Zaproszenie do sporządzenia informacji niezbędnych do ustalenia wartości zamówienia publicznego na: Audyt bezpieczeństwa oraz przygotowanie do certyfikacji Systemu PLI CBD

Szanowni Państwo,
Urząd Komunikacji Elektronicznej przygotowuje postępowanie o udzielenie zamówienia na **„Audyt bezpieczeństwa oraz przygotowanie do certyfikacji Systemu PLI CBD**".

Postępowanie przeprowadzone zostanie zgodnie z ustawą z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (tj. Dz.U. z 2010 r. Nr 113, poz. 759 z późn. zm.).
Zamawiający przed wszczęciem postępowania zobowiązany jest do ustalenia wartości zamówienia (art. 32 ustawy Prawo zamówień publicznych). W celu ustalenia wartości zamówienia, Zamawiający zaprasza zainteresowane podmioty do zapoznania się z załączoną informacją o zakresie świadczonych usług oraz przesłanie informacji nt. danych Wykonawcy i szacunkowych cen usług.

Informację sporządzoną według poniższego wzoru należy przesłać do dnia 27 czerwca 2014 r. do godz. 15.00 na adres p.swiader@uke.gov.pl

Dane Wykonawcy:
Nazwa:_____
Adres:_____
Tel.:_____
e-mail:_____
NIP:_____
REGON:_____

Szacunkowe ceny netto i brutto, zawierające wszystkie koszty realizacji usług.

Cena netto_____ Cena brutto_____

Dane kontaktowe osoby sporządzającej informację:
Imię i nazwisko:.....
Stanowisko:.....
Telefon:.....

Adres email:.....

1.Przedmiot zamówienia

Przedmiotem zamówienia jest:
- przeprowadzenie przez Wykonawcę na rzecz Zamawiającego audytu bezpieczeństwa systemu informatycznego PLI CBD,
- przeprowadzenie szkoleń dla pracowników Zamawiającego w zakresie ochrony informacji oraz zarządzania usługami informatycznymi,
- opracowanie i wdrożenie procedur dla systemu PLICBD zgodnych z powszechnie obowiązującymi normami w zakresie bezpieczeństwa informacji oraz zarządzania usługami informatycznymi,
- wdrożenie Zintegrowanego Systemu Zarządzania Bezpieczeństwem Informacji, ciągłością działania i jakością usług informatycznych,
- przygotowanie do uzyskania certyfikatów zgodności PLI CBD z normami PN-ISO/IEC 27001 oraz PN-ISO/IEC 20000-1 oraz PN-ISO/IEC 20000-2,

Należy w tym miejscu wskazać, iż w *rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U z 2012, poz. 526 z późn. zm)* w rozdziale IV *Minimalne wymagania dla systemów teleinformatycznych* w § 15 pkt 3 wskazane jest wprost, że wymagania zawarte w tym rozporządzeniu odnoszące się do sposobu projektowania, wdrażania i eksploatowania systemów teleinformatycznych uznaje się za spełnione jeżeli odbywają się z uwzględnieniem Polskich Norm: PN- ISO/IEC 20000-1 i PN-ISO/IEC 20000-2. Natomiast w § 20 jest wskazane, że wymagania w zakresie zarządzania bezpieczeństwem informacji uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001

- prowadzenie asysty powdrożeniowej w okresie 24 miesięcy od daty podpisania protokołu odbioru końcowego wdrożonego zintegrowanego systemu zarządzania bezpieczeństwem informacji, ciągłością działania i jakością usług informatycznych.

Audyt ma na celu również zidentyfikowanie słabych punktów w systemie informatycznym PLI CBD, których obecność może przyczynić się do przypadkowego lub celowego ujawnienia, modyfikacji, zniszczenia lub uniemożliwienia przetwarzania informacji przechowywanej i przesyłanej za pomocą systemu Zamawiającego.

Wszędzie tam, gdzie przedmiot zamówienia jest opisany poprzez wskazanie znaków towarowych, patentów, norm, aprobat, standardów lub pochodzenia, Zamawiający dopuszcza zastosowanie przez Wykonawcę rozwiązań równoważnych w stosunku do opisanych w niniejszym dokumencie, pod warunkiem, że będą one posiadały, co najmniej takie same lub lepsze parametry funkcjonalne i nie obniżą określonych w niniejszej specyfikacji standardów.

2. Zakres realizacji przedmiotu zamówienia

Realizacja zamówienia prowadzona ma być w ramach opisanych poniżej zadań:

1.Szkolenie wprowadzające dla zespołu wdrażającego system w zakresie ochrony informacji, inwentaryzacji aktywów informacyjnych oraz oceny ryzyka teleinformatycznego.

2.Testy penetracyjne Systemu PLI CBD w zakresie funkcjonalności związanej z przenoszeniem numerów, systemem obsługi użytkowników oraz modułem do administrowania aplikacją PLI CBD.

3.Przeprowadzenie przeglądu konfiguracji wybranych urządzeń wchodzących w skład Systemu PLI CBD.

4.Audyt ochrony danych osobowych w celu zbadania procesów przetwarzania danych osobowych w PLI CBD, Wykonawca dokona weryfikacji stanu faktycznego z opisanymi procesami w posiadanych przez Zamawiającego dokumentach (Polityka Bezpieczeństwa i Instrukcja Zarządzania Systemem Informatycznym) oraz z powszechnie obowiązującymi przepisami i standardami.

5.Systemu Zarządzania Bezpieczeństwem Informacji - opracowanie, wdrożenie oraz przygotowanie do certyfikacji zgodnie z wymaganiami normy PN-ISO/IEC 27001 oraz zaleceniami norm w zakresie:
1) w odniesieniu do ustanawiania zabezpieczeń PN-ISO/IEC 17799 ;
2) w odniesieniu do zarządzania ryzykiem PN-ISO/IEC 27005 ;
3) w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania PN-ISO/IEC 24762 .

6.Systemu Zarządzania Usługami Informatycznymi - opracowanie, wdrożenie oraz przygotowanie do certyfikacji zgodnie z wymaganiami normy PN-ISO/IEC 20000-1 oraz PN-ISO/IEC 20000-2.

7.Asysta powdrożeniowa w okresie 24 miesięcy od daty podpisania protokołu odbioru końcowego wdrożonego zintegrowanego systemu zarządzania bezpieczeństwem informacji, ciągłością działania i jakością usług informatycznych.

3.Termin i etapy realizacji przedmiotu zamówienia

Realizacja przedmiotu zamówienia nastąpi w II kwartale 2015 r. z wyłączeniem Etapu II.

3.1.Harmonogram ramowy

Wykonawca przygotuje i uzgodni z Zamawiającym, w terminie 2 tygodni od daty zawarcia Umowy, szczegółowy Harmonogram Projektu zawierający Listę Produktów do zrealizowania w każdym Etapie**.**

W ramach **Etapu I** Wykonawca wykona następujące zadania:

1.Szkolenia:
- wprowadzające dla zespołu wdrażającego system w zakresie ochrony informacji, zarządzania usługami informatycznymi, inwentaryzacji aktywów informacyjnych oraz oceny ryzyka teleinformatycznego;
- z zakresu projektowania i wdrażania System Zarządzania Bezpieczeństwem Informacji wg normy PN-ISO/IEC 27001;
- z zakresu projektowania i wdrażania System Zarządzania Usługami IT wg normy PN-ISO/IEC 20000-1 oraz PN-ISO/IEC 20000-2.

2.Audyt ochrony danych osobowych w celu zbadania procesów przetwarzania danych osobowych w PLI CBD. Wykonawca dokona weryfikacji stanu faktycznego z opisanymi procesami w posiadanych przez Zamawiającego dokumentach (Polityka Bezpieczeństwa i Instrukcja Zarządzania Systemem Informatycznym) oraz z powszechnie obowiązującymi przepisami i standardami.

3.Opracowanie planu wdrożenia oraz wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji zgodnie z wymaganiami normy PN-ISO/IEC 27001 oraz zaleceniami norm w zakresie:
1) w odniesieniu do ustanawiania zabezpieczeń PN-ISO/IEC 17799 ;
2) w odniesieniu do zarządzania ryzykiem PN-ISO/IEC 27005 ;
3) w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania PN-ISO/IEC 24762.

4.Opracowanie planu wdrożenia oraz wdrożenie Systemu Zarządzania Usługami Informatycznymi zgodnie z wymaganiami norm PN-ISO/IEC 20000-1 oraz PN-ISO/IEC 20000-2

5.Testy penetracyjne Rozbudowanego Systemu PLI CBD w zakresie funkcjonalności związanej z przenoszeniem numerów, systemem obsługi użytkowników oraz modułem do administrowania aplikacją PLI CBD.

6.Przegląd konfiguracji wybranych urządzeń wchodzących w skład Rozbudowanego Systemu PLI CBD.

Termin realizacji: II kwartał 2015 r. (dokładny termin realizacji prac zależny jest od postępu prac prowadzonych przez Wykonawcę rozbudowy systemu PLICBD).

ETAP II
W ramach etapu 2 Wykonawca wykona następujące zadania:

1.Przygotowanie do procesu certyfikacji Systemu Zarządzania Bezpieczeństwem Informacji zgodnie z wymaganiami normy PN-ISO/IEC 27001.

2.Przygotowanie do procesu certyfikacji Systemu Zarządzania Usługami Informatycznymi zgodnie z wymaganiami normy PN-ISO/IEC 20000-1 oraz PN-ISO/IEC 20000-2.

3.Asysta powdrożeniowa w okresie 24 miesięcy od daty podpisania protokołu odbioru końcowego wdrożonego Systemu Zarządzania Bezpieczeństwem Informacji oraz Systemu Zarządzania Usługami Informatycznymi.

4.Szkolenia z zakresu bezpieczeństwa informacji oraz zarządzania usługami informatycznymi dla audytorów wewnętrznych:
- z zakresu Audytor wewnętrzny systemu zarządzania bezpieczeństwem informacji wg PN-ISO/IEC 27001;
- z zakresu Audytor wewnętrzny systemu zarządzania usługami informatycznymi wg PN-ISO/IEC 20000-1 oraz PN-ISO/IEC 20000-2;

Termin realizacji: 24 miesiące od daty podpisania protokołu odbioru końcowego wdrożonego zintegrowanego systemu zarządzania bezpieczeństwem informacji, ciągłością działania i jakością usług informatycznych.

4.Szkolenia

Wykonawca audytu bezpieczeństwa Rozbudowanego Systemu PLI CBD zobowiązany będzie do przygotowania i przeprowadzenia szkoleń równolegle do prac wykonywanych w poszczególnych Etapach. Wykonawca przygotuje i przedstawi do akceptacji Zamawiającemu sposób organizacji szkoleń.
Wykonawca uzgodni, o ile nie zostało to zapisane w wymaganiach szczegółowych dla poszczególnych szkoleń, z Zamawiającym:
- kwalifikacje i doświadczenie wykładowców i trenerów z uwzględnieniem obszaru niezbędnej wiedzy dotyczącej elementów Systemu, które mają być przedmiotem szkolenia.
- harmonogram przeprowadzenia szkoleń uwzględniający w szczególności harmonogram wdrożenia Systemu.
- charakterystykę materiałów szkoleniowych.

4.1 Szkolenie - wymagania ogólne

1.Szkolenia muszą być prowadzone w języku polskim.
2.Wykonawca zapewni i przekaże uczestnikom materiały szkoleniowe w języku polskim.
3.Wykonawca pokrywa koszty przeprowadzenia szkoleń, przygotowania materiałów szkoleniowych, wyżywienia uczestników.

