Szablon raportu z Audytu zgodnego z ustawą o Krajowym Systemie Cyberbezpieczeństwa**[[1]](#footnote-1)**

Spis treści

[Metryka dokumentu 5](#_Toc27355283)

[Metryka audytu: 5](#_Toc27355284)

[Odpowiedzialności instytucjonalne w OUK 5](#_Toc27355285)

[Odpowiedzialności procesowe (formalne i nieformalne) w OUK 5](#_Toc27355286)

[Informacja o audytorach wykonujących (Dz.U. 2018 poz. 1999) 6](#_Toc27355287)

[Informacja o ekspertach wspierających audytorów 6](#_Toc27355288)

[Niezgodności z poprzednich dwóch audytów KSC 6](#_Toc27355289)

[Podsumowanie dla kierownictwa 7](#_Toc27355290)

[Cel i zakres prac 8](#_Toc27355291)

[Cel prac 8](#_Toc27355292)

[Celem wykonanych prac była ocena procesu zarządzania bezpieczeństwem informacji realizowanego przez ….<nazwa klienta>… oraz identyfikacja i analiza luki zgodności w wymaganiami Ustawy o Krajowym Systemie Cyberbezpieczeństwa 8](#_Toc27355293)

[Zakres prac 8](#_Toc27355294)

[Przebieg prac 9](#_Toc27355295)

[Wykluczenia i ograniczenia zakresu 9](#_Toc27355296)

[Wyniki prac 9](#_Toc27355297)

[Obszar 1: Organizacja zarządzania bezpieczeństwem informacji 11](#_Toc27355298)

[Kontekst w zakresie przepisów i norm 11](#_Toc27355299)

[Kontekst w zakresie Decyzji OUK 11](#_Toc27355300)

[Dokumentacja potwierdzająca wykonane działania zgodnie z harmonogramem wskazanym w ustawie: 11](#_Toc27355301)

[Opis Identyfikacji systemu informacyjnego wspierającego usługę krytyczną: 11](#_Toc27355302)

[Dokumentacja Systemu Informacyjnego wspierającego usługę kluczową 11](#_Toc27355303)

[Ryzyka zidentyfikowane w czasie audytu 12](#_Toc27355304)

[Zalecenia 12](#_Toc27355305)

[Obszar 2: Procesy zarządzania bezpieczeństwem informacji 13](#_Toc27355306)

[Kontekst w zakresie przepisów i norm 13](#_Toc27355307)

[Kontekst w zakresie Decyzji OUK 13](#_Toc27355308)

[System bazujący na SZBI ISO-27001 13](#_Toc27355309)

[Pracownicy CSIRT/SOC/DC – dokumentacja wskazująca na wykonywanie poniższych 13](#_Toc27355310)

[Dostęp do wiedzy z zakresu cyberbezpieczeństwa (Art. 9.1.2) – dokumentacja poświadczająca 14](#_Toc27355311)

[Potwierdzenie działań wynikających z komunikacji z procesem szacowania ryzyka SI\_OUK 14](#_Toc27355312)

[Ryzyka zidentyfikowane w czasie audytu 14](#_Toc27355313)

[Zalecenia 14](#_Toc27355314)

[Obszar 3: Zarządzanie ryzykiem 15](#_Toc27355315)

[Kontekst w zakresie przepisów i norm 15](#_Toc27355316)

[Kontekst w zakresie Decyzji OUK 15](#_Toc27355317)

[Proces zarządzania ryzykiem KSC 15](#_Toc27355318)

[Ryzyka zidentyfikowane w czasie audytu 15](#_Toc27355319)

[Zalecenia 15](#_Toc27355320)

[Obszar 4: Monitorowanie i reagowanie na naruszenia bezpieczeństwa 16](#_Toc27355321)

[Kontekst w zakresie przepisów i norm 16](#_Toc27355322)

[Kontekst w zakresie Decyzji OUK 16](#_Toc27355323)

[Dokumentacja procesu zarządzania Incydentami 16](#_Toc27355324)

