Ogłoszenie o wyniku postępowania
Usługi
Wykonanie audytu systemu bezpieczeństwa informacji SZBI wdrożonego w 14 jednostkach wraz z wykonaniem testów penetracyjnych w 3 jednostkach w ramach: Cyberbezpieczny samorząd w Gminie Czersk

SEKCJA I - ZAMAWIAJĄCY

1.1.) Rola zamawiającego
Postępowanie prowadzone jest samodzielnie przez zamawiającego

1.2.) Nazwa zamawiającego: GMINA CZERSK

1.4) Krajowy Numer Identyfikacyjny: REGON 092351274

1.5) Adres zamawiającego

1.5.1.) Ulica: ul. Kościuszki 27

1.5.2.) Miejscowość: Czersk

1.5.3.) Kod pocztowy: 89-650

1.5.4.) Województwo: pomorskie

1.5.5.) Kraj: Polska

1.5.6.) Lokalizacja NUTS 3: PL637 - Chojnicki

1.5.7.) Numer telefonu: 523954810

1.5.9.) Adres poczty elektronicznej: urzad_miejski@czersk.pl

1.5.10.) Adres strony internetowej zamawiającego: https://platformazakupowa.pl/pn/czersk

1.6.) Adres strony internetowej prowadzonego postępowania:
https://platformazakupowa.pl/pn/czersk

1.7.) Rodzaj zamawiającego: Zamawiający publiczny - jednostka sektora finansów publicznych - jednostka samorządu terytorialnego

1.8.) Przedmiot działalności zamawiającego: Ogólne usługi publiczne

SEKCJA II – INFORMACJE PODSTAWOWE

2.1.) Ogłoszenie dotyczy:

Zamówienia publicznego

2.2.) Ogłoszenie dotyczy usług społecznych i innych szczególnych usług: Nie

2.3.) Nazwa zamówienia albo umowy ramowej:
Wykonanie audytu systemu bezpieczeństwa informacji SZBI wdrożonego w 14 jednostkach wraz z wykonaniem testów penetracyjnych w 3 jednostkach w ramach: Cyberbezpieczny samorząd w Gminie Czersk

2.4.) Identyfikator postępowania: ocds-148610-0e7b5300-9ba2-4fd8-a646-69bc51cbfc88

2.5.) Numer ogłoszenia: 2026/BZP 00185154

2.6.) Wersja ogłoszenia: 01

2.7.) Data ogłoszenia: 2026-04-03

2.8.) Zamówienie albo umowa ramowa zostały ujęte w planie postępowań: Tak

2.9.) Numer planu postępowań w BZP: 2026/BZP 00026237/03/P

2.10.) Identyfikator pozycji planu postępowań:

1.3.7 Wykonanie audytu systemu bezpieczeństwa informacji SZBI wdrożonego w 14 jednostkach wraz z wykonaniem testów penetracyjnych w 3 jednostkach w ramach projektu pn. Cyberbezpieczny samorząd w Gm. Czersk

2.11.) Czy zamówienie albo umowa ramowa dotyczy projektu lub programu współfinansowanego ze środków Unii Europejskiej: Tak

2.12.) Nazwa projektu lub programu:
Zadanie finansowane z programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa konkurs grantowy w ramach Projektu grantowego „Cyberbezpieczny Samorząd” o numerze FERC.02.02-CS.01-001/23.

2.13.) Zamówienie/umowa ramowa było poprzedzone ogłoszeniem o zamówieniu/ogłoszeniem o zamiarze zawarcia umowy:
Tak

2.14.) Numer ogłoszenia: 2026/BZP 00134412

SEKCJA III – TRYB UDZIELENIA ZAMÓWIENIA LUB ZAWARCIA UMOWY RAMOWEJ

3.1.) Tryb udzielenia zamówienia wraz z podstawą prawną Zamówienie udzielane jest w trybie podstawowym na podstawie: art. 275 pkt 2 ustawy

SEKCJA IV – PRZEDMIOT ZAMÓWIENIA

4.1.) Numer referencyjny: ZP.271.5.2026

4.2.) Zamawiający udziela zamówienia w częściach, z których każda stanowi przedmiot odrębnego postępowania: Nie

