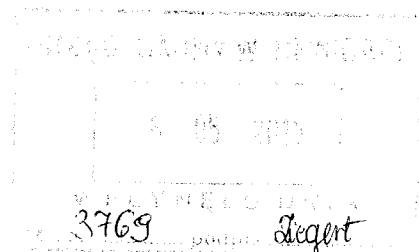


AW – 1720.3.2014

URZĄD GMINY  
84-312 w Cewicach  
ul. W. Witosa 16  
woj. pomorskie  
tel. 59 861 34 60, 861 34 61, fax 59 861 34 62  
NIP 841-10-13-327, REGON 000531677



## Sprawozdanie z przeprowadzenia audytu wewnętrznego

Urząd Gminy Cewice  
84-312 Cewice, ul. W. Witosa 16  
Cewice, 25 maja 2015r.

# Raport z zadania audytowego

## Audyt bezpieczeństwa informacji Urzędu Gminy w Cewicach

zadanie przeprowadzone przez: **Mariusz Mitura**

data opracowania:

wersja zadania: **1**

### Opis zadania

Audyt zgodności z normami PN-ISO/IEC 27001 i PN-ISO/IEC 17799

### Zakres podmiotowy

**Urząd Gminy Cewice**

### Systemy oceniania

#### 1. Ocena wstępna

typ oceny: **Suma ważona**

#### Podoceny

##### 1.1. Ocena-ABI

rodzaj oceny: **Ocena prosta ze zdefiniowanymi wartościami**

waga: **1**

waga względna: **16%**

##### 1.2. Ocena-Sekretarz Gminy

rodzaj oceny: **Ocena prosta ze zdefiniowanymi wartościami**

waga: **1**

waga względna: **16%**

##### 1.3. Ocena-Informatyk

rodzaj oceny: **Ocena prosta ze zdefiniowanymi wartościami**

waga: **1**

waga względna: **16%**

##### 1.4. Ocena-Z\_ ca Główniej Księgowej

rodzaj oceny: **Ocena prosta ze zdefiniowanymi wartościami**

waga: **1**

waga względna: **16%**

## 1.5. Ocena-Kadry

rodzaj oceny:	Ocena prosta ze zdefiniowanymi wartościami
waga:	1
waga względna:	16%

## 1.6. Ocena-Stanowisko ds. BHP

rodzaj oceny:	Ocena prosta ze zdefiniowanymi wartościami
waga:	1
waga względna:	16%

## Struktura przedmiotowa

### Wybrany element: Przedmiot Audytu

- **A.5 POLITYKA BEZPIECZEŃSTWA**
  - A.5.1 Polityka bezpieczeństwa informacji
- **A.6 ORGANIZACJA BEZPIECZEŃSTWA INFORMACJI**
  - A.6.1 Organizacja wewnętrzna
  - A.6.2 Strony zewnętrzne
- **A.7 ZARZĄDZANIE AKTYWAMI**
  - A.7.1 Odpowiedzialność za aktywa
  - A.7.2 Klasyfikacja informacji
- **A.8 BEZPIECZEŃSTWO ZASOBÓW LUDZKICH**
  - A.8.1 Przed zatrudnieniem
  - A.8.2 Podczas zatrudnienia
  - A.8.3 Zakończenie lub zmiana zatrudnienia
- **A.9 BEZPIECZEŃSTWO FIZYCZNE I ŚRODOWISKOWE**
  - A.9.1 Obszary bezpieczne
  - A.9.2 Bezpieczeństwo sprzętu
- **A.10 ZARZĄDZANIE SYSTEMAMI I SIECIAMI**
  - A.10.1 Procedury eksploatacyjne i zakresy odpowiedzialności
  - A.10.2 Zarządzanie usługami dostarczonymi przez strony trzecie
  - A.10.3 Planowanie i odbiór systemów
  - A.10.4 Ochrona przed kodem złośliwym i kodem mobilnym
  - A.10.5 Kopie zapasowe
  - A.10.6 Zarządzanie bezpieczeństwem sieci
  - A.10.7 Obsługa nośników
  - A.10.8 Wymiana informacji
  - A.10.9 Usługi handlu elektronicznego
  - A.10.10 Monitorowanie
- **A.11 KONTROLA DOSTĘPU**
  - A.11.1 Wymagania biznesowe wobec kontroli dostępu

- A.11.2 Zarządzanie dostępem użytkowników
- A.11.3 Odpowiedzialność użytkowników
- A.11.4 Kontrola dostępu do sieci
- A.11.5 Kontrola dostępu do systemów operacyjnych
- A.11.6 Kontrola dostępu do aplikacji i informacji
- A.11.7 Przetwarzanie mobilne i praca na odległość
- **A.12 POZYSKIWANIE, ROZWÓJ I UTRZYMANIE SYSTEMÓW INFORMACYJNYCH**
  - A.12.1 Wymagania bezpieczeństwa systemów informacyjnych
  - A.12.2 Poprawne przetwarzanie w aplikacjach
  - A.12.3 Zabezpieczenia kryptograficzne
  - A.12.4 Bezpieczeństwo plików systemowych
  - A.12.5 Bezpieczeństwo w procesach rozwojowych i obsługi informatycznej
  - A.12.6 Zarządzanie podatnościami technicznymi
- **A.13 ZARZĄDZANIE INCYDENTAMI ZWIĄZANYMI Z BEZPIECZEŃSTWEM INFORMACJI**
  - A.13.1 Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji i słabości
  - A.13.2 Zarządzanie incydentami związanymi z bezpieczeństwem informacji oraz udoskonaleniami
- **A.14 ZARZĄDZANIE CIĄGŁOŚCIĄ DZIAŁANIA**
  - A.14.1 Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania
- **A.15 ZGODNOŚĆ**
  - A.15.1 Zgodność z przepisami prawnymi
  - A.15.2 Zgodność z politykami bezpieczeństwa i standardami oraz zgodność techniczna
  - A.15.3 Rozważania dotyczące audytu systemów informacyjnych

