Szablon sprawozdania z audytu zgodnego z ustawą o krajowym systemie cyberbezpieczeństwa[1]

[1] Szablon należy interpretować jako wzór audytu oceny operatora usługi kluczowej zgodnie z krajowym systemem cyberbezpieczeństwa. Szablon należy wypełnić przy zachowaniu struktury rozdziałów pierwszego, drugiego i trzeciego poziomu. W celu zachowania zgodności oraz porównywalności niedopuszczalne jest kasowanie i modyfikowanie struktury rozdziałów. Zalecane jest dodawane podrozdziałów trzeciego poziomu zgodnie ze stanem faktycznym oraz wykonanymi pracami, jeżeli w opinii zespołu audytowego obecna struktura dokumentu nie jest kompletna. Nie należy usuwać żadnych rozdziałów z szablonu. Wszystkie niewypełnione rozdziały i podrozdziały powinny zostać oznaczone jako nieadekwatne z uzasadnieniem audytora.

Metryka sprawozdania z audytu UKSC

Metryka audytu:

Opis	Treść
Audytowana jednostka organizacyjna	
Cel audytu:	potwierdzenie zgodności bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia Usług Kluczowych z wymaganiami ustawy o krajowym systemie cyberbezpieczeństwa
Kryteria audytu	ustawa o krajowym systemie cyberbezpieczeństwa z 5 lipca 2018 wraz z rozporządzeniami
Data rozpoczęcia i zakończenia audytu	
Data wydania raportu	
Data sprawozdania poprzedniego i ilość niezgodności	
Data sprawozdania poprzedniego do poprzedniego i ilość niezgodności	

UK 1: <nazwa usługi kluczowej>[2]

Opis	Treść
Nazwa procesu	
Audytowane lokalizacje:	należy podać pełne dane teleadresowe
Zakres audytu – działalność	nazwa i zakres Usług Kluczowych
Zakres audytu – process	wsparcie systemu informacyjnego dla Usługi Kluczowej
Certyfikowane systemy zarządzania	System Zarządzania Bezpieczeństwem Informacji zgodny z ISO 27001, System Zarządzania Ciągłością Działania zgodny z ISO 22301, etc.
Zasoby informatyczne, w szczególności	wpisać ilość serwerów, systemy przetwarzania, aplikacje, bazy danych, stacje robocze, etc.
Systemy informacyjne od których zależy Usługa Kluczowa	
Data decyzji o uznaniu za OUK	
Sektor	
Podsektor	

[2] Proszę wypełnić tabelę oddzielnie dla każdego z audytowanych Usług Kluczowych (UK)

Opis	Treść
Opis progu uznania Incydentu za poważny	

Odpowiedzialności instytucjonalne w OUK

Osoby odpowiedzialne w OUK	Imię i Nazwisko
Prezes/dyrektor generalny	
Audytor wewnętrzny	
Pełnomocnik OUK	
Nadzorujący audyt OUK	

Odpowiedzialności procesowe (formalne i nieformalne) w OUK

Typ procesu / aktywności wymaganej w UKSC	Imię i Nazwisko pracownika OUK lub dane PŚUB, wyznaczonego przez Najwyższe Kierownictwo jako właściwego merytorycznie do uczestnictwa w Audycie[3]		
	UK 1	UK 2	UK 3
Zarządzanie ryzykiem			
Zarządzanie incydentem			
Identyfikacja zagrożeń			
Zarządzanie podatnościami			
Zarządzanie środkami technicznymi			
Zarządzanie środkami organizacyjnymi			
Utrzymanie i eksploatacja SI_OUK			
Bezpieczeństwo fizyczne i środowiskowe			
Bezpieczeństwo i ciągłość dostaw usług			
Zarządzanie ciągłością działania UK			
Zarządzanie systemem monitorowania w trybie ciągłym			
Zarządzanie łącznością w ramach UKSC			

[3] Proszę uzupełnić informacje oddzielnie dla każdej z audytowanych Usług Kluczowych (UK)

Informacja o audytorach wykonujących

Funkcja audytowa	Imię i Nazwisko	Potwierdzenie kwalifikacje (certyfikaty, wykształcenie i doświadczenie)	Audytowany obszar[4]
Audytor wiodący			
Audytor systemy operacyjne			
Audytor warstwa aplikacji i baz danych			
Audytor procesów 27001			
Audytor procesów 22301			
Audytor bezpieczeństwa procesów biznesowych			
Audytor systemów typu ICS / SCADA / OT			

Granica konfliktu interesu: Osoby tworzące zespół audytowy i bezpośrednio zaangażowane w weryfikacje zgodności muszą pozostać obiektywne i niezależne. Oznacza, to iż działając w ramach międzynarodowych standardów audytu nie mogą dokonywać oceny obszaru, za który były odpowiedzialne lub prowadziły czynności doradcze. Wszystkie osoby zaangażowane w badanie składają oświadczenie o braku konfliktu interesów, w szczególności w terminie ostatnich 24 miesięcy nie wykonywały osobiście prac doradczych, projektowych, architektonicznych lub implementacyjnych na rzecz audytowanego podmiotu w zakresie audytowanej usługi kluczowej.

Niezgodności z poprzednich dwóch audytów UKSC

Audyt poprzedni (jeśli dotyczy) z dnia:

Stwierdzenie faktu i opis niezgodności (w tym odniesienie do kryterium)	Priorytet	Data zamknięcia niezgodności

[4] Jeżeli będzie to zasadne proszę uzupełnić o informację o audytowanej UK

Audyt poprzedni do poprzedniego (jeśli dotyczy) z dnia:

Stwierdzenie faktu i opis niezgodności (w tym odniesienie do kryterium)	Priorytet	Data zamknięcia niezgodności

Podsumowanie dla kierownictwa

W dniach ..... - ..... przeprowadzono audyt cyberbezpieczeństwa na podstawie wymagań ustawy o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 1560). Prace audytowe zostały przeprowadzone przez ..... zgodnie z umową z dnia .....

Pierwszy etap prac polegał na "Zrozumieniu kontekstu działania organizacji oraz analizy dokumentacji" i został przeprowadzony w dniach ..... - ..... . Na podstawie dowodów audytowych udało się zidentyfikować .... niezgodności oraz zaplanowano drugi etap prac polegający na " Testach skuteczności funkcjonowania mechanizmów kontrolnych". Audytowi poddano … usług kluczowych obejmujących ..... procesów w ..... lokalizacjach oraz działalność .... dostawców i usługodawców.