4.3.) Wartość zamówienia: 126000,00 PLN

4.4.) Rodzaj zamówienia: Usługi

4.5.1.) Krótki opis przedmiotu zamówienia

Przedmiot zamówienia obejmuje: Wykonanie audytu systemu bezpieczeństwa informacji SZBI wdrożonego w 14 jednostkach wraz z wykonaniem testów penetracyjnych w 3 jednostkach w ramach projektu pn.: Cyberbezpieczny samorząd w Gminie Czersk.
I. JEDNOSTKI AUDYTOWANE:
1. Urząd Miejski w Czersku, ul. Kościuszki 27, 89-650 Czersk
2. AZK (Administracja Zasobów Komunalnych) w Czersku, ul. Tucholska 1, 89-650 Czersk
3. Centrum Usług Społecznych w Czersku, ul. Przytorowa 22, 89-650 Czersk
4. Gminne Centrum Kultury w Czersku, ul. Szkolna 11, 89-650 Czersk
5. Przedszkole Samorządowe nr 1 im. Kubusia Puchatka w Czersku, ul. Dąbrowskiego 4, 89-650 Czersk
6. Przedszkole Samorządowe nr 2 im. Jana Brzechwy w Czersku, ul. Chojnicka 5, 89-650 Czersk
7. Szkoła Podstawowa nr 1 im. Janusza Korczaka w Czersku , ul. Dworcowa 8, 89-650 Czersk
8. Szkoła Podstawowa nr 2 im. Jana Pawła II w Czersku, ul. Kościuszki 6, 89-650 Czersk
9. Szkoła Podstawowa w Gotelpiu Gotelp 12, 89-651 Gotelp
10. Środowiskowy Dom Samopomocy w Czersku, ul. Pomorska 12, 89-650 Czersk
11. Zespół Obsługi Finansowej, ul. Dworcowa 31 89-650 Czersk
12. Zespół Szkół w Łęgu, ul. Chojnicka 2A, 89-652 Łąg
13. Zespół Szkół w Rytlu, ul. Ks. Kowalkowskiego 6, 89-642 Rytel
14. Zespół Żłobków i Klubu Dziecięcego w Czersku, ul. Chojnicka 5A, 89-650 Czersk
II. ZAKRES PRAC AUDYTOWYCH

1. Przeprowadzenie:
1) audytu wdrożonego w Jednostce systemu bezpieczeństwa informacji SZBI,
2) analizę efektywności działań w zakresie monitorowania, pomiarów, analizy i oceny SZBI, w tym przegląd wskaźników ryzyka i zgodności.
2. Audyt powinien obejmować:

1) Analiza wstępna i określenie zakresu audytu
a) Zdefiniowanie obszarów, lokalizacji oraz jednostek organizacyjnych objętych SZBI.
b) Weryfikacja ewidencji obszaru przetwarzania informacji, w tym dokładność danych dotyczących lokalizacji, kondygnacji i adresów.
c) Sprawdzenie, czy zakres SZBI jest zgodny z wymaganiami norm ISO/IEC 27001 oraz potrzebami organizacji.

2) Weryfikacja dokumentacji systemowej
a) Wprowadzenie do SZBI: Ocena, czy dokumentacja zawiera podstawowe zasady zarządzania bezpieczeństwem informacji i zgodność z cyklem PDCA (Plan-Do-Check-Act).
b) Terminy i definicje: Sprawdzenie, czy wszystkie istotne pojęcia są zdefiniowane i zgodne z normami.
c) Kontekst organizacji: Analiza czynników wewnętrznych i zewnętrznych oraz ich wpływu na SZBI, w tym analiza ryzyk.

3) Zarządzanie ryzykiem
a) Ocena procesu identyfikacji i analizy ryzyk, w tym dokumentacji dotyczącej szacowania ryzyk.
b) Analiza działań zaradczych i korygujących dla zidentyfikowanych ryzyk.

4) Zabezpieczenia i deklaracja stosowania
a) Weryfikacja, czy deklaracja stosowania zabezpieczeń jest zgodna z Załącznikiem A normy ISO/IEC 27001.
b) Ocena skuteczności wdrożonych zabezpieczeń oraz uzasadnienia ewentualnych wyłączeń.

5) Dokumentacja operacyjna
a) Polityki i procedury: Sprawdzenie polityk bezpieczeństwa (np. kryptografii, zarządzania dostępem, bezpieczeństwa zasobów ludzkich) i ich zgodności z wymaganiami normatywnymi.
b) Ewidencje i rejestry: Ocena kompletności i aktualności ewidencji aktywów, obszarów przetwarzania informacji oraz rejestrów incydentów i zgłoszeń.
c) Zarządzanie dostępem: Sprawdzenie procedur przyznawania, zmiany i odbierania dostępu oraz zgodności z dokumentacją.

6) Zarządzanie incydentami i ciągłością działania
a) Ocena polityki zarządzania incydentami, w tym procedur zgłaszania, oceny i reagowania na incydenty.
b) Sprawdzenie planów zarządzania ciągłością działania i odtwarzania po katastrofie, w tym testów i analiz RTO, RPO, MTPD i MBCO.

