Pytania i odpowiedzi do postępowania w sprawie zamówienia o wartości równej lub wyższej 15.000,00 zł netto, ale mniejszej niż 50.000,00 zł netto pod nazwą:

1.a. Usługa opracowania dokumentacji oraz wdrożenie normy **PN-EN ISO/IEC 27001:2023-08** Systemu Zarządzania Bezpieczeństwem Informacji dla Zamawiającego, zgodnie z warunkami określonymi w § 19 Rozporządzenia KRI oraz § 3 ust. 2 pkt. 1 Regulaminu Konkursu Grantowego „Cyberbezpieczny Samorząd".

1.b. Przeprowadzenie szkolenia dla zespołu wdrożeniowego SZBI Zamawiającego,

1.c. Wsparcie merytoryczne zespołu wdrożeniowego SZBI Zamawiającego;

2. usługa opracowania szacowania ryzyka zgodnie z § 19 Rozporządzenia KRI oraz § 3 ust. 2 pkt. 1 Regulaminu Konkursu Grantowego „Cyberbezpieczny Samorząd".

1. **Czy planowane jest zmniejszenie liczby wymaganych referencji, zwłaszcza w zakresie różnych kategorii usług (szkolenia, audyty, szacowanie ryzyka, dokumentacja ISMS)?**
    - Aktualne wymagania są bardzo szerokie i mogą znacząco ograniczyć konkurencję, eliminując nawet doświadczone podmioty z rynku. Czy przewidują Państwo możliwość zmniejszenia liczby wymaganych referencji lub ich zakresu?

Utrzymanie obecnych wymagań referencyjnych wynika z konieczności weryfikacji kompetencji i jakości usług, minimalizacji ryzyka oraz zapewnienia uczciwej i przejrzystej oceny ofert. Referencje stanowią dowód na praktyczne doświadczenie wykonawców w obszarach takich jak szkolenia, audyty, szacowanie ryzyka i dokumentacja ISMS, co gwarantuje wysoką jakość realizowanych usług. Obniżenie kryteriów mogłoby dopuścić do postępowania podmioty bez wystarczających kompetencji, zwiększając ryzyko błędów i nieprawidłowości. Obecne wymagania zostały opracowane na podstawie wieloletnich doświadczeń i pozwalają na rzetelną selekcję wykonawców i zabezpieczenie interesów zamawiającego. Dlatego też nie przewiduje się zmniejszenia liczby wymaganych referencji ani ich zakresu, ponieważ służą one utrzymaniu wysokiego standardu usług.

Zamawiający nie przewiduje zmniejszenia liczby wymaganych referencji.

2. **Jaki jest cel referencji dotyczących szacowania ryzyka zgodnie z ISO 27005?**
    - Norma ISO 27005 zawiera ogólne wytyczne i najlepsze praktyki w zakresie zarządzania ryzykiem bezpieczeństwa informacji, ale nie określa obowiązkowego standardu wdrożenia. Czy referencje w tym zakresie dotyczą konkretnych wdrożeń systemu zarządzania ryzykiem, czy wystarczy potwierdzenie realizacji analiz ryzyka?

Celem referencji dotyczących szacowania ryzyka zgodnie z ISO 27005, wymienioną w *Rozporządzeniu w sprawie Krajowych Ram Interoperacyjności* (KRI) jako podstawa zarządzania ryzykiem, jest potwierdzenie realnego doświadczenia wykonawcy w

identyfikacji, analizie i ocenie ryzyka na bazie uznanych standardów i najlepszych praktyk. KRI wskazuje ISO 27005 jako podstawę spełnienia wymagań dotyczących zarządzania ryzykiem w ramach systemu zarządzania bezpieczeństwem informacji, dlatego zamawiający wymaga od potencjalnych wykonawców wykazania wykonania usług na podstawie tej normy.

3. **Czy referencje muszą pochodzić wyłącznie od podmiotów publicznych, czy możliwe jest uwzględnienie doświadczenia w sektorze prywatnym?**
    - Wiele firm posiada bogate doświadczenie we współpracy z sektorem prywatnym w zakresie cyberbezpieczeństwa i może przedstawić referencje na podobne usługi. Czy zostaną one uznane za wystarczające?

