

OPIS ZAŁOŻEŃ PROJEKTU INFORMATYCZNEGO

| | | | |
|-------------------------------------|---|------------------------|-----------|
| Tytuł projektu | Rozbudowa systemu zarządzania infrastrukturą teleinformatyczną statystyki publicznej i cyberbezpieczeństwa (CyberStat) | | |
| Wnioskodawca | Kancelaria Prezesa Rady Ministrów | | |
| Beneficjent | Główny Urząd Statystyczny | | |
| Partnerzy | Nie dotyczy | | |
| Źródło finansowania | Program Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 – FERC Działanie 02.01 Wysoka jakość i dostępność e-usług publicznych Budżet Państwa część 58 Główny Urząd Statystyczny | | |
| Całkowity koszt projektu | 49 900 374,75 zł | | |
| Planowany okres realizacji projektu | 10-2025 do 09-2028 | | |
| Osoba kontaktowa | Krzysztof Cegielko | k.cegielko@stat.gov.pl | 226083187 |

1. POWODY PODJĘCIA PROJEKTU

1.1. Identyfikacja problemu i potrzeb

Projekt CyberStat jest odpowiedzią na potrzeby usprawnienia wybranych procesów back-office, tj. związanych z zarządzaniem IT i bezpieczeństwem informacji. Usprawniane w wyniku realizacji projektu procesy to:

- zarządzanie architekturą korporacyjną, w tym architekturą bezpieczeństwa informacji;
- inwentaryzacja aktywów IT;
- zarządzanie ciągłością działania;
- zarządzanie ryzykiem bezpieczeństwa informacji.

Projekt przewiduje też:

- dostawę i wdrożenie potrzebnych rozwiązań informatycznych wspierających obsługę ww. procesów;
- uruchomienie wewnętrznej e-usługi (A2A) wspierającej zarządzanie architekturą korporacyjną;
- modernizację infrastruktury technicznej wspierającej bezpieczeństwo informacji;
- podniesienie kompetencji pracowników w zakresie zarządzania IT i bezpieczeństwa informacji.

Przedstawione powyżej usprawnienia przyczynią się do usprawnienia funkcjonowania zdecydowanej większości systemów jssp niemodyfikowanych w projekcie (w tym rejestrów publicznych REGON i TERYT stanowiących infrastrukturę krytyczną państwa), np. poprzez podniesienie poziomu ich bezpieczeństwa.

Objęte projektem udoskonalenia obszarów zarządzania IT i bezpieczeństwem informacji wynikają głównie z:

- obowiązku spełnienia wymagań wprowadzonych nowymi regulacjami prawnymi na poziomie UE (w tym NIS 2) oraz krajowym (m.in. przygotowywanej nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa /KSC);
- doświadczeń zdobytych w związku z realizacją projektu „Wdrożenie Kompleksowego Systemu Zarządzania Bezpieczeństwem Informacji – KSZBI dla statystyki publicznej” zakończonego w 2022 r.;

- lawinowo narastających zagrożeń dotyczących bezpieczeństwa informacji;
- dążenia do stałego podnoszenia jakości świadczonych usług publicznych, w tym zapewniania ich interoperacyjności i optymalizacji.

Realizacja projektu usprawni przekazywanie informacji do Systemu Inwentaryzacji Systemów Teleinformatycznych (SIST) oraz wzmocni komplementarność systemów GUS z Architekturą Korporacyjną Państwa (AIP).

| Interesariusz | Zidentyfikowany problem | Szacowana wielkość grupy |
|--|---|--------------------------|
| Kadra zarządzająca jednostkami służb statystyki publicznej (jssp) | <ul style="list-style-type: none"> - Utrudniona eliminacja powielania tworzenia rozwiązań aplikacyjnych, brak re-używalnych komponentów (tzw. architektonicznych bloków budowlanych) wskutek braku kompleksowego opisu architektury systemów teleinformatycznych i zasobów informacyjnych jssp w powiązaniu z procesami biznesowymi i strategią organizacji (tj. architektury korporacyjnej). - Utrudnione pozyskanie informacji o całościowym stanie posiadania aktywów IT w organizacji spowodowane rozproszeniem i odseparowaniem procesów inwentaryzacji aktywów IT. - Brak zapewnienia pełnej zgodności obecnej inwentaryzacji aktywów IT z wszystkimi wymogami efektywnego zarządzania bezpieczeństwem informacji (np. tymi wynikającymi z Narodowych Standardów Cyberbezpieczeństwa /NSC). - Utrudniony dostęp do usług wewnętrznych, w wyniku wystąpienia incydentu i czasu usuwania jego skutków. - Brak szyfrowania na warstwie aplikacyjnej wewnętrznej komunikacji realizowanej za pomocą poczty elektronicznej. | 82 |
| Pracownicy jednostek służb statystyki publicznej (jssp) zajmujący się zarządzaniem IT i bezpieczeństwem informacji | <ul style="list-style-type: none"> - Brak możliwości wdrożenia uporządkowanego, całościowego podejścia do zarządzania rozwojem systemów teleinformatycznych, m.in. z uwzględnieniem strategii rozwoju statystyki publicznej i strategicznych kierunków cyfryzacji kraju wskutek braku kompleksowego opisu architektury systemów teleinformatycznych i zasobów informacyjnych jssp, w powiązaniu z procesami biznesowymi i strategią organizacji (architektury korporacyjnej). - Utrudnione zarządzanie systemami teleinformatycznymi i bezpieczeństwem informacji ze względu na brak skonsolidowanej wiedzy nt. zarządzanego środowiska. - Utrudnione zarządzanie, wdrożonym w ramach projektu KSZBI, Systemem | 133 |

| Interesariusz | Zidentyfikowany problem | Szacowana wielkość grupy |
|--|---|--------------------------|
| | <p>Zarządzania Ciągłością Działania - analiza BIA prowadzona z użyciem odseparowanych arkuszy Excel dla kilkuset systemów sprawia, że analiza wyników, wyznaczanie RTO i klasyfikacja systemów według krytyczności jest czasochłonna i narażona na błędy.</p> <ul style="list-style-type: none"> - Utrudnione zarządzanie ryzykiem bezpieczeństwa informacji wskutek rozproszenia procesów inwentaryzacji zasobów IT oraz braku całościowego opisu architektury systemów teleinformatycznych i zasobów informacyjnych jssp w powiązaniu z procesami biznesowymi i strategią organizacji. - Utrudniona realizacja procesu szacowania ryzyka z wykorzystaniem MS Excel, co zwiększa ryzyko błędów ludzkich i ogranicza zakres kontroli dostępu. - Brak możliwości generowania raportów i powiadomień w procesie zarządzania ryzykiem, porównywania ryzyk w kolejnych cyklicznych przeglądach, wiązania ryzyk z różnych domen zarządzania ryzykiem i analizowania ich wpływu i zależności. - Niespełniająca potrzeb jakości i spójność procesu inwentaryzacji aktywów IT spowodowana prowadzeniem jej w odrębnych systemach w kilku odseparowanych domenach bezpieczeństwa. - Utrudniony dostęp do usług wewnętrznych wskutek wystąpienia incydentu i czasu usuwania jego skutków. - Brak szyfrowania na warstwie aplikacyjnej wewnętrznej komunikacji realizowanej za pomocą poczty elektronicznej. | |
| <p>Pracownicy jednostek służb statystyki publicznej (jssp) (z wyłączeniem kadry zarządzającej i pracowników jssp zajmujących się zarządzaniem IT i bezpieczeństwem informacji)</p> | <ul style="list-style-type: none"> - Niewystarczająco obiektywna ocena wpływu niedostępności systemu teleinformatycznego - Właściciel biznesowy systemu, arbitralnie oceniając wpływ niedostępności systemu teleinformatycznego, nie zawsze posiada pełną wiedzę na temat procesów biznesowych związanych z tym systemem, ich wpływu na działalność biznesową, powiązania pomiędzy systemami, zarówno tymi technologicznymi, jak i wynikającymi z przepływu danych pomiędzy systemami w procesach. - Niewystarczająca jakość procesów oceny wpływu niedostępności, określania kluczowych systemów i opracowania planów | <p>5000</p> |

