

Szczegółowy opis zadań realizowanych w ramach zamówienia:

**Kompleksowe opracowanie/aktualizacja dokumentacji SZBI, przegląd SZBI, przeprowadzenie audytu KRI, ksc i testów podatności, przeprowadzenie końcowego audytu wdrożonego systemu zarządzania bezpieczeństwem informacji, szkolenia dla pracowników i kierownictwa z SZBI oraz podstaw ISO 27001 w Urzędzie Gminy Zamość oraz GOPS Zamość w ramach projektu pn. „Cyberbezpieczna Gmina Zamość”**

Całość zamówienia musi być zrealizowana zgodnie z warunkami i wytycznymi konkursu grantowego „Cyberbezpieczny Samorząd”, Priorytet II: Zaawansowane usługi cyfrowe, działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa, Fundusze Europejskie na Rozwój Cyfrowy 2021 – 2027 (FERC).

Opis poszczególnych zadań realizowanych w ramach zamówienia:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Obszar organizacyjny |   |  |  |
| **Lp.** | **Zakres** | **szt./kpl/os.** | **Jednostka** | **Termin realizacji** |
| 1 | SZBI: Uaktualnienie dokumentacji, w tym opracowanie niezbędnych procedur do wymagań KRI/ISO27001, wdrożenie SZBI  | 1 | Urząd Gminy Zamość | 10.03.2025 |
| 2 | Szkolenie dla pracowników i kierownictwa z SZBI oraz podstaw ISO 27001 | 60 | Urząd Gminy Zamość | 28.02.2025 |
| 3 | Audyt KRI, ksc i testy podatności w 2024 r. w UG Zamość | 1 | Urząd Gminy Zamość | 29.11.2024 |
| 4 | Przegląd SZBI w 2025 r. dla UG Zamość | 1 | Urząd Gminy Zamość | 31.10.2025 |
| 5 | Końcowy audyt zgodności przeprowadzany przez uprawnionego audytora wiodącego ISO27001 w UG Zamość | 1 | Urząd Gminy Zamość | 28.11.2025 |
| 6 | Opracowanie pełnej dokumentacji tworzącej SZBI i niezbędnych procedur zgodnie z wymaganiami KRI/ISO27001 dla GOPS Zamość, wdrożenie SZBI w GOPS Zamość | 1 | GOPS Zamość | 10.03.2025 |
| 7 | Szkolenie dla pracowników i kierownictwa z SZBI oraz podstaw ISO 27001 | 27 | GOPS Zamość | 28.02.2025 |
| 8 | Audyt KRI, ksc i testy podatności GOPS Zamość | 1 | GOPS Zamość | 29.11.2024 |
| 9 | Przegląd SZBI w 2025 r. dla GOPS Zamość | 1 | GOPS Zamość | 31.10.2025 |
| 10 | Końcowy audyt zgodności przeprowadzony przez uprawnionego audytora wiodącego ISO27001 w GOPS Zamość  | 1 | GOPS Zamość | 28.11.2025 |

Ad.1

**SZBI: Uaktualnienie dokumentacji, w tym opracowanie niezbędnych procedur do wymagań KRI/ISO27001, wdrożenie SZBI**

1) Uaktualnienie posiadanej dokumentacji i procedur Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) - zgodnie z przepisami prawa unijnego, krajowego oraz normami odnoszącymi się do bezpieczeństwa informacji (np. ISO 27001, ISO 27002 dla systemów informatycznych**, ISO 22301**).

Dokumentacja SZBI musi być opracowana na podstawie Polskiej Normy PN-ISO/IEC 27001, na podstawie Polskich Norm związanych z tą normą, w tym: PN-ISO/IEC 27002 – w odniesieniu do ustanawiania zabezpieczeń, PN-ISO/IEC 27005 – w odniesieniu do zarządzania ryzykiem; PN-ISO/IEC 24762 – w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.

2) Wdrożenie opracowanej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)

3) Wykonawca zobowiązany jest do udziału w końcowym audycie zgodności przeprowadzonym przez uprawnionego audytora wiodącego ISO27001 w Urzędzie Gminy Zamość, który zostanie zlecony przez Zamawiającego w 2025 r.

W sytuacji, gdy końcowy audyt zgodności w 2025 r. przeprowadzany przez audytora wiodącego ISO27001 stwierdzi nieprawidłowości lub braki wynikające z winy Wykonawcy, wykonawca uaktualnienia SZBI zobowiązany będzie dostosować dokumentację do zaleceń poaudytowych.

