Załącznik nr 2 do Zaproszenie do udziału w rozeznaniu rynku

DEPARTAMENT INFORMATYZACJI I REJESTRÓW SĄDOWYCH	Warszawa, dnia ……..
Numer sprawy: DIRS-XX.043.3.2022	
Opis Przedmiotu Zamówienia	

Spis treści

„Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Społecznego Program Operacyjny Wiedza Edukacja Rozwój”

1. Opis Systemu KRK 2.0

Głównym zadaniem systemu teleinformatycznego Krajowego Rejestru Karnego jest przetwarzanie oraz udzielanie informacji o osobach:

- prawomocnie skazanych za przestępstwa lub przestępstwa skarbowe,
- przeciwko którym prawomocnie warunkowo umorzono postępowanie karne w sprawach o przestępstwa lub przestępstwa skarbowe,
- przeciwko którym prawomocnie umorzono postępowanie karne w sprawach o przestępstwa lub przestępstwa skarbowe na podstawie amnestii,
- będących obywatelami polskimi prawomocnie skazanymi przez sądy państw obcych,
- prawomocnie skazanych za wykroczenia na karę aresztu,
- wobec których prawomocnie orzeczono środki zabezpieczające w sprawach o przestępstwa lub przestępstwa skarbowe,
- poszukiwanych listem gończym,
- tymczasowo aresztowanych,
- odbywających karę pozbawienia wolności,
- nieletnich, wobec których prawomocnie orzeczono środki wychowawcze, poprawcze, leczniczo-wychowawcze albo którym wymierzono karę na podstawie art. 13 lub art. 94 ustawy z dnia 26 października 1982 r. o postępowaniu w sprawach nieletnich (Dz.U. z 2014 r. poz.382),
- nieletnich umieszczonych w schroniskach dla nieletnich,

a także o:

- podmiotach zbiorowych, wobec których prawomocnie orzeczono karę pieniężną, przepadek, zakaz lub podanie wyroku do publicznej wiadomości na podstawie ustawy z dnia 28 października 2002 r. o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary (Dz.U. z 2014 r. poz.1417, z późn. zm.).

2. Informacje o dotychczas wytworzonym środowisku systemu

2.1. Wykaz rodzajów środowisk systemu informatycznego

System KRK 2.0 obecnie składa się ze środowisk:

a) <u>produkcyjnego (łącznie 20 maszyn wirtualnych VMWare ESXI 6.5):</u>
   - system operacyjny: Windows Server 2016 ENG,
   - system operacyjny Red Hat Enterprise Linux 8,
   - baza danych: SQL Server 2017, AlwaysON Failover clustering,
   - serwery aplikacyjne IIS,
   - Net Framework 4.6.2,
   - kontrolery domeny, listener,

b) <u>preprodukcyjnego (łącznie 18 maszyn wirtualnych VMWare ESXI 6.5):</u>
   - system operacyjny: Windows Server 2016 ENG,
   - baza danych: SQL Server 2017, AlwaysON Failover clustering,
   - serwery aplikacyjne IIS,
   - Net Framework 4.6.2,
   - kontrolery domeny, listener,

c) <u>testowo-deweloperskiego (łącznie 22 maszyny wirtualne VMWare ESXI 6.5):</u>

„Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Społecznego Program Operacyjny Wiedza Edukacja Rozwój"

- system operacyjny: Windows Server 2016 ENG,
- baza danych: SQL Server 2017, AlwaysON Failover clustering,
- serwery aplikacyjne IIS,
- Net Framework 4.6.2,
- kontrolery domeny, listener,

d) testowo-deweloperskiego (łącznie 22 maszyny wirtualne VMWare ESXI 6.5):
- system operacyjny: Windows Server 2016 ENG,
- baza danych: SQL Server 2017, AlwaysON Failover clustering,
- serwery aplikacyjne IIS,
- Net Framework 4.6.2,
- kontrolery domeny, listener.

Liczba maszyn wirtualnych systemu, wersje oprogramowania mogą ulec zmianie, gdyż system KRK 2.0 jest rozwijany, rozbudowywany o kolejne usługi i integracje systemowe. Aktualnie realizowana jest min. budowa e-Usługi uzyskiwania informacji z Krajowego Rejestru Karnego (KRK) osadzonej na Portalu Rejestrów Sądowych. Środowisko produkcyjne oparte jest o macierze OpenShift.

