ROZPORZĄDZENIE DELEGOWANE KOMISJI (UE) 2022/1645

z dnia 14 lipca 2022 r.

ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1139 w odniesieniu do wymagań dotyczących zarządzania ryzykiem związanym z bezpieczeństwem informacji o potencjalnym wpływie na bezpieczeństwo lotnicze w odniesieniu do organizacji objętych zakresem stosowania rozporządzeń Komisji (UE) nr 748/2012 i (UE) nr 139/2014 oraz zmieniające rozporządzenia Komisji (UE) nr 748/2012 i (UE) nr 139/2014

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1139 z dnia 4 lipca 2018 r. w sprawie wspólnych zasad w dziedzinie lotnictwa cywilnego i utworzenia Agencji Unii Europejskiej ds. Bezpieczeństwa Lotniczego oraz zmieniające rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 2111/2005, (WE) nr 1008/2008, (UE) nr 996/2010, (UE) nr 376/2014 i dyrektywy Parlamentu Europejskiego i Rady 2014/30/UE i 2014/53/UE, a także uchylające rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 552/2004 i (WE) nr 216/2008 i rozporządzenie Rady (EWG) nr 3922/91 ([1]), w szczególności jego art. 19 ust. 1 lit. g) i art. 39 ust. 1 lit. b),

a także mając na uwadze, co następuje:

(1) Zgodnie z zasadniczymi wymogami określonymi w pkt 3.1 lit. b) załącznika II do rozporządzenia (UE) 2018/1139 organizacje projektujące i produkujące muszą wdrożyć i utrzymywać system zarządzania w celu zarządzania ryzykiem dotyczącym bezpieczeństwa.

(2) Ponadto zgodnie z zasadniczymi wymogami określonymi w pkt 2.2.1 i 5.2 załącznika VII do rozporządzenia (UE) 2018/1139 operatorzy lotniska i organizacje odpowiedzialne za zapewnianie służby zarządzania płytą postojową muszą wdrożyć i utrzymywać system zarządzania w celu zarządzania ryzykiem dotyczącym bezpieczeństwa.

(3) Ryzyko dotyczące bezpieczeństwa, o którym mowa w motywach 1 i 2, może mieć różne źródła, w tym wady projektowe, nieprawidłowe utrzymanie, aspekty wydolności ludzkiej, zagrożenia środowiskowe i zagrożenia dla bezpieczeństwa informacji. W systemach zarządzania wdrożonych przez organizacje, o których mowa w motywach 1 i 2, należy zatem uwzględnić nie tylko ryzyko dla bezpieczeństwa wynikające ze zdarzeń losowych, ale również ryzyko dla bezpieczeństwa wynikające z zagrożeń dla bezpieczeństwa informacji, jeżeli występujące wady mogą zostać wykorzystane przez osoby fizyczne w złym zamiarze. Tego typu ryzyko związane z bezpieczeństwem informacji stale wzrasta w środowisku lotnictwa cywilnego wraz z coraz większym powiązaniem istniejących systemów informatycznych, które coraz częściej stają się celem ataków dokonywanych przez osoby działające w złym zamiarze.

(4) Ryzyko związane z tymi systemami informatycznymi nie ogranicza się do ewentualnych ataków w cyberprzestrzeni, ale obejmuje również zagrożenia, które mogą wpływać na procesy i procedury, a także wydolność ludzką.

(5) Aby zapewnić bezpieczeństwo informacji i danych cyfrowych, wiele organizacji już teraz stosuje normy międzynarodowe, takie jak ISO 27001. Normy te mogą nie obejmować wszystkich aspektów lotnictwa cywilnego.

(6) Należy zatem określić wymagania dotyczące zarządzania ryzykiem związanym z bezpieczeństwem informacji o potencjalnym wpływie na bezpieczeństwo lotnicze.

(7) Ważne jest, aby takie wymagania obejmowały poszczególne dziedziny lotnictwa i ich wzajemne relacje, ponieważ lotnictwo stanowi wysoce powiązany system systemów. Wymagania te muszą zatem mieć zastosowanie do wszystkich organizacji, które już teraz są zobowiązane do posiadania systemu zarządzania zgodnie z obowiązującymi unijnymi przepisami dotyczącymi bezpieczeństwa lotniczego.

(8) Wymagania określone w niniejszym rozporządzeniu należy konsekwentnie stosować we wszystkich dziedzinach lotnictwa, a jednocześnie ich stosowanie powinno mieć jak najmniejszy wpływ na unijne przepisy dotyczące bezpieczeństwa lotniczego mające już zastosowanie do tych dziedzin.

([1]) Dz.U. L 212 z 22.8.2018, s. 1.

(9) Wymagania określone w niniejszym rozporządzeniu powinny pozostawać bez uszczerbku dla wymogów w zakresie bezpieczeństwa informacji i cyberbezpieczeństwa określonych w pkt 1.7 załącznika do rozporządzenia wykonawczego Komisji (UE) 2015/1998 ([2]) i w art. 14 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 ([3]).

(10) Definicji terminu „bezpieczeństwo informacji" stosowanej do celów niniejszego aktu prawnego nie należy interpretować jako rozbieżnej z definicją terminu „bezpieczeństwo sieci i systemów informatycznych" określoną w dyrektywie 2016/1148.

(11) Aby uniknąć powielania wymogów prawnych, jeżeli organizacje objęte zakresem niniejszego rozporządzenia podlegają już wymogom w zakresie bezpieczeństwa wynikającym z innych aktów Unii, o których mowa w motywie 9, i wywierającym taki sam skutek jak przepisy określone w niniejszym rozporządzeniu, zgodność z tymi wymogami w zakresie bezpieczeństwa należy uznać za tożsamą ze zgodnością z wymogami określonymi w niniejszym rozporządzeniu.

(12) Organizacje objęte zakresem stosowania niniejszego rozporządzenia, które już podlegają wymogom w zakresie bezpieczeństwa wynikającym z rozporządzenia wykonawczego (UE) 2015/1998, powinny również przestrzegać wymogów określonych w załączniku I (część IS.D.OR.230 „System zewnętrznego zgłaszania zdarzeń związanych z bezpieczeństwem informacji") do niniejszego rozporządzenia, ponieważ rozporządzenie wykonawcze (UE) 2015/1998 nie zawiera żadnych przepisów dotyczących zewnętrznego zgłaszania incydentów związanych z bezpieczeństwem informacji.

