OPIS PRZEDMIOTU ZAMÓWIENIA

Spis treści

1. Przedmiot zamówienia

Przedmiotem zamówienia jest wykonanie audytu zewnętrznego bezpieczeństwa infrastruktury teleinformatycznej dwudziestu dwóch podmiotów leczniczych, dla których Samorząd Województwa Mazowieckiego jest podmiotem tworzącym bądź właścicielem - Partnerów Projektu „E-zdrowie dla Mazowsza 2" polegającym na:

a) analizie i identyfikacji podatności i zagrożeń systemów teleinformatycznych;
b) analizie procesów przetwarzania danych wraz z analizą stanu zabezpieczeń systemowych;
c) analizie bezpieczeństwa fizycznego i środowiskowego dla zabezpieczenia realizacji usług medycznych;
d) analizie bezpieczeństwa i ciągłości dostaw i usług IT;
e) opracowaniu rekomendacji dotyczących wdrożenia wymaganych zabezpieczeń organizacyjnych i technicznych;
f) analizie bezpieczeństwa i wydajności infrastruktury pod kątem wymiany dużej ilości danych z podmiotem zewnętrznym.

Zamawiający wymaga, aby w ramach przeprowadzonej analizy stanu obecnego, Wykonawca dokonał przeglądu wszystkich obowiązujących w organizacji procedur dotyczących zapewnienia bezpieczeństwa cybernetycznego w zakresie ich zgodności z przepisami obowiązującego prawa. W wyniku przeprowadzonej analizy, Zamawiający wymaga:

a) przeprowadzenia analizy ryzyka w zakresie cyberbezpieczeństwa Partnerów, oceny prawdopodobieństwa wystąpienia incydentu, a także jego skutków oraz sporządzenia rejestru ryzyk i czynności wpływających na obniżenie poziomu prawdopodobieństwa wystąpienia i skutków ryzyka;
b) weryfikację istniejących u Partnerów procedur zgłaszania i obsługi incydentów zgodnie z wymaganiami obowiązującego prawa, obejmującej sposób gromadzenia informacji o zaistniałych incydentach oraz strategię komunikacji z odpowiednią instytucją sprawująca nadzór nad cyberbezpieczeństwem;
c) opracowania rekomendacji oraz sposobu ich wdrożenia i realizacji w zakresie wszystkich czynności obejmujących cyberbezpieczeństwo Partnerów i wymaganych przepisami prawa;
d) analizy i oceny potencjału oraz zasobów Partnerów w kontekście możliwości zapewnienia cyberbezpieczeństwa;
e) analizy możliwości zachowania ciągłości działania świadczenia usług medycznych oraz zapewniających poufność, integralność, dostępność i autentyczność informacji przez Partnerów;
f) analizy podatności systemów informatycznych Partnerów;
g) przeglądu procesów zarządczych, w tym procesów zarządczych IT i procesów zarządzania usługami IT u Partnerów;
h) przeglądu zgodności z krajowymi ramami interoperacyjności u Partnerów.

2. Szczegółowy zakres prac do wykonania.

Zadania realizowane przez Wykonawcę w ramach niniejszego postępowania zostały podzielone na poniżej określone obszary.

2.1. Audyt platform sprzętowych

Zakres zadań w odniesieniu do stacji roboczych (w tym laptopów), serwerów, urządzeń sieciowych, macierzy dyskowych, urządzeń NAS, UPSów, obejmuje**:**

a) weryfikację aktualności firmware sprzętu,
b) weryfikację wsparcia producenta w zakresie aktualizacji firmware i innego oprogramowania , np. denifnicji AV na urządzeniach UTM (w tym cykl życia produktu),
c) weryfikację obowiązującej gwarancji i rękojmi,
d) weryfikację dostępu do konfiguracji urządzenia na poziomie sprzętowym.