## Wyniki badań

### 1. Badanie wstępne poziomu niezgodności

Obszar:

#### 1. A.5 Polityka bezpieczeństwa

Waga:	2.00
Waga względna:	0.02
Właściciel:	Sekretarz Gminy - Kierownik Referatu (SG)

Wybrane oceny

Nazwa	Wartość oceny	Wartość oczekiwana	Wartość znormalizowana
Ocena wstępna	0.00	0.0000	0.0000

#### 2. A.6 Organizacja bezpieczeństwa informacji

Waga:	11.00
Waga względna:	0.08

Właściciel: **Informatyk**

**Wybrane oceny**

Nazwa	Wartość oceny	Wartość oczekiwana	Wartość znormalizowana
Ocena wstępna	0.00	0.0000	0.0000

**3. A.7 Zarządzanie aktywami**

Waga: **5.00**

Waga względna: **0.04**

Właściciel: **Sekretarz Gminy - Kierownik Referatu (SG)**

**Wybrane oceny**

Nazwa	Wartość oceny	Wartość oczekiwana	Wartość znormalizowana
Ocena wstępna	0.00	0.0000	0.0000

**4. A.8 Bezpieczeństwo zasobów ludzkich**

Waga: **9.00**

Waga względna: **0.07**

Właściciel: **Sekretarz Gminy - Kierownik Referatu (SG)**

**Wybrane oceny**

Nazwa	Wartość oceny	Wartość oczekiwana	Wartość znormalizowana
Ocena wstępna	0.08	0.7500	0.0056

**5. A.9 Bezpieczeństwo fizyczne i środowiskowe**

Waga: **13.00**

Waga względna: **0.10**

Właściciel: **Informatyk**

**Wybrane oceny**

Nazwa	Wartość oceny	Wartość oczekiwana	Wartość znormalizowana
Ocena wstępna	0.17	2.2500	0.0169

**6. A.10 Zarządzanie systemami i sieciami**

Waga: **32.00**

Waga względna: **0.24**

Właściciel: **Informatyk**

**Wybrane oceny**

Nazwa	Wartość oceny	Wartość oczekiwana	Wartość znormalizowana
Ocena wstępna	0.09	3.0000	0.0226

### 7. A.11 Kontrola dostępu

Waga: **25.00**  
Waga względna: **0.19**  
Właściciel: **Informatyk**

#### Wybrane oceny

Nazwa	Wartość oceny	Wartość oczekiwana	Wartość znormalizowana
Ocena wstępna	0.18	4.5000	0.0338

### 8. A.12 Pozyskiwanie, rozwój i utrzymanie systemów informacyjnych

Waga: **16.00**  
Waga względna: **0.12**  
Właściciel: **Informatyk**

#### Wybrane oceny

Nazwa	Wartość oceny	Wartość oczekiwana	Wartość znormalizowana
Ocena wstępna	0.00	0.0000	0.0000

### 9. A.13 Zarządzanie incydentami związanymi z bezpieczeństwem informacji

Waga: **5.00**  
Waga względna: **0.04**  
Właściciel: **Sekretarz Gminy - Kierownik Referatu (SG)**

#### Wybrane oceny

Nazwa	Wartość oceny	Wartość oczekiwana	Wartość znormalizowana
Ocena wstępna	0.00	0.0000	0.0000

### 10. A.14 Zarządzanie ciągłością działania

Waga: **5.00**  
Waga względna: **0.04**  
Właściciel: **Sekretarz Gminy - Kierownik Referatu (SG)**

#### Wybrane oceny

Nazwa	Wartość oceny	Wartość oczekiwana	Wartość znormalizowana
Ocena wstępna	0.25	1.2500	0.0094

### 11. A.15 Zgodność

Waga: **10.00**  
Waga względna: **0.08**  
Właściciel: **Informatyk**

#### Wybrane oceny

Nazwa	Wartość oceny	Wartość oczekiwana	Wartość znormalizowana
Ocena wstępna	0.25	2.5000	0.0188

### Ustalenia

Wykonawca w badaniu przyjął podejście ostrożnościowe, z uwagi iż jest to pierwsze badanie należy otrzymane oceny obdarzyć mniejszym zaufaniem. W związku z tym zalecenia wydano tylko dla kategorii bezpieczeństwa, które osiągnęły, bądź przekroczyły wysoki poziom ryzyka i należą do obszaru, który również osiągnął, bądź przekroczył ten poziom. Do sprawozdania załączono pełną mapę ryzyka bezpieczeństwa informacji w UG w Cewicach, oraz szczegółowe mapy obszarów z punktu 1) tj. tych, które przekroczyły wysoki poziom ryzyka.

1) Przekroczony wysoki poziom ryzyka:

obszary: A.10 - Zarządzanie systemami i sieciami, A.11 - Kontrola dostępu.

Pomiędzy średnim a wysokim poziomem ryzyka:

obszary: A.9 – Bezpieczeństwo fizyczne i środowiskowe, A.15 – Zgodność.

Pomiędzy niskim a średnim poziomem ryzyka:

obszary: A.14 - Zarządzanie ciągłością działania.

Poniżej niskiego poziomu ryzyka:

obszary: A.5 – Polityka bezpieczeństwa, A.6 – Organizacja bezpieczeństwa informacji, A.7 – Zarządzanie aktywami, A.8 – Bezpieczeństwo zasobów ludzkich, A.12 - Pozyskiwanie, rozwój i utrzymanie systemów informacyjnych, A.13 - Zarządzanie incydentami związanymi z bezpieczeństwem informacji.