(13) Rozporządzenia Komisji (UE) nr 748/2012 ([4]) i (UE) nr 139/2014 ([5]) należy zmienić, aby ustanowić związek między systemami zarządzania określonymi w wyżej wymienionych rozporządzeniach a wymaganiami dotyczącymi zarządzania bezpieczeństwem informacji określonymi w niniejszym rozporządzeniu.

(14) Aby organizacje miały wystarczająco dużo czasu na zapewnienie zgodności z nowymi przepisami i procedurami wprowadzonymi niniejszym rozporządzeniem, niniejsze rozporządzenie powinno mieć zastosowanie 3 lata od daty jego wejścia w życie.

(15) Wymagania określone w niniejszym rozporządzeniu opierają się na opinii nr 03/2021 ([6]) wydanej przez Agencję zgodnie z art. 75 ust. 2 lit. b) i c) oraz art. 76 ust. 1 rozporządzenia (UE) 2018/1139.

(16) Zgodnie z art. 128 ust. 4 rozporządzenia (UE) 2018/1139 Komisja skonsultowała się z ekspertami wyznaczonymi przez każde państwo członkowskie zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym z dnia 13 kwietnia 2016 r. w sprawie lepszego stanowienia prawa ([7]),

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

Przedmiot

W niniejszym rozporządzeniu określono wymagania, które muszą spełnić organizacje, o których mowa w art. 2, w celu określenia ryzyka związanego z bezpieczeństwem informacji o potencjalnym wpływie na bezpieczeństwo lotnicze, co może wpływać na systemy technologii informacyjno-komunikacyjnych i dane wykorzystywane do celów lotnictwa cywilnego, oraz w celu zarządzania tym ryzykiem, a także w celu wykrywania zdarzeń związanych z bezpieczeństwem informacji i identyfikacji zdarzeń, które uznaje się za incydenty związane z bezpieczeństwem informacji o potencjalnym wpływie na bezpieczeństwo lotnicze, reagowania na takie incydenty związane z bezpieczeństwem informacji i przywracania sytuacji sprzed takich incydentów związanych z bezpieczeństwem informacji.

([2]) Rozporządzenie wykonawcze Komisji (UE) 2015/1998 z dnia 5 listopada 2015 r. ustanawiające szczegółowe środki w celu wprowadzenia w życie wspólnych podstawowych norm ochrony lotnictwa cywilnego (Dz.U. L 299 z 14.11.2015, s. 1).

([3]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.U. L 194 z 19.7.2016, s. 1).

([4]) Rozporządzenie Komisji (UE) nr 748/2012 z dnia 3 sierpnia 2012 r. ustanawiające przepisy wykonawcze dotyczące certyfikacji statków powietrznych i związanych z nimi wyrobów, części i akcesoriów w zakresie zdatności do lotu i ochrony środowiska oraz dotyczące certyfikacji organizacji projektujących i produkujących (Dz.U. L 224 z 21.8.2012, s. 1).

([5]) Rozporządzenie Komisji (UE) nr 139/2014 z dnia 12 lutego 2014 r. ustanawiające wymagania oraz procedury administracyjne dotyczące lotnisk zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (WE) nr 216/2008 (Dz.U. L 44 z 14.2.2014, s. 1).

([6]) https://www.easa.europa.eu/document-library/opinions

([7]) Dz.U. L 123 z 12.5.2016, s. 1.

Artykuł 2

Zakres stosowania

1. Niniejsze rozporządzenie ma zastosowanie do następujących organizacji:

a) organizacje produkujące i organizacje projektujące podlegające części A podczęści G i J załącznika I (część 21) do rozporządzenia (UE) nr 748/2012, z wyjątkiem organizacji projektujących i produkujących, które zajmują się wyłącznie projektowaniem lub produkcją statków powietrznych ELA2 zdefiniowanych w art. 1 ust. 2 lit. j) rozporządzenia (UE) nr 748/2012;

b) operatorzy lotniska i instytucje zapewniające służbę zarządzania płytą postojową podlegający przepisom załącznika III „Część »Wymagania dla organizacji« (część ADR.OR)" do rozporządzenia (UE) nr 139/2014.

2. Niniejsze rozporządzenie pozostaje bez uszczerbku dla wymogów w zakresie bezpieczeństwa informacji i cyberbezpieczeństwa określonych w pkt 1.7 załącznika do rozporządzenia wykonawczego Komisji (UE) 2015/1998 i w art. 14 dyrektywy (UE) 2016/1148.

Artykuł 3

Definicje

Do celów niniejszego rozporządzenia zastosowanie mają następujące definicje:

1) „bezpieczeństwo informacji" oznacza zachowanie poufności, integralności, autentyczności i dostępności sieci i systemów informatycznych;

2) „zdarzenie związane z bezpieczeństwem informacji" oznacza zidentyfikowane zdarzenie w systemie, stanie usługi lub sieci wskazujące na możliwe naruszenie strategii bezpieczeństwa informacji, awarię kontroli bezpieczeństwa informacji, lub na wcześniej nieznaną sytuację, która może mieć znaczenie dla bezpieczeństwa informacji;

3) „incydent" oznacza każde zdarzenie, które ma niekorzystny wpływ na bezpieczeństwo sieci i systemów informatycznych, jak zdefiniowano w art. 4 pkt 7 dyrektywy (UE) 2016/1148;

4) „ryzyko związane z bezpieczeństwem informacji" oznacza ryzyko dla organizacji operacji, aktywów, osób fizycznych i innych organizacji w lotnictwie cywilnym, wynikające z potencjału zdarzenia związanego z bezpieczeństwem informacji. Ryzyko związane z bezpieczeństwem informacji wiąże się z możliwością wykorzystania podatności zasobów informacyjnych lub grupy zasobów informacyjnych na zagrożenia;

5) „zagrożenie" oznacza potencjalne naruszenie bezpieczeństwa informacji, które zachodzi w przypadku zaistnienia podmiotu, okoliczności, działania lub zdarzenia, które mogą spowodować szkodę;

6) „podatność" oznacza wadę lub słabość składnika aktywów lub systemu, procedur, projektu, sposobu wdrożenia lub środków bezpieczeństwa informacji, które mogą zostać wykorzystane i prowadzić do naruszenia lub pogwałcenia strategii bezpieczeństwa informacji.

Artykuł 4

Wymogi wynikające z innych przepisów unijnych

1. Jeżeli organizacja, o której mowa w art. 2, przestrzega wymogów w zakresie bezpieczeństwa określonych w art. 14 dyrektywy (UE) 2016/1148 równoważnych wymogom określonym w niniejszym rozporządzeniu, przestrzeganie tych wymogów uznaje się za tożsame z przestrzeganiem wymogów określonych w niniejszym rozporządzeniu.

