

Załącznik nr 1 do Umowy nr

Opis Przedmiotu Zamówienia

1. Wstęp

Przedmiotem zamówienia jest przeprowadzenie dwóch zewnętrznych audytów bezpieczeństwa, wydajności, dostępności oraz jakości kodu oprogramowania i zgodności z wytycznymi WCAG 2.1 dla systemu teleinformatycznego Elektroniczne Postępowanie Upominawcze 3.0 (zwanego dalej EPU3.0) oraz sporządzenie raportu z wykonania każdego tych audytów (zwanego dalej „Raportem”).

Przedmiot zamówienia dzieli się na dwa etapy:

Etap 1 - pierwszy audyt dotyczy infrastruktury Zamawiającego opisanej w pkt 2. i zaplanowany jest na III kwartał 2025, kończy się przedstawieniem raportu końcowego.

Etap 2 – drugi audyt dotyczy infrastruktury Zamawiającego opisanej w pkt 3. i zaplanowany jest na IV kwartał 2025. Rozpoczyna się po zakończeniu i odebraniu etapu 1 i kończy się przedstawieniem raportu końcowego.

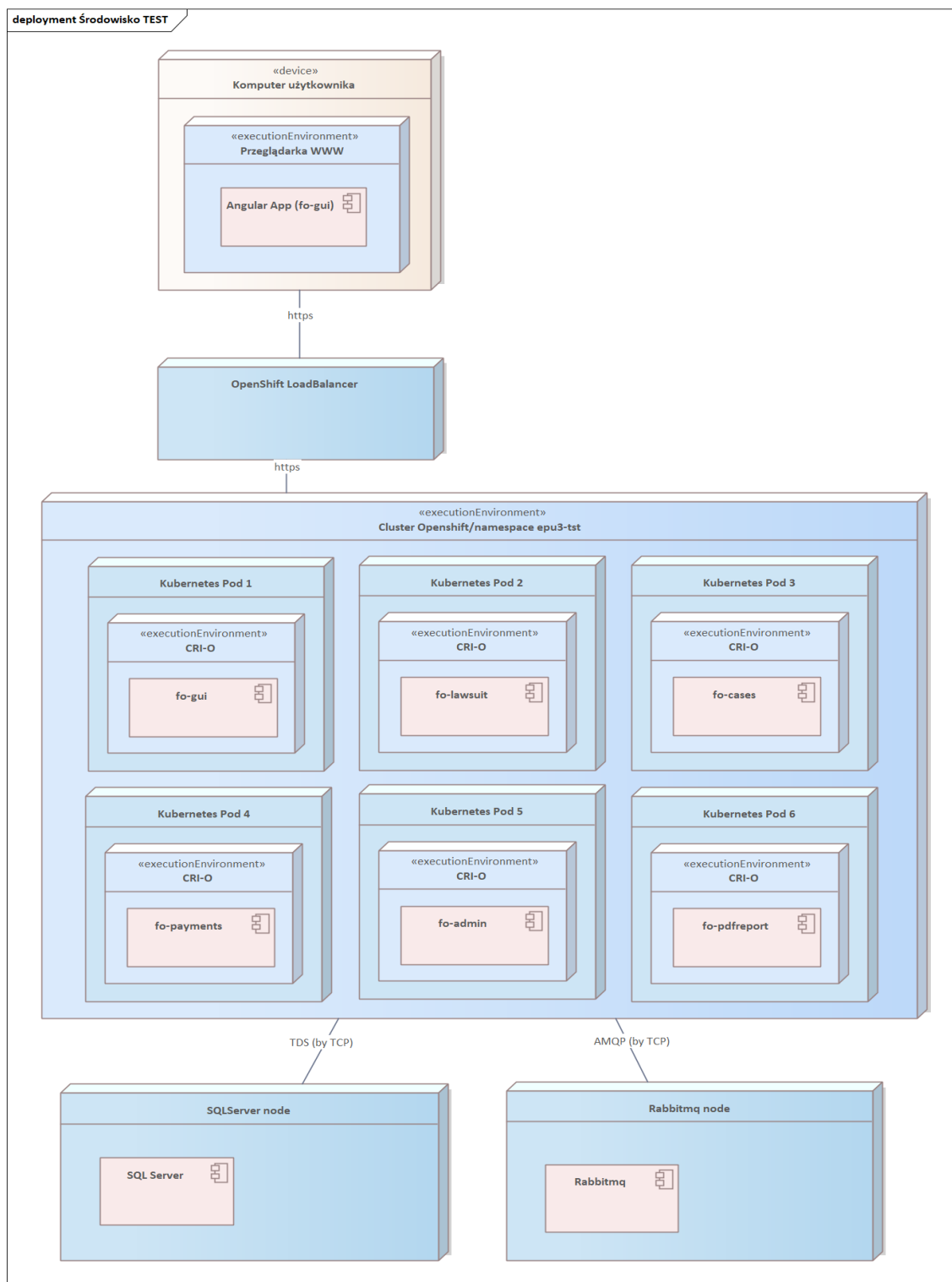
Każdy z obu audytów bezpieczeństwa systemu IT ma określić aktualny poziom zabezpieczeń EPU3.0 (zgodnie ze standardami określonymi w pkt. 5 OPZ) oraz wskazanie czynników mogących mieć wpływ na obniżenie tego poziomu. Ponadto poprzez wnioski zawarte w raporcie każdy z audytów ma na celu zaproponowanie rozwiązań, które doprowadzą system EPU3.0 do zwiększenia obecnego poziomu bezpieczeństwa. Każdy z audytów będzie obejmował przeprowadzenie badań i analiz umożliwiających wskazanie zagrożeń wynikających z:

- cech zaprojektowanej topologii i zasad współpracy systemów,
- zastosowanych technologii i standardów zabezpieczeń,
- jakości implementacji systemów,
- architektury styków międzysieciowych,
- słabości oprogramowania oraz poprawności konfiguracji komponentów rozwiązania, takich jak: systemy obsługi transmisji, systemy zaporowe i inne systemy usługowe i pomocnicze;

Wykonawcą testów bezpieczeństwa nie może być dostawca systemu EPU3.0 lub podmiot zależny od dostawcy systemu.