Zgromadzone dowody pozwalają /nie pozwalają na wydanie opinii audytorskiej i wydajemy opinię …….. (pozytywną, pozytywną z zastrzeżeniami, negatywną) / odstępujemy od badania.

Podczas audytu zidentyfikowano ..... niezgodności o krytycznym priorytecie, ... niezgodności o wysokim priorytecie, ... niezgodności o średnim priorytecie oraz ..... niezgodności o niskim priorytecie. Priorytety prac odnoszą się do potencjalnych poziomów istotności i należy je rozumieć w następujący sposób:

POZIOM ISTOTNOŚCI	INTERPRETACJA
KRYTYCZNY	Zidentyfikowano niezgodności świadczące o wystąpieniu incydentu poważnego lub wskazujące na nieskuteczność zabezpieczeń bezpośrednio umożliwiającą wystąpienie incydentu poważnego
WYSOKI	Wymagania, zabezpieczenia nie wdrożone – nie przedstawiono żadnego z wymaganych dokumentów oraz nie istnieją wewnętrzne nieformalne działania, które są powtarzalne i spełniają dobre praktyki wskazane w wymaganiu. Brak realizacji lub realizacja zadań na poziomie niskim. Znaczne prawdopodobieństwo naruszenia zapisów UKSC.
ŚREDNI	Wymagania, zabezpieczenia częściowo wdrożone – zachodzi co najmniej jedna z następujących okoliczności: • istnieje dokument, który został formalnie przyjęty (zatwierdzony) do stosowania, ale nie był aktualizowany po zmianach organizacyjnych lub technicznych; • zidentyfikowano dokument, jednakże nie znaleziono potwierdzenia, że zapisy są stosowane (przestrzegane) w praktyce lub testy techniczne (jeśli zabezpieczenie podlegało testom) wykazały istotne słabości zabezpieczenia;

POZIOM ISTOTNOŚCI	INTERPRETACJA
	• istniejący dokument nie zawiera wszystkich treści wymaganych przez wymagania lub wynikających z tzw. dobrych praktyk; • istnieją wewnętrzne nieformalne działania, które są powtarzalne, jednakże nie w pełni spełniają dobre praktyki wskazane w wymaganiu. Prawdopodobne uchybienia w realizacji zapisów UKSC.
NISKI	Istnieje(ą) dokument(y) formalnie przyjęty (zatwierdzony) do stosowania, który określa sposób realizacji danego zabezpieczenia lub testy techniczne (jeśli zabezpieczenie podlegało testom) wykazały skuteczne funkcjonowanie zabezpieczenia lub spełnienia wymogu.
NIE DOTYCZY	Zakres audytu nie obejmował danego obszaru lub ustalenia potwierdzają, iż obszar nie dotyczy danej organizacji.

Zdaniem zespołu audytowego, najważniejszymi niezgodnościami, którymi, w pierwszej kolejności powinno zająć się najwyższe kierownictwo są:

.....

Numer audytowanej UK, stwierdzenie faktu i opis niezgodności (w tym odniesienie do kryterium)	Priorytet

.....

Cel i zakres prac

Cel prac

Celem wykonanych prac była ocena bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usług kluczowych realizowanych przez ....<nazwa klienta>... oraz identyfikacja i analiza luki zgodności z wymaganiami ustawy o krajowym systemie cyberbezpieczeństwa.

Zakres prac

Zakres prac obejmował:

- zrozumienie kontekstu działania organizacji w tym wpływ systemów IT i/lub OT (SI_OUK) na usługi kluczowe;

- potwierdzenie realizacji obowiązków operatora usługi kluczowej zgodnie z artykułami 8-16 ustawy o krajowym systemie cyberbezpieczeństwa;
- analizę dokumentacji dotyczącą cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usług kluczowych;
- testy skuteczności funkcjonowania mechanizmów kontrolnych;
- opracowanie sprawozdania zawierającego opis zidentyfikowanych niezgodności wraz z rekomendacjami;
- przestawienie wyników audytu dla Najwyższego Kierownictwa.

Analiza objęła następujące usługi kluczowe:

- Usługa 1: …

- Usługa 2: …

Przebieg prac

Prace zostały wykonane w dniach ..... - ..... i polegały na analizie wybranej dokumentacji, wywiadach z wybranymi pracownikami, obserwacjach i wizji lokalnej w ..... jednostkach. Dodatkowo w ramach audytu przeprowadzono testy techniczne obejmujące swoim zakresem:

- weryfikację podatności na ... stacjach
- weryfikację luk w systemach ....

Prace realizowane były zgodnie z następującym harmonogramem:

1. Uruchomienie prac audytowych i spotkanie organizacyjne
2. Planowanie prac
3. Etap I
4. Etap II
5. Raportowanie wyników analizy luki zgodności
6. Przesłanie sprawozdania do uzgodnień
7. Przygotowanie ostatecznej wersji sprawozdania
8. Omówienie wyników analizy niezgodności

Wykluczenia i ograniczenia zakresu

Ograniczenie zakresu nałożone na Zespół Audytowy, które nie pozwoliły na realizację szczegółowych celów i planów Audytu bazujących na zapisach ustawy, rozporządzeń, metodyki lub/i charakteru organizacji:

- Brak

Opinia z badania

Przebieg audytu przeprowadzony był zgodnie ze standardami zapewnienia ustanowionymi przez (*wpisać na podstawie jakich standardów prowadzony był audyt np. ISACA, IIA*). Te standardy wymagają, aby prace audytowe były zaplanowane i wykonane tak, aby ich wynikiem było rozsądne zapewnienie, że we wszystkich istotnych obszarach system bezpieczeństwa jest rzetelnie przygotowany, a mechanizmy kontrolne odpowiednio zaprojektowane i operują w taki sposób, aby osiągnąć związane z nimi cele kontroli. Wierzymy, że zgromadzone dowody pozwalają /nie pozwalają na wydanie opinii audytorskiej i wydajemy opinię …… (pozytywną, pozytywną z zastrzeżeniami, negatywną) / odstępujemy od badania.

