OPIS ZAŁOŻEŃ PROJEKTU INFORMATYCZNEGO

Tytuł projektu	Wspólna Infrastruktura Informatyczna Państwa		
Wnioskodawca	Minister Cyfryzacji		
Beneficjent	Kancelaria Prezesa Rady Ministrów		
Partnerzy	Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy		
Źródło finansowania	Program Operacyjny Polska Cyfrowa, Działanie 2.1 Wysoka dostępność i jakość e-usług publicznych (tryb pozakonkursowy, typ II projektu) Cz. 27 Informatyzacja - budżetu państwa.		
Całkowity koszt projektu	159 666 380,17 zł		
Planowany okres realizacji projektu	04-2020 do 03-2023		
Osoba kontaktowa	Joanna Baranowska	joanna.baranowska@mc.gov.pl	222455521

1. POWODY PODJĘCIA PROJEKTU

1.1. Identyfikacja problemu i potrzeb

Konieczność realizacji projektu WIIP, wynika z pilnej potrzeby podniesienia bezpieczeństwa przetwarzania danych w administracji rządowej oraz optymalizacji kosztów utrzymania infrastruktury IT. Obecnie większość urzędów zapewnia bezpieczeństwo i infrastrukturę przetwarzania we własnym zakresie. Takie podejście jest nieefektywne i przekłada się wprost na szereg problemów, w tym m.in.: brak planów awaryjnych, ochrony fizycznej, niedostatki kompetencji i infrastruktury cyberbezpieczeństwa; wysokie koszty przetwarzania danych; długi czas pozyskania infrastruktury IT; brak optymalizacji zarządzania infrastrukturą IT (przeskalowanie, niedopasowanie do potrzeb); źle zarządzane rezerwy mocy obliczeniowej, itd. Realizacja projektu w proponowanym kształcie doprowadzi do odwrócenia powyższych trendów poprzez stworzenie wspólnej, bezpiecznej infrastruktury IT, która: - poprawi bezpieczeństwo przetwarzania danych i świadczenia e-usług;
- trwale obniży koszty stałe przetwarzania;
- podniesie efektywność wydatkowania środków w projektach IT;
- skróci czas realizacji nowych przedsięwzięć IT;
- pozwoli na wdrożenie usług świadczonych w modelu chmury obliczeniowej na potrzeby rozwoju systemów informatycznych i kluczowych rejestrów o znaczeniu krytycznym (z ang. mission critical) dla funkcjonowania państwa;
- upowszechni model chmury obliczeniowej jako główny sposób realizacji systemów informatycznych państwa (zmiana technologii wytwarzania oprogramowania);
- poprawi bezpieczeństwo przetwarzania danych i świadczenia e-usług;
- zoptymalizuje procesy zarządzania infrastrukturą IT (przeskalowanie, niedopasowanie do potrzeb).

Interesariusz	Zidentyfikowany problem	Szacowana wielkość grupy
Jednostki	Jednostki administracji rządowej realizujące	Administracja

Interesariusz	Zidentyfikowany problem	Szacowana wielkość grupy
administracji rządowej realizujące projekty wymagające rozwoju infrastruktury IT	projekty POPC, modernizujące infrastrukturę zakupioną w ramach POIG 2007-2013 lub planujące/dokonujące modernizacji ze środków krajowych, w szerszej perspektywie doświadczają podobnych problemów, do których zaliczyć można: - rozproszenie infrastruktury, ograniczenia skalowalności infrastruktury, długi czas wdrażania nowych systemów, generujące wysokie koszty utrzymania, - niewystarczający poziom bezpieczeństwa infrastruktury oraz systemów transmisji i przetwarzania danych, - niedostatki kadrowe, fluktuacja kadr i braki kompetencyjne ograniczające efektywność modernizacji.	rządowa centralna, obejmująca też niezespoloną administrację rządową w województwie – 95. Zespolona administracja rządowa w województwie – 16 urzędów wojewódzkich wraz z podmiotami podległymi.
Jednostki administracji samorządowej	Jednostki administracji samorządowej nie mają dostępu do dedykowanych narzędzi wspierających proces zamawiania usług IT oraz realizacji postępowań przetargowych w tym zakresie.	2 807 jednostek (gminy, powiaty, województwa)
Przedsiębiorcy działający w sektorze usług IT	Głównym problemem tej grupy jest niski poziom adopcji rozwiązań chmury obliczeniowej w administracji publicznej oraz brak standaryzowanego procesu zamówień publicznych na usługi IT.	76 302 podmioty działające na terenie Polski oraz ponad 400 tys. podmiotów na terenie UE.

1.2. Opis stanu obecnego

Obecnie podmioty administracji rządowej nie mają możliwości technicznych i organizacyjnych do współdzielenia zasobów informatycznych. Diagnoza oparta na danych Systemu Inwentaryzacji Systemów Informatycznych (SIST), wykazała szereg problemów w zakresie wykorzystania infrastruktury IT.
Centra przetwarzania danych polskiej adm. rządowej są rozproszone w kilkuset lokalizacjach o bardzo zróżnicowanym rozmiarze i jakości. Analiza potrzeb wskazuje na konieczność uruchomienia kilku dobrej jakości ośrodków rozmieszczonych na obszarze kraju, z bezpieczną siecią i racjonalnie zarządzanymi usługami. Rozwój techniki – gwałtowny wzrost możliwej do uzyskania gęstości mocy obliczeniowej – spowodował znaczny spadek zapotrzebowania na powierzchnię serwerowni. Administracja dziś dysponuje przestrzeniami serwerowni zaspokajającymi rzeczywiste potrzeby z dużą rezerwą. Obecny stan IT charakteryzują:
- zagrożenia bezpieczeństwa,
- wysoki koszt łączny, przy czym ponad połowa to koszt nieruchomości i utrzymania,
- długie czasy pozyskania infrastruktury IT,
- niedopasowane do potrzeb inwestycje w infrastrukturę,
- rozproszone i źle zarządzane rezerwy mocy i przestrzeni dyskowych,
- brak koordynacji inwestycji,

Analizy pokazują, że typowa infrastruktura IT małego urzędu:
- to niewielka liczba serwerów i macierzy dyskowych o niskim poziomie zabezpieczeń, - brak serwerowni zapasowej,

- rosnące koszty utrzymania łącza internetowego, ochrony sieciowej, sys. zarządzania i utrzymania.

