Załącznik nr 1 do Zamówienia – szczegółowy opis

**Szczegółowy opis przedmiotu zamówienia**

1. **zamówienie obejmuje 5 zadań do wykonania:**

**Zadanie 1:**

1. Wykonanie audytu wstępnego systemu zarządzania bezpieczeństwem informacji (SZBI)   
   w Urzędzie (Urząd Miejski w Orzyszu, ul. Rynek 3, 12-250 Orzysz)
2. Przeprowadzenie 6 audytów wstępnych Systemu Zarządzania Bezpieczeństwem Informacji w podległych jednostkach samorządu terytorialnego (JST):
3. Zespół Szkolno-Przedszkolny w Orzyszu, ul. Wojska Polskiego 14, 12-250 Orzysz,
4. Zespół Szkolno-Przedszkolny w Okartowie, Okartowo 22, 12-250 Orzysz,
5. Zespół Szkolno-Przedszkolny w Dąbrówce, Dąbrówka 40,12-250 Orzysz,
6. Miejski Ośrodek Sportu i Rekreacji w Orzyszu, ul. Osiedle Robotnicze 11A,12-250 Orzysz,
7. Miejski Ośrodek Pomocy Społecznej w Orzyszu, ul. Rynek 3, 12-250 Orzysz,
8. Środowiskowy Dom Samopomocy, ul. Wojska Polskiego 17B 12-250 Orzysz.

**Zadanie 2:**

1. Opracowanie nowych polityk i aktualizacja dokumentacji w ramach opracowania i wdrożenia SZBI w Urzędzie Miejskim w Orzyszu,
2. Opracowanie nowych polityk i aktualizacja dokumentacji w ramach opracowania i wdrożenia SZBI w 6 podległych jednostkach:
3. Zespół Szkolno-Przedszkolny w Orzyszu,
4. Zespół Szkolno-Przedszkolny w Okartowie,
5. Zespół Szkolno-Przedszkolny w Dąbrówce,
6. Miejski Ośrodek Sportu i Rekreacji w Orzyszu,
7. Miejski Ośrodek Pomocy Społecznej w Orzyszu,
8. Środowiskowy Dom Samopomocy)

**Zadanie 3:**

1. Przeprowadzenie szkoleń z zakresu bezpieczeństwa informacji oddzielnie:

a) dla kadry zarządzającej Urzędu Miejskiego w Orzyszu.

b) dla pozostałych pracowników Urzędu Miejskiego w Orzyszu.

2. Przeprowadzenie 6 odrębnych szkoleń z zakresu bezpieczeństwa informacji:

a) dla kadry zarządzającej jednostek podległych; (Zespół Szkolno-Przedszkolny w Orzyszu, Zespół Szkolno-Przedszkolny w Okartowie, Zespół Szkolno-Przedszkolny w Dąbrówce, Miejski Ośrodek Sportu i Rekreacji w Orzyszu, Miejski Ośrodek Pomocy Społecznej w Orzyszu, Środowiskowy Dom Samopomocy)

b) dla pozostałych pracowników podległych jednostek samorządu terytorialnego; (Zespół Szkolno-Przedszkolny w Orzyszu, Zespół Szkolno-Przedszkolny w Okartowie, Zespół Szkolno-Przedszkolny w Dąbrówce, Miejski Ośrodek Sportu i Rekreacji w Orzyszu, Miejski Ośrodek Pomocy Społecznej w Orzyszu, Środowiskowy Dom Samopomocy)

**Zadanie 4:**

1. Przeprowadzenie szkoleń z zakresu cyberbezpieczństwa dla pracowników Urzędu Miejskiego w Orzyszu
2. Przeprowadzenie 6 odrębnych szkoleń z zakresu cyberbezpieczństwa dla pracowników podległych jednostek samorządu terytorialnego. (Zespół Szkolno-Przedszkolny w Orzyszu, Zespół Szkolno-Przedszkolny w Okartowie, Zespół Szkolno-Przedszkolny w Dąbrówce, Miejski Ośrodek Sportu i Rekreacji w Orzyszu, Miejski Ośrodek Pomocy Społecznej w Orzyszu, Środowiskowy Dom Samopomocy)

