

AKF Kraków
al. Jana Pawła II 78

Kraków, dnia 30/04/2025 r.

31-571 Kraków

.....
[nazwa zamawiającego, adres]

WYKONAWCY

ubiegający się o zamówienie

Dotyczy: postępowania o udzielenie zamówienia publicznego:

Nazwa zamówienia: **Przeprowadzenie audytu cyberbezpieczeństwa systemów informatycznych AKF w Krakowie wraz z przygotowaniem dokumentacji poaudytowej**

Znak sprawy : K-2.381/11/BIP/2025

PYTANIA i ODPOWIEDZI
z dnia 30.04.2025

Zamawiający udostępnia poniżej treść zapytań oraz treść czterech ankiet, które zostały złożone do przedmiotowego postępowania wraz z odpowiedziami.

PYTANIE nr 1 Jaka jest liczba lokalizacji Państwa organizacji?

Odpowiedź: Jedna lokalizacja, kilka budynków w obrębie kampusu.

PYTANIE nr 2 Jaka jest liczba pracowników Państwa organizacji?

Odpowiedź: Umowa o prace około 460 osób, umowa zlecenie około 1000 osób.

PYTANIE nr 3 Jaka jest liczba pracowników IT?

Odpowiedź: Zespół 5 osób

PYTANIE nr 4 Ile mają Państwo systemów informatycznych?

Odpowiedź: W zasobach jest około 40 systemów informatycznych

PYTANIE nr 5 Jaka jest liczba serwerów?

Odpowiedź: Fizycznych serwerów 10, wirtualnych serwerów 80

PYTANIE nr 6 Jaka jest liczba stacji roboczych?

Odpowiedź: Stacji roboczych około 500 sztuk

PYTANIE nr 7 Czy wykorzystywane systemy informatyczne są scentralizowane?

Odpowiedź: Systemy są scentralizowane

PYTANIE nr 8 Czy któreś z poniżej przedstawionych usług są zlecane na zewnątrz:

- Ochrona fizyczna obiektów

Odpowiedź Zamawiającego: Tak

- Usługi przetwarzania danych (IT)
Odpowiedź Zamawiającego: Tak
- Usługi wydruku masowego
Odpowiedź Zamawiającego : Nie
- Utrzymanie środowiska PC –
Odpowiedź Zamawiającego : Nie
- Inne, jakie? –
Odpowiedź Zamawiającego :brak

PYTANIE nr 9 Czy w organizacji zdefiniowano formalne dokumenty zawierające:

- Zakres Systemu Zarządzania Bezpieczeństwem Informacji
- Politykę Bezpieczeństwa Informacji
- Deklarację stosowania
- Klasyfikację informacji
- Metodologię oceny ryzyka i postępowania z ryzykiem
- Raport z analizy ryzyka bezpieczeństwa informacji
- Plan postępowania z ryzykiem bezpieczeństwa informacji
- Plany ochrony obiektu / Politykę bezpieczeństwa fizycznego
- Politykę kontroli dostępu
- Politykę bezpieczeństwa dostawcy / strony trzeciej
- Procedurę zarządzania incydentami
- Procedurę ciągłości działania / plany awaryjne
- Procedury operacyjne w zakresie zarządzania IT

w tym regulujące:

- Aktualizacje
- kopie zapasowe
- kryptografia
- monitorowanie zdarzeń (logi systemowe)
- urządzenia mobilne
- zarządzanie licencjami
- zarządzanie stacjami roboczymi
- zarządzanie uprawnieniami
- zarządzanie zmianą
- zbywanie nośników danych

- Zasady bezpiecznego inżynierii systemu
- Zasady dopuszczalnego wykorzystania zasobów

Odpowiedź: W organizacji brak wskazanych wyżej dokumentów, będą one przedmiotem realizacji Wykonawcy.

PYTANIE nr 10 Czy w organizacji przeprowadza się udokumentowane testy planów awaryjnych

Odpowiedź: W organizacji nie prowadzi się udokumentowanych testów planów awaryjnych.

PYTANIE nr 11 Kto w organizacji odpowiada (koordynuje) obszar ochrony informacji

Odpowiedź: Za obszar ochrony informacji odpowiada Inspektor Ochrony Danych Osobowych

Ankieta nr 1 Ankieta wyceny testy penetracyjne : Aplikacja WEB

Pytanie A1.1 Do czego służy aplikacja? (What is the purpose of the application?)

