PART-IS

PRAKTYCZNY PRZEWODNIK

WDROŻENIOWY DLA ORGANIZACJI

(*) PRZEWODNIK OPRACOWANO NA BAZIE MATERIAŁÓW PART-IS.EU

SPIS TREŚCI

Wstęp

Określenie Part-IS odnosi się do przepisów uchwalonych w latach 2022-2023 w celu zwiększenia bezpieczeństwa informacji (znane również jako cyberbezpieczeństwo) w lotnictwie.

Przepisy te uwzględniają fakt, że branża lotnicza jest silnie powiązana i podatna na różne zagrożenia bezpieczeństwa, w tym cyber-ataki, błędy ludzkie i awarie procesów. Wdrażając te zasady, Unia Europejska dąży do ujednolicenia i wzmocnienia praktyk bezpieczeństwa i informacji, zwiększając w ten sposób odporność operacji lotniczych na złośliwe (zdolne do wyrządzenia szkody) zagrożenia i chroniąc bezpieczeństwo publiczne. Organizacje są zobowiązane do zintegrowania tych wymagań w zakresie bezpieczeństwa informacji z istniejącymi systemami zarządzania bezpieczeństwem lotniczym (SMS), zapewniając płynne i kompleksowe podejście do zarządzania zarówno ryzykiem związanym z bezpieczeństwem, jak i ochroną.

Podstawy prawne

Podstawa prawna dla PART-IS została ustanowiona przez **EAR-Easy Access Rules** dla bezpieczeństwa informacji. Dokument ten łączy wymagania ustanowione w różnych przepisach UE, zapewniając kompleksowy i czytelny format.

EAR dla ochrony informacji zawiera następujące rozporządzenia i decyzje:

Rozporządzenie wykonawcze Komisji (UE) 2023/203 z dnia 27 października 2022 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1139 w kwestii 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 1321/2014, (UE) nr 965/2012, (UE) nr 1178/2011, (UE) 2015/340, rozporządzeń wykonawczych Komisji (UE) 2017/373 i (UE) 2021/664 oraz właściwych organów objętych zakresem stosowania rozporządzeń Komisji (UE) nr 748/2012, (UE) nr 1321/2014, (UE) nr 965/2012, (UE) nr 1178/2011, (UE) 2015/340, rozporządzeń wykonawczych Komisji (UE) 2017/373, (UE) nr 139/2014 i (UE) 2021/664 oraz zmieniające rozporządzenia Komisji (UE) nr 1178/2011, (UE) nr 748/2012, (UE) nr 965/2012, (UE) nr 139/2014, (UE) nr 1321/2014, (UE) 2015/340 oraz rozporządzenia wykonawcze Komisji (UE) 2017/373 i (UE) 2021/664.

Niniejsze rozporządzenie ustanawia zasady stosowania *Rozporządzenia (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 (Tekst mający znaczenie dla EOG) dotyczącego zarządzania ryzykiem bezpieczeństwa informacji wpływającym na bezpieczeństwo lotnicze. Obejmuje ono organizacje i właściwe organy regulowane *Rozporządzeniem Komisji (UE) nr 1178/2011* z dnia 3 listopada 2011 r. ustanawiające wymagania techniczne i procedury administracyjne odnoszące się do załóg w lotnictwie cywilnym zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (WE) nr 216/2008 (Tekst mający znaczenie dla EOG) i zmienia wspomniane rozporządzenie, aby uwzględnić nowe wymagania.

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

Niniejsze rozporządzenie dotyczy również *Rozporządzenia (UE) 2018/1139*, określającego wymogi dotyczące zarządzania ryzykiem bezpieczeństwa informacji dla organizacji podlegających *Rozporządzeniom 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 (przekształcenie)-Tekst mający znaczenie dla EOG *i (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 (Tekst mający znaczenie dla EOG) oraz odpowiednio zmieniającego te rozporządzenia.

