OPIS PRZEDMIOTU ZAMÓWIENIA

Świadczenie usług w zakresie przeprowadzenia audytu Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w Mazowieckim Urzędzie Wojewódzkim w Warszawie i Jednostkach Administracji Zespolonej

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

Spis treści

Definicje **2**
Wprowadzenie i cel audytu **3**
Miejsce realizacji **3**
Termin realizacji **4**
Zakres audytu **4**
Audyt dokumentacji i jej ocena zgodności z wymaganiami formalnymi **4**
Audyt techniczny systemów teleinformatycznych i infrastruktury **9**
Harmonogram audytu **14**
Wymagania ogólne **15**

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

Definicje

1. **Audyt dokumentacji** – ocena zgodności dokumentacji organizacyjnej oraz procedur (Mazowieckiego Urzędu Wojewódzkiego i Jednostek Administracji Zespolonej wskazanych w załączniku nr 1 do OPZ) z wymaganiami KRI, KSC i ISO, wykonany według wytycznych określonych w OPZ;
2. **Audyt techniczny** – weryfikacja technicznych aspektów bezpieczeństwa informacji (środowisk IT Mazowieckiego Urzędu Wojewódzkiego i Jednostek Administracji Zespolonej wskazanych w załączniku nr 1 do OPZ, wykorzystywanych do przetwarzania informacji), obejmującej systemy teleinformatyczne, infrastrukturę sieciową oraz procesy operacyjne, pod kątem ich zgodności z wymaganiami KRI, KSC i ISO, wykonany według wytycznych określonych w OPZ;
3. **Dokumentacja** – komplet materiałów przygotowanych przez Wykonawcę składających się na Raporty z Audytów dokumentacji i Audytów technicznych, opisanych w Załączniku nr 1 do Umowy;
4. **Dzień roboczy** - każdy dzień tygodnia od poniedziałku do piątku, za wyjątkiem dni ustawowo wolnych od pracy w rozumieniu ustawy z dnia 18 stycznia 1951 r. o dniach wolnych od pracy (tekst jednolity Dz.U. 2015 poz. 90);
5. **ISO** – norma PN-EN ISO/IEC 27001:2023;
6. **KRI** – 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 (Dz.U. 2024 poz. 773);
7. **KSC** – ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (tekst jednolity Dz.U. 2026 poz. 20);
8. **OPZ** – opis przedmiotu zamówienia, stanowiący Załącznik nr 1 do umowy;
9. **Protokół Odbioru Raportu Audytu dokumentacji** – dokument potwierdzający odbiór Raportu Audytu dokumentacji, którego wzór stanowi załącznik nr 3;
10. **Protokół Odbioru Raportu Audytu technicznego** – dokument potwierdzający odbiór Raportu Audytu technicznego, którego wzór stanowi załącznik nr 4;
11. **Raport Audytu dokumentacji** – dokument zawierający szczegółowy opis i ocenę stanu wszystkich obszarów podlegających Audytowi technicznemu, opracowany przez Wykonawcę według wymagań określonych w Załączniku nr 1 do Umowy;
12. **Raport Audytu technicznego** – dokument zawierający szczegółowy opis i ocenę stanu wszystkich obszarów podlegających Audytowi technicznemu, opracowany przez Wykonawcę według wymagań określonych w Załączniku nr 1 do Umowy;

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

13. **Umowa** – niniejsza umowa między Stronami;
14. **Utwór** – oznacza każdy utwór w rozumieniu ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j.Dz.U.2021 , poz. 1062) wytworzony i dostarczony w ramach umowy przez Wykonawcę.

Wprowadzenie i cel audytu

Celem niniejszego audytu jest kompleksowa ocena zgodności organizacji (tj. Mazowieckiego Urzędu Wojewódzkiego oraz Jednostek Administracji Zespolonej wskazanych w załączniku nr 1 do OPZ) z wymaganiami:

- Rozporządzenia 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 (Dz.U. 2024 poz. 773) – KRI;
- Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (tekst jednolity Dz.U. 2026 poz. 20) – KSC;
- PN-EN ISO/IEC 27001:2023 – ISO

– rodzaj audytu, który ma zostać przeprowadzony w poszczególnych jednostkach jest wskazany w załączniku nr 1 do OPZ (we wszystkich jednostkach należy przeprowadzić audyt zgodności z KRI i KSC, a dla wybranych ISO).

