Załącznik nr 3 do Zapytania ofertowego

OPIS PRZEDMIOTU ZAMÓWIENIA

Audyt bezpieczeństwa systemu e-SOA 2.0

Zapytanie ofertowe nr 5/2026/e-SOA 2.0 — postępowanie w trybie konkurencyjnym, współfinansowane ze środków UE.

1. Przedmiot zamówienia i cel

Przedmiotem zamówienia, realizowanego przez wykonawcę (dalej: Audytor), jest niezależna weryfikacja bezpieczeństwa systemu e-SOA 2.0 (audyt bezpieczeństwa wraz z testami bezpieczeństwa i re-audytem), przeprowadzona w dwóch etapach odpowiadających etapom wdrożenia systemu: modułom podstawowym oraz całości systemu.

Cele zamówienia:

1. Potwierdzenie, że system i jego infrastruktura spełniają wymagania bezpieczeństwa określone w dokumentacji zamówienia na wykonanie systemu, zanim Zamawiający dokona odbiorów i uruchomienia produkcyjnego.
2. Identyfikacja podatności i niezgodności wraz z oceną ich istotności, w formie umożliwiającej Zamawiającemu wyegzekwowanie poprawek od wykonawcy systemu.
3. Potwierdzenie (re-audyt), że zalecenia zostały wdrożone.

2. Opis systemu i środowisk objętych audytem

e-SOA 2.0 to webowy system obsługi adwokatury z około 40 000 użytkowników (adwokaci, aplikanci, pracownicy NRA i okręgowych rad adwokackich), przetwarzający dane osobowe, w tym numery PESEL i dane finansowe. System składa się z 20 modułów wdrażanych w dwóch grupach: moduły podstawowe i moduły dodatkowe.

Element	Opis
Aplikacja	Aplikacja webowa (SPA) z API i przetwarzaniem asynchronicznym; wspólny panel administracyjny
Uwierzytelnianie użytkowników	Usługa zarządzania tożsamością z MFA dla wszystkich użytkowników, SSO, model ról z podziałem na izby i rolami administracyjnymi
Dostęp administracyjny do chmury	Federacja z katalogiem tożsamości Zamawiającego, MFA
Infrastruktura	Chmura AWS lub równoważna: organizacja z kontem produkcyjnym (PROD), przedprodukcyjnym (PRE-PROD) i kontem wspólnym (shared – logi, zarządzanie

Element	Opis
	tożsamością); region w UE z regionem zapasowym; usługi zarządzane (kontenery, relacyjna baza danych, magazyn obiektów, pamięć podręczna, kolejki, poczta, CDN, WAF); infrastruktura jako kod i potok CI/CD
Bezpieczeństwo i monitoring	Natywne usługi bezpieczeństwa, monitoringu, szyfrowania i zarządzania sekretami chmury
Integracje	Co najmniej 8 integracji z systemami zewnętrznymi (API i wymiana plików, w tym połączenia uwierzytelniane certyfikatami)

Środowiska objęte audytem:

- **PRE-PROD** – główne środowisko testów (konfiguracja jak PROD, dane zanonimizowane),
- **PROD** – przegląd konfiguracji w trybie tylko do odczytu; testy aktywne wyłącznie za odrębną zgodą Zamawiającego,
- **shared** – konto wspólne (logi, rejestr obrazów, zarządzanie tożsamością); przegląd konfiguracji w trybie tylko do odczytu,
- **repozytoria kodu aplikacji i infrastruktury** – dostęp tylko do odczytu.

Szczegółowy opis systemu (Załącznik poufny) oraz specyfikacja architektury infrastruktury zostaną przekazane wybranemu Audytorowi po zawarciu umowy i podpisaniu zobowiązania do poufności.

3. Zakres audytu

Zakres obejmuje siedem obszarów oraz weryfikację macierzy zgodności z wymaganiami bezpieczeństwa. Każdy obszar jest realizowany w obu etapach: w etapie A dla modułów podstawowych i całej infrastruktury, w etapie B dla modułów dodatkowych, zmian od etapu A i systemu jako całości.

