wystarczająco wykwalifikowanej i przeszkolonej siły roboczej, potrzebnej do wdrażania strategii i procesów bezpieczeństwa;

- *dopilnowywać (ensure),* by cały personel otrzymywał adekwatne i właściwe informacje dotyczące bezpieczeństwa w lotnictwie, także przeszkolenie, był kompetentny w sprawach bezpieczeństwa i żeby mu przydzielano tylko takie zadania, które są współmierne z jego umiejętnościami;

- *ustanowić poziomy i mierzyć* (*establish and measure)* działanie bezpieczeństwa względem realistycznych wskaźników działania bezpieczeństwa i działania celów w sferze bezpieczeństwa;

- *stale ulepszać* (*continually improve)* działanie bezpieczeństwa poprzez jego nieustanne monitorowanie i mierzenie, poprzez regularne przeglądy i dostosowywanie średnioodległych i bliskich celów bezpieczeństwa oraz ich konsekwentne osiąganie; oraz

- dopilnowywać *(ensure),* by systemy i usługi, dostarczane z zewnątrz dla wsparcia operacji, były dostarczane w stanie spełniającym minimalne standardy bezpieczeństwa.

Podpisał)

_____

CEO/Dyrektor Zarządzający

Rys. 5-1. Przykład oświadczenia dotyczącego polityki bezpieczeństwa

5.3.14. Polityka dyscyplinarna jest używana do ustalenia czy doszło do pogwałcenia wymagającego działania, wykraczającego poza wymogi analizy systemów zarządzania ryzykiem. Dlatego jest tak istotne, by dopilnowywać, aby osoby odpowiedzialne za dokonywanie ustaleń miały konieczną, techniczną wiedzę ekspercką, by móc w pełni uwzględniać kontekst dotyczący raportu, zatem zmniejszać prawdopodobieństwo, że taki personel i sam dostawca usługi będą mogli być narażeni na nieuczciwe lub niewłaściwe postępowanie dyscyplinarne. Jednym z podejść do zastosowania przez kierowników pierwszej linii w decydowaniu o osobistej odpowiedzialności osoby/osób uwikłanych w incydent jest algorytm Jamesa Reasona dla aktów niebezpiecznych. Innym źródłem w tym względzie jest książka Sidney'a Dekkera, zatytułowana *Just Culture: Balancing Safety and Accountability (Po prostu kultura, wyważenie bezpieczeństwa i odpowiedzialności personalnej)*.

5.3.15. Polityka odpowiedniego chronienia danych o bezpieczeństwie, jak również osób je raportujących, może mieć znaczny, dodatni wpływ na kulturę raportowania. Gdy już będzie jasne, że raport nie zawiera pogwałcenia, dostawca usług i państwo powinni dopuścić do odpersonalizowania i scalenia raportów po to, by przeprowadzić dogłębną analizę bez uderzania w personel ani w dostarczycieli konkretnych usług. Ponieważ większe wydarzenia mogą przywoływać pamięć o procesach i procedurach spoza SMS dostawcy usług, odpowiedni organ Państwa może nie pozwolić na wczesne odpersonalizowane raportów we wszystkich okolicznościach. Mimo to, polityka dopuszczająca odpowiednie odpersonalizowanie raportów może bardzo znacznie polepszyć jakość gromadzonych danych.

Element 1.2 SMS
Odpowiedzialność personalna za bezpieczeństwo

Dostawca usług musi:

a) ustalić tożsamość dyrektora osobiście odpowiedzialnego, który niezależnie od innych funkcji, ma – w imieniu organizacji – wpisaną w zakres obowiązków ostateczną odpowiedzialność, także finansową, za wdrożenie i utrzymywanie SMS;

b) jasno zdefiniować granice personalnej odpowiedzialności za bezpieczeństwo całej organizacji, w tym – ze strony naczelnego kierownictwa – bezpośrednią odpowiedzialność za bezpieczeństwo;

c) rozpoznać odpowiedzialność personalną wszystkich członków kierownictwa, niezależnie od innych funkcji, również pracowników, za działanie na rzecz bezpieczeństwa systemu SMS;

d) udokumentować i zakomunikować całej organizacji jakie są obowiązki i odpowiedzialność personalna dotycząca bezpieczeństwa, oraz uprawnienia; oraz

e) zdefiniować poziomy zarządzania i uprawnienia do podejmowania decyzji dotyczące tolerowania ryzyka w sferze bezpieczeństwa.

Wskazówki ogólne (General guidance)

5.3.16. W kontekście SMS, odpowiedzialność personalna oznacza ostateczną odpowiedzialność za działanie na rzecz bezpieczeństwa czy to na ogólnym poziomie SMS (Dyrektor Odpowiedzialny) czy za poziomy konkretnych produktów/procesów (członkowie zespołu kierowniczego). Odpowiedzialność oznacza bycie odpowiedzialnym za to, by podejmowane były stosowne działania korekcyjne wobec zgłaszanych zagrożeń i błędów, jak również za reagowanie na wypadki i incydenty.

5.3.17. Historycznie, w większości organizacji, całym procesem bezpieczeństwa zarządzało biuro bezpieczeństwa. Urzędnikiem ds. bezpieczeństwa była osoba z kompetencjami identyfikowania bieżących spraw bezpieczeństwa, proponowania rozwiązań, brania udziału we wdrażaniu tych rozwiązań, oraz monitorowania skuteczności tych rozwiązań. Taka praktyka lokowała władztwo nad procesem bezpieczeństwa całkowicie w biurze bezpieczeństwa, usuwając w ten sposób dyrektorów wykonawczych i kierowników liniowych z procesu decyzyjnego w sprawach bezpieczeństwa. Przez to zagadnienia bezpieczeństwa przestały być postrzegane jako odpowiedzialność kierownika liniowego; problemy bezpieczeństwa zaczęły być uważane za odpowiedzialność biura bezpieczeństwa i urzędnika ds. bezpieczeństwa. Dodatkowo, takie podejście zaniedbało cenny wkład jednostek produkcyjnych i operacyjnych, jaki mogą wnosić do procesu decyzyjnego w organizacji, w sprawach bezpieczeństwa.

5.3.18. Poprzez wymóg, by dostawca usług był tożsamy z dyrektorem odpowiedzialnym, odpowiedzialność za całokształt działania bezpieczeństwa zostaje położona w organizacji na poziom, który jest odpowiedni, by podejmować działania zapewniające skuteczność SMS. To jak definiować zakresy personalnej odpowiedzialności za bezpieczeństwo wszystkim członkom zespołu kierowniczego wewnątrz organizacji, objaśnia rama odpowiedzialności. Ramy odpowiedzialności muszą też obejmować personalną odpowiedzialność za działanie bezpieczeństwa u dostawców usług-dostarczycieli podproduktu lub u poddostawców usług, wobec których nie ma wymogu posiadania osobnego certyfikatu ani zatwierdzenia. Aby podejmować decyzje dotyczące zarządzania ryzykiem, muszą być określone zakresy obowiązków, uprawnienia i odpowiedzialność osób za bezpieczeństwo na każdym poziomie zarządzania w organizacji, oraz muszą być one dokumentowane i znane w całej organizacji. Dodatkowo, do odpowiedzialności personalnej kierowników powinno należeć przydzielanie zasobów ludzkich, technicznych, finansowych lub innych potrzebnych dla skutecznego i wydajnego działania SMS.

Uwaga.— W kontekście SMM, termin — „accountabilities" może być postrzegany jako odpowiedzialności, których nie należy przekazywać innym osobom.

Strategia wdrożeniowa (Implementation strategy)

5.3.19. Zarządzanie bezpieczeństwem powinno być dla każdego dostawcy usług lotniczych funkcją kluczową. Rozpisanie odpowiedzialności personalnych dla każdego pracownika, który ma do czynienia z bezpieczeństwem będzie służyć dostarczaniu bezpiecznych produktów i operacji, również właściwie zbalansowanej alokacji zasobów.

5.3.20. Wskazany przez dostawcę usług dyrektor odpowiedzialny jest osobą o jednoosobowej, ostatecznej odpowiedzialności za SMS, w tym, odpowiedzialną za dostarczanie zasobów istotnych dla wdrożenia i utrzymywania SMS. Obowiązki i personalne odpowiedzialności dyrektora odpowiedzialnego obejmują, ale nie ograniczają się do:

a) zapewniania i przydzielania ludzkich, technicznych, finansowych lub innych zasobów potrzebnych do skutecznego i wydajnego działania SMS;

b) bezpośredniej odpowiedzialności za prowadzenie spraw organizacji;

c) posiadania ostatecznej władzy nad operacjami wykonywanymi na mocy posiadanego przez organizację certyfikatu/zatwierdzenia;

d) ustanowienia i promowania polityki bezpieczeństwa;

e) ustanowienie celów bezpieczeństwa organizacji i celów w zakresie bezpieczeństwa;

f) bycia najlepszym w działaniach jakie organizacja wykonuje na rzecz bezpieczeństwa;

g) ponoszenia ostatecznej odpowiedzialności za rozwiązywanie wszystkich bieżących zagadnień związanych z bezpieczeństwem; oraz

h) ustanowienia i utrzymywania kompetencji organizacji do pobierania nauki z analizy danych zgromadzonych poprzez swój system raportowania o bezpieczeństwie.

Uwaga.— Zarysowanych powyżej odpowiedzialności nie należy przekazywać innej osobie.

5.3.21. Zależnie od wielkości, struktury i złożoności organizacji, dyrektorem odpowiedzialnym może być:

a) Dyrektor Naczelny organizacji dostawcy usług;

b) prezes zarządu;

c) wspólnik, lub

d) właściciel.

5.3.22. Dodatkowo, powołanie na funkcję dyrektora odpowiedzialnego kogoś komu daje się wymagane uprawnienia, wymagane jest by taka osoba posiadała atrybuty wymagane do spełniania tej roli. Dyrektor odpowiedzialny będzie mieć w organizacji wiele funkcji. Mimo to, rolą dyrektora odpowiedzialnego jest wzbudzać przekonanie, że kluczową wartością organizacji jest bezpieczeństwo oraz dopilnowywać, by SMS był właściwie wdrożony i utrzymywany, poprzez przydzielanie zasobów i zadań.

5.3.23. Wszystkie związane z lotnictwem stanowiska, zakres odpowiedzialności i władzy powinny być zdefiniowane, udokumentowane i zakomunikowane całej organizacji. Zakres odpowiedzialności każdego kierownika wyższej rangi (szef wydziału lub osoba odpowiedzialna za jednostkę organizacyjną wykonującą jakąś funkcję) są integralnymi komponentami ich zakresu obowiązków. Przy założeniu, że kluczową funkcją biznesu jest zarządzanie bezpieczeństwem, każdy wyższy kierownik posiada w jakimś stopniu udział w działaniu SMS. Takie zaangażowanie się jest z pewnością większe u tych kierowników, którzy są bezpośrednio odpowiedzialni za funkcyjne jednostki organizacyjne, które dostarczają organizacji produkty lub usługi (operacje, produkcja, obsługa techniczna, prace inżynierskie, szkolenie oraz odprawa [pasażerów i frachtu], i którzy od tej pory będą objęci terminem „line managers" (kierownicy liniowi) niż u tych, którzy są odpowiedzialni za funkcje pomocnicze (zasoby ludzkie, administracja, komórka prawna i finansowa).

5.3.24. Dostawca usług jest odpowiedzialny za bezpieczne działanie produktów lub usług swych podwykonawców usług, którzy osobno nie potrzebują certyfikacji ani zatwierdzenia. Choć nie od wszystkich podwykonawców usług będzie się koniecznie wymagać posiadanie własnego SMS, to jednak dostawca usług będzie odpowiadał za dopilnowanie, by spełniane były przez podwykonawców usług jego własne wymagania dotyczące bezpieczeństwa. W każdym razie, jest sprawą zasadniczą, by SMS dostawcy usług współpracował z systemami bezpieczeństwa podwykonawców usług, którzy dostarczają produkty i usługi przynależne bezpiecznemu operowaniu samolotu, tak płynnie, jak tylko to możliwe. Łącze między SMS organizacji a systemami bezpieczeństwa dostawców podproduktów lub podusług musi obsługiwać identyfikowanie zagrożeń, zarządzania ryzykiem oraz strategie łagodzenia go, tam gdzie możliwe. Dostawca usług powinien zadbać o to, by:

a) istniała polityka jasno ustanawiająca odpowiedzialność za bezpieczeństwo i przepływ odpowiedzialności między dostawcą usług a podwykonawcą usług;

b) podwykonawca usług posiadał, współmierny do swej wielkości i złożoności, system raportowania, który ułatwia wczesne rozpoznawanie zagrożeń i awarii systemów będących przedmiotem troski dostawcy usług;

c) w skład rady/zespołu dostawcy usług ds. przeglądania bezpieczeństwa wchodził, gdzie tylko możliwe, przedstawiciel podwykonawcy usług;

d) opracowane były, gdzie tylko możliwe, wskaźniki bezpieczeństwa/jakości do monitorowania działania podwykonawcy usług;

e) posiadany przez dostawcę usług proces promowania bezpieczeństwa zapewniał pracownikom podwykonawcy usług otrzymywanie jego odpowiednich komunikatów dotyczących bezpieczeństwa; oraz

f) w odpowiedzi na plan awaryjny dostawcy usług, zostały opracowane i przetestowane wszelkie role, zakres odpowiedzialności personalnej oraz zakres obowiązków dostawcy usług.

5.3.25. Związane z SMS zakres odpowiedzialności personalnej, zakresy odpowiedzialności oraz uprawnienia wszystkich wyższych kierowników muszą być opisane w dokumentacji SMS organizacji. Obowiązkowe funkcje dotyczące bezpieczeństwa, wykonywane przez kierownika bezpieczeństwa, biuro bezpieczeństwa, grupy działań w sferze bezpieczeństwa (safety action groups) itp., mogą być wpisane na stałe do istniejących zakresów obowiązków, do procesów i procedur.

5.3.26. Funkcja kierownika bezpieczeństwa jest opisana szczegółowo w następnym paragrafie. Z perspektywy odpowiedzialności personalnej, osoba wykonująca funkcję kierownika bezpieczeństwa odpowiada przed dyrektorem odpowiedzialnym za działanie SMS i za świadczenie usług dotyczących bezpieczeństwa pozostałym działom organizacji.

Element 1.3 SMS.
Mianowanie personelu kluczowego dla spraw bezpieczeństwa

Dostawca usługi musi ustanowić kierownika bezpieczeństwa, który będzie odpowiadać za wdrożenie i utrzymywanie skutecznego funkcjonowania SMS.

Wskazówki ogólne (General guidance)

5.3.27. Kluczowe dla skutecznego wdrożenia i funkcjonowania biura usług dotyczącego bezpieczeństwa jest ustanowienie wykwalifikowanego kierownika bezpieczeństwa. Stanowisko kierownika bezpieczeństwa może mieć różne nazwy w różnych organizacjach, ale dla potrzeb tego podręcznika stosowana jest nazwa rodzajowa, tj. kierownik bezpieczeństwa „safety manager".

Strategia wdrażania (Implementation strategy)

5.3.28. W większości organizacji, kierownik bezpieczeństwa jest osobą odpowiedzialną za opracowanie i utrzymywanie skutecznego SMS. Kierownik bezpieczeństwa również doradza dyrektorowi odpowiedzialnemu i kierownikom liniowym w sprawach zarządzania bezpieczeństwem, oraz jest odpowiedzialny za koordynowanie i komunikowanie aktualnych spraw wewnątrz organizacji, jak również zainteresowanym, zewnętrznym podmiotom. Obowiązki kierownika bezpieczeństwa obejmują, ale niekoniecznie ograniczają się do:

a) zarządzania planem wdrażania SMS w imieniu dyrektora odpowiedzialnego;

b) wykonywania/ułatwiania identyfikowania zagrożeń i proces zarządzania ryzykiem;

c) monitorowania działań korekcyjnych i oceniania ich rezultatów;

d) dostarczania okresowych raportów dotyczących działania bezpieczeństwa w organizacji;

e) przechowywania zapisów i dokumentacji dotyczących bezpieczeństwa;

f) planowania i ułatwiania szkolenia personelu w zakresie bezpieczeństwa;

g) udzielania niezależnych rad dotyczących spraw bezpieczeństwa;

h) monitorowania trosk dotyczących bezpieczeństwa w przemyśle lotniczym i tego jak postrzegany jest ich wpływ na te operacje organizacji, które nastawione są na świadczenie usług;

i) koordynowania i komunikowania aktualnych spraw dotyczących bezpieczeństwa (w imieniu dyrektora odpowiedzialnego) i pod nadzorem krajowego organu ds. nadzorowania a także innych, jeśli potrzeba, organów krajowych;

j) koordynowania i komunikowania (w imieniu dyrektora odpowiedzialnego) międzynarodowym organizacjom aktualnych spraw dotyczących bezpieczeństwa.

5.3.29. Kryteria selekcji na kierownika bezpieczeństwa powinny obejmować, ale niekoniecznie być ograniczone do poniższych:

a) doświadczenia w zarządzaniu bezpieczeństwem/jakością;

b) doświadczenia operacyjnego;

c) posiadania podstaw technicznych by rozumieć systemy, które wspierają realizację operacji lotniczych;

d) umiejętności interpersonalnych;

e) umiejętności analitycznych i umiejętności rozwiązywania problemów;

f) umiejętności zarządzania projektami; oraz

g) umiejętności ustnego i pisemnego przekazu.

Uwaga.— Próbka opisu pracy kierownika bezpieczeństwa jest zawarta w Dodatku 2 do tego rozdziału. W małych organizacjach, łączenie funkcji dotyczących bezpieczeństwa i jakości w obrębie jednego biura może być wykonalne.

5.3.30. Kierownik bezpieczeństwa jest na ogół wspierany przydzieleniem dodatkowego personelu. To będzie zależeć od wielkości, charakteru i złożoności organizacji. Kierownik bezpieczeństwa kontaktuje się bezpośrednio z kierownikami liniowymi, lub z ich kompetencyjnymi przedstawicielami, takimi gdzie wydziały operacyjne są wspierane przez dedykowanych oficerów bezpieczeństwa.

5.3.31. Kierownik bezpieczeństwa jest osobą odpowiedzialną za gromadzenie i analizowanie danych dotyczących bezpieczeństwa oraz dystrybucję informacji związanych z bezpieczeństwem, pośród kierowników liniowych. Takie rozsyłanie informacji o bezpieczeństwie przez biuro usług ds. bezpieczeństwa jest pierwszym krokiem w procesie zarządzania ryzykiem dotyczącym bezpieczeństwa. Te informacje muszą być wykorzystywane przez kierowników liniowych do łagodzenia ryzyka, co nieuchronnie wymaga odpowiedniej alokacji zasobów. Niezbędne zasoby mogą być w czytelny sposób udostępniane kierownikom dla realizacji takiego celu.

5.3.32. Ponadto, aby ocenić skuteczność i wydajności strategii łagodzących, stosowanych do osiągania uzgodnionych celów działania bezpieczeństwa w organizacji, potrzebny jest proces formalny. Jeden potencjalny proces obejmuje utworzenie komisji/zespołu przeglądu bezpieczeństwa (SRC). SRC zapewnia platformę pozwalającą na osiągnięcie założeń wynikających z przydzielenia środków oraz ocenę skuteczności i sprawności strategii łagodzenia ryzyka. SRC jest komisją/zespołem wysokiego szczebla, której przewodniczącym jest Dyrektor Odpowiedzialny, a w skład wchodzą kierownicy wyższego szczebla, włącznie z kierownikami liniowymi, odpowiedzialnymi za obszary funkcjonalne oraz z departamentów administracyjnych. Kierownik bezpieczeństwa uczestniczy w SRC tylko w zakresie doradczym. SRC nie spotyka się często, chyba że wyjątkowe okoliczności spowodują inaczej. Komisja/zespół SRC:

a) monitoruje skuteczność SMS;

b) monitoruje podjęcie niezbędnych działań naprawczych bez zbędnej zwłoki;

c) monitoruje działanie bezpieczeństwa w organizacji względem jego polityki bezpieczeństwa i celów;

d) jako jeszcze jeden zasadniczy proces biznesowy, komisja/zespół monitoruje skuteczność tych procesów zarządzania bezpieczeństwem w organizacji, które wspierają deklarowany priorytet korporacyjny jakim jest zarządzanie bezpieczeństwem;

e) monitoruje skuteczność nadzorowania bezpieczeństwa w operacjach zleconych podwykonawcom; oraz

f) dopilnowuje by przydzielane były stosowne zasoby, potrzebne dla osiągania bezpieczeństwa lepszego niż w przypadku, gdy tylko przestrzega się przepisów.

5.3.33. SRC ma znaczenie strategiczne i zajmuje się aktualnymi sprawami wysokiej rangi w sferze koncepcji politycznych organizacji, przydzielania zasobów i monitorowania działania organizacji. Gdy zostanie przez SRC opracowany kierunek strategiczny, wdrażanie strategii dotyczącej bezpieczeństwa będzie musiało być koordynowane w całej organizacji. Można tego dokonać przez powołanie grupy ds. działań na rzecz bezpieczeństwa {a safety action group (SAG)}. Grupy SAG komponuje się z kierowników liniowych i personelu pierwszej linii; normalnie, przewodniczy im wskazany kierownik liniowy. SAG są podmiotami taktycznymi, które zajmują się konkretnymi, bieżącymi sprawami wdrażania pod kierunkiem SRC. Grupa SAG:

a) nadzoruje działanie bezpieczeństwa operacyjnego w obszarach funkcjonalnych organizacji oraz dopilnowuje, by prowadzone były stosowne działania zarządzania ryzykiem dotyczącym bezpieczeństwa, przy zaangażowaniu się personelu, co jest konieczne dla budowania świadomości bezpieczeństwa;

b) koordynuje postanowienie dotyczące strategii łagodzenia rozpoznanych skutków zagrożeń oraz dopilnowuje, by istniały satysfakcjonujące rozwiązania służące wychwytywaniu danych o bezpieczeństwie, a także informacji zwrotnych od pracowników;

c) ocenia oddziaływanie bezpieczeństwa związanego z wprowadzaniem zmian operacyjnych bądź nowych technologii;

d) koordynuje wdrażanie planów działań korekcyjnych i dopilnowuje, by działanie korekcyjne było podjęte na czas;

e) przegląda skuteczność poprzednich zaleceń dotyczących bezpieczeństwa; oraz

f) nadzoruje działania promocyjne jako niezbędne dla zwiększania pracowniczej świadomości spraw bezpieczeństwa oraz zapewnienia, by pracownicy posiadali stosowne okazje do uczestniczenia w działaniach dotyczących zarządzaniem bezpieczeństwem.

Element 1.4 programu SMM
Koordynowanie planowania reagowania awaryjnego

Dostawca usług musi dopilnować, by plan reagowania awaryjnego był właściwie skoordynowany z planami reagowania awaryjnego tych organizacji, z którymi będzie musiał się kontaktować podczas świadczenia swych usług.

Strategia wdrażania (Implementation strategy)

5.3.34. Plan reagowania awaryjnego (ERP) dokumentuje akcje jakie mają być podjęte przez cały odpowiedzialny personel podczas sytuacji awaryjnej związanej z lotnictwem. Celem ERP jest dopilnowanie, by istniało uporządkowane i skuteczne przejście od operacji normalnych do operacji awaryjnych, obejmujące przydzielenie odpowiedzialności awaryjnych i przekazanie władzy. Jest w tym planie zawarte również udzielenie kluczowemu personelowi upoważnień do działania, jak też są w nim środki na koordynowanie wysiłków niezbędnych do poradzenia sobie z sytuacją awaryjną. Celem ogólnym jest ratowanie życia, bezpieczna kontynuacja operacji oraz powrót do operacji normalnych, możliwie w jak najkrótszym czasie.

5.3.35. Zastosowanie planowania reagowania awaryjnego rozciąga się na dostawców usług produktów lotniczych, którym, w danym wydarzeniu lotniczym, można przypisać rolę sprawcy lub poszkodowanego. Procesy dostawcy produktu są ogólnie nazywane wsparciem produktu na wszelki wypadek (contingency product support) i obejmują akcję na rzecz zdatności do lotu w sytuacji awaryjnej, także usługi alarmowe, oraz zajęcie się samolotem w miejscu wypadku. Dostarczyciel produktu nie musi zmienić nazw tych procesów wsparcia produktu na procesy ERP; jednak, muszą one być odpowiednio zapisywane w dokumentacji jego SMS-a. Dalsze wskazówki odnośnie ERP, znajdują się w Dodatku nr 3.

Element 1.5 programu SMS
Dokumentacja SMS

1.5.1 Dostawca usług musi opracować plan wdrożenia SMS, formalnie wspierany przez organizację, który definiuje jego podejście do zarządzania bezpieczeństwem w sposób spełniający jego cele w sferze bezpieczeństwa.

1.5.2 Dostawca usług musi opracować i prowadzić dokumentację SMS, opisującą:

a) politykę bezpieczeństwa i jej cele;

b) wymogi SMS;

c) proces i procedury SMS;

d) odpowiedzialności personalne i zakresy obowiązków oraz pełnomocnictwa dotyczące procesów i procedur SMS; oraz

e) wyniki/dane wychodzące z SMS.

1.5.3 Dostawca usług musi opracować i utrzymywać podręcznik SMS jako część swej dokumentacji SMS.

Wskazówki ogólne (General guidance)

5.3.36. Dokumentacja SMS powinna zawierać - jako autoprezentację (exposition) na najwyższym poziomie - dokument-opis, który opisuje SMS dostawcy usług według zawartych w nim komponentów i elementów. Taki dokument ułatwia

organizacji wewnętrzne administrowanie, komunikowanie i utrzymywanie SMS. Jednocześnie, służy on za zgłoszenie (declaration) SMS organizacji do odnośnej krajowej władzy lotniczego CAA dla potrzeb zgodnego z przepisami zaakceptowania, oceniania i dalszego nadzorowania SMS przez CAA. Ten odgórny dokument programu SMS może być dokumentem samodzielnym lub osobnym akapitem/rozdziałem "SMS section/chapter" w dokumencie zatwierdzonym przez krajową CAA lub przez organizację. Tam gdzie detalami procesów SMS organizacji już się zajęto w dokumentach istniejących, wystarczy podać odnośniki do takich dokumentów. Dokument SMS trzeba będzie uaktualniać na bieżąco, a tam gdzie zamierza się wprowadzić/lub się wprowadziło znaczne zmiany, być może konieczne będą uzgodnienia z krajowym CAA. Wskazówki jak opracować dokument SMS znajdują się w Dodatku 4.

5.3.37. Innym aspektem dokumentu SMS jest scalanie i przechowywanie zapisów uzasadniających istnienie SMS i stałe jego działanie. Takie zapisy powinny być porządkowane wg odpowiednich elementów SMS i związanych z nimi procesów. Dla niektórych procesów może wystarczyć, by system dokumentacji SMS zawierał kopie lub próbki zapisów przechowywanych w innych systemach dokumentacji organizacji (jak dział dokumentacji technicznej i centralna biblioteka). W początkowej fazie wdrożeniowej, dokumentacja SMS może zawierać zapis analizy luk i plan wdrażania fazowego.

Strategia wdrażania (Implementation strategy)

5.3.38. Dokumentacja SMS obejmuje wszystkie elementy i procesy SMS, i normalnie zawiera:

a) skonsolidowany opis komponentów i elementów SMS, takich jak:

1) zarządzanie dokumentami i zapisami;

2) wymogi przepisów, które dotyczą SMS;

3) rama, zakres i integracja;

4) polityka bezpieczeństwa i jego cele;

5) odpowiedzialności personalne oraz kluczowy personel;

6) system dobrowolnego raportowania niebezpieczeństw;

7) procedury raportowania o incydentach i ich badania;

8) procesy rozpoznawania zagrożeń i procesy zarządzania ryzykiem;

9) wskaźniki działania bezpieczeństwa;

10) szkolenie w sferze bezpieczeństwa i komunikowania;

11) ciągłe usprawnianie i audyt SMS;

12) zarządzanie zmianami; oraz

13) planowanie na ewentualność zaistnienia sytuacji awaryjnych lub ewentualnych operacji;

b) kompilacja aktualnych zapisów i dokumentów dotyczących SMS, takich jak:

1) rejestr raportów z niebezpieczeństw i próbek rzeczywistych raportów;

2) wskaźniki działania bezpieczeństwa i wykresy ich dotyczące;

3) zapis przeprowadzonych i wykonywanych aktualnie ocen z bezpieczeństwa;

4) zapisy z wewnętrznego przeglądu SMS lub z audytu;

5) zapisy z promowania bezpieczeństwa;

6) zapisy ze szkolenia dotyczące SMS/bezpieczeństwa;

7) protokół z posiedzenia komisji/zespołu dotyczący SMS/ bezpieczeństwa; oraz

8) plan wdrażania SMS (podczas procesu wdrażania).

Komponent nr 2 programu SMS. Zarządzanie ryzykiem dotyczącym bezpieczeństwa

Wskazania ogólne (General guidance)

5.3.39. Po to by osiągać swe cele w sferze bezpieczeństwa, dostawcy usług powinni dopilnować, by napotykane w działaniach lotniczych ryzyka dotyczące bezpieczeństwa były pod kontrolą. Ten proces jest znany jako zarządzanie ryzykiem dotyczącym bezpieczeństwa i obejmuje identyfikowanie zagrożeń, ocenę ryzyka dotyczącego bezpieczeństwa oraz wdrażanie odpowiednich środków naprawczych. Proces zarządzania ryzykiem dotyczącym bezpieczeństwa jest zilustrowany na Rys. 5-2.

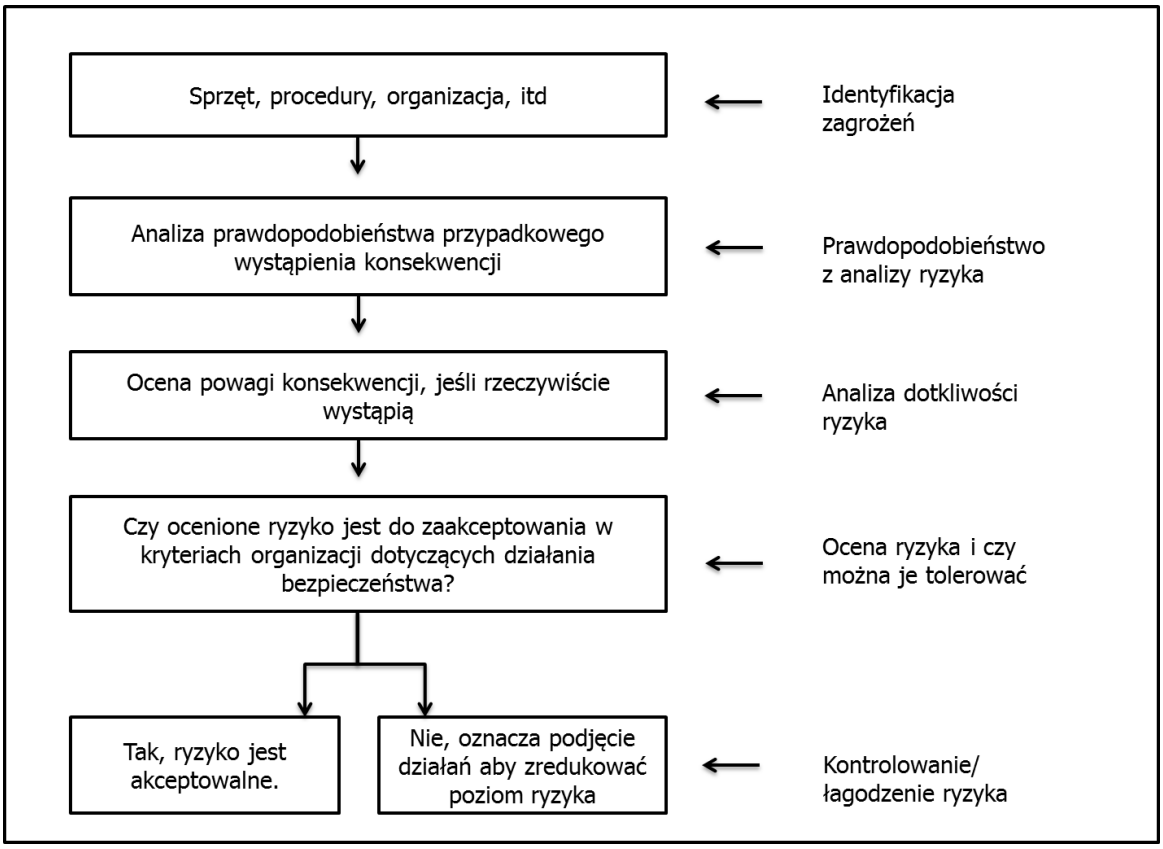
5.3.40. Komponent zarządzania ryzykiem systematycznie identyfikuje zagrożenia, które istnieją wewnątrz kontekstu dostarczania produktów lub usług. Zagrożenia mogą być rezultatem systemów, które mają niedostatki w swej konstrukcji, w funkcji technicznej, w kontaktach człowiek-człowiek lub we wzajemnych oddziaływaniach z innymi procesami i systemami. Mogą być one również rezultatem tego, że istniejące procesy lub systemy zawiodły i nie przystosowały się do zmian w operacyjnym środowisku dostawcy usług. Staranna analiza tych czynników podczas faz planowania, projektowania i wdrażania może często zidentyfikować potencjalne zagrożenia zanim system będzie oddany do użytku.

