*Audyt bezpieczeństwa i wydajności systemów teleinformatycznych - OPZ*

Spis treści

[Wstęp 4](#_Toc134081294)

[Część I - opis systemów oraz zakres czynności audytowych. 5](#_Toc134081295)

[*Audyt bezpieczeństwa Centralnej Ewidencji i Informacji o Działalności Gospodarczej (CEIDG) wraz z Hurtownią Danych (HD).* 5](#_Toc134081296)

[Opis CEIDG.gov.pl 5](#_Toc134081297)

[Opis Hurtownia Danych – dane.biznes.gov.pl 6](#_Toc134081298)

[Opis modułów funkcjonalnych Hurtowni 7](#_Toc134081299)

[Opis struktury modułów interfejsu API Hurtowni 7](#_Toc134081300)

[Opis infrastruktury utrzymującej system CEIDG i HD 8](#_Toc134081301)

[Zakres czynności dla audytu infrastruktury CEIDG i HD 9](#_Toc134081302)

[Zakres czynności dla audytu aplikacji webowej - ceidg.gov.pl oraz dane.biznes.gov.pl (API, aplikacja raportowa), w tym pentesty portalu WWW 10](#_Toc134081303)

[Zakres czynności dla audytu konfiguracji systemów operacyjnych i baz danych ceidg.gov.pl oraz dane.biznes.gov.pl 10](#_Toc134081304)

[Cel audytu 10](#_Toc134081305)

[*Testy wydajności CEIDG i Hurtowni Danych* 11](#_Toc134081306)

[*Audyt bezpieczeństwa systemu i wszystkich modułów Punktu Informacji dla Przedsiębiorcy funkcjonującego w domenie \*.biznes.gov.pl (PIP).* 11](#_Toc134081307)

[Opis systemu 11](#_Toc134081308)

[Opis infrastruktury utrzymującej system 15](#_Toc134081309)

[Zakres audytu infrastruktury systemu i wszystkich modułów Punktu Informacji dla Przedsiębiorcy funkcjonującego w domenie \*.biznes.gov.pl (PIP) 15](#_Toc134081310)

[Zakres audytu aplikacji webowych - systemu i wszystkich modułów Punktu Informacji dla Przedsiębiorcy funkcjonującego w domenie \*.biznes.gov.pl (PIP), w tym pentesty portalu WWW 15](#_Toc134081311)

[Zakres audytu konfiguracji systemów operacyjnych i baz danych środowiska produkcyjnego, w zakresie systemu i wszystkich modułów Punktu Informacji dla Przedsiębiorcy funkcjonującego w domenie \*.biznes.gov.pl (PIP) 16](#_Toc134081312)

[Cel audytu 16](#_Toc134081313)

[*Testy wydajności systemu i modułów systemu \*.biznes.gov.pl* 17](#_Toc134081314)

[Zakres audytu wydajności dla Systemu Konfiguratora eLF i Aplikacji Zaplecza 17](#_Toc134081315)

[Zakres audytu wydajności dla Systemu Runtime eLF 18](#_Toc134081316)

[Zakres audytu wydajności dla Podsystemu logowania/rejestracji 18](#_Toc134081317)

[Zakres audytu wydajności dla API – Baza Wiedzy - Zaplecza 18](#_Toc134081318)

[*Audyt bezpieczeństwa systemu Tracker 2.0, wraz z e-sługami Licencjonowania i ewidencjonowania obrotu towarami wrażliwymi na biznes.gov.pl (dla przedsiębiorców)* 19](#_Toc134081319)

[*Testy wydajności systemu teleinformatycznego Tracker 2.0* 19](#_Toc134081320)

[*Świadczenie usług wsparcia eksperckiego inżyniera bezpieczeństwa* 20](#_Toc134081321)

[Część II - opis systemów oraz zakres czynności audytowych. 20](#_Toc134081322)

[*Audyt bezpieczeństwa dwóch systemów informatycznych platformy PEF udostępnianych przez Brokerów PEF* 20](#_Toc134081323)

[*Audyt bezpieczeństwa systemu informatycznego Książki Adresowej PEF wraz z Wyszukiwarką na Portalu PEF (efaktura.gov.pl)* 21](#_Toc134081324)

[*Świadczenie usług wsparcia eksperckiego inżyniera bezpieczeństwa* 22](#_Toc134081325)

[Szczegóły dotyczące procesu realizacji usługi w ramach części I 22](#_Toc134081326)

[*Audyt bezpieczeństwa przetwarzania danych.* 22](#_Toc134081327)

[*Audyt bezpieczeństwa systemów teleinformatycznych.* 23](#_Toc134081328)

[*Audyt funkcjonowania systemów bezpieczeństwa*. 25](#_Toc134081329)

[*Raporty* 25](#_Toc134081330)

[Szczegóły dotyczące procesu realizacji usługi w ramach części II. 26](#_Toc134081331)

[*Audyt bezpieczeństwa przetwarzania danych.* 26](#_Toc134081332)

[*Audyt bezpieczeństwa systemów teleinformatycznych*. 27](#_Toc134081333)

[*Audyt funkcjonowania systemów bezpieczeństwa*. 29](#_Toc134081334)

[*Raporty* 29](#_Toc134081335)

[Harmonogram prac. 30](#_Toc134081336)

[*Zlecanie prac w przypadku audytów/testów wydajności* 30](#_Toc134081337)

[*Zlecanie prac w przypadku wsparcia inżyniera bezpieczeństwa IT.* 31](#_Toc134081338)

[Wymagania dotyczące współpracy Zamawiającego z Wykonawcą 32](#_Toc134081339)

[Załączniki: 32](#_Toc134081340)

# **Wstęp**

Przedmiotem zamówienia jest wykonanie audytów bezpieczeństwa i wydajności systemów teleinformatycznych wraz z usługą wsparcia eksperckiego inżyniera bezpieczeństwa IT zgodnie ze specyfikacją w poszczególnych rozdziałach.

Zamówienie zostało podzielone na dwie części:

1. **Część I zamówienia**:
2. Przeprowadzenie audytu bezpieczeństwa/wydajności/retestów Centralnej Ewidencji i Informacji o Działalności Gospodarczej (CEIDG) i Hurtowni Danych (HD), w tym weryfikacja zapewnienia niezbędnych zasobów do monitorowania bezpieczeństwa po stronie Zamawiającego.
3. Przeprowadzenie audytu bezpieczeństwa/wydajności/retestów Punktu Informacji dla Przedsiębiorcy funkcjonujący w domenie \*.biznes.gov.pl (PIP), w tym weryfikacja zapewnienia niezbędnych zasobów do monitorowania bezpieczeństwa po stronie Zamawiającego.
4. Przeprowadzenie audytu bezpieczeństwa Systemu Tracker 2.0, w tym m. in. eUsługi Licencjonowania i ewidencjonowania obrotu towarami wrażliwymi na biznes.gov.pl, oraz udostępnianych API,
5. Przeprowadzenie testów wydajności Systemu Tracker 2.0, w tym m. in. eUsługi Licencjonowania i ewidencjonowania obrotu towarami wrażliwymi na biznes.gov.pl, oraz udostępnianych API.
6. Świadczenie usług wsparcia eksperckiego inżyniera bezpieczeństwa w ilości 400 roboczogodzin.
7. **Część II zamówienia**:
8. Przeprowadzenie audytu bezpieczeństwa dwóch systemów informatycznych Platformy Elektronicznego Fakturowania (PEF) udostępnianych przez Brokerów PEF (brokerpefexpert.efaktura.gov.pl i brokerinfinite.efaktura.gov.pl),
9. Przeprowadzenie audytu bezpieczeństwa Portalu PEF (efaktura.gov.pl) wraz z Książką Adresową PEF.
10. Świadczenie usług wsparcia eksperckiego inżyniera bezpieczeństwa w ilości 50 roboczogodzin.

# **Część I - opis systemów oraz zakres czynności audytowych.**

##

## Audyt bezpieczeństwa Centralnej Ewidencji i Informacji o Działalności Gospodarczej (CEIDG) wraz z Hurtownią Danych (HD).

### Opis CEIDG.gov.pl

Zgodnie z obowiązującymi przepisami, minister właściwy do spraw gospodarki przy użyciu systemów teleinformatycznych prowadzi: Centralną Ewidencję i Informację o Działalności Gospodarczej (art. 2 ust. 1 ustawy z dnia 6 marca 2018 r. o Centralnej Ewidencji i Informacji o Działalności Gospodarczej i Punkcie Informacji dla Przedsiębiorcy) oraz Punkt Informacji dla Przedsiębiorcy (art. 51 ust. 1 ww. ustawy). Wpis, zmiana oraz wykreślenie przedsiębiorcy z CEIDG może się odbywać za pośrednictwem systemu CEIDG lub za pośrednictwem systemu Punktu Informacji dla Przedsiębiorcy (art. 3 ust. 1 ustawy z dnia 6 marca 2018 r. o Centralnej Ewidencji i Informacji o Działalności Gospodarczej i Punkcie Informacji dla Przedsiębiorcy).

Zadaniem CEIDG jest:

1. ewidencjonowanie przedsiębiorców będących osobami fizycznymi;
2. udostępnianie informacji o przedsiębiorcach oraz innych podmiotach w zakresie wskazanym w ustawie;
3. udostępnianie informacji o zakresie i terminie zmian we wpisach do CEIDG oraz w informacjach i danych udostępnianych w CEIDG, a także o wprowadzającym te zmiany podmiocie;
4. umożliwienie wglądu do danych bezpłatnie udostępnianych przez Centralną Informację Krajowego Rejestru Sądowego;
5. udostępnianie informacji o ustanowionym pełnomocniku lub prokurencie, w tym o zakresie udzielonego pełnomocnictwa lub o rodzaju i sposobie wykonywania prokury.

Minister właściwy do spraw gospodarki przechowuje i przetwarza dane oraz informacje związane z realizacją zadań wynikających z ustawy, w szczególności w związku z przyjmowaniem żądań, zgłoszeń, wniosków i zmian w Rejestrze CEIDG.

Na powyższym rysunku kolorem czerwonym oznaczono moduły wycofywane z Systeorzone.