2. Jeżeli organizacja, o której mowa w art. 2, jest operatorem lub podmiotem, o którym mowa w krajowych programach ochrony lotnictwa cywilnego państw członkowskich określonych zgodnie z art. 10 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 300/2008 ([8]), wymogi w zakresie cyberbezpieczeństwa zawarte w pkt 1.7 załącznika do rozporządzenia wykonawczego (UE) 2015/1998 uznaje się za równoważne wymogom określonym w niniejszym rozporządzeniu, z wyjątkiem pkt IS.D.OR.230 załącznika do niniejszego rozporządzenia, którego należy przestrzegać.

([8]) Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 300/2008 z dnia 11 marca 2008 r. w sprawie wspólnych zasad w dziedzinie ochrony lotnictwa cywilnego i uchylające rozporządzenie (WE) nr 2320/2002 (Dz.U. L 97 z 9.4.2008, s. 72).

3. Komisja, po konsultacji z EASA i grupą współpracy, o której mowa w art. 11 dyrektywy (UE) 2016/1148, może wydać wytyczne dotyczące oceny równoważności wymogów określonych w niniejszym rozporządzeniu i w dyrektywie (UE) 2016/1148.

Artykuł 5

Właściwy organ

1. Organem odpowiedzialnym za poświadczanie i nadzorowanie zgodności z niniejszym rozporządzeniem jest:

a) w odniesieniu do organizacji, o których mowa w art. 2 lit. a), właściwy organ wyznaczony zgodnie z załącznikiem I (część 21) rozporządzenia (UE) nr 748/2012;

b) w odniesieniu do organizacji, o których mowa w art. 2 lit. b), właściwy organ wyznaczony zgodnie z załącznikiem III (część ADR.OR) do rozporządzenia (UE) nr 139/2014.

2. Do celów niniejszego rozporządzenia, państwa członkowskie mogą na potrzeby wypełniania powierzonych im zadań i obowiązków właściwego organu, o którym mowa w ust. 1, wyznaczyć niezależny i samodzielny podmiot. W takim przypadku ustanawia się środki koordynacji między tym podmiotem a właściwym organem, o którym mowa w ust. 1, aby zapewnić skuteczny nadzór w zakresie wszystkich wymagań, które ma spełnić dana organizacja.

Artykuł 6

Zmiana rozporządzenia (UE) nr 748/2012

W załączniku I (część 21) do rozporządzenia (UE) nr 748/2012 wprowadza się następujące zmiany:

1) w spisie treści wprowadza się następujące zmiany:

   a) po nagłówku 21.A.139 dodaje się nagłówek w brzmieniu:

   „**21.A.139A System zarządzania bezpieczeństwem informacji**";

   b) po nagłówku 21.A.239 dodaje się nagłówek w brzmieniu:

   „**21.A.239A System zarządzania bezpieczeństwem informacji**";

2) po pkt 21.A.139 dodaje się pkt 21.A.139A w brzmieniu:

„**21.A.139A System zarządzania bezpieczeństwem informacji**

Oprócz systemu zarządzania produkcją wymaganego w pkt 21.A.139 organizacja produkująca ustanawia, wdraża i utrzymuje system zarządzania bezpieczeństwem informacji zgodnie z rozporządzeniem delegowanym Komisji (UE) 2022/1645 (*) w celu zapewnienia prawidłowego zarządzania ryzykiem związanym z bezpieczeństwem informacji, które może mieć wpływ na bezpieczeństwo lotnicze.

(*) Rozporządzenie delegowane Komisji (UE) 2022/1645 z dnia 14 lipca 2022 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1139 w odniesieniu do wymagań dotyczących zarządzania ryzykiem związanym z bezpieczeństwem informacji o potencjalnym wpływie na bezpieczeństwo lotnicze w odniesieniu do organizacji objętych zakresem stosowania rozporządzeń Komisji (UE) nr 748/2012 i (UE) nr 139/2014 oraz zmieniające rozporządzenia Komisji (UE) nr 748/2012 i (UE) nr 139/2014 (Dz.U. L 248 z 26.9.2022, s. 18).";

3) po pkt 21.A.239 dodaje się pkt 21.A.239A w brzmieniu:

„**21.A.239A System zarządzania bezpieczeństwem informacji**

Oprócz systemu zarządzania projektem wymaganego w pkt 21.A.239 organizacja projektująca ustanawia, wdraża i utrzymuje system zarządzania bezpieczeństwem informacji zgodnie z rozporządzeniem delegowanym (UE) 2022/1645 w celu zapewnienia prawidłowego zarządzania ryzykiem związanym z bezpieczeństwem informacji, które to ryzyko może mieć wpływ na bezpieczeństwo lotnicze.";

Artykuł 7

Zmiana rozporządzenia (UE) nr 139/2014

W załączniku III (część ADR.AR) do rozporządzenia (UE) nr 139/2014 wprowadza się następujące zmiany:

1) po pkt ADR.OR.D.005 dodaje się pkt ADR.OR.D.005 w brzmieniu:

„**ADR.OR.D.005A System zarządzania bezpieczeństwem informacji**

Operator lotniska ustanawia, wdraża i utrzymuje system zarządzania bezpieczeństwem informacji zgodnie z rozporządzeniem delegowanym Komisji (UE) 2022/1645 (*) w celu zapewnienia prawidłowego zarządzania ryzykiem związanym z bezpieczeństwem informacji, które może mieć wpływ na bezpieczeństwo lotnicze.

