

(173023)

Opis Przedmiotu Zamówienia

Przedmiotem zamówienia jest: **Wsparcie Zamawiającego w realizacji testów w systemach realizowanych przez Centrum e-Zdrowia.**

Zakres prac w ramach zamówienia:

1. Zapoznanie się Wykonawcy z infrastrukturą aplikacyjną i serwerową Zamawiającego.
 2. Usługa zarządzania testami w ramach systemów/projektów P1, P2, P4, ZSMOPL, KPK, SOLR, eTransplant, eKrew, SMKII, RPL, POPI, eGate, Choroby Rzadkie, SMWoUA, SMK II, RPWDL 2, eHemofilia i innych.
- Szacowana na potrzeby określenia maksymalnej wartości zamówienia liczba roboczogodzin, które mogą zostać wykorzystane wynosi maksymalnie 228 000 roboczogodzin, w tym dla zamówienia podstawowego (gwarantowane) 166 000 roboczogodzin oraz 62 000 roboczogodzin dla zamówienia opcjonalnego), w podziale na:
- a. testy bezpieczeństwa - 6 000 roboczogodzin w ramach zamówienia podstawowego (gwarantowane) oraz 2 000 roboczogodzin w ramach zamówienia opcjonalnego;
 - b. testy automatyczne i wydajnościowe - 50 000 roboczogodzin w ramach zamówienia podstawowego (gwarantowane) oraz 20 000 roboczogodzin w ramach zamówienia opcjonalnego;
 - c. pozostałe testy zwane funkcjonalnymi - 110 000 roboczogodzin w ramach zamówienia podstawowego (gwarantowane) oraz 40 000 roboczogodzin w ramach zamówienia opcjonalnego.
- Termin realizacji zamówienia od dnia podpisania Umowy na okres 18 miesięcy lub do dnia wyczerpania maksymalnego wynagrodzenia określonego w Umowie (zamówienie podstawowe). W przypadku skorzystania z prawa opcji termin obowiązywania Umowy zostaje wydłużony do 36 miesięcy od dnia jej zawarcia lub do dnia wyczerpania maksymalnego wynagrodzenia w zależności od tego, która z tych okoliczności nastąpi wcześniej.
- *Metodyka*

Testy muszą zostać wykonane zgodnie z metodyką opisaną w Załączniku nr 1 do OPZ - Metodyka testów.

Metodyka przeprowadzenia testów uwzględnia wszystkie poniższe wymagania minimalne łącznie. Testy muszą zostać wykonane zgodnie z metodyką zgodną z implementacją rekomendacji zawartych w normie

ISO/IEC/IEEE 29119 „Software and systems engineering — Software testing” lub równoważnej oraz muszą uwzględniać wytyczne następujących standardów łącznie:

- Normy ISO dotyczące zarządzania jakością z rodziny 9000 (obecnie 2500x), 90003 lub równoważne;
- IEEE (np. 829, 1012, 1044) lub równoważne;
- ISTQB (Agile, Advanced & Expert Level Syllabus) lub równoważne.

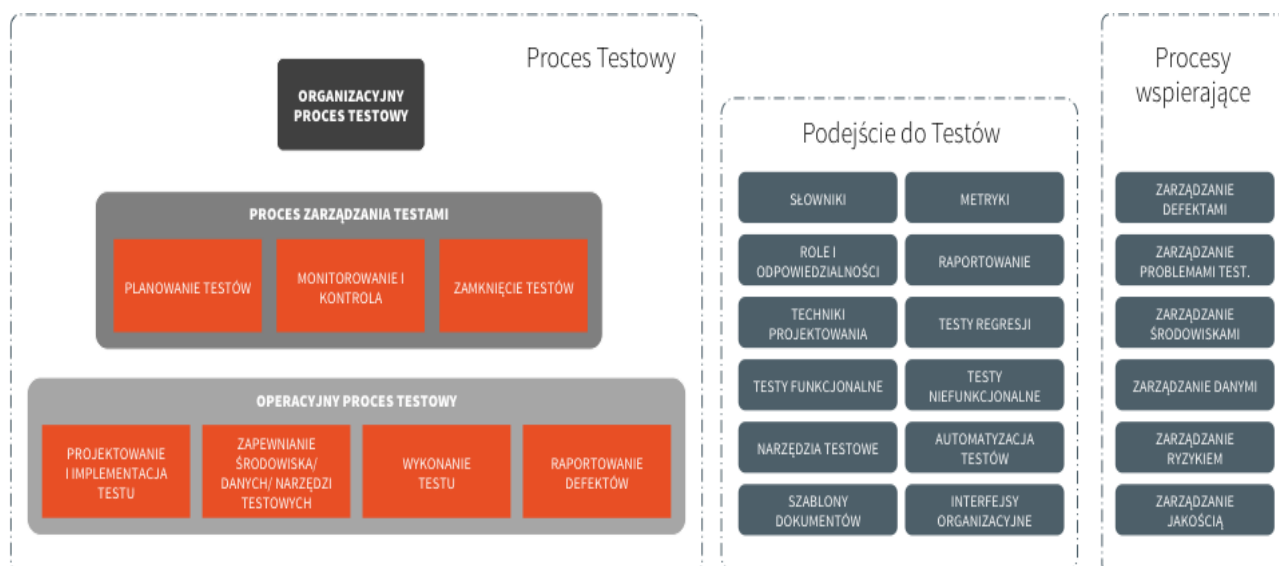
W tym celu, Wykonawca musi zweryfikować w ciągu 3 tygodni od dnia podpisania Umowy dokument „Metodyka przeprowadzenia testów”, który po dokonaniu czynności odbiorczych przez Zamawiającego będzie podstawą do przeprowadzenia testów.