Rysunek Schemat funkcjonalny ST CEIDG

**SYSTEM CEIDG**

**Rejestr CEIDG**

**Aplikacja Urzędnika**

**API
rejestru
CEIDG**

**Replika danych
rejestru CEIDG**

|  |  |
| --- | --- |
| Moduł  | Przeznaczenie i integracje  |
| Rejestr CEIDG(modernizacja) | Przeznaczenie:  Elektroniczny rejestr działający w ramach Systemu Teleinformatycznego Centralnej Ewidencji i Informacji o Działalności Gospodarczej, którego przeznaczeniem jest: ewidencjonowanie przedsiębiorców będących osobami fizycznymi; udostępnianie informacji o przedsiębiorcach i innych podmiotach w zakresie wskazanym w ustawie; umożliwienie wglądu do danych bezpłatnie udostępnianych przez Centralną Informację Krajowego Rejestru Sądowego: umożliwienia ustalenia terminu i zakresu zmian wpisów w CEIDG oraz wprowadzającego je organu. |
| API rejestru CEIDG(modernizacja) | Przeznaczenie: wielofunkcyjny interfejs programistyczny zapewniający dostęp do danych z rejestru CEIDG oraz realizujący dwukierunkową wymianę danych pomiędzy organami uczestniczącymi w procesie zakładania działalności gospodarczej, organami prowadzącymi rejestry działalności regulowanej  oraz innymi podmiotami przekazującymi dane do CEIDG na podstawie odrębnych porozumień. |
| Replika dla hurtowni danych i systemu CEIDG (modernizacja) | Przeznaczenie: mechanizm repliki transakcyjnej MS SQL dla danych z rejestru CEIDG służący do zasilenia Hurtowni Danych. |
| Aplikacja urzędnika(modernizacja) | Przeznaczenie: aplikacja udostępniona przez przeglądarkę internetową (aplikacja webowa) umożliwiającą urzędnikom realizacje zadań w procesach realizowanych przez CEIDG, m.ni. rejestracja i potwierdzanie konta urzędnika, składanie wniosków do CEIDG,  przekazanie informacji dot. wpisu do rejestrów działalności regulowanej,  wyszukiwarka przedsiębiorców, podgląd danych,  wykonywanie raportów. |

### Opis Hurtownia Danych – dane.biznes.gov.pl

Hurtownia Danych CEIDG i Biznes.gov.pl jest jednym z elementów ekosystemu Biznes.gov.pl. Użytkownicy mogą korzystać z usług po uprzednim uwierzytelnieniu się w serwisie Biznes.gov.pl.

W skład Hurtowni Danych wchodzą trzy aplikacje webowe:

* + Interfejs API (Gravitee) służący do administrowania interfejsem ,
	+ Aplikacja Raportowa (Wyn Enterprise) służąca do administrowania i generowania raportów,
	+ Aplikacja Monitorowania Przepływów Danych (Havran) służąca do oceny parametrów jakościowych i ilościowych transferów danych Hurtowni.

Możliwość skorzystania z poszczególnych aplikacji oraz funkcji uzależniona jest od ról, które są dostępne dla konkretnego, uwierzytelnionego Użytkownika.

Rysunek 2 – Hurtownia Danych CEIDG i jej otoczenie



### Opis modułów funkcjonalnych Hurtowni

|  |  |
| --- | --- |
| Moduł  | Przeznaczenie i integracje  |
| Interfejs API | Moduł realizujący usługi dostępu do danych z Repliki bazy CEIDG oraz Bazy Hurtowni Danych za pośrednictwem API (application programming interface). Integralną częścią Interfejsu API jest moduł administracyjny służący do zarządzania API. |
| Aplikacja Raportowania | Aplikacja umożliwiająca tworzenie oraz wyświetlanie raportów bazujących na danych Bazy Hurtowni Danych. Aplikacja służy również do zarządzania źródłami, zbiorami danych, szablonami raportów, regułami dystrybucji raportów, itp. |
| Aplikacja Monitorowania Przepływów Danych | Aplikacja przeznaczona dla Administratorów do monitorowania procesów ETL. |
| Replika Bazy CEiDG | Replika operacyjnej bazy danych Rejestru CEIDG, aktualizowana na bieżąco (tzw. replika transakcyjna); stanowi bezpośrednie źródło danych biznesowych dla Interfejsu API oraz Bazy Hurtowni Danych, jak również jest źródłem informacji o rolach urzędników dla Aplikacji Raportowej.  |
| Baza Hurtowni Danych (Analityczna) | Główna baza danych zasilająca Aplikację Raportową, w której składowane są dane z Repliki Bazy CEIDG w formie zoptymalizowanej pod kątem raportowania  |

### Opis struktury modułów interfejsu API Hurtowni

|  |  |
| --- | --- |
| Moduł  | Przeznaczenie i integracje  |
| API Gateway | Umożliwia nakładanie limitów na przesyłanie danych lub liczby zapytań w wybranym okresie czasu. Udziela dostępu do poszczególnych usług API lub odmawia dostępu w przypadku podania niezgodnego tokenu JWT. Pozwala na zarządzanie dostępem i użytkownikami API poprzez moduł API Management. Użytkownik może subskrybować wybrane API. Konieczna jest rejestracja użytkownika w API Gateway (poprzez udostępnioną usługę REST API w ramach API Gateway). Rejestracja jest dokonywana w Biznes.gov.pl w momencie generowania tokenu JWT dla użytkownika. |
| API | Zdefiniowano pięć usług zapewniających realizację wyszukiwania podmiotów w Replice bazy CEIDG oraz bezpośrednio w systemie zewnętrznym eKRS za pośrednictwem Wyszukiwarki KRS. API będzie łączyło wyniki znalezione w Replice bazy CEIDG oraz otrzymane przez WebService Wyszukiwarka KRS. Pozostałe usługi do pobierania listy raportów oraz konkretnego raportu będą wykorzystywały do tego Aplikację Raportową działającą w ramach Hurtowni Danych CEIDG. |
| API MSWF | Zdefiniowano pięć usług:Wyszukiwarka prosta umożliwia poprzez podanie w języku naturalnym zapytania i otrzymania wyników najbardziej zbliżonych do zapytania Wyszukiwanie zaawansowane umożliwia przeszukiwanie zasobów CEIDG oraz eKRS przy użyciu zamkniętego katalogu kryteriów wyszukiwawczych.Pobieranie informacji o wskazanych wpisach z CEIDG lub eKRS. Pobieranie na podstawie unikalnego numeru KRS informacji zgromadzonych w CEIDG na temat koncesji, zezwoleń, licencji oraz wpisów do rejestrów działalności regulowanej jak również kwalifikacjach zawodowych w kontekście podmiotu zarejestrowanego w eKRS.Pobieranie historii zmian zachodzących we wpisach pochodzących z CEIDG.  |
| Repozytorium Aplikacji Zarządzania API | Zawiera informacje o kontach użytkowników, subskrypcje do API, konfigurację limitów ilości żądań dla użytkowników. |
| Log RODO | Logi generowane podczas wyświetlania danych osobowych w raporcie. W logu rejestrowana jest informacja o tym kiedy, komu i jakie raporty z danymi osobowymi zostały udostępnione (format JSON). |
| Replika bazy CEIDG | Replika operacyjnej bazy danych Rejestru CEIDG, aktualizowana na bieżąco (tzw. replika transakcyjna); stanowi bezpośrednie źródło danych biznesowych dla Interfejsu API oraz Bazy Hurtowni Danych, jak również jest źródłem informacji o rolach urzędników dla Aplikacji. |
| eKRS | Serwis eKRS to serwis prowadzony przez Ministerstwo Sprawiedliwości udostępniający dokumenty i informacje z Krajowego Rejestru Sądowego (KRS). Dane i informacje z eKRS udostępniane są poprzez API i stronę internetową <https://ekrs.ms.gov.pl/>. Usługi eKRS umożliwiają wyszukiwanie podmiotów z rejestru KRS. |

### Opis infrastruktury utrzymującej system CEIDG i HD

Infrastruktura wykorzystywana przez systemy Ministerstwa Rozwoju i Technologii mieści się w różnych lokalizacjach:

1. Ośrodek Podstawowy dla systemów CEIDG i Hurtowni Danych – to Usługa Chmury (PaaS) świadczona przez Dostawcę Chmury,
2. Infrastruktura MRIT – zbudowana w oparciu o dwie instancje środowiska wirtualizowanego w oparciu o oprogramowanie Vmware będąca Ośrodkiem zapasowym dla CEIDG i Hurtowni Danych, Ośrodkiem podstawowym dla Biznes.gov.pl oraz środowiskiem publikacji instancji produkcyjnej, testowej i developerskiej dla eDoręczeń.
3. Serwerownia zewnętrzna realizująca funkcję środowiska zapasowego dla Biznes.gov.pl (replikacja maszyn wirtualnych instancji produkcyjnej).

Z punktu widzenia dostępności Systemu CEIDG wykorzystywane są dwie Instancje: Instancja w Ośrodku Podstawowym będąca rozproszonym klastrem HA (dwie lokalizacje) i Instancja w Ośrodku Zapasowym. Instancje w Ośrodku Podstawowym i Zapasowym współpracują w trybie Active-Passive.

System CEIDG wykorzystuje w Ośrodku Podstawowym infrastrukturę sprzętową oferowaną jako usługi IaaS i PaaS.

Zakłada się, że czas przełączenia pomiędzy ośrodkami w przypadku wystąpienia Awarii wynosi nie więcej niż 24 godziny.

1. Ośrodek Podstawowy CEIDG. Dwie lokalizacje geograficzne, w których jest eksploatowana Instancja produkcyjna Systemu CEIDG.
2. Ośrodek Zapasowy więcej niż jedna lokalizacji geograficznych, w których eksploatowane są:
3. instancja zapasowa Systemu (replika instancji produkcyjnej Systemu CEIDG),
4. instancja testowa Systemu CEIDG,
5. instancja deweloperska Systemu CEIDG.
6. systemy zewnętrzne z którymi integruje się System CEIDG,
7. systemy uruchomione w lokalizacji Wykonawcy to Portal Serwisowy, którego elementem jest System Monitorowania Stanu systemów.

Monitoring

Rysunek 3 Ideowy diagram rozmieszczenia ośrodka Podstawowego i Zapasowego Systemu CEIDG



### Zakres czynności dla audytu infrastruktury CEIDG i HD

* + analiza wersji oprogramowania pod kątem znanych podatności,
	+ analiza konfiguracji dostępu do urządzenia,
	+ przegląd konfiguracji dot. użytkowników korzystających z urządzenia, praw dostępu, list
	+ dostępów, testy słabych haseł,
	+ analiza konfiguracji i reguł VPN,
	+ analiza wykorzystanych mechanizmów kryptograficznych,
	+ analiza zasad filtracji ruchu sieciowego,
	+ analiza pod kątem obecności niepożądanych usług,
	+ analiza mechanizmów logowania zdarzeń.
	+ analiza pod kątem wydawania kolejnych wersji oprogramowania w środowisku CI/CD GitLab

### Zakres czynności dla audytu aplikacji webowej - ceidg.gov.pl oraz dane.biznes.gov.pl (API, aplikacja raportowa), w tym pentesty portalu WWW

* + walidacja danych wejściowych w tym:
		- pliki cookie,
		- nagłówki.
	+ parametry wysyłane metodami http:
		- badanie sesji użytkowników aplikacji,
		- badanie komunikatów błędów,
		- badanie mechanizmów przekierowań,
		- badanie danych zapisywanych do bazy danych,
		- badanie integralności logów aplikacji,
		- szukanie funkcjonalności potencjalnie niebezpiecznych pod kątem wykorzystywanych zasobów (DoS),
		- badanie błędów logicznych aplikacji w miejscach krytycznych.
	+ badanie środowiska pracy aplikacji:
		- uprawnień w systemie plików oraz zasobów,
		- wersji usług,
		- użytego oprogramowania podnoszącego poziom bezpieczeństwa,
		- architektury systemu dotyczącej wszelkich obszarów bezpieczeństwa (składowanie logów, obsługa wyjątków itd.),
		- konfiguracji serwerów, z których korzysta aplikacja pod kątem bezpieczeństwa.