Ad.2

**Szkolenie dla pracowników i kierownictwa z SZBI oraz podstaw ISO 27001**

Przeprowadzenie szkoleń dla pracowników i kierownictwa z SZBI oraz podstaw ISO 27001 – szkolenie stacjonarne dla 60 osób, w podziałach na min. 2 grupy, rozłożone na 2 dni robocze (jedna grupa = jeden dzień szkolenia), czas trwania co najmniej 5 godzin/każda grupa.

Miejsce szkolenia świetlica Urzędu Gminy Zamość (Zamość, ul. Peowiaków 92). Szkolenie zorganizowane w godz. 8.00 – 15.00, od poniedziałku do piątku.

Program szkolenia przygotowuje Wykonawca, program ma być dostosowany do tematyki szkolenia oraz przygotowany pod kątem uczestników szkolenia tj. pracownicy Urzędu Gminy Zamość. Program szkolenia musi uzyskać akceptację Zamawiającego.

Szkolenie zakończone uzyskaniem zaświadczenia o udziale w szkoleniu dla każdego pracownika/kierownika uczestniczącego w szkoleniu.

Ad.3

**Audyt KRI, ksc i testy podatności w 2024 r. w UG Zamość**

Audyt musi być dostosowany do wymagań rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, zgodny z wymogami ustawy KSC.

Audyt musi być przeprowadzony przez osobę posiadającą certyfikat uprawniający do przeprowadzenia audytu, o którym mowa w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu.

Minimalny zakres zadania:

Analiza wstępna stanu bezpieczeństwa informacji w UG Zamość w zakresie objętym audytem

Identyfikacja obowiązujących wymagań, ocena istniejących systemów i procedur

Zebranie wstępnych odpowiedzi i dowodów audytowych

rekomendacje dotyczące działań naprawczych i usprawnień

raport z audytu

wsparcie w dostosowaniu dokumentacji i procedur obowiązujących w UG Zamość

Przeprowadzenie testów podatności w UG Zamość

Wykonanie audytu zgodnie z wymaganiami art. 21 - 23 ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC) i § 19 rozporządzenia w sprawie Krajowych Ram Interoperacyjności (KRI)

Ocena zgodności z Krajowymi Ramami Interoperacyjności (KRI) / Krajowym Systemie Cyberbezpieczeństwa (KSC)

Opracowanie raportu z audytu wskazującego wykryte podatności oraz błędy wraz rekomendacjami działań naprawczych i korygujących umożliwiających minimalizację zidentyfikowanych ryzyk

Wsparcie poaudytowe, które polegać ma m.in. na udzielaniu informacji na temat udytowanych elementów wynikających z raportu, wsparcie w dostosowaniu dokumentacji i procedur obowiązujących w UG Zamość .

Audyt musi być wykonany przez osoby uprawnione przepisami prawa.

Ad.4

**Przegląd SZBI w 2025 r. dla UG Zamość**

Aktualizacja przygotowanej w 2024 r. dokumentacji SZBI, dostosowanie dokumentów do aktualnych wymagań.

Przegląd SZBI musi obejmować co najmniej:

- Sprawdzenie aktualności SZBI pod względem prawnym

- Sprawdzenie funkcjonalności SZBI - dostosowania do UG Zamość

- Ocena obecnego stanu Systemu Zarządzania Bezpieczeństwem Informacji w UG Zamość

- Analiza zgodności z wymaganiami ISO 27001 i ISO 27002.

- Identyfikacja luk i potencjalnych zagrożeń

- Raport z wykonanych prac zawierający niezgodności oraz rekomendacje.

Ad.5

**Końcowy audyt zgodności przeprowadzany przez uprawnionego audytora wiodącego ISO27001 w UG Zamość**

Wykonawca zobowiązany jest do opracowania audytu końcowego, który jest warunkiem prawidłowego rozliczenia projektu pn. „Cyberbezpieczna Gmina Zamość”.

