

Opis Przedmiotu Zamówienia
do postępowania na realizację zamówienia pn.:

Opracowanie, wdrożenie, przegląd, aktualizacja
Systemu Zarządzania Bezpieczeństwem Informacji

Część 1

1. Przedmiot zamówienia

Przedmiotem zamówienia jest **kompleksowa aktualizacja, dostosowanie, wdrożenie oraz przeprowadzenie przeglądu Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) funkcjonującego u Zamawiającego.**

Realizacja zamówienia obejmuje działania o charakterze analitycznym, wdrożeniowym, audytowym oraz doskonalącym, których rezultatem będzie spójny, kompletny i funkcjonujący System Zarządzania Bezpieczeństwem Informacji, zgodny z aktualnymi wymaganiami normatywnymi, prawnymi oraz rzeczywistymi uwarunkowaniami organizacyjnymi i technicznymi Zamawiającego.

Zamówienie nie ogranicza się do aktualizacji dokumentacji, lecz obejmuje również wdrożenie procesów, mechanizmów oraz zasad zarządzania bezpieczeństwem informacji w sposób zapewniający ich rzeczywiste funkcjonowanie w organizacji.

2. Podstawa normatywna i wymagania prawne

System Zarządzania Bezpieczeństwem Informacji powinien zostać opracowany i wdrożony zgodnie z:

- **PN-EN ISO/IEC 27001:2023-08 (ISO/IEC 27001:2022)** – Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania,
- **PN-EN ISO/IEC 27002:2023-01 (ISO/IEC 27002:2022)** – Technika informatyczna – Techniki bezpieczeństwa – Wytyczne dotyczące zabezpieczeń bezpieczeństwa informacji,
- **PN-EN ISO/IEC 27005:2025-01 (ISO/IEC 27005:2022)** – Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji,

w zakresie mającym zastosowanie do działalności, struktury organizacyjnej, procesów oraz środowiska technicznego Zamawiającego.

Wdrożenie powinno również uwzględniać wymagania wynikające z:

- ustawy o krajowym systemie cyberbezpieczeństwa,
- dyrektywy NIS2,
- Krajowych Ram Interoperacyjności,
- przepisów o ochronie danych osobowych (RODO).

W przypadku infrastruktury OT należy uwzględnić również wymagania norm serii IEC 62443.

3. Zakres przedmiotu zamówienia

3.1. Aktualizacja SZBI

Dostosowanie istniejącego SZBI do wymagań norm wskazanych w pkt 2, obejmujące w szczególności:

- dokumentację SZBI,
- procesy zarządzania bezpieczeństwem informacji,
- zabezpieczenia organizacyjne i techniczne,

oraz zapewnienie zgodności SZBI z wymaganiami norm i przepisów prawa.

3.2. Weryfikacja i uzupełnienie dokumentacji SZBI

Zakres obejmuje:

- przegląd istniejącej dokumentacji SZBI,
- identyfikacja braków, niespójności oraz obszarów wymagających aktualizacji,
- aktualizacja dokumentów,
- opracowanie brakujących elementów dokumentacji, w tym:
 - polityk,
 - procedur,
 - instrukcji,
 - rejestrów,
 - formularzy,

- zasad monitorowania i oceny skuteczności SZBI,
- prowadzenie warsztatów roboczych z Zamawiającym w celu opracowania i uzgodnienia dokumentacji,
- dostosowanie dokumentacji do rzeczywistego sposobu funkcjonowania organizacji.

Dokumentacja musi być kompletna, spójna oraz możliwa do stosowania w praktyce.

3.3. Analiza ryzyka

Zakres obejmuje:

- weryfikacja istniejącej analizy ryzyka,
- aktualizacja lub przeprowadzenie analizy ryzyka zgodnie z PN-EN ISO/IEC 27005:2025-01,
- identyfikacja aktywów, zagrożeń, podatności i scenariuszy ryzyka,
- ocena ryzyka,
- opracowanie lub aktualizacja:
 - rejestru ryzyk,
 - planu postępowania z ryzykiem.

Analiza musi być oparta na rzeczywistych warunkach funkcjonowania Zamawiającego.

3.4. Statement of Applicability (SoA)

Zakres obejmuje:

- przegląd istniejącego SoA,
- aktualizacja zgodnie z PN-EN ISO/IEC 27002:2023-01,
- powiązanie zabezpieczeń z ryzykiem, dokumentacją oraz dowodami wdrożenia.

3.5. Wdrożenie SZBI

Zakres obejmuje:

- wdrożenie zaktualizowanych zasad i procedur,
- przypisanie ról i odpowiedzialności,
- uruchomienie procesów:
 - zarządzania incydentami,
 - zarządzania ryzykiem,
 - nadzoru nad dokumentacją,
 - monitorowania i oceny skuteczności SZBI,
- zapewnienie funkcjonowania SZBI w praktyce.

Wdrożenie ma zapewnić prawidłowe funkcjonowanie SZBI u Zamawiającego.

