

OPIS ZAŁOŻEŃ PROJEKTU INFORMATYCZNEGO

Tytuł projektu	Budowa Platformy Wysokiej Dostępności dla usług IT Resortu Finansów i administracji publicznej.		
Wnioskodawca	Podsekretarz Stanu Jurand Drop w Ministerstwie Finansów		
Beneficjent	Centrum Informatyki Resortu Finansów		
Partnerzy	nie dotyczy		
Źródło finansowania	<p>Krajowy Plan Odbudowy i Zwiększania Odporności</p> <p>Inwestycja C2.1.1. E-usługi publiczne, rozwiązania IT usprawniające funkcjonowanie administracji i sektorów gospodarki oraz technologie przełomowe w sektorze publicznym, gospodarce i społeczeństwie</p> <p>KPO: 452 851 800,00 zł</p> <p>PFR - środki własne PFR (tzw. środki tarczowe) - środki na pokrycie podatku VAT dla państwowych jednostek budżetowych</p> <p>PFR: 99 756 750,00 zł (vat)</p>		
Całkowity koszt projektu	552 608 550,00 zł		
Planowany okres realizacji projektu	10-2025 do 08-2026		
Osoba kontaktowa	Aneta Głowicka	aneta.glowicka@mf.gov.pl	734115904

1. POWODY PODJĘCIA PROJEKTU

1.1. Identyfikacja problemu i potrzeb

Dynamiczny rozwój cyfrowych usług publ. oraz postępująca cyfryzacja procesów adm. powodują zwiększone zapotrzebowanie na wydajne, bezpieczne i odporne na awarie środowiska teleinform. Konieczna jest nieprzerwana dostępności usług, krótki czasu odpowiedzi systemów oraz stabilność procesów realizowanych drogą elektroniczną. Jednocześnie rośnie liczba usług międzyinstytucjonalnych, które wymagają ciągłej, niezawodnej wymiany danych pomiędzy różnymi podmiotami publicznymi.

Platforma Wysokiej Dostępności dla usług IT Resortu Finansów i administracji publicznej to zintegrowane środowisko technologiczne, na które składają się: serwery, pamięci masowe, urządzenia sieciowe i oprogramowanie, tworząc klaster obliczeniowy połączony z istniejącymi zasobami. Jest to fundament do budowania rozwiązań informatycznych. W tym przypadku platforma będzie stanowiła zaplecze IT dla funkcjonowania dwóch nowych systemów informatycznych: System HA CIRF, System IaaS CIRF (opisy systemów znajdują się w pkt 7 Architektura-Lista systemów wykorzystywanych w projekcie)

Podstawą do korzystania z Systemu IaaS CIRF będzie porozumienie określające warunki współpracy między dostawcą Systemu IaaS CIRF (CIRF) a podmiotami administracji publicznej, w tym zasady korzystania z funkcjonalności systemu i odpowiedzialność stron.

Celem Platformy Wysokiej Dostępności dla usług IT Resortu Finansów i administracji publicznej jest minimalizacja ryzyka przerw w dostępie do systemów poprzez zastosowanie:

- Redundancji

- Eliminacji pojedynczych punktów awarii (SPOF)
- Automatycznego przełączania (failover)
- Monitorowania i szybkiej reakcji
- Skalowalności

Dzięki rozproszeniu na niezależne elementy infrastruktury, platforma zapewnia wysoką dostępność usług IT, nawet w przypadku awarii.

Główne produkty:

1. System HA CIRF dla usług IT Resortu Finansów.
2. System IaaS CIRF w modelu chmury obliczeniowej dla jednostek administracji publicznej.
3. Dokumentacja powykonawcza.

Wszystkie produkty wymienione są w części 2.4

Interesariusz	Zidentyfikowany problem	Szacowana wielkość grupy
Pracownicy Ministerstwa Finansów oraz jednostek podległych i nadzorowanych	<ul style="list-style-type: none"> • niewystarczająca wydajność oraz przepustowość istniejącej infrastruktury IT względem rosnącego zapotrzebowania na przetwarzanie danych • rozproszona infrastruktura IT powodująca nieefektywne wykorzystanie zasobów i konieczność obsługi w wielu lokalizacjach • brak odpowiedniej automatyzacji procesów administracji infrastruktury, co wymusza ręczne zarządzanie zasobami • niska odporność części systemów resortowych na awarie sprzętowe lub środowiskowe • ograniczone możliwości rozwoju usług cyfrowych z uwagi na obecne limity infrastrukturalne 	64000,00
Osoby fizyczne	<ul style="list-style-type: none"> • niewystarczająca dostępność e-usług publicznych (częste przerwy techniczne, niska responsywność usług przy wysokim obciążeniu) • niewystarczająca niezawodność usług – podatność na awarie oraz ograniczona skalowalność w okresach wzmożonego ruchu • zwiększona ekspozycja na incydenty bezpieczeństwa wynikająca z ograniczeń dotychczasowej infrastruktury 	25516000,00
Organizacje i przedsiębiorcy (podmioty z nadanym nr NIP)	<ul style="list-style-type: none"> • niewystarczająca dostępność i stabilność e-usług publicznych wykorzystywanych do obowiązków sprawozdawczych i rozliczeniowych • ograniczona przepustowość systemów przekładająca się na spowolnienie procesów obsługi • większa podatność usług na zakłócenia wskutek przeciążenia infrastruktury 	2788814,00
Administracja publiczna (ministerstwa oraz	<ul style="list-style-type: none"> • niewystarczająca infrastruktura IT w wielu jednostkach, utrudniająca zapewnienie dostępności i bezpieczeństwa usług 	19 ministerstw; 985 jednostek podległych

Interesariusz	Zidentyfikowany problem	Szacowana wielkość grupy
jednostki im podległe i nadzorowane). Z jednostkami administracji publicznej planowane jest podpisanie porozumień określających zasady i warunki korzystania z Systemu IaaS CIRF.	<p>teleinformatycznych</p> <ul style="list-style-type: none"> • wysokie koszty utrzymania rozproszonej infrastruktury oraz duplikacji zasobów w poszczególnych jednostkach • brak ujednoliconych standardów technologicznych utrudniający szybkie dostarczanie, rozwój oraz integrację aplikacji i usług • ograniczona dostępność centralnego, skalowalnego środowiska IT wspierającego współdzielone usługi dla administracji publicznej • niewystarczający poziom odporności środowisk IT na awarie, co przekłada się na ryzyko przerw w świadczeniu e-usług publicznych utrudnione zarządzania zasobami i ich skalowalność • brak możliwości pełnej kontroli nad środowiskiem chmur publicznych i znajdujących się tam danych • zbyt wysoki koszt i czasochłonność przenoszenia zasobów pomiędzy zasobami operatorów chmur publicznych • celowe działania wymierzone w administrację takie jak ataki DDoS, ataki skierowane na podatności infrastruktury, próby infiltracji i przejęcia kontroli nad urządzeniami 	

1.2. Opis stanu obecnego

Aktualnie CIRF sprawuje nadzór nad e-usługami publicznymi w resorcie finansów (64) i kolejne są planowane do uruchomienia. Część usług publicznych świadczona jest na rzecz wszystkich obywateli.

