Warszawa, dnia 25 stycznia 2017 roku

**Dotyczy: Wyjaśnień do treści zapytania ofertowego w ramach postępowania na „Przeprowadzenie audytu informatycznego z zakresu inwentaryzacji zasobów sprzętowych i programowych systemu informatycznego oraz audyt bezpieczeństwa systemu informatycznego i bezpieczeństwa przetwarzania informacji”.**

**Wyjaśnienia do zapytania ofertowego**

**Zamawiający – Centrum Projektów Polska Cyfrowa – informuje, że w przedmiotowym postępowaniu Wykonawcy zwrócili się do Zamawiającego z wnioskami o wyjaśnienie treści zapytania ofertowego. W związku z powyższym, Zamawiający udzielił poniższych odpowiedzi:**

**Pytanie nr 1:**

Jaka jest szacowana liczba adresów IP (stacji roboczych i serwerów), które będą objęte testem penetracyjnym?

**Odpowiedź nr 1:**

**Szacowana liczba stacji roboczych i serwerów wynosi do 230.**

**Pytanie nr 2:**

Jaką ilość adresów IP ma obejmować zadanie polegające na weryfikacji poprawności aktualizacji systemu operacyjnego, definicji baz sygnatur wirusów?

**Odpowiedź nr 2:**

**Zadanie polegające na weryfikacji poprawności aktualizacji systemu operacyjnego ma obejmować do 230 stacji roboczych i serwerów.**

**Pytanie nr 3:**

Czy wszystkie urządzenia objęte audytem znajdują się w siedzibie Klienta, czy może u dostawców określonych usług?

**Odpowiedź nr 3:**

Dwa serwery znajduje się u dostawcy usługi, natomiast wszystkie pozostałe urządzenia znajdują się w siedzibie Zamawiającego.

**Pytanie nr 4:**

Jakie serwisy internetowe będą podlegały testom bezpieczeństwa?

**Odpowiedź nr 4:**

**W pytaniu nie sprecyzowano o jakie kategorie serwisów chodzi, w związku z tym zamawiający nie jest w stanie określić odpowiedzi w tym zakresie.**

**Pytanie nr 5:**

Czy testy sieci wewnętrznej mogą być przeprowadzone z komputerów Wykonawcy, czy może Zamawiający udostępni dedykowaną stację roboczą?

**Odpowiedź nr 5:**

Testy mogą być przeprowadzone z komputerów Wykonawcy po ich weryfikacji przez pracowników IT Zamawiającego.

**Pytanie 6:**

Czy testami penetracyjnymi ma być objęta wyłącznie infrastruktura czy również systemy użytkowane przez Zamawiającego np. systemy użytkowe, biurowe, poczta elektroniczna, dedykowane?

**Odpowiedź nr 6:**

Testami penetracyjnymi ma być objęta infrastruktura i systemy użytkowe.

**Pytanie nr 7:**

Jeśli testami penetracyjnymi objęte mają być również systemy/aplikacje - prosimy o informację jaka jest ilość aplikacji/serwerów i w jakiej technologii zostały stworzone?

**Odpowiedź nr 7:**

Do 12 serwerów fizycznych w architekturze Intel, do 30 maszyn wirtualnych Windows / Linux. **W pytaniu nie sprecyzowano o jakie aplikacje chodzi w związku z tym zamawiający nie jest w stanie określić odpowiedzi w tym zakresie.**

**Pytanie nr 8:**

Jeśli testami penetracyjnymi objęte mają być również systemy/aplikacje - jakie funkcje realizują aplikacje/systemy podlegające testom?

**Odpowiedź nr 8:**

**Posiadane aplikacje/systemy podlegające testom penetracyjnym posiadają standardowe funkcje właściwe dla ich przeznaczenia.**

**Pytanie nr 9:**

Jeśli testami penetracyjnymi objęte mają być również systemy/aplikacje - jaka jest szacunkowa liczba stron/formularzy dla każdej z aplikacji/systemu?

**Odpowiedź nr 9:**

**W pytaniu nie sprecyzowano o jakie strony/formularze chodzi, w związku z tym Zamawiający nie jest w stanie określić odpowiedzi w tym zakresie.**

**Pytanie nr 10:**

Jeśli testami penetracyjnymi objęte mają być również systemy/aplikacje - czy aplikacje/systemy posiadają mechanizm logowania? Jeśli tak, prosimy podanie ile różnych profili użytkownika obsługuje i czy wszystkie będą podlegały testom?

**Odpowiedź nr 10:**

Część aplikacji i systemów posiada mechanizm logowania. Wszystkie elementy badanych systemów mają podlegać testom.

**Pytanie nr 11:**

Jeśli testami penetracyjnymi objęte mają być również systemy/aplikacje - prosimy o informację czy wykorzystywane są w nich mechanizmy płatności?

**Odpowiedź nr 11:**

Systemy i aplikacje podlegające audytowi nie mają wbudowanego mechanizmu płatności. Kilka aplikacji pośredniczy w realizacji płatności.

**Pytanie nr 12:**

Jeśli testami penetracyjnymi objęte mają być również systemy/aplikacje - prosimy o informację z jakich protokołów komunikacyjnych korzystają określone aplikacje oraz jakie API udostępniają?