3.6. Audyt wewnętrzny SZBI

Zakres obejmuje:

- przeprowadzenie audytu zgodnie z ISO/IEC 27001:2022 (pkt 9.2),
- ocena zgodności i skuteczności SZBI,
- identyfikacja niezgodności i rekomendacji.

Audyt ma być przeprowadzony w pełnym zakresie funkcjonowania SZBI.

3.7. Przegląd zarządzania

Zakres obejmuje:

- przygotowanie danych wejściowych,
- przeprowadzenie przeglądu zgodnie z ISO/IEC 27001:2022 (pkt 9.3 normy),
- opracowanie protokołu przeglądu.

Przegląd zarządzania ma być przeprowadzony w całym zakresie funkcjonowania SZBI.

3.8. Weryfikacja funkcjonowania SZBI

Zakres obejmuje:

- udział w kontrolach wewnętrznych lub testach stosowania procedur,
- weryfikacja stosowania SZBI przez pracowników,
- identyfikacja obszarów wymagających korekty.

4. Charakter zamówienia

Zamówienie ma charakter:

- aktualizacyjny,
- wdrożeniowy,

- doskonalący,
- dostosowujący do wymagań normatywnych i prawnych,
- przygotowujący do audytu zewnętrznego i kontroli.

5. Efekt realizacji zamówienia

W wyniku realizacji zamówienia Zamawiający uzyska:

- zaktualizowany i kompletny SZBI,
- wdrożone i funkcjonujące procesy bezpieczeństwa informacji,
- aktualną analizę ryzyka,
- Statement of Applicability,
- przeprowadzony audyt wewnętrzny,
- przeprowadzony przegląd zarządzania.

6. Kluczowe wymaganie

Wdrożenie SZBI musi zapewniać jego praktyczne stosowanie, w szczególności:

- przypisanie ról i odpowiedzialności,
- realizację procedur przez personel,
- możliwość wykazania funkcjonowania SZBI w trakcie audytu lub kontroli,
- zapewnienie ciągłości funkcjonowania systemu po zakończeniu realizacji zamówienia.

7. Warunki odbioru przedmiotu zamówienia

Odbiór przedmiotu zamówienia nastąpi po potwierdzeniu przez Zamawiającego, że SZBI został nie tylko opracowany, lecz również wdrożony i funkcjonuje w praktyce.

Warunkiem odbioru jest w szczególności:

7.1. Weryfikacja dokumentacji

- przekazanie kompletnej dokumentacji SZBI,
- zgodność dokumentacji z wymaganiami norm wskazanych w OPZ,
- spójność dokumentów oraz ich dostosowanie do organizacji Zamawiającego.

7.2. Weryfikacja wdrożenia SZBI

- potwierdzenie przypisania ról i odpowiedzialności,
- potwierdzenie uruchomienia procesów bezpieczeństwa informacji,
- wyników raportu z monitorowania i stanu funkcjonowania SZBI,
- dostępność rejestrów i zapisów potwierdzających funkcjonowanie SZBI.

7.3. Weryfikacja stosowania SZBI przez pracowników

Zamawiający zastrzega możliwość przeprowadzenia:

- wywiadów z pracownikami,
- sprawdzenia znajomości podstawowych zasad bezpieczeństwa informacji,
- weryfikacji stosowania procedur w praktyce.

7.4. Test funkcjonowania SZBI

W ramach odbioru Zamawiający może przeprowadzić test obejmujący w szczególności:

- symulację incydentu bezpieczeństwa informacji,
- weryfikację sposobu jego zgłoszenia i obsługi,
- ocenę współpracy pomiędzy osobami odpowiedzialnymi.

7.5. Audyt i przegląd zarządzania

Zakres obejmuje:

- przekazanie raportu z audytu wewnętrznego,
- przekazanie raportu z monitorowania i stanu funkcjonowania,
- przekazanie protokołu przeglądu zarządzania,
- uwzględnienie zidentyfikowanych niezgodności lub rekomendacji.

Należy uwzględnić działania naprawcze w zakresie systemu SZBI.

8. Wymagania szczególne – zgodność z KSC, NIS2 oraz wymagania kontrolne.

W celu zapewnienia zgodności z wymaganiami regulacyjnymi oraz możliwości pozytywnej weryfikacji przez organy nadzorcze (w tym właściwe organy ds. cyberbezpieczeństwa, audytorów zewnętrznych oraz instytucje kontrolne), Zamawiający wprowadza następujące wymagania szczególne:

8.1. Wymagania dowodowe

Każdy element SZBI musi posiadać **dowody wdrożenia i funkcjonowania**, w szczególności:

- rejestry (np. ryzyk, incydentów, dostępów),
- zapisy z realizacji procesów,
- potwierdzenia szkoleń,
- logi systemowe,
- protokoły przeglądów,
- wyniki monitorowania i pomiarów.

Wykonawca zobowiązany jest wskazać w dokumentacji:

- miejsce przechowywania dowodów,
- odpowiedzialność za ich utrzymanie,
- sposób ich weryfikacji.