Zastosowane rozwiązania technologiczne dają możliwość łączenia różnych systemów, aplikacji i danych w jedną spójną i zintegrowaną infrastrukturę, co pozwala na usprawnienie przepływu informacji i zapewnienie interoperacyjności między różnymi elementami technologicznymi organizacji oraz systemami spoza niej.

CIRF dysponuje pełnym zestawem zaawansowanych kompetencji do budowy, rozbudowy oraz zarządzania Data Center na najwyższym poziomie infrastrukturalno-operacyjnym i bezpieczeństwa. CIRF posiada infrastrukturę IT, która obejmuje: 500+ serwerów fizycznych oraz 10 000+ maszyn wirtualnych, ponad 8 PB przestrzeni dyskowej, 200+ TB RAM-u oraz 40 000+ rdzeni CPU. Działa w modelu prywatnej chmury obliczeniowej, spójnej z siecią resortu, co pozwala efektywnie obsługiwać kluczowe e-usługi MF i KAS. CIRF utrzymuje kluczowe e-usług i systemy IT finansów państwa (614), zarządza cyfrowymi danymi podatkowymi w jednym z największych Data Center administracji publicznej w Polsce. Ośrodek jest obiektem infrastruktury krytycznej, z zaimplementowanymi zaawansowanymi systemami ochrony fizycznej i granulacją oraz kontrolą dostępu, monitoringiem środowiska fizycznego i cyberbezpieczeństwa.

Całodobowe 24/7 monitorowanie obejmuje wielowarstwowy nadzór – od warstwy aplikacji, usług IT, procesów, hostów po mechaniczną infrastrukturę Data Center. Zespół administratorów CIRF, systemowych, chmurowych i monitoringu zarządza usługami w oparciu o ITIL przy pomocy zaawansowanych narzędzi klasy enterprise, korzystając z 5 warstw monitoringu i 3-liniowego service desk.

2. EFEKTY PROJEKTU

2.1. Cele i korzyści wynikające z projektu

Cel - 1	Zapewnienie zwiększonej dostępności i ciągłości działania systemów informatycznych wspierających krytyczne/kluczowe usługi biznesowe świadczone przez administrację publiczną na rzecz jej interesariuszy poprzez budowę dwóch publicznych systemów informatycznych poprzez zbudowanie dwóch systemów informatycznych.
Cel strategiczny	<p>1. Krajowy Plan Odbudowy i Zwiększania Odporności</p> <p>Cel komponentu: C.2 Rozwój e-usług i ich konsolidacja, tworzenie warunków dla rozwoju zastosowań przełomowych technologii cyfrowych w sektorze publicznym, gospodarce i społeczeństwie, usprawnienie komunikacji między instytucjami publicznymi, obywatelami i biznesem oraz wyrównywanie poziomu wyposażenia szkół i podnoszenie kompetencji cyfrowych obywateli.</p> <p>Cel inwestycji: Zwiększenie liczby spraw możliwych do załatwienia drogą elektroniczną przy wykorzystaniu e-usług i procesów cyfrowych oraz zapewnienie modelowego systemu wsparcia zastosowań przełomowych technologii.</p> <p>2. Cele strategiczne Resortu Finansów: 4.1. Wzmocnienie potencjału organizacji</p> <p>Dokument strategiczny: Strategia Informatyzacji Resortu Finansów przyjęta przez Radę Informatyzacji MF w dniu 29 sierpnia 2025</p> <p>kluczowe usługi biznesowe KAS wspierane przez nowoczesne technologie IT $\geq 80\%$ kluczowych usług biznesowych KAS ze zdefiniowanego katalogu wspierane przez nowoczesne technologie w 2028 roku dostępność infrastruktury IT w ośrodku przetwarzania danych CIRF dla podatników $\geq 99,9\%$ dostępność infrastruktury i usług IT w CPD Radom w 2028 roku</p> <p>3. Cel Inicjatywy WIIP: przyczynienie się do zapewnienia wysokiego poziomu usług świadczonych społeczeństwu przez administrację publiczną w drodze wprowadzenia jednolitych wysokich standardów ochrony systemów informatycznych podmiotów publicznych oraz poprzez wspieranie podmiotów publicznych w utrzymaniu, a także w uzyskiwaniu usług niezbędnych do budowy, rozwoju i utrzymania tych systemów.</p> <p>Dokument strategiczny: uchwała Rady Ministrów nr 97 z dnia 11 września 2019 r. w sprawie Wspólnej Infrastruktury Informatycznej Państwa (WIIP)</p>
Korzyść:	1. Trwale zwiększona dostępność usług publicznych

	<p>Zapewnienie wysokiego poziomu dostępności e-usług publicznych poprzez wykorzystanie redundantnej, wysoko dostępnej infrastruktury IT.</p>
	<p>2. Trwałe ograniczenie nieplanowanych przerw w działaniu systemów</p> <p>Zmniejszenie liczby i czasu trwania przerw w funkcjonowaniu systemów krytycznych, dzięki środowisku o podwyższonej odporności na awarie infrastrukturalne i sprzętowe.</p>
	<p>3. Zwiększenie efektywności operacyjnej administracji publicznej</p> <p>Trwałe usprawnienie zarządzania zasobami IT poprzez centralizację, automatyzację i stosowanie skalowalnej architektury infrastruktury.</p>
	<p>4. Zwiększenie bezpieczeństwa cybernetycznego administracji publicznej</p> <p>Podniesienie trwałego poziomu bezpieczeństwa systemów informatycznych poprzez centralizację zabezpieczeń, stosowanie jednolitych standardów oraz rozwinięte mechanizmy ochrony i monitorowania.</p>
	<p>5. Zwiększenie odporności systemów publicznych na sytuacje kryzysowe</p> <p>Wzmocnienie ciągłości działania usług administracji publicznej dzięki infrastrukturze odpornej na awarie środowiskowe, sprzętowe i celowe działania osób trzecich.</p>
	<p>6. Ustandaryzowanie środowiska IT w administracji publicznej</p> <p>Wprowadzenie spójnych standardów technologicznych, architektonicznych i utrzymaniowych, umożliwiających bardziej efektywne wdrażanie, rozwój oraz utrzymanie usług cyfrowych.</p>
	<p>7. Długoterminowe obniżenie kosztów utrzymania IT w administracji publicznej</p> <p>Redukcja kosztu posiadania infrastruktury IT (TCO) dzięki centralizacji zasobów, współdzielonemu modelowi utrzymania oraz eliminacji duplikacji środowisk.</p>
	<p>8. Ograniczenie ryzyk wynikających z rozproszonej i przestarzałej infrastruktury IT</p> <p>Zmniejszenie ryzyk technicznych, organizacyjnych i finansowych po stronie jednostek administracji, wynikających wcześniej z konieczności samodzielnego utrzymywania lokalnych środowisk IT.</p>
	<p>9. Przyspieszenie cyfryzacji usług publicznych</p> <p>Zwiększenie tempa wdrażania nowych rozwiązań informatycznych oraz migracji istniejących systemów do nowoczesnego środowiska, co umożliwia szybsze dostarczanie usług cyfrowych obywatelom i przedsiębiorcom.</p>
	<p>10. Zwiększona skalowalność systemów administracji publicznej</p>