2.2. Technologie programistyczne

Lista wykorzystanych do budowy systemu technologii programistycznych obejmuje:
- Technologia .NET i .NET Core,
- Język programowania:
  Warstwa backend: C#,
  Warstwa frontend: Angular framework.

3. Cele audytowe

1) Celem głównym audytu jest określenie poziomu bezpieczeństwa systemu informatycznego Krajowego Rejestru Karnego 2.0, wskazanie punktów obniżających ten poziom oraz zaproponowanie rozwiązań, które doprowadzą środowisko do akceptowalnego przez Zamawiającego poziomu bezpieczeństwa.

2) Celem szczegółowym audytu jest przeprowadzenie badań i analiz umożliwiających wskazanie zagrożeń wynikających:
   a) z cech zaprojektowanej topologii i zasad współpracy systemów,
   b) z zastosowanych technologii i standardów zabezpieczeń,
   c) z jakości implementacji systemu,
   d) z architektury styków międzysieciowych,
   e) ze słabości oprogramowania oraz poprawności konfiguracji komponentów rozwiązania, takich jak, systemy obsługi transmisji, systemy zaporowe, i inne systemy usługowe i pomocnicze.

3) Zakres usług realizowanych w ramach audytu obejmuje przeprowadzenie:
   a) Audytu bezpieczeństwa systemów teleinformatycznych.
   Celem audytu jest wykrycie faktycznych oraz potencjalnych luk i błędów w oprogramowaniu, konfiguracji urządzeń informatycznych, portalach i aplikacjach webowych, które mogą być wykorzystane do naruszenia bezpieczeństwa przetwarzanych informacji, a także bezpieczeństwa Zamawiającego lub użytkowników systemów. Przeprowadzenie audytu na etapie wytwarzania i przekazywania do użytkowania systemów teleinformatycznych ma

„Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Społecznego Program Operacyjny Wiedza Edukacja Rozwój”

pozwolić na dostarczenie odbiorcom projektu rozwiązań gwarantujących osiągnięcie wymaganego poziomu bezpieczeństwa w fazie użytkowania.

Zakres audytu:

i) analiza architektury sieciowej:
- weryfikacja sieci LAN na strefy sieciowe (w tym wykorzystanie urządzeń typu firewall oraz VLAN),
- określenie usług działających w wybranych podsieciach (do 10 podsieci),
- poszukiwanie podatności w wybranych podsieciach (do 10 podsieci),
- weryfikacja mechanizmów ochronnych w warstwie 2 i 3 modelu OSI,
- weryfikacja dostępu do Internetu z LAN,
- szczegółowa analiza komunikacji sieciowej,
- weryfikacja zasad utrzymania sieci,

ii) analiza brzegu sieci:
- weryfikacja topologii/architektury sieci,
- testy szczelności systemów klasy firewall,
- ogólna analiza komunikacji sieciowej z poziomu sieci Internet,
- skanowanie portów różnymi technikami, w celu wykrycia potencjalnych luk bezpieczeństwa w udostępnianych usługach,
- wykrywanie usług sieciowych udostępnionych w sieci Internet,
- próba detekcji wersji oraz typu oprogramowania systemowego zainstalowanego na urządzeniach dostępnych z sieci Internet,
- testowanie odporności usług wystawionych do sieci Internet na ataki „Denial of Service" co najmniej 2 metodami zaproponowanymi przez Wykonawcę,
- testowanie odporności usług wystawionych do sieci Internet, za pomocą narzędzi eksploatujących typowe luki bezpieczeństwa,

