OPIS ZAŁOŻEŃ PROJEKTU INFORMATYCZNEGO

Tytuł projektu	Wspólna Infrastruktura Informatyczna Państwa		
Wnioskodawca	Minister Cyfryzacji		
Beneficjent	Ministerstwo Cyfryzacji		
Partnerzy	Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy		
Źródło finansowania	budżet państwa - cz. 27 Informatyzacja, budżet państwa - rezerwa celowa dedykowana Inicjatywie WIIP, Program Operacyjny Polska Cyfrowa, Działanie 2.1 Wysoka dostępność i jakość e-usług publicznych (tryb pozakonkursowy, typ II projektu).		
Całkowity koszt projektu	188 718 396,90 zł		
Planowany okres realizacji projektu	09-2019 do 06-2022		
Osoba kontaktowa	Joanna Baranowska	joanna.baranowska@mc.gov.pl	222455521

1. POWODY PODJĘCIA PROJEKTU

1.1. Identyfikacja problemu i potrzeb

Potrzeba realizacji projektu została zapisana w PZIP oraz Planie Działań Ministra Cyfryzacji. 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 i centrów zapasowych, 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.
Jednocześnie, użytkowane obecnie, kluczowe zasoby informatyczne dedykowane do utrzymania Systemu Rejestrów Państwowych wymagają pilnej modernizacji, ze względu na osiągane limity wydajności i skalowalności.
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 kluczowych komponentów Systemów Rejestrów Państwowych;
- upowszechni model chmury obliczeniowej, jako główny sposób realizacji systemów informatycznych państwa (zmiana technologii wytwarzania oprogramowania).
Dzięki wdrożeniu usługi odtworzenia danych na wypadek katastrofy, dedykowanej Systemowi Rejestrów Państwowych, stworzone zostaną warunki do sprawnej modernizacji zasobów oraz podstawy do dalszej adaptacji rozwiązań Rządowej Chmury Obliczeniowej (RChO) na potrzeby

kluczowych systemów.

Interesariusz	Zidentyfikowany problem	Szacowana wielkość grupy
Podmioty administracji rządowej realizujące projekty wymagające rozwoju infrastruktury IT	Jednostki administracji rządowej realizujące 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.	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 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.
Kluczowa infrastruktura dedykowana do obsługi Systemów Rejestrów Państwowych nie posiada zapasowego ośrodka obliczeniowego (centrum odtworzenia danych).

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	Głównym celem projektu jest dostarczanie infrastruktury informatycznej jako usługi w modelu chmury obliczeniowej oraz zapewnienie bezpieczeństwa systemów teleinformatycznych tam uruchomionych. Realizacja tego celu da możliwość utworzenia ram infrastrukturalnych oraz katalogu usług elektronicznych adresowanych do administracji rządowej (A2A), stanowiących niezbędne instrumentarium wdrażania i rozwoju e-usług publicznych (A2B, A2C) w oparciu o technologię przetwarzania w chmurze obliczeniowej. Wskazany cel stanowi bezpośrednia realizację założeń określonych w obowiązujących dokumentach strategicznych, do których należą: 1) Strategia Sprawne Państwo 2020 Cel - 1 wpisuje się w zadania określone dla celu głównego strategii „Zwiększenie skuteczności i efektywności państwa otwartego na współpracę z obywatelami”, a w szczególności cel „Efektywne świadczenie usług publicznych”, „5.5. Standaryzacja i zarządzanie usługami publicznymi ze szczególnym uwzględnieniem technologii cyfrowych”. 2) Program Zintegrowanej Informatyzacji Państwa W programie wskazano jako jeden z celów „przejście od administrowania zarządzania rozwojem, poprzez m.in. wprowadzenie spójnej strategii zarządzania informacją oraz jednolitych zasad, standardów budowy i eksploatacji budowy rozwiązań IT w administracji (e-administracja) oraz zwiększenie zarówno podaży oczekiwanych przez społeczeństwo wysokiej jakości publicznych e-usług w Polsce, jak i poziomu ich wykorzystania

