Załącznik nr 1

Znak sprawy: KL – 68/2026

OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

Kompleksowy audyt Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), Systemu Zarządzania Ciągłością Działania (SZCD) oraz zgodności z wymaganiami KRI, UoKSC i NIS2

1. Przedmiot zamówienia

Przedmiotem zamówienia jest przeprowadzenie kompleksowego, niezależnego audytu Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), Systemu Zarządzania Ciągłością Działania (SZCD) oraz zgodności z wymaganiami Krajowych Ram Interoperacyjności (KRI), ustawy o krajowym systemie cyberbezpieczeństwa (UoKSC) i dyrektywy NIS2, w zakresie mającym zastosowanie do Zamawiającego.

Audyt obejmuje ocenę ustanowienia, wdrożenia, funkcjonowania, utrzymywania, monitorowania i doskonalenia systemów zarządzania, w tym weryfikację rzeczywistego wdrożenia i skuteczności zabezpieczeń wynikających z analizy ryzyka, Deklaracji Stosowania, dokumentacji systemowej oraz wymagań prawnych.

Audyt powinien uwzględniać rzeczywiste uwarunkowania organizacyjne i techniczne przedsiębiorstwa wodociągowo-kanalizacyjnego, w tym środowiska IT, OT i ICS.

Zamówienie obejmuje ocenę zgodności dokumentacji ze stanem faktycznym oraz potwierdzenie realizacji wymagań.

2. Cel audytu

Celem audytu jest uzyskanie niezależnej i udokumentowanej oceny:

- zgodności i skuteczności SZBI w odniesieniu do wymagań PN-EN ISO/IEC 27001;
- prawidłowości procesu zarządzania ryzykiem bezpieczeństwa informacji w odniesieniu do PN-EN ISO/IEC 27005;
- adekwatności, rzeczywistego wdrożenia i skuteczności zabezpieczeń bezpieczeństwa informacji;
- zgodności i skuteczności SZCD w odniesieniu do PN-EN ISO 22301;
- zgodności z mającymi zastosowanie wymaganiami KRI, UoKSC i NIS2;
- spójności dokumentacji, przyjętych procesów i stosowanych zabezpieczeń z rzeczywistym sposobem funkcjonowania Zamawiającego;
- występujących niezgodności, luk oraz obszarów wymagających działań korygujących lub doskonalących.

Audyt powinien umożliwiać ustalenie, czy przyjęte zasady i zabezpieczenia są rzeczywiście stosowane, monitorowane i oceniane pod względem skuteczności

3. Podstawa normatywna i prawna

Audyt należy przeprowadzić z uwzględnieniem aktualnych na dzień jego realizacji wymagań normatywnych i prawnych.

Podstawę normatywną audytu stanowią:

1. **PN-EN ISO/IEC 27001:2023-08 wraz z A1:2025-02** – w zakresie wymagań Systemu Zarządzania Bezpieczeństwem Informacji.
2. **PN-EN ISO/IEC 27002:2023-01** – w zakresie wytycznych dotyczących doboru, wdrażania i funkcjonowania zabezpieczeń bezpieczeństwa informacji.
3. **PN-EN ISO/IEC 27005:2025**-01 – w zakresie wytycznych dotyczących zarządzania ryzykiem bezpieczeństwa informacji.
4. **PN-EN ISO 22301:2020-04 wraz z A1:2025-03** – w zakresie wymagań Systemu Zarządzania Ciągłością Działania.

Podstawę prawną audytu stanowią w szczególności:

1. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, z późniejszymi zmianami.
2. Przepisy wykonawcze do ustawy o krajowym systemie cyberbezpieczeństwa, mające zastosowanie do Zamawiającego.
3. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 (NIS2), z uwzględnieniem jej implementacji do krajowego porządku prawnego.
4. Rozporządzenie 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 – w zakresie mającym zastosowanie do Zamawiającego.
5. Inne obowiązujące przepisy związane z przedmiotem audytu, jeżeli mają zastosowanie do Zamawiającego.

Kryteriami audytu są również wymagania wynikające z obowiązującej dokumentacji SZBI i SZCD Zamawiającego.

4. Zakres organizacyjny i przedmiotowy audytu

Audyt obejmuje całość działalności przedsiębiorstwa Zamawiającego w zakresie bezpieczeństwa informacji, cyberbezpieczeństwa i ciągłości działania.

Zamawiający informacyjnie podaje, iż działa na terenie 4 gmin: Kielce, Masłów, Nowiny, Zagnańsk, zatrudnia ok. 360 pracowników, posiada 3 oczyszczalnie ścieków, 10 ujęć wody, 7 lokalnych centrów systemu SCADA, 7 serwerów fizycznych dla potrzeb IT, ok. 200 stacji roboczych.