**Zadanie 5:**

1. Przeprowadzenie audytu końcowego Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w Urzędzie; (Urząd Miejski w Orzyszu, ul. Rynek 3, 12-250 Orzysz)
2. Przeprowadzenie 6 audytów końcowych Systemu Zarządzania Bezpieczeństwem Informacji w podległych jednostkach samorządu terytorialnego (JST).
3. Zespół Szkolno-Przedszkolny w Orzyszu, ul. Wojska Polskiego 14, 12-250 Orzysz,
4. Zespół Szkolno-Przedszkolny w Okartowie, Okartowo 22, 12-250 Orzysz,
5. Zespół Szkolno-Przedszkolny w Dąbrówce, Dąbrówka 40,12-250 Orzysz,
6. Miejski Ośrodek Sportu i Rekreacji w Orzyszu, ul. Osiedle Robotnicze 11A,12-250 Orzysz,
7. Miejski Ośrodek Pomocy Społecznej w Orzyszu, ul. Rynek 3, 12-250 Orzysz,
8. Środowiskowy Dom Samopomocy, ul. Wojska Polskiego 17B 12-250 Orzysz.
9. **Jednostki objęte zamówieniem:**
10. Urząd Miejski w Orzyszu, ul. Rynek 3, 12-250 Orzysz
11. Zespół Szkolno-Przedszkolny w Orzyszu, ul. Wojska Polskiego 14, 12-250 Orzysz,
12. Zespół Szkolno-Przedszkolny w Okartowie, Okartowo 22, 12-250 Orzysz,
13. Zespół Szkolno-Przedszkolny w Dąbrówce, Dąbrówka 40,12-250 Orzysz,
14. Miejski Ośrodek Sportu i Rekreacji w Orzyszu, ul. Osiedle Robotnicze 11A,12-250 Orzysz,
15. Miejski Ośrodek Pomocy Społecznej w Orzyszu, ul. Rynek 3, 12-250 Orzysz,
16. Środowiskowy Dom Samopomocy, ul. Wojska Polskiego 17B 12-250 Orzysz.
17. **Liczba osób objętych szkoleniami:**

40 pracowników Urzędu Miejskiego w Poniatowej

40 pracowników podległych JST

1. **Ilość stacji roboczych:** 73 szt.
2. **Ilość serwerów:** 3 szt.
3. **Ilość urządzeń sieciowych:** 27 szt.
4. **SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA DLA ZADANIA NR 1:**
5. **Szczegółowe wymagania dotyczące audytów wstępnych SZBI**:
   1. **Liczba jednostek objętych audytami wstępnymi:** 7 (Urząd oraz 6 podległych JST)
   2. **Miejsce przeprowadzenia audytów:** Urząd Miejski w Orzyszu oraz siedziba każdej jednostki.
   3. Ilość wszystkich stacji roboczych: 73 szt.
   4. Ilość wszystkich serwerów: 3 szt.
   5. Ilość wszystkich urządzeń sieciowych: 27 szt.
   6. Zakres audytów wstępnych:
      1. **Ocena poziomu bezpieczeństwa organizacyjnego** związanego z posiadaną dokumentacją i procedurami.
      2. **Ocena poziomu bezpieczeństwa technicznego** związanego z posiadaną infrastrukturą, jej funkcjonowaniem i wydajnością.
      3. **Przeprowadzenie testów penetracyjnych** obejmujących testy styku sieci lokalnej z Internetem (Analiza topologii brzegu sieci, Weryfikacja mechanizmów ochronnych, Próba wykrycia usług sieciowych udostępnianych do Internetu, Detekcja wersji oraz typu oprogramowania dostępnego z sieci Internet, Exploitacja dostępnych urządzeń oraz usług wystawionych do sieci Internet.
      4. **Przeprowadzenie testów penetracyjnych** ze stacji roboczej podłączonej do wewnętrznego systemu informatycznego (Analiza topologii sieci LAN, Weryfikacja mechanizmów ochronnych w sieci, Analiza komunikacji sieciowej, Skanowanie portów TCP/UDP i próba wykrycia usług sieciowych, Skanowanie hostów aktywnych w sieci, Exploitacja dostępnych urządzeń oraz usług w sieci LAN.
   7. Zakres przeprowadzanych audytów w oparciu o przepisy i normy:
      1. Rozporządzenie 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.
      2. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.
      3. Ustawa o krajowym systemie cyberbezpieczeństwa.
      4. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679
      5. Normy ISO 27001.
   8. Raporty z audytów wstępnych muszą zawierać informacje o stanie aktualnym, stwierdzonych uchybieniach oraz zalecenia pokontrolne.
   9. **Forma przekazania i omówienia raportów:** Spotkania w siedzibach każdej JST, podczas których wyniki audytów zostaną omówione z kadrą kierowniczą.
   10. **Wymagania dla wykonawcy:**
       1. Wykonawca musi posiadać co najmniej 2 certyfikaty potwierdzające kwalifikacje do przeprowadzenia audytów SZBI zgodnie z Rozporządzeniem Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu.
       2. Wykonawca musi posiadać co najmniej 3 letnie, udokumentowane doświadczenie w przeprowadzaniu audytów SZBI i testów penetracyjnych oraz w opracowywaniu raportów pokontrolnych.
       3. Zespół kontrolny musi składać się z co najmniej 2 audytorów posiadających doświadczenie zawodowe i udokumentowaną wiedzę zarówno w kwestiach organizacyjno-prawnych w zakresie audytowania systemów zarządzania bezpieczeństwem informacji, jak i technicznych aspektów bezpieczeństwa IT w zakresie wykonywania testów penetracyjnych, co dodatkowo zostanie potwierdzone certyfikatem branżowym lub wykształceniem np. w postaci dyplomu ukończenia szkoły wyższej o kierunkach związanych z bezpieczeństwem informacji oraz informatyką.
   11. Terminy realizacji zamówienia: Zgodnie z projektem umowy.
6. **SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA DLA ZADANIA NR 2:**