2. Opis systemu EPU 3.0 – Część Publiczna – dla audytu I

W celu zobrazowania specyfiki systemu EPU3.0 zamieszczono poniżej podstawowy diagram i opis architektury oraz usług realizowanych przez system.



Rysunek 1. Diagram wdrożenia systemu EPU 3.0 Część Publiczna na środowisko Test

System EPU3.0 budowany jest w architekturze microserwisów i uruchamiany jest na prywatnej chmurze obliczeniowej. Środowiskiem uruchomieniowym dla kontenerów systemu jest dedykowany namespace (projekt) w ramach klastra OpenShift. Poszczególne kontenery (usługi) systemu EPU 3.0 można częściowo zakwalifikować do warstw z tradycyjnej, warstwowej architektury systemów:

1) warstwa prezentacji

Interfejsem użytkownika systemu EPU 3.0 jest aplikacja Angular działająca na poziomie okna przeglądarki internetowej. Aplikacja jest udostępniona do pobrania z kontenera **fo-gui**.

Część funkcjonalności aplikacji dostępna jest dla niezalogowanych użytkowników (mapa strony, aktualność, podstawowe informacje, weryfikacja dokumentu na podstawie kodu dostępu), główna część funkcjonalności dostępna jest dla zalogowanych użytkowników (wszystkie funkcjonalności, w tym składanie pozwów, pism procesowych, wniosków, środków odwoławczych, dostęp do skrzynek odbiorczych/nadawczych).

2) warstwa aplikacji i logiki biznesowej

Aplikacja angular komunikuje się po https (REST API) z różnymi modułami backendowymi, które dostarczają właściwych usług. W tej warstwie dostępne są następujące moduły backendowe:

- fo-lawsuit – usługa umożliwiająca złożenie nowych pozwów,
- fo-cases – usługa odpowiedzialna za wizualizację i zarządzanie sprawami sądowymi,
- fo-admin - usługa odpowiedzialna za dostarczanie funkcjonalności skrzynek dla dokumentów (obiektów procesowych),
- fo-payments – usługa wspomagająca dokonywania płatności za czynności procesowe,
- fo-pdfreport – usługa odpowiedzialna za generowanie dokumentów PDF.

Funkcjonalności (zasoby) wymagające identyfikacji i uwierzytelnienia użytkownika są zabezpieczone koniecznością przedstawienia w żądaniu poprawnego tokena JWT. Uzyskanie i weryfikacja tokena oparta jest o protokół OCID/OAuth2. Zaś jako serwer tożsamości wykorzystywany jest system Moduł Tożsamość.

3) warstwa bazodanowa

Wykorzystanymi bazami danych dla modułów backendowych są bazy MS SQL. W tej warstwie dostępne są następujące bazy danych:

- epu-lawsuit – baza danych dla modułu fo-lawsuit,
- epu-cases - baza danych dla modułu fo-cases,
- epu-admin - baza danych dla modułu fo-admin,
- epu-payments - baza danych dla modułu fo-payments

4) warstwa komunikacyjna/integracyjna

Komunikacja między poszczególnymi modułami backendowymi odbywa się poprzez REST API, w przypadku komunikacji synchronicznej lub w przypadku komunikacji

— asynchronicznej poprzez brokera wiadomości RabbitMQ. Docelowo RabbitMQ powinien

być wdrożony poza klastrem openshift, na dedykowanym serwerze (serwerach). Aktualnie na środowisku Test broker uruchomiony jest w ramach klastra OpenShift jako kolejny kontener (epu-rabbitmq).

5) Infrastruktura serwerowa

System EPU3.0 uruchamiany jest w kontenerach na klastrze RedHat OpenShift. A więc jest wysoce zwirtualizowany. Fizyczna architektura oraz warstwa systemu operacyjnego wynika ze sposobu instalacji i konfiguracji OpenShifta.

Aktualnie system EPU3.0 Część Publiczna korzysta z następujących technologii i narzędzi:

- a) technologie i biblioteki aplikacyjne - warstwa prezentacji:
 - Angular,
 - Nginx
- b) technologie i biblioteki aplikacyjne - warstwa aplikacji, logiki biznesowej:
 - Obraz bazowy dla kontenerów: mcr.microsoft.aspnet:8.0
 - Platforma SDK: .Net Core 8.0
 - Języki programowania: C#,
 - Serwer kolejek: RabbitMQ
- c) systemy operacyjne oraz platformy wizualizacyjne:
 - RedHat OpenShit,
 - Microsoft Windows Server (db SQLServer),

Wykonawca zrealizuje przedmiot umowy z siedziby zamawiającego lub w formie pracy zdalnej. Wymóg analizy architektury i konfiguracji sieci dotyczy tylko fragmentu infrastruktury związanego z systemem EPU3.0, np. zbadanie reguł komunikacji sieciowej pomiędzy komponentami, np. bazą danych a Frond-End, konfiguracji systemu operacyjnego pod kątem wdrożonych zabezpieczeń, tj. konfiguracji systemu operacyjnego np. uruchomianych usług, aktualizacji, konfiguracji lokalnych polityk FireWall etc. Badania muszą uwzględniać również kanał komunikacyjny pomiędzy systemem EPU3.0 a systemami zewnętrznymi podlegającymi integracji z EPU 3.0 Część publiczna :

System	Nazwa/Opis	Główny przeadek użycia/wymieniane informacje	Interfejs
e-Płatności	System płatności online	Dokonywanie płatności za złożony pozew. Zwrot opłaty.	REST & HTTP Redirect
Moduł Tożsamość	Węzeł Krajowy Identyfikacji Elektronicznej	Identyfikacja użytkownika	REST/OpenID Connect
KRS	Krajowy Rejestr Sądowy	walidacja/autouzupełnienie danych stron postępowania nie będących osobami fizycznymi	REST
ROBUS	Radcy, Adwokaci, Pełnomocnicy	Walidacja podczas zakładania konta o profilu pełnomocnika	