Metodyka musi zapewniać spójny i wysoki standard prac realizowanych przez Wykonawcę.

Przed rozpoczęciem prac testowych Wykonawca w ciągu maksimum 3 tygodni od dnia podpisania Umowy, musi zapoznać się z architekturą infrastruktury Zamawiającego, tak aby w oparciu o jej znajomość, standardy wynikające z certyfikatów oraz doświadczenie własnych ekspertów, adoptować i dostosować do sposobu i celu przeprowadzenia testów w tym uzupełnienie istniejącej metodyki o wykorzystanie potencjału AI w procesie testowym. W tym celu Wykonawca jest zobowiązany do stosowania metodyki usprawniania procesu testowego na podstawie:

- TPI NEXT (Test Process Improvement NEXT) lub równoważnej,
- TMMi (Test Maturity Model Integrated) lub równoważnej.

Dla spójnego i wysokiego standardu prac, jak również dla przejrzystej komunikacji oraz podziału aktywności i odpowiedzialności, Wykonawca musi stosować następującą matrycę RACI:



W procesie należy stosować formalny Proces testowy, który jest podzielony na warstwy organizacyjne. Takie działanie zagwarantuje zapewnienie w ramach opisywania poszczególnych aktywności uniwersalnego podejścia, a z drugiej uwzględnienie złożoności organizacyjnej Zamawiającego. Zakłada się, że formalny model Procesu Testowego będzie się składał z następujących warstw:

- Organizacyjny Proces Testowy – definiuje proces budowania i utrzymania organizacyjnych specyfikacji testowych tj. strategia, procesy, procedury i inne aktywa testowe.
- Proces Zarządzania Testami – definiuje procesy dotyczące zarządzania testami dla całych projektów testowych, poszczególnych faz czy typów testów (jak testy systemowe czy wydajnościowe).
- Operacyjny Proces Testowy – definiuje uniwersalne procesy i procedury prowadzenia testów dynamicznych i testów statycznych. Procesy takie mogą być stosowane zarówno do poszczególnych poziomów testów (np. systemowe, integracyjne) lub rodzajów testów (bezpieczeństwa, migracji danych) w ramach projektu testowego.



Proces testowy ma zapewnić dla Zamawiającego zastosowanie zarówno do zarządzania długoterminową strategią rozwoju, do zarządzania i realizacji testów w programie migracji do docelowej architektury i innych inicjatyw, jak też czynności wykonywanych przez testera, w ramach np. wykonywania testów. Testy mają obejmować zarówno infrastrukturę, wszystkie aplikacje, oraz bezpieczeństwo sieciowe, aplikacji i baz danych.

Testy penetracyjne systemów muszą zostać wykonane w oparciu o metodykę Black-Box, Grey Box lub White-box, w której zespół testujący opiera się o wiedzę o aplikacji i systemie zabezpieczeń taką jak inni jego użytkownicy. Wykonawca w swojej metodyce musi uwzględnić proces zdobywania wiedzy dla testerów w tym zakresie.

„Aplikacje oraz systemy mają zostać przetestowane w oparciu o najlepsze praktyki w zakresie testów bezpieczeństwa zawartych w standardach OWASP (Open Web Application Security Project), OSSTMM, ISSAF lub równoważnych, a w szczególności o aktualną klasyfikację OWASP Top 10 oraz OWASP Testing Guide 4.0 lub równoważnych.

➤ Plan i realizacja usługi testów

Testy systemowe

Cel:

Pełna weryfikacja nowych funkcjonalności dla procesów i produktów pod kątem spełnienia wymagań systemowych.

Zakres:

W ramach testów systemowych ma mieć miejsce weryfikacja kompletnego systemu (wersji/modułu) w działaniu przez użytkownika infrastruktury i aplikacji Zamawiającego oraz weryfikacja spełnienia wymagań. Muszą być to zarówno wymagania funkcjonalne jak i нефункционаłne. Testy systemowe mają wykorzystywać dostępne typy testów. Testy funkcjonalne na tym poziomie mają zweryfikować kompletny system w działaniu na podstawie wszystkich testów нефункционаłnych, takich jak testy wydajności, bezpieczeństwa, migracji i operacyjne. Testy systemowe muszą zawierać podzbiór testów negatywnych.

- Przygotowanie Planu Testów;
- Przygotowanie scenariuszy i przypadków testowych testów systemowych funkcjonalnych;
- Realizacja i raportowanie wyników testów.

Produkty wyjściowe:

- Plan Testów;
- Scenariusze testowe przygotowane na podstawie wymagań;
- Logi potwierdzające wykonanie testów i ich statusy (w szczególności zrzuty ekranu oraz zgłoszenia defektów);
- Raport z testów.

Testy akceptacyjne

Cel:

Testy formalne przeprowadzane w celu potwierdzenia, że wszelkie wymagania postawione przed systemem zostały spełnione na odpowiednio wysokim poziomie jakości, a sam system działa poprawnie.