| Interesariusz | Zidentyfikowany problem | Szacowana wielkość grupy |
|--|---|------------------------------------|
| | <p>ciągłości działania/ awaryjnych spowodowana brakiem całościowego opisu architektury systemów teleinformatycznych i zasobów informacyjnych jssp w powiązaniu z procesami biznesowymi i strategią organizacji (tj. architektury korporacyjnej).</p> <ul style="list-style-type: none"> - Niewystarczająca jakość procesu analizy BIA spowodowana korzystaniem z arkuszy MS Excel, co zwiększa ryzyko błędów ludzkich. - Utrudniona realizacja procesu szacowania ryzyka spowodowana korzystaniem z arkuszy MS Excel, co zwiększa ryzyko błędów ludzkich i powoduje ograniczenia w zakresie kontroli dostępu. - Brak możliwości generowania raportów i powiadomień w procesie zarządzania ryzykiem. - Utrudniony dostęp do usług wewnętrznych wskutek wystąpienia incydentu i czasu usuwania jego skutków. - Brak szyfrowania na warstwie aplikacyjnej wewnętrznej komunikacji realizowanej za pomocą poczty elektronicznej. | |
| <p>Obywatele i/lub mieszkańcy RP oraz innych krajów, zainteresowani dostępem do wyników badań i analiz statystycznych.</p> | <ul style="list-style-type: none"> - Utrudniony dostęp do usług, wskutek przerwania ciągłości (wystąpienia incydentu i czasu usuwania jego skutków). - Utrudniony dostęp do aktualnych informacji wynikowych wskutek wystąpienia incydentu uniemożliwiającego aktualizację baz, portali dostępu do usług. - Niewystarczający poziom bezpieczeństwa zbieranych od m.in. obywateli, przetwarzanych i udostępnianych informacji. | <p>150 000 (1% z ok. 15 mln)</p> |
| <p>Przedsiębiorcy wykorzystujący do swojej działalności operacyjnej i strategicznej dane o charakterze statystycznym.</p> | <ul style="list-style-type: none"> - Utrudniony dostęp do usług, wskutek przerwania ciągłości (wystąpienia incydentu i czasu usuwania jego skutków). - Utrudniony dostęp do aktualnych informacji wynikowych wskutek wystąpienia incydentu uniemożliwiającego aktualizację baz, portali dostępu do usług. - Niewystarczający poziom bezpieczeństwa zbieranych od m.in. przedsiębiorców, przetwarzanych i udostępnianych informacji. | <p>50 000 (2.5% z ok. 2 mln)</p> |
| <p>Administracja publiczna i inne instytucje korzystające z dostępu do danych GUS.</p> | <p>Utrudniona wymiana informacji w związku z rozwojem architektury korporacyjnej państwa (AIP) oraz przekazywaniem danych do SIST wskutek braku uporządkowanego, całościowego opisu architektury systemów teleinformatycznych i zasobów informacyjnych jssp w powiązaniu z</p> | <p>10 000 (1.5% z ok. 640 000)</p> |

| Interesariusz | Zidentyfikowany problem | Szacowana wielkość grupy |
|---------------|---|--------------------------|
| | procesami biznesowymi i strategią organizacji (tj. architektury korporacyjnej). | |

1.2. Opis stanu obecnego

Prezes GUS odpowiada za dostarczanie wiarygodnych i wysokiej jakości informacji statystycznych i w tym celu przetwarza ogromne ilości danych, w tym danych osobowych. Projekt w dużym stopniu jest kontynuacją projektu KSZBI (2019-2022), w ramach którego zmodernizowano istniejący System Zarządzania Bezpieczeństwem Informacji (SZBI) - opracowano i zaktualizowano dokumenty SZBI. Wdrożono rozwiązania techniczne i organizacyjne zarządzania bezpieczeństwem informacji podnoszące bezpieczeństwo systemów i realizowanych procesów, które obecnie wymagają rozwoju i dostosowania do aktualnych potrzeb i wymagań.

W zakresie architektury korporacyjnej, obejmującej też bezpieczeństwo informacji, prace mają charakter inicjalny i dotyczą wybranych aspektów tej architektury. Nie wdrożono holistycznego podejścia.

Procesy inwentaryzacji aktywów IT są odseparowane i rozproszone. Nie wdrożono rozwiązania holistycznego, hierarchicznego, opisującego aktywa IT, m.in. wraz z ich powiązaniami. Procesy wykorzystują różne, niepowiązane rozwiązania (np. Log System, arkusz Excel). W odseparowanych, niezależnych systemach wykonywana jest inwentaryzacja środków trwałych. Wdrożone w 2022 r. zarządzanie ciągłością działania koncentruje się na systemach i procesach dotyczących analizy wpływu (BIA), opracowywania planów awaryjnych i ich testowania. Efekty prac dokumentowane są w odrębnych plikach Excel, Word. Proces wymaga skorelowania z zarządzaniem ciągłością działania występującą na innych poziomach organizacyjnych. Efekty prac w obszarze zarządzania ryzykiem bezpieczeństwa informacji zapisywane są w odrębnych plikach Excel, co utrudnia porównywalność i identyfikację zależności i wpływu poszczególnych ryzyk. Proces wymaga korelacji z innymi domenami ryzyka m.in. z zarządzaniem ryzykiem na tzw. poziomie zarządczym.

Obecna skuteczność zarządzania ciągłością działania oraz ryzykiem jest determinowana ograniczeniami zawiązanymi z inwentaryzacją aktywów oraz architekturą korporacyjną.

2. EFEKTY PROJEKTU

2.1. Cele i korzyści wynikające z projektu

| | |
|-------------------------|---|
| Cel - 1 | Optimalizacja procesów wewnętrznych jednostek służb statystyki publicznej związanych z realizacją zadań statutowych z wykorzystaniem nowoczesnych i bezpiecznych rozwiązań informatycznych |
| Cel strategiczny | <ol style="list-style-type: none"> 1. Projekt Strategii Cyfryzacji Polski do 2035 roku: obszar horyzontalny 1.3 – Cyberbezpieczeństwo. 2. Strategia na rzecz Odpowiedzialnego Rozwoju do roku 2020 (z perspektywą do 2030 r.) - Obszar: np. e-państwo / Kierunek Interwencji: Budowa i rozwój e-administracji – orientacja administracji państwa na usługi cyfrowe. 3. Program operacyjny Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 Priorytet FERC.02: Zaawansowane usługi cyfrowe. |
| Korzyść: | Wdrożenie mechanizmów zarządzania architekturą korporacyjną (z |

