

OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

„Wykonanie audytu wstępnego zgodności KRI/KSC oraz zaprojektowanie i wdrożenie Zintegrowanego Systemu Zarządzania Bezpieczeństwem Informacji dla Ministerstwa Zdrowia”.

I. Zamawiający:

Ministerstwo Zdrowia z siedzibą w Warszawie, ul. Miodowa 15, 00-952 Warszawa.

II. Kontekst, założenia dotyczące zamówienia

1. Zamawiający prowadzi postępowanie o udzielenie zamówienia publicznego na **wykonanie audytu wstępnego zgodności Ministerstwa z Krajowymi Ramami Interoperacyjności i Krajowym Systemem Cyberbezpieczeństwa oraz zaprojektowanie i wdrożenie Zintegrowanego Systemu Zarządzania Bezpieczeństwem Informacji dla Ministerstwa Zdrowia.**
2. Zamówienie publiczne Wykonawca zrealizuje zgodnie z: ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2026 r. poz. 20, 252), rozporządzeniem Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. poz. 773) oraz zgodnie z aktami prawnymi wymienionymi w ust. 4.
3. Nazwa i kod zamówienia według Wspólnego Słownika Zamówień:
CPV: 79417000-0 – Usługi doradcze w zakresie bezpieczeństwa
79212000-3 – Usługi audytu
80510000-2 – Usługi szkolenia specjalistycznego
4. Celem zamówienia jest podniesienie poziomu bezpieczeństwa przetwarzanych informacji oraz systemów informatycznych funkcjonujących w Ministerstwie Zdrowia poprzez wykonanie audytu wstępnego KRI/KSC oraz zaprojektowanie i wdrożenie Zintegrowanego Systemu Zarządzania Bezpieczeństwem Informacji (zwanego dalej SZBI), zgodnie z wymaganiami obowiązujących nw. aktów prawnych, norm i wytycznych, w szczególności:
 - a) Rozporządzenia 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), w skrócie „RODO”;
 - b) Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2025 poz. 1703 z późn. zm.);
 - c) Ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2022 r. poz. 902 z późn. zm.);
 - d) Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 poz. 1781 z późn. zm.);
 - e) Polskiej normy PN-EN ISO/IEC 22301 lub równoważnej;
 - f) Polskiej normy PN-EN ISO/IEC 27001 lub równoważnej;
 - g) Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji

- w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. poz. 773).
- h) Dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2);
 - i) Dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE;
 - j) Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2026 r. poz. 20, 252).
5. Za parametry równoważności wobec normy PN-EN ISO/IEC 27001:2022 uważa się:
- a) Systemowe podejście do zarządzania bezpieczeństwem informacji, obejmujące:
 - ustanowienie polityki bezpieczeństwa informacji,
 - określenie celów i zasad SZBI,
 - stosowanie cyklu PDCA (Plan-Do-Check-Act) w zarządzaniu SZBI.
 - b) Zdefiniowanie kontekstu organizacji, w tym:
 - określenie stron zainteresowanych,
 - określenie zakresu SZBI.
 - c) Zarządzanie ryzykiem w obszarze bezpieczeństwa informacji, obejmujące:
 - identyfikację, analizę, ocenę i postępowanie z ryzykiem,
 - dokumentowanie ryzyk oraz środków zaradczych.
 - d) Stosowanie środków kontroli bezpieczeństwa, adekwatnych do zidentyfikowanych ryzyk, w szczególności:
 - zarządzanie dostępem,
 - ochrona przed złośliwym oprogramowaniem,
 - kontrola fizyczna i środowiskowa,
 - bezpieczeństwo zasobów ludzkich i ciągłości działania.
 - e) Utrzymywanie dokumentowanych procedur i polityk, m.in. w zakresie:
 - reagowania na incydenty,
 - zarządzania aktywami,
 - przetwarzania danych osobowych.
 - f) Audytowanie i przegląd zarządczy SZBI, w tym:
 - regularne audyty wewnętrzne, nie rzadziej niż raz w roku,
 - działania korygujące i doskonalące, nie rzadziej niż raz w roku.
 - g) Szkolenie i uświadamianie pracowników w zakresie bezpieczeństwa informacji.
 - h) Udokumentowanie wdrożenia i skutecznego funkcjonowania SZBI, np. poprzez:
 - rejestry audytów i incydentów,
 - analizę ryzyka,
 - protokoły przeglądów zarządczych.
6. Za parametry równoważności wobec normy PN-EN ISO/IEC 22301 uważa się:
- a) Systemowe zarządzanie ciągłością działania, oparte na podejściu procesowym i cyklu PDCA (Plan-Do-Check-Act), obejmujące:
 - ustanowienie polityki ciągłości działania,
 - określenie celów ciągłości i planu wdrożenia.
 - b) Zrozumienie kontekstu organizacji, w tym:
 - określenie istotnych interesariuszy i ich wymagań,
 - zdefiniowanie zakresu systemu zarządzania ciągłością działania (BCMS).
 - c) Przeprowadzenie analizy wpływu na działalność (BIA) oraz oceny ryzyka związanego z zakłóceniami działania.
 - d) Zdefiniowanie i wdrożenie strategii ciągłości działania, w tym:
 - identyfikacja krytycznych procesów i zasobów,
 - planowanie odzyskiwania i utrzymania usług (strategia RTO/RPO).
 - e) Opracowanie i utrzymywanie planów ciągłości działania i reagowania na incydenty, w tym:

