*Załącznik do KARTY OCENY ZAŁOŻEŃ PROJEKTU INFORMATYCZNEGO NR 457*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***Nazwa dokumentu:*** *Opis założeń projektu informatycznego pn.* ***„Rozbudowa systemu zarządzania infrastrukturą teleinformatyczną statystyki publicznej i cyberbezpieczeństwa (CyberStat)” –*** wnioskodawca: Kancelaria Prezesa Rady Ministrów, beneficjent: Główny Urząd Statystyczny | | | | | |
| **Lp.** | **Organ wnoszący uwagi** | **Jednostka redakcyjna, do której wnoszone są uwagi** | **Treść uwagi** | **Propozycja zmian zapisu** | **Odniesienie do uwagi** |
|  | **RA IT** | 1.1. Identyfikacja problemu i potrzeb | W opisie wskazano „*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)*”. Biorąc pod uwagę iż rejestry te nie będą przedmiotem modyfikacji w projekcie niniejsze może być mylące. Zamiast sugerować, że projekt usprawnia REGON i TERYT, można podkreślić, że poprawia ogólne bezpieczeństwo infrastruktury, na której one działają. | Proszę o analizę i korektę opisu założeń | Uwaga przyjęta, dokonano modyfikacji opisu założeń projektu informatycznego (zwanego dalej „**OZPI**”) dla projektu CyberStat. |
|  | **RA IT** | 1.1. Identyfikacja problemu i potrzeb | W tabeli interesariuszy przy grupie „*Pracownicy jednostek służb statystyki publicznej (jssp) zajmujący się zarządzaniem IT i bezpieczeństwem informacji” w identyfikacji problemu wskazano na „Utrudnione zarządzanie, wdrożonym w ramach projektu KSZBI, Systemem 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.*”  Czy oznacza to, że projekt KSZBI nie dostarczył odpowiednich narzędzi lub nie przewidziano tak dużej skali analiz w momencie jego wdrażania? Czy pierwotnie zakładano, że analiza wpływu awarii i zarządzanie ryzykiem będą realizowane w sposób rozproszony, czy też obecne trudności wynikają z niedostatecznej integracji wdrożonych w 2022 roku narzędzi? Czy na etapie wdrażania przewidywano konieczność skorelowania tych procesów z innymi poziomami organizacyjnymi? Jeśli tak, to jakie były główne przeszkody, które uniemożliwiły pełną integrację? | Proszę o doprecyzowanie/wyjaśnienie | Projekt KSZBI miał zdefiniowany i zaplanowany ściśle określony zakres - jak każdy projekt. Celem projektu było podniesienie bezpieczeństwa poprzez zastosowanie rozwiązań technicznych, uzupełniających stosowane dotąd, fizyczne urządzenia i dedykowane oprogramowanie (SIEM, WAF, WEB-GATEWAY, ATP); przeglądy i audyt bezpieczeństwa, opracowanie, weryfikację oraz aktualizację dokumentów Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).  Czyli nie były zaplanowane narzędzia wspomagające analizę BIA czy ryzyka – projekt w tym zakresie koncentrował się na przygotowaniu dokumentacji SZBI, odpowiednich procedur. I w takim zakresie projekt został zrealizowany. Nie planowano w projekcie KSZBI w tym zakresie wsparcia narzędziowego. W ramach jednego projektu nie było możliwe zrealizowanie wszystkich potrzeb w obszarze zarządzania IT i bezpieczeństwa informacji. Dlatego widzimy konieczność kontynuacji tych działań i rozwoju naszego SZI – co jest zgodne z normą ISO/IEC 27001, która zakłada ciągłe doskonalenie SZBI. |
