Załącznik nr 1 do umowy

(2.1) AKTUALIZACJA SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI (SZBI) WRAZ Z AKTUALIZACJĄ POLITYKI ZARZĄDZANIA RYZYKIEM I SZANSAMI ORAZ PRZEPROWADZENIE SZKOLENIA DLA PRACOWNIKÓW

Opis przedmiotu zamówienia (OPZ)

Przedmiotem zamówienia jest aktualizacja SZBI wraz z aktualizacją Polityki zarządzania ryzykami w Urzędzie Miasta Bełchatowa.
Aktualizacja SZBI w ramach tego zlecenia musi być zrealizowana z uwzględnieniem obowiązujących przepisów prawa oraz dobrych praktyk zawartych w innych dokumentach, w szczególności w poradniku grantu „Cyberbezpieczny Samorząd", w oparciu o przepisy rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (KRI) w szczególności Rozdział 4 oraz ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.
Zamawiający wymaga, aby obecnie funkcjonujący System Zarządzania Bezpieczeństwem (SZBI) Informacji oraz Polityka zarządzania ryzykami i szansami w Urzędzie Miasta Bełchatowa zaktualizowane zostały pod kątem cyberbezpieczeństwa i bezpieczeństwa informacji, mając na uwadze poszczególne polityki, procedury, kompetencje i narzędzia do kontroli dostępu, obsługę incydentów w tym incydentów cyberbezpieczeństwa, polityki zarządzania podatnościami, procedury ciągłości działania Urzędu, opracowanie polityki bezpieczeństwa w relacji z dostawcami usług, stosowanie kryptografii i szyfrowania. W Urzędzie rejestr ryzyk funkcjonuje w ramach Kontroli zarządczej w tym Polityki zarządzania ryzykami i szansami realizowanej w oparciu o funkcjonujący w Urzędzie System Zarządzania Jakością zgodny z normą ISO 9001.
Zamawiający oczekuje analizy obowiązujących w Urzędzie formalnych i nieformalnych procedur i polityk, określenia ich adekwatności i skuteczności oraz wskazania zestawienia brakującej dokumentacji jako podstawy przygotowania do zaktualizowania dokumentacji SZBI i Polityki zarządzania ryzykami.

I. Aktualizacja Polityki zarządzania ryzykiem i szansami

1. Konieczność aktualizacji Polityki zarządzania ryzykami i szansami w Urzędzie wynika z potrzeby systematycznego podejścia do identyfikacji, oceny i zarządzania ryzykiem w obszarze cyberbezpieczeństwa i bezpieczeństwa informacji w odniesieniu do zadań realizowanych przez Urząd. Aktualizacja rejestru ryzyk stanowi kluczowy element w procesie aktualizacji SZBI, co pozwoli na lepsze zrozumienie, monitorowanie i minimalizowanie ryzyk, a także zwiększenie odporności organizacyjnej na incydenty bezpieczeństwa. Aktualizacja ryzyka ma zapewnić spełnianie wymogów Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w

sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych oraz art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.