[Monitorowanie cyberbezpieczeństwa 17](#_Toc27355325)

[Poprawność procesu z KSC 17](#_Toc27355326)

[Potwierdzenie działań wynikających z komunikacji z procesem szacowania ryzyka SI\_OUK 17](#_Toc27355327)

[Ryzyka zidentyfikowane w czasie audytu 17](#_Toc27355328)

[Zalecenia 17](#_Toc27355329)

[Obszar 5: Zarządzanie zmianą 18](#_Toc27355330)

[Kontekst w zakresie przepisów i norm 18](#_Toc27355331)

[Kontekst w zakresie Decyzji OUK 18](#_Toc27355332)

[Dokumentacja procesu zarządzania zmianą 18](#_Toc27355333)

[Ryzyka zidentyfikowane w czasie audytu 18](#_Toc27355334)

[Zalecenia 18](#_Toc27355335)

[Obszar 6: Zarządzanie ciągłością działania 19](#_Toc27355336)

[Kontekst w zakresie przepisów i norm 19](#_Toc27355337)

[Kontekst w zakresie Decyzji OUK 19](#_Toc27355338)

[Dokumentacja procesu zarządzania ciągłością działania 19](#_Toc27355339)

[Ryzyka zidentyfikowane w czasie audytu 20](#_Toc27355340)

[Zalecenia 20](#_Toc27355341)

[Obszar 7: Utrzymanie systemów informatycznych 21](#_Toc27355342)

[Kontekst w zakresie przepisów i norm 21](#_Toc27355343)

[Kontekst w zakresie Decyzji OUK 21](#_Toc27355344)

[Dokumentacja procesu zarządzania podatnościami i zagrożeniami 21](#_Toc27355345)

[Ryzyka zidentyfikowane w czasie audytu 21](#_Toc27355346)

[Zalecenia 21](#_Toc27355347)

[Obszar 8: Utrzymanie i rozwój systemów bezpieczeństwa 22](#_Toc27355348)

[Kontekst w zakresie przepisów i norm 22](#_Toc27355349)

[Kontekst w zakresie Decyzji OUK 22](#_Toc27355350)

[Środowisko rozwojowe - dokumentacja 22](#_Toc27355351)

[Ryzyka zidentyfikowane w czasie audytu 22](#_Toc27355352)

[Zalecenia 22](#_Toc27355353)

[Obszar 9: Bezpieczeństwo fizyczne 23](#_Toc27355354)

[Kontekst w zakresie przepisów i norm 23](#_Toc27355355)

[Kontekst w zakresie Decyzji OUK 23](#_Toc27355356)

[Pomieszczenia CSIRT/SOC/Działu 23](#_Toc27355357)

[Ryzyka zidentyfikowane w czasie audytu 23](#_Toc27355358)

[Zalecenia 23](#_Toc27355359)

[Obszar 10: Zarządzanie bezpieczeństwem i ciągłością działania łańcucha usług 24](#_Toc27355360)

[Kontekst w zakresie przepisów i norm 24](#_Toc27355361)

[Kontekst w zakresie Decyzji OUK 24](#_Toc27355362)

[Dostawcy OUK - dokumentacja 24](#_Toc27355363)

[Dokumentacja podmiotu Świadczący Usługi Cyberbezpieczeństwa 24](#_Toc27355364)

[Ryzyka zidentyfikowane w czasie audytu 25](#_Toc27355365)

[Zalecenia 25](#_Toc27355366)

[Skróty i definicje 26](#_Toc27355367)