Wykonawca jest zobowiązany do przeprowadzenia audytu wdrożonego systemu zarządzania bezpieczeństwem informacji w związku z obowiązkiem ciążącym na kierownictwie podmiotu publicznego zgodnie z zapisami w § 20 ust. 2 pkt 14 rozporządzenia w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U.2017 poz. 2247), zwanego dalej „rozporządzeniem KRI”, zgodnie z poniższymi warunkami:

1) zakres audytu systemu bezpieczeństwa informacji wdrożonego w urzędzie JST obejmie zgodność z kryteriami zawartymi w § 20 ust. 2 ww. rozporządzenia KRI lub zgodność z wymaganiami normy PN-ISO/IEC 27001

2) raport z audytu zostanie podpisany przez audytora dokonującego audyt systemu bezpieczeństwa informacji wdrożonego w urzędzie JST i dostarczony do Zamawiającego

3) audyt systemu bezpieczeństwa informacji wdrożonego w Urzędzie Gminy Zamość zostanie przeprowadzony przez:

a) audytora zewnętrznego posiadającego przynajmniej jeden z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U.2018 poz. 1999)

lub

b) audytora wewnętrznego posiadającego przynajmniej jeden z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U.2018 poz. 1999) lub będącego audytorem zewnętrznym systemu zarządzania bezpieczeństwem informacji według normy PN-ISO/IEC 27001;

Przeprowadzenie audytu zgodności musi obejmować co najmniej:

Analiza końcowa stanu bezpieczeństwa informacji w urzędzie w zakresie objętym audytem

Identyfikacja obowiązujących wymagań, ocena istniejących systemów i

procedur

Zebranie końcowych odpowiedzi i dowodów audytowych

Wspólne zdefiniowanie rekomendowanych działań korygujących w zakresie objętym audytem, rekomendacje dotyczące działań naprawczych i usprawnień

Raport z audytu

Wsparcie w dostosowaniu dokumentacji i procedur obowiązujących w UG Zamość

Wykonanie audytu zgodnie z wymaganiami art. 21 - 23 ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC) i § 19 rozporządzenia w sprawie Krajowych Ram Interoperacyjności (KRI)

Ocena zgodności z Krajowymi Ramami Interoperacyjności (KRI) / Krajowym Systemie Cyberbezpieczeństwa (KSC)

Opracowanie raportu z audytu wskazującego wykryte podatności oraz błędy wraz rekomendacjami działań naprawczych i korygujących

Wsparcie poaudytowe, które polegać ma m.in. na: udzielanie informacji na temat audytowanych elementów wynikających z raportu.

Audyt musi być wykonany przez osoby uprawnione przepisami prawa.

W ramach zamówienia Wykonawca zobowiązany jest do opracowana „Ankiety dojrzałości Cyberbezpieczeństwa” na podstawie opracowanej ankiety przed realizacją projektu.

Ankieta jest załącznikiem nr 6 Ankieta Dojrzałości Cyberbezpieczeństwa w Jednostce Samorządu Terytorialnego (i Jednostkach Podległych) do regulaminu konkursu grantowego pn. „Cyberbezpieczny Samorząd”, Priorytet II: Zaawansowane usługi cyfrowe, działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa, Fundusze Europejskie na Rozwój Cyfrowy 2021 – 2027 (FERC).

Ad.6

**Opracowanie pełnej dokumentacji tworzącej SZBI i niezbędnych procedur zgodnie z wymaganiami KRI/ISO27001 dla GOPS Zamość, wdrożenie SZBI w GOPS Zamość**

1) Opracowanie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) spełniającego wymagania norm rodziny ISO 27000 w zakresie bezpieczeństwa informacji (w szczególności zgodnego z wymaganiami aktualnych norm PN-EN ISO/IEC 27001 oraz zaleceniami aktualnych norm PN-ISO/IEC 27002, PN-ISO-27005), ISO 22301 i ISO 31000 w zakresie zarządzania ryzykiem, ustawę o Krajowym Systemie Cyberbezpieczeństwa, dyrektywę NIS2 i Rozporządzenie Parlamentu Europejskiego RODO, ustawę o informatyzacji podmiotów realizujących zadania publiczne oraz przepisów wykonawczych. Dokumentacja musi zawierać wszystkie niezbędne polityki i procedury, dokumenty niezbędne do zarządzania bezpieczeństwem informacji, instrukcje, metodologie zarządzania ryzykiem itd.

Wykonawca zobowiązany jest wytworzyć spójne, jednolite, adekwatne do faktycznych ryzyk, procesów i potrzeb GOPS dokumentacje SZBI zgodne z wymaganiami powołanych wyżej norm.
Celem wdrożenia jest zapewnienie wysokiego poziomu bezpieczeństwa informacji w GOPS i spełnienie wymagań obowiązujących przepisów prawa.