iii) analiza bezpieczeństwa konfiguracji systemów informatycznych (urządzeń i aplikacji):
- analiza zgodności konfiguracji i sposobu funkcjonowania urządzeń:
  - weryfikacja udostępnionych usług sieciowych,
  - weryfikacja zbędnych usług wraz ze wskazaniem ich podatności,
  - weryfikacja zaimplementowanych systemów aktualizacji,
  - weryfikacja zaimplementowanych systemów logowania zdarzeń,
  - weryfikacja mechanizmów administracji zdalnej,
  - weryfikacja przypisania użytkowników do właściwych grup,
  - weryfikacja uprawnień zgodnie z pryncypium jak najmniejszych uprawnień (ang. „least privilige"),
  - przeprowadzenie prób obejścia uprawnień i uzyskania nieautoryzowanego dostępu do informacji,
  - weryfikacja sposobu udostępniania baz danych na poziomie sieciowym,
  - analiza implementacji podstawowych zasad hardeningowych bazy danych (np. wyłączenie nieużywanych usług, wyłączenie nieużywanych metod dostępu, konfiguracja uprawnień do obiektów, logowanie zdarzeń, składowanie logów, monitorowanie dostępu do obiektów, monitorowanie instrukcji języka SQL),
  - analiza architektury baz danych (np. wykorzystanie mechanizmów autoryzacji oraz uwierzytelniania, segmentacja uprawnień, wykorzystywanie widoków, wykorzystywanie procedur składowych,

„Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Społecznego Program Operacyjny Wiedza Edukacja Rozwój"

przechowywanie oraz dostęp do danych wrażliwych, przechowywanie oraz dostęp do danych audytowych, szyfrowanie danych),
- analiza komunikacji z klientami bazodanowymi (mechanizmy kryptograficzne, transfery danych),

- analiza podatności aplikacji:
  - wytypowanie wrażliwych punktów w aplikacji,
  - inspekcja mechanizmów uwierzytelniania / autoryzacji,
  - weryfikacja implementacji mechanizmów ochronnych dla serwerów aplikacyjnych,
  - weryfikacja obsługi błędów,
  - analiza poziomu bezpieczeństwa oferowanego przez aplikacje,
  - analiza kodu aplikacji, w tym:
    - zastosowanie dobrych praktyk zalecanych przez producenta(-ów) technologii, w których aplikacja została wytworzona,
    - zastosowanie wytycznych właściwych dla zastosowanej technologii,
    - konsekwencja w stosowaniu standardów, konwencji, itp.,
    - stosowanie wzorców projektowych,
    - stosowanie właściwych podziałów na warstwy i komponenty z zachowaniem zasad rozłącznego i osobliwego zastosowania (Separation of Concerns),
    - analiza użytych funkcji lub komponentów pod kątem elementów przestarzałych („deprecated") lub elementów posiadających znane luki bezpieczeństwa lub podatności,
    - dokumentowanie autorskiego kodu aplikacji, w sposób umożliwiający automatyczne wygenerowanie dokumentacji API,

iv) przeprowadzenie testów penetracyjnych i symulowanych ataków obejmujących:
- testy bezpieczeństwa aplikacji pod kątem:
  - ataków semantycznych na adres URL,
  - ataków związanych z ładowaniem plików,
  - ataków typu Cross-Site Scripting,
  - ataków typu Cross-Site Request Forgery,
  - ataków typu MITM (Man in the Middle),
  - podrabiania zarządzania formularza,
  - sfałszowania żądania http,
  - ujawnienia danych przechowywanych w bazie,
  - trawersowania katalogów,
  - ujawniania kodu źródłowego,
  - przepełnienia bufora lub stosu,
  - wstrzykiwania kodu wykonywalnego innych języków programowania,

- badanie enumeracji i wykorzystania znanych podatności w celu uzyskania nieautoryzowanego dostępu,
- badanie możliwości podszywania się pod użytkowników i uzyskania nieautoryzowanego dostępu do systemu,
- badanie możliwości podszywania się pod użytkowników uprzywilejowanych i uzyskanie dostępu do systemu,

„Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Społecznego Program Operacyjny Wiedza Edukacja Rozwój"

- badanie możliwości blokowania/umożliwienia dostępu do systemu wszystkim lub wybranym jej użytkownikom,
- badanie możliwości modyfikacji/usunięcia danych z systemu.

b) Audytu funkcjonowania systemów bezpieczeństwa.
Audyt obejmuje analizę funkcjonowania następujących systemów bezpieczeństwa:
   i) System antywirusowy.
   ii) System antyspamowy.
   iii) System DLP (Data Leak Prevention/Data Loss Prevention).
   iv) System Firewall.
   v) System backupowy.
   vi) System zasilania awaryjnego.

