DEPARTAMENT INFORMATYZACJI **I REJESTRÓW SĄDOWYCH**	Warszawa, dnia ……..
Numer sprawy:	
Opis Przedmiotu Zamówienia	

Załącznik nr 1 do Umowy nr …….. z dnia ……..

Spis treści

„Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Społecznego Program Operacyjny Wiedza Edukacja Rozwój”

1. Wstęp

Audyt bezpieczeństwa systemu IT ma określić poziom zabezpieczeń systemu teleinformatycznego elektroniczny Krajowy Rejestr Sądowy (zwany dalej eKRS), wskazanie punktów mogących mieć wpływ na obniżenie tego poziomu oraz zaproponowanie rozwiązań, które doprowadzą środowisko do akceptowalnego przez Zamawiającego poziomu bezpieczeństwa poprzez przeprowadzenie badań i analiz umożliwiających wskazanie zagrożeń wynikających:

- z cech zaprojektowanej topologii i zasad współpracy systemów,
- z zastosowanych technologii i standardów zabezpieczeń,
- z jakości implementacji systemów,
- z architektury styków międzysieciowych,
- ze 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 lub podmiot zależny od Dostawcy Systemu.

2. Opis systemu eKRS

W celu zobrazowania specyfiki oraz złożoności Systemu eKRS zamieszczono poniżej podstawowy opis architektury oraz usług realizowanych przez system eKRS, na który składają się:

1) **warstwa prezentacji Web**

   Portal jako interfejs użytkownika jest prezentowany z poziomu okna przeglądarki internetowej. Wstępna klasyfikacja modułów prezentacyjnych zakłada wizualizację danych dla: publiczności, zarejestrowanych użytkowników, formularzy i pism, procesów biznesowych, użytkowników wewnętrznych, sprawozdań i statystyk.

   Wybrane dane z systemu eKRS udostępniane są również poprzez portal e-Justice wystawiony i utrzymywany przez Komisję Europejską pod adresem *https://e-justice.europa.eu/content_find_a_company-489-pl.do*

2) **warstwa aplikacji i logiki biznesowej**

   W celu usprawnienia postępowań rejestrowych, ułatwienia dostępu do informacji o tych postępowaniach, usprawnienia komunikacji pomiędzy organami tych postępowań i ich uczestnikami oraz obniżenia kosztów postępowań związanych z obowiązkiem dokonywania ogłoszeń, modernizowany jest system teleinformatyczny eKRS, który udostępniany i administrowany przez Ministra Sprawiedliwości pełni następujące funkcje:

   - funkcję rejestru,
   - funkcję wspierającą postępowania rejestrowe,
   - funkcję informacyjną,
   - funkcję komunikacyjną (doręczania pism i innych dokumentów),

„Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Społecznego Program Operacyjny Wiedza Edukacja Rozwój”

- funkcję portalu orzeczniczego;

W tej warstwie dostępne są następujące aplikacje:

- SOW KRS – System Obsługi Wydziałów Krajowego Rejestru Sądowego – aplikacja przeznaczona dla pracowników sądów rejestrowych do obsługi wniosków (elektronicznych i papierowych) i dokonywania wpisów do Krajowego Rejestru Sądowego (rejestr publiczny),
- Tożsamość Cyfrowa – zapewnia obsługę uwierzytelniania użytkownika,
- Formularze elektroniczne KRS – umożliwia wypełnienie wniosków elektronicznych dla wszystkich form prawnych wpisywanych do KRS,
- Przeglądarka Repozytorium Akt Rejestrowych,
- Wyszukiwarka i przeglądarka Monitora Sądowego i Gospodarczego,
- S24 – rejestracja sp. z o.o. jawnej i komandytowej z wykorzystaniem wzorca udostępnionego w systemie – rozszerza funkcjonalność wniosków elektronicznych o możliwość rejestracji tych trzech podmiotów z wykorzystaniem wzorca umowy udostępnionego w systemie.
- RDF - Repozytorium Dokumentów Finansowych - Składanie sprawozdań finansowych i przeglądanie sprawozdań finansowych,
- Wyszukiwarka podmiotów w KRS i pobieranie bezpłatnie odpisów pełnych i aktualnych z KRS,
- Szyna usług FuseESB m.in. z usługami dla systemu BRIS (integracja rejestrów europejskich umożliwiająca wymianę komunikatów KRS z innymi rejestrami poprzez Centralną Platformę Europejską (ECP)) i Jednego Okienka - integracja KRS z GUS (REGON) i CRPKEP (NIP),
- ZSRK – Zintegrowany System Finansowo Księgowy resortu sprawiedliwości jako element wykorzystywany przez moduł Tożsamość Cyfrowa,
- ePłatności – system płatności elektronicznych resortu sprawiedliwości,

3) **warstwa bazodanowa oraz raportowanie**

Wykorzystanymi bazami danych dla aplikacji serwerowych są IBM DB2 oraz MS SQL.