5.3.41. Zrozumienie systemu i jego środowisko pracy jest niezbędne dla osiągnięcia wysokiego poziomu bezpieczeństwa. Zagrożenia mogą być odkryte podczas cyklu operacyjnego, za pośrednictwem raportów pracowniczych lub incydentów. Analiza tych zagrożeń powinna być przeprowadzana w ramach systemu. Ten kontekst jest kluczowy dla unikania przypisywania winy za wydarzenia pomyłce człowieka („human error"), w których to, usterki systemu mogą być zlekceważone, mogą pozostać w uśpieniu aż do przyszłych i potencjalnie poważniejszych, przypadkowych wydarzeń. Wskazówkami dotyczącymi procedur identyfikowania zagrożeń i proces zarządzania ryzykiem oraz ich formatu zajmują się paragrafy od 5.3.42 do 5.3.61, jak również, odpowiednio Rozdziały 2, 2.14 i 2.15.

Element 2.1 systemu SMS.
Identyfikacja zagrożeń

2.1.1 Dostawca usług musi opracować i utrzymywać proces formalny, który zapewnia to, że: Identyfikowane są zagrożenia związane z produktami lub usługami lotniczymi.

2.1.2 Identyfikowanie zagrożeń musi opierać się na kombinacji aktywnej, proaktywnej i przewidywalnej metody gromadzenia danych o bezpieczeństwie.



Rys. 5-2. Proces zarządzania ryzykiem dotyczącym bezpieczeństwa

Wskazówki ogólne (General guidance)

5.3.42. Zarządzanie ryzykiem wymaga, by dostawca usług ustanowił i utrzymywał formalny proces identyfikowania zagrożeń, które mogą się przyczyniać do występowania zdarzeń mających związek z bezpieczeństwem. Zagrożenia mogą zaistnieć w ciągłych działaniach lotniczych bądź mogą być wprowadzone w operację nieumyślnie przy okazji dokonywania zmian w systemie lotniczym. W takim przypadku, zidentyfikowanie zagrożenia jest integralną częścią procesów zarządzania, jak opisano w Elemencie 3.2 programu SMS - Zarządzanie zmianą.

5.3.43. Identyfikowanie zagrożeń jest oparte na kombinacji metod, aktywnego, proaktywnego i przewidywalnego gromadzenia danych, jak omówiono w Rozdziale 2. Identyfikowanie zagrożeń jest pierwszym krokiem w procesie zarządzania ryzykiem dotyczącym bezpieczeństwa. Następnym - jest ocenienie odpowiednich ryzyk dotyczących bezpieczeństwa w kontekście potencjalnie niszczących konsekwencji danego zagrożenia. Gdy ryzyka dotyczące bezpieczeństwa zostaną ocenione jako nieakceptowalne, trzeba w system wbudować dodatkowe sposoby kontrolowania ryzykiem.

5.3.44. W dojrzałych systemach zarządzania bezpieczeństwem, identyfikowanie zagrożeń jest prowadzone w sposób ciągły i stanowi integralną część procesów organizacyjnych dostawcy usług. Pewna liczba warunków uruchamia dogłębne i dalekosiężne działania identyfikacji zagrożeń; mogą nimi być:

a) przypadki gdy organizacja doświadcza niewytłumaczalnego wzrostu liczby wydarzeń mających związek z lotnictwem lub z nieprzestrzeganiem przepisów;

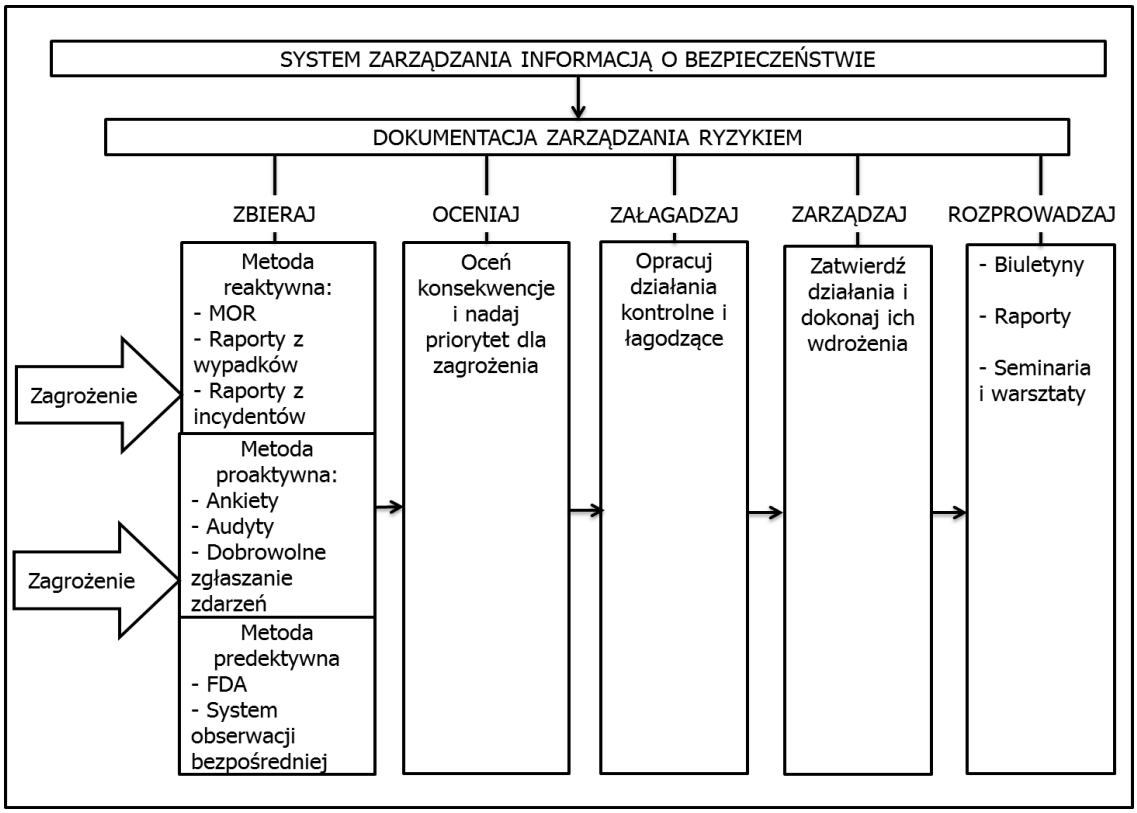
b) znaczne zmiany operacyjne, w tym spodziewane zmiany osobowe w kluczowym personelu, lub w innych głównych komponentach systemu; oraz

c) znaczące zmiany organizacyjne w organizacji, obejmujące spodziewany jego rozrost, kurczenie, łączenie się z/lub przejęcie innego/innych podmiotów.

5.3.45. Strukturalne podejście do identyfikacji zagrożeń może obejmować wykorzystywanie spotkań grup ekspertów (burze mózgów), podczas których eksperci od danego zagadnienia realizują scenariusze szczegółowej analizy. Takie sesje identyfikowania zagrożeń wymagają udziału pewnej liczby personelu z doświadczeniem operacyjnym i technicznym, a odbywają się pod kierunkiem organizatora (facilitator) posiedzenia. Tę samą grupę można także wykorzystać dla oceniania odpowiednich ryzykiem dotyczącym bezpieczeństwa.

5.3.46. Posiadany przez dostawcę usług system zarządzania informacjami o bezpieczeństwie powinien obejmować dokumentację z oceniania bezpieczeństwa, która zawiera opisy zagrożeń, spokrewnione konsekwencje, ocenione prawdopodobieństwo i dotkliwość ryzyka dotyczącego bezpieczeństwa, oraz powinien obejmować wymagane sposoby kontrolowania ryzykiem dotyczącego bezpieczeństwa. Istniejące oceny bezpieczeństwa należy przejrzeć za każdym razem, gdy zidentyfikowane zostaną ewentualne nowe zagrożenia i gdy zostaną przewidziane kolejne sposoby kontrolowania ryzykiem dotyczącego bezpieczeństwa.

5.3.47. Rysunek 5-3 ilustruje dokumentację zagrożeń oraz proces dalszego nimi zarządzania. Zagrożenia są rozpoznawane stale przez różne źródła danych. Od dostawcy usług oczekuje się, że będzie zagrożenia rozpoznawać i eliminować, bądź będzie łagodzić ryzyka, które są związane z tymi zagrożeniami. W przypadku zagrożeń zidentyfikowanych w produktach lub usługach dostarczonych poprzez poddostawców usług, łagodzenie może być wymogiem dostawcy usług wobec takich organizacji - by posiadały SMS lub równoważny proces służący identyfikowaniu zagrożeń i zarządzaniu ryzykiem.



Rys. 5-3. Dokumentacja zagrożeń i proces dalszego zarządzania ryzykiem

5.3.48. System zarządzania informacjami o bezpieczeństwie staje się źródłem wiedzy o bezpieczeństwie i ma być używany jako odniesienie dla procesów decyzyjnych organizacji. Takiej wiedzy o bezpieczeństwie dostarcza materiał dla analiz trendów w bezpieczeństwie jak również edukacja na rzecz bezpieczeństwa. Wskazówki dotyczące systemów dobrowolnego i poufnego raportowania zagrożeń są podane w Dodatku 5.

Strategia wdrażania (Implementation strategy)

5.3.49. Oto co można rozważać, gdy jest się zaangażowanym w proces identyfikowania zagrożeń:

a) czynniki projektowania, w tym sprzętu oraz projektowania zadaniowe;

b) ograniczenia ludzkiego działania (np. fizjologiczne, psychiczne i poznawcze);

c) procedury i praktyki operacyjne, w tym ich dokumentacje i listy kontrolne oraz ich uaktualnianie w istniejących warunkach operacyjnych;

d) czynniki komunikowania, w tym media, terminologia i język;

e) czynniki organizacyjne, takie jak, te które dotyczą rekrutacji, szkolenia i zatrzymywania personelu, zgodności produkcji z celami bezpieczeństwa, alokacji zasobów, nacisków w sferze operacyjnej oraz korporacyjnej kultury bezpieczeństwa;

f) czynniki związane ze środowiskiem operacyjnym systemu lotniczego (np. hałas otoczenia i wibracja, temperatura, oświetlenie i dostępność ochronnego sprzętu i odzieży);

g) czynniki nadzorowania przepisów, w tym stosowanie i egzekwowanie przepisów, oraz certyfikacja sprzętu, personelu i procedur;

h) systemy monitorowania działania, które mogą wykrywać dryf jaki występuje w praktyce oraz odstępstwa w operacjach; oraz

i) czynniki styku człowiek-maszyna.

5.3.50. Zagrożenia można rozpoznawać metodą proaktywną oraz przewidywalną, lub po wynikach badań wypadków bądź incydentów. Organizacja może skorzystać z istniejącej różnorodności wewnętrznych i zewnętrznych źródeł danych z identyfikacji zagrożeń. Przykłady wewnętrznych źródeł danych z identyfikacji zagrożeń obejmują:

a) schematy monitorowania normalnych operacji (np. analiza danych lotu dla operatorów samolotów);

b) systemy raportowania dobrowolnego i obowiązkowego;

c) pomiary bezpieczeństwa;

d) audyty bezpieczeństwa;

e) informacje zwrotne ze szkolenia; oraz

f) raporty z badań oraz ich ciąg dalszy po wypadkach/incydentach.

5.3.51. Przykłady wewnętrznych źródeł danych z identyfikacji zagrożeń obejmują:

a) raporty z badania wypadków w przemyśle;

b) krajowe systemy obowiązkowego raportowania incydentów;

c) krajowe systemy dobrowolnego raportowania incydentów;

d) krajowe audyty z nadzorowania; oraz

e) systemy wymieniania się informacjami.

5.3.52. Typ technologii stosowanej w procesie identyfikowania zagrożenia będzie zależeć od wielkości i złożoności dostawcy usług i jego działań lotniczych. We wszystkich przypadkach, posiadany przez dostawcę usług proces identyfikowania zagrożeń jest przejrzyście opisany w dokumentacji jego SMS lub w dokumentacji dotyczącej bezpieczeństwa. Proces identyfikowania zagrożeń uwzględnia wszystkie możliwe zagrożenia jakie mogą zaistnieć w zasięgu wewnętrznych działań lotniczych dostawcy usług, jak i w działaniach zewnętrznych, w tym w interfejsach z innymi systemami. Należy zaraz po zidentyfikowaniu zagrożeń ustalić jakie są ich konsekwencje, tj. wszelkie konkretne wydarzenia i to co z nich wynika (outcomes). Wskazówki dotyczące systemu poufnego raportowania dobrowolnego i obowiązkowego w organizacji, znajdują się w Dodatku 5.

Element 2.2 systemu SMS.
Ocena ryzyka dot. bezpieczeństwa i jego łagodzenie

Dostawca usług musi ustanowić i prowadzić proces, który zapewnia analizę, ocenę i kontrolę tych rodzajów ryzyka dotyczących bezpieczeństwa, które są związane z zagrożeniami zidentyfikowanymi.

Wskazania ogólne (General guidance)

5.3.53. Rys. 5-4 prezentuje proces zarządzania ryzykiem dotyczącym bezpieczeństwa w całej jego pełni. Proces zaczyna się identyfikowaniem zagrożeń i ich potencjalnych konsekwencji. Następnie, dla zdefiniowania wskaźników ryzyka dotyczącego bezpieczeństwa (safety risk index), trzeba je oszacować na prawdopodobieństwo i dotkliwość. Jeżeli oszacowanie ryzyka dotyczącego bezpieczeństwa uzna się za dające się tolerować, trzeba podjąć stosowaną akcję, a operacja będzie przebiegać dalej. Zakończony proces identyfikowania zagrożeń, proces zarządzania ryzykiem i proces łagodzenia ryzyka trzeba udokumentować, zatwierdzić jako właściwy i wtedy będzie stanowić część systemu zarządzania informacjami dotyczącymi bezpieczeństwa.

5.3.54. Jeżeli ryzyka dotyczące bezpieczeństwa zostaną oszacowane jako nietolerowalne, zasadnie będzie zapytać:

a) *Czy da się wyeliminować zagrożenia i związane z nimi ryzyko dotyczące bezpieczeństwa?* Jeśli odpowiedź jest na TAK, zostaje podjęta i dokumentowana jest stosowna akcja. Jeśli odpowiedź jest na NIE, następne pytanie jest takie:

b) *Czy da się złagodzić ryzyko dotyczące bezpieczeństwa?* Jeśli odpowiedź jest na NIE, trzeba unieważnić odpowiednie działania. Jeśli odpowiedź jest na TAK, podjęta zostaje odpowiednia akcja i następnym pytaniem jest:

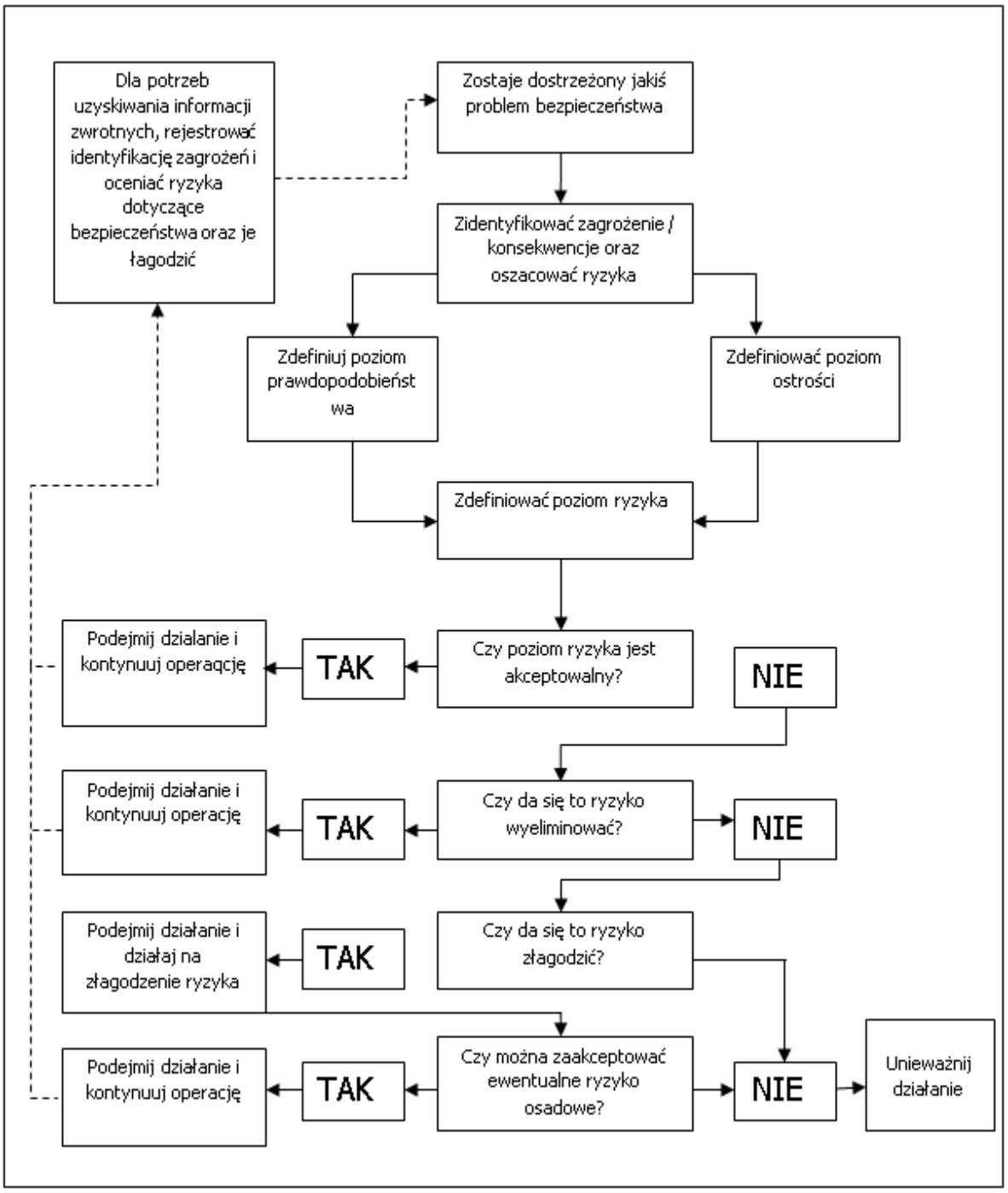
c) *Czy istnieje pozostałe ryzyko dotyczące bezpieczeństwa?* Jeśli odpowiedź jest na TAK, trzeba takie pozostałe ryzyko należy ocenić lub złagodzić na tyle na ile potrzeba, by zapewnić akceptowalny poziom działania bezpieczeństwa.

5.3.55. Proces zarządzania ryzykiem wymaga analizy zidentyfikowanych zagrożeń, która zawiera dwa komponenty:

a) dotkliwość wyników bezpieczeństwa (safety outcome); oraz

b) prawdopodobieństwo, że się zdarzy.

Wskazania dotyczące jakie powinny być informacje dotyczące bezpieczeństwa analizowane w złożonych, dużych organizacjach, przedstawia Rozdział 2. Po dokonaniu oceny ryzyka, dostawca usług zajmie się procesem decyzyjnym po to, by określić potrzebę wdrożenia miar łagodzenia ryzyka. Ten proces decyzyjny wymaga, by do kategoryzowania ryzyka użyć narzędzia, które może być w formie matrycy oceniania. Przykładowa matryca oceny ryzyka znajduje się w Rys. 5-5.



Rys. 5-4. Proces zarządzania ryzykiem

5.3.56. Używając tej matrycy, można ryzyko skategoryzować zgodnie z oceną jego potencjalnej dotkliwości i prawdopodobieństwa. Mimo że zalecana jest metodologia matrycy oceny, to inne ekwiwalentne metody przedstawiania tolerancji dla ryzyka są dostępne. Matrycę oceny ryzyka można dostosować do klienta tak, aby odzwierciedlała kontekst struktury organizacyjnej każdego dostawcy usług i działania lotnicze; może ona być uzależniona od zgody swych władz legislacyjnych. Ryzyko nieakceptowalne, odzwierciedlone przez ten przykład matrycy (kategorie czerwona i żółta) muszą być złagodzone po to, by zmniejszyła się ich dotkliwość i/lub prawdopodobieństwo. W braku działań łagodzących, które redukują

ryzyka do poziomu akceptowalnego, dostawca usług powinien rozważyć zawieszenie wszystkich działań, które nadal wystawiają jego organizację na nietolerowane ryzyka dotyczące bezpieczeństwa. Dodatkowe informacje dotyczące matrycy prawdopodobieństwa ryzyka, ich dotkliwości i możliwości ich tolerowania są zamieszczone w Rozdziale 2 niniejszego dokumentu.

5.3.57. Po oszacowaniu ryzyka, można wdrożyć stosowne środki łagodzące. Środki łagodzące ryzyko mogą obejmować cały szereg alternatyw, w tym, ale nie tylko modyfikacje istniejących procedur operacyjnych, programów szkoleniowych lub sprzętu używanego w dostarczaniu produktów i usług lotniczych. Dodatkowe alternatywy mogą obejmować wprowadzanie nowych procedur operacyjnych, programów szkoleniowych, technologii lub kontroli nadzorczych. Prawie bez zmian, takie alternatywy będą wymagać rozmieszczenia lub przemieszczenia trzech tradycyjnych sposobów obrony bezpieczeństwa lotniczego - technologii, szkolenia i przepisów. Określenia tego jakie mogą być niezamierzone konsekwencje, szczególnie wprowadzenia nowych zagrożeń, powinno się dokonać przed wdrożeniem jakichkolwiek miar łagodzenia ryzyka.

Prawdopodobieństwo wystąpienia ryzyka	Dotkliwość ryzyka				
	Katastrofalna A	Niebezpieczna B	Poważna C	Niewielka D	Nieistotna E
Częste: 5	5A	5B	5C	5D	5E
Sporadyczne: 4	4A	4B	4C	4D	4E
Dalekie: 3	3A	3B	3C	3D	3E
Nieprawdopodobne: 2	2A	2B	2C	2D	2E
Skrajnie nieprawdopodobne: 1	1A	1B	1C	1D	1E

Rys. 5-5. Przykład matrycy oceny ryzyka

5.3.58. Trzy kategorie podejść do łagodzenia ryzyka dotyczącego bezpieczeństwa obejmują:

a) *Unikanie (Avoidance).* Działanie zostaje zawieszone albo dlatego, że towarzyszące mu ryzyka dotyczącego bezpieczeństwa stają się niemożliwe do tolerowania, albo dlatego, że zostają uznane za nieakceptowalne w konfrontacji z korzyściami związanymi z działaniem.

b) *Redukcja (Reduction).* Pewna ekspozycja ryzyka dotyczącego bezpieczeństwa jest akceptowalna, choć związana z ryzykiem dotkliwość bądź prawdopodobieństwo ulega zmniejszeniu, możliwe że dzięki miarom, które łagodzą konsekwencje.

c) *Segregacja ekspozycji (Segregation of exposure*). Podejmuje się akcję dla odizolowania potencjalnych konsekwencji jakie są związane z zagrożeniem, bądź ustanawia się wiele warstw ochrony przed zagrożeniami.

5.3.59. Strategia łagodzenia ryzyka może wymagać któregoś wyżej opisanego podejścia lub może obejmować wielu podejść. Ważne, żeby dla znalezienia rozwiązania optymalnego, uwzględnić cały zakres możliwych środków kontrolnych. Zanim będzie można podjąć decyzję, oceniona musi być skuteczność każdej strategii alternatywnej. Każda proponowana alternatywa łagodzenia ryzyka dotyczącego bezpieczeństwa powinna być przeegzaminowana z poniższych perspektyw:

a) *Skuteczność (Effectiveness).* Jest to zasięg w jakim alternatywy redukują lub eliminują ryzyko dotyczące bezpieczeństwa. Skuteczność można określić pod względem technicznych, szkoleniowych bądź legislacyjnych sposobów obrony, które mogą ryzyko dotyczące bezpieczeństwa zredukować lub wyeliminować.

b) *Koszt/korzyść (Cost/benefit).* Jest to zasięg w jakim dostrzegane korzyści przeważają koszty łagodzenia.

c) *Praktyczność (Practicality).* Jest to zasięg w jakim łagodzenie daje się wdrożyć i na ile jest ono właściwe pod względem dostępnej technologii, finansów i zasobów administracyjnych, prawodawstwa i przepisów, woli politycznej itd.

d) *Akceptowalność (Acceptability).* Jest to zasięg w jakim alternatywa jest spójna z paradygmatami uczestników.

e) *Egzekwowalność (Enforceability).* Jest to zasięg w jakim przestrzeganie zasad, przepisów i procedur operacyjnych daje się monitorować.

f) *Trwałość (Durability).* Jest to zasięg w jakim łagodzenie będzie trwałe i skuteczne.

g) *Pozostałe ryzyko dotyczące bezpieczeństwa (Residual safety risks).* Jest to stopień ryzyka dotyczący bezpieczeństwa, który pozostaje po wdrożeniu łagodzenia wstępnego, i który może wymagać dodatkowych środków kontrolowania ryzyka.

h) *Niezamierzone konsekwencje (Unintended consequences).* Jest to wprowadzanie nowych zagrożeń i ryzyka dotyczącego bezpieczeństwa, związanych ze wdrożeniem dowolnej alternatywy łagodzenia.

5.3.60. Po zatwierdzeniu i wdrożeniu łagodzenia, każde z tym związane uderzenie w działanie bezpieczeństwa dostarcza informacji zwrotnych procesowi zapewniania bezpieczeństwa u dostawcy usług. Jest to potrzebne dla zapewnienia nierozerwalności, skuteczności i wydajności środków obrony w nowych warunkach operacyjnych.

5.3.61. Każde ćwiczenie dotyczące łagodzenia ryzyka musi być dokumentowane wraz z postępem prac. Można to zrealizować korzystając z różnych aplikacji począwszy od arkuszy lub tabel, a skończywszy na dostosowanym komercyjnym programie łagodzenia ryzyka. Zamknięte dokumenty dotyczące działań łagodzących ryzyko muszą być zatwierdzone przez kierownictwo odpowiedniego szczebla. Po przykład podstawowego arkusza roboczego dla łagodzenia ryzyka dotyczącego bezpieczeństwa, odsyłamy do Dodatku 2, Rozdział 2.

Komponent nr 3 programu SMS. Zapewnianie bezpieczeństwa

5.3.62. Zapewnianie bezpieczeństwa składa się z trzech procesów i działań podejmowanych przez dostawcę usług w celu określenia czy SMS działa zgodnie z oczekiwaniami i wymogami. Dostawca usług ciągle monitoruje swoje wewnętrzne procesy, jak również swoje operacyjne środowisko by wykrywać zmiany lub odchylenia, które mogą wprowadzić pojawiające się ryzyko dotyczące bezpieczeństwa lub spowodować degradację istniejących kontroli ryzyka. Takimi zmianami lub odstępstwami można się wtedy zająć razem z procesem zarządzania ryzykiem.

5.3.63. Proces zapewniania bezpieczeństwa uzupełnia proces zapewniania jakości, przy czym każdy z nich ma swoje wymagania wobec analizy, dokumentacji, audytów i przeglądów zarządzania, dla zapewnienia by spełniane były pewne kryteria działania bezpieczeństwa. Zapewnianie jakości koncentruje się typowo na przestrzeganiu przez organizację wymogów prawnych, a zapewnianie bezpieczeństwa monitoruje konkretnie skuteczność kontroli ryzyka dotyczącego bezpieczeństwa.

5.3.64. Ten uzupełnieniowy związek między zapewnianiem bezpieczeństwa i zapewnianiem jakości pozwala na integrowanie niektórych procesów pomocniczych. Taka integracja może służyć do uzyskania synergii dla zapewnienia, by spełniane były cele dostawcy usług w sferze bezpieczeństwo, jakości i handlu.

5.3.65. Na koniec, działania na rzecz zapewniania bezpieczeństwa powinny obejmować opracowywanie i wdrażanie działań korekcyjnych w odpowiedzi na ustalenia, że słabości zaistniałe w systemie mają potencjalny negatywny wpływ dla bezpieczeństwa. Odpowiedzialność organizacji za opracowanie i wdrożenie działań korekcyjnych powinna pozostawać w wydziałach zacytowanych w ustaleniach.

Element 3.1 systemu SMS.
Monitorowanie i mierzenie bezpieczeństwa

3.1.1 Dostawca usług musi opracować i utrzymywać środki do weryfikowania działania bezpieczeństwa w organizacji i uwierzytelniania skuteczności kontroli ryzyka dotyczącego bezpieczeństwa.

3.1.2 Działanie bezpieczeństwa u dostawcy usług musi być weryfikowane względem wskaźników działania bezpieczeństwa i działania celów SMS w sferze bezpieczeństwa.

Strategia wdrażania (Implementation strategy)

5.3.66. Informacje, wykorzystywane do mierzenia działania bezpieczeństwa w organizacji, są generowane przez systemy raportowania bezpieczeństwa tegoż dostawcy usług. Wskaźniki działania bezpieczeństwa są omówione szczegółowo pod 5.4.5 oraz w Dodatku 6 niniejszego rozdziału.

5.3.67. Są dwa typy systemów raportowania:

a) systemy obowiązkowego raportowania zdarzeń; oraz

b) systemy dobrowolnego raportowania zdarzeń.

5.3.68. System obowiązkowego raportowania zdarzeń wymaga raportowania niektórych typów zdarzeń (np. poważne incydenty, wtargnięcia na drogę startową). Wymaga on wdrożenia szczegółowych przepisów dla ustalenia kryteriów raportowania i zakresu w jakie zdarzenia mają być zgłaszane. Systemy raportowania obowiązkowego mają skłonność do gromadzenia większej liczby informacji związanych z usterkami technicznymi o dużych konsekwencjach, bardziej niż innych aspektów działań operacyjnych.

5.3.69. Systemy dobrowolnego raportowania dopuszczają składanie informacji związanych z zaobserwowanymi zagrożeniami lub nieumyślnymi pomyłkami, bez związanego z nimi prawnego lub administracyjnego wymogu. W tych systemach, legislacyjne organa lub organizacje mogą stosować zachętę do złożenia raportu. Na przykład, mogą znieść przymus raportowania nieumyślnych pomyłek lub niezamierzonych naruszeń. W takich sytuacjach, zgłaszane w raportach informacje powinny być użyte tylko na polepszanie jakości. Takie systemy uważa się za "non-punitive" (nieobarczone karą), ponieważ zapewniają ochronę osobom raportującym i dzięki temu zapewniają ciągłe pozyskiwanie takich informacji dla wspierania stałych ulepszeń w działaniu bezpieczeństwa. Choć charakter i zasięg koncepcji dostawców usług co do raportowania non-punitive może być różny, ich intencją jest promować kulturę raportowania skutecznego i proaktywną identyfikację potencjalnych niedostatków bezpieczeństwa.

5.3.70. Dobrowolne systemy raportowania mogą być poufne, z wymogiem by informacje identyfikujące informatorów pozostały znane tylko strażnikom systemów w celu umożliwienia kontynuowania czynności pozgłoszeniowych (follow-up actions). Systemy poufnego raportowania zdarzeń ułatwiają ujawnianie zagrożeń prowadzących do ludzkiej pomyłki, jednak bez obawy o ukaranie ani stawianie informatora w kłopotliwej sytuacji. Dobrowolne raporty można archiwizować i odpersonalizować po wykonaniu wszystkich czynności pozgłoszeniowych. Odpersonalizowane raporty mogą wspierać analizy przyszłych trendów po to, by korzystać ze skuteczności łagodzenia ryzyka i identyfikować pojawiające się zagrożenia.