Zakres audytu:
   i) Kompleksowa analiza skuteczności działania.
   ii) Analizę procedur utrzymaniowych i monitorowania systemów bezpieczeństwa.
   iii) Weryfikacja poprawności konfiguracji systemów bezpieczeństwa.
   iv) Weryfikacja i/lub opracowanie wskaźników efektywności.

4) W wyniku przeprowadzonego audytu wykonawca dostarczy raport zawierający:
   a) Opis przeprowadzonych działań (w tym weryfikacji komponentów systemu KRK 2.0 i wykonanych testów).

   b) Wyniki testów i ich interpretację, w szczególności:
      i) Informacje dotyczące ogólnej oceny poziomu bezpieczeństwa oraz odporności na ataki badanych systemów zawierające podsumowanie ilości stwierdzonych nieprawidłowości w podziale na systemy i krytyczności,
      ii) Opis lokalizacji wykrytych podatności - sposobu, w jaki można zlokalizować i powtórzyć testowy atak na podatność (Proof of Concept),
      iii) Informacje na temat poziomu ochrony realizowanego przez system zabezpieczeń.

   c) Wnioski z audytu (określenie ilościowego i jakościowego poziomu niebezpieczeństwa podatności).

   d) Rekomendacje i zalecenia pozwalające na usunięcie wykrytych słabości, a tym samym podniesienie poziomu bezpieczeństwa badanych systemów (określenia sposobu naprawy wykrytych podatności w tym zmian konfiguracyjnych).

   e) Raport musi być sporządzony w języku polskim, dostarczany w formie papierowej i elektronicznej (plik: *.DOC z możliwością edycji i *.PDF).

5) Zakres usług zostanie przeprowadzony zgodnie z harmonogramem:

Termin realizacji	**Czynność**
II kwartał 2023 r.	Przeprowadzenie audytu bezpieczeństwa KRK 2.0

6) Wymagania metodyczne:

„Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Społecznego Program Operacyjny Wiedza Edukacja Rozwój”

6.1. Standardy testowania bezpieczeństwa.

Zamawiający wymaga w ramach realizacji zadania wykonywania testów penetracyjnych wykorzystania standardów testowania bezpieczeństwa:

a) OWASP (Open Web Application Security Project) ASVS 2014,
b) Open Source Security Testing Methodology Manual (OSSTMM),
c) Penetration Testing Execution Standard (PTES),

lub równoważnych (za równoważne Zamawiający uzna, standardy opisujące przebieg procesu testowania bezpieczeństwa systemów IT oraz obszary systemowe, które muszą podlegać weryfikacji).

6.2. Opracowanie potrzeb w zakresie poziomu pokrycia testami.

Zamawiający wymaga wykorzystania następujących poziomów pokrycia systemu testami bezpieczeństwa.

a) Poziom 0 ma stanowić elastyczny poziom początkowy w hierarchii weryfikacyjnej. Wskazuje on, że aplikacja została poddana określonego rodzaju weryfikacji. Na poziomie 0 na potrzeby realizacji automatycznego, pobieżnego skanowania wszystkich posiadanych aplikacji zewnętrznych należy korzystać z wybranego narzędzia komercyjnego, podczas gdy inne mogą zdefiniować wymagania Poziomu 0 na podstawie danych odnośnie ostatnich przypadków naruszenia bezpieczeństwa. W przeciwieństwie do pozostałych poziomów, Poziom 0 nie jest niezbędny dla realizacji innych poziomów. Wykonywana na tym poziomie weryfikacja ręczna nie ma na celu zapewnienie kompletnej weryfikacji bezpieczeństwa, tylko upewnienie się, że wyniki testów automatycznych są poprawne i nie stanowią fałszywych wskazań.