### Zakres czynności dla audytu konfiguracji systemów operacyjnych i baz danych ceidg.gov.pl oraz dane.biznes.gov.pl

* + analizę architektury i technologii platformy,
	+ analizę konfiguracji serwera (+uprawnień plików/katalogów),
	+ analizę architektury i technologii bazy danych,
	+ analizę konfiguracji aplikacji bazy danych,
	+ analizę dostępu do bazy danych, uprawnień,
	+ analizę mechanizmów logowania,
	+ analizy możliwych ataków.

### Cel audytu

* + wykonanie prac związanych ze zbadaniem wewnętrznych i zewnętrznych podatności i wynikających z nich zagrożeń wraz z oceną poziomu bezpieczeństwa,
	+ weryfikacja poziomu zapewnienia zasobów do monitorowania bezpieczeństwa systemów,
	+ dostarczenie wniosków, zaleceń, rekomendacji w celu dokładnego rozpoznania i redukcji wskazanych podatności oraz wskazanie adekwatnych działań mających na celu wyeliminowanie zagrożeń.

Po zakończeniu czynności audytowych Wykonawca jest zobowiązany do przedstawienia opracowania eksperckiego w formie raportu (szczegóły w części poświęconej Raportom).

Załącznik nr 1 dotyczący szczegółowego opis systemu jest dostępny w siedzibie wykonawcy po podpisaniu umowy poufności.

## Testy wydajności CEIDG i Hurtowni Danych

W ramach testów wydajności Wykonawca jest zobowiązany do przeprowadzenia:

* + Testów wydajnościowych (performance testing) – testy sprawdzające funkcjonowanie systemu przy ustalonym obciążeniu;
	+ Testów obciążeniowych (load testing) – testy sprawdzające ilość realizowanych transakcji w zadanym czasie;
	+ Testów przeciążeniowych (stress testing) – testy sprawdzające przeciążenie systemu zbyt dużą liczbą transakcji / użytkowników / danych;
	+ Testów skalowalności (capacity testing) – testy zwiększania obciążania systemu w celu wykrycia anomalii.

Jako wynik testów wydajności Wykonawca jest zobowiązany do opracowania oceny eksperckiej dla każdego z prowadzonych testów i przedstawienia w formie raportu (szczegóły w części poświęconej Raportom).

Celem przeprowadzenia audytu wydajności jest identyfikacja podatności i nieprawidłowości, które mogą stanowić zagrożenie dla stabilności i ciągłości działania systemu. Poza zapewnieniem kwestii ogólnie pojętej wydajności systemu, testy mają również wykryć potencjalne błędy które mogą przyczynić się do zaburzenia ciągłości i stabilności działania systemu oraz ewentualnie wskazać zalecane parametry dla konfiguracji systemu poprawiające jego wydajność.

Testy wydajności dla CEIDG i HD zostaną opracowane w wspólnie z Zamawiającym i będą dotyczyć maksymalnie trzech scenariuszów:

* + logowanie do hurtowni danych i generowanie raportu prostego
	+ logowanie do hurtowni danych i generowanie raportu złożonego
	+ logowanie do CEIDG i wykonanie scenariuszy podstawowej ścieżki urzędnika gminy
	+ testy wydajności w zakresie udostępnianych API (API v2, MSWF oraz API niepublicznego).

##

## Audyt bezpieczeństwa systemu i wszystkich modułów Punktu Informacji dla Przedsiębiorcy funkcjonującego w domenie \*.biznes.gov.pl (PIP).

### Opis systemu

Biznes.gov.pl to serwis internetowy realizujący zadania Punktu Informacji dla Przedsiębiorcy (PIP), oraz Centralnej Ewidencji i Informacji o Działalności Gospodarczej (CEIDG), który udostępnia informacje oraz usługi e-administracji związane z rozpoczęciem, wykonywaniem (w tym uzyskiwaniem koncesji, zezwoleń, licencji) i kończeniem działalności gospodarczej w Polsce. Biznes.gov.pl ma dwie wersje językowe – polską oraz angielską. Treści każdej wersji dopasowane są do potrzeb użytkowników odpowiednio polsko- i angielskojęzycznych. Przygotowane narzędzie - serwis https://www.Biznes.gov.pl ma charakter intuicyjny i jest łatwy w użyciu.

Planowany dalszy kierunek rozwoju serwisu Biznes.gov.pl to optymalizacja zasobów portalu pod kątem potrzeb użytkowników oraz wymagań prawnych oraz rozwój części usługowej tak, aby portal stawał się usługowo-informacyjnym centrum informacji o zakładaniu i prowadzeniu działalności gospodarczej w Polsce dla przedsiębiorców polskich oraz zagranicznych.

Kluczowy kierunek dla dalszego rozwoju Systemu wynika bezpośrednio z realizacji przez Ministerstwo Rozwoju i Technologii projektu „Konto Przedsiębiorcy – usługi online dla firm w jednym miejscu”, w ramach którego dokonano połączenie CEIDG z serwisem Biznes.gov.pl oraz budową e-usług obejmujących możliwe działania na wpisie CEIDG, w tym rejestrację działalności gospodarczej w CEIDG.

W ramach powyższego podziału w portalu Biznes.gov.pl funkcjonują następujące treści:

* + **Opisy usług** – usługą jest każda sprawa urzędowa, wynikająca z obowiązków nałożonych przez państwo i inicjowana przez obywatela. Opis usługi to przebieg postępowania administracyjnego, podatkowego lub sądowego. Ustandaryzowany opis usługi zawiera m.in. takie informacje jak: nazwę organu realizującego, opis kogo dotyczy procedura, wykaz potrzebnych dokumentów, termin załatwienia sprawy, wysokość należnej opłaty oraz sposób wnoszenia odwołań. Serwis obecnie udostępnia ok. 1,1 tys. opisów usług o zróżnicowanej objętości
	+ **Artykuły** – teksty publicystyczne dotyczące aktualnych zagadnień z zakresu tematyki interesującej dla przedsiębiorców m.in. wprowadzanych zmian w obszarze istotnym dla prowadzących działalności gospodarczą. Serwis obecnie udostępnia ok. 500 artykułów
	+ **E-usługi** – sprawy urzędowe, które są możliwe do zrealizowania elektronicznie, poprzez portal Biznes.gov.pl.
	+ **FAQ** - krótkie i precyzyjne odpowiedzi na najczęściej zadawane przez użytkowników portalu pytania. Odpowiedzi zawierają również przekierowania do treści portalu Biznes.gov.pl, które pogłębiają interesujący czytającego temat. Serwis obecnie udostępnia ok. 96 takich odpowiedzi
	+ **Wzory dokumentów**, np. wnioski, formularze do pobrania opracowane przez właściwy dla danej usługi organ. Stanowią uzupełnienie opisów usług oraz e-usług. Serwis obecnie udostępnia ok. 3,5 tys. wzorów dokumentów

W skład Systemu wchodzą usługi i aplikacje:

| Lp. | Nazwa modułu | Opis | URL | Wersje usług |
| --- | --- | --- | --- | --- |
|  | Portal /serwis | Portal informacyjny dla obywateli autorskiego CMS’a.  | https://www.biznes.gov.pl/pl | PRODTEST |
|  | ELF | Platforma usług elektronicznych służąca konfigurowaniu transakcyjnych publicznych usług online, ich testowaniu i ostatecznie produkcyjnemu udostępnianiu użytkownikom końcowym. Platforma składa się z dwóch podstawowych modułów: Konfigurator eLF i Runtime eLF | https://konfigurator.biznes.gov.plwww.biznes.gov.pl/pl/uslugi-online  | PRODTEST |
|  | Zaplecze (Baza Wiedzy) | Moduł umożliwiający wyznaczonym pracownikom instytucji publicznych tworzenie i zarządzanie produktami w Bazie Wiedzy.  | https://Zaplecze.biznes.gov.pl | PRODTEST |
|  | Akademia | Platforma e-learningowa dla użytkowników wraz z treściami multimedialnymi w postaci kursów i poradników | https://Akademia.biznes.gov.pl | PRODTEST |
|  | API (Baza Wiedzy) | Interfejs komunikacji do udostępnienia danych zgromadzonych w Bazie Wiedzy zarówno wewnętrznym modułom serwisu biznes,gov.pl (np. portal, platforma e-usług) jak i zewnętrznym serwisom | https://Api.biznes.gov.pl | PRODTEST |
|  | Głos Przedsiębiorcy | Moduł online Systemu biznes.gov.pl do zbierania pomysłów na ulepszenie prawa gospodarczego z możliwością komentowania i głosowania. | https://biznes.gov.pl/glos-przedsiebiorcy | PRODTEST |
|  | CMS / Polska Strefa Inwestycji (dalej PSI) | Serwis internetowy oparty o CMS dedykowany dla stref inwestycyjnych w Polsce.  | https://biznes.gov.pl/inwestycjehttps://www.biznes.gov.pl/en | PRODTEST |
|  | SOZ | System obsługi zgłoszeń zbieranych od użytkowników wskazanych portali informacyjnych i następnie procesowanie tych zgłoszeń.  | https://Soz.biznes.gov.pl | PRODTEST |
|  | Konto (Baza Wiedzy) | Moduł pozwalający użytkownikom zarejestrować się w serwisie biznes.gov.pl oraz pozwalający im na zarządzanie swoimi danymi powiązanymi z ich kontem. | https://Konto.biznes.gov.pl | PRODTEST |
|  | Logowanie (Baza Wiedzy) | Moduł odpowiedzialnym za autentykację użytkowników serwisu. | https://Logowanie.biznes.gov.pl | PRODTEST |
|  | CI/CD | Środowisko dostarczania i integracji Systemu \*.biznes.gov.plModuł dostępny z wyznaczonych sieci.  | https://gitlab.biznes.gov.pl | PROD |
|  | Zulip | Platforma do komunikacji w departamencie, projektach i umowach prowadzonych przez departament.  | https://Zulip.biznes.gov.pl | PROD |
|  | Redmine | Oprogramowanie do zarządzania projektem.  | https://Zgłoszenia.biznes.gov.pl | PRODTEST |
|  | Media serwer | Serwer multimediów w portalu.  | https://Media.biznes.gov.pl | PRODTEST |
|  | Poczta | Serwer pocztowy w systemie. | https://Poczta.biznes.gov.pl | PRODTEST |
|  | Projekty | Serwer świadczący usługi związane z utrzymaniem design Systemu dla nowych formularzy CEIDG. | https://Projekty.biznes.gov.pl | PROD |
|  | SVN | Repozytorium plików projektu związanego z budową, utrzymaniem i rozwojem Systemu. | https://Svn.biznes.gov.pl | PROD |
|  | Styleguide | Zbiór makiet, wzorców graficznych, praktyk użyty do tworzenia stron interfejsów graficznych dla użytkowników Systemu we wszystkich aplikacjach Systemu. | https://Styleguide.biznes.gov.pl | PROD |
|  | Static | Serwer plików statycznych do Systemu.  | https://Static.biznes.gov.pl | PRODTEST |
|  | eDoręczenia | Moduł konta przedsiębiorcy do realizacji eDoręczeń | https://konto.biznes.gov.pl/pl/moje-konto/e-doreczenia/ | PRODTEST |
|  | Wyszukiwarka Firm | Front wyszukiwania firm w rejestrach CEIDG oraz KRS. | https://www.biznes.gov.pl/pl/wyszukiwarka-firm | PRODTEST |

### Opis infrastruktury utrzymującej system

W celu realizacji zadań Systemu został on zbudowany w oparciu o sprzęt serwerowy o architekturze kasetowej, sprzęt sieciowy zapewniający komunikację w ramach sieci LAN i WAN oraz realizujący ochronę przed nieuprawnionym dostępem i atakami sieciowymi. Dostarczone zostały również systemy pomocnicze:

1. Zarządzanie wirtualizacją
2. Kopie bezpieczeństwa
3. Monitorowanie i administracji

Sprzęt został zainstalowany w trzech szafach serwerowych w serwerowni Departamentu Gospodarki Cyfrowej wyposażonej w zabezpieczenia fizyczne i logiczne, spełniające wysokie wymogi bezpieczeństwa. Pełna specyfikacja sprzętowa oraz katalog technologii wykorzystywanych do utrzymywania systemu \*.biznes.gov.pl został opisany w załączniku numer 2.