**Opracowanie nowych polityk i aktualizacja dokumentacji w ramach wdrożenia SZBI**

* 1. Liczba jednostek objętych zamówieniem: 7 (Urząd Miejski w Orzyszu oraz 6 podległych JST).
  2. Obecny stan dokumentacji SZBI: Wymagane jest opracowanie nowych polityk oraz aktualizacja istniejącej dokumentacji.
  3. Podział dokumentacji: Wymagany jest podział dokumentacji na 4 części (Polityka Bezpieczeństwa Informacji, Polityka Bezpieczeństwa Danych Osobowych, Polityka Bezpieczeństwa Systemów Informatycznych, Polityka Bezpieczeństwa Fizycznego)
  4. **Obszary które powinny zostać objęte szczególnym uwzględnieniem w dokumentacji:**

1. Cel i zakres polityk w kontekście bezpieczeństwa informacji (BI);
2. Role i odpowiedzialności pracowników w zakresie BI;
3. Zarządzanie ryzykiem w obszarze BI;
4. Procedury zarządzania incydentami BI;
5. Deklarację stosowania zabezpieczeń;
6. Kontrole dostępu do informacji i zasobów;
7. Procedury związane z tworzeniem i prowadzeniem aktyw informacyjnych;
8. Zasady pracy na odległość i mobilny dostęp do informacji;
9. Bezpieczeństwo fizyczne pomieszczeń i obiektów związanych z BI;
10. Bezpieczeństwo fizyczne nośników informacji;
11. Bezpieczeństwo infrastruktury wspomagającej;
12. Inwentaryzacja systemów informacyjnych;
13. Zarządzanie bezpieczeństwem i ciągłością działania łańcuch dostaw;
14. Projektowanie i wdrażanie systemów teleinformatycznych;
15. Kopie zapasowe i zarządzanie ciągłością działania;
16. Sprzęt komputerowy, oprogramowanie strategiczne systemy i aplikacje;
17. Serwery, informatyczna sieć wewnętrzna;
18. Rozliczalność działań w systemach informatycznych;
19. Procedury uwzględnienia BI w procesach planowania i zarządzania ciągłością działania;
20. Procedury bezpieczeństwa informacji w relacjach z dostawcami;
21. Okresowe szkolenia i podnoszenie świadomości pracowników z zakresu BI;
22. Cykliczne audyty i monitorowanie SZBI.
    1. Dokumentacja musi zostać opracowana z uwzględnieniem przepisów RODO, ISO 27001, ustawy o krajowym systemie cyberbezpieczeństwa oraz rozporządzenia w sprawie krajowych ram interoperacyjności.
    2. Indywidualizacja dokumentacji Dokumentacja musi być opracowana z uwzględnieniem wymagań i potrzeb stron zainteresowanych (wewnętrznych i zewnętrznych), indywidualnie dla każdej jednostki i opracowana na podstawie przepisów oraz informacji udzielonych przez pracowników podczas spotkań projektowych.
    3. Wymagania dotyczące spotkań projektowych Liczba spotkań projektowych w każdej jednostce wynosi minimum 2-3 udokumentowane spotkania z kadrą kierowniczą. Spotkania te mają na celu zebranie informacji niezbędnych do opracowania indywidualnych procedur oraz omówienie specyficznych potrzeb i wymagań każdej jednostki.
    4. Termin zakończenia prac nad dokumentacją: Zgodnie z projektem umowy
    5. Raportowanie i zatwierdzenie dokumentacji:
       1. Po opracowaniu dokumentacji, wykonawca przekaże projekt do zatwierdzenia kierownictwu każdej jednostki.
       2. W przypadku zgłoszenia zmian lub poprawek wykonawca zobligowany jest do naniesienia poprawek lub przedstawienia pisemnych wyjaśnień w ciągu 14 dni.
