

Wstępne Konsultacje Rynkowe na usługę budowy i utrzymania systemu informatycznego dla Inspekcji Weterynaryjnej

Warszawa 5 marca 2021r.



- O NASK
- ZARZĄDZANIE PROJEKTEM
- HARMONGRAM i BUDŻET
- WYMAGANIA DOT. WYKONAWCÓW
- ISTOTNE KWESTIE W UMOWACH
- TESTOWANIE i WDRAŻANIE
- ARCHITEKTURA i ZAGADNIENIA TECHNICZNE
- SZKOLENIA i HELPDESK



O NASK

NASK Państwowy Instytut Badawczy

Misja: poszukiwanie i wdrażanie rozwiązań, służących rozwojowi sieci teleinformatycznych w Polsce oraz poprawie ich efektywności i bezpieczeństwa.

Działania: badania naukowe, prace rozwojowe, działalność operacyjna na rzecz bezpieczeństwa polskiej cywilnej cyberprzestrzeni, a także edukacja użytkowników oraz promowanie koncepcji społeczeństwa informacyjnego, głównie w celu ochrony dzieci i młodzieży przed zagrożeniami, związanymi z użytkowaniem nowych technologii.

Kompetencje i Doświadczenie:

Telekomunikacja - wieloletnie doświadczenie operatorskie (pełen zakres usług telekomunikacyjnych z zachowaniem niezawodności, szybkości i bezpieczeństwa).

Bezpieczeństwo – audyty bezpieczeństwa, wdrażanie mechanizmów uwierzytelniania, zapory sieciowe na styku z Internetem, ochrona przed atakami typu DDOS.

Wsparcie inżynierskie – przy optymalnej budowie środowiska teleinformatycznego organizacji oraz na każdym etapie przygotowania, uruchomienia i utrzymania usług.

Bezpieczeństwo informacji – wsparcie przy opracowaniu PBI zgodnie z normami i standardami.



ZARZĄDZANIE PROJEKTEM – METODYKA, ZESPOŁY

Koncepcja **zarządzania projektem** powinna zostać oparta na metodyce PRINCE 2:

- projekt złożony
- długi ale precyzyjnie określony czas realizacji projektu
- określone precyzyjnie produkty,
- wymagania formalne związane z dofinansowaniem UE

Na **poziomie realizacji** iteracyjnych procesów wytwórczych powinny zostać wykorzystane elementy metodyk zwinnych (agile) np. SCRUM

- stałymi w metodologii zwinnej są budżet, czas i jakość, zmienne za to są wymagania (zakres), które są na bieżąco priorytetyzowane przez partnerów,
- zaangażowanie użytkowników końcowych do współpracy w procesie wytwórczym oprogramowania, zapoznanie ich z nowymi funkcjami na makietach i prototypach, testowanie funkcjonalne oraz częste interakcje z zespołem wytwórczym, sprzyjając będą lepszemu zrozumieniu potrzeb, różnego rodzaju uwarunkowań (w tym uwarunkowań, które z różnych powodów mogą ulec zmianie) użytkowników co zapewni wytworzenie rozwiązania możliwie bliskiego ich oczekiwaniom.

Lp.	Poziom	Opis
1.	Zarządzanie strategiczne	Poziom Komitetu Sterującego odpowiada za sukces projektu. KS zatwierdza główne plany i zasoby, rozpatruje i zatwierdza odchylenia, zatwierdza zakończenie etapów, komunikuje się z pozostałymi interesariuszami. Przewodniczący KS przedstawiciel GIW a członkowie KS to odpowiednio przedstawiciele Użytkowników, Dostawców i Właścicieli Biznesowych. W przypadku działań angażujących inne podmioty (zewnętrzne) ich przedstawiciele powinni być włączani do KS.
2.	Zarządzanie operacyjne	Poziom Kierownika Projektu, który powinien być wyznaczony przez GIW, odpowiada za codzienne zarządzanie projektem w granicach wyznaczonych przez KS. Obowiązkiem KP jest, żeby projekt wytwarzał wymagane produkty zgodnie z ustalonymi wskaźnikami (zakres, jakość, termin, koszt). W przypadku projektu IW System warto rozważyć zaangażowanie w zarządzanie operacyjne również przedstawiciela/li innych niż GIW szczebli Inspekcji – np. jeśli chodzi o zakres szkoleń i wdrożeń.
3.	Dostarczanie produktów	Poziom Liderów Zespołów/obszarów, którzy są odpowiedzialni za wytworzenie odpowiednich produktów.



ZARZĄDZANIE PROJEKTEM – METODYKA, ZESPOŁY

Istotnym elementem zarządzania projektem będą kwestie komunikacji tj. plan i zakres spotkań oraz raportowanie zarządcze i statusowe.

W projekcie powinny być zaplanowane regularne spotkania projektowe:

Lp	Spotkanie	Organizator	Cel	Zakres	Częstotliwość
1.	Komitet Sterujący	Kierownik Projektu	Uzyskanie decyzji dot. realizacji kolejnych etapów zarządczych	Status prac projektowych Kluczowe decyzje (wykraczających poza uprawnienia Kierownika Projektu) Eskalacje Przegląd ryzyka	1 x miesiąc (docelowo po osiągnięciu wyższego poziomu dojrzałości projektowej KS powinien być zwoływany w terminach Etapów Zarządczych)
2.	Status projektu	Kierownik Projektu	Monitorowanie realizacji prac w projektowych projekcie Wyrównanie poziomu wiedzy członków zespołu	Status prac projektowych Decyzje Eskalacje	2 x miesiąc
3.	Status zespołu	Lider Zespołu	Monitorowanie realizacji prac w zespole Wyrównanie poziomu wiedzy członków zespołu	Status prac projektowych	1 x tydzień

Istotnym elementem zarządzania w części dotyczącej komunikacji są decyzje i eskalacje. Potrzeba podjęcia w projekcie decyzji lub eskalacji zgłaszana jest w ramach spotkań projektowych lub w raportach. Eskalacje i prośby o decyzję muszą być wyraźnie wskazywane.

Wnioski o podjęcie decyzji powinny zawierać możliwe warianty, wraz ze wskazaniem rekomendowanego.

Eskalacje powinny być przekazywane wraz z wskazaniem dotychczasowych reakcji na zagadnienie.

Zagadnienia, w tym problemy eskalowane będą „do góry” po szczeblach zarządczych, a decyzje „do dołu”.

Eskalowane są zagadnienia będące poza poziomem tolerancji dla danego szczebla zarządczego.



ZARZĄDZANIE PROJEKTEM – METODYKA, ZESPOŁY

Kolejnym istotnym elementem komunikacji jest raportowanie.

Formę raportowania oraz zakres informacyjny ustala Kierownik Projektu, a w zespołach ich liderzy. Propozycja :

Lp	Raport	Częstotliwość	Autor	Odbiorca
1.	Raport okresowy projektu	1 x tydzień	Kierownik Projektu	Komitety Sterujące Interesariusze
2.	Raport końcowy projektu	Na zakończenie projektu	Kierownik Projektu	Komitety Sterujące Interesariusze
3.	Raport końcowy etapu	Na zakończenie każdego Etapu (za wyjątkiem ostatniego)	Kierownik Projektu	Komitety Sterujące Interesariusze
4.	Raport zespołu	1 x tydzień	Lider Zespołu	Kierownik Projektu
5.	Raport rzeczowo-finansowy	1 x kwartał	Kierownik Projektu	Instytucja nadzorująca program w ramach, którego będzie realizowany projekt



ZARZĄDZANIE PROJEKTEM – METODYKA, ZESPOŁY

Proponowane składy zespołów po stronie Zamawiającego i Wykonawcy
(zakładamy, rekomendujemy wybór po stronie ZAMAWIAJĄCEGO firmy
doradczej/wsparcia/consulting

ZAMAWIAJĄCY

Rola	Liczba etatów
Kierownik Projektu	1
Analitik Biznesowy	2
Architekt Biznesowy	2
Tester UAT	2
Obsługa service desk	3
Obsługa Projektu	4 <ul style="list-style-type: none">• Biuro projektu - dokumentacja• Finanse, księgowość, kadry• Obsługa prawna oraz zamówienia publiczne• Wsparcie organizacji promocji• Wsparcie organizacji i prowadzenia szkoleń