Decyzja ED 2023/008/R: Zarządzanie ryzykiem bezpieczeństwa informacji — AMC i GM do artykułów Rozporządzenia delegowanego Komisji (UE) 2022/1645 i Rozporządzenia wykonawczego Komisji (UE) 2023/203

Niniejsza decyzja określa dopuszczalne sposoby zapewnienia zgodności (AMC) i materiały informacyjne (GM) związane z artykułami *Rozporządzenia (UE) 2022/1645 i Rozporządzenia (UE) 2023/203*. Wspiera ona wdrażanie zarządzania ryzykiem bezpieczeństwa informacji w sektorze lotnictwa.

Decyzja ED 2023/009/R: Zarządzanie ryzykiem bezpieczeństwa informacji — AMC i GM do części IS.D.OR i części IS.I.OR

Decyzja ta oferuje AMC i GM w celu wsparcia wdrażania pakietu regulacyjnego Part-IS, ze szczególnym uwzględnieniem **Part-IS.D.OR** (Projektowanie wymagań dla organizacji) i **Part-IS.I.OR** (Wymagania organizacji).

Decyzja ED 2023/010/R: Zarządzanie ryzykiem bezpieczeństwa informacji — AMC i GM do części IS.AR

Decyzja ta zapewnia AMC i GM w celu wsparcia wdrażania pakietu regulacyjnego Part-IS, ze szczególnym uwzględnieniem Part-IS.AR (Wymagania władz).

Po opublikowaniu *Rozporządzenia wykonawczego (UE) 2023/203*, EASA zaktualizowała wiele swoich głównych rozporządzeń, aby uwzględnić szczegółowe przepisy dotyczące Part-IS. Na przykład rozporządzenie EASA dotyczące operacji lotniczych zostało zmienione rewizją 20 w czerwcu 2023 r. w celu wprowadzenia Part-ORO.GEN.200A nakazującego stosowanie Part-IS dla operatorów statków powietrznych.

Zastosowanie

Wymagania dokumentu PART-IS dzielą się na trzy główne części:

Part IS.AR (Wymagania dla właściwych organów): Ta część określa wymagania dla krajowych organów nadzoru lotniczego i Europejskiej Agencji Bezpieczeństwa Lotniczego (EASA) dotyczące ich obowiązków w zakresie nadzoru i zapewniania zgodności z przepisami dotyczącymi bezpieczeństwa informacji.

Part IS.I.OR (Wymagania dla organizacji zawarte w rozporządzeniu wykonawczym): Ta część określa wymagania dla organizacji lotniczych, takich jak: operatorzy statków powietrznych w lotnictwie biznesowym, CAMO, organizacje obsługi technicznej i organizacje szkoleniowe.

Part IS.D.OR (Wymagania dotyczące organizacji zawarte w rozporządzeniu delegowanym): Ta część szczegółowo opisuje wymagania dla organizacji projektujących, produkujących i operatorów lotnisk.

Niniejszy przewodnik jest przeznaczony dla organizacji podlegających Części IS.I.OR, która jest określona w Załączniku II do Rozporządzenia (UE) 2023/203.

Wymagania dla organizacji, których dotyczy część IS.I.OR wchodzą w życie 22 lutego 2026 r.

Kluczowe wymagania PART-IS

Podstawowym wymogiem Part-IS dla organizacji jest ustanowienie Systemu Zarządzania Bezpieczeństwem Informacji (ISMS). Szczegóły wdrożenia tego systemu w praktyce pozostawia się do decyzji organizacji. Wymagania można spełnić integrując odpowiednie rozdziały rozporządzenia z istniejącymi zasadami i dokumentami, lub tworząc zupełnie nowe zasady i procedury zgodne z rozporządzeniem. Niektóre z kluczowych koncepcji ISMS, określonych przez Part-IS są dokładniej wyjaśnione w kolejnych akapitach.

Zasady i procedury

Opracowanie kompleksowych zasad i procedur bezpieczeństwa informacji jest podstawowym wymogiem w ramach Part-IS. Zasady i procedury te stanowią podstawę ISMS, zapewniając usystematyzowane podejście do zarządzania i ograniczania ryzyka związanego z bezpieczeństwem informacji.