**Odpowiedź nr 12:**

**Posiadane aplikacje korzystają ze standardowych protokołów komunikacji w większości TCP/IP, natomiast udostępniają API dostarczone przez producentów tych systemów.**

**Pytanie nr 13:**

Jeśli testami penetracyjnymi objęte mają być również systemy/aplikacje - czy są one zainstalowane na serwerach fizycznych, czy też wirtualnych?

**Odpowiedź nr 13:**

Systemy podlegające audytowi są zainstalowane na maszynach fizycznych i na maszynach wirtualnych.

**Pytanie nr 14:**

Czy Zamawiający dopuszcza instalację agentów na stacjach roboczych wykonywaną przez swój personel IT celem zebrania danych dla celów inwentaryzacji, czy może wszystkie prace mają być wykonane przez Zamawiającego?

**Odpowiedź nr 14:**

Wszystkie prace mają być wykonane przez Zamawiającego. Zamawiający nie dopuszcza instalacji agentów na stacjach roboczych.

**Pytanie nr 15:**

Pod jakim kątem ma zostać przeprowadzona weryfikacja kwalifikacji, odbytych szkoleń, zakresu uprawnień i odpowiedzialności pracowników pionów IT?

**Odpowiedź nr 15:**

Weryfikacja kwalifikacji, odbytych szkoleń, zakresu uprawnień i odpowiedzialności pracowników pionów IT ma zostać przeprowadzona pod kątem organizacyjnym.

**Pytanie nr 16:**

Czy Wykonawca może realizować badanie zgodności poszczególnych procesów na próbie, czy ma zostać poddana badaniu cała **populacja**? Prosimy o doprecyzowanie w każdym z elementów badania?

**Odpowiedź nr 16:**

Badaniu zgodności poszczególnych procesów ma zostać poddana cała populacja.

**Pytanie nr 17:**

W jaki sposób Zamawiający interpretuje następujące zapisy:

•Inwentaryzacja sprzętu działającego w infrastrukturze informatycznej.

•Inwentaryzacja usług sieciowych z opisem wzajemnych zależności tych usług.

•Inwentaryzacja baz danych ze wskazaniem aplikacji korzystających z tych baz.

•Inwentaryzacja używanych aplikacji ze wskazaniem administratorów tych aplikacji.

•Zarządzanie aplikacjami (wykaz licencji i aplikacji, zasady dostępu do aplikacji. monitorowanie instalacji oprogramowania oraz osoby nadzorujące).

**Odpowiedź nr 17:**

Zamawiający interpretuje ww. zapisy dosłownie, zgodnie z definicją słowa "inwentaryzacja".

**Pytanie nr 18:**

Czy w ramach w/w należy zinwentaryzować 100% wskazanych zasobów? W jakiej formie Zamawiający oczekuje przedstawienia rezultatów w/w pracy?

**Odpowiedź nr 18:**

Tak, należy zinwentaryzować 100% wskazanych zasobów. Rezultaty pracy powinny zostać przekazane w zrozumiałej, przejrzystej i czytelnej formie, elektronicznie i jako wydruki.

**Pytanie nr 19:**

Czy w ramach zapisu: „Przygotowaną przez Wykonawcę aktualizację i uzupełnienie zestawu dokumentów Polityki Bezpieczeństwa zgodną z aktualnie obowiązującymi aktami prawnymi. Dokumenty te Wykonawca przygotuje w porozumieniu z Zamawiającym, uwzględniając specyfikę działania i organizację pracy Zamawiającego.” Zamawiający oczekuje od Wykonawcy wykonania pełnej aktualizacji i sporządzenia brakującej dokumentacji? Jeśli tak to w odniesieniu do jakich wymagań (prosimy o wskazanie przepisów, norm, standardów, wytycznych).

**Odpowiedź nr 19:**

Zamawiający zmienia treść cytowanego fragmentu nadając mu następujące brzmienie:

„Przygotowaną przez Wykonawcę listę proponowanych nowelizacji wewnętrznych regulacji Zamawiającego w zakresie przetwarzania danych w systemach informatycznych, w szczególności: Polityki Bezpieczeństwa Informacji i Instrukcji Zarządzania Systemem Informatycznym. Propozycje te Wykonawca przygotuje w porozumieniu z Zamawiającym, uwzględniając specyfikę działania i organizację pracy Zamawiającego. Wykonawca nie jest zobowiązany do przygotowania nowych tekstów jednolitych regulacji wewnętrznych Zamawiającego ww. zakresie”.

**Pytanie nr 20:**

Prosimy o przesłanie treści klauzuli poufności, którą należy podpisać przed rozpoczęciem audytu.

**Odpowiedź nr 20:**

W opublikowanej, zaktualizowanej wersji zapytania ofertowego, w załączniku nr 5 znajduje się treść przedmiotowej klauzuli.

**Pytanie nr 21:**

Odnośnie pkt. III. 1 Szczegółowy zakres przetwarzania i ochrony danych osobowych:

**a.** Prosimy o wyspecyfikowanie aktów prawnych, o których mowa w pkt. 1.

**Odpowiedź dotycząca lit. a.:**

Zamawiający dokonał zmiany treści pkt. 1 w rozdziale III. Zmieniona oraz aktualna treść opisu przedmiotu zamówienia w tym zakresie została opublikowana na portalu Baza Konkurencyjności oraz na stronie internetowej Zamawiającego.

**b.** Prosimy o informację jakie Zamawiający posiada dokumenty w zakresie przetwarzania danych osobowych i jaka jest ich objętość.

