Załącznik nr 2 do zaproszenia do złożenia oferty

Kosakowo, 9 listopada 2026 r.

Opis przedmiotu zamówienia

Numer postępowania ADM.016.2026.10.AS

Audyt cyberbezpieczeństwa IT i OT oraz systemów zarządzania bezpieczeństwem i ciągłością działania

Zamawiający:
Przedsiębiorstwo Usług Komunalnych „PEKO” sp. z o.o. w Kosakowie,
ul. Chrzanowskiego 44,
81-198 Kosakowo.
Zamówienie realizowane w ramach projektu „Kompleksowa rozbudowa i modernizacja rozwiązań z zakresu cyberbezpieczeństwa w PUK PEKO”, programu „Cyberbezpieczne Wodociągi”, inwestycja C3.1.1 KPO.

1 Przedmiot i cel zamówienia

Przedmiotem zamówienia jest niezależny audyt organizacyjny i techniczny cyberbezpieczeństwa oraz ciągłości działania PUK PEKO, obejmujący ocenę dokumentacji, faktycznego stosowania procedur, zgodności z wymaganiami oraz skuteczności zabezpieczeń po ich wdrożeniu. Audyt obejmuje działalność wodociągową, kanalizacyjną, PSZOK, systemy informatyczne IT, systemy przemysłowe OT, oprogramowanie SCADA oraz istotne zależności od dostawców. Wynikiem mają być ustalenia poparte dowodami, ocena ryzyka i zalecenia działań naprawczych. Zamówienie nie obejmuje wdrażania zabezpieczeń, usuwania podatności, prowadzenia szkoleń ani certyfikacji.

2 Zakres audytu

Wykonawca zrealizuje wszystkie poniższe obszary, przedstawiając dla każdego odrębne ustalenia i wnioski:

Pozycja	Zakres
A1. Audyt SZBI	Ocena Systemu Zarządzania Bezpieczeństwem Informacji, polityk i procedur, zarządzania ryzykiem, aktywami, dostępem, incydentami, dostawcami oraz stosowania zabezpieczeń.
A2. Audyt SZCD	Ocena Systemu Zarządzania Ciągłością Działania, analizy BIA, planów BCP i DRP, zasobów, gotowości awaryjnej i możliwości odtworzenia usług.
A3. Audyt zgodności KRI i KSC	Ustalenie mających zastosowanie obowiązków i statusu regulacyjnego Spółki oraz ocena zgodności z KRI, ustawą o krajowym systemie cyberbezpieczeństwa i innymi właściwymi przepisami, z macierzą wymagań.
A4. Audyt techniczny IT	Ocena architektury sieci, konfiguracji urządzeń, serwerów, stacji, usług, dostępu, monitorowania, kopii zapasowych i zabezpieczeń infrastruktury IT.
A5. Audyt techniczny OT	Ocena architektury i zabezpieczeń OT, separacji IT/OT, zdalnego i serwisowego dostępu, urządzeń sterowania, telemetrii i systemów SCADA.
T1. Testy bezpieczeństwa IT	Uzgodnione skanowanie podatności i ręczna weryfikacja istotnych wyników w środowisku IT.
T2. Testy bezpieczeństwa OT	Kontrolowane, bezpieczne sprawdzenia zabezpieczeń OT, bez zakłócania procesów technologicznych.

Pozycja	Zakres
T3. Testy oprogramowania SCADA	Testy bezpieczeństwa aplikacji nadzoru i sterowania, w tym mechanizmów dostępu i znanych podatności, w bezpiecznym uzgodnionym środowisku. Badanie powinno obejmować co najmniej: • uwierzytelnianie; • uprawnienia i role użytkowników; • zarządzanie sesjami; • bezpieczeństwo dostępu zdalnego; • mechanizmy rejestrowania zdarzeń; • konfigurację komunikacji; • znane podatności komponentów aplikacji.

Audyt obejmuje również ocenę dokumentacji i wyników odrębnie realizowanych szkoleń, kampanii phishingowych i ćwiczenia reagowania na incydent, a także obserwację co najmniej jednej bezpiecznej próby odtworzenia danych lub usługi. Wykonawca uwzględni jedną weryfikację usunięcia ustaleń krytycznych i wysokich, jeżeli poprawki zostaną wykonane w uzgodnionym terminie przed odbiorem.