(*) Rozporządzenie delegowane Komisji (UE) 2022/1645 z dnia 14 lipca 2022 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1139 w odniesieniu do wymagań dotyczących zarządzania ryzykiem związanym z bezpieczeństwem informacji o potencjalnym wpływie na bezpieczeństwo lotnicze w odniesieniu do organizacji objętych zakresem stosowania rozporządzeń Komisji (UE) nr 748/2012 i (UE) nr 139/2014 oraz zmieniające rozporządzenia Komisji (UE) nr 748/2012 i (UE) nr 139/2014 (Dz.U. L 248 z 26.9.2022, s. 18).";

2) pkt ADR.OR.D.007 otrzymuje brzmienie:

„**ADR.OR.D.007 Zarządzanie danymi lotniczymi i informacjami lotniczymi**

a) W ramach swojego systemu zarządzania operator lotniska wdraża i utrzymuje system zarządzania jakością obejmujący następujące działania:

1) działania prowadzone przez niego w zakresie danych lotniczych;

2) działania prowadzone przez niego w ramach udzielania informacji lotniczych.

b) W ramach swojego systemu zarządzania operator lotniska wprowadza system zarządzania ochroną, aby zapewnić ochronę otrzymywanych, generowanych lub wykorzystywanych w inny sposób danych operacyjnych przez ograniczenie dostępu do tych danych, tak aby miały go wyłącznie osoby upoważnione.

c) System zarządzania ochroną określa następujące elementy:

1) procedury związane z oceną i ograniczaniem ryzyka związanego z bezpieczeństwem danych, monitorowaniem ochrony i jej poprawą, przeglądami ochrony i upowszechnianiem informacji o zdobytych doświadczeniach;

2) środki służące wykrywaniu naruszeń w zakresie ochrony i powiadamianiu personelu o niebezpieczeństwie za pomocą odpowiednich ostrzeżeń;

3) środki służące kontroli skutków naruszeń w zakresie ochrony oraz określeniu działań naprawczych i procedur ograniczających, aby zapobiec ponownemu wystąpieniu naruszeń.

d) Operator lotniska zapewnia, aby członkowie jego personelu posiadali poświadczenia bezpieczeństwa osobowego w odniesieniu do ochrony danych lotniczych.

e) Aspektami związanymi z bezpieczeństwem informacji zarządza się zgodnie z pkt ADR.OR.D.005A.";

3) po pkt ADR.OR.F.045 dodaje się pkt ADR.OR.F.045A w brzmieniu:

„**ADR.OR.F.045A System zarządzania bezpieczeństwem informacji**

Organizacja odpowiedzialna za zapewnianie AMS ustanawia, wdraża i utrzymuje system zarządzania bezpieczeństwem informacji zgodnie z rozporządzeniem delegowanym (UE) 2022/1645 w celu zapewnienia prawidłowego zarządzania ryzykiem związanym z bezpieczeństwem informacji, które może mieć wpływ na bezpieczeństwo lotnicze.";

Artykuł 8

Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po jego opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Rozporządzenie to stosuje się od dnia 16 października 2025 r.

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.

Sporządzono w Brukseli dnia 14 lipca 2022 r.

W imieniu Komisji
Przewodnicząca
Ursula VON DER LEYEN

ZAŁĄCZNIK

BEZPIECZEŃSTWO INFORMACJI – WYMAGANIA DLA ORGANIZACJI

[Część IS.D.OR]

IS.D.OR.100 Zakres stosowania

W niniejszej części ustanawia się wymagania, które muszą spełnić organizacje, o których mowa w art. 2 niniejszego rozporządzenia.

IS.D.OR.200 System zarządzania bezpieczeństwem informacji (SZBI)

a) Aby osiągnąć cele określone w art. 1, organizacja ustanawia, wdraża i utrzymuje system zarządzania bezpieczeństwem informacji (SZBI) zapewniający, aby dana organizacja:

1) ustanowiła strategię bezpieczeństwa informacji określającą ogólne zasady obowiązujące w danej organizacji w zakresie potencjalnego wpływu ryzyka związanego z bezpieczeństwem informacji na bezpieczeństwo lotnicze;

2) określiła i dokonała przeglądu ryzyka związanego z bezpieczeństwem informacji zgodnie z pkt IS.D.OR.205;

3) określiła i wdrożyła środki zmniejszające ryzyko związane z bezpieczeństwem informacji zgodnie z pkt IS.D.OR.210;

4) wdrożyła system wewnętrznego zgłaszania zdarzeń związanych z bezpieczeństwem informacji zgodnie z pkt IS.D.OR.215;

5) zdefiniowała i wdrożyła, zgodnie z pkt IS.D.OR.220, środki konieczne do wykrywania zdarzeń związanych z bezpieczeństwem informacji, identyfikowała takie zdarzenia, które uznaje się za incydenty o potencjalnym wpływie na bezpieczeństwo lotnicze, z wyjątkiem przypadków dopuszczonych w pkt IS.D.OR.205 lit. e), oraz reagowania na takie incydenty związane z bezpieczeństwem informacji i przywracania sytuacji sprzed takich incydentów związanych z bezpieczeństwem informacji;

6) wdrożyła środki, o których powiadomił właściwy organ, w ramach natychmiastowej reakcji na incydent związany z bezpieczeństwem informacji lub podatność mające wpływ na bezpieczeństwo lotnicze;

7) podjęła odpowiednie działanie, zgodnie z pkt IS.D.OR.225, aby wyeliminować niezgodności, o których powiadomił właściwy organ;

8) wdrożyła system zewnętrznego zgłaszania zdarzeń zgodnie z pkt IS.D.OR.230, aby właściwy organ mógł podjąć odpowiednie działania;

9) przestrzegała wymagań zawartych w pkt IS.D.OR.235 w przypadku zlecenia jakiejkolwiek części czynności, o których mowa w pkt IS.D.OR.200, innym organizacjom;

10) przestrzegała wymagań dotyczących personelu określonych w pkt IS.D.OR.240;

11) przestrzegała wymagań dotyczących prowadzenia rejestrów określonych w pkt IS.D.OR.245;

12) monitorowała przestrzeganie przez organizację wymagań określonych w niniejszym rozporządzeniu oraz udzielała informacji zwrotnych dotyczących niezgodności kierownikowi odpowiedzialnemu lub, w przypadku organizacji projektujących, dyrektorowi organizacji projektującej w celu zapewnienia skutecznego wdrożenia działań naprawczych;

13) chroniła – bez uszczerbku dla mających zastosowanie wymagań dotyczących zgłaszania incydentów – poufność wszelkich informacji, które organizacja mogła otrzymać od innych organizacji, zgodnie z poziomem ich wrażliwości.

b) Aby zapewnić stałe przestrzeganie wymagań, o których mowa w art. 1, organizacja wdraża proces ciągłego doskonalenia zgodnie z pkt IS.D.OR.260.

c) Organizacja dokumentuje, zgodnie z pkt IS.D.OR.250, wszystkie najważniejsze procesy, procedury, funkcje i obowiązki konieczne do zapewnienia zgodności z pkt IS.D.OR.200 lit. a) oraz ustanawia tryb zmiany tej dokumentacji. Zarządzanie zmianami tych procesów, procedur, funkcji i obowiązków przebiega zgodnie z pkt IS.D.OR.255.

