Opis Przedmiotu Zamówienia

Audyt dokumentacji Systemu Monitorowania Jakości Internetu (SMJI) oraz e-usługi pn. *Dostęp do bieżącej informacji o jakości usług IAS* oraz wsparcie Zamawiającego w fazach testów akceptacyjnych i odbioru końcowego

Urząd Komunikacji Elektronicznej

20 stycznia 2023 r.

Spis treści

1. Definicje 2
2. Cel zamówienia 2
3. Wymagania w zakresie audytu dokumentacji 2
4. Przepisy i wymogi prawne 5

1. Definicje

Termin	Definicja
E-Usługa	E-usługa p.n. *Dostęp do bieżącej informacji o jakości usług IAS*, udostępniona w ramach realizacji projektu *Dostęp do bieżącej informacji o jakości usług IAS w oparciu o System Monitorowania Jakości Internetu (SMJI)* realizowanego w ramach II osi Programu Operacyjnego Polska Cyfrowa „E-administracja i otwarty rząd", cel szczegółowy nr 2 „Wysoka dostępność i jakość e-usług publicznych", na podstawie porozumienia o dofinansowanie nr POPC.02.01.00-00-0136/21-00.
Projekt	Realizowany przez Zamawiającego projekt p.n. *Dostęp do bieżącej informacji o jakości usług IAS w oparciu o System Monitorowania Jakości Internetu (SMJI)* w ramach II osi Programu Operacyjnego Polska Cyfrowa „E-administracja i otwarty rząd", cel szczegółowy nr 2 „Wysoka dostępność i jakość e-usług publicznych", na podstawie porozumienia o dofinansowanie nr POPC.02.01.00-00-0136/21-00
System, SMJI	System Monitorowania Jakości Internetu – oprogramowanie, urządzenia, usługi i baza danych realizujące cele, założenia i wymagania określone w Specyfikacji Warunków Zamówienia w ogłoszonym przez Zamawiającego postępowaniu o udzielenie zamówienia pod nr BA.WZP.26.21.2022[1].
Zamówienie Główne	Zamówienie udzielone przez Zamawiającego, którego przedmiotem jest zaprojektowanie i zbudowanie Systemu Monitorowania Jakości Internetu (SMJI) oraz wdrożenie e-usługi pn. *Dostęp do bieżącej informacji o jakości usług IAS*, w ramach postępowania nr BA.WZP.26.21.2022.

2. Cel zamówienia

Zamówienie realizowane jest w ramach projektu p.n. *Dostęp do bieżącej informacji o jakości usług IAS w oparciu o System Monitorowania Jakości Internetu (SMJI)* w ramach II osi Programu Operacyjnego Polska Cyfrowa „E-administracja i otwarty rząd", cel szczegółowy nr 2 „Wysoka dostępność i jakość e-usług publicznych", na podstawie porozumienia o dofinansowanie nr POPC.02.01.00-00-0136/21-00.

Celem zamówienia jest realizacja założeń projektowych w zakresie bezpieczeństwa Systemu SMJI i E-Usługi, dotyczących sprawdzenia poziomu bezpieczeństwa poprzez audyt dokumentacji.

Przedmiotem audytu, jest System SMJI oraz E-Usługa zaprojektowane, zbudowane i wdrożone w ramach realizacji Zamówienia Głównego.

3. Wymagania w zakresie audytu dokumentacji

WAD-1. Przy realizacji zamówienia, Wykonawca zobowiązany jest do współpracy z Wykonawcą Zamówienia Głównego.

[1] Ogłoszenie o zamówieniu BA.WZP.26.21.2022 Zaprojektowanie i zbudowanie Systemu Monitorowania Jakości Internetu (SMJI), Biuletyn Informacji Publicznej Urzędu Komunikacji Elektronicznej, https://bip.uke.gov.pl/zamowienia-publiczne/ogloszenie-o-zamowieniu-ba-wzp-26-21-2022-zaprojektowanie-i-zbudowanie-systemu-monitorowania-jakosci-internetu-smji,691.html

Termin realizacji audytu

WAD-2. Audyt dokumentacji zostanie zrealizowany w terminie przewidzianym w harmonogramie realizacji Zamówienia Głównego, odpowiadającym trzeciej fazie testów akceptacyjnych Systemu SMJI oraz fazie Odbioru Końcowego Systemu i E-Usługi.

WAD-3. Wykonawca będzie pełnił rolę Podmiotu Eksperckiego (Audytora) do realizacji trzeciej fazy obiektywnych testów akceptacyjnych oraz fazy Odbioru Końcowego poszczególnych modułów E-Usługi i całości Systemu (tzw. Niezależnej Strony Trzeciej).

WAD-4. Zamawiający przewiduje realizację poszczególnych zadań dotyczących audytu dokumentacji w szczegółowych terminach uzgodnionych przez Strony w okresie od 1 września do 15 listopada 2023 r.

WAD-5. Zamawiający wymaga, aby czynności sprawdzające implementację zaleceń pokontrolnych czy też ponowny audyt (w zależności od rezultatów audytu) zakończyły się nie później niż 30 listopada 2023 r.