	<p>Zapewnienie trwałej możliwości elastycznego rozszerzania zasobów i uruchamiania nowych systemów bez konieczności kosztownych inwestycji infrastrukturalnych w poszczególnych jednostkach.</p> <p>11. Poprawa jakości usług świadczonych obywatelom i przedsiębiorcom</p> <p>Zwiększenie stabilności, wydajności i responsywności usług publicznych, co przekłada się na wyższy poziom satysfakcji użytkowników oraz lepszą realizację zadań administracji publicznej.</p>
KPI:	<p>KPI 1 - zakończenie procesu opracowywania nowych lub rozwijania istniejących publicznych systemów informatycznych</p> <p>KPI 2 - liczba systemów biznesowych zmigrowanych na Systemem HA CIRF</p> <p>KPI 3 - liczba wdrożonych katalogów funkcjonalności dostępnych dla Interesariuszy</p> <p>KPI 4 - podmioty korzystające z nowego Systemu IaaS CIRF</p>
Wartość aktualna i docelowa KPI:	<p>Wartość aktualna KPI 1 - 0</p> <p>Wartość aktualna KPI 2 - 0</p> <p>Wartość aktualna KPI 3 - 0</p> <p>Wartość aktualna KPI 4 - 0</p> <p>Wartość docelowa KPI 1 - 2</p> <p>Wartość docelowa KPI 2 - 8</p> <p>Wartość docelowa KPI 3 - 1</p> <p>Wartość docelowa KPI 4 - 2</p>
Metoda pomiaru KPI	<p>KPI 1 - Zakończenie procesu opracowywania nowych lub rozwijania istniejących publicznych systemów informatycznych</p> <p>metoda pomiaru: badanie ewaluacyjne ilościowe na podstawie danych zastanych</p> <p>źródło danych: protokół odbioru końcowego częstotliwość pomiaru: Przewiduje się jednokrotny pomiar wskaźnika, który będzie jednocześnie pomiarem wartości docelowej wskaźnika (krótki termin realizacji projektu nie pozwala na większą liczbę pomiarów).</p> <p>KPI 2 - liczba systemów biznesowych zmigrowanych na Systemem HA CIRF</p> <p>metoda pomiaru: badanie ewaluacyjne ilościowe na podstawie danych zastanych</p> <p>źródło danych: protokół z migracji systemu częstotliwość pomiaru: Przewiduje się jednokrotny pomiar wskaźnika, który będzie jednocześnie pomiarem wartości docelowej wskaźnika (krótki termin realizacji projektu nie pozwala na większą liczbę pomiarów).</p> <p>KPI 3 - liczba katalogów funkcjonalności dostępnych dla interesariuszy zewnętrznych (poza resortowych) w ramach Systemu IaaS CIRF</p> <p>metoda pomiaru: badanie ewaluacyjne ilościowe na podstawie danych zastanych</p> <p>źródło danych: protokół z migracji systemu częstotliwość pomiaru: Przewiduje się jednokrotny pomiar wskaźnika, który będzie jednocześnie pomiarem wartości docelowej wskaźnika (krótki termin realizacji projektu nie pozwala na większą liczbę pomiarów).</p> <p>Katalog będzie tworzony i dostosowywany na bieżąco w trakcie trwania projektu, jednak finalna wersja będzie dostępna po testach systemu IaaS,</p>

	<p>dlatego planowany jest jednokrotny pomiar na koniec realizacji projektu. Katalog będzie zawierał przynajmniej trzy funkcjonalności dla klienta zewnętrznego: stworzenie maszyny wirtualnej, poziomego skalowania infrastruktury poprzez zastosowanie równoważenia obciążenia sieciowego (loadbalncing), możliwość wykonania kopii zapasowej zasobów. Katalog będzie określał obowiązki Klienta i Dostawcy (CIRF) w zakresie procesów aktualizacji informacji dotyczących Systemu IaaS CIRF.</p> <p>KPI 4 (wskaźnik jakościowy) – podmioty korzystające z nowego Systemu IaaS CIRF metoda pomiaru: badanie ewaluacyjne ilościowe na podstawie danych zastanych źródło danych: podpisane porozumienia o współpracy częstotliwość pomiaru: jeden pomiar na kwartał od 01.09 2026 r. do 31.08.2027 r.</p>
--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

2.2. Udostępnione e-usługi

Lp.	Nazwa e-usługi	Typ	Zakres oddziaływania	Poziom dojrzałości e-usługi

2.3. Udostępnione informacje sektora publicznego i zdigitalizowane zasoby

Nie dotyczy

2.4. Produkty końcowe projektu

Nazwa produktu	Planowana data wdrożenia
Infrastruktura na potrzeby Systemu HA CIRF i Systemu IaaS CIRF	06-2026
System HA CIRF dla usług IT Resortu Finansów	07-2026
System IaaS CIRF w modelu chmury obliczeniowej dla jednostek administracji publicznej	07-2026
Protokoły z przeprowadzonych testów wydajności i bezpieczeństwa Systemu HA CIRF i Systemu IaaS CIRF	07-2026
Wzór porozumienia pomiędzy jednostkami administracji publicznej a CIRF określające zasady i warunki korzystania z Systemu IaaS CIRF	07-2026
Dokumentacja powykonawcza w szczególności: Instrukcja użytkownika	07-2026
Dokumentacja eksploatacyjna (w tym procedury operacyjne i administracyjne)	07-2026
Materiały informacyjno-promocyjne oraz dokumentacja fotograficzna	08-2026
Katalog funkcjonalności Systemu IaaS CIRF	07-2026

3. KAMIENIE MIŁOWE

Kamienie milowe	Planowany termin osiągnięcia
Podpisanie umów i przystąpienie do realizacji	2026-04-15
Zaprojektowana architektura rozwiązania Systemu HA CIRF (urządzenia, połączenia, integracja z istniejącą infrastrukturą)	2026-05-31
Zaprojektowana kompleksowa niezależna architektura rozwiązania Systemu IaaS CIRF	2026-05-31
Zrealizowane dostawy urządzeń na potrzeby Systemu HA CIRF i Systemu IaaS CIRF	2026-06-01
Dostarczony i odebrany System HA CIRF dla Resortu Finansów	2026-07-31
Dostarczony i odebrany System IaaS CIRF w modelu chmury obliczeniowej dla jednostek administracji publicznej	2026-07-31
Dostarczona i odebrana kompletna dokumentacja powykonawcza i wzór porozumień	2026-07-31
Zakończenie procesu opracowywania nowych lub rozwijania istniejących publicznych systemów informatycznych (C13ag KPO)	2026-08-31
Zakończenie procesu migracji 8 systemów do nowego Systemu HA CIRF	2026-08-15
Gotowa dokumentacja związana z rozliczeniem projektu	2026-08-31