## Metryka dokumentu

### Metryka audytu:

|  |  |
| --- | --- |
| Opis | Treść |
| Audytowana Jednostka Organizacyjna |  |
| Audytowane lokalizacje: |  |
| Cel Audytu: | Potwierdzenie zgodności bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi krytycznej z Kryteriami |
| Kryteria Audytu | Ustawa o Krajowym Systemie Cyberbezpieczeństwa z 5 lipca 2018 wraz z Załącznikami |
| Zakres Audytu - Działalność | Nazwa usługi krytycznej |
| Zakres audytu - Proces | Wsparcie systemu informacyjnego dla usługi krytycznej |
| Data(y) Audytu |  |
| Data wydania Raportu |  |
| Data Raportu Poprzedniego i ilość niezgodności |  |
| Data Raportu poprzedniego do poprzedniego i ilość niezgodności |  |
| Data objęcia Ustawą KSC |  |
| Sektor |  |
| Podsektor |  |
| 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 KSC | ​ |

### Odpowiedzialności procesowe (formalne i nieformalne) w OUK

|  |  |
| --- | --- |
| Typ procesu / aktywności wymaganej KSC | Imię i Nazwisko pracownika OUK lub dane dostawcy cyberbezpieczeństwa, wyznaczonego przez Najwyższe Kierownictwo jako właściwego merytorycznie do uczestnictwa w audycie |
| Zarządzanie ryzykiem | ​ |
| Zarządzania incydentem | ​ |
| Zarządzania zagrożeniami | ​ |
| Zarządzania 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 KSC | ​ |

### Informacja o audytorach wykonujących (Dz.U. 2018 poz. 1999)

|  |  |  |
| --- | --- | --- |
| Funkcja Audytowa | Imię i Nazwisko | Potwierdzenie kwalifikacje (certyfikaty, wykształcenie i doświadczenie) |
| Audytor Wiodący | ​ | ​ |
| Audytor Systemy Operacyjne | ​ | ​ |
| Audytor warstwa aplikacji i baz danych | ​ | ​ |
| Audytor procesów 27001 | ​ | ​ |
| Audytor procesów 22301 | ​ | ​ |
| Audytor bezpieczeństwa procesów biznesowych | ​ | ​ |

### Informacja o ekspertach wspierających audytorów

|  |  |  |
| --- | --- | --- |
| Funkcja | Imię i Nazwisko | Potwierdzenie kwalifikacje (certyfikaty, wykształcenie i doświadczenie) |
|  | ​ | ​ |
|  | ​ | ​ |

**Granica konfliktu interesu:** Osoby tworzące zespół audytowy i bezpośrednio zaangażowane w weryfikacje zgodności, oświadczają że 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 KSC

Audyt poprzedni (jeśli dotyczy) z dnia:

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

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 zgodności z wymaganiami Ustawy o Krajowym Systemie Cyberbezpieczeństwa (Dz.U. 2018 poz. 1999). Prace audytowe zostały przeprowadzone przez …… zgodnie z umową z dnia ……

Pierwszy etap prac polegał na “Zrozumieniu kontekstu działania organizacji oraz analizy dokumentacji” i został przeprowadzone w dniach ……. - ……. . Na podstawie otrzymanych informacji udało się zidentyfikować …. niezgodności oraz zaplanowano drugi etap prac polegający na “ Testach skuteczności funkcjonowania mechanizmów kontrolnych”. Audytowi poddano ….. procesów w ……. lokalizacjach oraz działalność …. dostawców i usługodawców.

Podczas audytu zidentyfikowano ….. niezgodności o krytycznym priorytecie, ….. niezgodności o wysokim priorytecie, ….. niezgodności o średnim priorytecie oraz ….. niezgodności o niskim priorytecie. Priorytety prac należy rozumieć w następujący sposób:

**krytyczny** - niezgodności mogące bezpośrednio doprowadzić do incydentu krytycznego lub uniemożliwić jego skuteczną obsługę

**wysoki** - niezgodności mogące bezpośrednio doprowadzić do incydentu poważnego lub ….. lub polegające na braku realizowania wymagań KSC

**średni** - niezgodności mogące doprowadzić do incydentu zwykłego, lub ……, lub polegające na nieskutecznej realizacji wymagań KSC

**niski** - obszary mogące w opinii zespołu audytowego doprowadzić w przyszłości do incydentów lub niezgodności o wyższym priorytecie

Kluczowymi niezgodnościami, którymi, zdaniem zespołu audytowego, w pierwszej kolejności powinno zająć się najwyższe kierownictwo są:

……..

|  |  |  |
| --- | --- | --- |
| Nr | Stwierdzenie faktu i opis niezgodności (w tym odniesienie do kryterium) | Priorytet |
| 1 |  |  |
| 2 |  |  |
| 3 |  |  |
| 4 |  |  |
| 5 |  |  |
| 6 |  |  |

## Cel i zakres prac

### Cel prac

### Celem wykonanych prac była ocena procesu zarządzania bezpieczeństwem informacji realizowanego przez ….<nazwa klienta>… oraz identyfikacja i analiza luki zgodności w wymaganiami Ustawy o Krajowym Systemie Cyberbezpieczeństwa

### Zakres prac

Zakres prac obejmował:

* Zrozumienie kontekstu działania organizacji w tym wpływy systemów IT na usługę krytyczną
* Analizę dokumentacji
* Testy skuteczności funkcjonowania mechanizmów kontrolnych
* Opracowanie raportu zawierającego opis zidentyfikowanych luk zgodności wraz z rekomendacjami
* Przestawienie wyników audytu dla najwyższego kierownictwa

### 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:

* Analizę podatności na xxx stacjach
* Analizę luk w systemie ….

Prace realizowane były zgodnie z następującym harmonogramem:

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

### 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.

### Wyniki prac

Szczegółowe wyniki wykonanych prac obejmują ocenę zgodności z wymaganiami Ustawy o Krajowym Systemie Cyberbezpieczeństwa, w tym zidentyfikowane luki, które mogą mieć wpływ na świadczenie Usług Kluczowych.

Do oceny priorytetów dla zidentyfikowanego ryzyka braku zgodności wykorzystano następujące skale:

**krytyczny** - niezgodności mogące bezpośrednio doprowadzić do incydentu krytycznego lub uniemożliwić jego skuteczną obsługę

**wysoki** - niezgodności mogące bezpośrednio doprowadzić do incydentu poważnego lub ..... lub polegające na braku realizowania wymagań KSC

**średni** - niezgodności mogące doprowadzić do incydentu zwykłego, lub ......, lub polegające na nieskutecznej realizacji wymagań KSC

**niski** - obszary mogące w opinii zespołu audytowego doprowadzić w przyszłości do incydentów lub niezgodności o wyższym priorytecie

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 KSC. Może też być elementem przeglądów realizowanych przed podmioty nadzorcze zgodnie z par............ KSC

W ramach z każdego 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 KSC.

## Kontekst w zakresie przepisów i norm

Zakres prac obejmował między innymi adekwatne wymagania:

* Artykuł 9, 14,15 i 16 KSC,
* Rozporządzenie XXXX z 23 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 2080 w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej
* Rozporządzenie1999 w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu
* Rozporządzenie1830 w sprawie kryteriów uznania naruszenia bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych za naruszenie o istotnym wpływie na funkcjonowanie sieci lub usług
* Normy ISO 27001 w rozdziałach 5, 7, 9 i 10
* Załącznika A do normy ISO 27001 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 krytyczną:

* Lista elementów składowych
* Lista osób odpowiedzialnych

### Dokumentacja Systemu Informacyjnego wspierającego usługę kluczową

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

## Ryzyka zidentyfikowane w czasie audytu

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Zdarzenie niepożądane | Opis ryzyka | Priorytet |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Zalecenia

|  |  |
| --- | --- |
| Obserwacja | Rekomendacje |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# Obszar 2: Procesy zarządzania bezpieczeństwem informacji

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

## Kontekst w zakresie przepisów i norm

Zakres prac obejmował między innymi adekwatne wymagania:

* Artykuł 8,10,11,15 KSC
* Rozporządzenie 2080 w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej
* Rozporządzenie2180 w sprawie progów uznania incydentu za poważny
* Wymagania normy ISO 27001 w rozdziałach 6, 8
* Wszystkie z wymienionych w Załączniku A do normy ISO 27001