8.2. Zgodność z wymaganiami KSC i NIS2

Wdrożony SZBI musi uwzględniać wymagania wynikające z:

- ustawy o krajowym systemie cyberbezpieczeństwa,
- dyrektywy NIS2 (w zakresie adekwatnym do statusu Zamawiającego),

w szczególności w zakresie:

- zarządzania ryzykiem cyberbezpieczeństwa,
- obsługi incydentów,
- ciągłości działania,
- zarządzania dostępem,
- bezpieczeństwa systemów i sieci,
- nadzoru nad dostawcami,
- raportowania i dokumentowania zdarzeń.

8.3. Spójność SZBI z rzeczywistym środowiskiem IT/OT

Wykonawca zobowiązany jest zapewnić, że:

- analiza ryzyka obejmuje rzeczywiste systemy i infrastrukturę,
- zabezpieczenia są adekwatne do stosowanych technologii,
- SZBI uwzględnia powiązania między systemami IT i OT,
- nie stosuje się rozwiązań abstrakcyjnych lub oderwanych od środowiska Zamawiającego.

8.4. Wymóg przygotowania do kontroli i audytu

Wykonawca zobowiązany jest przygotować SZBI w sposób umożliwiający jego ocenę przez:

- organy nadzorcze w zakresie KSC,
- podmioty kontrolne (np. NIK, instytucje finansujące),
- audytu zewnętrznego dotyczącego zgodności z wymaganiami prawnymi oraz certyfikującymi.

W szczególności wymagane jest:

- uporządkowanie dokumentacji,
- zapewnienie spójności zapisów,
- powiązanie dokumentów z wymaganiami norm,
- przygotowanie dowodów wdrożenia.

8.5. Zakaz stosowania rozwiązań pozornych

Zabrania się stosowania rozwiązań:

- niewdrożonych w praktyce,
- niespójnych z rzeczywistym funkcjonowaniem organizacji,
- nieposiadających dowodów realizacji,
- opracowanych wyłącznie w celu spełnienia wymagań formalnych.

W przypadku stwierdzenia takich rozwiązań Zamawiający ma prawo uznać zamówienie za nienależycie wykonane.

8.6. Wymóg trwałości SZBI

Wykonawca zobowiązany jest zapewnić, że:

- SZBI może być utrzymywany przez Zamawiającego po zakończeniu projektu,
- dokumentacja zawiera jasne zasady utrzymania i przeglądów,
- personel Zamawiającego posiada wiedzę umożliwiającą dalsze funkcjonowanie systemu.

8.7. Wymóg adekwatności i proporcjonalności

Zastosowane środki bezpieczeństwa muszą być:

- adekwatne do poziomu ryzyka,
- proporcjonalne do skali działalności Zamawiającego,
- możliwe do utrzymania organizacyjnie i finansowo.

9. Wymagania w zakresie kompetencji Wykonawcy oraz osób realizujących zamówienie

9.1. Wymagania ogólne wobec Wykonawcy

Wykonawca musi posiadać wiedzę, doświadczenie oraz potencjał organizacyjny umożliwiający realizację zamówienia o charakterze kompleksowym, obejmującym:

- analizę i ocenę systemów bezpieczeństwa informacji,
- projektowanie i wdrażanie SZBI,
- przeprowadzanie analizy ryzyka zgodnie z ISO/IEC 27005,
- opracowywanie dokumentacji zgodnej z ISO/IEC 27001 i ISO/IEC 27002,
- prowadzenie audytów SZBI,
- wdrażanie wymagań wynikających z KSC, KRI oraz NIS2.

9.2. Doświadczenie Wykonawcy

Wykonawca musi wykazać, że w okresie ostatnich **3 lat** przed upływem terminu składania ofert zrealizował co najmniej:

- **2 usługi** polegające na:
 - wdrożeniu lub aktualizacji Systemu Zarządzania Bezpieczeństwem Informacji z ISO/IEC 27001,
 - realizacji projektów obejmujących analizę ryzyka, dokumentację SZBI oraz audyt,

Każda usługa musi być potwierdzona referencjami lub dokumentami potwierdzającymi należyte wykonanie.

9.3. Zespół realizujący zamówienie

Wykonawca musi zapewnić realizację zamówienia przez zespół składający się z co najmniej **2 osób**, spełniających łącznie poniższe wymagania.

9.3.1. Audytor wiodący / Lider SZBI

Co najmniej jedna osoba musi:

- posiadać certyfikat:
 - Audytora Wiodącego ISO/IEC 27001
 - posiadać minimum **3-letnie doświadczenie** w realizacji projektów SZBI,
- brać udział w realizacji co najmniej:
 - **2 projektów** związanych z wdrożeniem i audytem SZBI,
- posiadać doświadczenie w:
 - analizie ryzyka,
 - opracowaniu dokumentacji SZBI,
 - audytach zgodnych z ISO/IEC 27001.

Osoba ta pełni funkcję kierownika merytorycznego projektu.