2.2. Audyt konfiguracji systemów operacyjnych

Zakres zadań obejmuje**:**

a) weryfikację uruchomionych usług sieciowych,
b) weryfikację kont systemowych,
c) weryfikację mechanizmów uwierzytelniania i autoryzacji,
d) weryfikację wdrożonych mechanizmów dostępu do zasobów,
e) weryfikację uprawnień do zasobów,
f) weryfikację wdrożonych mechanizmów instalacji aktualizacji,
g) weryfikację wdrożonych mechanizmów tworzenia kopii zapasowych,
h) weryfikację wdrożonych mechanizmów logowania zdarzeń,
i) weryfikację wdrożonych mechanizmów administracji zdalnej,
j) weryfikację wdrożonych mechanizmów zabezpieczenia systemu w fazie boot,
k) weryfikację wdrożonych mechanizmów zarządzania systemem,
l) weryfikację wdrożonych dodatkowych metod ochrony,
m) wskazanie zaleceń hardening'owych dla systemu operacyjnego,
n) weryfikację aktualności systemów operacyjnych pod kątem wsparcia i wydawania poprawek bezpieczeństwa przez producenta systemu.

2.3. Audyt konfiguracji baz danych

Zakres zadań obejmuje:

a) weryfikację wdrożenia podstawowych zasad hardeningowych bazy (np.: dostępność domyślnych użytkowników guest, partycjonowanie bazy, składowanie logów, logowanie nietypowych zdarzeń, dostępność wybranych niebezpiecznych procedur /funkcji składowanych),
b) weryfikację komunikacji z klientem bazodanowym - wykorzystanie mechanizmów kryptograficznych (logowanie się klienta oraz transfer danych),
c) ogólną recenzję architektury bazy (wykorzystane mechanizmy autoryzacji oraz uwierzytelniania segmentacja uprawnień, wykorzystanie widoków; wykorzystanie procedur składowanych),
d) weryfikację sposobu wykonywania kopii zapasowych oraz ich odtwarzania,

e) analizę sposobu udostępnienia RDBMS na poziomie sieciowym,
f) weryfikację dostępności (w zakresie technicznym i formalnym) do danych i mechanizmów bazodanowych (systemy ERP i HIS), w tym identyfikację interfejsów dostępu do danych.

2.4. Audyt bezpieczeństwa aplikacji

Zakres zadań obejmuje:

a) sprawdzenie architektury sieciowej i serwerowej pod kątem bezpieczeństwa,
b) weryfikację procedur zarządzania serwerami,
c) weryfikację podatności komponentów aplikacji (w tym serwerów aplikacyjnych i baz danych),
d) weryfikację sposobu instalacji aplikacji i procedur stosowanych przy wdrażaniu nowych aplikacji,
e) weryfikację mechanizmów uwierzytelniania / autoryzacji,
f) przeprowadzenie testów szczegółowych:
   - sprawdzenie zabezpieczeń panelu administracyjnego przed nieupoważnionym dostępem,
   - próby uzyskania dostępu do panelu administracyjnego za pomocą kont zwykłych użytkowników między innymi przez: wykorzystanie bieżącej sesji, podniesienie uprawnień,
   - próby uzyskania większych uprawnień,
   - próby uzyskania nieautoryzowanego dostępu do danych znajdujących się w systemie,
   - próby uzyskania nieautoryzowanego dostępu do plików znajdujących się na serwerze,
   - analizy możliwości enumeracji użytkowników,
   - próby ataków typowych dla aplikacji webowych i web services, m.in.: SQL Injection, Cross Site Scripting, IMAP/SMTP Injection, LDAP Injection, ORM Injection, XML Injection, XPath Injection, Code Injection, Command Injection, HTTP Splitting,
   - testów funkcji przekierowujących pod kątem walidacji wprowadzanych danych,
   - analizy polityki haseł w aplikacji,
   - próby ominięcia mechanizmu uwierzytelniania za pomocą między innymi analizy identyfikatorów sesji, manipulacji parametrami, bezpośredniego dostępu do widoku aplikacji,
   - próby ominięcia mechanizmu autoryzacji między innymi przez uzyskanie bezpośredniego dostępu do zasobów, manipulacje parametrami, uzyskanie wyższych uprawnień,
   - analizy wykorzystywanego przez aplikację szyfrowania przesyłanych danych, pod kątem dostępnych/wykorzystywanych algorytmów,
   - analizy mechanizmu logowania pod kątem możliwości ominięcia uwierzytelniania i możliwości podsłuchu przesyłanych danych,
   - analizy mechanizmu zakończenia sesji użytkownika pod kątem skuteczności i możliwości przeprowadzenia ataku Denial of Service,
   - analizy zabezpieczenia plików Cookie,
   - analizy zabezpieczenia serwera przed niebezpiecznymi metodami http,
   - analizy przesyłanego kodu pod kątem zawartości zbędnych informacji o aplikacji,
   - analizy nagłówków http pod kątem bezpieczeństwa,

- analizy błędów aplikacji pod kątem ujawniania informacji,
- analizy możliwości zapamiętywania przez przeglądarkę informacji klientów,
- próby odnalezienia wcześniejszych wersji kodu źródłowego i plików kopii zapasowych na serwerze.