    6. Aktualizacja dokumentacji: Wykonawca zobligowany jest do przeglądu i aktualizacji opracowanej dokumentacji po zrealizowaniu i wdrożeniu zakupów objętych projektem Cyberbezpieczny samorząd na wezwanie Zamawiającego w terminie 14 dni od otrzymania wezwania.
23. **SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA DLA ZADANIA NR 3:**
24. Szczegółowe wymagania dotyczące szkoleń z zakresu bezpieczeństwa informacji
    1. Zakres i cel szkoleń:
       1. Szkolenie będzie obejmowało szczegółowe omówienie opracowanej dokumentacji SZBI.
       2. Celem szkoleń jest zwiększenie świadomości pracowników, zapewnienie zgodności z przepisami oraz wdrożenie nowych procedur bezpieczeństwa informacji.
       3. Szkolenia obejmują tematykę związaną z RODO, bezpieczeństwem informacji, zarządzaniem incydentami, korzystaniem z urządzeń mobilnych, postępowaniem z nośnikami danych, kontrolą dostępu, zabezpieczaniem pomieszczeń i obiektów, czystym biurkiem, czystym ekranem, wykonywaniem kopii zapasowych, ochroną logów, bezpieczeństwem komunikacji, zarządzaniem bezpieczeństwem sieci, przesyłaniem informacji, opracowywaniem planów ciągłości działania, zarządzaniem incydentami bezpieczeństwa informacji, ochroną danych osobowych, szacowaniem ryzyka w obszarze bezpieczeństwa informacji oraz okresowymi szkoleniami personelu.
    2. Liczba uczestników i grup szkoleniowych:
       1. Całkowita liczba uczestników Urząd: 40
       2. Całkowita liczba uczestników JST: 40
       3. Liczba grup szkoleniowych: Minimum 2-3 grupy na każdą jednostkę aby uniknąć dezorganizacji normalnej pracy każdej jednostki.
       4. Podział na grupy: Kadra zarządzająca oraz pracownicy administracyjni i techniczni.
    3. Forma szkoleń:
       1. Szkolenia stacjonarne w siedzibach każdej jednostki oraz Urzędu.
       2. Metody szkoleniowe: wykłady, warsztaty, ćwiczenia praktyczne.
       3. Czas trwania szkolenia dla jednej grupy: 3 - 4 godziny.
       4. Szkolenia odbywać się będą od poniedziałku do piątku w godzinach 8:00-15:00.
    4. Materiały szkoleniowe:
       1. Wykonawca zapewni materiały szkoleniowe w formie prezentacji, ćwiczeń oraz podręczników.
       2. Materiały będą dostępne zarówno w formie drukowanej, jak i elektronicznej.
    5. Wymagania dotyczące wykonawcy
       1. Trenerzy muszą posiadać odpowiednie kwalifikacje i doświadczenie w prowadzeniu szkoleń z zakresu bezpieczeństwa informacji.
       2. Preferowane certyfikaty i akredytacje trenerów.
       3. Wykonawca musi posiadać certyfikat firmy szkoleniowej lub udokumentować przynależność do branżowych organizacji szkoleniowych.
    6. Konspekt szkolenia:
       1. Wykonawca opracuje szczegółowy konspekt szkolenia i przedstawi do akceptacji zamawiającemu.
       2. Zamawiający zastrzega sobie prawo do zmiany, uwagi i sugestii dotyczących programu szkolenia
    7. Ewaluacja szkoleń:
       1. Wykonawca zapewni ewaluację szkoleń poprzez testy wiedzy i ankiety satysfakcji uczestników.