Audyt ma objąć zarówno analizę dokumentacji organizacyjnej (w tym m.in.: polityk, procedur, regulaminów), jak i weryfikację technicznych aspektów bezpieczeństwa informacji. Głównym założeniem jest identyfikacja ewentualnych niezgodności oraz ocena stopnia wdrożenia praktyk zapewniających poufność, integralność i dostępność informacji przetwarzanych przez jednostki.

Miejsce realizacji

Miejscem realizacji audytu są wszystkie lokalizacje Zamawiającego – Mazowieckiego Urzędu Wojewódzkiego w Warszawie], w tym wydziały, biura oraz delegatury na terenie województwa mazowieckiego (zgodnie z wykazem dostępnym na stronie internetowej Zamawiającego: https://www.gov.pl/web/uw-mazowiecki/wydzialy-biura-delegatury) oraz Jednostki Administracji Zespolonej wskazane w Załączniku nr 1 do OPZ.

Czynności audytowe mogą być realizowane zarówno w formie stacjonarnej, jak i zdalnej, o ile nie wpływa to na osiągnięcie celów audytu.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

Identyfikacja podatności, w tym skanowanie podatności, nie może być realizowana wyłącznie z jednej wspólnej lokalizacji dla wszystkich podmiotów objętych zamówieniem. Czynności te powinny być realizowane odrębnie dla każdej jednostki, z uwzględnieniem jej środowiska IT i uwarunkowań technicznych. Sposób technicznej realizacji skanowania w danej jednostce, w tym możliwość jego realizacji zdalnej, podlega uzgodnieniu z Zamawiającym.

Zakres i liczba wizyt audytowych zostaną określone przez Wykonawcę w harmonogramie audytu i uzgodnione z Zamawiającym.

Termin realizacji

Wykonawca musi zrealizować wszystkie prace w terminie nie dłuższym niż 90 dni od zawarcia umowy.

Zakres audytu

Audyt ma zostać zrealizowany w dwóch głównych obszarach:

1. Audyt dokumentacji i jej ocena zgodności z wymaganiami formalnymi (KRI, KSC, ISO).
2. Audyt techniczny: systemów teleinformatycznych i infrastruktury sieciowej.

Audyty w obu obszarach mogą być realizowane równolegle.

Audyt dokumentacji i jej ocena zgodności z wymaganiami formalnymi

W ramach niniejszego obszaru przeprowadzona zostanie szczegółowa analiza dokumentacji organizacyjnej oraz ocena jej zgodności z wymaganiami wynikającymi z przepisów prawa oraz norm, tj.: KRI, KSC oraz PN-EN ISO/IEC 27001:2023. Celem etapu jest określenie stopnia formalnego wdrożenia systemu zarządzania bezpieczeństwem informacji (SZBI) oraz identyfikacja luk, niespójności i obszarów wymagających doskonalenia. Etap obejmuje zarówno analizę formalną dokumentacji, jak i ocenę jej praktycznego funkcjonowania w organizacji.

Zakres prac obejmuje w szczególności:

1. Identyfikację, przegląd i inwentaryzację dokumentacji, w tym m.in.:
   - zebranie, inwentaryzację i katalogowanie wszystkich obowiązujących dokumentów związanych z bezpieczeństwem informacji, tj.: (polityki, procedury, instrukcje, regulaminy),
   - identyfikację właścicieli dokumentów oraz odpowiedzialności za ich utrzymanie,
   - ocenę kompletności dokumentacji względem wymagań KRI, KSC i ISO/IEC 27001,
   - weryfikację aktualności dokumentów (daty przeglądów, wersjonowanie, zatwierdzenia),

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

- identyfikację brakujących, nieaktualnych lub niespójnych dokumentów, procedur, itp.
- weryfikację aktualności zasobów (aktywów) informacyjnych i w razie potrzeby identyfikacja nowych wraz z określeniem ich istotności i właścicieli,
- ocenę spójności dokumentów z obowiązującą strukturą organizacyjną.