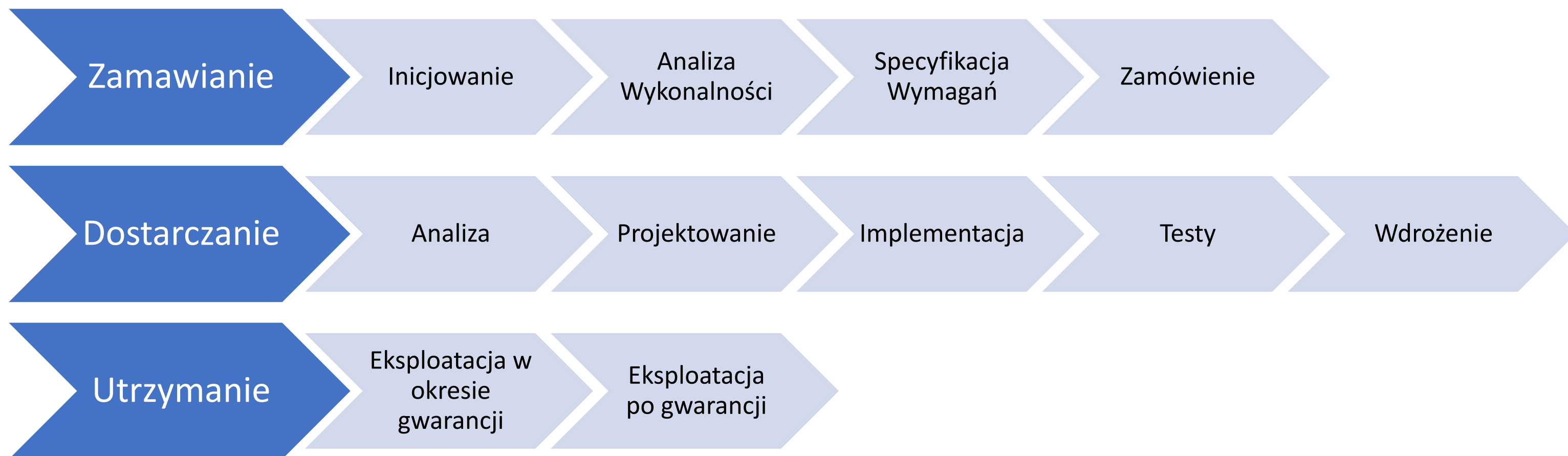
WYKONAWCA

Lp.	Rola	Liczba etatów
1	Główny Architekt	1
2	Główny Analitik Biznesowy	1
3	Kierownik Projektu	1
4	Zastępca Kierownika Projektu	1
5	Właściciel rozwiązania	1
6	Scrum Master	1
7	Analitik biznesowy	1
8	Analitik systemowy	1
9	Programista	2
10	Starszy programista	3
11	Tester automatyczny	1
12	Tester	1
13	Architekt IT	1
14	Ekspert przygotowania procedur	1



HARMONOGRAM I BUDŻET

Kroki procesu wytwórczego





HARMONOGRAM I BUDŻET

Etapy i terminy realizacji (harmonogram w podziale co najmniej na etap uzgodnień, realizacji, wdrożenia, uruchomienia)

Numer Etapu Technicznego	Ogólny zakres Etapu technicznego	Maksymalny czas zakończenia	Koszt etapu
Etap Zarządczy nr 1			
Etap 1	Opracowanie zasad organizacji i zarządzania realizacją Umowy.	30 dni od zawarcia Umowy	10% wartości Umowy
Etap Zarządczy nr 2			
Etap 2	Analiza przedwdrożeniowa – obejmuje przygotowanie: <ul style="list-style-type: none">architektury systemu wraz ze wstępnymi strukturami danych;listy wymagań z określeniem ich priorytetów;backlogu produktu dla całego zamówienia z ewentualnym podziałem dla poszczególnych zespołów realizacyjnych – DevTeam	5 mies. od zawarcia Umowy	30% wartości Umowy
Etap Zarządczy nr 3 - Etapy techniczne w ramach tego etapu realizowane są równolegle			
Etap 3	Realizacja prac w sposób przyrostowy w metodyce zwinnej wraz z prezentacją przyrostu Zamawiającemu – w razie potrzeby etap można podzielić na kilka równoległych etapów technicznych dla zespołów developerskich	Wymagany termin zakończenia realizacji umowy (2022-10)	50% wartości Umowy
Etap 4	Czyszczenie danych, wdrażanie docelowego modelu, migracje,	Wymagany termin zakończenia realizacji umowy (2022-10)	10% wartości Umowy
Etap 5	Administracja techniczna - realizowana na podstawie aktualnych potrzeb Zamawiającego	np. maksymalnie 1500 roboczogodzin	1500 rbh rozliczane wg stawki za roboczogodzinę



WYMAGANIA DOTYCZĄCE WYKONAWCÓW

Doświadczenie Wykonawcy i wymagania dotyczące osób planowanych do realizacji zamówienia i ich doświadczenia

Wykonawca powinien mieć doświadczenie :

- w realizacji dużych projektów usługowych powyżej 5 mln zł (nie dostaw),
- we współpracy z administracją publiczną,
- w realizacji projektów przekrojowych dotyczących wsparcia instytucji w realizacji procesów wewnętrznych (zarządzanie instytucją) oraz procesów biznesowych w tym związanych z informacją przestrzenną
- w realizacji projektów dotyczących rozwiązań integrujących wiele jednostek, wiele poziomów administracji oraz beneficjentów (podmioty, osoby fizyczne)

Wykonawca powinien dysponować osobami :

- Kierownika Projektu
- Architekta rozwiązań (w tym w zakresie rozwiązań GIS)
- Analityka biznesowego
- Analityka danych
- Eksperta ds. bezpieczeństwa
- Eksperta ds. wdrożeń



WYMAGANIA DOTYCZĄCE WYKONAWCÓW

Wymagania dotyczące osób planowanych do realizacji zamówienia i ich doświadczenia

Przykłady wymagań dla wybranych ról/osób planowanych do realizacji zamówienia

Kierownik projektu:

- a) posiada wykształcenie wyższe;
- b) w okresie ostatnich 5 lat przed terminem składania ofert brał udział jako kierownik projektu w co najmniej 3 projektach informatycznych, zakończonych do dnia składania ofert, których każdego przedmiotem była budowa lub rozbudowa systemów informatycznych, z których co najmniej jeden był o wartości minimum 5 000 000,00 zł brutto;
- c) posiada znajomość zasad zarządzania projektami zgodnie z metodyką powszechnie stosowaną (stosowanie nie wymaga opłat autorskich) i publicznie dostępną (opis metodyki jest opublikowany i szeroko dostępny), która stanowi zbiór reguł i zasad postępowania, stanowiący spójne pojęciowo podejście do wykonywania i zarządzania projektem oraz umożliwia adaptację do specjalnych potrzeb organizacji, programu lub projektu.

Analitik biznesowy / analitik systemowy:

- a) posiada wykształcenie wyższe;
- b) w okresie ostatnich 3 lat przed terminem składania ofert brał udział w co najmniej 2 projektach w zakresie prowadzenia analizy systemów związanych z przetwarzaniem i wizualizacją dużej ilości rozproszonych danych w tym danych przestrzennych;

- c) w okresie ostatnich 3 lat przed terminem składania ofert brał udział w co najmniej 2 projektach, w których zbierał i specyfikował wymagania oraz modelował artefakty analityczne z zastosowaniem notacji UML i/lub BPMN,
- d) posiada doświadczenie w posługiwaniu się oprogramowaniem służącym do modelowania architektury;
- e) w okresie ostatnich 3 lat przed terminem składania ofert wykonywał analizy biznesowe lub systemowe w co najmniej 2 projektach informatycznych, zakończonych do dnia składania ofert, polegających na budowie bazodanowych systemów informatycznych zawierających podsystem GIS, z których co najmniej jeden był o wartości minimum 1 000 000,00 zł brutto.

Analitik danych / ekspert w zakresie przetwarzania danych, projektowania baz danych:

- a) posiada potwierdzone doświadczenie w budowie baz danych w tym baz danych przestrzennych (WebGIS)
- b) posiada potwierdzone doświadczenie w posługiwaniu się narzędziami klasy ETL potwierdzone udziałem w co najmniej 1 zamówieniu polegającym na pozyskaniu danych dla baz danych z użyciem narzędzia klasy ETL,



WYMAGANIA DOTYCZĄCE WYKONAWCÓW

Kryteria oceny ofert

Czy w ramach kryteriów powinna być konieczność przygotowania/zaprezentowania próbki rozwiązań i jeśli tak, to w jakim zakresie

Z uwagi na to, że planowany system będzie rozwiązaniem pod konkretne potrzeby, ponadto dużą rolę w jego prawidłowym funkcjonowaniu będą miały kwestie dotyczące wykorzystania danych i usług udostępnianych z innych systemów, platform, ewentualne próbki powinny ograniczać się do prezentacji wybranych, kluczowych dla Zamawiającego komponentów lub scenariusze dotyczących wykorzystania danych za pomocą usług, świadczonych przez inne rozwiązania.

Czy w ramach kryteriów powinna być gwarancja na SLA świadczonych usług czy dostarczonych rozwiązań aplikacyjnych

SLA powinno być zdefiniowane jako kryterium z ograniczeniem górnego progu co do zakresu i okresu obowiązywania i wynikających z tego punktów. Powinien być również zdefiniowany poziom minimum i powinien on odpowiadać zwykłym potrzebom Zamawiającego wynikającym z oczekiwań w stosunku do czasów reakcji i usuwania problemów w związku z realizowanymi przez system zadaniami.