4. KOSZTY

4.1. Koszty ogólne projektu wraz ze sposobem finansowania

Całkowity koszt projektu (netto oraz brutto), w tym	Netto 452 851 800,00 zł Brutto 552 608 550,00 zł	
Procent dofinansowania ze środków UE (brutto)	82%	
Procent środków z budżetu państwa (brutto)	18%	
Podział całkowitego kosztu projektu na poszczególne lata (netto oraz brutto)	2025	Netto 4 098 600,00 zł Brutto 4 098 600,00 zł
	2026	Netto 448 753 200,00 zł Brutto 548 509 950,00 zł

4.2. Wykaz poszczególnych pozycji kosztowych

Nazwa pozycji kosztowej		Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
Oprogramowanie	System HA CIRF dla usług IT Resortu Finansów. System IaaS CIRF w modelu chmury obliczeniowej dla jednostek administracji publicznej.	47 094 293,00 zł	Zakup gotowych rozwiązań programistycznych (licencje). Zakup subskrypcji oprogramowania. Zakup specjalistycznego oprogramowania dedykowanego poprawie bezpieczeństwa przetwarzanych informacji.
Infrastruktura	Infrastruktura na potrzeby Systemu HA CIRF i Systemu IaaS CIRF. System HA CIRF dla usług IT Resortu Finansów. System IaaS CIRF w modelu chmury obliczeniowej dla jednostek administracji publicznej.	485 354 470,00 zł	Zakup infrastruktury IT oraz oprogramowania systemowego i narzędziowego dla Systemu HA CIRF i Systemu IaaS CIRF.
Koszty UX i grafiki			
Bezpieczeństwo	Protokoły z przeprowadzonych testów wydajności i bezpieczeństwa.	0,00 zł	Testy zostaną wykonane zasobami CIRF. Koszty związane z tymi pracami zostały ujęte w pozycji "Koszty zarządzania i wsparcia" (wynagrodzenia personelu).
Wydajność rozwiązań	Protokoły z przeprowadzonych testów wydajności i bezpieczeństwa.	0,00 zł	Testy zostaną wykonane zasobami CIRF. Koszty związane z tymi pracami zostały ujęte w pozycji "Koszty zarządzania i wsparcia" (wynagrodzenia personelu).
Szkolenia			
Działania informacyjno-promocyjne	Materiały informacyjno-promocyjne oraz dokumentacja fotograficzna.	209 100,00 zł	Wydatki niezbędne do przeprowadzenia działań informacyjnych oraz realizacji obowiązku informacyjnego.
Koszty zarządzania i wsparcia (w tym wynagrodzenia personelu wspomagającego)	Protokoły z przeprowadzonych testów wydajności i bezpieczeństwa. Dokumentacja powykonawcza w szczególności:	19 950 687,00 zł	Wydatki niezbędne do prawidłowej realizacji i rozliczenia projektu, związane z zaangażowaniem personelu w okresie realizacji projektu, podróżami służbowymi oraz kosztami administracyjnymi (m.

Nazwa pozycji kosztowej		Przewidywany koszt brutto	Uzasadnienie pozycji kosztowej (przeznaczenie)
	Instrukcja użytkownika. Wzór porozumienia pomiędzy jednostkami administracji publicznej a CIRF określające zasady i warunki korzystania z Systemu IaaS CIRF. Gotowa dokumentacja związana z rozliczeniem projektu.		in. koszty utrzymania biura (wynajem, media, materiały), usługi księgowe, prawne, a także opłaty bankowe, telekomunikacyjne oraz zaangażowaniem personelu wspomagającego). Pozycja obejmuje również usługę asysty (wsparcia).

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

Całkowity koszt utrzymania trwałości projektu (brutto)	99 455 669,00 zł		Źródło finansowania
Podział całkowitego kosztu utrzymania trwałości projektu na poszczególne lata (netto oraz brutto)	2026	5 244 288,00 zł (brutto) (4 906 976,00 zł netto)	krajowe środki publiczne - budżet państwa
	2027	15 255 792,00 zł (brutto) (14 236 127,00 zł netto)	krajowe środki publiczne - budżet państwa
	2028	15 891 192,00 zł (brutto) (14 703 529,00 zł netto)	krajowe środki publiczne - budżet państwa
	2029	45 966 092,00 zł (brutto) (39 222 204,00 zł netto)	krajowe środki publiczne - budżet państwa
	2030	17 098 305,00 zł (brutto) (15 762 330,00 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 zarządzania ryzykiem
Opóźnienia harmonogramowe – spowodowane np. trudnościami w przetargach	Duża	Wysokie	powołanie zespołu projektowego; bieżące monitorowanie; prace wyprzedzające związane z przygotowaniem postępowań
Niewystarczająca dostępność zasobów technicznych – sprzętu, licencji, infrastruktury	Średnia	Niskie	szczegółowe opisanie przedmiotu zamówienia; założenie tolerancji
Opóźnienia w dostawach	Średnia	Niskie	odpowiednie przygotowanie projektów umów zawierających kary za opóźnienia w dostawach; założenie tolerancji
Utrata kompetencji w zespołach ludzkich	Średnia	Średnie	odpowiednie zarządzanie zasobami ludzkimi (budowanie portfolio kandydatów); otwarcie rekrutacji w celu uzupełnienia kompetencji w zespołach
Niedoszacowanie budżetu – np. przez wzrost cen sprzętu, usług, licencji	Średnia	Średnie	przeprowadzenie wstępnej analizy rynku; monitorowanie budżetu i analiza dopuszczalnych przesunień
Ryzyko korekty finansowej – w przypadku naruszeń zasad konkurencyjności, pomocy publicznej, RODO itd.	Mała	Niskie	przygotowanie postępowań zgodnie z wymogami PZP i dbałością o finanse publiczne, wieloetapowy proces akceptacyjny
Brak akceptacji zmian organizacyjnych – np. konieczność reorganizacji procesów IT lub	Mała	Niskie	odpowiednie zarządzanie zasobami ludzkimi; opracowanie planu naprawczego i dywersyfikacji zasobów

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
pracy zespołów			
Błędy w projektowaniu architektury HA – np. źle dobrane komponenty, niewystarczające mechanizmy failover	Średnia	Niskie	analiza alternatywnych rozwiązań; wdrożenie planu naprawczego; zaangażowanie w projekt wykwalifikowanego personelu
Problemy z uzyskaniem refundacji – błędy formalne, opóźnienia w zatwierdzeniu kosztów.	Średnia	Niskie	wdrożenie mechanizmów monitorowania wydatków - ich zasadności i zgodności z wytycznymi; szkolenia dla pracowników; dokładna weryfikacja dokumentów przez ich złożeniem
Zaburzenia łańcucha dostaw – np. związane z sytuacją geopolityczną lub logistyczną	Średnia	Średnie	monitoring ryzyka geopolitycznego; opracowanie planów awaryjnych na wypadek przerwania dostaw
Zmiany w otoczeniu prawnym lub fiskalnym – nowe podatki, regulacje	Średnia	Średnie	monitoring legislacyjny; analiza skutków regulacji; dostosowanie się do obowiązujących regulacji
niestabilność rynku dostawców usług IT – np. przejęcia, upadłości kluczowych partnerów	Średnia	Średnie	umowy z klauzulami zabezpieczającymi; weryfikacja dostawców; monitorowanie rynku IT