Analogicznie w projektach IT finansowanych z UE zakupiono infrastrukturę IT o zbyt wysokich parametrach, która w momencie uruchomienia proj. była najczęściej przestarzała technologicznie.

Szacunkowe koszty jedn. przetwarzania danych w rozproszonych serwerowniach są 10-krotnie wyższe niż w Rządowej Chmurze Obliczeniowej.

2. EFEKTY PROJEKTU

2.1. Cele i korzysci wynikające z projektu

Cel - 1	Zapewnienie bezpieczeństwa danych przetwarzanych w systemach teleinformatycznych podmiotów administracji publicznej oraz optymalizacji kosztów utrzymania tych systemów
Cel strategiczny	- Strategia Sprawne i Nowoczesne Państwo 2030 – Cel III. Podniesienie sprawności realizacji zadań państwa poprzez wykorzystanie technologii cyfrowych i zmianę sposobu działania stosownie do możliwości, jakie stwarza technologia — kierunek interwencji 1: Tworzenie warunków dla efektywnej, dostępnej cyfrowo i bezpiecznej e-administracji - Strategia sprawne Państwo 2020 – cel Zwiększenie skuteczności i efektywności państwa otwartego na współpracę z obywatelami" — „Efektywne świadczenie usług publicznych", „5.5. Standaryzacja i zarządzanie usługami publicznymi ze szczególnym uwzględnieniem technologii cyfrowych". - Program Zintegrowanej Informatyzacji Państwa – Cel główny: Modernizacja administracji publicznej z wykorzystaniem technologii cyfrowych nakierowana na potrzebę podniesienia sprawności państwa i poprawienie jakości relacji administracji z obywatelami i innymi interesariuszami – Cel szczegółowy: Wzmocnienie dojrzałości organizacyjnej jednostek administracji publicznej oraz usprawnienie zaplecza elektronicznej administracji (back office). - Program Operacyjny Polska Cyfrowa – cel szczegółowy: wysoka dostępność i jakość e-usług w zakresie zapewnienia warunków do świadczenia usług elektronicznych przez administrację centralną - SzOOP Programu Polska Cyfrowa – cel: zapewnienie bezpiecznych systemów informatycznych oraz warunków do poprawy ich interoperacyjności.
Korzyść:	- zapewnienie bezpiecznych kanałów komunikacji elektronicznej na potrzeby budowy i eksploatacji rozwiązań dedykowanych administracji rządowej, opartych na technologii chmury obliczeniowej, - podstawa do dalszego rozwoju usług elektronicznych dla administracji rządowej, - wdrożenie Rządowego Klastra Bezpieczeństwa (RKB) usprawni przygotowanie i realizację wszystkich projektów IT obejmujących przetwarzanie danych systemów informatycznych i kluczowych rejestrów o znaczeniu krytycznym dla funkcjonowania państwa oraz będzie stanowić jeden z elementów zapewnienia ich interoperacyjności, - poprawa bezpieczeństwa przetwarzania danych i świadczenia usług elektronicznych w administracji rządowej, - podniesienie efektywności wydatkowania środków w projektach
KPI:	1) Liczba ośrodków CPD, objętych standardem technicznym i organizacyjnym w ramach Rządowego Klastra Bezpieczeństwa

	2) Liczba centrów operacji bezpieczeństwa i zarządzania siecią (SOC/NOC), które osiągnęły pełną gotowość operacyjną 3) Liczba opracowanych standardów bezpieczeństwa w zakresie CPD oraz usług świadczonych w ramach RChO
Wartość aktualna i docelowa KPI:	1) Wartość aktualna – 0 szt. (2020 r.) 2) Wartość aktualna – 0 szt. (2020 r.) 3) Wartość aktualna – 0 szt. (2020 r.) 1) Wartość docelowa (2023 r.) – 2 szt. 2) Wartość docelowa (2023 r.) – 1 szt. 3) Wartość docelowa (2023 r.) – 1 szt.
Metoda pomiaru KPI	1) Wskaźnik będzie monitorowany cyklicznie na podstawie analizy dokumentacji zastanej: raportów audytu wewnętrznego (certyfikacja wewnętrzna), raportów administratora sieci. Wartość wskaźnika będzie monitorowana z częstotliwością min. raz do roku. Za monitoring wskaźnika odpowiedzialny będzie Departament Rozwoju Usług KPRM, przy współpracy z dedykowanym zespołem obsługi COI. 2) Wskaźnik będzie monitorowany na podstawie analizy dokumentacji zastanej: raportów wewnętrznych. Wartość wskaźnika będzie monitorowana z częstotliwością min. raz do roku. Za monitoring wskaźnika odpowiedzialny będzie Departament Rozwoju Usług KPRM, przy współpracy z dedykowanym zespołem obsługi COI. 3) Wskaźnik będzie monitorowany na podstawie analizy dokumentacji zastanej: raportów wewnętrznych. Wartość wskaźnika będzie monitorowana z częstotliwością min. raz do roku. Za monitoring wskaźnika odpowiedzialny będzie Departament Rozwoju Usług KRPM, przy współpracy z dedykowanym zespołem NASK-PIB.
Cel - 2	Wprowadzenie jednolitych, wysokich standardów ochrony systemów informatycznych, a także wspieranie podmiotów administracji publicznej w utrzymaniu tych systemów oraz uzyskiwaniu usług niezbędnych do ich budowy
Cel strategiczny	- Strategia Sprawne i Nowoczesne Państwo 2030 – Cel III. Podniesienie sprawności realizacji zadań państwa poprzez wykorzystanie technologii cyfrowych i zmianę sposobu działania stosownie do możliwości, jakie stwarza technologia — kierunek interwencji 1: Tworzenie warunków dla efektywnej, dostępnej cyfrowo i bezpiecznej e-administracji - Strategia sprawne Państwo 2020 – cel Zwiększenie skuteczności i efektywności państwa otwartego na współpracę z obywatelami" — „Efektywne świadczenie usług publicznych", „5.5. Standaryzacja i zarządzanie usługami publicznymi ze szczególnym uwzględnieniem technologii cyfrowych". - Program Zintegrowanej Informatyzacji Państwa – Cel główny: Modernizacja administracji publicznej z wykorzystaniem technologii cyfrowych nakierowana na potrzebę podniesienia sprawności państwa i poprawienie jakości relacji administracji z obywatelami i innymi interesariuszami – Cel szczegółowy: Wzmocnienie dojrzałości organizacyjnej jednostek administracji publicznej oraz usprawnienie zaplecza elektronicznej administracji (back office).
Korzyść:	- zapewnienie bezpiecznych kanałów komunikacji elektronicznej na potrzeby budowy i eksploatacji rozwiązań dedykowanych administracji rządowej, wykorzystujących technologię chmury obliczeniowej. - podstawa do dalszego rozwoju usług elektronicznych dla administracji rządowej - wdrożenie standardu RKB usprawni przygotowanie i realizację wszystkich projektów IT obejmujących przetwarzanie danych rejestrów państwowych