	mierzonego odsetkiem obywateli i przedsiębiorców, korzystających z Internetu w relacjach z administracją publiczną". 3) Program Operacyjny Polska Cyfrowa Wskazany cel -1 wpisuje się w główny cel szczegółowy Działania 2.1 POPC, którym jest wysoka dostępność i jakość e-usług w zakresie zapewnienia warunków do świadczenia usług elektronicznych przez administrację centralną oraz zakres działań wskazanych w SzOOP, obejmujący zapewnienie bezpiecznych systemów informatycznych oraz warunków do poprawy ich interoperacyjności.
Korzyść:	Podstawową korzyścią będzie zapewnienie bezpiecznych kanałów komunikacji elektronicznej na potrzeby budowy i eksploatacji rozwiązań dedykowanych administracji rządowej, opartych na technologii chmury obliczeniowej. Realizacja celu jest warunkiem koniecznym do osiągnięcia zakładanych produktów projektu i jednocześnie daje podstawy do dalszego rozwoju usług elektronicznych dla administracji rządowej – wdrożenie Rządowego Klastra Bezpieczeństwa (RKB) usprawni przygotowanie i realizację wszystkich projektów IT obejmujących przetwarzanie danych rejestrów państwowych oraz będzie stanowić jeden z elementów zapewnienia ich interoperacyjności. W katalogu korzyści można wskazać przede wszystkim: - poprawę bezpieczeństwa przetwarzania danych i świadczenia usług elektronicznych w administracji rządowej, - podniesienie efektywności wydatkowania środków w projektach zawierających element infrastruktury bezpieczeństwa IT, - skrócenie czasu realizacji nowych przedsięwzięć informatycznych przez szybsze udostępnianie wymaganej infrastruktury bezpieczeństwa, - zniesienie części barier technicznych dla interoperacyjności w zakresie infrastruktury bezpieczeństwa.
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. (2019 r.) 2) Wartość aktualna – 0 szt. (2019 r.) 3) Wartość aktualna – 0 szt. (2019 r.) 1) Wartość docelowa (2022 r.) – 2 szt. 2) Wartość docelowa (2022 r.) – 1 szt. 3) Wartość docelowa (2022 r.) – 1 szt.
Metoda pomiaru KPI	1) Wskaźnik będzie monitorowany cyklicznie na podstawie analizy dokumentacji zastanej: raportów audytu wewnętrznego (certyfikacja wewnętrzna), certyfikatów zewnętrznych, raportów administratora sieci oraz informacji z weryfikacji przez podmiot wskazany przez ministra właściwego ds. informatyzacji. Wartość wskaźnika będzie monitorowana z częstotliwością min. raz do roku. Za monitoring wskaźnika odpowiedzialny będzie Departament Systemów Państwowych Ministerstwa Cyfryzacji, przy współpracy z dedykowanym zespołem obsługi COI. 2) Wskaźnik dotyczy SOC/NOC dedykowanego dla RChO oraz infrastruktury pozostającej w dyspozycji ministra właściwego ds. informatyzacji. 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 Systemów Państwowych Ministerstwa Cyfryzacji, 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 Systemów Państwowych Ministerstwa Cyfryzacji, 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	Wskazany cel stanowi bezpośrednią realizację założeń określonych w obowiązujących dokumentach strategicznych, do których należą: 1) Strategia Sprawne Państwo 2020 Cel - 1 wpisuje się w zadania określone dla celu głównego strategii „Zwiększenie skuteczności i efektywności państwa otwartego na współpracę z obywatelami", a w szczególności cel „Efektywne świadczenie usług publicznych", „5.5. Standaryzacja i zarządzanie usługami publicznymi ze szczególnym uwzględnieniem technologii cyfrowych". 2) Program Zintegrowanej Informatyzacji Państwa W programie wskazano jako jeden z celów „przejście od administrowania zarządzania rozwojem, poprzez m.in. wprowadzenie spójnej strategii zarządzania informacją oraz jednolitych zasad, standardów budowy i eksploatacji budowy rozwiązań IT w administracji (e-administracja) oraz zwiększenie zarówno podaży oczekiwanych przez społeczeństwo wysokiej jakości publicznych e-usług w Polsce, jak i poziomu ich wykorzystania mierzonego odsetkiem obywateli i przedsiębiorców, korzystających z Internetu w relacjach z administracją publiczną". 3) Program Operacyjny Polska Cyfrowa Wskazany cel - 1 wpisuje się w główny cel szczegółowy Działania 2.1 POPC, którym jest wysoka dostępność i jakość e-usług w zakresie zapewnienia warunków do świadczenia usług elektronicznych przez administrację centralną oraz zakres działań wskazanych w SzOOP, obejmujący zapewnienie bezpiecznych systemów informatycznych, warunków do poprawy ich interoperacyjności oraz optymalizację inwestycji w infrastrukturę, w szczególności dzięki wykorzystaniu technologii chmury obliczeniowej.
Korzyść:	Podstawową korzyścią będzie zapewnienie bezpiecznych kanałów komunikacji elektronicznej na potrzeby budowy i eksploatacji rozwiązań dedykowanych administracji rządowej, wykorzystujących technologię chmury obliczeniowej. Realizacja celu jest warunkiem koniecznym do osiągnięcia zakładanych produktów projektu i jednocześnie daje podstawy 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. W katalogu korzyści można wskazać przede wszystkim: - 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: 0,9 PB (2019 r.) 2) Wartość aktualna: 1 szt. (2019 r.) 3) Wartość aktualna: 0,00% (2019 r.) 4) Wartość aktualna: 600 szt. (2019 r.) 1) Wartość docelowa: 4,5 PB (2022 r.) 2) Wartość docelowa: 5 szt. (2022 r.) 3) Wartość docelowa: 98,75% (2022 r.) 4) Wartość docelowa: 3 800 szt. (2022 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	Wskazany cel stanowi bezpośrednia realizację założeń określonych w obowiązujących dokumentach strategicznych, do których należą: 1) Strategia Sprawne Państwo 2020 Cel - 1 wpisuje się w zadania określone dla celu głównego strategii „Zwiększenie skuteczności i efektywności państwa otwartego na współpracę z obywatelami”, a w szczególności cel „Efektywne świadczenie usług publicznych”, „5.5. Standaryzacja i zarządzanie usługami publicznymi ze szczególnym uwzględnieniem technologii cyfrowych”. 2) Program Zintegrowanej Informatyzacji Państwa W programie wskazano jako jeden z celów „przejście od administrowania zarządzania rozwojem, poprzez m.in. wprowadzenie spójnej strategii zarządzania informacją oraz jednolitych zasad, standardów budowy i eksploatacji budowy rozwiązań IT w administracji (e-administracja) oraz zwiększenie zarówno podaży oczekiwanych przez społeczeństwo wysokiej jakości publicznych e-usług w Polsce, jak i poziomu ich wykorzystania mierzonego odsetkiem obywateli i przedsiębiorców, korzystających z Internetu w relacjach z administracją publiczną”. 3) Program Operacyjny Polska Cyfrowa Wskazany cel - 1 wpisuje się w główny cel szczegółowy Działania 2.1 POPC, którym jest wysoka dostępność i jakość e-usług w zakresie zapewnienia warunków do świadczenia usług elektronicznych przez administrację centralną, dzięki wprowadzeniu dedykowanego katalogu usług A2A.