Odpowiedź : szczegółowy zakres aplikacji webowych zostanie ustalony po podpisaniu umowy

Pytanie A1.2 Jak rozbudowana jest aplikacja (szacunkowa liczba unikalnych ekranów/formularzy, np. do 10, 50, 100, etc.)? What is the estimated complexity of the application in terms of unique screens or forms (e.g., up to 10, 50, 100, etc.)?

Odpowiedź : do 150

Pytanie A1.3 Ile różnych grup użytkowników (o różnych uprawnieniach) posiada aplikacja i ile spośród nich musi zostać objętych audytem (rekomendujemy testy max. 3-4 grup)? What is the number of distinct user groups, each with different access rights, in the application, and how many of these groups should be included in the audit? It is suggested to test no more than 3-4 groups.

Odpowiedź : pracownicy etatowi, studenci, pracownicy na umowę zlecenie, osoby z zewnątrz

Pytanie A1.4 : Ile endpointów/metod API wykorzystuje aplikacja (np. 10 endpointów/metod dla REST API, 10 operacji/metod w ramach 2 usług SOAP)? How many API endpoints/methods does the application use (e.g., 10 endpoints/methods for REST API, 10 operations/methods within 2 SOAP services)?

Odpowiedź : w zależności od aplikacji minimum 10 endpointów

Pytanie A1.5 : W jakiej technologii wykonany jest system? What technology was used to build the system?

Odpowiedź : różnie - java, php, c#, dwu i trójwarstwowa architektura

Pytanie A1.6 W miarę możliwości proszę o przesłanie 2-3 zrzutów ekranowych z aplikacji.
If possible, please send us 2-3 screenshots of the application.

Odpowiedź : brak takiej możliwości

Pytanie A1.7 Jeśli audyt systemu ma obejmować audyt infrastruktury typu whitebox (analiza konfiguracji) proszę o podanie informacji jakie elementy miałyby zostać poddane testom – serwer HTTP (ile, jakie), baza danych (ile, jakie), system operacyjny (ile, jakie), np. (2 x Debian, 1 x PostgreSQL, 3 x Apache HTTPD) If the system audit is to include a whitebox infrastructure audit (configuration analysis), please provide information on which elements are to be tested - HTTP server (how many, which types), database (how many, which types), operating system (how many, which types), for example: 2 x Debian, 1 x PostgreSQL, 3 x Apache HTTPD.

Odpowiedź : Typ blackbox

Pytanie A1.8 Czy możliwe są testy zdalne (np. z wykorzystaniem tunelu VPN)? Is it possible to conduct the tests remotely (e.g., using a VPN tunnel)??

Odpowiedź : tak

Pytanie A1.9 Na jakim środowisku będzie przeprowadzany audyt (testowe/produkcyjne)?
Which environment will be used for the audit, test or production?

Odpowiedź : testowe/produkcyjne

Pytanie A1.10 Czy są jakieś ograniczenia czasowe w trybie przeprowadzania audytu (np. godziny nocne, etc.)? Are there any time restrictions on conducting the audit (e.g., night hours, etc.)?

Odpowiedź : nie

Pytanie A1.11 Jaki jest pożądany termin wykonania audytu? What is the desired deadline for the audit?

Odpowiedź : okres wakacyjny

Pytanie A1.12 Czy oferta ma zawierać retesty (tj. powtórne sprawdzenie czy wskazane w raporcie z testów podatności zostały skutecznie usunięte przez Zamawiającego)? Should the offer include retests (i.e., a second check to determine if the vulnerabilities indicated in the test report have been successfully remediated by the client)?

Odpowiedź : nie

Pytanie A1.13 W jaki sposób zrealizowane jest uwierzytelnianie do aplikacji (standardowa para login i hasło, certyfikaty, tokeny 2FA, etc)?

What methods are used for user authentication in the application? Does it use a standard username and password, certificates, 2FA tokens, or other methods?

Odpowiedź : para login + hasło

Pytanie A1.14 Czy aplikacja wykorzystuje dodatkowe metody autoryzacji wrażliwych operacji (np. przy pomocy kodów SMS, tokenów sprzętowych, tokenów mobilnych, certyfikatów kwalifikowanych, etc)? Are there any additional authorization methods implemented in the application for securing sensitive operations, like SMS codes, hardware tokens, mobile tokens, or qualified certificates?