Jako dodatkowe poza-cenowe kryteria oceny ofert warto rozważyć kwestie związane z :

- doświadczeniem polegającym na wykonaniu w przeszłości wysokiej jakości usług zbliżonych do obecnego Zamówienia np. w obszarze budowy rozwiązań korzystających z usług innych podmiotów administracji, bezpieczeństwa rozwiązań, wydajności i skalowalności, poprzez opisanie w koncepcji realizacji zamówienia sposobu podejścia do realizacji zamówienia w zakresie określonym przez zamawiającego,
- kompetencjami i doświadczeniem osób biorących udział w realizacji zamówienia w obszarze działania inspekcji weterynaryjnej czy chociażby szerzej w obszarze rolnictwa i administracji publicznej



ISTOTNE KWESTIE W UMOWACH

Warunki rękojmi i gwarancji

- Wykonawca udziela gwarancji na każdy Produkt od dnia podpisania Protokołu Odbioru Produktu lub Protokołu Etapu do upływu okresu miesięcy od dnia podpisania ostatniego Protokołu Odbioru Końcowego Umowy.
- Udzielona przez Wykonawcę gwarancja obejmuje poprawne działanie Systemu IW, zgodnie z wymaganiami funkcjonalnymi, technicznymi i organizacyjnymi określonymi w Umowie oraz poprawność i kompletność Dokumentacji odzwierciedlającej stan rzeczywisty Systemu.
- Przez okres gwarancji Wykonawca będzie usuwał wszelkie wady i usterki w Oprogramowaniu oraz aktualizował Dokumentację.
- Gwarancją nie są objęte wady i usterki będące następstwem:
 - ✓ zmian dokonanych w Systemie IW przez Zamawiającego lub przez osoby trzecie bez autoryzacji Wykonawcy;
 - ✓ usterek bądź nieprawidłowego działania sprzętu komputerowego lub oprogramowania współdziałającego z Oprogramowaniem lub zainstalowanego na sprzęcie komputerowym, a nie stworzonego (dedykowanego) lub standardowego dostarczonego przez Wykonawcę;
 - ✓ usterek bądź nieprawidłowego działania sieci komputerowej lub brakiem odpowiedniej przepustowości łącz;
 - ✓ działania czynników zewnętrznych, jak zwarcia instalacji elektrycznej;
 - ✓ zmian w parametryzacji Oprogramowania przez nieuprawnione osoby
 - ✓ zmian konfiguracji sprzętu komputerowego lub sieciowego bez wiedzy Wykonawcy;
 - ✓ nieautoryzowanej przez Wykonawcę ingerencji w kody źródłowe Oprogramowania.
- Gwarancja będzie świadczona przez Wykonawcę w miejscu użytkowania Oprogramowania lub Dokumentacji chyba, że Zamawiający wyrazi zgodę na jej zdalne świadczenie.
- O ile będzie to niezbędne na czas wykonywania gwarancji przedstawiciele Wykonawcy otrzymają od Zamawiającego niezbędne uprawnienia administracyjne. Wykonawca zobowiązany jest o takie uprawnienia wystąpić do Zamawiającego.
- Gwarancja nie wyłącza odpowiedzialności Wykonawcy wobec Zamawiającego z tytułu rękojmi.
- Wykonawca zapewnia, że wykonany, doręczony i odebrany przez Zamawiającego przedmiot Umowy będzie wolny od wad fizycznych i prawnych.
- W przypadku żądania przez Zamawiającego usunięcia wad i usterek w przedmiocie Umowy w ramach gwarancji, Wykonawca zobowiązany jest do ich nieodpłatnego usunięcia w terminie wyznaczonym przez Zamawiającego, liczonym od daty pisemnego zawiadomienia Wykonawcy przez Zamawiającego o tych wadach i usterkach.



ISTOTNE KWESTIE W UMOWACH

Warunki zmiany umowy wynikające :

- ze zmiany wymogów technologicznych, w szczególności, gdyby zastosowanie przewidzianych rozwiązań groziło niewykonaniem lub wadliwym wykonaniem przedmiotu Umowy;
- z konieczności wprowadzenia zmian będących następstwem zmian wytycznych, wymagań lub zaleceń instytucji, która przyznała środki na sfinansowanie Umowy – jeśli realizacja jest współfinansowana ze środków zewnętrznych.
- z zaistnienia siły wyższej, tj. zdarzenia losowego wywołanego przez czynniki zewnętrzne, którego nie można było przewidzieć ani mu zapobiec lub przezwyciężyć poprzez działanie z dochowaniem należytej staranności, w szczególności zagrażającego bezpośrednio życiu lub zdrowiu ludzi lub grożącego powstaniem szkody w znacznych rozmiarach;
- ze zmiany przepisów prawa mających wpływ na wykonanie przedmiotu Umowy, w szczególności mających wpływ na konieczność zastosowaniu innych rozwiązań technicznych lub materiałowych;
- z konieczności wykonania zamówień dodatkowych, czego nie można było przewidzieć w chwili zawarcia Umowy;
- z okoliczności, których Zamawiający, działając z należytą starannością, nie mógł przewidzieć a które mają istotny wpływ na prawidłową realizację przedmiotu Umowy;
- ze wstrzymania realizacji Umowy przez Zamawiającego, nie wynikającego z winy Wykonawcy,
- z opóźnień w przekazaniu danych i materiałów źródłowych niezbędnych do realizacji Umowy, o ile nie wynika to z przyczyn leżących po stronie Wykonawcy;
- z konieczności dostosowania Umowy w zakresie Usług i współpracy z Wykonawcą w przypadku wypowiedzenia Umowy w części i przejęcia jej przez inny podmiot, któremu powierzona zostanie do realizacji część prac objęta wypowiedzeniem,
- z konieczności zmiany zakresu Umowy, wynikającej z powstałej po zawarciu Umowy sytuacji braku środków Zamawiającego na sfinansowanie wykonania Umowy zgodnie z pierwotnymi warunkami;
- gdy zaistnieje przerwa w realizacji Umowy z przyczyn niezależnych od Wykonawcy;
- ze zmniejszenia zakresu przedmiotu Umowy.



ISTOTNE KWESTIE W UMOWACH

Zasady utrzymania w tym warunki i zakres usług administracji technicznej i asysty powdrożeniowej

Niezależnie od docelowej formuły/modelu utrzymania: utrzymanie „siłami własnymi”, utrzymanie poprzez wyspecjalizowane podmioty administracji, sektora finansów publicznych np. z obszaru rolnictwa lub z obszaru informatyzacji państwa, firmy komercyjne, model mieszany – w każdym przypadku istotne będą poniższe zagadnienia

1. W ramach świadczenia usług Administracji technicznej oraz Asysty powdrożeniowej Wykonawca zobowiązany będzie świadczyć usługi wsparcia Zamawiającego w siedzibie Zamawiającego w godzinach pracy Zamawiającego. W szczególnych przypadkach, za zgodą Zamawiającego, usługi będą mogły być świadczone w innej, uzgodnionej pomiędzy Stronami lokalizacji.
2. Usługi Administracji technicznej oraz Asysty powdrożeniowej będą świadczone przez Ekspertów odpowiednio do zakresu Zlecenia.
3. Zamawiający zobowiązuje się zapewnić stanowiska pracy niezbędne do świadczenia usług. Zamawiający nie zapewnia sprzętu komputerowego oraz oprogramowania.
4. Usługi Administracji technicznej oraz Asysty powdrożeniowej będą świadczone odpowiednio:
 - a) Administracja techniczna – świadczona od momentu podpisania Umowy do wdrożenia systemów.
 - b) Analiza powdrożeniowa – świadczona od momentu wdrożenia systemów do zakończenia okresu gwarancji. Usługami analizy powdrożeniowej będą objęte wszystkie produkty zrealizowane w ramach Umowy.
5. W zakres usług Administracji technicznej oraz Asysty powdrożeniowej wchodzi:
 - a) świadczenie wsparcia związanego z obsługą systemów (w tym m.in. zarządzanie użytkownikami: dodawanie, usuwanie, modyfikacja, zarządzanie prawami dostępu i parametrami uwierzytelniania) – dotyczy Administracji technicznej oraz Asysty powdrożeniowej,
 - b) świadczenie wsparcia w zakresie bezpośredniej obsługi, konfiguracji, optymalizacji i administracji systemami (w tym np. konfiguracja usług) – Administracji technicznej oraz Asysty powdrożeniowej,
 - c) świadczenie wsparcia w zakresie instalacji oprogramowania (w tym także ujednolicanie wersji oprogramowania, w zakresie licencji będących w posiadaniu Zamawiającego) - dotyczy Administracji technicznej oraz Asysty powdrożeniowej,
 - d) zasilanie danymi systemów oraz świadczenie pomocy merytorycznej i technicznej w procesie zasilania systemów (w tym także analiza błędów w danych) – dotyczy Administracji technicznej oraz Asysty powdrożeniowej,
 - e) organizacja i prowadzenie usług zdalnego (telefonicznego, e-mailowego) wsparcia użytkowników związanego z obsługą systemów – dotyczy Asysty powdrożeniowej,
 - f) zapewnienie ciągłego działania systemu, w tym utrzymywanie gotowości do reakcji na zgłaszane incydenty, ich klasyfikacja i rozwiązywanie – dotyczy Asysty powdrożeniowej.
6. Szczegóły i sposób wykonywania prac przez Wykonawcę będą uzgadniane pomiędzy Stronami i opisane w Zleceniu.
7. Czy należy rozważyć minimalny okres objęty umową utrzymania ?