d) Procesy, procedury, funkcje i obowiązki utworzone przez organizację w celu zapewnienia zgodności z pkt IS.D.OR.200 lit. a) odpowiadają charakterowi i złożoności działalności tej organizacji, na podstawie oceny właściwego dla tej działalności ryzyka związanego z bezpieczeństwem informacji, oraz mogą zostać włączone do innych systemów zarządzania już wdrożonych przez tę organizację.

e) Bez uszczerbku dla obowiązku przestrzegania wymagań w zakresie zgłaszania zdarzeń zawartych w rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 376/2014 ([1]) i wymagań pkt IS.D.OR.200 lit. a) ppkt 13 właściwy organ może zezwolić organizacji na niewdrożenie wymagań, o których mowa w lit. a)–d), oraz powiązanych wymagań zawartych w pkt IS.D.OR.205 do IS.D.OR.260, jeżeli organizacja ta wykaże w sposób spełniający oczekiwania tego organu, że jej działalność, obiekty i zasoby, a także służby, które obsługuje, zapewnia, otrzymuje i utrzymuje, nie stwarzają żadnego ryzyka związanego z bezpieczeństwem informacji o potencjalnym wpływie na bezpieczeństwo lotnicze ani wobec tej organizacji, ani wobec innych organizacji. Takie zezwolenie musi opierać się na udokumentowanej ocenie ryzyka związanego z bezpieczeństwem informacji przeprowadzonej przez tę organizację lub przez stronę trzecią zgodnie z pkt IS.D.OR.205 oraz sprawdzonej i zatwierdzonej przez jej właściwy organ.

Właściwy organ będzie przeprowadzał przegląd ciągłości ważności takiego zezwolenia po mającym zastosowanie cyklu nadzoru audytowego i zawsze gdy wprowadzane są zmiany w zakresie prac danej organizacji.

IS.D.OR.205 Ocena ryzyka związanego z bezpieczeństwem informacji

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

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

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

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

c) Jeżeli chodzi o elementy i interfejsy, o których mowa w lit. a) i b), organizacja identyfikuje ryzyko związane z bezpieczeństwem informacji, które może mieć potencjalny wpływ na bezpieczeństwo lotnicze. W odniesieniu do każdego zidentyfikowanego rodzaju ryzyka organizacja:

1) przypisuje poziom ryzyka zgodnie ze wstępnie określoną klasyfikacją ustanowioną przez daną organizację;

([1]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 376/2014 z dnia 3 kwietnia 2014 r. w sprawie zgłaszania i analizy zdarzeń w lotnictwie cywilnym oraz podejmowanych w związku z nimi działań następczych, zmiany rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 996/2010 oraz uchylenia dyrektywy 2003/42/WE Parlamentu Europejskiego i Rady i rozporządzeń Komisji (WE) nr 1321/2007 i (WE) nr 1330/2007 (Dz.U. L 122 z 24.4.2014, s. 18).

2) przypisuje każdy rodzaj ryzyka i jego poziom odpowiedniemu elementowi lub interfejsowi określonemu zgodnie z lit. a) i b).

W ramach wstępnie określonej klasyfikacji, o której mowa w pkt 1, bierze się pod uwagę możliwość wystąpienia scenariusza zagrożenia i dotkliwość jego skutków dla bezpieczeństwa. Na podstawie tej klasyfikacji i biorąc pod uwagę kwestię, czy organizacja stosuje zorganizowany i powtarzalny proces zarządzania ryzykiem w odniesieniu do operacji, taka organizacja musi być w stanie ustalić, czy ryzyko jest dopuszczalne czy wymaga zmniejszenia zgodnie z pkt IS.D.OR.210.

Aby umożliwić wzajemną porównywalność oceny ryzyka, przypisując poziom ryzyka na podstawie pkt 1, należy brać pod uwagę istotne informacje otrzymane we współpracy z organizacjami, o których mowa w lit. b).

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

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

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

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

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

IS.D.OR.210 Zmniejszanie ryzyka związanego z bezpieczeństwem informacji

a) Organizacja opracowuje środki służące wyeliminowaniu niedopuszczalnego ryzyka zidentyfikowanego zgodnie z pkt IS.D.OR.205, terminowo wdraża te środki i kontroluje ich ciągłą skuteczność. Środki te umożliwiają organizacji:

1) kontrolowanie okoliczności, które przyczyniają się do faktycznego wystąpienia scenariusza zagrożenia;

2) ograniczenie skutków dla bezpieczeństwa lotniczego urzeczywistnienia się scenariusza zagrożenia;

3) uniknięcia ryzyka.

Środki te nie mogą stwarzać jakiegokolwiek nowego potencjalnego niedopuszczalnego ryzyka dla bezpieczeństwa lotniczego.

b) Osobę, o której mowa w pkt IS.D.OR.240 lit. a) i b), oraz innych narażonych członków personelu organizacji należy powiadomić o wyniku oceny ryzyka przeprowadzonej zgodnie z pkt IS.D.OR.205 oraz o powiązanych scenariuszach zagrożenia i wprowadzanych środkach.

Organizacja informuje również organizacje, z którymi jest połączona interfejsem zgodnie z pkt IS.D.OR.205 lit. b), o każdym rodzaju ryzyka wspólnym dla obu organizacji.

IS.D.OR.215 System wewnętrznego zgłaszania zdarzeń związanych z bezpieczeństwem informacji

a) Organizacja ustanawia system wewnętrznego zgłaszania zdarzeń, aby móc gromadzić informacje o zdarzeniach związanych z bezpieczeństwem informacji, w tym o zdarzeniach zgłaszanych na podstawie pkt IS.D.OR.230, oraz oceniać takie zdarzenia.

b) Dzięki temu systemowi i procesowi, o którym mowa w pkt IS.D.OR.220, organizacja może:

1) określić, które zdarzenia zgłoszone na podstawie lit. a) uznaje się za incydenty związane z bezpieczeństwem informacji lub podatność o potencjalnym wpływie na bezpieczeństwo lotnicze;

2) określić przyczynę incydentów związanych z bezpieczeństwem informacji i podatności zidentyfikowanych zgodnie z pkt 1 oraz czynniki przyczyniające się do ich wystąpienia, a także uwzględnić je w procesie zarządzania ryzykiem związanym z bezpieczeństwem informacji zgodnie z pkt IS.D.OR.205 i IS.D.OR.220;

3) zapewnić ocenę wszystkich znanych, istotnych informacji dotyczących incydentów związanych z bezpieczeństwem informacji i podatności zidentyfikowanych zgodnie z ppkt 1;

4) zapewnić wdrożenie metody wewnętrznej dystrybucji informacji, stosownie do potrzeb.

c) Każda organizacja przyjmująca zlecenie, która może narazić organizację na ryzyko związane z bezpieczeństwem informacji o potencjalnym wpływie na bezpieczeństwo lotnicze, jest zobowiązana do zgłaszania organizacji zdarzeń związanych z bezpieczeństwem informacji. Takie zgłoszenia są dokonywane z użyciem procedur ustanowionych w drodze szczegółowych uzgodnień umownych oraz podlegają ocenie zgodnie z lit. b).

d) Organizacja współpracuje w ramach badań z każdą inną organizacją, która w sposób istotny przyczynia się do bezpieczeństwa informacji własnej działalności.

e) Organizacja może zintegrować taki system zgłaszania zdarzeń z innymi systemami zgłaszania, które już wdrożyła.