4.W przypadku szkoleń wielodniowych prowadzonych poza miejscem zatrudnienia Wykonawca ponosi koszty szkolenia, zakwaterowania oraz transportu z miejsca stałego zatrudnienia osób biorących udział w szkoleniu na miejsce szkolenia i z miejsca szkolenia do miejsca stałego zatrudnienia.
5.Po każdym szkoleniu Wykonawca sporządzi protokół wraz z listą obecności potwierdzoną podpisami uczestników, który następnie przekaże Zamawiającemu.
6.Po każdym szkoleniu Wykonawca sporządzi, dla każdego uczestnika szkolenia, imienne zaświadczenia/certyfikaty zawierające przynajmniej następujące informacje:
-temat szkolenia,
-imię i nazwisko przeprowadzającego szkolenie oraz jego kwalifikacje powiązane z tematem szkolenia,
-podpis prowadzącego szkolenie,
-nazwę firmy organizującej szkolenie,
-pieczątkę firmową firmy organizującej szkolenie,
-poruszane w trakcie szkolenia tematy,
-czas poświęcony na każdy temat,
-datę i miejsce przeprowadzenia szkolenia.
7.Plan szkoleń uwzględniający co najmniej: szczegółowo przedstawioną tematykę szkoleń, opis materiałów szkoleniowych, metodę prowadzenia szkoleń, miejsce i czas szkoleń, Wykonawca przedstawi do akceptacji Zamawiającemu.
8.Wykonawca ponosi koszty wynajmu pomieszczeń na cele szkolenia i dostarczenia niezbędnego wyposażenia do ich prowadzenia.
9.Szkolenia wymagające środowiska technicznego Systemu PLI CBD odbędą się w CPD w Boruczy. Miejsce pozostałych szkoleń Wykonawca uzgodni z Zamawiającym. W przypadku szkoleń odbywających się w CPD w Boruczy za organizację szkoleń odpowiada Wykonawca zgodnie z powyższymi zapisami.
10. Szkolenia muszą opisywać m.in. narzędzia i techniki, jakimi będzie posługiwał się Wykonawca podczas realizacji audytu bezpieczeństwa.
11. Każdy dzień szkolenia będzie trwał 8 godzin zegarowych. Każdy dzień szkolenia Wykonawca musi zaplanować tak, aby uwzględnić:
- czas na dydaktykę – 6 (sześć) godzin zegarowych,
- jedną przerwę obiadową –1 (jedna) godzina zegarowa,
- cztery przerwy kawowe – 15 (piętnaście) minut każda.
12.W ramach przerwy obiadowej Wykonawca zapewni obiad składający się, co najmniej z dwóch dań ciepłych, surówki, deseru i napojów.
13.W ramach przerw kawowych Wykonawca zapewni kawę, herbatę, wodę mineralną (gazowaną oraz niegazowaną), soki, ciastka oraz owoce.
14. Na czas trwania szkolenia Wykonawca musi zapewnić salę szkoleniową, wraz z sprzętem niezbędnym do przeprowadzenia szkolenia. Ponadto każdemu uczestnikowi szkolenia wykonawca zapewni po jednym komplecie materiałów szkoleniowych (w wersji papierowej oraz elektronicznej), oraz wyżywienie.
15.Wykonawca opracuje i przedstawi do akceptacji Zamawiającego agendę szkolenia zawierającą:
- cel i zakres szkolenia,
- metodę i formę szkolenia.

16. Przeprowadzenie szkolenia zostanie potwierdzone protokołem sporządzonym w dwóch jednobrzmiących egzemplarzach, po jednym dla Zamawiającego i Wykonawcy, zawierającym:
- nazwę i tematykę ze szkolenia,
- datę i miejsce przeprowadzenia szkolenia,
- czas trwania szkolenia,
- imię i nazwisko oraz specjalizację osób prowadzących szkolenie.

4.2 Szkolenie z zakresu projektowania i wdrażania System Zarządzania Bezpieczeństwem Informacji wg normy PN-ISO/IEC 27001

Przygotowanie i przeprowadzenie, dla grupy 4 pracowników Zamawiającego, trzydniowego szkolenia z zakresu: projektowania i wdrażania systemów zarządzania bezpieczeństwem informacji zgodnych z wymaganiami norm z rodziny PN-ISO/IEC 27000 zawierającego przynajmniej następujące elementy:
- kluczowe zagadnienia zarządzania bezpieczeństwem informacji,
- najlepsze praktyki oraz normy zarządzania bezpieczeństwem informacji,
- założenia i struktura norm z rodziny PN-ISO/IEC 27000,
- analiza i interpretacja wymagań normy PN-ISO/IEC 27001,
- zasady projektowania systemów zarządzania bezpieczeństwem informacji wg normy PN-ISO/IEC 27001,
- zasady wdrażania systemów zarządzania bezpieczeństwem informacji wg normy PN-ISO/IEC 27001,
- proces wdrażania systemów zarządzania bezpieczeństwem informacji wg normy PN-ISO/IEC 27001,
- wymagania dokumentacyjne systemu zarządzania bezpieczeństwem informacji zgodnego z PN-ISO/IEC 27001,
- wymagania normy PN-ISO/IEC 27001 a wymagania norm PN-ISO/IEC 20000-1 oraz PN-ISO/IEC 20000-2 omówienie obszarów wspólnych,
- korzyści z wdrożenia wymagań normy,
- proces certyfikacji;

Program szkolenia ma zostać przygotowany w oparciu o najlepsze praktyki stosowane podczas projektowania i wdrażania systemów zarządzania w zakresie ochrony i bezpieczeństwa informacji.

Prowadzący szkolenie musi wskazać się, co najmniej trzyletnią praktyką w prowadzeniu szkoleń z zakresy zarządzania bezpieczeństwem informacji wg normy PN-ISO/IEC 27001 lub projektowania lub wdrażania System Zarządzania Bezpieczeństwem Informacji wg normy PN-ISO/IEC 27001.

Każdy uczestnik szkolenia otrzyma materiały szkoleniowe opisane rozdziale 4.1 oraz najnowsze polskie, papierowe wydania norm: PN-ISO/IEC 27001, PN-ISO/IEC 27002 .

4.3 Szkolenie z zakresu projektowania i wdrażania System Zarządzania Usługami IT wg normy PN-ISO/IEC 20000-1 oraz PN-ISO/IEC 20000-2

Przygotowanie i przeprowadzenie, dla grupy 4 pracowników Zamawiającego, trzydniowego szkolenia z zakresu: **projektowania i wdrażania systemów zarządzania usługami IT zgodnych z wymaganiami normy PN-ISO/IEC 20000-1 oraz PN-ISO/IEC 20000-2** zawierającego przynajmniej następujące elementy:
- kluczowe zagadnienia zarządzania usługami informatycznymi,
- najlepsze praktyki oraz normy zarządzania usługami informatycznymi,
- założenia i struktura norm z rodziny PN-ISO/IEC 20000,
- analiza i interpretacja wymagań normy PN-ISO/IEC 20000-1,
- zasady projektowania systemów zarządzania usługami IT wg normy PN-ISO/IEC 20000-1,
- zasady wdrażania systemów zarządzania usługami IT wg normy PN-ISO/IEC 20000-1,
- proces wdrażania systemów zarządzania usługami IT wg normy ISO/IEC 20000-1,
- wymagania dokumentacyjne systemu zarządzania usługami IT zgodnego z PN-ISO/IEC 20000-1,
- wymagania normy PN-ISO/IEC 20000-1 a wymagania normy PN-ISO/IEC 27001- omówienie obszarów wspólnych,
- korzyści z wdrożenia wymagań normy,
- proces certyfikacji;

Program szkolenia ma zostać przygotowany w oparciu o najlepsze praktyki stosowane podczas projektowania i wdrażania systemów zarządzania w zakresie zarządzania usługami informatycznymi.

Prowadzący szkolenie musi wskazać się, co najmniej trzy letnią praktyką w prowadzeniu szkoleń z zakresy zarządzania usługami IT wg normy PN-ISO/IEC 20000-1 lub projektowania lub wdrażania System Zarządzania Usługami IT wg normy PN-ISO/IEC 20000-1.

Każdy uczestnik szkolenia otrzyma materiały szkoleniowe opisane rozdziale 4.1 oraz polskie, papierowe wydania norm PN-ISO/IEC 20000-1 i PN-ISO/IEC 20000-2.

4.4. Szkolenie z zakresu Audytor wewnętrzny systemu zarządzania bezpieczeństwem informacji wg PN-ISO/IEC 27001

Przygotowanie i przeprowadzenie, dla grupy 4 pracowników Zamawiającego, trzydniowego szkolenia z zakresu: **Audytor wewnętrzny systemu zarządzania bezpieczeństwem informacji wg PN-ISO/IEC 27001: 2013** zawierającego przynajmniej następujące elementy:
- najlepsze praktyki audytowania zgodnie z PN-ISO/IEC 19011,
- wymagania normy PN-ISO/IEC 27001 dotyczące audytowania,
- założenia dotyczące realizacji audytów wewnętrznych,
- planowanie audytów wewnętrznych i opracowanie planu audytu,
- realizacja badania audytowego,
- zgłaszanie niezgodności,
- opracowywanie raportu z audytu,
- działania korygujące i zapobiegawcze - planowanie i nadzór realizacji,
- wymagania audytowe odnośnie Systemu Zarządzania Usługami IT, procesów, dokumentacji i organizacji wg normy PN-ISO/IEC 27001.

Program szkolenia ma zostać przygotowany w oparciu o najlepsze praktyki stosowane podczas prowadzenia audytów wewnętrznych systemów zarządzania w zakresie ochrony i bezpieczeństwa informacji.

Prowadzący szkolenie musi wskazać się co najmniej trzyletnią praktyką w prowadzeniu szkoleń z zakresy prowadzenia audytów systemów zarządzania bezpieczeństwem informacji wg normy PN-ISO/IEC 27001.

4.5 Szkolenie z zakresu Audytor wewnętrzny systemu zarządzania usługami IT wg wg PN-ISO/IEC 20000-1

Przygotowanie i przeprowadzenie, dla grupy 4 pracowników Zamawiającego, trzydniowego szkolenia z zakresu: **Audytor wewnętrzny systemu zarządzania usługami IT wg PN-ISO/IEC 20000-1:** zawierającego przynajmniej następujące elementy:
- najlepsze praktyki audytowania zgodnie z ISO/IEC 19011,
- wymagania normy PN-ISO/IEC 20000-1 dotyczące audytowania,
- założenia dotyczące realizacji audytów wewnętrznych,
- planowanie audytów wewnętrznych i opracowanie planu audytu,
- realizacja badania audytowego,
- zgłaszanie niezgodności,
- opracowywanie raportu z audytu,
- działania korygujące i zapobiegawcze - planowanie i nadzór realizacji,
- wymagania audytowe odnośnie Systemu Zarządzania Usługami IT, procesów, dokumentacji i organizacji wg normy PN-ISO/IEC 20000-1.

Program szkolenia ma zostać przygotowany w oparciu o najlepsze praktyki stosowane podczas prowadzenia audytów wewnętrznych systemów zarządzania usługami informatycznymi.

Prowadzący szkolenie musi wskazać się co najmniej trzyletnią praktyką w prowadzeniu

szkoleń z zakresy prowadzenia audytów systemów zarządzania usługami informatycznymi wg normy PN-ISO/IEC 20000-1.

5. Testy penetracyjne

5.1 Cel Zadania

Przeprowadzone testy mają na celu zidentyfikowanie słabych punktów w Rozbudowanym Systemie Informatycznym PLI CBD, których obecność może przyczynić się do przypadkowego lub celowego ujawnienia, modyfikacji, zniszczenia lub uniemożliwienia przetwarzania informacji przechowywanej i przesyłanej za pomocą systemu Zamawiającego.

5.2 Zakres zadania

W ramach prowadzonego audytu Wykonawca wykona następujące typy testów penetracyjnych:

1.Testy penetracyjne typu black-box - testy penetracyjne prowadzone bez wiedzy na temat badanego obiektu. Wykonawca przeprowadza je wyłącznie z wykorzystaniem pozyskanej w wyniki białego wywiadu przez Zamawiającego na temat PLI CBD.

2.Testy penetracyjne typu grey-box - testy penetracyjne przy założeniu dysponowania standardowymi kontami w badanym systemie, mające na celu analizę podatności systemu na nieautoryzowane działania uprawnionych użytkowników zewnętrznych.

3.Testy penetracyjne typu white-box - testy penetracyjne z nieograniczonym dostępem do systemu po przekazaniu przez Zamawiającego niezbędnej wiedzy nt. zasad działania systemu, mające na celu analizę podatności systemu na nieautoryzowane działania uprawnionych użytkowników wewnętrznych.

5.3 Wymagania

1.Wszystkie wymienione wyżej testy Wykonawca wykona dla każdej lokalizacji ośrodka przetwarzania danych PLI CBD.

2.W żadnym momencie realizacji umowy Wykonawca nie może swoim działaniem spowodować całkowitego unieruchomienia Systemu ani poszczególnych jego funkcjonalności. Wszystkie prace mogące wprowadzić zmiany w systemie muszą uzyskać akceptację Zamawiającego. Podczas prac usługi świadczone przez System nie mogą ulec degradacji do poziomu, który uniemożliwi odbieranie i przesyłanie danych lokalizacyjnych.