**Odpowiedź dotycząca lit. b.:**

Zamawiający posiada w tym zakresie dokument Polityka Bezpieczeństwa Informacji z procedurami i wzorami (liczy on 104 strony).

**c.** Prosimy o informację ile jest zbiorów danych osobowych.

**Odpowiedź dotycząca lit. c.:**

Zamawiający dokonał zmiany treści pkt. 1 w rozdziale III. Zmieniona oraz aktualna treść opisu przedmiotu zamówienia w tym zakresie została opublikowana na portalu Baza Konkurencyjności oraz na stronie internetowej Zamawiającego.

**d.** Prosimy o informację ile osób zajmuje się przetwarzaniem danych osobowych.

**Odpowiedź dotycząca lit. d.:**

Przetwarzaniem danych osobowych zajmuje się do 180 osób.

**e.** Prosimy o informację ile osób pracuje w Pionie IT.

**Odpowiedź dotycząca lit. e.:**

Osoby zajmujące się IT pracują w Biurze Administracyjnym CPPC. Na chwilę obecną są to dwie osoby.

**f.** Prosimy o informację ile jest systemów IT, dla których wykonywane są kopie bezpieczeństwa.

**Odpowiedź dotycząca lit. f.:**

Kopie bezpieczeństwa wykonywane są dla grupy do 30 systemów.

**g.** Prosimy o informację jakie Zamawiający posiada dokumenty w zakresie ciągłości działania i jaka jest ich objętość.

**Odpowiedź dotycząca lit. g.:**

Zamawiający nie posiada takich dokumentów.

**h.** Prosimy o informację ile jest systemów IT oraz użytkowników tych systemów.

**Odpowiedź dotycząca lit. h.:**

Zamawiający posiada do 180 użytkowników.

**Pytanie nr 22:**

Odnośnie pkt. III. 2. Szczegółowy zakres bezpieczeństwa systemów informatycznych:

**a.** Prosimy o informację o jaki system informatyczny chodzi w pkt. 3a „przeprowadzenie testów penetracyjnych wykonanych ze stacji roboczej podłączonej do systemu informatycznego z zewnątrz mających na celu zidentyfikowanie podatności na
włamanie”.

**Odpowiedź dotycząca lit. a.:**

Chodzi o badanie podatności infrastruktury i systemów Zamawiającego na ataki z sieci innej niż sieć lokalna zamawiającego.

**b.** Prosimy o informację o jaki system informatyczny chodzi w pkt. 3b „przeprowadzenie testów penetracyjnych wykonanych ze stacji roboczej podłączonej do wewnętrznego systemu informatycznego w celu zidentyfikowania możliwości przeprowadzenia włamania z wewnątrz sieci Zamawiającego”.

**Odpowiedź dotycząca lit. b.:**

Chodzi o badanie podatności infrastruktury i systemów Zamawiającego na ataki z sieci lokalnej zamawiającego.

**c.** Ile jest IP adresów dostępnych z zewnątrz?

**Odpowiedź dotycząca lit. c.:**

**Posiadany zakres adresacji umożliwia użycie** do 36 adresów **publicznych.**

**d.** Ile jest aktywnych adresów IP wewnątrz sieci?

**Odpowiedź dotycząca lit. d.:**

**Wewnątrz sieci jest do 230 aktywnych adresów IP.**

**e.** Ile jest serwisów internetowych, które mają być objęte audytem?

**Odpowiedź dotycząca lit. e.:**

**W pytaniu nie sprecyzowano o jakie serwisy internetowe chodzi, w związku z tym Zamawiający nie jest w stanie określić odpowiedzi w tym zakresie.**

**f.** Prosimy o przesłanie linków do serwisów internetowych, które mają być objęte audytem.

**Odpowiedź dotycząca lit. f.:**

Niniejsze informacje mogą zostać przekazane Wykonawcy wybranemu w wyniku przedmiotowego zamówienia po złożeniu przez niego oświadczenia określonego w załączniku nr 5 do zapytania ofertowego.

**g.** Prosimy o doprecyzowanie pkt. „Weryfikacja podatności hostów na możliwość uzyskania nieautoryzowanego dostępu do zasobów plikowych.”

**Odpowiedź dotycząca lit. g.:**

Chodzi o badanie możliwości uzyskania nieautoryzowanego dostępu do zasobów plikowych za pośrednictwem hostów Zamawiającego **lub urządzeń nie będących własnością Zamawiającego** w sieci lokalnej Zamawiającego.

**h.** Prosimy o doprecyzowanie pkt. „Weryfikacja podatności hostów na możliwość uzyskania nieautoryzowanego zdalnego (przez WWW) dostępu do paneli administracyjnych.”

**Odpowiedź dotycząca lit. h.:**

Chodzi o badanie możliwości uzyskania nieautoryzowanego dostępu do paneli administracyjnych serwisów Zamawiającego udostępnionych w sieci Internet.

**i.** O jakie zabezpieczenia logiczne  chodzi w pkt. „Istniejące zabezpieczenia logiczne na styku sieci lokalnej z Internetem.”

**Odpowiedź dotycząca lit. i.:**

Chodzi o wykorzystywane systemy zabezpieczenia styku sieci lokalnej Zamawiającego z siecią Internet.

**j.** Ilu systemów i jakich (Windows, Linux, Unix, itp.) dotyczy pkt „Weryfikacja poprawności aktualizacji systemu informatycznego.”?