Korzyść:	Wdrożenie dedykowanego katalogu usług adresowanego do administracji rządowej pozwoli na wygenerowanie szeregu korzyści zarówno dla użytkowników końcowych (pracowników administracji rządowej), jak również będzie miało 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 3) Liczba systemów teleinformatycznych administracji publicznej korzystających z udostępnionych usług A2A
Wartość aktualna i docelowa KPI:	1) Wartość aktualna: 0 szt. (2019 r.) 2) Wartość aktualna: 0 szt. (2019 r.) 3) Wartość aktualna: 0 szt. (2019 r.) 1) Wartość docelowa: 6 szt. (2022 r.) 2) Wartość docelowa: 1 szt. (2022 r.) 3) Wartość docelowa: 8 szt. (2022 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 odpowiedzialny zespół administratorów RChO (COI). 2) Wskaźnik będzie monitorowany na podstawie protokołu odbioru. Wskaźnik będzie monitorowany jednorazowo (wraz podpisaniem protokołu odbioru systemu). Za monitoring wskaźnika będzie odpowiedzialny zespół MC. 3) 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 odpowiedzialny 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	Jednostki administracji samorządowej Podmioty administracji rządowej realizujące projekty wymagające rozwoju infrastruktury IT (rocznie ok 150 transakcji)	Nie dotyczy

