

ZAMAWIAJĄCY: MINISTERSTWO FINANSÓW
00-916 Warszawa, ul. Świętokrzyska 12,

OPIS PRZEDMIOTU ZAMÓWIENIA

*dotyczącego zamówienia publicznego na
Zamówienie usługi oceny (audytu ryzyka nadużyć) w organizacji we
wskazanych przez Zamawiającego obszarach*

PRZEDMIOT ZAMÓWIENIA

Przedmiotem zamawianej usługi jest ocena (audyt nadużyć) w organizacji we wskazanych przez Zamawiającego obszarach.

OGÓLNY OPIS ZAMÓWIENIA

1. Wykonawcą usługi audytu może być firma audytorska świadcząca usługi analizy i oceny w takich obszarach jak Organizacja i Zarządzanie, Informatyzacja, Bezpieczeństwo Informacji.
2. Miejscem realizacji zamówienia będzie siedziba Zamawiającego, tj. Ministerstwo Finansów ul. Świętokrzyska 12, 00-916 Warszawa lub siedziba jednostki organizacyjnej podległej lub nadzorowanej przez Ministra Finansów, w zależności od zakresu realizowanej analizy i oceny.
3. Zamówienie będzie realizowane w dni robocze w siedzibie Zamawiającego, lub zdalnie w zakresie uzgodnionym z Zamawiającym.
 - 1) Wyniki przedmiotu zamówienia będą zawarte w raportach z audytu sporządzonych przez Wykonawcę do każdego obszaru i etapu odrębnie. Zamawiający pod sformułowaniem „raport” rozumie treść zawierającą co najmniej:
 - a) zakres przedmiotowy, do którego odnosi się raport,
 - b) ogólny opis przeprowadzonego badania obejmujący wskazanie: co zostało wykonane, przy pomocy jakich narzędzi, metod doboru próby, przy wykorzystaniu jakich zasobów ludzkich w odniesieniu do posiadanych certyfikatów/uprawnień doświadczenia,
 - c) ogólna ocena badanego obszaru: z zastrzeżeniem, że ocena powinna być trójstopniowa (pozytywna, pozytywna z zastrzeżeniami, negatywna) i przedstawiona w formie opisowej wraz z uzasadnieniem oceny,
 - d) ryzyka zidentyfikowane w każdym z obszarów określonych w pkt 1,
 - e) ustalenia stanu faktycznego,
 - f) wnioski,
 - g) rekomendacje,
 - h) podpisy audytorów badających obszar,
 - i) inne załączniki wraz z ewentualną graficzną prezentacją wyników, np. diagramy, tabele, wykresy, inne przydatne do przedstawienia wyników audytu, w tym wyniki testów i ich interpretacje.
 - 2) Zbiorcze, kluczowe wyniki zostaną zawarte w streszczeniu przeznaczonym dla wyższej kadry kierowniczej MF, zawierającym co najmniej najważniejsze wnioski dla każdego z badanych obszarów, przedstawione również w formie graficznej.
4. Każda część badania audytowego, będzie zakończona prezentacją dla wskazanej przez Zamawiającego grupy pracowników, na której zostaną przedstawione i omówione wyniki właściwej części audytu.

