Załącznik nr 2A do zaproszenia do złożenia oferty

Skala środowiska i warunki audytu

Numer postępowania ADM.016.2026.10.AS

Kosakowo, 9 listopada 2026 r.

Załącznik określa dane do wyceny oraz organizację audytu A1–A5 i testów T1–T3. Dane o stanowiskach są orientacyjne, a zakres modernizacji nie stanowi dowodu jej zakończenia. Audyt obejmuje stan rzeczywisty i własne dowody audytora.

1 Organizacja i środowisko

Obszar	Dane do przygotowania oferty
Organizacja	PEKO, ul. Chrzanowskiego 44, 81-198 Kosakowo; do 45 pracowników. Działalność wodociągowa, kanalizacyjna, PSZOK oraz procesy biurowe i pomocnicze.
Stanowiska	Około 12 komputerów IT i docelowo 5 stanowisk OT. Są to wielkości orientacyjne przekazane przez PEKO, nie potwierdzona inwentaryzacja ani liczba sterowników. Audytor zweryfikuje strukturę zasobów i dobierze reprezentatywną próbę.
Serwery i kopie	Modernizacja: 2 fizyczne serwery HA, 1 serwer kopii zapasowych, 2 NAS, platforma wirtualizacji i maksymalnie 10 VM. Dokumentacja badania rozróżni stan istniejący i rozwiązania uruchomione w projekcie.
Sieć i dostęp	Modernizacja: 3 UTM (1 brzegowy, 2 segmentacyjne IT–iDMZ–OT), 2 przełączniki rdzeniowe i 3 dostępowe; VLAN i 802.1X, 1 kontroler Wi-Fi, 3 punkty dostępowe, WPA3-Enterprise; AD/GPO/MFA, 3 stacje przesiadkowe i 3 tokeny.
Ochrona i ciągłość	PAM oraz monitoring i aktualizacje dla 30 urządzeń końcowych; 30 nie oznacza całej floty PEKO. SIEM/SOAR, zarządzanie podatnościami, MDR/SOC, EDR i monitoring zagrożeń OT. Serwerownia: UPS, monitoring środowiska i agregat z SZR/ATS.
SCADA i telemetria	Opis wyjściowy: Wizcon 9.4, 2166 tagów aplikacji, w tym 1589 tagów PLC; jedna licencja serwerowo-obiektowa bez dodatkowych stacji View, Modbus RTU i SMS. Tagi są zmiennymi, nie liczbą PLC/RTU ani obiektów. Badaniu podlega konfiguracja rzeczywiście uruchomiona po modernizacji SCADA.

2 Dobór próby i obiektów

Audytor samodzielnie dobiera i uzasadnia próbę oraz obiekty wymagające wizyty, na podstawie ryzyka, wiedzy, doświadczenia i informacji pozyskanych w audycie. Plan uwzględnia siedzibę PEKO, PSZOK oraz reprezentatywne obiekty wodociągowe i kanalizacyjne na terenie gminy Kosakowo. Cena obejmuje co najmniej dwa dni robocze czynności na miejscu, potrzebne dojazdy oraz spotkanie otwierające i końcowe. Nie przewiduje się obowiązku wizyty w każdym obiekcie ani aktywnego testu każdego PLC/RTU.

Ocena architektury i separacji IT/OT obejmuje zależności całego środowiska objętego zamówieniem; szczegółowe badania prowadzi się na reprezentatywnej próbie zasobów i konfiguracji. Audytor opisze jej liczebność, kryteria doboru, zakres faktycznie sprawdzony i ograniczenia. Zmiana doboru próby nie może usuwać żadnej z ośmiu pozycji A1–A5 i T1–T3 ani zastępować testów samą analizą dokumentacji.

Materiały eksploatacyjne wskazują także Synology i Synology Drive, pocztę oraz stronę WWW w domenie pukpeko.pl, Symfonię, Firma2, R2Płatnika i Płatnika. Audyt uwzględni zależności i zabezpieczenia tych usług, BDO oraz dostępu dostawców. Zasoby zewnętrznego dostawcy można aktywnie badać wyłącznie za zgodą właściciela i w granicach upoważnienia. Zamówienie nie obejmuje odrębnego pełnego testu penetracyjnego każdej aplikacji biznesowej.

3 Środowisko testowe SCADA i odtworzenie

PEKO zapewnia z integratorem przygotowanie odseparowanego środowiska testowego SCADA na infrastrukturze serwerów wirtualnych instalowanej w projekcie. Obejmuje to potrzebne zasoby VM, instalację, konfigurację, legalną możliwość użycia licencji w testach, dane oraz udział upoważnionego administratora lub integratora. Gotowość środowiska wraz z bezpiecznym dostępem nastąpi najpóźniej 14 grudnia 2026 r. Audytor zapewnia własne narzędzia i metody badania; nie buduje w swojej cenie pełnej repliki instalacji technologicznej.