### Kryteria

Kryteria – wartości przyjęto arbitralnie kierując się wynikami ocen i wagami obszarów

Poziom ryzyka wysoki - wartość oczekiwana = 3.0

Poziom ryzyka średni - wartość oczekiwana = 2.0

Poziom ryzyka niski - wartość oczekiwana = 1.0

## 2. A.5 Polityka bezpieczeństwa

**Kategoria:**

### 1. A.5.1 Polityka bezpieczeństwa informacji

Waga: **2.00**

Waga względna: **1.00**

Właściciel: **Informatyk**

**Wybrane oceny**

Nazwa	Wartość oceny	Wartość oczekiwana	Wartość znormalizowana
Ocena wstępna	0.00	0.0000	0.0000

### Ustalenia

Poniżej niskiego poziomu ryzyka w kategorii bezpieczeństwa: A.5.1 Polityka bezpieczeństwa informacji

### Kryteria

Poziom ryzyka wysoki - wartość oczekiwana = 1.0

Poziom ryzyka średni - wartość oczekiwana = 0.5

Poziom ryzyka niski - wartość oczekiwana = 0.2

### 3. A.6 Organizacja bezpieczeństwa informacji

**Kategoria:**

#### 1. A.6.1 Organizacja wewnętrzna

Waga: **8.00**

Waga względna: **0.73**

Właściciel: **Sekretarz Gminy - Kierownik Referatu (SG)**

**Wybrane oceny**

Nazwa	Wartość oceny	Wartość oczekiwana	Wartość znormalizowana
Ocena wstępna	0.00	0.0000	0.0000

#### 2. A.6.2 Strony zewnętrzne

Waga: **3.00**

Waga względna: **0.27**

Właściciel: **Sekretarz Gminy - Kierownik Referatu (SG)**

**Wybrane oceny**

Nazwa	Wartość oceny	Wartość oczekiwana	Wartość znormalizowana
Ocena wstępna	0.00	0.0000	0.0000

#### **Ustalenia**

Poniżej niskiego poziomu ryzyka w kategorii bezpieczeństwa: A.6.1 Organizacja wewnętrzna, A.6.2 Strony zewnętrzne.

#### **Kryteria**

Poziom ryzyka wysoki - wartość oczekiwana = 1.0

Poziom ryzyka średni - wartość oczekiwana = 0.5

Poziom ryzyka niski - wartość oczekiwana = 0.2

### 4. A.7 Zarządzanie aktywami

**Kategoria:**

#### 1. A.7.1 Odpowiedzialność za aktywa

Waga: **3.00**

Waga względna: **0.60**

Właściciel: **Informatyk**

**Wybrane oceny**

Nazwa	Wartość oceny	Wartość oczekiwana	Wartość znormalizowana
Ocena wstępna	0.00	0.0000	0.0000



## 2. A.7.2 Klasyfikacja informacji

Waga: 2.00

Waga względna: 0.40

Właściciel: Sekretarz Gminy - Kierownik Referatu (SG)

### Wybrane oceny

Nazwa	Wartość oceny	Wartość oczekiwana	Wartość znormalizowana
Ocena wstępna	0.00	0.0000	0.0000

### Ustalenia

Poniżej niskiego poziomu ryzyka kategorii bezpieczeństwa A.7.1 Odpowiedzialność za aktywa, A.7.2 Klasyfikacja informacji.

### Kryteria

Poziom ryzyka wysoki - wartość oczekiwana = 1.0

Poziom ryzyka średni - wartość oczekiwana = 0.5

Poziom ryzyka niski - wartość oczekiwana = 0.2

## 5. A.8 Bezpieczeństwo zasobów ludzkich

### Kategoria:

#### 1. A.8.1 Przed zatrudnieniem

Waga: 3.00

Waga względna: 0.33

Właściciel: Stanowisko ds. kadr

### Wybrane oceny

Nazwa	Wartość oceny	Wartość oczekiwana	Wartość znormalizowana
Ocena wstępna	0.00	0.0000	0.0000

#### 2. A.8.2 Podczas zatrudnienia

Waga: 3.00

Waga względna: 0.33

Właściciel: Sekretarz Gminy - Kierownik Referatu (SG)

### Wybrane oceny

Nazwa	Wartość oceny	Wartość oczekiwana	Wartość znormalizowana
Ocena wstępna	0.25	0.7500	0.0833

#### 3. A.8.3 Zakończenie lub zmiana zatrudnienia

Waga: 3.00

Waga względna: 0.33

Właściciel: Stanowisko ds. kadr

### Wybrane oceny

Nazwa	Wartość oceny	Wartość oczekiwana	Wartość znormalizowana
Ocena wstępna	0.00	0.0000	0.0000

#### Ustalenia

Pomiędzy średnim a wysokim poziomem ryzyka w kategorii bezpieczeństwa: A.8.2 - Podczas zatrudnienia.

Poniżej niskiego poziomu ryzyka w kategorii bezpieczeństwa: A.8.1 - Przed zatrudnieniem, oraz A.8.3 - Zakończenie lub zmiana zatrudnienia.

#### Kryteria

Poziom ryzyka wysoki - wartość oczekiwana = 1.0

Poziom ryzyka średni - wartość oczekiwana = 0.5

Poziom ryzyka niski - wartość oczekiwana = 0.2

### 6. A.9 Bezpieczeństwo fizyczne i środowiskowe

#### Kategoria:

##### 1. A.9.1 Obszary bezpieczne

Waga: **6.00**

Waga względna: **0.46**

Właściciel: **Informatyk**

#### Wybrane oceny

Nazwa	Wartość oceny	Wartość oczekiwana	Wartość znormalizowana
Ocena wstępna	0.08	0.5000	0.0385

##### 2. A.9.2 Bezpieczeństwo sprzętu

Waga: **7.00**

Waga względna: **0.54**

Właściciel: **Informatyk**

#### Wybrane oceny

Nazwa	Wartość oceny	Wartość oczekiwana	Wartość znormalizowana
Ocena wstępna	0.25	1.7500	0.1346

#### Ustalenia

Przekroczony wysoki poziom ryzyka w kategorii bezpieczeństwa: A.9.2 Bezpieczeństwo sprzętu.