b) Poziom 1 obejmuje zagrożenia, które weryfikujący może zidentyfikować przy minimalnym lub umiarkowanym wysiłku. Poziomu 1 nie należy postrzegać jako poziomu szczegółowej kontroli lub weryfikacji aplikacji, lecz jako poziom szybkiej kontroli. Poziom 1 jest zwykle odpowiedni dla aplikacji, dla których wymagany jest pewien poziom zaufania co do poprawnego użycia mechanizmów bezpieczeństwa, bądź też w celu szybkiego pokrycia całego zbioru aplikacji instytucji oraz ułatwienia opracowania planu bardziej szczegółowych kontroli, które będą realizowane w późniejszym terminie. Typowymi zagrożeniami dla bezpieczeństwa aplikacji będą w tym przypadku napastnicy stosujący proste techniki umożliwiające łatwe wykrycie i zbadanie zagrożeń. Stanowią oni przeciwieństwo napastników zdeterminowanych, które wkładają większy wysiłek ukierunkowany na daną aplikację.

c) Poziom 2 zapewnia, że mechanizmy bezpieczeństwa funkcjonują w sposób prawidłowy i są użyte w aplikacji wszędzie tam, gdzie powinny być użyte by egzekwować polityki specyficzne dla aplikacji. Poziom 2 stanowi standard branżowy, któremu podlega większość wrażliwych aplikacji stosowanych przez organizacje. Poziom 2 jest zwykle odpowiedni dla aplikacji, które obsługują istotne transakcje biznesowe pomiędzy firmami, włączając to aplikacje przetwarzające dane o stanie zdrowia, aplikacje spełniające krytyczne dla biznesu, wrażliwe funkcje lub przetwarzające inne wrażliwe aktywa. Typowymi zagrożeniami dla bezpieczeństwa będą w tym przypadku napastnicy liczący na okazję oraz zdeterminowani napastnicy (wykwalifikowani i zmotywowani, skupieni na określonych celach, używający m.in. specjalnie przystosowanych narzędzi skanujących).

„Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Społecznego Program Operacyjny Wiedza Edukacja Rozwój”

d) Poziom 3 jest jedynym poziomem, który wymaga również kontroli projektu aplikacji. Ponadto obowiązują w tym przypadku następujące wymagania:
   - wszelkie istotne mechanizmy bezpieczeństwa, których oddziaływanie ma charakter przekrojowy (obejmując kontrolę danych wejściowych i proces uwierzytelniania) powinny zostać wdrożone w sposób scentralizowany,
   - mechanizmy bezpieczeństwa dokonujące kontroli bezpieczeństwa powinny podejmować decyzje w oparciu o listę dozwolonych wyników (model pozytywny),
   - kontroli danych wejściowych nie należy stosować jako jedynego mechanizmu obronnego względem praktyk tworzenia skryptów i wstrzykiwania kodów. Mechanizm ten powinien być stosowany jako dodatkowa linia obrony, uzupełniając parametryzację i kodowanie danych wejściowych. Weryfikacja na Poziomie 3 jest zwykle odpowiednia dla krytycznych aplikacji, od których zależy życie i bezpieczeństwo, krytyczna infrastruktura lub zadania związane z obronnością, bądź też które mogą ułatwić spowodowanie znacznych strat dla organizacji. Poziom 3 może być również odpowiedni dla aplikacji służących do przetwarzania wrażliwych aktywów. Zagrożeniami dla bezpieczeństwa w tym przypadku będą zdeterminowani napastnicy (wykwalifikowani i zmotywowani napastnicy skupieni na określonych celach, używający m.in. specjalnie przystosowanych narzędzi skanujących).

6.3. Wykorzystanie baz danych o znanych podatnościach i słabościach bezpieczeństwa.
Zamawiający wymaga wykorzystania znanych baz danych o podatnościach i słabościach bezpieczeństwa systemów informatycznych, w trakcie prac prowadzonych przez Wykonawcę w ramach przedmiotu zamówienia, np.:
a) SANS Top 20 Critical Security Controls,
b) Common Vulnerabilities and Exposures,
c) WASC (Web Application Security Consortium) Threat Classification,
lub równoważnych (za równoważne Zamawiający uzna takie bazy danych, które stanowią aktualne źródło informacji o lukach bezpieczeństwa, są publikowane lub utrzymywane przez uznane powszechnie organizacje, działające na rzecz zapewnienia bezpieczeństwa systemów informatycznych).

