INSTYTUT NAFTY I GAZU - Państwowy Instytut Badawczy
ul. Lubicz 25 A, 31-503 Kraków
tel.: +48 12 421 00 33 fax: +48 12 430 38 85
www.inig.pl office@inig.pl

JZDZ-DD-2301-963/2025

Kraków, 15 lipca 2025 r.

Dotyczy: zapytania ofertowego na **usługę przeprowadzenia audytu bezpieczeństwa i testów penetracyjnych aplikacji internetowej „Moduł KZR".**
W niniejszym postępowaniu nie stosuje się przepisów ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (t.j. Dz. U. 2024 r., poz. 1320 ze zm.). Szacowana wartość zamówienia nie przekracza 130.000 zł.

Zamawiający przekazuje wyjaśnienia odnoszące się do pytań zadanego przez Wykonawcę.

Pytania Wykonawcy
Poniżej przesyłamy pytania do zamówienia "Usługa przeprowadzenia audytu bezpieczeństwa i testów penetracyjnych aplikacji internetowej „Moduł KZR"."

Audyt bezpieczeństwa aplikacji webowej

1. W jakim trybie mają być przeprowadzone testy:
   a. Black-box – brak dostępu do dokumentacji / brak dostępu do aplikacji (testy BEZ logowania do aplikacji)?
   b. Grey-box – dostęp do dokumentacji / dostęp do aplikacji (testy po zalogowaniu do aplikacji)?
2. Krótki opis do czego służy aplikacja (np. aplikacja do realizacji transakcji bankowych, sklep internetowy) oraz kluczowe funkcje (lista głównych funkcji) oraz opis kategorii przetwarzanych danych (dane osobowe klientów, dane kartowe, dane transakcyjne, dane o stanie zdrowia etc.).
3. Lista metod logowania/uwierzytelniania: (np. ID, hasło, certyfikat, token, kod sms), które mają zostać objęte testami.
4. Lista metod autoryzacji operacji (jeśli występuje): (np. certyfikat, token (sprzętowy), kod sms, urządzenia HSM (Hardware Security Module, inne - proszę podać jakie), które mają zostać objęte testami.
5. Liczba ról, które mają podlegać testom (np. gość, użytkownik zwykły, użytkownik rozszerzony, operator, administrator, itp.) wraz z krótkim opisem (np. administrator – zarządza prawami dostępu innych użytkowników), które mają zostać objęte testami,
6. Sumaryczna, orientacyjna liczba pól we wszystkich formularzach, które mają zostać objęte testami.

Audyt wydajności aplikacji webowej

1. Jaki są zakładane poziomy wydajności i jej kontekstu dla danego procesu/czynności realizowanego w aplikacji (np. 300 jednoczesnych użytkowników wykonujących 20 logowań na minutę oraz 50 jednoczesnych procesów zakupowych)?
2. Prosimy o przesłanie listy procesów biznesowych, które mają być objęte testami oraz określenie założeń wydajności dla każdego z nich.
3. Prosimy o przeslanie listy endpointów wchodzących w skład testów (WEB/API/inne).
4. Prosimy o informacji o skali środowiska i podstawowe informacje nt. infrastruktury (np. serwis obsługiwany jest przez 25 serwerów web w cloud/na maszynach fizycznych/na serwerach wirtualnych, czy środowisko obsługiwane jest przez CDN, czy statyczny kontent jest oddzielony od dynamicznego, jakie zastosowano mechanizmy balansowania, jakie zastosowano mechanizmy cache'owania).

Audyt zgodności z przepisami

Organizacja:

5. Liczba pracowników w firmie.
6. Liczba użytkowników systemów informatycznych w firmie.
7. Liczba lokalizacji firmy(centrala + oddziały) z informacją, które z nich mają być objęte audytem.
8. Czy i jakie usługi IT są outsoursowane?

