Dotyczy: Zapytanie ofertowe: Realizacja szkoleń i opracowanie dokumentacji w ramach projektu grantowego Cyberbezpieczny Samorząd - "Cyberbezpieczna Gmina Somonino"

Uwaga: Zamawiający informuje, że wydłuża termin składania ofert do dnia: 20.08.2025 r.

W związku z pytaniami, które wpłynęły do Zmawiającego w dniu 08.08.2025 r. Zamawiający udziela następujących odpowiedzi:

1. **Zakres testów bezpieczeństwa a wymóg CEH**
   W OPZ wskazano, że w ramach audytu końcowego należy przeprowadzić „przeskanowanie infrastruktury sieciowej" i „identyfikację podatności". Czy Zamawiający potwierdza, że nie chodzi o pełne testy penetracyjne aplikacji i systemów, a jedynie o testy podatności (vulnerability scanning)?
   W przypadku potwierdzenia prosimy o uzasadnienie wymogu posiadania przez pentesterów certyfikatu CEH, który jest typowo wymagany do pełnych testów penetracyjnych, i rozważenie dopuszczenia równoważnych kwalifikacji lub doświadczenia praktycznego.

Odpowiedź:

Zamawiający potwierdza, że w ramach audytu końcowego przewidziano w szczególności przegląd i analizę zabezpieczeń oraz identyfikację podatności infrastruktury, zgodnie z opisem w pkt 1.3.2 OPZ. Nie przewiduje się pełnych testów penetracyjnych aplikacji w rozumieniu badań ingerencyjnych, chyba że analiza bezpieczeństwa wskaże potrzebę ich wykonania dla weryfikacji skuteczności wdrożonych zabezpieczeń. Wymóg posiadania certyfikatu CEH wynika z konieczności zapewnienia, że osoba realizująca zadania w zakresie identyfikacji podatności posiada kwalifikacje potwierdzające znajomość technik ataków i metod testowania bezpieczeństwa. Zamawiający dopuszcza certyfikaty równoważne w zakresie merytorycznym.

2. **Równoważność certyfikatów**
   Czy Zamawiający dopuszcza przedstawienie certyfikatów równoważnych wskazanym w OPZ (CEH, ISO/IEC 27001 Lead Auditor/Lead Implementer, ISO 22301, CISA), potwierdzających równorzędne kompetencje w zakresie bezpieczeństwa informacji, audytów i testów bezpieczeństwa?
   W branży funkcjonuje wiele uznanych certyfikatów o równoważnym zakresie merytorycznym, których wykluczenie może ograniczać konkurencję.

Odpowiedź:

Zamawiający dopuszcza przedstawienie certyfikatów równoważnych do wymienionych w OPZ (m.in. CEH, CISSP, ISO/IEC 27001 Lead Auditor/Lead Implementer, ISO 22301, CISA, CIA), potwierdzających równorzędne kompetencje w zakresie bezpieczeństwa informacji, audytów i testów bezpieczeństwa, wydanych przez uznane jednostki certyfikujące.

Uwaga! Należy wskazać w formularzu ofertowym jakie są to certyfikaty, aby umożliwić ocenę równoważności.

3. **Liczba pentesterów i audytorów**
   OPZ przewiduje, że w zespole musi być co najmniej 2 pentesterów oraz 2 audytorów. Czy Zamawiający rozważy dopuszczenie realizacji zamówienia przez mniejszy zespół, jeżeli

zapewni on wszystkie wymagane kompetencje i terminowość realizacji?
Zwiększyłoby to dostępność wykonawców i obniżyło koszty bez uszczerbku dla jakości.

Odpowiedź:

Zamawiający wymaga wykazania w ofercie osób spełniających minimalne kwalifikacje określone w rozdz. VII zapytania ofertowego. Dopuszcza się, aby jedna osoba posiadała kilka wymaganych certyfikatów (łączenie potencjału kadrowego), co może ograniczyć liczbę członków zespołu, pod warunkiem zapewnienia pełnego zakresu kompetencji i dotrzymania harmonogramu.

4. **Łączenie funkcji**
   Czy Zamawiający dopuszcza, aby ta sama osoba pełniła więcej niż jedną funkcję w projekcie (np. audytor może być jednocześnie koordynatorem lub osobą merytoryczną), o ile posiada wymagane kwalifikacje?
   Takie rozwiązanie jest często stosowane w projektach „Cyberbezpieczny Samorząd" i nie wpływa negatywnie na jakość.

Odpowiedź: Zgodnie z pkt. VII Warunki udziału w postępowaniu

Zamawiający dopuszcza, aby ta sama osoba pełniła więcej niż jedną funkcję w projekcie, o ile spełnia wymagania formalne i merytoryczne dla każdej z przypisanych ról.