Z praktycznego punktu widzenia organizacja powinna zacząć od przeprowadzenia dokładnej oceny ryzyka w celu zidentyfikowania potencjalnych zagrożeń i luk. Na podstawie tych ustaleń opracowana powinna być polityka, która jasno określi akceptowalny sposób korzystania z systemów informatycznych, zapewniając, że wszyscy pracownicy rozumieją, co stanowi właściwe i niewłaściwe zachowanie podczas obsługi zasobów cyfrowych. Zasady te powinny obejmować różne scenariusze, w tym pracę zdalną, korzystanie z urządzeń mobilnych i przetwarzanie danych, aby zapewnić wszechstronne zabezpieczenie.

Oprócz zasad akceptowalnego sposobu użytkowania, niezbędne jest opracowanie szczegółowych planów reagowania na incydenty. Plany te powinny zawierać precyzyjne instrukcje jak postępować krok po kroku podczas wykrywania, zgłaszania i reagowania na incydenty związane z

bezpieczeństwem informacji. Powinny one określać role i obowiązki podczas obsługi incydentu, w tym kto jest odpowiedzialny za komunikację, dochodzenie i rozwiązanie problemu. Środki kontroli dostępu są kolejnym istotnym elementem; zasady te powinny określać, w jaki sposób dostęp do systemów informatycznych i danych jest udzielany, zarządzany i odwoływany/cofany.

Należy ustanowić jasne wytyczne dotyczące ochrony danych, w tym szyfrowania, przechowywania danych oraz ich bezpiecznego usuwania. Aby zapewnić skuteczność tej polityki, musi być ona łatwo dostępna dla wszystkich pracowników, regularnie przeglądana i aktualizowana. Dzięki temu będzie odzwierciedlać zmiany w technologii, przepisach i pojawiające się nowe zagrożenia. Należy prowadzić regularne szkolenia i wdrażać programy podnoszące świadomość personelu, aby pracownicy byli na bieżąco informowani i przestrzegali najnowszych praktyk w zakresie bezpieczeństwa.

Mapowanie zależności

Mapowanie zależności w organizacji jest kluczowym etapem wdrażania skutecznego Systemu Zarządzania Bezpieczeństwem Informacji (ISMS), zgodnie z wymaganiami Part-IS.I.OR.

Proces ten polega na identyfikacji i udokumentowaniu zależności pomiędzy jednostkami organizacyjnymi oraz ich powiązań z zewnętrznymi dostawcami usług. Zrozumienie tych współzależności jest niezbędne do stworzenia kompleksowej strategii zarządzania ryzykiem.

Należy rozpocząć od zaangażowania każdego działu w proces określenia jego kluczowych funkcji oraz wewnętrznych i zewnętrznych zasobów. To od nich zależy prowadzenie działalności. Obejmuje to identyfikację systemów oprogramowania, przepływów danych i usług stron trzecich, które wspierają codzienne działania.

Part-IS.I.OR kładzie szczególny nacisk na rolę zewnętrznych dostawców usług, takich jak dostawcy oprogramowania czy firmy outsourcingowe, w ramach systemu bezpieczeństwa informacji. Podczas mapowania tych zależności ważne jest, aby ocenić poziom bezpieczeństwa zewnętrznych partnerów oraz ustalić czy podlegają wymaganiom Part-IS.

Należy ocenić ich polityki, praktyki i mechanizmy kontroli bezpieczeństwa informacji, aby upewnić się, że spełniają one standardy organizacji i wymogi przepisów. Zgodnie z GM1 IS.I.OR.205(b), interfejsy z innymi podmiotami, takimi jak dostawcy usług i łańcuchy dostaw, powinny być identyfikowane na podstawie wymiany danych i informacji, ponieważ mogą prowadzić do zwiększonego ryzyka bezpieczeństwa informacji z powodu wzajemnego narażenia.