5.2. Ryzyka wpływające na utrzymanie efektów

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
Rotacja kadry technicznej do utrzymania	Średnia	Średnie	Odpowiednie zarządzanie zasobami ludzkimi; zabezpieczenie zasobów; szkolenia; umowy SLA

Nazwa ryzyka	Siła oddziaływania	Prawdopodobieństwo wystąpienia ryzyka	Sposób zarządzania ryzykiem
systemów HA i IaaS			
Brak możliwości zatrudnienia osób o odpowiednich kompetencjach niezbędnych do utrzymania efektów projektu	Średnia	Średnie	analiza rynku pracy i konkurencyjności ofert; prowadzenie portfolio kandydatów; współpraca z firmami body leasingowymi
Brak wystarczających zasobów kadrowych do utrzymania efektów projektu	Średnia	Średnie	analiza rynku pracy i konkurencyjności ofert; prowadzenie portfolio kandydatów; współpraca z firmami body leasingowymi
Brak wystarczających środków na utrzymanie efektów projektu	Średnia	Średnie	poszukiwanie możliwości finansowania; zgłaszanie do budżetu niezbędnych kosztów utrzymania efektów projektu i uwzględniania ich w planie jednostki
Nieosiągnięcie wszystkich zaplanowanych korzyści	Średnia	Średnie	ewaluacja po zakończeniu projektu

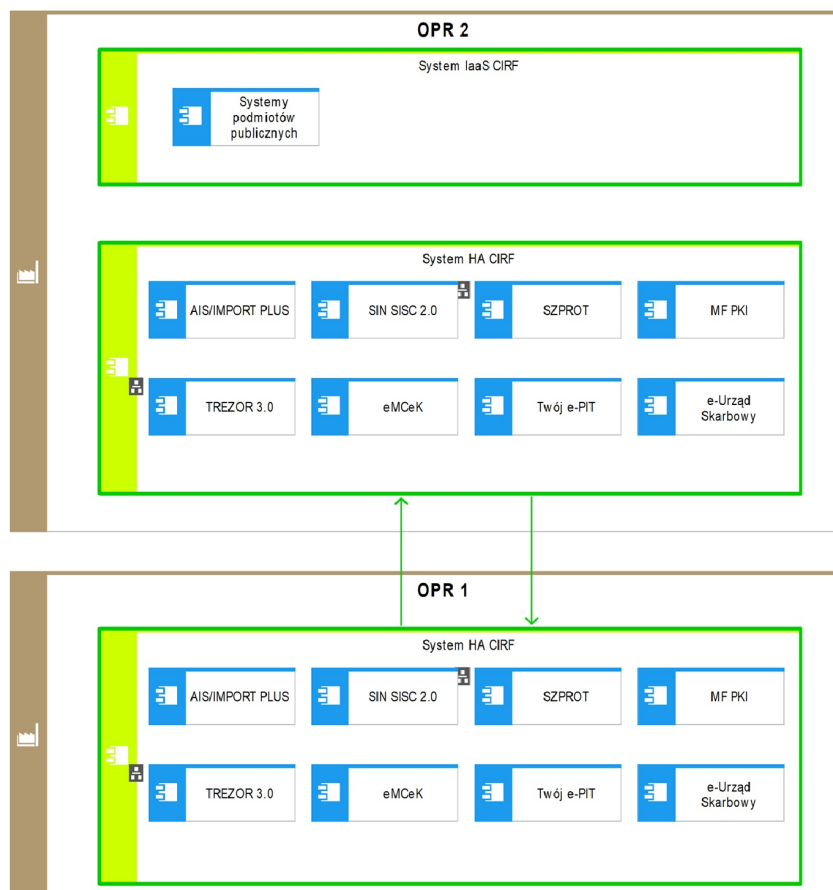
6. OTOCZENIE PRAWNE

Lp.	Tytuł aktu prawnego	Czy wymaga zmian	Opis zmian (jeśli dotyczy)	Etap prac legislacyjnych (jeśli dotyczy)
1	Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne	TAK/NIE		
2	Rozporządzenie Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych	TAK/NIE		
3	Ustawa o krajowym systemie cyberbezpieczeństwa	TAK/NIE		
4	Rozporządzenie Prezesa Rady Ministrów w	TAK/NIE		

Lp.	Tytuł aktu prawnego	Czy wymaga zmian	Opis zmian (jeśli dotyczy)	Etap prac legislacyjnych (jeśli dotyczy)
	sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego			
5	Ustawa o świadczeniu usług drogą elektroniczną	TAK/NIE		

7. ARCHITEKTURA

7.1. Widok kooperacji aplikacji



Legenda



Lista systemów wykorzystywanych w projekcie

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
1	AIS/IMPORT PLUS	Ministerstwo Finansów	Automatyczny System Importu (AIS/IMPORT PLUS) wspiera procesy biznesowe związane z importem towarów, wdrażając postanowienia Unijnego Kodeksu Celnego, w szczególności:	Istniejący	-

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			<p>załącznik B do rozporządzenia delegowanego Komisji Europejskiej nr 2015/2446 (z uwzględnieniem zmian w rozporządzeniach nr 2021/234 i 2024/249), załącznik B do rozporządzenia wykonawczego Komisji Europejskiej nr 2015/2447 (z uwzględnieniem zmian w rozporządzeniach nr 2021/235 i 2024/250).</p> <p>System umożliwia przesyłanie i obsługę przywózowych zgłoszeń celnych, powiadomień i deklaracji: zgłoszenia celne standardowe, uproszczone i uzupełniające – komunikat ZC415, powiadomienia o przedstawieniu towarów ujętych we wpisie do rejestru zgłaszającego – komunikaty PW433 (PWD-S) oraz ZC415DD, deklaracje do czasowego składowania – komunikat DS415, powiadomienia o przedstawieniu towarów wprowadzanych do WOC – komunikat PPX32 (PPW).</p> <p>Założenia systemu: pełna elektronizacja zgłoszeń celnych (z wyjątkiem zgłoszeń składanych przez podróżnych na dokumencie papierowym), dostosowanie zgłoszeń celnych do zakresu danych i formatów</p>		