9.3.2. Specjalista ds. bezpieczeństwa technologicznego

Co najmniej jedna osoba musi:

- posiadać:
 - wykształcenie wyższe informatyczne
 - minimum **3-letnie doświadczenie** w administrowaniu lub bezpieczeństwie systemów IT,
- posiadać doświadczenie w:
 - zabezpieczeniach systemów IT,
 - analizie środowisk teleinformatycznych,
 - wdrażaniu rozwiązań bezpieczeństwa,
 - znajomości funkcjonowania infrastruktury OT.

- brać udział w co najmniej:

- 2 projektach związanych z bezpieczeństwem informacji lub cyberbezpieczeństwem.

9.4. Kompetencje branżowe

Wykonawca powinien dysponować osobą posiadającą:

- doświadczenie w obszarze bezpieczeństwa systemów przemysłowych,
- znajomość norm serii IEC 62443,
- doświadczenie w integracji środowisk IT/OT.

9.5. Wymagania w zakresie znajomości regulacji

Osoby realizujące zamówienie muszą posiadać praktyczną znajomość:

- ISO/IEC 27001,
- ISO/IEC 27002,
- ISO/IEC 27005,
- KSC,
- KRI,
- NIS2.

9.6. Wymagania organizacyjne

Wykonawca zobowiązany jest:

- zapewnić ciągłość zespołu projektowego przez cały okres realizacji,
- wskazać osobę odpowiedzialną za kontakt z Zamawiającym,
- zapewnić dostępność zespołu w trakcie realizacji,
- realizować prace w sposób umożliwiający współpracę z personelem Zamawiającego.

Zmiana kluczowych członków zespołu wymaga zgody Zamawiającego i musi dotyczyć osób o równoważnych lub wyższych kwalifikacjach.

10. Okres realizacji

Przedmiot zamówienia należy zrealizować do 10 listopada 2026 r.

Wykonawca zobowiązany jest tak zorganizować realizację prac, aby wszystkie wymagane działania analityczne, dokumentacyjne, wdrożeniowe, szkoleniowe i testowe zostały zakończone w terminie określonym przez Zamawiającego.

Zamawiający zastrzega możliwość wydłużenia terminu, uwzględniając zmianę terminu realizacji projektu „Cyberbezpieczny Wodociąg” przed Grantodawcą.

11. Postanowienia końcowe

Wykonawca ponosi odpowiedzialność za kompletność, jakość, spójność oraz operacyjność wdrożonego Systemu Zarządzania Bezpieczeństwem Informacji, a także za zgodność rezultatów z wymaganiami określonymi w niniejszym Opisie Przedmiotu Zamówienia.

Wykonawca przekazuje prawa autorskie dokumentacji wykonanej zgodnie z zamówieniem Zamawiającego.

Zamawiający zastrzega możliwość oceny wdrożenia przez zewnętrznego audytora. Oznacza to, że rezultaty realizacji zamówienia powinny być przygotowane w sposób umożliwiający ich niezależną ocenę pod kątem zgodności, kompletności i przydatności praktycznej.

Część 2

Opracowanie i wdrożenie Systemu Zarządzania Ciągłością Działania STI (SZCD) oraz opracowanie planów ciągłości działania (BCP) i planów odtwarzania po awarii (DRP) dla systemów teleinformatycznych (STI)

1. Przedmiot zamówienia

Przedmiotem zamówienia jest opracowanie oraz wdrożenie Systemu Zarządzania Ciągłością Działania dla systemów teleinformatycznych (SZCD), obejmującego środowisko IT oraz OT, w tym systemy wspierające i realizujące procesy technologiczne, wraz z opracowaniem i wdrożeniem planów ciągłości działania (BCP) oraz planów odtwarzania po awarii (DRP).

Przez realizację zamówienia należy rozumieć wykonanie pełnego cyklu prac analitycznych, projektowych, dokumentacyjnych, wdrożeniowych i testowych, których rezultatem będzie funkcjonujący, spójny i możliwy do praktycznego zastosowania system zarządzania ciągłością działania. Zamówienie nie ma charakteru wyłącznie doradczego ani wyłącznie dokumentacyjnego. Efektem jego realizacji ma być wdrożenie rozwiązań, które będą mogły zostać wykorzystane operacyjnie w przypadku zakłócenia działalności, awarii, incydentu bezpieczeństwa lub innego zdarzenia kryzysowego.

System powinien zapewnić zdolność organizacji do:

- utrzymania realizacji kluczowych procesów,
- zapewnienia ciągłości usług krytycznych,
- ograniczenia skutków incydentów i awarii,
- sprawnego przywracania funkcjonowania systemów i infrastruktury,
- zapewnienia gotowości organizacji do działania w warunkach zakłóceń.

2. Zakres zamówienia

Zakres zamówienia obejmuje opracowanie i wdrożenie Systemu Zarządzania Ciągłością Działania w odniesieniu do kluczowych obszarów funkcjonowania organizacji, ze szczególnym uwzględnieniem zależności pomiędzy procesami organizacyjnymi, systemami IT, środowiskiem OT oraz infrastrukturą techniczną.

