Opis Przedmiotu Umowy

Dział A. Przedmiotem Umowy wykonawczej wykonywany będzie w następującym zakresie

1. Doradztwo, budowanie i weryfikacja architektury bezpieczeństwa rozwiązań informatycznych, a w szczególności:
    1) analiza ryzyka i modelowanie zagrożeń na podstawie koncepcji realizacji rozwiązania informatycznego,
    2) analiza wpływu badanego rozwiązania na inne rozwiązania pod względem bezpieczeństwa,
    3) analiza i definiowanie wymagań funkcjonalnych i niefunkcjonalnych w zakresie bezpieczeństwa,
    4) analiza i definiowanie architektury rozwiązań w zakresie bezpieczeństwa (koncepcja rozwiązania w zakresie bezpieczeństwa),
    5) analiza i wsparcie we wdrażaniu wewnętrznej architektury bezpieczeństwa Zamawiającego, w tym w zakresie architektury sieci, architektury rozwiązań zabezpieczających (w tym w warstwie sieci, bazy danych, na stacjach roboczych, w zakresie narzędzi do pozyskiwania, kolekcjonowania i zarządzania logami),
    6) dostarczenie informacji o rzeczywistym poziomie spełnienia wymagań w zakresie bezpieczeństwa oraz stosowanych zabezpieczeń,
    7) analiza założeń architektury bezpieczeństwa i zastosowanych zabezpieczeń w kontekście otoczenia prawnego i organizacyjnego.
2. lub Usługa z zakresu weryfikacji stanu bezpieczeństwa z zakresu określonego niżej:
    1) Prowadzenie testów bezpieczeństwa i testów penetracyjnych,
    2) Analiza infrastruktury Zamawiającego pod kątem bezpieczeństwa informacji i zapewnienia ciągłości działania,
    3) Analiza narzędzi i technik wykorzystywanych w procesie wytwórczym pod kątem bezpieczeństwa,
    4) Doradztwo w zakresie bezpiecznego utrzymania wdrażanych systemów,
    5) Weryfikacja systemu zapewnienia ciągłości działania w organizacji, w tym procedur utrzymaniowych, scenariuszy testowych,

6) Zadania związane z dochodzeniem po skutecznym ataku: definiowanie źródła ataku, zakresu, oceny strat oraz definiowanie działań naprawczych,
7) Testy bezpieczeństwa kodu źródłowego oprogramowania wytwarzanego przez Zamawiającego lub dla Zamawiającego - analiza statyczna kodu z wykorzystaniem narzędzi ze wsparciem manualnym w zakresie weryfikacji wykrytych nieprawidłowości,
8) Testy socjotechniczne.

3. Przy czym opis przedmiotu umowy wykonawczej każdorazowo będzie doprecyzowany w zaproszeniu do złożenia oferty w postępowaniu o udzielenie zamówienia wykonawczego (zwanego dalej „Zaproszeniem").Usługi wskazane w ust. 1 Wykonawca zobowiązany będzie realizować w zakresie określonym w Zaproszeniu co najmniej w obszarach wskazanych niżej:
   1) Architektury systemu i aplikacji – analiza, ocena i projektowanie, w tym:
      a) mechanizmów uwierzytelniania / autoryzacji,
      b) mechanizmów zarządzanie sesją,
      c) mechanizmów kontroli dostępu,
      d) mechanizmów walidacji wejść,
      e) mechanizmów kryptograficznych,
      f) obsługi błędów i logowania,
      g) ochrony danych,
      h) mechanizmów bezpieczeństwa komunikacji,
      i) mechanizmów bezpieczeństwa http,
      j) logiki biznesowej (wymagań),
      k) wykorzystania zasobów i plików w kontekście bezpieczeństwa,
      l) mechanizmów ochronnych dla danego serwera aplikacyjnego,
      m) obsługi błędów,
      n) wybranych elementów charakterystycznych dla serwera http,
      o) rozwiązania sprzętowego dla aplikacji pod katem bezpieczeństwa i wydajności,
      p) rozwiązań na poziomie architektury i ocena wpływu na wydajność systemu.
   2) Systemu operacyjnego - analiza, ocena, wytyczne i wsparcie w konfiguracji odnośnie: podziału przestrzeni dyskowej,
      a) udostępnione usługi sieciowe,
      b) utwardzenia – ocena i eliminacja zbędnych usług, konfiguracja,
      c) dodatkowe metody zabezpieczeń,
      d) zaimplementowanych systemów aktualizacji,
      e) zaimplementowanych systemów kopii zapasowych,
      f) zaimplementowanych systemów logowania zdarzeń,