|  | **RA IT** | 1.1. Identyfikacja problemu i potrzeb | Projekt CyberStat identyfikuje sześć głównych grup interesariuszy, z których trzy to pracownicy jednostek służb statystyki publicznej (jssp), co wynika z zakresu przedsięwzięcia. Wiele problemów przypisanych poszczególnym grupom powtarza się, co może sugerować niewystarczającą analizę ich rzeczywistych potrzeb. Szczególne wątpliwości budzi jednak traktowanie obywateli i przedsiębiorców jako interesariuszy, zwłaszcza że ich potrzeby nie zostały precyzyjnie określone. Ponieważ projekt koncentruje się na cyfryzacji procesów wewnętrznych administracji (back-office), obie te grupy powinny być raczej klasyfikowane jako interesariusze pośredni. Choć modernizacja infrastruktury może pośrednio poprawić stabilność i bezpieczeństwo systemów, nie stanowi głównego celu projektu, a jej wpływ na obywateli i przedsiębiorców wydaje się być drugorzędny. | Proszę o analizę i ewentualną korektę opisu założeń lub wyjaśnienia | Uwaga nie została przyjęta, poniżej przedstawiono krótkie wyjaśnienie.  Jeśli problem dotyczy wszystkich przedstawicieli danej populacji, w ramach której wyodrębniono rozłączne grupy interesariuszy (żaden z przedstawicieli jednej grupy nie może być ujęty innej grupie), wtedy nieuniknione jest wspomniane powtarzanie problemów, tj. przypisywanie danego problemu do wielu grup interesariuszy.  Wnioskodawcy nie są znane wytyczne dot. opracowania OZPI, z których wynikało by, że interesariuszy należałoby w jakiś sposób wartościować (np.: główni/ ważniejsi/ mniej ważni/ pośredni).  Projekt koncentruje się na cyfryzacji procesów wewnętrznych administracji (back-office), w szczególności po to, aby podnieść poziom cyberbezpieczeństwa usług świadczonych obywatelom, przedsiębiorcom i administracji. |
|  | **RA IT** | 2.1. Cele i korzyści wynikające z projektu | Dla obu celów projektowych jako cel strategiczny wskazano Projekt Strategii Cyfryzacji Polski do 2035 roku, w szczególności obszar horyzontalny 1.3 – Cyberbezpieczeństwo. Należy jednak zaznaczyć, że dokument ten nie został jeszcze przyjęty i pozostaje jedynie projektem, co słusznie zauważył Beneficjent. W tym polu powinny zostać wymienione obowiązujące na dzień opracowywania dokumentu strategie, programy strategiczne, etc. | Proszę o korektę opisu założeń | Uwaga przyjęta, dokonano modyfikacji OZPI. |
|  | **RA IT** | 2.1. Cele i korzyści wynikające z projektu | Wskaźniki ograniczają się do tych obowiązkowych, nie uwzględniając dodatkowych, które pozwalałyby na pełniejszą ocenę rzeczywistego wpływu projektu na organizację oraz użytkowników końcowych. Warto rozważyć rozszerzenie katalogu wskaźników, w tym dodanie KPI związanych z liczbą transakcji przeprowadzonych w systemie, co umożliwiłoby lepszą ocenę efektywności projektu.  Odnosząc się do wartości docelowej wskaźnika: "*Użytkownicy nowych i zmodernizowanych publicznych usług, produktów i procesów cyfrowych*", ponieważ projekt dotyczy głównie usług wewnątrzadministracyjnych, należy zweryfikować wartość docelową wskaźnika. W metodzie pomiaru wskazano użytkowników Portalu Korporacyjnego (Intranet), w szczególności witryny „Portal Architektury Korporacyjnej”, świadczącej wewnętrzną e-usługę (A2A) wspierającą zarządzanie architekturą IT. Jednak zaplanowana wartość 400 użytkowników wydaje się niedoszacowana w kontekście liczby interesariuszy z grupy Pracownicy jednostek służb statystyki publicznej.  Wskaźniki w zakresie celu 2 biorąc pod uwagę koszt szkoleń, a także liczbę interesariuszy również zdają się być niedoszacowane. | Proszę o analizę i wyjaśnienie | Uwaga dot. rozszerzenia katalogu wskaźników została przyjęta - zaproponowano wprowadzenie dodatkowego wskaźnika KPI 5 „*Liczba transakcji w udostępnionej usłudze wewnątrzadministracyjnej wspierającej zarządzanie architekturą korporacyjną*”.  