3 Kryteria audytu

Podstawą audytu są wymagania prawne mające zastosowanie do Spółki, w szczególności KRI, KSC, przepisy dotyczące bezpieczeństwa danych osobowych, obowiązki wynikające z projektu oraz dokumentacja wewnętrzna. Pomocniczo stosuje się odpowiednie normy i dobre praktyki, w szczególności ISO/IEC 27001, ISO/IEC 27002, ISO 22301, IEC 62443 oraz metodyki testowania bezpieczeństwa lub rozwiązania równoważne. W raporcie należy odróżnić obowiązki prawne od zaleceń i dobrych praktyk.

4 Sposób realizacji

Wykonawca przygotuje plan audytu, harmonogram, dobór próby, listę wymaganych materiałów i zasady testów. Audyt obejmie analizę dokumentacji, wywiady, oględziny, przegląd konfiguracji i uzgodnione testy techniczne. Należy przewidzieć spotkanie otwierające i końcowe oraz co najmniej dwa dni robocze czynności na miejscu, z uwzględnieniem siedziby, PSZOK oraz reprezentatywnych obiektów wodociągowych i kanalizacyjnych. Wszystkie testy wymagają uzgodnienia zakresu, upoważnień i warunków przerwania. Nie mogą zakłócać dostaw wody, odbioru ścieków ani pracy urządzeń sterowania. Testy ingerujące w SCADA wykonuje się w odseparowanym środowisku testowym. Istotne zagrożenia należy zgłaszać Zamawiającemu niezwłocznie.

4a Zasady bezpieczeństwa prac

- Prace techniczne wymagają zatwierdzonych zasad: cele, adresy i urządzenia, właściciele, zakres upoważnienia, okna prac, kopie, warunki przerwania i kontakt alarmowy. Zasób dostawcy zewnętrznego wymaga również jego zgody w potrzebnym zakresie.
- Zabrania się DoS/DDoS, złośliwego kodu, utrwalania dostępu, nieuzgodnionych zmian i pobierania danych produkcyjnych poza niezbędne, uzgodnione dowody. Socjotechnika i phishing są poza tym zamówieniem. Poświadczeń nie zamieszcza się w raportach.
- Aktywne skanowanie PLC, RTU, HMI i innych elementów sterowania jest zabronione bez odrębnej pisemnej zgody dla konkretnego zasobu, metody i okna serwisowego, po ocenie ryzyka i uzgodnieniu z obsługą OT. Brak takiej zgody nie uprawnia do naruszenia ciągłości usług.
- Wykonawca prowadzi dziennik działań, umożliwia natychmiastowe przerwanie testów i zgłasza niezwłocznie podatność krytyczną lub podejrzenie trwającego naruszenia, nie później niż w ciągu 4 godzin od wykrycia, telefonicznie i bezpiecznym kanałem pisemnym.

5 Audyt organizacyjny i zgodności

5a System zarządzania bezpieczeństwem informacji

Audyt SZBI obejmie zakres systemu i nadzór kierownictwa, role i zastępstwa, aktywa i klasyfikację informacji, analizę i akceptację ryzyka, polityki i rejestry, dostęp i uprawnienia, incydenty i zgłoszenia, zmiany, podatności, kopie, logi, kryptografię, dostawców oraz bezpieczeństwo fizyczne. Należy sprawdzić zatwierdzenie i udostępnienie procedur oraz dowody ich faktycznego stosowania, również przy współpracy biura z obsługą OT i pracownikami terenowymi.

5b Ciągłość działania i odtwarzanie

Audyt SZCD obejmie BIA, procesy krytyczne i zależności, zasoby, strategie awaryjne, kontakty, pracę zastępczą i ręczną, dostęp do planów offline, BCP i DRP, współpracę z dostawcami oraz powrót do normalnej pracy. Wykonawca porówna maksymalny tolerowany czas zakłócenia (MTPD), docelowy czas odtworzenia (RTO) i dopuszczalną utratę danych (RPO) z dowodami prób i dostępnymi zasobami. Wartości planowane, deklarowane i rzeczywiście zmierzone wykazuje się osobno.