5.3.71. Aby system taki był skuteczny, narzędzia umożliwiające zgłaszanie informacji o bezpieczeństwie muszą być łatwo dostępne dla pracowników operacyjnych. Personel operacyjny powinien być przeszkolony co do zalet systemów zgłaszania informacji o bezpieczeństwie i otrzymywać informację zwrotną dotyczącą działań naprawczych podjętych w odpowiedzi na zgłoszenie. Równoległe ustawienie wymagań dotyczących systemów zgłaszania, narzędzi i metod analitycznych ułatwi wymianę informacji o bezpieczeństwie, jak również porównanie pewnych wskaźników bezpieczeństwa. Wskazówki dobrowolnych i poufnych systemów raportowania są podane w Dodatku nr 5 do tego rozdziału.

5.3.72. Inne źródła informacji o bezpieczeństwie, mające wesprzeć monitorowanie i mierzenie, mogą obejmować:

a) *Studia nad bezpieczeństwem (Safety studies*) są to analizy wykorzystywane do osiągania zrozumienia szerokich spraw bezpieczeństwa lub spraw o charakterze globalnym. Na przykład, resort lotniczy może wydać zalecenia (recommendations) i wdrożyć pomiary dla zredukowania wypadków i incydentów w fazie zbliżania i lądowania. Poszczególni dostawcy usług mogą uznać, że takie globalne zalecenia polepszają bezpieczeństwo w kontekście ich działań lotniczych.

b) *Przeglądy bezpieczeństwa (Safety reviews)* są fundamentalnym komponentem zarządzania zmianami. Przeprowadzane są podczas wprowadzania nowych technologii, nowych procedur bądź zmian systemowych, które rzutują na operacje lotnicze. Przeglądy bezpieczeństwa mają wyraźnie określony cel, który jest podłączony do rozpatrywanej zmiany. Przeglądy bezpieczeństwa zapewniają to, że działanie bezpieczeństwa jest utrzymywane na odpowiednich poziomach przez okresy zmiany.

c) *Pomiary bezpieczeństwa (Safety surveys)* egzaminują procedury lub procesy związane z konkretną operacją. Pomiary bezpieczeństwa mogą wymagać stosowania list kontrolnych, kwestionariuszy i nieformalnych, poufnych przesłuchań (interviews). Generalnie, pomiary bezpieczeństwa dostarczają informacji ilościowych które, dla określenia jaka ma być odpowiednia akcja naprawcza, mogą wymagać uwierzytelnienia. Pomimo tego, pomiary mogą stanowić niedrogie źródło znaczących informacji o bezpieczeństwie.

d) *Audyty (Audits*) skupiaja się na tym czy zintegrowane są ze sobą - SMS organizacji i systemy go wspierające. Audyty dają ocenę kontroli ryzyka dotyczących bezpieczeństwa i spokrewnionych procesów zapewniania jakości. Audyty mogą być przeprowadzane przez podmioty zewnętrzne względem usługodawcy, lub mogą być wewnętrznym procesem rewizyjnym posiadającym niezbędne działania koncepcyjne (policies) oraz procedury na zapewnienie, że są niezależne i obiektywne. Audyty są przewidziane na zapewnianie funkcji zarządzania bezpieczeństwem, w tym obsadzania stanowisk, zgodności z zatwierdzonymi przepisami, poziomów kompetencji oraz szkolenia.

e) *Dochodzenia wewnętrzne (Internal investigations*) są prowadzone dla niektórych wydarzeń w sferze bezpieczeństwa, obowiązkowo raportowanych zgodnie z wymogami wewnętrznymi lub legislacyjnymi. Badane przez Państwo lub przez stosowne władze regionalne wypadki i poważne incydenty mogą także nadać impetu dochodzeniom wewnętrznym, które mają być podejmowane przez organizacje dostawców usług.

5.3.73. Ostatecznym rezultatem (Output) procesu monitorowania i mierzenia działania bezpieczeństwa jest opracowanie wskaźników działania bezpieczeństwa, opartych na analizie danych zgromadzonych przez ww. źródła. Proces monitorowania i mierzenia wymaga stosowania wyselekcjonowanych wskaźników działania bezpieczeństwa, odpowiadających im celów działania bezpieczeństwa i poziomów alarmowych. Wskazówki opracowania wskaźników działania bezpieczeństwa, ich ustalonych celów i poziomów alarmowych są podane pod 5.4.5 i w Dodatku 6.

Element 3.2 programu SMS.
Zarządzanie zmianami

Dostawca usług musi opracować i utrzymywać formalny proces do identyfikowania zmian, które mogą rzutować na związany z produktami i usługami lotniczymi poziom bezpieczeństwa, i do identyfikowania oraz zarządzania ryzykiem, jakie z tych zmian mogą powstawać.

Strategia wdrażania (Implementation strategy)

5.3.74. Dostawcy usług lotnictwa doświadczają zmian spowodowanych ilością czynników nie tylko tych wyszczególnionych poniżej:

a) rozrastanie lub kurczenie się organizacji;

b) zmiany w wewnętrznych systemach, procesach lub procedurach, które wspierają dostarczanie produktów i usług, oraz

c) zmiany w operacyjnym środowisku organizacji.

5.3.75. Zmiany mogą dotknąć samą zasadność lub skuteczność istniejących strategii łagodzenia ryzyka dotyczących bezpieczeństwa. Dodatkowo, nowe zagrożenia i związane z nimi ryzyka dotyczące bezpieczeństwa mogą być nieumyślnie wprowadzone do jakiejś operacji za każdym razem, gdy odbywa się jakaś zmiana. Takie zagrożenia należy identyfikować po to, by umożliwić ocenianie związanych z nimi ryzyka dotyczących bezpieczeństwa oraz ich kontrolowanie. Audyty bezpieczeństwa, omówione w dyskusji dotyczącej monitorowania i mierzenia działania bezpieczeństwa mogą być wartościowymi źródłami informacji na wsparcie procesów decyzyjnych i skutecznego zarządzania zmianami.

5.3.76. Zarządzanie procesem zmian u siebie w organizacji powinno brać pod uwagę trzy poniższe względy:

a) *Krytyka (Criticality).* O tym jakie systemy, sprzęt i działania będą istotne dla bezpiecznego latania decyduje ocena krytyczna. Opinie krytyczne są normalnie oceniane podczas procesu projektowania systemu, odbywa się to również w trakcie zmian. Systemy, sprzęt i działania, które otrzymują mocniejszą krytykę powinny być przeglądane po zmianie po to, by się upewnić, że będzie można zastosować działania korekcyjne dla kontrolowania ryzyka dotyczącego bezpieczeństwa, które mogą się pojawić.

b) *Stabilność systemów i środowisk operacyjnych (Stability of systems and operational environments).* Zmiany wolno jest planować pod bezpośrednią kontrolą organizacji. Planowane zmiany obejmują rozrost lub kurczenie się organizacji, ekspansję dostarczania produktów i usług lub wprowadzanie nowych technologii. Zmianami nieplanowanymi mogą być te, które dotyczą cykli ekonomicznych, zamieszek robotniczych, jak również mogą to być zmiany w środowisku politycznym, legislacyjnym lub operacyjnym.

c) *Wydajność w przeszłości (Past performance).* Do przewidywania i monitorowania działania bezpieczeństwa w sytuacjach, gdy zachodzą zmiany, wykorzystana być powinna przeszła wydajność krytycznych systemów, oraz analizy trendów. Monitorowanie osiągów z przeszłości zapewni również skuteczność akcji korekcyjnych, podejmowanych po to, by się zająć słabościami bezpieczeństwa, ujawnianymi jako wynik audytów, oceniania, dochodzeń lub raportów.

5.3.77. Wraz z rozwojem systemów, ilość zmian może się zakumulować, co wymagać będzie wprowadzenia zmian do pierwotnego opisu systemu. Tak więc, w celu stwierdzenia ciągłej ważności opisów systemów i analizy granicy zagrożenia, zarządzanie zmianą wymaga okresowych przeglądów.

Element 3.3 systemu SMS.
Ustawiczne ulepszanie SMS

Dostawca usług musi monitorować i oceniać skuteczność procesów swego SMS po to, by umożliwiać ulepszanie całego działania tegoż SMS.

Strategia wdrażania (Implementation strategy)

5.3.78. Ciągłe ulepszanie mierzy się poprzez monitorowanie wskaźników działania bezpieczeństwa w organizacji i pozostaje ono w związku z dojrzałością i skutecznością SMS. Ulepszenia są wspomagane procesami zapewniania bezpieczeństwa poprzez ciągłe działania weryfikacyjne i kontynuacyjne. Cele te osiąga się przez zastosowanie oceniania wewnętrznego i niezależnych audytów SMS.

5.3.79. Ocenianie wewnętrzne wymaga oszacowania lotniczych działań dostawcy usług, które mogą dostarczyć przydatnych informacji procesom decyzyjnym organizacji. To tu mają miejsce kluczowe działania SMS – identyfikacja zagrożeń i łagodzenie

ryzyka (HIRM). Ocenianie, przeprowadzone dla potrzeb tego wymogu, musi być wykonywane przez osoby lub organizacje, które są funkcjonalnie niezależne od technicznych procesów będących przedmiotem oceniania.

5.3.80. Wewnętrzne audyty wymagają systematycznego i zaplanowanego badania działań lotniczych dostawcy usług, także takich, które są specyficzne dla wdrażania SMS. Dla większej skuteczności, audyty wewnętrzne są przeprowadzane przez osoby lub wydziały niezależne od funkcji ocenianych. Funkcja wewnętrznego oceniania obejmuje ocenianie funkcji zarządzania bezpieczeństwem, ustanawiania polityki, zarządzania ryzykiem, zapewniania bezpieczeństwa i promowania bezpieczeństwa w całej organizacji.

5.3.81. Zewnętrzne audyty SMS mogą być przeprowadzane przez odpowiednie władze, odpowiedzialne za zaakceptowanie SMS dostawcy usług. Dodatkowo, audyty mogą być przeprowadzane przez przemysłowe zjednoczenia lub przez inne strony trzecie, wybrane przez dostawcę usług. Takie zewnętrzne audyty doprecyzowują system wewnętrznych audytów, a także dają ogląd niezależny.

5.3.82. Streszczając, ocenianie i procesy audytowania przyczyniają się do umiejętności dostawcy usług osiągania ciągłej poprawy bezpieczeństwa. Stałe monitorowanie SMS, związane z nim środki kontrolowania bezpieczeństwa oraz systemy wspierające zapewniają osiągalność celów przez proces zarządzania bezpieczeństwem.

Komponent nr 4 systemu SMS. Promowanie bezpieczeństwa

5.3.83. Promowanie bezpieczeństwa pobudza właściwą kulturę bezpieczeństwa i tworzy środowisko, które sprzyja osiąganiu przez dostawcę usług swych celów w sferze bezpieczeństwa. Pozytywną kulturę bezpieczeństwa cechują wartości, podejścia do sprawy oraz zachowania świadczące o zaangażowaniu się w wysiłki organizacji na rzecz bezpieczeństwa. Osiąga się to poprzez kombinację kompetencji technicznych stale dopracowywanych poprzez szkolenie i edukację, skuteczne komunikowanie i dzielenie się informacjami. Wyższe kierownictwo zapewnia przewodzenie w promowaniu kultury bezpieczeństwa po całej organizacji.

5.3.84. Sam wysiłek organizacji, skierowany na bezpieczeństwo, nie jest w stanie odnieść sukcesu z obowiązku, ani poprzez ścisłe trzymanie się koncepcji (policies). Promocja bezpieczeństwa wpływa zarówno na postępowanie jednostek, jak i organizacji oraz uzupełnia koncepcje organizacji, procedury i procesy – dając system wartości, który wspiera wysiłki na rzecz bezpieczeństwa.

5.3.85. Dostawca usług musi ustanowić i utrzymywać procesy i procedury, które ułatwiają skuteczną komunikację po wszystkich poziomach organizacji. Dostawcy usług powinni komunikować o swych celach w sferze bezpieczeństwa, jak również o bieżącym stanie wszystkich pokrewnych działań i wydarzeń. Dostawcy usług muszą również zachęcać do komunikacji oddolnej, zapewniającej istnienie środowiska dzięki któremu wyższe kierownictwo może otrzymywać od personelu operacyjnego otwarte i konstruktywne informacje zwrotne.

Element 4.1 systemu SMS.
Szkolenie i edukacja

4.1.1 Dostawca usług musi opracować i utrzymywać program szkolenia dotyczącego bezpieczeństwa, który zapewnia to, że personel jest przeszkolony i kompetentny do wykonywania swych obowiązków związanych z SMS.

4.1.2 Zakres programu szkolenia dotyczącego bezpieczeństwa musi być stosowny do indywidualnego udziału w SMS, poszczególnej osoby.

Strategia wdrażania (Implementation strategy)

5.3.86. Kierownik bezpieczeństwa powinien dostarczać informacji bieżących i ułatwiać otrzymanie przeszkolenia odpowiedniego dla konkretnych, bieżących spraw bezpieczeństwa, na które napotykają się jednostki organizacyjne danej organizacji. Zapewnianie właściwemu personelowi właściwego szkolenia, niezależnie od ich hierarchicznego poziomu w organizacji, jest wykładnią zaangażowania się kierownictwa w to, żeby SMS był skuteczny. Programy szkolenia dotyczące bezpieczeństwa i programy edukacyjne powinny składać się z:

a) polityki bezpieczeństwa w organizacji, cele i założenia;

b) ról odgrywanych w organizacji w zakresie bezpieczeństwa oraz z zakresów odpowiedzialności za bezpieczeństwo;

c) podstawowych zasad zarządzania ryzykiem;

d) systemów raportowania o bezpieczeństwie;

e) wsparcia dla zarządzania bezpieczeństwem (w tym programami oceniania i audytowania);

f) łącz komunikacyjnych, także do rozpowszechniania informacji o bezpieczeństwie;

g) procesu uwierzytelniania (validation process), który mierzy skuteczność szkolenia; oraz

h) z udokumentowanej, początkowej indoktrynacji i wymogu powtarzania szkoleń.

5.3.87. Wymogi szkoleniowe, spójne z potrzebami i złożonością organizacji powinny być dokumentowane dla każdego obszaru działania. Dla każdego pracownika, w tym kierownictwa, powinna być opracowana ścieżka szkoleniowa.

5.3.88. Wewnętrzne szkolenie dotyczące bezpieczeństwa musi dawać pewność, że personel jest kompetentny do wykonywania swych, związanych z bezpieczeństwem, obowiązków. Procedury szkoleniowe powinny wyszczególniać standardy szkoleniowe w szkoleniach początkowych i powtarzalnych personelu operacyjnego, kierowników i nadzorców, wyższych kierowników i dyrektorów personalnie odpowiedzialnych. Dawka szkolenia w sferze bezpieczeństwa powinna odpowiadać zakresowi obowiązków danej osoby i jej udziału w SMS. Dokumentacja ze szkolenia powinna również wyszczególniać odpowiedzialności za opracowywanie treści szkolenia i za harmonogramy, jak również za zarządzanie dziennikami szkoleń.

5.3.89. Szkolenie powinno obejmować politykę bezpieczeństwa organizacji, role i odpowiedzialności za bezpieczeństwo, zasady SMS związane z zarządzaniem ryzykiem dotyczącymi bezpieczeństwa i zapewnianiem bezpieczeństwa, jak również zasady korzystania z wewnętrznych systemu/ów raportowania bezpieczeństwa.

5.3.90. Szkolenie dotyczące bezpieczeństwa dla wyższych kierowników powinno zawierać treści związane z przestrzeganiem krajowych i firmowych wymogów dotyczących bezpieczeństwa, rozdzielnictwem zasobów i aktywną promocją SMS, w tym skuteczną komunikację między wydziałami w zakresie bezpieczeństwa. Dodatkowo, szkolenie dotyczące bezpieczeństwa dla kierowników wyższego szczebla powinno obejmować materiały dotyczące ustanawiania celów działania bezpieczeństwa oraz poziomów alarmowych.

5.3.91. W ostateczności, programem szkolenia dotyczącym bezpieczeństwa może być sesja zaprojektowana konkretnie dla danego dyrektora odpowiedzialnego. Taka sesja szkoleniowa powinna być na wysokim poziomie, dostarczając dyrektorowi odpowiedzialnemu rozumienie SMS i związków SMS z całościową strategią biznesową organizacji.

Element 4.2 systemu SMS.
Komunikacja bezpieczeństwa

Dostawca usług musi opracować i utrzymywać formalne środki komunikacji w sprawach bezpieczeństwa, które:

a) zapewniają to, że personel jest świadom SMS w stopniu współmiernym do zajmowanego stanowiska;

b) przekazują krytyczne dla bezpieczeństwa informacje;

c) wyjaśniają dlaczego podejmowane są konkretne akcje dotyczące bezpieczeństwa; oraz

d) wyjaśniają dlaczego są wprowadzane i zmieniane procedury bezpieczeństwa.

Strategia wdrażania (Implementation strategy)

5.3.92. Dostawca usług powinien komunikować cele i procedury SMS organizacji całemu personelowi operacyjnemu. Kierownik bezpieczeństwa powinien regularnie przekazywać informacje dotyczące trendów w działaniu bezpieczeństwa, także konkretne aktualne zagadnienia, poprzez biuletyny i odprawy. Kierownik bezpieczeństwa powinien także dopilnowywać, by nauki z konkretnych badań i przypadków oraz doświadczeń, zarówno wewnętrznych, jak i spoza organizacji, były szeroko rozpowszechniane. Działanie bezpieczeństwa będzie bardziej sprawne, jeśli personel operacyjny będzie aktywnie zachęcany do zauważania zagrożeń i ich raportowania. Zatem, komunikacja ma za cel:

a) zapewnić by personel miał pełną świadomość SMS;

b) przekazywać informacje, które są krytyczne dla bezpieczeństwa;

c) podnosić świadomość akcji korekcyjnych; oraz

d) dostarczać informacji dotyczących nowych lub poprawionych procedur dotyczących bezpieczeństwa.

5.3.93. Przykłady komunikacji w organizacji obejmują:

a) rozpowszechnianie podręcznika SMS;

b) procesy i procedury dotyczące bezpieczeństwa;

c) biuletyny okazjonalne dotyczące bezpieczeństwa, ogłoszenia i biuletyny; oraz

d) strony internetowe oraz pocztę elektroniczną.

5.4. PLANOWANIE WDROŻENIA SMS

5.4.1. Opis systemu

Pierwszym krokiem w definiowaniu zakresu SMS i jego przydatności jest przegląd systemu i opis elementów SMS oraz ich łącz z istniejącymi systemami i procesami. Niniejsze ćwiczenie daje okazję do zidentyfikowania wszelkich luk dotyczących komponentów i elementów SMS dostawcy usług. Opis systemu obejmuje istniejące w organizacji łącza SMS, jak również odpowiednie łącza do organizacji zewnętrznych, takich jak podwykonawcy usług. Do dokumentacji SMS powinien być włączony ogląd opisu systemu i jego struktury pod względem odpowiedzialności i raportowania. Odnośnie dużych i złożonych organizacji, detale ich podstawowych systemów i procedur są omówione w przedmiotowych prezentacyjnych i administracyjnych podręcznikach dostawcy usług. W takich przypadkach, dla potrzeb opisania systemu, wystarczyć może krótki zarys plus schemat organizacyjny ze stosownymi odnośnikami.

5.4.2. Integracja systemów zarządzania

5.4.2.1. Zależnie od organizacyjnych, operacyjnych i legislacyjnych kontekstów, dostawca usług może wdrożyć SMS zintegrowany. Scalanie systemów ma potencjał wywoływania synergii poprzez zarządzanie ryzykiem dotyczącymi bezpieczeństwa w wielu obszarach działań lotniczych. Na przykład, dostawca usług może wdrożyć pojedynczy SMS dla swego działu projektowania, organizacji produkcji i zarobkowych operacji lotniczych (flight department). Alternatywnie, mogą być sytuacje gdzie indywidualny SMS będzie odpowiedni dla każdego typu działalności lotniczych. Organizacja może zdefiniować najlepszy środek dla zintegrowania lub posegregowania swego SMS, taki jaki będzie pasował do jego biznesowego lub organizacyjnego modelu, pod warunkiem, że Państwo uzna iż obowiązki wynikające z jego SMS są wykonywane odpowiednio we wszystkich rolach dostawcy usług. SMS dostawcy usług może być również scalony z systemami ochrony, zdrowia pracowników, zarządzania środowiskiem.

Integracja SMS i QMS

5.4.2.2. Dostawcy usług lotniczych typowo wdrażają systemy obejmujące całą organizację. Działanie bezpieczeństwa w organizacji jest zależne od skutecznego zintegrowania tych systemów dla wspomagania dostarczania produktów i usług. W kontekście SMS, najbardziej istotnym aspektem integracji jest zintegrowanie z należącym do dostawcy usług systemem zarządzania jakością (QMS). QMS jest generalnie definiowany jako struktura organizacyjna z przynależnymi odpowiedzialnościami personalnymi, zasobami, procesami i procedurami, potrzebnymi dla ustanowienia i promowania systemu ustawicznego zapewniania i poprawiania dostarczanego produktu bądź usługi. QMS jest istniejącym wymogiem prawnym wobec większości dostawców usług, także wymogiem dla zatwierdzenia produkcji (Załącznik 8 do Konwencji chicagowskiej), wobec organizacji wykonujących obsługę techniczną (Załącznik 6 do Konwencji chicagowskiej, Część I) i wobec dostarczycieli usług meteorologicznych i aeronautycznych (Załączniki do Konwencji chicagowskiej, odpowiednio, 3 i 15).

5.4.2.3. QMS i SMS uzupełniają się. QMS skupia się na zgodności z obowiązującymi przepisami i wymogami po to by spełniać oczekiwania klientów i zobowiązania kontraktowe, a SMS skupia się na działaniu bezpieczeństwa. Celami SMS jest identyfikować zagrożenia dotyczące bezpieczeństwa, oszacować związane z tym ryzyko i wdrożyć skuteczną kontrolę ryzyka. Dla kontrastu, QMS skupia się na konsekwentnym dostarczaniu produktów i usług, które spełniają odpowiednie parametry. Jednak zarówno SMS, jak i QMS:

a) muszą być zaplanowane i zarządzane;

b) być zależne od obmierzania i monitorowania przez wskaźniki osiągów;

c) obejmować wszystkie stanowiska pracy, które są związane z dostawą produktów i usług lotniczych; oraz

d) stale się ulepszać.

5.4.2.4. SMS i QMS korzystają z tych samych procesów zarządzania ryzykiem i jakością. Celem SMS jest zidentyfikować zagrożenia dotyczące bezpieczeństwa, wobec których staje organizacja i panować nad ryzykiem związanym z takimi zagrożeniami. SMS jest zaprojektowany do zarządzania ryzykiem i do mierzenia działania bezpieczeństwa podczas dostarczania produktów i usług. Proces zarządzania ryzykiem eliminuje zagrożenia lub dostarcza skutecznych kontroli dla łagodzenia ryzyka poprzez utrzymywanie równowagi w przydzielaniu odpowiednich zasobów na produkcję i na zabezpieczanie spełniające wymogi bezpieczeństwa.

5.4.2.5. QMS zapewnia ciągłość dostaw produktów i usług zgodnych ze standardami, jak również z oczekiwaniami klientów. QMS ma także niezależną funkcję zapewniania dostaw, która wykorzystuje pętlę informacji zwrotnych dla zapewniania dostaw produktów i usług, które nadają się oraz są wolne od wad i błędów. Funkcja zapewniania jakości rozpoznaje nieskuteczne procesy i procedury, które trzeba przeprojektować na wydajne i skuteczne.

5.4.2.6. Co więcej, SMS QMS wykorzystują te same narzędzia. Fachowcy od bezpieczeństwa i jakości są zasadniczo skupieni na tym samym celu jakim jest dostarczenie klientom bezpiecznych i niezawodnych produktów i usług. Zarówno fachowcy od bezpieczeństwa, jak i jakości są szkoleni różnymi metodami analitycznymi obejmującymi analizę podstawową i statystyczną analizę trendów.

5.4.2.7. Przy uzupełniających się aspektach SMS i QMS istnieje możliwość ustanowienia związku polegającego na synergii między oboma systemami, co można tak streścić:

a) SMS jest wspierany procesami QMS, takimi jak audyt, inspekcja, dochodzenie, dogłębna analiza przyczyn, projekt procesu, analiza statystyczna i środki prewencyjne;

b) QMS potrafi przewidywać istnienie bieżących zagadnień bezpieczeństwa, pomimo tego, że organizacja działa zgodnie ze standardami i specyfikacjami; i

c) zasady jakości, koncepcje i stosowane praktyki są przyłączone do celów zarządzania bezpieczeństwem.

5.4.2.8. Wzajemna relacja między SMS a QMS prowadzi do uzupełniających się działań każdego systemu na rzecz celów jakimi są bezpieczeństwo organizacji oraz jakość. Streszczenie porównawcze tych dwu systemów znajduje się w Tabeli 5-1.

Tabela 5-1. Streszczenie porównawcze QMS i SMS
(Summary comparison of QMS and SMS)

QMS	*SMS*
Jakość	Bezpieczeństwo
Zapewnianie jakość	Zapewnianie bezpieczeństwa
Kontrola jakości	Identyfikowanie zagrożeń i kontrola ryzyka
Kultura jakości	Kultura bezpieczeństwa
Przestrzeganie wymogów	Akceptowalny poziom działania bezpieczeństwa
Jest nakazowy	Opiera się na działaniu bezpieczeństwa
Standardy i specyfikacje	Czynnik korporacyjny oraz ludzki
Jest reaktywny > proaktywny	Jest proaktywny > predykatywny

5.4.3. Analiza luk

5.4.3.1. Analiza luk porównuje posiadane przez dostawcę usług istniejące procesy zarządzania bezpieczeństwem i procedury z wymogami zawartymi w ramie SMS. Dostawcy usług lotniczych typowo wdrażają różne funkcje SMS z powodu ich zgodności z krajowymi przepisami lub z powodu przyjmowania najlepszych praktyk stosowanych w branży. SMS powinno się opracować na istniejących w organizacji strukturach i systemach kontroli. Analiza luk ułatwia opracowanie planu wdrożenia SMS przez identyfikowanie luk, którymi trzeba się zająć, by SMS wdrożyć w pełni. Po ukończeniu analizy luk i pełnym jej udokumentowaniu, podstawę planu wdrażania SMS będą tworzyć zasoby i procesy, które były rozpoznane za niewystarczające lub nieistniejące.

5.4.3.2. Dodatek 7 do tego rozdziału dostarcza listę pytań dotyczących analizy luk, by pomóc dostawcom usług w systematycznym ocenianiu istniejących u siebie procesów. Z przedmiotowego odzewu po każdym pytaniu dotyczącym analizy luk stanie się oczywiste jakich dopracować potrzeba.

5.4.4. Plan wdrożenia SMS

5.4.4.1. Plan wdrożenia SMS opracowuje się w konsultacji z dyrektorem odpowiedzialnym i kierownikami odpowiedzialnymi za dostawy produktów i usług mających związek z, lub wspierających bezpieczne eksploatowanie samolotów. Po zamknięciu planu, plan jest parafowany przez Dyrektora Odpowiedzialnego. Plan wdrożenia SMS uwzględnia terminy i kamienie milowe zgodne ze zidentyfikowanymi w procesie analizy luk wymaganiami, wielkością podmiotu i złożonością wyrobów lub usług. Plan powinien omawiać koordynację/współpracę z organizacjami zewnętrznymi lub dostawcami usług, tam gdzie ma to zastosowanie.

5.4.4.2. Wdrożenie planu przez dostawcę usług może być dokumentowane w różny sposób, od prostych rozkładówek po specjalistyczne oprogramowanie dla zarządzania projektami. Plan wdrożenia powinien zajmować się lukami poprzez przeprowadzanie konkretnych akcji i przez przestrzeganie międzyczasów podanego harmonogramu. Odpowiedzialność jest w całym procesie wdrażania zapewniana przez to, że każde działanie ma swego adresata. Plan powinien być przeglądany regularnie i uaktualniany w miarę potrzeb. Przykład formatu planu/harmonogramu wdrażania SMS znajduje się w Dodatku 7 do tego rozdziału.

5.4.4.3. Pełne wdrożenie wszystkich komponentów i elementów ramy SMS może zająć do pięciu lat, zależnie od dojrzałości i złożoności organizacji. Wdrażanie SMS, w tym wskazówki dla każdego podejścia fazowego, jest omówione w paragrafie 5.5.

5.4.5. Wskaźniki działania bezpieczeństwa

5.4.5.1. SMS definiuje to jakie mają być mierzalne wartości wyjściowe, po to by określić czy system rzeczywiście działa według oczekiwań projektu, a nie tylko spełnia wymagania legislacyjne. Do monitorowania znanego ryzyka i do wykrywania nowego występującego ryzyka, oraz do określania ewentualnych akcji korekcyjnych, używa się wskaźników działania bezpieczeństwa.

5.4.5.2. Wskaźniki dotyczące bezpieczeństwa dostarczają legislatorowi obiektywnych dowodów, by ocenił skuteczność SMS dostawcy usług i monitorował osiągnięcie celów w sferze bezpieczeństwa. Wskaźniki działania bezpieczeństwa u dostawcy usług uwzględniają czynniki takie jak tolerancja ryzyka dotycząca bezpieczeństwa, koszt/korzyść wdrożenia ulepszeń w system, wymogi przepisów, oraz oczekiwania opinii publicznej. Wskaźniki działania bezpieczeństwa powinny być wyselekcjonowane i opracowane w konsultacji z władzą legislacyjną nad dostawcą usług. Taki proces jest konieczny, by ułatwić prawodawcy scalenie i zharmonizowanie posiadanych przez dostawcę usług wskaźników działania bezpieczeństwa z tym samym sektorem lotnictwa.

5.4.5.3. Wskaźniki działania bezpieczeństwa i związane z nimi cele powinny uzyskać akceptację Państwa, które dostawca usług autoryzował, certyfikował lub wyznaczył. Wskaźniki działania bezpieczeństwa są uzupełnieniem wszystkich wymogów prawnych oraz przepisów i nie zwalniają dostawców usług z zobowiązań zawartych w przepisach.

5.4.5.4. W praktyce, działanie bezpieczeństwa SMS jest wyrażane przez wskaźniki działania bezpieczeństwa i przez odpowiadające im wartości alarmowe i docelowe. Dostawca usług powinien monitorować działanie aktualnych wskaźników w kontekście trendów z przeszłości, po to by identyfikować wszelkie nienormalne zmiany w działaniu bezpieczeństwa. Podobnie, ustawienia docelowe i alarmowe powinny uwzględniać działanie danego wskaźnika w nieodległej przeszłości. Pożądane cele poprawy powinny być dla dostawcy usług i odpowiedniego sektora lotnictwa realistyczne i osiągalne.

5.4.5.5. Z perspektywy monitorowania ryzyka, ustanowienie dla wskaźnika bezpieczeństwa poziomu alarmowego ma sens. Poziom alarmowy konkretnego wskaźnika bezpieczeństwa jest powszechnym kryterium rozgraniczania obszarów działania akceptowalnego od nieakceptowalnego. Według podstawowych podręczników metrologii bezpieczeństwa, podstawową obiektywną metodą nastawiania niesterowalnych kryteriów alarmowych (OOC) jest zastosowanie zasady odchylenia standardowego. Ta metoda uwzględnia, dla danego wskaźnika bezpieczeństwa, odchylenie od standardu i średnie wartości punktów danych historycznych. Te dwie wartości zostają wówczas wykorzystane do ustanowienia dla wskaźnika na jakim poziomie ma być alarm monitorowany przez następny okres.