Procesy

9. Lista usług świadczonych przez Internet.
10. Jak jest lista procesów IT i bezpieczeństwa, które dotyczą Systemu i mają być objęte audytem (np. proces rozwoju Systemu, proces zarządzania dostępem do Systemu, itp.)?
11. Liczba dostawców usług IT ze wskazaniem kluczowych
12. Lista usług świadczonych przez dostawców IT (outsourcing usług IT), np.
    a. Środowisko chmurowe dla infrastruktury
    b. Środowisko chmurowe dla back office
    c. Środowisko programistyczne
    d. Inne środowisko (opisać)
7. Czy procesy bezpieczeństwa zostały wdrożone w oparciu o jakieś normy / standardy? Jakie?

Infrastruktura IT

8. Liczba i rodzaj systemów, które mają być objęte audytem:
    a. Aplikacje biznesowe (transakcyjne, operacyjne, finansowe, księgowe, kadrowe, biurowe - np. Symfonia, Navision, Teta, SAP, itp.),
    b. Serwery oraz systemy operacyjne (Windows, Linux, Unix, itp.),
    c. Bazy danych (MySQL, MS SQL, Oracle, itp.),
    d. Urządzenia sieciowe (rutery, switche, itp.),
    e. Systemy wspomagające bezpieczeństwo (SIEM, NAC, firewall, IDS, VPN itp.),
    f. Stacje robocze,
    g. Inne – jakie?
9. Liczba zewnętrznych adresów IP, które mają podlegać technicznemu, zewnętrznemu audytowi.
10. Linki (URL) do strony www, aplikacji webowych dostępnych przez Internet, które mają zostać objęte audytem. -
11. Lista rozwiązań chmurowych, które mają być objęte audytem:
    a. MS AZURE
    b. AWS
    c. GCP
    d. …

Bezpieczeństwo fizyczne

12. Gdzie (miejscowość) zlokalizowana jest:
    a. Główna serwerownia?
    b. Zapasowa serwerownia?

Dokumentacja

13. Jak obszerna jest dokumentacja, którą należy objąć audytem? Jaka jest szacowana liczba stron

<u>Analiza kodu źródłowego</u>

1. Technologia aplikacji:
    a. Język w jakim napisana jest aplikacja (np. .Net, JavaScript, J2EE, PHP) wraz z informacją o użytych frameworkach.
    b. Sposób budowy (MVC, MVP, itp).
    c. Użyta technologia backend (SQL, NoSQL, itp.).
2. Wielkość kodu wraz z bibliotekami zewnętrznymi, ale z pominięciem wszystkich resource'ów (takich jak: pliki graficzne, metadane systemów zarządzania kodem, itp. - chodzi wyłącznie o sam kod badanej aplikacji oraz biblioteki zewnętrzne z których korzysta:
    a. Liczba linii kodu z komentarzami
    b. Liczba linii kodu bez komentarzy
    c. Objętość (MB)
3. Czy zakres audytu ma obejmować cały kod (wszystkie linie kodu), czy też wybrane, najważniejsze fragmenty?

4. Czy audyt można wykonać zdalnie?

Analiza konfiguracji systemów

1. Zakres adresacji IP objętych testami.
2. Orientacyjna liczba aktywnych IP w ramach adresacji objętej testami.
3. Proszę podać godziny, w których można przeprowadzać testy, oraz dni i godziny, w których środowiska testowe będą dostępne.
4. Prosimy o specyfikację komponentów infrastruktury, które mają być objęte testami:

a. Rodzaj (np. serwer aplikacyjny, serwer www, serwer bazodanowy, system operacyjny Windows, system operacyjny Linux, drukarka, skaner, urządzenie aktywne, inne, itp.).
b. Producent
c. Wersja
d. Dla baz danych rosimy o podanie liczby baz danych dla każdej z instancji z baz danych, które mają być objęte testami.

Przykładowo:
MS SQL 2019 wersja 15.0.2000.5, 2 instancje, 2 bazy w instancji nr 1 i 3 bazy w instancji nr 2

Odpowiedz Zamawiającego:
Zamawiający ze względów bezpieczeństwa audytowanej aplikacji internetowej „Moduł KZR", pozostawia zadane przez Wykonawcę pytania bez odpowiedzi.

Powyższe wyjaśnienia stają się integralną częścią zapytania ofertowego i nie powodują zmiany terminu składania ofert.

p.o. Kierownika
Działu Zamówień i Administracji
mgr inż. Elżbieta Turek