Lp.	Nazwa e-usługi	Typ	Zakres oddziaływania	Poziom dojrzałosci e-usługi
2	Dostawa usług w zakresie infrastruktury IT (IaaS) oraz platform systemowych	A2A	Podmioty administracji rządowej realizujące projekty wymagające rozwoju infrastruktury IT (rocznie ok 150 transakcji)	Nie dotyczy
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 (Help desk) – elektroniczna obsługa zgłoszeń	A2A	Podmioty administracji rządowej realizujące projekty wymagające rozwoju infrastruktury IT (rocznie ok 300 transakcji)	Nie dotyczy
6	Usługa odtworzenia danych w przypadku poważnej awarii (DRaaS) dedykowana rejestrom państwowym	A2A	Podmioty administracji rządowej realizujące projekty wymagające rozwoju infrastruktury IT	Nie dotyczy

Lp.	Nazwa e-usługi	Typ	Zakres oddziaływania	Poziom dojrzałosci e-usługi
			(rocznie ok 35600 transakcji)	

2.3. Udostępnione informacje sektora publicznego i zdigitalizowane zasoby

Rodzaj informacji/zasobów	Planowana data udostępnienia	Szacowana liczba obiektów objętych digitalizacją (udostępnianiem informacji)

Czy wszystkie zdigitalizowane zasoby objęte projektem będą udostępniane bezpłatnie?
TAK/NIE

2.4. Produkty końcowe projektu

Nazwa produktu	Planowana data wdrożenia
Rządowy Klaster Bezpieczeństwa - Wyposażenie i oprogramowanie RKB	08-2020
Rządowy Klaster Bezpieczeństwa - Katalog usług bezpieczeństwa	01-2021
Rządowy Klaster Bezpieczeństwa - Zasoby organizacyjne - gotowość zespołu obsługi RKB	02-2020
Rządowy Klaster Bezpieczeństwa - Standardy i polityki bezpieczeństwa	11-2019
Rządowa Chmura Obliczeniowa - Wyposażenie i oprogramowanie CPD	08-2020
Rządowa Chmura Obliczeniowa - Katalog usług RChO (wydanie inicjalne)	01-2021
Rządowa Chmura Obliczeniowa - Zasoby organizacyjne - gotowość zespołu obsługi RChO	08-2020
Rządowa Chmura Obliczeniowa - Docelowy model zarządzania popytem	12-2019
Rządowa Chmura Obliczeniowa - Model finansowania	12-2019
Rządowa Chmura Obliczeniowa - Katalog usług RChO (usługi PaaS)	06-2021
Rządowa Chmura Obliczeniowa - Usługa DRaaS dla Systemu Rejestrów Państwowych	12-2021
Rządowa Chmura Obliczeniowa - Katalog usług RChO (usług SaaS)	04-2022
System Zapewniania Usług Chmurowych - wersja produkcyjna	06-2021
System Zapewniania Usług Chmurowych - Katalog usług chmury publicznej (wydanie inicjalne)	03-2020
System Zapewniania Usług Chmurowych - Model zakupu usług chmury	12-2019