- scenariusze awaryjne i plany postępowania,
 - przypisanie ról i odpowiedzialności.
- f) Testowanie i doskonalenie planów, w szczególności poprzez:
- testy, ćwiczenia, symulacje,
 - działania korygujące po testach i incydentach.
- g) Szkolenie i uświadamianie pracowników w zakresie ciągłości działania.
- h) Przegląd i audytowanie systemu BCMS, w tym:
- przeglądy zarządzania,
 - audyty wewnętrzne,
 - rejestr działań doskonalących i niezgodności.
- i) Udokumentowanie systemu, m.in. poprzez:
- procedury, plany, analizy BIA i ryzyka,
 - raporty z testów, przeglądów i audytów.
7. Realizacja zamówienia ma na celu:
- a) przedstawienie aktualnego stanu systemu zarządzania bezpieczeństwem informacji w Ministerstwie Zdrowia,
- b) zapewnienie bezpieczeństwa danych i systemów informacyjnych użytkowanych w Ministerstwie Zdrowia oraz powierzanych w oparciu o inne akty prawne,
- c) ograniczenie czasu niedostępności systemów informacyjnych Ministerstwa Zdrowia z powodu ich awarii, poprzez zapewnienie poufności, integralności oraz dostępności informacji,
- d) zapewnienie bezpieczeństwa procesu udostępniania danych.
8. Zintegrowany System Zarządzania Bezpieczeństwem Informacji nie będzie obejmował zasad bezpieczeństwa dla informacji niejawnych określonych w ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2025 poz. 1209).
9. Informacje ogólne o środowisku Zamawiającego:
- a) Przetwarzanie informacji odbywa się w następujących lokalizacjach Ministerstwa:
- Warszawa, ul. Miodowa 15;
 - Warszawa, ul. Długa 38/40;
 - Warszawa, Aleje Jerozolimskie 155;
 - Warszawa, al. Księcia Józefa Poniatowskiego 1.
- b) Przetwarzanie informacji odbywa się również zdalnie za pośrednictwem systemu informacyjnego.