2. Analizę zgodności formalnej, w tym m.in.:
   - ocenę zgodności dokumentacji z wymaganiami:
     - § 19 KRI (m.in. zarządzanie bezpieczeństwem informacji, ryzykiem, ciągłością działania),
     - przepisami znowelizowanej ustawy o KSC (m.in. obowiązki podmiotów krajowego systemu cyberbezpieczeństwa),
     - wymaganiami normy PN-EN ISO/IEC 27001:2023 (w tym, m.in. kontekstu organizacji, przywództwa, planowania, wsparcia, operacji, oceny i doskonalenia) – jeśli dotyczy,
   - mapowanie istniejących dokumentów do wymagań norm i przepisów (tzw. macierz zgodności),
   - identyfikacja brakujących polityk, procedur lub rejestrów wymaganych przepisami.
3. Ocenę kompletności i jakości dokumentacji, w tym m.in.:
   - analizę zakresu i szczegółowości dokumentacji (np. polityki bezpieczeństwa informacji, procedury zarządzania dostępem, procedury zarządzania incydentami, itd.),
   - ocenę adekwatności procedur do rzeczywistych procesów organizacji,
   - ocenę, czy dokumenty zawierają wymagane elementy, np:
     - role i odpowiedzialności,
     - zasady zarządzania ryzykiem,
     - procedury reagowania na incydenty,
     - plany ciągłości działania (BCP/DRP),
     - mechanizmy kontroli i monitorowania,
     - uwzględniają cykl życia informacji oraz aktywów,
   - ocenę zgodności dokumentacji z zasadą „need-to-know” i klasyfikacją (istotnością) informacji,
   - ocenę jakości dokumentacji pod kątem:
     - spójności i jednoznaczności zapisów,
     - adekwatności do skali i charakteru organizacji,
     - czytelności i zrozumiałości dla użytkowników.
4. Weryfikację wdrożenia dokumentacji w praktyce, w tym m.in.:
   - sprawdzenie, czy zapisy dokumentów są faktycznie stosowane w organizacji,
   - identyfikację rozbieżności pomiędzy stanem formalnym a rzeczywistymi praktykami i funkcjonowaniem organizacji,

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

- analizę dowodów stosowania procedur (np. rejestry, logi, zgłoszenia incydentów, raporty),
- ocenę skuteczności mechanizmów nadzoru i kontroli wewnętrznej.

5. Wywiady i warsztaty z pracownikami, w tym m.in.:
   - przeprowadzenie ustrukturyzowanych wywiadów z (dopuszcza się wywiady zdalnie za pomocą narzędzi do telekonferencji – bez możliwości utrwalania):
     - kadrą kierowniczą,
     - osobami odpowiedzialnymi za bezpieczeństwo informacji (zgodnie z wyznaczonymi rolami w organizacji),
     - właścicielami procesów,
   - weryfikację znajomości i rozumienia obowiązujących polityk i procedur,
   - ocenę poziomu świadomości pracowników w zakresie obowiązujących regulacji,
   - identyfikację nieformalnych praktyk i obejść (tzw. workarounds).
6. Ocenę zarządzania ryzykiem, w tym m.in.:
   - analizę metodologii zarządzania ryzykiem,
   - weryfikację rejestru ryzyk oraz jego aktualności,
   - ocenę powiązania ryzyk z zabezpieczeniami,
   - sprawdzenie, czy wyniki analizy ryzyka wpływają na dokumentację i decyzje organizacyjne,
   - przedstawienie rekomendacji dotyczących doskonalenia procesu zarządzania ryzykiem.
7. Wstępną ocenę dojrzałości SZBI, w tym m.in.:
   - określenie poziomu dojrzałości systemu zarządzania bezpieczeństwem informacji (ocena dojrzałości zostanie przeprowadzona wg modelu zaproponowanego przez wykonawcę i zaakceptowanego przez Zamawiającego),
   - identyfikację kluczowych luk systemowych i obszarów ryzyka,
   - ocenę stopnia formalizacji i systematyczności działań,
   - wskazanie obszarów krytycznych wymagających pilnych działań,
   - ocenę adekwatności zasobów do zadań.
8. Raportowanie wyników, w tym m.in.:
   - przygotowanie pełnego raportu zawierającego m.in. zidentyfikowane:
     - niezgodności,
     - obserwacje,
     - rekomendacje,
   - przypisanie poziomu istotności (np. wysoki / średni / niski),
   - przypisanie typu rekomendacji (operacyjne (techniczne), organizacyjne, strategiczne),
   - identyfikację tzw. „quick wins” (działań możliwych do szybkiego wdrożenia),

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

- wskazanie zależności między niezgodnościami (analiza przyczynowa),
- wskazanie odniesienia do konkretnych wymagań KRI, KSC i ISO,
- opracowanie rekomendacji działań naprawczych i usprawniających,
- przygotowanie podsumowania dla kierownika jednostki, dyrektora generalnego i głównego administratora bezpieczeństwa (wraz z prezentacją) dla Mazowieckiego Urzędu Wojewódzkiego oraz Jednostek Administracji Zespolonej wskazanych w załączniku nr 1 do OPZ.