	oraz będzie stanowić jeden z elementów zapewnienia ich interoperacyjności, - poprawa efektywności wydatkowania środków w projektach zawierających element infrastruktury obliczeniowej IT, - skrócenie czasu realizacji nowych przedsięwzięć informatycznych przez szybsze udostępnianie wymaganej infrastruktury obliczeniowej - ograniczenie redundancji (wielokrotnego gromadzenia tych samych danych) dzięki zniesieniu części barier technicznych dla interoperacyjności.
KPI:	1) Przestrzeń dyskowa serwerowni 2) Liczba wdrożonych platform wirtualizacyjnych 3) Średni poziom dostępności świadczonych usług (SLA) 4) Ilość dostępnych rdzeni fizycznych procesorów
Wartość aktualna i docelowa KPI:	1) Wartość aktualna: 100 TB (2020 r.) 2) Wartość aktualna: 1 szt. (2020 r.) 3) Wartość aktualna: 0,00% (2020 r.) 4) Wartość aktualna: 600 szt. (2020 r.) 1) Wartość docelowa: 3 416 TB (2023 r.) 2) Wartość docelowa: 4 szt. (2023 r.) 3) Wartość docelowa: 98,75% (2023 r.) 4) Wartość docelowa: 3 800 szt. (2023 r.)
Metoda pomiaru KPI	1) Wskaźnik będzie mierzony cyklicznie min. raz do roku na podstawie raportu zainstalowanej pojemności przestrzeni dyskowej na poziomie orkiestratora zasobów infrastrukturalnych połączonych CPD. Za monitoring wskaźnika będzie odpowiedziany zespół administratorów RChO (COI). 2) Wskaźnik będzie mierzony cyklicznie min. raz do roku na podstawie raportu udostępnionych platform wirtualizacyjnych. Za monitoring wskaźnika będzie odpowiedziany zespół administratorów RChO (COI). 3) Wskaźnik będzie mierzony cyklicznie min. raz do roku na podstawie raportu dostępności usługi (poziomu SLA). Za monitoring wskaźnika będzie odpowiedziany zespół administratorów RChO (COI). 4) Wskaźnik będzie mierzony cyklicznie min. raz do roku na podstawie raportu dostępnej ilości rdzeni fizycznych procesorów dostępnych w RChO. Za monitoring wskaźnika będzie odpowiedziany zespół administratorów RChO (COI).
Cel - 3	Zapewnienie wysokiego poziomu usług świadczonych społeczeństwu przez administrację publiczną
Cel strategiczny	- Strategia Sprawne i Nowoczesne Państwo 2030 – Cel III. Podniesienie sprawności realizacji zadań państwa poprzez wykorzystanie technologii cyfrowych i zmianę sposobu działania stosownie do możliwości, jakie stwarza technologia — kierunek interwencji 1: Tworzenie warunków dla efektywnej, dostępnej cyfrowo i bezpiecznej e-administracji - Strategia sprawne Państwo 2020 – cel Zwiększenie skuteczności i efektywności państwa otwartego na współpracę z obywatelami" — „Efektywne świadczenie usług publicznych", „5.5. Standaryzacja i zarządzanie usługami publicznymi ze szczególnym uwzględnieniem technologii cyfrowych". - Program Zintegrowanej Informatyzacji Państwa – Cel główny: Modernizacja administracji publicznej z wykorzystaniem technologii cyfrowych nakierowana na potrzebę podniesienia sprawności państwa i poprawienie jakości relacji administracji z obywatelami i innymi interesariuszami – Cel szczegółowy: Wzmocnienie dojrzałości organizacyjnej jednostek administracji publicznej oraz usprawnienie zaplecza elektronicznej administracji (back office). - Program Operacyjny Polska Cyfrowa – cel szczegółowy: wysoka dostępność