III. Przedmiot zamówienia

Realizacja Przedmiotu zamówienia obejmuje wykonanie czterech etapów:

1. **Etap I** – Przeprowadzenie audytu funkcjonującego w Ministerstwie Zdrowia systemu zarządzania bezpieczeństwem informacji w zakresie zgodności z Polską Normą PN-EN ISO/IEC 27001 lub równoważną, uwzględniając obecne wymagania prawa, w szczególności wymagania Krajowych Ram Interoperacyjności i Krajowego Systemu Cyberbezpieczeństwa i przekazanie Ministerstwu Zdrowia jego wyników w formie podpisanego raportu końcowego z przeprowadzonego audytu, który uwzględnia m.in. opis zakresu przeprowadzonych prac audytowych, sumaryczne zestawienie wyników audytu w odniesieniu do wymagań bezpieczeństwa oraz stwierdzone niezgodności, luki, a także rekomendacje.
- Zadanie obejmuje dokonanie analizy funkcjonujących w Ministerstwie zabezpieczeń organizacyjno-technicznych mających na celu zachowanie poufności, integralności oraz dostępności wszystkich informacji przetwarzanych w Ministerstwie Zdrowia, w szczególności zapewnienia ciągłości działania kluczowych procesów organizacji zgodnie z Polską Normą PN-EN ISO/IEC 22301 lub równoważną.
- Termin realizacji Etapu I** do 30 dni od dnia podpisania umowy. Zakończenie Etapu I realizacji przedmiotu zamówienia, potwierdzone właściwym protokołem zaakceptowanym przez Zamawiającego, warunkuje przejście do kolejnych etapów realizacji zamówienia.
2. **Etap II** – Opracowanie i przekazanie Ministerstwu Zdrowia:

- a) Dokumentacji Zintegrowanego Systemu Zarządzania Bezpieczeństwem Informacji - ZSZBI, zawierającej niezbędne polityki i procedury, w szczególności:
- Polityka bezpieczeństwa fizycznego i środowiskowego;
 - Polityka bezpieczeństwa informacji;
 - Polityka ciągłości działania;
 - Polityka i metodyka zarządzania ryzykiem;
 - Polityka klasyfikacji informacji;
 - Polityka haseł;
 - Polityka kontroli dostępu;
 - Polityka używania AI w Ministerstwie;
 - Polityka ochrony własności intelektualnej;
 - Polityka stosowania urządzeń mobilnych i pracy zdalnej;
 - Polityka zarządzania aktywami informacyjnymi;
 - Polityka zarządzania certyfikatem kwalifikowalnym podpisu elektronicznego;
 - Polityka zarządzania informatycznymi nośnikami danych;
 - Polityka zarządzania uprawnieniami;
 - Procedura audytu ZSZBI;
 - Procedura działań doskonalących;
 - Procedura oznaczania dokumentów klasyfikowanych;
 - Procedura przeglądu zarządzania;
 - Procedura zarządzania bezpieczeństwem zasobów ludzkich;
 - Procedura zarządzania incydentami bezpieczeństwa informacji;
 - Procedura zarządzania tożsamością i uprawnieniami;
 - Procedura zarządzania wyjątkami bezpieczeństwa informacji;
 - Regulamin bezpiecznego użytkowania systemu informacyjnego;
 - Strategia ciągłości działania;
 - Wykaz stron zainteresowanych;
 - Wzorcowy wykaz zabezpieczeń informacji (Załącznik A normy PN-EN ISO/IEC 27001 lub normy równoważnej);
 - Zasady bezpieczeństwa informacji dla wykonawców;
 - Eksploatacja systemów i sieci, zasady bezpieczeństwa przy korzystaniu z poczty elektronicznej,
 - Ochrona systemowa poczty przychodzącej,
 - Polityka zarządzania kopiami bezpieczeństwa,
 - Polityka postępowania z informacją,
 - Polityka czystego biurka i ekranu,
 - Zarządzanie i nadzór nad incydentami,
 - Pomiar skuteczności zabezpieczeń,
 - Plany ciągłości działania w kontekście bezpieczeństwa informacji.
- b) Innej dokumentacji Zintegrowanego Systemu Zarządzania Bezpieczeństwem Informacji, niezbędnej do skutecznego zarządzania bezpieczeństwem informacji w Ministerstwie, niewymienionej w pkt a).
- c) Zamawiający zastrzega sobie prawo do wnoszenia uwag do tworzonej przez Wykonawcę dokumentacji. Wykonawca jest zobowiązany do uwzględnienia w dokumentacji uwag wniesionych przez Zamawiającego.
- d) Zamawiający akceptuje przygotowaną w formie elektronicznej dokumentację.
- e) Wykonawca przekazuje Zamawiającemu zaakceptowaną przez Zamawiającego dokumentację w formie elektronicznej:
- w plikach zapisanych w formatach edytowalnych w szczególności .docx, .xlsx
 - w plikach w formacie .pdf opatrzonych kwalifikowanym podpisem elektronicznym lub podpisanym profilem zaufanym lub podpisem osobistym wykonanym przez upoważnionego przedstawiciela Wykonawcy.