3. Wykonawca powinien wykazać, że w realizacji przedmiotu umowy będzie dysponował:

co najmniej (2) dwiema osobami, które będą uczestniczyć w wykonywaniu zamówienia, posiadającymi doświadczenie w wykonywaniu testów bezpieczeństwa i potwierdzić ich uczestnictwo w wykonaniu co najmniej 2 (dwóch) audytów systemu bezpieczeństwa IT w administracji publicznej;

oraz co najmniej (1) jedną osobę, która będzie realizowała przedmiot zamówienia, a która uczestniczył/a w wykonaniu co najmniej 2 (dwóch) audytów systemu bezpieczeństwa IT w administracji publicznej;

c) posiada co najmniej jeden z poniższych certyfikatów:

- Certified Information System Auditor (CISA);
- Certified in the Governance of Enterprise IT (CGEIT);
- Certified Internal Auditor (CIA);
- Certified Information Systems Security Professional (CISSP);
- Europejski Certyfikat Umiejętności Zawodowych Informatyka - EUCIP Professional specjalizacja Audytor Systemów Informacyjnych;
- Systems Security Certified Practitioner (SSCP);

4.Wykonawca powinien przedstawić Zamawiającemu wykaz osób, które będą uczestniczyć w wykonywaniu zamówienia, wraz z informacjami na temat ich kwalifikacji zawodowych, doświadczenia i wykształcenia niezbędnych do wykonania zamówienia, a także zakresu wykonywanych przez nie czynności, oraz informacje o podstawie do dysponowania tymi osobami.

5.Wykonawca przedstawi Zamawiającemu informację o adresie pocztowym oraz o sieciowych adresach logicznych, miejsc(a) z których będą dokonywane testy penetracyjne

6.Realizatorzy umowy po stronie Wykonawcy przed przystąpieniem do prac zobowiązani będą do podpisania stosownych oświadczeń o zachowaniu tajemnicy związanych z przedmiotem zamówienia w tym technicznych oraz dotyczących danych osobowych uzyskanych w trakcie realizacji umowy.

7. Osoby biorące udział ze strony Wykonawcy w realizacji zamówienia oraz osoby kierujące i nadzorujące, ich pracą zobowiązane są do zapoznania się z zarządzeniem dotyczącym Polityki bezpieczeństwa danych osobowych w Urzędzie Komunikacji Elektronicznej i podpisania oświadczenia stanowiącego załącznik do zarządzenia.

8.Testy penetracyjne prowadzone w ramach audytu muszą zawierać min. następujące kategorie ataków:

- Wykorzystania znanych wad produkcyjnych (bugs) oprogramowania badanego systemu.
- Przenikanie filtrów sieciowych.
- Podsłuch ruchu sieciowego.
- Przejęcia sesji.
- Kryptoanaliza
- Ataki wewnętrzne na zasoby sieci lokalnej.
- Ataki na aplikację Zamawiającego.
- Skierowanie mechanizmów ochronnych przeciw elementom Systemu.
- Ataki kombinowane.

Minimalny zakres prac :

- Analiza udostępnianych informacji przez PLI CBD.
- Analiza wersji i konfiguracji zastosowanego oprogramowania.
- Próby wykrycia możliwych dostępów administracyjnych.
- Analiza mechanizmów uwierzytelniania i autoryzacji stosowanych w PLI CBD.
- Próby przełamania i ominięcia mechanizmów uwierzytelniania oferowanych przez PLI CBD.
- Sprawdzenie trywialności haseł (ataki metodą słownikową).
- Manipulacja wartościami znajdującymi się w pliku cookie przesyłanym przez PLI CBD.
- Analiza zabezpieczenia przesyłu identyfikatorów sesji.
- Próby odgadnięcia sposobu generowania identyfikatorów sesji.
- Próby podszycia się pod sesję innego użytkownika.
- Próby rozszerzenia nadanych uprawnień przez użytkowników.
- Próby uzyskania nieautoryzowanego dostępu do danych innych użytkowników.
- Analiza danych wysyłanych i odbieranych przez PLI CBD.
- Próby manipulacji wartościami ukrytymi znajdującymi się w formularzach HTML.
- Analizę reakcji PLI CBD na wprowadzanie nieoczekiwanych lub nieprawidłowych danych.
- Próby destabilizacji pracy PLI CBD przy pomocy nieprawidłowych wartości w żądaniach.
- Próby destabilizacji PLI CBD przy pomocy nieprawidłowych wartości w nagłówkach protokołu http.
- Próby ataków: “Reflected/Stored/ Dom Based Cross-site scripting”, “Cross Site Flashing”, „Server Side Include”, “SQL Injection”, “CSRF”, “XPATH Injection”, “IMAP/SMTP Injection”, “Code Injection”, “OS Commanding”, “Buffer Overflow”, “HTTP Spliting/Smuggling”, “Denial of Service”.
- Analiza możliwości powtórnego przesyłania przechwyconych danych.
- Analiza błędów typowych dla wykorzystywanej przez PLI CBD technologii.
- Weryfikacja szyfrowania danych przez PLI CBD.
- Testowanie możliwości dostępu do usług sieciowych (zarówno faktycznie wykorzystywanych serwisów, jak i domyślnie otwartych i zapomnianych portów),
- Przeanalizowanie potencjalnych zagrożeń dla istniejących serwerów usług (wersje systemów, wersje oprogramowania, otwarte porty, podatność na znane ataki)
- Przesyłanie odpowiednio spreparowanych oraz zainfekowanych plików XML do sytemu PLI CBD.

9.Testy należy przeprowadzić zgodnie z metodyką OWASP (Open Web Application Security Project) uwzględniając listę TOP10 kategorii ataków lub równoważnej.

10. Przed przystąpieniem do testów penetracyjnych Wykonawca uzgodni i przedstawi Zamawiającemu do akceptacji dokument pn.”Zakres i plan testów penetracyjnych dla systemu PLI CBD”. Dokument musi zawierać listę rozważanych ataków, opis i scenariusze przeprowadzania ataków oraz informacje o tym przeciwko jakiemu elementowi infrastruktury Zamawiającego próba jest skierowana i możliwych skutkach udanej próby. Ponadto dokument musi zawierać harmonogram testów.

11. Po przeprowadzonych testach penetracyjnych Wykonawca przekaże Zamawiającemu dokumentu: „Raport z przeprowadzonych testów penetracyjnych systemu PLI CBD", zawierający szczegółowy opis wszystkich przeprowadzonych ataków, ich rezultaty - logi systemowe, zapisy sesji, kopie z ekranu (tam gdzie jest to możliwe), oraz sugestie dotyczące sposobu usunięcia wskazanych nieprawidłowości.

12. Po zgłoszeniu przez Zamawiającego gotowości, Wykonawca, w terminie 7 dni roboczych, dokona ponownych testów penetracyjnych, w szczególności w obszarach wcześniej wskazach, jako zagrażające bezpieczeństwu informacji w przetwarzanych w Systemie PLI CBD.
Po przeprowadzonych ponownych testach Wykonawca przedstawi Raport końcowy zawierający:
- weryfikację czy zaproponowane w etapach opisanych w punktach podatności i problemy z bezpieczeństwem zostały rozwiązane poprawianie,
- opis aktualnego poziomu bezpieczeństwa,
- rekomendację wskazującą kierunki dalszego podnoszenia bezpieczeństwa Systemu.
Raport końcowy musi być dostarczony w formie pisemnej i elektronicznej.

13.W przypadku stwierdzenia rażącego naruszenie zasad bezpieczeństwa mogącego wpłynąć na znaczne obniżenie bezpieczeństwa Systemu PLI CBD Wykonawca zobowiązany jest do bezzwłocznego poinformowania o zaistniałym fakcie Zmawiającego.

6. Przegląd konfiguracji urządzeń IT

6.1 Cel Zadania

Przegląd konfiguracji urządzeń wchodzących w skład Systemu PLI CBD ma na celu zidentyfikowanie słabych punktów w konfiguracji tych urządzeń, których obecność może przyczynić się do przypadkowego lub celowego ujawnienia, modyfikacji, zniszczenia lub uniemożliwienia przetwarzania informacji przechowywanej i przesyłanej za pomocą Systemu Zamawiającego.

6.2 Zakres i wymagania zadania

1.Przed przystąpieniem do przeglądu konfiguracji urządzeń wchodzących w skład Systemu PLI CBD Wykonawca przedstawi i uzgodni z Zamawiającym szczegółowy zakres i plan przeglądu konfiguracji.

2.W zależności od urządzenia zakres prac powinien obejmować minimum następujące czynności:
Weryfikację zainstalowanych poprawek bezpieczeństwa na serwerach i stacjach roboczych.
Sprawdzenie zgodności konfiguracji z przyjętymi w organizacji standardami.
Sprawdzenie zgodności konfiguracji z zaleceniami producentów oprogramowania i powszechnie dostępnymi dobrymi praktykami bezpiecznej konfiguracji.
Sprawdzenie zasobów udostępnianych przez testowany system.

Weryfikację zastosowanych systemów plików i prawidłowości ustawienia praw dostępu do wybranych plików systemowych i aplikacji.
Przeprowadzenie analizy zaimplementowanej polityki haseł użytkowników.
Sprawdzenie metody uwierzytelniania i kontroli dostępu na serwerach i stacjach roboczych.
Weryfikację zaimplementowanej polityki blokowania kont użytkowników.
Sprawdzenie zaimplementowania szablonów bezpieczeństwa.
Weryfikację praw dostępu do wybranych kluczy rejestrów systemowych.
Weryfikację parametrów sieciowych systemu operacyjnego serwera lub stacji roboczej.
Weryfikację uruchomionych usług lokalnych na serwerach i stacjach roboczych.
Sprawdzenie, w jakim stopniu wykorzystane są mechanizmy rejestrowania zdarzeń oferowane przez system.

3.Wykonawca przeprowadzi analizę konfiguracji urządzeń, które uczestniczą w procesie przesyłania i przechowywania danych. Analiza musi zostać przeprowadzony dla:
Ustawień serwerów DNS.
Ustawień serwerów WWW.
Ustawień serwerów plików.
Konfiguracji serwerów bazy danych.
Ustawień systemów Firewall, włącznie z analizą reguł dostępowych.
Ustawień systemu antywirusowego.
Architektury sieci przewodowej, bezprzewodowej.

4.Po przeprowadzonych przeglądach konfiguracji Wykonawca przekaże Zamawiającemu dokument pn. „Raport z przeprowadzonych przeglądów konfiguracji urządzeń wchodzących w skład infrastruktury IT systemu PLI CBD", zawierający szczegółowy opis wszystkich wykrytych nieprawidłowości, możliwe skutki ich wykorzystania oraz przedstawi sugerowaną metodę usunięcia błędów lub nieprawidłowości.

5.W przypadku stwierdzenia rażącego naruszenie zasad bezpieczeństwa mogącego wpłynąć na znaczne obniżenie bezpieczeństwa Systemu PLI CBD Wykonawca zobowiązany jest do bezzwłocznego poinformowania o zaistniałym fakcie Zmawiającego.

6.Sprawdzenie konfiguracji urządzeń IT musi być dokonane w jednym z Centrów Przetwarzania Danych w CPD w Boruczy lub w CPD Siemianowice Śl. Nie dopuszcza się dokonania takiego sprawdzenia w sposób zdalny oraz przekazywania plików konfiguracyjnych do analizy w trybie off-line.

7.Po zgłoszeniu przez Zamawiającego gotowości, Wykonawca, w terminie 7 dni roboczych, dokona ponownego sprawdzenia konfiguracji urządzeń, w szczególności w obszarach wcześniej wskazach, jako zagrażające bezpieczeństwo informacji w przetwarzanych w Systemie PLI CBD.
Po ponownym sprawdzeniu konfiguracji urządzeń Wykonawca przedstawi Raport końcowy zawierający:
- weryfikację czy zaproponowane w etapach opisanych w punktach podatności i problemy z bezpieczeństwem zostały rozwiązane poprawianie,

- opis aktualnego poziomu bezpieczeństwa,
- rekomendację wskazującą kierunki dalszego podnoszenia bezpieczeństwa Systemu.

Raport końcowy musi być dostarczony w formie pisemnej i elektronicznej.

8.W ramach przeglądu konfiguracji Wykonawca dokona analizy konfiguracji dla następującej ilości urządzeń:
- platforma serwerowa – do 30 % zasobów wskazanych w opisie Systemu PLI CBD.
- platforma sieciowa – do 25% zasobów wskazanych w opisie Systemu PLI CBD.
- inne elementy infrastruktury współpracujące z platformą serwerową i sieciową – do 20%
- stacje robocze – do 10% zasobów wskazanych w opisie Systemu PLI CBD.

7. Audyt bezpieczeństwa danych osobowych

7.1 Cel audytu danych osobowych

Celem audytu danych osobowych jest zbadanie procesów przetwarzania danych osobowych w ramach Systemu PLI CBD administrowanego przez Zamawiającego.

7.2 Zakres audytu przetwarzania danych osobowych

Plan wykonania zadania:
1. Audyt przetwarzania danych osobowych
Audyt przetwarzania danych osobowych ma na celu weryfikacja stanu faktycznego z obowiązującymi przepisami prawa:
- Ustawą z dnia 29 sierpnia 1997 roku o Ochronie Danych Osobowych (tj. Dz.U. 2002 r. Nr 101, poz. 926 z późn. zm).;
- Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024).