Uzasadnieniem wyboru oceny jest ……

Wyniki prac

Szczegółowe wyniki wykonanych prac obejmują ocenę zgodności z wymaganiami ustawy o krajowym systemie cyberbezpieczeństwa, w tym zidentyfikowane niezgodności, które mogą mieć wpływ na świadczenie usług kluczowych.

Do określenia skutków zidentyfikowanych niezgodności wykorzystano następujące skale:

POZIOM ISTOTNOŚCI	**INTERPRETACJA**
KRYTYCZNY	Zidentyfikowano niezgodności świadczące o wystąpieniu incydentu poważnego lub wskazujące na nieskuteczność zabezpieczeń bezpośrednio umożliwiającą wystąpienie Incydentu Poważnego
WYSOKI	Wymagania, zabezpieczenia nie wdrożone – nie przedstawiono żadnego z wymaganych dokumentów oraz nie istnieją wewnętrzne nieformalne działania, które są powtarzalne i spełniają dobre praktyki wskazane w wymaganiu. Brak realizacji lub realizacja zadań na poziomie niskim. Znaczne prawdopodobieństwo naruszenia zapisów UKSC
ŚREDNI	Wymagania, zabezpieczenia częściowo wdrożone – zachodzi co najmniej jedna z następujących okoliczności: • istnieje dokument, który został formalnie przyjęty(zatwierdzony) do stosowania, ale nie był aktualizowany po zmianach organizacyjnych lub technicznych; • zidentyfikowano dokument, jednakże nie znaleziono potwierdzenia, że zapisy są stosowane (przestrzegane) w praktyce lub testy techniczne (jeśli zabezpieczenie podlegało testom) wykazały istotne słabości zabezpieczenia; • istniejący dokument nie zawiera wszystkich treści wymaganych przez wymagania lub wynikających z tzw. dobrych praktyk; • · istnieją wewnętrzne nieformalne działania, które są powtarzalne, jednakże nie w pełni spełniają dobre praktyki wskazane w wymaganiu. Prawdopodobne uchybienia w realizacji zapisów UKSC.

POZIOM ISTOTNOŚCI	INTERPRETACJA
NISKI	Istnieje(ą) dokument(y) formalnie przyjęty (zatwierdzony) do stosowania, który określa sposób realizacji danego zabezpieczenia lub testy techniczne (jeśli zabezpieczenie podlegało testom) wykazały skuteczne funkcjonowanie zabezpieczenia lub spełnienia wymogu. Istnieją wewnętrzne nieformalne działania, które są powtarzalne i w pełni spełniają dobre praktyki wskazane w wymaganiu. Pełna realizacja zadań lub realizacja zadań na poziomie prawie pełnym.
NIE DOTYCZY	Zakres audytu nie obejmował danego obszaru lub ustalenia potwierdzają, iż obszar nie dotyczy danej organizacji.

Poszczególne niezgodności powinny zostać usunięte zgodnie z wdrożonym w organizacji procesem zarządzania ryzykiem. Terminowość i skuteczność wdrożenia rekomendacji powstałych w wyniku niniejszego audytu powinna stanowić wkład w kolejne audyty zgodności z wymaganiami UKSC. Może też być elementem przeglądów realizowanych przed podmioty nadzorcze w ramach Art 42 UKSC.

W ramach każdego z weryfikowanych obszarów zgrupowano obserwacje powstałe w wyniku analizy dokumentacji, obserwacji i wywiadów, testów przeprowadzonych w ramach audytu oraz analizy innych przedstawionych wyników testów technicznych.

Obszar 1: Organizacja zarządzania bezpieczeństwem informacji

W ramach audytu zespół koncentrował się na potwierdzeniu zgodności z wymaganiami w zakresie stworzenia i utrzymywania systemu zarządzania zapewniającego zgodność z UKSC.

Kontekst w zakresie przepisów i normy

Zakres prac obejmował między innymi adekwatne wymagania:

- Artykułu 8, 9,10, 14, 15 i 16 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560 ze zm.);
- Rozporządzenia Ministra Cyfryzacji z dnia 4 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo (Dz.U. 2019 poz. 2479);
- Rozporządzenia Rady Ministrów z dnia 16 października 2018 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej (Dz. U. poz. 2080);
- Rozporządzenia Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz. U. poz. 1999);
- Rozporządzenia Ministra Cyfryzacji z dnia 20 września 2018 r. w sprawie kryteriów uznania naruszenia bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych za naruszenie o istotnym wpływie na funkcjonowanie sieci lub usług (Dz. U. poz. 1830);
- Polskiej Normy PN-EN ISO/IEC 27001 w rozdziałach 5, 7, 9 i 10;
- Załącznika A do Polskiej Normy PN-EN ISO/IEC 27001 w wymaganiach A.5, A.6 i A.18.

Kontekst w zakresie Decyzji OUK

Dokumentacja potwierdzająca wykonane działania zgodnie z harmonogramem wskazanym w ustawie:

- Czynności wykonane w terminie 3 miesięcy
- Czynności wykonane w terminie 6 miesięcy
- Czynności wykonane w terminie 12 miesięcy

Opis Identyfikacji systemu informacyjnego wspierającego usługę kluczową:

- lista elementów składowych
- lista osób odpowiedzialnych

Dokumentacja Systemu Informacyjnego wspierającego usługę kluczową

1. Raporty z audytów systemów informacyjnych wspierających usługę kluczową
2. Potwierdzenie działań wynikających z komunikacji z procesem szacowania ryzyka SI_OUK
3. Dokumentacja architektury zastosowanych zabezpieczeń
4. Dokumentacja architektury sieci
5. Baza danych konfiguracji urządzeń aktywnych
6. Dokumentacja zmian w systemach informacyjnych
7. Dokumentacja dotycząca monitorowania w trybie ciągłym
8. Umowy z dostawcami (wsparcie techniczne) itp.
9. Umowy z dostawcami usług z zakresu cyberbezpieczeństwa
10. Wyniki audytów u dostawców usług cyberbezpieczeństwa
11. Dokumentacja zabezpieczeń fizycznych i środowiskowych
12. Rejestr dostępu do dokumentacji systemu informacyjnego

Wnioski z prac audytowych

Niezgodności zidentyfikowane w czasie audytu

ID	Numer UK	Zdarzenie niepożądane	Opis ryzyka	Priorytet
1				
2				
3				
4				

Zalecenia

ID	Numer UK	Obserwacja	Rekomendacje
1			
2			
3			
4			

Obszar 2: Procesy zarządzania bezpieczeństwem informacji

W ramach audytu zespół koncentrował się na potwierdzeniu zgodności z wymaganiami bezpieczeństwa informacji w zakresie poprawności ich zdefiniowania, wdrożenia, eksploatacji i nadzorowania procesów zapewniających bezpieczeństwem informacji.