Odpowiedź : tak, 2fa z kodem na adres email

Pytanie A1.15 Czy istnieje możliwość uzyskania dostępu do aplikacji przed złożeniem oferty (np. do wersji demo)? Can we obtain access to the application or a demo version prior to making a proposal?

Odpowiedź : nie

Ankieta nr 2 Ankieta wyceny testy penetracyjne: Testy infrastruktury LAN/WAN i sieci

Pytanie A2.1 Liczba domen/subdomen publicznych objętych testami. Number of public domains/subdomains covered by tests.

Odpowiedź: 1 domena, około 30 subdomen

Pytanie A2.2 Liczba adresów IP objętych testami z podziałem na publiczne i wewnętrzne, które będą objęte testami. The total count of IP addresses being tested, divided into public and internal categories, that are currently undergoing testing.

Odpowiedź : 20 publicznych/ 80 wewnętrznych

Pytanie A2.3 Liczba lokalizacji podlegająca audytowi (miasto). The number of locations subject to audit, divided by city.

odpowiedź : 1 lokalizacja

Pytanie A2.4 Liczba sieci WiFi dostępnych w lokalizacji (np. Gości/biuro) The number of WiFi networks available at a location (e.g., Guest/Office).

Odpowiedź : 1 sieć quest

Pytanie A2.5 Jaki jest pożądany termin wykonania audytu? What is the desired deadline for the audit?

Odpowiedź : okres wakacyjny

Pytanie A2.6 Liczba systemów wewnętrznych podlegających testom (np. SAP, ERP itd.)
The count of internal systems being tested, such as SAP, ERP, and others.

Odpowiedź : 20

Pytanie A2.7 Wdrożone systemy bezpieczeństwa np. IPS/IDS/EDR/inne
Implemented security systems, such as IPS/IDS/EDR/other.

Odpowiedź : Nie

Pytanie A2.8 Producent/modeli wykorzystywanych urządzeń sieciowych. In simpler terms, it means "The brands and specific models of network equipment in use.

Odpowiedź : Cisco, Juniper

Pytanie A2.9 Ilość VLANów w sieci wewnętrznej. The number of VLANs in the internal network.

Odpowiedź : 80

Pytanie A2.10 Czy sieć LAN jest podzielona na segmenty? (separacja sieci). Is the LAN segmented into different segments for network separation?

Odpowiedź : Tak

Pytanie A2.11 Ilość stacji roboczych/użytkowników. The number of workstations/users.

Odpowiedź : 500

Pytanie A2.12 Dodatkowe Additional information
odpowiedź : nie dotyczy

Ankieta nr 3 Ankieta wyceny testy penetracyjne : API

Pytanie A3.1 Jakiego typu jest to API (np. Webservice/SOAP, RESTful API, etc)?
What type of API is this (e.g., Webservice/SOAP, RESTful API, etc.)?

Odpowiedź : Brak realizacji testów penetracyjnych w tym zakresie

Pytanie A3.2 Ile endpointów/metod API będzie podlegać weryfikacji (np. POST /login, GET /profile - 2 endpointy/metody REST API)? How many API endpoints/methods will be subject of verification (e.g., POST /login, GET /profile - 2 REST API endpoints/methods)?

Odpowiedź : Brak realizacji testów penetracyjnych w tym zakresie

Pytanie A3.3 Czy możliwe jest dostarczenie przykładowych poprawnych wywołań endpointów/metod API (schema + poprawne wartości parametrów), np. w postaci kolekcji Postman, projektu SoapUI lub innym, równoważnym formacie? Is it possible to provide

examples of correct calls for the API endpoints/methods (schema + correct parameter values), e.g., in the form of a Postman collection, SoapUI project, or another equivalent format?

Odpowiedź : Brak realizacji testów penetracyjnych w tym zakresie

Pytanie A3.4 W jaki sposób zrealizowane jest uwierzytelnianie do API? How does the API handle authentication?

Odpowiedź : Brak realizacji testów penetracyjnych w tym zakresie

Pytanie A3.5 Czy możliwe są testy zdalne? Is it possible to conduct the tests remotely?

Odpowiedź : Brak realizacji testów penetracyjnych w tym zakresie

Pytanie A3.6 Na jakim środowisku będzie przeprowadzany audyt (testowe/produkcyjne)? Which environment will be used for the audit, test or production?