	i jakość e-usług w zakresie zapewnienia warunków do świadczenia usług elektronicznych przez administrację centralną - SzOOP Programu Polska Cyfrowa – cel: zapewnienie bezpiecznych systemów informatycznych oraz warunków do poprawy ich interoperacyjności.
Korzyść:	- wdrożenie dedykowanego katalogu usług adresowanego do administracji rządowej pozwoli na wygenerowanie szeregu korzyści zarówno dla użytkowników końcowych (pracowników administracji rządowej - bezpośredni, pozytywny wpływ na efektywność finansową zadań publicznych finansowanych z budżetu państwa, w obszarze wykorzystania narzędzi IT.
KPI:	1) Liczba udostępnionych usług wewnątrzadministracyjnych (A2A) 2) Liczba uruchomionych systemów teleinformatycznych w podmiotach wykonujących zadania publiczne
Wartość aktualna i docelowa KPI:	1) Wartość aktualna: 0 szt. (2020 r.) 2) Wartość aktualna: 0 szt. (2020 r.) 1) Wartość docelowa: 5 szt. (2023 r.) 2) Wartość docelowa: 1 szt. (2023 r.)
Metoda pomiaru KPI	1) Wskaźnik będzie monitorowany na podstawie automatycznie generowanych raportów wykorzystania usług elektronicznych. Wskaźnik będzie monitorowany w sposób ciągły (raport zbiorczy min. raz do roku). Za monitoring wskaźnika będzie odpowiedziany zespół administratorów RChO (COI). 2) Wskaźnik będzie monitorowany na podstawie automatycznie generowanych raportów wykorzystania usług elektronicznych. Wskaźnik będzie monitorowany w sposób ciągły (raport zbiorczy min. raz do roku). Za monitoring wskaźnika będzie odpowiedziany zespół administratorów RChO (COI).

2.2. Udostępnione e-usługi

Lp.	Nazwa e-usługi	Typ	Zakres oddziaływania	Poziom dojrzałosci e-usługi
1	Zamówienie usługi IT świadczonej w modelu chmury obliczeniowej z wykorzystaniem systemu ZUCH	A2A	Podmioty administracji rządowej realizujące projekty wymagające rozwoju infrastruktury IT Jednostki administracji samorządowej Przedsiębiorcy działający w sektorze usług IT (rocznie ok 150 transakcji)	Nie dotyczy
2	Dostawa usług w zakresie infrastruktury IT (IaaS) oraz platform systemowych	A2A	Podmioty administracji rządowej realizujące projekty wymagające rozwoju infrastruktury IT (rocznie ok 150	Nie dotyczy

Lp.	Nazwa e-usługi	Typ	Zakres oddziaływania	Poziom dojrzałosci e-usługi
			transakcji)	
3	Dostarczanie oprogramowania i usług w modelu chmury obliczeniowej (PaaS/ SaaS)	A2A	Podmioty administracji rządowej realizujące projekty wymagające rozwoju infrastruktury IT (rocznie ok 150 transakcji)	Nie dotyczy
4	System raportowania i rozliczeń udostępnianych usług	A2A	Podmioty administracji rządowej realizujące projekty wymagające rozwoju infrastruktury IT (rocznie ok 800 transakcji)	Nie dotyczy
5	Wsparcie techniczne (Service desk) – elektroniczna obsługa zgłoszeń	A2A	Podmioty administracji rządowej realizujące projekty wymagające rozwoju infrastruktury IT (rocznie ok 300 transakcji)	Nie dotyczy

2.3. Udostępnione informacje sektora publicznego i zdigitalizowane zasoby

Nie dotyczy

2.4. Produkty końcowe projektu

Nazwa produktu	Planowana data wdrożenia
System Zapewniania Usług Chmurowych - wersja produkcyjna	02-2022
System Zapewniania Usług Chmurowych - model zakupu usług Publicznej Chmury Obliczeniowej (PChO)	03-2022
Rządowy Klaster Bezpieczeństwa - Wyposażenie i oprogramowanie RKB	03-2022
Rządowa Chmura Obliczeniowa - Wyposażenie i oprogramowanie wraz z Katalogiem usług RChO	05-2022
Rządowy Klaster Bezpieczeństwa - Standardy i polityki bezpieczeństwa	08-2022
Rządowy Klaster Bezpieczeństwa - Zasoby organizacyjne - gotowość zespołu obsługi RKB	10-2022
Rządowa Chmura Obliczeniowa - Zasoby organizacyjne - gotowość zespołu obsługi RChO	10-2022
System Zapewniania Usług Chmurowych - Katalog usług chmury publicznej	01-2023

3. KAMIENIE MILOWE

Kamienie milowe	Planowany termin osiągnięcia
Opracowanie standardów bezpieczeństwa chmury obliczeniowej	2020-04-13
Odbiór koncepcji realizacyjnej SOC/NOC	2022-01-14
Wydanie docelowego katalogu chmury publicznej	2022-03-21
Wydanie inicjalnego katalogu usług Rządowej Chmury Obliczeniowej — Uruchomienie katalogu usług IaaS	2022-11-22
Uruchomienie Rządowego Klastra Bezpieczeństwa	2022-11-22
Wydanie katalogu usług PaaS Rządowej Chmury Obliczeniowej – rozbudowa katalogu usług o elementy PaaS	2022-11-22
Wydanie katalogu usług bezpieczeństwa w ramach RKB – uruchomienie usług bezpieczeństwa w modelu chmurowym	2022-11-22
Wydanie inicjalnego katalogu usług chmury publicznej – uruchomienie systemu ZUCH wraz z opublikowaniem 1 katalogu usług Publicznej Chmury Obliczeniowej (PChO)	2023-01-09
Wydanie docelowego katalogu chmury publicznej – uruchomienie co najmniej 1 usługi w modelu SaaS	2023-01-20
Wydanie katalogu usług SaaS Rządowej Chmury Obliczeniowej – uruchomienie co najmniej 1 usługi w modelu SaaS	2023-01-27

4. KOSZTY

4.1. Koszty ogólne projektu wraz ze sposobem finansowania

Całkowity koszt projektu (netto oraz brutto), w tym	Netto 132 446 599,02 zł Brutto 159 666 380,17 zł	
Procent dofinansowania ze środków UE (brutto)	84,63%	
Procent środków z budżetu państwa (brutto)	15,37%	
Podział całkowitego kosztu projektu na poszczególna lata (netto oraz brutto)	2020	Netto 3 102 412,98 zł Brutto 3 597 109,86 zł
	2021	Netto 11 110 718,15 zł Brutto 12 515 853,60 zł
	2022	Netto 116 219 752,56 zł Brutto 141 230 142,55 zł
	2023	Netto 2 013 715,33 zł Brutto 2 323 274,16 zł

