Nr sprawy: O-ZP.253.58.2026 Olsztyn, dnia 17.04.2026 r.

Do wszystkich wykonawców uczestniczących w postępowaniu

Dotyczy: postępowania o udzielenie zamówienia publicznego, którego przedmiotem zamówienia jest **Usługa przeprowadzenia audytu systemu zarządzania bezpieczeństwem informacji, nr sprawy: O-ZP.253.58.2026.**

Zamawiający, przekazuje treść zapytania wraz z wyjaśnieniami dotyczącymi OPZ:

Pytanie 1

Kiedy przewidywane jest podpisanie umowy z wybranym wykonawcą? (orientacyjna data)

Odpowiedź:

Podpisanie umowy z wybranym Wykonawcą nastąpi niezwłocznie po otrzymaniu od wybranego wykonawcy danych do umowy, uzyskaniu akceptacji prawnej oraz kontrasygnaty Głównej Księgowej.

Pytanie 2

W jakich terminach w maju 2026 możliwe jest przeprowadzenie prac audytowych on-site (wywiady, wizja lokalna, przegląd dokumentacji)?

Odpowiedź:

Przeprowadzenie prac audytowych on-site (wywiady, wizja lokalna, przegląd dokumentacji) możliwe jest po podpisaniu umowy, w dowolnych terminach (wyłączając weekendy).

Pytanie 3

Czy w maju 2026 planowane są nieobecności / urlopy kluczowego personelu IT lub osoby odpowiedzialnej za bezpieczeństwo informacji?

Odpowiedź:

W maju 2026 r., nie są planowane nieobecności / urlopy kluczowego personelu IT lub osoby odpowiedzialnej za bezpieczeństwo informacji.

Pytanie 4

Ile dni roboczych szacuje Zamawiający na przeprowadzenie prac audytowych on-site w siedzibie Urzędu?

Odpowiedź:

Zamawiający oczekuje odpowiedzi od audytora.

Pytanie 5

Czy Zamawiający wyznaczy koordynatora projektu (single point of contact) po swojej stronie na czas trwania audytu?

Odpowiedź:

Zamawiający na czas trwania audytu wyznaczy osobę do kontaktu.

Pytanie 6

Kto po stronie Zamawiającego będzie merytorycznie oceniał Raport z Audytu?

Odpowiedź:

Raport z przeprowadzonego audytu ocenią osoby wyznaczone przez Zamawiającego.

Pytanie 7

Czy audytor będzie miał dostęp read-only do systemów IT (logi, konfiguracje, konsole zarządzania), czy wyłącznie dostęp do dokumentacji i wywiadów?

Odpowiedź:

Audytor otrzyma dostęp do audytowanych systemów w trybie nadzorowanym podczas sesji z administratorem IT.

Pytanie 8

Czy Zamawiający jest w stanie udostępnić dokumentację SZBI z wyprzedzeniem — co najmniej 7 dni przed planowaną wizytą on-site?

Odpowiedź:

Zamawiający udostępni posiadaną dokumentację Wykonawcy po podpisaniu umowy wraz z umową o zachowaniu poufności.

Pytanie 9

Czy Zamawiający przewiduje możliwość przekazania wersji roboczej raportu (draft) do wstępnej akceptacji przed złożeniem dokumentu finalnego?

Odpowiedź:

Zamawiający przewiduje możliwość przekazania wersji roboczej raportu (draft) do wstępnej akceptacji przed złożeniem dokumentu finalnego.

Pytanie 10

W jakim terminie Zamawiający zobowiązuje się do przekazania uwag po dostarczeniu raportu / wersji roboczej?

Odpowiedź:

Zamawiający zobowiązuje się do przekazania uwag po dostarczeniu raportu / wersji roboczej w terminie do 3 dni roboczych.

Pytanie 11

Jakie są kryteria akceptacji Raportu z Audytu ('bez uwag')? Czy istnieje formalny checklist odbiorowy lub wytyczne dotyczące wymaganej zawartości?

Odpowiedź:

Kryteria akceptacji raportu wynikają z założeń projektu Cyberbezpieczny Samorząd.

Pytanie 12

Ile departamentów / komórek organizacyjnych Urzędu Marszałkowskiego Województwa Warmińsko-Mazurskiego wchodzi w zakres audytu?