3.1 Testy penetracyjne aplikacji i API

1. Testy typu grey-box aplikacji webowej i API na środowisku PRE-PROD, z kontami testowymi dla każdej roli użytkownika (w tym ról administracyjnych i użytkowników różnych izb).
2. Metodyka: OWASP Web Security Testing Guide, weryfikacja wymagań OWASP ASVS 4.0 poziom 2 oraz OWASP API Security Top 10 (lub równoważne).
3. Obszary obowiązkowe:
    - uwierzytelnianie, MFA, SSO, odzyskiwanie dostępu, blokady i ochrona przed brute force,
    - zarządzanie sesją i tokenami (czas życia, rotacja, unieważnianie, reautoryzacja przed operacjami wrażliwymi),
    - autoryzacja na poziomie funkcji i obiektu (IDOR), eskalacja uprawnień poziomych i pionowych, separacja danych między izbami, funkcje administracyjne podwyższonego ryzyka,
    - walidacja danych wejściowych (injection, XSS, deserializacja), przesyłanie i przechowywanie plików,

- eksporty i raporty (limity, znakowanie, rejestr pobrań), importy i operacje wsadowe,
- API udostępniane przez e-SOA na potrzeby integracji oraz zabezpieczenia kanałów integracyjnych (mTLS, uwierzytelnianie), bez testów po stronie systemów zewnętrznych,
- konfiguracja warstwy brzegowej: TLS, nagłówki bezpieczeństwa, CORS, WAF i limity wywołań,
- autoryzacja operacji finansowych i odporność na manipulację kwotami (składki, salda, płatności).

4. Weryfikacja testów negatywnych wymaganych przed uruchomieniem produkcyjnym: brak nieuprawnionego dostępu, brak eskalacji, prawidłowa obsługa limitów i wygaśnięć.

3.2 Weryfikacja kodu źródłowego pod kątem podatności

1. Analiza narzędziowa (SAST, SCA, wykrywanie sekretów) kodu aplikacji i jej zależności oraz ręczny przegląd kodu w obszarach: uwierzytelnianie i sesje, autoryzacja i separacja danych między izbami, funkcje administracyjne, operacje wysokiego ryzyka.
2. Przegląd kodu infrastruktury (IaC) i konfiguracji potoku CI/CD.
3. Weryfikacja implementacji szyfrowania danych szczególnie chronionych.
4. Dostęp do repozytoriów tylko do odczytu, na zasadach z pkt 6.

3.3 Analiza konfiguracji środowiska produkcyjnego

1. Przegląd konfiguracji organizacji i kont chmurowych PROD, PRE-PROD i shared względem CIS AWS Foundations Benchmark (lub równoważnego) i założonej architektury.
2. Obszary: polityki organizacyjne (SCP), uprawnienia IAM i analiza nadmiarowych uprawnień, sieć i ekspozycja usług, szyfrowanie i zarządzanie kluczami, sekrety, magazyny danych (publiczny dostęp, wersjonowanie, Object Lock), bazy danych, kontenery i rejestr obrazów, WAF i CDN, kopie zapasowe i replikacja do regionu zapasowego.
3. Weryfikacja zgodności stanu faktycznego z kodem infrastruktury (dryf konfiguracji).
4. Przegląd realizowany w roli tylko do odczytu (np. SecurityAudit / ReadOnly), bez zmian w środowisku.

3.4 Ocena procesu zarządzania podatnościami systemu

Obszar obejmuje proces zarządzania podatnościami e-SOA 2.0, który wykonawca systemu prowadzi zgodnie z OPZ (rozdz. 23) i Załącznikiem „Wymogi bezpieczeństwa” (pkt 11.2). Audytor ocenia go na podstawie dokumentów, rejestrów i raportów przekazanych przez wykonawcę systemu oraz dostępu tylko do odczytu do repozytoriów i potoku CI/CD.

