

Załącznik nr 1 do zapytania ofertowego

Opis przedmiotu zamówienia

I. Audyty KRI, RODO oraz SZCD w trybie zdalnym.

Audyt SZBI & KRI & UoKSC dla urzędu

1. Wstępny audyt SZBI & KRI & UoKSC

a) Realizacja wymienionych w regulaminie konkursu grantowego audytów SZBI oraz KRI/UoKSC w oparciu o:

-Rozporządzenie Krajowych Ram Interoperacyjności (w tym rozbudowane testy podatności infrastruktury IT jednostki),

-Ustawy o Krajowym Systemie Cyberbezpieczeństwa,

-metodologii Systemów Zarządzania Bezpieczeństwem Informacji określonych w:

▪ normie ISO 27001 (SZBI),

▪ normie ISO 22301 (SZCD),

▪ wytycznych Ministerstwa Cyfryzacji dla kontroli działania systemów teleinformatycznych używanych do realizacji zadań publicznych,

▪ oraz wielu innych standardów związanych z bezpieczeństwem informacji (w tym RFC),

b) W ramach przedmiotowego audytu wstępnego aktualizacja posiadanej przez jednostkę dokumentacji SZBI o wszelkie procedury z zakresu:

-bezpieczeństwa informacji (rozbudowany System Zarządzania Bezpieczeństwem Informacji (SZBI) z niedawno wprowadzonymi przez nas zmianami w zakresie polityk, w tym m.in.:

- Polityki Bezpieczeństwa Informacji,

-Polityki Bezpieczeństwa Teleinformatycznego,

-szacowania ryzyka bezpieczeństwa informacji (Analiza ryzyka ogólnego oraz Ocena skutków dla przetwarzania danych (DPIA)),

-szacowanie ryzyka bezpieczeństwa informacji pracy zdalnej,

-ciągłości działania (rozbudowany SZCD - System Zarządzania Ciągłością Działania wg ISO 22301).

2. Końcowy audyt SZBI & KRI & UoKSC

a) Ponowny pełny zakres audytowy, który został wskazany we wstępnym audycie SZBI & KRI/UoKSC) zgodnie z zapisem & 3 ust. 3 pkt 5 Regulaminu Konkursu Grantowego „Cyberbezpieczny Samorząd”.

b) Szacowanie ryzyka (Analiza ryzyka ogólnego oraz ocena skutków (DPIA)).

Audyt SZBI & KRI & UoKSC dla jednostek podległych: Miejsko-Gminny Ośrodek Pomocy Społecznej (MGOPS), Gminny Zakład Komunalny (GZK), Zespół Administracyjnej Obsługi Oświaty (ZAOO)

1. Wstępny audyt SZBI & KRI & UoKSC

a) Realizacja wymienionych w regulaminie konkursu grantowego audytów SZBI oraz KRI/UoKSC w oparciu o:

-Rozporządzenie Krajowych Ram Interoperacyjności (w tym rozbudowane testy podatności infrastruktury IT jednostki),

-Ustawy o Krajowym Systemie Cyberbezpieczeństwa,

-metodologii Systemów Zarządzania Bezpieczeństwem Informacji określonych w:

▪ normie ISO 27001 (SZBI),

▪ normie ISO 22301 (SZCD),

▪ wytycznych Ministerstwa Cyfryzacji dla kontroli działania systemów teleinformatycznych używanych do realizacji zadań publicznych,

▪ oraz wielu innych standardów związanych z bezpieczeństwem informacji (w tym RFC),

b) W ramach przedmiotowego audytu wstępnego aktualizacja posiadanej przez jednostkę dokumentacji SZBI o wszelkie procedury z zakresu:



Fundusze Europejskie
na Rozwój Cyfrowy



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



CENTRUM
PROJEKTÓW
POLSKA
CYFROWA

-bezpieczeństwa informacji (rozbudowany System Zarządzania Bezpieczeństwem Informacji (SZBI) z niedawno wprowadzonymi przez nas zmianami w zakresie polityk, w tym m.in.:

-Polityki Bezpieczeństwa Informacji,

-Polityki Bezpieczeństwa Teleinformatycznego,

-szacowania ryzyka bezpieczeństwa informacji (Analiza ryzyka ogólnego oraz Ocena skutków dla przetwarzania danych (DPIA)),

-szacowanie ryzyka bezpieczeństwa informacji pracy zdalnej.

2. Końcowy audyt SZBI & KRI & UoKSC

a) Ponowny pełny zakres audytowy, który został wskazany we wstępnym audycie SZBI & KRI/UoKSC) zgodnie z zapisem & 3 ust. 3 pkt 5 Regulaminu Konkursu Grantowego „Cyberbezpieczny Samorząd”.

b) Szacowanie ryzyka (Analiza ryzyka ogólnego oraz ocena skutków (DPIA)).

Audyt musi być przeprowadzony przez co najmniej 2 osoby posiadające certyfikat uprawniający do przeprowadzenia audytu o którym mowa w Rozporządzeniu Ministra Cyfryzacji z 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu.

Audyt wstępny dla urzędu i jednostek powinien zostać przeprowadzony w połowie roku 2024 natomiast audyt końcowy pod koniec roku 2025 lub w pierwszej połowie 2026 wg terminów określonych w zapytaniu.

Zlecenie obejmuje przygotowanie i przesłanie raportu poaudytowego wstępnego i końcowego w terminie 14 dni licząc od dnia zakończenia czynności audytu.

Płatność za wykonaną usługę zrealizowaną będzie w dwóch transzach: pierwsza po przesłaniu raportu poaudytowego wstępnego, druga po przesłaniu raportu poaudytowego końcowego z 14 dniowym terminem płatności.

Przeprowadzenie audytu powinno odbyć się w godzinach pracy Urzędu Gminy i Miasta w Sianowie w siedzibie organizacji oraz jednostkach uczestniczących w audycie. Proces wykonywania zewnętrznych testów podatności może rozpocząć się od dnia nawiązania umowy, a zakończyć się w ciągu 14 dni licząc od ostatniego dnia audytu przeprowadzanego w siedzibie organizacji w formie zdalnej.