5.4.5.6. Pewien asortyment wskaźników dużych konsekwencji, jak również małych konsekwencji daje bardziej całościowy wgląd w działanie bezpieczeństwa u dostawcy usług. A to daje pewność zajęcia się danymi wyjściowymi (duże konsekwencje, np. wypadki i poważne incydenty), jak również wydarzeniami o małych konsekwencjach (np. incydenty, raporty o nieprzestrzeganiu, odchylenia). Wskaźniki działania bezpieczeństwa są w swej istocie wykresami trendów danych (trending charts), które idą śladem zdarzeń, wyrażając je liczbowo (np. liczbą incydentów na 1 000 godzin lotu). W pierwszej kolejności należy się zająć wskaźnikami dużych konsekwencji, a wskaźniki konsekwencji małych można opracować w bardziej dojrzałej fazie wdrażania SMS.

5.4.5.7. Po zdefiniowaniu wskaźników działania bezpieczeństwa i odpowiadających im celów i poziomów alarmowych, wynik każdego wskaźnika działania bezpieczeństwa powinien być regularnie uaktualniany i monitorowany. Aby zorientować się w stanie bezpieczeństwa, można tropić poziom docelowy i alarmowy każdego wskaźnika. Skonsolidowane zestawienia docelowych i alarmowych danych wyjściowych pakietu wskaźników działania bezpieczeństwa można także skompilować/złączyć za dany okres monitorowania. Za każdy osiągnięty cel i za każdy nieprzekroczony poziom można przyznać wartości ilościowe zadowalająca/niezadowalająca. Alternatywnie, aby dostarczyć miarę ilościową dla całego działania pakietu wskaźników, można użyć wartości liczbowych (punkty). Przykłady działania wskaźników bezpieczeństwa i kryteria dla celów i poziomów alarmowych są podane w Dodatku 6 do tego rozdziału.

5.5. WDRAŻANIE FAZOWE

5.5.1. Ogólnie

5.5.1.1. Celem tego paragrafu jest przedstawienie przykładu czterech faz wdrażania SMS. Wdrażanie SMS jest procesem systematycznym. Mimo to, ten proces może być zadaniem będącym sporym wyzwaniem, zależnie od czynników takich jak osiągalność materiałów wytycznych i zasobów potrzebnych dla wdrażania, a także do wcześniejszej wiedzy dostawcy usług o procesach i procedurach SMS.

5.5.1.2. Argumenty za fazowym podejściem do wdrożenia SMS obejmują:

a) zapewnienie szeregu wykonywalnych kolejno stopni wdrażania SMS, w tym przydziału zasobów;

b) potrzebę dopuszczenia do tego, by wdrażanie elementów ramy SMS odbywało się w różnych kolejnościach, zależnie od rezultatów analizy luk u każdego dostawcy usług;

c) początkową dostępność danych i procesów analitycznych, na wsparcie reaktywnych, proaktywnych i przewidywalnych praktyk zarządzania bezpieczeństwem; oraz

d) potrzebę by proces był metodyczny, co zapewni, że wdrożenie SMS będzie skuteczne i trwałe.

5.5.1.3. Podejście fazowe bierze pod uwagę to, że wdrożenie w pełni dojrzałego SMS jest procesem wieloletnim. Wdrażanie fazami pozwala na umacnianie się SMS wraz z zakończeniem każdej fazy wdrażania. Fundamentalne procesy zarządzania bezpieczeństwem kończą się zanim przejdzie się do kolejnych faz, wymagających większej złożoności.

5.5.1.4. Proponuje się dla SMS cztery fazy wdrażania. Każda faza jest związana z różnymi elementami (lub pod-elementami), jak wg ramy ICAO SMS. Jest oczywiste, że poszczególna konfiguracja elementów w tym materiale wytycznym nie jest uważana za ostateczną. Państwa i dostawcy usług mogą postanowić dokonać zmian jakie uznają za odpowiednie dla danych okoliczności. Zestawienie czterech faz wdrażania SMS i odpowiadających im elementów jest pokazane w Tabeli 5-2.

5.5.2. Faza 1

5.5.2.1. Celem wdrożenia pierwszej fazy SMS jest dostarczenie wzorca tego jak wymagania będą spełniane i integrowane w systemy kontrolne organizacji, jak również dostarczenie ramy odpowiedzialności za wdrażania SMS.

5.5.2.2. Podczas Fazy nr 1, ustanawiane jest podstawowe planowanie i przydzielane są zakresy odpowiedzialności. Głównym elementem Fazy nr 1 jest analiza luk. Z analizy luk może organizacja określić stan swych aktualnych procesów zarządzania bezpieczeństwem i może zacząć planować opracowywanie dalszych procesów zarządzania bezpieczeństwem. Znaczącym wynikiem Fazy nr 1 jest plan wdrażania SMS.

5.5.2.3. Na zakończenie Fazy nr 1, powinny zostać sfinalizowane następujące działania w sposób, który spełnia oczekiwania władz nadzorujących lotnictwo cywilne, jak wyłożono w odpowiednich wymogach materiału wytycznego.

Angażowanie się kierownictwa i zakres obowiązków — Element 1.1 (i)

a) przypisać dyrektorowi odpowiedzialnemu i kierownikom zakresy obowiązków w sferze bezpieczeństwa. Ta czynność ma oparcie w Elementach 1.1 oraz 1.2 ramy ICAO SMS.

b) Powołać zespół ds. wdrożenia SMS. Zespół powinien składać się z przedstawicieli odpowiednich wydziałów. Rolą zespołu jest wdrażanie SMS od etapu planowania po końcowe wdrożenie. Inne funkcje zespołu wdrożeniowego będą obejmować, ale nie będą ograniczone do:

    1) opracowania planu wdrożenia SMS;

    2) zapewnienia adekwatnego szkolenia na SMS i technicznej fachowości zespołu dla skutecznego wdrażania elementów SMS i procesów pokrewnych; oraz

    3) monitorowania i raportowania postępów we wdrażaniu SMS, zapewniającego regularne uaktualnienia oraz koordynację z dyrektorem odpowiedzialnym za SMS.

c) Zdefiniować zakres działań organizacji (wydziałów/oddziałów), do których SMS będzie miał zastosowanie. Zakres zastosowania SMS organizacji trzeba będzie później opisać w dokumentacji SMS. Ta czynność ma oparcie w Elemencie 1.5 ramy ICAO SMS. Wskazówki dotyczące opisu systemu są w paragrafie 5.4.1 tego rozdziału.

d) Przeprowadzić analizę luk w bieżących systemach organizacji i w procesach mających związek z wymogami ramy ICAO SMS (lub odpowiednimi wymogami legislacyjnymi wobec SMS). Wskazówki dotyczące analizy luk SMS danego dostawcy usług są w Dodatku 7 do tego rozdziału.

Tabela 5-2. Cztery fazy wdrażania SMS

Faza nr 1 (12 miesięcy)*	*Faza nr 2 (12 miesięcy)*	*Faza nr 3 (18 miesięcy)*	*Faza nr 4 (18 miesięcy)*
1. SMS Element 1.1 (i): a) wskazać dyrektora personalnie odpowiedzialnego za SMS; b) powołać zespół ds. wdrażania SMS; c) zdefiniować zakres SMS; d) wykonać analizę luk w SMS. 2. SMS Element 1.5 (i): a) opracować plan wdrażania SMS. 3. SMS Element 1.3: a) ustanowić kluczową osobę/biuro z odpowiedzialnością za administrowanie i utrzymywanie SMS. 4. SMS Element 4.1 (i): a) ustanowić program szkoleniowy SMS dla personelu, dający pierwszeństwo zespołowi wdrażającemu SMS. 5. SMS Element 4.2 (i): a) zainicjować komunikacyjne/ SMS kanały bezpieczeństwa.	1. SMS Element 1.1 (ii): a) ustanowić politykę bezpieczeństwa i średnio odległe cele. 2. SMS Element 1.2: a) zdefiniować zakresy odpowiedzialności za bezpieczeństwo, także odpowiedzialności personalne we wszystkich odnośnych działach organizacji; b) ustanowić w systemie SMS mechanizm/zespół ds. koordynacji bezpieczeństwa; c) ustanowić SAG, gdzie się da - wydziałowe/oddziałowe grupy akcji na rzecz bezpieczeństwa; 3. SMS Element 1.4: a) ustanowić plan reagowania na sytuacje awaryjne. 4. SMS Element 1.5 (ii): a) zainicjować progresywne opracowywanie dokumentacji /podręcznika SMS i innej dokumentacji pomocniczej.	1. SMS Element 2.1 (i): a) ustanowić procedurę dobrowolnego raportowania zagrożeń. 2. SMS Element 2.2: a) ustanowić procedury zarządzania ryzykiem dotyczącymi bezpieczeństwa. 3. SMS Element 3.1 (i): a) ustanowić procedury badania wydarzeń i ich raportowania; b) ustanowić system zbierania i przetwarzania danych o dużych konsekwencjach; c) opracować wskaźniki wysokopoziomowych konsekwencji (SPI) i związanych z nimi poziomów alarmowych i docelowych. 4. SMS Element 3.2: a) ustanowić zarządzanie procedurą zmian, które obejmuje proces zarządzania ryzykiem. 5. SMS Element 3.3 (i): a) ustanowić wewnętrzny program audytowania jakości; b) ustanowić zewnętrzny program audytowania jakości.	1. SMS Element 1.1 (iii): a) dopracować istniejącą procedurę dyscyplinarną/ politykę z należytym uwzględnieniem błędów niezamierzonych lub pomyłek, które nie są umyślne ani nie są naruszeniami rażącymi. 2. SMS Element 2.1 (ii): a) wprowadzić zagrożenia, zidentyfikowane w raportach z badania wydarzeń, do systemu dobrowolnego raportowania o zagrożeniach; b) zintegrować procedury zarządzania ryzykiem i identyfikowania zagrożeń z SMS podwykonawcy lub klienta, gdzie możliwe. 3. SMS Element 3.1 (ii): a) dopracować system zbierania i przetwarzania danych o bezpieczeństwie, tak by objął wydarzenia o mniejszych konsekwencjach; b) opracować wskaźniki niskopoziomowych konsekwencji (SPI) i związane z nimi poziomy alarmowe i docelowe. 4. SMS Element 3.3 (ii): a) ustanowić programy audytu SMS lub wstawić je do istniejącego programu wewnętrznego i zewnętrznego; b) ustanowić w SMS inne programy operacyjne do przeglądania/mierzenia. 5. SMS Element 4.1 (ii): a) dopilnować by program szkolenia SMS dla całego odpowiedniego personelu był przeprowadzony w całości. 6. SMS Element 4.2 (ii): a) promować wewnętrzne i zewnętrzne dzielenie się informacjami o bezpieczeństwie.
SMS Element 1.5: Dokumentacja SMS (Fazy 1 do 4) >>>			
SMS Element 4.1 oraz 4.2: Szkolenie dotyczące SMS, edukacja i komunikacja (Faza nr 1 dalsze) >>>>>>>>>>>>>>>>>>			
Uwaga 1.— Wskazany okres wdrożeniowy jest przybliżony. Rzeczywisty okres wdrożeniowy jest zależny od zakresu działań wymaganych dla każdego przydzielonego elementu i wielkości/złożoności organizacji. *Uwaga 2.— Numery elementów SMS odpowiadają numerom elementów w ICAO SMS. Przyrostki, takie jak a), b) oraz c) wskazują na to, że element został podzielony dla ułatwienia wdrażania fazowego.*			

Plan wdrażania SMS — Element 1.5 (i)

a) Opracować plan dotyczący, jak organizacja będzie wdrażać SMS na bazie - wynikających z przeanalizowania - zidentyfikowanych luk w systemie i w procesie. Przykład podstawowego planu wdrażania SMS jest w Dodatku 7 do tego rozdziału.

Powołanie kluczowego personelu — Element 1.3

a) Wskazać w organizacji kluczową dla SMS osobę (funkcja: bezpieczeństwo/jakość), która będzie odpowiadać za administrowanie SMS w imieniu dyrektora odpowiedzialnego.

b) Założyć biuro usług dotyczących bezpieczeństwa.

Szkolenie i edukacja - Element 4.1 (i)

a) Przeprowadzić analizę potrzeb szkoleniowych.

b) Zorganizować i sporządzić plan stosownych zajęć szkoleniowych dla personelu, przystosowany do ich indywidualnych odpowiedzialności i udziału w SMS.

c) Zorganizować szkolenie dotyczące bezpieczeństwa, z uwzględnieniem:

1) początkowe (bezpieczeństwo ogólne), szkolenie ukierunkowane na konkretne stanowisko pracy; oraz

2) szkolenia powtarzalne.

d) Rozpoznać koszty związane ze szkoleniem.

e) Ustanowić proces zatwierdzania szkolenia, który mierzy skuteczność szkolenia.

f) Założyć kartotekę szkolenia dotyczącą bezpieczeństwa.

Komunikacja dotycząca bezpieczeństwa — Element 4.2 (i)

a) Uruchomić odpowiedni mechanizm lub środek łączności do komunikowania się w sprawach bezpieczeństwa.

b) Ustanowić odpowiedni środek do przekazywania informacji o bezpieczeństwie za pomocą:

1) biuletynów okazjonalnych i regularnych, oraz ogłoszeń;

2) stron internetowych;

3) poczty elektronicznej (email).

5.5.3. Faza 2

Celem Fazy nr 2 jest wdrożenie zasadniczych procesów zarządzania bezpieczeństwem, jednocześnie korygując potencjalne niedostatki w istniejących procesach zarządzania bezpieczeństwem. W większości organizacji prowadzi się jakieś podstawowe działania w sferze bezpieczeństwa na różnych poziomach wdrożenia. Ta faza ma na celu skonsolidowanie istniejących działań i opracowanie tych, które jeszcze nie istnieją.

Zaangażowanie kierownictwa i zakres odpowiedzialności personalnych — Element 1.1 (ii)

a) Opracowanie polityki bezpieczeństwa.

b) Dyrektor odpowiedzialny podpisuje politykę bezpieczeństwa.

c) Komunikować politykę bezpieczeństwa po całej organizacji.

d) Ustalić harmonogram przeglądania polityki bezpieczeństwa po to by mieć pewność, że pozostaje ona dla organizacji istotną i odpowiednią.

e) Ustanowić dla SMS cele bezpieczeństwa poprzez opracowanie standardów dla działania bezpieczeństwa, w formie:

1) wskaźników działania bezpieczeństwa;

2) celów jakim ma służyć działanie bezpieczeństwa oraz poziomów alarmowych; oraz

3) planów akcji.

f) Ustanowić w SMS wymogi wobec podwykonawców:

1) ustanowić procedurę, by wymogi SMS wpisywać w proces zawierania kontraktów; oraz

2) ustanowić w dokumentacji przetargowej wymogi SMS.

Odpowiedzialność personalna za bezpieczeństwo — Element 1.2

a) Zdefiniować odpowiedzialności za bezpieczeństwo i rozpowszechnić je po całej organizacji.

b) Powołać grupę reagowania ds. bezpieczeństwa (SAG).

c) Powołać komisję/zespół ds. koordynacji bezpieczeństwa/SMS.

d) Zdefiniować wyraźnie funkcje (stanowiska) dla komisji/grupy SAG i komisji/zespołu ds. koordynacji bezpieczeństwa/SMS.

e) Ustanowić linie łączności między biurem usług dotyczących bezpieczeństwa, dyrektorem odpowiedzialnym, grupą SAG i komisją/zespołem ds. koordynacji bezpieczeństwa/SMS.

f) Powołać dyrektora odpowiedzialnego na przewodniczącego komisji/zespołu ds. koordynacji bezpieczeństwa/SMS.

g) Opracować, w miarę potrzeb, harmonogram zebrań biura usług dotyczących bezpieczeństwa z komisją/ zespołem ds. koordynacji i z grupą SAG, bezpieczeństwa/SMS.

Koordynacja planów reagowania awaryjnego — Element 1.4

a) Przejrzeć szkic ERP, dotyczący przekazywania władzy i nakładania odpowiedzialności w sytuacjach awaryjnych.

b) Ustanowić procedury koordynacyjne dla akcji wykonywanych przez kluczowy personel podczas sytuacji awaryjnej i podczas przywracania operacji do stanu normalnego.

c) Zidentyfikować podmioty zewnętrzne, które będą współredagować z organizacją/ przedsiębiorstwem w sytuacjach awaryjnych.

d) Ocenić programy ERP odpowiednich podmiotów zewnętrznych.

e) Ustanowić koordynację między poszczególnymi ERP.

f) Włączyć do dokumentacji SMS organizacji informacje korporacyjne o koordynacji między poszczególnymi ERP.

Uwaga.— Po dalsze wskazówki dotyczące ERP – patrz Dodatek 5.

Dokumentacja SMS — Element 1.5 (ii)

a) Utworzyć system dokumentowania SMS, aby opisywać, przechowywać, korzystać oraz archiwizować wszystkie informacje i zapisy dotyczące SMS, poprzez:

1) opracowanie dokumentu SMS, który jest albo samodzielnym podręcznikiem, albo jest wyróżnioną częścią w istniejącym podręczniku organizacji kontrolowanego (po wskazówki dotyczące opracowania podręcznika SMS patrz Dodatek 4);

2) ustanowienie kartoteki SMS na gromadzenie i przechowywanie zapisów dotyczących procesów będących w toku w organizacji;

3) przechowywanie zapisów by stanowiły materiał porównawczy i świadczyły o aktualnym stanie wszystkich procesów SMS, takich jak: rejestr zagrożeń (hazard register); wykaz ukończonych przeglądów bezpieczeństwa (index of completed safety assessments); dzienniki szkoleń na SMS/bezpieczeństwo (SMSS/safety training records); bieżące SPI i związane z nimi cele; raporty z wewnętrznych audytów SMS; protokoły z posiedzeń komisji/zespołu ds. SMS/bezpieczeństwa oraz plan wdrożenia SMS;

4) przechowywanie zapisów, które będą służyć jako dowody działania SMS i działań podczas wewnętrznego i zewnętrznego oceniania lub audytowania SMS.

5.5.4. Faza 3

Celem Fazy nr 3 jest ustanowić procesy zarządzania ryzykiem dotyczącym bezpieczeństwa. Pod koniec Fazy nr 3, organizacja będzie gotowa zbierać dane o bezpieczeństwie i wykonywać analizy oparte na informacjach uzyskanych przez różne systemy raportowania.

Identyfikowanie zagrożeń — Element 2.1 (i)

a) Ustanowić procedurę raportowania dobrowolnego. Po wskazówki, patrz Dodatek 5.

b) Ustanowić program/ harmonogram dla systematycznego przeglądania wszystkich odpowiednich procesów/sprzętu lotniczego, który kwalifikuje się do procesu HIRM.

c) Ustanowić proces dla oceniania zagrożeń i nadawania im kolejności łagodzenia.

Oceniania zagrożeń dotyczących bezpieczeństwa i ich łagodzenie — Element 2.2

a) Ustanowić procedurę zarządzania ryzykiem dotyczącym bezpieczeństwa, w tym jej zatwierdzenie i proces okresowego audytu.

b) Opracować i przyjąć matryce ryzyka dotyczących bezpieczeństwa, odpowiednie dla operacyjnych i produkcyjnych procesów organizacji.

c) Włączyć przyjęte matryce ryzyka dotyczących bezpieczeństwa oraz związane z nimi instrukcje, zawarte w SMS organizacji, lub materiały szkolenia zarządzaniem ryzyka.

Monitorowanie i mierzenie działania bezpieczeństwa — Element 3.1 (i)

a) Ustanowić procedurę raportowania i badania wydarzeń wewnątrz organizacji. Może ona obejmować raporty obowiązkowe lub raporty dotyczące poważniejszych usterek (MDR).

b) Ustanowić gromadzenie danych o bezpieczeństwie, a dane wyjściowe o dużych konsekwencjach poddawać przetwarzaniu i analizowaniu.

c) Ustanowić wskaźniki wysokopoziomowych konsekwencji dotyczących bezpieczeństwa (początkowy ALoSP) i związane z nimi poziomy alarmowe i docelowe. Przykładami wysokopoziomowych wskaźników konsekwencji dotyczących bezpieczeństwa jest liczba wypadków, poważnych incydentów oraz monitorowanie skutków będących konsekwencją nieprzestrzegania bezpieczeństwa. Po wskazówki dotyczące działania wskaźników bezpieczeństwa, patrz Dodatek 6.

d) Osiągnąć porozumienie z krajowym organem nadzorującym, dotyczące wskaźników działania i celów działania bezpieczeństwa.

Zarządzanie zmianami - Element 3.2

a) Ustanowić formalny proces zarządzania zmianami, który uwzględnia:

1) wrażliwość systemów i działań;

2) stabilność systemów i środowisk operacyjnych;

3) wyniki z przeszłości;

4) legislacyjne, branżowe i technologiczne zmiany.

b) Dopilnować - przed wdrożeniem nowych zmian - by zarządzanie procedurami zmian zajmowało się wpływem istniejących zapisów działania bezpieczeństwa i łagodzenia ryzyka.

c) Ustanowić procedury, które będą zapewniać, że zanim zostaną zamówione związane z lotnictwem nowe operacje, procesy i sprzęt, przeprowadzona będzie ocena ich bezpieczeństwa (lub że zostanie uznana za wystarczającą).

Ciągłe doskonalenie SMS - Element 3.3 (i)

a) Opracować formularze wewnętrznego oceniania.

b) Zdefiniować proces wewnętrznego audytu.

c) Zdefiniować proces zewnętrznego audytu.

d) Zdefiniować harmonogram oceniania urządzeń, sprzętu, dokumentacji i procedur, które mają być poddane audytom i pomiarom.

e) Opracować dokumentację dotyczącą zapewnienia bezpieczeństwa operacyjnego.

5.5.5. Faza 4

Faza nr 4 jest końcową fazą wdrażania SMS. Faza ta wymaga, by zarządzanie ryzykiem dotyczącym bezpieczeństwa, jak i zapewnianie bezpieczeństwa były wdrażane w sposób zaawansowany. W tej fazie, w celu utrzymania skuteczności kontroli ryzyk dotyczących bezpieczeństwa, zapewnianie bezpieczeństwa operacyjnego ocenia się poprzez wdrożenie okresowego monitorowania, poprzez informacje zwrotne i poprzez ciągłe działania korekcyjne.

Angażowanie się kierownictwa i odpowiedzialności - Element 1.1 (iii)

a) Dopracowanie istniejących procedur dyscyplinarnych/polityki, z należytym uwzględnieniem niezamierzonych błędów/pomyłek wynikających z umyślnych lub rażących naruszeń.

Identyfikacja zagrożeń — Element 2.1 (ii)

a) zintegrować zagrożenia, zidentyfikowane w sprawozdaniach z badań wydarzeń, z systemem raportowania dobrowolnego.

b) zintegrować procedury identyfikacji zagrożeń i zarządzania ryzykiem z SMS podwykonawcy lub klienta, tam gdzie jest to możliwe.

c) jeśli potrzeba, to opracować proces do priorytetyzowania zagrożeń zgromadzonych na łagodzenie ryzyka, na bazie obszarów o większych potrzebach lub wymagających większej troski. Po wskazówki, patrz Dodatek 3 do Rozdziału 2.

Monitorowanie poziomu bezpieczeństwa i pomiar - Element 3.1 (ii)

a) Rozwijać/ulepszać system zbierania i przetwarzania danych o bezpieczeństwie tak by objął wydarzenia skutkujące mniejszymi konsekwencjami.

b) Ustanowić wskaźniki mniejszych konsekwencji dotyczących bezpieczeństwa/jakości, z monitorowaniem docelowego/alarmowego poziomu (dojrzałe ALoSP).

c) Osiągnąć porozumienie z krajowym organem nadzorującym dotyczące niskopoziomowych wskaźników konsekwencji dla działania bezpieczeństwa i dotyczące docelowych/alarmowych poziomów działania bezpieczeństwa.

Ciągłe doskonalenie SMS - Element 3.3 (ii)

a) Ustanowić audyty dla SMS lub je wprowadzić do istniejących wewnętrznych i zewnętrznych programów audytorskich.

b) Ustanowić inne operacyjne programy audytorskie/mierzenia SMS, tam gdzie stosowne.

Szkolenie i edukacja — Element 4.1 (ii)

a) Zrealizuj cały program szkoleniowy SMS dla wszystkich odpowiednich pracowników.

Komunikacja w sprawach bezpieczeństwa — Element 4.2 (ii)

a) Ustanowić mechanizmy do promowania dzielenia się i wymieniania się informacjami o bezpieczeństwie wewnątrz i na zewnątrz organizacji.

5.5.6. Elementy SMS stopniowo realizowane po, w całych Fazach 1-4

We wdrażaniu fazowym, wdrażane są progresywnie na całym obszarze w każdej fazie, trzy kluczowe elementy:

Dokumentacja — Element 1.5

W miarę jak dojrzewa SMS, przedmiotowy podręcznik SMS oraz dokumentacja bezpieczeństwa musi być stosownie weryfikowana i uaktualniana. Takie działania muszą być na trwałe wpisane we wszystkie fazy wdrażania SMS i utrzymywane również po wdrożeniu.

Szkolenie i edukacja — Element 4.1 oraz Komunikacja dotycząca bezpieczeństwa — Element 4.2

Tak jak ważna jest dokumentacja SMS, szkolenie, edukacja i komunikacja dotycząca bezpieczeństwa, tak samo ważne są działania prowadzone we wszystkich fazach wdrażania SMS. W miarę jak ewoluuje SMS, mogą zacząć działać nowe procesy, procedury lub przepisy, bądź to mogą się zmienić istniejące procedury - po to by zadbać o wymogi SMS. Dla zapewnienia by te zmiany zostały skutecznie zrozumiane i wdrażane przez personel wykonujący obowiązki związane z bezpieczeństwem, sprawą żywotną jest to by szkolenie i komunikacja były nadal prowadzone przez cały okres wdrażania SMS, jak również po całkowitym wdrożeniu.

Dodatek 1 do Rozdziału 5
PODPISY ELEKTRONICZNE

Uwaga. — Ten Dodatek składa się z wyciągów z Okólnika Doradczego Federalnej Administracji Lotniczej (FAA) AC Nr: 120-78 „Przyjęcie i stosowanie podpisów elektronicznych, elektronicznych systemów przechowywania zapisów i elektronicznych podręczników/instrukcji" z dnia 29 października 2002.[3] Należy rozumieć, że poniższe informacje są zaledwie ilustracyjne i że nie są pomyślane jako restrykcyjne w jakikolwiek sposób. Ten Dodatek nie jest pomyślany jako jedyny komplet informacji potrzebnych do stosowania podpisów elektronicznych. W tym Dodatku nie ma niczego co by rzutowało na prawo Umawiających się Państw do opracowania i/lub stosowania własnych materiałów dotyczących podpisów elektronicznych.

1. Jaki jest cel niniejszego okólnika doradczego (AC)?

a) Niniejszy AC nie jest obowiązkowy i nie jest przepisem. Niniejszy AC zawiera wskazówki dotyczące akceptowania i stosowania podpisów elektronicznych tak by spełniać poszczególne wymagania operacyjne i obsługi technicznej. Ten AC dostarcza również wskazówek dotyczących akceptowania elektronicznych systemów przechowywania zapisów, elektronicznych podręczników obsługi technicznej, w tym podręczników procedur inspekcyjnych, zapewnienia jakości, instrukcji operacyjnych i podręczników szkoleniowych wymaganych przez Tom 14 (Title 14) Spisu Przepisów Federalnych (14 CFR).

b) Niniejszy AC opisuje sposób akceptowalny, ale nie jedyny, spełnienia wymagań operacyjnych i obsługowych FAA. Szczególnie, nadal są akceptowane odręczne podpisy, zapisy i pieczątki mechaników. Jeżeli jednak stosowalny jest opisany w AC elektroniczny środek, należy go stosować w każdym istotnym zakresie.

2. Kogo dotyczy niniejszy Okólnik Doradczy AC?

- Przewoźników lotniczych, na mocy części 121, 129, lub 135 Tomu nr 14 CFR
- Operatorów, na mocy części 91, 125, 133, lub 137 Tomu nr 14 CFR
- Osób dokonujących certyfikacji lotników, na mocy części 61, 63, 65, 141, lub 142 Tomu nr 14 CFR
- Osób wykonujących obsługę techniczną lub konserwacyjną, na mocy części 43 Tomu nr 14 CFR
- Baz obsługi technicznej, na mocy części 145 Tomu nr 14 CFR
- Szkół technicznych obsługi lotnictwa, na mocy części 147 Tomu nr 14 CFR

3. Definicje

. . .

d) **Podpis cyfrowy** [obejmuje] dane, wygenerowane jako zaszyfrowane, które identyfikują sygnatariusza dokumentu i potwierdzają, że dokument nie jest zmieniony. Technologia podpisu elektronicznego stanowi podstawę różnorodności zabezpieczeń, elektronicznej działalności gospodarczej i elektronicznego obrotu handlowego. Technologia jest oparta na powszechnym/prywatnym kluczu szyfrowania, technologii podpisu elektronicznego, która jest stosowana w bezpiecznym przekazywaniu wiadomości, infrastrukturze klucza publicznego (PKI), prywatnej sieci wirtualnej (VPN), internetowych standardach przeznaczonych dla zabezpieczania transakcji i cyfrowych podpisach elektronicznych.

e) **Podpis elektroniczny** [jest] internetowym odpowiednikiem podpisu odręcznego. Jest to elektroniczny sygnał, symbol lub proces podłączony do/lub logicznie powiązany z kontraktem lub innym zapisem i jest wykonany/ lub zaakceptowany przez osobę fizyczną. Identyfikuje w sposób elektroniczny i potwierdza autentyczność osoby, która poprzez komputer wprowadza zapisy, weryfikuje je lub dokonuje ich audytu. Podpis elektroniczny łączy w sobie szyfrograficzne funkcje podpisów cyfrowych z obrazem odręcznego podpisu osoby prywatnej lub z innym widocznym znakiem uznanym za akceptowalny w tradycyjnym procesie podpisywania. Podpis elektroniczny nadaje przesyłanym danym autentyczności poprzez użycie algorytmu hash (#) i zapewnia permanentne, bezpieczne potwierdzania autentyczności użytkownika.

. . .

[3] Pełen tekst FAA AC Nr: 120-78 można znaleźć na stronie internetowej FAA:
http://www.faa.gov/regulations_policies/advisory_circulars/index.cfm/go/document.information/documentID/23224

5. Czym jest akceptowalny podpis elektroniczny?

a) **Ogólnie.** Przed ostatnio dokonanymi zmianami zezwalającymi na stosowanie podpisów elektronicznych w jakimkolwiek wymaganym zapisie, wpisie lub dokumencie, stosowano podpisy odręczne. Cel podpisu elektronicznego jest identyczny jak podpisu odręcznego lub każdej innej formy podpisu, obecnie akceptowanej przez FAA. Podpis odręczny jest akceptowany uniwersalnie ponieważ ma pewne cechy i właściwości {np. poniższy podparagraf c(4)(d) dotyczący ustania umowy o zatrudnianiu}, które należy zachować w każdym podpisie elektronicznym. Dlatego, podpis elektroniczny powinien posiadać takie cechy i właściwości jakie gwarantują autentyczność podpisu odręcznego.

b) **Formy podpisów elektronicznych.**

1) Podpis elektroniczny może być w następującej formie:

- Podpisu cyfrowego
- Cyfrowego obrazu podpisu na papierze
- Zapisu niestandardowymi znakami graficznymi
- Kodu elektronicznego
- Każdej innej unikalnej formie identyfikacji osoby prywatnej, która może być użyta jako środek uwierzytelnienia autentyczności zapisu, wpisu lub dokumentu.

2) Nie wszystkie informacje identyfikujące, które się znajdują w systemie elektronicznym stanowią podpis. Na przykład, wpisanie nazwiska jakiejś osoby do systemu elektronicznego nie może stanowić podpisu elektronicznego. Trzeba zastosować jakieś inne gwarancje, równoważne podpisowi odręcznemu.

c) **Atrybuty akceptowalnego podpisu elektronicznego**. Po pierwsze i przede wszystkim, podpis elektroniczny musi być częścią dobrze zaprojektowanego programu. Jako minimum, taki program powinien uwzględnić:

1) **Unikalność**. Podpis elektroniczny powinien zachować właściwości podpisu odręcznego, co gwarantuje jego unikalność. Podpis powinien identyfikować konkretną osobę i być trudny do skopiowania. Wyjątkowość podpisu jest dowodem na to, że dana osoba zgadza się z tym, co podpisała. System elektroniczny nie zapewni identyfikacji jednostkowej z rozsądną dozą pewności, chyba że podszycie się pod tożsamość będzie dla nieupoważnionej osoby trudne.