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			<p>określonych w ww. rozporządzeniach Komisji Europejskiej.</p> <p>AIS/IMPORT PLUS jest zintegrowany z następującymi systemami: CVED/CED – system obsługi świadectw weterynaryjnych, Cyfrowa Granica – platforma wspierająca odprawy graniczne, EMCS PL2 – system monitorowania przemieszczania wyrobów akcyzowych, ISZTAR4 – system taryfowy i statystyczny, NCTS2 PLUS – system obsługi procedury tranzytu, OSOZ2 – system ochrony zdrowia, PDR PL/UE – Platforma Dokumentów Rejestrowych, PKI – infrastruktura klucza publicznego, PKWD-SW – system kontroli weterynaryjnej, REX/CRS – system rejestracji eksporterów, RPS – Rejestr Podmiotów Systemowych, SEAP PLUS – system elektronicznej administracji publicznej, SZPROT PLUS – system zarządzania protokołami, ZEFIR2 – system finansowo-księgowy administracji celnej, ZISAR – system zarządzania ryzykiem.</p>		
2	SIN SISC 2.0	Ministerstwo Finansów	System Informowania o Niedostępnościach Komponentów Systemu	Istniejący	-

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			<p>Informacyjnego Skarbowo-Celnego (SIN SISC 2.0) to system, który wspiera proces informowania użytkowników biznesowych o aktualnym stanie dostępności komponentów systemów IT, z uwzględnieniem awarii oraz planowanych okien serwisowych. Celem systemu jest zapewnienie przejrzystej i bieżącej informacji o dostępności usług IT dla pracowników resortu finansów. System nie prowadzi rejestrów publicznych. System wspiera następujące funkcjonalności: prezentację danych o dostępności usług IT – wizualizacja statusów komponentów systemów IT, informowanie o awariach i oknach serwisowych – komunikaty o bieżących i planowanych niedostępnościach, dostęp dla użytkowników biznesowych – interfejs umożliwiający przeglądanie informacji przez pracowników resortu finansów.</p> <p>Integracje z innymi systemami: System SIN SISC 2.0 jest zasilany danymi z systemu Dziennik Administratora Granica (DAG), który dostarcza informacje o stanie komponentów systemów IT.</p>		

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
3	SZPROT	Ministerstwo Finansów	<p>System Zintegrowanej Rejestracji Przedsiębiorców i Obsługi Wniosków (SZPROT)</p> <p>System SZPROT wspiera: rejestrowanie i udostępnianie danych rejestrowych wszystkich podmiotów działających w obszarze właściwości Krajowej Administracji Skarbowej (KAS), z dostępem dla systemów informatycznych KAS oraz wybranych systemów Unii Europejskiej, elektroniczne wspomaganie składania i rozpatrywania wniosków dotyczących działalności podmiotów – zarejestrowany podmiot ma możliwość przeglądania swoich danych, a elektroniczne formularze umożliwiają automatyczne wypełnianie wniosków, rejestrowanie i udostępnianie danych osób fizycznych działających w imieniu podmiotów – w tym rejestracja, aktualizacja i dezaktywacja przedstawicieli oraz zakresu reprezentacji, elektroniczne wspomaganie wydawania rozstrzygnięć w postępowaniu audytowym oraz monitorowanie wykorzystania wydanych pozwoleń, obsługę wniosków i wydawanie rozstrzygnięć w obszarach: cło, akcyza, gry hazardowe, INTRASTAT oraz urzędowe sprawdzenie.</p>	Istniejący	-

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			<p>Rejestry publiczne prowadzone w systemie:</p> <p>CRPA – Centralny Rejestr Podmiotów Akcyzowych</p> <p>Lista Agentów Celných</p> <p>Rejestr Podmiotów EORI</p> <p>Integracje z systemami krajowymi:</p> <p>SEAP</p> <p>PDR</p> <p>CEIDG – Centralna Ewidencja i Informacja o Działalności Gospodarczej</p> <p>CRP-KEP – Centralny Rejestr Podmiotów – Krajowa Ewidencja Podatników</p> <p>ZEFIR2</p> <p>ZISAR II</p> <p>OSOZ2</p> <p>MCA</p> <p>PKI</p> <p>Integracje z systemami unijnymi:</p> <p>EOS EORI</p> <p>EOS AEO</p> <p>CRS</p> <p>SEED UE</p>		
4	MF PKI	Ministerstwo Finansów	<p>System Infrastruktury Klucza Publicznego (MF PKI) wspiera realizację usług zaufania na potrzeby systemów i usług Ministerstwa Finansów (MF) oraz Krajowej Administracji Skarbowej (KAS). Został utworzony w celu wspierania:</p> <p>poboru i dystrybucji należności publicznoprawnych, obsługi obrotu towarowego, utrzymania infrastruktury teleinformatycznej i</p>	Istniejący	-

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			<p>systemów IT resortu finansów.</p> <p>System nie prowadzi rejestrów publicznych. System wspiera następujące funkcjonalności:</p> <p>emisję niekwalifikowanych certyfikatów cyfrowych, wykonywanie podpisów i pieczęci elektronicznych, walidację podpisów elektronicznych (kwalifikowanych, zaufanych, osobistych oraz celnych).</p> <p>Usługi świadczone są na rzecz systemów i usług MF oraz KAS. Integracje z innymi systemami: System IKP jest zintegrowany m.in. z:</p> <p>Platformą Usług Elektronicznych Skarbowo-Celnych (PUESC), Krajowym Systemem e-Faktur (KSeF), innymi systemami resortu finansów.</p>		
5	TREZOR 3.0	Ministerstwo Finansów	System TREZOR 3.0 wspiera następujące obszary działalności Ministerstwa Finansów oraz dysponentów środków budżetowych: usprawnienie przepływu informacji pomiędzy dysponentami środków budżetowych a Ministerstwem Finansów w zakresie planowania, wykonywania budżetu	Istniejący	-

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			<p>państwa oraz sprawozdawczości budżetowej, usprawnienie zarządzania płynnością budżetu państwa, wsparcie państwowych jednostek budżetowych w realizacji zasad bankowej obsługi budżetu państwa, w tym w zakresie zapotrzebowań na środki na wydatki.</p> <p>System wspiera następujące funkcjonalności: Sprawozdawczość budżetowa – sporządzanie i przekazywanie okresowych sprawozdań z wykonania budżetu państwa przez dysponentów środków, Planowanie budżetu państwa – opracowanie projektu ustawy budżetowej oraz planu finansowego, Wykonywanie budżetu państwa – przekazywanie środków, zarządzanie płynnością oraz prowadzenie rachunkowości budżetowej.</p> <p>Integracje z innymi systemami: System TREZOR 3.0 wymienia dane z następującymi systemami: ZEFIR2 – system finansowo-księgowy administracji celnej, BeSTi@ (w tym SJO BeSTi@) – system obsługi jednostek</p>		