       2. Wymagane jest przeprowadzenie pretestu przed rozpoczęciem szkolenia w celu oceny początkowego poziomu wiedzy uczestników.
       3. Wymagane jest przeprowadzenie posttestu po zakończeniu szkolenia w celu oceny zdobytej wiedzy i efektywności szkolenia.
       4. Wyniki ewaluacji będą uwzględnione w końcowym raporcie.
       5. Po zakończeniu szkolenia każdy uczestnik otrzyma certyfikat uwzględniający zakres szkolenia oraz potwierdzający udział i zdobyte umiejętności.
    8. Termin szkolenia: Zgodnie z projektem umowy.
25. **SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA DLA ZADANIA NR 4:**
26. Szczegółowe wymagania dotyczące szkoleń z zakresu cyberbezpieczeństwa
    1. Zakres i cel szkoleń:
       1. Celem szkoleń jest zwiększenie świadomości zagrożeń, edukowanie uczestników o aktualnych zagrożeniach cybernetycznych, takich jak phishing, ransomware, malware, ataki DDoS i inne rodzaje cyberataków. Zrozumienie, jak te zagrożenia mogą wpływać na organizację oraz jakie mogą być konsekwencje ich wystąpienia.
       2. Minimalny zakres tematyczny szkoleń musi nawiązywać do wprowadzenia do zagadnień związanych z cyberbezpieczeństwem, zarządzanie incydentami bezpieczeństwa cyfrowego, ochrona przed zagrożeniami cyfrowymi, bezpieczeństwo sieci i infrastruktury IT, zarządzanie hasłami i uwierzytelnianiem, bezpieczne korzystanie z urządzeń mobilnych , postępowanie z nośnikami danych, tworzenie i zarządzanie kopiami zapasowymi, ochrona logów systemowych, zarządzanie bezpieczeństwem sieci, przesyłanie informacji, szacowanie ryzyka w obszarze bezpieczeństwa informacji
    2. Liczba uczestników i grup szkoleniowych:
       1. Całkowita liczba uczestników Urząd: 40
       2. Całkowita liczba uczestników JST: 40
    3. Liczba grup szkoleniowych: Minimum 2-3 grupy na każdą jednostkę aby uniknąć dezorganizacji normalnej pracy każdej jednostki.
    4. Forma szkoleń:
       1. Szkolenia stacjonarne w siedzibach każdej jednostki oraz Urzędu.
       2. Metody szkoleniowe: Wykłady, warsztaty, ćwiczenia praktyczne.
       3. Czas trwania szkolenia dla jednej grupy: 3 - 4 godziny.
       4. Szkolenia odbywać się będą od poniedziałku do piątku w godzinach 8:00-15:00.
    5. Materiały szkoleniowe:
       1. Wykonawca zapewni materiały szkoleniowe w formie prezentacji, ćwiczeń oraz podręczników.
       2. Materiały będą dostępne zarówno w formie drukowanej, jak i elektronicznej.
    6. Wymagania dotyczące kwalifikacji trenerów:
       1. Trenerzy muszą posiadać odpowiednie kwalifikacje i doświadczenie w prowadzeniu szkoleń z cyberbezpieczeństwa.
       2. Preferowane certyfikaty i akredytacje trenerów.
       3. Wykonawca musi posiadać certyfikat firmy szkoleniowej lub udokumentować przynależność do branżowych organizacji szkoleniowych.
    7. Konspekt szkolenia:
       1. Wykonawca opracuje szczegółowy konspekt szkolenia i przedstawi do akceptacji zamawiającemu.
       2. Zamawiający zastrzega sobie prawo do zmiany, uwagi i sugestii dotyczących programu szkolenia
    8. Ewaluacja szkoleń:
       1. Wykonawca zapewni ewaluację szkoleń poprzez testy wiedzy i ankiety satysfakcji uczestników.