1. Rejestr komponentów (SBOM) i jego zgodność z wdrożoną wersją systemu.
2. Skanowanie kodu, zależności i obrazów w CI/CD oraz blokady wdrożenia przy podatnościach krytycznych i wysokich: konfiguracja potoku i wyniki ostatnich uruchomień.
3. Rejestr podatności i dotrzymywanie terminów usuwania (krytyczne 48 h, wysokie 7 dni, średnie 30 dni, niskie 90 dni), na próbie wpisów.
4. Raporty z testów bezpieczeństwa i testów penetracyjnych przedstawiane przez wykonawcę systemu przy odbiorach: zakres, metodyka, pokrycie, zamknięcie ustaleń.

5. Zabezpieczenia łańcucha dostaw oprogramowania widoczne w repozytoriach i CI/CD: ochrona gałęzi, przeglądy zmian, pochodzenie i wersjonowanie artefaktów.
6. Punkt kontaktowy i procedura przyjmowania zgłoszeń podatności.

3.5 Testy bezpieczeństwa danych

1. Szyfrowanie danych w spoczynku i w tranzycie, w tym ruchu wewnętrznego i integracji.
2. Separacja środowisk: brak danych rzeczywistych poza PROD, skuteczność anonimizacji danych w PRE-PROD.
3. Kopie zapasowe i odtwarzanie: udział Audytora jako obserwatora w teście odtworzenia lub teście przełączenia do regionu zapasowego przeprowadzanym przez wykonawcę systemu; ocena osiągniętych RPO i RTO względem wartości docelowych wskazanych w Załączniku poufnym.
4. Ochrona danych w eksportach, raportach, plikach i powiadomieniach (zakres ujawnianych danych, znakowanie, limity) – w warstwie technicznej, bez oceny prawnej.

3.6 Audyt zarządzania tożsamością i dostępem

1. Użytkownicy systemu: konfiguracja usługi tożsamości (polityka haseł, MFA, blokady, sesje), federacja SSO, model ról i uprawnień (matryca ról a stan faktyczny), mechanizm przeglądu uprawnień.
2. Dostęp administracyjny do chmury: federacja z katalogiem tożsamości Zamawiającego, przypisania grup do zestawów uprawnień, wymuszenie MFA, czas sesji, brak długoterminowych kluczy, procedura dostępu awaryjnego i alarmy użycia kont uprzywilejowanych.
3. Dostęp uprzywilejowany wykonawców (wykonawca systemu, partner chmurowy): zasada minimalnych uprawnień, imienność i rozliczalność.

3.7 Audyt logów i monitoringu bezpieczeństwa

1. Kompletność katalogu zdarzeń bezpieczeństwa i operacyjnych (logowania, dostęp do danych, eksporty, zmiany uprawnień, operacje wsadowe, operacje administracyjne) a faktycznie rejestrowane zdarzenia.
2. Nienaruszalność i retencja rejestrów (np. Object Lock, walidacja integralności), separacja kont logowania.
3. Progi alarmowe i ścieżki powiadamiania; skuteczność wykrywania (weryfikacja na zdarzeniach wygenerowanych podczas testów penetracyjnych).
4. Procedura reagowania na incydenty i ograniczania ekspozycji: przegląd procedury ograniczenia ekspozycji i runbooka reakcji na incydent oraz udział Audytora jako obserwatora w ćwiczeniu reakcji przeprowadzanym przez wykonawcę systemu.

3.8 Weryfikacja macierzy zgodności

Audytor weryfikuje macierz zgodności z wymaganiami bezpieczeństwa (pkt 4.1 poz. 1–4), przygotowaną przez wykonawcę systemu i przekazaną przez Zamawiającego: w pełni dla wymagań objętych obszarami 3.1–3.7, a dla pozostałych wymagań na próbie. Wynikiem jest zweryfikowana macierz: wymaganie – status (spełnione / częściowo / niespełnione / nie zweryfikowano) – dowód – odniesienie do ustalenia.

4. Kryteria odniesienia i klasyfikacja ustaleń

Ustalenia są oceniane względem wymagań umownych wykonawcy systemu, bo tylko niezgodność z nimi Zamawiający może wyegzekwować w ramach odbiorów i gwarancji. Pozostałe ustalenia Audytor przedstawia jako rekomendacje.