Osiągnięty średni poziom ryzyka w kategorii bezpieczeństwa: A.9.1 Obszary bezpieczne.

#### Kryteria

Poziom ryzyka wysoki - wartość oczekiwana = 1.0

Poziom ryzyka średni - wartość oczekiwana = 0.5

Poziom ryzyka niski - wartość oczekiwana = 0.2

#### Zalecenia

## 1. Zalecenie A.9.2 - Bezpieczeństwo sprzętu

### Treść zalecenia:

Ponieważ cały obszar A. 9.(Bezpieczeństwo fizyczne i środowiskowe) nie osiągnął wysokiego poziomu ryzyka, zaleceń nie wydano dla tej kategorii.

## 7. A.10 Zarządzanie systemami i sieciami

### Kategoria:

#### 1. A.10.1 Procedury eksploatacyjne i zakresy odpowiedzialności

Waga: 4.00  
Waga względna: 0.13  
Właściciel: Informatyk

#### Wybrane oceny

Nazwa	Wartość oceny	Wartość oczekiwana	Wartość znormalizowana
Ocena wstępna	0.00	0.0000	0.0000

#### 2. A.10.2 Zarządzanie usługami dostarczonymi przez strony trzeci

Waga: 3.00  
Waga względna: 0.09  
Właściciel: Informatyk

#### Wybrane oceny

Nazwa	Wartość oceny	Wartość oczekiwana	Wartość znormalizowana
Ocena wstępna	0.00	0.0000	0.0000

#### 3. A.10.3 Planowanie i odbiór systemów

Waga: 2.00  
Waga względna: 0.06  
Właściciel: Informatyk

#### Wybrane oceny

Nazwa	Wartość oceny	Wartość oczekiwana	Wartość znormalizowana
Ocena wstępna	0.25	0.5000	0.0156

#### 4. A.10.4 Ochrona przed kodem złośliwym i kodem mobilnym

Waga: 2.00  
Waga względna: 0.06  
Właściciel: Informatyk

#### Wybrane oceny

Nazwa	Wartość oceny	Wartość oczekiwana	Wartość znormalizowana
Ocena wstępna	0.25	0.5000	0.0156

### 5. A.10.5 Kopie zapasowe

Waga: 1.00  
Waga względna: 0.03  
Właściciel: Informatyk

#### Wybrane oceny

Nazwa	Wartość oceny	Wartość oczekiwana	Wartość znormalizowana
Ocena wstępna	0.00	0.0000	0.0000

### 6. A.10.6 Zarządzanie bezpieczeństwem sieci

Waga: 2.00  
Waga względna: 0.06  
Właściciel: Informatyk

#### Wybrane oceny

Nazwa	Wartość oceny	Wartość oczekiwana	Wartość znormalizowana
Ocena wstępna	0.50	1.0000	0.0313

### 7. A.10.7 Obsługa nośników

Waga: 4.00  
Waga względna: 0.13  
Właściciel: Referat Budżetowy (SK)

#### Wybrane oceny

Nazwa	Wartość oceny	Wartość oczekiwana	Wartość znormalizowana
Ocena wstępna	0.25	1.0000	0.0313

### 8. A.10.8 Wymiana informacji

Waga: 5.00  
Waga względna: 0.16  
Właściciel: Kierownik USC (ABI)

#### Wybrane oceny

Nazwa	Wartość oceny	Wartość oczekiwana	Wartość znormalizowana
Ocena wstępna	0.00	0.0000	0.0000

### 9. A.10.9 Usługi handlu elektronicznego

Waga: 3.00  
Waga względna: 0.09  
Właściciel: Informatyk

#### Wybrane oceny

Nazwa	Wartość oceny	Wartość oczekiwana	Wartość znormalizowana
Ocena wstępna	0.00	0.0000	0.0000

#### 10. A.10.10 Monitorowanie

Waga: **6.00**  
Waga względna: **0.19**  
Właściciel: **Informatyk**

#### Wybrane oceny

Nazwa	Wartość oceny	Wartość oczekiwana	Wartość znormalizowana
Ocena wstępna	0.00	0.0000	0.0000

#### Ustalenia

Osiągnięty wysoki poziom ryzyka w kategorii bezpieczeństwa: A.10.6 Zarządzanie bezpieczeństwem sieci, oraz A.10.7 Obsługa nośników.

Osiągnięty średni poziom ryzyka w kategorii bezpieczeństwa: A.10.3 Planowanie i odbiór systemów, oraz A.10.4 Ochrona przed kodem złośliwym i kodem mobilnym.

Poniżej niskiego poziomu ryzyka w kategorii bezpieczeństwa: A.10.1 Procedury eksploatacyjne i zakresy odpowiedzialności, oraz A.10.2 Zarządzanie usługami dostarczonymi przez strony trzecie, oraz A.10.5 Kopie zapasowe, oraz A.10.8 Wymiana informacji, oraz A.10.9 Usługi handlu elektronicznego, oraz A.10.10 Monitorowanie.

