Załącznik nr 1

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest wdrożenie modułów, świadczenie usługi wsparcia wraz z gwarancją w okresie 36 miesięcy oraz rozwój Systemu zarządzania ryzykiem (RM) (zwany dalej Systemem) w ramach roboczogodzinowych rozliczeń z puli 200 godzin.

1. Dostawa i przedmiot zamówienia z podziałem na etapy

Celem jest wdrożenie i uruchomienie produkcyjne w Systemie następujących modułów:

- Dokumenty,
- Incydenty,
- Ciągłość działania z analizą BIA,
- Czytelnia norm,

oraz rozwój Systemu w ramach realizacji zleceń z puli 200 godzin, zgodnie z Załącznikiem nr 3 (Zal do OPZ nr 3 Warunki rozwoju.docx).

1.1 Etap 1 – wdrożenie Modułu Dokumenty w Systemie (na instancji testowej i produkcyjnej) wraz z instruktażem stanowiskowym w ramach obsługi, administracji oraz wprowadzenia dokumentów ZSZ SZBI, ZSZ ZSCD, ZR[1] oraz m. in.: zamodelowanie procesu obsługi dokumentów, opracowanie i zaprojektowanie formularzy, skryptów, monitów, wgranie/wprowadzenie danych do bibliotek systemowych, definicja ról i uprawnień użytkowników, zdefiniowanie kont użytkowników zgodnie z rolami i uprawnieniami, przygotowanie i przekazanie czytelnej instrukcji obsługi i administracji wyżej wymienionym modułem, konfiguracji w języku polskim w formie pliku/plikach PDF oraz instrukcje użytkownika i administratora modułu.

Etap 1 zostanie zrealizowany w czasie – 10 dni roboczych od podpisania umowy.

1.2 Etap 2 – wdrożenie Modułu Incydenty w Systemie (na instancji testowej i produkcyjnej) wraz z instruktażem stanowiskowym w ramach obsługi, administracji oraz zaimportowanie bazy danych incydentów zgodnie z formatem CSV udostępnionym przez Zamawiającego, ponadto zamodelowanie procesu obsługi incydentów[2], opracowanie i zaprojektowanie formularzy, skryptów, monitów, wgranie/wprowadzenie danych do bibliotek systemowych, definicja ról i uprawnień użytkowników, zdefiniowanie kont użytkowników zgodnie z rolami i uprawnieniami, przygotowanie i przekazanie czytelnej instrukcji obsługi i administracji wyżej wymienionym modułem, konfiguracji w języku polskim w formie pliku/plikach PDF oraz instrukcje użytkownika i administratora modułu.

Etap 2 zostanie zrealizowany w czasie – 10 dni roboczych od zakończenia i odbioru Etapu 1.

1.3 Etap 3 – dostawa i wdrożenie Modułu Ciągłości działania z analizą BIA[3] w Systemie (na instancji testowej i produkcyjnej) wraz z instruktażem stanowiskowym w ramach obsługi, administracji.

[1] Zintegrowany System Zarządzania - System Zarządzania Bezpieczeństwem Informacji, Zintegrowany System Zarządzania - System Zarządzania Ciągłości Działania, Zarządzanie Ryzykiem.

[2] Incydenty, Incydenty RODO, Incydenty Cyber. Zgodnie z wymaganiami: UoKSC i RODO w szczególności uwzględnieniem formularzy zgłaszania incydentów – CSIRT GOV, PUODO.

[3] BIA - Business Impact Analysis (Analiza Wpływu Biznesowego). Analizę BIA przeprowadza się, by pokazać, jak poszczególne zagrożenia wpływają na funkcjonowanie organizacji i jakich przedsięwzięć wymagają. Służy ona określenia ram czasowych i powiązanych zasobów niezbędnych do zapewnienia ciągłej realizacji zadań. Definicja na podstawie – D. Wróblewski – „Zarządzanie ryzykiem. Przegląd wybranych metodyk", CNBOP 2015. s.84-85

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706

Ponadto zamodelowanie procesu ciągłości działania w tym analizy BIA, opracowanie i zaprojektowanie formularzy, skryptów, monitów, wgranie/wprowadzenie danych do bibliotek systemowych, definicja ról i uprawnień użytkowników, zdefiniowanie kont użytkowników zgodnie z rolami i uprawnieniami, przygotowanie i przekazanie czytelnej instrukcji obsługi i administracji wyżej wymienionym modułem, konfiguracji w języku polskim w formie pliku/plikach PDF oraz instrukcje użytkownika i administratora modułu.

Etap 3 zostanie zrealizowany w czasie – 5 dni roboczych od zakończenia i odbioru Etapu 2.