IS.D.OR.220 Incydenty związane z bezpieczeństwem informacji – wykrywanie, reagowanie i działania naprawcze

a) Na podstawie wyniku oceny ryzyka przeprowadzonej zgodnie z pkt IS.D.OR.205 i wyniku procesu zmniejszania ryzyka przeprowadzonego zgodnie z pkt IS.D.OR.210 organizacja wdraża środki służące do wykrywania incydentów i podatności, które wskazują na ewentualne urzeczywistnienie się niedopuszczalnego ryzyka i mogą mieć potencjalny wpływ na bezpieczeństwo lotnicze. Dzięki takim środkom wykrywania organizacja może:

1) identyfikować odstępstwa od wcześniej określonych wartości bazowych dotyczących osiągów funkcjonalnych;

2) wysyłać ostrzeżenia służące uruchomieniu odpowiednich środków reagowania w przypadku każdego odstępstwa.

b) Organizacja wdraża środki reagowania na wszelkie zdarzenia zidentyfikowane zgodnie z lit. a), które mogą przerodzić się lub już przerodziły się w incydent związany z bezpieczeństwem informacji. Dzięki takim środkom reagowania organizacja może:

1) rozpocząć działanie w reakcji na ostrzeżenia, o których mowa w lit. a) ppkt 2, poprzez uruchomienie wcześniej określonych zasobów i sposobu postępowania;

2) ograniczyć rozprzestrzenianie ataku i uniknąć pełnego urzeczywistnienia się scenariusza zagrożenia;

3) kontrolować tryb awaryjny uszkodzonych elementów określonych w pkt IS.D.OR.205 lit. a).

c) Organizacja wdraża środki służące przywróceniu stanu sprzed incydentów związanych z bezpieczeństwem informacji, w tym w razie potrzeby środki reagowania w sytuacjach zagrożeń. Dzięki takim środkom naprawczym organizacja może:

1) wyeliminować stan będący źródłem incydentu lub ograniczyć go do dopuszczalnego poziomu;

2) doprowadzić do bezpiecznego stanu uszkodzone elementy określone w pkt IS.D.OR.205 lit. a) w czasie naprawy wcześniej określonym przez organizację.

IS.D.OR.225 Reagowanie na niezgodności, o których powiadomił właściwy organ

a) Po otrzymaniu powiadomienia o niezgodnościach stwierdzonych przez właściwy organ organizacja:

1) identyfikuje przyczynę lub przyczyny niezgodności oraz czynniki sprzyjające jej wystąpieniu;

2) określa plan działań naprawczych;

3) wykazuje wyeliminowanie niezgodności w sposób spełniający oczekiwania właściwego organu.

b) Działania, o których mowa w lit. a), przeprowadza się w okresie uzgodnionym z właściwym organem.

IS.D.OR.230 System zewnętrznego zgłaszania zdarzeń związanych z bezpieczeństwem informacji

a) Organizacja wdraża system zgłaszania zdarzeń związanych z bezpieczeństwem informacji, który jest zgodny z wymaganiami określonymi w rozporządzeniu (UE) nr 376/2014 i w jego aktach delegowanych i wykonawczych, jeżeli rozporządzenie to ma zastosowanie do danej organizacji.

b) Bez uszczerbku dla obowiązków określonych w rozporządzeniu (UE) nr 376/2014 organizacja zapewnia, aby każdy incydent związany z bezpieczeństwem informacji lub podatność, które mogą stanowić poważne ryzyko dla bezpieczeństwa lotniczego, zgłaszano właściwemu organowi, któremu podlega. Ponadto:

1) jeżeli taki incydent lub taka podatność ma wpływ na statek powietrzny lub powiązany system lub komponent, organizacja zgłasza taki incydent lub taką podatność również posiadaczowi zatwierdzenia projektu;

2) jeżeli taki incydent lub taka podatność ma wpływ na system lub część składową wykorzystywane przez organizację, organizacja ta zgłasza taki incydent lub taką podatność organizacji odpowiedzialnej za projekt danego systemu lub danej części składowej.

c) Organizacja zgłasza stan, o których mowa w lit. b), w następujący sposób:

1) właściwemu organowi i, w stosownych przypadkach, posiadaczowi zatwierdzenia projektu lub organizacji odpowiedzialnej za projekt danego systemu lub danej części składowej zostaje przedstawione powiadomienie, jak tylko organizacja dowie się o zaistnieniu danego stanu;

2) właściwemu organowi i, w stosownych przypadkach, posiadaczowi zatwierdzenia projektu lub organizacji odpowiedzialnej za projekt danego systemu lub danej części składowej zostaje przedstawione zgłoszenie w możliwie najszybszym trybie, ale nie później niż 72 godziny od chwili, w której organizacja dowiedziała się o zaistnieniu danego stanu, chyba że wyjątkowe okoliczności to uniemożliwią.

Dokonywane zgłoszenie musi mieć formę określoną przez właściwy organ i musi zawierać wszystkie istotne informacje na temat stanu znanego organizacji;

3) właściwemu organowi i, w stosownych przypadkach, posiadaczowi zatwierdzenia projektu lub organizacji odpowiedzialnej za projekt danego systemu lub danej części składowej zostaje przedstawione zgłoszenie uzupełniające zawierające szczegóły działań, jakie organizacja podjęła lub zamierza podjąć w celu przywrócenia sytuacji sprzed incydentu, oraz działań, jakie zamierza podjąć w celu zapobieżenia występowaniu podobnych incydentów związanych z bezpieczeństwem informacji w przyszłości.

Zgłoszenie uzupełniające przedstawia się niezwłocznie po identyfikacji działań i sporządza się w formie określonej przez właściwy organ.