5. Dobór metody, technik i narzędzi analizy obszarów audytu w celu realizacji przedmiotu zamówienia leży po stronie Wykonawcy.
6. Wykonanie usługi będzie zrealizowane z zachowaniem wszystkich norm i przepisów zawodowych audytorów, gwarantujących odpowiednią jakość usługi oraz właściwy poziom etyczny.
7. Zamawiający zapewni miejsca pracy, udostępni niezbędne dokumenty, procedury oraz udzieli odpowiedzi na wszystkie zadane pytania. Przy czym:
 - 1) Zamawiający nie udostępni dokumentów publicznych powszechnie dostępnych.
 - 2) Zamawiający wskaże osobę/osoby do bieżącej współpracy z audytorami.
8. W ramach realizacji usługi Wykonawca jest zobowiązany do:
 - 1) Przedstawienia i omówienia metody i zakresu badania przed dokonaniem czynności,
 - 2) Bieżącej współpracy z osobami wskazanymi do kontaktów z Wykonawcą, a w szczególności do niezwłocznego informowania:
 - a) o problemach w realizacji usługi,
 - b) o ryzyku niedotrzymania terminów,
 - c) o niewłaściwej współpracy pracowników Ministerstwa Finansów (dalej: Ministerstwo) w audytowanym obszarze,
 - d) o nieotrzymaniu żądanych dokumentów, odpowiedzi na pytania we wskazanym terminie.
 - 3) Korzystania z własnych zasobów informatycznych (komputer, drukarka, Internet, inne).
 - 4) Jeżeli, zaplanowana przez audytora metodyka badania, będzie wymagała zainstalowania oprogramowania w infrastrukturze Zamawiającego, jest on zobowiązany do wcześniejszego poinformowania Zamawiającego o sposobie i zakresie działania oprogramowania oraz uzyskania zgody odpowiednich służb Ministerstwa.
9. Harmonogram realizacji usługi:
 - 1) Przygotowanie badania zakresu etapu I – do _____,
 - 2) Zakończenie badania zakresu etapu I – do _____,
 - 3) Przekazanie raportów z badania zakresu etapu I – do _____,
 - 4) Akceptacja i odbiór raportów z etapu I z uwzględnieniem dni przewidzianych na zgłoszenie zastrzeżeń przez zamawiającego – do _____,
 - 5) Realizacja prezentacji i omówienie wyników etapu I - _____,
 - 6) Rozliczenie etapu I – do _____,
 - 7) Przygotowanie badania zakresu etapu II – do _____,
 - 8) Zakończenie badania zakresu etapu II – do _____,
 - 9) Przekazanie raportów z badania zakresu etapu II – do _____,
 - 10) Akceptacja i odbiór raportów z etapu II z uwzględnieniem dni przewidzianych na zastrzeżenia przez zamawiającego – do _____,
 - 11) Realizacja prezentacji i omówienie wyników etapu II – do _____,
 - 12) Rozliczenie i zakończenie umowy – do _____,

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

1. W obszarze Organizacja i Zarządzanie:

- 1) przeprowadzenie analizy procedur i realizowanych procesów z obszaru kompetencji Dyrektora Generalnego w zakresie zapewnienia zgodności z przepisami prawa realizacji zadań, wraz z rekomendacją w zakresie zmian w procedurach i optymalizacji procesów z uwzględnieniem procesu dotyczącego:
 - ✓ naboru pracowników,
 - ✓ innego procesu wytypowanego/ zaproponowanego przez Wykonawcę (audytora) na podstawie analizy ryzyka i doświadczenia zawodowego, charakteryzującego się najwyższym prawdopodobieństwem możliwości wystąpienia ryzyka nadużyć (wytypowany przez Wykonawcę proces, będzie omówiony, uzgodniony i zaakceptowany przez Zamawiającego). Zamawiający zachowuje prawo do wskazania innego procesu niż wskazany przez Wykonawcę.
- 2) przeprowadzenie analizy efektywności zarządzania projektami, w tym szczególnie struktury projektowej w kontekście zakładanych i osiągniętych celów (badanie na wybranej próbie realizowanych projektów).

Dla prawidłowego wykonania powyższego zakresu Zamawiający oczekiwać będzie:

- a) raportu dotyczącego procedur i procesów (pkt 1), zawierającego ustalenia czy ustanowione (wybrane przez Zamawiającego) procedury i procesy zapewniają zgodną z prawem realizację zadań w komórkach organizacyjnych nadzorowanych przez Dyrektora Generalnego i ograniczają możliwość wystąpienia ewentualnych nieprawidłowości, wraz z rekomendacją ewentualnej zmiany w procedurach i optymalizacji tych procesów, jeśli będzie potrzebna;
- b) raportu dotyczącego zarządzania strukturą projektową (pkt 2) i realizacji poszczególnych projektów, zawierającego ustalenia:
 - i. czy wdrożony model zarządzania i realizacji projektami jest efektywny, wraz z rekomendacją modelu i sposobu usprawnienia, optymalizacji procesów zarządzania i realizacji projektów, jeśli będzie potrzebna,
 - ii. czy obecna struktura zarządzania projektami pozwala na skuteczną realizację projektów wraz z rekomendacją optymalizacji struktury, jeśli będzie potrzebna;
- c) przeprowadzenia prezentacji dla określonej grupy pracowników wskazanej przez Zamawiającego, w celu przedstawienia i omówienia ustaleń zawartych w raporcie.