**Odpowiedź dotycząca lit. j.:**

Punkt „Weryfikacja poprawności aktualizacji systemu informatycznego” dotyczy do 30 systemów Windows i Linux.

**k.** Ile jest serwerowni?

**Odpowiedź dotycząca lit. k.:**

Zamawiający posiada 4 serwerownie.

**l.** Czy wszystkie serwerownie są zlokalizowane w Warszawie?

**Odpowiedź dotycząca lit. l.:**

Tak, wszystkie serwerownie są zlokalizowane w Warszawie.

**m.** Ile urządzeń sieciowych i jakich (routery, switche) mają być objęte pkt. „Konfiguracja urządzeń sieciowych.”?

**Odpowiedź dotycząca lit. m.:**

**Punktem „Konfiguracja urządzeń sieciowych” ma być objęte do 20 urządzeń.**

**n.**  Prosimy o informację co ma być wynikiem realizacji pkt. „Określenie istotnych danych i istotnych zasobów informatycznych.”?

**Odpowiedź dotycząca lit. n.:**

Określenie zasobów krytycznych, których awaria **lub brak dostępu** uniemożliwia **poprawne** działanie któregoś z systemów informatycznych **lub prowadzenie działalności** Zamawiającego.

**Pytanie nr 23:**

Odnośnie pkt. III.3 Szczegółowy zakres zasobów informatycznych:

**a.** Prosimy o informację co ma być wynikiem realizacji pkt. „Ewidencja oprogramowania dopuszczonego do użytkowania”.

**Odpowiedź dotycząca lit. a.:**

Wynikiem realizacji punktu „Ewidencja oprogramowania dopuszczonego do użytkowania” ma być spis oprogramowania z jego opisem oraz wskazaniem najważniejszych cech: funkcji, licencji, wymagań, itp.

**b.** Prosimy o informację co ma być wynikiem realizacji pkt. „Ewidencja prowadzonych kontroli w zakresie legalności oprogramowania instalowanego na stacjach roboczych”.

**Odpowiedź dotycząca lit. b.:**

Wynikiem realizacji punktu „Ewidencja prowadzonych kontroli w zakresie legalności oprogramowania instalowanego na stacjach roboczych” ma być spis lub lista wykonywanych kontroli z wyszczególnieniem ich zakresu.

**c.** Prosimy o informację co ma być wynikiem realizacji pkt. „Inwentaryzacja sprzętu działającego w infrastrukturze informatycznej”.

**Odpowiedź dotycząca lit. c.:**

Wynikiem ma być szczegółowy spis sprzętu zgodnie z definicją słowa "inwentaryzacja" **ze wskazaniem najważniejszych cech: funkcji, licencji, wymagań, itp.**

**d.** Prosimy o informację co ma być wynikiem realizacji pkt. „Inwentaryzacja usług sieciowych z opisem wzajemnych zależności tych usług”.

**Odpowiedź dotycząca lit. d.:**

Wynikiem ma być szczegółowy spis usług sieciowych z wyszczególnieniem **ich najważniejszych funkcji i parametrów technicznych** oraz wzajemnych zależności **między zidentyfikowanymi usługami**.

**e.** Prosimy o informację co ma być wynikiem realizacji pkt. „Inwentaryzacja baz danych ze wskazaniem aplikacji korzystających z tych baz”.

**Odpowiedź dotycząca lit. e.:**

Wynikiem realizacji punktu „Inwentaryzacja baz danych ze wskazaniem aplikacji korzystających z tych baz” ma być szczegółowy spis baz danych ze wskazaniem ich nazw oraz wskazaniem aplikacji korzystających z tych baz zgodnie z definicją słowa "inwentaryzacja".

**f.** Prosimy o informację co ma być wynikiem realizacji pkt. „Inwentaryzacja używanych aplikacji ze wskazaniem administratorów tych aplikacji”.

**Odpowiedź dotycząca lit. f.:**

Wynikiem ma być szczegółowy spis aplikacji działających w systemach Zamawiającego ze wskazaniem osób administrujących merytorycznie tymi aplikacjami **ze wskazaniem najważniejszych cech: funkcji, licencji, wymagań, itp.** zgodnie z definicją słowa "Inwentaryzacja".

**g.** Prosimy o informację co ma być wynikiem realizacji pkt. „Zarządzanie aplikacjami (wykaz licencji i aplikacji, zasady dostępu do aplikacji. monitorowanie instalacji oprogramowania oraz osoby nadzorujące)”.

**Odpowiedź dotycząca lit. g.:**

Wynikiem realizacji punktu „Zarządzanie aplikacjami (wykaz licencji i aplikacji, zasady dostępu do aplikacji. monitorowanie instalacji oprogramowania oraz osoby nadzorujące)” ma być szczegółowy spis aplikacji działających w systemach Zamawiającego  oraz opis sposobu zarządzania tymi aplikacjami.

**Pytanie nr 24:**

Odnośnie pkt. IV Wymagane rezultaty audytu:

**a.** Prosimy o informację co ma być wynikiem realizacji pkt. „Zobrazowanie połączeń logicznych, sieci lokalnej oraz styku sieci lokalnej z siecią Internet, z uwzględnieniem wszystkich urządzeń ich adresacji i działających usług, używanych portów i protokołów.”

