Centrum Informatyki Statystycznej

Załącznik nr 1 do zapytania ofertowego CIS-WAZ.2720.23.2019

Opis Przedmiotu Zamówienia

Przygotowanie aktualizacji dokumentacji bezpieczeństwa systemu Operacyjnej Bazy Mikrodanych do wymagań Wspólnych Ram Bezpieczeństwa Europejskiego Systemu Statystycznego

I. Tło akcji

W 2015 r. Eurostat i wybrane państwa członkowskie przeprowadziły w ramach projektu SIMSTAT próbną wymianę mikrodanych z handlu wewnętrznego pochodzących z systemu INTRASTAT (dane zbierane oraz kontrolowane dla celów statystyki handlu zagranicznego przez Ministerstwo Finansów, dalej jako „MF").

Celem projektu SIMSTAT było przetestowanie zdolności państw członkowskich do wymiany mikrodanych statystycznych na próbnych danych. Wymiana danych między hubem Eurostatu a GUS była przeprowadzona przez komponent SIMSTAT przy użyciu bramki CCN w Ministerstwie Finansów. Wymiana danych w projekcie SIMSTAT została zakończona sukcesem. Wymiana danych miała charakter próbny i nie jest obecnie prowadzona.

Eurostat, w ramach realizowanej obecnie Wizji ESS 2020, planuje rozpocząć od 2020 r. wymianę mikrodanych dot. handlu wewnętrznego pomiędzy państwami członkowskimi. W tym celu realizowany jest projekt ESDEN (*European statistical data exchange network*). Dane dot. wywozu towarów z Polski będą wysyłane przez GUS wraz z ID partnera zagranicznego (*towar od partnera X <polskiego> do partnera Y z kraju członkowskiego w ujęciu miesięcznym*). Dane będą wysyłane poprzez centralny punkt (hub utworzony w Eurostat) do innych państw członkowskich. Dane innych państw będą przysyłane do GUS przez hub centralny.

Dane przeznaczone do wymiany mają różny poziom zabezpieczeń zależnie od regulacji krajowych państw członkowskich. ESSC (Komitet Sterujący ESS) w maju 2016 r. przyjął dokument „Wspólne ramy bezpieczeństwa IT ESS" (*IT Common Security Framework* lub *IT Security Framework*) określający jednolity standard zabezpieczeń dla wszystkich państw członkowskich. Dokument został przygotowany na podstawie rodziny norm ISO/IEC 27000 wraz z powiązanymi normami (w szczególności ISO/IEC 27000, 27001 i 27002). Dokument zawiera ponad 90 wymagań dotyczących bezpieczeństwa informacji. Zakres dokumentu pokrywa przede wszystkim obszar systemów teleinformatycznych i organizacyjny, w mniejszym stopniu procesów kadrowych i bezpieczeństwa fizycznego.

Wymiana mikrodanych z handlu wewnętrznego została wpisana do aktualnie procedowanego dokumentu FRIBS (*Framework Regulation Integrating Business Statistics*) jako obowiązkowa od 2021 r. Eurostat planuje umożliwić fizyczną wymianę danych po weryfikacji czy dane państwo spełnia wymagania bezpieczeństwa określone w *IT Security Framework*. W związku z powyższym Eurostat zaplanował certyfikację państw członkowskich oraz Eurostatu przez zewnętrznego audytora. GUS / CIS został zgłoszony do procesu certyfikacyjnego na 2019 r.

Centrum Informatyki Statystycznej

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

Zakres certyfikacji określają dwa dokumenty:

- „Wspólne ramy bezpieczeństwa IT ESS" w zakresie wskazania obszarów certyfikacji, dowodów koniecznych do wykazania spełnienia wymagań oraz koniecznych przeglądów bezpieczeństwa (Załącznik nr 1 do OPZ).
- Dokument „Mitigation of risks related to the exchange of identifiable micro-data" stanowiący uzupełnienie powyższego dokumentu o wskazanie wymagań, które mają zastosowanie do całej organizacji (obszar organizacji) lub jedynie obszaru wykorzystania mikrodanych z handlu wewnętrznego (obszar MDE, ang. Micro Data Exchange) (Kolumna „Zakres" w Tabeli nr 1).