2. Zamówienie realizowane przez Wykonawcę dotyczy aktualizacji istniejącego w Urzędzie rejestru ryzyk i SZBI **(Zamawiający nie dopuszcza utworzenia procedury zarządzania ryzykiem od podstaw lub na podstawie innego szablonu niż obowiązujący w Urzędzie).** Celem jest zintegrowanie i usprawnienie procesów zarządzania ryzykiem w zakresie cyberbezpieczeństwa i bezpieczeństwa informacji, aktualizacja procedury zarządzania incydentami. Aktualizacja rejestru ryzyk musi być przeprowadzona zgodnie z międzynarodowymi standardami, musi zapewnić spójność z aktualizacją funkcjonującego Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), w oparciu o KRI oraz ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.
3. Wykonawca jest zobowiązany do przeprowadzenia kompleksowej analizy obecnego rejestru ryzyk oraz do jego aktualizacji, uwzględniając cyberbezpieczeństwo i bezpieczeństwo informacji oraz mając na uwadze następujące aspekty:
   1) Wykonawca odpowiada za zapewnienie, że wszyscy użytkownicy rejestru ryzyk zostaną odpowiednio przeszkoleni w zakresie zarządzania ryzykiem oraz w zakresie zaktualizowanego SZBI, w odniesieniu do zaktualizowanego rejestru ryzyk uwzględniającego cyberbezpieczeństwo i bezpieczeństwo informacji.
   2) Wykonawca musi dokonać szczegółowej analizy aktualnego rejestru ryzyk utworzonego i używanego przez Urząd. Analiza ta obejmie przegląd wszystkich oszacowanych / zdefiniowanych ryzyk, ich kategorii, priorytetów oraz sposobów zarządzania nimi. Celem tej analizy jest zrozumienie aktualnego poziomu zarządzania ryzykiem oraz identyfikacja potencjalnych obszarów wymagających usprawnień lub aktualizacji.
   3) Wykonawca musi przeprowadzić proces identyfikacji nowych zagrożeń i ryzyk, które mogły pojawić się od czasu ostatniej aktualizacji rejestru (np. przy zmianie planu pracy (wykreślenie/dodanie zadania). Proces ten musi obejmować analizę zmian w otoczeniu zewnętrznym i wewnętrznym Urzędu, a także uwzględnienie nowych technologii, procesów operacyjnych i zmian w przepisach prawnych, które mogą wpłynąć na poziom ryzyka.
4. Po zidentyfikowaniu ryzyk, Wykonawca musi przeprowadzić ich ocenę. Ocena ta musi obejmować analizę prawdopodobieństwa wystąpienia każdego ryzyka oraz potencjalnych skutków dla Urzędu. Na podstawie tej analizy ryzyka zostaną sklasyfikowane, co umożliwi efektywne zarządzanie ryzykiem.
5. Po aktualizacji rejestru, Wykonawca zaktualizuje procedurę zarządzania ryzykiem uwzględniając międzynarodowe standardy w zakresie cyberbezpieczeństwa, jak również normę ISO, na której opiera się obecnie procedura zarządzania ryzykiem. Te muszą obejmować ciągłe doskonalenie metod zarządzania ryzykiem, aby zapewnić ich aktualność i skuteczność.

6. Realizacja zamówienia wymaga zastosowania narzędzi (arkuszy kalkulacyjnych), które wspomogą procesy identyfikacji, analizy oraz zarządzania ryzykiem:
   1) Wykonawca wykorzysta obecnie funkcjonujące w Urzędzie i dostarczy Zamawiającemu arkusze kalkulacyjne do zarządzania ryzykiem, które umożliwią systematyczne śledzenie, analizę ryzyk.
   2) Zamawiający zleca Wykonawcy aktualizację rejestru ryzyk, podzieloną na części, aby zapewnić systematyczne i zgodne z normami podejście do zarządzania ryzykiem. Każda część musi mieć jasno określone cele, zadania i przypisane zasoby. Proces planowania musi obejmować co najmniej części:
      a) Wykonawca musi ustalić zakres zadania i cele.
      b) Wykonawca musi przeprowadzić przegląd i ocenę istniejącego rejestru ryzyk w Urzędzie.
      c) Wykonawca musi przeprowadzić identyfikację ryzyk oraz ich analizę przy użyciu ustalonych z Zamawiającym metod i narzędzi.
      d) Wykonawca musi wprowadzić zmiany do rejestru ryzyk na podstawie wyników analiz.
      e) Wykonawca musi przeprowadzić szkolenia dla pracowników Zamawiającego z zarządzania ryzykami w połączeniu z zaktualizowaną dokumentacją SZBI.
7. Wykonawca musi zrealizować każdą część zadania zgodnie z ustalonym harmonogramem z Zamawiającym, który określi kluczowe daty i terminy, w tym co najmniej:
   1) Datę rozpoczęcia aktualizacji rejestru ryzyk.
   2) Termin, do którego wykonawca musi przeprowadzić pełną analizę obecnych danych.
   3) Termin, do którego wykonawca musi zaktualizować rejestr ryzyk.
   4) Datę formalnego zakończenia aktualizacji, wraz z przekazaniem pełnej dokumentacji i przeprowadzeniem szkoleń.
8. Zakończenie każdej części przez Wykonawcę będzie wymagało spełnienia określonych warunków:
   1) Każda część musi być udokumentowana przez Wykonawcę, włączając w to raporty, analizy i aktualizacje rejestru.
   2) Uprawnieni pracownicy Zamawiającego muszą zaakceptować wyniki każdej części przed przejściem do następnego.
   3) Wszystkie działania Wykonawcy muszą być zgodne z zasadami i wytycznymi międzynarodowych norm w tym normy, na której oparty jest system kontroli zarządczej w Urzędzie.