#### Kryteria

Poziom ryzyka wysoki - wartość oczekiwana = 1.0

Poziom ryzyka średni - wartość oczekiwana = 0.5

Poziom ryzyka niski - wartość oczekiwana = 0.2

#### Zalecenia

##### 1. Zalecenie A.10.6 Zarządzanie bezpieczeństwem sieci.

adresat: **Informatyk**

##### Treść zalecenia:

Zaleca się rozważyć zasadność wdrożenia oprogramowania do monitorowania sieci.

##### 2. Zalecenie A.10.7 Obsługa nośników

adresat: **Informatyk**

##### Treść zalecenia:

Zaleca się rozważyć potrzebę ewidencjonowania dostępu do pomieszczenia serwerowni.

#### 8. A.11 Kontrola dostępu

##### Kategoria:

##### 1. A.11.1 Wymagania biznesowe wobec kontroli dostępu

Waga: **1.00**  
Waga względna: **0.04**  
Właściciel: **Kierownik USC (ABI)**

#### Wybrane oceny

Nazwa	Wartość oceny	Wartość oczekiwana	Wartość znormalizowana
Ocena wstępna	0.00	0.0000	0.0000

### 2. A.11.2 Zarządzanie dostępem użytkowników

Waga: **4.00**

Waga względna: **0.16**

Właściciel: **Kierownik USC (ABI)**

#### Wybrane oceny

Nazwa	Wartość oceny	Wartość oczekiwana	Wartość znormalizowana
Ocena wstępna	0.00	0.0000	0.0000

### 3. A.11.3 Odpowiedzialność użytkowników

Waga: **3.00**

Waga względna: **0.12**

Właściciel: **Informatyk**

#### Wybrane oceny

Nazwa	Wartość oceny	Wartość oczekiwana	Wartość znormalizowana
Ocena wstępna	0.25	0.7500	0.0300

### 4. A.11.4 Kontrola dostępu do sieci

Waga: **7.00**

Waga względna: **0.28**

Właściciel: **Informatyk**

#### Wybrane oceny

Nazwa	Wartość oceny	Wartość oczekiwana	Wartość znormalizowana
Ocena wstępna	0.25	1.7500	0.0700

### 5. A.11.5 Kontrola dostępu do systemów operacyjnych

Waga: **6.00**

Waga względna: **0.24**

Właściciel: **Informatyk**

#### Wybrane oceny

Nazwa	Wartość oceny	Wartość oczekiwana	Wartość znormalizowana
Ocena wstępna	0.25	1.5000	0.0600

### 6. A.11.6 Kontrola dostępu do aplikacji i informacji

Waga: **2.00**

Waga względna: **0.08**

Właściciel: **Informatyk**

**Wybrane oceny**

Nazwa	Wartość oceny	Wartość oczekiwana	Wartość znormalizowana
Ocena wstępna	0.25	0.5000	0.0200

**7. A.11.7 Przetwarzanie mobilne i praca na odległość**

Waga: **2.00**

Waga względna: **0.08**

Właściciel: **Informatyk**

**Wybrane oceny**

Nazwa	Wartość oceny	Wartość oczekiwana	Wartość znormalizowana
Ocena wstępna	0.00	0.0000	0.0000

**Ustalenia**

Przekroczony wysoki poziom ryzyka w kategorii bezpieczeństwa: A.11.4 Kontrola dostępu do sieci oraz A.11.5 Kontrola dostępu do systemów operacyjnych.

Pomiędzy średnim a wysokim poziomem ryzyka w kategorii bezpieczeństwa: A.11.3 Odpowiedzialność użytkowników.

Osiągnięty średni poziom ryzyka w kategorii bezpieczeństwa: A.11.6 Kontrola dostępu do aplikacji i informacji.

Poniżej niskiego poziomu ryzyka w kategorii bezpieczeństwa A.11.1 - Wymagania biznesowe wobec kontroli dostępu oraz A.11.2 Zarządzanie dostępem użytkowników oraz A.11.7 - Przetwarzanie mobilne i praca na odległość.

**Kryteria**

Poziom ryzyka wysoki - wartość oczekiwana = 1.0

Poziom ryzyka średni - wartość oczekiwana = 0.5

Poziom ryzyka niski - wartość oczekiwana = 0.2

**Zalecenia**

**1. Zalecenie A 11.4 Kontrola dostępu do sieci i A.11.5 Kontrola dostępu do systemów operacyjnych**

adresat: **Informatyk**

**Treść zalecenia:**

Zaleca się rozważyć zasadność wdrożenia oprogramowania do monitorowania sieci.

**9. A.12 Pozyskiwanie, rozwój i utrzymanie systemów informacyjnych**

**Kategoria:**

**1. A.12.1 Wymagania bezpieczeństwa systemów informacyjnych**

Waga: **1.00**

Waga względna: **0.06**

Właściciel: **Informatyk**

**Wybrane oceny**

Nazwa	Wartość oceny	Wartość oczekiwana	Wartość znormalizowana
Ocena wstępna	0.00	0.0000	0.0000

### **2. A.12.2 Poprawne przetwarzanie w aplikacjach**

Waga: **4.00**

Waga względna: **0.25**

Właściciel: **Informatyk**

**Wybrane oceny**

Nazwa	Wartość oceny	Wartość oczekiwana	Wartość znormalizowana
Ocena wstępna	0.00	0.0000	0.0000

### **3. A.12.3 Zabezpieczenia kryptograficzne**

Waga: **2.00**

Waga względna: **0.13**

Właściciel: **Informatyk**

**Wybrane oceny**

Nazwa	Wartość oceny	Wartość oczekiwana	Wartość znormalizowana
Ocena wstępna	0.00	0.0000	0.0000

### **4. A.12.4 Bezpieczeństwo plików systemowych**

Waga: **3.00**

Waga względna: **0.19**

Właściciel: **Informatyk**

**Wybrane oceny**

Nazwa	Wartość oceny	Wartość oczekiwana	Wartość znormalizowana
Ocena wstępna	0.00	0.0000	0.0000