Zakres:

Testy akceptacyjne muszą stanowić podzbiór testów systemowych. Ich wykonanie ma nastąpić przy współudziale użytkownika końcowego Zamawiającego i/lub analityków biznesowych znających daną domenę. Do przeprowadzenia testów musi zostać wybrany podzbiór scenariuszy dla wszystkich testów нефункционаłnych, takich jak testy wydajności, bezpieczeństwa, migracji i operacyjne, który zaproponuje Wykonawca tak, aby móc przeprowadzić testy funkcjonalne w oparciu o techniki czarnoskrzynkowe.

Zaplanowane testowanie akceptacyjne będzie testowaniem potwierdzającym, co oznacza, że jego celem jest potwierdzenie możliwości użycia oprogramowania do realizacji celu, do którego zostało stworzone. Przy znalezieniu błędów Wykonawca musi sprawdzić i opisać możliwość pracy na obejściu tych błędów.

- Przygotowanie Planu Testów;
- Przygotowanie scenariuszy i przypadków testowych;
- Realizacja i raportowanie wyników testów.

Produkty wyjściowe:

- Plan Testów;
- Scenariusze testowe;
- Logi potwierdzające wykonanie testów i ich statusy;
- Raport z testów.

Testy regresji

Cel:

Sprawdzenie poprawności działania niezmiennych części oprogramowania, sprawdzenie, czy system nie uległ degradacji (regresji) po wprowadzeniu zmian.

Zakres:

Przy wyborze scenariuszy przewidzianych do zestawu testów regresji, musi zostać przeprowadzona analiza wpływu zmian w systemach na istniejące funkcjonalności biznesowe, które nie były modyfikowane w ramach wdrożeń. W zakresie testów muszą zostać uwzględnione priorytety biznesowe testowanych procesów oraz ryzyka techniczne i biznesowe systemów, w których te procesy są realizowane.

- Przygotowanie Planu Testów;
- Przygotowanie scenariuszy i przypadków testowych;
- Realizacja i raportowanie wyników testów.

Produkty wyjściowe:

- Plan Testów;
- Scenariusze testowe;
- Logi potwierdzające wykonanie testów i ich statusy;
- Raport z testów.

Testy End-to-End

Cel:

Sprawdzenie kompletnego procesu biznesowego, również w zakresie wykraczającym poza systemy informatyczne.

Zakres:

W celu sprawdzenia kompletnego procesu biznesowego Wykonawca musi zaproponować testy E2E, zarówno dla procesów, które przebiegają przez wiele systemów, jak i gdy część procesu wymaga przetwarzania manualnego poza systemami informatycznymi.

Jeżeli testy systemowe będą prowadzone w oparciu o specyfikację (wymagania), to dla lepszego pokrycia oprogramowania testami, testy akceptacyjne muszą zostać przygotowane w oparciu o procesy biznesowe (procesy E2E).

- Przygotowanie Planu Testów;
- Przygotowanie scenariuszy i przypadków testowych;
- Realizacja i raportowanie wyników testów.

Produkty wyjściowe:

- Plan Testów;

- Scenariusze testowe;
- Logi potwierdzające wykonanie testów i ich statusy;
- Raport z testów.

Testy wydajnościowe

Cel:

Wykonawca musi zaproponować i przeprowadzić testy wydajnościowe, które mają na celu określenie:

- wydajności podstawowej (Baseline Test),
- wydajności systemu przy zakładanym obciążeniu produkcyjnym (Load Test),
- obciążenia systemu przez dłuższy czas (Soak Test),
- maksymalnego dopuszczalnego obciążenia systemu przez jego zwiększanie, aż do momentu wystąpienia jego awarii (Stress Test),
- wydajności systemu w sytuacji konieczności obsługi dużych wolumenów danych lub operacji (Volume Test).

Zakres:

Realizacja testów obejmuje wykonanie zaproponowanego i odpowiedniego rodzaju testu wydajnościowego przy pomocy dedykowanych skryptów testowych, opisanych w metodyce, odzwierciedlających konkretne scenariusze wykorzystania aplikacji przez użytkownika lub żądania generowane w ramach integracji pomiędzy systemami. Skrypty służące do realizacji takiego testu mają zostać stworzone przy pomocy dedykowanego narzędzia wspierającego testy wydajnościowe i polegają na nagraniu ruchu generowanego i odbieranego przez aplikację, a następnie – odpowiednio sparametryzowane – uruchamiane będą wielokrotnie, symulując wykorzystywanie aplikacji przez określoną liczbę użytkowników. Wykonawca w swojej metodyce ma zaproponować i uzasadnić liczbę cykli wykonywania testu i iteracji, przy czym plan musi uwzględniać różne cele kolejnych cykli/iteracji – np.: weryfikacja wydajności systemu po implementacji poprawek, weryfikacja wydajności systemu po implementacji poszczególnych zmian, badanie wydajności systemu przy zmieniającym się obciążeniu. Testy wydajnościowe muszą polegać na weryfikacji wydajności systemu po stronie serwera/ów aplikacji i/lub bazy danych, jak i na badaniu czasu reakcji samego interfejsu graficznego użytkownika w czasie obciążenia systemu. Wykonawca do tych pomiarów musi użyć własnych dodatkowych narzędzi, które musi dostarczyć i zaimplementować w infrastrukturze Zamawiającego.