2) Wdrożenie opracowanego Systemu Zarządzania Bezpieczeństwem Informacji

3) Wykonawca zobowiązany jest do udziału w końcowym audycie zgodności przeprowadzonym przez uprawnionego audytora wiodącego ISO27001 w GOPS Zamość, który zostanie zlecony przez Zamawiającego w 2025 r.

Zadaniem Wykonawcy będzie udzielanie wyjaśnień i konsultacji dotyczących wdrożonego SZBI oraz wprowadzenie ewentualnych zmian lub poprawek w dokumentacji SZBI w przypadku wykazania takiej konieczności.

Ad.7

**Szkolenie dla pracowników i kierownictwa z SZBI oraz podstaw ISO 27001**

Przeprowadzenie szkoleń dla pracowników i kierownictwa z SZBI oraz podstaw ISO 27001 – szkolenie stacjonarne dla 27 osób, w podziałach na 2 grupy, rozłożone na 2 dni robocze (jedna grupa = jeden dzień szkolenia), zorganizowane w godz.: 8:00-15:00 od poniedziałku do piątku, czas trwania co najmniej 5 godzin/każda grupa.

Program szkolenia przygotowuje Wykonawca, program ma być dostosowany do tematyki szkolenia oraz przygotowany pod kątem uczestników szkolenia tj. pracownicy GOPS Zamość. Miejsce szkolenia świetlica Gminnego Ośrodka Pomocy Społecznej w Zamościu (Zamość, ul. Szczebrzeska 120).

Szkolenie zakończone uzyskaniem zaświadczenia o przeprowadzonym szkoleniu dla każdego pracownika/kierownika uczestniczącego w szkoleniu.

Ad.8

**Audyt KRI, ksc i testy podatności w 2024 r. w GOPS Zamość**

Przeprowadzenie audytu KRI, ksc i testów podatności w GOPS Zamość zgodnie z wymaganiami i przepisami

Audyt musi być dostosowany do wymagań rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, zgodny z wymogami ustawy KSC.

Audyt musi być przeprowadzony przez osobę posiadającą certyfikat uprawniający do przeprowadzenia audytu, o którym mowa w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu.

Minimalny zakres zadania:

Analiza wstępna stanu bezpieczeństwa informacji w UG Zamość w zakresie objętym audytem

Identyfikacja obowiązujących wymagań, ocena istniejących systemów i procedur

Zebranie wstępnych odpowiedzi i dowodów audytowych

rekomendacje dotyczące działań naprawczych i usprawnień

raport z audytu

wsparcie w dostosowaniu dokumentacji i procedur obowiązujących w UG Zamość

Przeprowadzenie testów podatności w UG Zamość

Wykonanie audytu zgodnie z wymaganiami art. 21 - 23 ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC) i § 19 rozporządzenia w sprawie Krajowych Ram Interoperacyjności (KRI)

Ocena zgodności z Krajowymi Ramami Interoperacyjności (KRI) / Krajowym Systemie Cyberbezpieczeństwa (KSC)

Opracowanie raportu z audytu wskazującego wykryte podatności oraz błędy wraz rekomendacjami działań naprawczych i korygujących umożliwiających minimalizację zidentyfikowanych ryzyk

Wsparcie poaudytowe, które polegać ma m.in. na udzielaniu informacji na temat udytowanych elementów wynikających z raportu, wsparcie w dostosowaniu dokumentacji i procedur obowiązujących w GOPS Zamość .

Audyt musi być wykonany przez osoby uprawnione przepisami prawa.

Ad.9

**Przegląd SZBI w 2025 r. dla GOPS Zamość**

Aktualizacja przygotowanej w 2024 r. dokumentacji SZBI, dostosowanie dokumentów do aktualnych wymagań.

Przegląd SZBI musi obejmować co najmniej:

- Sprawdzenie aktualności SZBI pod względem prawnym

- Sprawdzenie funkcjonalności SZBI - dostosowania do GOPS

- Ocena obecnego stanu Systemu Zarządzania Bezpieczeństwem Informacji w GOPS

- Analiza zgodności z wymaganiami ISO 27001 i ISO 27002.

- Identyfikacja luk i potencjalnych zagrożeń

- Raport z wykonanych prac zawierający niezgodności oraz rekomendacje.