W wyniku realizacji Audytu dokumentacji Wykonawca sporządzi i przekaże Zamawiającemu jeden Raport Audytu dokumentacji dla Mazowieckiego Urzędu Wojewódzkiego w Warszawie oraz odrębne Raporty Audytu technicznego dla każdej Jednostki Administracji Zespolonej wskazanej w załączniku nr 1 do OPZ, zawierające ustalenia z wykonanych czynności, zgodnie z wymaganiami wskazanymi w zakresie prac powyżej, w tym m.in.:

- analizę dokumentacji,
- ocenę poziomu zgodności,
- wykaz zidentyfikowanych niezgodności i luk,
- rekomendacje działań naprawczych i usprawniających,
- ocenę zarządzania ryzykiem
- prezentację wyników.

Kryteria odbioru jakościowego

Zamawiający uzna Raporty Audytu dokumentacji za należycie wykonane wyłącznie w przypadku, gdy każdy z nich spełnia łącznie następujące kryteria jakościowe:

1. Kompletność:
   - raport obejmuje wszystkie obszary wskazane w OPZ powyżej,
   - zawiera odniesienia do wszystkich wymaganych regulacji, tj. KRI, KSC oraz PN-EN ISO/IEC 27001:2023,
   - uwzględnia wszystkie podmioty objęte zakresem audytu określone w OPZ oraz załączniku nr 1;
2. Jednoznaczność i weryfikowalność ustaleń:
   - każda zidentyfikowana niezgodność, obserwacja i rekomendacja jest jasno opisana,
   - wskazane są konkretne dowody (np. dokumenty, zapisy, wyniki wywiadów),
   - wskazane są konkretne wymagania (przepis/norma), do których odnosi się dana niezgodność;
3. Powiązanie z wymaganiami formalnymi:

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

- każda niezgodność zawiera odniesienie do konkretnego przepisu KRI, KSC lub punktu normy ISO,
- zastosowana jest spójna struktura mapowania (np. zgodna z macierzą zgodności);

4. Ocena istotności:
   - każda niezgodność i obserwacja posiada przypisany poziom istotności (np. wysoki / średni / niski),
   - zastosowane kryteria oceny istotności są opisane i spójnie stosowane w całym raporcie;
5. Wartość praktyczna rekomendacji:
   - rekomendacje są konkretne, możliwe do wdrożenia i adekwatne do skali organizacji,
   - wskazują proponowany kierunek działań naprawczych,
   - zawierają priorytety wdrożeniowe;
6. Analiza przyczynowa:
   - raport zawiera identyfikację przyczyn źródłowych kluczowych niezgodności (a nie wyłącznie ich opis),
   - wskazane są zależności między problemami;
7. Spójność i czytelność:
   - raport jest logicznie uporządkowany, spójny i jednoznaczny,
   - stosowane nazewnictwo jest jednolite,
   - dokument jest zrozumiały dla odbiorców nietechnicznych (w szczególności kadry kierowniczej);
8. Ocena dojrzałości SZBI:
   - zawiera jasno określoną metodykę oceny,
   - wskazuje poziom dojrzałości wraz z uzasadnieniem,
   - identyfikuje kluczowe luki systemowe;
9. Uwzględnienie aspektów praktycznych:
   - raport odnosi się nie tylko do dokumentacji, ale również do faktycznego funkcjonowania organizacji,
   - zawiera wnioski z wywiadów oraz analizy dowodów stosowania procedur;
10. Podsumowanie zarządcze:
    - raport zawiera syntetyczne podsumowanie dla kierownictwa,
    - wskazuje kluczowe ryzyka oraz obszary wymagające pilnych działań,
    - zawiera listę rekomendacji strategicznych.