g) mechanizmów administracji zdalnej,
h) przypisania użytkowników do właściwych grup,
i) uprawnień do najważniejszych zasobów (np. systemów plików).

3) Bazy danych – analiza, ocena, projektowanie, wsparcie, konfiguracja:
   a) udostępnianie bazy danych na poziomie sieciowym,
   b) systemów kopii zapasowych,
   c) zasad utwardzania bazy danych (np. logowanie zdarzeń, składowanie logów, partycjonowanie bazy, monitorowanie dostępu do obiektów, monitorowanie instrukcji języka SQL),
   d) architektury bazy danych (np. wykorzystanie mechanizmów autoryzacji oraz uwierzytelniania, segmentacja uprawnień, wykorzystywanie widoków, wykorzystywanie procedur składowych, przechowywanie oraz dostęp do danych wrażliwych, przechowywanie oraz dostęp do danych audytowych, szyfrowanie danych),
   e) komunikacji z klientami bazodanowymi (mechanizmy kryptograficzne, transfery danych).
4) Sieci – analiza, ocena, projektowanie, wsparcie, konfiguracja:
   a) LAN, w tym:
      i. podziału na strefy (wraz z wykorzystaniem urządzeń typu firewall oraz VLANów),
      ii. usług działających w wybranych podsieciach,
      iii. mechanizmów ochronnych w warstwie 2 i 3 modelu OSI,
   b) WLAN, w tym:
      i. Analiza konfiguracji urządzeń obsługujących sieć bezprzewodową,
      ii. Analiza poprawności zaprojektowania topologii sieci WiFi, także w relacji do LAN,

      ze szczególnym uwzględnieniem styku pomiędzy sieciami i obowiązujących zasad dostępu,
   c) dostępu do Internetu,
   d) topologii/architektury sieci,
   e) brzegu sieci,
   f) urządzeń bezpieczeństwa, w tym IPS, WAF, anty DDoS, sandbox (architektura, polityki, reguły, tuning),
   g) zasad utrzymania.

5) Środowiska użytkownika końcowego Zamawiającego – analiza, ocena, projektowanie, wsparcie, konfiguracja:
   a) stacja użytkownika końcowego – system operacyjny, polityki, narzędzia zabezpieczające stację,
   b) telefonia komórkowa i udostępnione usługi,
   c) poczta elektroniczna,
   d) Active Directory,
   e) usługi PKI,
6) Testów wydajności systemu – wykonawca wskaże maksymalną liczbę jednoczesnych użytkowników systemu przy określonych założeniach infrastrukturalnych, zbada skalowalność rozwiązania i wskaże konieczność zmian w zakresie infrastruktury lub składowych systemu w celu osiągnięcia maksymalnej wydajności systemu.