ISTOTNE KWESTIE W UMOWACH

Zasady utrzymania w tym warunki i zakres usług administracji technicznej i asysty powdrożeniowej

Finansowanie usług asysty powinno być realizowane na podstawie szczegółowej wyceny zakresu prac dostarczonych przez Wykonawcę.

Usługi Asysty powinny dotyczyć m.in:

- a) prac o charakterze analitycznym i projektowym;
- b) prac związanych z administrowaniem, utrzymaniem i konfiguracją systemów
- c) prac związanych ze świadczeniem usług wsparcia/helpdesk



TESTOWANIE I WDRAŻANIE

W ramach prac przygotowawczych do realizacji zamówienia powinna powstać metodyka prowadzenia testów.

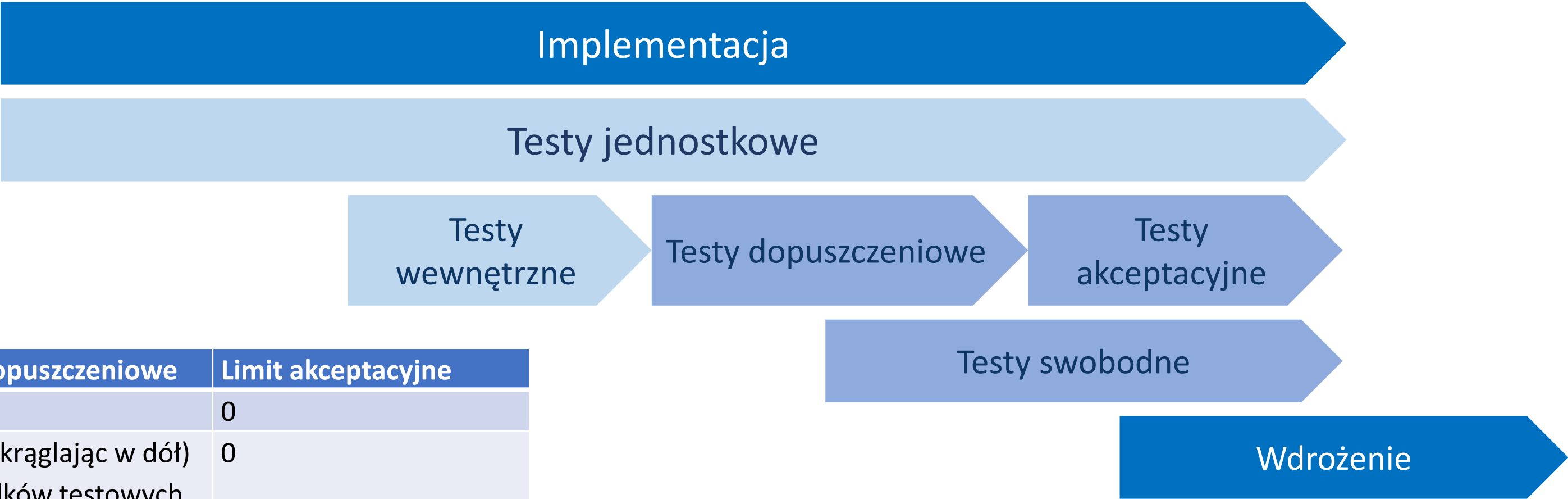
Rozróżnia się następujące rodzaje testów, które powinny zostać wykonane:

- Testy wewnętrzne,
- Testy dopuszczeniowe,
- Testy akceptacyjne,
- Testy jednostkowe,
- Testy swobodne.

Termin	Definicja
Testowanie	Element procesu wytwarzania oprogramowania. Jego celem jest badanie, czy dane oprogramowanie posiada określone cechy określone w specyfikacji (i wyrażone w niej np. poprzez wymagania). Testowanie dostarcza także wiedzy o ryzyku odbioru systemu.
Przypadek testowy	Przypadek testowy to opis pewnej liniowej ścieżki interakcji z systemem, która, przy założeniu wykorzystania określonych danych i przy określonym stanie początkowym systemu i jego otoczenia (tzw. warunkach początkowych), jednoznacznie doprowadza do sekwencji określonych, obserwowalnych stanów systemu.
Scenariusz testowy	Scenariusze i przypadki testowe są działaniami zapisanymi w Planie testów i przeznaczonymi do wykonania w ramach testów weryfikujących spełnienie wymagań stawianych danemu rozwiązaniu.
Wymaganie funkcjonalne	Cecha jakościowa oprogramowania zgodna z taksonomią normy ISO-9126 lub norm jej równoważnych powinna być określona w OPZ dotyczącym systemu
Wymaganie pozafunkcyjne	



TESTOWANIE I WDRAŻANIE



Kategoria	Limit dopuszczeniowe	Limit akceptacyjne
Krytyczny	0	0
Poważny	1% (zaokrąglając w dół) przypadków testowych	0
Średni	10% (zaokrąglając w dół) przypadków testowych	5% (zaokrąglając w dół) przypadków testowych
Kosmetyczny	Bez limitu	Bez limitu

- Scenariusze i przypadki testowe
- Kategorie błędów
- Limity błędów
- Ujęcie testów w harmonogramie projektu



TESTOWANIE I WDRAŻANIE

Testy jednostkowe - zorientowane na weryfikację określonych elementów oprogramowania, towarzyszą podprocesowi implementacji, ich realizacja leży po stronie Wykonawcy - Zamawiający obserwuje jedynie wyniki.

Testy wewnętrzne - obejmują weryfikację rozwiązania pod względem realizacji przez nie wymagań funkcjonalnych, prowadzone przez Wykonawcę w jego środowisku. Wykonawca przekazuje Raport z testów wewnętrznych przed rozpoczęciem testów dopuszczeniowych.

Testy dopuszczeniowe - obejmują weryfikację rozwiązania pod względem realizacji przez nie wymagań funkcjonalnych. Testy dopuszczeniowe są przeprowadzane przez Wykonawcę w obecności Zamawiającego lub są przeprowadzane przez Zamawiającego.