Zamawiający ma prawo odmówić odbioru Raport Audytu dokumentacji w przypadku:

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

- braku spełnienia któregokolwiek z kryteriów określonych w pkt Kryteria odbioru jakościowego,
- ogólnikowego charakteru ustaleń lub rekomendacji,
- braku powiązania ustaleń z wymaganiami formalnymi,
- braku dowodów potwierdzających ustalenia audytu.

Niedopuszczalne jest:

- formułowanie ogólnych, nieweryfikowalnych wniosków,
- brak wskazania podstawy ustaleń,
- stosowanie niejednoznacznych lub niespójnych kryteriów oceny.

W przypadku odmowy odbioru Wykonawca zobowiązany jest do poprawy Raport Audytu dokumentacji zgodnie z uwagami Zamawiającego w terminie nie dłuższym niż 5 dni roboczych.

Audyt techniczny systemów teleinformatycznych i infrastruktury

Celem Audytu technicznego jest przeprowadzenie kompleksowej, mierzalnej i opartej na dowodach weryfikacji technicznych aspektów bezpieczeństwa informacji (środowiska IT Mazowieckiego Urzędu Wojewódzkiego i Jednostek Administracji Zespolonej wskazanych w załączniku nr 1 do OPZ, wykorzystywanego do przetwarzania informacji), obejmującej systemy teleinformatyczne, infrastrukturę sieciową oraz procesy operacyjne, pod kątem ich zgodności z wymaganiami:

- Rozporządzenia 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 (Dz.U. 2024 poz. 773) – KRI;
- Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (tekst jednolity Dz.U. 2026 poz. 20) – KSC;
- PN-EN ISO/IEC 27001:2023 – ISO

– rodzaj audytu, który ma zostać przeprowadzony w poszczególnych jednostkach jest wskazany w załączniku nr 1 do OPZ (we wszystkich jednostkach należy przeprowadzić audyt zgodności z KRI i KSC, a dla wybranych ISO).

Celem szczegółowym jest:

- ocena poziomu bezpieczeństwa infrastruktury technicznej,
- ocena skuteczności wdrożonych zabezpieczeń technicznych i stosowanych mechanizmów ochrony (np. sieciowej, systemowej, aplikacyjnej),
- identyfikacja podatności, luk i słabych punktów,

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

- weryfikacja zgodności konfiguracji systemów i infrastruktury z dokumentacją oraz wymaganiami formalnymi, tj. ocena stanu i konfiguracji sieci teleinformatycznej (LAN/WAN/Wi-Fi), w tym segmentacji, kontroli dostępu, detekcji zagrożeń, redundancji oraz monitoringu,
- ocena wpływu zidentyfikowanych ryzyk na poufność, integralność i dostępność informacji.

Audyt techniczny stanowi rozwinięcie i weryfikację ustaleń Audytu dokumentacji w warstwie technicznej.

Zakres prac obejmuje w szczególności:

1. Inwentaryzację i analizę środowiska IT, w tym m.in.:
   - identyfikację i klasyfikację systemów, aplikacji, zasobów i usług IT,
   - weryfikację kompletności ewidencji aktywów (sprzęt, oprogramowanie, dane, itp.),
   - analizę architektury systemowej i sieciowej (LAN/WAN/Wi-Fi, strefy bezpieczeństwa),
   - identyfikację systemów krytycznych oraz punktów styku z systemami zewnętrznymi,
   - ocenę spójności środowiska technicznego z dokumentacją.
2. Analizę ryzyka (techniczną), w tym m.in.:
   - identyfikację ryzyk technicznych i operacyjnych wynikających z konfiguracji i architektury,
   - mapowanie zagrożeń oraz ich potencjalnych skutków dla ciągłości działania,
   - ocenę wpływu ryzyk na:
     - systemy krytyczne,
     - dane osobowe,
     - dostępność usług publicznych,
   - weryfikację spójności analizy ryzyka z dokumentacją SZBI,
   - uzupełnienie lub doprecyzowanie rejestru ryzyk (jeśli wymagane).
3. Weryfikację procesów operacyjnych, w tym m.in.:
   - ocenę skuteczności procesów:
     - zarządzania incydentami,
     - zarządzania zmianą,
     - zarządzania dostępem,
     - backupu i odtwarzania danych,
     - zarządzania podatnościami i aktualizacjami,
   - weryfikację faktycznego stosowania procedur,
   - analizę dowodów operacyjnych (logi, zgłoszenia, raporty),
   - ocenę zgodności działań operacyjnych z dokumentacją,
   - ocenę poziomu świadomości i przygotowania personelu (w kontekście technicznym).
4. Audyt systemów informatycznych, w tym m.in.:

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

1) Ocenę konfiguracji i zabezpieczeń

- weryfikację konfiguracji systemów operacyjnych, serwerów i aplikacji,
- ocenę zgodności konfiguracji z politykami bezpieczeństwa,
- analizę mechanizmów:
  - kontroli dostępu,
  - uwierzytelniania (w tym MFA),
  - rejestrowania zdarzeń,
  - szyfrowania danych,
- ocenę poziomu hardeningu systemów.