4.1 Kryteria odniesienia

1. Opis przedmiotu zamówienia na wykonanie e-SOA 2.0: wymagania niefunkcjonalne z obszaru bezpieczeństwa (WMNF), rozdział 23 „Bezpieczeństwo systemu", założenia dotyczące 2FA, SSO i szyfrowania komunikacji, w tym WMNF_001 – art. 24 i 32 RODO w zakresie środków technicznych.
2. Załącznik „Wymogi bezpieczeństwa do przedmiotu zamówienia" wraz z kryteriami odbioru i wymaganymi dowodami.
3. OWASP ASVS 4.0 poziom 2 dla części webowej (Zał. 5 pkt 11.1), z odniesieniem ustaleń także do wymagania WMNF_002 (poziom 1, wskazane sekcje), oraz OWASP API Security Top 10 dla API (lub równoważne).
4. Zaakceptowana specyfikacja architektury infrastruktury (wersja obowiązująca w dniu rozpoczęcia etapu).
5. CIS AWS Foundations Benchmark (lub równoważny) dla konfiguracji chmury.
6. Minimalne wymagania dla systemów teleinformatycznych (rozporządzenie w sprawie Krajowych Ram Interoperacyjności)– jako odniesienie dla rekomendacji, bez odrębnej oceny zgodności.

4.2 Klasyfikacja ustaleń

Każde ustalenie ma dwie cechy: istotność i kwalifikację.

Istotność	Ocena
Krytyczna	CVSS 9,0–10,0
Wysoka	CVSS 7,0–8,9
Średnia	CVSS 4,0–6,9
Niska	CVSS 0,1–3,9
Informacyjna	bez oceny

Kategorie istotności odpowiadają kategoriom z Zał. 5 pkt 11.2 OPZ; przypisanie według skali jakościowej CVSS (OPZ rozdz. 23).

Ocena według CVSS w wersji 3.1 lub 4.0, z wektorem i uzasadnieniem. Dla ustaleń konfiguracyjnych i procesowych, które nie poddają się ocenie CVSS, Audytor stosuje tę samą skalę z uzasadnieniem opisowym.

Kwalifikacja:

- **Niezgodność** – naruszenie wymagania z pkt 4.1 pozycje 1–4, ze wskazaniem konkretnego zapisu,
- **Rekomendacja** – ustalenie wykraczające poza wymagania umowne (dobra praktyka, wymaganie z pozycji 5–6 nieprzeniesione do umowy wykonawcy systemu).

5. Etapy i harmonogram

Prace są uruchamiane zgłoszeniem gotowości przez Zamawiającego, a nie sztywnymi datami, gdyż zależą od postępu wykonawcy systemu. Terminy Audytora liczone są od zgłoszeń Zamawiającego. Zamawiający planuje zgłoszenie gotowości do etapu A w styczniu–lutym 2027 r., a do etapu B w kwietniu–maju 2027 r. Umowa zostanie zawarta na czas określony do 30.09.2027 r.

Wskazane okresy mają charakter orientacyjny. Ich zmiana nie stanowi podstawy do roszczeń Audytora ani do zmiany wynagrodzenia. Zamawiający poinformuje Audytora o planowanym terminie zgłoszenia gotowości z wyprzedzeniem co najmniej 10 dni roboczych.

5.1 Etapy realizacji

1. **Etap 0 – przygotowanie.** W ciągu 10 dni roboczych od zawarcia umowy: spotkanie otwierające, plan audytu, zasady prowadzenia testów zaakceptowane przez Zamawiającego (pkt 6.2), lista kont i dostępów.
2. **Etap A – moduły podstawowe i infrastruktura.**
    - rozpoczęcie w ciągu 5 dni roboczych od zgłoszenia przez Zamawiającego gotowości PRE-PROD z modułami podstawowymi (planowo styczeń–luty 2027),
    - raport z etapu w ciągu 30 dni roboczych od rozpoczęcia,
    - re-audyt w ciągu 10 dni roboczych od zgłoszenia przez Zamawiającego usunięcia ustaleń; raport z re-audytu w ciągu 5 dni roboczych od jego zakończenia.
3. **Etap B – całość systemu (moduły dodatkowe, zmiany od etapu A, system jako całość).**
    - rozpoczęcie w ciągu 5 dni roboczych od zgłoszenia gotowości modułów dodatkowych (planowo kwiecień–maj 2027),
    - raport z etapu w ciągu 20 dni roboczych od rozpoczęcia,
    - re-audyt i raport jak w etapie A.