Umowy z tymi dostawcami powinny zawierać klauzule, które wymagają zgodności z wymaganiami organizacji dotyczącymi bezpieczeństwa oraz umożliwiają przeprowadzanie audytów w celu weryfikacji przestrzegania tych standardów.

Ocena ryzyka i zarządzanie

W początkowej fazie wdrażania Part-IS, przeprowadzenie dokładnej oceny ryzyka jest kluczowe dla identyfikacji zagrożeń bezpieczeństwa informacji, które mogą mieć wpływ na bezpieczeństwo lotnicze. Należy zacząć od stworzenia dedykowanego zespołu, który będzie składać się z

przedstawicieli różnych działów, między innymi: IT, operacji naziemnych, operacji lotniczych, szkoleń, obsługi technicznej, czarterów, finansów, zasobów ludzkich i przedstawicieli kadry zarządzającej.

Zespół ten powinien przeprowadzić całościowy przegląd wszystkich systemów informacyjnych i komunikacyjnych oraz dostępnych danych by móc zidentyfikować potencjalne słabe punkty i zagrożenia. Możliwe jest wykorzystanie standardowych ram / narzędzi branżowych, takich jak ISO 27001, NIST lub dedykowany zestaw narzędzi Part-IS, aby prowadzić proces oceny w sposób systematyczny i dokładny.

Ustalenia należy udokumentować w rejestrze ryzyka, kategoryzując ryzyka w oparciu o ich potencjalny wpływ na bezpieczeństwo oraz prawdopodobieństwo wystąpienia. Takie ustrukturyzowane podejście zapewnia zidentyfikowanie wszystkich potencjalnych ryzyk i ustalenie ich priorytetów.

Po zakończeniu oceny ryzyka, kolejnym krokiem jest opracowanie i wdrożenie planów postępowania z ryzykiem, aby ograniczyć zidentyfikowane zagrożenia. Polega to na wyborze odpowiednich środków kontroli, a także działań mających na celu zmniejszenie ryzyka w zależności od jego wagi.

W przypadku ryzyka o charakterze technicznym, warto rozważyć wdrożenie rozwiązań takich jak zapory sieciowe (firewalle), szyfrowanie, zarządzanie hasłami i systemy wykrywania włamań. W przypadku ryzyka związanego z procesami, należy wprowadzić usprawnienia, takie jak regularne audyty, procedury reagowania na incydenty oraz środki kontroli dostępu.

Należy upewnić się, że wszystkie środki ograniczające ryzyko są udokumentowane oraz zintegrowane z systemem ISMS. Plany te powinny być regularnie przeglądane i aktualizowane, aby dostosować je do nowych zagrożeń i zmian w środowisku organizacyjnym przy zastosowaniu proaktywnego podejścia do zarządzania bezpieczeństwem informacji.

Wykrywanie incydentów, reagowanie na nie i przywracanie do stanu normalnego

Ustanowienie skutecznych mechanizmów wykrywania incydentów, odpowiednie reagowanie na nie oraz odzyskiwanie danych będzie miało kluczowe znaczenie dla ochrony zasobów informacyjnych organizacji. Należy zacząć od zainstalowania i konfiguracji zaawansowanych narzędzi monitorujących, które będą wykrywać potencjalne zagrożenia w czasie rzeczywistym. Narzędzia te powinny być zdolne do identyfikacji nietypowych wzorców, takich jak nieautoryzowane próby dostępu, aktywność złośliwego oprogramowania i wycieki danych.

Należy wyznaczyć zespół (wewnętrzny lub zewnętrzny) odpowiedzialny za ciągłe monitorowanie tych alertów i zapewnianie szybkiego wykrywania incydentów.

Opracowany przez organizację plan reagowania na incydenty określi jakie kroki należy podjąć po zidentyfikowaniu potencjalnego zagrożenia, w tym opisze natychmiastowe działania mające na celu zatrzymanie takiego zagrożenia, by natychmiast zapobiec dalszym szkodom.

Istotne jest ustanowienie procedur reagowania na incydenty oraz odzyskiwania danych po takich incydentach. Procedury te powinny szczegółowo określać role i obowiązki odpowiednich pracowników w razie wykrycia incydentu. Zapewni to skoordynowane i efektywne działania.