2.5. Audyt bezpieczeństwa infrastruktury (testy zewnętrzne i wewnętrzne)

Zakres zadań obejmuje:

a) audyt architektury bezpieczeństwa infrastruktury IT, w tym:
- analiza środowiska serwerowego (systemy kontroli dostępu, wyposażenie: szafy RACK, klimatyzacja, zabezpieczenie p.poż, monitoring warunków środowiskowych, systemy zasilania i zasilania awaryjnego)
- weryfikacja architektury infrastruktury serwerowej i sieciowej oraz jej konfiguracji pod kątem wystepowania pojedynczego punktu awarii,
- analizę przepustowości sieci LAN oraz łączy internetowych,

b) testy penetracyjne zewnętrzne:
- identyfikacje dostępnych serwisów sieciowych, określenie oraz weryfikacja ich podatności,
- penetracja systemu za pomocą skanerów TCP i UDP,
- bezpieczeństwo aplikacji oraz usług dostępnych z zewnątrz,
- analiza topologii sieci widzianej z zewnątrz,
- możliwość uzyskania nieautoryzowanego dostępu do danych,
- badanie podatności związanych atakami typu DDoS,
- konfiguracja komunikacji z usługami (np. konfiguracja SSL/TSL, IPsec),
- weryfikacja procedur zarządzania siecią WAN.

d) testy penetracyjne wewnętrzne:
- bezpieczeństwo urządzeń sieciowych,
- bezpieczeństwo protokołów trasowania,
- analiza topologii sieci i logiki jej segmentacji,
- bezpieczeństwo maszyn zlokalizowanych w obrębie sieci (serwery, stacje robocze),
- bezpieczeństwo usług zlokalizowanych na każdym z dostępnych w sieci urządzeniu oraz maszynie, Istnienie nieautoryzowanych urządzeń (np. nieautoryzowanego urządzenia bezprzewodowego wpiętego do sieci),
- filtrowanie komunikacji wewnętrznej (np. konfiguracja firewall, IDS/IPS, WAF, separacja pomiędzy kluczowymi podsieciami),
- konfiguracja komunikacji z zasobami (np. konfiguracja SSL/TLS dla kluczowych aplikacji),
- możliwość uzyskania nieautoryzowanego dostępu do danych (np. danych wrażliwych),
- przegląd danych dostępnych na udziałach sieciowych – weryfikujemy, czy możliwe jest uzyskanie nieautoryzowanego dostępu do danych na udziałach sieciowych takich jak hasła do systemów, czy też kluczowych dla działania organizacji danych,

- podatność na ataki DDoS,
- weryfikacja zasad bezpieczeństwa na wybranych stacjach roboczych,
- weryfikacja dostępu do Internetu z LAN,
- weryfikacja procedur zarządzania siecią LAN.

2.6. Testy bezpieczeństwa urządzeń sieciowych

Opisane w punkcie: Audyt bezpieczeństwa infrastruktury (wewnętrzne)
Zakres zadań obejmuje:

a) zbadanie odporności urządzeń na ataki z poziomu Internetu,
b) wskazanie potencjalnych skutków ataku dla znalezionych luk i określenie ich krytyczności,
c) wskazanie potencjalnych, dodatkowych metod ochrony sieci,
d) analiza podatności na ataki,
e) skanowanie portów TCP / UDP,
f) skanowanie hostów aktywnych w danej podsieci,
g) określenie ścieżki sieciowej do urządzenia,
h) próba detekcji typu oraz wersji usług sieciowych działających w systemie,
i) próba detekcji wersji oraz typu oprogramowania systemowego zainstalowanego na urządzeniu,
j) po udanej detekcji wersji oprogramowania systemowego / usług – próba lokalizacji znanych podatności w danych wersjach oprogramowania,
k) próba komunikacji w obrębie protokołu ICMP,
l) próba generacji pakietów o dużym rozmiarze (np. powiększonych pakietów ICMP echo).