7) Zgodność z przepisami i ochroną danych osobowych
a) Ocena dokumentacji dotyczącej przetwarzania danych osobowych, w tym zgodności z RODO.

8) Dokumentacja operacyjna
a) Analiza polityk i procedur dotyczących korzystania z systemów, urządzeń i sieci.
b) Weryfikacja zasad postępowania z nośnikami informacji, tworzenia haseł i korzystania z Internetu oraz poczty elektronicznej.

9) Zarządzanie dostawcami
a) Sprawdzenie polityk i procedur związanych z bezpieczeństwem informacji w relacjach z dostawcami.

10) Zgodność z wymaganiami prawnymi
a) Weryfikacja dokumentacji dotyczącej monitorowania i przestrzegania wymagań prawnych, regulacyjnych i umownych.
b) Analiza zgodności z politykami zgodności oraz audytami technicznymi.

III. DO ZADAŃ WYKONAWCY AUDYTU BĘDZIE NALEŻEĆ:

1. Przeprowadzenie szczegółowej analizy i oceny SZBI, obejmującej:
1) Identyfikację niezgodności i słabości w dokumentacji oraz wdrożeniu systemu.
2) Przeprowadzenie wywiadów z wybranym personelem, w tym z Burmistrzem, Zastępcą Burmistrza, Sekretarzem i Pełnomocnikiem ds. Bezpieczeństwa Informacji.

2. Przekazanie dla Kierownika/Dyrektora Jednostki oraz dla Zamawiającego podpisanego przez audytora raportu z audytu wdrożonego w Jednostce systemu bezpieczeństwa informacji SZB.

3. Wykonawca udokumentuje wykonanie zadania poprzez okazanie protokołu odbioru.

IV. UPRAWNIENIA DO PRZEPROWADZENIA AUDYTU

1. Potencjał kadrowy Wykonawcy: osoba/-y, która/-e będzie/będą wykonywały audyt - posiada/-ją przynajmniej jeden z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U.2018 poz. 1999):
1) Certified Internal Auditor (CIA);
2) Certified Information System Auditor (CISA);
3) Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób;
4) Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r.
o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;
5) Certified Information Security Manager (CISM);
6) Certified in Risk and Information Systems Control (CRISC);
7) Certified in the Governance of Enterprise IT (CGEIT);
8) Certified Information Systems Security Professional (CISSP);
9) Systems Security Certified Practitioner (SSCP);

10) Certified Reliability Professional;
11) Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert

2. Zamawiający zastrzega możliwość weryfikacji uprawnień audytorów (ważności uprawnień, akredytacja jednostki wydającej uprawnienia).
I. TESTY PENETRACYJNE

Jednostki podlegające testom penetracyjnym:
1. Urząd Miejski w Czersku , ul. Kościuszki 27, 89-650 Czersk
2. Centrum Usług Społecznych w Czersku, ul. Przytorowa 22, 89-650 Czersk
3. Zespół Obsługi Finansowej, ul. Dworcowa 31 89-650 Czersk
Wykonawca posiada potencjał techniczny i osobowy niezbędny do wykonania zamówienia.
Potencjał techniczny przedstawia się poprzez posiadanie narzędzi takich jak automatyczny skaner podatności posiadający funkcje pozwalające na:
1) wykonanie skanowań z wykorzystaniem wbudowanych szablonów;
2) skanowanie sieciowe (wykrywanie otwartych portów i rozpoznanie uruchomionych na nich usług, wskazywanie listy podatności na wykryte usługi);
3) weryfikacje domyślnych haseł według zadanego słownika;
4) skanowanie systemów operacyjnych z uwierzytelnieniem (sprawdzenie wersji systemu, zainstalowanych na nim aplikacji, brakujących aktualizacji, wskazywanie listy podatności na wykryte systemy i aplikacje) oraz weryfikację uprawnień zadanego użytkownika;
5) ustawienia harmonogramu skanowań;
6) możliwość porównania wyników poszczególnych skanowań;
7) możliwość konfigurowania zawartości raportu ze skanowania oraz dobieranie różnych formatów wyjściowych raportów (w tym HTML, CVS i XML);
8) możliwość wyświetlania wyników na bieżąco oraz możliwość grupowania podobnej klasy podatności
i możliwość sortowania po IP i podatnościach.