### **5. A.12.5 Bezpieczeństwo w procesach rozwojowych i obsługi informatycznej**

Waga: **5.00**

Waga względna: **0.31**

Właściciel: **Informatyk**

**Wybrane oceny**

Nazwa	Wartość oceny	Wartość oczekiwana	Wartość znormalizowana
Ocena wstępna	0.00	0.0000	0.0000

### **6. A.12.6 Zarządzanie podatnościami technicznymi**

Waga: **1.00**



Waga względna: **0.06**  
Właściciel: **Informatyk**  
**Wybrane oceny**

Nazwa	Wartość oceny	Wartość oczekiwana	Wartość znormalizowana
Ocena wstępna	0.00	0.0000	0.0000

#### **Ustalenia**

Poniżej niskiego poziomu ryzyka w kategorii bezpieczeństwa: A.12.1 Wymagania bezpieczeństwa systemów informacyjnych, oraz A.12.2 Poprawne przetwarzanie w aplikacjach, oraz A.12.3 Zabezpieczenia kryptograficzne, oraz A.12.4 Bezpieczeństwo plików systemowych, oraz A.12.5 Bezpieczeństwo w procesach rozwojowych i obsługi informatycznej, oraz A.12.6 Zarządzanie podatnościami technicznymi.

#### **Kryteria**

Poziom ryzyka wysoki - wartość oczekiwana = 1.0

Poziom ryzyka średni - wartość oczekiwana = 0.5

Poziom ryzyka niski - wartość oczekiwana = 0.2

### **10. A.13 Zarządzanie incydentami związanymi z bezpieczeństwem informacji**

#### **Kategoria:**

#### **1. A.13.1 Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji i słabości**

Waga: **2.00**  
Waga względna: **0.40**  
Właściciel: **Kierownik USC (ABI)**

#### **Wybrane oceny**

Nazwa	Wartość oceny	Wartość oczekiwana	Wartość znormalizowana
Ocena wstępna	0.00	0.0000	0.0000

#### **2. A.13.2 Zarządzanie incydentami związanymi z bezpieczeństwem informacji oraz udoskonaleniami**

Waga: **3.00**  
Waga względna: **0.60**  
Właściciel: **Kierownik USC (ABI)**

#### **Wybrane oceny**

Nazwa	Wartość oceny	Wartość oczekiwana	Wartość znormalizowana
Ocena wstępna	0.00	0.0000	0.0000

#### **Ustalenia**

Poniżej niskiego poziomu ryzyka w kategorii bezpieczeństwa: A.13.1 Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji i słabości, oraz A.13.2 Zarządzanie incydentami związanymi z bezpieczeństwem informacji oraz udoskonaleniami.

#### Kryteria

Poziom ryzyka wysoki - wartość oczekiwana = 1.0

Poziom ryzyka średni - wartość oczekiwana = 0.5

Poziom ryzyka niski - wartość oczekiwana = 0.2

### 11. A.14 Zarządzanie ciągłością działania

#### Kategoria:

#### 1. A.14.1 Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania

Waga: **5.00**

Waga względna: **1.00**

Właściciel: **Sekretarz Gminy - Kierownik Referatu (SG)**

#### Wybrane oceny

Nazwa	Wartość oceny	Wartość oczekiwana	Wartość znormalizowana
Ocena wstępna	0.25	1.2500	0.2500

#### Ustalenia

Przekroczony wysoki poziom ryzyka kategorii bezpieczeństwa A.14.1 Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania.

#### Kryteria

Poziom ryzyka wysoki - wartość oczekiwana = 1.0

Poziom ryzyka średni - wartość oczekiwana = 0.5

Poziom ryzyka niski - wartość oczekiwana = 0.2

#### Zalecenia

#### 1. Zalecenie A.14.1. Aspekty bezpieczeństwa informacji w zarządzaniu

##### Treść zalecenia:

Ponieważ cały obszar A. 14.(Zarządzanie ciągłością działania) nie osiągnął wysokiego poziomu ryzyka, zaleceń nie wydano dla tej kategorii.