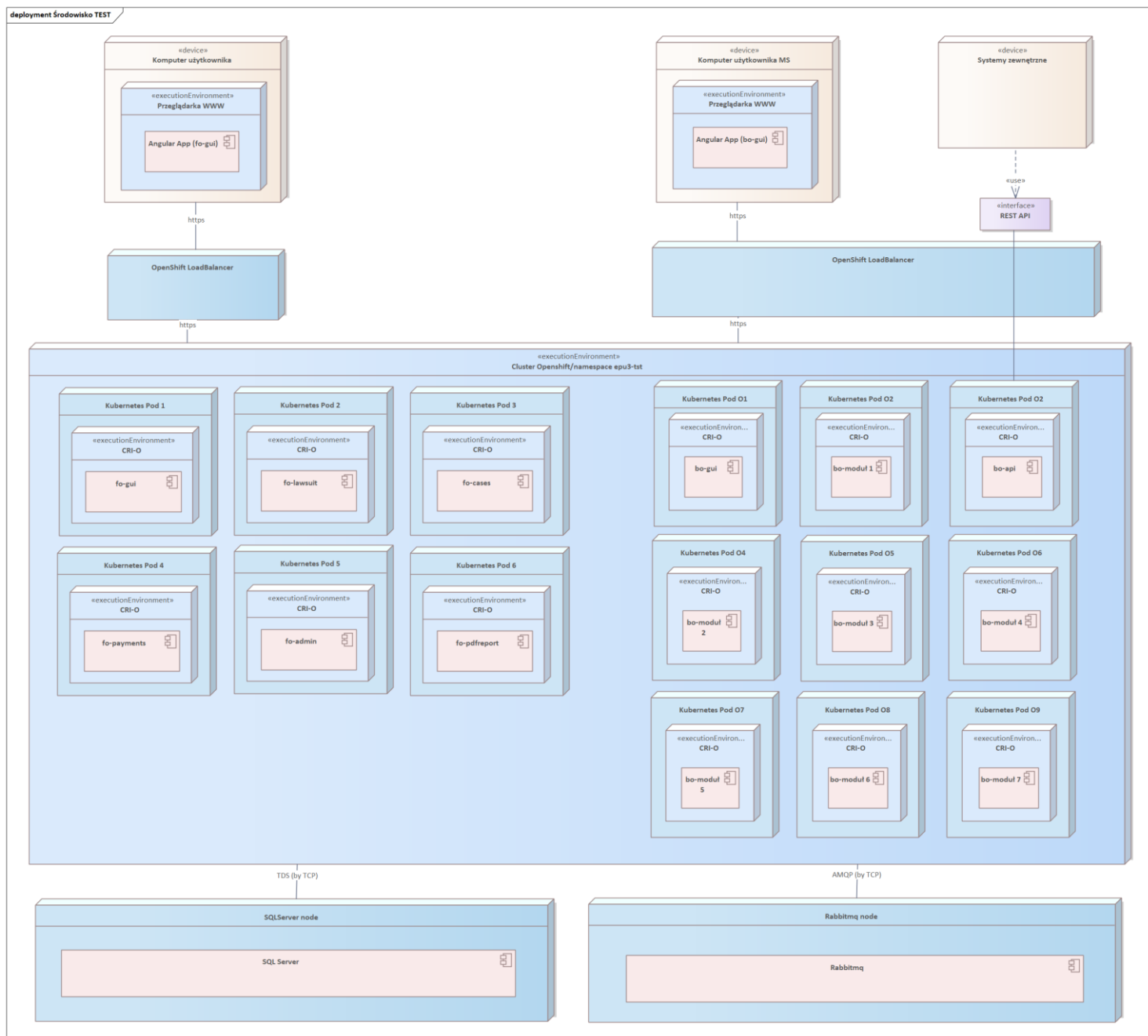
		zawodowego/Informacje o radcach prawnych, adwokatach, pełnomocnikach.	
UCPE	Podpis elektroniczny	Podpisywanie elektroniczne dokumentów cyfrowych przy użyciu różnych dostępnych metod	REST & HTTP Redirect
CEIDG	Centralna Ewidencja i Informacja o Działalności Gospodarcze	walidacja/autouzupełnienie danych stron postępowania nie będących osobami fizycznymi	REST
CRD	Centralne Repozytorium Dokumentów	zapisywanie/pobieranie dokumentów (tekstowych i binarnych)	REST
PDDD2	Broker Komunikacyjnych PDDD2 (eDochody, KRK, PESEL, TERYT)	integracja z bazami PESEL i TERYT - walidacja danych personalnych i teleadresowych	REST

Wymiana danych następuje poprzez web serwisy. Szyfrowanie danych nie jest zaimplementowane.

3. Opis systemu EPU 3.0 – Część Publiczna oraz Orzecznicza – dla audytu II

W celu zobrazowania specyfiki systemu EPU3.0 zamieszczono poniżej podstawowy diagram i opis architektury oraz usług realizowanych przez system. System składa się z dwóch głównych części logicznych:

- **EPU 3.0 – Część publiczna** – funkcjonalność przeznaczona dla użytkowników zewnętrznych (obywateli, pełnomocników zawodowych, komorników sądowych). Interfejs GUI i API do tych funkcjonalności dostępny będzie z sieci publicznej (internet)
- **EPU 3.0 – Część orzecznicza** – funkcjonalność przeznaczona dla użytkowników wewnętrznych (pracowników Ministerstwa Sprawiedliwości i pracowników Sądów). Funkcjonalność ta dostępna będzie z sieci wewnętrznej.



Rysunek 3 Diagram wdrożenie systemu EPU 3.0 na środowisko Test

System EPU3.0 budowany jest w architekturze microserwisów i uruchamiany jest na prywatnej chmurze obliczeniowej. Środowiskiem uruchomieniowym dla kontenerów system jest dedykowany namespace (projekt) w ramach klastra OpenShift. Poszczególne kontenery (usługi) systemu EPU 3.0 można częściowo zakwalifikować do warstw z tradycyjnej, warstwowej architektury systemów:



1) warstwa prezentacji

Interfejsem użytkownika systemu EPU 3.0 jest aplikacja Angular działająca na poziomie okna przeglądarki internetowej. Aplikacja jest udostępniona do pobrania z kontenera:

- **fo-gui** – GUI dla Części publicznej
- **bo-gui** – GUI dla Części orzeczniczej

Cześć funkcjonalności części publicznej aplikacji dostępna jest dla niezalogowanych użytkowników (mapa strony, aktualność, podstawowe informacje, weryfikacja dokumentu na podstawie kodu dostępu), główna część funkcjonalności dostępna jest dla zalogowanych użytkowników (wszystkie funkcjonalności, w tym składanie pozwów, pism procesowych, wniosków, środków odwoławczych, dostęp do skrzynek odbiorczych/nadawczych).