Odpowiedź:

Zakres przedmiotowego audytu obejmuje 35 departamentów / komórek organizacyjnych Urzędu Marszałkowskiego Województwa Warmińsko-Mazurskiego

Pytanie 13

Czy audyt obejmuje wyłącznie siedzibę główną, czy również inne lokalizacje lub jednostki podległe WM? Jeśli tak — proszę wymienić.

Odpowiedź:

Miejsce i zakres audytu został określony w Opisie przedmiotu zamówienia, stanowiącym Załącznik 1.

Pytanie 14

Jaka jest orientacyjna liczba pracowników Urzędu objętych audytem?

Odpowiedź:

Liczba pracowników Urzędu Marszałkowskiego Województwa Warmińsko-Mazurskiego objętych audytem wynosi 1080.

Pytanie 15

Kto jest właścicielem i operatorem infrastruktury IT: Urząd Marszałkowski czy WM CNT? Jak wygląda podział odpowiedzialności?

Odpowiedź:

Właścicielem infrastruktury IT będącej przedmiotem audytu jest Województwo Warmińsko-Mazurskie, natomiast WMCNT jest operatorem.

Pytanie 16

Ile systemów teleinformatycznych podlega audytowi w zakresie §19 ust. 2 Rozporządzenia KRI (Dz.U. 2024 poz. 773)? Prosimy o orientacyjną listę lub liczbę.

Odpowiedź:

w zakresie §19 ust. 2 Rozporządzenia KRI (Dz.U. 2024 poz. 773) audytowi podlega do 48 systemów teleinformatycznych.

Pytanie 17

Czy istnieje aktualna inwentaryzacja zasobów IT / rejestr aktywów informacyjnych, który zostanie udostępniony audytorowi przed rozpoczęciem prac?

Odpowiedź:

Istnieje aktualna inwentaryzacja zasobów IT / rejestr aktywów informacyjnych, który zostanie udostępniony audytorowi przed rozpoczęciem prac jednakże po podpisaniu umowy wraz z umową o zachowaniu poufności.

Pytanie 18

Czy systemy teleinformatyczne są hostowane lokalnie (on-premise), w chmurze czy w modelu hybrydowym?

Odpowiedź:

Systemy teleinformatyczne są hostowane lokalnie oraz w chmurze.

Pytanie 19

Które systemy należy uznać za krytyczne z perspektywy działalności Urzędu (np. EZD, systemy finansowe, obsługa funduszy europejskich, GIS)?

Odpowiedź:

Pełna informacja zostanie przekazana Wykonawcy po podpisaniu umowy wraz z umową o zachowaniu poufności.

Pytanie 20

Czy przeprowadzono wcześniej audyt SZBI/KRI w Urzędzie? Jeśli tak — kiedy i czy raport jest dostępny?

Odpowiedź:

TAK, przeprowadzono wcześniej audyt SZBI/KRI w Urzędzie, natomiast pełna dokumentacja zostanie przekazana Wykonawcy po podpisaniu umowy wraz z umową o zachowaniu poufności.

Pytanie 21

Czy Urząd posiada formalną dokumentację SZBI: Politykę Bezpieczeństwa Informacji, Statement of Applicability (SoA) oraz analizę ryzyka ICT?

Odpowiedź:
Brak SZBI w rozumieniu ISO 27001.

Pytanie 22
Jaka metodyka zarządzania ryzykiem ICT jest stosowana w Urzędzie (np. ISO 27005, OCTAVE, własna)?

Odpowiedź:

Stosowana jest własna metodyka zarządzania ryzykiem ICT.

Pytanie 23

Czy istnieje formalny rejestr incydentów bezpieczeństwa? Ile incydentów odnotowano w ciągu ostatnich 12 miesięcy?

Odpowiedź:
Istnieje rejestr incydentów bezpieczeństwa, natomiast pełna dokumentacja zostanie przekazana Wykonawcy po podpisaniu umowy wraz z umową o zachowaniu poufności.

Zamawiający przesuwa termin składania ofert na dzień **21.04.2026 r. do godziny 12:00**, wyłącznie na adres mailowy: **zakupy@wmcnt.pl**

W tytule wiadomości proszę o wpisanie numeru sprawy: **O-ZP.253.58.2026**.