Ustalenia o istotności krytycznej lub wysokiej Audytor sygnalizuje Zamawiającemu w trakcie prac, przed przekazaniem raportu. Ustalenia dotyczące środowiska produkcyjnego zgłasza niezwłocznie.

6. Warunki realizacji

Wszystkie działania Audytora są nieinwazyjne i prowadzone według zasad zaakceptowanych przez Zamawiającego.

6.1 Dostępy zapewniane przez Zamawiającego

- konta testowe w aplikacji dla każdej roli na PRE-PROD,
- dostęp do kont PROD, PRE-PROD i shared w roli audytorskiej (konfiguracja i metadane), nadawany przez Zamawiającego przez federację z katalogiem tożsamości Zamawiającego, z MFA (konta imienne),
- dostęp do repozytoriów kodu aplikacji, infrastruktury i procedur operacyjnych tylko do odczytu,
- dokumentacja: specyfikacja architektury, macierz ról, katalog zdarzeń, dowody zgodności i raporty z testów wykonawcy systemu, procedury odtwarzania i ograniczania ekspozycji (Zał. 5 pkt 11.8 i 12) oraz runbooki ze specyfikacji architektury (pkt 10.5),

- kontakt techniczny po stronie Zamawiającego oraz kontakt do wykonawcy systemu wskazany przez Zamawiającego.

6.2 Zasady prowadzenia testów

Przed etapem A Audytor przygotowuje, a Zamawiający akceptuje dokument zasad testów, obejmujący co najmniej:

1. zakres i cele (adresy, konta, środowiska), wyłączenia i ograniczenia,
2. okna czasowe testów i zasady testów obciążających lub mogących zakłócić działanie,
3. adresy IP i tożsamości testerów (np. do odróżnienia w logach i regułach WAF),
4. zakaz testów socjotechnicznych i DoS, zakaz modyfikacji kodu i konfiguracji, zakaz trwałego pozostawiania artefaktów,
5. tryb wstrzymania testów i ścieżkę eskalacji, w tym zgłaszanie podatności krytycznych,
6. potwierdzenie przez Zamawiającego wykonania kopii zapasowej środowiska przed rozpoczęciem testów aktywnych.

Testy aktywne na PROD są dopuszczalne wyłącznie za odrębną pisemną zgodą Zamawiającego i w uzgodnionym oknie.

6.3 Poufność

- Audytor i każda osoba z jego zespołu podpisują zobowiązanie do zachowania poufności przed uzyskaniem dostępów.
- Materiały robocze i dane uzyskane w trakcie audytu są przechowywane w sposób zaszyfrowany i usuwane po zakończeniu umowy, z wyjątkiem raportów.

6.4 Dane osobowe

Audyt jest prowadzony na danych zanonimizowanych lub testowych. Dostęp do kont PROD i shared obejmuje konfigurację i metadane usług (rola typu SecurityAudit), bez dostępu do treści danych: plików, rekordów baz danych i kopii zapasowych. Jeżeli w trakcie realizacji Audytor mógłby uzyskać dostęp do danych osobowych przetwarzanych w systemie, Strony zawrą umowę powierzenia przed nadaniem takiego dostępu. Audytor niezwłocznie zgłasza każde przypadkowe zetknięcie z danymi rzeczywistymi.

6.5 Komunikacja z wykonawcą systemu

Komunikacja Audytora z wykonawcą systemu odbywa się za pośrednictwem Zamawiającego lub z jego udziałem.