Dla części orzeczniczej wszystkie funkcjonalności wymagają zalogowania i autoryzacji.

2) warstwa aplikacji i logiki biznesowej

EPU 3.0 – Część publiczna

Aplikacja angular komunikuje się po https (REST API) z różnymi modułami backendowymi, które dostarczają właściwych usług. W tej warstwie dostępne są następujące moduły backendowe:

- fo-lawsuit – usługa umożliwiająca złożenie nowych pozwów,
- fo-cases – usługa odpowiedzialna za wizualizację i zarządzanie sprawami sądowymi,
- fo-admin - usługa odpowiedzialna za dostarczanie funkcjonalności skrzynek dla dokumentów (obiektów procesowych),
- fo-payments – usługa wspomagająca dokonywania płatności za czynności procesowe,
- fo-pdfreport – usługa odpowiedzialna za generowanie dokumentów PDF
- bo-api – usługa udostępniająca API Rest dla systemów zewnętrznych

Funkcjonalności (zasoby) wymagające identyfikacji i uwierzytelnienia użytkownika są zabezpieczone koniecznością przedstawienia w żądaniu poprawnego tokena JWT.

Uzyskanie i weryfikacja tokena oparta jest o protokół OCID/OAuth2. Zaś jako serwer tożsamości wykorzystywany jest system Moduł Tożsamość.

Usługa API (która jest przed fazą realizacji) może być zabezpieczona certyfikatem i/lub kluczem API, w zależności od finalnych wymagań i decyzji projektowych.

EPU 3.0 – Część orzecznicza

Ta część systemu aktualnie jest w fazie przygotowawczej, w związku z tym podział na moduły jest w tej chwili estymowany i może finalnie się zmienić. Co do zasady technologie i rozwiązania projektowe będą spójne z Częścią Publiczną. Aplikacja angular (bo-gui) będzie komunikowała się z różnymi modułami backendowymi części orzeczniczej. Na tę chwilę estymowane jest powstanie około 7 modułów (na diagramie oznaczone jako bo-moduł x).

3) warstwa bazodanowa

Wykorzystanymi bazami danych dla modułów backendowych są bazy MS SQL. W tej warstwie dostępne są następujące bazy danych dla EPU 3.0 Część publiczna:

- epu-lawsuit – baza danych dla modułu fo-lawsuit,
- epu-cases - baza danych dla modułu fo-cases,
- epu-admin - baza danych dla modułu fo-admin,
- epu-payments - baza danych dla modułu fo-payments

Dla EPU 3.0 Część orzecznicza dla modułów backendowych powstaną dedykowane bazy danych w tej samej technologii.

4) warstwa komunikacyjna/integracyjna

Komunikacja między poszczególnymi modułami backendowymi odbywa się poprzez REST API, w przypadku komunikacji synchronicznej lub w przypadku komunikacji asynchronicznej poprzez brokera wiadomości RabbitMQ. Docelowo RabbitMQ powinien być wdrożony poza klastrem openshift, na dedykowanym serwerze (serwerach). Aktualnie na środowisku Test broker uruchomiony jest w ramach klastra OpenShift jako kolejny kontener (epu-rabbitmq).

Komunikacja pomiędzy komponentami Części publicznej a komponentami Części orzeczniczej odbywa się poprzez broker wiadomości RabbitMQ.

5) Infrastruktura serwerowa

System EPU3.0 uruchamiany jest w kontenerach na klastrze RedHat OpenShift. A więc jest wysoce zwirtualizowany. Fizyczna architektura oraz warstwa systemu operacyjnego wynikają ze sposobu instalacji i konfiguracji OpenShifta.

Aktualnie system EPU3.0 korzysta z następujących technologii i narzędzi:

- a) technologie i biblioteki aplikacyjne - warstwa prezentacji:
 - Angular,
 - Nginx
- b) technologie i biblioteki aplikacyjne - warstwa aplikacji, logiki biznesowej:
 - Obraz bazowy dla kontenerów: mcr.microsoft.aspnet:8.0
 - Platforma SDK: .Net Core 8.0
 - Języki programowania: C#,
 - Serwer kolejek: RabbitMq
- c) systemy operacyjne oraz platformy wirtualizacji:
 - RedHat OpenShit,
 - Microsoft Windows Server (db SQLServer),

Wykonawca zrealizuje przedmiot umowy z jednego fizycznego miejsca. Wymóg analizy architektury i konfiguracji sieci dotyczy tylko fragmentu infrastruktury związanego z systemem EPU3.0, np. zbadanie reguł komunikacji sieciowej pomiędzy komponentami, np.



bazą danych a Frond-End, konfiguracji systemu operacyjnego pod kątem wdrożonych zabezpieczeń, tj. konfiguracji systemu operacyjnego, np. uruchomianych usług, aktualizacji, konfiguracji lokalnych polityk FireWall etc. Badania muszą uwzględniać również kanał komunikacyjny pomiędzy systemem EPU3.0 a systemami zewnętrznymi podlegającymi integracji z EPU 3.0, w tym co najmniej :