Kontekst w zakresie przepisów i normy

Zakres prac obejmował między innymi adekwatne wymagania:

- Artykułu 8,10,11,15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560 ze zm.);
- Rozporządzenia Rady Ministrów z dnia 16 października 2018 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej (Dz. U. poz. 2080);
- Rozporządzenia Rady Ministrów z dnia 31 października 2018 r. w sprawie progów uznania incydentu za poważny (Dz. U. poz. 2180);
- Polskiej Normy PN-EN ISO/IEC 27001 w rozdziałach 6, 8;
- Wszystkie z wymienionych w Załączniku A do Polskiej Normy PN-EN ISO/IEC 27001.

Kontekst w zakresie Decyzji OUK

System zarządzania bezpieczeństwem informacji bazujący na ISO-27001

1. Weryfikacja polityki bezpieczeństwa. Określone i zakomunikowane cele działania systemu w odpowiedzialnej komórce za cyberbezpieczeństwo (Dz.U. 2019 poz. 2479)
2. Role i odpowiedzialności w DC Deklaracja stosowania
3. Dokumentacja powołania DC
4. Plany postępowania z ryzykiem
5. Przegląd komunikatów z DC do organizacji
6. Raport z wykonanych audytów wewnętrznych i zewnętrznych SZBI
7. Raport z przeglądów zarządzania
8. Dokumentacja nadzoru nad utrzymaniem
9. Baza konfiguracji urządzeń / inwentaryzacja aktywów
10. Określenie obszarów obowiązywania SZBI (zakres)

Pracownicy CSIRT/SOC/DC – dokumentacja wskazująca na nadzór nad zabezpieczeni bezpieczeństwem następujących obszarów

1. Proces weryfikacji kandydatów (przed zatrudnieniem)
2. Podnoszenie kwalifikacji pracowników
3. Akceptowalne użycie aktywów przez pracowników
4. Nośniki wymienne – udokumentowany sposób podstępowania/ procedury
5. Uprawnienia / dostęp do systemów – procedury w zakresie:
6. Przydzielanie dostępu
7. Odbieranie dostępu
8. Pomieszczenie w dyspozycji struktur zespołu odpowiedzialnego za cyberbezpieczeństwo OUK **(Dz.U. 2019 poz. 2479)**
9. Dokumentacja i rozliczalność w zakresie dostępów realizowanych przez VPN (Dz.U. 2019 poz. 2479)
10. Dokumentacja umiejętności personelu w zakresie identyfikacji zagrożeń dla ICT / ICS – usługi kluczowej
11. Dokumentacja umiejętności personelu w zakresie analizowania oprogramowania szkodliwego Procedura i dokumentacja przebiegu identyfikacji wpływu oprogramowania złośliwego na usługę kluczową
12. Przebieg zabezpieczenia śladów kryminalistycznych
13. Narzędzia do przeprowadzania analizy szkodliwości kodu

Dostęp do wiedzy z zakresu cyberbezpieczeństwa (Art. 9.1.2) – dokumentacja poświadczająca

1. Dokumentacja Identyfikacji odbiorcy
2. Dokumentacja przeprowadzonego szkolenia
3. Dokumentacja Komunikatów

Wnioski z prac audytowych

Niezgodności zidentyfikowane w czasie audytu

ID	Numer UK	Zdarzenie niepożądane	Opis ryzyka	Priorytet
1				
2				

ID	Numer UK	Zdarzenie niepożądane	Opis ryzyka	Priorytet
3				
4				

Zalecenia

ID	Numer UK	Obserwacja	Rekomendacje
1			
2			
3			
4			

Obszar 3: Zarządzanie ryzykiem

W ramach audytu zespół koncentrował się na potwierdzeniu zgodności z wymaganiami w zakresie poprawności stosowanej metodyki zarządzania ryzykiem oraz kompletności procesu zarządzania ryzykiem poczynając od identyfikacji ryzyka aż po nadzór nad wprowadzeniem rekomendacji.

Kontekst w zakresie przepisów i normy

Zakres prac obejmował między innymi adekwatne wymagania:

- Artykułu 8, 10 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560 ze zm.);
- Rozporządzenia Rady Ministrów z dnia 16 października 2018 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej (Dz. U. poz. 2080);
- Polskiej Normy PN-EN ISO/IEC 27001 w rozdziałach 6, 8, 9, 10;
- Załącznika A do Polskiej Normy PN-EN ISO/IEC 27001 w wymaganiach A.6, A.18.

Kontekst w zakresie Decyzji OUK

1. Procedury związane z identyfikacją ryzyka
2. Procedury związane z przeglądem ryzyka
3. Rejestr ryzyka
4. Dokumentacja szacowania ryzyka dla obiektów infrastruktury
5. Dokumentacja zapewnienia ochrony fizycznej

Proces zarządzania ryzykiem usługi kluczowej

1. Powtarzalność identyfikacji ryzyka
2. Poprawność zastosowanych działań w zakresie analizy
3. Adekwatność w ocena ryzyka

Wnioski z prac audytowych

Niezgodności zidentyfikowane w czasie audytu

ID	Numer UK	Zdarzenie niepożądane	Opis ryzyka	Priorytet
1				

ID	Numer UK	Zdarzenie niepożądane	Opis ryzyka	Priorytet
2				
3				
4				

Zalecenia

ID	Numer UK	Obserwacja	Rekomendacje
1			
2			
3			
4			

Obszar 4: Monitorowanie i reagowanie na incydenty bezpieczeństwa

W ramach audytu zespół koncentrował się na potwierdzeniu zgodności z wymaganiami w zakresie zdefiniowania wymagań, wdrożenia i konfiguracji narzędzi, ciągłego monitorowania i skutecznego reagowania na potencjalne incydenty.