Nazwa produktu	Planowana data wdrożenia
publicznej	
System Zapewniania Usług Chmurowych - Katalog usług chmury publicznej (pierwsze wydanie)	03-2021
System Zapewniania Usług Chmurowych - Katalog usług chmury publicznej (drugie wydanie)	03-2022

3. KAMIENIE MILOWE

Kamienie milowe	Planowany termin osiągnięcia
Wydanie inicjalnego katalogu usług chmury publicznej	2020-03-30
Wydanie inicjalnego katalogu usług Rządowej Chmury Obliczeniowej	2021-01-18
Uruchomienie Rządowego Klastra Bezpieczeństwa	2021-01-14
Wydanie docelowego katalogu chmury publicznej	2022-03-30
Wydanie katalogu usług PaaS Rządowej Chmury Obliczeniowej	2021-06-30
Wydanie katalogu usług Rządowego Klastra Bezpieczeństwa	2021-01-14
Wydanie katalogu usług SaaS Rządowej Chmury Obliczeniowej	2022-04-30

4. KOSZTY

4.1. Koszty ogólne projektu wraz ze sposobem finansowania

Całkowity koszt projektu (netto oraz brutto), w tym	Netto 156 670 005,56 zł Brutto 188 718 396,90 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)	2019	Netto 7 670 181,47 zł Brutto 8 622 872,36 zł
	2020	Netto 92 484 732,66 zł Brutto 112 475 256,33 zł
	2021	Netto 46 915 397,49 zł Brutto 56 445 619,09 zł
	2022	Netto 9 599 693,94 zł Brutto 11 174 649,12 zł

4.2. Wykaz poszczególnych pozycji kosztowych

Nazwa pozycji kosztowej		Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
Oprogramowanie	Oprogramowanie wdrażane na potrzeby RKB, RChO oraz niezbędne do budowy usługi DRaaS	37 104 804,30 zł	21 162 804,30 zł - Oprogramowanie na potrzeby RChO. Wytworzenie oprogramowania na potrzeby obsługi procesu zamawiania i realizacji usług elektronicznych przewidzianych w ramach projektu. 6 642 000,00 zł - Oprogramowanie wdrażane na potrzeby RKB. Obejmuje oprogramowanie wirtualizacyjne, zarządzania zasobami sprzętowymi, orkiestracji zasobów logicznych, bilingu (licencje oprogramowania standardowego wraz z wdrożeniem w CPD). 9 300 000,00 zł - Pozycja dotyczy oprogramowania niezbędnego do budowy dedykowanej usługi odtworzenia danych na wypadek katastrofy (DRaaS), z której korzystać będą wszystkie systemy wchodzące w skład Systemu Rejestrów

Nazwa pozycji kosztowej		Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
			Państwowych.
Infrastruktura	Wyposażenie centrów obliczeniowych Rządowej Chmury Obliczeniowej, wyposażenie do budowy usługi DRaaS dla Systemu Rejestrów Państwowych, wyposażenie techniczne (urządzenia sieciowe, serwery) Rządowego Klastra Bezpieczeństwa, wyposażenie stanowisk pracy (NASK-PIB)	98 331 665,42 zł	42 321 998,75 zł - Wyposażenie centrów obliczeniowych Rządowej Chmury Obliczeniowej. Pozycja obejmuje nakłady na dostawę sprzętu od wybranych CPD, który będzie stanowił podstawę do budowy środowiska chmury obliczeniowej. 17 220 000,00 zł - Wyposażenie techniczne (urządzenia sieciowe, serwery) Rządowej Klastra Bezpieczeństwa. Dotyczy wyposażenia technicznego sieci komputerowej i bezpieczeństwa transmisji danych pomiędzy wybranymi CPD (Rządowy Klaster Bezpieczeństwa) – koszty obejmuje zarówno dostawy wyposażenia oraz oprogramowania. 38 666 666,67 zł - Wyposażenie do budowy usługi DRaaS dla Systemu Rejestrów Państwowych. Pozycja dotyczy wyposażenia niezbędnego od budowy dedykowanej usługi odtworzenia danych na wypadek katastrofy (DRaaS), z której korzystać będą wszystkie systemy wchodzące w skład Systemu Rejestrów Państwowych. 123 000,00 zł - Wyposażenie stanowisk pracy. Pozycja obejmuje wyposażenie stanowisk pracy personelu NASK-PIB.
Koszty UX i grafiki			
Bezpieczeństwo			
Wydajność rozwiązań			
Szkolenia	Szkolenia personelu projektu	349 704,07 zł	Pozycja obejmuje specjalistyczne szkolenia zespołów obsługi procesów IT związanych z funkcjonowaniem wdrażanych usług elektronicznych.
Działania informacyjno-promocyjne	Promocja projektu	1 464 930,00 zł	W ramach tej kategorii przewidziano koszty obligatoryjnych działań