System	Nazwa/Opis	Główny przebieg użycia/wymieniane informacje	Interfejs
e-Płatności	System płatności online	Dokonywanie płatności za złożony pozew. Zwrot opłaty.	REST & HTTP Redirect
Moduł Tożsamość	Węzeł Krajowy Identyfikacji Elektronicznej	Identyfikacja użytkownika	REST/OpenID Connect
KRS	Krajowy Rejestr Sądowy	walidacja/autouzupełnienie danych stron postępowania nie będących osobami fizycznymi	REST
ROBUS	Radcy, Adwokaci, Pełnomocnicy	Walidacja podczas zakładania konta o profilu pełnomocnika zawodowego/Informacje o radcach prawnych, adwokatach, pełnomocnikach.	
UCPE	Podpis elektroniczny	Podpisywanie elektroniczne dokumentów cyfrowych przy użyciu różnych dostępnych metod	REST & HTTP Redirect
CEIDG	Centralna Ewidencja i Informacja o Działalności Gospodarcze	walidacja/autouzupełnienie danych stron postępowania nie będących osobami fizycznymi	REST
CRD	Centralne Repozytorium Dokumentów	zapisywanie/pobieranie dokumentów (tekstowych i binarnych)	REST
PDDD2	Broker Komunikacyjnych PDDD2 (eDochody, KRK, PESEL, TERYT)	integracja z bazami PESEL i TERYT - walidacja danych personalnych i teleadresowych	REST
CPE	System poczty elektronicznej (Exchange)	Wysyłanie informacji drogą email	SMTP
EPO	Elektroniczne Potwierdzenie Odbioru	Informacje o statusie doręczenia/dacie odbioru przesyłek	
ZSRK	Zintegrowany system rachunkowości i kadr (SAP)	Wymiana informacji o opłatach, zwrotach, należnościach sądowych. Informacje o nieobecnościach/urlopach pracowników sądów.	SOAP



ROBUS	Radcy, Adwokaci, Pełnomocnicy	Walidacja podczas zakładania konta o profilu pełnomocnika zawodowego/Informacje o radcach prawnych, adwokatach, pełnomocnikach.	
SCW	System Centralnego Wydruku	Wydruk i wysyłanie dokumentów pocztą tradycyjną	
e- Doręczenia	Elektroniczne Doręczenie Korespondencji	Wysyłanie informacji/decyzji do stron postępowania w przypadku nie korzystania z wewnątrzsystemowej (w ramach systemu EPU) komunikacji elektronicznej.	REST
CBDOPW	Centralna Baza Danych Osob Pozbawionych Wolności	Informacja o pozbawieniu wolności osoby	

Wymiana danych następuje poprzez web serwisy. Szyfrowanie danych nie jest zaimplementowane.

4. Cele audytu I oraz audytu II

Celami obu audytów jest:

- A. wskazanie punktów obniżających poziom bezpieczeństwa, wydajności, dostępności oraz jakości kodu oprogramowania dla systemu EPU3.0,
- B. weryfikacja zgodności z wytycznymi WCAG 2.1 w ramach systemu EPU3.0.,
- C. sporządzenie raportu, o którym mowa jest w pkt. 6, zawierającego rekomendacje racjonalnych działań i usprawnień oraz rozwiązania, które doprowadzą systemu EPU3.0 do podniesienia poziomu bezpieczeństwa, wydajności, dostępności oraz jakości kodu oprogramowania oraz doprowadzą systemu EPU3.0 do zapewnienia zgodności z wytycznymi WCAG 2.1.

Celem drugiego audytu jest dodatkowo weryfikacja zaleceń pierwszego audytu i uwzględnienie ich wyników w raporcie końcowym.

System informatyczny zawiera wiele różnego rodzaju zabezpieczeń technicznych. Każdy z dwóch audytów bezpieczeństwa musi obejmować swoim zasięgiem wszystkie te zabezpieczenia. Techniczne środki ochrony systemu informatycznego podzielą się na następujące kategorie:

- zabezpieczenia aplikacji (np. kontrola dostępu do operacji),
- zabezpieczenia bazy danych (np. kontrola dostępu do tabel relacyjnej bazy danych),
- zabezpieczenia systemu operacyjnego (np. kontrola dostępu do plików, logi systemowe),

- zabezpieczenia sieciowe (np. Firewall, VPN, IDS),
- zabezpieczenia wspomagające (np. serwery kontroli zawartości, serwery uwierzytelniania, PKI).

W celu zapewnienia realizacji celów audytowych każdy z dwóch ww. audytów zewnętrznych systemu EPU3.0 musi składać się co najmniej z następujących, jednostkowych audytów:

- 1) audyt bezpieczeństwa teleinformatycznego Systemu, w tym środowiska infrastrukturalnego, na którym funkcjonuje;
- 2) testy penetracyjne (identyfikacja słabych punktów systemu zabezpieczeń, symulacja włamań);
- 3) weryfikacja kodu źródłowego systemu informatycznego EPU3.0,
- 4) audyt zgodności z wytycznymi WCAG 2.1 lub wyższe,
- 5) audytu bezpieczeństwa w zakresie dotyczącym portalu internetowego EPU3.0

ad 1) Audyt bezpieczeństwa teleinformatycznego systemu EPU3.0, w tym środowiska infrastrukturalnego, na którym funkcjonuje, musi obejmować co najmniej:

1) Analizę architektury i konfiguracji systemu EPU3.0, w tym szyny komunikacyjnej, w tym co najmniej:

- a) mechanizmów autoryzacji i uwierzytelniania,
- b) mechanizmów kontroli dostępu,
- c) mechanizmów bezpieczeństwa komunikacji,
- d) mechanizmów logowania i obsługi błędów i zdarzeń,
- e) mechanizmów ochrony danych,
- f) mechanizmów odpowiedzialnych za wysoką dostępność i niezawodność,
- g) mechanizmów administracji zdalnej z poziomu aplikacji,
- h) zaimplementowanych systemów aktualizacji aplikacji,
- i) zaimplementowanych mechanizmów backupu i odtwarzania aplikacji;

2) Analizę architektury i konfiguracji systemów zarządzania bazami danych i baz danych EPU3.0, w tym co najmniej:

- a) mechanizmów autoryzacji oraz uwierzytelniania,
- b) konfiguracji uprawnień do obiektów i segmentacji uprawnień,
- c) logowania zdarzeń, składowania i retencji logów,
- d) monitorowania dostępu do obiektów,
- e) monitorowania instrukcji języka SQL,
- f) przechowywania oraz dostępu do danych, w tym widoczności danych dla administratorów,
- g) przechowywania oraz dostępu do danych audytowych,
- h) mechanizmów ochrony danych,
- i) zarządzania uprawnieniami,
- j) metod dostępu do danych i ich transmisji,
- k) mechanizmów odpowiedzialnych za wysoką dostępność i niezawodność,

- l) mechanizmów administracji zdalnej bazami danych,
- m) zaimplementowanych systemów aktualizacji baz danych,
- n) zaimplementowanych mechanizmów backupu i odtwarzania systemów zarządzania bazami danych i baz danych,
- o) komunikacji z klientami bazodanowymi (m.in. protokoły, mechanizmy kryptograficzne, transfery danych, pule połączeń),
- p) implementacji zasad hardeningowych (usuwanie luk bezpieczeństwa) dla systemów zarządzania bazami danych i baz danych (m.in. w zakresie wyłączenia nieużywanych usług i funkcji, wyłączenia nieużywanych metod dostępu, zainstalowanych komponentów i składników środowiska baz danych, optymalnych parametrów baz danych).