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			samorządu terytorialnego, SFINKS – system finansowy resortu finansów, Analizy Budżetowe – system wspierający analitykę budżetową, inne systemy resortu Finansów.		
6	eMCeK	Ministerstwo Finansów	System Multkanałowe Centrum Komunikacji (eMCeK) wspiera komunikację pomiędzy klientami a organami Krajowej Administracji Skarbowej (KAS), udostępniając szereg narzędzi umożliwiających zdalną obsługę w kanałach: telefonicznym, czatowym, e-mailowym oraz wideo. System działa w ramach integralnej platformy komunikacyjnej. System wspiera: obsługę klientów niezidentyfikowanych oraz zidentyfikowanych w kanałach zdalnych (telefon, czat, e-mail, wideo), zarządzanie dostępem zdalnym i działaniami w rozproszonych lokalizacjach, integrację z narzędziami klasy AI (Voicebot, Chatbot), w tym automatyzację kontaktu z klientem oraz rozpoznanie i utrzymanie kontekstu rozmów – budowa Wirtualnego Asystenta Klienta KAS, automatyzację badań poziomu satysfakcji klienta.	Istniejący	-

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			<p>Główna funkcjonalność systemu: wydawanie interpretacji podatkowych, udostępnianie informacji podatkowej i celnej.</p> <p>System eMCeK jest zintegrowany z: narzędziami klasy AI (Voicebot, Chatbot), platformami komunikacyjnymi wykorzystywanymi w MF i KAS.</p>		
7	Twój e-PIT	Ministerstwo Finansów	<p>System Twój e-PIT wspiera podatnika w realizacji obowiązku podatkowego polegającego na złożeniu rocznego zeznania podatkowego w podatku dochodowym od osób fizycznych (PIT). Narzędzie jest udostępniane w serwisie e-Urząd Skarbowy. System został utworzony na podstawie: art. 45cd ustawy o podatku dochodowym od osób fizycznych, art. 20c ustawy o ryczałcie od przychodów ewidencjonowanych, wprowadzonych ustawą z dnia 4 października 2018 r. o zmianie ustawy o podatku dochodowym od osób fizycznych oraz niektórych innych ustaw (Dz. U. z 2018 r. poz. 2126 z późn. zm.).</p> <p>System wspiera następujące obszary funkcjonalne: pobór i dystrybucję należności</p>	Istniejący	-

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			<p>publicznoprawnych, utrzymanie zasobu otrzymanych i wytworzonych dokumentów.</p> <p>Procesy obsługiwane przez system: obsługa deklaracji podatkowych, obsługa informacji podatkowych, definiowanie zasad dotyczących obsługi interesariuszy.</p> <p>System Twój e-PIT jest zintegrowany z następującymi systemami resortu finansów: e-Urząd Skarbowy – jako platforma udostępniająca usługę, Krajowy System e-Faktur (KSeF) – w zakresie weryfikacji danych podatkowych, CRP KEP – Centralny Rejestr Podmiotów – Krajowa Ewidencja Podatników, ZEFIR2 – system finansowo-księgowy administracji skarbowej, PDR – Platforma Dokumentów Rejestrowych, PKI – infrastruktura klucza publicznego – obsługa podpisów elektronicznych, OSOZ2 – system obsługi zdrowotnej – w zakresie danych przekazywanych przez ZUS, MCA – system komunikacji administracyjnej – obsługa powiadomień i komunikatów</p>		

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			oraz Centralna Ewidencja i Informacja o Działalności Gospodarczej (CEIDG) .		
8	e-Urząd Skarbowy	Ministerstwo Finansów	<p>Serwis KAS – Katalog e-Urzędu</p> <p>Serwis KAS to aplikacja webowa i mobilna, która wspiera realizację e-usług Krajowej Administracji Skarbowej. System umożliwia użytkownikom zalogowanym (m.in. przez Węzeł Krajowy) dostęp do usług cyfrowych przygotowanych w ramach projektu e-Urząd, obejmującego:</p> <p>e-podatnik e-płatnik e-pełnomocnik e-komornik e-notariusz</p> <p>System wspiera obsługę następujących usług szczegółowych:</p> <p>e-konto podatnika – dla podatników PIT, CIT, VAT (osoby fizyczne i organizacje), umożliwia realizację czynności związanych z transakcjami, obowiązkami informacyjnymi oraz postępowaniem podatkowym drogą elektroniczną.</p> <p>e-konto płatnika – dla płatników zaliczek na PIT, umożliwia realizację czynności podatkowych drogą elektroniczną.</p> <p>e-konto pełnomocnika – dla osób fizycznych posiadających pełnomocnictwo,</p>	Istniejący	-

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			<p>umożliwia dostęp do danych i spraw podatkowych.</p> <p>e-konto komornika – dla komorników sądowych, umożliwia realizację obowiązków informacyjnych oraz czynności egzekucyjnych w administracji.</p> <p>e-konto notariusza – dla notariuszy, umożliwia realizację obowiązków informacyjnych i transakcyjnych.</p> <p>System wspiera również publikację innych e-usług realizowanych w ramach odrębnych projektów.</p> <p>Źródło danych: System korzysta z danych zgromadzonych w platformie Data Hub.</p> <p>Integracje z innymi systemami: Serwis KAS jest zintegrowany z:</p> <p>Węzłem Krajowym – uwierzytelnianie użytkowników, Data Hub – centralne repozytorium danych.</p>		
9	System HA CIRF	Ministerstwo Finansów	<p>System HA CIRF wspiera zapewnienie wysokiej dostępności usług IT resortu finansów poprzez utworzenie zwirtualizowanej platformy sprzętowo programowej (prywatnej chmury obliczeniowej), rozproszonej na niezależnych obiektach.</p> <p>Celem systemu jest minimalizacja ryzyka niedostępności usług</p>	Planowany	-

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			<p>wynikającej z awarii infrastruktury mechanicznej i informatycznej serwerowni, dywersyfikacja zasobów oraz odmiejszczenie systemów IT.</p> <p>System nie prowadzi rejestrów publicznych.</p> <p>System wspiera następujące funkcjonalności:</p> <p>Zarządzanie dostępnością usług IT – monitorowanie ciągłości działania, automatyczne przełączanie (failover), redundancja systemów i danych, raportowanie poziomu dostępności (SLA).</p> <p>Bezpieczeństwo i ochrona danych – kontrola dostępu, autoryzacja użytkowników, szyfrowanie transmisji i danych, ochrona przed cyberatakami (IDS/IPS, firewall, SIEM), backup i disaster recovery.</p> <p>Zarządzanie infrastrukturą IT – centralne zarządzanie serwerami, pamięcią masową i siecią, optymalizacja zasobów (load balancing), integracja z chmurą prywatną/publiczną, skalowanie usług.</p> <p>Wsparcie dla usług resortu finansów – hosting systemów resortowych (np. e-Podatki, e-Cło, e-Faktura), zapewnienie dostępności dla krytycznych procesów fiskalnych, integracja międzyresortowa (API, wymiana danych),</p>		