Wykonawca, poza wygenerowaniem obciążenia, musi na bieżąco przeprowadzać monitoring parametrów środowiska testowanego. Monitoring musi zostać prekonfigurowany wg planu przy pomocy dedykowanego do tego celu narzędzia i umożliwiać wskazanie zależności pomiędzy generowanym obciążeniem i ewentualnym obniżeniem wydajności poszczególnych komponentów środowiska, tak aby było możliwe zidentyfikowanie „wąskich gardeł” systemu. Monitoring musi zostać zastosowany minimum do następujących komponentów i ich parametrów:

- system operacyjny serwera bazy danych,
- system operacyjny serwera aplikacji,
- serwer aplikacji,
- silnik bazy danych.

Realizacja testów wydajnościowych obejmuje wykonanie następujących kroków:

- Opracowanie Profilu Ruchu;
- Przygotowanie Planu Testów;
- Przygotowanie środowiska uruchomieniowego dla skryptów wydajnościowych;
- Generowanie danych wejściowych, wymaganych do realizacji testów wydajnościowych;
- Projektowanie i implementacja automatów testowych;
- Zestawienie i konfiguracja monitoringu;
- Badanie możliwości środowiska (skalowanie środowiska);
- Wykonanie Testu (pomiar wydajności środowiska);
- Analiza wyników i raportowanie.

Produkty wyjściowe:

- Plan Testów;
- Profil Ruchu;
- Skrypty testów wydajnościowych;
- Raport z testów wydajnościowych, w tym rekomendacje zmian.

Testy bezpieczeństwa (Testy penetracyjne aplikacji)

Cel:

Wykonawca musi wykonać zaawansowane testy bezpieczeństwa pod kątem przedstawienia rzeczywistego obrazu bezpieczeństwa aplikacji. Obejmą one w całości problem bezpieczeństwa danego systemu oraz wykonaniu kontrolowanych prób ataku. Muszą pozwolić Zamawiającemu na ocenę bezpieczeństwa aplikacji poprzez symulację ataku prawdziwego włamywacza komputerowego lub złośliwego użytkownika sieci. Testy te muszą być wykonane na kopii realnego środowiska np. w środowisku zwirtualizowanym tak, aby sprawdzić realne, a nie potencjalne zagrożenia zabezpieczenia. Testy te muszą dotyczyć samej aplikacji, jak i systemów zabezpieczeń chroniących dostęp do aplikacji.

Zakres:

- Przygotowanie Planu Testów;
- Przygotowanie przypadków testowych na wysokim poziomie szczegółowości, jakie będą wykorzystywane do przeprowadzenia testów penetracyjnych;
- Realizacja testów:
 - analiza sposobu działania systemu (aplikacji),
 - testy analityczne aplikacji pod kątem bezpieczeństwa informacji przekazywanych pomiędzy aplikacją a przeglądarką internetową,
 - analiza zarządzania sesjami autoryzowanych użytkowników,
 - analiza informacji zapisywanych po stronie użytkownika, np. w obiektach „cookie”,
 - testy skanerami automatycznymi, również z poziomu zalogowanego użytkownika,
 - sprawdzenie odporności na ataki typu XSS (Cross-Site Scripting),

- sprawdzenie odporności na ataki typu XSRF (Cross-Site RequestForgery),
 - praktyczna weryfikacja znalezionych podatności – exploity i programy autorskie.
- Raportowanie wyników testów - w oparciu o zmodyfikowany w tym celu szablon Zamawiającego, bądź szablon Wykonawcy, dedykowany do raportowania testów bezpieczeństwa

Produkty wyjściowe:

- Raport z testów bezpieczeństwa zawierający wykryte podatności wraz z oceną odporności aplikacji na ataki oraz rekomendacjami dotyczącymi naprawy wykrytych uchybień;
- Plan testów bezpieczeństwa;
- Scenariusze testowe;
- Raport z testów bezpieczeństwa dla kadry zarządczej z przeprowadzonych testów bezpieczeństwa;
- Raporty z testów bezpieczeństwa muszą być dostarczone zarówno w formacie pdf, jak i MS Word.

Testy użyteczności

Cel:

Weryfikacja i efektywność satysfakcji z jaką użytkownicy aplikacji Zamawiającego realizują określone zadania w systemie, w zdefiniowanym kontekście.

Zakres:

Wykonawca musi przetestować aplikacje każdego obszaru pod kątem użyteczności systemu bazując na wytycznych dotyczących ergonomii systemów, pokazując możliwość zwiększenia funkcjonalności systemu, przejrzystości systemu i funkcjonalności oczekiwanej systemu (Usability Testing).

Użyteczność aplikacji jaka ma zostać określona to:

- efektywność wykonywania zadań przez użytkownika,
- liczbę popełnianych błędów,
- łatwość nauczenia się obsługi systemu,
- łatwość zapamiętania jego obsługi,
- satysfakcję z użytkowania.

W podejściu Wykonawcy do testów użyteczności muszą się znaleźć trzy główne grupy działań, służące ocenie użyteczności:

- audyt ekspercki,
- testy z użytkownikami,
- analiza porównawcza rozwiązań z rynku.

Wykonawca musi również przeprowadzić analizę porównawczą rynku jako narzędzie dodatkowe w przypadku oceny rozwiązań typowych, które mają swoje odpowiedniki na rynku.

Produkty wyjściowe:

- Plan Audytu eksperckiego;
- Plan Testów z Użytkownikiem;
- Scenariusze testowe;

- Heurystyki i listy kontrolne;
- Logi potwierdzające wykonanie testów i ich statusy;
- Raport z testów.

Testy integracyjne

Cel:

Wykrycie defektów i problemów w interfejsach i interakcjach pomiędzy systemami.