2. W obszarze Informatyzacja:

- 1) przeprowadzenie analizy podziału kompetencji, zadań i struktury w obszarze IT (Ministerstwo, Departament Transformacji Cyfrowej, Pełnomocnik Ministra ds. Informatyzacji, Pełnomocnik ds. Sztucznej Inteligencji, Zespół Oceny Inicjatyw Biznesowych, Rada Informatyzacji, Aplikacje Krytyczne Sp. z o.o.,

Centrum Informatyki Resortu Finansów, jednostki KAS oraz inne role w obszarze IT, o ile zostały powołane do dnia zawarcia umowy z Wykonawcą), przy wykorzystaniu modelu referencyjnego procesu COBIT 5, z uwzględnieniem istniejących dokumentów dotyczących powołania struktur, zarządzania i nadzoru IT.

- 2) przeprowadzenie analizy obecnie realizowanych procesów budowy, wytwarzania, rozwoju i monitorowania usług informatycznych, z uwzględnieniem procesu opiniowania projektów aktów prawnych, na podstawie których inicjowany jest proces wytwarzania i rozwoju usług IT. Analiza procesów nie będzie obejmować etapów realizowanych poza MF.

Dla prawidłowego wykonania powyższego zakresu Zamawiający oczekiwać będzie:

- a) raportu dotyczącego struktury organizacyjnej, podziału kompetencji i spójności ról, realizowanych zadań w zakresie jednostek IT funkcjonujących w resorcie finansów (pkt 1), wraz z rekomendacjami dotyczącymi optymalizacji struktury procesów, w tym procesów w zakresie nadzoru i zarządzania, jeśli będzie potrzebna;
- b) raportu dotyczącego oceny procesów budowy, wytwarzania, rozwoju i monitorowania usług informatycznych oraz procesów procedowania i opiniowania aktów prawnych w zakresie wymagań biznesowych oraz zarządzania zmianą w projektach informatycznych (pkt 2) wraz z rekomendacjami dotyczącymi standaryzacji i optymalizacji ocenianych procesów;
- c) przeprowadzenia prezentacji dla określonej grupy pracowników wskazanej przez Zamawiającego, w celu przedstawienia i omówienia ustaleń zawartych w raportach.

3. W obszarze Bezpieczeństwo Informacji:

- 1) przeprowadzenie analizy bezpieczeństwa procesów związanych z przepływem informacji, infrastruktury, oprogramowania oraz zabezpieczeń techniczno-organizacyjnych pod kątem adekwatności, efektywności oraz zgodności z odpowiednimi przepisami prawa i obowiązującymi normami, ze szczególnym uwzględnieniem procesu:

✓ obsługi incydentów bezpieczeństwa informacji.

Dla prawidłowego wykonania powyższego zakresu Zamawiający oczekiwać będzie:

- a) raportu z przeprowadzenia analizy procesów, a także przeglądu dokumentacji wchodzącej w skład Systemu Zarządzania Bezpieczeństwem Informacji Zamawiającego, w szczególności deklaracji stosowania zabezpieczeń, określonych w załączniku A do normy PN-EN ISO/IEC 27001:2017-06, zawierającego identyfikację potencjalnych zagrożeń, wraz z rekomendacjami dotyczącymi działań, które należy podjąć w celu spełnienia wymogów dotyczących zarządzania bezpieczeństwem informacji, zgodnie z wytycznymi PN-EN ISO/IEC 27001:2023, ze szczególnym uwzględnieniem zabezpieczeń niewystępujących w wydaniu PN-EN ISO/IEC 27001:2017-06; realizacja tych

rekomendacji powinna pozwolić na zapewnienie gotowości Zamawiającego do procesu certyfikacji na zgodność z normą PN-EN ISO/IEC 27001:2023;

- b) przeprowadzenia prezentacji dla określonej grupy pracowników wskazanej przez Zamawiającego, w celu przedstawienia i omówienia ustaleń zawartych w raporcie.