2) Zarządzanie podatnościami i aktualizacjami

- ocenę procesu patch management,
- weryfikację aktualności systemów i aplikacji,
- analizę wyników skanów podatności (jeśli dostępne),
- ocenę reakcji organizacji na wykryte podatności.

5. Monitorowanie i reagowanie na incydenty, w tym m.in.:
   - ocenę systemów monitorowania (np. SIEM, systemy logowania),
   - weryfikację zakresu, retencji i integralności logów,
   - ocenę zdolności wykrywania incydentów,
   - analizę procesów reagowania i eskalacji,
   - weryfikację zgodności z wymaganiami KSC w zakresie raportowania incydentów.
6. Audyt infrastruktury sieciowej, w tym m.in.:

1) Architektura i segmentacja

- ocenę topologii sieci (LAN, WAN, Wi-Fi),
- weryfikację segmentacji (VLAN, strefy bezpieczeństwa, DMZ),
- identyfikację nieautoryzowanych połączeń i urządzeń,
- ocenę redundancji i odporności infrastruktury.

2) Urządzenia i konfiguracja

- audyt konfiguracji:
  - firewalli,
  - routerów,
  - przełączników,
- weryfikację:
  - polityk dostępu,
  - reguł ACL i NAT,

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

- zabezpieczeń administracyjnych,

- ocena aktualności firmware i konfiguracji.

3) Bezpieczeństwo dostępu i sieci bezprzewodowych

- ocena kontroli dostępu do sieci,
- weryfikacja zabezpieczeń Wi-Fi (uwierzytelnianie, szyfrowanie),
- analiza izolacji zasobów krytycznych.

7. Testy techniczne, w tym m.in.:
   - przeprowadzenie skanów podatności (np. narzędzia klasy Nmap, Nessus, OpenVAS), (przedmiot zamówienia nie obejmuje testów penetracyjnych ani prób eksploatacji podatności; zakres obejmuje wyłącznie nieinwazyjne skanowanie podatności),
   - identyfikacja otwartych portów i podatnych usług,
   - analiza wyników testów i klasyfikacja podatności.
8. Ocenę zgodności technicznej, w tym m.in.:
   - mapowanie zabezpieczeń technicznych do wymagań:
     - KRI,
     - KSC,
     - ISO/IEC 27001,
   - identyfikacja braków i niezgodności,
   - ocena adekwatności zabezpieczeń względem poziomu ryzyka,
   - weryfikacja spójności między dokumentacją (Etap 1) a stanem technicznym.
9. Wstępną ocenę dojrzałości technicznej
   - ocenę dojrzałości zabezpieczeń technicznych (model analogiczny do Etapu 1),
   - identyfikację kluczowych luk systemowych,
   - ocenę zdolności organizacji do wykrywania i reagowania na zagrożenia,
   - ocenę adekwatności zasobów technicznych.

W wyniku realizacji Audytu technicznego Wykonawca sporządzi i przekaże Zamawiającemu jeden Raport Audytu technicznego dla Mazowieckiego Urzędu Wojewódzkiego w Warszawie oraz odrębne Raporty Audytu technicznego dla każdej Jednostki Administracji Zespolonej wskazanej w załączniku nr 1 do OPZ zawierające ustalenia z wykonanych czynności, zgodnie z wymaganiami wskazanymi w zakresie prac powyżej, w tym m.in.:

- opis przeprowadzonych działań audytowych,

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

- pełną listę:
    - niezgodności,
    - podatności,
    - zagrożeń,
- ocenę poziomu zgodności z wymaganiami,
- analizę przyczyn źródłowych,
- rekomendacje:
- plan działań korygujących (z priorytetami),
- ocenę ryzyka,
- ocenę dojrzałości technicznej,
- podsumowanie zarządcze.