5. **Forma zatrudnienia członków zespołu**
   Czy Zamawiający dopuści możliwość zatrudnienia członków zespołu na podstawie umów cywilnoprawnych lub kontraktów B2B, zamiast wyłącznie umów o pracę?
   Wymóg wyłącznego zatrudnienia na umowę o pracę może ograniczać konkurencję i jest nieadekwatny do specyfiki branży IT.

Odpowiedź:

Zamawiający dopuszcza realizację zamówienia przez osoby zatrudnione zarówno na podstawie umowy o pracę, jak i umów cywilnoprawnych lub kontraktów B2B, pod warunkiem spełnienia wymagań dotyczących kwalifikacji. W niniejszym zamówieniu nie przewidziano obowiązku zatrudnienia na umowę o pracę.

6. **Doświadczenie wykonawcy**
   Czy Zamawiający dopuszcza, aby wymagane doświadczenie w realizacji podobnych usług było spełnione łącznie przez wykonawcę i podwykonawców lub członków konsorcjum?
   Ograniczenie doświadczenia wyłącznie do podmiotu składającego ofertę może wyeliminować wyspecjalizowane firmy o wąskiej, ale unikalnej ekspertyzie.

Odpowiedź:

Zamawiający dopuszcza, aby wykonawca w celu potwierdzenia spełnienia warunków udziału w postępowaniu polegał na doświadczeniu innych podmiotów, w tym podwykonawców lub członków konsorcjum. W takim przypadku wykonawca jest zobowiązany przedstawić zobowiązanie tych podmiotów do oddania mu do dyspozycji wymaganych zasobów na okres realizacji zamówienia, wraz z określeniem zakresu ich udziału w jego wykonaniu.

UWAGA! Do oferty należy dołączyć Zobowiązanie innego podmiotu do udostępnienia niezbędnych zasobów Wykonawcy – wzór udostępniono jako załącznik nr 8 do Zapytania.

7. **Możliwość realizacji w konsorcjum**
   Czy Zamawiający przewiduje możliwość składania ofert wspólnych przez konsorcja, w których doświadczenie i kompetencje członków będą sumowane?
   Takie rozwiązanie zwiększa konkurencję i jest powszechnie stosowane w projektach finansowanych ze środków UE.

Odpowiedź:

Zamawiający, dopuszcza możliwość wspólnego ubiegania się o udzielenie zamówienia przez wykonawców (konsorcjum). W przypadku złożenia oferty wspólnej warunki udziału w postępowaniu mogą być spełniane łącznie przez wszystkich członków konsorcjum. Zamawiający nie wymaga, aby każdy członek konsorcjum samodzielnie spełniał wszystkie warunki udziału w postępowaniu, chyba że specyfika zamówienia wymaga posiadania określonych uprawnień lub kwalifikacji przez danego członka w zakresie realizowanej części zamówienia.

8. **Zakres szkoleń**
   W OPZ wskazano obowiązek przeprowadzenia szkoleń, ale brak szczegółowego programu. Czy Zamawiający mógłby określić minimalny zakres tematyczny i liczbę godzin dla poszczególnych grup szkoleniowych?
   Pozwoli to uniknąć różnic w interpretacji i lepiej oszacować koszty.

Odpowiedź:

Szczegółowy zakres szkoleń został określony w rozdz. 2.2–2.5 OPZ. Minimalny czas trwania modułów: Moduł I – 6 godzin/grupa, Moduł II – 6 godzin/grupa, szkolenie kadry kierowniczej – 6 godzin, szkolenia specjalistyczne – zgodnie z programem w OPZ. Zakres tematyczny obejmuje m.in. wprowadzenie do cyberbezpieczeństwa, zasady ochrony informacji, zagrożenia socjotechniczne, wdrożony SZBI, procedury bezpieczeństwa, obsługę wskazanych narzędzi i systemów.

9. **Metodyka analizy ryzyka**
   Czy Zamawiający dopuszcza zastosowanie różnych uznanych metodyk analizy ryzyka (np. ISO 27005, OCTAVE, MEHARI), pozostawiając wykonawcy wybór optymalnej?
   Wskazanie wyłącznie jednej metodyki mogłoby ograniczyć konkurencję.

Odpowiedź:

Zamawiający dopuszcza zastosowanie różnych uznanych metodyk analizy ryzyka (np. ISO 27005, OCTAVE, MEHARI), pozostawiając wykonawcy wybór optymalnej, pod warunkiem zapewnienia zgodności z wymaganiami normy ISO/IEC 27001 oraz przepisami krajowymi.

10. **Realizacja testów zdalnie**
    W OPZ zapisano, że testy mogą być realizowane zdalnie. Czy Zamawiający może potwierdzić, że dopuszcza w pełni zdalną realizację testów, jeśli zapewnione będzie bezpieczeństwo transmisji i poufność danych?
    Pozwoli to zwiększyć dostępność wykonawców spoza regionu.

Odpowiedź:

Zamawiający dopuszcza zdalną realizację testów, pod warunkiem zapewnienia bezpieczeństwa transmisji i poufności danych.