II. Cel zamówienia

Niniejsze zapytanie ofertowe ma na celu aktualizację dokumentacji bezpieczeństwa Operacyjnej bazy Mikrodanych i przygotowanie organizacji do planowanej certyfikacji.

III. Przedmiot zamówienia

Przedmiotem zamówienia jest usługa pt. „**Przygotowanie aktualizacji dokumentacji bezpieczeństwa systemu Operacyjnej Bazy Mikrodanych do wymagań Wspólnych Ram Bezpieczeństwa Europejskiego Systemu Statystycznego**".

1. Planowana architektura rozwiązania (MDE) obejmuje dwa obszary techniczno-organizacyjne:
    a. Projektowany wydzielony obszar wymiany mikrodanych obsługiwany przez Edamis4 za pomocą sieci TESTA wraz ze wstępną weryfikacją wysyłanych danych (Obszar wymiany).
    b. Istniejący wydzielony obszar przetwarzania i składowania mikrodanych w istniejącej Operacyjnej Bazie Mikrodanych (OBM).
2. Niniejsze zamówienie ma na celu aktualizację dokumentacji bezpieczeństwa wyłącznie w obszarze OBM.
3. Dla obszaru OBM istnieje polityka bezpieczeństwa. Istniejąca dokumentacja bezpieczeństwa OBM została wdrożona na podstawie nieaktualnej już wersji normy ISO27001 i odnosi się przede wszystkim do bezpieczeństwa danych osobowych z niewystarczającym uwzględnieniem danych przewidzianych do wymiany.
4. Aktualziacja dokumentacji będzie polegac na weryfikacji istniejących zapisów i zaproponowaniu zaktualziowanje ich treści bez konieczności dodawania nowych obszarów aktualnie nie uwzględnionych w dokumentacji.
5. Zakres przewidywanych prac do realizacji:
    a. Analiza dokumentacji bezpieczeństwa OBM względem zgodności z aktualną wersją normy ISO27001 i norm powiązanych.
    b. Propozycja zmian obejmująca:
        i. Aktualizację zapisów polityki bezpieczeństwa OBM.
        ii. Aktualizację listy załączonych środków technicznych przeznaczonych do zapewnienia bezpieczeństwa wraz z określeniem zasad ich stosowania.

iii. Weryfikację ról i odpowiedzialności określonych w polityce bezpieczeństwa OBM względem aktualnych wymagań z rodzny norm ISO 27000.

6. Dokumentacja bezpieczeństwa informacji w organizacji:
    a. Polityka Bezpieczeństwa Informacji Statystyki Publicznej (zasady ogólne, role i obowiązki, ogólna klasyfikacja informacji, dokument o charakterze organizacyjnym).
    b. Dokumenty uzupełniające.
    c. Obszar OBM posiada wdrożoną dokumentację bezpieczeństwa.
    d. Obszar wymiany posiada wdrożoną dokumentację bezpieczeństwa.
7. Zagadnienia bezpieczeństwa informacji określone w dokumentacji bezpieczeństwa OBM:
    a. Podstawa prawna Polityki bezpieczeństwa i źródła wymagań bezpieczeństwa
    b. Podstawowe zasady bezpieczeństwa
    c. Metodyka i zasady analizy ryzyka
    d. Polityka danych osobowych
    e. Wykaz ról i odpowiedzialności
    f. Procedury kontroli dostępu i nadawnaia uprawnień
    g. Metody i środki uwierzytelniania
    h. Procedury bezpiecznej pracy użytkowników systemu
    i. Procedury backupu
    j. Sposób, miejsce i okres przechowywyania danych
    k. Procedury antymalware
    l. Procedury zbierania logów
    m. Przegląd, konserwacja i serwisowanie systemu
8. Informacje uzupełniające:
    a. Infrastruktura bezpieczeństwa i informatyczna zlokalizowana jest w budynku GUS.
    b. Pracownicy służb statystyki publicznej zaangażowani w proces wymiany i przetwarzania mikrodanych są wyłącznie pracownikami Głównego Urzędu Statystycznego i Centrum Informatyki Statystycznej pracującymi w budynku GUS.
    c. Liczba pracowników Zamawiającego z którymi może zaistnieć konieczność wywiadu w przypadku wątpliwości co do treści dokumentacji: obszar OBM – 3 administratorów oraz możliwość rozmowy audytowej z 2 przedstawicielami biznesu.
9. Z usługi należy sporządzić raport w języku polskim zawierający skrócony opis zrealziwoanych działań.