4.2. Wykaz poszczególnych pozycji kosztowych

Nazwa pozycji kosztowej		Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
Oprogramowanie	Koszty wytworzenia oprogramowania, koszty stworzenia prototypowych e-usług, prototypów aplikacji, koszty zakupu gotowych rozwiązań programistycznych (licencje, produkty), koszty zakupu licencji oprogramowania standardowego. W tej kategorii kosztów ujęto również koszty UX i grafiki, a także wydatki personelu oraz na usługi związane z wdrożeniem (np. bodyleasingu).	77 072 521,08 zł	Koszty: 1) usług zespołu body leasingu w latach 2020-2023, obejmujące prace koncepcyjne, projektowanie, nadzór nad wykonawcami oraz odbiór produktów związanych z budową Katalogu usług Rządowej Chmury Obliczeniowej, 2) usług głównego wykonawcy in-house COI, dostaw oprogramowania wraz z wdrożeniem na potrzeby Rządowej Chmury Obliczeniowej, 3) Koszty personelu bezpośrednio zaangażowanego w realizację zadań projektu.
Infrastruktura	Koszty zakupu	69 311 470,23 zł	Wyposażenie dwóch ośrodków

Nazwa pozycji kosztowej		Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
	infrastruktury na potrzeby Rządowej Chmury Obliczeniowej oraz Rządowego Klastra Bezpieczeństwa		obliczeniowych stanowiących podstawę działania RChO i RKB.
Koszty UX i grafiki			
Bezpieczeństwo	Koszty wytwarzania i zakupu rozwiązań związanych z zapewnieniem i podnoszeniem bezpieczeństwa danych, aplikacji i systemów	6 747 408,10 zł	Koszty usług głównego wykonawcy in-house w zakresie budowy RKB.
Wydajność rozwiązań			
Szkolenia	Koszty szkolenia zespołu projektowego.	349 704,08 zł	Niezbędne w procesie wdrożenia szkolenia personelu KPRM oraz NASK-PIB.
Działania informacyjno-promocyjne	Koszty wszystkich działań informacyjno-promocyjnych	1 464 930,00 zł	Koszty działań promocyjnych w tym kampanii marketingowej, pozwalające mitygować ryzyko związane z zarządzaniem popytem na produkty projektu.
Koszty zarządzania i wsparcia (w tym wynagrodzenia personelu wspomagającego)	Koszty zespołu wspomagającego realizację projektu, koszty usług wspierających realizację projektu (finansowe, księgowe, prawne).	4 720 346,68 zł	Pozycja obejmuje wynagrodzenia personelu wsparcia projektowego oraz kosztów pośrednich.

4.3. Koszty ogólne utrzymania wraz ze sposobem finansowania (okres 5 lat)

Całkowity koszt utrzymania trwałości projektu (brutto)	116 380 798,01 zł		**Źródło finansowania**
Podział całkowitego kosztu utrzymania trwałości projektu	2023	5 803 141,98 zł (brutto) (4 776 079,04 zł netto)	krajowe środki publiczne - budżet państwa

na poszczególna lata (netto oraz brutto)	2024	8 832 758,69 zł (brutto) (7 239 182,06 zł netto)	krajowe środki publiczne - budżet państwa
	2025	8 897 288,75 zł (brutto) (7 291 645,52 zł netto)	krajowe środki publiczne - budżet państwa
	2026	69 956 673,59 zł (brutto) (56 933 421,81 zł netto)	krajowe środki publiczne - budżet państwa
	2027	22 890 935,00 zł (brutto) (18 668 593,69 zł netto)	krajowe środki publiczne - budżet państwa

4.4. Planowane koszty ogólne realizacji (w przypadku projektu współfinansowanego – wkład krajowy z budżetu państwa) oraz koszty utrzymania projektu:

- zostaną pokryte w ramach budżetów odpowiednich dysponentów części budżetowych bez konieczności występowania o dodatkowe środki z budżetu państwa
~~- będą powodować konieczność przyznania dodatkowych kwot~~

5. GŁÓWNE RYZYKA

5.1. Ryzyka wpływające na realizację projektu

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarzadzania ryzykiem
Opóźnienia przetargów	Duża	Wysokie	Realizacja zadań z wykorzystaniem istniejącej infrastruktury poprzez ograniczenie zakresu do czasu zakończenia procesów zakupowych.
Ograniczenia w dostępności kadry	Duża	Średnie	Zapewnienie wsparcia szkoleniowego oraz odpowiedniego funduszu wynagrodzeń.
Ograniczenia licencyjne	Średnia	Średnie	Zastosowanie dedykowanych licencji (brak współdzielenia). Budżet ryzyka.
Zbyt mały lub zbyt duży popyt na usługi oferowane przez Chmurę Rządową	Duża	Średnie	Podjęcie działań promocyjnych i regulacyjnych (pobudzanie popytu) oraz zapewnienie skalowalności infrastruktury w celu dostosowania do popytu.
Opóźnienia związane z COVID-19	Duża	Średnie	Modyfikacja Harmonogramu prac planowanych w ramach WIIP POPC – adaptacja do zmieniających się

Nazwa ryzyka	Siła oddziaływania	Prawdopo-dobieństwo wystąpienia ryzyka	Sposób zarzadzania ryzykiem
			warunków realizacji projektu.
Przekroczenie zakładanego budżetu na infrastrukturę i oprogramowanie WIIP	Duża	Średnie	Przesunięcie środków w programie POPC lub zapewnienie źródeł finansowania spoza programu.