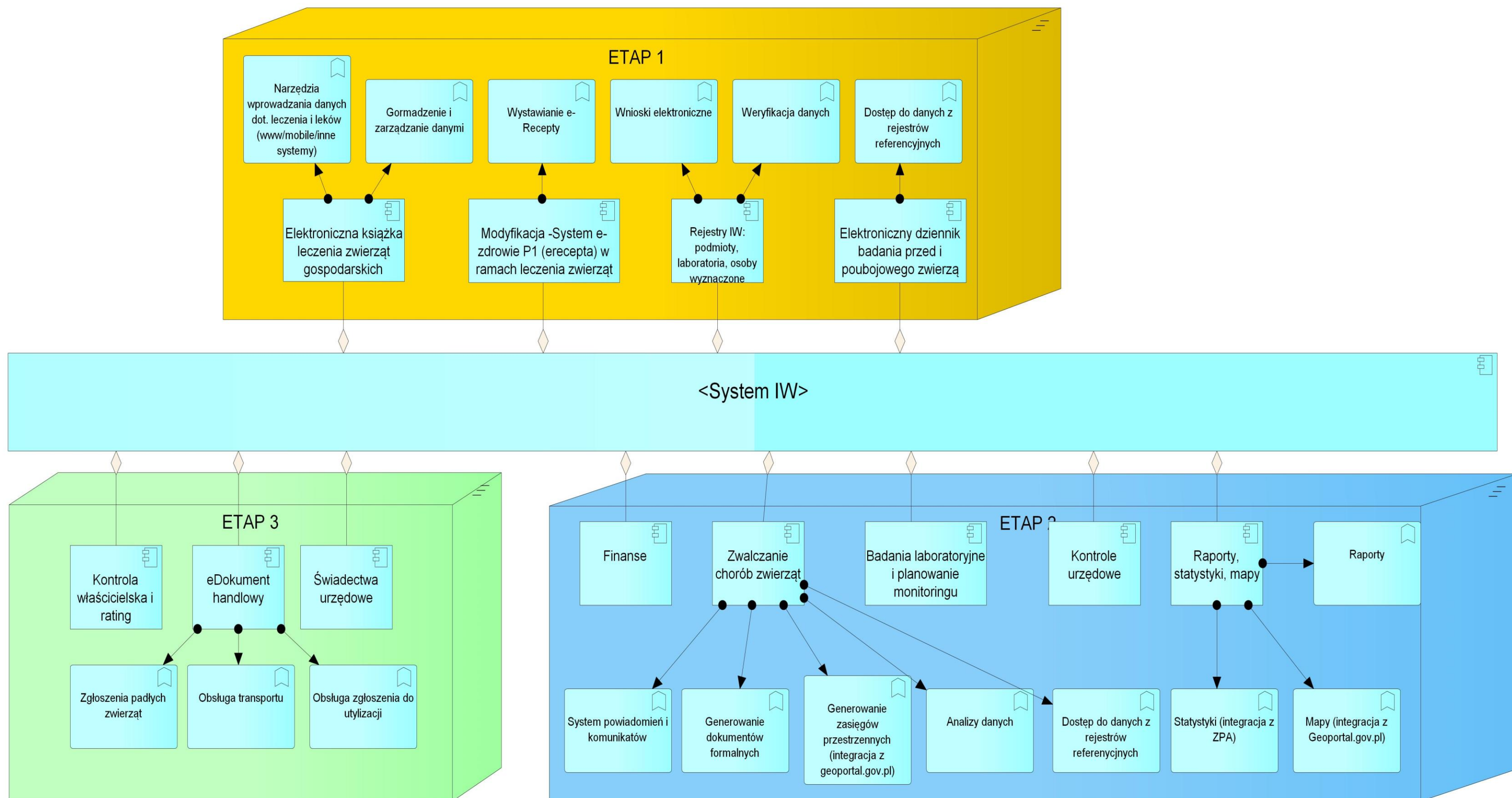
Testy akceptacyjne - obejmują weryfikację oprogramowania w zakresie funkcjonalności oraz wymagań pozafunkcyjnych poprzez wykonanie testów specyficznych dla testowania poszczególnych wymagań pozafunkcyjnych w tym uwzględnienia testów wydajnościowych (w tym przeciążeniowych), bezpieczeństwa i automatycznych. Przeprowadzane są przez Wykonawcę w obecności Zamawiającego lub są przeprowadzane przez Zamawiającego.

Testy swobodne - przeprowadzane są Zamawiającego, najczęściej bez obecności Wykonawcy. Celem testów swobodnych jest weryfikacja funkcjonalności rozwiązania oraz jego cech pozafunkcyjnych. Rezultaty testów swobodnych są przedmiotem osobnych ustaleń projektowych.

Ze względu na możliwe występnie błędów w trakcie testów, w harmonogramie realizacji zamówienia powinien zostać uwzględniony dodatkowy czas na ewentualnie wydłużenie się testów.



ARCHITEKTURA I ZAGADNIENIA TECHNICZNE





ARCHITEKTURA I ZAGADNIENIA TECHNICZNE

Wymagania

Elementem dokumentacji przetargowej powinien być Rejestr wymagań

Dokument powinien zawierać wykaz wymagań funkcjonalnych (planowanych do realizacji w ramach budowy systemu) i pozafunkcjonalnych (dotyczących realizacji usług, jakości i efektywności pracy – parametry wymagań pozafunkcjonalnych mogą być modyfikowane).

Wymagania powinny być podzielone na grupy odnoszące się do poszczególnych podsystemów biznesowych Systemu IW np. :

- Książki Leczenia,
- Dziennika Badań,
- Rejestru podmiotów,
- Rejestru lekarzy,
- wszelkich eDokumentów w tym eRecepty

oraz podsystemów biznesowych o charakterze wspierających np.: moduły statystyk, moduły i aplikacje mapowe, moduły analityczne i podsystemów wspierających realizację zadań: nadzór w tym nadzór procesów kontrolnych, rozliczenia, finanse również w odniesieniu do planowanych usług.

Identyfikator	Obszar	Treść wymagania	Status	Stopień powinności	Rodzaj wymagania
---------------	--------	-----------------	--------	-----------------------	---------------------

Wymagania dotyczące kryteriów weryfikacji i odbioru wymagań funkcjonalnych oraz pozafunkcjonalnych powinny zostać dokładnie opisane w ramach Procedury odbioru, a wszelkie testy przeprowadzone zgodnie ze znaną obu stronom umowy metodyką.

- kanał web – podstawowy kanał komunikacji w systemie zarówno wewnątrz struktury organizacyjnej Inspekcji jak i ze środowiskiem zewnętrznym
- kanał mobile – co najmniej w zakresie działań terenowych Inspekcji oraz publikacji informacji, map dot. zagrożeń i sytuacji kryzysowych.

Moduł	Nazwa usługi	Skrócona nazwa usługi
-------	--------------	-----------------------



ARCHITEKTURA I ZAGADNIENIA TECHNICZNE

Wstępny opis wymagań funkcjonalnych oraz нефункциональных

Dla przykładu kilka wymagań dot. rozwiązań mapowych.

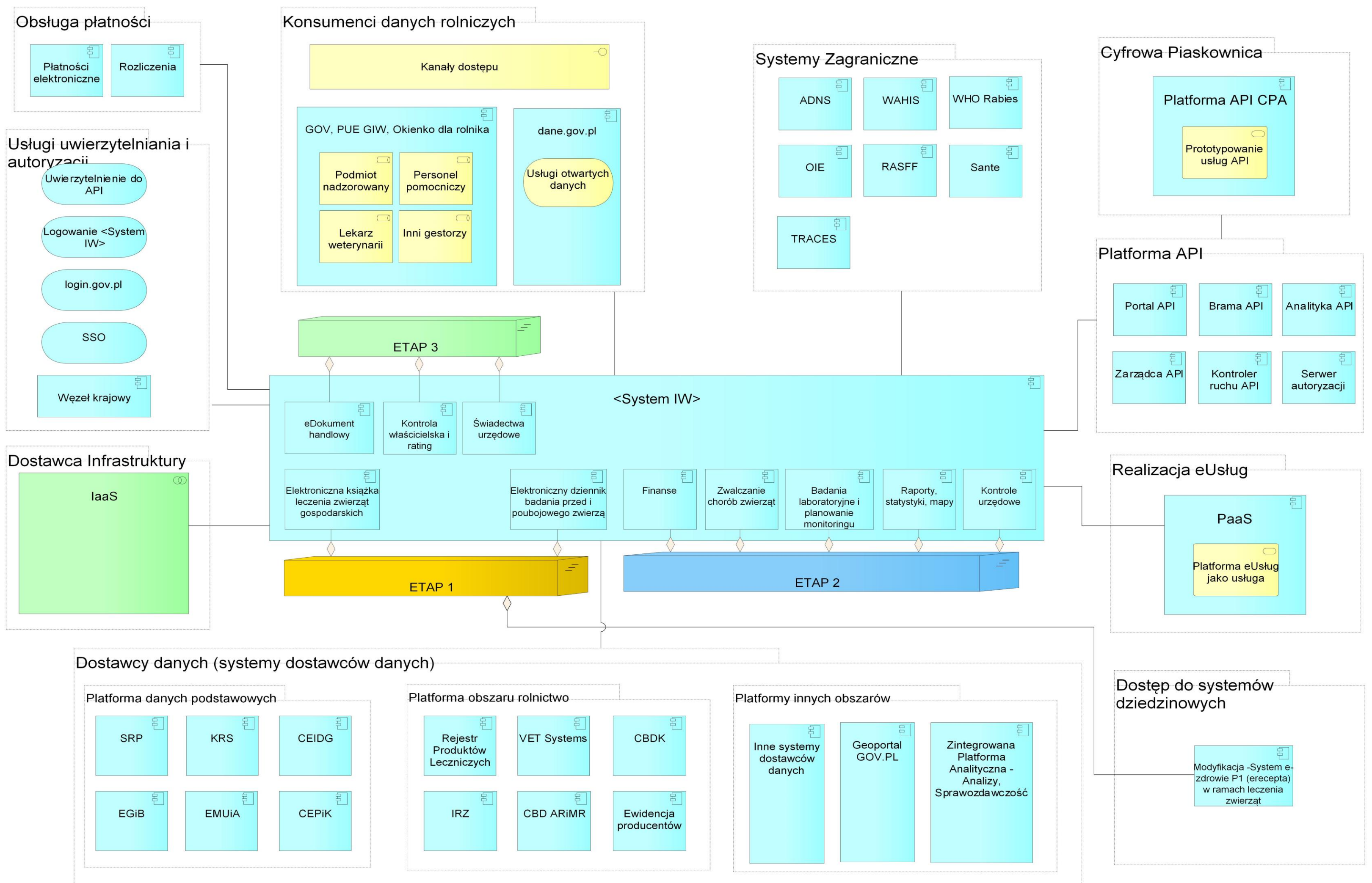
Aplikacja mapowa oraz aplikacja mobilna powinny :

- pozwalać na zarządzanie warstwami tematycznymi w oknie mapowym, co najmniej aktywowania i dezaktywowania treści poszczególnych warstw oraz zarządzaniu przezroczystością poszczególnych warstw.
- być wyposażona w narzędzia pozwalające na nawigację użytkownika w oknie mapy, co najmniej przybliżanie, powiększanie, przesuwanie zawartości okna mapy, pełny zasięg
- być wyposażona w wyszukiwarkę jednostek administracyjnych oraz obiektów geograficznych z automatycznych przybliżeniem i centrowaniem okna mapy do wyszukanego obiektu.
- być wyposażone w narzędzie identyfikacji obiektu, za pomocą którego użytkownik będzie mógł wyświetlić dodatkowe informacje opisowe w kontekście wyświetlanych danych w oknie mapy.
- posiadać narzędzie umożliwiające użytkownikowi prowadzenie analiz czasowych na warstwach tematycznych wyświetlanych w oknie mapy.