1.4 Etap 4 – dostawa i wdrożenie Modułu Czytelnia norm w Systemie (na instancji testowej i produkcyjnej) wraz z instruktażem stanowiskowym w ramach obsługi, administracji. Ponadto opracowanie i zaprojektowanie formularzy, skryptów, monitów, wgranie/wprowadzenie danych do bibliotek systemowych, definicja ról i uprawnień użytkowników, zdefiniowanie kont użytkowników zgodnie z rolami i uprawnieniami, przygotowanie i przekazanie czytelnej instrukcji obsługi i administracji wyżej wymienionym modułem, konfiguracji w języku polskim w formie pliku/plikach PDF oraz instrukcje użytkownika i administratora modułu.

Etap 4 zostanie zrealizowany w czasie – 5 dni roboczych od zakończenia i odbioru Etapu 3.

1.5 Etapy 1, 2, 3 i 4 mogą odbywać się symultanicznie.

2. Minimalne wymagania co do zgodności

Wymagane jest, aby System do zarządzania ryzykiem wraz z jego modułami był zgodny w szczególności z następującymi normami, ustawami oraz aktami wykonawczymi do tych ustaw, rozporządzeniami oraz zarządzeniami regulaminami zawartymi m.in. w dokumentach zamawiającego:

2.1 Zgodność z normami ISO 31000:2018, ISO 27005:2018, ISO 27001:2017 oraz ISO 22301:2020, a także ISO 27799:2016 i ISO 27002:2017.

2.2 Zgodność z RODO – Rozporządzeniem 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.

2.3 Zgodność z obowiązującą Ustawą o krajowym systemie cyberbezpieczeństwa wraz z rozporządzeniami szczególnie w kontekście zakresu obowiązków Operatora Usługi Kluczowej.

2.4 Zgodność z wymaganiami audytu oceny Operatora Usługi Kluczowej zgodnie z Krajowym Systemem Cyberbezpieczeństwa w zakresie zgodności z Ustawą o krajowym systemie cyberbezpieczeństwa (Ustawa z dnia 05 lipca 2018 Dz.U. 2018 poz. 1560[4]), szczególnie (ale nie tylko) w zakresie zarzadzania ryzykiem (Obszar 3) – zgodnie z szablonem opublikowanym przez Ministerstwo Cyfryzacji 28 kwietnia 2020 r[5].

2.5 Zgodność z obowiązującym Rozporządzeniem KRI z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2012 r. poz. 526).[6]

2.6 Art. 226 Ustawy z dnia 26.04.1974 r. Kodeks pracy (Dz.U. Nr 21, poz. 94 z późn. zm.) – Pracodawca ocenia i dokumentuje ryzyko zawodowe związane z wykonywaną praca oraz

[4] https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001560
[5] https://mc.bip.gov.pl/krajowy-system-cyberbezpieczenstwa/operatorzy-uslug-kluczowych/szablon-sprawozdania-z-audytu-zgodnego-z-ustawa-o-krajowym-systemie-cyberbezpieczenstwa.html
[6] Standardy Krajowych Ram Interoperacyjności

stosuje niezbędne środki profilaktyczne zmniejszające ryzyko, informuje pracowników o ryzyku zawodowym, które wiąże się z wykonywaną pracą, oraz o zasadach ochrony przed zagrożeniami.

3. Wymagania funkcjonalne i poza funkcjonalne:

3.1 po wdrożeniu każdego z modułów System musi posiadać wszystkie funkcjonalności zgodnie z Załącznikiem nr 2 (Zal do OPZ nr 2 Opis obecnych funkcjonalności Systemu.docx),

3.2 mieć dołączone diagramy BPMN z wdrożonych modułów: Dokumenty, Incydenty, BIA. w nim procesów zarządzania ryzykiem, oraz musi zapewniać ich edycję wraz z rozwojem i dostosowywaniem metodyki do potrzeb,

3.3 musi w ramach konfiguracji modułów: Dokumenty, Incydenty, BIA dawać możliwość tworzenia i wiązania formularzy wraz z relacjami,

3.4 umożliwiać wizualizację Incydentów, Dokumentów, Analiz BIA w postaci konfigurowalnych dashboardów z prezentowaniem na nich danych w formie tabelarycznej, wykresów czy opisów,

3.5 umożliwić automatyczne powiadomienia, monity mailowe (m.in. przypomnienia o nadchodzących terminach związanych z obsługą modułów: Dokumenty, Incydenty, BIA, w tym szczególności incydentów, dokumentów, analiz BIA,

3.6 umożliwić konfigurowalne, automatyczne wysyłanie raporty i powiadomień (oraz na żądanie) – w definiowalnych interwałach czasowych,

3.7 umożliwiać generowanie raportów z modułów: Dokumenty, Incydenty, BIA do formatów minimalnie: .XLSX, .PDF, oraz do dashboardów w wersji graficznej,

3.8 umożliwiać import danych do bibliotek, definicji, formularzy minimalnie z plików płaskich .txt, .csv, oraz posiadać instrukcję i procedurę w języku polskim – jak realizować krok po kroku.