Kontekst w zakresie przepisów i normy

Zakres prac obejmował między innymi adekwatne wymagania:

- Artykułu 8, 11, 12, 13 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560 ze zm.);
- Rozporządzenie Ministra Cyfryzacji z 4 grudnia 2019 w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo;
- Rozporządzenie Rady Ministrów z dnia 16 października 2018 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej (Dz. U. poz. 2080);
- Rozporządzenie Rady Ministrów z dnia 31 października 2018 r. w sprawie progów uznania incydentu za poważny (Dz. U. poz. 2180);
- Polskiej Normy PN-EN ISO/IEC 27001 w rozdziałach 6, 8, 9, 10;
- Załącznika A do Polskiej Normy PN-EN ISO/IEC 27001 w wymaganiach A.6, A.12, A.16;
- Wymagania Polskiej Normy PN-EN ISO 22301 w rozdziałach 8.4, 9.1.

Kontekst w zakresie Decyzji OUK

Dokumentacja procesu zarządzania incydentami

1. Procedury zarządzania incydentami
2. Przyjęta taksonomia w zakresie rodzajów zagrożeń
3. Procedury postępowania ze znanymi incydentami
4. Raportowanie poziomów pokrycia scenariuszami znanych incydentów
5. Dokumentacja przebiegu reakcji na incydent
6. Dostęp do miejsca, w którym przechowywana jest dokumentacja lub weryfikacja dokumentacji poświadczającej właściwe praktyki ochrony fizycznej

7. Dokumentacja dotycząca przekazywania informacji do właściwego zespołu CSIRT poziomu krajowego/ sektorowego zespołu cyberbezpieczeństwa
8. Zabezpieczenia i gromadzenie materiału dowodowego oraz zapewnienie rozliczalności w całym procesie monitorowania i reagowania na incydenty
9. Dokumentacja systemu do automatycznego rejestrowania zgłoszeń incydentów
10. Potwierdzenie działań wynikających z komunikacji z procesem szacowania ryzyka SI_OUK
11. Dokumentacja doskonalenia procesu zarządzania incydentami i wniosków (w oparciu o zidentyfikowane słabości)

Monitorowanie cyberbezpieczeństwa

1. Monitorowanie i wykrycie incydentów w zakresie poufności
2. Monitorowanie i wykrycie incydentów w zakresie dostępności
3. Monitorowanie i wykrycie incydentów w zakresie integralność
4. Monitorowanie i wykrycie incydentów w zakresie autentyczności

Poprawność procesu z UKSC

1. Dokumenty potwierdzające wyszukiwanie podobieństw
2. Identyfikacja i dokumentowanie przyczyn wystąpienia incydentów
3. Dowody świadczące o opracowywaniu i implementacji wniosków wynikających z obsługi incydentu
4. Dowody poprawnej obsługi incydentu
5. Kontekst personelu i dokumentacji umiejętności (Dz.U. 2019 poz. 2479 par. 1 ust. 1 pkt. 4)
6. Kontekst narzędzi (Dz.U. 2019 poz. 2479 par. 2 ust. 1 pkt. 1)

Wnioski z prac audytowych

Niezgodności zidentyfikowane w czasie audytu

ID	Numer UK	Zdarzenie niepożądane	Opis ryzyka	Priorytet
1				
2				
3				
4				

Zalecenia

ID	Numer UK	Obserwacja	Rekomendacje
1			
2			
3			
4			

Obszar 5: Zarządzanie zmianą

W ramach audytu zespół koncentrował się na potwierdzeniu zgodności w wymaganiami w zakresie identyfikowania potrzeby zmian, ustalania wymagań bezpieczeństwa, wyboru rozwiązań, dokumentowania, testowania i wdrażania zmian.

Kontekst w zakresie przepisów i normy

Zakres prac obejmował między innymi adekwatne wymagania:

- Artykułu 8, 10 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560 ze zm.);
- Rozporządzenia Rady Ministrów z dnia 16 października 2018 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej (Dz. U. poz. 2080);
- Polskiej Normy PN-EN ISO/IEC 27001 w rozdziałach 6, 8;
- Załącznika A do Polskiej Normy PN-EN ISO/IEC 27001 w wymaganiach A.6, A.8, A.12, A.14, A.15, A.16.

Kontekst w zakresie Decyzji OUK

Dokumentacja procesu zarządzania zmianą

1. Rejestr wyjątków braku aktualizacji
2. Wyniki skanowania podatności ze strony sieci
3. Wyniki skanowania podatności ze strony systemu operacyjnego
4. Wyniki skanowania podatności aplikacji
5. Dekompozycja na komponenty składowe (biblioteki / moduły) – materiały opisowe
6. Wyniki audytów w procesie zarządzania zmianą
7. Potwierdzenie działań wynikających z komunikacji z procesem szacowania ryzyka SI_OUK

Wnioski z prac audytowych

Niezgodności zidentyfikowane w czasie audytu

ID	Numer UK	Zdarzenie niepożądane	Opis ryzyka	Priorytet
1				
2				

ID	Numer UK	Zdarzenie niepożądane	Opis ryzyka	Priorytet
3				
4				

Zalecenia

ID	Numer UK	Obserwacja	Rekomendacje
1			
2			
3			
4			

Obszar 6: Zarządzanie ciągłością działania

W ramach audytu zespół koncentrował się na potwierdzeniu zgodności w wymaganiami w zakresie dokonania analizy i zdefiniowania wymagań dla ciągłości działania, wdrożenia rozwiązań zapasowych i redundantnych, testowaniu zdolności, przygotowania odpowiednich umów z dostawcami oraz nadzorowaniu ich sposobu zapewnienia ciągłości działania.

Kontekst w zakresie przepisów i normy

Zakres prac obejmował między innymi adekwatne wymagania:

- Artykuł 8 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560 ze zm.);
- Rozporządzenie Rady Ministrów z dnia 16 października 2018 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej (Dz. U. poz. 2080);
- Polskiej Normy PN-EN ISO/IEC 27001 w rozdziałach 6, 8, 9;
- Załącznika A do Polskiej Normy PN-EN ISO/IEC 27001 w wymaganiach A.6, A.17;
- Wymagania Polskiej Normy PN-EN ISO 22301.