Zakres obejmuje w szczególności:

- procesy zarządcze, podstawowe i wspierające;
- usługi związane z poborem, uzdatnianiem, magazynowaniem i dystrybucją wody;
- usługi odbioru i oczyszczania ścieków;
- jednostki i komórki organizacyjne;
- personel, role i odpowiedzialności;
- aktywa informacyjne oraz aktywa wspierające;
- systemy teleinformatyczne i środowiska IT;

- środowiska OT i ICS, w tym systemy wykorzystywane do sterowania i monitorowania procesów technologicznych;
- obiekty i lokalizacje;
- dostawców i usługi zewnętrzne mające wpływ na bezpieczeństwo informacji lub ciągłość działania.

Wykonawca powinien ocenić prawidłowość przyjętego zakresu SZBI i SZCD, w tym zasadność ewentualnych wyłączeń.

5. Audyt Systemu Zarządzania Bezpieczeństwem Informacji – SZBI

Audyt SZBI powinien obejmować wszystkie wymagania rozdziałów 4–10 PN-EN ISO/IEC 27001, z uwzględnieniem specyfiki działalności Zamawiającego.

W szczególności należy ocenić:

1. **Kontekst organizacji** – uwarunkowania wewnętrzne i zewnętrzne, strony zainteresowane, wymagania oraz zakres SZBI.
2. **Przywództwo** – zaangażowanie kierownictwa, politykę bezpieczeństwa informacji, role, odpowiedzialności i uprawnienia.
3. **Planowanie** – działania dotyczące ryzyk i szans, cele bezpieczeństwa informacji oraz planowanie zmian.
4. **Wsparcie** – zasoby, kompetencje, świadomość, komunikację oraz nadzór nad udokumentowanymi informacjami.
5. **Działania operacyjne** – realizację przyjętych procesów, zarządzanie ryzykiem oraz wdrażanie i utrzymywanie zabezpieczeń.
6. **Ocenę działania** – monitorowanie, pomiary, audyty wewnętrzne i przeglądy zarządzania.
7. **Doskonalenie** – identyfikację niezgodności, działania korygujące i ciągłe doskonalenie SZBI.

Audytor powinien potwierdzić, czy ustanowione procesy są rzeczywiście realizowane oraz czy Zamawiający posiada dowody ich funkcjonowania.

6. Audyt zarządzania ryzykiem i wdrożenia zabezpieczeń

6.1. Zarządzanie ryzykiem bezpieczeństwa informacji

Wykonawca zweryfikuje proces zarządzania ryzykiem bezpieczeństwa informacji w odniesieniu do wymagań PN-EN ISO/IEC 27001 oraz wytycznych PN-EN ISO/IEC 27005.

Audyt obejmuje w szczególności:

- przyjętą metodykę zarządzania ryzykiem;
- określenie kontekstu oraz kryteriów oceny i akceptacji ryzyka;
- identyfikację aktywów, zagrożeń, podatności i scenariuszy ryzyka;
- analizę i ocenę poziomu ryzyka;
- identyfikację właścicieli ryzyka;
- określenie sposobu postępowania z ryzykiem;
- rejestr ryzyk i plan postępowania z ryzykiem;
- ocenę ryzyka rezydualnego i jego akceptację;

- monitorowanie, przegląd i aktualizację ryzyka.

Wykonawca powinien potwierdzić, czy analiza ryzyka uwzględnia rzeczywiste procesy, usługi, informacje, zasoby i środowiska IT/OT/ICS Zamawiającego.

6.2. Weryfikacja zabezpieczeń bezpieczeństwa informacji

Audyt obejmuje ocenę prawidłowości doboru oraz rzeczywistego wdrożenia zabezpieczeń wynikających z analizy ryzyka, planu postępowania z ryzykiem, Deklaracji Stosowania (SoA), dokumentacji SZBI oraz mających zastosowanie wymagań prawnych.

Weryfikacji podlegają w szczególności:

- zasadność doboru zabezpieczeń oraz uzasadnienie ich ewentualnego wyłączenia;
- zgodność SoA z wynikami analizy ryzyka;
- rzeczywiste wdrożenie przyjętych zabezpieczeń;
- przypisanie odpowiedzialności za zabezpieczenia;
- stosowanie zabezpieczeń w praktyce;
- istnienie dowodów ich funkcjonowania;
- monitorowanie oraz ocena skuteczności zabezpieczeń;
- podejmowanie działań korygujących w przypadku stwierdzenia nieskuteczności.

Ocenę należy przeprowadzić z wykorzystaniem wytycznych PN-EN ISO/IEC 27002, w zakresie odpowiednim do przyjętych zabezpieczeń.