Poniżej przedstawiono wyjaśnienia dla pozostałych uwag.  Wskaźnik dotyczy wewnętrznej e-usługi (A2A) wspierającej zarządzanie architekturą korporacyjną. Usługa ta będzie dostępna dla wszystkich pracowników, jednakże należy mieć na uwadze, że nie wszyscy pracownicy jssp będą aktywnie uczestniczyć w pracach dot. zarządzania architekturą korporacyjną. W tym kontekście wartość wskaźnika wydaje się ambitna, ale również osiągalna.  W opisie wskaźników: *Liczba pracowników IT objętych wsparciem szkoleniowym* oraz *Liczba pracowników nie będących pracownikami IT*, objętych wsparciem szkoleniowym w zakresie celu 2 wskazane są osoby, którym podnoszone będą kompetencje z zakresu ICT. Łącznie planowana jest seria 26 szkoleń, dla 765 uczestników.  Zgodnie z wytycznymi w zakresie ustalenia wartości docelowej wskaźników osoby, które będą uczestniczyły w kilku szkoleniach powinny być liczone tylko raz (niezależnie od liczby szkoleń, w których uczestniczą).  Biorąc pod uwagę powyższe, wartości wskaźników są ustalone na niższym poziomie niż to wynika z sumy osób uczestniczących we wszystkich szkoleniach. |
|  | **RA IT** | 2.4. Produkty końcowe projektu | W zakresie produktów wątpliwości budzi zakres niektórych komponentów infrastrukturalnych, w szczególności infrastruktury klucza publicznego, centrum certyfikacji oraz urządzeń HSM, których powiązanie z założeniami projektu nie zostało dostatecznie wyjaśnione. Podobnie niejasna jest ponowna inwestycja w WAF (Web Application Firewall), który był już produktem wcześniejszego projektu.  Warto również rozważyć różne daty wdrożenia poszczególnych systemów, co pozwoliłoby na ich dokładniejsze przetestowanie i przeprowadzenie rzetelnego odbioru. Obecnie 6 z 9 produktów zaplanowano na ostatni miesiąc projektu (wrzesień 2028), co niesie ryzyko problemów z integracją z obecnymi systemami oraz ogranicza możliwość wprowadzania ewentualnych poprawek. Zaleca się etapowe wdrażanie systemów i wyraźne rozróżnienie między datą odbioru systemów a terminem zakończenia testów. | Proszę o analizę i korektę opisu założeń | W sekcji 1.1 OZPI poinformowano, że projekt przewiduje m.in. modernizację infrastruktury technicznej wspierającej bezpieczeństwo informacji oraz podano kontekst tej modernizacji.  Aby uniknąć ew. wątpliwości do nazwy produktu: „*Modernizacja infrastruktury technicznej*” dodano „*związanej z cyberbezpieczeństwem*”.  Należy zwrócić uwagę, że praktycznie każde z zaawansowanych rozwiązań teleinformatycznych ma określony cykl życia, z czego m.in. wynika potrzeba modernizacji WAF.  Uwaga przyjęta, dokonano modyfikacji OZPI, zmodyfikowano terminy wdrożenia produktów. |
|  | **RA IT** | 3. Kamienie milowe | Kamienie milowe powinny pozwalać na monitorowe poszczególnych etapów projektu. Przyjęty harmonogram wymaga dopracowania.  Dokumentacja przetargowa na wybór Inżyniera Projektu ma być gotowa dopiero 31.03.2026, mimo że projekt zakłada rozpoczęcie już w październiku 2025 r., może to skutkować problemami z nadzorem nad realizacją w początkowej fazie.  Zbyt krótki czas na realizację systemów – dokumentacja przetargowa na system zarządzania architekturą korporacyjną (SZ\_AK) ma być opracowana do 31.03.2027, co oznacza, że na przeprowadzenie przetargu oraz wdrożenie systemu pozostaje niespełna 1,5 roku. Jest to znaczące ryzyko dla terminowej realizacji projektu.  Niejasne działania w pierwszych 1,5 roku projektu – oprócz szkoleń i przygotowania dokumentacji przetargowej brak szczegółowych informacji na temat działań planowanych do końca I kwartału 2027 r.  