Kontekst w zakresie Decyzji OUK

Dokumentacja procesu zarządzania ciągłością działania

1. Harmonogram i rodzaje testów ciągłości działania
2. Wyniki testów ciągłości działania

3. Konfiguracja systemów do wykonywania kopii bezpieczeństwa
4. Raport z przeglądów i testów odtwarzania kopii bezpieczeństwa
5. Rejestr przeprowadzonych przeglądów
6. Retencja danych – dokumenty potwierdzające
7. Przechowywanie kopii zapasowych - procedury
8. Dokumentacja analizy BIA i analizy ryzyka
9. Strategia i polityka ciągłości działania
10. Dokumentacja wyjątków i odstępstw od założeń polityki
11. Dokumentacja MAK (Minimalna akceptowalna konfiguracja)
12. Struktura organizacyjna w odpowiedzi na incydent
13. Procedury ciągłości działania, awaryjne oraz odtwarzania po katastrofie (DRP)
14. Scenariusze testowe
15. Procedury komunikacji z mediami i komunikacji wewnętrznej
16. Rejestr kluczowych dostawców w ramach UK
17. Procedury współpracy z podmiotami zewnętrznymi
18. Potwierdzenie działań wynikających z komunikacji z procesem szacowania ryzyka SI_OUK
19. Dokumentacja wyników ocen i pomiarów (w tym testów) SZCD i jego elementów oraz działań korygujących (oraz ich status)

Wnioski z prac audytowych

Niezgodności zidentyfikowane w czasie audytu

ID	Numer UK	Zdarzenie niepożądane	Opis ryzyka	Priorytet
1				
2				
3				
4				

Zalecenia

ID	Numer UK	Obserwacja	Rekomendacje
1			

2			
3			
4			

Obszar 7: Utrzymanie systemów informacyjnych

W ramach audytu zespół koncentrował się na potwierdzeniu zgodności w wymaganiami w zakresie ustalania i nadzorowania wymagań bieżącej eksploatacji systemów informacyjnych.

Kontekst w zakresie przepisów i normy

Zakres prac obejmował między innymi adekwatne wymagania:

- Artykułu 8, 10 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560 ze zm.);
- Rozporządzenia Rady Ministrów z dnia 16 października 2018 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej (Dz. U. poz. 2080);
- Polskiej Normy PN-EN ISO/IEC 27001 w rozdziałach 6, 7, 8, 9, 10;
- Załącznika A do Polskiej Normy PN-EN ISO/IEC 27001 w wymaganiach A.5, A.6, A.8, A.9, A.10, A.11, A.12, A.14, A.14, A.18.

Kontekst w zakresie Decyzji OUK

Dokumentacja procesu zarządzania podatnościami i zagrożeniami

1. Opis procesu
2. Harmonogramy skanowania podatności
3. Wyniki skanowania podatności
4. Wyniki zmiany priorytetyzacji w raportach
5. Aktualny status realizacji postępowania z podatnościami - lista
6. Procedury związane ze z identyfikowaniem (wykryciem) podatności
7. Współpraca z osobami odpowiedzialnymi za procesy zarządzania incydentami
8. Potwierdzenie działań wynikających z komunikacji z szacowaniem ryzyka SI_OUK

Wnioski z prac audytowych

Niezgodności zidentyfikowane w czasie audytu

ID	Numer UK	Zdarzenie niepożądane	Opis ryzyka	Priorytet
1				

ID	Numer UK	Zdarzenie niepożądane	Opis ryzyka	Priorytet
2				
3				
4				

Zalecenia

ID	Numer UK	Obserwacja	Rekomendacje
1			
2			
3			
4			

Obszar 8: Utrzymanie i rozwój systemów informacyjnych

W ramach audytu zespół koncentrował się na potwierdzeniu zgodności w wymaganiami w zakresie ustalania i nadzorowania wymagań bieżącej eksploatacji systemów informatycznych wykorzystywanych do zapewniania, monitorowania i reagowania na incydenty bezpieczeństwa.

Kontekst w zakresie przepisów i normy

Zakres prac obejmował między innymi adekwatne wymagania:

- Artykułu 8, 10 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560 ze zm.);
- Rozporządzenia Rady Ministrów z dnia 16 października 2018 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej (Dz. U. poz. 2080);
- Polskiej Normy PN-EN ISO/IEC 27001 w rozdziałach 6, 7, 8, 9, 10;
- Załącznika A do Polskiej Normy PN-EN ISO/IEC 27001A.5, A.6, A.8, A.9, A.10, A.11, A.12, A.14, A.14, A.18.

Kontekst w zakresie Decyzji OUK

Środowisko rozwojowe - dokumentacja

1. Procedury migracji / tworzenia danych testowych
2. Dostęp do środowisk DEV / TEST / QA – zasady udokumentowane
3. Rozliczalność dostępów - procedury

Wnioski z prac audytowych

Niezgodności zidentyfikowane w czasie audytu

ID	Numer UK	Zdarzenie niepożądane	Opis ryzyka	Priorytet
1				
2				
3				
4				

Zalecenia

ID	Numer UK	Obserwacja	Rekomendacje
1			
2			
3			
4			

Obszar 9: Bezpieczeństwo fizyczne

W ramach audytu zespół koncentrował się na potwierdzeniu zgodności w wymaganiami w zakresie skuteczności procesu ochrony fizycznej i środowiskowej.

Kontekst w zakresie przepisów i normy

Zakres prac obejmował między innymi adekwatne wymagania:

- Artykułu 8, 10, 14 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560 ze zm.);
- Ustawy z dnia 22 sierpnia 1997 o ochronie osób i mienia (Dz.U. 1997 nr 114 poz. 740);
- Rozporządzenia Ministra Cyfryzacji z 4 grudnia 2019 w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo (Dz.U. 2019 poz. 2479);
- Rozporządzenia Rady Ministrów z dnia 16 października 2018 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej (Dz. U. poz. 2080);
- Polskiej Normy PN-EN ISO/IEC 27001 w rozdziałach 6, 8;
- Załącznika A do Polskiej Normy PN-EN ISO/IEC 27001 w wymaganiach A.6, A.11, A17.