2.7. Testy bezpieczeństwa VPN (IPsec)

Opisane w punkcie: Audyt bezpieczeństwa infrastruktury (wewnętrzne)
Zakres zadań obejmuje:

a) zbadanie poziomu bezpieczeństwa systemów klasy VPN,
b) weryfikacja możliwości użycia systemów klasy VPN jako punkt pośredniego do ataku na infrastrukturę IT,
c) określenie realnego zabezpieczenia komunikacji sieciowej oferowanej przez wdrożoną u Partnerów implementację VPN,
d) próba wykrycia aktywności serwera VPN,
e) próba wykrycia rodzaju wykorzystywanego rozwiązania VPN (dostawcy sprzętu),
f) próby inicjowania tunelu z różnymi algorytmami kryptograficznymi (szyfry symetryczne, funkcje skrótu, metoda uwierzytelniania, grupa DH),
g) skanowanie portów oraz podatności na koncentratorze VPN,
h) weryfikacja wykorzystanych trybów połączenia (transport, tunnel, ESP, AH),
i) weryfikacja przyjętych metod uwierzytelniania (np. PKI, hasła jednorazowe),

j) weryfikacja przyjętych polityk bezpieczeństwa dla urządzeń klienckich korzystających z VPN (pod względem możliwości ataku na infrastrukturę VPN - inicjowanych z urządzeń klienckich),
k) podstawowa analiza architektury sieci – pod względem rozmieszczenia komponentów.

2.8. Audyty zarządcze

W wyniku prac wymagane jest przygotowanie raportu obejmującego:

a) szczegółowy opis podejścia do realizacji audytu, w szczególności zastosowane do weryfikacji standardy, listy kontrolne i narzędzia,
b) szczegółowy opis i dowód każdego uchybienia lub wykrytej podatności,
c) wpływ danego uchybienia/podatności na bezpieczeństwo badanego obszaru,
d) ocenę poziomu ryzyka,
e) szczegółowe rekomendacje dotyczące sposobów usunięcia uchybienia.

2.9. Audyt procesów zarządczych IT (w zakresie serwerów, sieci, infrastruktury, baz danych, aplikacji)

Zakres zadań obejmuje:

a) podział ról i odpowiedzialności za zarządzanie w badanym obszarze,
b) analiza architektury w badanym obszarze,
c) procesy zarządzania zmianą,
d) procesy obsługi incydentów,
e) procesy wdrażania nowych rozwiązań,
f) procesy wycofywania,
g) procesy utrzymania.

2.10. Audyt procesów zarządzania usługami IT

Zakres zadań obejmuje:

a) analiza usług świadczonych przez Partnerów,
b) audyt procesów wg ITIL v3 w obszarach:
    - Strategia Usług (ang. service strategy),
    - Projektowanie Usług (ang. service design),
    - Przekazanie Usług (ang. service transition),
    - Eksploatacja Usług (ang. service operation),
    - Ustawiczne Doskonalenie Usług (ang. continual service improvement).
c) analiza architektury rozwiązań infrastrukturalnych i ich wsparcia dla świadczonych usług.

2.11. Audyt stosowania Krajowych Ram Interoperacyjności

Zakres zadań obejmuje:

a) przeprowadzenie audytu na zgodność z krajowymi ramami interoperacyjności, w szczególności w zakresie zagadnień:
   - Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami/rejestrami informatycznymi i wspomaganie świadczenia usług drogą elektroniczną:
     i. Usługi elektroniczne,
     ii. Centralne repozytorium wzorów dokumentów elektronicznych,
     iii. Model usługowy,
     iv. Współpraca systemów teleinformatycznych z innymi systemami,
     v. Obieg dokumentów w jednostce,
     vi. Formaty danych udostępniane przez systemy teleinformatyczne.