4. Usługi wskazane w ust. 2 Wykonawca zobowiązany będzie realizować w zakresie określonym w Zaproszeniu co najmniej w obszarach wskazanych niżej:
   1) Testów penetracyjnych i symulowania ataków na aplikację, w tym:
      a) Ataki semantyczne na adres URL,
      b) Ataki związane z ładowaniem plików,
      c) Ataki typu Cross-Site Scripting,
      d) Ataki typu Cross-Site Request Forgery,
      e) Ataki typu MITM (Man in the Middle),
      f) Podrabianie zarządzania formularza,
      g) Sfałszowanie żądania http,
      h) Ujawnienie danych przechowywanych w bazie,
      i) Trawersowanie katalogów,
      j) Ujawnianie kodu źródłowego,
      k) Przepełnienie bufora lub stosu,
      l) Wstrzykiwanie kodu wykonywalnego innych języków programowania.
      m) Badania:
         i. wykorzystania znanych podatności w celu uzyskania nieautoryzowanego dostępu,
         ii. możliwości podszywania się pod użytkowników i uzyskania nieautoryzowanego dostępu do systemu,

iii. możliwości podszywania się pod użytkowników uprzywilejowanych i uzyskanie dostępu do systemu,
iv. możliwości blokowania/umożliwienia dostępu do systemu wszystkim lub wybranym jej użytkownikom,
v. możliwości modyfikacji/usunięcia danych z systemu
vi. mechanizmów uwierzytelniania / autoryzacji,
vii. implementacji mechanizmów ochronnych dla danego serwera aplikacyjnego,
viii. obsługi błędów.

Przy czym Wykonawca przeprowadzi testy w trybie black-box (bez wiedzy na temat badanego obiektu) lub grey-box (przy założeniu dysponowania standardowymi kontami w badanym systemie) lub white-box (z nieograniczonym dostępem do systemu i pełną wiedzą o zasadach działania systemu).

2) testów bezpieczeństwa kodu źródłowego oprogramowania, w tym:
   a) wykonanie analizy statycznej kodu źródłowego wytwarzanego przez Zamawiającego lub dla Zamawiającego – w tym analiza statyczna kodu z zastosowaniem oprogramowania do tej analizy wykonującego analizę automatycznie, umożliwiającego również wykonywanie analizy przez osobę korzystająca z tego oprogramowania, w tym w zakresie weryfikacji wykrytych nieprawidłowości. Przy czym oprogramowanie to nie może stanowić SaaS (Software as a Service) oraz nie może wykorzystywać chmury obliczeniowej do swojego działania.
   b) analiza odbywać się będzie w środowisku Zamawiającego. Wykonawca musi dysponować oprogramowaniem zapewniającym wykonanie analizy, o którym mowa w lit. a). Zamawiający może zapewni stację roboczą, maszynę wirtualną oraz przestrzeń dyskową. Odpowiednio do wymagań określonych w Zaproszeniu Zamawiający może zastrzec dopuszczalność wykorzystywania połączenia/połączeń z: Internetem, zasobami dostępnymi w Internecie lub przez Internet lub dowolną inną siecią nienależąca do Zamawiającego.
   c) przedstawieniem wyników przeprowadzonych analiz zawierających wskazanie błędu/błędów i ich źródeł, oraz opisem sposobu usunięcia błędu/błędów z kodu lub ich zabezpieczenia
   d) w ramach testów Wykonawca zapewni wsparcie polegające na udzielaniu odpowiedzi na zadawane przez Zamawiającego pytania dotyczące wyników testów .