Kontekst w zakresie Decyzji OUK

Pomieszczenia CSIRT/SOC/Działu

1. Dokumentacja i zasadność instalacji systemu zabezpieczeń (drzwi / okna / ściany)
2. Dokumentacja i zasadność instalacji systemu alarmowego i antynapadowego
3. Atestacja szaf i sejfów
4. Dokumentacja i zasadność konfiguracji systemu przeciwpożarowego
5. Przechowywanie i dostęp do dokumentacji
6. Potwierdzenie działań wynikających z komunikacji z szacowaniem ryzyka SI_OUK
7. Dokumentacja i zasadność konfiguracji systemu podtrzymania i stabilizacji prądu
8. Dokumentacja i zasadność konfiguracji systemu podtrzymania warunków temperatury, wilgotności i wentylacji pomieszczeń
9. Rejestr przeglądów i konserwacji elementów w/w użytkowanych systemów

10. Dokumentacja testów bezpieczeństwa w odniesieniu do elementów systemu zabezpieczeń fizycznych
11. Dokumentacja i testy procedur ewakuacyjnych
12. Dokumentacja i procedury kontaktu ze służbami

Wnioski z prac audytowych

Niezgodności zidentyfikowane w czasie audytu

ID	Numer UK	Zdarzenie niepożądane	Opis ryzyka	Priorytet
1				
2				
3				
4				

Zalecenia

ID	Numer UK	Obserwacja	Rekomendacje
1			
2			
3			
4			

Obszar 10: Zarządzanie bezpieczeństwem i ciągłością działania łańcucha usług

W ramach audytu zespół koncentrował się na potwierdzeniu zgodności w wymaganiami w zakresie definiowania i nadzorowania stosowania wymagań bezpieczeństwa informacji i ciągłości działania przez dostawców usług bezpieczeństwa informacji oraz usług wdrażania i utrzymywania systemów informatycznych wykorzystywanych do świadczenia usług kluczowych.

Kontekst w zakresie przepisów i normy

Zakres prac obejmował między innymi adekwatne wymagania:

- Artykułu 8, 14 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560 ze zm.);
- Rozporządzenia Rady Ministrów z dnia 16 października 2018 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej (Dz. U. poz. 2080);
- Polskiej Normy PN-EN ISO 22301 w rozdziałach 8.3;
- Polskiej Normy PN-EN ISO/IEC 27001 w rozdziałach 6, 7, 8;
- Załącznika A do Polskiej Normy PN-EN ISO/IEC 27001 w wymaganiach A.6, A.15, A.17.

Kontekst w zakresie Decyzji OUK

Dostawcy OUK - dokumentacja

1. Polityka bezpieczeństwa w relacjach z dostawcami
2. Standardy i wymagania w zakresie cyberbezpieczeństwa nakładane na dostawców w umowach
3. Ocena zdolności dostawcy do zachowania ciągłości działania
4. Bezpieczeństwo łańcucha dostaw
5. Bieżące monitorowanie i przegląd usług świadczonych przez dostawców
6. Umowy z dostawcami (wymagany poziom usług) i standardy w umowach dotyczące cyberbezpieczeństwa
7. Rejestr kluczowych dostawców w ramach UK
8. Wyniki audytów drugiej i trzeciej strony
9. Techniki zdalnego dostępu, nadzór nad poprawnością zakres zdalnego dostępu oraz stosowane metody uwierzytelnienia

10. Akceptowalne użycie aktywów – lista przypadków

Dokumentacja podmiotu świadczącego usługi cyberbezpieczeństwa

1. Wymagania osobowe wymienione w paragrafie 1 ustęp 1 punkt 4 (Dz.U. 2019 poz. 2479)
2. Wymagania w zakresie ochrony fizycznej (Dz.U. 2019 poz. 2479)
3. Zastosowane systemy zabezpieczeń w zakresie dostępów do dokumentacji (Dz.U. 2019 poz. 2479)
4. Zastosowane systemy zabezpieczeń teleinformatycznych w zakresie pracy zdalnej (Dz.U. 2019 poz. 2479)

Wnioski z prac audytowych

Niezgodności zidentyfikowane w czasie audytu

ID	Numer UK	Zdarzenie niepożądane	Opis ryzyka	Priorytet
1				
2				
3				
4				

Zalecenia

ID	Numer UK	Obserwacja	Rekomendacje
1			
2			
3			
4			

Skróty i definicje

Definicja	Wyjaśnienie
Audyt	niezależne i obiektywne potwierdzenie zgodności z wymaganiami
UKSC	ustawa o krajowym systemie cyberbezpieczeństwa z 5 lipca 2018 (Dz.U.2018 poz. 1560)
Sprawozdanie z audytu	dokument wynikowy prac audytorskich.
Sprawozdanie Poprzednie	sprawozdanie z poprzedniego audytu zgodnego z ustawą o krajowym systemie cyberbezpieczeństwa