### Zakres audytu infrastruktury systemu i wszystkich modułów Punktu Informacji dla Przedsiębiorcy funkcjonującego w domenie \*.biznes.gov.pl (PIP)

* + analiza wersji oprogramowania pod kątem znanych podatności,
	+ analiza konfiguracji dostępu do urządzeń,
	+ przegląd konfiguracji dot. użytkowników korzystających z urządzeń, prawa dostępu, listy
	+ dostęp testy słabych haseł,
	+ analiza konfiguracji i reguł VPN,
	+ analiza wykorzystanych mechanizmów kryptograficznych,
	+ analiza zasad filtracji ruchu sieciowego,
	+ analiza pod kątem obecności niepożądanych usług,
	+ analiza mechanizmów logowania zdarzeń.

### Zakres audytu aplikacji webowych - systemu i wszystkich modułów Punktu Informacji dla Przedsiębiorcy funkcjonującego w domenie \*.biznes.gov.pl (PIP), w tym pentesty portalu WWW

* + walidacja danych wejściowych w tym:
		- pliki cookie,
		- nagłówki.
	+ parametry wysyłane metodami http:
		- badanie sesji użytkowników aplikacji,
		- badanie komunikatów błędów,
		- badanie mechanizmów przekierowań,
		- badanie danych zapisywanych do bazy danych,
		- badanie integralności logów aplikacji,
		- szukanie funkcjonalności potencjalnie niebezpiecznych pod kątem wykorzystywany zasobów (DoS),
		- badanie błędów logicznych aplikacji w miejscach krytycznych.
	+ badanie środowiska pracy aplikacji:
		- uprawnień w systemie do plików oraz zasobów,
		- użytego oprogramowania podnoszącego poziom bezpieczeństwa,
		- architektury systemu dotyczącej wszelkich obszarów bezpieczeństwa (składowanie logów, obsługa wyjątków itd.),
		- konfiguracji serwerów, z których korzysta aplikacja pod kątem bezpieczeństwa.

### Zakres audytu konfiguracji systemów operacyjnych i baz danych środowiska produkcyjnego, w zakresie systemu i wszystkich modułów Punktu Informacji dla Przedsiębiorcy funkcjonującego w domenie \*.biznes.gov.pl (PIP)

* + analiza architektury i technologii platformy,
	+ analiza konfiguracji serwerów (+uprawnień plików/katalogów),
	+ analiza architektury i technologii bazy danych,
	+ analiza konfiguracji aplikacji bazy danych,
	+ analiza dostępu do bazy danych i uprawnień,
	+ analiza mechanizmów logowania,
	+ analiza możliwych ataków

Przeprowadzone badania i analiza w trakcie audytu powinny wskazać podatności i zagrożenia wynikające z:

* + zastosowanych technologii i standardów zabezpieczeń,
	+ słabości oprogramowania oraz poprawności konfiguracji systemów sieciowych,
	+ faktu istnienia styków sieci o różnym charakterze, np. styku z siecią Internet, styku

systemów z innymi sieciami, w tym potencjalne zagrożenia ze strony sieci zewnętrznej,

* + polityk bezpieczeństwa skonfigurowanych na ww. urządzeniach.

### Cel audytu

* + wykonanie prac związanych ze zbadaniem wewnętrznych i zewnętrznych podatności i wynikających z nich zagrożeń wraz z oceną poziomu bezpieczeństwa,
	+ dostarczenie wniosków, zaleceń, rekomendacji w celu dokładnego rozpoznania i redukcji wskazanych podatności oraz wskazanie adekwatnych działań mających na celu wyeliminowanie zagrożeń.

Po zakończeniu czynności audytowych Wykonawca jest zobowiązany do przedstawienia opracowania eksperckiego w formie raportu (szczegóły w części poświęconej Raportom).

## Testy wydajności systemu i modułów systemu \*.biznes.gov.pl

Punkt Informacji dla Przedsiębiorcy składa się z następujących autonomicznych elementów:

* + System Konfiguratora ELF
	+ System Runtime ELF
	+ Aplikacja Zaplecza
	+ API Zaplecza
	+ Podsystem logowania/rejestracji
	+ CMS / Polska Strefa Inwestycji (dalej PSI)

SMCCelem przeprowadzenia audytu wydajności jest identyfikacja podatności i nieprawidłowości, które mogą stanowić zagrożenie dla stabilności i ciągłości działania systemu. Poza zapewnieniem kwestii ogólnie pojętej wydajności systemu, testy mają również wykryć potencjalne błędy które mogą przyczynić się do zaburzenia ciągłości i stabilności działania systemu oraz ewentualnie wskazać zalecane parametry dla konfiguracji systemu poprawiające jego wydajność.

Celem testów jest ustalenie :

* + liczba sesji dla której charakterystyka obciążenia w funkcji czasu odchodzi od zależności liniowej
	+ średni czas odpowiedzi ładowania strony zaczyna rosnąć gwałtownie),
	+ liczba sesji dla której czas średni odpowiedzi (ładowania strony) zaczyna rosnąć,
	+ liczba sesji dla której czas średni odpowiedzi (ładowania strony) wynosi maksymalnie 10 sek.

Do testów należy założyć, że średnio akcja użytkownika w sesji skutkująca przeładowanie strony odbywa się przeciętnie co 10 sekund.

Testy wydajności powinny uwzględniać:

* + Upload załączników realizowanych metodą HTTP POST,
	+ Testy end-end z uwzględnieniem ograniczeń łącza dostępowego symetrycznego (dla 50, 100,
	+ 150, 200 Mb),
	+ Testy z pominięciem ograniczeń jakie wprowadza wydajność łącza dostępowego,

Jako wynik testów wydajności Wykonawca jest zobowiązany do opracowania oceny eksperckiej dla każdego z prowadzonych testów i przedstawienia w formie raportu (szczegóły w części poświęconej Raportom).

### Zakres audytu wydajności dla Systemu Konfiguratora eLF i Aplikacji Zaplecza

Testy serwera www: dla jednoczesnych sesji: 0…5000 – pomiar czasów odpowiedzi serwera i czasu załadowania strony (gotowość usługi dla: nowa usługa, edycja usługi) Czasy odpowiedzi i ładowania maja obejmować wartości średnie i maksymalne dla każdego punktu pomiarowego.

Konfigurator eLF działa w oparciu o AngularJS oraz mikroserwisy, co może wymagać od systemu testującego symulowanie rzeczywistych działań przeglądarki przez uruchomienie aplikacji JS.

Aplikacja Zaplecza (PHP) wymaga dodatkowo symulacji logowania na jedno lub wiele indywidualnych kont.

### Zakres audytu wydajności dla Systemu Runtime eLF

Testy serwera www: dla jednoczesnych sesji: 0…5000 – pomiar czasów odpowiedzi serwera i czasu załadowania stron (liczona jako osiągnięcie stanu aplikacji JS na przeglądarce, objawiająca się odpowiednim HTML). Kolejne strony są sterowane i przełączane w ramach danej sesji przez aplikację JS (nie ma możliwości wywołania ich przechodząc do ich URL).

Czasy odpowiedzi i ładowania maja obejmować wartości średnie i maksymalne dla każdego punktu pomiarowego. Aplikacja działa w oparciu o AngularJS oraz mikroserwisy, co może wymagać od systemu testującego symulowanie rzeczywistych działań przeglądarki przez uruchomienie aplikacji JS.

Elementami pełnej sesji użytkownika jest podpisanie oraz przesłanie pliku, a na jej koniec upload utworzonego dokumentu (wielkość dokumentu 1MB, 5MB, 10MB). W trakcie samej sesji mogą być również przesyłane załączniki.

### Zakres audytu wydajności dla Podsystemu logowania/rejestracji

Test serwera www: dla jednoczesnych sesji: 0…5000 – pomiar czasów załadowania strony Podsystem ten wymaga przeprowadzenia testów dwóch procesów.

Procesu rejestracji:

* + wypełnienie i przesłanie formularza,
	+ odebranie wiadomości z kodem,
	+ wprowadzenie otrzymanego kodu w formularzu na stronie

Procesu logowania:

* + zalogowanie się na utworzone konto,
	+ symulacje działań użytkownika w serwisie w szczególności:

### Zakres audytu wydajności dla API – Baza Wiedzy - Zaplecza

* + Średni i maksymalne czasy odpowiedzi dla dwu rodzajów zapytań:
	+ Zapytania proste (zawierające listę parametrów, zmieniających się przy wywołaniach w ramach zdefiniowanych zakresów lub random)
* /ApiProcedures/getDetails
* /ApiCommons/getPKD
* /ApiInstitutions/getCategories
* /ApiProcedures/getList
* /ApiPublications/getDetails
* /ApiCommons/getPKDDetails
* /ApiProcedures/getThematicCategories
* /ApiInstitutions/getDetails
* /ApiGuide/getList
* /ApiProcedures/getProfessionCategories
* /ApiPnaAddress/getListByPostCode
* /ApiPnaAddress/getStreetHints
	+ Zapytania złożone - sekwencja wywołań, która przyjmuje wartości otrzymane w odpowiedziach poprzedzających zapytań:
* /ApiGuide/getDescription
* /ApiGuide/startGuide
* /ApiGuide/setAnswer
* wielokrotnie, aż odpowiedź wskaże, że to ostatnie pytanie
* /ApiGuide/getSummary
* /ApiGuide/getPDFGuide
	+ • Każdy z testów dla 0…10 000 jednoczesnych zapytań

API nie wymaga logowania, jednak w samych zapytaniach złożonych ważna jest kolejność oraz przeparsowania odebranych odpowiedzi. Na początku sesji jest wymaganie odczytanie otrzymanego Hash w celu wykorzystania go do dalszej komunikacji.