Oceniamy, że tylko dla jednego modułu dotyczącego rozwiązań mapowych takich wymagań funkcjonalnych i нефункциональных powinno być około 20.

Kilka przykładów wymagań w zakresie architektury

System nie może posiadać pojedynczego punktu awarii (dotyczy środowiska produkcyjnego).	Serwery mimo wystarczającej wydajności muszą zostać co najmniej zduplikowane, aby nie stanowiły wrażliwego elementu i nie powodowały swoją awarią niedostępności całego Systemu.
Architektura systemu musi umożliwiać jego skalowanie.	Architektura systemu powinna umożliwiać skalowanie aplikacji, w tym dodawanie nowych węzłów z nowymi instalacjami komponentów systemu.
System musi posiadać jednorodny, spójny interfejs użytkownika	Interfejs Użytkownika Systemu (modułu systemu) musi być jednolity dla wszystkich podsystemów, z których ten użytkownik korzysta.
System musi prawidłowo działać w aktualnych wersjach przeglądarek internetowych.	Aplikacja webowa musi być przetestowana na aktualnych wersjach przeglądarek, co najmniej MS Edge, Firefox, Safari i Google Chrome. Przez wersję aktualną rozumie się najnowszą, stabilną wersję, dostępna na rynku w momencie rozpoczęcia testów.
System musi sygnalizować pracę Systemu.	System powinien zapewnić sygnalizację pracy Systemu (np. klepsydra - animowana ikona podczas oczekiwania na wynik przetwarzania) podczas przetwarzania danych lub generowania raportów.



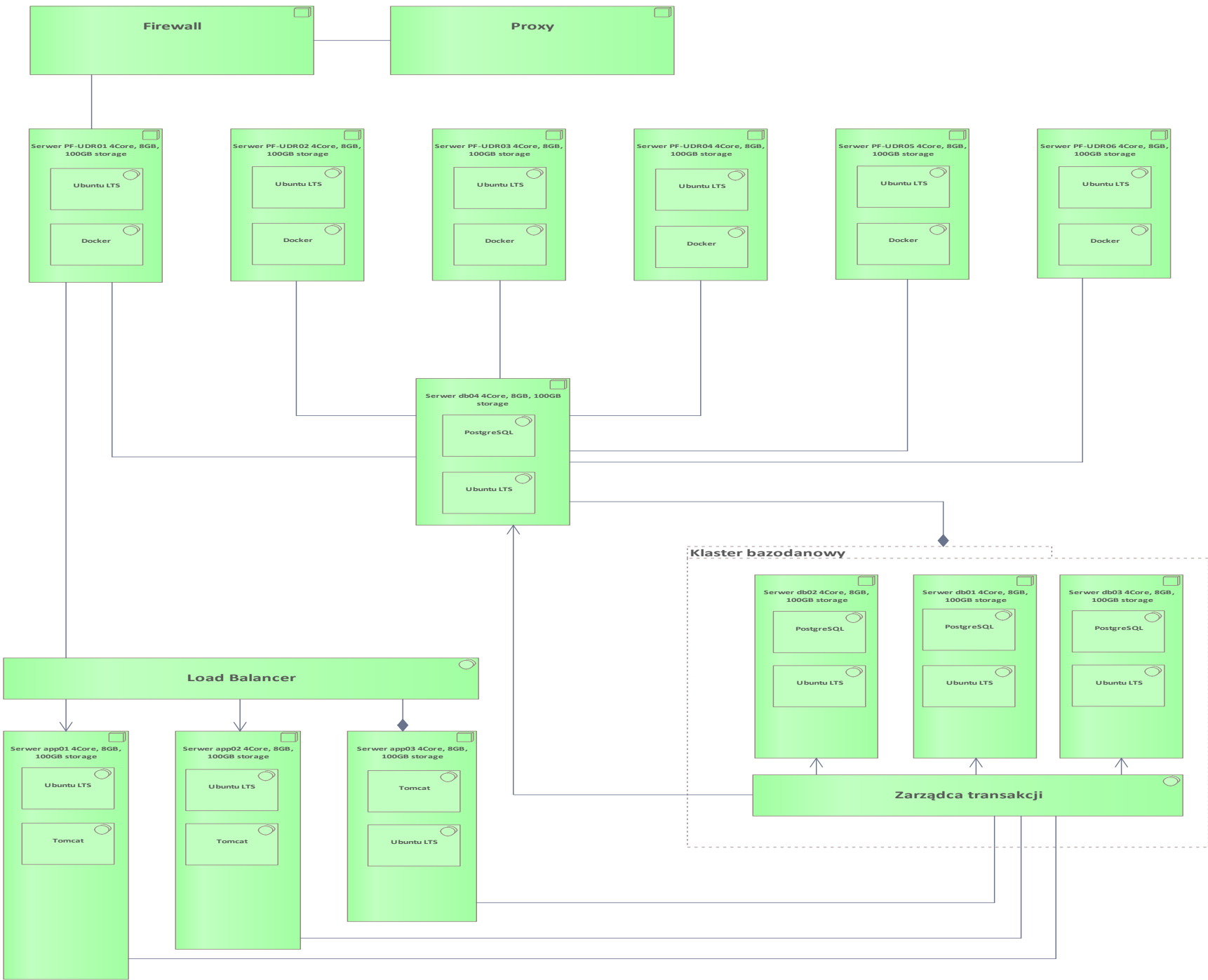


ARCHITEKTURA I ZAGADNIENIA TECHNICZNE

Wymagania w zakresie infrastruktury technicznej

Fragment środowiska uwzględniający architekturę opartą na wykorzystaniu rozwiązania o charakterze Platformy obszarowej (obszar rolnictwa), oraz Platformy dostępu do danych i usług podstawowych /referencyjnych.

Serwer app01 4Core, 8GB, 100GB storage	Serwer aplikacyjny
Serwer app02 4Core, 8GB, 100GB storage	Serwer aplikacyjny
Serwer app03 4Core, 8GB, 100GB storage	Serwer aplikacyjny
Serwer db01 4Core, 8GB, 100GB storage	Serwer bazodanowy
Serwer db02 4Core, 8GB, 100GB storage	Serwer bazodanowy
Serwer db03 4Core, 8GB, 100GB storage	Serwer bazodanowy
Serwer db04 4Core, 8GB, 100GB storage	Serwer bazodanowy
Serwer PF-UDR01 4Core, 8GB, 100GB storage	Serwer Docker
Serwer PF-UDR02 4Core, 8GB, 100GB storage	Serwer Docker
Serwer PF-UDR03 4Core, 8GB, 100GB storage	Serwer Docker
Serwer PF-UDR04 4Core, 8GB, 100GB storage	Serwer Docker
Serwer PF-UDR05 4Core, 8GB, 100GB storage	Serwer Docker
Serwer PF-UDR06 4Core, 8GB, 100GB storage	Serwer Docker
Zarządca transakcji	Zarządzanie transakcjami bazodanowymi
Docker	Kontenery
Ubuntu LTS	System operacyjny
PostgreSQL	Baza danych
Tomcat	Kontener aplikacji webowych





ARCHITEKTURA I ZAGADNIENIA TECHNICZNE

Należy oczekiwać, że w ramach infrastruktury chmurowej będą świadczone następujące usługi