3) Analizę architektury i konfiguracji systemów operacyjnych systemu EPU3.0, w tym co najmniej:

- a) mechanizmów autoryzacji oraz uwierzytelniania,
- b) zarządzania uprawnieniami, w tym przypisania użytkowników do właściwych grup i weryfikacji uprawnień zgodnie z pryncypium jak najmniejszych uprawnień (ang. „least privilege”),
- c) logowania zdarzeń, składowania i retencji logów,
- d) wdrożonych metod zabezpieczeń,
- e) poprawności udostępniania usług sieciowych,
- f) poziomu bezpieczeństwa i monitorowania dostępu,
- g) poprawności konfiguracji uprawnień,
- h) monitorowania i rejestrowania dostępu do obiektów systemu,
- i) przechowywania oraz dostępu do danych audytowych,
- j) mechanizmów ochrony danych,
- k) mechanizmów odpowiedzialnych za wysoką dostępność i niezawodność,
- l) mechanizmów administracji zdalnej,
- m) zaimplementowanych systemów aktualizacji,
- n) zaimplementowanych mechanizmów backupu i odtwarzania,
- o) implementacji zasad hardeningu systemów operacyjnych (m.in. w zakresie weryfikacji udostępnionych lub zbędnych usług sieciowych, zainstalowanych komponentów i składników systemu, wyłączenia nieużywanych metod dostępu, optymalnych parametrów systemu pod kątem przyjętego zastosowania);

4) Analizę architektury i konfiguracji sieci, w której pracuje system EPU3.0, w tym co najmniej:

- a) podziału na VLAN-y,
- b) zastosowanych mechanizmów ochrony danych,
- c) urządzeń sieciowych,
- d) urządzeń bezpieczeństwa,
- e) dostępu do Internetu,

f) mechanizmów odpowiedzialnych za wysoką dostępność i niezawodność;

oraz wytworzenie opisu technicznego do raportu, o którym mowa jest w pkt. 6, zawierającego wnioski z audytu I i audytu II w powyższym zakresie, w tym wskazanie obszaru zrealizowanych badań oraz użytych do nich metod, wykryte nieprawidłowości w architekturze systemu i konfiguracji poszczególnych komponentów, ich wpływ na aplikacje i systemy, zalecenia i instrukcje do wprowadzenia korekt architektonicznych i konfiguracyjnych niezbędnych dla poprawy zapewnienia bezpieczeństwa systemu EPU3.0.

Ad 2) Testy penetracyjne (Grey Box) - w sieci wewnętrznej Zamawiającego z wykorzystaniem dostępu i informacji przekazanych przez Zamawiającego, które Zamawiający uzna za istotne do przeprowadzenia testów bezpieczeństwa systemu EPU3.0, przy czym Zamawiający:

- nie przewiduje testów fizycznego (osobowego) dostępu do infrastruktury i zasobów, sprawdzeń możliwości wpięcia urządzeń do sieci Zamawiającego do niego nienależących, jak również nie przewiduje audytu socjotechnicznego,
- dopuszcza wykonanie części testów z zewnątrz organizacji po uprzednim uzgodnieniu ich warunków (co do terminu przeprowadzenia testów, tzw. okno serwisowe).

W zakresie prowadzenia testów penetracyjnych Wykonawca przeprowadzi:

1) Enumerację sieci wewnętrznej systemu EPU3.0, w tym co najmniej:

a) skanowanie sieci, w tym:

- skanowanie danej grupy adresów IP,
- określanie typów i rodzajów systemów,
- określanie dostępnych usług i ich wersji,

b) określanie potencjalnych wektorów ataku, w tym:

- analiza zgromadzonych danych i uszeregowanie znalezionych podatności,

2) Analizę właściwą podatności, w tym co najmniej:

- a) detekcję odkrytych jawnych i niejawnych informacji wysyłanych przez aplikacje i systemy wewnętrzne IT,
- b) detekcję błędów aplikacji i systemów poprzez proxowanie zapytań i manipulacje odpowiedziami,
- c) detekcja błędów aplikacji minimum poprzez metody wstrzyknięcia treści (SQL injection, XSS, XSRF, enumeracja zasobów, spoofing, masquerading, flooding),
- d) detekcja sposobu zabezpieczeń integralności aplikacji (bezaudytoracyjna modyfikacja jej składowych),
- e) detekcję wyświetlanych błędów systemów i aplikacji oraz ich audytowalności,
- f) detekcję błędów technik autentykacji stosowanych dla zapewnienia kontroli dostępu do zasobów,
- g) weryfikację mechanizmów zabezpieczających aktualizację zasobów;

3) Atak na system EPU3.0, w tym co najmniej:

- a) pozyskiwanie danych z serwerów (np. enumeracja użytkowników, próba transferu danych, pozyskiwania danych konfiguracyjnych),
- b) przeprowadzanie ataków słownikowych,