**Odpowiedź dotycząca lit. a.:**

Wynikiem ma być graficzny schemat sieci logicznej z uwzględnieniem wszystkich urządzeń, ich adresacji i działających usług, używanych portów i protokołów. **~~oraz opis konfiguracji wszystkich urządzeń ich adresacji i działających usług, używanych portów i protokołów.~~**

**b.** Prosimy o informację w jakiej formie ma być przedstawiony wyniku pkt. „Szczegółową, elektroniczną inwentaryzację sprzętu i oprogramowania działającego w infrastrukturze informatycznej Zamawiającego”.

**Odpowiedź dotycząca lit. b.:**

Wynik realizacji punktu „Szczegółowa, elektroniczna inwentaryzację sprzętu i oprogramowania działającego w infrastrukturze informatycznej Zamawiającego” ma być przedstawiony w formie elektronicznej, tj. edytowalnych plików oraz wydruku.

**Pytanie nr 25:**

Odnośnie pkt. „2. Dysponowanie osobami zdolnymi do wykonania zamówienia:” Czy konsultant powinien posiadać dwa certyfikaty tj. ISO 27001 oraz ISO 22301 czy jeden z nich?

**Odpowiedź nr 25:**

Przynajmniej jeden z ekspertów ds. audytu IT i bezpieczeństwa powinien posiadać oba certyfikaty.  Pozostali mogą posiadać jeden z dwóch certyfikatów.

**Pytanie nr 26:**

Ile jest zbiorów danych osobowych opisanych w dokumentacji ochrony danych osobowych, ile z nich zostało zarejestrowanych w GIODO?

**Odpowiedź nr 26:**

Zamawiający dokonał zmiany treści pkt. 1 w rozdziale III. Zmieniona oraz aktualna treść opisu przedmiotu zamówienia w tym zakresie została opublikowana na portalu Baza Konkurencyjności oraz na stronie internetowej Zamawiającego.

**Pytanie nr 27:**

Czy następuje przekazywanie danych za granicę?

**Odpowiedź nr 27:**

Nie, nie następuje przekazywanie danych za granicę.

**Pytanie nr 28:**

Ile jest systemów teleinformatycznych przetwarzających dane osobowe?

**Odpowiedź nr 28:**

Dane osobowe przetwarza do 30 systemów.

**Pytanie nr 29:**

Zakładając, że Zamawiający ma więcej, niż jedną lokalizację – czy są one powtarzalne pod względem infrastruktury teleinformatycznej, zabezpieczeń fizycznych i technicznych, czy też każdą z lokalizacji należy audytować niezależnie?

**Odpowiedź nr 29:**

Zamawiający ma jedną lokalizację.

**Pytanie nr 30:**

Ile jest umów przetwarzania danych?

**Odpowiedź nr 30:**

W pytaniu nie sprecyzowano o jakie umowy chodzi (Beneficjenci, Wykonawcy), w związku z tym Zamawiający nie jest w stanie określić odpowiedzi w tym zakresie.

**Pytanie nr 31:**

Ilu pracowników Zamawiającego posiada upoważnienia do przetwarzania danych osobowych?

**Odpowiedź nr 31:**

W pytaniu nie sprecyzowano o jakie upoważnienia (do jakich celów: kadry, nabór ekspertów) chodzi, w związku z tym Zamawiający nie jest w stanie określić odpowiedzi w tym zakresie.

**Pytanie nr 32:**

Ile stacji roboczych posiada Zamawiający?

**Odpowiedź nr 32:**

Zamawiający posiada do 180 stacji roboczych.

**Pytanie nr 33:**

Ile serwerów (fizycznych i wirtualnych) posiada Zamawiający?

**Odpowiedź nr 33:**

Zamawiający posiada do 30 serwerów.

**Pytanie nr 34:**

Czy wszystkie serwisy internetowe wymagające badania znajdują się w domenie cppc.gov.pl? Jeżeli nie to prosimy o wskazanie serwisów poza domeną.

**Odpowiedź nr 34:**

Domeny Zamawiającego to: cppc.gov.pl, wwpe.gov.pl.

**Pytanie nr 35:**

Czy Zamawiający posiada lokalizację poza Warszawą? Jeżeli tak to gdzie?

**Odpowiedź nr 35:**

Zamawiający nie posiada lokalizacji poza Warszawą.

**Pytanie nr 36:**

Jakie urządzenia sieciowe (jakiego producenta) posiada Zamawiający?

**Odpowiedź nr 36:**

Zamawiający posiada następujące urządzenia sieciowe: przełączniki, routery, UTM, AP. CISCO, FortiNet, DELL, HP, Edimax.

**Pytanie nr 37:**

Ile serwerów jest do przetestowania?

**Odpowiedź nr 37:**

Przetestowaniu podlegać będzie do 30 serwerów.

**Pytanie nr 38:**

Ile aplikacji jest do przetestowania?

**Odpowiedź nr 38:**

**W pytaniu nie sprecyzowano o jakie aplikacje chodzi, w związku z tym Zamawiający nie jest w stanie określić odpowiedzi w tym zakresie.**

**Pytanie nr 39:**

Ile stacji końcowych jest do przetestowania?

**Odpowiedź nr 39:**

Przetestowaniu podlegać będzie do 180 stacji roboczych.

**Pytanie nr 40:**

Jaka jest szacowana ilość aplikacji uruchomionych na stacjach klienckich?