## Kontekst w zakresie Decyzji OUK

### System bazujący na SZBI ISO-27001

1. Weryfikacja polityki. Określone i zakomunikowane cele działania systemu w odpowiedzialnej komórce (Dz. U. XXX z 23.12.2019)
2. Role i odpowiedzialności w DC Deklaracja stosowania (Norma-> 6.1.3.d)
3. Dokumentacja powołania DC
4. Plany postępowania z ryzykiem
5. Przegląd komunikatów z DC do organizacji (Norma-> 7.4)
6. Raport z wykonanych audytów wewnętrznych i zewnętrznych SZBI
7. Raport z przeglądów zarządzania
8. Dokumentacja nadzoru nad utrzymaniem (Norma-> 8.1)
9. Baza konfiguracji urządzeń / inwentaryzacja aktywów
10. Określenie obszarów obowiązywania SZBI (zakres)

### Pracownicy CSIRT/SOC/DC – dokumentacja wskazująca na wykonywanie poniższych

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 zakresie zespołu (Dz. U. XXXX z 23.12.2019)
9. Dokumentacja i rozliczalność w zakresie VPN (Dz. U. XXXX x 23.12.2019)
10. Dokumentacja umiejętności identyfikacji zagrożeń dla ICT / ICS – usługi kluczowej
11. Dokumentacja umiejętności analizowania oprogramowania szkodliwego Procedura i dokumentacja przebiegu identyfikacji wpływu oprogramowania złośliwego na usługę kluczową
12. Przebieg zabezpieczenia śladów kryminalistycznych
13. Narzędzia do wykonywania analizy kodu w celu uznania za szkodliwy

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

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

### Potwierdzenie działań wynikających z komunikacji z procesem szacowania ryzyka SI\_OUK

## Ryzyka zidentyfikowane w czasie audytu

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Zdarzenie niepożądane | Opis ryzyka | Priorytet |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Zalecenia

|  |  |
| --- | --- |
| Obserwacja | Rekomendacje |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# 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 norm

Zakres prac obejmował między innymi adekwatne wymagania:

* Artykuł 8 KSC
* Rozporządzenie 2080 w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej
* Normy ISO 27001 w rozdziałach 6,8,9,10
* Załącznika A do normy ISO 27001 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 KSC

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

## Ryzyka zidentyfikowane w czasie audytu

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Zdarzenie niepożądane | Opis ryzyka | Priorytet |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Zalecenia

|  |  |
| --- | --- |
| Obserwacja | Rekomendacje |
|  |  |
|  |  |
|  |  |

# Obszar 4: Monitorowanie i reagowanie na naruszenia 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 norm

Zakres prac obejmował między innymi adekwatne wymagania:

* Artykuł 8,11,12,13 Ustawy o Krajowym Systemie Cyberbezpieczeństwa
* Rozporządzenie XXXX z 23 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 2080 w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej
* Rozporządzenie 2180 w sprawie progów uznania incydentu za poważny
* Rozporządzenie 1830 w sprawie kryteriów uznania naruszenia bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych za naruszenie o istotnym wpływie na funkcjonowanie sieci lub usług
* Wymagania normy ISO 27001 w rozdziałach 6, 8, 9,10
* Załącznika A do normy ISO 27001 A.6, A.12, A.16

## Kontekst w zakresie Decyzji OUK

### Dokumentacja procesu zarządzania Incydentami

1. Procedury zarządzania incydentami
2. Przyjęta taksonomia
3. Procedury postępowania ze znanymi incydentami lub/i naruszeniami
4. Raportowanie poziomów pokrycia scenariuszami znanych incydentów lub/i naruszeń
5. Dokumentacja przebiegu reakcji na incydent
6. Dostęp do miejsca, w którym przechowywana jest dokumentacja (jeżeli tylko wirtualnie to wizja lokalna w serwerowni)
7. Dokumentacja dotycząca przekazywania informacji do CSIRT sektorowego / narodowego
8. Zabezpieczenia i gromadzenie materiału dowodowego
9. Dokumentacja systemu do automatycznego rejestrowania zgłoszeń incydentów
10. Potwierdzenie działań wynikających z komunikacji z procesem szacowania ryzyka SI\_OUK