Odpowiedź : Brak realizacji testów penetracyjnych w tym zakresie

Pytanie A3.7 Czy są jakieś ograniczenia czasowe w trybie przeprowadzania audytu (np. godziny nocne, etc.)? Are there any time restrictions on conducting the audit (e.g., night hours, etc.)?

Odpowiedź : Brak realizacji testów penetracyjnych w tym zakresie

Pytanie A3.8 Jaki jest pożądany termin wykonania audytu? What is the desired deadline for the audit?

Odpowiedź : Brak realizacji testów penetracyjnych w tym zakresie

Pytanie A3.9 Czy oferta ma zawierać retesty (tj. powtórne sprawdzenie czy wskazane w raporcie z testów podatności zostały skutecznie usunięte przez Zamawiającego)? Should the offer include retests (i.e., a second check to determine if the vulnerabilities indicated in the test report have been successfully remediated by the client)?

Odpowiedź : Brak realizacji testów penetracyjnych w tym zakresie

Ankieta nr 4 Ankieta wyceny testy penetracyjne : DESKTOP

Pytanie A4.1 W jakiej technologii jest napisana aplikacja (np. C++/Java/C# etc.)? What technology was used to build the application (e.g., C++/Java/C# etc.)?

Odpowiedź: W zależności od producenta

Pytanie A4.2 Z ilu ekranów składa się aplikacja? How many interactive screens does the application have?

Odpowiedź: nie dotyczy

Pytanie A4.3 Czy możliwe są testy zdalne? Is it possible to conduct the tests remotely?

odpowiedź : tak

Pytanie A4.4 Na jakim środowisku będzie przeprowadzany audyt (testowe/produkcyjne)?
Which environment will be used for the audit, test or production?

Odpowiedź : test/produkcja

Pytanie A4.5 Czy są jakieś ograniczenia czasowe w trybie przeprowadzania audytu (np. godziny nocne, etc.)? Are there any time restrictions on conducting the audit (e.g., night hours, etc.)?

odpowiedź : brak

Pytanie A4.6 Jaki jest pożądany termin wykonania audytu? What is the desired deadline for the audit?

odpowiedź : okres wakacyjny

Pytanie A4.7 Czy oferta ma zawierać retesty (tj. powtórne sprawdzenie czy wskazane w raporcie z testów podatności zostały skutecznie usunięte przez Zamawiającego)?

Should the offer include retests (i.e., a second check to determine if the vulnerabilities indicated in the test report have been successfully remediated by the client)?

Odpowiedź : nie

Pytanie A4.8 W jaki sposób zrealizowane jest uwierzytelnianie do aplikacji (standardowa para login i hasło, certyfikaty, tokeny 2FA, etc)? What methods are used for user authentication in the application? Does it use a standard username and password, certificates, 2FA tokens, or other methods?

Odpowiedź : login, hasło , 2fa

Pytanie A4.9 Czy aplikacja wykorzystuje dodatkowe metody autoryzacji wrażliwych operacji (np. przy pomocy kodów SMS, tokenów sprzętowych, certyfikatów kwalifikowanych, etc)? Are there any additional authorization methods implemented in the application for securing sensitive operations, like SMS codes, hardware tokens, mobile tokens, or qualified certificates?

Odpowiedź :kody wysyłane na adres email

Pytanie A4.10 Czy audyt możliwy będzie do wykonania na stacji roboczej Wykonawcy np. na maszynie wirtualnej? Czy Zamawiający przekaze Wykonawcy pliki instalacyjne aplikacji?Is it possible to conduct the audit on the contractor's workstation, such as a virtual machine? Will the client supply the contractor with the application's installation files?

Odpowiedź : Tak

Pytanie A4.11 Czy możliwe będzie dostarczenie tzw Mocków które symulować będą urządzenia zewnętrzne? Is it possible provided application with mocks simulating external devices?

Odpowiedź : tak

Pytanie A4.12 Czy oferta ma zawierać retesty (tj. powtórne sprawdzenie czy wskazane w raporcie z testów podatności zostały skutecznie usunięte przez Zamawiającego)? Should the offer include retests (i.e., a second check to determine if the vulnerabilities indicated in the test report have been successfully remediated by the client)?

Odpowiedź : nie

Przedmiotowe odpowiedzi stanowią integralną część ogłoszenia o zamówieniu

Zamawiający
Zastępca Kanclerza AKF w Krakowie
mgr Piotr Słomiński