II. Aktualizacja dokumentacji i procedur Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)

1. Aktualizacja SZBI musi być zrealizowana z uwzględnieniem obowiązujących przepisów prawa oraz dobrych praktyk zawartych w innych dokumentach, w szczególności w poradniku grantu „Cyberbezpieczny Samorząd” oraz KRI.

2. Wykonawca musi zaktualizować SZBI na podstawie funkcjonującej dokumentacji w Urzędzie, w tym procedury i wdrożenie nowych procedur z zakresu cyberbezpieczeństwa i bezpieczeństwa informacji.
3. Wykonawca musi zaplanować system w strukturach Zamawiającego, włączając odpowiednie konfiguracje techniczne i organizacyjne.
4. Względem funkcjonującego SZBI w Urzędzie Wykonawca musi opracować procedury na bazie obecnie obowiązujących w Urzędzie. Struktura dokumentacji powinna być jasna i zrozumiała dla wszystkich użytkowników systemu w Urzędzie. Dokumentacja ma być zaktualizowana poprzez dodanie dodatkowych sekcji i procedur, celem ułatwienia zarządzania systemem i jego przeglądu **(Zamawiający nie dopuszcza utworzenia SZBI od podstaw lub na podstawie innego szablonu niż obowiązuje w Urzędzie).** Format dokumentacji powinien obejmować wersje elektroniczne, zapewniające pełną dostępność i możliwość archiwizacji.
5. Jeżeli Wykonawca uzna, że konieczne jest dołączenie dodatkowych dokumentów lub procedur, może je włączyć w ramach aktualizacji, aby jeszcze lepiej/precyzyjniej dostosować SZBI do potrzeb Urzędu.
6. Dokumenty muszą zawierać kompleksową analizę kontekstu operacyjnego Urzędu, identyfikując wewnętrzne i zewnętrzne czynniki, które mogą wpłynąć na zarządzanie bezpieczeństwem informacji. Dokument musi określać zakres SZBI, obejmujący zidentyfikowane wymagania organizacyjne, prawne i regulacyjne.
7. Celem aktualizacji dokumentu jest dostarczenie kompleksowego przeglądu i wskazówek dotyczących wszystkich aspektów SZBI zaimplementowanego w Urzędzie. Dokument musi zawierać szczegółowy opis SZBI, jego celów, zakresu działania oraz mechanizmów kontroli wdrażanych w celu ochrony danych i informacji przed potencjalnymi zagrożeniami.
8. Wykonawca opracuje i zatwierdzi w porozumieniu z Zamawiającym szczegółowy plan aktualizacji SZBI.
9. Wykonawca musi zidentyfikować i omówić specyficzne cele, które kierownictwo Zamawiającego chce osiągnąć poprzez zaktualizowanie SZBI, w tym związane z tym korzyści organizacyjne i operacyjne. Zadaniem Wykonawcy jest zapewnienie, że cele te są jasno zrozumiałe i że SZBI będzie odpowiednio dostosowany do potrzeb organizacyjnych Zamawiającego.
10. Wykonawca odpowiedzialny jest za organizację sesji informacyjnych i dyskusji z kluczowymi członkami kierownictwa Zamawiającego, aby uzyskać ich opinie, doprecyzować oczekiwania i zbudować silne poparcie dla realizacji zadania. Spotkania te będą miały na celu zapewnienie, że wszystkie strony mają jednolite rozumienie zakresu i oczekiwań dla realizacji zadania.
11. Wykonawca przygotuje (na bazie istniejącego SZBI) formalny dokument SZBI, który zostanie przedłożony do zatwierdzenia przez Zamawiającego. Dokument ten będzie zawierał szczegółowy opis zakresu, cele związane z cyberbezpieczeństwem i bezpieczeństwem informacji, a także zobowiązania organizacji dotyczące przestrzegania wymogów prawnych i regulacyjnych.