Jednocześnie Zamawiający zastrzega, że w przypadku, gdy ze względów bezpieczeństwa lub ograniczeń technologicznych przeprowadzenie określonych czynności testowych w trybie zdalnym będzie niemożliwe lub niewystarczające, wykonawca będzie zobowiązany do realizacji tych czynności w trybie stacjonarnym, w siedzibie Zamawiającego.

11. **Zastąpienie członka zespołu**
    Czy Zamawiający dopuszcza zastąpienie członka zespołu osobą o równoważnych kwalifikacjach w trakcie realizacji projektu, w przypadku zdarzeń losowych?
    Takie rozwiązanie jest standardem rynkowym i minimalizuje ryzyko niewykonania umowy.

Odpowiedź:

Zamawiający dopuszcza możliwość zastąpienia członka zespołu osobą o kwalifikacjach i doświadczeniu nie gorszych niż wymagane w zapytaniu ofertowym, w przypadku wystąpienia zdarzeń losowych lub innych okoliczności uniemożliwiających dalszy udział danej osoby w realizacji zamówienia. Zmiana taka będzie dopuszczalna pod warunkiem uzyskania akceptacji Zamawiającego oraz wprowadzenia stosownej zmiany do umowy. Wykonawca jest zobowiązany do niezwłocznego przedstawienia kandydata zastępczego wraz z dokumentami potwierdzającymi spełnianie przez niego wszystkich wymaganych kwalifikacji.

12. **Termin audytu końcowego**
    Czy Zamawiający może doprecyzować, czy termin wykonania audytu końcowego jest uzależniony od zakończenia innych zadań w projekcie i czy przewiduje możliwość jego przesunięcia w przypadku opóźnień niezależnych od wykonawcy?

Odpowiedź:

Wprowadzono zmiany do załącznika nr 7 – wzór umowy. Dodano do wzoru: „ § 13. Zmiany postanowień Umowy”. W dokumencie wskazano warunki zmiany Umowy, w tym termin realizacji.

13. **Uzasadnienie wymogów**
    Czy Zamawiający mógłby przedstawić uzasadnienie dla wskazanych wymagań, w szczególności dotyczących liczebności zespołu, określonych certyfikatów oraz formy zatrudnienia, w kontekście zasady uczciwej konkurencji z regulaminu projektu „Cyberbezpieczny Samorząd”?

Odpowiedź:

Wymagania dotyczące liczby i kwalifikacji członków zespołu wynikają z konieczności zapewnienia zgodności z Regulaminem Konkursu Grantowego oraz celami projektu „Cyberbezpieczny Samorząd”, w tym zapewnienia wysokiej jakości wdrożenia SZBI, zgodności z normą ISO/IEC 27001 oraz dyrektywą NIS2, a także realizacji obowiązków wynikających z ustawy o krajowym systemie cyberbezpieczeństwa. W szczególności wymóg posiadania określonych certyfikatów odnosi się do § 20 ust. 2 rozporządzenia w sprawie Krajowych Ram Interoperacyjności oraz do Rozporządzenia Ministra Cyfryzacji z dnia 12 października 2018 r. (Dz.U. poz. 1999), które określa wykaz certyfikatów uprawniających do przeprowadzenia audytu, m.in.: CIA, CISA, CISSP, CISM, CRISC, CGEIT, SSCP, certyfikat audytora wiodącego ISO/IEC 27001 oraz ISO 22301, wydane przez akredytowane jednostki certyfikujące. W zapytaniu ofertowym wskazano certyfikaty: CISSP, CEH, ISO 27001:2022 Audytor wiodący, ISO 22301:2019 Audytor wiodący, CIA. Dobór ten nie jest przypadkowy – wynika z potrzeby zapewnienia, aby zespół projektowy posiadał zarówno kompetencje techniczne (np. CEH, CISSP), jak i

kompetencje audytowe w zakresie systemów zarządzania bezpieczeństwem informacji i ciągłości działania (ISO 27001, ISO 22301) oraz audytu wewnętrznego (CIA). Jest to zgodne z zakresem zadań opisanych w OPZ, obejmujących audyty, analizy, wdrożenia polityk oraz testy bezpieczeństwa. Określenie wymagań ma na celu zapewnienie, że osoby realizujące audyty i prace wdrożeniowe dysponują wiedzą i umiejętnościami potwierdzonymi w sposób obiektywny, umożliwiający prawidłowe przeprowadzenie audytu końcowego i realizację celów projektu, zgodnie z zasadą uczciwej konkurencji z dopuszczeniem certyfikatów równoważnych w zakresie merytorycznym.

Z up. Wójta Gminy Somonino

Zastępca Wójta Gminy Somonino

Andrzej Peta

Andrzej Peta

Elektronicznie podpisany przez Andrzej Peta
Data: 2025.08.13 16:31:48 +02'00'