| | |
|---|--|
| | <p>uwzględnieniem architektury bezpieczeństwa informacji) i utrzymywanie uporządkowanego, całościowego opisu architektury systemów teleinformatycznych i zasobów informacyjnych jssp w powiązaniu z procesami biznesowymi i strategią organizacji przyczyni się m.in. do:</p> <ul style="list-style-type: none"> • Skuteczniejszego podejmowanie decyzji zarządczych; • Poprawy efektywności i skuteczności działań operacyjnych; • Podniesienia trafności i efektywności inwestycji; • Skrócenia czasu przygotowania nowych produktów lub usług; • Poprawy re-używalności posiadanych rozwiązań i eliminacji ich duplikowania; • Podniesienia bezpieczeństwa funkcjonowania organizacji; • Poprawy interoperacyjności systemów GUS; • Usprawnienia współpracy z podmiotami zewnętrznymi. <p>Produkty projektu dotyczące zarządzania IT i bezpieczeństwa informacji przyczynią się m.in. do:</p> <ul style="list-style-type: none"> • Usprawnienia procesów inwentaryzacji aktywów IT, co skutkować będzie: <ul style="list-style-type: none"> - podniesieniem efektywności zarządzania aktywami IT organizacji; - możliwością przedstawienia zintegrowanego, holistycznego i hierarchicznego stanu aktywów IT wraz z ich powiązaniami; - dostosowaniem do wymogów związanych z zarządzaniem bezpieczeństwem informacji (np. tych wynikających z NSC, NIS 2, KSC). • Usprawnienia zarządzania ciągłością działania, co skutkować będzie: <ul style="list-style-type: none"> - wdrożeniem kompleksowego podejścia do zarządzania ciągłością działania obejmującego zarówno procesy biznesowe jak i systemy teleinformatyczne; - zapewnieniem scentralizowanego środowiska pracy dla osób zajmujących się ciągłością działania w organizacji; - podniesieniem bezpieczeństwa funkcjonowania organizacji. • Usprawnienia zarządzania ryzykiem bezpieczeństwa informacji, co skutkować w szczególności będzie: <ul style="list-style-type: none"> - rozszerzeniem stopnia szczegółowości i głębokości wykonywania analizy ryzyka informacji; - możliwością wdrożenia kompleksowego podejścia do zarządzania ryzykiem w organizacji, m.in. z uwzględnieniem korelacji ryzyk pomiędzy poziomami/ domenami ryzyka; - zapewnieniem scentralizowanego środowiska pracy dla osób zajmujących się zarządzaniem ryzykiem; - podniesieniem bezpieczeństwa funkcjonowania organizacji. |
| KPI: | <p>KPI 1 - Liczba udostępnionych usług wewnątrzadministracyjnych (A2A);</p> <p>KPI 2 - Liczba uruchomionych systemów teleinformatycznych w podmiotach wykonujących zadania publiczne;</p> <p>KPI 3 - Użytkownicy nowych i zmodernizowanych publicznych usług, produktów i procesów cyfrowych;</p> <p>KPI 4 - Liczba zoptymalizowanych procesów wewnątrzadministracyjnych.</p> |
| Wartość aktualna i docelowa KPI: | <p>KPI 1 wartość aktualna: 0</p> <p>KPI 2 wartość aktualna: 0</p> <p>KPI 3 wartość aktualna: 0</p> <p>KPI 4 wartość aktualna: 0</p> <p>KPI 1</p> |

| | |
|---------------------------|---|
| | wartość docelowa: 1 KPI 2 wartość docelowa: 3 KPI 3 wartość docelowa: 400 KPI 4 wartość docelowa: 3 |
| Metoda pomiaru KPI | <p>KPI1: Metoda oraz sposób pomiaru: Pomiar wskaźnika będzie dokonany po uruchomieniu wewnętrznej e-usługi (A2A) wspierającej zarządzanie architekturą korporacyjną; Źródło: Protokół potwierdzający uruchomienie wewnętrznej e-usługi (A2A) wspierającej zarządzanie architekturą korporacyjną; Częstotliwość: Pomiar jednorazowy po uruchomieniu wewnętrznej e-usługi (A2A) wspierającej zarządzanie architekturą korporacyjną tj. 29.09.2028 r.</p> <p>KPI 2: Metoda oraz sposób pomiaru: Pomiar wskaźnika będzie dokonany po uruchomieniu: - Systemu zarządzania architekturą korporacyjną; - Systemu zarządzania ciągłością działania i ryzykiem bezpieczeństwa informacji; - Systemu inwentaryzacji aktywów IT (modernizacja). Źródło: Protokół odbioru potwierdzający uruchomienie: - Systemu zarządzania architekturą korporacyjną; - Systemu zarządzania ciągłością działania i ryzykiem bezpieczeństwa informacji; - Systemu inwentaryzacji aktywów IT (modernizacja). Częstotliwość: Pomiar jednorazowy po uruchomieniu systemów tj. 29.09.2028 r.</p> <p>KPI 3: Metoda oraz sposób pomiaru: Raporty generowane w ramach Portalu korporacyjnego (Intranet), dla dedykowanej witryny „Portal architektury korporacyjnej” świadczącej wewnętrzną e-usługę (A2A) wspierającą zarządzanie architekturą korporacyjną; Źródło: Raport aktywności użytkowników Portalu korporacyjnego (Intranet) w ramach witryny „Portal architektury korporacyjnej” świadczącej wewnętrzną e-usługę (A2A) wspierającą zarządzanie architekturą korporacyjną; Częstotliwość: Pomiar jednorazowy do 12 miesięcy po zakończeniu realizacji projektu tj. do 29.09.2029 r.</p> <p>KPI 4: Metoda oraz sposób pomiaru: Pomiar wskaźnika będzie dokonany po wdrożeniu zoptymalizowanych procesów wewnątrzadministracyjnych ; Źródło: Protokół potwierdzający wdrożenie zoptymalizowanych procesów; Częstotliwość: Pomiar jednorazowy do 12 miesięcy po zakończeniu realizacji projektu tj. do</p> |

| | |
|---|--|
| | 29.09.2029 r. |
| Cel - 2 | Podniesienie poziomu bezpieczeństwa cyfrowego gromadzonych, przetwarzanych i udostępnianych zasobów informacyjnych jednostek służb statystyki publicznej. |
| Cel strategiczny | <ol style="list-style-type: none"> 1. Projekt Strategii Cyfryzacji Polski do 2035 roku: obszar horyzontalny 1.3 – Cyberbezpieczeństwo. 2. Strategia na rzecz Odpowiedzialnego Rozwoju do roku 2020 (z perspektywą do 2030 r.) - Obszar: np. e-państwo / Kierunek Interwencji: Budowa i rozwój e-administracji – orientacja administracji państwa na usługi cyfrowe, 3. Program operacyjny Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 Priorytet FERC.02: Zaawansowane usługi cyfrowe. |
| Korzyść: | <p>Produkty projektu dotyczące infrastruktury IT, systemów zarządzania IT, bezpieczeństwem informacji oraz szkoleń specjalistycznych przyczynią się m.in. do:</p> <ul style="list-style-type: none"> • Obniżenia ryzyka utraty danych oraz ciągłości działania spowodowanych awariami, cyberatakami lub innymi zagrożeniami – co dotyczy w szczególności niemodyfikowanych w projekcie składników infrastruktury krytycznej, którymi są rejestry publiczne REGON i TERYT prowadzone przez prezesa GUS. • Poprawy kontroli dostępu do posiadanych aktywów IT. • Poprawy bieżącego monitorowania stanu posiadanych aktywów IT. • Podniesienia efektywności operacyjnej organizacji. • Dostosowania infrastruktury IT do wymogów związanych z bezpieczeństwem informacji (np. tych wynikających z NSC, NIS 2, KSC). • Podniesienia kompetencji pracowników jssp, w szczególności w zakresie bezpieczeństwa informacji, zarządzania IT oraz architektury korporacyjnej, które są niezbędne dla zapewnienia bezpieczeństwa cyfrowego organizacji. |
| KPI: | <p>KPI 1 - Instytucje publiczne otrzymujące wsparcie na opracowywanie usług, produktów i procesów cyfrowych;</p> <p>KPI 2 - Liczba pracowników IT podmiotów wykonujących zadania publiczne objętych wsparciem szkoleniowym;</p> <p>KPI 3 - Liczba pracowników podmiotów wykonujących zadania publiczne nie będących pracownikami IT, objętych wsparciem szkoleniowym.</p> |
| Wartość aktualna i docelowa KPI: | <p>KPI 1 wartość aktualna: 0</p> <p>KPI 2 wartość aktualna: 0</p> <p>KPI 3 wartość aktualna: 0</p> <p>KPI 1 wartość docelowa: 1</p> <p>KPI 2 wartość docelowa: 50</p> <p>KPI 3 wartość docelowa: 30</p> |
| Metoda pomiaru KPI | <p>KPI 1: Metoda oraz sposób pomiaru: Wartość wskaźnika będzie weryfikowana na podstawie umowy o dofinansowanie projektu. Za monitoring i pomiar wskaźnika odpowiedzialny będzie jeden z pracowników wyznaczonych do prac związanych z realizacją</p> |