WAD-6. Wykonawca w porozumieniu z Zamawiającym, biorąc pod uwagę poziom zaawansowania prac Wykonawcy Zamówienia Głównego, przygotuje w terminie nie krótszym niż 5 Dni Roboczych od dnia zawarcia Umowy i nie późniejszym niż 5 Dni Roboczych od planowanego rozpoczęcia testów penetracyjnych Systemu lub E-Usługi Plan Audytu, zawierający w szczególności Harmonogram Szczegółowy.

WAD-7. Harmonogram Szczegółowy zawiera szczegółowy wykaz i terminy realizacji poszczególnych zadań Wykonawcy. Harmonogram Szczegółowy musi uwzględniać wymagania wskazane w OPZ.

Cel, zakres i kryteria audytu

WAD-8. Celem audytu jest zbadanie aktualnego stanu zabezpieczenia zasobów informacyjnych pod względem poufności, integralności i dostępności, wskazanie niezgodności z zaleceniami normy PN-ISO/IEC 27001 oraz przygotowaniu rekomendacji związanych z wprowadzeniem mechanizmów służących do uzyskania bezpieczeństwa informacji, zgodnego z normą.

WAD-9. Kryteria audytu określone są przez wymagania dotyczące bezpieczeństwa zawarte w:

1. Specyfikacji Warunków Zamówienia dla Zamówienia Głównego, w szczególności Opisie Przedmiotu Zamówienia;
2. ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. z 2022 r. poz. 1863);
3. rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j. Dz.U. z 2017 r. poz. 2247);
4. uchwale nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 (MP 2019.1037.1);
5. uchwale nr 97 Rady Ministrów z dnia 11 września 2019 r. w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa” (MP 2019.862.1);
6. Narodowych Standardach Cyberbezpieczeństwa (NSC) w zakresie architektury bezpieczeństwa systemów teleinformatycznych w modelu „Zero zaufania” (NSC 800-207);

7. Narodowych Standardach Cyberbezpieczeństwa w zakresie przewodnika po telepracy w przedmiocie publicznym (NSC 800-46);
8. dokumencie „Standardy Cyberbezpieczeństwa Chmur Obliczeniowych" opracowanym w ramach zbioru Narodowych Standardów Cyberbezpieczeństwa;
9. rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz.UE.L 2016 Nr 119, str. 1);
10. ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. 2019 poz. 1781 z późn. zm.);
11. rozporządzeniu Ministra Cyfryzacji z dnia 10 marca 2020 r. w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system teleinformatyczny służący do uwierzytelniania użytkowników (Dz.U. z 2020 r. poz. 399);
12. ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących działania publiczne (t.j. Dz.U. z 2021 r. poz. 2070 z późn. zm.);
13. rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j. Dz.U. z 2017 r. poz. 2247);
14. ustawie z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz.U. z 2020 r. poz. 344 z późn. zm.);
15. normie PN-ISO/IEC 27001.

WAD-10. Zakresem audytu objęta jest Dokumentacja Użytkownika, Dokumentacja Techniczna, Dokumentacja Instruktażowa, Dokumentacja Administratora oraz Dokumentacja Testowa Systemu SMJI i E-Usługi.

WAD-11. Audyt zostanie przeprowadzony w obszarach (z odniesieniem do normy PN-ISO/IEC 27001):

1. kontroli dostępu (A.9),
2. kryptografii (A.10),
3. bezpiecznej eksploatacji (A.12),
4. bezpieczeństwa komunikacji (A.13),
5. pozyskiwania, rozwoju i utrzymania systemów (A.14),
6. relacji z dostawcami (A.15),
7. aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania (A.17),
8. zgodności (A.18).

Przebieg audytu i raport

WAD-12. Audyt musi zostać przeprowadzony przez personel Wykonawcy, przy czym co najmniej jeden członek tego zespołu musi posiadać uprawnienia potwierdzone posiadaniem co najmniej jednym z certyfikatów wskazanych w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu:

1. Certified Internal Auditor (CIA);
2. Certified Information System Auditor (CISA);

3. Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób;
4. Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;
5. Certified Information Security Manager (CISM);
6. Certified in Risk and Information Systems Control (CRISC);
7. Certified in the Governance of Enterprise IT (CGEIT);
8. Certified Information Systems Security Professional (CISSP);
9. Systems Security Certified Practitioner (SSCP);
10. Certified Reliability Professional;
11. Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.

WAD-13. Raport z audytu powinien zawierać w szczególności:

1. szczegóły dotyczące audytowanego,
2. cel i zakres (obszary) audytu,
3. stosowaną normę,
4. opis metodyki audytu,
5. imiona i nazwiska audytorów,
6. ustalenia (próbki) oraz dowody tych ustaleń,
7. listy kontrolne,
8. sformułowane niezgodności wraz ze wskazaniem punktów normy, w których te niezgodności występują,
9. rekomendacje do działań korygujących.

4. Przepisy i wymogi prawne

Wykonawca jest zobowiązany do zapewnienia zgodności przedmiotu zamówienia z przepisami prawa obowiązującymi na terytorium Polski w dniu przekazania przedmiotu zamówienia do Odbioru Końcowego.