- f) Dokumentację Wykonawca zabezpieczy przed nieuprawnionym dostępem zgodnie z wytycznymi Zamawiającego i przekaże Zamawiającemu na informatycznym nośniku danych, a także prześle pocztą elektroniczną na adresy email wskazane przez Zamawiającego.

Termin realizacji Etapu II do 90 dni od zakończenia etapu I, jednak nie później niż do 20 października 2026 r.

3. **Etap III** – przeprowadzenie procesu szacowania ryzyka utraty poufności, integralności i dostępności informacji przetwarzanych w Ministerstwie, w szczególności:

- a) Opracowanie metodyki szacowania ryzyka dla informacji przetwarzanych w Ministerstwie, spełniającej wymagania Krajowych Ram Interoperacyjności, norm PN-EN ISO/IEC 27001 oraz PN-EN ISO/IEC 27005 lub norm równoważnych. Zamawiający zastrzega sobie prawo do wnoszenia uwag do opracowanej metodyki analizy ryzyka, a Wykonawca zobowiązany jest je uwzględnić. Ponadto Wykonawca zobowiązany jest do przeprowadzenia procesu szacowania ryzyka zgodnie z opracowaną przez Wykonawcę i zatwierdzoną przez Zamawiającego metodyką szacowania ryzyka;
- b) Opracowanie kryteriów akceptacji ryzyka i określenie poziomów ryzyk;
- c) Przeprowadzenie szkolenia (w formie zdalnej) dla maksymalnie 50 pracowników Ministerstwa Zdrowia wyznaczonych przez Zamawiającego w zakresie przyjętej metodyki szacowania ryzyka. Przeprowadzenie szkolenia na jednej z ogólnodostępnych, bezpłatnych platform służących komunikacji online (szkolenie realizowane w formie online w czasie rzeczywistym), do której dostęp zapewni Wykonawca;
- d) Przeprowadzenie, wspólnie z wyznaczonymi pracownikami Ministerstwa Zdrowia, procesu szacowania ryzyka, w tym: zinventaryzowanie zasobów (aktywa informacyjne) oraz ich właścicieli, określenie zagrożeń dla zasobów, określenie podatności dla zasobów, określenie skutków utraty poufności, integralności i dostępności zasobów oraz przeanalizowanie i ocenę zidentyfikowanych ryzyk;
- e) Opracowanie raportów z procesu szacowania ryzyka, uwzględniających wszystkie zidentyfikowane ryzyka utraty poufności, integralności i dostępności informacji Ministerstwa;
- f) Opracowanie, przy współudziale wyznaczonych pracowników Ministerstwa Zdrowia, planu postępowania z ryzykiem.

Termin realizacji Etapu III do 100 dni od zakończenia etapu I, jednak nie później niż do 6 listopada 2026 r. Realizacja Etapu III nie jest uwarunkowana zakończeniem Etapu II. Zakończenie Etapów I, II i III, potwierdzone właściwymi protokołami zaakceptowanymi przez Zamawiającego, warunkuje przejście do etapu IV realizacji przedmiotu zamówienia.