| | |
|--|---|
| | <p>projektu.</p> <p>Źródło:</p> <p>Podpisana umowa o dofinansowanie projektu w ramach „Fundusze Europejskie na Rozwój Cyfrowy, Działanie 2.1 Wysoka jakość i dostępność e-usług publicznych (FERC.02.01)”.</p> <p>Częstotliwość:</p> <p>Pomiar jednorazowy, w dniu podpisania umowy o dofinansowanie projektu.</p> <p>KPI 2:</p> <p>Metoda oraz sposób pomiaru:</p> <p>Wskaźnik weryfikowany będzie na podstawie listy obecności na szkoleniu stacjonarnym lub on-line. Za monitoring i pomiar wskaźnika odpowiedzialny będzie jeden z pracowników wyznaczonych do prac związanych z realizacją projektu.</p> <p>Źródło:</p> <p>Lista obecności na szkoleniu.</p> <p>Częstotliwość:</p> <p>Pomiar na koniec ostatniego etapu szkoleń.</p> <p>KPI 3:</p> <p>Metoda oraz sposób pomiaru:</p> <p>Wskaźnik weryfikowany będzie na podstawie listy obecności na szkoleniu stacjonarnym lub on-line. Za monitoring i pomiar wskaźnika odpowiedzialny będzie jeden z pracowników wyznaczonych do prac związanych z realizacją projektu.</p> <p>Źródło:</p> <p>Lista obecności na szkoleniu</p> <p>Częstotliwość:</p> <p>Pomiar na koniec ostatniego etapu szkoleń.</p> |
|--|---|

2.2. Udostępnione e-usługi

| Lp. | Nazwa e-usługi | Typ | Zakres oddziaływania | Poziom dojrzałości e-usługi |
|-----|---|-----|--|-----------------------------|
| 1 | <p>Wewnętrzna e-usługa (A2A) wspierająca zarządzanie architekturą korporacyjną. (Usługa współtworzenia i zarządzania modelami architektury na różnych poziomach, przechowywania i zarządzania artefaktami architektonicznymi, wspierania procesu planowania i zarządzania zmianami, wspierania komunikacji między interesariuszami. Usługa będzie utworzona w ramach Portalu korporacyjnego.)</p> | A2A | <p>Pracownicy jednostek służb statystyki publicznej (jssp) zajmujący się zarządzaniem IT i bezpieczeństwem informacji</p> <p>Pracownicy jednostek służb statystyki publicznej (jssp) (z wyłączeniem kadry zarządzającej i pracowników jssp zajmujących się zarządzaniem IT i bezpieczeństwem informacji)</p> <p>(rocznie ok 4000</p> | Dwustronna interakcja |

| Lp. | Nazwa e-usługi | Typ | Zakres oddziaływania | Poziom dojrzałości e-usługi |
|-----|----------------|-----|----------------------|-----------------------------|
| | | | transakcji) | |

2.3. Udostępnione informacje sektora publicznego i zdigitalizowane zasoby

Nie dotyczy

2.4. Produkty końcowe projektu

| Nazwa produktu | Planowana data wdrożenia |
|--|--------------------------|
| Szkolenia specjalistyczne | 09-2027 |
| Modernizacja infrastruktury technicznej, w zakresie infrastruktury klucza publicznego, centrum certyfikacji, urządzeń HSM, web application firewall, load balancer, przełączników sieciowych, dysków SSD, macierzy dyskowych | 03-2028 |
| Raport z testów UX | 07-2028 |
| Modernizacja systemu inwentaryzacji aktywów IT (S_INW_AIT) - w zakresie: budowy modułu Integracja inwentaryzacji aktywów IT, modyfikacji modułu Inwentaryzacja systemów | 09-2028 |
| System zarządzania architekturą korporacyjną (SZ_AK) | 09-2028 |
| System zarządzania ciągłością działania i ryzykiem bezpieczeństwa informacji (SZ_CD_RBI) | 09-2028 |
| Materiały informacyjno-promocyjne | 09-2028 |
| Pozytywny raport z testów bezpieczeństwa | 09-2028 |
| Pozytywny raport z testów wydajności | 09-2028 |

3. KAMIENIE MIŁOWE

| Kamienie milowe | Planowany termin osiągnięcia |
|--|------------------------------|
| Opracowana dokumentacja przetargowa na wybór Inżyniera Projektu | 2026-03-31 |
| Opracowany szczegółowy plan szkoleń specjalistycznych oraz dokumentacja przetargowa na szkolenia | 2026-09-30 |
| Opracowana dokumentacja przetargowa na system zarządzania architekturą korporacyjną | 2027-03-31 |
| Zakończone szkolenia specjalistyczne | 2027-09-30 |
| Zakończona modernizacja infrastruktury technicznej | 2028-03-31 |

| Kamienie milowe | Planowany termin osiągnięcia |
|--|------------------------------|
| Zakończone dostawy oprogramowania wspierającego zarządzanie architekturą korporacyjną, zarządzanie ciągłością działania i ryzykiem bezpieczeństwa informacji | 2028-06-30 |
| Uruchomiona wewnętrzna e-usługa (A2A) wspierająca zarządzanie architekturą korporacyjną | 2028-09-15 |
| Uruchomiony system zarządzania architekturą korporacyjną | 2028-09-29 |
| Uruchomiony system zarządzania ciągłością działania i ryzykiem bezpieczeństwa informacji | 2028-09-29 |
| Uzyskany pozytywny wynik testów bezpieczeństwa | 2028-09-29 |
| Uzyskany pozytywny wynik testów wydajności | 2028-09-29 |
| Uzyskany pozytywny wynik testów badań UX | 2028-09-29 |

4. KOSZTY

4.1. Koszty ogólne projektu wraz ze sposobem finansowania

| | | |
|--|---|---|
| Całkowity koszt projektu (netto oraz brutto), w tym | Netto 42 465 800,47 zł Brutto 49 900 374,75 zł | |
| Procent dofinansowania ze środków UE (brutto) | 79,71% | |
| Procent środków z budżetu państwa (brutto) | 20,29% | |
| Podział całkowitego kosztu projektu na poszczególne lata (netto oraz brutto) | 2025 | Netto 822 206,90 zł Brutto 822 206,90 zł |
| | 2026 | Netto 28 528 312,79 zł Brutto 34 317 577,20 zł |
| | 2027 | Netto 7 112 590,25 zł Brutto 7 976 238,48 zł |
| | 2028 | Netto 6 002 690,53 zł Brutto 6 784 352,17 zł |