3) Badania bezpieczeństwa sieci, w tym:
   a) sieci LAN, podziału na strefy sieciowe (w tym wykorzystanie urządzeń typu firewall oraz VLAN),
   b) analiza usług działających w wybranych podsieciach,
   c) poszukiwanie podatności w kilku wybranych podsieciach,
   d) weryfikacja mechanizmów ochronnych w warstwie 2 i 3 modelu OSI,
   e) analiza brzegu sieci,
   f) weryfikacja dostępu do Internetu,
   g) analiza dostępu VPN,
   h) analiza wybranej komunikacji sieciowej,
   i) testy szczelności poszczególnych systemów bezpieczeństwa (WAF, firewall, IPS, sandbox itd.),
   j) skanowanie portów różnymi technikami,
   k) wykrywanie usług sieciowych udostępnionych w Internecie,
   l) próba detekcji wersji oraz typu oprogramowania systemowego zainstalowanego na urządzeniach dostępnych z Internetu,
   m) testowanie odporności wybranych usług wystawionych do sieci Internet na ataki Denied of Service co najmniej 2 różnymi metodami zaproponowanymi przez Wykonawcę,
   n) testy WLAN: wykrywanie obecności i zasięgu sieci bezprzewodowych, możliwości podsłuchu, przełamania użytych mechanizmów zabezpieczeń, zakłócania oraz zablokowania pracy, weryfikacja podatności, podszywania się pod autoryzowane urządzenia mobilne, wykrywanie nieautoryzowanych urządzeń sieciowych dołączonych do sieci wewnętrznej organizacji,
   o) weryfikacja zasad utrzymania sieci.
4) Badania systemów operacyjnych:
   a) weryfikację podziału przestrzeni dyskowej,
   b) weryfikację udostępnionych usług sieciowych,
   c) weryfikację zbędnych usług wraz ze wskazaniem ich podatności,
   d) weryfikację dodatkowych metod zabezpieczeń (np. systemy antywirusowe, itp.),
   e) weryfikację zaimplementowanych systemów aktualizacji,
   f) weryfikację zaimplementowanych systemów kopii zapasowych,
   g) weryfikację zaimplementowanych systemów logowania zdarzeń,
   h) weryfikację mechanizmów administracji zdalnej,
   i) weryfikację przypisania użytkowników do właściwych grup,
   j) weryfikację uprawnień do najważniejszych zasobów (np. systemów plików).

5) Badania baz danych:
    a) sposobu udostępniania bazy danych,
    b) zaimplementowanych systemów kopii zapasowych,
    c) implementacji podstawowych zasad hardeningowych bazy danych (np. logowanie zdarzeń, składowanie logów, partycjonowanie bazy, monitorowanie dostępu do obiektów, monitorowanie instrukcji języka SQL.),
    d) architektury bazy danych (np. wykorzystanie mechanizmów autoryzacji oraz uwierzytelniania, segmentacja uprawnień, wykorzystywanie widoków, wykorzystywanie procedur składowych, przechowywanie oraz dostęp do danych wrażliwych, przechowywanie oraz dostęp do danych audytowych, szyfrowanie danych),
    e) komunikacji z klientami bazodanowymi (mechanizmy kryptograficzne, transfery danych).

6) Testów socjotechnicznych
    a) Pozyskiwanie danych uwierzytelniających lub wskazanych wrażliwych danych w trakcie kontaktu z pracownikiem Zamawiającego,
    b) Ocena odporności Zamawiającego na otwieranie maili z nieznanego źródła, linków, załączników, mediów społecznościowych,
    c) Odporność na wykorzystanie narzędzi lub urządzeń pochodzących z nieznanego źródła (pendrive'y, myszki, klawiatury, nośników z narzędziami).

Dział B. Wymagania metodyczne

1. Wykonawca zobowiązany jest stosować co najmniej następujące metody i standardy odpowiednio do zakresu przedmiotu umowy wykonawczej:
    1) Wykorzystanie baz danych o znanych podatnościach i słabościach bezpieczeństwa:
    SAN Top 20 Critical Security Controls lub równoważne,
    Common Vulnerabilities and Exposures lub równoważne,
    WASC (Web Application Security Consortium) Threat Classifications lub równoważne,
    Przy czym za równoważne Zamawiający uzna, takie bazy danych, które stanowią aktualne źródło informacji o lukach bezpieczeństwa:
        - są publikowane i utrzymywane przez którekolwiek Państwo będące członkiem paktu NATO lub