Zakres:

Wykonawca wykona testy styków integracyjnych oraz wykona walidację danych znajdujących się w obydwu systemach w zakresie wszystkich interfejsów systemowych, które zostały zinwentaryzowane na etapie wstępnym niniejszego zamówienia. Testy muszą objąć sprawdzenie zintegrowanego rozwiązania z perspektywy użytkownika systemu pod kątem nowych funkcjonalności.

- Przygotowanie Planu Testów (szczegółowe podejście do realizacji testów, lista scenariuszy testowych, wymagania co do WSDL, przykładowych XML oraz zaślepek i symulatorów niezbędnych do wykonania testów);
- Przygotowanie scenariuszy i przypadków testowych testów funkcjonalnych;
- Realizacja i raportowanie wyników testów.

Produkty wyjściowe:

- Plan Testów;
- Scenariusze testowe przygotowane na podstawie wymagań;
- Logi potwierdzające wykonanie testów i ich statusy (w szczególności zrzuty ekranu oraz zgłoszenia defektów);
- Raport z testów.

Inne usługi

Wykonawca w ramach zamówienia musi zaproponować wszystkie rodzaje testów, jakie ma wykonać, również te które są niezbędne a nie zostały wymienione powyżej. Dodatkowe testy muszą wynikać z potrzeb architektury aplikacji wynikającej z inwentaryzacji.

➤ *Zarządzanie testami*

Wykonawca w metodyce swojego działania musi opisać, a po akceptacji Zamawiającego stosować, model zarządzania testami.

Zarządzanie testami musi obejmować m.in.:

1. Analizę i dobór odpowiedniego modelu organizacyjnego najlepszego dla Zamawiającego.
2. Tworzenie indywidualnej lub modyfikacja istniejącej strategii oraz metodyki testów.
3. Organizację procesu testów zgodnie z modelem przyjętym przez Zamawiającego.
4. Budowanie i zarządzanie zespołami testów.
5. Tworzenie planu dostarczenia środowisk testowych.
6. Przygotowanie danych testowych wraz z ich anonimizacją.
7. Zdefiniowanie narzędzi testowych oraz podejścia do ich użytkowania.

8. Nadzór nad prawidłowym przebiegiem procesu testowego (planowanie/realizacja).
9. Nadzór nad przebiegiem poprawności cyklu życia zgłoszonych defektów.

Zarządzanie problemami testowymi obejmuje takie aktywności jak:

- identyfikacja defektów blokujących testy,
- identyfikacja problemów testowych wymagających rozwiązania,
- komunikację problemów blokujących,
- aktywne wsparcie rozwiązywania problemów – obejmujące takie działania jak: egzekwowanie działań poszczególnych uczestników wdrożenia, spotkania i konferencje, angażowanie Kierowników Projektów, eskalacje.

➤ *Automatyzacja testów*

Cel:

Zwiększenie pokrycia testami i skrócenie czasu trwania testów w obszarach systemu, które są kluczowe z punktu widzenia biznesu, a przy tym wymagają częstej weryfikacji przy pojawianiu się kolejnych wersji aplikacji lub po poprawie wykrytych problemów.

Zakres:

Automatyzacja testów ma zostać zrealizowana w połączonym modelu tradycyjnym (waterfall) i zwinnym (agile), zintegrowanym ze środowiskiem programistycznym i z wykorzystaniem serwera ciągłej integracji (Continuous Integration). Dodatkowo w procesie wytwarzania skryptów testowych mają zostać zastosowane techniki Behavior-Driven Development i wspierające je dedykowane narzędzia do integracji środowiska w pełni zautomatyzowanych testów funkcjonalnych i wydajnościowych. Dla obu modeli ma zostać zbudowane Środowisko Testów Automatycznych wraz z repozytorium skryptów testów automatycznych.

W ramach automatyzacji testów funkcjonalnych zakłada się realizację przez Wykonawcę następujących rodzajów testów:

- Smoke testy – zestaw testów przeznaczony do podstawowej weryfikacji środowiska testowego po jego instalacji i/lub wdrożeniu każdej kolejnej wersji systemu (np. wersji poprawkowej), umożliwiającej weryfikację i ocenę poprawności działania środowiska przed rozpoczęciem na nim innych aktywności testowych;
- Testy regresji – zestawy testów, przeznaczone do weryfikacji funkcjonalności nieobjętych zmianami w ramach wdrożenia nowej wersji systemu; zakres automatycznych testów regresji będzie ustalany dla danego projektu, z uwzględnieniem następujących kryteriów:
 - potrzeby,
 - korzyści,
 - możliwości/latwości utrzymania.

Wykonawca przygotowuje testy automatyczne zgodnie z poniższymi zasadami:

- Testy będą odpowiednio sparametryzowane, a dane do testów w miarę możliwości będą pozyskiwane w sposób automatyczny (na przykład przez zapytanie PL/SQL). Jeśli w systemie nie ma odpowiednich danych to zostanie podjęta próba poprzedzenia wykonania danego testu dedykowanym skryptem przygotowującym odpowiednie dane. W szczególnych przypadkach,

w zależności od charakterystyki systemu oraz specyfiki przygotowania niezbędnych danych, automatyzacja procesu przygotowywania danych może okazać się nieefektywna pod względem czasowym i kosztowym.