4.2. Wykaz poszczególnych pozycji kosztowych

| Nazwa pozycji kosztowej | | Przewidywany koszt brutto | Uzasadnienie pozycji kosztowej (przeznaczenie) |
|-------------------------|----------------------|---------------------------|---|
| Oprogramowanie | Usługi informatyczne | 21 809 927,25 zł | W związku z koniecznością usprawnienia procesów |

| Nazwa pozycji kosztowej | | Przewidywany koszt brutto | Uzasadnienie pozycji kosztowej (przeznaczenie) |
|-------------------------|--|---------------------------|--|
| | związane z przygotowaniem dokumentacji analitycznej, zaprojektowaniem, opracowaniem systemów objętych zakresem projektu, rozbudową istniejących systemów, wdrożeniem dostarczonych rozwiązań, przeprowadzenie testów funkcjonalnych dostarczonych rozwiązań, przeprowadzenie instruktaży dla użytkowników i administratorów, przygotowanie dokumentacji powykonawczej i szkoleniowej, migracja treści i zasobów określonych przez GUS. Zakup oprogramowania. | | <p>związanych z zarządzaniem architekturą korporacyjną, inwentaryzacją aktywów IT, zarządzaniem ciągłością działania, zarządzaniem ryzykiem bezpieczeństwa informacji niezbędny jest zakup usług informatycznych (w tym oprogramowania i licencji) w celu wdrożenia potrzebnych rozwiązań informatycznych wspierających obsługę ww. procesów.</p> <p>Koszty obejmują również zasilenie wspomnianych rozwiązań dotychczasowymi danymi lub opracowanie nowych, np. architektura korporacyjna - stan obecny. Pozycja kosztowa obejmuje także przygotowanie i uruchomienia usługi A2A.</p> <p>Środki zostaną przeznaczone również na wynagrodzenia dla członków zespołu projektowego, wykonujących zadania merytoryczne i techniczne związane z przygotowaniem dokumentacji analitycznej, zaprojektowaniem, wytworzeniem dedykowanego oprogramowania, rozbudową istniejących systemów, wdrożeniem dostarczonych rozwiązań, przeprowadzeniem testów funkcjonalnych dostarczonych rozwiązań, przeprowadzeniem instruktaży dla użytkowników i administratorów, przygotowaniem dokumentacji powykonawczej i szkoleniowej, migracją treści i zasobów określonych przez GUS.</p> |
| Infrastruktura | Koszt sprzętu i back-officowych systemów cyberbezpieczeństwa wraz z niezbędnym oprogramowaniem, | 14 106 099,00 zł | Środki umożliwią zakup uzupełniający niezbędnej infrastruktury teleinformatycznej dla prawidłowej realizacji przedsięwzięcia bezpośrednio związanej z podniesieniem cyberbezpieczeństwa |

| Nazwa pozycji kosztowej | | Przewidywany koszt brutto | Uzasadnienie pozycji kosztowej (przeznaczenie) |
|-------------------------|--|---------------------------|---|
| | licencjami i wdrożeniem: infrastruktura klucza publicznego, centrum certyfikacji, urządzenia HSM, web application firewall, load balancer, przełączniki dostępowe LAN oraz rozbudowa przestrzeni dyskowej vSAN | | (infrastruktura klucza publicznego, web application firewall, load balancer, urządzenia sieciowe, rozbudowa przestrzeni dyskowej). Środki zostaną również przeznaczone na wynagrodzenia pracowników merytorycznych jssp. |
| Koszty UX i grafiki | Koszty testowania rozwiązań wśród docelowych użytkowników oraz przeprowadzenia testów WCAG dostarczonych rozwiązań | 685 537,00 zł | Koszty pracowników merytorycznych jssp zaangażowanych w prace związane z opracowaniem merytorycznym i graficznym systemów a także przeprowadzeniem testów i audytów WCAG. Koszty zewnętrznego wykonawcy ujęte są w ramach pozycji kosztowej „Oprogramowanie”. |
| Bezpieczeństwo | Opracowanie architektury bezpieczeństwa informacji. Aktualizacja dokumentacji SZBI. Audyty bezpieczeństwa, testy bezpieczeństwa i podatności poszczególnych systemów objętych projektem CyberStat. | 4 578 991,00 zł | Środki przeznaczone zostaną na gruntowną, kompleksową rozbudowę systemu zarządzania bezpieczeństwem informacji – SZBI (obejmującego również wew. polityki, procedury, instrukcje, zalecenia, etc.), tak aby zapewnić całościową spójność wdrażanych rozwiązań m.in. z procesami biznesowymi organizacji oraz obowiązującymi normami i regulacjami prawnymi (z uwzględnieniem planowanych zmian). Środki umożliwią zapewnienie optymalnych i bezpiecznych rozwiązań. Zostaną przeznaczone m.in. na przeprowadzenie testów bezpieczeństwa niezbędnych do uruchomienia produkcyjnego rozwiązań dostarczonych w ramach realizacji przedsięwzięcia. Środki zostaną |

| Nazwa pozycji kosztowej | | Przewidywany koszt brutto | Uzasadnienie pozycji kosztowej (przeznaczenie) |
|-------------------------|--|---------------------------|--|
| | | | również przeznaczone na sfinansowanie wynagrodzeń pracowników merytorycznych jssp zaangażowanych w prace związane z przeprowadzeniem testów bezpieczeństwa i testów podatności poszczególnych systemów objętych projektem CyberStat. |
| Wydajność rozwiązań | Koszty testów wydajności projektowanego rozwiązania | 495 310,00 zł | Środki umożliwią zapewnienie optymalnych parametrów wydajnościowych z uwzględnieniem planowanej liczby obsługiwanych użytkowników dostarczanych rozwiązań. Środki zostaną przeznaczone m.in. na przeprowadzenie testów wydajnościowych. Środki zostaną również przeznaczone na wynagrodzenia pracowników merytorycznych jssp zaangażowanych w prace związane z przeprowadzeniem niezbędnych działań i analiz dla budowanego rozwiązania/ systemu pod kątem wydajnościowym. Kwota została oszacowana na podstawie dotychczas realizowanych zamówień przez jssp. |
| Szkolenia | Materiały szkoleniowe i szkolenia specjalistyczne z zakresu architektury informacyjnej, zarządzania IT i bezpieczeństwa informacji | 3 230 000,00 zł | Środki umożliwią przygotowanie i przeprowadzenie kompleksowych działań szkoleniowych podnoszących kwalifikacje pracowników jssp w zakresie: 1) obsługi i postępowania z incydentami, cyberbezpieczeństwa, bezpieczeństwa informacji, zarządzania ryzykiem, a także dla audytorów, Pełnomocnika NIS 2 oraz norm 2300X i 2700X; 2) zarządzania procesami IT, architektury korporacyjnej oraz zarządzania projektami. Celem szkoleń będzie zapewnienie prawidłowego, bezpiecznego i efektywnego |

| Nazwa pozycji kosztowej | | Przewidywany koszt brutto | Uzasadnienie pozycji kosztowej (przeznaczenie) |
|--|---|---------------------------|--|
| | | | korzystania z rozwiązań, które zostaną wdrożone w obszarze bezpieczeństwa informacji. |
| Działania informacyjno-promocyjne | Przeprowadzenie działań informacyjno-promocyjnych zgodnych z "Podręcznikiem wnioskodawcy i beneficjenta Funduszy Europejskich na lata 2021-2027 w zakresie informacji i promocji" | 130 000,00 zł | Środki umożliwią przeprowadzenie działań informacyjno-promocyjnych w celu zwiększenia świadomości, zaangażowania i ułatwienia korzystania z nowych technologii . W ramach działań planowane jest przeprowadzenie kampanii informacyjno-promocyjnej, konferencji podsumowującej projekt oraz przygotowanie materiałów informacyjno-promocyjnych (w tym tablicy informacyjnej). |
| Koszty zarządzania i wsparcia (w tym wynagrodzenia personelu wspomagającego) | Wynagrodzenia członków zespołu projektowego w ramach kosztów pośrednich | 4 864 510,50 zł | <ol style="list-style-type: none"> 1. Koszty usługi zewnętrznej związanej z zaangażowaniem Inżyniera projektu 2. Koszty wynagrodzenia kierownika projektu 3. Koszty personelu wchodzącego w skład biura projektu zaangażowanego w realizację projektu, w tym: w zarządzanie, rozliczanie, monitorowanie projektu lub prowadzenie innych działań administracyjnych w projekcie, jak również osób uprawnionych do reprezentowania jednostki i osób należących do personelu obsługowego (m. in. obsługa kadrowa, finansowa, księgowa, administracyjna, obsługa prawna, zamówień) w ramach kosztów pośrednich, zgodnie z definicją stosowaną w projektach współfinansowanych ze środków UE. <p>Realizacja projektu wymaga zaangażowania zespołu zarządzania oraz wsparcia przedsięwzięcia przez wszystkie jssp.</p> |