5c KRI KSC i status regulacyjny

Wykonawca ustali podstawę i zakres stosowania KRI oraz KSC dla poszczególnych usług i systemów, biorąc pod uwagę działalność, wielkość i powiązania przedsiębiorstwa oraz decyzje lub wpisy przekazane przez PEKO. Macierz obejmie obowiązki, podstawę, termin, stan wykonania, dowód i zalecenie.

6 Próba odtworzenia i sprawdzenie poprawek

Co najmniej jedna próba odtworzenia obejmie wskazany w załączniku nr 2A system lub usługę, rzeczywistą kopię i weryfikację odtworzonych danych lub funkcji w odseparowanym środowisku. Czynności odtworzenia wykonuje upoważniony administrator PEKO lub dostawca pod obserwacją audytora. Audytor dokumentuje datę kopii, punkt odzyskania danych, początek i koniec pomiaru, walidację, uzyskany wynik i ograniczenia. Próba nie może nadpisywać produkcji ani uruchamiać sterowania urządzeniami. Wyniku jednego systemu nie przenosi się na całą organizację.

Cena obejmuje jedną ponowną weryfikację ustaleń krytycznych i wysokich, jeżeli PEKO lub jego dostawcy usuną wskazane przyczyny do 22 grudnia 2026 r. Ponowna weryfikacja dotyczy pierwotnie badanego zakresu i musi zmieścić się w terminie odbioru. Obejmuje bezpieczne sprawdzenie poprawki lub dowodów; nie obejmuje jej wdrożenia. Niewykonane lub niesprawdzone działania pozostają otwarte.

7 Wymagania wobec wykonawcy i zespołu

Podmiot faktycznie wykonujący usługi musi mieć stosowne kwalifikacje i co najmniej 2-letnie doświadczenie w projektach z obszaru cyberbezpieczeństwa. W okresie ostatnich 3 lat przed terminem ofert musi należycie wykonać co najmniej dwa odrębne audyty bezpieczeństwa informacji lub systemów informacyjnych, w tym jeden obejmujący środowisko przemysłowe OT/ICS. Dwa audyty mogą być wykonane w ramach jednej umowy. Nie wymaga się realizacji wyłącznie w przedsiębiorstwach wodociągowych.

Wykonawca zapewnia co najmniej dwie różne osoby audytujące oraz łączne pokrycie bezpieczeństwa informacji, ciągłości działania i IT/OT. Poszczególne role można łączyć, jeśli osoba spełnia wszystkie przypisane wymagania, przy zachowaniu minimalnej liczby dwóch audytorów.

Rola	Minimalne wymagania
Kierownik audytu	3 lata doświadczenia w audycie bezpieczeństwa informacji oraz kierowanie co najmniej dwoma zakończonymi audytami SZBI, KSC lub systemów informacyjnych w ostatnich 5 latach. Certyfikat CISA, CISSP, CISM, audytora wiodącego ISO/IEC 27001 lub równoważne potwierdzenie kompetencji.
Audytor ciągłości działania	Udział w co najmniej jednym zakończonym audycie obejmującym BIA, BCP i DRP w ostatnich 5 latach. Szkolenie audytorskie z egzaminem lub certyfikat w zakresie ciągłości działania, bezpieczeństwa informacji albo równoważne potwierdzenie kompetencji.

Rola	Minimalne wymagania
Ekspert techniczny IT i OT	2 lata praktyki w bezpieczeństwie IT i udział w co najmniej jednym audycie lub projekcie testów bezpieczeństwa OT/ICS w ostatnich 5 latach. Certyfikat lub kwalifikacja obejmująca badanie bezpieczeństwa technicznego, testy lub bezpieczeństwo przemysłowe, np. OSCP, CEH Practical, GICSP, GRID, ISA/IEC 62443 albo równoważny.