WYMAGANA DOKUMENTACJA AUDYTOWA

1. Na podstawie realizowanej przez Wykonawcę usługi, Zamawiający oczekiwać będzie sporządzenia następujących dokumentów:

- 1) **Dokumentacja dla etapu I:**

- a) **w obszarze Organizacja i Zarządzanie:**

- i. raport odnoszący się do pkt 1, w zakresie obszaru Organizacja i Zarządzanie/adekwatność procedur i procesów z uwzględnieniem procesu wskazanego oraz wytypowanego przez Wykonawcę,
 - ii. prezentacja

- b) **w obszarze Informatyzacja:**

- i. raport odnoszący się do pkt 1, w zakresie obszaru Informatyzacja,
 - ii. prezentacja

- c) **w obszarze Bezpieczeństwo Informacji:**

- i. raport, odnoszący się do pkt 1 w zakresie obszaru Bezpieczeństwo Informacji
 - ii. prezentacja

- 2) **Dokumentacja dla etapu II:**

- a) **w obszarze Organizacja i Zarządzanie:**

- i. raport odnoszący się do pkt 2 w zakresie obszaru Organizacja i Zarządzanie/ zarządzanie projektami,
 - ii. prezentacja

- b) **w obszarze Informatyzacja:**

- i. raport odnoszący się do pkt 2 w zakresie obszaru Informatyzacja,
 - ii. prezentacja

2. Dokumentacja podsumowująca realizację audytu w zakresie I i II etapu:

- a) streszczenie przeznaczone dla wyższej kadry kierowniczej MF,
 - b) prezentacja multimedialna podsumowująca wszystkie najważniejsze wyniki audytu.

WYMAGANIA DOTYCZĄCE WYKONAWCY

1. Wykonawcą może być podmiot gospodarczy, który zrealizował co najmniej 2 usług w zakresie audytu w każdym z obszarów:

- 1) **Organizacja i Zarządzanie**, w tym:

- a) ocena procesów i ich projektowanie,

- b) adekwatność procedur,
 - c) zarządzanie projektami,
- 2) **Informatyzacja**, w tym:
 - a) adekwatność zadań i podział kompetencji oraz mechanizmy i formy nadzoru i zarządzania w zakresie IT,
- 3) **Bezpieczeństwo Informacji**, w tym System Zarządzania Bezpieczeństwem Informacji z uwzględnieniem:
 - a) normy PN-EN ISO/IEC 27001:2023,
 - b) wymagań zawartych w Rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247),
 - c) Dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii Europejskiej (dyrektywa NIS 2).
- 2. Wykonawca musi dysponować (samodzielnie lub przez podwykonawców na zasadzie zawartych umów o współpracy) osobą lub osobami posiadającymi łącznie:
 - a. certyfikat CIA (Certified Internal Auditor),
 - b. audytora/audytora wiodącego ISO 27001:2023,
 - c. ITIL 4 lub COBIT 5,
 - d. audytora/audytora wiodącego ISO 22301,
 - e. uprawnienia do certyfikacji systemu zarządzania bezpieczeństwem informacji na zgodność z normą PN-EN ISO/IEC 27001:2023,

Przy czym każda z osób musi posiadać co najmniej 2 letnie doświadczenie w prowadzeniu audytu w jednym z obszarów wskazanych w pkt 1, tak, aby doświadczenie w prowadzeniu audytu obejmowało łącznie wszystkie obszary określone w pkt 1.

OGÓLNE ZAŁOŻENIA REALIZACJI AUDYTU

1. Audyt zakończy się w terminie dni od dnia podpisania umowy.
2. Audyt będzie realizowany w dwóch etapach.
 - 1) przedstawienie i omówienie wyników badania etapu I – powinno zakończyć się do dnia (z uwzględnieniem procedury zastrzeżeń Zamawiającego),
 - 2) przedstawienie i omówienie wyników badania etapu II - powinno zakończyć się do dnia (z uwzględnieniem procedury zastrzeżeń Zamawiającego).
3. Przystąpienie do realizacji etapu II będzie możliwe dopiero po odbiorze (bez zastrzeżeń) realizacji etapu I (z uwzględnieniem terminów przewidzianych na zastrzeżenia).
4. Wykonawca przekaze Zamawiającemu wymaganą dokumentację w formie papierowej (z zastrzeżeniem, że treść raportu prezentowana w formie wykresów, diagramów, lub innych metod graficznych musi być wykonana w kolorze) i elektronicznej, pliki w formacie pdf oraz edytowalnej pliki w formacie MS Office.

5. Płatności będą realizowane po odbiorze poszczególnych etapów bez zastrzeżeń, przy czym, płatność za I etap będzie wynosił 40% całkowitej wartości umowy oraz 60% po właściwym zrealizowaniu i odbiorze etapu II oraz po zrealizowaniu prezentacji multimedialnej podsumowującej wszystkie najważniejsze wyniki audytu.

OKREŚLENIE WŁAŚCIWYCH KODÓW CPV USŁUGI

Kod CPV: 79212000-3 Usługi audytu