T3 obejmuje jedną aplikację SCADA PEKO: uwierzytelnianie, role i uprawnienia, sesje i dostęp zdalny, rejestrowanie zdarzeń, bezpieczeństwo konfiguracji, komunikację i znane podatności w dostępnym zakresie. Sterowanie rzeczywistymi urządzeniami musi być zablokowane; funkcje mogą być sprawdzane z użyciem symulacji. Testy ingerujące w aplikację odbywają się w izolacji, bez połączenia wykonawczego z produkcyjnymi PLC/RTU.

Próba odtworzenia obejmie co najmniej aplikację SCADA z konfiguracją i dostępnymi danymi archiwalnymi, z rzeczywistej kopii do odseparowanej VM. Operatora i obsługę integratora zapewnia PEKO. Audytor obserwuje przebieg, mierzy czas, ocenia punkt odzyskania danych oraz sprawdza uruchomienie, dostęp i zgodność odtworzonych danych lub funkcji. Próba nie uruchamia sterowania produkcyjnego. Uzgodnienie terminu i szczegółów w planie nie zastępuje faktycznej próby.

4 Gotowość i dostęp do materiałów

Audyt rozpoczyna się od dostępnej dokumentacji i istniejącego OT, bez oczekiwania na całość nowych wdrożeń. Końcowe SZBI, SZCD, BIA, BCP i DRP PEKO przekaże do 11 grudnia 2026 r. Dokumentacja powykonawcza, cała infrastruktura objęta badaniem, w tym IT i separacja IT/OT, dostępy oraz środowisko testowe będą udostępnione najpóźniej 14 grudnia. Są to obowiązki organizacyjne Zamawiającego, a nie potwierdzenie obecnej gotowości.

PEKO udostępnia wersje polityk i procedur, analizy ryzyka, rejestry, protokoły wdrożeniowe, umowy i dowody odtwarzania oraz posiadane decyzje lub wpisy dotyczące KSC. Audytor ustala ich rzeczywisty status i zastosowanie przepisów w A3. Braku dokumentu, wdrożenia lub dowodu nie zastępuje założeniem spełnienia wymagania. Projekty dokumentacji można przeglądać wcześniej, ale końcowa ocena SZBI/SZCD uwzględnia przyjęte wersje i dowody stosowania.

Dowody szkoleń, kampanii phishingowych i ćwiczenia PEKO przekazuje sukcesywnie do 16 grudnia; uzupełnienia niezwłocznie do zakończenia badania. Audyt nie potwierdza przyszłego okresu dostępu do platformy ani usług utrzymania. Brak gotowości zgłasza się natychmiast z wpływem na harmonogram. Nie można uznać testu projektu rozwiązania za test rozwiązania działającego.

5 Współpraca i granice odpowiedzialności

PEKO organizuje dostęp do właścicieli procesów i administratorów IT/OT, udział integratorów, potrzebne licencje i zgody dostawców oraz bezpieczne okna prac. Imienne kontakty, adresy zasobów, upoważnienia, kopie, metody, warunki przerwania i kontakt alarmowy ustala się w planie przed testami. Audytor odpowiada za dobór próby i metodykę, bezpieczeństwo własnych czynności, niezależne dowody i rzetelność wniosków.

Testy funkcjonalne i odbiorowe integratorów są materiałem wejściowym. T1–T3 wymagają własnych niezależnych sprawdzeń audytora. Wspólna próba odtworzenia jest dopuszczalna przy odrębnej obserwacji i ocenie audytora; nie rozlicza się ponownie tych samych czynności integratora. Instruktaż dokumentacji, szkolenia i opracowanie D1–D3 nie należą do tego zamówienia.

Lokalizacji krytycznych, adresacji, poświadczeń i podatności nie publikuje się w ogłoszeniu. Materiały potrzebne do wyceny PEKO udostępnia na równych zasadach zgodnie z zaproszeniem. Poufność, przetwarzanie danych i bezpieczne metody określają OPZ i umowa.

6 Terminy audytu i odbioru

Zasadnicze badania i raport do uwag: 18 grudnia; uwagi PEKO: 21 grudnia; poprawki zabezpieczeń PEKO lub integratorów: 22 grudnia; jedna ponowna weryfikacja i podpisany raport końcowy: 28 grudnia; usunięcie wad raportu: 29 grudnia; odbiór i faktura: 30 grudnia; płatność: 31 grudnia 2026 r. Szczegółowe godziny i zasady określa umowa. Nieusunięte podatności pozostają otwarte; nie są same w sobie wadą rzetelnie wykonanego audytu.