Nazwa usługi	Opis usługi
Wirtualna maszyna	Usługa przetwarzania. Grupa wirtualnych maszyn w określonych konfiguracjach wirtualnego procesora, pamięci i przestrzeni dyskowej, przygotowana do uruchomienia systemu operacyjnego.
Przestrzeń dyskowa	Usługa przetwarzania. Grupa przestrzeni dyskowych typu blokowego oraz obiektowego, o określonej pojemności i wydajności podsystemu dyskowego.
VPN Gateway	Usługa sieciowa (z ang. Virtual Private Network). Bramka VPN umożliwiająca połączenie ze sobą dwóch lub więcej urządzeń, sieci lub zdalnych centrów danych. Można utworzyć dwa rodzaje bramek VPN: punkt-lokacja (P2S VPN) i lokacja-lokacja (S2S VPN).
Sieć prywatna	Usługa sieciowa. Umożliwia budowanie sieci i podsieci łączności lokalnych dla systemów informatycznych zainstalowanych w tenancie, z wykorzystaniem pul adresów IP zarezerwowanych do użytkowania prywatnego.
Dodatkowy IP	Usługa sieciowa. Dodatkowy publiczny adres IP wykorzystywany do konfiguracji innych usług.
Loadbalancer	Usługa sieciowa. Usługa infrastrukturalna dostarczająca funkcji równoważenia obciążenia ruchu sieciowego.
DNS	Usługa sieciowa (z ang. Domain Name Service). Hierarchiczny rozproszony system nazw sieciowych, który odpowiada na zapytania o nazwy urządzeń sieciowych lub ich adresy IP.
Firewall	Usługa bezpieczeństwa. Obejmuje zaporę sieciową, ochronę przed nieautoryzowanym dostępem, IPS.
System operacyjny	Usługa przetwarzania. Obraz komercyjnego systemu operacyjnego poprawnie licencjonowanego w modelu subskrypcyjnym, rozliczany za jego użycie.
Baza danych	Usługa typu PaaS. Usługa transakcyjnej bazy danych.



ARCHITEKTURA I ZAGADNIENIA TECHNICZNE

Proponowana chmura obliczeniowa

Należy rozważyć wykorzystanie istniejących w administracji chmur obliczeniowych lub infrastruktur - rozwiązanie chmurowe z rynku będzie zdecydowanie droższe a ponadto w ramach współpracy w administracji, infrastruktura w zależności od potrzeb aplikacyjnych może być skalowana w reakcji na zdarzenia obniżonej wydajności wynikające z monitoringu w ramach usługi helpdesk.

System operacyjny, baza danych

Ubuntu LTS, baza danych Postgres w konfiguracji klastra wydajnościowego. W zakresie systemów operacyjnych stosujemy licencjonowane produkty.

Systemy wspierające – monitoring, zarządzanie,

Adaptacja i użycie rozwiązań typu APM (Application Performance Monitoring) np. Prometheus poprzez ustalenie wymaganych KPIs potrzebnych do monitorowania kluczowych aplikacji.

Wykorzystanie procesów DevOps w celu zarządzania procesem wytwórczym i wdrożeniowym w oparciu o takie narzędzia jak: Gitlab, Jenkins, Nexus, Docker oraz Kubernetes



ARCHITEKTURA I ZAGADNIENIA TECHNICZNE

Helpdesk

Zgłaszanie i obsługa problemów poprzez dedykowaną aplikację web.

Aplikacje mobilne,

Wykorzystanie ugruntowanych frameworków dla tworzenia aplikacji mobilnych zarówno w trybie native oraz hybrydowym.

Jakie rozwiązania off-line oraz jakie rozwiązania zapewniające integralność i zabezpieczenia danych po przejściu na tryb on-line i upload danych do systemu

Aplikacje dla użytkownika w technologii SPA (Single Page Application) lub PWA (Progressive Web Application). Przesyłanie danych z API, które wykorzystuje struktury zapytań typu jsonAPI czy GraphQL w celu minimalizacji przesyłanych danych.

Dla budowy aplikacji w trybie offline zastosowanie mechanizmów „cache storage” , „service worker”. Dla utrwalania aktywności użytkownika oraz przechowywania i replikacji danych offline wykorzystanie mechanizmów typu IndexedDB.

Rozwiązania uwierzytelniające użytkowników, wprowadzanie danych.



ARCHITEKTURA I ZAGADNIENIA TECHNICZNE

Propozycje związane z obszarem archiwizacji i backup'ów

Należy rozróżnić pojęcia „archiwizacji” od „kopii zapasowych”

Archiwizacja oznacza przeniesienie danego obiektu (np. pliku) do archiwum, czyli wykonanie kopii archiwalnej obiektu przed jego zastąpieniem nowym obiektem (np. nową wersją pliku).

Kopie zapasowe są mechanizmem zapewniającym przywrócenie systemu / danych do stanu z pewnego określonego momentu w czasie, wykorzystywanym na przykład po utracie danych będącej skutkiem awarii systemu (nie chronią jednak przed samą awarią).

Archiwizacja

Rekomendujemy ustalenie szczegółów w zakresie archiwizacji na etapie analizy przedwdrożeniowej. W szczególności rekomendujemy rozważenie zasadności i zasad archiwizowania (tworzenia archiwum) plików, które mogą być modyfikowane przez wielu użytkowników, tak aby istniała możliwość odtworzenia / przywrócenia wcześniejszej wersji pliku, jak również wyświetlenia / odtworzenia historii zmian wprowadzanych przez różnych użytkowników.

Kopie zapasowe

Wykonywanie kopii zapasowych jest elementem zarządzania

kryzysowego, mającego na celu umożliwienie odtworzenia danych po poważnych katastrofach (np. pożar, zalanie serwerowni), awariach urządzeń, na których funkcjonują systemy informatyczne, jak również w przypadku poważnych incydentów bezpieczeństwa (takich jak na przykład ataki ransomware).

W przypadku odtwarzania danych z kopii zapasowej najczęściej nie będzie możliwe odzyskanie wszystkich danych – utracone zostaną dane wprowadzone do systemu od momentu wykonania ostatniej kopii zapasowej do momentu wystąpienia awarii / utraty danych. Uwzględniając potencjalną możliwość utraty pewnej ilości danych (parametry RTO i RPO), należy określić częstotliwość i rodzaj wykonywanych kopii zapasowych (pełne, przyrostowe, różnicowe, itp.), jak również zakres wykonywania kopii zapasowych (dane, serwery, obrazy maszyn wirtualnych, migawki, systemy operacyjne, oprogramowanie bazodanowe, aplikacje, itd.).

W trakcie planowania wykonywania kopii zapasowych należy uwzględnić zasady rotacji nośników (zgodnie z zaleceniami producenta danego nośnika), jak również konieczność okresowego zapisywania kopii zapasowych na nośnikach zewnętrznych (poza systemami informatycznymi) i przechowywania ich w innej lokalizacji. Należy ponadto rozważyć zasadność szyfrowania kopii zapasowych.

Kopie zapasowe powinny być okresowo testowane, w celu zapewnienia poprawności kopii zapasowych oraz możliwości ich odtworzenia w przypadku konieczności odtworzenia danych lub systemów.



ARCHITEKTURA I ZAGADNIENIA TECHNICZNE

Rozwiązania w zakresie bezpieczeństwa oraz cyberbezpieczeństwa

Infrastruktura

Infrastruktura musi posiadać aktywną gwarancję lub umowę wsparcia pozwalającą na aktualizację firmware (z autoryzowanych źródeł) oraz wymianę wadliwych komponentów.

Uszkodzone elementy, który zawierają lub potencjalnie mogą zawierać dane z systemu lub dane konfiguracyjne powinny być przekazywane GIW (i trwale niszczone, niezależnie od warunków gwarancji), a w ich miejsce dostarczane nowe elementy.

Należy zapewnić neutralność technologiczną (vendor locking), uniknięcie nieuzasadnionego uzależnienia od konkretnego dostawcy usług bądź od konkretnego producenta sprzętu lub oprogramowania.

Pomieszczenia infrastruktury przetwarzania (lokalna serwerownia) powinny posiadać co najmniej zasilanie awaryjne umożliwiające bezpieczne zamknięcie systemów, systemy monitorowania warunków środowiskowych (temperatura, wilgotność), automatyczny system gaszenia dla pomieszczenia lub szaf serwerowych, system kontroli dostępu do pomieszczeń.

Pomieszczenia zewnętrznego centrum przetwarzania danych (zewnętrzna serwerownia) powinny spełniać wymagania normy PN-EN 50600 dla klasy 3 w kategoriach: dostępność, zabezpieczenie przed nieuprawnionym dostępem, zabezpieczenie przed zagrożeniami środowiskowymi.

Należy zapewnić, że dane przetwarzane w systemie będą przesyłane przez sieć internet w sposób bezpieczny – możliwe mechanizmy bezpieczeństwa to na przykład wykorzystywanie dedykowanych połączeń, sieci VPN (Virtual Private Network), szyfrowanie połączeń (np. HTTPS z implementacjami TLS).

Systemy operacyjne i aplikacje

Wykorzystywane systemy operacyjne, wirtualizatory, kontenery powinny pochodzić z autoryzowanych źródeł z zapewnieniem wsparcia co najmniej w zakresie poprawek bezpieczeństwa w okresie eksploatacji systemu. Aktualizacja używanych systemów operacyjnych w zakresie poprawek bezpieczeństwa powinna następować możliwie najszybciej.