Audyt przetwarzania danych osobowych ma na celu weryfikacja stanu faktycznego z opisanym w dokumentach:
- polityka bezpieczeństwa wraz z wytycznymi w zakresie opracowania i wdrożenia polityki bezpieczeństwa opublikowanymi przez Głównego Inspektora Ochrony Danych Osobowych,
- instrukcja zarządzania systemem informatycznym wraz z wytycznymi w zakresie opracowania i wdrożenia instrukcji zarządzania systemem informatycznym opublikowanymi przez Głównego Inspektora Ochrony Danych Osobowych.

Po przeprowadzonym audycie przetwarzania danych osobowych Wykonawca przekaże Zamawiający dokument „Raport z audytu przetwarzania danych osobowych" w którym opracuje i przedstawi Zamawiającemu obszary wymagające zmian oraz przedstawi Zamawiającemu do akceptacji zalecenia korygujące.

2.Wykonawca dokona stosownych zmian i poprawek w dokumentacji już istniejącej lub przygotuje nowe wersje dokumentacji zgodnej z obowiązującymi przepisami prawa w zakresie ochrony danych osobowych.

3.Reaudyt przetwarzania danych osobowych.
Wykonawca dokona weryfikacji stanu faktycznego z obowiązującymi przepisami prawa wymienionymi w pkt. 1 po dokonanych zmianach przez Wykonawcę wskazanych nieprawidłowości w Raporcie z audytu przetwarzania danych osobowych.
Po przeprowadzonym reaudycie przetwarzania danych osobowych Wykonawca przekaże Zamawiający dokument „Raport z reaudytu przetwarzania danych osobowych".

8. Systemu Zarządzania Bezpieczeństwem Informacji i ciągłością działania

8.1 Cel Systemu Zarządzania Bezpieczeństwem Informacji i ciągłości działania

Celem zadania jest opracowanie, wdrożenie oraz przygotowanie do certyfikacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) zgodnie z wymaganiami normy PN-ISO/IEC 27001 oraz zaleceniami norm w zakresie:
1) w odniesieniu do ustanawiania zabezpieczeń PN-ISO/IEC 17799 ;
2) w odniesieniu do zarządzania ryzykiem PN-ISO/IEC 27005;
3) w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania PN-ISO/IEC 24762 .

W ramach zadania Wykonawca wykona wszelkie niezbędne prace wymagane do uzyskania przez Zamawiającego przy wsparciu Wykonawcy certyfikatu na zgodność z normą PN-ISO/IEC 27001.

8.2 Zakres przygotowania Systemu Zarządzania Bezpieczeństwem Informacji i ciągłości działania

Plan wykonania zadania:

1.Wstępny audyt bezpieczeństwa informacji oraz opracowanie koncepcji wdrożenia SZBI wg PN-ISO/IEC 27001.

W ramach audytu wstępnego Wykonawca dokona analizy istniejącego systemu zarządzania bezpieczeństwem informacji Zamawiającego w ramach Systemu PLI CBD pod kątem wymagań norm: PN-ISO/IEC 27001, PN-ISO/IEC 17799 oraz PN-ISO/IEC 24762.
W ramach audytu wstępnego Wykonawca wykona następujące usługi:
- analiza funkcjonującej dokumentacji,
- weryfikacja stosowanych sposobów rozwiązywania problemów i wykonywania zadań na rzecz użytkowników,
- weryfikacja sposobu zarządzania konfiguracją, zmianą i wydaniem,
- ocena zapewnienia dostępności i ciągłości działania rozwiązań informatycznych,

- analiza stosowanych mechanizmów bezpieczeństwa informacji,
- analiza relacji z dostawcami i klientami zewnętrznymi,
- opracowanie rekomendacji dotyczących poprawy bezpieczeństwa informacji.

Po przeprowadzonym audycie wstępnym Wykonawca przekaże Zamawiający dokument „Raport z audytu wstępnego-System Zarządzania Bezpieczeństwie Informacji" oraz opracuje i przedstawi do akceptacji Zamawiającego dokument „Koncepcji wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji wg PN-ISO/IEC 27001" zawierający m.in. elementy wymienione w OPZ oraz szczegółowy harmonogram wdrożenia SZBI.
Wykonawca przygotuje i przeprowadzi prezentację „Raport z audytu wstępnego" oraz „Koncepcji wdrożenia Systemu Zarządzania Bezpieczeństwie Informacji wg PN-ISO/IEC 27001".

2.Szkolenia wstępne dla pracowników Zamawiającego.
Szkolenie ma zaprezentować i wyjaśnić postanowienia norm: PN-ISO/IEC 27001, PN-ISO/IEC 17799 oraz PN-ISO/IEC 24762 pracownikom Zamawiającego odpowiedzialnym za utrzymanie SZBI. Szkolenie ma zostać przeprowadzone zgodnie z wymaganiami wymienionymi w pkt. 4.1 Szkolenie - wymagania ogólne. Szkolenie ma zostać przeprowadzone dla grupy maksymalnie 24 osób wskazanych przez Zamawiającego.

3.Opracowanie niezbędnej dokumentacji.
W celu zapewnienia skutecznego planowania, działania i kontroli bezpieczeństwa informacji Wykonawca utworzy i dostarczy Zamawiającemu procedury opisujące następujące procesy:

a) Polityka bezpieczeństwa informacji;

b) Organizacja bezpieczeństwa informacji:
- umowy z firmami zewnętrznymi.

c) Zarządzanie aktywami:
- klasyfikacja informacji.

d) Zarządzanie ryzykiem;

e) Bezpieczeństwo zasobów ludzkich:
- etap naboru pracownika;
- zatrudnienie;
- zakończenie zatrudnienia.

f) Bezpieczeństwo fizyczne i środowiskowe:
- obszary bezpieczne;
- ochrona sprzętu.

g) Zarządzanie systemami informacyjnymi;
- zasady użytkowania;
- umowy serwisowe;

- minimalizacja ryzyka awarii systemów;
- ochrona integralności oprogramowania;
- kopie zapasowe;
- bezpieczeństwo sieci;
- zarządzanie nośnikami informacji;
- zasady bezpiecznej wymiany informacji;
- monitorowanie.

h) Kontrola dostępu:
- zarządzanie dostępem użytkowników;
- zakres odpowiedzialności użytkowników;
- kontrola dostępu do sieci;
- kontrola dostępu do systemów operacyjnych;
- kontrola dostępu do aplikacji;

i) Wdrażanie i serwis systemów informacyjnych:
- wymagania bezpieczeństwa;
- projektowanie zabezpieczeń;
- ochrona kryptograficzna;
- zasady bezpieczeństwa plików systemowych;
- wymagania bezpieczeństwa podczas procesów rozwojowych i obsługowych;
- zarządzanie podatnościami technicznymi.

j) Zarządzanie incydentami związanymi z bezpieczeństwem informacji:
- zgłaszanie zdarzeń;
- postępowanie z incydentami.

k) Zarządzanie ciągłością działania:
- zapewnienie ciągłości działania;
- identyfikacja zdarzeń i szacowanie ryzyka;
- plany ciągłości działania;
- odtwarzanie po katastrofie.

l) Zapewnienie zgodność:
- zgodności z prawem;
- zgodności ze standardami.

m) Pomiary Systemu Zarządzania Bezpieczeństwem Informacji
- przegląd SZBI;
- cele pomiaru bezpieczeństwa informacji;
- model pomiaru SZBI;
- pomiary;
- wskaźniki.

4.Wdrożenie systemu zarządzania bezpieczeństwem informacji.

Wdrożenie SZBI w organizacji Zamawiającego poprzez integrację w ramach Zintegrowanego Systemu Zarządzania, systemu zarządzania jakością PN-ISO/IEC 9001 oraz systemu zarządzania usługami informatycznymi PN-ISO/IEC 20000-1.
Wykonawca przygotuje i przeprowadzi dla pracowników Zamawiającego odpowiedzialnym za utrzymanie SZBI szkolenie z zakresu opracowanych polityk, planów i procedur. Szkolenie ma zostać przeprowadzone zgodnie z wymaganiami wymienionymi w pkt. 4.1 Szkolenie - wymagania ogólne. Szkolenie ma zostać przeprowadzone dla grupy maksymalnie 24 osób wskazanych przez Zamawiającego.

5.Przeprowadzenie powdrożeniowego audytu wewnętrznego (etap 2).
Audyt powdrożeniowy ma celu ocenę poprawności wdrożonego SZBI, a także zdefiniować rozbieżności oraz wskazać ewentualne dalsze wytyczne naprawcze.
Po przeprowadzonym audycie powdrożeniowym Wykonawca przekaże Zamawiającemu dokument „Raport z audytu powdrożeniowego-System Zarządzania Bezpieczeństwem Informacji".
Wykonawca przygotuje i przeprowadzi prezentację „Raport z audytu powdrożeniowego System Zarządzania Bezpieczeństwem Informacji".

6.Wsparcie Zamawiającego w wyborze jednostki certyfikującej i nadzór nad procesem certyfikacji (etap 2).
Wykonawca ma wskazać Zamawiającemu i przedstawić ofertę usług certyfikacji na zgodność z normą PN-ISO/IEC 27001 nie mniej niż trzech jednostek certyfikujących wraz z podaniem całkowitego kosztu uzyskania certyfikatu.
Wykonawca przygotuje wszystkie niezbędne dokumenty formalne wymagane w procesie certyfikacji (np. wniosek o certyfikację lub inne).
Konsultant Wykonawcy, na wezwanie Zamawiającego, będzie uczestniczył w całym procesie certyfikacji oraz w audycie zewnętrznym.
Przed przystąpieniem do procesu certyfikacji Wykonawca przeprowadzi dla pracowników Zamawiającego odpowiedzialnych za utrzymanie SZBI szkolenie przypominające dotyczące obowiązujących procesów i procedur.

7. Wykonanie działań korygujących po audycie jednostki certyfikującej (etap 2).
W przypadku stwierdzenia nieprawidłowości podczas audytu certyfikacyjnego Wykonawca wykona wszystkie niezbędne działania korygujące wykrytych niezgodności.

Wszystkie szkolenia oraz prezentacji dla pracowników Zamawiających przewidziane w tym zadaniu zostaną przeprowadzone oddzielnie dla pracowników zatrudnianych w PLI CBD w Boruczy oraz dla pracowników zatrudnianych w PLI CBD w Siemianowicach Śl. w miejscu ich pracy.

9. Systemu Zarządzania Usługami Informatycznymi

9.1 Cel Systemu Zarządzania Usługami Informatycznymi

Celem zadania jest opracowanie, wdrożenie oraz przygotowanie do certyfikacji Systemu Zarządzania Usługami Informatycznymi (SZUI) zgodnie z wymaganiami normy

PN-ISO/IEC 20000-1 oraz PN-ISO/IEC 20000-2
W ramach zadania Wykonawca wykona wszelkie niezbędne prace wymagane do uzyskania przez Zamawiającego przy wsparciu Wykonawcy certyfikatu na zgodność z normą
PN-ISO/IEC 20000-1 oraz PN-ISO/IEC 20000-2

9.2 Zakres przygotowania Systemu Zarządzania Usługami Informatycznymi

Plan wykonania zadania:

1.Wstępny audyt jakości usług informatycznych oraz opracowanie koncepcji wdrożenia SZUI wg PN-ISO/IEC 20000-1 oraz PN-ISO/IEC 20000-2.

W ramach audytu wstępnego Wykonawca dokona analiza istniejącego systemu zarządzania usługami informatycznymi Zamawiającego w ramach Systemu PLI CBD pod kątem wymagań normy PN-ISO/IEC 20000-1 oraz PN-ISO/IEC 20000-2.
W ramach audytu wstępnego Wykonawca wykona następujące usługi:
- analiza funkcjonującej dokumentacji,
- weryfikacja stosowanych sposobów rozwiązywania problemów i wykonywania zadań na rzecz użytkowników,
- weryfikacja sposobu zarządzania konfiguracją, zmianą i wydaniem,
- ocena zapewnienia dostępności i ciągłości rozwiązań informatycznych,
- analiza stosowanych mechanizmów bezpieczeństwa informacji,
- analiza relacji z dostawcami i klientami zewnętrznymi,
- opracowanie rekomendacji dotyczących poprawy jakości usług informatycznych.

Po przeprowadzonym audycie wstępnym Wykonawca przekaże Zamawiającemu dokument „Raport z audytu wstępnego-System Zarządzania Usługami Informatycznymi" oraz opracuje i przedstawi do akceptacji Zamawiającego dokument „Koncepcji wdrożenia Systemu Zarządzania Usługami Informatycznymi wg PN-ISO/IEC 20000-1 oraz PN-ISO/IEC 20000-2" zawierający m.in. elementy wymienione w OPZ oraz szczegółowy harmonogram wdrożenia SZUI.
Wykonawca przygotuje i przeprowadzi prezentację „Raport z audytu wstępnego System Zarządzania Usługami Informatycznymi" oraz „Koncepcji wdrożenia Systemu Zarządzania Usługami Informatycznymi wg PN-ISO/IEC 20000-1 oraz PN-ISO/IEC 20000-2".