Kryteria odbioru jakościowego

Zamawiający uzna Raport Audytu technicznego za należycie wykonany wyłącznie w przypadku, gdy spełnia on łącznie następujące kryteria jakościowe:

- spełnia wszystkie kryteria jakościowe określone dla Audytu dokumentacji,
- każda podatność posiada:
    - opis,
    - dowód,
    - poziom istotności,
    - rekomendację,
- wyniki testów technicznych są udokumentowane,
- wskazano powiązanie między:
    - lukami technicznymi,
    - procesami,
    - dokumentacją,
- raport zawiera analizę wpływu na systemy krytyczne.

Zamawiający ma prawo odmówić odbioru Raport Audytu technicznego w przypadku:

- braku spełnienia któregokolwiek z kryteriów określonych w pkt Kryteria odbioru jakościowego,
- ogólnikowego charakteru ustaleń lub rekomendacji,

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

- braku powiązania ustaleń z wymaganiami formalnymi,
- braku dowodów potwierdzających ustalenia audytu.

Niedopuszczalne jest:

- formułowanie ogólnych, nieweryfikowalnych wniosków,
- brak wskazania podstawy ustaleń,
- stosowanie niejednoznacznych lub niespójnych kryteriów oceny.

W przypadku odmowy odbioru Wykonawca zobowiązany jest do poprawy Raport Audytu technicznego zgodnie z uwagami Zamawiającego w terminie nie dłuższym niż 5 dni roboczych.

Harmonogram audytu

Wykonawca, w terminie do 10 dni roboczych od dnia podpisania umowy, opracuje i przekaże Zamawiającemu:

1. Harmonogram zbiorczy realizacji audytu, obejmujący zarówno obszar organizacyjny (analiza dokumentacji), jak i techniczny, z podziałem na:
   - Mazowiecki Urząd Wojewódzki w Warszawie (MUW),
   - Jednostki Administracji Zespolonej (JAZ) wskazane w załączniku nr 1 do OPZ;
2. Harmonogramy szczegółowe dla poszczególnych podmiotów objętych audytem (MUW oraz Jednostek Administracji Zespolonej wskazanych w załączniku nr 1 do OPZ).

Harmonogramy szczegółowe dotyczące Jednostek Administracji Zespolonej będą podlegały opiniowaniu i uzgodnieniu z właściwymi Jednostkami przez Zamawiającego. Wykonawca ma obowiązek uwzględnić zgłoszone uwagi Zamawiającego do harmonogramu zbiorczego i harmonogramów szczegółowych

Harmonogramy szczegółowe będą określały w szczególności:

- terminy realizacji poszczególnych etapów audytu,
- planowane terminy wizyt audytowych,
- zakres czynności realizowanych przez Wykonawcę,
- przewidywane terminy przekazywania wyników cząstkowych oraz raportów.

Wykonawca zobowiązany jest do bieżącej aktualizacji harmonogramów w przypadku wystąpienia okoliczności mających wpływ na terminy realizacji audytu, po uprzednim uzgodnieniu zmian z Zamawiającym.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

Wymagania ogólne

Raporty, o których mowa powyżej, zostaną przekazane w formie elektronicznej w formatach PDF, DOCX oraz XLSX, umożliwiających odczyt oraz edycję (kompatybilnym z pakietem Microsoft Office 2016 lub nowszym) – zarówno w edytorze tekstu, jak i arkuszu kalkulacyjnym z odblokowanymi formułami, widokiem zawartości komórek i łączami (bez odwołań do źródeł zewnętrznych poza zbiorczym plikiem). Wykonawca dostarczy również wszelkie użyte w raportach rysunki, wykresy i inne opracowania w postaci umożliwiającej ich edycję (wersje źródłowe).