7. Produkty i wymagania wobec raportów

Produkt	Etap	Zawartość
Plan audytu i zasady testów	0	Zakres, metodyka, harmonogram, zespół, wymagane dostępy, zasady z pkt 6.2
Raport z etapu	A, B	Według struktury poniżej

Produkt	Etap	Zawartość
Macierz zgodności	A, B	Wymaganie – status – dowód – ustalenie (pkt 3.8)
Raport z re-audytu	A, B	Status każdego ustalenia: usunięte / częściowo / nieusunięte / ryzyko zaakceptowane, z dowodem weryfikacji
Prezentacja wyników	A, B	Do 2 godzin, dla Zamawiającego i wykonawcy systemu, zdalnie
Zgłoszenia pilne	A, B	Sygnalizacja ustaleń krytycznych i wysokich w trakcie prac; dotyczących PROD – niezwłocznie

Raport z etapu zawiera co najmniej:

1. podsumowanie zarządcze: ogólna ocena, liczba ustaleń według istotności i kwalifikacji, najważniejsze ryzyka, w języku zrozumiałym dla osób nietechnicznych,
2. zakres, metodykę, środowiska, okres testów, wersje komponentów (identyfikator wdrożenia lub commit) i ograniczenia,
3. dla każdego ustalenia: identyfikator, tytuł, opis, lokalizację, kroki odtworzenia, dowody (zrzuty, żądania i odpowiedzi), istotność z wektorem CVSS, kwalifikację z odniesieniem do wymagania (pkt 4.2), wpływ i rekomendację naprawy,
4. ocenę każdego z siedmiu obszarów zakresu (pkt 3.1–3.7), także gdy nie stwierdzono ustaleń,
5. listę ustaleń w formacie edytowalnym (arkusz kalkulacyjny lub CSV) do śledzenia napraw.

Raporty są w języku polskim, w formatach PDF i edytowalnym, oznaczone jako poufne i opatrzone wymaganym oznakowaniem projektu.

Struktura raportu zostanie uzgodniona z Zamawiającym w etapie 0.

8. Procedura odbioru

1. Zamawiający zgłasza uwagi do raportu w ciągu 5 dni roboczych od jego doręczenia, a Audytor uwzględnia je w ciągu 5 dni roboczych.
2. Odbiór etapu A i etapu B następuje protokołem po doręczeniu raportu z re-audytu, czyli każdy etap obejmuje audyt i weryfikację wdrożenia zaleceń. Protokół jest podstawą płatności za etap.
3. Odbiór nie jest uzależniony od tego, czy wykonawca systemu usunął wszystkie ustalenia. Raport z re-audytu dokumentuje stan na dzień weryfikacji.
4. Kryterium odbioru: raport zawiera wszystkie elementy z pkt 7, obejmuje wszystkie obszary z pkt 3, a każde ustalenie można odtworzyć na podstawie opisu.

9. Wymagania wobec Wykonawcy

9.1 Niezależność

Na etapie podpisania umowy Wykonawca złoży oświadczenie potwierdzające, że ani on, ani osoby z zespołu, ani jego podwykonawcy:

- nie są powiązani kapitałowo lub osobowo z wykonawcą systemu e-SOA 2.0, tj. Devqube Sp. z o.o. ani z wykonawcą usług chmurowych dla e-SOA 2.0,
- nie uczestniczyli w projektowaniu, wytwarzaniu, konfiguracji ani utrzymaniu systemu e-SOA 2.0 lub jego infrastruktury,
- nie świadczą i nie będą świadczyć w okresie umowy usług na rzecz tych podmiotów w związku z e-SOA 2.0.

Przez powiązania kapitałowe lub osobowe rozumie się powiązania między Wykonawcą, osobami z jego zespołu lub jego podwykonawcami a wykonawcą systemu e-SOA 2.0 lub wykonawcą usług chmurowych dla e-SOA 2.0, polegające w szczególności na:

a. uczestniczeniu w spółce jako wspólnik spółki cywilnej lub spółki osobowej,

b. posiadaniu co najmniej 10% udziałów lub akcji,

c. pełnieniu funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika,

d. pozostawaniu w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa drugiego stopnia lub powinowactwa drugiego stopnia w linii bocznej lub w stosunku przysposobienia, opieki lub kurateli albo pozostawaniu we wspólnym pożyciu z jego wykonawcą, jego zastępca prawnym lub członkami organów zarządzających lub organów nadzorczych wykonawców ubiegających się o udzielenie zamówienia,

e. pozostawaniu z wykonawcą w takim stosunku prawnym lub faktycznym, że istnieje uzasadniona wątpliwość co do ich bezstronności lub niezależności w związku z postępowaniem o udzielanie zamówienia