### 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 poufności autentyczności

### Poprawność procesu z KSC

1. Dokumenty potwierdzające wyszukiwanie podobieństw
2. Identyfikacja i dokumentowanie przyczyn wystąpienia
3. Dowody świadczące o opracowywaniu i implementacji wniosków wynikających z obsługi incydentu
4. Dowody poprawnej obsługi incydentu (1.1.10)
5. Kontekst personelu i dokumentacji umiejętności (Rozporządzenie XXXX z 23.12.2019 par. 1 ust. 1 pkt. 4)
6. Kontekst narzędzi (Rozporządzenie XXXX z 23.12.2019 par. 2 ust. 1 pkt. 1)

### Potwierdzenie działań wynikających z komunikacji z procesem szacowania ryzyka SI\_OUK

## Ryzyka zidentyfikowane w czasie audytu

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Zdarzenie niepożądane | Opis ryzyka | Priorytet |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Zalecenia

|  |  |
| --- | --- |
| Obserwacja | Rekomendacje |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# Obszar 5: Zarządzanie zmianą

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

## Kontekst w zakresie przepisów i norm

Zakres prac obejmował między innymi adekwatne wymagania:

* Artykuł 8,10 KSC
* Rozporządzenie 2080 w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej
* Wymagania normy ISO 27001 w rozdziałach 6, 8
* Załącznika A do normy ISO 27001 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 skanów podatności ze strony sieci
3. Wyniki skanów podatności ze strony systemu operacyjnego
4. Wyniki skanów 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

## Ryzyka zidentyfikowane w czasie audytu

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Zdarzenie niepożądane | Opis ryzyka | Priorytet |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Zalecenia

|  |  |
| --- | --- |
| Obserwacja | Rekomendacje |
|  |  |
|  |  |
|  |  |

# Obszar 6: Zarządzanie ciągłością działania

W ramach audytu zespół koncentrował się na potwierdzeniu zgodności z 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 norm

Zakres prac obejmował między innymi adekwatne wymagania:

* Artykuł 8 KSC
* Rozporządzenie 2080 w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej
* Wymagania normy ISO 27001 w rozdziałach 6, 8, 9
* Załącznika A do normy ISO 27001 A.6, A.17
* Wymagania normy ISO 22301

## Kontekst w zakresie Decyzji OUK

### Dokumentacja procesu zarządzania ciągłością działania

1. Wyniki testów ciągłości działania
2. Konfiguracja systemów kopii bezpieczeństwa
3. Raport z audytu przeglądu systemów kopii bezpieczeństwa
4. Rejestr przeprowadzonych przeglądów
5. Retencja danych – dokumenty potwierdzające
6. Przechowywanie kopii zapasowych - procedury
7. Dokumentacja BIA analizy ryzyka
8. Strategia i polityka ciągłości działania
9. Procedury awaryjne (DRP)
10. Scenariusze testowe
11. Procedury komunikacji z mediami
12. Procedury współpracy z podmiotami zewnętrznymi
13. Potwierdzenie działań wynikających z komunikacji z procesem szacowania ryzyka SI\_OUK

## Ryzyka zidentyfikowane w czasie audytu

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Zdarzenie niepożądane | Opis ryzyka | Priorytet |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Zalecenia

|  |  |
| --- | --- |
| Obserwacja | Rekomendacje |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# Obszar 7: Utrzymanie systemów informatycznych

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

## Kontekst w zakresie przepisów i norm

Zakres prac obejmował między innymi adekwatne wymagania:

* Artykuł 8 KSC
* Rozporządzenie 2080 w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej
* Wymagania normy ISO 27001 w rozdziałach 6, 7, 8, 9,10
* Załącznika A do normy ISO 27001 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 skanów 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 procesami zarządzania incydentami
8. Potwierdzenie działań wynikających z komunikacji z szacowaniem ryzyka SI\_OUK