System powinien obejmować w szczególności:

- procesy organizacyjne i technologiczne,
- systemy teleinformatyczne wspierające działalność operacyjną i zarządczą,
- środowiska IT i OT, w tym systemy SCADA, HMI, PLC, systemy telemetryczne oraz inne elementy automatyki przemysłowej,
- infrastrukturę serwerową, sieciową, zasilającą i backupową,
- zasoby ludzkie niezbędne do utrzymania ciągłości działania,
- mechanizmy komunikacji kryzysowej,
- procedury reagowania na incydenty, awarie i sytuacje nadzwyczajne,
- mechanizmy odtwarzania usług, danych, systemów i infrastruktury.

Zakres zamówienia obejmuje również identyfikację oraz opis powiązań pomiędzy środowiskiem IT i OT, a także ocenę wpływu zakłóceń w tych obszarach na zdolność organizacji do realizacji usług i procesów krytycznych.

3. Podstawa normatywna i prawna

Przedmiot zamówienia należy zrealizować z uwzględnieniem wymagań aktualnych norm, dobrych praktyk oraz obowiązujących przepisów prawa odnoszących się do ciągłości działania, bezpieczeństwa informacji i cyberbezpieczeństwa.

W szczególności należy uwzględnić:

- ISO 22301:2019 – System zarządzania ciągłością działania – wymagania,
- ISO 22313:2020 – Wytyczne dotyczące wdrażania systemu zarządzania ciągłością działania,
- ISO 22317:2021 – Wytyczne dotyczące analizy wpływu na działalność (BIA),
- ISO 22318:2021 – Ciągłość działania w relacjach z dostawcami,
- ISO/IEC 27001:2022 – System zarządzania bezpieczeństwem informacji,
- ISO/IEC 27002:2022 – Zabezpieczenia bezpieczeństwa informacji,
- ISO/IEC 27005:2022 – Zarządzanie ryzykiem bezpieczeństwa informacji,
- ISO/IEC 27031:2011 – Gotowość ICT do zapewnienia ciągłości działania,
- normy serii IEC 62443 – w zakresie środowisk OT i systemów automatyki przemysłowej.

W zakresie zgodności prawnej należy uwzględnić co najmniej:

- Krajowe Ramy Interoperacyjności,
- ustawę o krajowym systemie cyberbezpieczeństwa,
- wymagania wynikające z dyrektywy NIS2,
- inne obowiązujące przepisy prawa krajowego i branżowego, o ile mają zastosowanie do działalności Zamawiającego.

4. Cel realizacji zamówienia

Celem realizacji zamówienia jest podniesienie odporności organizacji na zdarzenia zakłócające jej działalność oraz zapewnienie zdolności do utrzymania albo szybkiego przywrócenia realizacji procesów krytycznych i usług kluczowych.

Realizacja zamówienia ma doprowadzić w szczególności do:

- uporządkowania obszaru ciągłości działania w ujęciu organizacyjnym, technicznym i proceduralnym,
- identyfikacji procesów, usług i zasobów krytycznych,
- określenia dopuszczalnych parametrów przerwy w działalności, w tym RTO, RPO i MTPD,
- opracowania skutecznych strategii ciągłości działania i odtwarzania po awarii,
- wdrożenia dokumentacji możliwej do praktycznego wykorzystania,
- przygotowania personelu do działania w sytuacjach kryzysowych,
- potwierdzenia skuteczności rozwiązań poprzez testy i ćwiczenia.

W przypadku organizacji wykorzystujących środowiska IT/OT celem zamówienia jest również zapewnienie ciągłości funkcjonowania procesów technologicznych i zależnych od nich systemów teleinformatycznych, z uwzględnieniem bezpieczeństwa operacyjnego oraz specyfiki infrastruktury przemysłowej.

5. Zakres prac wymaganych od Wykonawcy

5.1. Analiza stanu obecnego

W pierwszym etapie realizacji zamówienia Wykonawca przeprowadzi analizę stanu obecnego organizacji w zakresie przygotowania do zapewnienia ciągłości działania. Analiza ta powinna obejmować zarówno obszary organizacyjne, jak i techniczne, w tym istniejące procedury, zasady reagowania, zasoby oraz rozwiązania stosowane w środowiskach IT i OT.

Analiza stanu obecnego powinna obejmować w szczególności:

- analizę procesów organizacyjnych i technologicznych,
- analizę systemów teleinformatycznych i ich roli w realizacji procesów,
- analizę infrastruktury technicznej, w tym serwerów, sieci, systemów backupu, wirtualizacji oraz infrastruktury OT,
- analizę istniejących mechanizmów bezpieczeństwa i odporności,
- analizę obowiązującej dokumentacji,
- analizę sposobu reagowania na incydenty, awarie i zakłócenia działalności.

Rezultatem tego etapu powinien być raport zawierający:

- ocenę poziomu dojrzałości organizacji w obszarze ciągłości działania,
- identyfikację luk i obszarów wymagających poprawy,
- rekomendacje dotyczące wdrożenia SZCD, BCP oraz DRP.

5.2. Analiza wpływu na działalność (BIA)

Wykonawca przeprowadzi analizę wpływu na działalność (Business Impact Analysis), której celem będzie identyfikacja procesów, usług i zasobów krytycznych oraz określenie skutków ich zakłócenia lub niedostępności.