Nazwa pozycji kosztowej		Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
			informacyjnych właściwych dla POPC oraz działań promocyjnych adresowanych do podmiotów administracji rządowej, mających na celu jak najszersze wykorzystanie zakresu udostępnianych usług.
Koszty zarządzania i wsparcia (w tym wynagrodzenia personelu wspomagającego)	Wynagrodzenia osobowe i koszty pośrednie, personel projektu (usługi body leasingu), pozostałe usługi (w tym in-house COI)	51 467 293,11 zł	13 750 020,37 zł - Wynagrodzenia osobowe i koszty pośrednie. Kategoria obejmuje koszty osobowe związane z pracami przygotowawczymi i wdrożeniem projektu (zarządzanie, zespoły zadaniowe, personel pomocniczy) wszystkich partnerów zaangażowanych w jego realizację. 11 879 100,00 zł - Personel projektu (usługi body leasingu). Pozycja obejmuje koszty usług body leasingu realizowanego zgodnie z przyjętym modelem zaangażowania zewnętrznych specjalistów do zespołów projektowych Ministerstwa Cyfryzacji. 25 838 172,74 zł - Pozostałe usługi (w tym in-house COI). Pozycja obejmuje koszty usług utrzymania świadczonych przez COI oraz pozostałe usługi doradcze.

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

Całkowity koszt utrzymania trwałości projektu (brutto)	207 294 297,15 zł		Źródło finansowania
Podział całkowitego kosztu utrzymania trwałości projektu na poszczególna lata (netto oraz brutto)	2022	24 879 728,26 zł (brutto) (20 379 225,30 zł netto)	krajowe środki publiczne - budżet państwa
	2023	30 865 479,88 zł (brutto) (25 245 690,04 zł netto)	krajowe środki publiczne - budżet państwa
	2024	31 101 330,22 zł (brutto) (25 437 438,28 zł netto)	krajowe środki publiczne - budżet państwa
	2025	88 866 759,17 zł (brutto) (72 401 201,66 zł netto)	krajowe środki publiczne - budżet państwa
	2026	31 580 999,62 zł (brutto) (25 827 413,40 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
Zbyt mały lub zbyt duży popyt na usługi oferowane przez WIIP	Średnia	Średnie	Mitygacja. Podjęcie działań promocyjnych i regulacyjnych (pobudzanie popytu) oraz zapewnienie skalowalności infrastruktury w celu dostosowania do popytu.
Niezakończenie postępowań zakupowych w terminach zgodnych z	Duża	Wysokie	Plan rezerwowy. Zastosowanie dwustopniowej procedury wyboru