3.9 umożliwiać import danych konfiguracyjnych w formie minimalnie płaskich tabel w plikach tekstowych.

3.10 umożliwiać okresowe automatyczne generowanie predefiniowanych raportów w tym w formie graficznej, tabelarycznej, opisowej.

3.11 umożliwiać ocenę krytyczności procesów w tym systemów i usług w zakresie, zagrożeń ciągłości działania zgodnie z ISO 22301:2020.

3.12 umożliwiać opracowywanie i przygotowywanie raportów indywidualnych, poprzez m.in. filtrowanie danych ze względu na konfigurowalne kryteria i zdefiniowane kwerendy i zapytania.

3.13 umożliwiać definiowanie, tworzenie i zapisywanie formularzy, skryptów i monitów wg konfigurowalnych parametrów.

3.14 umożliwiać wprowadzanie i monitorowanie zdarzeń operacyjnych, incydentów w związku z bieżącą działalnością, oraz na tej podstawie m.in. umożliwiać wprowadzania planów działania,

3.15 umożliwiać dokonanie szacowania ryzyk powiązanych ze zdarzeniami, incydentami, również w oparciu o zgormadzone dane historyczne,

3.16 Instrukcja obsługi powinna być poza dostarczoną w plikach PDF oraz zaszyta w system w formie „dymków" lub podpowiedzi.

3.17 System musi działać w środowisku Windows Server 2016 lub nowszym, posiadającym wsparcie producenta co najmniej w okresie 36 miesięcy od daty podpisania protokołu

odbioru.

3.18 Silnik bazy danych systemu musi być oparty o aktualny i wspieraną wersję przez producenta MS SQL 2016 co najmniej przez następne 36 miesiące.

3.19 System musi umożliwić śledzenie, audyt zmian w konfiguracji oprogramowania i bazy danych. Baza danych powinna mieć zaimplementowaną i włączoną funkcję audytu bazy danych, polegającą na rejestrowaniu działań wszystkich użytkowników.

3.20 System musi po stronie klienta być obsługiwany poprzez znane przeglądarki wiodących producentów i być aktualizowany, aby w czasie trwania umowy zapewnić ciągłość działania poprzez m.in. wsparcie i obsługę.

3.21 System musi posiadać kreator umożliwiający dodawanie i konfigurowanie, parametrów, formularzy i ankiet w systemie nie wymagający wiedzy programistycznej.

3.22 System musi umożliwić sprawną pracę dla najmniej 80 osób jednocześnie, z możliwością w przypadku nieobecności danego pracownika zastąpienia go innym.

3.23 System musi być wyposażony przez producenta w API, umożliwiające jego przyszłą integrację z systemami zewnętrznymi i posiadać do niego czytelną dokumentację techniczną, umożliwiającą jego wykorzystanie przez developerów, m.in. do np. zasilania podatnościami, incydentami, czy danymi z innych systemów bezpieczeństwa jak SIEM[7], DLP[8], EDR[9], skaner podatności, antywirus, firewall[10], itp., oraz ticketowych – Jira / Jira Service Desk.

3.24 System musi posiadać możliwość eksportu danych, raportów z analiz do formatu Microsoft Excela oraz formatu PDF.

3.25 System musi posiadać możliwość rozwijania samodzielnie przez Zamawiającego rozwiązania m.in. przez dodawanie kolejnych obszarów dla wszystkich wdrożonych modułów.

3.26 Gwarancję na okres 26 miesięcy od daty podpisania protokołu odbioru ostatniego etapu wdrożenia – Załącznik nr 1 (Zal do OPZ nr 1 Warunki gwarancji.docx).

4. Dokumentacja powinna zawierać:

1 wzorcowe dokumenty używane we wszystkich wdrożonych modułach dołączone w formie załączników, w formie edytowalnych plików .DOCX,

2 dołączone procesy zapisane w notacji BPMN w stopniu szczegółowości biznesowej stanowiące załączniki do metodologii, w formie plików .PDF i w formie dołączonych załączników do metodologii,

3 dołączoną instrukcję do poszczególnych procesów w formie edytowalnych plików .DOCX,

4 czytelną instrukcję obsługi i administracji systemem, konfiguracji w języku polskim w formie pliku/plikach PDF,

5 dokumentację techniczną wdrożonego systemu.