- są stworzone i utrzymywane przez organizacje, niezależnie od ich form (komercyjna, non-profit w tym zorganizowana społeczność internetowa) których celem działalności jest zapewnienie bezpieczeństwa systemów i rozwiązań informatycznych, Zamawiający nie dopuszcza zastosowania baz, których wiarygodność została podważona w zakresie ich wykorzystania przez administracje publiczną tych Państw,

2) Odpowiednio do zakresu, zastosowanie list kontrolnych udostępnianych przez organizacje pracujące na rzecz bezpieczeństwa systemów IT do projektowania i oceny bezpieczeństwa systemów operacyjnych, baz danych, tj.:
   a) National Security Agency (NSA) lub równoważne,
   b) Center for Internet Security (CIS) lub równoważne,

   Przy czym za równoważne Zamawiający uzna, takie listy kontrolne, które opisują całość procesów audytu systemów oraz rozwiązań informatycznych w nie mniejszym zakresie, z nie mniejszą szczegółowością i systematyką wykonywania audytu.
3) Odpowiednio do zakresu, zastosowanie do testów bezpieczeństwa jednego ze standardów:
   a) OWASP (Open Web Application Security Project) ASVS 20141 lub równoważne,
   b) Open Source Security Testing Methodology Manual (OSSTMM) lub równoważne,
   c) Penetration Testing Execution Standard (PTES) lub równoważne,
   h) Przy czym za równoważne Zamawiający uzna standardy opisujące cały przebieg procesu testowania bezpieczeństwa systemów IT oraz obszary systemowe, które muszą podlegać weryfikacji, w nie mniejszym zakresie, z nie mniejszą szczegółowością i systematyką wykonywania audytu.

4) Wykonawca musi, odpowiednio do zakresu przedmiotu umowy wykonawczej, w ramach realizacji testów penetracyjnych wykonać wymienione niżej zadania:
   a) Ustalenie zakresu docelowego – ustalenie charakteru i zasięgu testów,
   b) Gromadzenie Informacji – pasywne zbieranie informacji na temat obiektu testów,
   c) Odkrywanie Celu – pół-pasywne zbieranie informacji, poznanie celów, identyfikacja podsieci, rodzaju architektury, systemów operacyjnych,
   d) Wyliczanie Elementów – aktywne zbieranie informacji, weryfikacja usług, portów, wykrywanie systemów bezpieczeństwa IDS/IPS, FW),
   e) Mapowanie Podatności – poszukiwanie podatności w elementach znalezionych w poprzednich fazach,
   f) Docelowe wykorzystanie podatności – 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) Eskalacja uprawnień – zwiększenie uprawnień w przełamanym systemie i przeniesienie kontroli na kolejne usługi lub systemy),

5) zapewnienie ciągłości uzyskanego dostępu wynikającego z przełamania zabezpieczeń, w tym weryfikacja możliwości zainstalowania oprogramowania typu „tylna furtka", lub rootkit-ów, lub innego złośliwego oprogramowania.
6) Dokumentacja i raportowanie – raport powinien zawierać informacje o znalezionych podatnościach oraz zauważonych problemach

Dział C. Wymagania dotyczące produktów

1. Wykonawca musi odpowiednio do wymagań określonych w Zaproszeniu wykonać Raporty zawierające:
   1) Opracowanie ogólne, zawierające streszczenie managerskie oraz informacje opisujące jakościowo wyniki usługi, przy czym raport nie może zawierać informacji, które zmniejszają bezpieczeństwo badanego obszaru lub systemu; dokument ma być wykonany w wykorzystywanych przez Zamawiającego formatach: edytowalnej prezentacji .pptx i pdf (przeszukiwalny). Szczegółowy wymagany zakres zostanie określony w Zaproszeniu
   2) Opracowanie szczegółowe, wykonane w wykorzystywanych przez Zamawiającego formatach .docx (edytowalny) i pdf (przeszukiwalny), które będzie zawierać:
      a) W części ogólnej:
         i. Streszczenie, w tym w zależności od zakresu Zamówienia szczegółowego ogólną opinię nt. bezpieczeństwa, zgodności z określonymi standardami i regulacjami wewnętrznymi i zewnętrznymi, zakres analizy lub koncepcji
         ii. Główne ustalenia, zalecenia lub założenia – odpowiednio do zakresu Zamówienia szczegółowego.
      b) W części szczegółowej:
         i. Obserwacje audytowe
         ii. Wyniki testów i ich interpretację
         iii. Listę wykrytych luk (w tym podatności) opatrzonych komentarzem audytora wraz z ich kwalifikacją w znaczeniu dla bezpieczeństwa (krytyczność)
         iv. Wnioski z audytu
         v. Zalecenia i rekomendacje