b. System zarządzania bezpieczeństwem informacji w systemach teleinformatycznych:
   - dokumenty z zakresu bezpieczeństwa informacji, zaangażowanie kierownictwa podmiotu,
   - analiza zagrożeń związanych z przetwarzaniem informacji,
   - inwentaryzacja sprzętu i oprogramowania informatycznego,
   - zarządzanie uprawnieniami do pracy w systemach informatycznych,
   - szkolenia pracowników zaangażowanych w proces przetwarzania informacji,
   - praca na odległość i mobilne przetwarzanie danych,
   - dostęp zdalny,
   - serwis sprzętu informatycznego i oprogramowania,
   - procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji,
   - audyt wewnętrzny z zakresu bezpieczeństwa informacji,
   - kopie zapasowe,
   - projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych,
   - zabezpieczenia techniczno-organizacyjne dostępu do informacji,
   - zabezpieczenia techniczno-organizacyjne systemów informatycznych,
   - rozliczalność działań w systemach teleinformatycznych,

c. Zapewnienie dostępności informacji zawartych na stronach internetowych Partnerów dla osób niepełnosprawnych.

3. Sposób realizacji prac.

Wszystkie prace związane z realizacją zamówienia wykonywane będą w sposób następujący:

1) Audyt, o ktorym mowa w pkt.1., opierać się będzie na wizji lokalnej przeprowadzonej przez wskazane przez Wykonawcę osoby we wszystkich lokalizacjach Partnerów Projektu. Ponadto analiza oparta będzie o wywiad i oświadczenia osoby upoważnionej do reprezentowania Partnera. W przypadku braku możliwości przeprowadzenia wizji lokalnej przez Wykonawcę,

dopuszczalne jest przeprowadzenia prac zdalnie, o ile Partner zapewni taką możliwość. Wykonawca opracuje raporty szczegółowe z Audytu u każdego Partnera oraz raport podsumowujący wszystkie audyty u Partnerów i przekaże je Zamawiającemu;

2) Audyt będzie prowadzony na poziomie trzech warstw: metodologicznej, organizacyjnej oraz dokumentacyjnej;
3) Analiza podatności infrastruktury teleinformatycznej, sytemów i procesów Partnerów odbędzie się w sposób zdalny, z wykorzystaniem zdalnego dostępu o ile taki dostęp będzie możliwy u Partnera, po podpisaniu Umowy powierzenia przetwarzania danych osobowych stanowiącej Załącznik nr 3 do Umowy. W przypadku braku możliwości zdalnego dostępu do Infrastruktury Partnera, analiza zostanie wykonania przez Wykonawcę w siedzibie Partnera;
4) Zamawiający wymaga, aby przedmiotowa analiza i ocena cyberbezpieczeństwa realizowana była w oparciu o normę PN ISO/IEC 27001 oraz normę PN ISO/IEC 22301.

4. Wymagane przepisy prawa i normy

Całość Audytu musi być zgodna z obowiązującymi przepisami prawa i normami. Wykonawca przeprowadzi analizę obowiązujących przepisów uwzględniając między innymi:

1) Rozporządzenie Ministra Zdrowia z dnia 6 kwietnia 2020 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania.
2) Ustawa z 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz. U. 2019 poz. 848)
3) Rozporządzenie Ministra Cyfryzacji z dnia 4 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo (Dz.U. z 2019 r. poz. 2479).
4) Rozporządzenie Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. z 2018 r. poz. 1999).
5) Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 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. z 2017 r. poz. 2247)
6) Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2020 r. poz. 346).
7) Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2020 r. poz. 344).
8) Ustawa z dnia 4 lutego 1994 r. o Prawie autorskim i prawach pokrewnych (Dz.U. z 2019 r. poz. 1231).
9) Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369).

10) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
11) Ustawa o ochronie danych osobowych (Dz.U. 2018 poz. 1000).
12) Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2019 r. poz. 742).
13) Polska Norma PN-ISO/IEC 27001:
    a) PN-ISO/IEC 17799 – w odniesieniu do ustanawiania zabezpieczeń;
    b) PN-ISO/IEC 27005 – w odniesieniu do zarządzania ryzykiem;
    c) PN-ISO/IEC 24762 – w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.

5. Raport z audytu

Zamawiający wymaga aby Wykonawca opracował raporty z przeprowadzonego Audytu u każdego Partnera oraz raport zarządczy, podsumowujący wszystkie Audyty Partnerów i przekazał je Zamawiającemu.