10. Spotkania robocze Zamawiającego z Wykonawcą będą odbywać się w siedzibie Zamawiającego lub zostaną przeprowadozne zdalnie. Spotkanie otwierające i zamykające musza odbyć się w siedzibie Zamawiajacego.

11. Na potrzeby opracowania przedmiotu zamówienia Zamawiający udostępni w siedzibie Zamawiającego i po podpisaniu umowy posiadane materiały i dokumenty, jak również zapewni współpracę właściwych pracowników.

IV. Wymagania dla dokumentów

Wykonawca będzie zobowiązany do wykonania Przedmiotu zamówienia z należytą starannością, zgodnie z zasadami wiedzy technicznej oraz obowiązującymi przepisami prawa polskiego i europejskiego.

Dokumentacja zostanie przygotowane z uwzględnieniem następujących wymagań:

1. Będzie opracowaniem kompletnym i wyczerpującym z punktu widzenia celu, któremu ma służyć,

2. Zostanie przygotowany w języku polskim w formie papierowej (format A-4, średnia ilość znaków na stronie – 1 900) oraz formie elektronicznej w formacie plików do edycji. Forma graficzna publikacji, czcionki, formatowanie strony, wygląd ew. ilustracji, itp., wynikająca z księgi znaków Zamawiającego, zostanie przekazana Wykonawcy po podpisaniu umowy.

3. Wykonawca zobowiązuje się do przekazywania Zamawiającemu wszelkich informacji mających wpływ na realizację przedmiotu zamówienia oraz do niezwłocznego udzielania odpowiedzi i wyjaśnień na zgłaszane przez Zamawiającego uwagi dotyczące jego realizacji w formie pisemnej.

4. Wykonawca dostarczy Zamawiającemu ostateczną i zaakceptowaną przez Zamawiającego wersję dokumentów, w wersji papierowej w 2 egzemplarzach oraz w wersji elektronicznej. Dokumenty zostaną dostarczone do siedziby Zamawiającego.

V. Odbiór Przedmiotu Zamówienia

1. Dokumentacja opracowana w ramach realizacji Przedmiotu Zamówienia weryfikowana będzie według następujących kryteriów:
   1) zawartość merytoryczna – treść dokumentu powinna zawierać informacje istotne, niosące treść adekwatną do zakresu dokumentu;
   2) zakres – treść dokumentu winna obejmować uzgodniony zakres prac, wszystkie kwestie mieszczące się w uzgodnionym zakresie muszą zostać zawarte w dokumencie;
   3) klarowność – dokument winien być tak napisany, by czytelnik był w stanie zrozumieć jego treść bez potrzeby zasięgania wyjaśnień u autora, szczególnie istotna jest struktura oraz czytelność raportów, w określonych przypadkach dokument winien zawierać słowniczek używanych terminów lub inne materiały pomocnicze;
   4) precyzja – specyfikacje, opisy czy uwagi zawarte w dokumencie winny być poprawne, jednoznaczne i kompletne.

2. Wykonawca zobowiązuje się do wprowadzenia uwag lub poprawek zamawiającego w dokumentach przed datą odbioru umowy.