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			<p>obsługa systemów analitycznych (Big Data, AI).</p> <p>Monitoring i diagnostyka – bieżące monitorowanie parametrów technicznych, alerty o awariach, narzędzia diagnostyczne i predykcyjne (AIOps), dashboardy administracyjne.</p> <p>Zarządzanie użytkownikami i uprawnieniami – integracja z resortowym katalogiem użytkowników (Active Directory, LDAP), nadawanie i odbieranie uprawnień, audyt działań, mechanizmy SSO.</p> <p>Zarządzanie konfiguracją i zmianami – wersjonowanie konfiguracji, automatyzacja wdrożeń (DevOps, CI/CD), kontrola zmian, testowanie usług przed wdrożeniem produkcyjnym.</p> <p>Integracje z innymi systemami resortu finans.: e-Podatki, e-Cło, e-Faktura, DevOps: CI/C</p>		
10	System IaaS CIRF	Ministerstwo Finansów	<p>System IaaS CIRF w modelu chmury obliczeniowej wspiera jednostki administracji publicznej w budowie, migracji i utrzymaniu systemów informatycznych poprzez udostępnienie zwirtualizowanej platformy sprzętowo-programowej (prywatnej chmury obliczeniowej).</p> <p>Celem systemu jest zapewnienie wysokiej dostępności usług IT,</p>	Planowany	-

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			<p>podniesienie poziomu bezpieczeństwa danych oraz optymalizacja kosztów utrzymania infrastruktury.</p> <p>System umożliwia korzystanie z ustandaryzowanych zasobów informatycznych (serwery, pamięć masowa, sieć), wspiera wdrażanie jednolitych standardów ochrony systemów IT oraz zapewnia dostęp do usług niezbędnych do ich rozwoju i eksploatacji. System nie prowadzi rejestrów publicznych.</p> <p>System wspiera następujące funkcjonalności:</p> <p>Katalog usług dla użytkowników – dostęp do usług infrastrukturalnych i platformowych.</p> <p>Zarządzanie zasobami i użytkownikami – przydzielanie i monitorowanie zasobów (CPU, storage, sieć), automatyczne skalowanie, zarządzanie kontami, rolami i uprawnieniami (IAM), rozliczanie zużycia zasobów (billing).</p> <p>Bezpieczeństwo i zgodność – uwierzytelnianie (MFA, integracja z eID), szyfrowanie danych, backup i disaster recovery, zgodność z przepisami.</p> <p>Integracja i interoperacyjność – API, usługi sieciowe, integracja</p>		

Lp.	Nazwa systemu	Gestor systemu	Opis systemu	Status	Krótki opis ewentualnej zmiany
			<p>z innymi systemami administracji publicznej.</p> <p>Monitoring i audyt – monitorowanie dostępności i wydajności, audyt działań użytkowników i administratorów, raportowanie zgodności.</p> <p>Interfejs samoobsługowy – portal usługowy z mechanizmami zgłaszania incydentów i powiadomień.</p> <p>Integracje z innymi systemami:</p> <p>Systemy administracji publicznej korzystające z infrastruktury chmurowej,</p> <p>Narzędzia do uwierzytelniania i autoryzacji (np. eID, LDAP),</p> <p>Systemy monitorujące i raportujące (SIEM, APM),</p> <p>Rejestry państwowe zintegrowane przez API.</p>		

Lista przepływów

Lp.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
1	System HA CIRF (OPR1)	System HA CIRF (OPR2)	Pełna integracja	Integracja będzie zrealizowana poprzez umożliwienie komunikacji pomiędzy systemami za pomocą sieci LAN we wszystkich niezbędnych warstwach OSI (LAN --> SO	Odmiejscowienie krytycznych komponentów systemów biznesowych w celu wyeliminowania ryzyka wynikającego ze środowiska technicznego.	warstwa 2 i 3 modelu OSI

Lp.	System źródłowy	System docelowy	Zakres wymienianych danych	Sposób wymiany danych	Typ modyfikacji	Typ interfejsu
				Open Systems Interconnection Reference Model) oraz SAN poprzez sprzężenie urządzeń dystrybucyjnych (SAN Directors).		

7.2. Kluczowe komponenty architektury rozwiązania



7.3. Przyjęte założenia technologiczne

Lp.	Obszar	Założenie technologiczne
1.	Infrastruktura	Zasoby sprzętu serwerowego oparte na standardzie x86_64 zgodny z architekturą referencyjną CIRF.
2.	Sieć i bezpieczeństwo	W oparciu o już posiadany i eksploatowany model warstwowy zgodny z architekturą referencyjną CIRF.
3.	Standardy wymiany danych	Istniejące w obecnie eksploatowanych systemach oparte o posiadane rozwiązania "Platforma Integracyjna".
4.	Systemy operacyjne serwerowe	Windows Server, RHEL, SLES, OEL zgodny z architekturą referencyjną CIRF.
5.	Bazy danych	Oracle, MS SQL, PGS, MongoDB, MySQL zgodny z architekturą

Lp.	Obszar	Założenie technologiczne
		referencyjną CIRF.
6.	Serwery aplikacji	JavaScript, WebLogic, JBoss, PHP/Tomcat, WildFly zgodny z architekturą referencyjną CIRF.
7.	Portale	Interfejs dla użytkownika końcowego systemu IaaS CIRF.
8.	Inne	OpenStack

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

Bezpieczeństwo danych zostanie zapewnione w modelu trójwarstwowym – na poziomie organizacyjnym, procesowym oraz technicznym. Ochrona danych obejmie trzy podstawowe aspekty: integralność, poufność oraz dostępność zarówno danych, jak i całego systemu.

Na poziomie organizacyjnym kluczowe będzie ustanowienie i wdrożenie struktury organizacyjnej odpowiedzialnej za bezpieczeństwo systemu. Struktura ta powinna mieć jasno zdefiniowane role, obowiązki oraz zakres odpowiedzialności. Role związane z bezpieczeństwem muszą obejmować wszystkie grupy użytkowników systemu – od administratorów, przez operatorów, po użytkowników końcowych – aby zapewnić pełne pokrycie i odpowiedzialność na każdym etapie działania systemu.

Na poziomie procesów bezpieczeństwo danych będzie gwarantowane poprzez wdrożenie spójnych, zdefiniowanych procedur dla kluczowych obszarów, takich jak:

proces zarządzania zmianami,

proces zarządzania uprawnieniami,

proces monitorowania bezpieczeństwa,

proces zarządzania ciągłością działania.

Wdrożone zostaną także dodatkowe zabezpieczenia wykraczające poza minimalne wymagania KRI (Krajowe Ramy Interoperacyjności). Uzasadnieniem dla zastosowania wyższych standardów jest specyfika systemu i przetwarzanych danych – np. ich wrażliwość, znaczenie dla ciągłości działania instytucji lub podwyższone ryzyko ataków zewnętrznych. Takie podejście pozwoli na

osiągnięcie wyższego poziomu odporności na incydenty oraz szybsze reagowanie na zagrożenia.

Na poziomie technologicznym bezpieczeństwo zostanie zapewnione poprzez zastosowanie sprawdzonych mechanizmów kryptograficznych, systemów kontroli dostępu, rejestrowania i audytu działań użytkowników oraz technologii wykrywających i zapobiegających incydom (IDS/IPS). System będzie regularnie testowany pod kątem podatności oraz aktualizowany w celu eliminacji znanych luk bezpieczeństwa.