9.2 Zespół

Oferent dysponuje zespołem co najmniej 2 osób, który łącznie spełnia poniższe wymagania:

Rola	Kwalifikacje (aktualne certyfikaty lub równoważne)	Doświadczenie w ostatnich 3 latach
Kierownik audytu	CISA, CISSP, CISM lub certyfikat audytora wiodącego ISO/IEC 27001 wydany przez akredytowaną jednostkę	Kierowanie co najmniej 2 audytami bezpieczeństwa systemów teleinformatycznych
Pentester aplikacji	OSCP, OSWE, OSEP, GWAPT, eWPTX	Co najmniej 3 testy penetracyjne aplikacji webowych i API
Audytor chmury	AWS Certified Security – Specialty, CCSP	Co najmniej 2 przeglądy bezpieczeństwa konfiguracji chmury publicznej

Na potwierdzenie spełniania powyższego warunku oferent przedłoży wykaz osób, zawierający dla każdej osoby pełnioną rolę, posiadane certyfikaty (nazwa, numer lub identyfikator, data ważności), opis

doświadczenia (zleceniodawca, przedmiot, okres realizacji) oraz podstawę dysponowania osobą, wraz z kopiami certyfikatów.

Jedna osoba może pełnić więcej niż jedną rolę, jeżeli spełnia wymagania dla każdej z nich. Zespołu wskazanego w ofercie nie można zmienić bez zgody Zamawiającego, a zastępca musi mieć co najmniej równoważne kwalifikacje.

9.3 Doświadczenie oferenta

W ostatnich 3 latach oferent wykonał należycie co najmniej 2 usługi, z których każda obejmowała audyt cyberbezpieczeństwa systemu teleinformatycznego lub infrastruktury obsługującej co najmniej 1 000 użytkowników albo test penetracyjny systemu teleinformatycznego obsługującego co najmniej 1 000 użytkowników.
Na potwierdzenie spełniania powyższego warunku oferent przedłoży wykaz zrealizowanych usług oraz referencje.

10. Struktura ceny i kryterium oceny

Oferent podaje ceny ryczałtowe netto w PLN odrębnie dla każdej pozycji z poniższej tabeli.

Poz.	Pozycja	Sposób wyceny
1	Etap 0 i etap A z re-audytem	Ryczałt
2	Etap B z re-audytem	Ryczałt

W ofercie oferent podaje także szacowaną liczbę osobodni dla pozycji 1 i 2 w podziale na obszary pkt 3.1–3.7.

Jedynym kryterium oceny ofert jest cena (100%), obliczana jako suma cen pozycji 1–2 z powyższej tabeli.

11. Materiały udostępniane Wykonawcy

Materiał	Kiedy
Opis systemu z pkt 2 niniejszego dokumentu	Z zapytaniem
Wyciąg z wymagań bezpieczeństwa OPZ systemu (WMNF z obszaru bezpieczeństwa, rozdz. 23) i Załącznik „Wymogi bezpieczeństwa”	Po zawarciu umowy i podpisaniu zobowiązania do poufności
Specyfikacja wymagań technicznych – Infrastruktura AWS lub równoważna	Po zawarciu umowy i podpisaniu zobowiązania do poufności
Załącznik poufny – szczegółowy opis systemu (komponenty, konta i regiony, usługi bezpieczeństwa, integracje, wartości docelowe RPO/RTO)	Po zawarciu umowy i podpisaniu zobowiązania do poufności

Materiał	Kiedy
Macierz ról, katalog zdarzeń, runbooki, dowody zgodności i raporty z testów wykonawcy systemu	Na początku etapu