2) **Istota, znaczenie**. Aby się podpisać, osoba posługująca się podpisem elektronicznym powinna podjąć działanie przemyślane i honorowane. Wykonanie akceptowalnych, celowych czynności dla utworzenia cyfrowego podpisu elektronicznego obejmuje, ale nie ogranicza się do:

- Przeciągnięcia identyfikatora przez czytnik
- Podpisania elektronicznego dokumentu rysikiem
- Wstukania kombinacji klawiszy
- Użycia podpisu cyfrowego.

3) **Zakres.** Zakres informacji potwierdzanej podpisem elektronicznym powinien być jasny dla sygnatariusza i kolejnych osób czytających zapis, wpis lub dokument. Dokumenty odręczne umieszczają podpis blisko informacji, by rozpoznać te elementy, które podpis zaświadcza. Dokumenty elektroniczne mogą jednak nie ustawiać podpisu w taki sam sposób. Dlatego, jest istotne, by wyraźnie oddzielić konkretne sekcje zapisu lub dokumentu, które podpis poświadcza, od partii tekstu, których podpis nie poświadcza. Akceptowalne metody oznaczania takich obszarów obejmują, ale nie są ograniczone do podświetlania, odwrócenia kontrastu ani do korzystania ze znaków marginesu lub znaków migających. Dodatkowo, system powinien powiadamiać sygnatariusza o tym, że się podpisał.

4) **Zabezpieczenie podpisu**. Zabezpieczeniem podpisu odręcznego danej osoby jest fakt, że dla innej osoby jest on trudny do skopiowania lub podrobienia. Podpis elektroniczny powinien utrzymywać równoważny poziom zabezpieczenia. System elektroniczny, który generuje podpisy, powinien ograniczać innym osobom podpisanie się za kogoś pod zapisem, wpisem bądź dokumentem…

5) **Niewypieranie się.** Podpis elektroniczny powinien uniemożliwiać danej osobie zaprzeczenia, że się podpisała pod konkretnym zapisem, wpisem bądź dokumentem. Im trudniej jest skopiować podpis, tym bardziej jest prawdopodobne, że podpis został utworzony przez sygnatariusza. Cechy zabezpieczające systemu, które innym utrudniają skopiowanie podpisów lub podrobienie dokumentów podpisanych, zazwyczaj zapewniają, że podpis był faktycznie złożony przez sygnatariusza….

6) **Wykrywalność.** Podpis elektroniczny powinien zapewnić pewne dotarcie do osoby, która podpisała zapis, wpis lub każdy inny dokument.

d) **Inne akceptowalne formy podpisywania/identyfikacji**. Choć niniejszy Okólnik Doradczy AC konkretnie zajmuje się podpisami elektronicznymi, inne typy podpisów, takie jak pieczątka mechanika, mogą również być akceptowane przez FAA. Jeżeli stosuje się identyfikację inną niż podpis odręczny, dostęp do takiej formy identyfikacji powinien być ograniczony tylko do osoby wymienionej.

e) **Spełnienie innych wymagań ustawowych**. Chociaż FAA dopuszcza obecnie stosowanie podpisów elektronicznych dla spełnienia pewnych wymagań operacyjnych i obsługowych FAA, to każde oprzyrządowanie stosowane do wygenerowania wymaganych dokumentów i zapisów nadal musi spełniać aktualne wymagania ustawowe. Podpis, prawidłowo złożony na nieprawidłowo utworzonych dokumentach nadal skutkuje tym, że dokument nie spełnia wymagań ustawowych. Metody i procedury stosowane do wygenerowania podpisu elektronicznego muszą zatem spełniać wszystkie wymagania ustawowe dla systemu przechowywania dokumentacji, który ma być używany przez właścicieli, operatorów lub techniczny personel obsługowy. Ponadto, podpisy elektroniczne należy wyłącznie stosować dla spełnienia wymagań obsługowych i operacyjnych związanych z niniejszym AC. Podpisy elektroniczne nie mogą być uważane za akceptowalne w innych obszarach objętych Tomem 14 CFR, który posiada specyficzne zastosowanie (np. oświadczenia składane pod przysięgą i różne inne wnioski). Choć akceptowanie podpisów elektronicznych będzie sprzyjać stosowaniu elektronicznych systemów dokumentacji, to aby spełniać aktualne wymagania ustawowe, FAA nadal akceptuje dokumenty w formie papierowej.

Dodatek 2 do Rozdziału 5
OPIS PRZYKŁADOWEGO STANOWISKA KIEROWNIKA BEZPIECZEŃSTWA

1. CEL OGÓLNY

Kierownik bezpieczeństwa jest odpowiedzialny przed dyrektorem wykonawczym za dostarczanie wytycznych i zaleceń dla planowania, wdrażania i działania systemu zarządzania bezpieczeństwem (SMS) organizacji. Kierownik bezpieczeństwa zapewnia usługi związane z SMS, dla obszarów certyfikowanych, niecertyfikowanych i dla obszarów stron trzecich organizacji, które są zamieszczone w SMS i które być może scedowały swe odpowiedzialności na osoby piastujące stanowiska przepisami wymagane.

2. ROLE KLUCZOWE

Zwolennik bezpieczeństwa (Safety advocate)

- wykazuje doskonałe zachowanie i postawę w sferze bezpieczeństwa, przestrzega praktyk legislacyjnych i zasad, rozpoznaje i raportuje zagrożenia oraz promuje skuteczne raportowanie bezpieczeństwa.

Przywódca (Leader)

- modeluje i promuje kulturę korporacyjną, która sprzyja praktykom dotyczącym bezpieczeństwa poprzez skuteczne przywództwo.

Komunikator (Communicator)

- działa jako kanał informacji, podający kwestie bezpieczeństwa do wiadomości kierownictwa i dostarczający pracownikom, kontrahentom i zainteresowanym stronom informacji na temat bezpieczeństwa.

Kreator (Developer)

- asystuje w ciągłym doskonaleniu schematów identyfikacji zagrożeń i procesie zarządzania ryzykiem dotyczącego bezpieczeństwa SMS organizacji.

Manager relacji międzyludzkich (Relationship builder)

- buduje i utrzymuje doskonałe stosunki pracy z grupą działań (SAG) na rzecz bezpieczeństwa organizacji oraz z biurem usług dotyczących bezpieczeństwa (SSO).

Ambasador

- reprezentuje organizację w komisjach rządowych, międzynarodowych organizacji i przemysłowych (np. ICAO, IATA, CAA, AIB itp).

Analityk

- analizuje dane techniczne dotyczące trendów związanych z zagrożeniami, wydarzeniami i zjawiskami.

Kierownik procesów (Process manager)

- dla wypełniania swych funkcji i zakresów odpowiedzialności, skutecznie spożytkowuje odpowiednie procesy i procedury;
- bada okazje zwiększania efektywności procesów;
- mierzy skuteczność jakości procesów i dąży do ciągłego ich ulepszania.

3. ZAKRES OBOWIĄZKÓW

Wśród innych obowiązków, kierownik bezpieczeństwa odpowiedzialny jest za:

- kierowanie działaniem systemu zarządzania bezpieczeństwem;
- punktualne zbieranie i analizowanie informacji dotyczących bezpieczeństwa;
- aplikowanie wszelkich, związanych z bezpieczeństwem, metod mierzenia - ankiet;
- monitorowanie i ocenianie rezultatów działań korekcyjnych;

- dopilnowywanie by przeprowadzano ocenę ryzyka, tam gdzie to możliwe;
- monitorowanie branży pod kątem zagrożeń dla bezpieczeństwa, które mogą rzutować na organizację;
- angażowanie się po stronie rzeczywistych odpowiedzi na sytuacje awaryjne;
- zaangażowanie się w opracowywanie i aktualizację procedur oraz planu reagowania awaryjnego;
- dopilnowywanie by informacje dotyczące bezpieczeństwa, w tym cele i zadania organizacji były udostępniane wszystkim pracownikom za pośrednictwem ustalonych procesów komunikacji.

4. CHARAKTER I ZAKRES OBOWIĄZKÓW

Kierownik bezpieczeństwa musi współdziałać z personelem operacyjnym, starszymi kierownikami i szefami wydziałów w całej organizacji. Kierownik bezpieczeństwa powinien również wspierać pozytywne relacje z władzami legislacyjnymi, agencjami oraz dostawcami produktów i usług spoza organizacji. Inne kontakty będą ustalane na poziomie roboczym w miarę potrzeb.

5. KWALIFIKACJE

Aby się nadawać na kierownika bezpieczeństwa trzeba mieć:

- pełnoetatowe doświadczenie w dziedzinie bezpieczeństwa lotniczego w charakterze badacza bezpieczeństwa lotniczego (investigator), kierownika bezpieczeństwa/jakości, lub kierownika ds. ryzyka dotyczącego bezpieczeństwa;
- solidną wiedzę dotyczącą operacji, procedur i działań organizacji;
- szeroką lotniczą wiedzę techniczną;
- szeroką znajomość systemów zarządzania bezpieczeństwem (SMS) i ukończone odpowiednie szkolenie SMS;
- rozumienie zasad zarządzania ryzykiem i sposobów wspierania SMS;
- doświadczenie we wdrażaniu SMS i-lub/ lub zarządzaniu SMS;
- doświadczenie i kwalifikacje do badania wypadków lotniczych/incydentów oraz czynnika ludzkiego;
- doświadczenie i kwalifikacje do przeprowadzania audytów oraz inspekcji bezpieczeństwa/jakości;
- solidną wiedzę z zakresu przepisów lotniczych, w tym norm ICAO i zalecanych metod postępowania (SARPs) oraz odpowiednich przepisów dla lotnictwa cywilnego;
- zdolność porozumiewania się na wszystkich poziomach zarówno wewnątrz, jak i na zewnątrz firmy;
- zdolność do obrony swoich przekonań, promowania kultury sprawiedliwej i uczciwej („just and fair culture") i tworzenia atmosfery otwartej na raportowanie bez konsekwencji karnych;
- zdolność komunikowania w zaufaniu swemu dyrektorowi odpowiedzialnemu, jako jego doradca i powiernik;
- dobrze rozwinięte umiejętności komunikacyjne i widoczne umiejętności interpersonalne wyższego rzędu, z umiejętnością współpracy z różnymi osobami i przedstawicielami organizacji, w tym z osobami z innych kręgów kulturowych;
- podstawową znajomość pracy na komputerze oraz najwyższe umiejętności analityczne.

6. WŁADZA

6.1. W kwestiach bezpieczeństwa, kierownik bezpieczeństwa ma bezpośredni dostęp do dyrektora odpowiedzialnego i kierownictwa wyższego i średniego szczebla.

6.2. Kierownik bezpieczeństwa jest władny, pod kierunkiem dyrektora odpowiedzialnego, do przeprowadzania audytów bezpieczeństwa, pomiarów i inspekcji w każdym aspekcie operacji, zgodnie z procedurami wyszczególnionymi w dokumentacji systemu zarządzania bezpieczeństwem.

6.3. Kierownik bezpieczeństwa jest uprawniony, pod kierunkiem dyrektora odpowiedzialnego, do prowadzenia dochodzeń wewnętrznych zdarzeń dotyczących bezpieczeństwa, zgodnie z procedurami wyszczególnionymi w dokumentacji SMS organizacji.

6.4. Kierownik bezpieczeństwa nie powinien piastować innych stanowisk ani posiadać obowiązków, które kłócą się lub utrudniają jego rolę jako kierownika SMS/kierownika bezpieczeństwa. Jego stanowisko powinno być stanowiskiem kierownika wyższego szczebla, nie niższe niż, ani nie podporządkowane stanowiskom z obszaru produkcyjnego w organizacji.

Dodatek 3 do Rozdziału 5
PLANOWANIE REAGOWANIA AWARYJNEGO

1. Być może dlatego, że wypadki lotnicze są rzadkością, niewiele organizacji jest przygotowanych na taką ewentualność. Wiele organizacji nie ma skutecznych planów zarządzania zdarzeniami w trakcie lub po sytuacji awaryjnej lub kryzysowej. To jak organizacja sobie radzi w następstwie wypadku lub innej sytuacji awaryjnej, może zależeć od tego, jak dobrze organizacja radzi sobie w ciągu kilku pierwszych godzin i dni po większym zdarzeniu dotyczącym bezpieczeństwa. Plan reagowania awaryjnego (ERP) podaje w zarysie, co należy zrobić po wypadku lub sytuacji awaryjnej w lotnictwie, a także wskazuje odpowiedzialność personalną kto jest odpowiedzialny za każdą przeprowadzoną akcję. U różnych dostawców produktów i usług, takie planowanie awaryjne może być znane pod różnymi określeniami, takimi jak plan na ewentualność nieprzewidzianego zdarzenia (contingency plan), plan zarządzania kryzysowego (crisis management) i plan wsparcia ciągłej zdatności do lotu (continuing airworthiness support plan). W tym podręczniku, na dany plan nieprzewidzianego zdarzenia, którego posiadania oczekujemy od dostawców usług lotnictwa i których produkty/usługi mogą rzutować na bezpieczeństwo lotnicze, używane jest określenie rodzajowe – plan reagowania awaryjnego (emergency response plan (ERP).

2. Choć istnieje tendencja myślenia o planowaniu reagowania awaryjnego, taka że przytrafiają się tylko operacjom z udziałem statku powietrznego lub na lotnisku, zazwyczaj na skutek wypadku samolotu, można równie dobrze oczekiwać takiego planowania od innych dostawców usług lotnictwa. W przypadku dostawców ATS, awaria może obejmować wyłącznie elektryczności lub utratę radaru, łączności lubi innych głównych elementów infrastruktury. Dla organizacji obsługi technicznej może to oznaczać poważne naruszenie wymogów zdatności do lotu, co skutkuje uziemieniem floty (AOG). Dla biura projektowego lub producenta samolotów, poważna wada projektowa może doprowadzić do globalnego AOG, co wymaga awaryjnego przeprojektowania, modyfikacji, produkcji i doposażenia (dyrektywy awaryjnej zdatności do lotu). Tam gdzie istnieje możliwość, że operacje lotnicze lub działania organizacji będą narażone na szwank przez inne kryzysy lub sytuacje awaryjne pochodzące ze źródeł zewnętrznych, jak zdrowie publiczne, zagrożenia chorobami, takie scenariusze powinna organizacja również odpowiednio uwzględnić w swoim lotniczym ERP. Stąd, ERP jest w istocie integralnym komponentem procedury zarządzania ryzykiem dotyczącym bezpieczeństwa w organizacji, który ma zająć się wszystkimi możliwymi awariami związanymi z bezpieczeństwem lub jakością, kryzysami lub wydarzeniami, gdyż produkty lub usługi organizacji mogą się przyczyniać do stworzenia sytuacji sprzyjającej ryzyku, lub kojarzenia się z nimi. ERP powinien zająć się wszystkimi możliwymi/prawdopodobnymi scenariuszami i powinien dawać odpowiednie działania łagodzące lub mieć takie procesy na miejscu, tak aby organizacja, jego klienci, społeczeństwo i/lub przemysł, mogli mieć lepszy poziom zapewniania bezpieczeństwa a także ciągłości usług.

3. Udana reakcja na sytuację awaryjną zaczyna się od skutecznego planowania. ERP daje podstawę dla stosowania systematycznego podejścia do zarządzania sprawami organizacji w następstwie znacznego nieplanowanego wydarzenia - w najgorszym wypadku, poważnego zdarzenia.

4. Celem planu reagowania awaryjnego jest zapewnienie:

   a) udzielenie władzy nad sytuacją awaryjną;

   b) przydzielenia odpowiedzialności w sytuacji awaryjnej;

   c) dokumentacji procedur i procesów w sytuacjach awaryjnych;

   d) koordynacji działań ratowniczych, wewnętrznie i z podmiotami zewnętrznymi;

   e) bezpiecznego kontynuowania działań zasadniczych podczas zajmowania się sytuacją awaryjną;

   f) proaktywnej identyfikacji wszystkich możliwych scenariuszy awaryjnych wydarzeń/scenariuszy i ich odnośnych działań łagodzących itp.

5. Aby ERP był skuteczny, powinien:

   a) być odpowiedni do wielkości, charakteru i złożoności organizacji;

   b) być łatwo dostępny dla wszystkich odpowiednich pracowników i innych organizacji;

   c) zawierać listy kontrolne i procedury odnoszące się do konkretnych sytuacji awaryjnych;

   d) posiadać dane kontaktowe odpowiednich pracowników;

   e) być regularnie testowany poprzez ćwiczenia;

   f) być okresowo przeglądany i uaktualniany, gdy zmieniają się detale itp.

Treść planu ERP

6. Normalnie, ERP będzie dokumentowany w formie podręcznika, który powinien przedstawiać zakresy odpowiedzialności, role i działania różnych agencji i personelu zaangażowanego w rozwiązywaniu konkretnych sytuacji awaryjnych. ERP powinien uwzględnić takie okoliczności jak:

a) *Obowiązujące koncepcje działań* (*Governing policies*). ERP powinien zapewnić kierunek reagowania na zagrożenia, takie jak obowiązujące prawa i przepisy dotyczące badań zdarzeń, porozumień z władzami lokalnymi, koncepcjami działań firmy i priorytety.

b) *Organizacja. (Organization*). ERP powinien dawać zarys intencji kierownictwa w odniesieniu do reagującej organizacji, poprzez:

1) określenie kto będzie przewodził i kto będzie przypisany do zespołów reagowania;

2) określenie ról i obowiązków pracowników przypisanych do zespołów reagowania;

3) wyjaśnienie po jakich liniach ma się odbywać raportowanie o zwierzchności;

4) utworzenie centrum zarządzania awaryjnego (EMC);

5) ustanowienie procedur dla przyjmowania dużej liczby próśb o informacje, zwłaszcza w ciągu pierwszych kilku dni po większym wypadku;

6) wyznaczenie rzecznika do kontaktów z mediami;

7) określanie jakie zasoby będą dostępne, w tym wskazanie władz finansowych dla działań natychmiastowych;

8) wyznaczenie przedstawiciela firmy do wszystkich formalnych badań podejmowanych przez urzędników krajowych;

9) ustalanie planu wydzwaniania do kluczowych pracowników.

Do przedstawiania, kto jaką ma funkcję w organizacji oraz jak się ze sobą komunikują, możliwe jest używanie schematu organizacyjnego.

c) *Powiadamianie (Notifications).* Plan powinien wyszczególniać, kto w organizacji powinien być powiadomiony o sytuacji awaryjnej, kto dokona powiadomień na zewnątrz i jakim sposobem. Należy rozważyć poniższe potrzeby powiadamiania:

1) zarządzających;

2) organów krajowych (poszukiwania i ratownictwa, organu legislacyjnego, zespołu ds. badania wypadków itp.);

3) lokalnych służb reagowania w sytuacjach awaryjnych (władze lotniskowe, straż pożarna, policja, pogotowie ratunkowe, agencje medyczne itp.);

4) krewnych ofiar (delikatna kwestia, ponieważ w wielu Państwach, tym zajmuje się policja);

5) personel firmy;

6) mediów; oraz

7) prawników, księgowych, ubezpieczycieli itp.

d) *Reakcja początkowa*. W zależności od okoliczności, do miejsca wypadku może być wysłany zespół reagowania początkowego by powiększyć zasoby lokalne i nadzorować interesy organizacji. Czynniki, które należy dla takiego zespołu uwzględnić:

1) Kto powinien przewodzić zespołowi reagowania początkowego?

2) Kto powinien być włączony do zespołu reagowania początkowego?

3) Kto powinien mówić w imieniu organizacji na miejscu wypadku?

4) Co byłoby wymagane, jeśli chodzi o specjalistyczny sprzęt, odzież, dokumentację, transport, zakwaterowanie itp.?

e) *Pomoc dodatkowa*. Pracownicy o odpowiednim przeszkoleniu i doświadczeniu mogą dać przydatne wsparcie podczas przygotowywania, realizowania i uaktualniania ERP organizacji. Ich fachowość może być przydatna w takich zadaniach planowaniu i realizowania, jako:

1) występujących w charakterze pasażerów i klientów w ćwiczeniach;

2) opiekunowie osób i stron trzecich, które przeżyły;

3) osoby kontaktujące się z najbliższymi rodzinami, władzami itd.

f) *Centrum zarządzania sytuacjami awaryjnymi (EMC).* Normalnie, EMC (w trybie oczekiwania) może być ustanowione w siedzibie organizacji, gdy tylko będą spełnione kryteria aktywacji. Dodatkowo, można ustanowić posterunek dowodzenia (CP) na miejscu awarii lub w pobliżu. ERP powinien zająć się tym jak mają być spełnione poniższe wymagania:

1) obsada (być może w początkowym okresie reakcji przez 24 godziny na dobę, 7 dni w tygodniu);

2) sprzęt łączności (telefony, faks, Internet itd.);

3) wymagania dotyczące dokumentacji, utrzymanie dzienników działań podczas zdarzeń awaryjnych;

4) konfiskata zapisów firmy nt. zdarzenia;

5) wyposażenie biurowe i materiały eksploatacyjne; oraz

6) dokumenty referencyjne (takie jak listy kontrolne i procedury reagowania w sytuacjach awaryjnych, podręczniki firmy, plany awaryjne lotnisk i spisy telefonów).

Usługi centrum kryzysowego mogą być zamawiane przez linie lotnicze lub inne organizacje specjalistyczne po to, by zadbać o interesy dostawcy usług w sytuacji kryzysowej poza bazą macierzystą. Normalnie, personel firmy wspomoże wynajęte centrum możliwie w jak najszybszy sposób.

g) *Zapisy.* Oprócz potrzeby organizacji prowadzenia dzienników wydarzeń i działań, od organizacji będzie się wymagać by dostarczała informacji do jakiegokolwiek państwowego zespołu dochodzeniowego. ERP powinien objąć następujące rodzaje informacji wymaganych przez badaczy:

1) wszystkie odpowiednie zapisy dotyczące danego produktu lub usługi;

2) wykazy punktów kontaktowych i wszelki personel mający związek z wydarzeniem;

3) notatki ze wszystkich wywiadów (i ich treść) z każdym kto miał związek z wydarzeniem;

4) wszelkie fotograficzne lub inne dowody.

h) *Miejsce wypadku.* Gdy wypadek jest poważny, przedstawiciele wielu władz mają uzasadnione powody, by posiadać dostęp do miejsca wypadku i zająć się ofiarami śmiertelnymi, na przykład: policji, straży pożarnej, ratownictwa medycznego, władz lotniskowych, patolodzy, badacze wypadków reprezentujący Państwo, agencje pomocy jak Czerwony Krzyż, a nawet media. Chociaż koordynacja działań tych zainteresowanych stron jest obowiązkiem policji Państwa i/lub organu prowadzącego postępowanie, dostawca usług powinien wyjaśnić następujące aspekty działań na miejscu wypadku:

1) powołanie wysokiej rangi przedstawiciela firmy na miejscu wypadku, jeżeli:

— w macierzystej bazie;

— z dala od bazy macierzystej;

— na morzu lub w państwie obcym;

2) zarządzanie dotyczące ofiar, które przeżyły;

3) potrzeby krewnych ofiar;

4) zabezpieczenie szczątków [samolotu];

5) postępowanie ze szczątkami ludzkimi i majątkiem osobistym osób zmarłych;

6) zachowanie dowodów [zdarzenia];

7) udzielanie pomocy (jeśli będzie wymagana) organom śledczym;

8) usunięcie i pozbycie się szczątków [samolotu] itd.

i) *Media.* To jak firma reaguje na media może mieć wpływ na to jak się firma podźwignie po wydarzeniu. Wymagany jest jasny kierunek, dotyczący na przykład tego*:*

1) jakie informacje są chronione przez ustawę (dane FDR, CVR i nagrania ATC, zeznania świadków itd.);

2) kto może wypowiadać się w imieniu organizacji w jego siedzibie i na miejscu wypadku (kierownik ds. kontaktów public relations manager, dyrektor naczelny lub inny Senior Executive, kierownik, właściciel);

3) kto przygotowuje oświadczenia jako odpowiedzi natychmiastowe na zapytania mediów;

4) akie informacje mogą być udostępnione (czego należy unikać);

5) po jakim czasie i jaka będzie treść wstępnego oświadczenia firmy;

6) kiedy media będą otrzymywać uaktualnienia dotyczące zajścia.

j) *Dochodzenia formalne*. Należy dostarczyć firmie wskazówek jak jej personel ma postępować z badaczami wypadku, którzy reprezentują Państwo i policję.

k) *Pomoc rodzinom.* ERP powinien również zawierać wytyczne dotyczące podejścia organizacji do pomagania ofiarom katastrofy lub organizacjom konsumenckim. Wytyczne te mogą obejmować takie rzeczy jak:

1) wymagania Państwa, by świadczyć usługi pomocowe;

2) załatwianie podróży i zakwaterowania osobom pragnącym przybyć na miejsce katastrofy;

3) poinformowanie kto jest koordynatorem programu oraz wskazanie punktu(ów) spotkaniowych z ofiarami/klientami;

4) udzielanie informacji najświeższych;

5) tymczasowa pomoc ofiarom lub klientom.

Uwaga.– Okólnik nr 285I CAO zawiera dalsze wytyczne dotyczące pomocy ofiarom wypadków samolotowych i ich rodzinom.

l) *Przegląd powypadkowy.* Trzeba podać wskazówkę, że po sytuacji awaryjnej, kluczowy personel ma przeprowadzić pełną odprawę i ma zarejestrować wszystkie istotne wnioski z ww. sytuacji, które mogą prowadzić do zmian w ERP i w związanych z nim procedurach*.*

Listy kontrolne

7. Każdy kto uczestniczył w początkowej fazie w dużym wypadku lotniczym będzie w jakimś stopniu cierpieć na pewien stopień dezorientacji. Dlatego proces reakcji na sytuację awaryjną uwzględnia zastosowanie listy kontrolnej. Takie listy kontrolne mogą stanowić integralną część podręcznika operacyjnego firmy lub podręcznika reagowania awaryjnego. Aby były skuteczne, listy kontrolne muszą być regularnie:

a) sprawdzane i aktualizowane (na przykład, aktualność spisu wzywania personelu przez telefon, i danych kontaktowych); oraz

b) testowane w realistycznych ćwiczeniach.

Szkolenia i ćwiczenia

8. ERP jest napisanym na papierze wskazaniem jaka jest jego intencja. Należy wyrazić nadzieję, że ERP nigdy nie będzie przetestowany w rzeczywistych warunkach. Aby zapewnić, że te intencje będą wspierane przez umiejętności operacyjne, wymagane jest szkolenie. Ponieważ szkolenie szybko się dezaktualizuje, wskazane są regularne ćwiczenia praktyczne i teoretyczne. Niektóre części EPR, takie jak wydzwanianie i plan łączności, mogą być przetestowane w klasie. Inne aspekty, takie jak działania na miejscu, wymagające udziału innych agencji/podmiotów, muszą być wykonywane w regularnych odstępach czasu. Takie ćwiczenia mają tę zaletę, że ukazują niedostatki w planie, więc mogą być usunięte przed rzeczywistą sytuacją awaryjną. W przypadku niektórych dostawców usług, takich jak lotniska, okresowe badanie adekwatności planu i przebiegu ćwiczeń sytuacji awaryjnych na pełną skalę mogą być obowiązkowe.

Dodatek 4 do Rozdziału 5
WSKAZÓWKA DOTYCZĄCA OPRACOWYWANIA PODRĘCZNIKA SMS

1. OGÓLNIE

1.1. Niniejszy Dodatek służy kierowaniu organizacji w ich opracowaniu podręczników (lub dokumentów) na najwyższym poziomie, aby określić ich ramy SMS i związane z nim elementy. Podręcznik może nie być z niczym połączony lub może być zintegrowany jako skonsolidowana część paragrafu/rozdziału SMS w stosownie zatwierdzonym podręczniku organizacji (np. podręcznika eksponującego organizację lub podręcznika firmy). Rzeczywista konfiguracja może zależeć od oczekiwań prawodawcy.

1.2. Użycie sugerowanego formatu oraz akapitów treści tego Dodatku i zaadaptowanie ich jako właściwych jest jednym ze sposobów dzięki któremu organizacja może opracować własny podręcznik SMS na najwyższym poziomie. Rzeczywiste akapity treści będą zależeć od konkretnej ramy SMS i elementów organizacji. Opis pod każdym elementem będzie współmierny do zakresu i złożoności procesów SMS organizacji.

1.3. Podręcznik będzie służyć skomunikowaniu ramy SMS organizacji wewnętrznie, jak również z właściwymi organizacjami zewnętrznymi. Podręcznik może podlegać poparciu lub zatwierdzeniu przez krajowy CAA na dowód zaakceptowania SMS.

Uwaga.- Trzeba dokonać rozgraniczenia pomiędzy podręcznikiem SMS a wspierającymi go zapisami operacyjnymi. To drugie dotyczy zapisów historycznych i bieżących oraz dokumentów generowanych podczas wdrażania SMS i działania jego rożnych procesów. Jest to dokument dowodowy, iż SMS organizacji działa.

2. FORMAT PODRĘCZNIKA SMS

2.1. Podręcznik SMS może być sformatowany w sposób następujący:

a) nagłówek paragrafu;

b) cel;

c) kryteria;

d) dokumenty porównawcze.

2.2. Pod każdym nagłówkiem jest opis „celu" danego paragrafu, po którym następuje jego „kryterium" i „dokumenty porównawcze". Celem jest to co organizacja zamierza osiągnąć robiąc to co jest opisane w danym paragrafie. Słowo kryteria definiuje zakres tego, co powinno się uwzględnić podczas pisania tego paragrafu. Dokumenty porównawcze przyłączają informacje do innych odpowiednich podręczników SOP organizacji, zawierających szczegóły elementu procesu, jeśli ma to zastosowanie.

3. TREŚĆ PODRĘCZNIKA

3.1. Zawartość podręcznika może zawierać następujące sekcje:

1. Kontrola dokumentów;
2. Wymogi legislacyjne wobec SMS;
3. Zakres i integracja systemu zarządzania bezpieczeństwem;
4. Polityka bezpieczeństwa;
5. Cele bezpieczeństwa;
6. Zakresy odpowiedzialności za bezpieczeństwo i kluczowy personel;
7. Raportowanie dotyczące bezpieczeństwa i akcje zaradcze;
8. Identyfikacja zagrożeń i ocena ryzyka;
9. Monitorowanie bezpieczeństwa i pomiarów;
10. Dochodzenia związane z bezpieczeństwem i działania zaradcze;
11. Szkolenia w sferze bezpieczeństwa i komunikacji;
12. Ciągłe ulepszanie i audyt SMS;

13. Zarządzania rejestrami SMS;

14. Zarządzanie zmianami; oraz

15. Plan reagowania awaryjnego/przypadki.

3.2. Poniżej jest przykład rodzaju informacji, które mogą być włączone w każdy paragraf za pomocą formatu określonego w pkt 2.2.

1. Kontrola dokumentów

Cel

Opisać jak podręcznik będzie na bieżąco aktualizowany i jak organizacja zapewni, by wszyscy pracownicy pełniący obowiązki związane z bezpieczeństwem posiadali jego najbardziej aktualne wydanie.

Kryteria

a) Wersja ostateczna lub kontrolowane media elektroniczne oraz lista dystrybucyjna.

b) Korelacja pomiędzy podręcznikiem SMS i innymi istniejącymi podręcznikami, takimi jak podręcznik kontroli obsługi technicznej (MCM) lub podręcznikiem operacyjnym.

c) Proces okresowej weryfikacji podręcznika i związanych z nim formularzy/dokumentów w celu zapewnienia ich stałej przydatności, adekwatności i skuteczności.

d) Proces rozdawania podręcznika, zatwierdzenia i legislacyjny proces akceptacji.

Dokumenty porównawcze

Podręcznik jakości, podręcznik techniczny itp.

2. Wymogi legislacyjne wobec SMS

Cel

Zająć się aktualnymi przepisami dotyczącymi SMS i materiałami wytycznymi dla uzyskiwania potrzebnych odniesień i zająć się tym, by wszyscy których one dotyczą byli ich świadomi.