Brak wyszczególnienia przetargu na infrastrukturę sprzętową, która wydaje się iż stanowi istotny element projektu, jednak nie została ujęta jako osobny kamień milowy.  Ponadto należy rozważyć zmianę sposobu określania kamieni milowych – zamiast wskazywania terminu opracowania dokumentacji przetargowej, bardziej adekwatne byłoby uwzględnienie terminu rozstrzygnięcia przetargów, co dałoby realny obraz postępu projektu. | Proszę o analizę i korektę opisu założeń | Uwaga przyjęta, dokonano modyfikacji OZPI. |
|  | **RA IT** | 4.1. Koszty ogólne projektu wraz ze sposobem finansowania | Najwyższe koszty projektu przewidziano na rok 2026 (34 317 577,20 zł brutto) podczas gdy w tym okresie nie zaplanowano realizacji kluczowych produktów ani kamieni milowych – poza szkoleniami i wyborem Inżyniera Projektu. Budzi to wątpliwości co do prawidłowego podziału całkowitych kosztów projektu na poszczególne lata. | Proszę o analizę i korektę opisu założeń | Uwaga przyjęta, dokonano modyfikacji OZPI. |
|  | **RA IT** | 4.2. Wykaz poszczególnych pozycji kosztowych | Zastrzeżenia dotyczą alokacji środków w poszczególnych kategoriach wydatków:  - Wynagrodzenia pracowników merytorycznych jssp zostały uwzględnione w kosztach infrastruktury, co wydaje się być nieuzasadnione. Ponadto, wynagrodzenia dla członków zespołu projektowego znalazły się również w pozycji „Oprogramowanie”, co może sugerować podwójne finansowanie niektórych zadań.  - 3,2 mln zł na szkolenia to znaczna kwota w kontekście stosunkowo niewielkiej liczby przeszkolonych osób. Warto doprecyzować, jakie elementy składają się na tę sumę i czy obejmuje ona np. materiały szkoleniowe, platformy e-learningowe lub certyfikacje. | Proszę o analizę i ewentualną korektę opisu założeń lub wyjaśnienia | W odniesieniu do zastrzeżeń dotyczących wydatków w kategorii wynagrodzenia pracowników merytorycznych wyjaśniamy, że:  - w pozycji Infrastruktura znalazły się koszty wynagrodzeń pracowników merytorycznych związanych z pracami w zakresie modernizacji infrastruktury,  - w pozycji oprogramowanie znalazły się koszty wynagrodzeń pracowników 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.  Nie ma więc niebezpieczeństwa podwójnego finansowania zadań ponieważ zadania ujęte w pozycji Infrastruktura są rozdzielne z pozycją Oprogramowanie.    W odniesieniu do zastrzeżeń dotyczących wydatków w kategorii szkolenia wyjaśniamy, że łącznie planowana jest seria 26 szkoleń dla 765 uczestników.  Koszty szkoleń oprócz udziału uczestników obejmują również materiały szkoleniowe, certyfikacje, delegacje, w tym opłaty za hotel.  Te same osoby będą uczestniczyły w różnych szkoleniach, natomiast zgodnie z wytycznymi w zakresie ustalania wartości wskaźników, mogą być liczone wówczas tylko raz (pomimo uczestnictwa np. w 10 szkoleniach).  W opisie wskaźników jest określone aby wskazywać jedynie osoby, którym podniesiono kompetencje z zakresu ICT.  Dlatego wskaźniki są ustalone na niższym poziomie. |
|  | **RA IT** | 7.3. Przyjęte założenia technologiczne | Ponieważ projekt stanowi kontynuację wcześniejszych działań, zaleca się pełniejsze uzupełnienie założeń technologicznych, zwłaszcza w obszarach Infrastruktury IT oraz Sieci i cyberbezpieczeństwa – określenie standardów zabezpieczeń, szczególnie w kontekście integracji z istniejącymi systemami i nowymi wymaganiami regulacyjnymi. | Proszę o analizę i ewentualną korektę opisu założeń | Uwaga przyjęta, dokonano modyfikacji OZPI. |