- Testy będą opisane w sposób umożliwiający zrozumienie zakresu weryfikacji; w szczególności będą posiadały nagłówek w formie komentarza, w którym będzie opisane co skrypt robi, jakie ma zależności i ewentualnie jakie ograniczenia. Ponadto, każdy skrypt będzie zawierał również informacje o rewizji wersji.

Na potrzeby realizacji automatyzacji testów, Wykonawca będzie wybierał i uzgadniał z Zamawiającym narzędzie wspierające automatyzację testów funkcjonalnych w danym obszarze/systemie. Wykonawca będzie w pierwszej kolejności starał się zastosować narzędzia typu open-source. Mogą jednak zaistnieć sytuacje, w których tego typu narzędzia nie będą spełniały oczekiwań i w takich sytuacjach będzie rekomendowane zastosowanie narzędzia komercyjnego.

Produkty wyjściowe:

- Środowisko Testów Automatycznych;
- Repozytorium Automatycznych Skryptów Testowych;
- Raport z testów automatycznych wraz z logami oraz np. zrzutami ekranów;
- Raport zgłoszonych i otwartych błędów.

➤ *Przygotowanie i utrzymanie środowisk testowych, w tym anonimizacja danych*

Przygotowanie i anonimizacja danych testowych

Przy generowaniu i anonimizacji testów, muszą zostać uwzględnione następujące elementy:

- spójność danych pomiędzy zintegrowanymi ze sobą systemami w danym środowisku testowym,
- zakres niezbędnych danych i ewentualne zakwalifikowanie ich jako wrażliwe,
- odpowiednia ilość danych,
- zgodność poszczególnych typów danych z przyjętym dla nich formatem (maskowanie),
- algorytmy generowania danych (np. PESEL),
- zgodność typów danych i odpowiedniego zakresu słownikowego,
- możliwość generowania/anonimizowania danych z wykorzystaniem losowych ciągów znaków.

Wykonawca musi założyć, że odpowiedzialność za dostępność danych testowych na potrzeby realizacji testów będzie po jego stronie, a zapewniona będzie przez wygenerowanie nowych danych lub zanonimizowanie już istniejących. Generowanie i anonimizacja danych musi odbywać się na podstawie materiałów wejściowych tylko ze strony Zamawiającego. W celu zapewnienia danych testowych (w tym anonimizacji) i w zależności od warunków technicznych, Wykonawca stosuje jedno z lub zestaw kilku przeznaczonych do tego narzędzi dostępnych na rynku. W przypadku zaistnienia takiej potrzeby, proces generowania danych może zostać wsparty przy pomocy dedykowanych skryptów automatycznych testów funkcjonalnych i/lub wydajnościowych.

Przygotowanie i utrzymanie środowisk testowych

W zakresie procesu przygotowania i utrzymania środowisk testowych (w tym zarządzania środowiskiem) Wykonawca musi zarekomendować zastosowanie jednego z dostępnych i sprawdzonych narzędzi DevOps.

Opis narzędzia musi się znaleźć w metodyce testów. Narzędzia te muszą wspierać wymienione wcześniej procesy przez maksymalną automatyzację związanych z nimi zadań oraz zwiększenie przejrzystości procesu wdrażania kolejnych wersji oprogramowania. Narzędzia będą w przyszłości wykorzystywane przez różne zespoły biorące udział w procesie wytwarzania i wdrażania oprogramowania, co ma na celu:

- skrócić czas trwania cykli wydań aplikacji,
- zwiększyć elastyczność biznesową i operacyjną,
- uprościć i ustandaryzować proces wydań oprogramowania,
- zredukować koszty związane z developmentem,
- wspierać współpracę pomiędzy różnymi zespołami IT (np. rozwojowym i utrzymaniowym).

W zależności od potrzeb, Wykonawca zapewni instalację, konfigurację, a następnie aktualizację i utrzymanie środowisk testowych.

➤ *Dokumentacja testów*

Dokumentacja testów będzie realizowana zgodnie z propozycją zakresu dokumentów wymienionych w niniejszym OPZ oraz z potrzebami wynikłymi na etapie inwentaryzacji. Szczegółowy zakres prac w zakresie dokumentacji testów będzie ujęty w ramach opisu metodyki testów.

Wykonawca musi przygotować minimum:

- Plan testów, zawierający:
 - cele i zakres testów,
 - harmonogram testowania,
 - podejście (sposób przeprowadzenia testów),
 - techniki projektowania i wykonania testów,
 - zasoby niezbędne do realizacji czynności testowych,
 - produkty prac testowych,
 - ryzyka związane z testowaniem.
- Scenariusze testowe, zawierające:
 - uporządkowany zbiór (sekwencja) przypadków testowych, które mają być wykorzystane do przetestowania konkretnego procesu biznesowego lub User Story opisującego wymagania w ramach danego zamówienia.
- Przypadki testowe, mające na celu:
 - wykonanie testów części scenariusza, który może zawierać wiele przypadków testowych. Z reguły przypadek testowy zamyka się w czynnościach do wykonania w jednym systemie przez jedną osobę.

Proces raportowania testów obejmie zarówno raportowanie realizacji testów na poziomie Operacyjnego Procesu Testowego, jak również Procesu Zarządzania Testami. Strategia testów musi zawierać metody nadzoru i raportowania postępu w testach oraz rekomendacje odnośnie raportowania (liczby, częstotliwości raportów).

W ramach raportowania i monitorowania prac testowych zakłada się przygotowywanie i dystrybucję

następujących raportów:

- Raporty postępu prac (dzienny lub tygodniowy),
- Raport końcowy z testów.