vi. Zakres czynności niezbędnych do weryfikacji i potwierdzenia luk (podatności) – o ile przedmiot audytu tego dotyczy

c) Zakres czynności niezbędnych do zaimplementowania rekomendacji poaudytowych

d) Przypadku konieczności wykonania zmian konfiguracyjnych lub instalacji uaktualnień/poprawek, Wykonawca przedstawi opis konfiguracji lub instalacji

e) Szczegółowy wymagany zakres zostanie określony w Zaproszeniu

2. Oczekiwana zawartość informacyjna raportu

1) Przeprowadzane badania i analizy muszą wskazać zagrożenia i ryzyka wynikające z:

a) Zastosowanych technologii i standardów zabezpieczeń

b) Błędów oprogramowania

c) Poprawnej konfiguracji komponentów systemowych i sieciowych

d) Istniejących / Wykrytych styków sieci o różnym charakterze (np. styku z siecią Internet, styku sieci systemów utrzymywanych / budowanych w MF z innymi sieciami,

e) Potencjalnych zagrożeń ze strony sieci wewnętrznej (LAN/WAN/WLAN) i zewnętrznej (Internet)

f) Zastosowanych rozwiązań na poziomie architektury i ich wpływu na wydajność systemu

g) Prawidłowości wyboru rozwiązania sprzętowego dla aplikacji pod katem bezpieczeństwa i wydajności,

2) Przeprowadzone badania i analizy jakości kodu muszą uwzględniać przede wszystkim:

a) Podatności systemów (wynikające z błędów w aplikacji i oprogramowania, z którymi aplikacja się komunikuje np. bazy danych, serwery proxy, etc) na znane ataki

b) Jakości kodu z punktu widzenia bezpieczeństwa aplikacji – weryfikacja, czy kod spełnia dobre wzorce projektowe oraz dobre praktyki przyjęte u Zamawiającego oraz w analogicznych systemach informatycznych

c) Jakości kodu z punktu widzenia wydajności aplikacji – zbadanie czy ilość przesyłanych/przetwarzanych danych jest optymalna przy przyjętym rozwiązaniu

Dział D. Wymagania dotyczące członków zespołu audytowego

1. Wykonawca zobowiązuje się świadczyć Przedmiot Umowy:

1) w zakresie określonym w Dział A ust.1 przez co najmniej jednego konsultanta ds. bezpieczeństwa:

a) posiadającego co najmniej 3 letnie doświadczenie w wykonywaniu audytów bezpieczeństwa z zakresu określonego w Dział A ust. 1

b) ponadto Zamawiający przyzna punkty jeśli wskazany w toku postępowania o udzielenie umowy wykonawczej ofercie, w której wykonawca wskaże do realizacji zamówienia wykonawczego konsultanta ds. bezpieczeństwa posiadającego wiedzę potwierdzoną certyfikatem CISA Certified Information Systems Auditor - za równoważny Zamawiający uzna certyfikat wystawionym przez niezależny od Wykonawcy podmiot, specjalizujący się w certyfikacji wiedzy z obszaru co najmniej bezpieczeństwa informatycznego potwierdzający posiadanie wiedzy na nie niższym poziomie, z co najmniej tego samego zakresu,