W celu zapewnienia kwalifikacji do niezależnej oceny KSC Zamawiający wymaga, jako warunku umownego, wykazania jednej ze ścieżek z art. 15 ust. 2 KSC: właściwej akredytacji jednostki oceniającej zgodność, zespołu co najmniej dwóch uprawnionych audytorów albo właściwego CSIRT sektorowego z uprawnionymi audytorami. W ścieżce zespołu każda z co najmniej dwóch osób wykazuje certyfikat z obowiązującego wykazu albo wymaganą praktykę, ewentualnie praktykę i wykształcenie. Praktykę dokumentuje się zgodnie z art. 15 ust. 3. Przykłady kwalifikacji w tabeli nie zastępują tych przesłanek. Warunek nie przesądza statusu regulacyjnego PEKO; ustalenie tego statusu należy do A3.

Równoważne potwierdzenie kompetencji musi wykazywać imienną kwalifikację, niezależną weryfikację wiedzy lub egzamin oraz zakres odpowiadający danej roli. Wykonawca przedstawi wystawcę, datę, zakres i sposób weryfikacji. Równoważności umownej nie stosuje się zamiast zamkniętych wymagań ustawowych.

Do oferty należy dołączyć wykaz usług z datami, zakresem i potwierdzeniami należytego wykonania oraz wykaz osób, ról, kwalifikacji i doświadczenia. Dowody muszą pozwalać powiązać wymagane zadanie z osobą. Dopuszcza się doświadczenie nabyte u innych pracodawców, anonimizację zbędnych danych oraz udokumentowane doświadczenie osób udostępnionych do realizacji. Sama data rejestracji firmy lub ogólne oświadczenie nie potwierdza okresu praktyki. Zastępca musi spełniać te same wymagania i uzyskać akceptację PEKO.

7a Niezależność

Osoby oceniające nie mogą badać własnej pracy, prowadzić lub rozliczać ocenianych szkoleń ani odpowiadać za wdrożenie, opracowanie lub bieżące działanie badanych rozwiązań. Każdy audytor spełni także ograniczenie z art. 15 ust. 2a KSC dotyczące wykonywania wskazanych tam zadań w audytowanym podmiocie w okresie roku przed audytem. Wykonawca ujawni powiązania z wykonawcami dokumentacji, infrastruktury i szkoleń oraz przedstawi oświadczenia zespołu o niezależności. Powiązania stwarzające konflikt interesów muszą zostać usunięte przed dopuszczeniem osoby do badania.

Dopuszcza się wskazanych podwykonawców i ekspertów spełniających wymagania, objętych poufnością, zasadami dostępu oraz niezależności. Wykonawca odpowiada za ich pracę. Wynagrodzenie i odbiór nie mogą zależeć od pozytywnej oceny audytowanej organizacji.

8 Wyniki i raportowanie

Wykonawca przekaże plan audytu, raport z części organizacyjnej i zgodności, raport z części technicznej i testów oraz raport końcowy zawierający podsumowanie, macierz zgodności, rejestr niezgodności i podatności, ocenę ryzyka oraz plan działań naprawczych z priorytetami. Raport może stanowić jedno opracowanie z wyraźnie rozdzielonymi częściami A1–A5 i T1–T3. Każde ustalenie powinno wskazywać kryterium, dowód, ocenę wpływu i rekomendację. Należy dokumentować zakres rzeczywiście wykonanych testów, ograniczenia i wyniki próby odtworzenia. Materiały należy przekazać po polsku w wersji edytowalnej i PDF, a rejestry oraz macierze w formacie arkusza kalkulacyjnego.

Ocena szkoleń i usług utrzymania obejmuje stan i dowody dostępne do dnia badania. Nie potwierdza realizacji przyszłego okresu dostępu do platformy szkoleniowej ani przyszłego utrzymania MDR/SOC.