Kryteria

a) Wyraźnie wyjaśnić obowiązujące przepisy/standardy dotyczące SMS. Wstawić ramy czasowe dla zgodności z nimi oraz uwzględnić odnośniki do materiałów pomocniczych.

b) W odpowiednich przypadkach, rozwinąć i wyjaśnić znaczenie i konsekwencje przepisów dla organizacji.

c) W odpowiednich przypadkach, ustanowić korelację z innymi wymaganiami dotyczącymi bezpieczeństwa lub standardów.

Dokumenty referencyjne

Odnośniki do przepisów/wymogów dotyczących SMS, odnośniki do dokumentów pomocniczych itp.

3. Zakres i integracja systemu zarządzania bezpieczeństwem

Cel

Opisać zakres i zasięg operacji lotniczych oraz obiektów organizacji, w obrębie których SMS będzie stosowalny. Należy się również zająć zakresem procesów, urządzeniami i operacjami, które zostaną uznane za kwalifikujące się do posiadanego przez organizację programu identyfikacji zagrożeń i zarządzania ryzykiem (HIRM).

Kryteria

a) Wyraźnie wyjaśnić charakter działań lotniczych organizacji i jego pozycji lub roli w branży jako całości.

b) Określić główne obszary, działy, warsztaty i urządzenia związane z organizacją/przedsiębiorstwem, w obrębie których będzie SMS miał zastosowanie.

c) Zidentyfikować główne procesy, operacje i sprzęt urządzenia, które są uznane za kwalifikujące się do programu HIRM organizacji, zwłaszcza te które są istotne dla bezpieczeństwa lotniczego. Jeśli zakres

procesów, operacji i urządzeń jest zbyt szczegółowy lub obszerny, może być kontrolowany w ramach dodatkowego dokumentu jako wygodniejszy.

d) Tam gdzie jest oczekiwanie, że będzie się SMS-em operować lub administrować w grupie ze sobą powiązanych organizacji lub wykonawców, trzeba zdefiniować i udokumentować takie zintegrowanie i związane z tym zakresy odpowiedzialności.

e) Gdy w organizacji są inne, skojarzone systemy kontrolowania/zarządzania, takie jak QMS, OSHE i SMS, trzeba rozpoznać jak są zintegrowane w lotniczym SMS.

Dokumenty referencyjne.

Podręcznik jakości, podręcznik techniczny itp.

4. Polityka bezpieczeństwa

Cel

Opisać intencje organizacji, zasady zarządzania i zaangażowanie się w poprawianie bezpieczeństwa lotniczego w odniesieniu do dostawców usług. Opis polityki bezpieczeństwa powinien być krótki, podobnym do oświadczenia jakim jest misja organizacji.

Kryteria

a) Polityka bezpieczeństwa powinna być dostosowana do wielkości i złożoności organizacji.

b) Polityka bezpieczeństwa stwierdza jakie są intencje organizacji, zasady zarządzania i zaangażowanie w ciągłe polepszanie bezpieczeństwa lotniczego.

c) Politykę bezpieczeństwa zatwierdza i podpisuje dyrektor odpowiedzialny.

d) Politykę bezpieczeństwa promuje dyrektor odpowiedzialny i wszyscy inni kierownicy.

e) Politykę bezpieczeństwa weryfikuje się okresowo.

f) W utworzenie i utrzymanie systemu zarządzania bezpieczeństwem angażuje się personel na wszystkich szczeblach.

g) Polityka bezpieczeństwa jest komunikowana wszystkim pracownikom z intencją, by byli świadomi swoich indywidualnych zobowiązań wobec bezpieczeństwa.

Dokumenty referencyjne

Polityka bezpieczeństwa OSHE, itd.

5. Cele bezpieczeństwa

Cel

Opisać jakie cele bezpieczeństwa ma organizacja. Cele bezpieczeństwa należy przedstawić w krótkim oświadczeniu, które opisuje w zarysie, co organizacja ma nadzieję osiągnąć.

Kryteria

a) Cele w zakresie bezpieczeństwa zostały ustalone.

b) Cele bezpieczeństwa wyraża się w formie oświadczenia najwyższego poziomu, opisującego zaangażowanie się organizacji w osiąganie bezpieczeństwa.

c) Istnieje formalny proces opracowywania spójnego zestawu celów bezpieczeństwa.

d) Cele bezpieczeństwa się upublicznia i rozprowadza.

e) Zasoby zostały przydzielone na osiąganie celów.

f) Cele bezpieczeństwa są związane ze wskaźnikami bezpieczeństwa po to, by ułatwić monitorowanie i pomiar w stosownych przypadkach.

Dokumenty referencyjne

Dokument dotyczący wskaźników działania bezpieczeństwa itp.

6. Role i obowiązki

Cel

Opisać organa bezpieczeństwa, zakresy obowiązków i odpowiedzialności personelu uczestniczącego w SMS.

Kryteria

a) Dyrektor odpowiedzialny jest odpowiedzialny za zapewnienie, by system zarządzania bezpieczeństwem był odpowiednio wdrażany i by działał zgodnie z wymaganiami we wszystkich obszarach organizacji.

b) Powołano odpowiedniego kierownika bezpieczeństwa (biuro), komisję bezpieczeństwa lub grupy akcji na rzecz bezpieczeństwa.

c) Zdefiniowane i udokumentowane zostały organy bezpieczeństwa, zakresy obowiązków i odpowiedzialności personelu na wszystkich poziomach organizacji.

d) Wszyscy pracownicy rozumieją swoje władze, zakresy obowiązków i odpowiedzialności za procesy zarządzania bezpieczeństwem, oraz za swoje decyzje i podejmowane działania.

e) Dostępny jest wykres odpowiedzialności za realizację SMS organizacji.

Dokumenty referencyjne

Podręcznik eksponujący firmę, podręcznik SPO, podręcznik administrowania, itp.

7. Raportowanie bezpieczeństwa

Cel

System raportowania powinien zawierać raporty zarówno reaktywne (raporty wypadków/incydentów itp.), jak i proaktywne oraz przewidywalne (raporty zagrożeń). Opisać odpowiednie systemy raportowania. Czynniki do rozważenia to: format raportu, poufność, adresaci, procedury badań/oceniania, działania korygujące/ zapobiegawcze oraz ich rozpowszechnianie.

Kryteria

a) Organizacja ma procedurę, która zapewnia wykrywanie zdarzeń wewnętrznych, w tym wypadków, incydentów i innych zdarzeń istotnych dla SMS.

b) Należy dokonać rozróżnienia pomiędzy obowiązkowymi raportami (wypadki, poważne incydenty, większe wady itd.), których zgłaszanie do krajowego CAA jest wymagane, a innymi rutynowymi raportami ze zdarzeń, które pozostają w organizacji.

c) Istnieje również system dobrowolnego i poufnego raportowania o zagrożeniach/zdarzeniach, który zawiera odpowiednią ochronę tożsamości/danych.

d) Poszczególne procesy raportowania są proste, dostępne i współmierne do wielkości organizacji.

e) Raportami zgłaszającymi duże konsekwencje i związanymi z nimi zaleceniami zajmuje się odpowiedni poziom zarządzania, który je przegląda.

f) Raporty są gromadzone w odpowiedniej bazie danych w celu ułatwienia sporządzenia niezbędnych analiz.

Dokumenty referencyjne

- - - - - - - - - - -

8. Identyfikacja zagrożeń i ocena ryzyka

Cel

Opisać system identyfikacji zagrożeń i jak są takie dane sortowane. Opisać proces kategoryzacji zagrożeń oraz ich kolejną priorytetyzację dla dokonania udokumentowanej oceny bezpieczeństwa. Opisać w jaki sposób prowadzony jest proces oceny bezpieczeństwa i jak wdrażane są plany działań prewencyjnych.

Kryteria

a) Zidentyfikowane zagrożenia są oceniane, priorytetyzowane i przetwarzane pod kątem oceny ryzyka.

b) Istnieje złożony proces oceny ryzyka, obejmujący kontrole oceniające nasilenie, prawdopodobieństwo, tolerancyjność i prewencję.

c) Procedury identyfikacji zagrożeń i oceny ryzyka skupiają się na bezpieczeństwie lotnictwa, będącym ich kontekstem fundamentalnym.

d) Proces oceny ryzyka wykorzystuje rozkładówki, formularze lub oprogramowanie odpowiednie do złożoności organizacji i wykonywanych operacji.

e) Dokonane oceny bezpieczeństwa są zatwierdzane przez odpowiedni poziom zarządzania.

f) Istnieje proces oceniania skuteczności opracowanych środków korekcyjnych, prewencyjnych i środków odzyskiwania opracowanych danych.

g) Istnieje proces okresowego przeglądania ukończonych ocen bezpieczeństwa i dokumentowanie ich wartości wyjściowych.

Dokumenty referencyjne

- - - - - - - - - - - - - -

9. Monitorowanie działania bezpieczeństwa i pomiary

Cel

Opisać komponent SMS, odpowiedzialny za monitorowanie działania bezpieczeństwa i pomiary. Obejmuje wskaźniki (SPI) efektywności bezpieczeństwa posiadanego przez organizację SMS.

Kryteria

a) Formalny proces opracowania i utrzymania zestawu wskaźników dotyczących bezpieczeństwa i związanych z nimi celów wydajności.

b) Ustanowiona korelacja pomiędzy wskaźnikami SPI i celami bezpieczeństwa organizacji, tam gdzie możliwe, a procesem akceptacji przepisów.

c) Proces monitorowania wyników tych SPI, w tym procedury działania akcji naprawczych, za każdym razem gdy się uruchomią nieakceptowalne lub trendy odbiegające od normy.

d) Wszelkie inne uzupełniające kryteria lub procesy SMS, lub monitorowania i mierzenia działania bezpieczeństwa.

Dokumenty referencyjne

- - - - - - - - - - - -

10. Badania dotyczące bezpieczeństwa i akcje naprawcze

Cel

Opisać jak wypadki/incydenty/zdarzenia są badane i przetwarzane w organizacji, także ich korelację z systemem identyfikacji zagrożeń i zarządzania ryzykiem SMS.

Kryteria

a) Procedury na zapewnienie by zgłoszone wypadki i incydenty były badane wewnętrznie.

b) Rozpowszechnianie wewnątrz organizacji ukończonych raportów z przeprowadzonych dochodzeń wewnętrznych, jak również przesyłanie do krajowej CAA, o ile jest wymagane.

c) Proces zapewniający, że podejmowane lub zalecane akcje korekcyjne zostały przeprowadzane oraz że służą ocenie wartości wyjściowych lub skuteczności.

d) Procedura dla dochodzenia dyscyplinarnego i działań związanych z wartościami wyjściowymi w raporcie z dochodzenia.

e) Jasno zdefiniowane warunki, na których byłyby rozpatrywane w postępowaniu dyscyplinarnym (np. nielegalna działalność, lekkomyślność, rażące niedbalstwo lub umyślne działanie szkodliwe).

f) Proces na zapewnienie, że badania obejmują identyfikację aktywnych awarii oraz ubocznych czynników i zagrożeń.

g) Procedura dochodzeniowa i jej format zapewniają, że ustalenia dotyczące czynników ubocznych lub zagrożeń pozostaną, tam gdzie jest to stosowne, a następnie będą przetworzone dla potrzeb dalszego ciągu akcji w systemie identyfikacji zagrożeń i zarządzania ryzykiem w organizacji.

Dokumenty referencyjne

- - - - - - - - - -

11. Szkolenie dotyczące bezpieczeństwa i komunikacji

Cel

Opisać rodzaj szkoleń SMS i inne szkolenia związane z bezpieczeństwem, które pracownicy otrzymują, oraz opisać proces zapewniający skuteczność szkoleń. Opisać jak są dokumentowane takie procedury szkoleniowe. Opisać jakie są w organizacji procesy/kanały komunikacji dotyczące bezpieczeństwa.

Kryteria

a) Dokumentuje się program szkoleniowy, wymagania i co musi pracownik sobą reprezentować, by mógł przystąpić do szkolenia.

b) Istnieje proces potwierdzający, który mierzy skuteczność szkolenia.

c) Istnieją kursy szkoleniowe wstępne, powtórzeniowe, i aktualizacyjne, wedug potrzeb.

d) Szkolenie w zakresie SMS organizacji jest częścią całości programu szkoleniowego organizacji.

e) Świadomość SMS jest włączona do programu zatrudniania lub indoktrynacji.

f) Procesy/kanały komunikacji dotyczące bezpieczeństwa w organizacji.

Dokumenty referencyjne

- - - - - - - - - - - - - -

12. Ciągłe ulepszanie SMS i audytu

Cel

Opisać proces ciągłego weryfikowania i ulepszania SMS.

Kryteria

a) Proces regularnego wewnętrznego audytowania/weryfikowania SMS organizacji dla zapewnienia jego stałej przydatności, adekwatności i skuteczności.

b) Opisać wszelkie inne programy przyczyniające się do ciągłego doskonalenia SMS organizacji oraz działania na rzecz bezpieczeństwa, np. MEDA, pomiary bezpieczeństwa, systemy ISO.

Dokumenty referencyjne

- - - - - - - - - - - - - -

13. Zarządzanie dokumentacją SMS

Cel

Opisać sposób przechowywania wszystkich dokumentów rejestrowanych i dokumentów związanych z SMS.

Kryteria

a) Organizacja posiada dokumentację SMS lub system ich archiwizacji, który zapewnia zachowanie dokumentacji wygenerowanej w związku z wdrażaniem i stosowaniem SMS.

b) Zapisy, które mają być przechowywane to raporty zagrożeń, raporty dotyczące z oceny ryzyka, notatki grupy ds. akcji dotyczących bezpieczeństwa/notatki z zebrań, karty wskaźników działania bezpieczeństwa, raporty z audytów SMS i dzienniki kursów szkolenia dotyczące SMS.

c) Zapisy powinny dawać możliwość odszukania/prześledzenia wszystkich elementów SMS i powinny być dostępne dla rutynowego administrowania SMS, a także do potrzeb audytów wewnętrznych i zewnętrznych.

Dokumenty referencyjne

- - - - - - - - -

14. Zarządzanie zmianami

Cel

Opisać posiadany przez organizację proces zarządzania zmianami, który może rzutować na ryzyko dotyczące bezpieczeństwa i opisać jak takie procesy są integrowane w SMS.

Kryteria

a) Procedury na zapewnienie, że istotne zmiany w organizacji, lub zmiany operacyjne, obejmują każdy wpływ jaki mogą one mieć na istniejące ryzyko dotyczące bezpieczeństwa.

b) Procedury na zapewnienie, że zanim będzie wprowadzony nowy sprzęt lub procesy rzutujące na ryzyko dotyczące bezpieczeństwa, dokonana będzie stosowna ocena bezpieczeństwa.

c) Procedury na przeglądanie istniejących ocen bezpieczeństwa za każdym razem, gdy odbywają się zmiany w procesie lub sprzęcie związanym z bezpieczeństwem.

Dokumenty referencyjne

SPO firmy, dotyczący zarządzania zmianami, itp.

15. Plan reagowania awaryjnego/przypadki

Cel

Opisać intencje organizacji co do sytuacji awaryjnych, zajmowania się nimi i związanych z nimi kontroli powrotu do stanu normalnego. Plan reagowania awaryjnego może być dokumentem osobnym lub częścią podręcznika SMS.

Kryteria (na tyle na ile dają się zastosować w organizacji)

a) Organizacja ma plan na sytuacje awaryjne, który nakreśla role i odpowiedzialności na okoliczność większego incydentu, kryzysu lub wypadku.

b) Istnieje proces zawiadamiania, który obejmuje spis telefonów do obdzwonienia oraz proces wewnętrznej mobilizacji.

c) Organizacja ma układy z innymi agencjami w sprawie pomocy i świadczenia usług awaryjnych, w miarę potrzeb.

d) Organizacja ma procedury dla operacji działania w trybie awaryjnym.

e) Istnieje procedura na opiekuńcze nadzorowanie wszystkich osób, które ucierpiały i na zawiadomienie najbliższej rodziny.

f) Organizacja opracowała procedury postępowania z mediami i załatwiania spraw związanych z ubezpieczeniami.

g) Organizacja ma zdefiniowane odpowiedzialności w zakresie badania wypadków.

h) Wymóg zachowania dowodów, zabezpieczenie terenu zdarzenia i obowiązkowe/rządowe raportowanie jest jasno wyartykułowane.

i) Istnieje gotowość na sytuację awaryjną oraz szkolenie pracowników jak reagować.

j) Plan ewakuacji ludzi i sprzętu z niepełnosprawnego samolotu został opracowany przez organizację po skonsultowaniu z właścicielami samolotu/ sprzętu, operatorami lotnisk i z innymi agencjami według potrzeb.

k) Istnieje procedura rejestrowania czynności w trakcie reagowania na sytuację awaryjną.

Dokumenty referencyjne

Podręczniki ERP itp.

Dodatek 5 do Rozdziału 5
DOBROWOLNE I POUFNE SYSTEMY RAPORTOWANIA

(Patrz 5.3.42; 5.3.52; 5.3.66 do 5.3.73, 5.5.4, Element 2.1 a))

Uwaga. – Poniższa wskazówka bazuje na przykładzie zintegrowanej organizacji przewoźnika lotniczego i organizacje technicznej obsługi samolotów. Dla innych typów organizacji świadczących usługi, materiał ten może być dostosowywany do ich typu.

Posiadany przez organizację system dobrowolnego i poufnego raportowania powinien, jako minimum, określać:

a) cel systemu raportowania;

Przykład:

Kluczowym celem [nazwa organizacji] systemu dobrowolnego i poufnego raportowania jest uwydatnić bezpieczeństwo działań lotniczych naszej firmy poprzez gromadzenie raportów o rzeczywistych lub potencjalnych niedoskonałościach w zakresie bezpieczeństwa, które inaczej nie byłyby zgłoszone innymi kanałami. Raporty mogą dotyczyć zdarzeń, zagrożeń lub gróźb istotnych dla bezpieczeństwa naszych działań lotniczych. System nie eliminuje potrzeby formalnego raportowania wypadków i incydentów według SOP naszej firmy, a także składania obowiązkowych raportów z zdarzeń, do odpowiednich organów regulacyjnych.

[Nazwa systemu] jest systemem dobrowolnego, bezsankcyjnego, poufnego raportowania zdarzeń i zagrożeń, administrowanym przez [Nazwa wydziału/biura]. Zapewnia on kanał dla dobrowolnego, raportowania wydarzeń lub zagrożeń dotyczących działań lotniczych naszej organizacji, przy czym chroni tożsamość informatora.

Uwaga. – Ustanawiając taki system, organizacja będzie musiała swój system bezpieczeństwa pracy, zdrowia i środowiska (OSHE) zintegrować z systemem raportowania bezpieczeństwa w lotnictwie czy go wyłączyć. A to może zależeć od oczekiwań i wymagań odpowiednich władz lotnictwa i OSHE. Gdy w organizacji istnieje odrębny system raportowania OSHE, taki fakt powinien być wyraźnie zaznaczony w niniejszym paragrafie, by poprowadzić informatora, jeśli potrzeba.

b) zakres sektorów lotnictwa/obszarów objętych systemem;

Przykład:

[Nazwa systemu] obejmuje takie dziedziny, jak:

a) operacje lotnicze;

b) hangarowa obsługa samolotów;

c) warsztatowa obsługa komponentów;

d) techniczne zarządzanie flotą;

e) zarządzanie zapasami technicznymi;

f) planowanie inżynieryjne;

g) usługi techniczne;

h) zapisy techniczne;

i) obsługa liniowa (na płycie postojowej);

j) itp.

c) kto może sporządzić raport dobrowolny:

Przykład:

Jeśli należysz do któregokolwiek z tych obszarów operacyjnych, lub działów, możesz przyczynić się do poprawy bezpieczeństwa lotniczego poprzez [nazwa systemu], raporty dotyczące zdarzeń, zagrożeń lub gróźb związanych z poniższymi działaniami lotniczymi naszej organizacji:

a) personel kabiny pilotów i kabiny pasażerskiej;

b) kontrolerzy ruchu lotniczego;

c) licencjonowani inżynierowie samolotowi, technicy i mechaników;

d) pracowników obsługi technicznej, projektowania i produkcji organizacji;

e) operatorzy naziemnej obsługi pasażerów i bagażu;

f) pracownicy lotniska;

g) personel lotnictwa ogólnego;

h) itp.

d) kiedy sporządzić taki raport:

Przykład:

Raport należy sporządzić, gdy:

a) chcesz by inni dowiedzieli się o, i skorzystali na incydencie lub zagrożeniu lecz martwisz się czy twoja tożsamość będzie chroniona;

b) nie ma innej stosownej procedury ani kanału; oraz

c) wypróbowałeś inne procedury raportowania, lub kanały, ale przypadkiem przez ciebie zgłoszonym nie zajęto się.

e) jak są raporty procedowane:

Przykład:

[Nazwa systemu] zwraca szczególną uwagę na konieczność ochrony tożsamości informatora podczas przetwarzania wszystkich raportów. Każdy raport zostanie przeczytany i zatwierdzony przez kierownika. Kierownik może skontaktować się z informatorem, aby się upewnić, że rozumie charakter i okoliczności zgłoszonego zdarzenia/zagrożenia i/lub po to, by uzyskać niezbędne dodatkowe informacji i objaśnienia.

Gdy kierownik uzna, że otrzymane informacje są kompletne i komunikatywne, odpersonalizuje te informacje i wprowadzi ich dane do [Nazwa] bazy danych. Gdyby zaistniała konieczność poszukania jakichś danych u jakiejkolwiek strony trzeciej, wykorzystane będą tylko dane odpersonalizowane.

Formularz [Nazwa systemu], z odnotowaną datą zwrotu, zostanie ostatecznie zwrócony informatorowi. Kierownik będzie dążyć do zakończenia przetwarzania w ciągu 10 (dziesięciu) dni roboczych, jeśli nie będą potrzebne dodatkowe informacje. W przypadkach, gdy kierownik będzie potrzebować coś omówić z informatorem lub skonsultować się z jakąś osobą trzecią, więcej czasu może być potrzebne.

Jeśli kierownika nie będzie w biurze przez dłuższy czas, inny kierownik zajmie się raportem. Informatorzy mogą być spokojni, że każdy [nazwa systemu] raport będzie przeczytany i będzie załatwiany albo przez kierownika albo przez kierownika alternatywnego.

Dzielenie się informacjami dotyczącymi bezpieczeństwa, w obrębie firmy i ze społecznością lotniczą

Istotnymi, odpersonalizowanymi raportami i ich fragmentami można się dzielić w ramach firmy, jak również z zewnętrznymi zainteresowanymi stronami w dziedzinie lotnictwa, wedle uznania. To umożliwi wszystkim zainteresowanym pracownikom i działom w firmie, a także odpowiednim, zainteresowanym zewnętrznym osobom/podmiotom lotnictwa dokonać przeglądu własnych operacji i dać poparcie ulepszaniu bezpieczeństwa lotniczego jako całości.

Jeżeli zawartość w [nazwa systemu] raportu sugeruje sytuację lub stan, który stanowi bezpośrednie lub pilne zagrożenie dla bezpieczeństwa lotnictwa, raport będzie potraktowany priorytetowo i po odpersonalizowaniu będzie przekazany do odpowiednich organizacji lub organów tak szybko jak to możliwe, aby im umożliwić podjęcie niezbędnych działań w zakresie bezpieczeństwa.

f) kontaktowanie się z kierownikiem [nazwa systemu];

Przykład:
Zapraszamy do zatelefonowania do kierownika [nazwa systemu], aby zapytać o [nazwa systemu] lub poprosić o wstępną dyskusję z kierownikiem [nazwa systemu] przed sporządzeniem. Z kierownikiem i z kierownikiem alternatywnym można się kontaktować w godzinach biurowych od poniedziałku do piątku telefonując na numery:

Administrator [Nazwa systemu]	Administrator alternatywny
Pan	Pan .....
Tel .:	Tel .: .....

Dodatek 6 do Rozdziału 5
WSKAŹNIKI SMS DZIAŁANIA BEZPIECZEŃSTWA

1. Tabele od 5-A6-1 do 5-A6-4 (przykłady wskaźników bezpieczeństwa) podają przykłady krajowych wskaźników (SPI) łącznego działania bezpieczeństwa i odpowiadające im kryteria ustawiania poziomu alarmowego i docelowego. SMS SPI są widoczne na prawej stronie tabel. Odpowiednie kryteria poziomów alarmowych i docelowych dla każdego wskaźnika mają być przedstawiane tak jak pokazano. Wskaźniki SSP skuteczności bezpieczeństwa, po stronie lewej tabel, są pokazane po to, by wskazać niezbędną korelację pomiędzy wskaźnikami SMS i SSP. Wskaźniki SMS SPI powinny być opracowane przez dostawców usług w porozumieniu z odpowiednimi organizacjami regulacyjnymi swych Państw. Proponowane przez nich SPI będą musiały być w harmonii ze wskaźnikami bezpieczeństwa krajowego SSP; stąd konieczność uzyskania umowy/akceptacji.

2. Tabela 5-A6-5 (przykład wykresu działania wskaźnika bezpieczeństwa SMS) jest przykładem tego jak wygląda wykres wysokopoziomowego wskaźnika konsekwencji dotyczących bezpieczeństwa. W tym przypadku jest to liczba incydentów u operatora lotniczego, zgłoszonych/obowiązkowych. Wykres po lewej stronie pokazuje jaka była wydajność w roku poprzednim, a wykres po prawej stronie pokazuje będące w toku uaktualnienia roku bieżącego. Nastawa poziomu alarmowego bazuje na kryteriach odchyleń od standardowych, podstawowych miar bezpieczeństwa. Formuła arkusza Excel to: ”=STDEVP”. Dla potrzeb obliczenia odchylenia od standardu podręcznikowego, formułą jest:

$$\sigma = \sqrt{\frac{\sum(x \ -\mu)^2}{N}}$$

gdzie „X” jest wielkością każdego punktu danych. „N” jest liczbą punktów danych, a „μ” jest wielkością średnią wszystkich punktów danych.

3. Poziom docelowy jest pożądanym ulepszeniem procentowym (w tym przypadku 5%) powyżej średniej punktów danych roku poprzedniego. Wykres ten jest generowany przez arkusz danych, przedstawiony w Tabeli 5-A6-6.

4. Arkusz danych w Tabeli 5-A6-6 służy do generowania pokazanego w tabeli 5-A6-5 wykresu wskaźnika działania bezpieczeństwa. To samo można użyć do wygenerowania jakiegokolwiek innego wskaźnika działania bezpieczeństwa, wprowadzając odpowiednie dane i poprawienie deskryptora wskaźnika działania bezpieczeństwa.

5. Tabela 5-A6-7 (przykład sumarycznego działania SMS) podaje podsumowanie wskaźników bezpieczeństwa SMS wszystkich operatorów, z odnotowaniem wyników dla ich odnośnych poziomów docelowych i alarmowych. Takie zestawienie może być skompilowane na koniec każdego okresu monitorowania, aby zapewnić przegląd działania SMS. Jeśli pożądane jest zestawienie pomiaru bardziej ilościowego, to za każde docelowe i alarmowe dane wyjściowe można przydzielić każdemu wynikowi Tak/ Nie odpowiednie punkty. Przykład:

Wskaźniki wysokopoziomowych konsekwencji:

Nienaruszony poziom alarmowy [Tak (4), Nie (0)]

Osiągnięty cel [Tak (3), Nie (0)]

Wskaźniki niskopoziomowych konsekwencji:

Nienaruszony poziom alarmowy [Tak (2), Nie (0)]

Osiągnięty cel [Tak (1), Nie (0)]

To może dopuścić do uzyskania wyniku sumarycznego (w procentach), co będzie wskazywać jaka jest całościowa wydajność bezpieczeństwa SMS na koniec dowolnego okresu monitorowania.

Tabela 5-A6-1. Przykłady wskaźników działania bezpieczeństwa - dla przewoźników lotniczych

Wskaźniki bezpieczeństwa SSP (w całym Państwie)						*Wskaźniki osiągów bezpieczeństwa SMS (dostawca usług indywidualny)*					
Wskaźniki wysokopoziomowe (oparte na zdarzeniach/danych wyjściowych)			*Wskaźniki niskopoziomowe (oparte na wydarzeniach /działaniach)*			*Wskaźniki wysokopoziomowe (oparte na zdarzeniach/danych wyjściowych*			*Wskaźniki niskopoziomowe oparte na wydarzeniach/działaniach)*		
Wskaźnik bezpieczeństwa	*Kryteria poziomu alarmowego*	*Kryteria poziomu docelowego*	*Wskaźnik bezpieczeństwa*	*Kryteria poziomu alarmowego*	*Kryteria poziomu docelowego*	*Wskaźnik działania bezpieczeństwa*	*Kryteria poziomu alarmowego*	*Kryteria poziomu docelowego*	*Wskaźnik działania bezpieczeństwa*	*Kryteria poziomu alarmowego*	*Kryteria poziomu docelowego*
Operatorzy lotniczy (tylko operatorzy danego Państwa)											
Zbiorcza, miesięczna/ kwartalna ilość wypadków/ poważnych incydentów u przewoźników CAA, (np. na 1000 FH (godzin wylatanych)	Średnia +1/2/3 SD. (ustawienie roczne lub dwuletnie	__% (np. 5%) poprawy pomiędzy każdą roczną średnią wartością	%LEI lub inne wykrycia CAA w dorocznym audycie śledzenia operatorów (ilość wykryć per audyt)	Rozważane	Rozważane	Ilość poważnych incydentów, miesięcznie, we flocie danego przewoźnika (np. na 1000 FH)	Średnia +1/2/3 SD (ustawienie roczne lub dwuletnie)	___% (np. 5%) poprawy pomiędzy każdą, roczną średnią	Ilość incydentów, miesięcznie, w połączonej flocie danego przewoźnika (np. na 1000 FH)	Średnia +1/2/3 SD (ustawienie roczne lub dwuletnie)	__% (np. 5%) poprawy pomiędzy każdą roczną średnią
Ilość (zbiorczo) wypadków wyłączenia się silnika w locie (IFSD) u przewoźników CAA (np. na 1000 FH)	Średnia +1/2/3 SD (ustawienie roczne lub dwuletnie)	__%(np.5%) poprawy pomiędzy każdą roczną średnią	%LEI (zbiorczo) w dorocznej, inspekcjonowanej przez CAA obsłudze liniowej, lub ilość wykryć per inspekcja	Rozważane	Rozważane	Ilość poważnych incydentów, miesięcznie, w połączonej flocie danego przewoźnika (np. na 1000 FH)	Średnia +1/2/3 SD. (ustawienie roczne lub dwuletnie)	__%(np.5%) poprawy pomiędzy każdą roczną średnią	% LEI lub ilość odkryć w wewnętrznym rocznym audycie QMS/SMS przewoźnika (ilość odkryć per audyt)	Rozważane	Rozważanie
			Średni %LEI lub wielkości ustaleń CAA w dorocznej inspekcji śledzenia obcych przewoźników przy rampie (dla każdego zagranicznego operatora)	Rozważane	Rozważane	Ilość incydentów wyłączenia się silnika w locie (IFSD) u przewoźnika (np. na 1000 FH)	Średnia +1/2/3 SD (ustawienie roczne lub dwuletnie)	__%(np.5%) poprawy pomiędzy każdą roczną średnią	Ilość dobrowolnych raportów przewoźników o zagrożeniach (np. na 1000 FH)	Rozważanie	Rozważanie
			Zbiorcza ilość zgłoszonych do CAA incydentów DGR u przewoźników (np. 1000 FH)	Średnia + 1/2/3 SD (dorocznie lub 2-letnio)	__% (np.5%) poprawy pomiędzy każdą roczną średnią				Ilość zgłoszonych incydentów DGR przewoźników (np. na 1000 FH)		
Itd.											