Zamawiający przewiduje przekazywanie częściami wytworzonej Dokumentacji, sukcesywnie przez okres jej tworzenia, jako materiałów roboczych do weryfikacji przez Zamawiającego, w celu wcześniejszego zapoznania się z Dokumentacją i usprawnienia procedury odbiorowej.
Zamawiający przewiduje sukcesywne przekazywanie przez Wykonawcę poszczególnych Raportów Audytu dokumentacji i Raportów Audytu technicznego przed upływem terminu realizacji przedmiotu zamówienia.
Odbiór Raportów Audytu dokumentacji i/lub Raportów Audytu technicznego, dla każdej jednostki wskazanej w załączniku nr 1, nastąpi na podstawie odpowiedniego Protokołu Odbioru Raportu Audytu dokumentacji i/lub Protokołu Odbioru Audytu technicznego podpisanego przez Strony, po uprzedniej weryfikacji kompletności i zgodności przekazanych materiałów z wymaganiami określonymi w OPZ.
Zamawiający zastrzega sobie prawo zgłoszenia uwag do otrzymanych Raportów Audytu dokumentacji i/lub Raportów Audytu technicznego w terminie 7 Dni roboczych od dnia otrzymania każdego z nich. Wykonawca zobowiązany jest do uwzględnienia zgłoszonych uwag i przekazania poprawionej wersji w terminie nie dłuższym niż 5 Dni roboczych.
Raporty dotyczące Jednostek Administracji Zespolonej Zamawiający przekaże do opiniowania i uzgodnienia tym Jednostkom.
Za datę wykonania przedmiotu zamówienia uznaje się datę podpisania ostatniego / ostatnich Protokołów Odbioru Audytu dokumentacji oraz Protokołów Odbioru Audytu technicznego dla wszystkich jednostek wskazanych w załączniku nr 1, w tym bez żadnych uwag i zastrzeżeń ze strony Zamawiającego.

KRAJOWY PLAN ODBUDOWY
Rzeczpospolita Polska
Sfinansowane przez Unię Europejską NextGenerationEU

Załącznik nr 1 do OPZ

Lp.	Skrót Jednostki	Nazwa Jednostki	Adres	Audyt KRI i KSC?	Czy dodatkowo audyt ISO 27001?
1	WSSE	Wojewódzka Stacja Sanitarno-Epidemiologiczna w Warszawie	ul. Żelazna 79, 00-875 Warszawa	tak	nie
2	WITD	Wojewódzki Inspektorat Transportu Drogowego w Radomiu	ul. Limanowskiego 29A, 26-610 Radom	tak	nie
3	WIOŚ	Wojewódzki Inspektorat Ochrony Środowiska w Warszawie	ul. Bartycka 110A, 00-716 Warszawa	tak	tak
4	WINB	Wojewódzki Inspektorat Nadzoru Budowlanego w Warszawie	ul. Bitwy Warszawskiej 1920 r. 11, 02-366 Warszawa	tak	nie
5	PSSE Zwoleń	Powiatowa Stacja Sanitarno-Epidemiologiczna w Zwoleniu	ul. Bogusza 37, 26-700 Zwoleń	tak	nie
6	PSSE Wyszków	Powiatowa Stacja Sanitarno-Epidemiologiczna w Wyszkowie	ul. Daszyńskiego 28, 07-200 Wyszków	tak	nie
7	PSSE Przysucha	Powiatowa Stacja Sanitarno-Epidemiologiczna w Przysusze	ul. Szkolna 7, 26-400 Przysucha	tak	nie
8	PSSE Przasnysz	Powiatowa Stacja Sanitarno-Epidemiologiczna w Przasnyszu	ul. Gołymińska 13, 06-300 Przasnysz	tak	nie
9	PSSE Płock	Powiatowa Stacja Sanitarno-Epidemiologiczna w Płocku	ul. Kolegialna 20, 09-402 Płock	tak	nie
10	PSSE Ostrołęka	Powiatowa Stacja Sanitarno-Epidemiologiczna w Ostrołęce	ul. Targowa 4, 07-410 Ostrołęka	tak	nie
11	PSSE Maków Maz.	Powiatowa Stacja Sanitarno- Epidemiologiczna w Makowie Mazowieckim	ul. Mickiewicza 31, 06-200 Maków Mazowiecki	tak	nie
12	PSSE Grodzisk Maz.	Powiatowa Stacja Sanitarno-Epidemiologiczna w Grodzisku Mazowieckim	ul. Żwirki i Wigury 10, 05-825 Grodzisk Mazowiecki	tak	tak
13	PSSE Garwolin	Powiatowa Stacja Sanitarno-Epidemiologiczna w Garwolin	ul. Wyszyńskiego 38, 08-400 Garwolin	tak	nie
14	MUW	Mazowiecki Urząd Wojewódzki w Warszawie	pl. Bankowy 3/5, 00-950 Warszawa	tak	tak