3.Szkolenia wstępne dla pracowników Zamawiających.
Szkolenie ma zaprezentować i wyjaśnić postanowienia normy PN-ISO/IEC 20000-1 oraz PN-ISO/IEC 20000-2 pracownikom Zamawiającym odpowiedzialnym za utrzymanie SZUI. Szkolenie ma zostać przeprowadzone zgodnie z wymaganiami wymienionymi w pkt. 4.1 Szkolenie - wymagania ogólne. Szkolenie ma zostać przeprowadzone dla grupy maksymalnie 24 osób wskazanych przez Zamawiającego.

4.Opracowanie niezbędnej dokumentacji.
W celu zapewnienia skutecznego planowania, działania i kontroli usług Wykonawca opisze i dostarczy Zamawiającemu procedury opisujące następujące procesy:

a) Polityka zarządzania usługami informatycznymi;

b) Procesy dostarczania usług:
- zarządzanie poziomem usług,
- zarządzanie potencjałem wykonawczym,
- zarządzanie ciągłością i dostępnością usług,
- tworzenie budżetu i rozliczanie usług IT,
- zarządzanie bezpieczeństwem informacji,
- sporządzanie raportu z usług.

c) Procesy związków:
- zarządzanie związkami biznesu,
- zarządzanie poddostawcami.

d) Procesy rozwiązań:
- zarządzanie incydentem,
- zarządzanie problemem.

e) Procesy kontrolne:
- zarządzanie konfiguracja,
- zarządzanie zmianami.

f) Procesy wydawania:
- zarządzanie wydawaniem.

5.Wdrożenie systemu zarządzania usługami informatycznymi.
Wdrożenie SZUI w organizacji Zamawiającego poprzez integrację w ramach Zintegrowanego Systemu Zarządzania, systemu zarządzania jakością ISO/IEC 9001 oraz systemu zarządzania bezpieczeństwem informacji ISO/IEC 27001 w którym wydzielone zostaną procesy z obszaru IT.
Wykonawca przygotuje i przeprowadzi dla pracowników Zamawiającego odpowiedzialnym za utrzymanie SZUI szkolenie z zakresu opracowanych polityk, planów i procedur. Szkolenie ma zostać przeprowadzone zgodnie z wymaganiami wymienionymi w pkt. 4.1 Szkolenie - wymagania ogólne. Szkolenie ma zostać przeprowadzone dla grupy maksymalnie 24 osób wskazanych przez Zamawiającego

6.Przeprowadzenie powdrożeniowego audytu wewnętrznego (etap 2).
Audyt powdrożeniowy ma celu ocenę poprawności wdrożonych SZUI, a także zdefiniować rozbieżności oraz ewentualne dalsze wytyczne naprawcze.
Po przeprowadzonym audycie powdrożeniowym Wykonawca przekaże Zamawiającemu dokument „Raport z audytu powdrożeniowego-Systemu Zarządzania Usługami Informatycznymi".
Wykonawca przygotuje i przeprowadzi prezentację „Raport z audytu powdrożeniowego Systemu Zarządzania Usługami Informatycznymi".

7.Wsparcie Zamawiającego w wyborze jednostki certyfikującej i nadzór nad procesem certyfikacji (etap 2).

Wykonawca ma wskazać Zamawiającemu i przedstawić ofertę usług certyfikacji na zgodność z normą PN-ISO/IEC 20000-1 nie mniej niż trzech jednostek certyfikujących wraz z podaniem całkowitego kosztu uzyskania certyfikatu.
Wykonawca przygotuje wszystkie niezbędne dokumenty formalne wymagane w procesie certyfikacji (np. wniosek o certyfikację lub inne).
Konsultant Wykonawcy, na wezwanie Zamawiającego, będzie uczestniczył w całym procesie certyfikacji oraz w audycie zewnętrznym.
Przed przystąpieniem do procesu certyfikacji Wykonawca przeprowadzi dla pracowników Zamawiającego odpowiedzialnych za utrzymanie SZUI szkolenie przypominające dotyczące obowiązujących procesów i procedur.

8. Wykonanie działań korygujących po audycie jednostki certyfikującej (etap 2).
W przypadku stwierdzenia nieprawidłowości podczas audytu certyfikacyjnego Wykonawca wykona wszystkie niezbędne działania korygujące wykrytych niezgodności.

Wszystkie szkolenia oraz prezentacji dla pracowników Zamawiających przewidziane w tym zadaniu zostaną przeprowadzone oddzielnie dla pracowników zatrudnianych w PLI CBD w Boruczy oraz dla pracowników zatrudnianych w PLI CBD w Siemianowicach w miejscu ich pracy.

10.Asysta powdrożeniowa

W okresie 24 miesięcy od daty podpisania protokołu odbioru końcowego wdrożonego zintegrowanego systemu zarządzania bezpieczeństwem informacji, ciągłością działania i jakością usług informatycznych Wykonawca będzie świadczył na rzecz Zamawiającego usługi wsparcia.

10.1 Zakres asysty powdrożeniowej

a) ochrona danych osobowych:
- przegląd i aktualizacja dokumentacji związanej z procesem przetwarzania danych osobowych nie rzadziej niż raz na sześć miesięcy,
- przegląd i aktualizacja dokumentacji związanej z procesem przetwarzania danych osobowych w przypadku zmiany przepisów prawa w zakresie przetwarzania danych osobowych, nie rzadziej niż raz na sześć miesięcy,
- przegląd i aktualizacja dokumentacji związanej z procesem przetwarzania danych osobowych na każdorazowe wezwanie Zamawiającego, przy czym przewiduje się maksymalnie cztery takie wezwania niezależnie od zapisów powyżej.

b) Systemu Zarządzania Usługami Informatycznymi:
- przeprowadzenie powdrożeniowego audytu wewnętrznego,
- wsparcie Zamawiającego w wyborze jednostki certyfikującej, nadzór i udział w procesie certyfikacji,
- wykonanie działań korygujących po audycie jednostki certyfikującej.
- przegląd i aktualizacja dokumentacji związanej z SZUI nie rzadziej niż raz na sześć miesięcy,
- przegląd i aktualizacja dokumentacji związanej z SZUI każdorazowo w przypadku zmiany norm z rodziny PN-ISO/IEC 20000-1,

- przegląd i aktualizacja dokumentacji związanej z SZUI na każdorazowe wezwanie Zamawiającego, przy czym przewiduje się maksymalnie cztery takie wezwania niezależnie od zapisów powyżej,
- dwudniowe szkolenie z zakresu Audytor wewnętrzny systemu zarządzania usługami informatycznymi wg ISO/IEC 2000-1 dla grupy trzech osób wskazanych przez Zamawiającego. Zakres szkolenia: cel i wymagania normy PN-ISO/IEC 20000-1, planowanie audytu, przebieg audytu, raportowanie i dalsze postępowanie.
- konsultacje eksperckie przy rozwiązywaniu problemów. Zgłoszenie zapytań będzie odbywać się drogą telefoniczną lub na dedykowany adres e-mail. Maksymalny czas na odpowiedź konsultanta w przypadku pytań specjalistycznych wynosić będzie 2 dni robocze.
Miesięcznie Wykonawca będzie zobowiązany do udzielenia odpowiedzi na maksymalnie 10 zapytań. Liczba niewykorzystanych pytań w danym miesiącu nie będzie przechodziła na następny miesiąc.

c) Systemu Zarządzania Bezpieczeństwem Informacji i ciągłością działania:
- przeprowadzenie powdrożeniowego audytu wewnętrznego,
- wsparcie Zamawiającego w wyborze jednostki certyfikującej, nadzór i udział w procesie certyfikacji,
- wykonanie działań korygujących po audycie jednostki certyfikującej,
- przegląd i aktualizacja dokumentacji związanej z SZBI nie rzadziej niż raz na sześć miesięcy,
- przegląd i aktualizacja dokumentacji związanej z SZBI w przypadku zmiany norm z rodziny PN-ISO/IEC 27001, nie rzadziej niż raz na sześć miesięcy
- przegląd i aktualizacja dokumentacji związanej z SZBI na każdorazowe wezwanie Zamawiającego, przy czym przewiduje się maksymalnie cztery takie wezwania niezależnie od zapisów powyżej,
- dwudniowe szkolenie z zakresu Audytor wewnętrzny systemu zarządzania bezpieczeństwem informacji wg PN-ISO/IEC 27001 dla grupy trzech osób wskazanych przez Zamawiającego. Zakres szkolenia: cel i wymagania normy PN-ISO/IEC 27001, planowanie audytu, przebieg audytu, raportowanie i dalsze postępowanie.
- konsultacje eksperckie przy rozwiązywaniu problemów. Zgłoszenie zapytań będzie odbywać się drogą telefoniczną lub na dedykowany adres e-mail. Maksymalny czas na odpowiedź konsultanta w przypadku pytań specjalistycznych wynosić będzie 2 dni robocze.
Miesięcznie Wykonawca będzie zobowiązany do udzielenia odpowiedzi na maksymalnie 10 zapytań. Liczba niewykorzystanych pytań w danym miesiącu nie będzie przechodziła na następny miesiąc.

d) Przegląd konfiguracji urządzeń IT
- dwukrotne wykonanie przeglądów konfiguracji urządzeń IT, w okresie asysty, w zakresie i ilości opisanej w pkt. 5. Przegląd konfiguracji urządzeń IT.

e) Testy penetracyjne
- dwukrotne wykonanie testów penetracyjnych, w okresie asysty, w zakresie i ilości opisanej w pkt. 6. Testy penetracyjne.

11.Opis Systemu PLI CBD wraz z wykaz zainstalowanego sprzętu,

oprogramowania oraz licencji

Niniejszy opis stanowi wykaz zasobów sprzętowych i programowych (licencji) posiadanych przez Zamawiającego . Wykaz ten dotyczy całego obecnego rozwiązania PLI CBD w obydwu Centrach Przetwarzania Danych. Wykaz dotyczy zarówno sprzętu IT PLI CBD jak i systemów infrastruktury budynkowej Centrów Przetwarzania Danych.

W skład infrastruktura PLI CBD wchodzą dwa centra przetwarzania danych zlokalizowane w Siemianowicach Śl. i Boruczy (56 km od centrum Warszawy).

Serwery.
Poniżej zamieszczony został ilościowy wykaz serwerów fizycznych oraz zwirtualizowanych Wykaz ten zawiera również informację o zainstalowanych systemach operacyjnych jak również dodatkowym oprogramowaniu.

Wykaz serwerów z systemami operacyjnymi CPD Siemianowice Śl.

Lp	Urządzenie	Funkcja	System operacyjny
1	IBM x3650 M2 TYP I	Serwer Aplikacyjny1/1	MS Windows Server 2008 R2 Standard
2	IBM x3650 M2 TYP I	Serwer Aplikacyjny1/2	MS Windows Server 2008 R2 Standard
3	IBM x3650 M2 TYP I	Serwer Aplikacyjny2/1	MS Windows Server 2008 R2 Standard
4	IBM x3650 M2 TYP I	Serwer Aplikacyjny2/2	MS Windows Server 2008 R2 Standard
5	IBM x3650 M2 TYP I	Serwer Aplikacyjny3/1	MS Windows Server 2008 R2 Standard
6	IBM x3650 M2 TYP I	Serwer Aplikacyjny3/2	MS Windows Server 2008 R2 Standard
7	IBM x3650 M2 TYP II	Serwer Bazodanowy1/1	MS Windows Server 2008 R2 Standard
8	IBM x3650 M2 TYP II	Serwer Bazodanowy1/2	MS Windows Server 2008 R2 Standard
9	IBM x3650 M2 TYP II	Serwer Bazodanowy2/1	MS Windows Server 2008 R2 Standard
10	IBM x3650 M2 TYP II	Serwer Bazodanowy2/2	MS Windows Server 2008 R2 Standard
11	IBM x3550 M2 TYP I	Serwer Backupów 1/1	MS Windows Server 2008 R2 Enterprise
12	IBM x3550 M2 TYP I	Serwer Backupów 1/2	MS Windows Server 2008 R2 Enterprise
13	IBM x3550 M2 TYP II	Serwer PKI 1/1	MS Windows Server 2008 R2 Enterprise
14	IBM x3550 M2 TYP II	Serwer PKI 1/2	MS Windows Server 2008 R2 Enterprise