IS.D.OR.235 Zlecanie czynności w zakresie zarządzania bezpieczeństwem informacji

a) Organizacja zapewnia, aby w przypadku zlecenia innym organizacjom realizacji dowolnej części czynności, o których mowa w pkt IS.D.OR.200, zlecane czynności były zgodne z wymaganiami określonymi w niniejszym rozporządzeniu, a organizacja przyjmująca zlecenie wykonywała prace pod jej nadzorem. Organizacja zapewnia odpowiednie zarządzanie ryzykiem związanym ze zlecanymi czynnościami.

b) Organizacja zapewnia właściwemu organowi, na żądanie, możliwość dostępu do organizacji przyjmującej zlecenie w celu ustalenia stałego przestrzegania mających zastosowanie wymagań określonych w niniejszym rozporządzeniu.

IS.D.OR.240 Wymagania dotyczące personelu

a) Kierownik odpowiedzialny w organizacji lub, w przypadku organizacji projektujących, dyrektor organizacji projektującej wyznaczony zgodnie z rozporządzeniem (UE) nr 748/2012 i rozporządzeniem (UE) nr 139/2014, o których to organizacjach jest mowa w art. 2 ust. 1 lit. a) i b) niniejszego rozporządzenia, posiada uprawnienia służbowe w celu zapewnienia możliwości finansowania i prowadzenia wszystkich czynności wymaganych w niniejszym rozporządzeniu. Osoba ta:

1) zapewnia dostępność wszystkich zasobów niezbędnych do zapewnienia zgodności z wymaganiami niniejszego rozporządzenia;

2) ustanawia i promuje strategię bezpieczeństwa informacji, o której mowa w pkt IS.D.OR.200 lit. a) ppkt 1;

3) jest w stanie wykazać się podstawową wiedzą na temat niniejszego rozporządzenia.

b) Kierownik odpowiedzialny lub, w przypadku organizacji projektujących, dyrektor organizacji projektującej wyznacza osobę lub grupę osób odpowiedzialnych za utrzymanie zgodności organizacji z wymaganiami niniejszego rozporządzenia oraz określa zakres kompetencji tych osób. Taka osoba lub grupa osób odpowiada bezpośrednio przed kierownikiem odpowiedzialnym lub w przypadku organizacji projektujących dyrektorem organizacji projektującej oraz legitymuje się wiedzą, praktyką i doświadczeniem zawodowym odpowiednimi do powierzonego zakresu odpowiedzialności. W procedurach określa się, kto zastępuje daną osobę w przypadku jej długotrwałej nieobecności.

c) Kierownik odpowiedzialny lub, w przypadku organizacji projektujących, dyrektor organizacji projektującej wyznacza osobę lub grupę osób odpowiedzialnych za zarządzanie funkcją monitorowania zgodności, o której mowa w pkt IS.D.OR.200 lit. a) ppkt 12.

d) Jeżeli struktury organizacyjne, strategie, procesy i procedury w zakresie bezpieczeństwa informacji organizacji są wspólne z innymi organizacjami lub z obszarami własnej organizacji, które nie są objęte zatwierdzeniem ani oświadczeniem, kierownik odpowiedzialny lub, w przypadku organizacji projektujących, dyrektor organizacji projektującej mogą delegować swoje działania wspólnej osobie odpowiedzialnej.

W takim przypadku wprowadza się środki koordynacji między kierownikiem odpowiedzialnym organizacji lub, w przypadku organizacji projektujących, dyrektorem organizacji projektującej a wspólną osobą odpowiedzialną w celu zapewnienia odpowiedniej integracji zarządzania bezpieczeństwem informacji w organizacji.

e) Kierownik odpowiedzialny, lub dyrektor organizacji projektującej, lub wspólna osoba odpowiedzialna, o której mowa w lit. d), posiada uprawnienia służbowe do ustanowienia i utrzymania struktur organizacyjnych, strategii, procesów i procedur niezbędnych do wdrożenia pkt IS.D.OR.200.

f) Organizacja stosuje procedurę zapewniającą dysponowanie personelem dyżurującym wystarczającym do przeprowadzenia czynności objętych niniejszym załącznikiem.

g) Organizacja stosuje procedurę zapewniającą, aby personel, o którym mowa w lit. f), posiadał niezbędne kompetencje do realizacji powierzonych mu zadań.

h) Organizacja stosuje procedurę zapewniającą, aby personel przyjmował do wiadomości obowiązki związane z przydzielonymi funkcjami i zadaniami.

i) Organizacja zapewnia, aby prawidłowo ustalono tożsamość i wiarygodność personelu mającego dostęp do systemów informatycznych i danych podlegających wymaganiom niniejszego rozporządzenia.

IS.D.OR.245 Prowadzenie rejestrów

a) Organizacja prowadzi rejestr swoich działań w zakresie zarządzania bezpieczeństwem informacji.

1) Organizacja zapewnia, aby następujące zapisy były archiwizowane i możliwe do zidentyfikowania:

(i) każde otrzymane zatwierdzenie i każda powiązana ocena ryzyka związanego z bezpieczeństwem informacji zgodnie z pkt IS.D.OR.200 lit. e);

(ii) umowy dotyczące czynności, o których mowa w pkt IS.D.OR.200 lit. a) ppkt 9;

(iii) rejestr najważniejszych procesów, o których mowa w pkt IS.D.OR.200 lit. d);

(iv) dokumentacja ryzyka zidentyfikowanego w ocenie ryzyka, o której mowa w pkt IS.D.OR.205, wraz z powiązanymi środkami zmniejszania ryzyka, o których mowa w pkt IS.D.OR.210;

(v) dokumentacja incydentów związanych z bezpieczeństwem informacji i podatności zgłoszonych za pośrednictwem systemów zgłaszania zdarzeń, o których mowa w pkt IS.D.OR.215 i IS.D.OR.230;

(vi) dokumentacja zdarzeń związanych z bezpieczeństwem informacji, które mogą wymagać ponownej oceny w celu identyfikacji niewykrytych incydentów związanych z bezpieczeństwem informacji lub podatności.

2) Dokumentację, o której mowa w pkt 1 ppkt (i), przechowuje się przez co najmniej 5 lat od utraty ważności zatwierdzenia.

3) Dokumentację, o której mowa w pkt 1 ppkt (ii), przechowuje się przez co najmniej 5 lat od zmiany lub rozwiązania umowy.

4) Dokumentację, o której mowa w pkt 1 ppkt (iii), (iv) i (v), przechowuje się przez co najmniej 5 lat.