Należy wdrożyć ustrukturyzowany proces oceny wpływu incydentu, określenia jego zakresu oraz identyfikacji dotkniętych systemów i danych.

Następnie należy wdrożyć środki ograniczające rozprzestrzenianie się zagrożenia, działania mające na celu usunięcie szkodliwych elementów oraz kroki mające na celu przywrócenie normalnego działania uszkodzonych systemów i danych. Warto zawsze upewnić się, że wszystkie podjęte działania są udokumentowane na potrzeby analizy i raportowania po incydencie.

Opracowany przez organizację plan ciągłości działania powinien zawierać strategie utrzymania podstawowych operacji i bezpieczeństwa lotów w trakcie incydentu, minimalizacji zakłóceń oraz szybkiego powrotu do normalnego działania.

Należy regularnie testować i aktualizować te procedury za pomocą symulacji i ćwiczeń, aby zapewnić gotowość i skuteczność w rzeczywistych sytuacjach.

Szkolenie personelu

Kiedy rozważamy bezpieczeństwo informacji, zazwyczaj skupiamy się na wymaganiach technicznych i funkcjach zarządzanych przez dział IT. Jednak powszechnie uznaje się, że jednym z najbardziej podatnych punktów bezpieczeństwa organizacji jest jej personel. Błędy ludzkie, brak świadomości i niewystarczające szkolenia, mogą prowadzić do poważnych naruszeń bezpieczeństwa. Dlatego szkolenie personelu jest kluczowym elementem Systemu Zarządzania Bezpieczeństwem Informacji (ISMS) opisanego w Part-IS.I.OR.

Na etapie początkowej implementacji konieczne jest opracowanie kompleksowego programu szkoleniowego, który obejmie wszystkie aspekty bezpieczeństwa informacji istotne dla danej organizacji. Należy rozpocząć od analizy potrzeb szkoleniowych, aby zidentyfikować luki w wiedzy i określić wymagania szkoleniowe dla różnych ról / stanowisk w organizacji.

Następnie należy odpowiednio dostosować moduły szkoleniowe w taki sposób, by odpowiadały konkretnym potrzebom, w tym tematy takie jak rozpoznawanie prób wyłudzania informacji (phishingu), prawidłowe postępowanie z danymi osobowymi oraz znaczenie przestrzegania protokołów bezpieczeństwa.

Regularne sesje szkoleniowe, warsztaty i moduły e-learningowe mogą być skuteczne w utrzymywaniu wysokiego poziomu świadomości bezpieczeństwa wśród pracowników. Dodatkowo, należy wdrożyć okresowe oceny i kursy odświeżające wiedzę, aby upewnić się, że pracownicy pozostają na bieżąco z najnowszymi praktykami i zagrożeniami w zakresie bezpieczeństwa.

Raportowanie i ciągłe doskonalenie

Prowadzenie szczegółowej dokumentacji incydentów związanych z bezpieczeństwem informacji i podjętych działań ma zasadnicze znaczenie dla skuteczności Systemu Zarządzania Bezpieczeństwem Informacji (ISMS). W początkowej fazie wdrażania należy ustanowić solidne wewnętrzne mechanizmy raportowania, zapewniające terminową / bieżącą komunikację dotyczącą incydentów w organizacji.

Każdy incydent powinien być odpowiednio udokumentowany – należy opisać jego charakter, podjęte działania oraz rezultaty tych działań. Taka dokumentacja nie tylko pomaga lepiej zrozumieć dany incydent, ale również dostarcza cenne dane do analizy trendów i identyfikacji powtarzających się problemów.

Należy również zadbać o to, aby zapisy incydentów były bezpiecznie przechowywane i łatwo dostępne do wykorzystania w przyszłości na potrzeby audytów zgodności oraz analiz.