5.2. Ryzyka wpływające na utrzymanie efektów

Nazwa ryzyka	Siła oddziaływania	Prawdopo-dobieństwo wystąpienia ryzyka	Sposób zarzadzania ryzykiem
Niski popyt na usługi oferowane w wyniku realizacji projektu – brak wykorzystania pełnego potencjału środowiska obliczeniowego i usług chmurowych przez użytkowników końcowych.	Duża	Niskie	Mitygacja. Podjęcie działań promocyjnych i regulacyjnych (pobudzanie popytu).
Ograniczenia limitów finansowych budżetu państwa związanych z utrzymaniem i rozwojem RChO i RKB.	Duża	Średnie	Mitygacja. Uwzględnienie planów wydatków związanych z RChO i RKB w wieloletnim planie finansowym budżetu państwa oraz zastosowanie przesunięć z cz. budżetowych klientów RChO do dedykowanej rezerwy celowej WIIP
Trudności związane z adaptacją nowych rozwiązań organizacyjnych oraz zasady współdzielonej odpowiedzialności pomiędzy	Duża	Średnie	Mitygacja. Wprowadzenie działań pilotażowych i testujących, w tym wprowadzenie zmian legislacyjnych dot. wprowadzenia zasady współdzielonej odpowiedzialności za realizację zdań publicznych pomiędzy różnymi jednostkami.

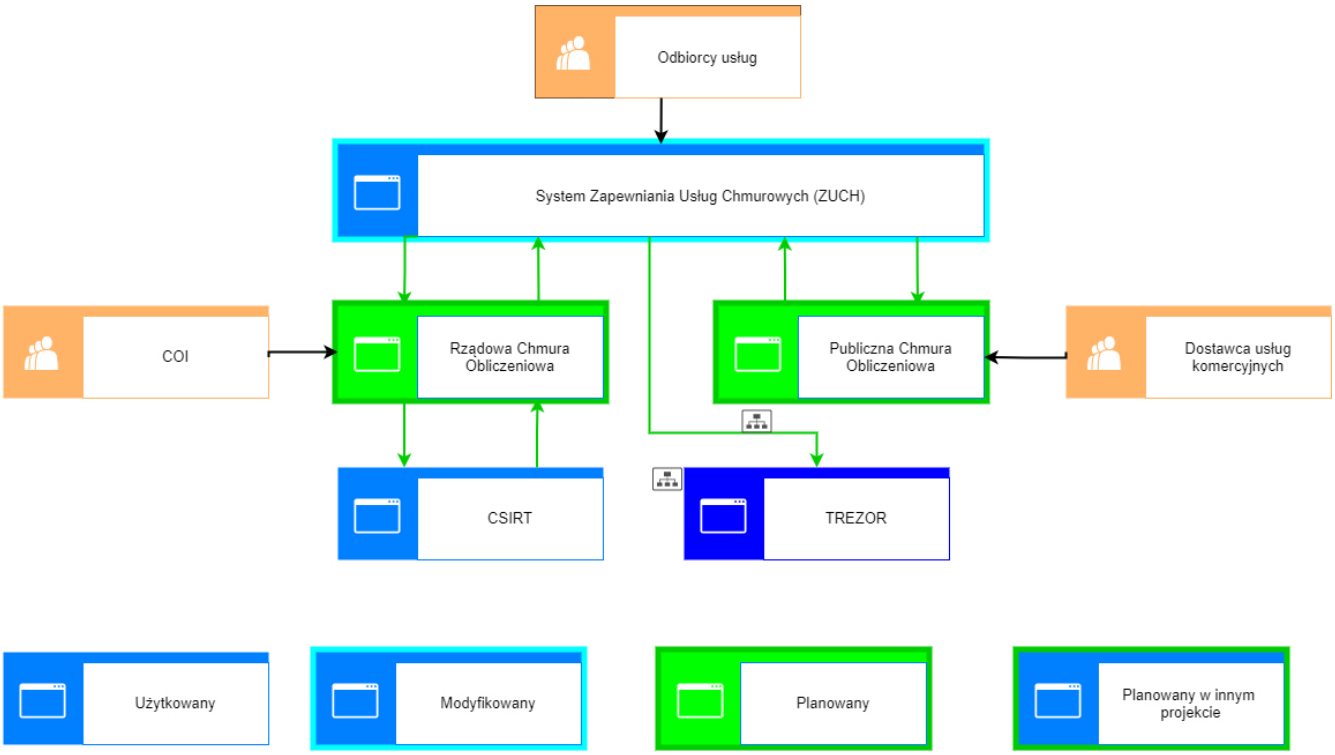
Nazwa ryzyka	Siła oddziaływania	Prawdopo-dobieństwo wystąpienia ryzyka	Sposób zarzadzania ryzykiem
jednostkami administracji publicznej.			

6. OTOCZENIE PRAWNE

Lp.	Tytuł aktu prawnego	Czy wymaga zmian	Opis zmian (jeśli dotyczy)	Etap prac legislacyjnych (jeśli dotyczy)
1	Uchwała nr 97 Rady Ministrów z dnia 11 września 2019 r. w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa” (M.P. z 2019 r. poz. 862)	~~TAK~~/NIE		
2	Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tj. Dz.U. 2021 poz. 670)	~~TAK~~/NIE		
3	Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (tj. Dz.U. 2017 poz. 2247)	~~TAK~~/NIE		
4	Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (tj. Dz.U. 2020 poz. 1369)	~~TAK~~/NIE		

7. ARCHITEKTURA

7.1. Widok kooperacji aplikacji



Lista systemów wykorzystywanych w projekcie

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
1	System Zapewniania Usług Chmurowych (ZUCH)	KPRM	System ZUCH jest narzędziem informatycznym służącym do wsparcia administracji publicznej w procesie zamawiania usług chmurowych. W zależności od wyniku kwalifikacji istniejącego lub nowego systemu lub przetwarzanych przez ten system danych, zostanie on zainstalowany w RChO lub w PChO. Wybór dostawcy usług z PChO będzie przeprowadzony zgodnie z pzp. i z zachowaniem konkurencyjności ofert. ZUCH, oprócz katalogu usług RChO, będzie zawierał również katalog usług PChO. Katalog publicznej chmury	Modyfikowany	Modyfikacja systemu ZUCH.