### 12. A.15 Zgodność

#### Kategoria:

#### 1. A.15.1 Zgodność z przepisami prawnymi

Waga: **6.00**

Waga względna: **0.60**

Właściciel: **Kierownik USC (ABI)**

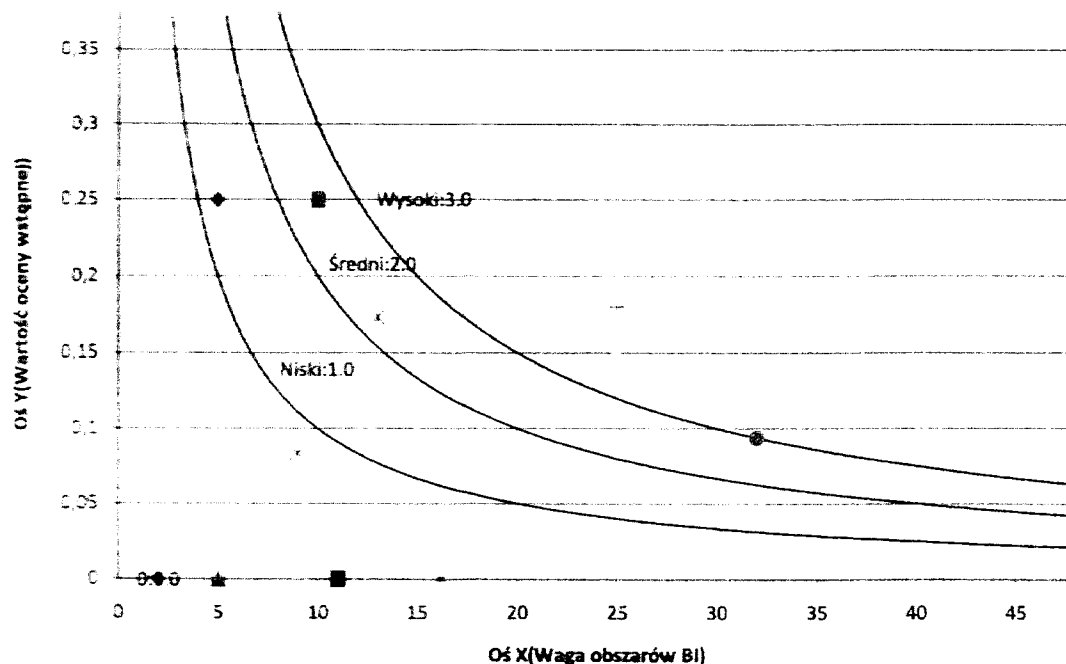
#### Wybrane oceny

Nazwa	Wartość oceny	Wartość oczekiwana	Wartość znormalizowana
Ocena wstępna	0.25	1.5000	0.1500



## Obszary - ocena wstępna poziomu niezgodności w UG Cewice

Załącznik do sprawozdania z audytu bezpieczeństwa informacji



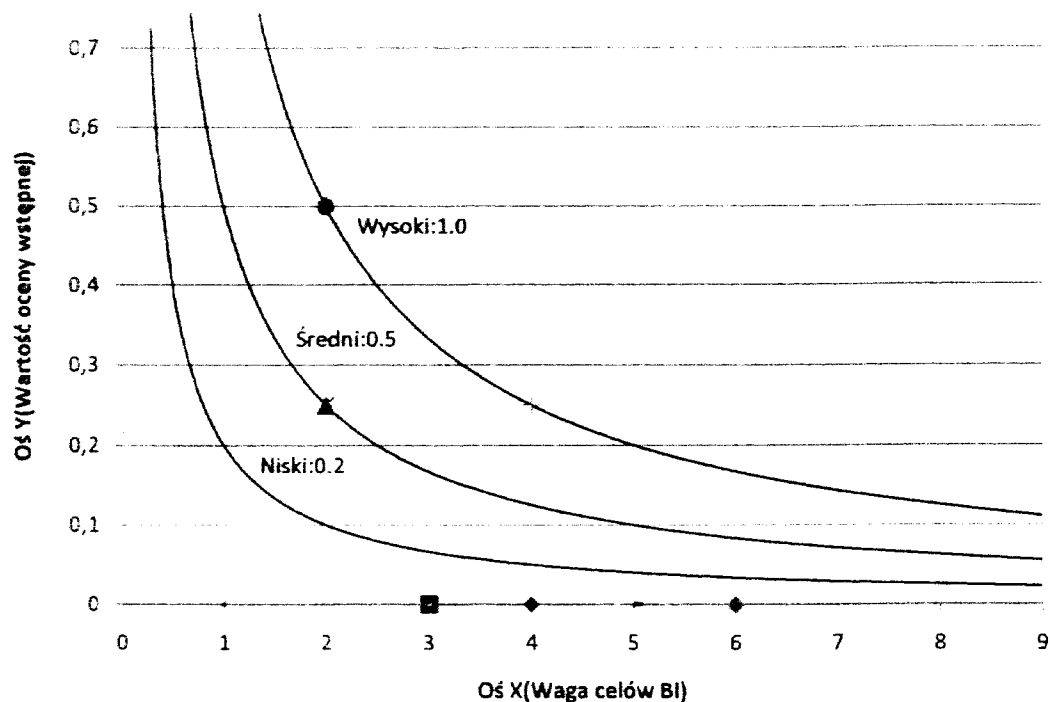
- ◆ A.5 Polityka bezpieczeństwa
- A.6 Organizacja bezpieczeństwa informacji
- ▲ A.7 Zarządzanie aktywami
- × A.8 Bezpieczeństwo zasobów ludzkich
- × A.9 Bezpieczeństwo fizyczne i środowiskowe
- A.10 Zarządzanie systemami i sieciami
- + A.11 Kontrola dostępu
- A.12 Pozyskiwanie, rozwój i utrzymanie systemów informacyjnych
- A.13 Zarządzanie incydentami związanymi z bezpieczeństwem informacji
- ◆ A.14 Zarządzanie ciągłością działania

Obszar	Waga obszarów BI	Wartość oceny wstępnej	wynik
A.5 Polityka bezpieczeństwa	2	0	0,000 poniżej niskiego
A.6 Organizacja bezpieczeństwa informacji	11	0	0,000 poniżej niskiego
A.7 Zarządzanie aktywami	5	0	0,000 poniżej niskiego
A.8 Bezpieczeństwo zasobów ludzkich	9	0,083333333	0,750 poniżej niskiego
A.9 Bezpieczeństwo fizyczne i środowiskowe	13	0,173076923	2,250 pomiędzy średnim a wysokim
A.10 Zarządzanie systemami i sieciami	32	0,09375	3,000 wysoki
A.11 Kontrola dostępu	25	0,18	4,500 wysoki
A.12 Pozyskiwanie, rozwój i utrzymanie systemów informacyjnych	16	0	0,000 poniżej niskiego
A.13 Zarządzanie incydentami związanymi z bezpieczeństwem informacji	5	0	0,000 poniżej niskiego
A.14 Zarządzanie ciągłością działania	5	0,25	1,250 pomiędzy niskim a średnim
A.15 Zgodność	10	0,25	2,500 pomiędzy średnim a wysokim