5. Wymagania wobec Wykonawcy

Zamawiający wymaga, aby Wykonawca spełniał następujące kryteria:

1) winien wykazać, że w okresie ostatnich 2 lat przed upływem terminu składania ofert, a jeżeli okres

[7] SIEM - to skrót od Security Information and Event Management
[8] DLP - Data Loss Prevention
[9] EDR (Endpoint Detection and Response)
[10] FIREWALL - rodzaj zapory sieciowej

prowadzenia działalności przez Wykonawcę jest krótszy – w tym okresie wykonał, a w przypadku świadczeń okresowych lub ciągłych wykonuje co najmniej **trzy usługi** związane z opracowaniem i wdrożeniem – metodyki zarządzania ryzykiem w cyberbezpieczeństwie dla operatora usługi kluczowej lub systemu zarządzania ryzykiem w cyberbezpieczeństwie.

2) wyznaczył konsultanta / opiekuna do stałego kontaktu z Zamawiającym w trakcie realizacji wdrożenia, który będzie dysponował co najmniej kwalifikacjami potwierdzonymi certyfikatami w biegłości z zakresu bezpieczeństwa informacji – ISO 27001, oraz w zakresie: ISO 31000, oraz w zakresie Zarządzania ciągłości działania ISO 22301.

3) posiadał w składzie zespołu projektowego co najmniej jedną osobę na poziomie auditora wiodącego ISO 27001/22301 (lub posiadającą ekwiwalentne certyfikaty międzynarodowe zarządzania ryzykiem) oraz miał udokumentowany udział w pracach przy co najmniej dwóch projektach wdrażających system zarządzania ryzykiem dla operatorów usługi kluczowej

4) jeżeli Wykonawca przy realizacji przedmiotu zamówienia będzie polegał na wiedzy i potencjale osób zdolnych do wykonywania zamówienia dla podmiotów, niezależnie od charakteru prawnego, łączących go z nimi stosunków, musi udowodnić Zamawiającemu, iż będzie dysponował zasobami niezbędnymi do realizacji zamówienia, w szczególności przedstawiając pisemne zobowiązanie tych podmiotów do oddania do dyspozycji niezbędnych zasobów na okres wykonywania umowy. Wykonawca jest zobowiązany do wskazania, które Etapy czy podzadania zamówienia będą realizowane przez inne podmioty.

5) weryfikacja poprawności wdrożonego systemu będzie odbywać się protokołem odbioru poszczególnych etapów.

6) podpisany przez obie strony protokół wykonania przedmiotu zamówienia będzie stanowił podstawę do wystawienia faktury VAT przez Wykonawcę. Protokół zostanie sporządzony w dwóch egzemplarzach, po jednym dla każdej ze stron.

7) płatność zostanie uregulowana przelewem na podstawie poprawnie wystawionej Faktury VAT w terminie nie dłuższym niż 30 dni od daty otrzymania faktury. Faktura zostanie wystawiona po pełnym wykonaniu usługi.

8) Gwarancja świadczona będzie przez okres 24 miesięcy od dnia odbioru Systemu i będzie polegać na:

   a diagnozowaniu Systemu,

   b usuwaniu Błędów,

   c przeglądzie poprawek dla eksploatowanych środowisk wykorzystujących System.

   d ocenie konieczności zastosowania poprawek rekomendowanych przez producenta oprogramowania w eksploatowanych środowiskach oraz ich wdrożenie.

   e doradztwie architektonicznym w zakresie zgodności sposobu wykorzystywania Oprogramowania z najlepszymi praktykami rekomendowanymi przez dostawcę oraz zgodności z warunkami Umowy,

   f doradztwie technicznym i implementacyjnym w zakresie adaptacji nowych lub istotnie zmodyfikowanych wersji Oprogramowania (tj. wersje główne Oprogramowania oraz zestawy poprawek – tzw. Patches) lub migracji środowisk,

   g informowaniu Zamawiającego o przyczynach i sposobach rozwiązywania problemów związanych z nieprawidłowym działaniem Systemu,

h założeniu zgłoszenia serwisowego w serwisie pomocy technicznej producenta, w przypadku wad i błędów Oprogramowania składającego się na System, przekazanie zgłoszenia serwisowego do producenta oprogramowania oraz prowadzenie zgłoszenia w imieniu Zamawiającego,

i instruktażu uwzględniającym nowe funkcjonalności po aktualizacji Systemu, aktualizacja dokumentacji technicznej Systemu,

j doradztwie technicznym, przekazywaniu na bieżąco informacji o nowych funkcjonalnościach możliwych do zaimplementowania w Systemie,

k wsparciu w konfiguracji i optymalizacji Systemu,

Załącznik:

1) Zal do OPZ nr 1 Warunki gwarancji.docx
2) Zal do OPZ nr 2 Opis obecnych funkcjonalności Systemu.docx
3) Zal do OPZ nr 3 Warunki rozwoju.docx

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706