## Audyt bezpieczeństwa systemu Tracker 2.0, wraz z e-sługami Licencjonowania i ewidencjonowania obrotu towarami wrażliwymi na biznes.gov.pl (dla przedsiębiorców)

Minister właściwy do spraw gospodarki prowadzi rejestr udzielonych zezwoleń indywidualnych i zezwoleń globalnych oraz podmiotów korzystających z zezwoleń generalnych, w tym rejestr udzielonych zezwoleń na wywóz broni palnej, części i istotnych komponentów oraz amunicji.

Rejestr jest prowadzony przy wykorzystaniu systemu teleinformatycznego Tracker.

Systemem Tracker 2.0 wykorzystuje udostępnione na portalu Biznes.gov.pl e-usługi, za pośrednictwem których przedsiębiorcy będą realizować sprawy związane z obrotem towarami, technologiami i usługami o znaczeniu strategicznym. System Tracker 2.0 i system biznes.gov.pl komunikują się z ePUAP i Login.gov.pl.

Specyfikacja sprzętowa oraz katalog technologii wykorzystywanych do utrzymywania systemu Tracker 2.0 został opisany w Załączniku nr 3 do OPZ.

Zamawiający udostępni Załącznik nr 3 do OPZ w siedzibie Zamawiającego po uprzednim podpisaniu przez zainteresowane podmioty oświadczenia o poufności.

W ramach audytu Wykonawca jest zobowiązany do:

1. przeprowadzenia badań i testów bezpieczeństwa e-usług na biznes.gov.pl (nie więcej niż 12 e-usług) wykorzystywanych na potrzeby realizować sprawy związane z obrotem towarami, technologiami i usługami o znaczeniu strategicznym,
2. opracowania oceny eksperckiej dla każdej z badanych i testowanych e-usług i przedstawienia w formie raportu,
3. przedstawienia na podstawie wyników oceny stanowiska dotyczącego potrzeb wprowadzenia zmian w e-usługach w formie raportu,
4. przeprowadzenia badań i testów bezpieczeństwa systemu Tracker 2.0, zgodnie z wymaganiami określonymi w OPZ i dobrymi praktykami prowadzenia audytów bezpieczeństwa,
5. przeprowadzenia audytu bezpieczeństwa przetwarzania danych, w tym danych osobowych,
6. opracowania oceny eksperckiej z przeprowadzonych badań i testów i przedstawienia w formie raportu,
7. przedstawienia rekomendacji zmian (jeżeli będą wskazane potrzeby zmian) w zakresie bezpieczeństwa systemu Tracker 2.0, bezpieczeństwa przetwarzania danych, w tym danych osobowych i przedstawienia w formie raportu.

## Testy wydajności systemu teleinformatycznego Tracker 2.0

W ramach testów wydajności Wykonawca jest zobowiązany do przeprowadzenia:

1. Testów wydajnościowych (performance testing) – testy sprawdzające funkcjonowanie systemu przy ustalonym obciążeniu;
2. Testów obciążeniowych (load testing) – testy sprawdzające ilość realizowanych transakcji w zadanym czasie;
3. Testów przeciążeniowych (stress testing) – testy sprawdzające przeciążenie systemu zbyt dużą liczbą transakcji / użytkowników / danych;
4. Testów skalowalności (capacity testing) – testy zwiększania obciążania systemu w celu wykrycia anomalii.

Jako wynik testów wydajności Wykonawca jest zobowiązany do opracowania oceny eksperckiej dla każdego z prowadzonych testów i przedstawienia w formie raportu (szczegóły w części poświęconej Raportom).

## Świadczenie usług wsparcia eksperckiego inżyniera bezpieczeństwa

Wykonawca zobowiązany jest do udzielania wsparcia eksperckiego w kwestiach związanych z bezpieczeństwem i jakością tworzonego lub utrzymywanego oprogramowania w zakresie m.in.:

1. wdrożeń rozwiązań informatycznych obszaru monitorowania bezpieczeństwa IT,
2. analizy zagrożeń zewnętrznych i wewnętrznych w obszarze cyberbezpieczeństwa,
3. detekcji błędów aplikacyjnych,
4. recenzji architektury logicznej,
5. analizy podatności występujących w zainstalowanej wersji serwera,
6. skanowania podatności w udostępnionych usługach sieciowych,
7. detekcji podatności w udostępnionych aplikacjach webowych (np. próby ominięcia ekranów logowania, kradzież danych z aplikacji),
8. próby eskalacji ataku na pozostałe maszyny, systemy w LAN po przejęciu kontroli nad jedną z aplikacji,
9. analizy kodu źródłowego aplikacji.

Jako wynik prac Wykonawca jest zobowiązany do opracowania oceny eksperckiej i przedstawienia w formie raportu (szczegóły w części poświęconej Raportom).

# **Część II -** **opis systemów oraz zakres czynności audytowych.**

## Audyt bezpieczeństwa dwóch systemów informatycznych platformy PEF udostępnianych przez Brokerów PEF

Aplikacje PEF służą użytkownikom do wymiany elektronicznych dokumentów, w tym ustrukturyzowanych faktur elektronicznych.

Wykonawca wykona audyt aplikacji i systemów Brokerów PEF.

Audytem zostanie objęte nie więcej niż 15 serwerów fizycznych/wirtualnych dla każdego z dwóch systemów informatycznych. Zakres audytów obejmuje dwa portale internetowe. Dla każdego z systemów audytem objęte zostanie nie więcej niż 20 formularzy HTML oraz nie więcej niż 2 zapory sieciowe. Dla każdego z systemów audytem powinno być objęte nie więcej niż 10 przełączników, nie więcej niż 2 load-balancery oraz nie więcej niż 2 routery (trasowniki). Dla każdego z systemów zakres audytu obejmuje nie więcej niż 5 dedykowanych systemów bezpieczeństwa – typy minimum IDS/IPS, UTM, WAF. Każdy z systemów posiada nie więcej niż 5 hostów w puli adresacji zewnętrznej.

Każda z aplikacji zawiera około 40 podstron i ekranów, z czego około połowa to formularze dynamicznie generowane. Łączna liczba pól w formularzach przekracza 300 dla każdej z aplikacji, a liczba wszystkich używanych zmiennych w systemach przekracza 1000.

Aplikacje PEF umożliwiają utworzenie różnych typów użytkowników.

W ramach audytu Wykonawca jest zobowiązany do:

1. przeprowadzenia badań i testów bezpieczeństwa systemu informatycznego platformy PEF oddzielnie dla każdego z dwóch Brokerów, w szczególności:
	* proces rejestracji konta podmiotu
	* proces rejestracji i uwierzytelniania kont użytkowników
	* proces tworzenia, przesyłania i odbierania dokumentów elektronicznych, w tym wykorzystania mechanizmów API
	* prawidłowość funkcjonowania sesji zalogowanego użytkownika
	* aktualność oprogramowania
	* procedury tworzenia kopii bezpieczeństwa
	* podatności systemu
	* zastosowanych technologii i standardów zabezpieczeń,
	* metod i protokołów wymiany danych oraz architektury interfejsów międzysystemowych i międzysieciowych w tym z siecią Peppol,
	* poprawności konfiguracji komponentów rozwiązania, takich jak, systemy obsługi transmisji, systemy zaporowe i inne systemy usługowe i pomocnicze,
	* odporność na ataki m.in. typu Injection, DoS/DDoS,
2. przeprowadzenia audytu bezpieczeństwa przetwarzania danych, w tym danych osobowych,
3. opracowania raportów wraz z ocenami eksperckimi (osobno dla każdego z systemów Brokerów) obejmujących stwierdzone nieprawidłowości oraz wymagane do wprowadzenia zmiany w systemach informatycznych i e-usługach wraz z sugerowanym sposobem ich implementacji.

## Audyt bezpieczeństwa systemu informatycznego Książki Adresowej PEF wraz z Wyszukiwarką na Portalu PEF (efaktura.gov.pl)

Portal efaktura.gov.pl stanowi kompendium wiedzy o elektronicznym fakturowaniu w zamówieniach publicznych oraz repozytorium dokumentacji użytkowników. Portal umożliwia wyszukanie adresu PEF odbiorcy dokumentu, przechowywanego w bazie adresowej podmiotów zarejestrowanych na PEF – Książce Adresowej PEF.

Audytem zostanie objęte:

* + nie więcej niż 6 serwerów fizycznych/wirtualnych
	+ portal internetowy oraz aplikacja webowa
	+ nie więcej niż 18 formularzy HTML
	+ nie więcej niż 2 zapory sieciowe działające w trybie HA
	+ 1 load-balancer, 2 przełączniki i 2 trasowniki działające w trybie HA
	+ dla każdego z systemów zakres audytu obejmuje nie więcej niż 5 dedykowanych systemów bezpieczeństwa – typy minimum IDS/IPS, UTM, WAF.

W ramach audytu Wykonawca jest zobowiązany do:

1. przeprowadzenia badań i testów bezpieczeństwa Portalu PEF (<https://efaktura.gov.pl>) oraz systemu informatycznego Książki Adresowej PEF, w szczególności:
	* proces rejestracji i uwierzytelniania kont użytkowników,
	* prawidłowość funkcjonowania sesji zalogowanego użytkownika,
	* aktualność oprogramowania,
	* procedury tworzenia kopii bezpieczeństwa,
	* podatności systemu,
	* zastosowanych technologii i standardów zabezpieczeń,
	* metod i protokołów wymiany danych oraz architektury interfejsów międzysystemowych i międzysieciowych,
	* poprawności konfiguracji komponentów rozwiązania, takich jak, systemy obsługi transmisji, systemy zaporowe i inne systemy usługowe i pomocnicze,
	* odporność na ataki m.in. typu Injection, DoS/DDoS,
2. audyt bezpieczeństwa przetwarzania danych, w tym danych osobowych.
3. opracowania raportu wraz z oceną ekspercką obejmującą stwierdzone nieprawidłowości oraz wymagane do wprowadzenia zmiany w systemie informatycznym wraz z sugerowanym sposobem ich implementacji

## Świadczenie usług wsparcia eksperckiego inżyniera bezpieczeństwa

Wykonawca zobowiązany jest do udzielania wsparcia eksperckiego w kwestiach związanych z bezpieczeństwem i jakością tworzonego lub utrzymywanego oprogramowania w zakresie m.in.:

1. wdrożeń rozwiązań informatycznych obszaru monitorowania bezpieczeństwa IT,
2. analizy zagrożeń zewnętrznych i wewnętrznych w obszarze cyberbezpieczeństwa,
3. detekcji błędów aplikacyjnych,
4. recenzji architektury logicznej,
5. analizy podatności występujących w zainstalowanej wersji serwera,
6. skanowania podatności w udostępnionych usługach sieciowych,
7. detekcji podatności w udostępnionych aplikacjach webowych (np. próby ominięcia ekranów logowania, kradzież danych z aplikacji),
8. próby eskalacji ataku na pozostałe maszyny, systemy w LAN po przejęciu kontroli nad jedną z aplikacji,
9. analizy kodu źródłowego aplikacji.