Wymóg, by referencje pochodziły wyłącznie podmiotów publicznych, wynika z konieczności potwierdzenia doświadczenia w realizacji usług w środowisku objętym regulacjami prawnymi i procedurami właściwymi dla sektora publicznego. Właśnie z tego powodu doświadczenie zdobyte wyłącznie w sektorze prywatnym może nie odzwierciedlać w pełni kompetencji niezbędnych do realizacji projektów w warunkach administracji publicznej. Konieczność przedstawienia referencji od podmiotów publicznych zapewnia więc, że wykonawca posiada praktyczne umiejętności w spełnianiu specyficznych wymogów prawnych i organizacyjnych charakterystycznych dla sektora publicznego.

4. **Czy wymagania dotyczące wartości referencji (15 000 zł netto) odnoszą się do pojedynczego projektu, czy możliwe jest wykazanie sumarycznej wartości kilku mniejszych realizacji?**
    - Czy w przypadku wieloletniej współpracy z jednym podmiotem można przedstawić łączną wartość realizowanych usług?

Wymóg wykazania wartości 15 000 zł netto odnosi się do pojedynczego projektu i nie dopuszcza sumowania kilku mniejszych realizacji ani łączenia wieloletniej współpracy w jedną referencję. Określenie minimalnej wartości jednego przedsięwzięcia ma na celu zweryfikowanie, czy wykonawca potrafi skutecznie zrealizować zadanie o określonym rozmiarze i złożoności, co stanowi ważny wskaźnik jego zdolności organizacyjnych, finansowych oraz kompetencyjnych. Gromadzenie kilku mniejszych usług w jedną całość utrudniałoby rzetelną ocenę skali poszczególnych prac oraz odpowiedzialności wykonawcy, dlatego właśnie przyjęto jednolity próg wartości dla pojedynczego zamówienia.

5. **Czy w przypadku projektów realizowanych przez konsorcjum możliwe jest wykazanie referencji dla poszczególnych członków konsorcjum, czy tylko dla lidera?**
    - Wiele firm realizuje złożone projekty we współpracy z innymi podmiotami – czy można wykazać referencje na podstawie udziału w takich przedsięwzięciach?

W przypadku realizacji projektów w formie konsorcjum, każda ze stron musi dysponować referencjami wydanymi bezpośrednio na jej rzecz, jeśli zamierza się nimi posłużyć w postępowaniu. Oznacza to, że nie wystarczy samo uczestnictwo w projekcie pod auspicjami lidera – referencje powinny wyraźnie wskazywać podmiot, który faktycznie realizował określone zadania i wobec którego zostały wystawione. Taki wymóg zapewnia rzetelną ocenę kompetencji każdego z członków konsorcjum, umożliwiając zamawiającemu dokładne ustalenie, kto posiada doświadczenie w danym obszarze usług.

6. **Czy referencje dotyczące dokumentacji systemu zarządzania bezpieczeństwem informacji (ISMS) powinny obejmować pełny zakres wdrożenia, czy wystarczy realizacja poszczególnych elementów dokumentacji?**
    - Warto zaznaczyć, że większość firm nie rozdziela wdrożenia na szczegółowe etapy, ponieważ standardowy schemat wdrożenia zarówno ISO 27001, jak i ISO 22301 obejmuje **audyt wstępny -> przygotowanie dokumentacji -> testy i szkolenia -> wdrożenie -> audyt zamykający**. W związku z tym, czy konieczne jest wykazywanie osobnych referencji dla poszczególnych etapów, czy możliwe jest przedstawienie referencji dotyczących całościowego wdrożenia?

Wymóg przedstawiania referencji za konkretne usługi jest niezbędny, aby zapewnić rzetelną ocenę faktycznego doświadczenia i kompetencji wykonawcy w danym obszarze. Jeśli referencje dotyczyłyby wyłącznie całościowego wdrożenia, trudno byłoby ustalić, czy dany wykonawca faktycznie odpowiadał za kluczowe prace związane z przygotowaniem i opracowaniem odpowiedniego etapu. Rozbicie zakresu pozwala zamawiającemu zweryfikować, który podmiot rzeczywiście przeprowadził poszczególne etapy i czy dysponuje doświadczeniem przydatnym w kontekście konkretnych zadań.

7. **Czy dopuszczalne jest przedstawienie referencji potwierdzających wykonanie usług na podstawie protokołów odbioru, jeśli zamawiający nie wystawił formalnej referencji?**

Niektóre instytucje publiczne nie wystawiają referencji w standardowej formie – czy akceptowane będą inne dokumenty potwierdzające realizację usług (np.

W ramach dokumentów, o których mowa, dopuszcza się referencje bądź inne dokumenty sporządzone przez podmiot, na rzecz którego dostawy lub usługi zostały wykonane.