Analiza BIA powinna obejmować:

- identyfikację procesów krytycznych,
- identyfikację usług krytycznych,
- identyfikację zasobów wspierających realizację tych procesów i usług,
- określenie zależności pomiędzy procesami, systemami, personelem i infrastrukturą,
- ocenę skutków przerwy w działalności w różnych perspektywach czasowych.

W ramach BIA należy określić co najmniej:

- RTO – docelowy czas odtworzenia,
- RPO – dopuszczalny poziom utraty danych,
- MTPD – maksymalny tolerowany okres zakłócenia.

Analiza BIA nie może mieć charakteru wyłącznie teoretycznego. Musi zostać przeprowadzona na podstawie rzeczywistych danych uzyskanych w toku prac z udziałem przedstawicieli Zamawiającego. W związku z tym Wykonawca zobowiązany jest do:

- przeprowadzenia warsztatów lub wywiadów z właścicielami procesów,
- analizy obowiązującej dokumentacji,
- analizy rzeczywistej infrastruktury IT/OT,
- uzasadnienia przyjętych parametrów czasowych i poziomów krytyczności.

5.3. Analiza ryzyka dla ciągłości działania

Wykonawca przeprowadzi analizę ryzyka związanego z ciągłością działania, uwzględniającą zagrożenia mogące zakłócić realizację procesów, funkcjonowanie systemów oraz dostępność usług.

Analiza ryzyka powinna obejmować w szczególności:

- zagrożenia dla procesów organizacyjnych i technologicznych,
- zagrożenia dla systemów IT i OT,
- zagrożenia dla infrastruktury technicznej,
- zagrożenia związane z zasobami ludzkimi,
- zagrożenia środowiskowe, zasilaniowe, lokalizacyjne i komunikacyjne,

- zagrożenia wynikające z incydentów cyberbezpieczeństwa.

Analiza powinna zostać przeprowadzona zgodnie z uznaną metodyką, preferencyjnie zgodnie z ISO/IEC 27005:2022 lub ISO 31000:2018 z uwzględnieniem charakteru działalności Zamawiającego oraz specyfiki jego środowiska technicznego.

Rezultatem tego etapu ma być raport zawierający:

- opis scenariuszy ryzyka,
- ocenę poziomu ryzyka,
- wskazanie istniejących i brakujących zabezpieczeń,
- rekomendowane działania ograniczające ryzyko.

5.4. Opracowanie strategii ciągłości działania i odtwarzania

Na podstawie wyników analizy BIA oraz analizy ryzyka Wykonawca opracuje strategię ciągłości działania i strategię odtwarzania po awarii. Strategie te mają określać sposób utrzymania funkcjonowania procesów oraz przywracania systemów i usług do wymaganego poziomu działania.

Strategie powinny obejmować w szczególności:

- zasady utrzymania funkcjonowania procesów w warunkach zakłóceń,
- zasady odtwarzania systemów teleinformatycznych i infrastruktury,
- zasady utrzymania lub przejścia do trybu awaryjnego,
- zasady komunikacji i eskalacji w sytuacjach kryzysowych,
- zasady współpracy z dostawcami i podmiotami zewnętrznymi.

W odniesieniu do środowisk IT/OT strategie powinny uwzględniać rzeczywiste możliwości techniczne organizacji, w tym dostępność backupów, redundancję, tryby awaryjne, ręczne obejścia procesów oraz kolejność przywracania poszczególnych usług, systemów i komponentów infrastruktury.

5.5. Opracowanie dokumentacji SZCD, BCP i DRP

Wykonawca opracuje kompletną dokumentację Systemu Zarządzania Ciągłością Działania, obejmującą dokumenty strategiczne, procedury operacyjne, plany oraz dokumenty wspierające.

Dokumentacja powinna obejmować co najmniej:

- politykę ciągłości działania,
- politykę odtwarzania po awarii,
- procedurę zarządzania ciągłością działania,
- procedurę zarządzania sytuacją kryzysową,
- procedurę reagowania na incydenty i awarie,
- procedurę odtwarzania systemów i infrastruktury,
- procedurę komunikacji kryzysowej,
- procedurę testowania i przeglądu SZCD,
- plan ciągłości działania (BCP),
- plan odtwarzania po awarii (DRP),
- plan komunikacji kryzysowej,
- plan odtworzenia infrastruktury krytycznej,
- rejestr procesów krytycznych,
- rejestr zasobów krytycznych,
- rejestr scenariuszy awarii,
- rejestr planów i testów.

Wykaz wskazany powyżej nie stanowi katalogu zamkniętego. Jeżeli w toku realizacji zamówienia okaże się, że dla zapewnienia kompletności i operacyjności systemu niezbędne jest opracowanie dodatkowych dokumentów, Wykonawca będzie zobowiązany do ich przygotowania.