12. Wykonawca musi zapewnić, że zakres aktualizacji SZBI jest w pełni zintegrowany z obecnymi procesami funkcjonującymi w Urzędzie oraz infrastrukturą technologiczną Zamawiającego, co umożliwi sprawną implementację i późniejsze funkcjonowanie SZBI.
13. Wykonawca współpracując z Zamawiającym, musi przeprowadzić szczegółową inwentaryzację wszystkich zasobów informacyjnych istotnych dla organizacji oraz musi ocenić potencjalne ryzyka związane z ich bezpieczeństwem.
14. Wykonawca musi wdrożyć wszystkie zaktualizowane i nowe komponenty SZBI, zapewniając ich integrację oraz funkcjonalność.
15. Wykonawca musi opracować i zaimplementować zaktualizowany SZB, który będzie integralnie powiązany z kluczowymi procesami biznesowymi Zamawiającego.
16. Wykonawca musi zapewnić, że wszystkie wymagane dokumenty, takie jak polityki, procedury, instrukcje operacyjne i rejestry ryzyka, będą opracowane.
17. Wykonawca opracuje szablony dokumentów i narzędzia wspomagające, które będą wykorzystywane w codziennej pracy związanej z SZBI, zaktualizuje obecnie funkcjonujące, takie jak formularze do zgłaszania incydentów bezpieczeństwa, checklisty audytowe, narzędzia do monitorowania zgodności, itp.
18. Wykonawca stworzy i zaimplementuje procedury odpowiedzi na incydenty bezpieczeństwa informacji, które określą, jak identyfikować, reagować i zarządzać incydentami.
19. Zamawiający wymaga od Wykonawcy opracowania szczegółowego harmonogramu wdrożenia aktualizacji SZBI.
20. Harmonogram ten musi być zatwierdzony przez Zamawiającego przed rozpoczęciem implementacji.
21. Harmonogram wdrożenia aktualizacji musi zostać przedłożony Zamawiającemu do akceptacji przed rozpoczęciem jakichkolwiek działań. Zatwierdzenie to musi być udokumentowane i może wymagać modyfikacji na żądanie Zamawiającego w celu lepszego dopasowania do warunków operacyjnych Zamawiającego.
22. Wykonawca jest zobowiązany do regularnego przeglądu i aktualizacji harmonogramu w odpowiedzi na zmieniające się otoczenie i zmiany organizacyjne realizacji zadania lub na wniosek Zamawiającego. Wszelkie zmiany w harmonogramie muszą być niezwłocznie komunikowane Zamawiającemu i podlegają jego zatwierdzeniu.
23. Wykonawca jest odpowiedzialny za monitorowanie postępów w realizacji harmonogramu i regularne raportowanie statusu Zamawiającemu. Raporty powinny zawierać szczegółowe informacje o ukończonych, bieżących oraz planowanych działaniach, a także o wszelkich wyzwaniach czy odchyleniach od pierwotnego planu.
24. Wykonawca w uzgodnieniu z Zamawiającym musi przeprowadzić szczegółowy przegląd końcowy zaktualizowanego SZBI, w tym ocenę zgodności z pierwotnie ustalonymi celami i specyfikacjami. Przegląd ten ma na celu upewnienie się, że wszystkie elementy systemu działają prawidłowo i spełniają wymagania bezpieczeństwa.