Audytor powinien zweryfikować powiązanie:

analiza ryzyka → plan postępowania z ryzykiem → Deklaracja Stosowania → wdrożone zabezpieczenie → dowód funkcjonowania → ocena skuteczności.

7. Audyt Systemu Zarządzania Ciągłością Działania – SZCD

Audyt SZCD powinien obejmować wszystkie wymagania rozdziałów 4–10 PN-EN ISO 22301.

W szczególności należy ocenić:

1. **Kontekst organizacji** – strony zainteresowane, wymagania oraz zakres SZCD.
2. **Przywództwo** – politykę ciągłości działania, zaangażowanie kierownictwa, role i odpowiedzialności.
3. **Planowanie** – ryzyka i szanse, cele ciągłości działania oraz planowanie zmian.
4. **Wsparcie** – zasoby, kompetencje, świadomość, komunikację i dokumentację SZCD.
5. **Działania operacyjne** – BIA, ocenę ryzyka zakłóceń, strategie ciągłości działania, plany i procedury, testy i ćwiczenia.
6. **Ocenę działania** – monitorowanie, pomiary, audyty wewnętrzne i przeglądy zarządzania.
7. **Doskonalenie** – niezgodności, działania korygujące i ciągłe doskonalenie SZCD.

W ramach oceny działań operacyjnych audytor powinien zweryfikować w szczególności:

- prawidłowość przeprowadzenia analizy wpływu na działalność (BIA);
- identyfikację procesów i usług priorytetowych oraz zasobów niezbędnych do ich realizacji;

- określenie skutków zakłóceń i wymagań dotyczących odtworzenia, w tym RTO, MTPD oraz RPO w odniesieniu do danych i systemów, dla których parametr ten ma zastosowanie;
- ocenę ryzyka zakłócenia działalności;
- przyjęte strategie i rozwiązania zapewniające ciągłość działania;
- kompletność, aktualność i wykonalność planów BCP oraz DRP;
- zasady reagowania, komunikacji i eskalacji;
- program testów i ćwiczeń;
- wyniki testów oraz realizację działań korygujących.

Audytor powinien ocenić, czy rozwiązania dotyczące ciągłości działania zostały dostosowane do rzeczywistych usług, procesów, zasobów oraz infrastruktury Zamawiającego.

8. Audyt zgodności z KRI, UoKSC i NIS2

Wykonawca przeprowadzi ocenę zgodności z wymaganiami prawnymi mającymi zastosowanie do Zamawiającego.

Przed rozpoczęciem oceny Wykonawca ustali i udokumentuje zakres obowiązków wynikający ze statusu prawnego Zamawiającego, charakteru świadczonych usług oraz właściwych przepisów, z uwzględnieniem okresów przejściowych.

Audyt obejmuje w szczególności ocenę:

- systemowego zarządzania cyberbezpieczeństwem;
- zarządzania ryzykiem;
- polityk i procedur bezpieczeństwa;
- zarządzania incydentami oraz realizacji obowiązków zgłoszeniowych;
- ciągłości działania i odtwarzania;
- zarządzania dostępem;
- zarządzania aktywami i podatnościami;
- bezpieczeństwa systemów i sieci;
- zarządzania dostawcami i łańcuchem dostaw;
- monitorowania i oceny skuteczności zabezpieczeń;
- kompetencji, szkoleń i świadomości personelu;
- odpowiedzialności kierownictwa;
- dokumentowania realizacji obowiązków.

Ocena wymagań wynikających z dyrektywy NIS2 powinna uwzględniać ich implementację do prawa krajowego, bez nieuzasadnionego powielania tych samych obowiązków.

W przypadku KRI Wykonawca powinien wskazać przepisy mające zastosowanie do Zamawiającego i udokumentować podstawę przyjętego zakresu oceny.

9. Metodyka audytu

W szczególności obejmuje:

- analizę dokumentacji SZBI i SZCD;
- analizę rejestrów, raportów i zapisów;
- wywiady z kierownictwem, właścicielami procesów i personelem;
- analizę dowodów wdrożenia zabezpieczeń;
- weryfikację rzeczywistego funkcjonowania wybranych procesów;
- dobór i badanie próbek audytowych;
- obserwację oraz wizję lokalną w uzasadnionym zakresie;
- ocenę skuteczności przyjętych rozwiązań organizacyjnych i technicznych.

W przypadku środowisk IT, OT i ICS Wykonawca powinien zweryfikować wybrane zabezpieczenia i dowody ich funkcjonowania odpowiednio do zakresu audytu.

Czynności audytowe należy prowadzić w sposób zapewniający bezpieczeństwo procesów technologicznych Zamawiającego. Działania mogące oddziaływać na produkcyjne środowiska OT/ICS wymagają wcześniejszego uzgodnienia i zgody Zamawiającego.