Jako wynik prac Wykonawca jest zobowiązany do opracowania oceny eksperckiej i przedstawienia w formie raportu (szczegóły w części poświęconej Raportom).

# **Szczegóły dotyczące procesu realizacji usługi w ramach części I**

## Audyt bezpieczeństwa przetwarzania danych.

Audyt **bezpieczeństwa przetwarzania danych** będzie realizowany zgodnie z wymaganiami wymienionymi w rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności oraz zgodnie z normami: ISO 27001 „Technika informatyczna. Techniki Bezpieczeństwa. systemu zarządzania bezpieczeństwem informacji. Wymagania” i ISO 27002 „Technika informatyczna – Praktyczne zasady zarządzania bezpieczeństwem informacji”.

W audytowanych systemach nie będą przetwarzane dane niejawne w rozumieniu ustawy o ochronie informacji niejawnych z 5 sierpnia 2010 (Dz. U. z 2010 r. nr 182, poz. 1228).

W obszarze zapewnienia bezpieczeństwa przetwarzanych danych oraz ochrony danych, audytowane systemy powinny zagwarantować:

1. poufność – zabezpieczenie danych przed ich udostępnieniem nieuprawnionemu odbiorcy,
2. integralność – zabezpieczenie danych przed modyfikacją lub zniekształceniem przez nieuprawnionych użytkowników,
3. rozliczalność – określenie i weryfikowanie odpowiedzialności za wykorzystanie systemu,
4. autentyczność – weryfikacje tożsamości podmiotów i prawdziwości zasobów,
5. niezawodność – gwarancja oczekiwanego zachowania systemu.

**Audyt obejmuje sprawdzenie aktualnego stanu przetwarzania danych osobowych** zarówno pod kątem zagadnień technicznych, organizacyjnych oraz prawnych ze szczególnym uwzględnieniem wymagań opisanych w ustawie o ochronie danych osobowych.

Zakres audytu:

1. Przegląd i analiza dokumentacji, w tym analiza dokumentacji polityk bezpieczeństwa i procedur, pod kątem zgodności z wymaganiami (w zakresie jak wyżej) Rozporządzenia, ze szczególnym uwzględnieniem zagadnień IT.
2. Weryfikacja zgodności systemów z wymaganiami Rozporządzenia (w zakresie jak wyżej), ze szczególnym uwzględnieniem zagadnień IT.
3. Weryfikacja kwalifikacji personelu odpowiedzialnego za bezpieczeństwo badanych systemów oraz przestrzegania procedur bezpieczeństwa przez pracowników (realizujących postanowienia polityk bezpieczeństwa).

## Audyt bezpieczeństwa systemów teleinformatycznych.

Celem audytów jest wykrycie faktycznych oraz potencjalnych luk i błędów w oprogramowaniu, konfiguracji urządzeń informatycznych, portalach i aplikacjach webowych, które mogą być wykorzystane do naruszenia bezpieczeństwa przetwarzanych informacji, a także bezpieczeństwa Zamawiającego lub użytkowników systemów.

Zakres audytu (założenia ramowe):

* 1. analiza architektury sieciowej,
		+ weryfikacja sieci LAN na strefy sieciowe (w tym wykorzystanie urządzeń typu firewall oraz VLAN),
		+ określenie usług działających w wybranych podsieciach (do 10 podsieci – nie więcej niż 15 hostów dla jednego systemu),
		+ poszukiwanie podatności w wybranych podsieciach (do 10 podsieci – nie więcej niż 15 hostów dla jednego systemu),
		+ weryfikacja mechanizmów ochronnych w warstwie 2 i 3 modelu OSI,
		+ weryfikacja dostępu do Internetu z LAN,
		+ szczegółowa analiza komunikacji sieciowej,
		+ weryfikacja zasad utrzymania sieci,
		+ analiza wersji oprogramowania pod kątem znanych podatności (firmware),
		+ analiza konfiguracji dostępu do urządzenia,
		+ przegląd konfiguracji dot. użytkowników korzystających z urządzenia, praw dostępu, list dostępów, testy słabych haseł,
		+ analiza konfiguracji i reguł VPN,
		+ analiza wykorzystanych mechanizmów kryptograficznych,
		+ analiza zasad filtracji ruchu sieciowego,
		+ analiza pod kątem obecności niepożądanych usług,
		+ analiza mechanizmów logowania zdarzeń
	2. analiza brzegu sieci
		+ weryfikacja topologii/architektury sieci,
		+ testy szczelności systemów klasy firewall (w tym działania funkcji IPS obsługującej w czasie rzeczywistym zagrożenia typu nadużycie protokołu, próby tunelowania, oprogramowania typu exploit, kontrola aplikacji, ataki ogólnego typu bez predefiniowanych sygnatur, ruchu generowanego przez szkodliwe oprogramowanie, podatności serwera i klienta wraz z możliwością definiowania własnych sygnatur, regularności aktualizacji firewall w celu przeciwdziałania nowym zagrożeniom, itp.)
		+ ogólna analiza komunikacji sieciowej z poziomu sieci Internet,
		+ skanowanie portów różnymi technikami, w celu wykrycia potencjalnych luk bezpieczeństwa w udostępnianych usługach,
		+ wykrywanie usług sieciowych udostępnionych w sieci Internet,
		+ próba detekcji wersji oraz typu oprogramowania systemowego zainstalowanego na urządzeniach dostępnych z sieci Internet,
		+ testowanie odporności usług wystawionych do sieci Internet na ataki „Denial of Service” co najmniej 2 metodami zaproponowanymi przez Wykonawcę,
		+ testowanie odporności usług wystawionych do sieci Internet, za pomocą narzędzi eksploatujących typowe luki bezpieczeństwa.
	3. analiza bezpieczeństwa konfiguracji systemów informatycznych (urządzeń i aplikacji)
		+ analiza zgodności konfiguracji i sposobu funkcjonowania urządzeń:
	+ weryfikacja udostępnionych usług sieciowych,
	+ weryfikacja zbędnych usług wraz ze wskazaniem ich podatności,
	+ weryfikacja zaimplementowanych systemów aktualizacji,
	+ weryfikacja zaimplementowanych systemów logowania zdarzeń,
	+ weryfikacja mechanizmów administracji zdalnej,
	+ weryfikacja przypisania użytkowników do właściwych grup,
	+ weryfikacja uprawnień zgodnie z pryncypium jak najmniejszych uprawnień (ang. „least privilige”),
	+ przeprowadzenie prób obejścia uprawnień i uzyskania nieautoryzowanego dostępu do informacji,
	+ weryfikacja sposobu udostępniania baz danych na poziomie sieciowym,
	+ analiza implementacji podstawowych zasad hardeningowych bazy danych (np. wyłączenie nieużywanych usług, wyłączenie nieużywanych metod dostępu, konfiguracja uprawnień do obiektów, logowanie zdarzeń, składowanie logów, monitorowanie dostępu do obiektów, monitorowanie instrukcji języka SQL),
	+ analiza architektury baz danych (np. wykorzystanie mechanizmów autoryzacji oraz uwierzytelniania, segmentacja uprawnień, wykorzystywanie widoków, wykorzystywanie procedur składowych, przechowywanie oraz dostęp do danych wrażliwych, przechowywanie oraz dostęp do danych audytowych, szyfrowanie danych),
	+ analiza komunikacji z klientami bazodanowymi (mechanizmy kryptograficzne, transfery danych).
		- analiza podatności aplikacji
	+ wytypowanie wrażliwych punktów w aplikacji,
	+ inspekcja mechanizmów uwierzytelniania / autoryzacji,
	+ zabezpieczenia interfejsu użytkownika za pomocą captcha oraz za pomocą zweryfikowanego certyfikatu, two-factor authentication (2FA)
	+ weryfikacja implementacji mechanizmów ochronnych dla serwerów aplikacyjnych,
	+ weryfikacja obsługi błędów,
	+ analiza poziomu bezpieczeństwa oferowanego przez aplikacje,
	1. przeprowadzenie testów penetracyjnych i symulowanych ataków (wg najnowszych wytycznych OWASP wymienionych na liście TOP10 aktualnej na dzień realizacji audytu) obejmujących:
		+ testy bezpieczeństwa aplikacji pod kątem, m.in.:
	+ ataków semantycznych na adres URL,
	+ ataków związanych z ładowaniem plików,
	+ ataków typu Cross-Site Scripting,
	+ ataków typu Cross-Site Request Forgery,
	+ ataków typu MITM (Man in the Middle),
	+ ataków typu Cross Site Tracing,
	+ ataków typu Session Hijacking / Session Fixation,
	+ ataków typu Forced Browsing,
	+ ujawnienia kodu/ścieżki dostępu (Path Disclousure),
	+ ujawnienia parametrów ograniczających (Parameter Delimiter)
	+ podrabiania zarządzania formularza,
	+ sfałszowania żądania http,
	+ ujawnienia danych przechowywanych w bazie,
	+ trawersowania katalogów (Path Traversal),
	+ ujawniania kodu źródłowego,
	+ przepełnienia bufora lub stosu,
	+ wstrzykiwania kodu wykonywalnego innych języków programowania (np. SQL Injection / JSON Injection),
	+ niepożądanego przekierowania,
		- badanie enumeracji i wykorzystania znanych podatności w celu uzyskania nieautoryzowanego dostępu,
		- badanie możliwości podszywania się pod użytkowników i uzyskania nieautoryzowanego dostępu do systemu
		- badanie możliwości podszywania się pod użytkowników uprzywilejowanych i uzyskanie dostępu do systemu
		- badanie możliwości blokowania/umożliwienia dostępu do systemu wszystkim lub wybranym jej użytkownikom,
		- badanie możliwości modyfikacji/usunięcia danych z systemu.

## *Audyt funkcjonowania systemów bezpieczeństwa*.

Audyt obejmuje analizę i ocenę funkcjonowania następujących systemów bezpieczeństwa:

1. System antywirusowy.
2. System antyspamowy.
3. System DLP (Data Leak Prevention/Data Loss Prevention).
4. System Firewall.
5. System backupowy wraz z testem odtworzenia systemu z backupu (Zamawiający nie wymaga odtwarzania systemu na zasobach Wykonawcy), ocena lokalizacji baz danych zawierających kopie bezpieczeństwa (bezpieczeństwo ośrodka, ośrodek zapasowy).
6. System zasilania awaryjnego.

Zakres audytu:

1. Kompleksowa analiza skuteczności działania.
2. Analizę procedur utrzymaniowych i monitorowania systemów bezpieczeństwa.
3. Weryfikacja poprawności konfiguracji systemów bezpieczeństwa.
4. Weryfikacja i/lub opracowanie wskaźników efektywności.