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarzadzania ryzykiem
założeniami harmonogramu			wykonawców. Przyśpieszenie terminu publikacji ogłoszenia.
Przedłużanie się procesu legislacyjnego związanego z wydaniem uchwały Rady Ministrów	Średnia	Średnie	Plan rezerwowy. Przeniesienie zakresu prac na elementy niewymagające podjęcia uchwały.
Brak możliwości wykorzystania sieci rządowych w zakresie połączeń pomiędzy data center WIIP (brak przepustowości, konieczność rozbudowy węzłów o dodatkowe urządzenia i związane z tym długie postępowania przetargowe)	Średnia	Średnie	Akceptacja ryzyka.
Ograniczenia dostępności wysokokwalifikowanych kadr na potrzeby działania SOC / NOC.	Duża	Wysokie	Mitygacja. Zapewnienie wsparcia szkoleniowego oraz odpowiedniego funduszu wynagrodzeń.
Brak możliwości oferowania maszyn wirtualnych z systemami operacyjnymi z powodu niewypracowania nowych modeli licencjonowania uwzględniających specyfikę współdzielenia licencji w ramach administracji rządowej (pula licencji na procesor fizyczny umożliwiająca nielimitowane wykorzystanie w ramach tworzenia dowolnej ilości maszyn wirtualnych na infrastrukturze WIIP)	Średnia	Średnie	Plan rezerwowy. Zastosowanie dedykowanych licencji (brak współdzielenia). Budżet ryzyka.

5.2. Ryzyka wpływające na utrzymanie efektów

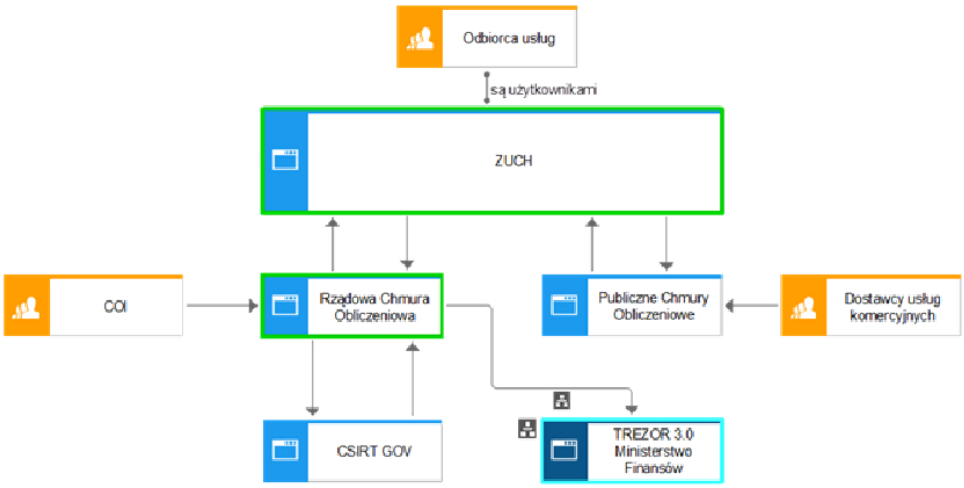
Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarzadzania ryzykiem
Niski popyt na usługi oferowane w wyniku realizacji projektu – brak wykorzystania pełnego potencjału środowiska obliczeniowego i usług chmurowych przez użytkowników końcowych.	Duża	Średnie	Mitygacja. Podjęcie działań promocyjnych i regulacyjnych (pobudzanie popytu).

6. OTOCZENIE PRAWNE

Lp.	Tytuł aktu prawnego	Czy wymaga zmian	Opis zmian (jeśli dotyczy)	Etap prac legislacyjnych (jeśli dotyczy)
1	Uchwała Rady Ministrów w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa”	~~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)	Ministerstwo Cyfryzacji	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 publicznych chmur	Planowany	Utworzenie nowego systemu ZUCH.