**Odpowiedź nr 40:**

**W pytaniu nie sprecyzowano o jakie aplikacje chodzi, w związku z tym Zamawiający nie jest w stanie określić odpowiedzi w tym zakresie.**

**Pytanie nr 41:**

Jaka jest ilość serwisów internetowych wymagających przetestowania?

**Odpowiedź nr 41:**

**W pytaniu nie sprecyzowano o jakie serwisy internetowe chodzi, w związku z tym Zamawiający nie jest w stanie określić odpowiedzi w tym zakresie.**

**Pytanie nr 42:**

Jaka jest ilość hostów wymagających przetestowania?

**Odpowiedź nr 42:**

**Przetestowaniu podlegać będzie do 230 stacji roboczych i serwerów.**

**Pytanie nr 43:**

Warunki udziału w postępowaniu "Zamawiający uzna, że Wykonawca spełnia warunek wiedzy i doświadczenia, gdy Wykonawca w okresie ostatnich trzech lat przed upływem terminu składania ofert (a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie) wykonał lub wykonuje co najmniej dwie usługi odpowiadające swoim rodzajem usługom stanowiącym przedmiot zamówienia, każda o wartości nie mniejszej niż 30.000,00 złotych brutto (słownie złotych brutto: trzydzieści tysięcy złotych)."

Mamy nadzieję, że Wykonawca prawidłowo rozumie sformułowanie "odpowiadające rodzajem" tj. jako realizacje projektów o takim samym i podobnym zakresie jak przedmiot zapytania?

**Odpowiedź nr 43:**

Zamawiający pod pojęciem „usług odpowiadających swoim rodzajem usługom stanowiącym przedmiot zamówienia” rozumie usługi przeprowadzania audytów informatycznych, mających w swoim zakresie m.in. inwentaryzację zasobów sprzętowych i programowych systemów informatycznych, bezpieczeństwo systemów informatycznych i bezpieczeństwo przetwarzania informacji.

Przedmiotowe wyjaśnienie zostało uwzględnione w rozdziale V pkt 1 zaktualizowanego zapytania ofertowego.

**Pytanie nr 44:**

Czy Zmawiający dopuszcza by określone w punkcie V.2. wymagania członkowie zespołu spełniali wspólnie?

**Odpowiedź nr 44:**

Treść warunku opisanego w rozdziale V pkt. 2 zaktualizowanego zapytania ofertowego brzmi następująco:

„O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy wykażą, że dysponują lub będą dysponować osobami, które będą uczestniczyć w wykonaniu zamówienia, spełniającymi następujące wymagania:

Ekspert ds. audytu IT i bezpieczeństwa - minimum 2 osoby posiadające następujące kwalifikacje i doświadczenie zawodowe:

* wykształcenie wyższe;
* posiada co najmniej 3-letnie doświadczenie w zakresie przeprowadzania audytów odpowiadających swoim zakresem przedmiotowi niniejszego zamówienia;
* co najmniej jeden z ekspertów powinien posiadać aktualne certyfikaty Audytora Wiodącego norm: ISO 27001 i ISO 22301 lub równoważne;
* pozostali członkowie zespołu eksperckiego powinni posiadać certyfikat Audytora Wiodącego norm: ISO 27001 lub ISO 22301 lub równoważne;
* co najmniej jeden z ekspertów powinien posiadać aktualny certyfikat z zakresu zarządzania projektami PRINCE 2 lub równoważny.

Jako certyfikat równoważny zamawiający rozumie posiadanie certyfikatów analogicznych do zakresu wskazanych certyfikatów tj. dotyczących analogicznej dziedziny merytorycznej wynikającej z roli, której dotyczy certyfikat, analogicznego stopnia poziomu kompetencji, analogicznego poziomu doświadczenia zawodowego wymaganego dla otrzymania danego certyfikatu itp.”

**Pytanie nr 45:**

Czy za równoważne Wykonawca uzna certyfikaty techniczne, które gwarantują poziom wiedzy niezbędny do wykonania testów penetracyjnych tj. GXPN,CEH,OSCP,CISSP. Zamawiający nie określił w zapytaniu swoich oczekiwań względem członka zespołu wykonującego testy penetracyjne, a jest to znaczący etap projektu.

**Odpowiedź nr 45:**

W związku z warunkiem opisanym w rozdziale V pkt 2 zapytania ofertowego Zamawiający wyjaśnia, że nie uzna za równoważne certyfikatów technicznych, które gwarantują poziom wiedzy niezbędny do wykonania testów penetracyjnych tj. GXPN,CEH,OSCP,CISSP w odniesieniu do wymaganych przez Zamawiającego certyfikatów Audytora Wiodącego norm: ISO 27001 i ISO 22301.