## Raporty

W wyniku przeprowadzonych prac Wykonawca dostarczy raporty (na zasadach określonych dla każdego etapu) zawierające przykładowo:

1. opis przeprowadzonych działań (w tym weryfikacji dokumentacji i wykonanych testów)
2. opis ryzyka dla danego systemu informatycznego
3. propozycja uruchomienia dodatkowych mechanizmów bezpieczeństwa umożliwiających ochronę przed możliwymi atakami sieciowymi i aplikacyjnymi
4. wyniki działań, testów i ich interpretacja, w szczególności:
	* + informacje dotyczące ogólnej oceny poziomu bezpieczeństwa oraz odporności na ataki badanych systemów zawierające podsumowanie ilości stwierdzonych nieprawidłowości w podziale na systemy i krytyczności,
		+ opis lokalizacji wykrytych podatności - sposobu, w jaki można zlokalizować i powtórzyć testowy atak na podatność,
		+ Informacje na temat poziomu ochrony realizowanego przez system zabezpieczeń
5. opis technicznych znalezionych podatności w obu obszarach wraz z zaleceniami i rekomendacjami mającymi na celu zminimalizowanie bądź całkowitą redukcję ryzyka związanego z wykrytymi podatnościami
6. identyfikacja tzw. wąskich gardeł
7. wnioski z audytu, działań (określenie ilościowego i jakościowego poziomu niebezpieczeństwa podatności)
8. Rekomendacje i zalecenia pozwalające na usunięcie wykrytych słabości, a tym samym podniesienie poziomu bezpieczeństwa badanych systemów (określenia sposobu naprawy wykrytych podatności w tym zmian konfiguracyjnych)
9. rekomendacje w zakresie rozbudowy systemu informatycznego w celu podniesienia bezpieczeństwa
10. Ilość godzin z przyporządkowaniem do pracowników wykonujących prace
11. Podsumowanie/streszczenie dla kierownictwa

Szczegółowy zakres raportu zostanie ustalony na etapie zlecania prac, powyższe ma charakter zbioru zagadnień do wyboru. Raport należy dostarczyć Zamawiającemu w formie elektronicznej – w formacie .DOC i .PDF., najpóźniej w ostatnim dniu realizacji prac, audytu.

# **Szczegóły dotyczące procesu realizacji usługi w ramach części II.**

## Audyt bezpieczeństwa przetwarzania danych.

Audyt **bezpieczeństwa przetwarzania danych** będzie realizowany zgodnie z wymaganiami wymienionymi w rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności oraz zgodnie z normami: ISO 27001 „Technika informatyczna. Techniki Bezpieczeństwa. systemu zarządzania bezpieczeństwem informacji. Wymagania” i ISO 27002 „Technika informatyczna – Praktyczne zasady zarządzania bezpieczeństwem informacji”.

W audytowanych systemach nie będą przetwarzane dane niejawne w rozumieniu ustawy o ochronie informacji niejawnych z 5 sierpnia 2010 (Dz. U. z 2010 r. nr 182, poz. 1228).

W obszarze zapewnienia bezpieczeństwa przetwarzanych danych oraz ochrony danych, audytowane systemy powinny zagwarantować:

1. poufność – zabezpieczenie danych przed ich udostępnieniem nieuprawnionemu odbiorcy,
2. integralność – zabezpieczenie danych przed modyfikacją lub zniekształceniem przez nieuprawnionych użytkowników,
3. rozliczalność – określenie i weryfikowanie odpowiedzialności za wykorzystanie systemu,
4. autentyczność – weryfikacje tożsamości podmiotów i prawdziwości zasobów,
5. niezawodność – gwarancja oczekiwanego zachowania systemu.

**Audyt obejmuje sprawdzenie aktualnego stanu przetwarzania danych osobowych** zarówno pod kątem zagadnień technicznych, organizacyjnych oraz prawnych ze szczególnym uwzględnieniem wymagań opisanych w ustawie o ochronie danych osobowych.

Zakres audytu:

1. Przegląd i analiza dokumentacji, w tym analiza dokumentacji polityk bezpieczeństwa i procedur, pod kątem zgodności z wymaganiami (w zakresie jak wyżej) Rozporządzenia, ze szczególnym uwzględnieniem zagadnień IT.
2. Weryfikacja zgodności systemów z wymaganiami Rozporządzenia (w zakresie jak wyżej), ze szczególnym uwzględnieniem zagadnień IT.

## *Audyt bezpieczeństwa systemów teleinformatycznych*.

Celem audytów jest wykrycie faktycznych oraz potencjalnych luk i błędów w oprogramowaniu, konfiguracji urządzeń informatycznych, portalach i aplikacjach webowych, które mogą być wykorzystane do naruszenia bezpieczeństwa przetwarzanych informacji, a także bezpieczeństwa Zamawiającego lub użytkowników systemów.

Zakres audytu (założenia ramowe):

1. analiza architektury sieciowej,
	* + weryfikacja sieci LAN na strefy sieciowe (w tym wykorzystanie urządzeń typu firewall oraz VLAN),
		+ określenie usług działających w wybranych podsieciach (do 10 podsieci – nie więcej niż 15 hostów dla jednego systemu),
		+ poszukiwanie podatności w wybranych podsieciach (do 10 podsieci – nie więcej niż 15 hostów dla jednego systemu),
		+ weryfikacja mechanizmów ochronnych w warstwie 2 i 3 modelu OSI,
		+ weryfikacja dostępu do Internetu z LAN,
		+ szczegółowa analiza komunikacji sieciowej,
		+ weryfikacja zasad utrzymania sieci,
		+ analiza wersji oprogramowania pod kątem znanych podatności (firmware),
		+ analiza konfiguracji dostępu do urządzenia,
		+ przegląd konfiguracji dot. użytkowników korzystających z urządzenia, praw dostępu, list dostępów, testy słabych haseł,
		+ analiza konfiguracji i reguł VPN,
		+ analiza wykorzystanych mechanizmów kryptograficznych,
		+ analiza zasad filtracji ruchu sieciowego,
		+ analiza pod kątem obecności niepożądanych usług,
		+ analiza mechanizmów logowania zdarzeń
2. analiza brzegu sieci
	* + weryfikacja topologii/architektury sieci,
		+ testy szczelności systemów klasy firewall (w tym działania funkcji IPS obsługującej w czasie rzeczywistym zagrożenia typu nadużycie protokołu, próby tunelowania, oprogramowania typu exploit, kontrola aplikacji, ataki ogólnego typu bez predefiniowanych sygnatur, ruchu generowanego przez szkodliwe oprogramowanie, podatności serwera i klienta wraz z możliwością definiowania własnych sygnatur, regularności aktualizacji firewall w celu przeciwdziałania nowym zagrożeniom, itp.)
		+ ogólna analiza komunikacji sieciowej z poziomu sieci Internet,
		+ skanowanie portów różnymi technikami, w celu wykrycia potencjalnych luk bezpieczeństwa w udostępnianych usługach,
		+ wykrywanie usług sieciowych udostępnionych w sieci Internet,
		+ próba detekcji wersji oraz typu oprogramowania systemowego zainstalowanego na urządzeniach dostępnych z sieci Internet,
		+ testowanie odporności usług wystawionych do sieci Internet na ataki „Denial of Service” co najmniej 2 metodami zaproponowanymi przez Wykonawcę,
		+ testowanie odporności usług wystawionych do sieci Internet, za pomocą narzędzi eksploatujących typowe luki bezpieczeństwa.
3. analiza bezpieczeństwa konfiguracji systemów informatycznych (urządzeń i aplikacji)
	* + analiza zgodności konfiguracji i sposobu funkcjonowania urządzeń:
	* weryfikacja udostępnionych usług sieciowych,
	* weryfikacja zbędnych usług wraz ze wskazaniem ich podatności,
	* weryfikacja zaimplementowanych systemów aktualizacji,
	* weryfikacja zaimplementowanych systemów logowania zdarzeń,
	* weryfikacja mechanizmów administracji zdalnej,
	* weryfikacja przypisania użytkowników do właściwych grup,
	* weryfikacja uprawnień zgodnie z pryncypium jak najmniejszych uprawnień (ang. „least privilige”),
	* przeprowadzenie prób obejścia uprawnień i uzyskania nieautoryzowanego dostępu do informacji,
	* weryfikacja sposobu udostępniania baz danych na poziomie sieciowym,
	* analiza implementacji podstawowych zasad hardeningowych bazy danych (np. wyłączenie nieużywanych usług, wyłączenie nieużywanych metod dostępu, konfiguracja uprawnień do obiektów, logowanie zdarzeń, składowanie logów, monitorowanie dostępu do obiektów, monitorowanie instrukcji języka SQL),
	* analiza architektury baz danych (np. wykorzystanie mechanizmów autoryzacji oraz uwierzytelniania, segmentacja uprawnień, wykorzystywanie widoków, wykorzystywanie procedur składowych, przechowywanie oraz dostęp do danych wrażliwych, przechowywanie oraz dostęp do danych audytowych, szyfrowanie danych),
	* analiza komunikacji z klientami bazodanowymi (mechanizmy kryptograficzne, transfery danych).
		+ analiza podatności aplikacji
	* wytypowanie wrażliwych punktów w aplikacji,
	* inspekcja mechanizmów uwierzytelniania / autoryzacji,
	* zabezpieczenia interfejsu użytkownika przy wykorzystaniu mechanizmów uwierzytelniania (w tym: login.gov.pl oraz narzędzi two-factor authentication - 2FA).
	* weryfikacja implementacji mechanizmów ochronnych dla serwerów aplikacyjnych,
	* weryfikacja obsługi błędów,
	* analiza poziomu bezpieczeństwa oferowanego przez aplikacje,
4. przeprowadzenie testów penetracyjnych i symulowanych ataków (wg najnowszych wytycznych OWASP wymienionych na liście TOP10 aktualnej na dzień realizacji audytu) obejmujących:
	* + testy bezpieczeństwa aplikacji pod kątem, m.in.:
	* ataków semantycznych na adres URL,
	* ataków związanych z ładowaniem plików,
	* ataków typu Cross-Site Scripting,
	* ataków typu Cross-Site Request Forgery,
	* ataków typu MITM (Man in the Middle),
	* ataków typu Cross Site Tracing,
	* ataków typu Session Hijacking / Session Fixation,
	* ataków typu Forced Browsing,
	* ujawnienia kodu/ścieżki dostępu (Path Disclousure),
	* ujawnienia parametrów ograniczających (Parameter Delimiter)
	* podrabiania zarządzania formularza,
	* sfałszowania żądania http,
	* ujawnienia danych przechowywanych w bazie,
	* trawersowania katalogów (Path Traversal),
	* ujawniania kodu źródłowego,
	* przepełnienia bufora lub stosu,
	* wstrzykiwania kodu wykonywalnego innych języków programowania (np. SQL Injection / JSON Injection),
	* niepożądanego przekierowania,
		+ badanie enumeracji i wykorzystania znanych podatności w celu uzyskania nieautoryzowanego dostępu,
		+ badanie możliwości podszywania się pod użytkowników i uzyskania nieautoryzowanego dostępu do systemu
		+ badanie możliwości podszywania się pod użytkowników uprzywilejowanych i uzyskanie dostępu do systemu
		+ badanie możliwości blokowania/umożliwienia dostępu do systemu wszystkim lub wybranym jej użytkownikom,
		+ badanie możliwości modyfikacji/usunięcia danych z systemu.