Samo posiadanie dokumentacji nie stanowi wystarczającego dowodu spełnienia wymagania, jeżeli brak potwierdzenia jej rzeczywistego stosowania.

10. Wymagania wobec Wykonawcy i Audytorów

10.1. Wymagania wobec Wykonawcy

Wykonawca musi posiadać zdolność organizacyjną oraz dysponować wykwalifikowanymi audytorami umożliwiającymi wykonanie pełnego zakresu zamówienia.

Wykonawca zobowiązany jest:

- zapewnić audytora / zespół audytowy o kwalifikacjach odpowiednich do zakresu zamówienia;
- wskazać osobę odpowiedzialną za kierowanie audytem;
- zapewnić niezależność i bezstronność prowadzonego audytu;
- zapewnić zachowanie poufności informacji;
- zapewnić realizację audytu zgodnie z uzgodnionym planem.

10.2. Minimalne wymagania dotyczące kwalifikacji Audytorów

Audyt musi być przeprowadzony przez audytora / zespół audytorów posiadających wiedzę i kompetencje do przeprowadzenia audytu SZBI, SZCD.

W celu potwierdzenia kwalifikacji Zamawiający uzna certyfikaty wskazane w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. z 2018 r. poz. 1999).

Co najmniej jeden audytor powinien posiadać odpowiedni certyfikat potwierdzający kompetencje audytowe.

Na potwierdzenie spełnienia wymagań Wykonawca przedstawi wykaz osób skierowanych do realizacji zamówienia, wraz ze wskazaniem uprawnień do przeprowadzenia audytu zgodnie z wymaganiami prawnymi określonymi w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. z 2018 r. poz. 1999).

10.3. Niezależność i bezstronność

Audytorzy muszą zachować niezależność i bezstronność w stosunku do ocenianych obszarów.

W szczególności audytorzy nie mogą oceniać własnych prac wdrożeniowych w sposób naruszający niezależność audytu.

Przed rozpoczęciem audytu Wykonawca przedłoży oświadczenie o niezależności, bezstronności, braku konfliktu interesów oraz zachowaniu poufności.

11. Produkty końcowe

W ramach realizacji zamówienia Wykonawca przekaże:

1. **Plan audytu**, zawierający zakres, kryteria, metody, harmonogram i skład zespołu.
2. **Kompleksowy raport końcowy,** obejmujący ocenę SZBI, zarządzania ryzykiem, wdrożenia zabezpieczeń, SZCD oraz zgodności z KRI, uoKSC i NIS2.
3. **Zestawienie niezgodności i obserwacji,** wraz ze wskazaniem kryteriów i dowodów audytowych.
4. **Rekomendacje działań korygujących i doskonalących,** z określeniem priorytetów.
5. **Podsumowanie wyników audytu dla kierownictwa Zamawiającego**.

Dopuszcza się ujęcie wszystkich wyników w jednym raporcie, z wyraźnym podziałem na poszczególne obszary audytu.

Każda niezgodność powinna zawierać co najmniej:

- wskazanie niespełnionego wymagania;
- opis stanu faktycznego;
- dowód audytowy;
- ocenę znaczenia ustalenia;
- rekomendowane działanie.

Wykonawca powinien wyraźnie odróżniać niezgodności od obserwacji i możliwości doskonalenia.

Raport oraz zestawienia powinny zostać przekazane w języku polskim, w formie elektronicznej PDF oraz w odpowiednim formacie edytowalnym.

12. Organizacja realizacji i termin

Realizacja zamówienia obejmuje:

1. Spotkanie otwierające i uzgodnienie planu audytu.
2. Analizę dokumentacji SZBI i SZCD oraz materiałów związanych z KRI, uoKSC i NIS2.
3. Przeprowadzenie czynności audytowych.
4. Przygotowanie i przedstawienie projektu wyników audytu.
5. Spotkanie zamykające oraz przekazanie dokumentacji końcowej.

Zamawiający dopuszcza wykonanie części czynności zdalnie.

Termin realizacji: do 21 grudnia 2026.

Szczegółowy harmonogram zostanie uzgodniony z Zamawiającym przed rozpoczęciem czynności audytowych.

13. Poufność

Wykonawca zobowiązany jest do zachowania poufności wszystkich informacji uzyskanych podczas realizacji zamówienia.

Obowiązek ten dotyczy w szczególności dokumentacji SZBI i SZCD, wyników analizy ryzyka, informacji o zabezpieczeniach, incydentach, podatnościach, architekturze IT/OT/ICS oraz planach ciągłości działania.

Informacje uzyskane podczas audytu mogą być wykorzystywane wyłącznie do realizacji przedmiotu zamówienia.