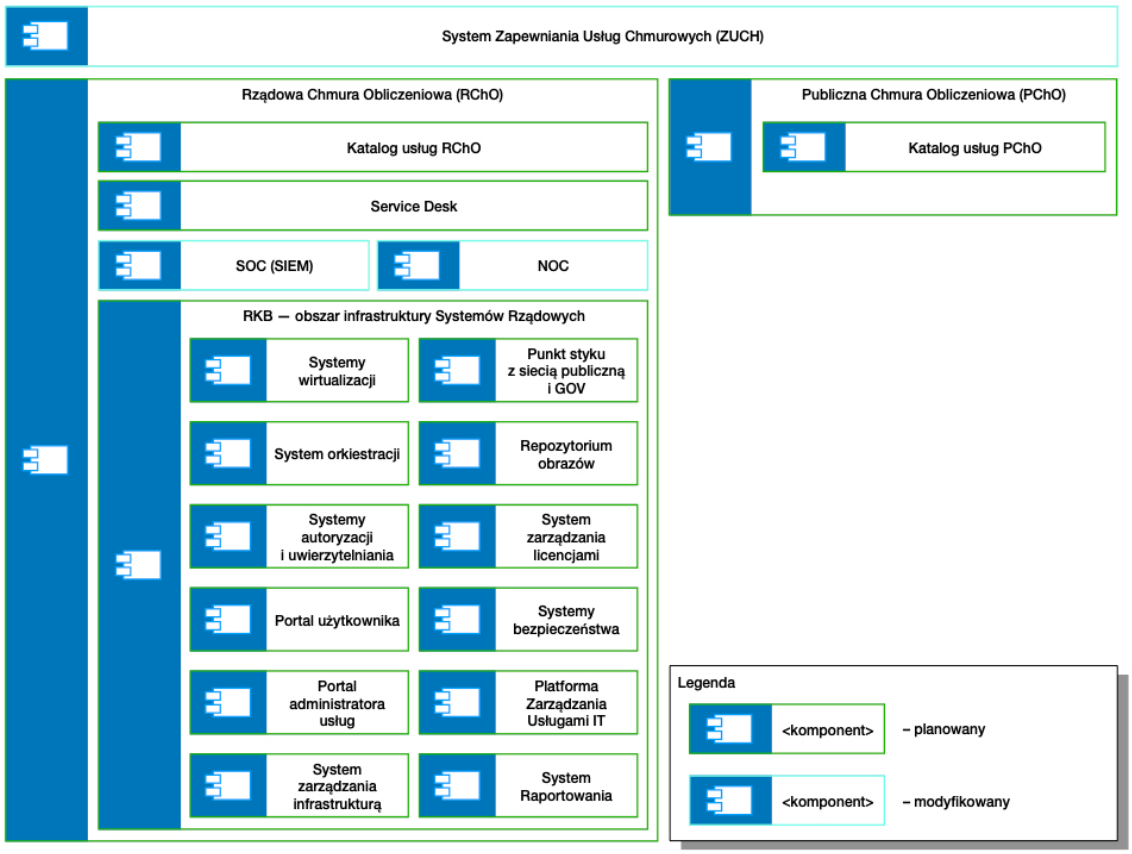
Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			obliczeniowej publikowany będzie w kolejnych iteracjach. Potencjalni dostawcy, którzy wyrażą zainteresowanie udostępnianiem swoich usług w ramach danej iteracji będą publikować swoją ofertę w Systemie ZUCH.		
2	Rządowa Chmura Obliczeniowa	KPRM	RChO będzie dostarczać infrastrukturę informatyczną, platformy oraz oprogramowanie w modelu usługowym zapewniając dla wszystkich systemów i aplikacji standard bezpieczeństwa, nadmiarowość, skalowalność i bezpieczne współdzielenie zasobów informatycznych.	Planowany	Budowa Rządowej Chmury Obliczeniowej.
3	CSIRT	ABW, MON, NASK	System wsparcia Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego.	Istniejący	Brak zmiany. Wyłącznie wymiana informacji.
4	Publiczna Chmura Obliczeniowa	KPRM	Usługi informatyczne świadczone w modelu chmury obliczeniowej IaaS, PaaS, SaaS przez podmioty komercyjne. Usługi wsparcia przy migracji do PChO, administracji i utrzymania.	Planowany	Budowa katalogu usług. Wyłącznie wymiana informacji z podmiotami komercyjnymi.
5	TREZOR	Ministerstwo Finansów	Informatyczny system obsługi budżetu Państwa.	Istniejący	Brak zmiany. Wyłącznie wymiana informacji.

Lista przepływów

Lp.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
1	ZUCH	Rządowa Chmura Obliczeniowa	Dane dot. usług uruchamianych w Rządowej Chmurze Obliczeniowej (rodzaj, ilość).	tryb odwołań bezpośrednich	Utworzenie (krytyczny dla sukcesu projektu).	Interfejs REST API (JSON).
2	Rządowa Chmura Obliczeniowa	ZUCH	Informacja o wykorzystaniu usług (rozliczenia, utylizacja zasobów, bilingi).	tryb odwołań bezpośrednich	Utworzenie (krytyczny dla sukcesu projektu)	Interfejs REST API (JSON).
3	ZUCH	Publiczna Chmura Obliczeniowa	Dane dot. podstępowania zakupowego na dostawę usług (rodzaj, ilość).	tryb odwołań bezpośrednich	Utworzenie (krytyczny dla sukcesu projektu)	Interfejs REST API (JSON)
4	Publiczna Chmura Obliczeniowa	ZUCH	Dane dot. realizacji świadczenia usług przez dostawcę. Informacje o kosztach wykorzystania usług, faktycznej utylizacji.	tryb odwołań bezpośrednich	Utworzenie (krytyczny dla sukcesu projektu)	Interfejs REST API (JSON)
5	ZUCH	TREZOR	Dane dot. kosztów świadczenia usług Rządowej Chmury Obliczeniowej.	kopiowanie danych	Utworzenie (krytyczny dla sukcesu projektu)	Interfejs REST API
6	Rządowa Chmura Obliczeniowa	CSIRT	Dane dot. zagrożeń bezpieczeństwa (incydenty)	kopiowanie danych	Utworzenie (krytyczny dla sukcesu projektu).	
7	CSIRT	Rządowa Chmura Obliczeniowa	Dane dot. zagrożeń bezpieczeństwa (incydenty) - krajowe i międzynarodo	kopiowanie danych	Utworzenie (krytyczny dla sukcesu projektu)	

Lp.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
			we.			