4.3. Koszty ogólne utrzymania wraz ze sposobem finansowania

(okres 5 lat)

| | | | |
|--|------------------|---|---|
| Całkowity koszt utrzymania trwałości projektu (brutto) | 14 178 766,25 zł | | Źródło finansowania |
| Podział całkowitego kosztu utrzymania trwałości projektu na poszczególne lata (netto oraz brutto) | 2028 | 282 396,66 zł (brutto) (264 445,44 zł netto) | krajowe środki publiczne - budżet państwa |
| | 2029 | 2 547 086,65 zł (brutto) (2 210 220,80 zł netto) | krajowe środki publiczne - budżet państwa |
| | 2030 | 1 129 586,65 zł (brutto) (1 057 781,77 zł netto) | krajowe środki publiczne - budżet państwa |
| | 2031 | 1 129 586,65 zł (brutto) (1 057 781,77 zł netto) | krajowe środki publiczne - budżet państwa |
| | 2032 | 8 242 919,65 zł (brutto) (6 840 979,33 zł netto) | krajowe środki publiczne - budżet państwa |
| | 2033 | 847 189,99 zł (brutto) (793 336,33 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 |
|---|--------------------|---------------------------------------|--|
| Przedłużające się procedury przetargowe | Średnia | Średnie | Rozpoczynanie procedur przetargowych z wyprzedzeniem, właściwe opisanie przedmiotu zamówienia, dobrze opracowane kryteria i sposoby oceny ofert oraz warunki udziału w |

| Nazwa ryzyka | Siła oddziaływania | Prawdopodobieństwo wystąpienia ryzyka | Sposób zarządzania ryzykiem |
|--|--------------------|---------------------------------------|---|
| | | | postępowaniu, a także wykonanie niezbędnych prac własnymi zasobami (np. opracowanie ogłoszenia o zamówieniu publicznym, przygotowanie części SWZ-u), zapewnienie współpracy z komórkami organizacyjnymi GUS w celu prawidłowego przeprowadzenia postępowań. |
| Zmiany rynkowe związane ze zmianami cen usług podczas realizacji projektu | Średnia | Niskie | Dogłębna analiza związana z wszelkimi aspektami budowy i wdrożenia systemu. Ciągłe monitorowanie trendów rynkowych. Zabezpieczenie odpowiednich rezerw finansowych. |
| Zmiany w otoczeniu zewnętrznym (w obszarze prawnym i obszarze IT) | Średnia | Średnie | Stały monitoring zmian w otoczeniu prawnym i technologicznym, a także elastyczne podejście do zarządzania projektem, które umożliwi dostosowanie się do nowych okoliczności. W celu minimalizacji ryzyka należy rozpoznać i monitorować, czy planowane są zmiany w otoczeniu prawnym i otoczeniu IT i na bieżąco reagować. |
| Brak możliwości zapewnienia na każdym etapie realizacji projektu składu Zespołu Projektowego o wystarczających: 1. umiejętnościach technicznych, 2. doświadczeniach z projektami tej skali i specyfiki | Mała | Średnie | Zapewnienie efektywnej komunikacji oraz ciągłego monitorowania i szkolenia zespołu. W miarę możliwości, przesuwanie zasobów między różnymi projektami, w celu zapewnienia odpowiedniej ilości doświadczonego personelu w kluczowych momentach projektu. Określenie wymagań dotyczących kwalifikacji i doświadczenia członków zespołu projektowego, regularne szkolenia i podnoszenie kwalifikacji członków zespołu projektowego, odpowiednie prowadzenie procesów rekrutacyjnych. |
| Istotny wzrost cen zaawansowanych i specjalistycznych urządzeń oraz oprogramowania dot. cyberbezpieczeństwa | Średnia | Niskie | Zaplanowanie dodatkowych środków budżetowych dla całości projektu i w budżetach rocznych. Planowanie kwoty do przetargu z racjonalnym zapasem. |
| Nieprecyzyjne określenie | Średnia | Niskie | Precyzyjne określenie potrzeb i wymagań dla poszczególnych systemów |

| Nazwa ryzyka | Siła oddziaływania | Prawdopodobieństwo wystąpienia ryzyka | Sposób zarządzania ryzykiem |
|---|--------------------|---------------------------------------|---|
| wymagań w opisie przedmiotu zamówienia w odniesieniu do wymagań prawnych i potrzeb użytkowników | | | w specyfikacji przetargowej oraz ich spełnienie na etapie zatwierdzania koncepcji i projektów realizacyjnych poszczególnych elementów systemu. |
| Nieterminowa realizacja umów przez Wykonawców | Średnia | Średnie | Wprowadzenie odpowiednich zapisów w umowach z Wykonawcami, które precyzyjnie określą reguły współpracy oraz zdefiniują sankcje związane z niewywiązywaniem się z umowy lub jej niepełną realizacją. |
| Nieosiągnięcie wskaźników projektu oraz celu projektu | Średnia | Niskie | Bieżący, regularny monitoring wskaźników postępu w projekcie. Transparentna komunikacja z interesariuszami oraz elastyczność w dostosowywaniu planów. Cykliczny monitoring harmonogramu realizacji produktów w projekcie. Elastyczne zarządzanie zasobami. Eskalowanie problemów na poziom kierownictwa instytucji. Systematyczność w podejściu do zarządzania ryzykiem pozwoli na minimalizowanie negatywnego wpływu na projekt i zwiększenie szans na osiągnięcie założonych celów. |

5.2. Ryzyka wpływające na utrzymanie efektów

| Nazwa ryzyka | Siła oddziaływania | Prawdopodobieństwo wystąpienia ryzyka | Sposób zarządzania ryzykiem |
|---|--------------------|---------------------------------------|--|
| Brak zastępowalności i niedostępność specjalistów z zakresu zarządzania i cyberbezpieczeństwa | Średnia | Średnie | Racjonalna, przemyślana polityka kadrowa oraz system motywacyjny. Racjonalne nabywanie usług zewnętrznych. |
| Brak wsparcia technicznego dla | Mała | Niskie | Zapewnienie odpowiednich kompetencji poprzez zawieranie umów serwisowych |

| Nazwa ryzyka | Siła oddziaływania | Prawdopodobieństwo wystąpienia ryzyka | Sposób zarządzania ryzykiem |
|--|--------------------|---------------------------------------|--|
| technologii wspierającej produkty projektu | | | z dostawcami technologii, które gwarantują odpowiednie wsparcie techniczne. Dokładne badanie różnych dostępnych technologii i kierowanie się nie tylko ich obecną popularnością czy łatwością użycia, ale również ich potencjałem do długoterminowego wsparcia i rozwoju. Utrzymywanie regularnego kontaktu z dostawcami technologii i monitorowanie ich polityki wsparcia. Inwestowanie w szkolenia dla zespołu projektowego w celu zwiększenia ich kompetencji technicznych. |
| Znaczące zmiany w przepisach prawa i w zakresie standardów obowiązujących całą administrację publiczną, które wpływają na systemy wytworzone w ramach projektu | Mała | Niskie | Modyfikowanie systemów w sposób elastyczny i modularny, co umożliwi łatwe wprowadzanie zmian. Utrzymywanie ścisłej współpracy z organami regulacyjnymi i prawnymi w celu monitorowania zmian w przepisach i standardach, które mogą wpłynąć na system. |
| Niewystarczające środki w budżecie na zapewnienie efektów projektu | Średnia | Średnie | Odpowiednio wczesne planowanie środków na zapewnienie utrzymania efektów projektu. Przedstawienie problemu kierownictwu wyższego szczebla. Wygospodarowanie środków z innych zadań realizowanych u Beneficjenta lub podejmowanie działań mających na celu pozyskanie z Ministerstwa Finansów środków na utrzymanie efektów projektu po jego zakończeniu, a także w pozostałym, całym okresie trwałości. |
| Brak zapewnienia odpowiednich zasobów personalnych odpowiedzialnych za rozwój i utrzymanie systemów | Średnia | Średnie | Konieczność zabezpieczenia kadry merytorycznej i informatycznej do utrzymania systemów oraz ich dalszego rozwoju. |
| Nieosiągnięcie wszystkich | Średnia | Niskie | Uruchomienie dodatkowych przedsięwzięć. |

| Nazwa ryzyka | Siła oddziaływania | Prawdopodobieństwo wystąpienia ryzyka | Sposób zarządzania ryzykiem |
|------------------------|--------------------|---------------------------------------|-----------------------------|
| zaplanowanych korzyści | | | |