5) Dokumentację, o której mowa w pkt 1 ppkt (vi), przechowuje się do czasu ponownej oceny zdarzeń związanych z bezpieczeństwem informacji, dokonywanej z częstotliwością określoną w ramach procedury ustanowionej przez organizację.

b) Organizacja prowadzi rejestr kwalifikacji i doświadczenia własnego personelu zaangażowanego w działania w zakresie zarządzania bezpieczeństwem informacji.

1) Dokumentację kwalifikacji i doświadczenia członków personelu przechowuje się przez cały okres zatrudnienia tych osób w organizacji i przez co najmniej 3 lata po opuszczeniu przez nie organizacji.

2) Członkowie personelu na żądanie otrzymują dostęp do swoich akt osobowych. Ponadto organizacja przekazuje członkom personelu na żądanie egzemplarz ich akt osobowych w chwili, gdy osoby te opuszczają organizację.

c) Format dokumentacji musi być określony w procedurach organizacji.

d) Rejestry przechowuje się w sposób zapewniający ochronę przed uszkodzeniem, zmianą i kradzieżą, a informacje klasyfikowane, w razie potrzeby, w zależności od poziomu klauzuli tajności. Organizacja zapewnia przechowywanie rejestrów w sposób gwarantujący ich integralność, autentyczność i uprawniony dostęp.

IS.D.OR.250 Podręcznik zarządzania bezpieczeństwem informacji

a) Organizacja udostępnia właściwemu organowi podręcznik zarządzania bezpieczeństwem informacji oraz, w stosownych przypadkach, wszelkie przywołane powiązane podręczniki i procedury, zawierający:

1) oświadczenie podpisane przez kierownika odpowiedzialnego lub, w przypadku organizacji projektujących, dyrektora organizacji projektującej potwierdzające, że organizacja zawsze będzie prowadzić prace zgodnie z niniejszym załącznikiem i z podręcznikiem zarządzania bezpieczeństwem informacji. Jeżeli kierownik odpowiedzialny lub, w przypadku organizacji projektujących, dyrektor organizacji projektującej nie jest dyrektorem generalnym organizacji, wówczas taki dyrektor generalny musi kontrasygnować takie oświadczenie;

2) tytuł(-y), imię(imiona) i nazwisko(-a), obowiązki, zakresy odpowiedzialności, zadania i uprawnienia osoby lub osób, o których mowa w pkt IS.D.OR.240 lit. b) i c);

3) w stosownych przypadkach tytuł, imię i nazwisko, obowiązki, zakresy odpowiedzialności, zadania i uprawnienia wspólnej osoby odpowiedzialnej, o której mowa w pkt IS.D.OR.240 lit. d);

4) stosowaną przez organizację strategię bezpieczeństwa informacji, o której mowa w pkt IS.D.OR.200 lit. a) ppkt 1;

5) ogólny opis liczby i kategorii pracowników oraz wprowadzonego systemu umożliwiającego planowanie dostępności pracowników zgodnie z wymaganiami pkt IS.D.OR.240;

6) tytuł(-y), imię(imiona) i nazwisko(-a), obowiązki, zakresy odpowiedzialności, zadania i uprawnienia kluczowych osób odpowiedzialnych za realizację pkt IS.D.OR.200, w tym osoby lub osób odpowiedzialnych za funkcję monitorowania zgodności, o której mowa w pkt IS.D.OR.200 lit. a) ppkt 12;

7) schemat organizacyjny ukazujący powiązaną strukturę odpowiedzialności w odniesieniu do osób, o których mowa w ppkt 2 i 6;

8) opis systemu wewnętrznego zgłaszania zdarzeń, o którym mowa w pkt IS.D.OR.215;

9) procedury wskazujące, w jaki sposób organizacja zapewnia zgodność z niniejszą częścią, a w szczególności:

(i) pkt IS.D.OR.200 lit. c) dotyczący dokumentacji;

(ii) procedury określające, w jaki sposób organizacja kontroluje wszelkie zlecane czynności, o których mowa w pkt IS.D.OR.200 lit. a) ppkt 9;

(iii) procedurę zmiany podręcznika zarządzania bezpieczeństwem informacji określoną w lit. c);

10) szczegóły aktualnie zatwierdzonych alternatywnych sposobów spełnienia wymagań.

b) Właściwy organ zatwierdza pierwsze wydanie podręcznika zarządzania bezpieczeństwem informacji i zachowuje jego egzemplarz. W razie potrzeby w podręczniku zarządzania bezpieczeństwem informacji wprowadza się zmiany niezbędne do zachowania aktualnego opisu SZBI organizacji. Właściwy organ otrzymuje egzemplarz wszelkich zmian w podręczniku zarządzania bezpieczeństwem informacji.

c) Zarządzanie zmianami podręcznika zarządzania bezpieczeństwem informacji przebiega zgodnie z procedurą ustanowioną przez organizację. Wszelkie zmiany nieobjęte zakresem stosowania tej procedury, jak również wszelkie zmiany związane ze zmianami, o których mowa w pkt IS.D.OR.255 lit. b), podlegają zatwierdzeniu przez właściwy organ.

d) Organizacja może włączyć podręcznik zarządzania bezpieczeństwem informacji do innych posiadanych charakterystyk i podręczników zarządzania, pod warunkiem że stosuje się wyraźne odniesienia wskazujące, które części charakterystyki lub podręcznika zarządzania odnoszą się do poszczególnych wymagań zawartych w niniejszym załączniku.

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

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

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

W odniesieniu do takich zmian:

1) wniosek składa się przed zaistnieniem takiej zmiany w celu umożliwienia właściwemu organowi stwierdzenia, czy nadal istnieje zgodność z niniejszym rozporządzeniem, oraz – jeśli zajdzie taka potrzeba – zmiany certyfikatu organizacji szkoleniowej i powiązanych warunków zatwierdzania dołączonych do certyfikatu;

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

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

4) podczas wprowadzania tego typu zmian organizacja działa zgodnie z warunkami określonymi przez właściwy organ.

IS.D.OR.260 Ciągłe doskonalenie

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

b) Jeżeli w toku oceny przeprowadzonej zgodnie z lit. a) zostają wykryte uchybienia, organizacja podejmuje niezbędne środki poprawy w celu zapewnienia, aby system SZBI w dalszym ciągu był zgodny z mającymi zastosowanie wymaganiami i umożliwiał utrzymanie dopuszczalnego poziomu ryzyka związanego z bezpieczeństwem informacji. Ponadto organizacja ponownie ocenia elementy SZBI, na które przyjęte środki wpływają.