25. Po pomyślnym zaktualizowaniu SZBI wymagane jest formalne zatwierdzenie dokumentu przez Zamawiającego. To zatwierdzenie będzie dokumentowane w formie formalnego dokumentu przekazania na podstawie protokołu.
26. **Wykonawca przeszkoli pracowników Urzędu** z zaktualizowanego i zatwierdzonego przez Zamawiającego SZBI i z zarządzania ryzykami. Wykonawca jest zobowiązany zapewnić, aby szkolenie pokrywało kluczowe obszary takie jak, procedury operacyjne i reagowania na incydenty, zarządzanie ryzykiem, wdrożone i zaktualizowane polityki a także prawne i regulacyjne aspekty ochrony danych i cyberbezpieczeństwa. Szkolenie powinno również skupić się na umiejętnościach praktycznych, takich jak właściwe postępowanie w przypadku wykrycia zagrożeń dla bezpieczeństwa informacji, cyberzagrożeń oraz na rozwijaniu świadomości i kultury bezpieczeństwa wśród pracowników.
27. Zamawiający podkreśla znaczenie szkolenia jako integralnej części procesu wdrażania zaktualizowanego SZBI oraz Polityki zarządzania ryzykami mającego na celu nie tylko zwiększenie kompetencji pracowników, ale także poprawę ogólnego poziomu bezpieczeństwa informacji w Urzędzie. **Wykonawca musi więc zaprojektować program szkolenia**, który jest interaktywny i dostosowany do różnych poziomów wiedzy uczestników, aby maksymalizować jego efektywność i zapewnić, że wszystkie cele szkoleniowe są osiągane. Materiały te muszą być zaprojektowane w sposób umożliwiający łatwe zrozumienie i przyswajanie wiedzy przez uczestników o różnym poziomie zaawansowania oraz różnych potrzebach. Materiały powinny również zawierać praktyczne wskazówki dotyczące wdrażania polityk i procedur w życie codzienne Urzędu, uwzględniając specyfikę i potrzeby Urzędu oraz promując praktyki zapewniające równość i niedyskryminację.
28. **Wykonawca musi zaprojektować i opracować szczegółowy program szkolenia, który następnie musi zostać przedstawiony Zamawiającemu do zatwierdzenia. Program ten musi być dostosowany do potrzeb Urzędu, zgodnie z wymogami dotyczącymi SZBI oraz procedury zarządzania ryzykiem.**
29. Wykonawca opracuje harmonogram szkolenia, który uwzględni czas trwania szkolenia, daty, czas na pytania i odpowiedzi uczestników szkolenia oraz na interaktywne dyskusje, czas na przerwy, aby umożliwić im wyjaśnienie wszelkich wątpliwości.
30. Po opracowaniu programu szkolenia, Wykonawca przedstawi go Zamawiającemu do akceptacji. Zamawiający przeprowadzi przegląd programu, aby upewnić się, że spełnia on wszystkie wymagane standardy oraz adekwatnie adresuje potrzeby i specyfikę Urzędu, a w razie potrzeby Zamawiający może zaproponować zmiany lub uzupełnienia, które zostaną omówione i wdrożone przez Wykonawcę przed ostatecznym zatwierdzeniem programu.
31. Wykonawca przeprowadzi szkolenie stacjonarnie w siedzibie Zamawiającego, w grupach po maksymalnie **50 osób (kolejno po sobie lub rozłożone w ciągu 14 dni) x 4 godziny zajęć, dzień (jedna/dwie grupy). Jednostką czasową szkolenia jest 1 godzina szkoleniowa = 45 minut, przewiduje się dwie przerwy trwające po 15**

minut w ciągu dnia, przy czym łączna liczba osób do przeszkolenia wynosi **230 (liczba osób może ulec zmianie o +/- 10%).**
W przypadku szkoleń zdalnych grupy mogą być liczniejsze, ale wymaga to dodatkowych ustaleń z Zamawiającym.

32. Zamawiający wymaga, aby treści szkoleniowe były zróżnicowane w zależności od roli uczestników:
    1) **Dla zwykłych użytkowników** – program szkolenia skupi się na podstawowych aspektach SZBI oraz zarządzaniu ryzykami, w tym na zrozumieniu polityk bezpieczeństwa, zasadach postępowania w przypadku zauważenia potencjalnego zagrożenia w wykonywaniu codziennych zadań.
    2) **Dla kadry kierowniczej** – szkolenie będzie zawierało rozszerzone moduły dotyczące zarządzania ryzykiem, strategii odpowiedzi na incydenty bezpieczeństwa oraz zaawansowanych aspektów tworzenia i utrzymania polityk bezpieczeństwa, nadzoru nad bezpieczeństwem informacji.
33. Zamawiający dopuszcza możliwość przeprowadzenia szkolenia w formie zdalnej. Wykonawca jest zobowiązany do zapewnienia odpowiedniego narzędzia do zdalnego połączenia, które umożliwi efektywne i interaktywne przekazywanie wiedzy oraz aktywne uczestnictwo pracowników w szkoleniu. Narzędzie to musi umożliwiać prowadzenie transmisji wideo, współdzielenie ekranu, interaktywne dyskusje w czasie rzeczywistym.

Cześć prac może być wykonana zdalnie. Jednakże Zamawiający oczekuje **minimum pięciu spotkań** w Urzędzie, na których w formie warsztatów zostaną przedstawione propozycje zmian do dokumentacji. Spotkania powinny być zaplanowane na ok **4 godziny** i powinny zawierać krótkie szkolenie przedstawiające omawiany temat z punktu widzenia SZBI oraz warsztaty, na których wspólnie przedstawiciele Urzędu oraz Wykonawca wypracują wnioski do dalszych etapów aktualizacji SZBI i Polityki zarządzania ryzykami.

Wszystkie opracowane polityki, procedury, procesy muszą zostać skutecznie wdrożone w Urzędzie.