## Ryzyka zidentyfikowane w czasie audytu

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Zdarzenie niepożądane | Opis ryzyka | Priorytet |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Zalecenia

|  |  |
| --- | --- |
| Obserwacja | Rekomendacje |
|  |  |
|  |  |
|  |  |

# Obszar 8: Utrzymanie i rozwój systemów bezpieczeństwa

W ramach audytu zespół koncentrował się na potwierdzeniu zgodności z 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 norm

Zakres prac obejmował między innymi adekwatne wymagania:

* Artykuł 8 KSC
* Rozporządzenie 2080 w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej
* Wymagania normy ISO 27001 w rozdziałach 6, 7, 8, 9,10
* Załącznika A do normy ISO 27001 A.5, A.6, A.8, A.9, A.10, A.11, A.12, 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

## Ryzyka zidentyfikowane w czasie audytu

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Zdarzenie niepożądane | Opis ryzyka | Priorytet |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Zalecenia

|  |  |
| --- | --- |
| Obserwacja | Rekomendacje |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# Obszar 9: Bezpieczeństwo fizyczne

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

## Kontekst w zakresie przepisów i norm

Zakres prac obejmował między innymi adekwatne wymagania:

* Artykuł 8,10,14 KSC
* Ustawy o ochronie osób i mienia
* Rozporządzenie XXXX z 23 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 2080 w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej
* Wymagania normy ISO 27001 w rozdziałach 6, 8
* Załącznika A do normy ISO 27001 A.6, A.11

## 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 szafy i sejfy
4. Dokumentacja i zasadność konfiguracji systemu przeciwpożarowego
5. Przechowywanie i dostęp do dokumentacji przez PŚUB
6. Potwierdzenie działań wynikających z komunikacji z szacowaniem ryzyka SI\_OUK

## Ryzyka zidentyfikowane w czasie audytu

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Zdarzenie niepożądane | Opis ryzyka | Priorytet |
|  |  |  |  |
|  |  |  |  |

## Zalecenia

|  |  |
| --- | --- |
| Obserwacja | Rekomendacje |
|  |  |
|  |  |
|  |  |

# Obszar 10: Zarządzanie bezpieczeństwem i ciągłością działania łańcucha usług

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

## Kontekst w zakresie przepisów i norm

Zakres prac obejmował między innymi adekwatne wymagania:

* Artykuł 8,14 KSC
* Rozporządzenie 2080 w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej
* ​wymagania normy ISO 27001 w rozdziałach 6, 7, 8
* Załącznika A do normy ISO 27001 A.6, A.15, A.17

## Kontekst w zakresie Decyzji OUK

### Dostawcy OUK - dokumentacja

1. Polityka bezpieczeństwa w relacjami z dostawcami
2. Standardy i wymagania nakładane na dostawców w umowach w zakresie Cyberbezpieczeństwa
3. Bezpieczeństwo łańcucha dostaw
4. Monitorowanie bieżące i przegląd usług świadczonych przez dostawców
5. Standardy w umowach dotyczące „cyber”
6. Wyniki audytów 2 / 3 strony (zewnętrzne)
7. Dostęp do VPN
8. Akceptowalne użycie aktywów – lista przypadków

### Dokumentacja podmiotu Świadczący Usługi Cyberbezpieczeństwa

1. Wymagania w zakresie personelu (Dz.U XXXX z 23.12.2019r)
2. Wymagania w zakresie ochrony fizycznej podmiotu
3. Zastosowane systemy zabezpieczeń teleinformatycznej w zakresie dostępów do dokumentacji
4. Zastosowane systemy zabezpieczeń teleinformatycznej w zakresie pracy zdalnej