Tabela 5-A6-2. Przykłady wskaźników działania bezpieczeństwa - dla operatorów lotnisk

Wskaźniki działania bezpieczeństwa SSP (Ogółem Państwo)						*Wskaźniki działania bezpieczeństwa SMS (indywidualny dostawca usług lotniczych)*					
Wskaźniki wysokopoziomowe konsekwencji (oparte na zdarzeniach/wynikach)			*Wskaźniki niskopoziomowe konsekwencji (oparte na zdarzeniach/działaniach)*			*Wskaźniki wysokopoziomowe konsekwencji (oparte na zdarzeniach/wynikach*			*Wskaźniki niskopoziomowe konsekwencji oparte na zdarzeniach/działaniach)*		
Wskaźnik bezpieczeństwa	*Kryteria poziomu alarmowego*	*Kryteria poziomu docelowego*	*Wskaźnik bezpieczeństwa*	*Kryteria poziomu alarmowego*	*Kryteria poziomu docelowego*	*Wskaźnik działania bezpieczeństwa*	*Kryteria poziomu alarmowego*	*Kryteria poziomu docelowego*	*Wskaźnik działania bezpieczeństwa*	*Kryteria poziomu alarmowego*	*Kryteria poziomu docelowego*
Operatorzy lotnisk											
CAA - zbiorcza miesięczna / kwartalna liczba wypadków na ziemi/ poważnych zdarzeń dotycząca każdego st. pow. ogółem CAA (na 10.000 ruchów naziemnych)	Średnia +1/2/3 SD (ustawienie roczne lub dwuletnie)	__%(np.5%) poprawy pomiędzy każdą średnią roczną	CAA - zbiorczo , liczba % LEI z wew. rocznego audytu lub niezgodności u operatora lotniska (ilość niezgodności na audyt)	Rozważanie	Rozważanie	Liczba, kwartalnie, wypadków na ziemi/ poważnych incydentów z udziałem wszystkich st. pow. u operatora lotniska (np. na 10.000 ruchów naziemnych)	Średnia +1/2/3 SD (wyciągana rocznie lub okresami dwuletnimi)	__% (np. 5%) poprawy pomiędzy każdą średnią roczną	Współczynnik LEI% wewnętrznego rocznego audytu QMS/SMS lub niezgodności u operatora lotniska (ilość niezgodności na audyt)	Rozważanie	Rozważanie
CAA - zbiorcza miesięczna / kwartalna liczba wypadnięcia z pasa startowego dotyczące każdego st. pow. (np. na 10.000 odlotów)	Średnia +1/2/3 SD (wyciągana rocznie lub dwuletnio)	__% (np.5%) poprawy pomiędzy każdą średnią roczną				Liczba, kwartalnie, wypadnięć z drogi startowej, dotycząca każdego st. pow. ogółem u operatora lotniska (np. na 10.000 ruchów naziemnych)	Średnia +1/2/3 SD (wyciągana rocznie lub dwuletnio)	__% (np. 5%) poprawy pomiędzy każdą średnią roczną	Współczynnik kwartalny zgłoszenia obcych przedmiotów na pasie startowym/zagrożenia odłamkami u operatora lotniska (np. na 10000 operacji naziemnych)	Rozważanie	Rozważanie
CAA - zbiorcza miesięczna / kwartalna liczba wypadnięcia z pasa startowego dotyczące każdego st. pow. (np. na 10.000 odlotów)	Średnia +1/2/3 SD (wyciągana rocznie lub dwuletnio)	___% (np. 5%) poprawy pomiędzy każdą średnią roczną				Liczba, kwartalnie, wtargnięć na drogę startową, dotycząca każdego st. pow. ogółem u operatora lotniska (np. na 10.000 ruchów naziemnych)	Średnia +1/2/3 SD (wyciągana rocznie lub dwuletnio)	_% (np.5%) poprawy pomiędzy każdą średnią roczną	Współczynnik dobrowolnych zgłoszeń zagrożenia u operatora lotniska	Rozważanie	Rozważanie
									Współczynnik kwartalny zgłoszenia obcych przedmiotów na pasie startowym/zagrożenia odłamkami u operatora lotniska (np. na 10000 operacji naziemnych)	Średnia +1/2/3 SD (ustawienie roczne lub dwuletnie)	-% (np. 5%) poprawy pomiędzy każdą roczną średnią
Itd.											

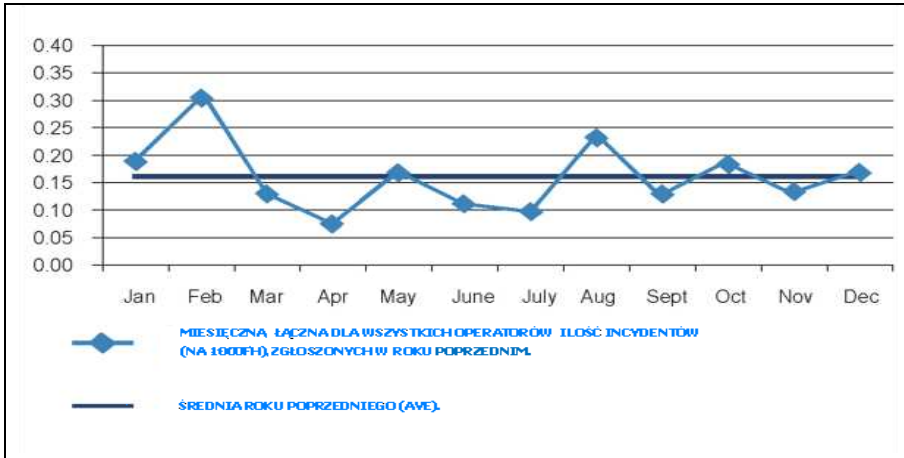
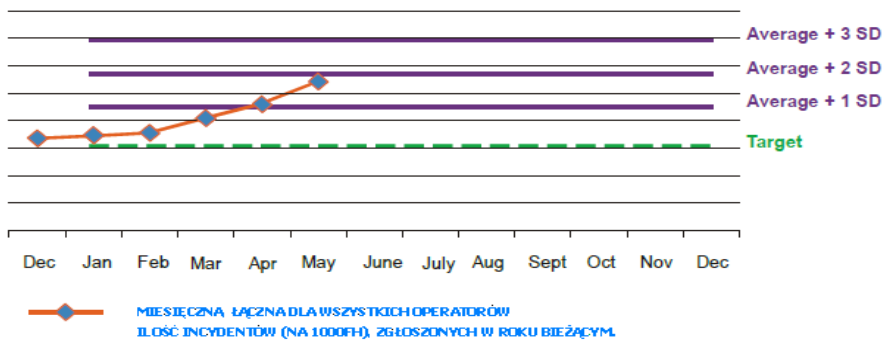
Tabela 5-A6-3. Przykłady wskaźniki działania bezpieczeństwa - dla operatorów ATS

Wskaźniki działania bezpieczeństwa SSP (Ogółem Państwo)						*Wskaźniki działania bezpieczeństwa SMS (indywidualny podmiot lotniczy)*					
Wskaźniki wysokopoziomowe konsekwencji (oparte na zdarzeniach/wynikach			*Wskaźniki niskopoziomowe konsekwencji (oparte na zdarzeniach/działaniach)*			*Wskaźniki wysokopoziomowe konsekwencji (oparte na zdarzeniach/wynikach*			*Wskaźniki niskopoziomowe konsekwencji (oparte na zdarzeniach/działaniach)*		
Wskaźnik bezpieczeństwa	*Kryteria poziomu alarmowego*	*Kryteria poziomu docelowego*	*Wskaźnik bezpieczeństwa*	*Kryteria poziomu alarmowego*	*Kryteria poziomu docelowego*	*Wskaźnik działania bezpieczeństwa*	*Kryteria poziomu alarmowego*	*Kryteria poziomu docelowego*	*Wskaźnik działania bezpieczeństwa*	*Kryteria poziomu alarmowego*	*Kryteria poziomu docelowego*
Operatorzy ATS											
Zbiorczo, kwartalnie, liczba poważnych zdarzeń ATS w FIR (w powietrzu) - dotyczący każdego st. pow. CAA (np. na 100.000 ruchów w locie)	Średnia +1/2/3 SD (wyciągana rocznie lub dwuletnio)	__% (np. 5%) poprawy pomiędzy każdą średnią roczną	Zbiorczo, kwartalnie, liczba incydentów ATS – z udziałem dowolnego statku. pow. w CAA FIR TCAS RA (np. na 100.000 ruchów w locie)	Średnia +1/2/3 SD (wyciągana rocznie lub dwuletnio)	__% (np. 5%) poprawy pomiędzy każdą średnią roczną	Zbiorczo, kwartalnie, liczba poważnych incydentów z udziałem dowolnych samolotów (np. na 100.000 ruchów w locie)	Średnia +1/2/3 SD (wyciągana rocznie lub dwuletnio)	__% (np. 5%) poprawy pomiędzy każdą średnią roczną	Współczynnik kwartalny ATS dla zdarzeń FIR TCAS RA dotyczący każdego st. pow (np. na 100000 operacji lotniczych)	Średnia +1/2/3 SD (ustawienie rocznie lub dwuletnie)	-% (np. 5%) poprawy pomiędzy każdą roczną średnią
			CAA FIR ATS- zbiorczo, kwartalnie, liczba nietrzymania poziomu / separacji LOS (np. na 100.000 ruchów w locie)	Średnia +1/2/3 SD (wyciągana rocznie lub dwuletnio)	__% (np. 5%) poprawy pomiędzy każdą średnią roczną	Liczba niebezp. zbliżeń statków pow. operatorów ATS kwartalnie/ rocznie (np. na 100.000 operacji lotniczych)	Przyjmując że historyczna średnia roczna wynosi 3, to ewent. liczba alarmowa mogłaby wynieść 5	Przyjmując że historyczna średnia roczna wynosi 3, to ewent. liczba alarmowa mogłaby wynieść 2	Współczynnik kwartalny ATS dla zdarzeń FIR level Bust (LOS)- dotyczący każdego st. pow (np. na 100000 operacji lotniczych)	Średnia +1/2/3 SD (ustawienie rocznie lub dwuletnie)	-% (np. 5%) poprawy pomiędzy każdą roczną średnią
			CAA- zbiorczy % LEI lub liczba ustaleń (niezgodności) per roczny audyt śledzenia u operatora ATS	Rozważanie	Rozważanie				Współczynnik LEI% wewnętrznego rocznego audytu QMS/SMS lub niezgodności u operatora ATS (ilość niezgodności na audyt)	Rozważanie	Rozważanie
Itd.											

Tabela 5-A6-4. Przykłady wskaźników działania bezpieczeństwa dla organizacji obsługi technicznej, produkcyjnych i projektowych (DOA/POA/MRO)

Wskaźniki działania bezpieczeństwa SSP (Ogółem Państwo)						*Wskaźniki działania bezpieczeństwa SMS (indywidualny podmiot lotniczy)*					
Wskaźniki wysokopoziomowe konsekwencji (oparte na zdarzeniach/wynikach			*Wskaźniki niskopoziomowe konsekwencji (oparte na zdarzeniach/działaniach)*			*Wskaźniki wysokopoziomowe konsekwencji (oparte na zdarzeniach/wynikach*			*Wskaźniki niskopoziomowe konsekwencji (oparte na zdarzeniach/działaniach)*		
Wskaźnik bezpieczeństwa	*Kryteria poziomu alarmowego*	*Kryteria poziomu docelowego*	*Wskaźnik bezpieczeństwa*	*Kryteria poziomu alarmowego*	*Kryteria poziomu docelowego*	*Wskaźnik działania bezpieczeństwa*	*Kryteria poziomu alarmowego*	*Kryteria poziomu docelowego*	*Wskaźnik działania bezpieczeństwa*	*Kryteria poziomu alarmowego*	*Kryteria poziomu docelowego*
Organizacje DOA/POA/MRO											
Zbiorczo, kwartalnie, ilość obowiązkowych zgłoszeń usterek (MDR) do CAA od MRO kwartalnych	Średnia +1/2/3 SD. (ustawienie roczne lub dwuletnie)	__% (np. 5%) poprawy pomiędzy każdą średnią roczną	Dla CAA –zbiorczo, %LEI lub liczba niezgodności (per audyt) wykazanych. w dorocznym audycie śledzenia w MRO/POA/ DOA	Rozważanie	Rozważanie	Liczba, kwartalnie, gwarancji/reklamacji MRO/POA na komponenty	Średnia +1/2/3 SD (ustawienie roczne lub dwuletnie)	__% (np. 5%) poprawy pomiędzy każdą średnią roczną	Zbiorczy współczynnik LEI% rocznego audytu lub niezgodności dla MRO/POA/DOA (ilość niezgodności na audyt)	Rozważanie	Rozważanie
Liczba, zbiorczo, kwartalnych zgłoszeń do CAA od POA/DOA produktów operacyjnych, podległych dyrektywie AD/ Biuletynom Serwisowym ((w rozbiciu na linie produktów)	Rozważanie	Rozważanie				Liczba kwartalnych zgłoszeń POA/DOA wyrobów operacyjnych podległych dyrektywie AD, Biuletynom Serwisowym (w rozbiciu na linie produktów)	Rozważanie	Rozważanie	Współczynnik kwartalny inspekcji końcowej/awarii podczas prób/ odrzucenia dla MRO/POA/DOA (zgodnie z zag. jakości wew.)	Rozważanie	Rozważanie
						Liczba kwartalnych zgłoszeń obowiązkowych MRO/POA o stwierdzonych poważnych niesprawnościach (zgodnie z wewn. zagadnieniami jakości)	Rozważanie	Rozważanie	Współczynnik dobrowolnych zgłoszeń o zagrożeniach dla MRO/POA/DOA dla personelu operacyjnego na kwartał)	Rozważanie	Rozważanie
Itd.											

Tabela 5-A6-5. Przykład wykresu wskaźnika działania bezpieczeństwa SMS (z ustalaniem poziomów alarmowych i docelowych)

<table>
<tr>
<td> 
</td>
<td> 
</td>
</tr>
<tr>
<td>a) Ustawienie poziomu alarmowego:

Poziom alarmu dla nowego okresu monitorowania (rok bieżący) jest oparty na wynikach poprzedniego okresu w (rok poprzedni), mianowicie, na jego średniej punktów danych i odchylenia od standardu. Trzy linie alarmowe to średnia + 1 SD, średnia + 2 SD i średnia + 3 SD.

b) Przekroczenie poziomu alarmowego:

Pojawi się wskazanie alarmu (nieprawidłowy/niedopuszczalne trend) gdy dla bieżącego okresu monitorowania (rok bieżący) spełniony zostanie którykolwiek z poniższych warunków:

- dowolny pojedynczy punkt jest powyżej linii 3 SD

- 2 kolejne punkty są powyżej linii 2 SD

- 3 kolejne punkty są powyżej linii 1 SD.

Po wzbudzeniu alarmu (potencjalnie duże ryzyko lub sytuacja poza kontrolą), oczekuje się dalszego działania, takiego jak dalsza analiza w celu określenia źródła i pierwotnej przyczyny nienormalnej liczby wypadków, oraz zajęcia się takim nieakceptowalnym trendem.</td>
<td>c) Ustawienie poziomu docelowego (planowana poprawa):

Ustawienie poziomu docelowego może być mniej złożone niż ustawienie poziomu alarmowego, np. ustal tak by docelowa średnia wielkość okresu monitorowania była, powiedzmy, o 5% mniejsza (lepsza) niż średnia wielkość okresu poprzedniego.

d) Osiąganie celu:

Pod koniec bieżącego roku, jeżeli wielkość średnia bieżącego roku będzie niższa o co najmniej 5% od średniej wielkości poprzedniego roku, należy uznać że cel, czyli 5% poprawa, będzie osiągnięty.

e) Poziomy alarmowe i docelowe - okres ważności:

Alarmowe i docelowe poziomy powinny zostać poddane przeglądowi/ustawione na nowo dla każdego nowego okresu monitorowania, na bazie wielkości średniej i SD.</td>
</tr>
</table>

Tabela 5-A6-6. Próbka arkusza danych, stosowanego do generowania wykresu wskaźnika bezpieczeństwa SSP (z kryteriami ustanawiania poziomów alarmowych i docelowych)

Rok poprzedni				
miesiąc	Łączna FH wszystkich operatorów	Incydenty wszystkich operatorów	Wielkość zdarzeń *	średnia
styczeń	3992	--	0.00	0.21
luty	3727	1.00	0.27	0.21
marzec	3900	1.00	0.26	0.21
kwiecień	3870	--	0.00	0.21
maj	3976	--	0.00	0.21
czerwiec	3809	--	0.00	0.21
lipiec	3870	1.00	0.26	0.21
sierpień	3904	1.00	0.26	0.21
wrzesień	3864	1.00	0.26	0.21
październik	3973	2.00	0.50	0.21
listopad	3955	2.00	0.51	0.21
grudzień	4369	1.00	0.23	0.21
		Średnia	0.21	
		SD	0.18	

Rok bieżący							
Miesiąc	Łączna FH wszystkich operatorów	Incydenty wszystkich operatorów	Wielkość zdarzeń *	Średnia roku poprzedniego +1SD	Średnia roku poprzedniego +2SD	Średnia roku poprzedniego +3SD	średnia docelowa na rok bież
styczeń	4369	1.00	0.23	0.39	0.56	0.73	0.21
luty	4090	0.00	0.00	0.39	0.56	0.73	0.20
marzec	3316	0.00	0.00	0.39	0.56	0.73	0.20
kwiecień	3482	2.00	0.57	0.39	0.56	0.73	0.20
maj	3549	0.00	0.00	0.39	0.56	0.73	0.20
czerwiec	3633	1.00	0.28	0.39	0.56	0.73	0.20
lipiec				0.39	0.56	0.73	0.20
sierpień				0.39	0.56	0.73	0.20
wrzesień				0.39	0.56	0.73	0.20
październik				0.39	0.56	0.73	0.20
listopad				0.39	0.56	0.73	0.20
grudzień				0.39	0.56	0.73	0.20
		Średnia					
		SD					

Średnia +1SD	Średnia +2SD	Średnia +3SD
0.39	0.56	0.73

Celem roku bieżącego jest, powiedzmy, polepszenie średniej o 5% w stosunku do średniej z roku poprzedniego, która stanowi	0.20

Kryteria ustanawiania poziomu alarmowego na rok bazują na roku poprzednim [śred. + 1/2/3 SD]

* Obliczenie wielkości (na 1000 FH)

Tabela 5-A6-7. Przykład pomiaru działania bezpieczeństwa SMS linii lotniczej Alpha Airlines (powiedzmy za rok 2010)

Wskaźniki wysokopoziomowych konsekwencji dotyczących bezpieczeństwa					
Opis wskaźnika bezpieczeństwa (SPI)		Kryteria poziomów alarmowych SPI (dla 2010)	Czy przekroczono poziom alarmowy? [TAK/NIE]	Kryteria poziomu docelowego SPI (dla 2010)	Czy osiągnięto cel? [TAK/NIE]
1	Liczba poważnych incydentów floty A320 linii Alpha Airline (zbiorczo miesięcznie) [na 1000FH]	Średnia +1/2/3 SD. (wyciągana corocznie lub 2-letnio)	Tak	Poprawa średniej 2010 o 5% względem średniej z 2009	Nie
2	Liczba incydentów zgaśnięć IFSD we flocie Alpha Airline [np. na 1000 FH]	Średnia +1/2/3 SD. (wyciągana corocznie lub 2-letnio)	Tak	Poprawa średniej roku 2010 o 3% względem średniej z 2009	Tak
	itd.				

Wskaźniki niskopoziomowych konsekwencji dotyczących bezpieczeństwa					
Opis wskaźnika bezpieczeństwa (SPI)		Kryteria poziomów alarmowych SPI (dla 2010)	Czy przekroczono poziom alarmowy? [TAK/NIE]	Kryteria poziomu docelowego SPI (dla 2010)	Czy osiągnięto cel? [TAK/NIE]
1	Liczba incydentów (miesięcznie) połączonej floty operatorów (np. na 1000FH)	Średnia + 1/2/3 SD (roczna lub 2-letnia)	Tak	Poprawa średniej roku 2010 o 5% względem średniej z 2009	Nie
2	% LEI lub liczba ustaleń niezgodności QMS (per wewnętrzny audyt roczny operatora)	>25% średniej LEI lub każda niezgodność na Poziomie 1 lub ponad 5 niezgodności na Poziomie 2, na audyt	Tak	Poprawa średniej roku 2010 o 5% względem średniej z 2009	Tak
3	Liczba dobrowolnych zgłoszeń zagrożeń u operatora (np. na 1000FH)	Ma być dostarczona		Ma być dostarczona	
4	Liczba zgłoszeń incydentów z DGR u operatora (np. na 1000FH)	Średnia + 1/2/3 SD (roczna lub dwuletnia)	Nie	Poprawa średniej roku 2010 o 5% względem średniej z 2009	Tak
	itd.				

Uwaga 1. – Inne wskaźniki procesu. Poza powyższymi wskaźnikami bezpieczeństwa SMS, mogą być wskaźniki poziomów innych systemów znajdujących się w każdym obszarze operacyjnym organizacji. Przykłady obejmowałyby wskaźniki specyficzne dla monitorowania procesów i wskaźniki specyficzne dla monitorowania systemów w problemach inżynieryjnych, operacyjnych, w QMS, itd., bądź wskaźniki związane z programami bazującymi na osiągach, jak zarządzanie ryzykiem związanym ze zmęczeniem materiału lub zarządzanie paliwem. Takimi specyficznymi dla procesu lub systemu wskaźnikami powinno się administrować jako częścią odpowiedniego systemu lub procesu. Mogą one być postrzegane jako specyficzne wskaźniki poziomów systemu lub procesu, będąc uzupełnieniem wskaźników działania bezpieczeństwa na wyższym poziomie. Powinny się znaleźć w podręcznikach odpowiednich systemów lub procesów/SOP. Niemniej jednak, najlepiej, powinno się kryteria ustalania alarmowych bądź docelowych poziomów dla takich wskaźników zgrać z poziomami wskaźników działania bezpieczeństwa SMS.

Uwaga 2. – Wybór wskaźników i ustawień. Wyboru kombinacji (lub pakietu) wskaźników wysokopoziomowych i niskopoziomowych konsekwencji dotyczących bezpieczeństwa ma dokonać organizacja zgodnie z zakresem swego lotniczego. Dla tych wskaźników, do których kryteria nastawiania alarmowego lub docelowego poziomu nie mają zastosowania, Państwo może uznać za właściwe każde inne alternatywne kryteria. Generalna wytyczna – nastaw alarmy i cele które biorą pod uwagę ostatnie wyniki historyczne lub osiągi bieżące.

Dodatek 7 do Rozdziału 5
LISTA KONTROLNA LUK SMS I PLAN WDROŻENIOWY

1. POCZĄTKOWA LISTA KONTROLNA ANALIZY LUK (TABELA 5-A7-1)

1.1. Początkową listę kontrolną analizy luk w Tabeli 5-A7-1 można użyć jako szablonu do wykonania pierwszego kroku w analizę luk SMS. Ten format z jego ogólnymi odpowiedziami „Tak/Nie/Częściowo" da początkowe wskazanie co do szerokości zakresu, stąd, jakiego ogólnego nakładu pracy należy się spodziewać. Kwestionariusz można dostosować tak, by pasował do potrzeb organizacji i charakteru dostarczanego produktu lub usługi. Ta wstępna informacja powinna być przydatna dla kierownictwa wyższego szczebla w przewidywaniu skali wysiłku wdrożenia SMS, a więc środków, które należy dostarczyć. Po tej początkowej liście kontrolnej musiałby iść odpowiedni plan wdrożeniowy, jak na Tabelach 5-A7-2 i 5-A7-3.

1.2. Odpowiedź „TAK" wskazuje, że organizacja spełnia lub przekracza oczekiwania danego pytania. Odpowiedź „NIE" wskazuje na znaczną lukę w istniejącym systemie co do oczekiwań pytania. Odpowiedź „CZĘŚCIOWO" wskazuje na to, że potrzebne jest dalsze dopracowywanie lub rozwijanie istniejącego procesu po to, by zaspokoić oczekiwania pytania.

Uwaga. – Podane w kwadratowych nawiasach [ ] odnośniki SSP odsyłają w tym podręczniku do materiałów wytycznych, istotnych dla analizy luk.

Tabela 5-A7-1. Lista kontrolna analizy luk

Nr	*Aspekt do przeanalizowania lub pytanie wymagające odpowiedzi*	*Odpowiedź*	*Stan wdrożenia*
Komponent 1 – POLITYKA BEZPIECZEŃSTWA PAŃSTWA I CELE			
Element 1.1 – Zaangażowanie się kierownictwa i odpowiedzialność			
1.1-1	Czy jest na miejscu polityka bezpieczeństwa? [5.3.7. do 5.3.15; 5.5.3]	□ Tak □ Nie □ Częściowo	
1.1-2	Czy polityka bezpieczeństwa odzwierciedla angażowanie się wyższego kierownictwa w zarządzanie bezpieczeństwem? [5.3.7 do 5.3.15]	□ Tak □ Nie □ Częściowo	
1.1-3	Czy polityka bezpieczeństwa jest odpowiednia do wielkości, charakteru i złożoności organizacji? [5.3.7 do 5.3.15]	□ Tak □ Nie □ Częściowo	
1.1-4	Czy polityka bezpieczeństwa jest właściwa dla bezpieczeństwa w lotnictwie? [5.3.7 do 5.3.15]	□ Tak □ Nie □ Częściowo	
1.1-5	Czy polityka bezpieczeństwa jest sygnowana przez dyrektora odpowiedzialnego? [5.3.7 do 5.3.15; 5.5.3]	□ Tak □ Nie □ Częściowo	
1.1-6	Czy polityka bezpieczeństwa jest komunikowana po całej organizacji, z widocznym jej popieraniem? [5.5.3]	□ Tak □ Nie □ Częściowo	
1.1-7	Czy polityka bezpieczeństwa jest okresowo przeglądana dla upewnienia się, że pozostaje dla organizacji właściwą i odpowiednią? [5.5.3]	□ Tak □ Nie □ Częściowo	
Element 1.2 – Odpowiedzialności za bezpieczeństwo			
1.2-1	Czy organizacja ustaliła kto ze szczebla kierowniczego będzie mieć w zakresie obowiązków, w imieniu organizacji - niezależnie od innych funkcji - ostateczną odpowiedzialność za wdrożenie i utrzymywania SMS? [5.3.16 do 5.3.26; 5.5.2]	□ Tak □ Nie □ Częściowo	
1.2-2	Czy dyrektor odpowiedzialny ma pełną kontrolę nad zasobami finansowymi i ludzkimi jakie są wymagane, by prowadzenie operacji było autoryzowane na mocy certyfikatu dla operacji? [5.3.16 do 5.3.26]	□ Tak □ Nie □ Częściowo	
1.2-3	Czy dyrektor odpowiedzialny ma władzę ostateczną nad lotniczymi działaniami swej organizacji? [5.3.16 do 5.3.26]	□ Tak □ Nie □ Częściowo	
1.2-4	Czy organizacja przydzieliła kierownictwu, jak również personelowi operacyjnemu i czy udokumentowała w SMS zakresy ich odpowiedzialności za bezpieczeństwo? [5.3.16 do 5.3.26]	□ Tak □ Nie □ Częściowo	

Nr	*Aspekt do przeanalizowania lub pytanie wymagające odpowiedzi*	*Odpowiedź*	*Stan wdrożenia*
1.2-5	Czy istnieje komisja/zespół ds. przeglądania SMS i działania bezpieczeństwa? [5.3.27 do 5.3.33; Dodatek 4]	□ Tak □ Nie □ Częściowo	
1.2-6	Czy komisji/zespołowi ds. bezpieczeństwa przewodniczy - należycie uzasadniony w podręczniku SMS - dyrektor odpowiedzialny lub stosownie przydzielony zastępca? [5.3.27 do 5.3.33; Dodatek 4]	□ Tak □ Nie □ Częściowo	
1.2-7	Czy w składzie komisji/zespołu ds. bezpieczeństwa są szefowie działów - operacyjnego, lub odnośnych innych? [5.3.27 do 5.3.33; Dodatek 4]	□ Tak □ Nie □ Częściowo	
1.2-8	Czy są grupy akcji na rzecz bezpieczeństwa, działające łącznie z komisją/ zespołem ds. bezpieczeństwa (szczególnie w dużych/ złożonych organizacjach)? [5.3.27 do 5.3.33; Dodatek 4]	□ Tak □ Nie □ Częściowo	
Element 1.3 – Wyznaczenie personelu kluczowego ds. bezpieczeństwa			
1.3-1	Czy organizacja wyznaczyła wykwalifikowaną osobę do zarządzania i nadzorowania codziennego działania SMS? [5.3.27 do 5.3.33; 5.5.2; Dodatek 2]	□ Tak □ Nie □ Częściowo	
1.3-2	Czy ta wykwalifikowana osoba ma bezpośredni dostęp do dyrektora odpowiedzialnego w sprawach wdrażania i działania SMS? [5.3.27 do 5.3.33; 5.5.2; Dodatek 2, 6.1]	□ Tak □ Nie □ Częściowo	
1.3-3	Czy dyrektor, który odpowiada za administrowanie SMS, czy ma inne funkcje które mogą być w konflikcie z jego rolą jako kierownika SMS, lub które mogą ją osłabiać? [Dodatek 2, 6.4]	□ Tak □ Nie □ Częściowo	
1.3-4	Czy stanowisko kierownika SMS, jako pozycja w kierownictwie wyższego szczebla nie jest stanowiskiem niższym od/lub podległym stanowiskom operacyjnym lub produkcyjnym? [Dodatek 2, 6.4]	□ Tak □ Nie □ Częściowo	
Element 1.4 – Koordynacja planowania reagowania awaryjnego			
1.4-1	Czy organizacja ma plan reagowania awaryjnego; odpowiedni do wielkości, charakteru i złożoności organizacji? [Dodatek 3]	□ Tak □ Nie □ Częściowo	
1.4-2	Czy ten plan zajmuje się wszystkimi ewentualnymi lub prawdopodobnymi scenariuszami sytuacji awaryjnych/kryzysowych, dotyczących dostarczanego przez organizację lotniczego produktu lub usługi? [Dodatek 3, 4f)]	□ Tak □ Nie □ Częściowo	
1.4-3	Czy plan ERP obejmuje procedury na bezpieczne kontynuowanie produkcji, dostaw lub wsparcia swych produktów i usług w czasie takich sytuacji lub ewentualności awaryjnych? [Dodatek 3, 4e)]	□ Tak □ Nie □ Częściowo	
1.4-4	Czy jest plan i rejestr ćwiczeń nadrzędnych i podrzędnych dotyczących ERP? [Dodatek 3, 5c)]	□ Tak □ Nie □ Częściowo	
1.4-5	Czy ERP zajmuje się niezbędną koordynacją swych procedur reagowania w sytuacjach awaryjnych z procedurami sytuacji awaryjnych innych organizacji? [Dodatek 3, 4d)]	□ Tak □ Nie □ Częściowo	
1.4-6	Czy organizacja ma proces dystrybucji ERP i komunikowania go wszystkim odnośnym pracownikom, w tym odnośnym organizacjom? [Dodatek 3, 5d)]	□ Tak □ Nie □ Częściowo	
1.4-7	Czy jest procedura na okresowe przeglądanie ERP w celu zapewnienia by dalej był właściwy i skuteczny? [Dodatek 3, 5f)]	□ Tak □ Nie □ Częściowo	
Element 1.5 – Dokumentacja SMS			
1.5-1	Czy istnieje - opracowany na najwyższym poziomie - sumaryczny lub autoprezentacyjny dokument SMS, zatwierdzony przez kierownika odpowiedzialnego i zaakceptowany przez CAA? [5.3.36 do 5.3.38]	□ Tak □ Nie □ Częściowo	
1.5-2	Czy dokumentacja SMS zajmuje się SMS-em organizacji i związanymi z nim komponentami oraz elementami? [5.3.36 do 5.3.38; 5.4.1; Dodatek 4]	□ Tak □ Nie □ Częściowo	