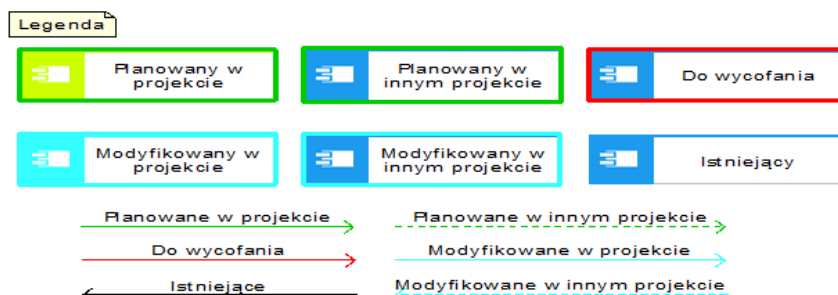
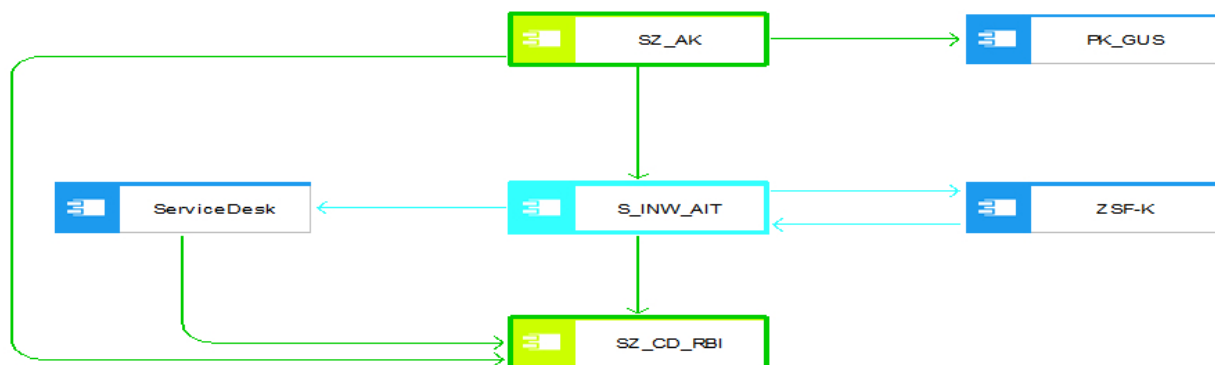
6. OTOCZENIE PRAWNE

| Lp. | Tytuł aktu prawnego | Czy wymaga zmian | Opis zmian (jeśli dotyczy) | Etap prac legislacyjnych (jeśli dotyczy) |
|-----|---|------------------|----------------------------|--|
| 1 | Ustawa z dnia 29 czerwca 1995 r. o statystyce publicznej (Dz. U. z 2024 poz. 17799) | TAK/NIE | | |
| 2 | Dyrektywa 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii (Dyrektywa NIS2) | TAK/NIE | | |
| 3 | Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne. | TAK/NIE | | |
| 4 | Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2024 poz. 773). | TAK/NIE | | |
| 5 | Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 r. poz. 1560, z późn. zm.) | TAK/NIE | | |
| 6 | Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO) | TAK/NIE | | |
| 7 | Ustawa z dnia 28 kwietnia 2022 r. o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021-2027 | TAK/NIE | | |
| 8 | Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 2021/1060 z dnia 24 czerwca 2021 r. | TAK/NIE | | |
| 9 | Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/1058 z dnia 24 czerwca 2021r. ustanawiające wspólne przepisy dotyczące funduszy europejskich | TAK/NIE | | |

| Lp. | Tytuł aktu prawnego | Czy wymaga zmian | Opis zmian (jeśli dotyczy) | Etap prac legislacyjnych (jeśli dotyczy) |
|-----|---|---------------------|----------------------------|--|
| 10 | Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej | TAK /NIE | | |
| 11 | Kodeks postępowania administracyjnego (KPA) z dnia 14 czerwca 1960 r. | TAK /NIE | | |
| 12 | Ustawa z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego | TAK /NIE | | |
| 13 | Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych (Dz. U. 2024 poz. 1254 | TAK /NIE | | |
| 14 | Ustawa z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych | TAK /NIE | | |
| 15 | Ustawa z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych | TAK /NIE | | |
| 16 | Ustawa z dnia 21 listopada 2024 r. o doręczeniach elektronicznych | TAK /NIE | | |
| 17 | Rozporządzenie Ministra Cyfryzacji z dnia 16 czerwca 2021 r. w sprawie profilu zaufanego i podpisu zaufanego | TAK /NIE | | |
| 18 | Rozporządzenie Ministra Cyfryzacji z dnia 10 marca 2020 r. w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system teleinformatyczny służący do uwierzytelniania użytkowników | TAK /NIE | | |
| 19 | Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego | 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 | SZ_AK | Główny Urząd Statystyczny | System zarządzania architekturą korporacyjną (SZ_AK) – system umożliwiający modelowanie, planowanie, nadzór oraz wizualizację architektury korporacyjnej organizacji, z uwzględnieniem architektury bezpieczeństwa informacji, w tym: - modelowanie architektury – tworzenie diagramów i modeli, które odzwierciedlają aktualny stan organizacji (w tym procesów biznesowych i systemów teleinformatycznych); - planowanie transformacji – np. planowanie zmian w | Planowany | Nowy system |

| Lp. | Nazwa systemu | Gestor systemu | Opis systemu | Status | Krótki opis ewentualnej zmiany |
|-----|---------------|---------------------------|---|--------------|---|
| | | | warstwie biznesowej i technologicznej; - mapowanie powiązań – łączenie procesów biznesowych z rozwiązaniami teleinformatycznymi; - zarządzanie repozytorium architektonicznym; - raportowanie i analizy. | | |
| 2 | SerwisDesk | Główny Urząd Statystyczny | System wspierający zarządzanie usługami IT, w tym m.in. zarządzanie incydentami, problemami, wnioskami dotyczącymi tych usług oraz obsługujący zdarzenia dotyczące bezpieczeństwa informacji. System wspomaga monitorowanie postępów prac nad incydemem i eskalacjami zgodnie z ustalonymi poziomami świadczenia usług, informowanie użytkowników o statusie zgłoszenia. System udostępnia użytkownikom informacje o posiadanych aktywach IT. | Istniejący | |
| 3 | S_INW_AIT | Główny Urząd Statystyczny | System inwentaryzacji aktywów IT (S_INW_AIT) – system odpowiadający za inwentaryzację wszystkich aktywów IT w ramach jssp. System składa się z wydzielonych komponentów: - Inwentaryzacja systemów informatycznych; - Inwentaryzacja serwerów, oprogramowania serwerowego oraz urządzeń sieciowych; | Modyfikowany | Uruchomienie komponentu (integracja inwentaryzacji aktywów IT) zapewniającego przedstawienie zintegrowanego, holistycznego i hierarchicznego obrazu aktywów IT wraz z ich |