15	IBM x3550 M2 TYP II	Serwer Monitoringu 1	Red Hat Enterprise Linux 5.2 "Tikanga"
16	HP DL12066	Serwer OsTicket	Debian 6.0 Linux 2.6.32-5-amd64
17	maszyna wirtualna	Serwer ADDS 1/1	MS Windows Server 2008 R2 Enterprise
18	maszyna wirtualna	Serwer ADDS 1/2	MS Windows Server 2008 R2 Enterprise
19	maszyna wirtualna	Serwer ADCS 1/1	MS Windows Server 2008 R2 Enterprise
20	maszyna wirtualna	Serwer ADCS 1/2	MS Windows Server 2008 R2 Enterprise
21	maszyna wirtualna	Serwer ADCS 1/3	MS Windows Server 2008 R2 Enterprise

Wykaz serwerów z systemami operacyjnymi CPD Borucza

Lp	Urządzenie	Funkcja	Sytem operacyjny
1	IBM x3650 M2 TYP I	Serwer Aplikacyjny1/1	MS Windows Server 2008 R2 Standard
2	IBM x3650 M2 TYP I	Serwer Aplikacyjny1/2	MS Windows Server 2008 R2 Standard
3	IBM x3650 M2 TYP I	Serwer Aplikacyjny2/1	MS Windows Server 2008 R2 Standard
4	IBM x3650 M2 TYP I	Serwer Aplikacyjny2/2	MS Windows Server 2008 R2 Standard
5	IBM x3650 M2 TYP I	Serwer Aplikacyjny3/1	MS Windows Server 2008 R2 Standard
6	IBM x3650 M2 TYP I	Serwer Aplikacyjny3/2	MS Windows Server 2008 R2 Standard
7	IBM x3650 M2 TYP II	Serwer Bazodanowy1/1	MS Windows Server 2008 R2 Standard
8	IBM x3650 M2 TYP II	Serwer Bazodanowy1/2	MS Windows Server 2008 R2 Standard
9	IBM x3650 M2 TYP II	Serwer Bazodanowy2/1	MS Windows Server 2008 R2 Standard
10	IBM x3650 M2 TYP II	Serwer Bazodanowy2/2	MS Windows Server 2008 R2 Standard
11	IBM x3550 M2 TYP I	Serwer Backupów 1/1	MS Windows Server 2008 R2 Enterprise
12	IBM x3550 M2 TYP I	Serwer Backupów 1/2	MS Windows Server 2008 R2 Enterprise
13	IBM x3550 M2 TYP II	Serwer PKI 1/1	MS Windows Server 2008 R2 Enterprise
14	IBM x3550 M2 TYP II	Serwer PKI 1/2	MS Windows Server 2008 R2 Enterprise
15	IBM x3550 M2 TYP II	Serwer Monitoringu 1	Red Hat Enterprise Linux 5.2

			"Tikanga"
16	IBM x3650 M2 TYP III	Serwer Testowy 1	MS Windows Server 2008 R2 Standard
17	maszyna wirtualna	Serwer ADDS 1/1	MS Windows Server 2008 R2 Enterprise
18	maszyna wirtualna	Serwer ADDS 1/2	MS Windows Server 2008 R2 Enterprise
19	maszyna wirtualna	Serwer ADCS 1/1	MS Windows Server 2008 R2 Enterprise
20	maszyna wirtualna	Serwer ADCS 1/2	MS Windows Server 2008 R2 Enterprise

Konfiguracja sprzętowa

Poniżej przedstawione zostały podstawowe parametry sprzętowe poszczególnych urządzeń.

IBM x3650 M2 TYP I

- procesory 64-bitowe 4-rdzeniowe, taktowane zegarem 2,26GHz, 8MB Cache, szyna danych 1066MHz, architektura INTEL
- 32 GB RAM (max. 128GB)
- 2 zasilacze 675W typu „hot swap”
- Napęd CD-RW/DVD (combo)
- Obudowa RACK (19”) 2U
- Karta graficzna SVGA 16MB
- Kontroler RAID (M5014: RAID 0,1,5,6,10)
- 2 dyski 146 GB 2.5”
- 2xKarta FC
- 4x Ethernet 10/100/1000
- 4x USB
- Karta zdalnego zarządzania IBM Virtual Media Key
- Panel diagnostyczny, diagnostyczne kontrolki LED
- Hot-swap’owe redundantne wentylatory
- Wbudowany wielokanałowy kontroler SR BR10i

IBM x3650 M2 TYP II

- procesory 64-bitowe 4-rdzeniowe, taktowane zegarem 2,26GHz, 8MB Cache, szyna danych 1066MHz, architektura INTEL
- 48 GB RAM (max. 128GB)
- 2 zasilacze 675W typu „hot swap”
- Napęd CD-RW/DVD (combo)
- Obudowa RACK (19”) 2U
- Karta graficzna SVGA 16 MB
- Kontroler RAID (M5014: RAID 0,1,5,6,10)
- 6 dysków 146GB 2.5” 15k rpm (RAID1: 2 dyski RAID 5: 4 dyski)
- 2xKarta FC

- 2x Ethernet 10/100/1000
- 4x USB
- Karta zdalnego zarządzania IBM Virtual Media Key
- Panel diagnostyczny, diagnostyczne kontrolki LED
- Hot-swap'owe redundantne wentylatory
- Wbudowany wielokanałowy kontroler SR BR10i
- IBM x3650 M2 TYP III
- procesory 64-bitowe 4-rdzeniowe, taktowane zegarem 2,26GHz, 8MB Cache, szyna danych 1066MHz, architektura INTEL
- 48 GB RAM (max. 128GB)
- 2 zasilacze 675W typu „hot swap"
- Napęd CD-RW/DVD (combo)
- Obudowa RACK (19") 2U
- Karta graficzna SVGA 16 MB
- Kontroler RAID (M5014: RAID 0,1,5,6,10)
- 6 dysków 146GB 2.5" 15k rpm
- 2xKarta FC
- 2x Ethernet 10/100/1000
- 4x USB
- Karta zdalnego zarządzania IBM Virtual Media Key
- Panel diagnostyczny, diagnostyczne kontrolki LED
- Hot-swap'owe redundantne wentylatory
- Wbudowany wielokanałowy kontroler SR BR10i

IBM x3550 M2 TYP I

- 1 procesor 64-bitowy 4-rdzeniowy, taktowany zegarem 2,26GHz, 8MB Cache, szyna danych 1066MHz, architektura INTEL
- 48 GB RAM (max. 128GB)
- zasilacze 675W typu „hot swap"
- Napęd CD-RW/DVD (combo)
- Obudowa RACK (19") 2U
- Karta graficzna SVGA 16 MB
- 2 dyski 146GB 2.5"
- 2xKarta FC
- 2x Ethernet 10/100/1000
- 4x USB
- Karta zdalnego zarządzania IBM Virtual Media Key
- Panel diagnostyczny, diagnostyczne kontrolki LED
- Hot-swap'owe redundantne wentylatory
- Wbudowany wielokanałowy kontroler SR BR10i
- IBM x3550 M2 TYP II
- 1 procesor 64-bitowy 4-rdzeniowy, taktowany zegarem 2,0GHz, 8MB Cache, szyna danych 1066MHz, architektura INTEL
- 48 GB RAM (max. 128GB)

- 2 zasilacze 675W typu „hot swap”
- Napęd CD-RW/DVD (combo)
- Obudowa RACK (19”) 2U
- Karta graficzna SVGA 16 MB
- 2 dyski 146GB 2.5”
- 2x Ethernet 10/100/1000
- 4x USB
- Karta zdalnego zarządzania IBM Virtual Media Key
- Panel diagnostyczny, diagnostyczne kontrolki LED
- Hot-swap’owe redundantne wentylatory
- Wbudowany wielokanałowy kontroler SR BR10i

HP DL12066

- 1 procesor Intel
- 1 dysk SATA 160GB
- 4 GB RAM DDR3
- 1 x PCI E x16 v2.0
- 1 x PCI E x4 v2.0
- 2x Ethernet 10/100/1000
- 5x USB 2.0
- 1 zasilacz 500W

Wykaz oprogramowania
Serwery Aplikacyjne

- IIS 7
- Aplikacja PLI-CBD
- .NET
- Agent oprogramowania Symantec BackupExec
- Qlogic SANsurfer (zarządzanie kartami HBA firmy Qlogic)
- Broadcom Advanced Control Suite (zarządzanie kartami sieciowymi Broadcom)

Serwery Bazodanowe

- MS SQL SERVER 2008 R2 (SP1) Standard Edition (x64)
- Agent oprogramowania Symantec BackupExec
- Qlogic SANsurfer (zarządzanie kartami HBA firmy Qlogic)
- Broadcom Advanced Control Suite (zarządzanie kartami sieciowymi Broadcom)

Serwery Archiwizacji

- Symantec BackupExec 12.5
- IBM Systems Director (zarządzanie środowiskami IBM)
- IBM N series System Manager (zarządzanie macierzą)
- Qlogic SANsurfer (zarządzanie kartami HBA firmy Qlogic)
- Broadcom Advanced Control Suite (zarządzanie kartami sieciowymi Broadcom)
- Hosty maszyn wirtualnych

- VMWARE Server 2.0.2
- VMWARE Tools
- Monitoring
- Nagios Core 3.2.3
- MRTG

Aplikacja PLI CBD

Środowisko Programistyczne

Aplikacja PLI CBD przygotowana została do pracy w środowisku systemu operacyjnego Windows 2008 x64, bazy danych MS SQL Server 2008 x64 oraz środowiska .NET 4.0. Podstawowym narzędziem developerskim które posłużyło do wytworzenia kodu aplikacji było Visual Studio 2010. Kod źródłowy aplikacji napisany został w języku C#.

Dodatkowo zastosowana została biblioteka Chilkat firmy ChilkatSoftware, Inc. Biblioteka zawiera klasy do tworzenia i wysyłania maili, kompresji danych oraz dostępu do serwerów SFTP.

Komponenty systemu rozlokowane są na wszystkich serwerach aplikacyjnych w obu lokalizacjach oraz na wszystkich serwerach bazodanowych. W przypadku serwerów aplikacyjnych są to aplikacje przeznaczone do uruchamiania w środowisku .NET w ramach serwera IIS 7.5 – webserwisy oraz aplikacje ASP.NET. W przypadku serwerów aplikacyjnych i serwerów bazodanowych są to także serwisy systemowe, uruchamiane w środowisku .NET.

Dostęp z serwerów aplikacyjnych do baz danych wykorzystuje protokół TCP/IP. Dostęp z serwisów systemowych umieszczonych na serwerach bazodanowych wykorzystuje szybką i wydajną technologię Shared Memory. Rozmieszczenie komponentów jest takie, aby manipulacje większymi porcjami danych wykonywane były poprzez serwisy na serwerach bazodanowych, dzięki temu w pełni wykorzystane są zalety wydajnego dostępu do danych.

Model bazy danych

Z uwagi na wymóg zapewnienia bardzo wysokiej niezawodności systemu architektura rozwiązania bazuje na równolegle pracujących, redundantnych komponentach i bazach danych.

Całość danych utrzymywanych w bazach relacyjnych podzielona jest na pięć osobnych baz:

E112 – operacyjna baza danych obsługująca wywołania i zapytania lokalizacyjne. W każdej lokalizacji są dwie równoległe instancje tej bazy uruchamiane na osobnych serwerach bazodanowych. Pliki z danymi i logami utrzymywane są na macierzy dyskowej obecnej w danej lokalizacji. Aktualny rozmiar bazy (danych i logu transakcyjnego) wynosi ok. 100 GB.

NP – operacyjna baza danych obsługująca komunikaty i procesy przenoszenia numerów. W każdej lokalizacji jest jedna, spójna z drugą lokalizacją wersja tej bazy. Baza podłączona jest do jednego z serwerów bazodanowych w lokalizacji i jest replikowana poprzez wewnętrzny mechanizm serwera SQL (mirroring) na drugi serwer. Aktualny rozmiar bazy (danych i logu transakcyjnego) wynosi ok. 12 GB.

MAIN – referencyjna baza danych utrzymująca konfigurację, słowniki i aktualne tabele z bieżącym obrazem numerów przeniesionych, umowy o udostępnianie numeracji i zakresy numeracji przydzielone przez UKE. W każdej lokalizacji jest jedna, spójna z drugą lokalizacją, wersja tej bazy. Pliki z danymi i logami utrzymywane są na macierzy dyskowej obecnej w danej lokalizacji. Baza podłączona jest do jednego z serwerów bazodanowych w lokalizacji i

jest replikowana poprzez wewnętrzny mechanizm serwera SQL (mirroring) na drugi serwer. Aktualny rozmiar bazy (danych i logu transakcyjnego) wynosi ok. 125 GB.

ARCH_E112 – baza archiwizacyjna danych E112. W każdej lokalizacji jest jedna, spójna z drugą lokalizacją, wersja tej bazy. Pliki z danymi i logami utrzymywane są na macierzy dyskowej obecnej w danej lokalizacji. Baza podłączona jest do jednego z serwerów bazodanowych w lokalizacji i jest replikowana poprzez wewnętrzny mechanizm serwera SQL (mirroring) na drugi serwer. Aktualny rozmiar bazy (danych i logu transakcyjnego) wynosi ok. 400 GB.