Dokumentacja musi mieć charakter praktyczny i operacyjny. Oznacza to, że powinna:

- jasno określać role, odpowiedzialności i zasady eskalacji,
- zawierać czytelne instrukcje postępowania,
- uwzględniać dane niezbędne do działania w sytuacji kryzysowej,
- być dostosowana do rzeczywistej struktury organizacyjnej i technicznej Zamawiającego,
- umożliwiać zastosowanie przez personel bez konieczności udziału Wykonawcy.

5.6. Wdrożenie systemu

W ramach realizacji zamówienia Wykonawca zobowiązany jest nie tylko do opracowania dokumentacji, ale także do wdrożenia SZCD w organizacji. Wdrożenie powinno obejmować działania organizacyjne, proceduralne i szkoleniowe, mające na celu uruchomienie systemu oraz przygotowanie personelu do stosowania opracowanych rozwiązań.

Wdrożenie powinno obejmować w szczególności:

- przeprowadzenie warsztatów z kierownictwem,
- przeprowadzenie warsztatów z właścicielami procesów i personelem kluczowym,
- omówienie i wdrożenie opracowanych procedur oraz planów,
- wsparcie Zamawiającego w przypisaniu ról i odpowiedzialności,
- przygotowanie organizacji do działania w warunkach zakłócenia.

5.7. Testowanie i weryfikacja skuteczności

Po opracowaniu i wdrożeniu systemu Wykonawca przeprowadzi testy i ćwiczenia mające na celu potwierdzenie, że przyjęte rozwiązania są wykonalne i skuteczne.

Testy powinny obejmować co najmniej:

- testy scenariuszy awaryjnych,
- testy planów ciągłości działania,
- testy planów odtwarzania po awarii,
- testy komunikacji kryzysowej,
- testy przywracania systemów, danych i usług,
- weryfikację zdolności działania w trybie awaryjnym, jeżeli ma zastosowanie.

Każdy test powinien zostać udokumentowany. Wykonawca zobowiązany jest do przygotowania:

- scenariuszy testów,
- protokołów lub raportów z ich przeprowadzenia,
- listy stwierdzonych niezgodności, słabości lub braków,
- propozycji działań korygujących i usprawniających.

6. Wymagania dotyczące analizy infrastruktury IT i OT

Analiza BIA, analiza ryzyka oraz plany DRP muszą zostać opracowane na podstawie rzeczywistej analizy infrastruktury Zamawiającego. Niedopuszczalne jest opracowanie dokumentacji w oderwaniu od faktycznego środowiska technicznego, jego architektury, ograniczeń i zależności.

Wykonawca zobowiązany jest do przeprowadzenia analizy obejmującej co najmniej:

- architekturę systemów teleinformatycznych,
- infrastrukturę serwerową i sieciową,
- środowiska wirtualizacji,
- systemy kopii zapasowych i mechanizmy odtwarzania,
- systemy OT, w tym systemy SCADA, HMI, PLC i telemetryczne, jeżeli występują,
- integracje pomiędzy środowiskami IT i OT,
- systemy i zasoby krytyczne dla działalności Zamawiającego.

Rezultatem analizy powinny być również materiały techniczne wspierające działanie systemu, w szczególności:

- opisy architektury,
- mapy zależności systemów i usług,
- identyfikacja punktów krytycznych infrastruktury,
- wskazanie zależności pomiędzy procesami a komponentami technicznymi.

Jeżeli charakter infrastruktury tego wymaga, Wykonawca powinien przeprowadzić wizję lokalną oraz zweryfikować faktyczny sposób funkcjonowania wybranych systemów i mechanizmów zabezpieczających.

7. Wymagania wobec Wykonawcy

Wykonawca musi dysponować zespołem projektowym składającym się z co najmniej dwóch osób, posiadających kwalifikacje i doświadczenie adekwatne do przedmiotu zamówienia.

Wykonawca musi wykazać, że w okresie ostatnich 3 lat przed upływem terminu składania ofert zrealizował co najmniej:

- 2 usługi polegające na:
 - wdrożeniu lub aktualizacji Systemu Zarządzania Ciągłością Działania zgodną z ISO/IEC 22301,
 - realizacji projektów obejmujących analizę ryzyka, dokumentację SZBI oraz audyt,

Każda usługa musi być potwierdzona referencjami lub dokumentami potwierdzającymi należyte wykonanie. W skład zespołu powinna wchodzić co najmniej:

- jedna osoba posiadająca certyfikat Audytora Wiodącego ISO/IEC 27001 lub Audytora Wiodącego ISO 22301, a także wykształcenie wyższe wyższego w zakresie systemów informatycznych lub z zakresu zarządzania systemami informatycznymi lub równoważne (przez wykształcenie równoważne rozumie

się wykształcenie wyższe inne niż informatyczne, które w połączeniu z doświadczeniem zawodowym zapewnia wiedzę i umiejętności w zakresie IT lub cyberbezpieczeństwa, niezbędne do realizacji przedmiotu zamówienia, w szczególności dotyczy to kierunków technicznych lub pokrewnych (np. teleinformatyka, elektronika, automatyka) albo innych, uzupełnionych odpowiednim doświadczeniem zawodowym) oraz minimum 3-letnie doświadczenie zawodowe w realizacji projektów dotyczących systemów zarządzania bezpieczeństwem informacji lub ciągłości działania,