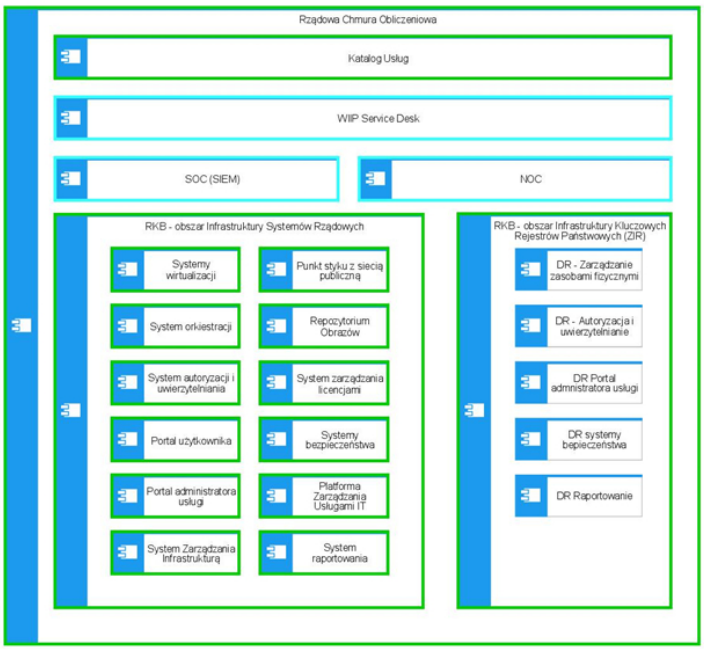
Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			obliczeniowych publikowany będzie w kolejnych iteracjach. Potencjalni dostawcy, którzy wyrażą zainteresowanie udostępnianiem swoich usług w ramach danej iteracji będą publikować swoją ofertę w Systemie ZUCH.		
2	Rządowa Chmura Obliczeniowa	Ministerstwo Cyfryzacji	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 GOV	Agencja Bezpieczeństwa Wewnętrznego	System wsparcia Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego	Istniejący	Brak zmiany. Wyłącznie wymiana informacji.
4	Publiczne Chmury Obliczeniowe	Podmioty komercyjne (wiele)	Usługi informatyczne świadczone w modelu chmury obliczeniowej IaaS, PaaS, SaaS.	Istniejący	Brak zmian. Wyłączenie wymiana informacji.
5	TREZOR	Ministerstwo Finansów	Informatyczny system obsługi budżetu Państwa.	Istniejący	Brak zmian. Wyłączenie wymiana informacji.

Lista przepływów

Lp.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
1	ZUCH	Rządowa Chmura	Dane dot. usług	tryb odwołań bezpośrednich	Utworzenie (krytyczny dla	Interfejs REST API

Lp.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
		Obliczeniowa	uruchamianych w Rządowej Chmurze Obliczeniowej (rodzaj, ilość).		sukcesu projektu)	(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	Publiczne Chmury Obliczeniowe	Dane dot. podstępowania zakupowego na dostawę usług (rodzaj, ilość).	tryb odwołań bezpośrednich	Utworzenie (krytyczny dla sukcesu projektu)	Interfejs REST API (JSON).
4	Publiczne Chmury Obliczeniowe	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 GOV	Dane dot. zagrożeń bezpieczeństwa (incydenty)	kopiowanie danych	Utworzenie (krytyczny dla sukcesu projektu)	
7	CSIRT GOV	Rządowa Chmura Obliczeniowa	Dane dot. zagrożeń bezpieczeństwa (incydenty) - krajowe i międzynarodowe.	kopiowanie danych	Utworzenie (krytyczny dla sukcesu projektu)	

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 usługach teletransmisji świadczonych przez MSWiA oraz utworzeniu dedykowanej infrastruktury technicznej i organizacyjnej (SOC/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: VMvare ESX, Microsoft HyperV oraz KVM.

Lp.	Obszar	Założenie technologiczne
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 chmur publicznych.
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 pozostające w gestii ministra właściwego ds. informatyzacji, oprogramowanie, systemy monitorowania, zespoły SOC, NOC itd.) należące do administracji rządowej. Realizacja RChO zakłada dostarczenie usług w trzech wątkach realizacji:
1. Rządowy Klaster Bezpieczeństwa (RKB);
2. Infrastruktura Systemów Rządowych (ISR);
3. Zintegrowana Infrastruktura Rejestrów (ZIR).

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.