Raporty będą przygotowywane na podstawie informacji dostępnych w wykorzystywanych narzędziach do zarządzania testami oraz rozsyłane do interesariuszy w formie elektronicznej.

Zakres i częstotliwość raportowania będą uzależnione od złożoności zakresu i/lub przedmiotu testów.

- Raport z postępu prac zawiera:
 - Informacje z postępu testów w formacie wskazanym przez Zamawiającego w trybie tygodniowym.
 - Raport przygotowywany w celu monitorowania bieżącego statusu testów. Zbudowany jest na podstawie danych z całego okresu testów, umożliwiając obserwację postępu prac wykonanych, kontrolę zgodności z harmonogramem oraz szybkie identyfikowanie i reagowanie na zagrożenia dla realizacji planu.
 - Raport obejmuje podsumowanie statusu prac w kluczowych obszarach związanych z testami dotyczącymi postępu realizacji testów, statystyki defektów, ryzyk, problemów, kluczowych defektów.
- Raport końcowy z wykonania testów zawiera:
 - Informacje umożliwiające ocenę jakości testowanego rozwiązania, tworzony na zakończenie projektu bądź całego programu, w ramach procesu zamknięcia testów.
 - Zakres zrealizowanych testów, ze szczególnym uwzględnieniem różnic względem zakresu opisanego w Planie testów.
 - Podsumowanie przebiegu prac uwzględniające napotkane trudności i ewentualne odstępstwa od Planu testów.
 - Podsumowanie wyników testów.
 - Łączną listę otwartych problemów wraz z planem ich usunięcia. Wykonawca nie odpowiada za realizację w/w planu w szczególności, gdy działania dotyczą Zamawiającego lub stron trzecich.
 - Rekomendację przekazania systemu/aplikacji do kolejnego etapu testów oraz szczegółowe wyniki/rezultaty (dokumentacja efektów przeprowadzonych testów).
 - Ze względu na różnice metodyczne w podejściu i realizacji różnych rodzajów testów, Wykonawca zakłada dostosowanie raportu z zakończenia testów do różnych potrzeb. W przypadku testów bezpieczeństwa raport końcowy zawierać będzie min. opis zakresu testów i środowiska testowego, wykryte podatności i błędy oraz ocenę odporności aplikacji na ataki komputerowe, rekomendacje dotyczące naprawy wykrytych uchybień.
 - Raporty z testów bezpieczeństwa zostaną przekazane Zamawiającemu w postaci zaszyfrowanej, drogą elektroniczną na wskazany przez Zamawiającego adres e-mail, za pośrednictwem ustalonych wcześniej bezpiecznych kanałów komunikacji.

Zamawiający dostarczy szablony/wzory dokumentów, jakie mają być stosowane przez Wykonawcę. W przypadku ich braku lub uwag co do zawartości Wykonawca zaproponuje swoje rozwiązania lub zmiany.

➤ *Role i odpowiedzialności*

Wykonawca odpowiada za:

- przyjęcie zgłoszenia i przygotowanie dla niego wyceny zakresu i harmonogram prac,
- usługę przygotowania i realizacji testów, w szczególności:
 - analizę wymagań do systemów i zmian systemów,
 - dostarczenia wszystkich składników procesu testowania,
 - wykonanie testów, retestów poprawek i utrzymanie repozytorium dokumentacji testów.

Zamawiający odpowiada za:

- dostarczenie niezbędnych danych, dokumentacji i informacji niezbędnej do oszacowania zgłoszenia,
- dostarczenie szablonów dokumentów oraz opisu obowiązujących u Zamawiającego procesów obsługi błędów i scenariuszy testowych oraz innych procesów mających z nim styk,
- zapewnienie środowiska testowego zasilonego inicjalnie danymi, przez cały okres świadczenia usługi.

➤ *Ogólne założenia realizacyjne*

Na etapie finalnych uzgodnień pomiędzy Zamawiającym, a Wykonawcą, odnośnie podejścia do realizacji usług, zakłada się utworzenie bardziej szczegółowej listy zadań oraz przypisanie odpowiedzialności w układzie macierzy RACI.

Ponadto:

- 1) Wykonawca wyznaczy Koordynatora, odpowiedzialnego za obsługę zleceń, koordynację prac zespołu po stronie Wykonawcy, komunikację w zakresie kluczowych zagadnień (np. raportowanie postępu, bieżące zarządzanie zagrożeniami dla efektywnej i terminowej realizacji prac) oraz za realizację usług zgodnie z zamówieniem.
- 2) Zamawiający wyznaczy Koordynatora, którego rolą będzie zapewnienie dostępu do wymaganych zasobów potrzebnych dla zaplanowania i realizacji testów, w tym:
 - a. podejmowanie kluczowych decyzji w zakresie testów, wyznaczanie priorytetów,
 - b. wyznaczanie osób merytorycznych ze strony Zamawiającego,
 - c. zapewnienie wsparcia merytorycznego prac w kwestiach specyficznych dla badanego systemu, w szczególności przy opracowywaniu Profilu Ruchu i budowie monitoringu testowanego środowiska,
 - d. ustalanie spotkań z osobami merytorycznymi,
 - e. dostarczanie dokumentacji niezbędnej do realizacji prac testowych,
 - f. zapewnienie dostępności środowiska testowego na uzgodnionym poziomie,
 - g. zapewnienie wsparcia administratorów systemu w trakcie prac, w szczególności na potrzeby: zapewnienia bezpieczeństwa danych, filtrowania danych testowych, zarządzania ruchem sieciowym, zarządzanie dostęпами aplikacyjnymi.