W tej warstwie dostępne są następujące bazy danych:

- RAR – Repozytorium Akt Rejestrowych – metadane dokumentów przetwarzanych w sądzie rejestrowym,
- RDF – Repozytorium Dokumentów Finansowych – baza danych sprawozdań finansowych składanych bezpłatnie przez przedsiębiorców poza sądem rejestrowym,
- CZD – Centralny Zbiór Dokumentów – wybrane dokumenty podmiotów wpisywanych do KRS, które są udostępniane min. na portalu e-Justice przy prezentacji danych podmiotu,
- CRD – Centralny Rejestr Dokumentów – oryginalne wersje dokumentów (archiwum),
- CBD KRS – Centralna Baza Danych Krajowego Rejestru Sądowego.

4) **infrastruktura serwerowa**

„Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Społecznego Program Operacyjny Wiedza Edukacja Rozwój”

System eKRS jako warstwę systemu operacyjnego dla Aplikacji GUI oraz serwerowych wykorzystuje Red Hat Enterprise Server. Raportowanie wykorzystuje Windows Serwer.

5) **Aktualnie system eKRS wykorzystuje następujące technologie i narzędzia:**
   a) technologie i biblioteki aplikacyjne - warstwa prezentacji:
      - Glassfish,
      - WildFly,
      - Liferay,
      - Usługa katalogowa: Microsoft AD,

   b) technologie i biblioteki aplikacyjne - warstwa aplikacji, logiki biznesowej, raportowania:
      - IBM Webshpere
      - Apache Tomcat
      - Języki programowania: OpenJDK,
      - Balansowanie ruchu jest realizowane poprzez urządzenie F5,
      - Usługa katalogowa: Microsoft AD,
      - Serwer kolejek: IBM WebsphereMQ

   c) systemy operacyjne oraz platformy wizualizacyjne:
      - Microsoft Windows Server,
      - RedHat Enterprise Server Linux,
      - Red Hat JBoss EAP, Red Hat JBoss Fuse ESB
      - Vmware.

Zamawiający zakłada realizację prac z jednego fizycznego miejsca. Wymóg analizy architektury i konfiguracji sieci dotyczy tylko fragmentu infrastruktury związanego z systemem eKRS 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 mają obejmować również kanał komunikacyjny pomiędzy systemem eKRS a systemami zewnętrznymi podlegającymi integracji z eKRS m.in.:

- Węzeł Krajowy – do uwierzytelniania użytkownika
- PESEL – do uwierzytelniania użytkownika
- RPA - Rejestr ewidencji profesji prawniczych (np. radcy prawni, adwokaci)
- ECP – Centralna Platforma Europejska (BRIS) – przechowuje i aktualizuje na bieżąco dane podstawowe podmiotów objętych BRIS w bazie danych w ECP (około 20 mln podmiotów ze wszystkich państw członkowskich) oraz przekazuje komunikaty pomiędzy handlowymi rejestrami europejskimi,
- Portal e-Justice – portal Komisji Europejskiej umożliwiający wyszukiwanie podmiotów we wszystkich handlowych rejestrach europejskich i udostępnianie dokumentów dotyczących podmiotu. Wyszukiwanie i prezentacja danych dostępne są we wszystkich językach narodowych państw członkowskich UE,
- REGON (GUS) – wpisuje lub aktualizuje w KRS nr REGON podmiotu

„Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Społecznego Program Operacyjny Wiedza Edukacja Rozwój”

- NIP (CRPKEP) – wpisuje lub aktualizuje w KRS nr NIP
- TERYT (GUS) – wspiera wpisywanie danych adresowych,
- CREWAN (Centralne Repozytorium Elektronicznych Wypisów Aktów Notarialnych) – udostępnia sądom rejestrowym wypisy elektroniczne aktów notarialnych przy rejestracji podmiotów drogą elektroniczną,
- Podpisy elektroniczne (kwalifikowany, Profil Zaufany, osobisty)
- Krajowy Rejestr Zadłużonych (KRZ) – weryfikacja osób w KRZ przed wpisem do KRS,
- Elektroniczne Potwierdzenie Odbioru (EPO),
- Centralny Wydruk (CW).