Definicja	Wyjaśnienie
Niezgodność	odstępstwo od przepisu, normy, standardu, wymagania, niespełnienie założonego celu mechanizmu kontrolnego (zabezpieczenia), nieskuteczność mechanizmu kontrolnego (zabezpieczenia).
Incydent poważny	incydent poważny w rozumieniu Rozporządzenia Rady Ministrów z dnia 31 października 2018 r. w sprawie progów uznania incydentu za poważny (Dz. U. poz. 2180),
Audytor Wiodący	audytor wyznaczony jako lider zespołu audytowego, odpowiedzialny za realizację audytu zgodnie z zakresem, programem i ocenę dowodów w odniesieniu do kryteriów audytu, wybór technik badawczych oraz przygotowanie zbiorczego raportu
Common Vulnerability Scoring System (CVSS)	międzynarodowa skala stosowana podczas analizy ryzyk związanych z technicznymi podatnościami systemów informatycznych. Jest stosowana przez wszystkich głównych dostawców systemów informatycznych oraz powszechnie wykorzystywana na całym świecie przez zespoły IT. Jest szerzej opisana na stronie https://www.first.org/cvss/
PŚUB	Podmiot świadczący usługi z zakresu cyberbezpieczeństwa w rozumieniu UKSC
DC	dział, departament, biuro lub inna jednostka organizacyjna bezpośrednio odpowiedzialne za realizację zadań w zakresie cyberbezpieczeństwa OUK
OUK	operator usługi kluczowej w rozumieniu UKSC
UK	usługa kluczowa – usługa, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, wymienioną w wykazie usług kluczowych Rozporządzenie Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych (Dz. U. poz. 1806)
Mechanizm kontrolny	środków technicznych i organizacyjnych (fizyczne i informatyczne narzędzia, procedury operacyjne i instrukcje oraz struktura organizacyjna) mające na celu zmniejszanie zidentyfikowanego ryzyka. Jest to tożsame z terminem „zabezpieczenie”
Najwyższe Kierownictwo	osoba lub grupa osób, które na najwyższym szczeblu kierują organizacją i ją nadzorują
Opinia pozytywna	opis systemu bezpieczeństwa został przygotowany z należytą starannością. Mogą istnieć drobne błędy lub pominięcia, jednakże ich waga nie jest znacząca. Mechanizmy kontrolne istnieją. Skuteczność mechanizmów kontrolnych w odniesieniu celów jest spełniona. Mogą istnieć drobne błędy lub odchylenia, jednakże ich waga nie jest znacząca.
Opinia pozytywna z zastrzeżeniami	opis systemu bezpieczeństwa został przygotowany z należytą starannością, jednakże zawiera błędy lub pominięcia. Mechanizmy kontrolne istnieją, lecz ich skuteczność w odniesieniu do celów zawiera odchylenia.
Opinia negatywna	opis systemu bezpieczeństwa nie został przygotowany z należytą starannością i zawiera rażące błędy lub pominięcia. Mechanizmy kontrolne nie istnieją lub ich skuteczność w odniesieniu celów zawiera znaczące odchylenia.
Odstąpienie od badania	audytujący nie otrzymali dowodów, na podatawie których mogliby wydać opinię.
Program audytu	przygotowany przez audytora wiodącego i zatwierdzony przez operatora usługi kluczowej program zadania audytowego

Definicja	Wyjaśnienie
Sprawozdanie z audytu	pisemne sprawozdanie przygotowany pod nadzorem audytora wiodącego zawierający obserwacje (ustalenia stanu faktycznego) w zakresie zaobserwowanych niezgodności, ocenę systemu, klasyfikację zidentyfikowanego ryzyka oraz rekomendacje dla Kierownictwa OUK, a także zawierający dokumentacje z przeprowadzonego audytu.
Skuteczność mechanizmu kontrolnego	zapewnienie, że mechanizm kontrolny realizuje postawione przed nim cele
Zespół audytowy	audytor wiodący oraz co najmniej jeden dodatkowy audytor przeprowadzający zadanie audytowe
System informacyjny	system informatyczny oraz otaczający ekosystem procesów wykorzystywany do świadczenia usługi kluczowej
Operator usługi kluczowej	podmiot, o którym mowa w załączniku nr 1 do UKSC, posiadający jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, wobec którego organ właściwy do spraw cyberbezpieczeństwawydał decyzję o uznaniu za operatora usługi kluczowej.
Organ właściwy	organami właściwymi do spraw cyberbezpieczeństwa są organy administracji państwowej wymienione w art. 41 pkt 1-9 UKSC.
Zarządzanie incydentem	Bieżący i udokumentowany proces ogólnego postępowania w trakcie obsługi incydentu polegającego co najmniej na podejmowaniu działań i dokumentowania z podziałem na fazy:wyszukiwanie powiązań między incydentami,usuwanie przyczyn ich wystąpieniaopracowywanie wnioskówwynikających z obsługi incydentu
Szacowanie ryzyka	bieżące prace polegające na ocenie sytuacji w zarządzanej cyberprzestrzeni polegające co najmniej na:identyfikacjianalizieocenie ryzyka
Obsługa incydentu	szczegółowy zestaw czynności wykonywanych w sposób powtarzalny i udokumentowany, a składający się z co najmniej faz:wykrywanierejestrowanieanalizowanieklasyfikowaniepriorytetyzacjępodejmowanie działań naprawczychograniczenie skutków incydentu
Osoba do kontaktu	osoba odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, ze szczególnym uwzględnieniem zespołów CSIRT i organów właściwych.
Właściciel procesu zarządzania ryzykiem	osoba odpowiedzialna u OUK za wypełnianie obowiązków operatora w zakresie artykułu 8 punkt 1.
Właściciel procesu zarządzania incydentem	osoba odpowiedzialna u OUK za wypełnianie obowiązków operatora w zakresie artykułu 8 punkt 4
Właściciel procesu zarządzania zagrożeniami	osoba odpowiedzialna u OUK za wypełnianie obowiązków operatora w zakresie artykułu 8 punkt 3 w zakresie zbieranie informacji o zagrożeniach cyberbezpieczeństwa dla systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej.
Właściciel procesu	osoba odpowiedzialna u OUK za wypełnianie obowiązków operatora w zakresie artykułu 8 punkt 3 w zakresie identyfikacji i postępowania z podatnościami na

Definicja	Wyjaśnienie
zarządzania podatnościami	incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej.
Właściciel procesu zarządzanie środkami technicznymi	Osoba odpowiedzialna u OUK za wypełnianie obowiązków operatora w zakresie artykułu 8 punkt 2 w zakresie wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych uwzględniających najnowszy stan wiedzy zabezpieczający systemy informacyjne wykorzystywane do świadczenia usługi kluczowej.
Właściciel procesu zarządzanie środkami organizacyjnymi	Osoba odpowiedzialna u OUK za wypełnianie obowiązków operatora w zakresie artykułu 8 punkt 2 w zakresie wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków organizacyjnych uwzględniających najnowszy stan wiedzy zabezpieczający systemy informacyjne wykorzystywane do świadczenia usługi kluczowej.
SI_OUK	System informacyjny/systemy informacyjne operatora usługi kluczowej, od którego zależne jest świadczenie usługi kluczowej.
SZBI	System Zarządzania Bezpieczeństwem Informacji
SZCD	System Zarządzania Ciągłością Działania

Uwagi i poprawki: https://github.com/issa-polska/Audyt_KSC/issues

Strona Projektu: https://issapolska.github.io/Audyt_KSC/

Kontakt mailowy: ksc@issa.org.pl

[5] Uwagi do kolejnych wersji prosimy zgłaszać przez https://github.com/issapolska/Audyt_KSC/issues