ARCH_NP – baza archiwizacyjna danych NP. W każdej lokalizacji jest jedna, spójna z drugą lokalizacją, wersja tej bazy. Pliki z danymi i logami utrzymywane są na macierzy dyskowej obecnej w danej lokalizacji. Baza podłączona jest do jednego z serwerów bazodanowych w lokalizacji i jest replikowana poprzez wewnętrzny mechanizm serwera SQL (mirroring) na drugi serwer. Aktualny rozmiar bazy (danych i logu transakcyjnego) wynosi ok. 10 GB.

Dodatkowe uwagi dotyczące aplikacji PLI CBD

Z uwagi na wymóg zapewnienia bardzo wysokiej niezawodności systemu w zakresie przyjmowania i przetwarzania zdarzeń lokalizacyjnych architektura rozwiązania bazuje na równolegle pracujących, redundantnych komponentach i bazach danych.

System pracuje w dwóch lokalizacjach współpracujących ze sobą w klastrze Active-Active (Borucza – Siemianowice Śląskie). Do równoważenia obciążenia i procesów synchronizacji został stworzone specjalnie dedykowane oprogramowanie i komponenty umożliwiające dostęp do obu lokalizacji.

Moduły systemu pracują na serwerach podzielonych na 5 grup:

Serwery aplikacyjne do przyjmowania i przetwarzania zdarzeń E112

Serwery aplikacyjne do obsługi zapytań służb ratunkowych

Serwery aplikacyjne do obsługi procesów NP

Serwery bazodanowe do obsługi zdarzeń E112

Serwery bazodanowe do przechowywania danych operacyjnych i archiwalnych E112 i NP

Dla wszystkich serwerów w ramach lokalizacji jest zapewniona redundancja. Serwery bazodanowe do obsługi zdarzeń E112 pracują w ramach lokalizacji w klastrze Active-Active . Serwery bazodanowe do przechowywania danych operacyjnych i archiwalnych E112 i NP w celu zwiększenia niezawodności w ramach lokalizacji wykorzystują mechanizmów SQL Server Database Mirroring.

System pracuje w systemach operacyjnego Windows 2008 x64, przy wykorzystaniu bazy danych MS SQL Server 2008 x64 oraz środowiska .NET 4.0. Podstawowym narzędziem developerskim jest Visual Studio 2010.

Zarówno od strony świata zewnętrznego jak i lokalnej sieci operatorów PLI CBD dostęp do systemu zawsze odbywa się przy użyciu protokołu HTTPS. Każdy z użytkowników lub interfejsów używa wydanego przez PLI CBD certyfikatu klienckiego. Certyfikaty są wystawiana za pomocą hierarchicznego PKI uruchomionego w infrastrukturze PLI CBD.

Do zarządzania, udostępniania danych i raportowania zostały stworzone aplikacje webowe w języku programowania ASP.NET. Każda aplikacja pobiera dane z dwóch lokalizacji, monitorując sytuacje niedostępności jednej z nich. Przy braku dostępności jednej z lokalizacji wszystkie funkcje aplikacji są w pełni funkcjonalne, a wszelkie dane dodane lub zmodyfikowane zostaną zsynchronizowane po przywróceniu dostępności.

Replikacja danych pomiędzy lokalizacjami jest oprogramowana w języku C# .NET bez wykorzystania komercyjnych mechanizmów. W ramach lokalizacji część baz danych jest

zdublowana przy użyciu SQL Server Database Mirroring, a część objęta mechanizmem synchronizacji i równoległego zapisu oprogramowanego w C# .NET. Dane są replikowane na bieżąco w ramach i pomiędzy lokalizacjami a w przypadku braku dostępności synchronizowane po przywróceniu dostępu.
Wszystkie aplikacje objęte są monitoringiem w celu wykrywania błędów, sytuacji awaryjnych jak również wykrywaniu braków w przekazywanych danych przez operatorów telekomunikacyjnych i dostawców usług. Monitoring jest obsługiwany przez oprogramowanie Nagios działające w systemie operacyjnym Linux. Wszystkie moduły systemu PLI CBD są zintegrowane z systemem Nagios i monitorują na bieżąco wszystkie sytuacje awaryjne i ostrzeżenia.
Moduły PLICBD są zintegrowane z systemem RSA Envision, który zbiera, zabezpiecza i archiwizuje i monitoruje wszystkie zdarzenia.
IBM InfoSphere Guardium jest używany do nadzoru i detekcji zapytań do bazy danych.

Wykaz raportów w aplikacji.

- Informacja o przynależności numeru
- Lista logicznych punktów dostępu
- Eksport danych zakresów numeracji
- Lista służb alarmowych
- Lista operatorów
- Lista NKA
- Lista numerów technicznych
- Lista numerów rutingowych
- Pobieranie danych wsadowych
- Statystyki danych wsadowych
- Ilość zdarzeń wg operatora i powiatu
- Ilość zapytań wg służb i obszaru numeracji
- Lista archiwalnych lokalizacji wg operatora i powiatu
- Lista archiwalnych zapytań służb
- Plik statystyczny ilości zdarzeń
- Plik statystyczny ilości zapytań służb
- Aktualne zdarzenia dla numeru
- Aktualne zapytania dla numeru
- Statystyka niezgodności wg operatora
- Lista zdarzeń lokalizacyjnych dla numeru
- Lista nieprzetworzonych zdarzeń dla numeru
- Zmiany danych wsadowych dla numeru
- Zapytania o lokalizację dla numeru
- Raport spraw
- Raport bieżących spraw
- Raport otrzymanych paczek NP.
- Raport wysłanych paczek NP.

Stacje robocze PLICBD
Obsługa PLI CBD wyposażona jest w stacje robocze Lenovo M0843-RY5. Zamawiający dysponuje 28 zestawami komputerowymi w obu lokalizacjach.

Konfiguracja sprzętowa
Microsoft Windows XP Professional 5.1.2600 Dodatek Service Pack 3 Kompilacja 2600 architektura x86
procesor Intel 2 Quad Q9500 2,8 GHz
3 GB RAM (max. 128GB)
Napęd CD-RW/DVD (combo)
Obudowa "Desktop"
Karta graficzna Intel G41 Express 512 MB
1 dysk 300 GB 2.5"
1x Ethernet 10/100/1000
6x USB

Storage

W każdej z lokalizacji PLI CBD utworzona jest sieć SAN. W jej skład wchodzą macierze dyskowe IBM N6070 oraz biblioteki taśmowe IBM TS 3200. Komunikacja w ramach sieci SAN oparta jest na technologii Fibre Channel (FC).
Każda z bibliotek taśmowych TS 3200 wyposażona jest w dwa napędy taśm Linear Tape-Open™ (LTO) IBM TotalStorage® Ultrium 4z interfejsami Fibre Channel 4 Gb/s.
Tworzenie kopii zapasowych w środowisku PLICBD realizowane jest w oparciu o oprogramowanie Symantec Backup Exec 12.5
Wykaz urządzeń
CPD Siemianowice

L.p.	Urządzenie	Oprogramowanie	Wersja
1	Macierz dyskowa N6070	IBM Data ONTAP	7.3.5P1
2	Biblioteka taśmowa IBM TS 3200	TS 3200 Firmware	9.2 / 3.00e
3	Biblioteka taśmowa IBM TS 3200	TS 3200 Firmware	9.2 / 3.00e

CPD Borucza

L.p.	Urządzenie	Oprogramowanie	Wersja
1	Macierz dyskowa N6070	IBM Data ONTAP	7.3.5P1
2	Biblioteka taśmowa IBM TS 3200	TS 3200 Firmware	9.2 / 3.00e
3	Biblioteka taśmowa IBM TS 3200	TS 3200 Firmware	9.2 / 3.00e

Komponenty macierzy N6070
W każdym CPD PLI CBD macierze dyskowe N6070 wyposażone są w następujące komponenty sprzętowe oraz licencje:
Komponenty N6070

Numer producenta	Nazwa elementu	Liczba sztuk (w każdej macierzy)
	IBM System Storage N6070 Model A21	
2858-A21	IBM System Storage N6070 Model A21	1
1033	SnapMirror over FC HBA PCIe	2
1035	4-Port 4-Gbps FC HBA Tape/Disk	4
6057	SnapMirror	1

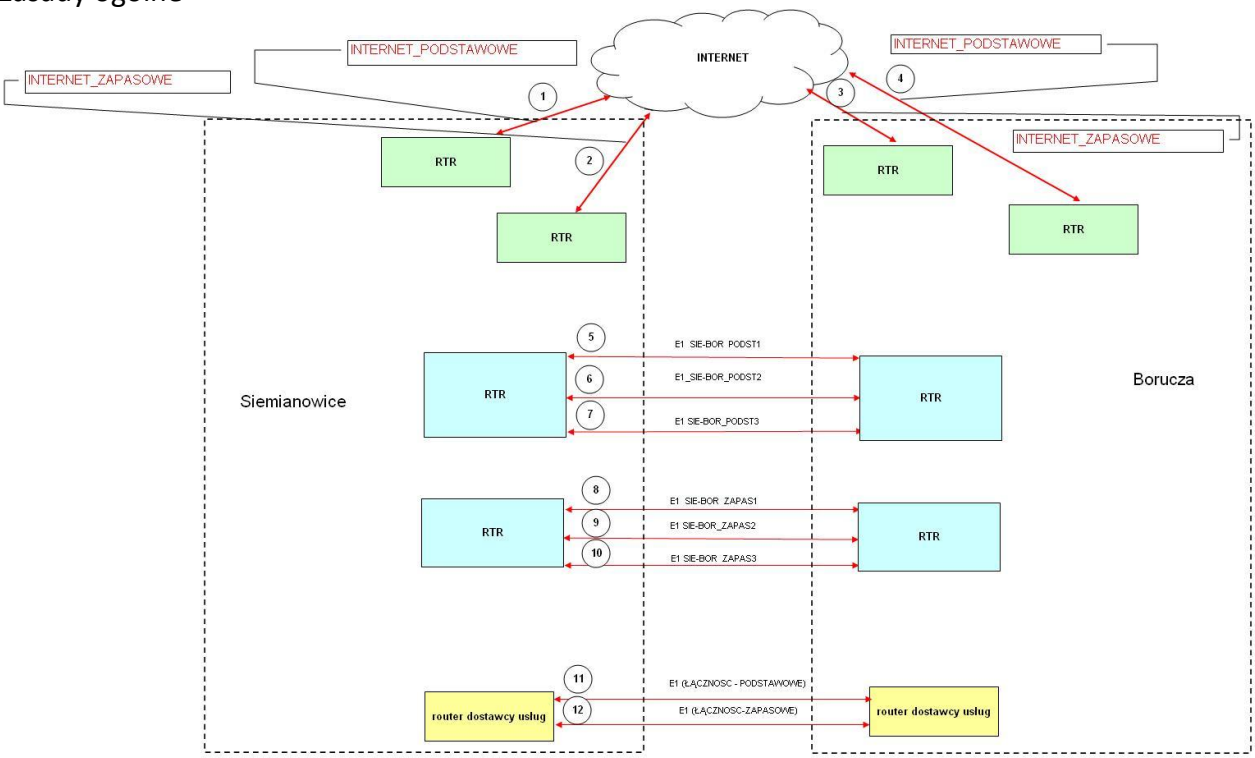
6066	SyncMirror	1
6072	NearStore	1
6074	SAN Bundle	1
6075	iSCSI Protocol	1
6082	Adv. Single Instance Storage	1
6201	Data ONTAP	1
8255	DFM Server License	1
8258	Operations Mgr Media Kit	1
8265	Ops Mgr Core tier 5 license	2
9001	Power Cord, Cont. Europe	1
9202	Field install rack mount kit	1
9552	DFM 3.7+ Identifier	1
9557	Num. of FC Target Ports	2
9558	Num. of FC Storage Loops	2
9560	Dual-path FC Cabling	1
	IBM System Storage EXN4000 Expansion	
2863-004	IBM System Storage EXN4000 Expansion	2
2011	4-Gbps SFP GBIC	4
2044	5.0 m FC Optical Cable	4
4006	300 GB, 15K RPM FC HDD	28
9001	Power Cord, Cont. Europe	2
9202	Field install rack mount kit	2
	IBM System Storage EXN4000 Expansion	
2863-004	IBM System Storage EXN4000 Expansion	2
2011	4-Gbps SFP GBIC	4
2042	1.0 m FC Optical Cable	2
4006	300 GB, 15K RPM FC HDD	28
9001	Power Cord, Cont. Europe	2
9202	Field install rack mount kit	2
	IBM System Storage N6070 Licensed Functions 584	
2870-584	IBM System Storage N6070 Licensed Functions 584	1
6057	SnapMirror	1
6066	SyncMirror	1
6072	NearStore	1
6074	SAN Bundle	1
6075	iSCSI Protocol	1
6082	Adv. Single Instance Storage	1
6201	Data ONTAP	1
8255	DFM Server License	1
8258	Operations Mgr Media Kit	1
8265	Ops Mgr Core tier 5 license	2
9552	DFM 3.7+ Identifier	1

Infrastruktura sieciowa

Architektura sieciowa w obu CPD oparta jest o urządzenia klasy Enterprise firm Juniper, CheckPoint, Cisco. W warstwie sieciowej wykorzystywana jest technologia Ipv4.
Topologia sieci
Topologia sieci odpowiada strukturze Systemu PLI CBD oraz wynikającego z niej przepływu danych.