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

Szczegółowy opis oraz wymagania zostały przedstawione w dokumentach zamieszczonych na Portalu eZamówienia MS, numer postępowania: BF- …… (dostępne pod adresem https://ezamowienia.ms.gov.pl/czs/public/postepowanie?postepowanie=), w szczególności: Załącznik nr 1 do umowy - Opis Przedmiotu Zamówienia.

3. Cele audytowe

System informatyczny zawiera wiele różnego rodzaju zabezpieczeń technicznych. Audyt bezpieczeństwa powinien obejmować swoim zasięgiem wszystkie te zabezpieczenia. Techniczne środki ochrony systemu informatycznego można podzielić na następujące kategorie:

- zabezpieczenia aplikacji (np. kontrola dostępu do operacji, szyfrowanie danych aplikacji),
- 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).

Przedmiotem zamówienia jest przeprowadzenie audytu bezpieczeństwa i wydajności, dostępności oraz jakości kodu oprogramowania systemu eKRS, a także wskazanie punktów obniżających ten poziom oraz zaproponowanie rozwiązań, które doprowadzą środowisko do akceptowalnego przez Zamawiającego poziomu bezpieczeństwa oraz audytu zgodności z wytycznymi WCAG 2.1. Audyt systemu eKRS 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 eKRS,
4) audyt zgodności z wytycznymi WCAG 2.1.

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

1) **Analizę architektury i konfiguracji systemu eKRS, w tym szyny komunikacyjnej, w szczególności:**
   a) mechanizmów autoryzacji i uwierzytelniania,
   b) mechanizmów kontroli dostępu,

„Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Społecznego Program Operacyjny Wiedza Edukacja Rozwój"

c) mechanizmów kryptograficznych,
d) mechanizmów bezpieczeństwa komunikacji,
e) mechanizmów logowania i obsługi błędów i zdarzeń,
f) mechanizmów ochrony danych,
g) mechanizmów odpowiedzianych za wysoką dostępność i niezawodność,
h) mechanizmów administracji zdalnej z poziomu aplikacji,
i) zaimplementowanych systemów aktualizacji aplikacji,
j) zaimplementowanych mechanizmów backupu i odtwarzania aplikacji;

2) Analizę architektury i konfiguracji systemów zarządzania bazami danych i baz danych eKRS, w szczególności:

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 kryptograficznych, w tym szyfrowania danych,
i) mechanizmów ochrony danych,
j) zarządzania uprawnieniami,
k) metod dostępu do danych i ich transmisji,
l) mechanizmów odpowiedzianych za wysoką dostępność i niezawodność,
m) mechanizmów administracji zdalnej bazami danych,
n) zaimplementowanych systemów aktualizacji baz danych,
o) zaimplementowanych mechanizmów backupu i odtwarzania systemów zarządzania bazami danych i baz danych,
p) komunikacji z klientami bazodanowymi (m.in. protokoły, mechanizmy kryptograficzne, transfery danych, pule połączeń).
q) 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 eKRS, w szczególności:

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 privilige”),
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,

„Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Społecznego Program Operacyjny Wiedza Edukacja Rozwój”

h) monitorowania i rejestrowania dostępu do obiektów systemu,
i) przechowywania oraz dostępu do danych audytowych,
j) mechanizmów kryptograficznych, w tym szyfrowania danych,
k) mechanizmów ochrony danych,
l) mechanizmów odpowiedzianych za wysoką dostępność i niezawodność,
m) mechanizmów administracji zdalnej,
n) zaimplementowanych systemów aktualizacji,
o) zaimplementowanych mechanizmów backupu i odtwarzania,
p) 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 eKRS, w szczególności:
a) podziału na VLAN-y,
b) zastosowanych mechanizmów ochrony danych,
c) urządzeń sieciowych,
d) urządzeń bezpieczeństwa,
e) dostępu do Internetu,
f) mechanizmów odpowiedzianych za wysoką dostępność i niezawodność;

oraz wytworzenie opisu technicznego do raportu zawierającego wykryte nieprawidłowości w architekturze systemu i konfiguracji poszczególnych komponentów, ich wpływ na aplikacje i systemy, zalecenia i instrukcje do wprowadzenia korekt architektonicznych i konfiguracyjnych właściwych dla zapewnienia bezpieczeństwa systemu eKRS.