1) Raport z audytu przeprowadzonego u każdego Partnera musi stanowić ocenę cyberbezpieczeństwa teleinfrastruktury Partnerów i zawierać:
    a) cel i zakres przeprowadzonych prac,
    b) opis metodyki prowadzonych prac oraz szczegółowy opis przeprowadzonych prac,
    c) wyszczególnienie narzędzi oraz technik użytych podczas realizacji prac,
    d) szczegółowy opis wykrytych nieprawidłowości lub podatności,
    e) ocenę poziomu ryzyka wraz ze wskazaniem wagi zidentyfikowanych podatności lub błędów w konfiguracji, zawierającą opis potencjalnego wykorzystania wykrytych podatności lub błędów konfiguracyjnych,
    f) mapę ryzyka wystąpienia incydentu, która może mieć wpływ na cyberbezpieczeństwo,
    g) sposób zarządzania incydentami w zakresie cyberbezpieczeństwa,
    h) analizę dostępości do danych i opis mechanizmów bazodanowych (systemy ERP i HIS),
    i) propozycję stworzenia lub aktualizacji procedur i dostosowania systemu zabezpieczeń do standardów zapewniających bezpieczeństwo teleinformatyczne u Partnera,
    j) wykaz proponowanych do zakupu, niezbędnych do zapewnienia cyberbezpieczeństwa urządzeń (infrastruktura sieciowo serwerowa, stacje robocze), oprogramowania oraz licencji, wraz z określeniem parametrów technicznych oraz szacunkową wyceną,
    k) wytyczne, rekomendacje oraz opisy techniczne rozwiązań, dotyczące sposobu wdrożenia odpowiednich, do oszacowanego ryzyka, środków technicznych i organizacyjnych, w tym:
        - utrzymania i bezpiecznej eksploatacji systemów informacyjnych;
        - bezpieczeństwa fizycznego i środowiskowego, uwzględniając kontrolę dostępu;
        - bezpieczeństwa oraz ciągłości dostaw i usług,
        - wdrażania, dokumentowania i utrzymywania planów działania umożliwiajacych ciągłe i niezakłócone świadczenie usług oraz zapewniajacych poufność, integralność, dostępność i autentyczność informacji;

- objęcia systemów teleinformatycznych, wykorzystywanych do świadczenia usług, systemem monitorowania w trybie ciągłym;
- wdrożenia odpowiednich środków organizacyjnych wymaganych obowiązującymi przepisami prawa.

2) Raport zarządczy, podsumowujący wszystkie Audyty u Partnerów musi zawierać:
   a) streszczenie raportów z przeprowadzonych audytów u Parnerów wraz podsumowaniem i zalecanymi działaniami dla Samorządu Województwa Mazowieckiego,
   b) rekomendacje na poziomie województwa w postaci listy sprzętu, oprogramowania oraz licencji do zakupu na rzecz Partnerów w celu zapewnienia cyberbezpieczeństwa teleinfrastruktury wraz z szacunkową wyceną w podziale na kategorie zakupu:
      - krytyczne do natychmiastowej realizacji,
      - niezbędne w celu zapewnieniu prawidłowego działania jednostki,
      - wymagane w najbliższych latach,
      - opcjonalne.
3) Raport z audytu przeprowadzonego u każdego Partnera oraz Raport zarządczy, podsumowujący wszystkie Audyty u Partnerów musi:
   a) być zgodny z zapisami Szczegółowego Opisu Przedmiotu Zamówienia;
   b) być sporządzony poprawnie pod względem stylistycznym i ortograficznym,
   c) zawierać informacje i dane wolne od błędów rzeczowych i logicznych,
   d) być uporządkowany pod względem wizualnym,
   e) być sformatowany w sposób jednolity, wpływając na czytelność i przejrzystość raportu,
   f) w sposób przystępny dla odbiorców prezentować wyniki analiz,
   g) zawierać do wszystkich istotnych wniosków sformułowane rekomendacje,
   h) przedstawiać rekomendacje wynikające w sposób logiczny z wniosków,
   i) zawierać rekomendacje sformułowane w sposób precyzyjny oraz umożliwiający ich bezpośrednie zastosowanie w praktyce.