- jedna osoba posiadające wykształcenie wyższe w zakresie systemów informatycznych lub z zakresu zarządzania systemami informatycznymi lub równoważne (przez wykształcenie równoważne rozumie się wykształcenie wyższe inne niż informatyczne, które w połączeniu z doświadczeniem zawodowym zapewnia wiedzę i umiejętności w zakresie IT lub cyberbezpieczeństwa, niezbędne do realizacji przedmiotu zamówienia, w szczególności dotyczy to kierunków technicznych lub pokrewnych (np. teleinformatyka, elektronika, automatyka) albo innych, uzupełnionych odpowiednim doświadczeniem zawodowym) oraz minimum 3-letnie doświadczenie w administracji systemami teleinformatycznymi, a także doświadczenie w zakresie ciągłości działania w środowiskach IT lub IT/OT.

W przypadku środowisk obejmujących systemy przemysłowe lub automatykę dopuszcza się wymaganie, aby członek zespołu posiadał doświadczenie w pracy z infrastrukturą OT, systemami SCADA lub rozwiązaniami przemysłowymi.

8. Termin realizacji zamówienia

Przedmiot zamówienia należy zrealizować do 10 listopada 2026 r.

Wykonawca zobowiązany jest tak zorganizować realizację prac, aby wszystkie wymagane działania analityczne, dokumentacyjne, wdrożeniowe, szkoleniowe i testowe zostały zakończone w terminie określonym przez Zamawiającego.

Zamawiający zastrzega możliwość wydłużenia terminu, uwzględniając zmianę terminu realizacji projektu „Cyberbezpieczny Wodociąg” przed Grantodawcą.

9. Produkty końcowe

W ramach realizacji zamówienia Wykonawca zobowiązany jest do dostarczenia kompletu produktów końcowych potwierdzających wykonanie wszystkich wymaganych etapów prac.

Produkty końcowe powinny obejmować co najmniej:

9.1. Dokumentację analityczną, w tym:

- raport z analizy stanu obecnego,
- raport z analizy wpływu na działalność (BIA),
- raport z analizy ryzyka dla ciągłości działania.

9.2. Dokumentację systemową SZCD, w tym:

- polityki,
- procedury,
- plany BCP i DRP,
- dokumenty wspierające i rejestry.

9.3. Dokumentację techniczną, w tym:

- opis architektury IT/OT powiązanej z ciągłością działania,
- mapy zależności systemów i usług,
- opis środowiska backupowego,
- opis środowiska odtworzeniowego i rozwiązań DR,
- schematy infrastruktury krytycznej.

9.4. Wyniki testów i ćwiczeń, w tym:

- scenariusze testowe,
- raporty z testów,
- wykaz stwierdzonych niezgodności,
- plan działań korygujących.

9.5. Potwierdzenie działań szkoleniowych, w tym:

- programy lub zakresy szkoleń,
- materiały szkoleniowe,
- listy obecności albo inne dowody udziału.

Wszystkie produkty końcowe muszą być przekazane w formie uzgodnionej z Zamawiającym, w sposób umożliwiający ich dalsze wykorzystanie, aktualizację i stosowanie operacyjne.

10. Wymagania jakościowe

Dokumentacja i wdrożone rozwiązania muszą być kompletne, spójne, logicznie uporządkowane i dostosowane do rzeczywistych warunków organizacyjnych oraz technicznych Zamawiającego. W szczególności wymaga się, aby:

- dokumentacja była napisana w sposób jednoznaczny i zrozumiały,
- plany BCP i DRP były możliwe do zastosowania w praktyce,
- rozwiązania były dostosowane do faktycznej infrastruktury, a nie oparte na wzorcach ogólnych,
- system umożliwiał jego utrzymanie, przegląd i aktualizację po zakończeniu realizacji zamówienia,
- wdrożone rozwiązania mogły zostać wykorzystane bez konieczności stałego wsparcia Wykonawcy.

Zamawiający oczekuje dostarczenia systemu, który będzie miał charakter operacyjny i użyteczny, a nie wyłącznie formalny lub dokumentacyjny.

11. Postanowienia końcowe

Wykonawca ponosi odpowiedzialność za kompletność, spójność i jakość opracowanego oraz wdrożonego Systemu Zarządzania Ciągłością Działania, a także za zgodność przekazanych rezultatów z wymaganiami określonymi w niniejszym Opisie Przedmiotu Zamówienia.

Wykonawca przekazuje prawa autorskie dokumentacji wykonanej zgodnie z zamówieniem Zamawiającego.

Dokumentacja musi być gotowa do natychmiastowego zastosowania przez Zamawiającego i stanowić realne wsparcie dla organizacji w sytuacjach zakłóceń, incydentów, awarii i kryzysów. Zamówienie ma charakter wdrożeniowy, a jego wykonanie będzie oceniane nie tylko przez pryzmat przekazania dokumentów, ale również przez pryzmat ich przydatności, kompletności i możliwości rzeczywistego wykorzystania.