W przypadku wykorzystania oprogramowania z otwartym kodem źródłowym (ang. Open Source), powinno być ono zgodne z ich postanowieniami licencyjnymi, i być pobierane z autoryzowanych, rozpoznawalnych źródeł oraz powinno mieć zapewnione wsparcie społeczności (ang. community) co najmniej w zakresie publikowania poprawek bezpieczeństwa.

W przypadku wykorzystania w kodzie źródłowym projektowanego systemu oprogramowania Open Source należy zapewnić, że są one regularnie testowane pod kątem bezpieczeństwa (włączając w to również zależności).

System powinien być chroniony co najmniej z wykorzystaniem: oprogramowania zabezpieczającego przed złośliwym oprogramowaniem, urządzeń typu firewall, IDS / IPS (Intrusion Detection System / Intrusion Prevention System), WAF (Web Application Firewall), mechanizmów ochrony przed atakami typu DDos (Distributed Denial of Service) mającymi na celu spowodowanie niedostępności serwera, usługi lub infrastruktury.

Projektowany system oraz wszystkie wykorzystywane komponenty muszą umożliwiać zmianę domyślnych poświadczeń administratora.

Projektowany system powinien zapewniać silne uwierzytelnienie użytkowników (w szczególności uprzywilejowanych).



ARCHITEKTURA I ZAGADNIENIA TECHNICZNE

Rozwiązania w zakresie bezpieczeństwa oraz cyberbezpieczeństwa

Przetwarzanie danych w chmurze

W przypadku wykorzystania rozwiązań korzystających z usług chmurowych należy zapewnić, że architektura systemu umożliwia wycofanie się z tych usług w skończonym / założonym czasie. Powinien zostać opracowany i przetestowany plan wyjścia z korzystania z usług przetwarzania w chmurze (exit plan).

Należy zapewnić, że natywne mechanizmy bezpieczeństwa platformy dostarczającej usługi przetwarzania danych w chmurze są stosowane i udokumentowane.

Należy zapewnić, że dostawca usług chmurowych będzie przetwarzać danych na terytorium państw, które zapewniają należyty poziom ochrony danych i/lub których systemy prawne dają gwarancję należytej ochrony praw i wolności osób, których dane dotyczą – możliwe mechanizmy bezpieczeństwa to na przykład ograniczenie przetwarzania danych wyłącznie do terytorium Unii Europejskiej (w tym również przez podwykonawców dostawcy usług chmurowych), zakaz ujawniania danych organom państw, w których przetwarzane są dane, o ile nie wynika to wprost z przepisów obowiązującego prawa.

Należy zapewnić, że stosowane przez dostawcę usług chmurowych mechanizmy izolacji danych poszczególnych Klientów dostawcy zapobiegają przypadkowemu ujawnieniu danych z systemu innemu Klientowi dostawcy.

Monitorowanie systemu

System powinien zapewniać możliwość rejestrowania / logowania zdarzeń w formacie umożliwiającym ich przetwarzanie w systemach typu SIEM / SOAR (Security Information and Event Management / Security Orchestration, Automation And Response). Logi zdarzeń powinny być zabezpieczone przed modyfikacją i usunięciem.

Architektura systemu (pojemność) powinna zapewniać możliwość przechowywania logów przez okres minimum 1 roku, w sposób umożliwiający ich powtórny i/lub późniejszą analizę.

System przechowywania logów powinien automatycznie raportować do wskazanych osób o błędach w zapisywaniu logów, zatrzymaniu zapisywania logów, wyczerpującym się miejscu, w którym są zapisywane logi (zgodnie z wcześniej zdefiniowanymi progami pojemności), itp.

Organizacja odpowiedzialna za utrzymanie systemu powinna zapewnić struktury zapewniające analizę zdarzeń w zakresie bezpieczeństwa (w trybie i zakresie wynikającym z analizy ryzyka) z wykorzystaniem odpowiednich kompetencji bazujących na wykształceniu, wyszkoleniu, umiejętności i doświadczeniu personelu.



SZKOLENIA I HELPDESK

Szkolenia

Szkolenia wewnętrzne pracowników Inspekcji

- szkolenia ogólne dla pracowników zaangażowanych w obsługę systemu
- szkolenia dla administratorów (iteracyjne)
- szkolenia trenerów (iteracyjne)

Szkolenia dla podmiotów zaangażowanych w procesy obsługiwane przez System IW

Środowisko szkoleniowe

Rodzaje szkoleń

- szkolenia stacjonarne/zdalne
- szkolenia e-learning – konieczność przygotowania materiałów (do wykorzystania istniejące w administracji systemu e-learning)

Materiały szkoleniowe

- prezentacje, ulotki, broszury, filmy
- materiały e-learning
- use cases



SZKOLENIA I HELPDESK

Szkolenia

Szkolenia w ramach umowy z dostawcą systemu

Szkolenia dodatkowe w ramach odrębnego projektu z uwagi na rozbudowaną strukturę organizacyjną oraz obszar objęty systemem (np. POPT)

Koszty

- w przypadku szkoleń zdalnych brak kosztów cateringu, logistyki
- dwu dniowe szkolenie to rynkowy koszt ok. 1500 pln
- odrębne jednorazowe koszty to przygotowanie materiałów szkoleniowych oraz materiałów dla e-learning

Warunki dot. szkoleń zdalnych:

- narzędzie musi być przystosowane do pracy w języku polskim i bezpłatne dla uczestników szkolenia,
- oprogramowanie nie powinno wymagać interwencji administratora na komputerze uczestnika szkolenia,
- oprogramowanie powinno mieć co najmniej opcję do prowadzenia dyskusji, zadawania pytań, rejestrowania, wykorzystania wideo połączenia.
- należy zadbać o dodatkowe oświadczenia dotyczące ochrony wizerunku i danych osobowych z uwagi na możliwość nagrywania szkoleń w tym również możliwości rejestracji wypowiedzi uczestników.



SZKOLENIA i HELPDESK

Organizacja HELPDESK, rozliczanie

Przygotowanie: Przygotowanie do możliwych wariantów rozliczania wymaga analizy obszaru.

Kategoryzacja zgłoszeń – kategoryzacja pozwala na zbadaniu potrzeb i przygotowaniu zebranego zakresu w podziale na poszczególne kategorie w celu przygotowania optymalnych planów ich finansowania. Analiza powinna odnosić się do obszaru (IT, Biznesowe, Administracyjne), użytkowników (wewnętrzni, zewnętrzni), specjalizacji (urządzenia peryferyjne, sieć, uprawnienia, aplikacje, sprzęt, procesy biznesowe), lokalizacji (wewnętrzna, wewnętrzna rozproszona, zewnętrzna).

Analiza częstotliwości zgłoszeń – przy najczęstszych zgłoszeniach należy wziąć pod uwagę zbudowanie kompetencji wewnętrznych, dla zgłoszeń rzadkich outsourcing)

Mapowanie zakresów zgłoszeń – weryfikacja możliwości wewnętrznych i mapowanie ich na kategorie zgłoszeń.

Przygotowanie zakresu na wsparcie zewnętrzne – kategoryzacja i przygotowanie wymagać merytorycznych oraz technicznych dla oczekiwanego czasu obsługi spraw w celu pozyskania wsparcia zewnętrznego.

Dany zakres może zostać podzielony na etapy wydzielając różne poziomy wsparcia w zależności od złożoności prac, wymaganej wiedzy eksperckiej i czasu wymaganego na ich obsłużenia



SZKOLENIA i HELPDESK

Organizacja HELPDESK, rozliczanie

Telefoniczne – rozliczanie konsultantów wewnętrznych, zewnętrznych

- Czas rozmowy telekonsultanta
- Wg. wskaźnika przypisanego dla kategorii zgłoszenia
- Wg. wskaźnika uwzględniającego godziny pracy i godziny dostępności

Etaty – pracownicy organizacji. Rozliczani w ramach umowy o pracę, ale rozliczani dodatkami i premiami w zależności od podjętych zgłoszeń (system zgłoszeń pozwala na etapie zgłaszania dokonać wstępnego podziału kategorii oraz określenie priorytetu wagi co przelicza się na pkt.

Wykonawca zewnętrzny - w zależności od oczekiwanego czasu naprawy, lub wsparcia np. przy migracji, konfiguracjach i instalacjach nowych wersji softu. Czas w ramach umowy utrzymaniowej ryczałt na wsparcie określonej liczby godzin wsparcia zdalnego oraz 2-3 wizyty osobiste. Po przekroczeniu ryczałtu według ustalonych godzinowych stawek. Stawki podzielone na kategorie w zależności od rodzaju wymaganego specjalisty. Katalogi możliwych zadań zesłownikowane tzn. wskazany zakres i charakter prac jaki może wykonać analityk, specjalista/projektant, ekspert (godzina każdego inaczej wyceniona).



Dziękujemy