20.04.2021 r.

Wyjaśnienia treści ogłoszenia

1. **Czy wszystkie prace mogą zostać wykonane zdalnie? Jeśli nie jaki zakres prac musi być wykonany na miejscu?**

Odpowiedź:

Ze względu na stan epidemii COVID-19, Zamawiający dopuszcza możliwość przeprowadzenia prac audytowych w formie zdalnej. Jeżeli będzie wymagane przeprowadzenie audytu stacjonarnego w zakresie weryfikacji normy ISO/IEC 27001, jego zakres zostanie ustalony z Zamawiającym na etapie realizacji audytu. W takim przypadku Wykonawca uzyska dostęp do infrastruktury w zakresie ustalonym z Zamawiającym. Serwerownie znajdują się w okolicach Warszawy, Lublina oraz Katowic.

1. **Czy prace będą wykonywane na środowisku testowym, czy produkcyjnym?**

Odpowiedź:

Prace będą wykonywane na środowisku testowym.

1. **Czy Zamawiający wymaga wykonywania testów w określonych godzinach?**

Odpowiedź:

Zamawiający nie wymaga, aby testy były wykonywane we wskazanych przez niego godzinach.

1. **Czy testy mogą zostać wykonane ze stacji roboczych pentesterów, czy też Zamawiający oczekuje wykonywania testów ze swojej stacji przesiadkowej?**

Odpowiedź:

Testy mogą być wykonywane ze stacji roboczych audytorów.

1. **W oparciu o jakie technologie został zbudowane systemy podlegające testom.**

Odpowiedź:

Przy budowie aplikacji webowych podlegających audytowi użyto m. in. technologii PHP, Angular, projekty graficzne opracowano w oparciu o Framework CSS Bootstrap, w przypadku portalu web również technologia Wordpress.

1. **Czy podczas testów będzie można wykonać ataki, które mogą spowodować niedostępność systemu tj. ataki DoS? Czy należy powiadamiać o dokładnym terminie wykonania takich testów?**

Odpowiedź:

Zamawiający dopuszcza wykonanie takich ataków na środowisku testowym. Termin wykonania testów powinien zostać uprzednio uzgodniony z Zamawiającym.

1. **Czy Zamawiający zapewni szybką reakcję administratorów mającą na celu niezwłoczne przywrócenie systemu w przypadku skutecznego ataku DoS?**

Odpowiedź:

Z zastrzeżeniem odpowiedzi na pyt. nr 6, Wykonawca jest zobowiązany do poinformowania o prowadzeniu takich testów co umożliwi reakcję administratora systemu.

1. **Od osoby "Osoba nr 2 osoba pełniąca rolę inżyniera bezpieczeństwa IT" wymagane jest doświadczeniu w wykonywaniu analiz wymagań bezpieczeństwa, natomiast szablon "Wykaz\_osób\_kryterium" każe wskazać doświadczenie z audytu. Czy to błąd szablonu z Wykazem?**

Odpowiedź:

Zamawiający wyjaśnia, że treść dokumentów jest prawidłowa. W ramach pozacenowego kryterium punktowane są dodatkowe cechy członków zespołu audytorskiego, wykraczające poza wymagania niezbędne.

1. **W jaki sposób liczone będzie "Doświadczenie zespołu realizującego zamówienie"? Czy będzie to suma doświadczeń wskazanych członków zespołu? Doświadczenie osoby z największym doświadczeniem?**

Odpowiedź:

Punktowana będzie suma doświadczeń wszystkich wskazanych w wykazie osób.

1. **Na przygotowanie raportu z audytu jest w jednym miejscu 14 dni ("w terminie do 14 dni od zakończenia danego etapu prac"), a w innych w ramach czasu przeznaczonego na sam audyt ("Raport musi być dostarczony Zamawiającemu, w formie elektronicznej – w formacie .DOC i .PDF., najpóźniej w ostatnim dniu realizacji audytu"). Prośba o uspójnienie. 2-3 tygodnie na audyt wraz z przygotowaniem raportu to trochę mało, szczególnie gdy dany audyt składa się z wielu elementów. Dodatkowe 5 dni na przygotowanie raportu umożliwi przygotowanie lepiej uporządkowanego raportu.**

Odpowiedź:

Zamawiający wyjaśnia, że czas trwania każdego z procesów audytowych został oszacowany z uwzględnieniem jego czasochłonności, zaś wskazany termin 14-dniowy sporządzenia raportu jest terminem maksymalnym w odniesieniu do każdego z etapów. Zamawiający nie zmienia zapisów OPZ.

1. **Czy systemy, które podlegają audytowi to wyłącznie aplikacje webowe i usługi API (REST/WS) czy także inne aplikacje klienckie?**

Odpowiedź:

W ramach audytu badane będą aplikacje webowe w tym strony web oraz usługi API.

1. **Pytanie do analizy kodu aplikacji. Jaka jest wielkość aplikacji (np. liczba linii kodu) i jaki język programowania?**

Odpowiedź:

Wielkość aplikacji jest zróżnicowana, w zależności od ich charakteru – np. dla aplikacji Książki Adresowej PEF jest to ok. 35 000 linii kodu w warstwie frontendowej i ok. 12 000 linii kodu w warstwie backendowej, z kolei w przypadku aplikacji brokerskich PEF jest są to wartości przekraczające 100 000 linii kodu osobno dla każdej z warstw. Użyte języki i formaty to głównie Type Script, HTML, PHP, ale również m. in. Sass, JSON, Javascript, Yaml, Blade.

1. **Czy Zamawiający oczekuje by w ramach prac miały miejsce spotkania audytowe prowadzone przez Wykonawcę z udziałem Zamawiającego i Wykonawcy systemów informatycznych?**

Odpowiedź:

Zamawiający przewiduje takie spotkania w formie zdalnej.

1. **Jednocześnie zwracam się z prośbą o przedłużenie terminu składania ofert o tydzień tj. do 29 kwietnia 2021 r.**

Odpowiedź:

Zamawiający nie wyraża zgody na przedłużenie terminu składania ofert.