- c) próby wywołania błędów aplikacji (fuzzing, wartości graniczne, niepoprawne typy wartości, brak wartości, przepełnienie bufora, przepełnienie parametrów, powtórzenia parametrów, odgadywanie parametrów),
- d) zakłócenia funkcjonowania usługi/systemu/urządzenia,
- e) uzyskania nieautoryzowanego dostępu / modyfikacji do danych,
- f) uzyskania nieautoryzowanego dostępu do aplikacji/systemu/sieci (próba przejęcia kontroli),
- g) wprowadzenia danych do aplikacji/systemu/urządzenia,
- h) zablokowania działania aplikacji/systemu/urządzenia,
- i) próby ataków semantycznych na adres URL,
- j) próby ataków związanych z ładowaniem plików,
- k) próby ataków typu Cross-Site Scripting,
- l) próby ataków typu Cross-Site Request Forgery,
- m) próby ataków typu MITM (Man in the Middle),
- n) próby podrabiania zarządzania formularza,
- o) próby sfałszowania żądania http,
- p) próby ujawnienia danych przechowywanych w bazie,
- q) próby trawersowania katalogów,
- r) próby ujawniania kodu źródłowego,
- s) próby przepełnienia bufora lub stosu,
- t) wstrzykiwania kodu wykonywalnego innych języków programowania,
- u) badanie enumeracji wykorzystania znanych podatności w celu uzyskania nieautoryzowanego dostępu,
- v) badanie możliwości podszywania się pod użytkowników i uzyskania nieautoryzowanego dostępu do systemu,
- w) badanie możliwości podszywania się pod użytkowników uprzywilejowanych i uzyskanie dostępu do systemu,
- x) badanie możliwości blokowania/umożliwienia dostępu do systemu wszystkim lub wybranym jej użytkownikom,
- y) badanie możliwości modyfikacji/usunięcia danych z systemu w nieautoryzowany sposób.

4) Identyfikację zagrożeń z użyciem specjalistycznych narzędzi (w tym narzędzi, które dostępne są również dla hackerów), w tym co najmniej:

- a) wykorzystanie gotowych narzędzi i skryptów,
- b) wykorzystanie gotowych baz testowych/grup testów,
- c) wykorzystanie gotowych słowników;

5) Wychwytywanie słabych punktów konfiguracji, w tym co najmniej:

- a) identyfikację potencjalnie niebezpiecznych wersji stosowanego oprogramowania,
- b) identyfikację widocznych luk/błędów w konfiguracji (mających bezpośredni wpływ na bezpieczeństwo lub ułatwiających ataki),

- c) analizę danych pozostających po stronie użytkownika (pliki cookies, dane tymczasowe, mechanizm przekazywania danych pomiędzy klientem a serwerem, etc);

oraz wytworzenie opisu technicznego z testów penetracyjnych (Grey Box) do raportu, o którym mowa jest w pkt. 6, zawierającego wnioski z audytu I i audytu II w powyższym zakresie, w tym wskazanie obszaru zrealizowanych badań oraz użytych do nich metod, wykryte podatności, ich wpływ na aplikacje i systemy, zalecenia i instrukcje do wprowadzenia korekt konfiguracyjnych w celu ich eliminacji, a także ocenę stanu bezpieczeństwa systemu EPU3.0.

Ad 3) Weryfikacja kodu źródłowego Systemu musi obejmować co najmniej:

- 1) pełny wykaz zastosowanych technologii programistycznych we wszystkich warstwach,
- 2) ocenę poprawności wykorzystania frameworków,
- 3) badanie wydajności kodu źródłowego,
- 4) badanie podatności na ataki XSS, Sql Injection, CSRF, DoS,
- 5) określenie poziomu skalowalności kodu źródłowego,
- 6) badanie poprawności realizacji połączeń do baz danych,
- 7) weryfikację struktury baz danych (stopnia optymalizacji i normalizacji bazy danych),
- 8) weryfikację architektury aplikacji,
- 9) badanie zgodności z modelem MVC (Model-View-Controller),
- 10) badanie jakości i rzetelności w procesie wytwarzania pod kątem Continuous Integration (uwzględniając dostępne repozytorium),
- 11) badanie poziomu kosztów i pracochłonności modyfikowania kodu podczas utrzymania i rozwoju,
- 12) badanie stopnia odporności na wprowadzanie zmian, możliwość refactoringu oraz reusability,
- 13) weryfikację przejrzystości kodu,
- 14) weryfikację jakości udokumentowania kodu,
- 15) weryfikację komplementarności kodu w repozytorium,
- 16) weryfikację jakości testów (dla testów wykonywanych w zautomatyzowany sposób),
- 16) weryfikację zastosowania dobrych praktyk zalecanych przez producentów technologii, w których aplikacja została wytworzona,
- 17) weryfikację zastosowania wytycznych właściwych dla zastosowanej technologii,
- 18) weryfikację konsekwencji w stosowaniu standardów, konwencji, itp.
- 19) weryfikację stosowania wzorców projektowych,
- 20) weryfikację stosowania właściwych podziałów na warstwy i komponenty z zachowaniem zasad rozłącznego i osobliwego zastosowania (Separation of Concerns),
- 21) analizę użytych funkcji lub komponentów pod kątem elementów przestarzałych („deprecated”) lub elementów posiadających znane luki bezpieczeństwa lub podatności.

oraz wytworzenie opisu technicznego z weryfikacji kodu źródłowego do raportu, o którym mowa jest w pkt. 6, zawierającego wnioski z audytu I i audytu II w powyższym zakresie, w tym ocenę stanu bezpieczeństwa systemu EPU3.0.

Ad 4) Audyt zgodności systemu EPU 3.0 z wytycznymi WCAG 2.1 w zakresie opartym na głównych zasadach WCAG 2.1, którymi są:

- a) Postrzegalność (ang. Perceivable),
- b) Funkcjonalność (ang. Operable),
- c) Zrozumiałość (ang. Understandable),
- d) Solidność (ang. Robust).

Wykonawca w ramach czynności audytu I i audytu II w zakresie zgodności systemu EPU3.0 z wytycznymi WCAG 2.1 przedstawi Zamawiającemu raport, o którym mowa jest w pkt. 6, zawierający pełną analizę rezultatów wykonanych weryfikacji wraz ze wskazówkami i instrukcjami dotyczącymi wyeliminowania lub ograniczenia zidentyfikowanych barier lub nieprawidłowości systemu EPU 3.0 z wytycznymi WCAG 2.1.

Ad 5) Audyt bezpieczeństwa w zakresie dotyczącym portalu internetowego EPU3.0 w zakresie:

- a) szacunkowej, planowanej liczby formularzy HTML na poziomie około 130,
- b) szacunkowej, planowanej liczby ról (kont użytkowników) na poziomie około 4,
- c) szacunkowej, planowanej, sumarycznej liczby linii kodu na poziomie około 120 000, z zastrzeżeniem, że liczba linii kodu może ulec zmianie.
- d) serwerów wirtualnych na poziomie 8, z zastrzeżeniem, że liczba serwerów wirtualnych może ulec zmianie.