Oprócz wewnętrznego raportowania, konieczne jest zgłaszanie poważnych incydentów odpowiednim organom, zgodnie z wymogami IS.I.OR.230. Zapewnia to przejrzystość i zgodność z przepisami prawa, co pomaga budować zaufanie wobec organów regulacyjnych i interesariuszy.

Należy regularnie monitorować i aktualizować swoje procedury w oparciu o wnioski wyciągnięte z przeszłych incydentów i zmieniających się zagrożeń. Okresowe audyty i oceny powinny być przeprowadzane w celu oceny skuteczności zastosowanych środków bezpieczeństwa oraz identyfikacji obszarów wymagających doskonalenia.

Warto promować kulturę informacji zwrotnej w organizacji. Dzięki temu pracownicy mogą proponować usprawnienia i zgłaszać potencjalne luki bez obawy przed ukaraniem.

Integracja z istniejącym SMS

Part IS.I.OR zapewnia elastyczność organizacjom w zakresie integracji Systemu Zarządzania Bezpieczeństwem Informacji (ISMS) z istniejącymi systemami zarządzania. To podejście jest zarówno praktyczne, jak i efektywne, ponieważ pozwala organizacjom na wykorzystanie bieżących procesów, polityk, zasad i mechanizmów kontroli, zmniejszając tym samym dodatkowy wysiłek i koszty związane z wdrażaniem nowego, samodzielnego systemu.

Zgodnie z materiałem informacyjnym GM1 IS.I.OR.200(d), taka integracja pomoże zapewnić spójność i zgodność z ogólnym podejściem organizacji do zarządzania.

Zintegrowane podejście oznacza, że organizacje mogą wykorzystywać swoje funkcjonujące już systemy zarządzania bezpieczeństwem (SMS) jako fundament dla ISMS. Na przykład istniejące procesy zarządzania ryzykiem mogą zostać dostosowane w taki sposób, aby uwzględniały ryzyka związane z bezpieczeństwem informacji, dostosowując je do ryzyka związanego z bezpieczeństwem lotniczym.

Ponadto obecne środki kontroli, takie jak zarządzanie dostępem i procedury reagowania na incydenty, można rozszerzyć o aspekty bezpieczeństwa informacji. Takie podejście usprawnia wdrożenie, przyspiesza proces zaznajamiania się z systemem oraz wspiera ciągłe doskonalenie poprzez wykorzystanie istniejących mechanizmów w ramach SMS do regularnych przeglądów i aktualizacji.

To całościowe podejście nie tylko upraszcza proces wdrażania, ale też zapewnia, że bezpieczeństwo informacji jest osadzone w szerzej pojmowanej kulturze bezpieczeństwa organizacji, wspierając jednolite zaangażowanie w ochronę zarówno zasobów fizycznych, jak i cyfrowych.

Następne kroki

Gdy organizacja rozpoczyna proces wdrożenia Part-IS, zainicjowanie wstępnej oceny w każdym dziale jest kluczowym krokiem. Ten proaktywny środek pomaga rozwijać kulturę bezpieczeństwa informacji w całej organizacji. Należy więc zachęcać każdy dział / komórkę organizacyjną do oceny konkretnych ryzyk i podatności związanych z bezpieczeństwem informacji. Angażując wszystkich od samego początku, zapewnia się kompleksowe zrozumienie potencjalnych ryzyk i wspiera kulturę świadomości bezpieczeństwa w całej organizacji. Ustanowienie sprawnego kanału komunikacji z właściwym organem jest również niezbędne. Wczesne zaangażowanie tego organu może zapewnić cenne spostrzeżenia i wskazówki, pomagając zapewnić zgodność z wymogami Part-IS. Bycie jednym z pierwszych podmiotów wdrażających część IS będzie korzystne dla organizacji. Takie podejście nie tylko pokazuje zaangażowanie organizacji w bezpieczeństwo informacji, ale także pozycjonuje ją jako lidera w zakresie zgodności i najlepszych praktyk bezpieczeństwa. To proaktywne podejście może korzystnie wpłynąć na reputację i zbudować zaufanie wśród interesariuszy, klientów i właściwych organów.