6.4. Wykorzystanie list kontrolnych.
Zamawiający wymaga aby w ramach realizacji audytu bezpieczeństwa do oceny wykorzystywane były listy kontrolne udostępniane przez uznane organizacje pracujące na rzecz bezpieczeństwa systemów IT, tj.:
a) National Security Agency (NSA),
b) Center for Internet Security (CIS),
lub równoważnych (w szczególności takich, które stanowią aktualne źródło informacji o bezpiecznej konfiguracji, są publikowane lub utrzymywane przez uznane powszechnie organizacje, działające na rzecz zapewnienia bezpieczeństwa systemów informatycznych).

6.5. Uwzględnienie typowych dla testowania penetracyjnego zadań
Zamawiający wymaga aby w ramach realizacji testów penetracyjnych obejmowały one typowe, wymienione niżej zadania (będące elementem każdej metodyki testów penetracyjnych):
a) Target Scoping (Zakres Docelowy – ustalenie charakteru i zasięgu testów),
b) Information Gathering (Gromadzenie Informacji – pasywne zbieranie informacji na temat obiektu testów),
c) Target Discovery (Odkrywanie Celu – pół-pasywne zbieranie informacji, poznanie celów, identyfikacja podsieci, rodzaju architektury, systemów operacyjnych),

„Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Społecznego Program Operacyjny Wiedza Edukacja Rozwój”

d) Enumerating Target (Wyliczanie Elementów – aktywne zbieranie informacji, enumeracja usług, portów, wykrywanie systemów bezpieczeństwa IDS/UPS, FV),
e) Vulnerability Mapping (Mapowanie Podatności – poszukiwanie podatności w elementach znalezionych w poprzednich fazach),
f) Target Exploitation (Docelowa Eksploatacja – stworzenie wektora inicjalizującego atak, który ma na celu ominąć zabezpieczenia w celu naruszenia poufności, integralności oraz dostępności danych osobowych, przejęcia systemów, odcięcia systemu od sieci zewnętrznej),
g) Privilage Escalation (Eskalacja Uprawnień – zwiększenie uprawnień w przełamanym systemie i przeniesienie kontroli na kolejne usługi lub systemy),
h) Maintaining Access (Utrzymanie Dostępu – utrzymanie dostępu do skompromitowanego systemu, instalacja tylnych furtek, rootkit-ów,
i) Documentation & Reporting (Dokumentacja i Raportowanie – raport powinien zawierać informacje o znalezionych podatnościach oraz zauważonych problemach).

6.6. Obszary bezpieczeństwa

Zamawiający wymaga aby zakres weryfikacji bezpieczeństwa adresował ryzyka występujące w poniższej przedstawionych obszarach:
a) Uwierzytelnianie,
b) Zarządzanie sesją,
c) Kontrola dostępu,
d) Walidacja wejścia,
e) Kryptografia,
f) Obsługa błędów i logowanie,
g) Ochrona danych,
h) Bezpieczeństwo komunikacji,
i) Wyszukiwanie złośliwego kodu,
j) Logika biznesowa,
k) Weryfikacja zasobów i plików.

Wykonawca zobowiązany jest skierować do realizacji audytu zespół ekspertów o specjalizacjach wskazanych w tabeli nr 1 (poniżej), legitymujących się kwalifikacjami zawodowymi oraz doświadczeniem określonym w tabeli nr 2 (poniżej).

Tabela 1 - Wykaz osób po stronie Wykonawcy, które będą uczestniczyć w realizacji audytu KRK 2.0

L.p.	Specjalizacja	liczba specjalistów
1.	Kierownik projektu	1
2.	Analityk	1
3.	Specjalista ds. architektury systemów IT	1
4.	Audytor wiodący	1
5.	Specjalista ds. bezpieczeństwa systemów IT	3
6.	Specjalista ds. wdrożeń i utrzymania	1

„Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Społecznego Program Operacyjny Wiedza Edukacja Rozwój”

Dysponowanie odpowiednim potencjałem technicznym oraz osobami zdolnymi do wykonania zamówienia:

Potencjał techniczny

Zamawiający odstępuje od opisu sposobu oceny spełniania warunków w tym zakresie. Zamawiający dokona oceny spełniania warunków udziału w postępowaniu w tym zakresie na podstawie oświadczenia o spełnianiu warunków udziału w postępowaniu.