## Ryzyka zidentyfikowane w czasie audytu

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Zdarzenie niepożądane | Opis ryzyka | Priorytet |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Zalecenia

|  |  |
| --- | --- |
| Obserwacja | Rekomendacje |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# Skróty i definicje

|  |  |
| --- | --- |
| Definicja | Wyjaśnienie |
| ​  Audytor Wiodący | Audytor wyznaczony jako lider zespołu audytowego, odpowiedzialny za zakres audytu, jego programu, 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 cyberbezpieczeństwa |
| KSC | Ustawa o Krajowym Systemie Cyberbezpieczeństwa |
| OUK | Operator Usługi Kluczowej |
| DC | Dział, Departament lub Biuro bezpośrednio odpowiedzialne za realizacje zadań w zakresie cyberbezpieczeństwa OUK |
| UK | Usługa Kluczowa - zestaw funkcji, towarów i usług uznanych przez Organ Właściwych za istotny dla sprawnego działania Cyberbezpieczeństwa Rzeczypospolitej Polskiej |
| ​  Mechanizm kontrolny | Środki techniczne i organizacyjne (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 |
| ​  Program audytu | Przygotowany przez Audytora Wiodącego i zatwierdzony przez Operatora Usługi Kluczowej program zadania audytowego |
| ​  Raport z audytu | Dokument przygotowany pod nadzorem Audytora Wiodącego zawierający obserwacje (ustalenia stanu faktycznego) w zakresie zaobserwowanych niezgodności, ocenę systemu, klasyfikację zidentyfikowanego ryzyka oraz rekomendacje dla Kierownictwa OUK |
| ​  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 informatyczny | System informatyczny wykorzystywany do świadczenia usługi kluczowej |
| Operator usługi kluczowej | Podmiot gospodarczy wykonujący działania uznane przez państwo Polskie za istotne, a wobec którego organ właściwy do spraw cyberbezpieczeństwa wydał decyzję o uznaniu za operatora usługi kluczowej |
| Organ właściwy | Organami właściwymi do spraw cyberbezpieczeństwa są ministrowie właściwi do spraw zgodnie z podziałem sektorowym. Organ właściwy kontroluje i nakłada kary pieniężne na operatorów usług kluczowych i dostawców usług cyfrowych |
| 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 wystąpienia * opracowywanie wniosków   wynikających z obsługi incydentu |
| Szacowanie ryzyka | Bieżące prace polegające na ocenie sytuacji w zarządzanej cyberprzestrzeni polegające co najmniej na:  ​identyfikacji   * analizie * ocenie ryzyka |
| Obsługa incydentu | Szczegółowy zestaw czynności wykonywanych w sposób powtarzalny i udokumentowany, a składający się z co najmniej faz:   * wykrywanie * rejestrowanie * analizowanie * klasyfikowanie * priorytetyzację * podejmowanie działań naprawczych * ograniczenie skutków incydentu |
| Pełnomocnik OUK | osoba odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa |
| 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 zarządzania podatnościami | Osoba odpowiedzialna u OUK za wypełnianie obowiązków operatora w zakresie artykułu 8 punkt 3 w zakresie identyfikacji i postępowania z podatnościami na 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 operatora usługi kluczowej identyfikowany w organizacji jako jeden lub wiele komponentów technologicznych potrzebnych do poprawnego i optymalnego z punktu widzenia ekonomicznego działania zestawu usług / produktów uznanych przez organ właściwy za podstawę działania usługi kluczowej |

Notatka Licencyjna: Dokument utworzony na bazie szablonu audytu przygotowanego przez członków „ISSA Polska Stowarzyszenie ds. Bezpieczeństwa Systemów Informacyjnych”, „Instytut Audytorów Wewnętrznych IIA Polska” na licencji MIT (https://pl.wikipedia.org/wiki/Licencja\_MIT) [[2]](#footnote-2)

Uwagi i poprawki: <https://github.com/issapolska/Audyt_KSC/issues>

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

Kontakt mailowy: [ksc@issa.org.pl](mailto:ksc@issa.org.pl)

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. [↑](#footnote-ref-1)
2. Uwagi do kolejnych wersji prosimy zgłaszać przez <https://github.com/issapolska/Audyt_KSC/issues> [↑](#footnote-ref-2)