Centrum Informatyki Statystycznej

Znak: CIS-WAG.2720.08.2018

Warszawa, dnia 6 marca 2018 roku

Dotyczy: zapytania ofertowego CIS-WAG.2720.08.2018 z dnia 02.03.2018 r. na **„Przeprowadzenie audytu bezpieczeństwa informacji dla systemu wymiany mikrodanych wg wymagań Wspólnych Ram Bezpieczeństwa Europejskiego Systemu Statystycznego"**.

W dniu 5 marca 2018 r. do Zamawiającego wpłynęły następujące pytania:

Pytanie 1

Jako niezbędny warunek udziału w postępowaniu Zamawiający wskazał posiadanie certyfikatu PN-ISO/IEC 27006 lub równoważnego (punkt 2 Zapytania ofertowego). W naszej opinii oznacza to dopuszczenie do udziału w postępowaniu wyłącznie organizacji posiadających akredytację (np. Polskiego Centrum Akredytacji) uprawniającą do certyfikowania SZBI na zgodność z ISO27001

pytanie: czy Zamawiający dopuści do udziału organizacje na stałe współpracujące z audytorami biorącymi czynny udział w certyfikacji? Wnosimy o dodanie alternatywnego warunku udziału "stałą współpracę z audytorami posiadającymi ważne zaświadczenie o byciu audytorem jednostki certyfikującej"

Odpowiedź 1

Zgodnie z odpowiedzią na pytanie nr 5 Zamawiający nie może usunąć tego wymagania. Tak, zamawiający uzna warunek za spełniony w stosunku do organizacji posiadających akredytację (np. Polskiego Centrum Akredytacji) uprawniającą do certyfikowania SZBI na zgodność z ISO27001.

Pytanie 2

Jako metodologię audytu Zamawiający wskazał normę PN-ISO/IEC 27006, podczas gdy norma ta opisuje wymagania wobec jednostek świadczących audyty certyfikowane (punkt III.6 OPZ). W naszej opinii zasadne jest użycie normy ISO/IEC 27007, a nie tej wymienionej w OPZ. Norma ISO/IEC 27007 opisuje wymagania na proces audytu, a więc usługę, którą zamawia Zamawiający.

wnosimy o aktualizację zapytania ofertowego

Odpowiedź 2

Przez metodologię z normy PN-ISO/IEC 27006 Zamawiający rozumiał organizację audytującą wg rodziny norm ISO 27k w tym wg metodologii wskazanych tej rodzinie norm.

Centrum Informatyki Statystycznej

Aleja Niepodległości 208, 00-925 Warszawa
tel. 22 608 31 44
cissek@stat.gov.pl
cis.stat.gov.pl

Pytanie 3

Ilu pracowników Zamawiającego jest zatrudnionych w obszarze objętym audytem? Informacje jest niezbędna do ustalenia czasu audytu zgodnie z wytycznymi odpowiednich norm.

Odpowiedź 3

W planowanym obszarze wymiany mikrodanych - 0. Obszar na dzień dzisiejszy jest jedynie planowany. Posiada przygotowane założenia do budowy i dokumentację bezpieczeństwa. Możliwość rozmowy audytowej z **2 osobami** (statystyk - przedstawiciel biznesu, przedstawiciel projektantów).

W istniejącym obszarze OBM (przetwarzanie i składowanie mikordanych), ale aktualnie nie przystosowanym do wymiany mikrodanych– **4 osoby** (2 administratorów, wiodący administrator, osoba odpowiedzialna za składnicę danych).

W obszarze organizacji ze względu na docelowe przetwarzanie / składowanie / wysyłanie mikrodanych w wydzielonym, odseparowanym środowisku wyłącznie przez pracowników CIS i GUS (statystycy) przyjęto że w ograniczonym zakresie należy zaudytować 3 serwerownie w budynku GUS (w ramach zespołu współpracującego z wykonawcą), dostęp fizyczny (1 osoba), sieć (w ramach zespołu współpracującego z wykonawcą), firewalle (1 osoba), usługa katalogowa (1 osoba), procesy kadrowe (1 osoba) – **4 osoby**.

Razem – 10 osób.

Niezależnie, współpracę z wykonawcą przez cały czas trwania audytu zapewni zespół zamawiającego złożony z kierownika projektu, specjalisty ds. bezpieczeństwa informacji (ABI) i przedstawiciela wydziału sieciowego.