Potencjał kadrowy

Wykonawca musi wskazać osoby, które będą uczestniczyć w wykonywaniu zamówienia, legitymujące się doświadczeniem zawodowym odpowiednim do funkcji, jaka zostanie im powierzona.
Wykonawca przedstawi kandydatów na poniższe stanowiska, którzy spełniają następujące wymagania wymienione w tabeli nr 2:

Tabela nr 2 - Wymagane kwalifikacje zawodowe oraz wykształcenie

Stanowisko	Minimalna liczba personelu	Wymagane kwalifikacje zawodowe oraz wykształcenie	Minimalne doświadczenie
Specjalista ds. architektury systemów IT	1	1) Wykształcenie wyższe 2) Certyfikat TOGAF 9 Certified (level 2) lub równoważny	1) W ciągu ostatnich 5 lat pełnił rolę specjalisty ds. architektury systemów informatycznych w realizacji co najmniej 2 projektów (zakończonych i odebranych przez zlecającego) dotyczących budowy lub wdrożenia systemów informatycznych o wartości minimum 5 000 000,00 złotych brutto każdy, w których zajmował się językiem UML lub Archimate do modelowania architektury. 2) W ciągu ostatnich 5 lat w co najmniej 2 projektach (zakończonych i odebranych przez zlecającego) dotyczących budowy lub wdrożenia systemów informatycznych wykorzystywał metodykę służącą do wytworzenia i utrzymania architektury np. TOGAF lub równoważną. 3) W ciągu ostatnich 5 lat brał udział w co najmniej 2 projektach (zakończonych i odebranych przez zlecającego) dotyczących budowy lub wdrożenia systemów

„Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Społecznego Program Operacyjny Wiedza Edukacja Rozwój”

			informatycznych o wartości co najmniej 5 000 000,00 złotych brutto każdy, obejmujących swym zakresem budowę architektury systemu zorientowanego na usługi w architekturze wielowarstwowej o wysokiej wydajności i niezawodności oraz wykorzystującej bazę danych.
Specjalista ds. bezpieczeństwa systemów IT	3	1) Wykształcenie wyższe 2) Co najmniej 1 z poniższych certyfikatów: • Certyfikat CISM lub równoważny, • Certyfikat CISA, lub równoważny, • Certyfikat CISSP lub równoważny, • Certyfikat CASP lub równoważny.	W ciągu ostatnich 5 lat pełnił rolę specjalisty ds. bezpieczeństwa systemów informatycznych w realizacji co najmniej 2 projektów (zakończonych i odebranych przez zlecającego) dotyczących budowy lub wdrożenia systemów informatycznych o wartości minimum 5 000 000,00 złotych brutto każdy.
Specjalista ds. wdrożeń i utrzymania	1	Wykształcenie wyższe	W ciągu ostatnich 5 lat brał udział w co najmniej 2 projektach (zakończonych i odebranych przez zlecającego) dotyczących budowy lub wdrożenia systemów informatycznych o wartości minimum 5 000 000,00 złotych brutto każdy, w których zajmował się: a. wdrożeniem systemu informatycznego działającego w środowisku rozproszonym, o liczbie użytkowników końcowych nie mniejszej niż 1 000 osób. b. wdrożeniem polityki utrzymania ciągłości działania systemu informatycznego, obejmującego zagadnienia związane z synchronizowaniem i przełączaniem centrów przetwarzania danych, konfiguracją systemów backupu, systemów odtwarzania danych po awarii, budową systemów wysokiej niezawodności i dostępności. c. opisywaniem procesów utrzymaniowych, ról i odpowiedzialności oraz

„Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Społecznego Program Operacyjny Wiedza Edukacja Rozwój”

			zdefiniowaniem katalogu usług.
Analityk	1	Wykształcenie wyższe	W ciągu ostatnich 5 lat brał udział w co najmniej 2 projektach (zakończonych i odebranych przez zlecającego) dotyczących budowy lub wdrożenia systemów informatycznych o wartości minimum 5 000 000,00 złotych brutto każdy, opartych na modelu usługowym składających się z co najmniej 3 biznesowo niezależnych podsystemów, w których zajmował się modelowaniem procesów biznesowych i specyfikacją wymagań dla systemów informatycznych oraz projektowaniem w języku UML lub Archimate oraz modelowaniem przy użyciu narzędzia SPARX Enterprise Architect.
Kierownik projektu	1	Co najmniej 1 z poniższych certyfikatów: • Certyfikat Prince2 Foundation lub równoważny, • Certyfikat PMP (Project Management Professional) lub równoważny	1) W ciągu ostatnich 5 lat pełnił rolę kierownika projektu w realizacji co najmniej 2 projektów (zakończonych i odebranych przez zlecającego) dotyczących zaprojektowania systemów informatycznych o wartości minimum 5 000 000,00 złotych brutto każdy. 2) W ciągu ostatnich 5 lat pełnił rolę kierownika projektu w realizacji co najmniej 2 projektów dotyczących wdrożenia systemów informatycznych o wartości minimum 5 000 000,00 złotych brutto każdy.
Audytor wiodący	1	1) Wykształcenie wyższe 2) Co najmniej 1 z poniższych certyfikatów: • Certyfikat CISSP lub równoważny, • Certyfikat CISA lub równoważny, • Certyfikat CISM lub równoważny Oraz 3) Certyfikat audytora wiodącego normy PN-ISO/IEC/27001 lub równoważny	1) W ciągu ostatnich 5 lat brał udział w co najmniej 2 projektach (zakończonych i odebranych przez zlecającego) dotyczących budowy i wdrożenia systemów informatycznych o wartości minimum 5 000 000,00 złotych brutto każdy, w których z pełnił rolę eksperta ds. bezpieczeństwa 2) W ciągu ostatnich 5 lat uczestniczył we wdrożeniu wymagań dla systemu zarządzania bezpieczeństwem informacji.

„Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Społecznego Program Operacyjny Wiedza Edukacja Rozwój”

Wszystkie osoby wykonujące w ramach realizacji zamówienia wskazane przez Zamawiającego czynności, których wykonanie polega na wykonywaniu pracy w sposób określony w art. 22 § 1 ustawy Kodeks pracy muszą być zatrudnieni przez Wykonawcę na podstawie umowy o pracę.

Wszystkie osoby skierowane do realizacji zamówienia muszą posiadać aktualne odpowiednie poświadczenia bezpieczeństwa, o którym mowa w art. 21 ust. 1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz.1228) tj. poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych oznaczonych klauzulą „zastrzeżone" zgodnie z ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz.1228) wraz z aktualnym zaświadczeniem o odbyciu szkolenia z zakresu ochrony informacji niejawnych lub pisemne upoważnienie kierownika jednostki organizacyjnej, jeżeli nie posiadają one poświadczenia bezpieczeństwa, o którym mowa w art. 21 ust. 4 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych lub inne uprawnienia do ochrony informacji niejawnych o klauzuli równorzędnej do klauzuli „zastrzeżone" określone w dwustronnej umowie międzyrządowej o wzajemnej ochronie informacji niejawnych – dla osób wskazanych do realizacji zamówienia.

Jako certyfikat równoważny Zamawiający rozumie certyfikat analogiczny co do zakresu wskazanego certyfikatu, co jest rozumiane jako:

1) analogiczna dziedzina merytoryczna wynikająca z roli, której dotyczy certyfikat (np. zarządzenie bazami danych, kompetencje związane z zarządzaniem projektami, testowaniem, administracją bazami danych, programowanie, etc.),
2) analogiczny stopień poziomu kompetencji (np. podstawowy, zaawansowany, ekspert),
3) analogiczny poziom doświadczenia zawodowego wymagany dla otrzymania danego certyfikatu (np.: konieczność wykazania się uczestnictwem w określonej liczbie projektów w danej roli, etc.),
4) analogiczny okres i zakres szkolenia, jeśli uzyskanie certyfikatu uzależnione jest od odbycia szkolenia,
5) potwierdzenie certyfikatu egzaminem, jeśli uzyskanie certyfikatu wymaga złożenia egzaminu.

„Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Społecznego Program Operacyjny Wiedza Edukacja Rozwój"