Nr	*Aspekt do przeanalizowania lub pytanie wymagające odpowiedzi*	*Odpowiedź*	*Stan wdrożenia*
1.5-3	Czy rama SMS organizacji jest „zgrana" z ramą przepisów rządzących SMS-ami? [5.3.36 do 5.3.38; 5.4.1; Dodatek 4]	□ Tak □ Nie □ Częściowo	
1.5-4	Czy organizacja prowadzi rejestr przedmiotowej dokumentacji wspierającej, adekwatnej dla wdrażania i działania SMS? [5.3.36 do 5.3.38; 5.5.5]	□ Tak □ Nie □ Częściowo	
1.5-5	Czy organizacja ma w planie wdrażania SMS, plan jak ustanowić proces jego wdrażania, w tym konkretne zadania i daty ich wdrożenie? [5.4.4]	□ Tak □ Nie □ Częściowo	
1.5-6	Czy plan wdrażania SMS zajmuje się koordynacją między SMS dostawcy usług a SMS-ami zewnętrznych organizacji? [5.4.4]	□ Tak □ Nie □ Częściowo	
1.5-7	Czy plan wdrażania SMS jest popierany przez dyrektora odpowiedzialnego? [5.4.4; 5.5.2]	□ Tak □ Nie □ Częściowo	
Komponent 2 – ZARZĄDZANIE RYZYKIEM DOTYCZĄCYM BEZPIECZEŃSTWA			
Element 2.1 – Identyfikacja zagrożeń			
2.1-1	Czy jest proces dobrowolnego zgłaszania zagrożeń/gróźb przez wszystkich pracowników? [5.3.42 do 5.3.52; 5.5.4]	□ Tak □ Nie □ Częściowo	
2.1-2	Czy dobrowolne zgłaszanie zagrożeń/gróźb jest proste i dostępne wszystkim pracownikom wykonującym prace związane z bezpieczeństwem, i czy jest współmierne z wielkością dostawcy usług? [5.3.42 do 5.3.52]	□ Tak □ Nie □ Częściowo	
2.1-3	Czy system SDCPS organizacji zawiera procedury na raportowanie incydentów/wypadków przez personel operacyjny lub produkcyjny? [5.3.42 do 5.3.52; 5.5.4; Rozdział 4, Dodatek 3]	□ Tak □ Nie □ Częściowo	
2.1-4	Czy system raportowania incydentów/wypadków przez cały personel zaangażowany w prace związane z bezpieczeństwem jest prosty i czy jest współmierne z wielkością dostawcy usług? [5.3.42 do 5.3.52; 5.5.4]	□ Tak □ Nie □ Częściowo	
2.1-5	Czy organizacja ma procedury na badanie wszystkich zgłoszonych incydentów/wypadków? [5.3.42 do 5.3.52; 5.5.4]	□ Tak □ Nie □ Częściowo	
2.1-6	Czy są procedury na upewnienie się, że procesy badania zidentyfikowanych lub odkrytych zagrożeń/gróźb są odpowiednio zapewnione i wstawione w procedurę łagodzenia ryzyka i gromadzenia zagrożeń w organizacji? [2.13.9; 5.3.50 f); 5.5.5]	□ Tak □ Nie □ Częściowo	
2.1-7	Czy są procedury na przeglądanie zagrożeń/gróźb z raportów z przemysłu by - w ich konsekwencji - móc podejmować działania lub dokonywać oceny? [5.3.5.1]	□ Tak □ Nie □ Częściowo	
Element 2.2 – Oszacowanie ryzyka dotyczących bezpieczeństwa i ich łagodzenie			
2.2-1	Czy jest udokumentowana procedura identyfikowania zagrożeń i łagodzenia ryzyka (HIRM), która wymagałaby użycia narzędzi do analizowania ryzyka obiektywnych? [2.13; 2.14; 5.3.53 do 5.3.61]	□ Tak □ Nie □ Częściowo	
2.2-2	Czy sprawozdania z oceny ryzyka są zatwierdzane przez kierowników działów, czy na szczeblu wyższym? [2.15.5; 5.3.53 do 5.3.61]	□ Tak □ Nie □ Częściowo	
2.2-3	Czy jest procedura na okresowe przeglądanie zapisów z istniejącego ryzyka? [5.5.4]	□ Tak □ Nie □ Częściowo	
2.2-4	Czy jest procedura brania pod uwagę akcji łagodzących zawsze, gdy zostaną zidentyfikowane nieakceptowalne poziomy ryzyka? [5.5.4]	□ Tak □ Nie □ Częściowo	
2.2-5	Czy, dla potrzeb akcji łagodzenia ryzyka, jest procedura nadawania priorytetu zagrożeniom rozpoznanym? [5.5.4]	□ Tak □ Nie □ Częściowo	`

Nr	*Aspekt do przeanalizowania lub pytanie wymagające odpowiedzi*	*Odpowiedź*	*Stan wdrożenia*
2.2-6	Czy jest program na systematyczne i progresywne przeglądanie wszystkich związanych z lotniczym bezpieczeństwem operacji procesów, obiektów i sprzętu, które podlegają procesowi HIRM jako zidentyfikowane przez organizację? [5.5.4]	□ Tak □ Nie □ Częściowo	
Komponent 3 – ZAPEWNIANIE BEZPIECZEŃSTWA			
Element 3 – Monitorowanie i mierzenie działania bezpieczeństwa			
3.1-1	Czy w lotniczych działaniach organizacji są zidentyfikowane wskaźniki działania bezpieczeństwa, potrzebne do mierzenia go i monitorowania? [5.3.66 do 5.3.73; 5.4.5; 5.5.4; 5.5.5; Dodatek 6]	□ Tak □ Nie □ Częściowo	
3.1-2	Czy są wskaźniki działania bezpieczeństwa, odpowiednie dla polityki bezpieczeństwa organizacji jak i dla wysokich, bliższych i dalszych celów kierownictwa? [5.3.66 do 5.3.73; 5.4.5; Dodatek 6]	□ Tak □ Nie □ Częściowo	
3.1-3	Czy wskaźniki działania bezpieczeństwa obejmują ustawienia alarmowe/ docelowe, potrzebne dla definiowania rejonów działania nieakceptowanego i dla dalszych celów jakim jest ulepszenie planowania? [5.3.66 do 5.3.73; 5.4.5; 5.5.4; 5.5.5; Dodatek 6]	□ Tak □ Nie □ Częściowo	
3.1-4	Czy ustawianie poziomów alarmowych i kryteria tego co pozostaje poza kontrolą jest oparte na metrycznych, ilościowych zasadach bezpieczeństwa? [5.3.66 do 5.3.73; 5.4.5; Dodatek 6]	□ Tak □ Nie □ Częściowo	
3.1-5	Czy wskaźniki działania bezpieczeństwa obejmują ilościowe monitorowanie wyników *(outcomes)* dużych konsekwencji dotyczących bezpieczeństwa (np. ilości wypadków i poważnych incydentów), a także wydarzeń o małych konsekwencjach (np. ilości nieprzestrzegań, odstępstw)? [5.3.66 do 5.3.73; 5.4.5; 5.5.4; 5.5.5; Dodatek 6]	□ Tak □ Nie □ Częściowo	
3.1-6	Czy wskaźniki działania bezpieczeństwa i związane z nimi ustawienia działania są opracowywane po konsultacji z organem zarządzającym lotnictwem cywilnym i za jego zgodą? [5.3.66 do 5.3.73; 5.4.5.2; 5.5.4; 5.5.5]	□ Tak □ Nie □ Częściowo	
3.1-7	Czy jest procedura na podjęcie działania dalszego i korekcyjnego gdy nie zostaną osiągnięte cele bliższe i gdy przekroczone/naruszone zostaną poziomy alarmowe? [5.4.5; Dodatek 6, Tabela 5-A6-5 b)]	□ Tak □ Nie □ Częściowo	
3.1-8	Czy wskaźniki działania bezpieczeństwa są okresowo przeglądane? [5.4.5; Dodatek 6]	□ Tak □ Nie □ Częściowo	
Element 3.2 – Zarządzanie zmianami			
3.2-1	Czy jest procedura na przeglądanie istotnych, istniejących, związanych z lotniczym bezpieczeństwem obiektów i sprzętu (w tym zapisów HIRM) za każdym razem gdy zajdą jakieś przedmiotowe zmiany w tych obiektach lub w sprzęcie? [5.3.74 do 5.3.77; 5.5.4]	□ Tak □ Nie □ Częściowo	
3.2-2	Czy jest procedura na przeglądanie istotnych, istniejących, związanych z lotniczym bezpieczeństwem operacji i procesów (w tym zapisów HIRM) za każdym razem gdy zajdą jakieś zmiany dotyczące tych operacji lub procesów? [5.3.74 do 5.3.77; 5.5.4]	□ Tak □ Nie □ Częściowo	
3.2-3	Czy jest procedura przeglądania nowych operacji i procesów przed ich uruchomieniem pod kątem zagrożeń/ryzyka związanych z bezpieczeństwem lotniczym? [5.5.4]	□ Tak □ Nie □ Częściowo	
3.2-4	Czy jest procedura przeglądania istniejących obiektów, wyposażenia, operacji i procesów związanych z bezpieczeństwem lotniczym (włącznie z dokumentacją HIRM), zawsze, gdy mają miejsce zmiany zewnętrzne poza organizacji takie jak ustawowe/standardy przemysłu, najlepsze praktyki lub technologie? [5.5.4]	□ Tak □ Nie □ Częściowo	
Element 3.3 – Ciągłe usprawnianie SMS			

Nr	*Aspekt do przeanalizowania lub pytanie wymagające odpowiedzi*	*Odpowiedź*	*Stan wdrożenia*
3.3-1	Czy jest procedura dla prowadzenia okresowych wewnętrznych audytów/ocen SMS? [5.3.78 do 5.3.82; 5.5.4; 5.5.5]	□ Tak □ Nie □ Częściowo	
3.3-2	Czy jest aktualnie obowiązujący plan audytu/oceny SMS? [5.3.78 do 5.3.82; 5.5.4; 5.5.5]	□ Tak □ Nie □ Częściowo	
3.3-3	Czy plan audytu SMS obejmuje próbkowanie zakończonych/prowadzonych ocen ryzyka bezpieczeństwa? [5.5.5]	□ Tak □ Nie □ Częściowo	
3.3-4	Czy plan audytu SMS obejmuje próbkowanie wskaźników poziomu bezpieczeństwa pod kątem aktualności danych i ich wartości docelowych/poziomów alarmowych? [5.4.5; 5.5.5]	□ Tak □ Nie □ Częściowo	
3.3-5	Czy plan audytu SMS obejmuje współpracę SMS z podwykonawcami lub klientami, tam gdzie dotyczy? [5.4.1; 5.5.5]	□ Tak □ Nie □ Częściowo	
3.3-6	Czy jest proces nakazujący omawianie lub składanie raportów z audytu/oceny SMS do wiadomości Dyrektora Odpowiedzialnego, jeżeli ma to zastosowanie? [5.3.80; 5.5.5]	□ Tak □ Nie □ Częściowo	
Komponent 4 – PROMOWANIE BEZPIECZEŃSTWA			
Element 4.1 – Szkolenie i edukacja			
4.1-1	Czy jest program zapewniający szkolenie/zapoznanie się z SMS przez personel zaangażowany we wdrożenie lub działania SMS? [5.3.86 do 5.3.91; 5.5.5]	□ Tak □ Nie □ Częściowo	
4.1-2	Czy Dyrektor Odpowiedzialny przeszedł odpowiednie szkolenie zapoznawcze, omówienie lub szkolenie? [5.3.86 do 5.3.91; 5.5.5]	□ Tak □ Nie □ Częściowo	
4.1-3	Czy personel zajmujący się łagodzeniem ryzyka został przeszkolony w zakresie łagodzenia ryzyka lub odbył szkolenie zapoznawcze? [5.3.86 do 5.3.91; 5.5.5]	□ Tak □ Nie □ Częściowo	
4.1-4	Czy są dowody, że w organizacji prowadzono ogólne szkolenie z zakresu SMS lub dołożono wysiłków w celu uświadomienia o SMS? [5.3.86 do 5.3.91; 5.5.5]	□ Tak □ Nie □ Częściowo	
Element 4.2 – Komunikacja bezpieczeństwa			
4.2-1	Czy organizacja uczestniczy w dzieleniu się informacjami bezpieczeństwa z odpowiednimi przemysłowymi dostawcami wyrobu lub usług lub organizacjami, włącznie z ustawowymi instytucjami lotniczymi? [5.3.92; 5.3.93; 5.5.5]	□ Tak □ Nie □ Częściowo	
4.2-2	Czy są dowody potwierdzające publikowanie informacji bezpieczeństwa (SMS), okólników lub stworzenie kanału przekazywania zagadnień dotyczących bezpieczeństwa (SMS) pracownikom? [5.3.92; 5.3.93; 5.5.5]	□ Tak □ Nie □ Częściowo	
4.2-3	Czy istniejący w organizacji podręcznik SMS lub powiązane z tym materiały pomocnicze są dostępne lub upowszechniane wśród pracowników, których to dotyczy? [5.3.92; 5.3.93; 5.5.5]	□ Tak □ Nie □ Częściowo	

2. SZCZEGÓŁOWA ANALIZA LUK ORAZ ZADANIA WDROŻENIOWE (TABELA 5-A7-2)

Wtedy, trzeba postępować według początkowej listy kontrolnej analizy luk ,Tabela 5-A7-1, posługując się „planem identyfikowania zadań wdrożeniowych i analizowania luk w SMS" z Tabeli 5-A7-2. Po skończeniu, Tabela 5-A7-2 wyda dalszą analizę szczegółów luk i pomoże je przełożyć na faktycznie wymagane zadania i podzadania w kontekście procesów i procedur organizacji. Każde zadanie zostanie wtedy odpowiednio przydzielone właściwym osobom lub grupom. Ważne, żeby w Tabeli 5-A7- 2 uwzględnić korelację opracowywania poszczególnych elementów/zadań z miejscami przeznaczonymi na ich opis (placeholders) w dokumencie SMS, po to by uruchamiać progresywne uaktualnianie szkicu dokumentu SMS w miarę jak każdy element jest wdrażany lub ulepszany. (Początkowe wpisywanie elementów do dokumentów SMS skłania się ku przewidywaniom; nie ma ono charakteru deklaratywnego).

3. HARMONOGRAM DZIAŁAŃ/ZADAŃ WDROŻENIOWYCH (TABELA 5-A7-3)

Tabela 5-A7-3 pokaże kamienie milowe (datę rozpoczęcia, zakończenia każdego zadania/akcji). W fazowym podejściu do wdrażania, trzeba będzie te zadania/akcje klasyfikować według przydziału ich elementów do faz. Po priorytetyzację przydziału elementów SMS do poszczególnych faz patrz pkt 5.5 niniejszego rozdziału. Tabela 5-A7-3 może być oddzielną konsolidacją wszystkich pozostałych działań/zadań lub, jeśli jest to korzystne, kontynuacją Tabeli 5-A7-2 w formie arkusza kalkulacyjnego. Tam gdzie się przewiduje, że rzeczywista liczba zadań/działań i ich etapy są wystarczająco obszerne i złożone tak, aby wymagać wykorzystania oprogramowania do zarządzania projektami, można to zrobić używając oprogramowania takiego jak projekt MS/wykres Gantt, w zależności które będzie właściwe. Tabela 5-A7-4 jest ilustracją wykresu Gantta.

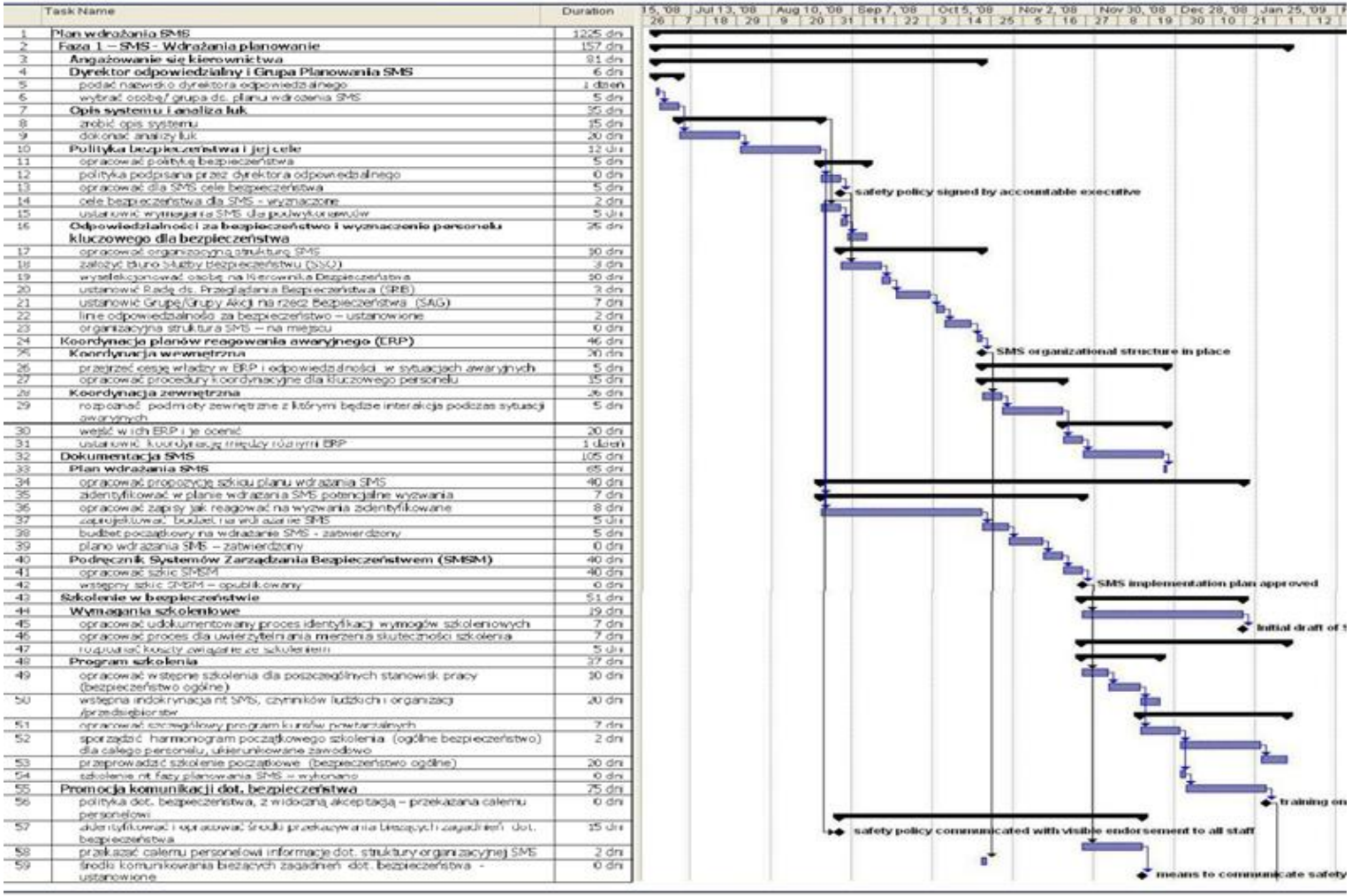
Tabela 5-A7-2. Przykład planu rozpoznawania zadań wdrożeniowych i analizy luk w SMS

Odnośnik GAQ	*Pytania z analizy luk*	*Odpowiedź: TAK / NIE / CZĘŚCIOWO*	*Opis luki*	*Zadanie/działanie wymagane dla wypełnienia luki*	*Grupa/ Osoba przydzielona do wykonania zadania*	*Odnośnik do dokumentu w SSP*	*Stan działania/zadania (otwarte/w toku/ zamknięte)*
1.1-1	Czy jest na miejscu polityka bezpieczeństwa?	Częściowo	Istniejąca polityka bezpieczeństwa zajmuje się OSHE	a) dopracować istniejącą politykę bezpieczeństwa tak aby objęła lotnicze i polityczne cele SMS lub opracować osobną politykę bezpieczeństwa lotniczego. b) niech dyrektor odpowiedzialny zatwierdzi i podpisze politykę bezpieczeństwa	Grupa zadaniowa 1	Rozdział 1, Sekcja 1.3	Otwarte
Itp.							

Tabela 5-A7-3. Przykład harmonogramu wdrażania SMS

Działanie / zadanie potrzebne dla wypełnienia luki	*Odnośnik GAQ*	*Przydzielona Grupa Zadaniowa / Osoba*	*Stan działania / zadania*	*Harmonogram/przedział czasowy (początek – koniec)*												
				1Q 10	2Q 10	3Q 10	4Q 10	1Q 11	2Q 11	3Q 11	4Q 11	1Q 12	2Q 12	3Q 12	4Q 12	itd.
1.1-1 a) Dopracować istniejącą politykę tak, by objęła w SMS cele lotnicze i koncepcje albo opracować osobną politykę lotniczego bezpieczeństwa.	Rozdział 1, sekcja 1.3	Grupa Zadaniowa 1	Otwarte													
1.1-1 b) Zażądać by dyrektor odpowiedzialny zatwierdził i podpisał politykę bezpieczeństwa.																
Itd.																

Tabela 5-A7-4. Przykładowy schemat wdrażania SMS (wykres Gantt-a)



	Task Name	Duration
1	Plan wdrażania SMS	1225 dni
2	Faza 1 – SMS - Wdrażania planowanie	157 dni
3	Angażowanie się kierownictwa	81 dni
4	Dyrektor odpowiedzialny i Grupa Planowania SMS	6 dni
5	podać nazwisko dyrektora odpowiedzialnego	1 dzień
6	wybrać osobę/ grupa dc. planu wdrożenia SMS	5 dni
7	Opis systemu i analiza luk	35 dni
8	zrobić opis systemu	15 dni
9	dokonać analizy luk	20 dni
10	Polityka bezpieczeństwa i jej cele	12 dni
11	opracować politykę bezpieczeństwa	5 dni
12	polityka podpisana przez dyrektora odpowiedzialnego	0 dni
13	opracować dla SMS cele bezpieczeństwa	5 dni
14	cele bezpieczeństwa dla SMS - wyznaczone	2 dni
15	ustanowić wymagania SMS dla podwykonawców	5 dni
16	Odpowiedzialności za bezpieczeństwo i wyznaczenie personelu kluczowego dla bezpieczeństwa	26 dni
17	opracować organizacyjną strukturę SMS	10 dni
18	założyć biuro Służby bezpieczeństwu (SSU)	3 dni
19	wyselekcjonować osobę na Kierownika Bezpieczeństwa	10 dni
20	ustanowić Radę ds. Przeglądania Bezpieczeństwa (SRB)	3 dni
21	ustanowić Grupę/Grupy Akcji na rzecz Bezpieczeństwa (SAG)	7 dni
22	linie odpowiedzialności za bezpieczeństwo – ustanowione	2 dni
23	organizacyjna struktura SMS – na miejscu	0 dni
24	Koordynacja planów reagowania awaryjnego (ERP)	46 dni
25	Koordynacja wewnętrzna	20 dni
26	przejrzeć cesję władzy w ERP i odpowiedzialności w sytuacjach awaryjnych	5 dni
27	opracować procedury koordynacyjne dla kluczowego personelu	15 dni
28	Koordynacja zewnętrzna	26 dni
29	rozpoznać podmioty zewnętrzne z którymi będzie interakcja podczas sytuacji awaryjnych	5 dni
30	wejść w ich ERP i je ocenić	20 dni
31	ustanowić koordynację między różnymi ERP	1 dzień
32	Dokumentacja SMS	105 dni
33	Plan wdrażania SMS	65 dni
34	opracować propozycję szkicu planu wdrażania SMS	40 dni
35	zidentyfikować w planie wdrażania SMS potencjalne wyzwania	7 dni
36	opracować zapisy jak reagować na wyzwania zidentyfikowane	8 dni
37	zaprojektować budżet na wdrożenie SMS	5 dni
38	budżet początkowy na wdrażanie SMS - zatwierdzony	5 dni
39	plano wdrażania SMS – zatwierdzony	0 dni
40	Podręcznik Systemów Zarządzania Bezpieczeństwem (SMSM)	40 dni
41	opracować szkic SMSM	40 dni
42	wstępny szkic SMSM – opublikowany	0 dni
43	Szkolenie w bezpieczeństwie	51 dni
44	Wymagania szkoleniowe	19 dni
45	opracować udokumentowany proces identyfikacji wymogów szkoleniowych	7 dni
46	opracować proces dla uwierzytelniania mierzenia skuteczności szkolenia	7 dni
47	rozpocząć kwestie związane ze szkoleniem	5 dni
48	Program szkolenia	27 dni
49	opracować wstępne szkolenia dla poszczególnych stanowisk pracy (bezpieczeństwo ogólne)	10 dni
50	wstępna indoktrynacja nt SMS, czynników ludzkich i organizacj /przedsiębiorstw	20 dni
51	opracować szczegółowy program kursów powtarzalnych	7 dni
52	sporządzić harmonogram początkowego szkolenia (ogólne bezpieczeństwo) dla całego personelu, ukierunkowane zawodowo	2 dni
53	przeprowadzić szkolenie początkowe (bezpieczeństwo ogólne)	20 dni
54	szkolenie nt fazy planowania SMS – wykonano	0 dni
55	Promocja komunikacji dot. bezpieczeństwa	75 dni
56	polityka dot. bezpieczeństwa, z widoczną akceptacją – przekazana całemu personelowi	0 dni
57	zidentyfikować i opracować środki przekazywania bieżących zagadnień dot. bezpieczeństwa	15 dni
58	przekazać całemu personelowi informacje dot. struktury organizacyjnej SMS	2 dni
59	środki komunikowania bieżących zagadnień dot. bezpieczeństwa - ustanowione	0 dni

Załącznik
MATERIAŁY WYTYCZNE ICAO

PODRĘCZNIKI

Advanced Surface Movement Guidance and Control Systems (A-SMGCS) Manual (Doc 9830) — Podręcznik systemów sterowania i zaawansowanego poruszania powierzchniami.

Airport Services Manual (Doc 9137) — Podręcznik usług lotniskowych.

Part 1 — Rescue and Fire Fighting — Ratownictwo i pożarnictwo.

Part 5 — Removal of Disabled Aircraft — Usuwanie niesprawnych samolotów.

Part 7 — Airport Emergency Planning — Planowanie dla sytuacji awaryjnych.

Airworthiness Manual (Doc 9760) — Podręcznik zdatności do lotu.

Global Air Navigation Plan (Doc 9750) — Globalna mapa nawigacji lotniczej.

Global Air Traffic Management Operational Concept (Doc 9854) — Koncepcja opcjonalna globalnego zarządzania operacjami ruchu lotniczego.

Human Factors Guidelines for Air Traffic Management (ATM) Systems (Doc 9758) — Wytyczne dotyczące czynników ludzkich, dla systemów zarządzania ruchem lotniczym.

Human Factors Guidelines for Aircraft Maintenance Manual (Doc 9824) — Wytyczne dotyczące czynników ludzkich, do podręcznika technicznej obsługi samolotów

Human Factors Guidelines for Safety Audits Manual (Doc 9806) — Wytyczne dotyczące czynników ludzkich, do podręcznika audytowania bezpieczeństwa.

Human Factors Training Manual (Doc 9683) — Podręcznik szkolenia o czynnikach ludzkich.

Line Operations Safety Audit (LOSA) (Doc 9803) — Audyt bezpieczeństwa operacji linii lotniczych.

Manual Concerning Interception of Civil Aircraft (Doc 9433) — Podręcznik dotyczący przechwytywania samolotów cywilnych.

Manual Concerning Safety Measures Relating to Military Activities Potentially Hazardous to Civil Aircraft Operations (Doc 9554) — Podręcznik dotyczący środków bezpieczeństwa odnoszących się do działań wojskowych, potencjalnie groźnych dla lotów cywilnych.

Manual of Aircraft Accident and Incident Investigation (Doc 9756) — Podręcznik badania wypadków i incydentów lotniczych.

Part I — Organization and Planning — Organizacja i planowanie.

Part II — Procedures and Checklists — Procedury i listy kontrolne.

Part III — Investigation — Badanie [wypadków i incydentów lotniczych].

Part IV — Reporting — Zgłaszanie [zdarzeń].

Manual of Aircraft Ground De-icing/Anti-icing Operations (Doc 9640) — Podręcznik odladzania samolotów na ziemi i opryskiwania zapobiegawczego.

Manual of All-Weather Operations (Doc 9365) — Podręcznik latania w każdej pogodzie.

Manual of Civil Aviation Medicine (Doc 8984) — Podręcznik medycyny dla lotnictwa cywilnego.

Manual of Procedures for Operations Inspection, Certification and Continued Surveillance (Doc 8335) Att-2 Safety Management Manual (SMM) — Podręcznik procedur dla inspekcjonowania operacji, certyfikacji i stałego śledzenia. Załącznik nr 2: Podręcznik zarządzania bezpieczeństwem.

Manual of Radiotelephony (Doc 9432) — Podręcznik radiotelefonii.

Manual of Surface Movement Guidance and Control Systems (SMGCS) (Doc 9476) — Podręcznik systemów kierowania ruchem naziemnym i systemy kierowania [ruchem].

Manual on Air Traffic Management System Requirements (Doc 9882) — Podręcznik wymogów systemu zarządzania ruchem lotniczym.

Manual on Airspace Planning Methodology for the Determination of Separation Minima (Doc 9689) — Podręcznik metodologii planowania [wykorzystania] przestrzeni powietrznej dla określania minimów separacji.

Manual on Certification of Aerodromes (Doc 9774) — Podręcznik certyfikowania lotnisk.

Manual on Global Performance of the Air Navigation System (Doc 9883) — Podręcznik globalnego działania systemu nawigacji lotniczej.

Manual on Implementation of a 300 m (1 000 ft) Vertical Separation Minimum Between FL 290 and FL 410 Inclusive (Doc 9574) — Podręcznik wdrażania 300 m (1 000 ft) jako minimalnej separacji pionowej pomiędzy poziomem 290 i 410 włącznie.

Manual on Regional Accident and Incident Investigation Organization (Doc 9946) — Podręcznik organizowania regionalnych badań wypadków i incydentów.

Manual on Required Communication Performance (RCP) (Doc 9869) — Podręcznik działania wymaganej łączności.

Manual on Simultaneous Operations on Parallel or Near-Parallel Instrument Runways (SOIR) (Doc 9643) — Podręcznik operacji jednoczesnych na drogach startowych równoległych lub prawie równoległych w locie przyrządowym.

Manual on the Prevention of Runway Incursions (Doc 9870) — Podręcznik zapobiegania wtargnięciu na drogę lotniczą.

Manual on the Quality Management System for the Provision of Meteorological Service for International Air Navigation (Doc 9873) — Podręcznik systemu zarządzania jakością dla zapewnienia usług meteo dla międzynarodowej żeglugi powietrznej.

Normal Operations Safety Survey (NOSS) (Doc 9910) — Przegląd bezpieczeństwa w operacjach normalnych.

Performance-based Navigation (PBN) Manual (Doc 9613) — Podręcznik nawigacji opartej na osiągach [samolotu].

Safety Oversight Manual (Doc 9734) — Podręcznik oglądu bezpieczeństwa.

Universal Safety Oversight Audit Programme Continuous Monitoring Manual (Doc 9735) — Podręcznik audytowania programu stałego monitorowania nadzorowania bezpieczeństwa ogólnego.

OKÓLNIKI

A Unified Framework for Collision Risk Modelling in Support of the Manual on Airspace Planning Methodology for the Determination of Separation Minima (Doc 9689) (Cir. 319) — Ujednolicona rama dla modelowania ryzyk podczas kolizji – materiał pomocniczy dla podręcznika metodologii planowania przestrzeni powietrznej dla potrzeb określenia minimów separacji.

Assessment of ADS-B and Multilateration Surveillance to Support Air Traffic Services and Guidelines for Implementation (Cir 326) — Ocena ADS-B oraz wielorakiego śledzenia wielobocznego, na wsparcie usług lotniczych i wytycznych, przewidzianych do wdrożenia.

Guidance on Assistance to Aircraft Accident Victims and their Families (Cir 285) — Wytyczna dotycząca pomagania ofiarom wypadków lotniczych i ich rodzinom.

Hazards at Aircraft Accident Sites (Cir 315) — Zagrożenia na miejscach wypadków lotniczych.

Human Factors Digest No 15 — Human Factors in Cabin Safety (Cir 300) — Czynniki ludzkie a bezpieczeństwo w kabinie (Zeszyt nr 15 Human Factors Digest).

Human Factors Digest No. 16 — Cross-Cultural Factors in Aviation Safety (Cir 302) Attachment Att-3 — Czynniki ludzkie a bezpieczeństwo w lotnictwie (Zeszyt nr 16 Human Factors Digest).

Human Factors Digest No. 17 — Threat and Error Management (TEM) in Air Traffic Control (Cir 314) — Zarządzanie groźbami/zagrożeniami i pomyłkami w kontrolowaniu ruchu lotniczego (Zeszyt nr 17 Human Factors Digest).

Operation of New Larger Aeroplanes at Existing Aerodromes (Cir 305) — Operacje nowych, dużych samolotów na istniejących lotniskach.

Training Guidelines for Aircraft Accident Investigators (Cir 298) — Wytyczne szkoleniowe dla inspektorów wypadków lotniczych.

— KONIEC —