Ad.10

**Końcowy audyt zgodności przeprowadzony przez uprawnionego audytora wiodącego ISO27001 w GOPS Zamość**

Wykonawca zobowiązany jest do opracowania audytu końcowego, który jest warunkiem prawidłowego rozliczenia projektu pn. „Cyberbezpieczna Gmina Zamość”.

Wykonawca jest zobowiązany do przeprowadzenia audytu wdrożonego systemu zarządzania bezpieczeństwem informacji w związku z obowiązkiem ciążącym na kierownictwie podmiotu publicznego zgodnie z zapisami w § 20 ust. 2 pkt 14 rozporządzenia w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U.2017 poz. 2247), zwanego dalej „rozporządzeniem KRI”, zgodnie z poniższymi warunkami:

1) zakres audytu systemu bezpieczeństwa informacji wdrożonego w GOPS Zamość obejmie zgodność z kryteriami zawartymi w § 20 ust. 2 ww. rozporządzenia KRI lub zgodność z wymaganiami normy PN-ISO/IEC 27001

2) raport z audytu zostanie podpisany przez audytora dokonującego audyt systemu bezpieczeństwa informacji wdrożonego w GOPS Zamość i dostarczony do Zamawiającego

3) audyt systemu bezpieczeństwa informacji wdrożonego w GOPS Zamość zostanie przeprowadzony przez:

a) audytora zewnętrznego posiadającego przynajmniej jeden z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U.2018 poz. 1999)

lub

b) audytora wewnętrznego posiadającego przynajmniej jeden z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U.2018 poz. 1999) lub będącego audytorem zewnętrznym systemu zarządzania bezpieczeństwem informacji według normy PN-ISO/IEC 27001;

Przeprowadzenie audytu zgodności musi obejmować co najmniej:

Analiza końcowa stanu bezpieczeństwa informacji w urzędzie w zakresie objętym audytem

Identyfikacja obowiązujących wymagań, ocena istniejących systemów i

procedur

Zebranie końcowych odpowiedzi i dowodów audytowych

Wspólne zdefiniowanie rekomendowanych działań korygujących w zakresie objętym audytem, rekomendacje dotyczące działań naprawczych i usprawnień

Raport z audytu

Wsparcie w dostosowaniu dokumentacji i procedur obowiązujących w GOPS Zamość

Wykonanie audytu zgodnie z wymaganiami art. 21 - 23 ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC) i § 19 rozporządzenia w sprawie Krajowych Ram Interoperacyjności (KRI)

Ocena zgodności z Krajowymi Ramami Interoperacyjności (KRI) / Krajowym Systemie Cyberbezpieczeństwa (KSC)

Opracowanie raportu z audytu wskazującego wykryte podatności oraz błędy wraz rekomendacjami działań naprawczych i korygujących

Wsparcie poaudytowe, które polegać ma m.in. na: udzielanie informacji na temat audytowanych elementów wynikających z raportu.

W ramach zamówienia Wykonawca zobowiązany jest do opracowana „Ankiety dojrzałości Cyberbezpieczeństwa” na podstawie opracowanej ankiety przed realizacją projektu.

Ankieta jest załącznikiem nr 6 Ankieta Dojrzałości Cyberbezpieczeństwa w Jednostce Samorządu Terytorialnego (i Jednostkach Podległych) do regulaminu konkursu grantowego pn. „Cyberbezpieczny Samorząd”, Priorytet II: Zaawansowane usługi cyfrowe, działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa, Fundusze Europejskie na Rozwój Cyfrowy 2021 – 2027 (FERC).

Wykonanie dokumentacji oraz przeprowadzenie audytów w ramach niniejszego zamówienia musi odbyć się po przeprowadzeniu wizji lokalnej przez Wykonawcę w UG Zamość i GOPS Zamość oraz po szczegółowym zapoznaniu się z posiadanymi dokumentami/warunkami/systemami itp. stacjonarnie w UG Zamość i GOPS Zamość – co najmniej 2 wizyty.

Wszelkie opracowane dokumenty, raporty Wykonawca przekaże w wersji papierowej w ilości 2 szt. oraz wersji elektronicznej na płycie CD.

Wykonawca musi posiadać niezbędną wiedzę fachową, kwalifikacje, możliwości i uprawnienia konieczne do prawidłowego wykonania zamówienia. Dokumentacja, audyty, szkolenia muszą być opracowane i przeprowadzone przez wykwalifikowane osoby.