Aplikacje do testów stron i aplikacji internetowych posiadającej funkcje pozwalające na:
1) przechwytywanie wszystkich zapytań i odpowiedzi pomiędzy przeglądarką a aplikacją docelową, nawet gdy używany jest HTTPS;
2) przeglądanie, edytowanie oraz upuszczanie pojedynczych wiadomości, w celu manipulacji komponentami aplikacji po stronie serwera lub klienta;
3) dodawanie adnotacji do poszczególnych elementów w celu ich oznaczenia do późniejszego sprawdzenia;
4) wykonywanie różnych automatycznych modyfikacji odpowiedzi w calu ułatwienia testowania;
5) tworzenie reguł dopasowywania i zastępowania do automatycznego stosowania własnych modyfikacji do żądań i odpowiedzi przechodzących przez serwer Proxy;
6) precyzyjna konfiguracja reguł przechwytywania wiadomości;
7) możliwość wyeliminowania ostrzeżeń bezpieczeństwa przeglądarki, mogących się pojawiać podczas przechwytywania połączeń HTTPS;
8) pokazanie całej zawartości odkrytej podczas testowania umieszczana na mapie skanowanej witryny. Treść prezentowana w widoku drzewa, odpowiadającego strukturze stron URL;
9) żądania i odpowiedzi dostępne w edytorze http;
10) narzędzie do ręcznej edycji i ponownego wstawiania żądań;
11) narzędzie do analizy statystycznej tokenów sesji;
12) możliwość zapisu pracy na poszczególnych etapach w czasie rzeczywistym oraz powrót do zapisanego miejsca;
13) biblioteka konfiguracji do szybkiego uruchomienia ukierunkowanego skanowania z różnymi ustawieniami;
14) możliwość ręcznego umieszczania punktów wstawiania w dowolnych miejscach żądania, w celu poinformowania skanera o niestandardowych formatach danych i wejściach;
15) skanowanie na żywo podczas przeglądania, zapewniające pełną kontrolę nad działaniami wykonywanymi dla żądań;
16) możliwość analizy docelowej aplikacji internetowych.
17) narzędzie do automatycznego przechwytywania szczegółowych wyników o niestandardowych atakach na aplikacje.
UWAGA. W związku z ograniczoną liczbą znaków pełen opis przedmiotu zamówienia znajduje się w zał. nr 6 do SWZ

4.5.3.) Główny kod CPV: 72800000-8 - Usługi audytu komputerowego i testowania komputerów

SEKCJA V ZAKOŃCZENIE POSTĘPOWANIA

5.1.) Postępowanie zakończyło się zawarciem umowy albo unieważnieniem postępowania: Postępowanie/cześć postępowania zakończyła się zawarciem umowy

SEKCJA VI OFERTY

6.1.) Liczba otrzymanych ofert lub wniosków: 3

6.1.1.) Liczba otrzymanych ofert wariantowych: 0

6.1.2.) Liczba ofert dodatkowych: 0

6.1.3.) Liczba otrzymanych od MŚP: 3

6.1.4.) Liczba ofert wykonawców z siedzibą w państwach EOG innych niż państwo zamawiającego: 0

6.1.5.) Liczba ofert wykonawców z siedzibą w państwie spoza EOG: 0

6.1.6.) Liczba ofert odrzuconych, w tym liczba ofert zawierających rażąco niską cenę lub koszt: 0

6.1.7.) Liczba ofert zawierających rażąco niską cenę lub koszt: 0

6.2.) Cena lub koszt oferty z najniższą ceną lub kosztem: 54587,40 PLN

6.3.) Cena lub koszt oferty z najwyższą ceną lub kosztem: 154980,00 PLN

6.4.) Cena lub koszt oferty wykonawcy, któremu udzielono zamówienia: 54587,40 PLN

6.5.) Do wyboru najkorzystniejszej oferty zastosowano aukcję elektroniczną: Nie

6.6.) Oferta wybranego wykonawcy jest ofertą wariantową: Nie

SEKCJA VII WYKONAWCA, KTÓREMU UDZIELONO ZAMÓWIENIA

7.1.) Czy zamówienie zostało udzielone wykonawcom wspólnie ubiegającym się o udzielenie zamówienia: Nie

7.2.) Wielkość przedsiębiorstwa wykonawcy: Średni przedsiębiorca

7.3.) Dane (firmy) wykonawcy, któremu udzielono zamówienia:

7.3.1) Nazwa (firma) wykonawcy, któremu udzielono zamówienia: TestArmy Group SA

7.3.2) Krajowy Numer Identyfikacyjny: 8992754194

7.3.3) Ulica: Petuniowa

7.3.4) Miejscowość: Wrocław

7.3.5) Kod pocztowy: 53-238

7.3.6.) Województwo: dolnośląskie

7.3.7.) Kraj: Polska

7.4.) Czy wykonawca przewiduje powierzenie wykonania części zamówienia podwykonawcom?: Nie

SEKCJA VIII UMOWA

8.1.) Data zawarcia umowy: 2026-04-02

8.2.) Wartość umowy/umowy ramowej: 54587,40 PLN

8.3.) Okres realizacji zamówienia albo umowy ramowej:
do 2026-05-29