- 3) Szczegółowy zakres prac i podejście do jego realizacji, warunki realizacji, harmonogram a także stosowane narzędzia, mierniki KPI/SLA, będą każdorazowo określone na etapie procesowania zamówienia i ustalania warunków realizacji usług testowych.
- 4) Zamawiający udostępni środowisko testowe dla przygotowania i realizacji uzgodnionych testów, w tym funkcjonalnych i нефункциональных, w terminach wynikających z uzgodnionego harmonogramu prac, w tym:
 - a. otworzy porty i ruch sieciowy dla komunikacji monitoringu środowisk,
 - b. wykona strojenie, poprawki i zmianę konfiguracji aplikacji w sytuacji, gdy okaże się, że środowisko tego wymaga,
 - c. wyznaczy okna testowe dla testów wydajnościowych.
- 5) Zamawiający zapewni dostęp zdalny (VPN) w zakresie wymaganym do świadczenia usługi w trybie 24x7 dla wskazanych przez Wykonawcy członków zespołu projektowego.
- 6) Zamawiający zapewni i przekaze zespołowi Wykonawcy niezwłocznie po podpisaniu Umowy, w ramach której będzie realizowane procesowanie zgłoszeń, następujące materiały:
 - a. aktualną dokumentację organizacji procesu wytwórczego, w tym:
 - i. strukturę organizacyjną obszaru realizującego projekty deweloperskie, wraz z liczbą pracowników,
 - ii. roadmapę projektów i cele realizacyjne,
 - iii. dostęp do wiedzy domenowej o systemach i aplikacjach testowanych będących przedmiotem testów;
 - b. aktualną dokumentację procesu testowego, w tym:
 - i. istniejącą politykę i strategię testów,
 - ii. istniejące opisy procesów, procedur,
 - iii. istniejące szablony dokumentów (produkty testowe) tj. plan testów, raport z testów, zgłoszenia defektów, itp.;
 - c. opisy innych procedur, procesów mających styk z procesem testowym, tj. proces zarządzania zmianą, proces zarządzania wdrożeniami, proces zarządzania ryzykiem, proces zarządzania środowiskami testowymi itp.
- 7) Zamawiający zapewni dostępność niezbędnych pracowników w celu przeprowadzenia wywiadów i szkoleń dla Wykonawcy.
- 8) Do przeprowadzenia testów penetracyjnych niezbędne jest:
 - a. zapewnienie wsparcia Administratora Zamawiającego dla systemów podlegającym testowaniu,
 - b. udostępnienie aplikacji będącej przedmiotem testów po adresie IP lub po nazwie domenowej,
 - c. zapewnienie kont dla użytkowników o wszystkich przewidywanych profilach uprawnień dla każdej z aplikacji (w liczbie co najmniej dwa konta dla danej roli) – jeśli nie wszystkie testy interfejsów aplikacyjnych będą wymagały udostępnienia kont testowych, bądź Zamawiający uzna, że system nie będzie testowany z ujęciem profili, wówczas Wykonawca przeprowadzi testy bez posiadania użytkowników w systemie.

- 9) Jeśli na środowisku testowym zastosowane są jakieś blokujące analizatory pakietów TCP / IP / service (IPS), to przed rozpoczęciem każdego procesu testowania wpisy dla dostępów Wykonawcy powinny zostać wyczyszczone, aby uniknąć blokad dostępu maszyn Wykonawcy po serii np. "groźnych zapytań".

➤ *Personel Wykonawcy*

Wykonawca zobowiązuje się, że 35 osób bezpośrednio realizujących Umowę będzie w okresie realizacji Umowy zatrudnionych na pełen etat na podstawie umowy o pracę w rozumieniu przepisów ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 2022 r. poz. 1510, z późn. zm.).

➤ *Równoważność*

- Opisując przedmiot zamówienia przez odniesienie w dokumentacji do norm, klasyfikacji oraz standardów, Zamawiający wskazuje, że dopuszcza rozwiązania równoważne opisywanym, tj. nie gorsze niż parametry jakimi charakteryzuje się opis wskazany w niniejszej dokumentacji, służący uzyskaniu jak najwyższej jakości do realizacji przedmiotu zamówienia.

➤ *Minimalna, wymagana lista ról projektowych, jakich oczekuje Zamawiający do realizacji Umowy:*

1. Koordynator testów AI – 1 osoba
2. Koordynator Testów – 2 osoby
3. Audytor – 1 osoba
4. Tester Wiodący Bezpieczeństwa – 1 osoba
5. Analityk Architektury – 1 osoba
6. Analityk Baz danych – 1 osoba
7. Tester – 40 osób
8. Tester Automatyczny – 6 osób
9. Tester Wydajnościowy – 6 osób
10. Tester bezpieczeństwa – 4 osoby
11. Tester bezpieczeństwa – obszaru konteneryzacji – 1 osoba
12. Tester Wiodący Wydajności – 1 osoba
13. Tester Wiodący Automatyzacji – 1 osoba

Załączniki do Opisu Przedmiotu Zamówienia (OPZ):

Załącznik nr 1 - Metodyka testów;

Załącznik nr 2 - Wymagania do testów bezpieczeństwa - penetracyjnych;

Załącznik nr 3 - Minimalna, wymagana lista ról projektowych.