Węzły sieci
Węzły sieci znajdują się w następujących lokalizacjach:
- CPD PLI CBD w Boruczy, gm. Strachówka,
- CPD PLI CBD w Siemianowicach Śląskich.
Urządzenia sieciowe na potrzeby łączności między administratorami
Na potrzeby łączności VoIP między administratorami w każdym CPD znajduje się router. (schemat topologii łącz – Rys 1)

Zasady ogólne



Rys 1. Topologia łącza WAN PLI CDB

Lokalizacje PLI CBD – na potrzeby komunikacji między Systemami PLI CBD obie lokalizacje połączone są wydzielonymi łączami telekomunikacyjnymi E1 z wykorzystaniem techniki VPN.
Łącza te są pogrupowane w dwóch grupach po trzy łącza E1, z których żadna z nich, w żadnym punkcie trasy nie może mieć punktu wspólnego zarówno w zakresie kanalizacji kablowej, jak i medium transmisyjnego oraz innych warstw.
Dodatkowo, lokalizacje PLI CBD – na potrzeby administrowania Systemami PLI CBD oraz łączności VoIP – połączone są łączami telekomunikacyjnymi E1 (podstawowym oraz

zapasowym – zestawienie łącz oraz ich przepływności wyszczególnione zostały w poniższej Tabeli 1. Koszty związane z eksploatacją łącz ponosi Zamawiający. Reżim SLA dla każdego z łącz przewiduje maksymalnie 8h 45minut niedostępności każdego w skali roku).

Tabela 1 – Zestawienie łącz.

L.p.	Łącze	Stan obecny (przepływność)	Nowa umowa (przepływność)	Zmiana przepływności od dnia 1.03.2014
1	Internetowe 1 (podstawowe Siemianowice)	8Mbps	24Mbps	24Mbps
2	Internet 2 (zapasowe Siemianowice)	8Mbps	24Mbps	24Mbps
3	Internetowe 1 (podstawowe Borucza)	8Mbps	24Mbps	24Mbps
4	Internetowe 2 (zapasowe Borucza)	8Mbps	24Mbps	24Mbps
5	Siemianowice - Borucza podstawowe 1	2Mbps(E1)	2Mbps(E1)	4Mbps (Ethernet)
6	Siemianowice - Borucza podstawowe 2	2Mbps(E1)	2Mbps(E1)	4Mbps (Ethernet)
7	Siemianowice - Borucza podstawowe 3	2Mbps(E1)	2Mbps(E1)	4Mbps (Ethernet)
8	Siemianowice - Borucza zapasowe 1	2Mbps(E1)	2Mbps(E1)	4Mbps (Ethernet)
9	Siemianowice - Borucza zapasowe 2	2Mbps(E1)	2Mbps(E1)	4Mbps (Ethernet)
10	Siemianowice - Borucza zapasowe 3	2Mbps(E1)	2Mbps(E1)	4Mbps (Ethernet)
11	Siemianowice-Borucza administracyjne 1	2Mbps(E1)	2Mbps(E1)	Bez zmian
12	Siemianowice-Borucza administracyjne 2	2Mbps(E1)	2Mbps(E1)	Bez zmian

Obydwie lokalizacje PLI CBD na potrzeby dostępu do Systemu PLI CBD w obu lokalizacjach są podłączone do sieci Internet z wykorzystaniem łączy symetrycznych o przepływności 24 Mbps.
Zakończenia łączy E1 to modemy ze stykiem typu „serial” (wejście WAN ze standardu G.703 przekonwertowane na standard V.35).

Każda lokalizacja podłączona jest do sieci Internet, łączem podstawowym oraz łączem zapasowym.
Łącza do sieci Internet w warstwie pierwszej oraz drugiej są w standardzie Ethernet.
Służba ustawowo powołana do niesienia pomocy, inna niż wymieniona w art. 78 ust. 4 pkt 1 ustawy Pt, pozyskuje informacje, łącząc się z PLI CBD za pośrednictwem sieci Internet z wykorzystaniem techniki VPN.
Obydwa rodzaje połączeń (między lokalizacjami PLI CBD oraz podłączenia lokalizacji do Internetu) są fizycznie oddzielone.
Na potrzeby funkcjonowania Systemu PLI CBD – są zbudowane: 6 (sześć) łączy E1 między lokalizacjami PLI CBD. Od marca 2014 roku łącza E1 będą zastąpione łączami Ethernetowymi o zwiększonej przepustowości podanej w Tabeli 1
Na potrzeby administrowania Systemem PLI CBD – są zbudowane: 2 (dwa) łącza typu E1 między lokalizacjami PLI CBD (podstawowe i zapasowe).
Parametry jakościowe dla kanałów cyfrowych E1 – definiują zalecenia ITU-T, w szczególności G826 i M2100
Wykaz urządzeń

Wykaz sprzętu sieciowego:

CPD PLICBD Siemianowice Śląskie

L.p.	Urządzenie	Oprogramowanie	Wersja
1	Router Juniper j6350	Junos	10.4R2.7
2	Router Juniper j6350	Junos	10.4R2.7
3	Router Juniper j6350	Junos	10.4R2.7
4	Router Juniper j6350	Junos	11.4R2.14
5	Router Juniper j6350	Junos	10.4R2.7
6	Router Juniper j6350	Junos	10.4R2.7
7	Switch Juniper EX3200-24t	Junos	10.3R2.11
8	Switch Juniper EX3200-24t	Junos	10.3R2.11
9	Switch Juniper EX4200-48t	Junos	10.1R1.8
10	Switch Juniper EX4200-48t	Junos	10.1R1.8
11	Switch Juniper EX4200-48t	Junos	10.1R1.8
12	Switch Juniper EX4200-48t	Junos	10.1R1.8
13	Switch Juniper EX4200-48t	Junos	10.1R1.8
14	F5 BIG-IP Load balancer 6900	BIG-IP	10.2.0 (Build 1755.1)
15	F5 BIG-IP Load balancer 6900	BIG-IP	10.2.0 (Build 1755.1)
16	Firewall/VPN Juniper NetScreen ISG 1000	ScreenOS	Hardware version: 3010 (0)-(04) Software version:6.3.0r6.0
17	Firewall/VPN Juniper NetScreen ISG 1000	ScreenOS	Hardware version: 3010 (0)-(04) Software version:6.3.0r6.0
18	Juniper NSM Network and Security Manager	Linux	Web 2010.3 JDK Version 16.3-b01 Linux: 2.6.9-55.0.2.ELsmp
19	Juniper NSM Network and Security Manager	Linux	Web 2010.3 JDK Version 16.3-b01

			Linux: 2.6.9-55.0.2.ELsmp
20	Klaster Firewall Check Point UTM-1 1073	UTM-1 NGX	R70.1
21	Klaster Firewall Check Point UTM-1 1073	UTM-1 NGX	R70.1
22	Router Cisco	IOS C2901-Uniwersal K9-M	Ver 15.1(2)T2
23	Router Cisco	IOS C2901 - Uniwersal K9-M	Ver 15.1(2)T2
24	Spectracom Netclock 9389		NTP Rev 4.2.0@1.1161-r
25	Spectracom Netclock 9389		NTP Rev 4.2.0@1.1161-r
26	Switch FC Cisco (MDS 9124)	Cisco Nexus Operating System (NX-OS)	ver. 5.0(7) BIOS ver (1.0.19)
27	Switch FC Cisco (MDS 9124)	Cisco Nexus Operating System (NX-OS)	ver. 5.0(7) BIOS ver (1.0.19)
28	Juniper IC-4500 (NAC Network Admission Control)	NAC	4.1R2 (build 17391)
29	Juniper IC-4500 (NAC Network Admission Control)	NAC	4.1R2 (build 17391)

Wykaz sprzętu sieciowego:
CPD PLI CBD Borucza

L.p.	Urządzenie	Oprogramowanie	Wersja
1	Router Juniper j6350	Junos	10.4R2.7
2	Router Juniper j6350	Junos	10.4R2.7
3	Router Juniper j6350	Junos	10.4R2.7
4	Router Juniper j6350	Junos	11.4R2.7
5	Router Juniper j6350	Junos	10.4R2.7
6	Router Juniper j6350	Junos	10.4R2.7
7	Switch Juniper EX3200-24t	Junos	10.3R2.11
8	Switch Juniper EX3200-24t	Junos	10.3R2.11
9	Switch Juniper EX4200-48t	Junos	10.1R1.8
10	Switch Juniper EX4200-48t	Junos	10.1R1.8
11	Switch Juniper EX4200-48t	Junos	10.1R1.8
12	Switch Juniper EX4200-48t	Junos	10.1R1.8
13	Switch Juniper EX4200-48t	Junos	10.1R1.8
14	F5 BIG-IP Load balancer 6900	BIG-IP	10.2.0 (Build 1755.1)
15	F5 BIG-IP Load balancer 6900	BIG-IP	10.2.0 (Build 1755.1)
16	Firewall/VPN Juniper NetScreen ISG 1000	ScreenOS	Hardware version: 3010 (0)-(04) Software version:6.3.0r6.0
17	Firewall/VPN Juniper NetScreen ISG 1000	ScreenOS	Hardware version: 3010 (0)-(04)

			Software version:6.3.0r6.0
18	Juniper NSM Network and Security Manager	Linux	Web 2010.3 JDK Version 16.3-b01 Linux: 2.6.9-55.0.2.ELsmp
19	Juniper NSM Network and Security Manager	Linux	Web 2010.3 JDK Version 16.3-b01 Linux: 2.6.9-55.0.2.ELsmp
20	Klaster Firewall Check Point UTM-1 1073	UTM-1 NGX	R70.1
21	Klaster Firewall Check Point UTM-1 1073	UTM-1 NGX	R70.1
22	Router Cisco	IOS C2901-Uniwersal K9-M	Ver 15.1(2)T2
23	Router Cisco	IOS C2901 - Uniwersal K9-M	Ver 15.1(2)T2
24	Spectracom Netclock 9389		NTP Rev 4.2.0@1.1161-r
25	Spectracom Netclock 9389		NTP Rev 4.2.0@1.1161-r
26	Switch FC Cisco (MDS 9124)	Cisco Nexus Operating System (NX-OS)	ver. 5.0(7) BIOS ver (1.0.19)
27	Switch FC Cisco (MDS 9124)	Cisco Nexus Operating System (NX-OS)	ver. 5.0(7) BIOS ver (1.0.19)
28	Juniper IC-4500 (NAC Network Admission Control)	NAC	4.1R2 (build 17391)
29	Juniper IC-4500 (NAC Network Admission Control)	NAC	4.1R2 (build 17391)
30	Amptrac Analyzer	iTRACS	

Systemy kolekcji logów i ochrony baz danych.

W ramach środowiska PLI CBD wdrożone zostały systemy klasy SIEM oraz ochrony baz danych. W każdym z CPD zainstalowane są po dwa urządzenia do zarządzania i archiwizacji logów oraz monitorowania ruchu bazodanowego.

Wykaz urządzeń CPD Siemianowice

L.p.	Urządzenie	Oprogramowanie	Wersja
1	RSA Envision	SIEM	4.0
2	RSA Envision	SIEM	4.0
3	Guardium G2000	IBM InfoSphere Guardium	Version 8.2
4	Guardium G2000	IBM InfoSphere Guardium	Version 8.2

Wykaz urządzeń CPD Borucza

L.p.	Urządzenie	Oprogramowanie	Wersja
1	RSA Envision ES Series	SIEM	4.0
2	RSA Envision ES Series	SIEM	4.0

3	Guardium G2000	IBM InfoSphere Guardium	Version 8.2
4	Guardium G2000	IBM InfoSphere Guardium	Version 8.2

Szczegółowe informacje dotyczące zakresu rozbudowy Systemu PLI CBD można znaleźć na stronie internetowej Zamawiającego pod adresem:
http://www.uke.gov.pl/ogloszenie-o-zamowieniu-sprawa-nr-bak-wzp-231-6213-13073