(2.2) USŁUGA PRZEPROWADZENIA AUDYTU WDROŻONEGO SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI (AUDYT KRI) I USŁUGA PRZEPROWADZENIA AUDYTU PODATNOŚCI/testów podatności

Opis przedmiotu zamówienia (OPZ)

Przedmiotem zamówienia jest przeprowadzenie audytu wdrożonego Systemu Zarządzania Bezpieczeństwem Informacji w oparciu o przepisy rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (KRI) w szczególności Rozdział 4 oraz ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. **Przeprowadzenie trzech audytów KRI (jeden w roku 2024, drugi w roku 2025, trzeci w roku 2026) i trzech audytów podatności (jeden w roku 2024, drugi w roku 2025, trzeci w roku 2026).** Przygotowany w wyniku audytu raport ma zawierać opis sytuacji aktualnej, dowody potwierdzające zgodność oraz wskazywać obszary, w których nie ma zgodności z wymaganiami oraz zalecenia dotyczące tych obszarów. Zamawiający oczekuje omówienia wyników audytu na spotkaniu z przedstawicielami kierownictwa Urzędu na miejscu u Zamawiającego (wykluczona forma zdalna).

Zamawiający oczekuje, że Wykonawca posiada doświadczenie w realizacji podobnych zadań i może się wykazać odpowiednimi referencjami i certyfikatami.

1) Zamawiający wymaga od Wykonawcy opracowania szczegółowego harmonogramu przeprowadzenia audytów.
2) Harmonogram ten musi być zatwierdzony przez Zamawiającego przed rozpoczęciem audytów.
3) Harmonogram musi zostać przedłożony Zamawiającemu do akceptacji przed rozpoczęciem jakichkolwiek działań. Zatwierdzenie to musi być udokumentowane i może wymagać modyfikacji na żądanie Zamawiającego w celu lepszego dopasowania do warunków operacyjnych Zamawiającego.
4) Wykonawca jest zobowiązany do regularnego przeglądu i aktualizacji harmonogramu w odpowiedzi na zmieniające się otoczenie i zmiany organizacyjne realizacji zadania lub na wniosek Zamawiającego. Wszelkie zmiany w harmonogramie muszą być niezwłocznie komunikowane Zamawiającemu i podlegają jego zatwierdzeniu.
5) Wykonawca jest odpowiedzialny za monitorowanie postępów w realizacji harmonogramu i regularne raportowanie statusu Zamawiającemu. Raporty powinny zawierać szczegółowe informacje o ukończonych, bieżących oraz planowanych działaniach, a także o wszelkich wyzwaniach czy odchyleniach od pierwotnego planu.

Audyt KRI zostanie przeprowadzony w siedzibie Zamawiającego **(nie dopuszcza się realizacji w sposób zdalny).**

Testy zostaną zrealizowane zgodnie z międzynarodową metodologią NIST, PTES, OWASP w aktualnie obowiązującej wersji. Zidentyfikowane ryzyka zostaną sklasyfikowane w oparciu o kryteria Common Vulnerability Scoring System, które umożliwiają precyzyjne, liczbowe opisanie ryzyka zidentyfikowanej podatności. Zamawiający wymaga, aby wszystkie testy podatności były przeprowadzane w sposób ręczny, przy wykorzystaniu automatycznych narzędzi jedynie na tych etapach, gdzie automatyzacja podstawowych prac pozwoli zaoszczędzić czas i przekierować go na działanie z jednoznaczną korzyścią dla Zamawiającego. Przedstawiony raport z przeprowadzonych prac będzie zawierał minimum:

a) Metrykę testu - zawierającą informacje o zespole wykonującym test, dacie testu, dacie sporządzenia raportu.
b) Ujęcie wniosków strategicznych w podsumowaniu zarządczym raportu.
c) Cel i zakres testów.
d) Przyjęcie modelu klasyfikacji ryzyka.
e) Metodologię oraz narzędzia.
f) Szczegółowy opis podatności wraz z rekomendacjami ich usunięcia.

Zamawiający wymaga, aby testy podatności były prowadzone w sposób hybrydowy. Minimum 2 dni robocze w siedzibie Zamawiającego.
Scenariusz zostanie opracowany i przygotowany z uwzględnieniem systemów i usług wykorzystywanych przez zamawiającego i potwierdzony z zespołem IT u Zamawiającego. Zamawiający nie doszcza, aby scenariusz testów był narzucony przez Wykonawcę (z puli odgórnie ustalonych scenariuszy).
Działania zostaną zakończone szczegółowym raportem z przeprowadzonych testów z podsumowaniem dla kierownictwa Zamawiającego.