       2. Wymagane jest przeprowadzenie pretestu przed rozpoczęciem szkolenia w celu oceny początkowego poziomu wiedzy uczestników.
       3. Wymagane jest przeprowadzenie posttestu po zakończeniu szkolenia w celu oceny zdobytej wiedzy i efektywności szkolenia.
       4. Wyniki ewaluacji będą uwzględnione w końcowym raporcie.
       5. Po zakończeniu szkolenia każdy uczestnik otrzyma certyfikat uwzględniający zakres szkolenia oraz potwierdzający udział i zdobyte umiejętności.
    9. Termin szkolenia: Zgodnie z projektem umowy.
27. **SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA DLA ZADANIA NR 5:**
28. **Szczegółowe wymagania dotyczące audytów końcowych**:
    1. **Liczba jednostek objętych audytami końcowymi:** 7 (Urząd Miejski w Orzyszu oraz 6 podległych JST).
    2. **Miejsce przeprowadzenia audytów końcowych:** Urząd Miejski w Orzyszu oraz siedziba każdej JST.
    3. Zakres audytów końcowych:
       1. **Ocena poziomu bezpieczeństwa organizacyjnego** związanego z posiadaną dokumentacją i procedurami.
       2. **Ocena poziomu bezpieczeństwa technicznego** związanego z posiadaną infrastrukturą, jej funkcjonowaniem i wydajnością.
       3. **Przeprowadzenie testów obejmujących konfigurację zakupionych w ramach projektu grantowego urządzeń i oprogramowania zwiększającego poziom bezpieczeństwa cyfrowego**
    4. Zakres przeprowadzanych audytów na podstawie przepisów:
       1. Rozporządzenie 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.
       2. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.
       3. Ustawa o krajowym systemie cyberbezpieczeństwa.
       4. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679
       5. Normy ISO 27001.
    5. Raporty z audytów końcowych muszą zawierać co najmniej informacje o tym jak zakupy w ramach projektu wpłynęły na poprawę bezpieczeństwa informacji i cyberbezpieczeństwa w jednostce.
    6. **Forma przekazania i omówienia raportów:** Spotkania w siedzibach Urzędu oraz podległych JST, podczas których wyniki audytów zostaną omówione z kadrą kierowniczą.
    7. **Wymagania dla wykonawcy:**
       1. Wykonawca musi posiadać co najmniej 2 certyfikaty potwierdzające kwalifikacje do przeprowadzenia audytów SZBI zgodnie z Rozporządzeniem Ministra Cyfryzacji z dnia 12 października 2018 r.
       2. Wykonawca musi posiadać co najmniej 3 letnie, udokumentowane doświadczenie w przeprowadzaniu audytów SZBI i testów penetracyjnych oraz w opracowywaniu raportów pokontrolnych.
       3. Zespół kontrolny musi składać się z co najmniej 2 audytorów posiadających doświadczenie zawodowe i udokumentowaną wiedzę zarówno w kwestiach organizacyjno-prawnych w zakresie audytowania systemów zarządzania bezpieczeństwem informacji, jak i technicznych aspektów bezpieczeństwa IT w zakresie wykonywania testów penetracyjnych, co dodatkowo zostanie potwierdzone certyfikatem branżowym lub wykształceniem np. w postaci dyplomu ukończenia szkoły wyższej o kierunkach związanych z bezpieczeństwem informacji oraz informatyką.
    8. Terminy realizacji zamówienia: Zgodnie z projektem umowy.