4. **Etap IV** – przygotowanie i przeprowadzenie szkolenia w formie zdalnej. Przeprowadzenie jednorazowego szkolenia na jednej z ogólnodostępnych, bezpłatnych platform służących komunikacji online do której dostęp zapewni Wykonawca (szkolenie realizowane w formie online w czasie rzeczywistym) dla maksymalnie 50 pracowników Ministerstwa Zdrowia wyznaczonych przez Zamawiającego w zakresie wytworzonej w etapie II Dokumentacji ZSZBI. Dodatkowo wymaga się opracowania materiałów szkoleniowych w formie elektronicznej w formacie edytowalnym pliku .pptx, z zakresu systemu zarządzania bezpieczeństwem informacji, w tym w szczególności z ochrony danych osobowych i cyberbezpieczeństwa - na potrzeby uruchomienia przez Zamawiającego szkoleń wewnętrznych w formie e-learningu. Wykonawca zabezpieczy pliki szkolenia przed nieuprawnionym dostępem, zgodnie z wytycznymi Zamawiającego i przekaże Zamawiającemu na informatycznym nośniku danych.

Termin realizacji Etapu IV do 21 dni od dnia podpisania ostatniego z protokołów zaakceptowanych przez Zamawiającego dokumentujących ukończenie wcześniejszych Etapów, jednak nie później niż do dnia zakończenia realizacji przedmiotu zamówienia tj. do dnia 30 listopada 2026 r.

IV. Harmonogram realizacji zamówienia

1. Maksymalny termin realizacji całości zamówienia - nie później niż do dnia 30 listopada 2026 roku. Oznacza to, że do tego terminu zostanie obustronnie podpisany protokół końcowy odbioru przedmiotu umowy.
2. Po zawarciu umowy, do 3 dni, Wykonawca prześle Zamawiającemu szczegółowy harmonogram etapów realizacji przedmiotu umowy. Zamawiający ma prawo do wnoszenia uwag do przedstawionego harmonogramu w terminie do 3 dni od dnia otrzymania ww. harmonogramu. Wykonawca zobowiązany jest do ich uwzględnienia w terminie do 3 dni od dnia wniesienia uwag. Uzgodniony harmonogram podlega akceptacji przez Zamawiającego.
3. Harmonogram musi zawierać terminy wykonania poszczególnych etapów, w tym uwzględniać terminy wnoszenia i akceptacji uwag do elementów ujętych w danym etapie oraz terminy rozpoczęcia i zakończenia danego etapu.
4. Wykonawca o rozpoczęciu i zakończeniu każdego z etapów realizacji przedmiotu umowy będzie niezwłocznie informował Zamawiającego. Informacja będzie przekazywana w formie elektronicznej na adresy e-mail osób wskazanych do kontaktu. Zakończenie każdego z etapów realizacji przedmiotu umowy wymaga potwierdzenia właściwym protokołem zaakceptowanym przez Zamawiającego.
5. Zamawiający ma do 4 dni na wniesienie uwag do dokumentów przekazywanych Zamawiającemu w ramach zakończenia Etapu I-III oraz materiałów szkoleniowych opracowanych w ramach Etapu IV.
6. Wykonawca dostarczy zamawiającemu dokumenty oraz materiały szkoleniowe o których mowa w pkt. 5 w terminie umożliwiającym wniesienie uwag, uwzględniając terminy zakończenia poszczególnych etapów.

Uwagi:

1. Zamawiający informuje, że w przypadku wystąpienia w dokumentacji zamówienia lub innych dokumentach odniesienia do konkretnych norm, aprobat, specyfikacji czy systemów, do których nie opisano parametrów równoważności, należy potraktować je jako przykładowe. Zamawiający informuje, że w każdym takim przypadku dopuszcza się dokumenty równoważne, przy czym obowiązek potwierdzenia równoważności dokumentów leży po stronie Wykonawcy.
2. Zamawiający po wyborze oferty najkorzystniejszej i przed zawarciem umowy będzie wymagał okazania kopii potwierdzonych za zgodność z oryginałem posiadanych przez osoby skierowane do realizacji umowy aktualnych certyfikatów.

VI. Termin realizacji zamówienia

Wykonawca jest zobowiązany wykonać zamówienie nie później niż w terminie do dnia 30 listopada 2026 r. Oznacza to, że do tego terminu zostanie obustronnie podpisany protokół końcowy odbioru przedmiotu umowy.