**Pytanie nr 46:**

Ekspert ds. audytu IT i bezpieczeństwa - minimum 2 osoby posiadające następujące kwalifikacje i doświadczenie zawodowe - posiada uprawnienia audytora wewnętrznego w jednostkach sektora finansów publicznych. W odczuciu Wykonawcy powyższy wymóg posiadania kompetencji, w sposób znaczący wykracza po za potrzeby projektowe. Audytor ten swoje zadania realizuje względem całej organizacji a nie jedynie obszaru bezpieczeństwa - jest to rodzaj audytu zarządczego.
Audyt ten obejmować może obszar operacyjny, finansowy, informatyczny. Czy nawet audyty bezpieczeństwa ruchu drogowego, efektywności energetycznej, norm jakości ISO oraz wiele innych. Ponadto osoba która takim audytorem chce zostać dobrze by posiadała (Zgodnie z ustawą o finansach publicznych) kwalifikacje tj:

a) jeden z certyfikatów: Certified Internal Auditor (CIA), Certified Government Auditing Professional (CGAP), Certified Information Systems Auditor (CISA), Association of Chartered Certified Accountants (ACCA), Certified Fraud Examiner (CFE), Certification in Control Self Assessment (CCSA), Certified Financial Services Auditor (CFSA) lub Chartered Financial Analyst (CFA), lub

b) złożyła, w latach 2003–2006, z wynikiem pozytywnym egzamin na audytora wewnętrznego przed Komisją Egzaminacyjną powołaną przez Ministra Finansów, lub

c) uprawnienia biegłego rewidenta, lub

d) dwuletnią praktykę w zakresie audytu wewnętrznego i legitymuje się dyplomem ukończenia studiów podyplomowych w zakresie audytu wewnętrznego, wydanym przez jednostkę organizacyjną, która w dniu wydania dyplomu była uprawniona, zgodnie z odrębnymi ustawami, do nadawania stopnia naukowego doktora nauk ekonomicznych lub prawnych.

Za praktykę w zakresie audytu wewnętrznego, o której mowa w ust. 1 pkt 5 lit. d, uważa się udokumentowane przez kierownika jednostki wykonywanie czynności, w wymiarze czasu pracy nie mniejszym niż 1/2 etatu, związanych z:

1) przeprowadzaniem audytu wewnętrznego pod nadzorem audytora wewnętrznego;
2) realizacją przez inspektorów kontroli skarbowej czynności z zakresu certyfikacji i wydawania deklaracji zamknięcia pomocy finansowej ze środków pochodzących z Unii Europejskiej, o których mowa w ustawie z dnia 28 września 1991 r. o kontroli skarbowej (Dz. U. z 2011 r. Nr 41, poz. 214, z późn. zm. );

3) nadzorowaniem lub wykonywaniem czynności kontrolnych, o których mowa w ustawie z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 2012 r. poz. 82, 1529 i 1544).
Powyższy opis jasno wskazuje na szerokie uprawnienia takiej osoby. Jednakże kompetencje te w dużej mierze dot. samych finansów publicznych, projekt zaś obejmuje audyt infrastruktury informatycznej. Co powoduje że wachlarz tych kompetencji nie zostanie wykorzystany - jest zbyteczny w tym projekcie.
W naszym odczuciu warunek ten nie powinien być obligatoryjnym gdyż, jego spełnienie nie gwarantuje Zmawiającemu odpowiedniej jakości realizacji projektu, zaś jego nie spełnienie - nie będzie stratą dla Zamawiającego. Wykonawca, który go nie spełnia, może być zdolny do wykonania projektu tj. posiadać rozległą wiedze, kompetencje i doświadczenie.

Ponadto warunek ten w znaczy sposób, ogranicza konkurencyjność. Mamy ograniczoną ilość osób, które jednocześnie posiadają (wymagane) kompetencje audytora wewnętrznego oraz są zdolne do wykonywania testów penetracyjnych.

Biorąc pod uwagę powyższe, uprzejmie prosimy o usunięcie wymogu posiadania uprawnień audytora wewnętrznego w jednostkach sektora finansów publicznych.

**Odpowiedź nr 46:**

Treść warunku opisanego w rozdziale V pkt. 2 zaktualizowanego zapytania ofertowego brzmi następująco:

„O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy wykażą, że dysponują lub będą dysponować osobami, które będą uczestniczyć w wykonaniu zamówienia, spełniającymi następujące wymagania:

Ekspert ds. audytu IT i bezpieczeństwa - minimum 2 osoby posiadające następujące kwalifikacje i doświadczenie zawodowe:

* wykształcenie wyższe;
* posiada co najmniej 3-letnie doświadczenie w zakresie przeprowadzania audytów odpowiadających swoim zakresem przedmiotowi niniejszego zamówienia;
* co najmniej jeden z ekspertów powinien posiadać aktualne certyfikaty Audytora Wiodącego norm: ISO 27001 i ISO 22301 lub równoważne;
* pozostali członkowie zespołu eksperckiego powinni posiadać certyfikat Audytora Wiodącego norm: ISO 27001 lub ISO 22301 lub równoważne;
* co najmniej jeden z ekspertów powinien posiadać aktualny certyfikat z zakresu zarządzania projektami PRINCE 2 lub równoważny.

Jako certyfikat równoważny zamawiający rozumie posiadanie certyfikatów analogicznych do zakresu wskazanych certyfikatów tj. dotyczących analogicznej dziedziny merytorycznej wynikającej z roli, której dotyczy certyfikat, analogicznego stopnia poziomu kompetencji, analogicznego poziomu doświadczenia zawodowego wymaganego dla otrzymania danego certyfikatu itp.”

**Pytanie nr 47:**

Informacje dotyczące warunków składania ofert. Mając na względzie pytania, które pojawią się w postępowaniu oraz niezbędny czas dla Zamawiającego na przygotowanie odpowiedzi. Uprzejmie prosimy o przedłużenie terminu składania ofert do dnia 27.01.2017.