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 eKRS 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),

<u>W zakresie prowadzenia testów penetracyjnych Zamawiający zakłada, że Wykonawca przeprowadzi:</u>

1) Enumerację sieci wewnętrznej systemu eKRS, w szczególności:
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,

„Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Społecznego Program Operacyjny Wiedza Edukacja Rozwój”

- analiza ścieżki/ścieżek przeprowadzenia potencjalnego ataku;

2) Analizę właściwą podatności, w szczególności:
   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 (bezautoryzacyjna 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 eKRS, w szczególności:
   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 i wykorzystania znanych podatności w celu uzyskania nieautoryzowanego dostępu,

„Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Społecznego Program Operacyjny Wiedza Edukacja Rozwój”

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

5) Wychwytywanie słabych punktów konfiguracji, w szczególności:
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 zawierającego 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 eKRS.

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,
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 przejrzystość kodu,
14) weryfikację jakości udokumentowania kodu,
15) weryfikację komplementarności kodu w repozytorium,

„Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Społecznego Program Operacyjny Wiedza Edukacja Rozwój”

16) weryfikację jakości testów (dla testów wykonywanych w zautomatyzowany sposób),
17) weryfikację zastosowania dobrych praktyk zalecanych przez producentów technologii, w których aplikacja została wytworzona,
18) weryfikację zastosowania wytycznych właściwych dla zastosowanej technologii,
19) weryfikację konsekwencji w stosowaniu standardów, konwencji, itp.
20) weryfikację stosowania wzorców projektowych,
21) weryfikację stosowania właściwych podziałów na warstwy i komponenty z zachowaniem zasad rozłącznego i osobliwego zastosowania (Separation of Concerns),
22) analizę użytych funkcji lub komponentów pod kątem elementów przestarzałych („deprecated") lub elementów posiadających znane luki bezpieczeństwa lub podatności,
23) weryfikację dokumentowania autorskiego kodu aplikacji, w sposób umożliwiający automatyczne wygenerowanie dokumentacji API.

Ad 4) Audyt zgodności z wytycznymi WCAG 2.1.

Wykonawca po wykonaniu prac wchodzących w skład jednostkowych audytów, przedstawi Zamawiającemu Raport, osobno dla każdego z wykonanych jednostkowych Audytów, zawierający pełną analizę rezultatów wykonanych weryfikacji wraz ze wskazówkami i instrukcjami dotyczącymi wyeliminowania lub ograniczenia dostrzeżonych słabości kodu lub nieprawidłowości, a także przedstawi ze swojej perspektywy prognozę dalszego jego utrzymywania i rozwijania.

4. Metodyka prowadzenia testów

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 inny równoważny (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 informację 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 innych równoważnych (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

„Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Społecznego Program Operacyjny Wiedza Edukacja Rozwój"

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 inne równoważne (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.

5. Raportowanie

Raport musi być sporządzony w języku polskim, dostarczany w formie papierowej i elektronicznej (plik: *.DOC/DOCX z możliwością edycji i *.PDF), będzie zawierał co najmniej:

1) streszczenie raportu dla kadry zarządzającej,
2) opis przeprowadzonych działań (w tym weryfikacji dokumentacji, komponentów systemu eKRS i wykonanych testów),
3) przyjęty model klasyfikacji ryzyka,
4) klasyfikację ryzyka dla wykrytych podatności,
5) wyniki analizy, testów i ich interpretację, w szczególności:
   a) informacje dotyczące ogólnej oceny poziomu bezpieczeństwa oraz odporności na ataki systemu eKRS i jego środowiska infrastrukturalnego zawierające podsumowanie ilości stwierdzonych nieprawidłowości w podziale na system eKRS i jego środowisko infrastrukturalne oraz ich krytyczności, w postaci raportu dla kierownictwa Zamawiającego,
   b) 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,
   c) informacje na temat poziomu i jakości zabezpieczeń realizowanych przez system eKRS,
   d) wnioski z audytu (określenie ilościowego i jakościowego poziomu niebezpieczeństwa podatności),
   e) rekomendacje i zalecenia pozwalające na usunięcie wykrytych słabości, a tym samym podniesienie poziomu bezpieczeństwa systemu eKRS i jego środowiska infrastrukturalnego (określenia sposobu naprawy wykrytych podatności, w tym zmian konfiguracyjnych).

„Projekt współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Społecznego Program Operacyjny Wiedza Edukacja Rozwój”