9 Terminy i odbiór

Audyt prowadzi się etapami od zawarcia umowy: najpierw przegląd dostępnych dokumentów i istniejącego środowiska, następnie badanie przyjętej dokumentacji SZBI/SZCD oraz niezależne testy uruchomionych rozwiązań IT/OT i SCADA. PEKO przekazuje końcową dokumentację do 11 grudnia i zapewnia gotowość całego środowiska do 14 grudnia 2026 r. Zasadnicze badania i raport do uwag należy zakończyć do 18 grudnia; poprawki zabezpieczeń do ponownej weryfikacji PEKO lub dostawcy wykonują do 22 grudnia. Ponowna weryfikacja i podpisany raport końcowy mają być przekazane do 28 grudnia, a usunięcie wad raportu do 29 grudnia. Odbiór i doręczenie prawidłowej faktury do 30 grudnia; płatność do 31 grudnia 2026

r., zgodnie z umową. Odbiór wymaga kompletnego audytu, testów, raportów i rozpatrzenia uwag; nie zależy od pozytywnej oceny bezpieczeństwa. Cena obejmuje wszystkie prace, dojazdy, narzędzia, raportowanie, prezentację i poprawki.

10 Poufność i prawa do wyników

Dane PEKO, wyniki audytu i informacje o zabezpieczeniach są poufne. Wykonawca zapewni upoważniony personel, niezbędny zakres dostępów, szyfrowaną wymianę i przechowywanie oraz oddzielne przekazywanie haseł do plików. Dane i kopie pozostają w UE. Przed dostępem strony ustalą role w RODO i zawrą potrzebną umowę powierzenia oraz zobowiązania do poufności. Podwykonawca i dalsze powierzenie wymagają uprzedniej pisemnej akceptacji PEKO.

Zdalny dostęp z państwa trzeciego wymaga odrębnej uprzedniej pisemnej zgody i spełnienia RODO, przy zachowaniu przechowywania w UE. Zakazuje się własnego marketingu, profilowania i trenowania AI na danych PEKO. Naruszenie danych Wykonawca zgłasza niezwłocznie, najpóźniej w ciągu 24 godzin od stwierdzenia; dla zagrożeń z części 4a obowiązuje krótszy termin.

Umowa zapewni PEKO przechowywanie, kopiowanie, wewnętrzne udostępnianie i aktualizację raportów oraz przekazywanie ich organom, kontrolującym i wykonawcom działań naprawczych. Prawa do narzędzi osób trzecich nie mogą ograniczać użycia wyników. Po odbiorze Wykonawca rozliczy dostępy, zwróci materiały i potwierdzi usunięcie kopii zgodnie z umową i prawem. Poufność obowiązuje także po zakończeniu usługi.

11 Informacje o środowisku

Skalę środowiska i warunki wyceny określa załącznik nr 2A. Dane około 12 stanowisk IT i docelowo 5 stanowisk OT są orientacyjne. Audytor dobiera i uzasadnia reprezentatywną próbę oraz obiekty do wizyt na podstawie ryzyka, wiedzy, doświadczenia i informacji uzyskanych podczas audytu. Dobór uwzględnia siedzibę, PSZOK oraz reprezentatywne obiekty wodociągowe i kanalizacyjne, przy co najmniej dwóch dniach roboczych na miejscu. Nie wymaga się aktywnego testowania każdego sterownika ani wizyty w każdym obiekcie. Plan nie może pomijać żadnej z ośmiu pozycji A1–A5 i T1–T3 ani zastępować testów analizą projektu. Ograniczenia należy uzasadnić i wskazać bezpieczny sposób sprawdzenia.

Szkolenia, cztery kampanie phishingowe i ćwiczenie reagowania są realizowane odrębnie w postępowaniu ADM.014.2026.10.AS. Audytor ocenia ich dowody, bez powtarzania tych usług. Planowane rozwiązania nie stanowią dowodu ich wdrożenia. Ograniczenia i elementy niesprawdzone należy wykazać w raporcie.

T1–T3 są niezależnymi testami bezpieczeństwa audytora po wdrożeniu. Testy funkcjonalne, odbiorowe, pierwsze skanowanie i usuwanie wad należą do wykonawców wdrożeń; ich protokoły są materiałem wejściowym. Audytor określi własne cele, metody i wyniki T1–T3 oraz odróżni je od dostarczonych protokołów. Nie rozlicza jako własnej usługi czynności wykonanych przez integratora. Obserwacja próby odtworzenia może odbyć się przy teście integratora; audytor rozlicza wyłącznie własną obserwację i ocenę.

Signature Not Verified

Dokument podpisany przez Julia Nowak
Data: 2026.11.10 15:36:19 CET