ALPHAGROUP WĘSKA 100-100  
*Marion Kistner*  
 Kierownik Biura

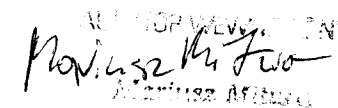
## A.10 Zarządzanie systemami i sieciami w UG Cewice

Załącznik do sprawozdania z audytu bezpieczeństwa informacji

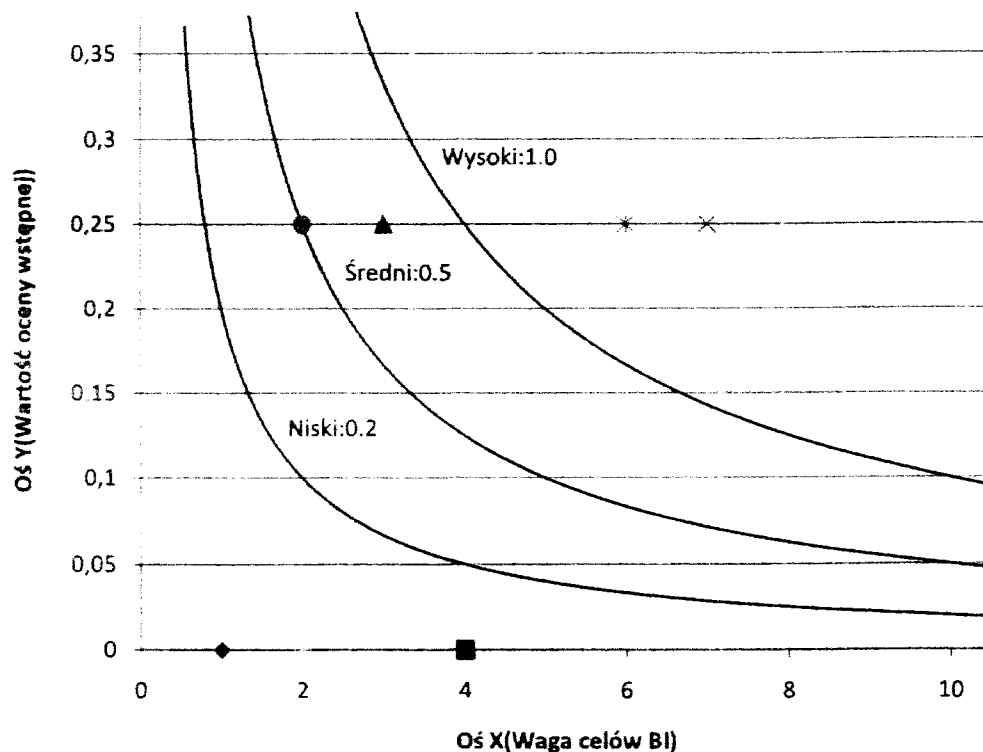


- ◆ A.10.1 Procedury eksploatacyjne i zakresy odpowiedzialności
- A.10.2 Zarządzanie usługami dostarczonymi przez strony trzecie
- ▲ A.10.3 Planowanie i odbiór systemów
- × A.10.4 Ochrona przed kodem złośliwym i kodem mobilnym
- × A.10.5 Kopie zapasowe
- A.10.6 Zarządzanie bezpieczeństwem sieci
- + A.10.7 Obsługa nośników
- A.10.8 Wymiana informacji
- A.10.9 Usługi handlu elektronicznego

	Waga celów BI	Wartość oceny wstępnej	wynik
A.10.1 Procedury eksploatacyjne i zakresy odpowiedzialności	4	0	0 poniżej niskiego
A.10.2 Zarządzanie usługami dostarczonymi przez strony trzecie	3	0	0 poniżej niskiego
A.10.3 Planowanie i odbiór systemów	2	0,25	0,5 średni
A.10.4 Ochrona przed kodem złośliwym i kodem mobilnym	2	0,25	0,5 średni
A.10.5 Kopie zapasowe	1	0	0 poniżej niskiego
A.10.6 Zarządzanie bezpieczeństwem sieci	2	0,5	1 wysoki
A.10.7 Obsługa nośników	4	0,25	1 wysoki
A.10.8 Wymiana informacji	5	0	0 poniżej niskiego
A.10.9 Usługi handlu elektronicznego	3	0	0 poniżej niskiego
A.10.10 Monitorowanie	6	0	0 poniżej niskiego

  
 Piotr Kozłowski  
 Audytor

## A.11 Kontrola dostępu w UG Cewice



Załącznik do sprawozdania z audytu bezpieczeństwa informacji

- ◆ A.11.1 Wymagania biznesowe wobec kontroli dostępu
- A.11.2 Zarządzanie dostępem użytkowników
- ▲ A.11.3 Odpowiedzialność użytkowników
- × A.11.4 Kontrola dostępu do sieci
- × A.11.5 Kontrola dostępu do systemów operacyjnych
- A.11.6 Kontrola dostępu do aplikacji i informacji
- A.11.7 Przetwarzanie mobilne i praca na odległość

	Waga celów BI	Wartość oceny wstępnej	wynik
A.11.1 Wymagania biznesowe wobec kontroli dostępu	1	0	0 poniżej niskiego
A.11.2 Zarządzanie dostępem użytkowników	4	0	0 poniżej niskiego
A.11.3 Odpowiedzialność użytkowników	3	0,25	0,75 pomiędzy średnim a wysokim
A.11.4 Kontrola dostępu do sieci	7	0,25	1,75 wysoki
A.11.5 Kontrola dostępu do systemów operacyjnych	6	0,25	1,5 wysoki
A.11.6 Kontrola dostępu do aplikacji i informacji	2	0,25	0,5 średni
A.11.7 Przetwarzanie mobilne i praca na odległość	2	0	0 poniżej niskiego

ALTUSOR WAWOŁCZYŃSKI  
*Manusia*  
 Marcin Miłan