**Odpowiedź nr 47:**

Zgodnie z informacją opublikowaną przez Zamawiającego na jego stronie internetowej oraz na portalu Baza Konkurencyjności w dniu 20 stycznia 2017, **termin składania ofert został wyznaczony na dzień 6 lutego 2017 na godz. 10.00**.

**Pytanie nr 48:**

Czy Zamawiający w zakresie kompetencji Audytora Wiodącego systemu ISO22301 uzna za równoważne posiadanie ważnego certyfikatu CISA (Certified Information Systems Auditor)?

**Odpowiedź nr 48:**

Tak, Zamawiający w zakresie kompetencji Audytora Wiodącego systemu ISO22301 uzna za równoważne posiadanie ważnego certyfikatu CISA (Certified Information Systems Auditor).

**Pytanie nr 49:**

Czy w związku z wymaganiem dotyczącym kompetencji osób wykonujących zamówienie, a mianowicie posiada aktualny certyfikat Audytora Wiodącego norm ISO 27001, ISO 22301 lub równoważne. Należy rozumieć, że każda osoba uczestnicząca w wykonaniu zamówienia musi posiadać łącznie wymienione kompetencje odnośnie certyfikatów ISO, tzn. zarówno certyfikat Audytora Wiodącego ISO27001, jak i certyfikat Audytora Wiodącego ISO22301?

**Odpowiedź nr 49:**

Przynajmniej jeden z ekspertów ds. audytu IT i bezpieczeństwa powinien posiadać oba certyfikaty.  Pozostali mogą posiadać jeden z dwóch certyfikatów.

**Pytanie nr 50:**

Czy każdy z Ekspertów ds. audytu IT musi legitymować się łącznie certyfikatami Audytora Wiodącego  ISO 27001 i ISO 22301, czy wymagane jest by każdy posiadał tylko jeden z ww. certyfikatów?

**Odpowiedź nr 50:**

Przynajmniej jeden z ekspertów ds. audytu IT i bezpieczeństwa powinien posiadać oba certyfikaty.  Pozostali mogą posiadać jeden z dwóch certyfikatów.

**Pytanie nr 51:**

Jaka jest liczba lokalizacji objętych zakresem badania?

**Odpowiedź nr 51:**

Zakresem badania objęta jest jedna lokalizacja.

**Pytanie nr 52:**

Jaka jest szacunkowa liczba pracowników organizacji?

**Odpowiedź nr 52:**

Szacunkowa liczba pracowników organizacji wynosi do 180.

**Pytanie nr 53:**

Jaka jest szacunkowa liczba pracowników odpowiedzialnych za obszar IT (administratorów IT)?

**Odpowiedź nr 53:**

Dwie osoby są w organizacji odpowiedzialne za obszar IT.

**Pytanie nr 54:**

Jaka jest liczba utrzymywanych systemów teleinformatycznych objętych zakresem audytu?

**Odpowiedź nr 54:**

**W pytaniu nie sprecyzowano o jakie systemy teleinformatyczne chodzi, w związku z tym Zamawiający nie jest w stanie określić odpowiedzi w tym zakresie.**

**Pytanie nr 55:**

Jaka jest liczba stacji roboczych objętych zakresem audytu?

**Odpowiedź nr 55:**

Zakresem audytu objętych jest do 180 stacji roboczych.

**Pytanie nr 56:**

Jaka jest liczba serwerów fizycznych / serwerów wirtualnych?

**Odpowiedź nr 56:**

Do 30 serwerów.

**Pytanie nr 57:**

Jaka jest liczba stron internetowych?

**Odpowiedź nr 57:**

Dwa podstawowe serwisy.

**Pytanie nr 58:**

Jaka jest liczba pomieszczeń serwerowni / lokalnych punktów dystrybucyjnych?

**Odpowiedź nr 58:**

Cztery pomieszczenia serwerowni .

**Pytanie nr 59:**

Jaka jest liczba urządzeń sieciowych z rozbiciem na poszczególne typy (zapora sieciowa, trasownik, przełącznik)?

**Odpowiedź nr 59:**

**Zamawiający na ten moment nie ma pełnej wiedzy na ten temat.**

**Pytanie nr 60:**

Czy organizacja posiada wdrożone Active Directory w pełnym zakresie (jeżeli nie to w jakim zakresie)?

**Odpowiedź nr 60:**

Organizacja posiada wdrożone Active Directory.

**Pytanie nr 61:**

Czy w organizacji wytwarza się oprogramowanie?

**Odpowiedź nr 61:**

Nie, w organizacji nie wytwarza się oprogramowania.

**Pytanie nr 62:**

Czy w organizacji zdefiniowano i wdrożono formalne dokumenty w zakresie bezpieczeństwa informacji? Jeżeli tak, proszę podać ich zakres przedmiotowy (np. obszar ochrony fizycznej, obszar teleinformatyki, zarządzanie incydentami, itd.).

**Odpowiedź nr 62:**

**W organizacji wdrożono formalnie Politykę Bezpieczeństwa Informacji. ~~W organizacji nie zdefiniowano i nie wdrożono formalnych dokumentów w zakresie bezpieczeństwa informacji.~~**

**Pytanie nr 63:**

Czy inwentaryzacja aktywów ma zakładać tryb manualny (weryfikacja fizyczna aktywa, oznacza w praktyce, że audytor uda się do pokoju / biura w którym znajduje się aktywo)?

**Odpowiedź nr 63:**

Tak, inwentaryzacja aktywów ma zakładać tryb manualny.