c) ponadto Zamawiający przyzna punkty jeśli wskazany w toku postępowania o udzielenie umowy wykonawczej ofercie, w której wykonawca wskaże do realizacji zamówienia wykonawczego konsultanta ds. bezpieczeństwa posiadającego wiedzę potwierdzoną certyfikatem Certified Information Security Professional (CISSP) lub równoważnego - za równoważny Zamawiający uzna certyfikat wystawionym przez niezależny od Wykonawcy podmiot, specjalizujący się w certyfikacji wiedzy z obszaru co najmniej bezpieczeństwa informatycznego potwierdzający posiadanie wiedzy na nie niższym poziomie, z co najmniej tego samego zakresu,

d) ponadto Zamawiający przyzna punkty ofercie jeśli wskazany w toku postępowania o udzielenie umowy wykonawczej ofercie, w której wykonawca wskaże do realizacji zamówienia wykonawczego konsultanta ds. bezpieczeństwa posiadającego powyżej 3 lat doświadczenia w wykonywaniu audytu z zakresu określonego w Dział A ust.1.

2) W zakresie określonym w Dział A ust. 2 przez co najmniej jednego konsultanta ds. audytu stanu bezpieczeństwa:

a) posiadającego co najmniej 3 letnie doświadczenie w wykonywaniu audytów bezpieczeństwa z zakresu określonego w Dział A ust. 2

b) ponadto Zamawiający przyzna punkty jeśli wskazany w toku postępowania o udzielenie umowy wykonawczej ofercie, w której wykonawca wskaże do realizacji zamówienia wykonawczego ds. audytu stanu bezpieczeństwa posiadającego wiedzę potwierdzoną certyfikatem Licensed Penetration Tester (LPT) - za równoważny Zamawiający uzna certyfikat wystawionym przez niezależny od Wykonawcy podmiot, specjalizujący się w certyfikacji wiedzy z obszaru co najmniej bezpieczeństwa informatycznego potwierdzający posiadanie wiedzy na nie niższym poziomie, z co najmniej tego samego zakresu,

c) ponadto Zamawiający przyzna punkty jeśli wskazany w toku postępowania o udzielenie umowy wykonawczej ofercie, w której wykonawca wskaże do realizacji zamówienia wykonawczego ds. audytu stanu bezpieczeństwa posiadającego wiedzę potwierdzoną

certyfikatem Certified Expert Penetration Tester (CEPT) - za równoważny Zamawiający uzna certyfikat wystawionym przez niezależny od Wykonawcy podmiot, specjalizujący się w certyfikacji wiedzy z obszaru co najmniej bezpieczeństwa informatycznego potwierdzający posiadanie wiedzy na nie niższym poziomie, z co najmniej tego samego zakresu,

d) Zamawiający przyzna punkty ofercie jeśli wskazany w toku postępowania o udzielenie umowy wykonawczej ofercie, w której wykonawca wskaże do realizacji zamówienia wykonawczego konsultanta ds. audytu stanu bezpieczeństwa posiadającego powyżej 3 lat doświadczenia w wykonywaniu audytu z zakresu określonego w Dział A ust.2.

3) Liczby punktów i wagi kryteriów zostaną każdorazowo określone w Zaproszeniu.

2. Osoby wchodzące w skład zespołu audytowego muszą być bezstronne i niezależne. Przy czym za bezstronne i niezależne Strony rozumieją osoby, które w ciągu ostatnich trzech lat przed dniem wszczęcia postępowania o udzielenie zamówienia wykonawczego nie uczestniczyły:
   1) ani w zaprojektowaniu,
   2) ani w wykonaniu
   3) ani w uruchomieniu
   4) ani w eksploatacji

   systemu lub innego rozwiązania informatycznego, którego przedmiot umowy wykonawczej dotyczy