1) Zamawiający umożliwi Wykonawcy dostęp do dokumentacji API,

2) Zamawiający umożliwi Wykonawcy dostęp do testowych żądań API wraz z danymi tekstowymi w zakresie dotyczącym dwóch zdefiniowanych API.

3) System teleinformatyczny EPU3.0 podlega aktualnie szeregu modyfikacjom, wobec tego Zamawiający przed zawarciem umowy określi i doprecyzuje zdefiniowanie 2 (dwóch) webserwisów, z zastrzeżeniem, że liczba webserwisów może ulec zmianie, przy czym nie będzie ona mniejsza niż 1

oraz wytworzenie opisu technicznego z audytu portalu internetowego do raportu, o którym mowa jest w pkt. 6, zawierającego wnioski z audytu I i audytu II w powyższym zakresie, w tym ocenę stanu bezpieczeństwa systemu EPU3.0.

5. Metodyka prowadzenia testów dla audytu I i audytu II

1) Zamawiający wymaga, aby Wykonawca w ramach wykonywania testów penetracyjnych wykorzystywał co najmniej jeden z powszechnie uznawanych i aktualnych standardów testowania bezpieczeństwa, np:

- a) OWASP Application Security Verification Standard (ASVS),
- b) ~~Open Source Security Testing Methodology Manual (OSSTMM),~~

- c) Penetration Testing Execution Standard (PTES),
- d) OWASP Risk Rating Methodology,

lub równoważny standard testowania bezpieczeństwa (za równoważny Zamawiający uzna standard opisujący przebieg procesu testowania bezpieczeństwa systemów IT oraz obszary systemowe, które muszą podlegać weryfikacji). Równoważny standard testowania bezpieczeństwa nie może być opracowany przez Wykonawcę lub podmiot zależny od Wykonawcy.

- 2) Zamawiający wymaga, aby Wykonawca w ramach wykonywania przedmiotu zamówienia korzystał z aktualnych baz danych zawierających informacje o podatnościach i słabościach bezpieczeństwa systemów teleinformatycznych, np.

- a) SANS Top 20 Critical Security Controls,
- b) Common Vulnerabilities and Exposures,
- c) WASC (Web Application Security Consortium) Threat Classification,

lub równoważnych baz danych (za równoważne Zamawiający uzna takie bazy danych, które stanowią aktualne źródło informacji o lukach bezpieczeństwa, są publikowane lub utrzymywane przez uznane powszechnie organizacje, działające na rzecz zapewnienia bezpieczeństwa systemów teleinformatycznych). Równoważne bazy danych zawierające informacje o podatnościach i słabościach bezpieczeństwa systemów teleinformatycznych nie mogą być opracowane przez Wykonawcę lub podmiot zależny od Wykonawcy.

- 3) Zamawiający wymaga, aby Wykonawca w ramach wykonywania audytu bezpieczeństwa do oceny wykorzystywał aktualne listy kontrolne udostępniane przez uznane organizacje pracujące na rzecz bezpieczeństwa systemów IT, np:

- a) National Security Agency (NSA),
- b) Center for Internet Security (CIS),

lub równoważne listy kontrolne (za równoważne Zamawiający uzna takie, które stanowią aktualne źródło informacji o bezpiecznej konfiguracji, są publikowane lub utrzymywane przez uznane powszechnie organizacje, działające na rzecz zapewnienia bezpieczeństwa systemów teleinformatycznych). Równoważne listy kontrolne nie mogą być opracowane przez Wykonawcę lub podmiot zależny od Wykonawcy.

6. Raportowanie dla audytu I i audytu II

Raport z wykonania przedmiotu zamówienia musi być sporządzony odrębnie dla audytu I oraz odrębnie dla audytu II w języku polskim, dostarczany w formie papierowej i elektronicznej (plik: *.DOC/DOCX z możliwością edycji i *.PDF), będzie zawierał co najmniej:

- 1) streszczenie raportu,
- 2) opis przeprowadzonych działań (w tym weryfikacji dokumentacji, komponentów systemu EPU3.0 i wykonanych testów),
- 3) przyjęty model klasyfikacji ryzyka,

- 4) opisy techniczne, o których mowa jest w pkt. 4, sporządzone do audytu bezpieczeństwa teleinformatycznego systemu, testów penetracyjnych, weryfikacji kodu źródłowego systemu oraz audytu bezpieczeństwa w zakresie dotyczącym portalu internetowego EPU3.0,
- 5) klasyfikację ryzyka dla wykrytych podatności,
- 6) wyniki analizy, testów i ich interpretację, w tym co najmniej:
 - a) informacje dotyczące ogólnej oceny poziomu bezpieczeństwa oraz odporności na ataki systemu EPU3.0 i jego środowiska infrastrukturalnego zawierające podsumowanie ilości stwierdzonych nieprawidłowości w podziale na system EPU3.0 i jego środowisko infrastrukturalne oraz ich krytyczności, w postaci raportu dla kierownictwa Zamawiającego,
 - b) opis wykorzystanych metod prowadzenia testów oraz zbadanych obszarów podlegających audytowi,
 - c) listę i opis wykrytych podatności (wg numeru CVE i wagi CVSS, jeśli istnieją w bazie CVE) oraz listę użytych narzędzi - sposobu, w jaki można zlokalizować i powtórzyć testowy atak na podatność,
 - d) informacje na temat poziomu i jakości zabezpieczeń realizowanych przez system EPU3.0,
 - e) wnioski z audytu (określenie ilościowego i jakościowego poziomu niebezpieczeństwa podatności),
 - f) rekomendacje i zalecenia dotyczące podjęcia racjonalnych działań i usprawnień oraz propozycje rozwiązań pozwalających na usunięcie wykrytych słabości, a tym samym podniesienie poziomu bezpieczeństwa, wydajności, dostępności oraz jakości kodu oprogramowania oraz zapewnienie zgodności z wytycznymi WCAG 2.1. systemu EPU3.0 i jego środowiska infrastrukturalnego (określenie sposobu naprawy wykrytych podatności, w tym zmian konfiguracyjnych).

Raport drugiego audytu będzie weryfikował stopień wdrożenia zaleceń zawartych w raporcie z pierwszego audytu.