7.2. Kluczowe komponenty architektury rozwiązania



7.3. Przyjęte założenia technologiczne

Lp.	Obszar	Założenie technologiczne
1.	Infrastruktura	Zakłada się wykorzystanie wysoce skalowalnych rozwiązań opartych na węzłach obliczeniowych (compute node) i przechowywania danych (storage node), mechanizmów orkiestracji zasobów, umiejscowionych w dwóch, współpracujących ze sobą centrach przetwarzania danych.
2.	Sieć i bezpieczeństwo	Rozwiązanie bazuje na wykorzystaniu wydzielonych łącz pozostających w dyspozycji jednostek administracji rządowej oraz modyfikacji infrastruktury technicznej i organizacyjnej (SOC/

Lp.	Obszar	Założenie technologiczne
		NOC) w oparciu o zasoby osobowe COI. Planuje się wdrożenie standardu Rządowego Klastra Bezpieczeństwa (RKB) w poszczególnych obszarach infrastruktury wraz z dedykowaną infrastrukturą techniczną.
3.	Standardy wymiany danych	
4.	Systemy operacyjne serwerowe	Projekt zakłada udostępnienie użytkownikom końcowym maszyn fizycznych oraz konfigurowalnych środowisk wirtualnych wykorzystujących Microsoft Windows Server oraz niekomercyjne systemy operacyjne. Planowane jest uruchomienie co najmniej trzech środowisk wirtualizacji.
5.	Bazy danych	W RChO bazy danych dostarczane jako usługa PaaS.
6.	Serwery aplikacji	
7.	Portale	Planowane jest utworzenie nowego portalu dostępowego (w ramach ZUCH), pozwalającego autoryzowanym użytkownikom na samodzielne zamawianie prekonfigurowanych usług IaaS i PaaS, dostępnych w ramach utworzonych katalogów usług Rządowej Chmury Obliczeniowej oraz Publicznej Chmury Obliczeniowej.
8.	Inne	

7.4. Opis zasobów danych przetwarzanych w planowanym rozwiązaniu

Czy nowy system będzie tworzył zasoby danych o charakterze rejestru publicznego?
~~TAK~~/NIE
Czy nowy system będzie przetwarzał (używał, zmieniał) zawartość innych rejestrów publicznych?
~~TAK~~/NIE

7.5. Bezpieczeństwo

Planowany poziom zapewnienia bezpieczeństwa (w rozumieniu przepisów §20 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności […] (Dz. U. 2012, poz. 526 z późn. zm.) w zakresie dot. systemu zarządzania bezpieczeństwem informacji:
~~- system nie podlega rygorom KRI – należy wyjaśnić czy istnieją inne normy bezpieczeństwa, które będą spełnione przez system zgodnie z wymogami KRI~~
- dodatkowe zabezpieczenia powyżej wymogów KRI: należy wskazać uzasadnienie

Przedmiotem projektu jest zapewnienie odpowiednich warunków technicznych, koniecznych do udostępnienia administracji rządowej bezpiecznego i wydajnego środowiska informatycznego działającego w technologii chmury obliczeniowej. Centralnym elementem tego zamierzenia jest opracowanie i wdrożenie standardów bezpieczeństwa składowania i przetwarzania danych oraz sieci administracji rządowej.
Planowana budowa RChO będzie realizowana w oparciu o fizyczne zasoby teleinformatyczne (centra danych, serwery, przestrzeń dyskowa, sieci, oprogramowanie, systemy monitorowania, zespoły SOC, NOC itd.) należące do administracji rządowej. Realizacja RChO zakłada dostarczenie usług w dwóch wątkach realizacji: 1. Rządowy Klaster Bezpieczeństwa (RKB);
2. Infrastruktura Systemów Rządowych (ISR).

Wątek RKB to opracowanie standardów bezpieczeństwa dla poszczególnych obszarów oraz świadczenie usług bezpieczeństwa.
RKB zapewni ochronę:

- informacji przetwarzanych w RChO w tym zasobów systemów wewnętrznych administracji oraz e-usług świadczonych przez Internet;
- punktu styku z Internetem, uwzględniając odpowiednie wytyczne co do ilości operatorów świadczących usługę oraz sposobu zapewnienia na poziomie operatorskim zabezpieczenia przed atakami wolumetrycznymi;
- punktu styku ww. infrastruktury z wewnętrznymi sieciami rządowymi – uwaga sieci te świadczą wrażliwe usługi dla podmiotów administracji centralnej w zakresie ochrony bezpieczeństwa publicznego.

W zakresie zgodności z ustawą o ochronie informacji niejawnych projekt WIIP przewiduje osiągnięcie bezpieczeństwa teleinformatycznego pozwalającego na uzyskanie akredytacji ABW na podstawie przeprowadzonego audytu wybranego zakresu infrastruktury.
Z uwagi na konieczność zapewnienia bezpieczeństwa teleinformatycznego szczegóły architektury bezpieczeństwa projektu WDROŻENIE ROZWIĄZANIA CHMURY RZĄDOWEJ nie zostaną ujawnione.