| Lp. | Nazwa systemu | Gestor systemu | Opis systemu | Status | Krótki opis ewentualnej zmiany |
|-----|---------------|---------------------------|---|-----------|--|
| | | | <ul style="list-style-type: none"> - Inwentaryzacja maszyn wirtualnych - centralna baza aktywów użytkowników (CMDDB). | | powiązaniami (z uwzględnieniem informacji architektonicznej z SZ_AK). Usprawnienie mechanizmów uzgadniania danych inwentaryzacyjnych pomiędzy S_INW_AIT a ZSF-K. |
| 4 | SZ_CD_RBI | Główny Urząd Statystyczny | <p>System zarządzania ciągłością działania i ryzykiem bezpieczeństwa informacji (SZ_CD_RBI) to rozwiązania zapewniające całościowe, zintegrowane wsparcie dla:</p> <ul style="list-style-type: none"> - zarządzania ryzykiem bezpieczeństwa informacji obejmującego w szczególności identyfikację, analizę i minimalizację ryzyka związanego z bezpieczeństwem informacji - integralności, poufności i dostępności danych; - zarządzania ciągłością działania uwzględniającego m.in. przygotowanie organizacji na zakłócenia w funkcjonowaniu, np. takie jak awarie systemów czy cyberataki, aby zapewnić nieprzerwane funkcjonowanie procesów biznesowych i świadczenie usług. - implementacja międzynarodowych standardów, np. takich jak ISO/IEC 27001 (zarządzanie | Planowany | Nowy system |

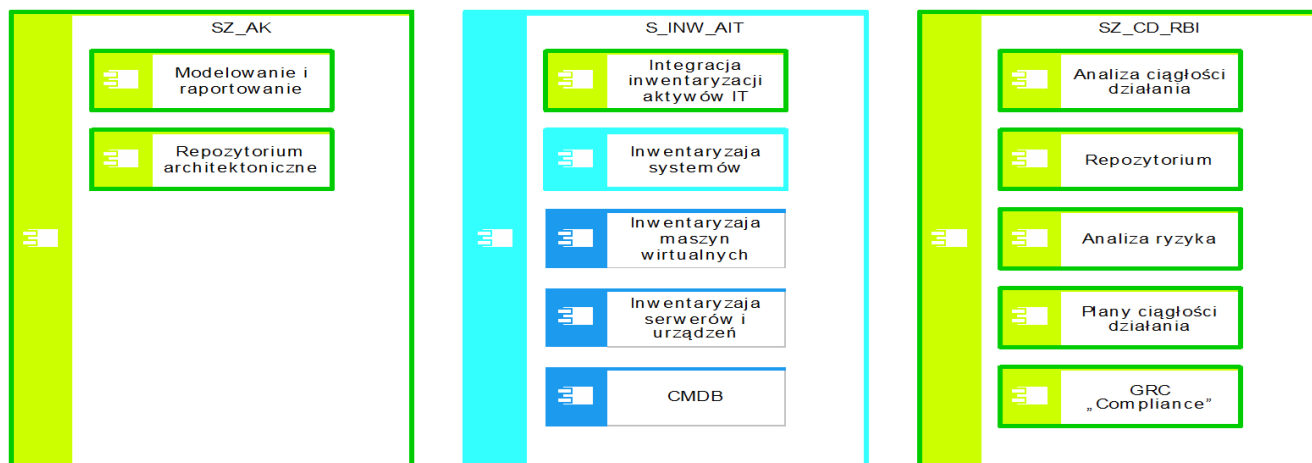
| Lp. | Nazwa systemu | Gestor systemu | Opis systemu | Status | Krótki opis ewentualnej zmiany |
|-----|---------------|---------------------------|---|------------|--------------------------------|
| | | | bezpieczeństwem informacji) oraz ISO 22301 (zarządzanie ciągłością działania) oraz powiązanych regulacji prawnych. | | |
| 5 | PK_GUS | Główny Urząd Statystyczny | Portal korporacyjny – Intranet (PK_GUS) – system zapewniający wewnętrzny serwis informacyjny (informacje korporacyjne, witryny jednostek/ komórek organizacyjnych/ zespołów/ projektów/ linki) oraz środowisko pracy grupowej (dokumenty, harmonogramy, repozytoria, raportowanie). W ramach PK_GUS w wyniku odpowiedniej konfiguracji oraz zasilenia danymi uruchomiona zostanie wewnętrzna e-usługa (A2A) wspierająca zarządzanie architekturą korporacyjną. | Istniejący | |
| 6 | ZSF-K | Główny Urząd Statystyczny | Zintegrowany system finansowo-księgowy (ZSF-K) – system finansowo-księgowy gdzie prowadzona jest m.in. ewidencja środków trwałych. | Istniejący | |

Lista przepływów

| Lp. | System źródłowy | System docelowy | Zakres wymienianych danych | Sposób wymiany danych | Typ modyfikacji | Typ interfejsu |
|-----|-----------------|-----------------|---|-----------------------|--------------------------------|-----------------------------|
| 1 | SZ_AK | PK_GUS | obiekty architektury korporacyjnej, w tym | kopiowanie danych | krytyczny dla sukcesu projektu | format wymiany danych: text |

| Lp. | System źródłowy | System docelowy | Zakres wymienianych danych | Sposób wymiany danych | Typ modyfikacji | Typ interfejsu |
|-----|-----------------|-----------------|--|-----------------------|--------------------------------|-----------------------------|
| | | | architektury bezpieczeństwa informacji | | | |
| 2 | SZ_AK | S_INW_AIT | obiekty architektury korporacyjnej, w tym architektury bezpieczeństwa informacji | kopiowanie danych | krytyczny dla sukcesu projektu | format wymiany danych: text |
| 3 | SZ_AK | SZ_CD_RBI | obiekty architektury korporacyjnej, w tym architektury bezpieczeństwa informacji | kopiowanie danych | krytyczny dla sukcesu projektu | format wymiany danych: text |
| 4 | S_INW_AIT | SZ_CD_RBI | aktywa IT wraz z powiązaniem | kopiowanie danych | krytyczny dla sukcesu projektu | format wymiany danych: text |
| 5 | ServiceDesk | SZ_CD_RBI | opis incydentu | kopiowanie danych | krytyczny dla sukcesu projektu | format wymiany danych: text |
| 6 | S_INW_AIT | ServiceDesk | aktywa IT wraz z powiązaniem | kopiowanie danych | krytyczny dla sukcesu projektu | format wymiany danych: text |
| 7 | S_INW_AIT | ZSF-K | aktywa IT wymagające korekty w ewidencji środków trwałych | kopiowanie danych | krytyczny dla sukcesu projektu | format wymiany danych: text |
| 8 | ZSF-K | S_INW_AIT | środki trwałe będące aktywami IT | kopiowanie danych | krytyczny dla sukcesu projektu | format wymiany danych: text |

7.2. Kluczowe komponenty architektury rozwiązania



7.3. Przyjęte założenia technologiczne

| Lp. | Obszar | Założenie technologiczne |
|-----|------------------------------|---|
| 1. | Infrastruktura | Dla wdrażanych aplikacji, systemów i baz danych wykorzystana będzie posiadana scentralizowana infrastruktura (ICT) wraz z platformą wirtualizacyjną Vmware w aktualnej wersji vCenter 8.0.2 |
| 2. | Sieć i bezpieczeństwo | Zapewnione przez wdrożone i funkcjonujące w infrastrukturze Wnioskodawcy systemy bezpieczeństwa |
| 3. | Standardy wymiany danych | - |
| 4. | Systemy operacyjne serwerowe | - |
| 5. | Bazy danych | - |
| 6. | Serwery aplikacji | Wirtualne, utworzone w platformie wirtualizacyjnej Vmware |
| 7. | Portale | Wykorzystanie portalu korporacyjnego (Intranet) |
| 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~~