## *Audyt funkcjonowania systemów bezpieczeństwa*.

Audyt obejmuje analizę i ocenę funkcjonowania następujących systemów bezpieczeństwa:

1. System antywirusowy.
2. System antyspamowy.
3. System DLP (Data Leak Prevention/Data Loss Prevention).
4. System Firewall.
5. System backupowy wraz z testem odtworzenia systemu z backupu (Zamawiający nie wymaga odtwarzania systemu na zasobach Wykonawcy), ocena lokalizacji baz danych zawierających kopie bezpieczeństwa (bezpieczeństwo ośrodka, ośrodek zapasowy).
6. System zasilania awaryjnego.

Zakres prac:

1. Kompleksowa analiza skuteczności działania.
2. Analiza procedur utrzymaniowych i monitorowania systemów bezpieczeństwa.
3. Weryfikacja poprawności konfiguracji systemów bezpieczeństwa.
4. Weryfikacja i/lub opracowanie wskaźników efektywności.

## Raporty

W wyniku przeprowadzonych prac Wykonawca dostarczy raporty (na zasadach określonych dla każdego etapu) zawierające przykładowo:

1. opis przeprowadzonych działań (w tym weryfikacja dokumentacji i wykonanych testów)
2. opis ryzyka dla danego systemu informatycznego
3. propozycja uruchomienia dodatkowych mechanizmów bezpieczeństwa umożliwiających ochronę przed możliwymi atakami sieciowymi i aplikacyjnymi
4. wyniki działań, testów i ich interpretacja, w szczególności:
	* + informacje dotyczące ogólnej oceny poziomu bezpieczeństwa oraz odporności na ataki badanych systemów zawierające podsumowanie ilości stwierdzonych nieprawidłowości w podziale na systemy i krytyczności,
		+ opis lokalizacji wykrytych podatności - sposobu, w jaki można zlokalizować i powtórzyć testowy atak na podatność,
		+ Informacje na temat poziomu ochrony realizowanego przez system zabezpieczeń
5. opis podatności znalezionych w obu obszarach wraz z zaleceniami i rekomendacjami mającymi na celu zminimalizowanie bądź całkowitą redukcję ryzyka związanego z wykrytymi podatnościami
6. identyfikacja tzw. wąskich gardeł
7. wnioski z audytu, działań (określenie ilościowego i jakościowego poziomu niebezpieczeństwa podatności)
8. rekomendacje i zalecenia pozwalające na usunięcie wykrytych słabości, a tym samym podniesienie poziomu bezpieczeństwa badanych systemów (określenia sposobu naprawy wykrytych podatności w tym zmian konfiguracyjnych)
9. rekomendacje w zakresie rozbudowy systemu informatycznego w celu podniesienia bezpieczeństwa
10. ilość godzin z przyporządkowaniem do pracowników wykonujących prace
11. podsumowanie/streszczenie dla kierownictwa.

Szczegółowy zakres raportu zostanie ustalony na etapie zlecania prac, powyższe ma charakter zbioru zagadnień do wyboru. Raport należy dostarczyć Zamawiającemu w formie elektronicznej – w formacie .DOC i .PDF., najpóźniej w ostatnim dniu realizacji prac, audytu.

# **Harmonogram prac.**

Zamówienie z każdej części zostanie podzielone na etapy (3 etapy dla cz. I litery a-c; 2 etapy dla cz. II lit. a i b). Każdy etap realizacji zakończy się sporządzeniem raportu.

Przewiduje się ramowy harmonogram prac audytowych, przy czym ze względu na postęp prac w ramach poszczególnych projektów zaproponowany harmonogram może ulegać zmianom na etapie realizacji umowy.

**Część I zamówienia:**

1. Centralna Ewidencja i Informacja o Działalności Gospodarczej (CEIDG), wraz z Hurtownią Danych (HD) - rozpoczęcie **3-4Q.2023 r.**
2. Punktu Informacji dla Przedsiębiorcy funkcjonujący w domenie \*.biznes.gov.pl (PIP) rozpoczęcie **3-4Q.2023 r.**
3. System Tracker 2.0 i eUsługi Licencjonowania i ewidencjonowania obrotu towarami wrażliwymi na biznes.gov.pl – rozpoczęcie **3-4Q.2023 r.**

**Część II zamówienia:**

1. Systemy informatyczne platformy PEF udostępnianych przez Brokerów PEF – rozpoczęcie **3-4 Q.2023 r**.
2. System informatyczny Książki Adresowej PEF oraz Portalu PEF **–** rozpoczęcie **3-4 Q.2023 r.**

##

## *Zlecanie prac w przypadku audytów/testów wydajności*

1. Przed rozpoczęciem danego etapu Zamawiający wystawi **Zlecenie na wykonanie audytu/testów wydajności~~.~~** Zlecenie będzie zawierać m. in. proponowaną datę rozpoczęcia i zakończenia czynności oraz obszar podlegający audytowi/testom.
2. Wykonawca uwzględniając wymagania oraz informacje zawarte w zleceniu, w terminie 14 dni liczonych od dnia otrzymania zlecenia, przedstawi Zamawiającemu szczegółową propozycję **Planu audytu/testów wydajności**, wraz ze wskazaniem:
	* + pracochłonności - z podaniem pracownika, prac które ma wykonać i z przeliczeniem na roboczogodziny
		+ osoby odpowiedzialnej za realizację zlecenia.
3. Zamawiający po otrzymaniu propozycji planu, w terminie 7 dni liczonych od dnia jej otrzymania, przedstawi Wykonawcy ewentualne uwagi do planu, bądź dokona jego zatwierdzenia.
4. W przypadku zgłoszenia uwag, zamawiający wskaże termin (nie krótszy, niż 3 dni robocze) przedstawienia przez Wykonawcę poprawionego planu. Do ponownej akceptacji planu stosuje się odpowiednio zapisy lit c-d.
5. Zatwierdzenia Planu audytu/testów wydajności dokona upoważniony pracownik Zamawiającego, w formie gwarantującej ślad rewizyjny, np. informując Wykonawcę o zatwierdzeniu planu poprzez e-mail.
6. Wykonawca przystąpi do wykonywania audytu/testów nie wcześniej niż w dniu zatwierdzenia planu.
7. Czynności audytowe/testowe dla danego etapu nie mogą trwać dłużej niż 21 dni. Termin może ulec wydłużeniu po uprzednim uzyskaniu zgody Zamawiającego.
8. Wykonawca sporządzi **Raport z audytu/testów wydajności** w terminie nie dłuższym niż 7 dni liczonych od dnia zakończenia czynności audytowych/testowych.
9. Wykonawca podczas trwania **audytu/testów wydajności** przedstawia zamawiającemu **raport z cotygodniowych prac**
10. Zamawiający po otrzymaniu **Raportu z audytu/testów wydajności**, w terminie 7 dni liczonych od dnia jego otrzymania, przedstawi Wykonawcy ewentualne uwagi do raportu, bądź dokona jego zatwierdzenia.
11. Zatwierdzenie raportu bez uwag oznacza odbiór danego procesu audytowego.

## *Zlecanie prac w przypadku wsparcia inżyniera bezpieczeństwa IT.*

* 1. Zamawiający wystawi **Zlecenie na wsparcie eksperckie**, które będzie zawierać m. in. proponowaną datę rozpoczęcia i zakończenia prac oraz zakres prac.
	2. Wykonawca uwzględniając wymagania oraz informacje zawarte w zleceniu w terminie 7 dni liczonych od daty otrzymania zlecenia przedstawi Zamawiającemu **Propozycję realizacji zlecenia** wraz ze wskazaniem pracochłonności (wyrażonej w roboczogodzinach) potrzebnej na jego wykonanie.
	3. Zamawiający po otrzymaniu propozycji, w terminie 7 dni kalendarzowych liczonych od dnia jej otrzymania, przedstawi Wykonawcy ewentualne uwagi do propozycji, bądź dokona jej zatwierdzenia.
	4. Zatwierdzenie propozycji dokona upoważniony pracownik Wykonawcy, w formie gwarantującej ślad rewizyjny, np. informując Wykonawcę o zatwierdzeniu prac poprzez e-mail.
	5. Wykonawca przystąpi do wykonania prac na podstawie propozycji zatwierdzonej przez Zamawiającego.
	6. Wykonawca podczas realizacji zlecenia przedstawia zamawiającemu **raport z cotygodniowych prac**
	7. Najpóźniej w ostatnim dniu realizacji danego zlecenia Wykonawca przedstawi **Zamawiającemu** **Raport z wykonanego zlecenia**.
	8. Zamawiający w terminie 7 dni liczonych od dnia otrzymania raportu, przedstawi Wykonawcy ewentualne uwagi do wykonanych prac, bądź dokona zatwierdzenia raportu.
	9. W przypadku zgłoszenia uwag do zlecenia, zamawiający wskaże termin (nie krótszy, niż 3 dni robocze) na prawidłowe wykonanie zlecenia.
	10. Do ponownej akceptacji prac stosuje się odpowiednio zapisy lit. h-i.
	11. Zamawiający będzie realizował płatności w cyklach miesięcznych za odebrane w danym miesiącu prace.
	12. Podstawą płatności będą zatwierdzone Raporty z wykonania zleceń za dany miesiąc.

# **Wymagania dotyczące współpracy Zamawiającego z Wykonawcą**

Zamawiający dopuszcza możliwość przeprowadzenia prac audytowych w formie zdalnej. W przypadku konieczności przeprowadzenia audytu stacjonarnego, jego zakres zostanie ustalony z Zamawiającym na etapie realizacji audytu. W takim przypadku Wykonawca uzyska dostęp do infrastruktury w zakresie ustalonym z Zamawiającym.

Serwerownie znajdują się w okolicach Warszawy, Lublina, Katowic lub innych miejscowości na terenie Polski – Wykonawca musi uwzględniać możliwość wykonywania podróży służbowych w celu realizacji audytu stacjonarnego, w ramach wynagrodzenia, które otrzyma.

Zamawiający nie dopuszcza możliwości włączenia maszyny Wykonawcy do sieci w audytowanej infrastrukturze.

W ramach współpracy Wykonawca i Zamawiający wyznaczają w swoich strukturach osobę prowadzącą zlecenie oraz osobę zastępującą. Wykonawca zobowiązany jest do sprawnej i terminowej realizacji zamówienia oraz stałej współpracy z Zamawiającym, w tym:

* + pozostawania w stałym kontakcie (kontakt telefoniczny oraz drogą elektroniczną; spotkania z Zamawiającym w miarę potrzeb; wyznaczenie osoby do kontaktów roboczych);
	+ informowania o stanie prac, pojawiających się problemach i innych zagadnieniach istotnych dla realizacji badania.

# Załączniki:

Załączniki mogą zostać udostępnione do wglądu w siedzibie Zamawiającego po uprzednim złożeniu oświadczenia o poufności.

Nr 1 – szczegółowy opis systemu

Nr2 – specyfikacja sprzętowa oraz katalog technologii wykorzystywanych do utrzymywania systemu \*.biznes.gov.pl

Nr 3 - Specyfikacja sprzętowa oraz katalog technologii wykorzystywanych do utrzymywania systemu Tracker 2.0