W związku z ograniczonym zakresem przedmiotowym audytu, wskazaną wyżej niewielką liczbą osób objętych audytem, częściowym niespełnieniem wymagań wskazanych w OPZ których w związku z tym nie sposób poddać audytowi (niektóre wymagania przewidziane są do spełnienia w kolejnych latach, Zamawiający szacuje je na 30-50% całości w tym np. pracochłonna audytowo klasyfikacja informacji wg wymagań rodziny ISO27k i wszystkie pochodne wymagania) oraz przygotowaniu przez Zamawiającego listy wymaganych dowodów i tabeli audytowej (załącznik nr 1 do OPZ), wystarczający do dokonania audytu wg szacunków Zamawiającego jest zespół audytowy składający się z audytora i drugiego pracownika w tym jedna z tych osób powinna posługiwać się językiem angielskim w sposób umożliwiający wypełnienie załączonej w OPZ tabeli po angielsku i na bieżąco napisać raport z audytu w dwóch językach. Zamawiający szacuje czas rzeczywistej pracy Wykonawcy, przy zaangażowaniu zespołu Zamawiającego, na około 40 roboczogodzin.

W związku z powyższym Zamawiający podtrzymuje czas realizacji umowy.

Pytanie 4

We wzorze umowy Zamawiający określił czas realizacji usługi na 3 dni robocze (par 2). W naszej ocenie tak, krótki termin realizacji usługi nie pozostawia możliwości zaplanowania działań związanych z organizacją audytu: przeprowadzenie wstępnego spotkania z Zamawiającym, przygotowanie i uzgodnienie planu audytu, przygotowanie wersji roboczej raportu i notatek, opracowanie raportu. Ponadto tak krótki czas dyskryminuje organizacje dysponujące mniejszą liczbą audytorów oraz faworyzuje organizacje posiadające uprzednią znajomość struktury organizacji Zamawiającego

wnosimy o wydłużenie czasu realizacji umowy do 5 tygodni.

Odpowiedź 4

Odpowiedź w pytaniu nr 3.

Centrum Informatyki Statystycznej

Aleja Niepodległości 208, 00-925 Warszawa
tel. 22 608 31 44
cissek@stat.gov.pl
cis.stat.gov.pl

Pytanie 5

Zamawiający wymaga posiadania certyfikatu PN-ISO/IEC 27006:2016, który jest właściwy dla jednostek certyfikujących SZBI. Z analizy zakresu zamówienie nie wynika jednak, żeby przedmiotem prac było wsparcie w certyfikacji, ani nawet projektowanie SZBI pod kątem certyfikacji.

Czy w związku z tym Zmawiający byłby skłonny usunąć w/w wymaganie jako nadmiarowe w stosunku do przedmiotu zamówienia?

Odpowiedź 5

Zamawiający w żadnym wypadku nie oczekuje audytu na skalę pełnego SZBI, a jedynie audytu wskazanych obszarów wg wymagań i dowodów określonych w OPZ i załączniku do OPZ opartych na dokumencie „IT Security Framework". Jest prawdą, że ww dokument jest dość wierną kopią rodziny norm ISO27k, jednakże zawiera znacznie mniej wymagań. Dodatkowo, zgodnie z OPZ i odpowiedzią na pytanie nr 1, zakres audytu został istotnie ograniczony w stosunku do audytów SZBI.

Wymaganie certyfikatu wynika z wymagań Eurostatu. Założeniem Eurostatu jest by audyt kończący grant, w którym przygotowano istotną część dokumentacji bezpieczeństwa dla wymiany mikrodanych, został przeprowadzony przez audytorów o takich samych kompetencjach jak przewidziany audyt certyfikacyjny w 2019 r. W związku z powyższym Zamawiający niestety nie może usunąć tego wymagania.

W zakresie spełnienia wymagań: odpowiedź na pytanie nr 1.

Pytanie 6

Zamawiający nie określił bezwzględnego terminu realizacji usługi. We wzorze umowie zdefiniowano jedynie czas względny od dnia podpisania umowy (3 dni robocze). Z naszej strony jest to istotne przy weryfikacji dostępności audytorów.

pytanie: jaki jest oczekiwany termin zakończenia usługi?

Odpowiedź 6

15 marca 2018 r.

Pytanie 7

W nawiązaniu do ogłoszonego zapytania proszę o następujące informacje:

- ile osób objętych jest zakresem audytu?
- w zapytaniu zapisaliście Państwo, ze audyt ma być wykonany trzy dni po podpisaniu umowy, ale nie określiliście Państwo mniej więcej w jakim terminie (miesiąc) ma być przeprowadzony audyt- proszę o podanie przybliżonej daty.

Odpowiedź 7

Odpowiedź w pytaniu nr 3 i nr 6.

DYREKTOR
Stanisław Stelużycki

Centrum Informatyki Statystycznej

Aleja Niepodległości 208, 00-925 Warszawa
tel. 22 608 31 44
cissek@stat.gov.pl
cis.stat.gov.pl