Znak sprawy: *OR-IV.272.2.1.2014* *Załącznik Nr 1 do SIWZ*

Województwo Podkarpackie
Urząd Marszałkowski Województwa Podkarpackiego

OPIS PRZEDMIOTU ZAMÓWIENIA

w postępowaniu o udzielenie zamówienia publicznego na usługę
pod nazwą:

Audyt zewnętrzny projektu o nazwie „Podkarpacki System Informacji Medycznej" „PSIM"

Zamówienie jest współfinansowane ze środków Unii Europejskiej w ramach Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Państwa w ramach Regionalnego Programu Operacyjnego Województwa Podkarpackiego na lata 2007-2013.

Dokument opracowany przez konsorcjum:
Europejskie Centrum Technologii Informatycznych i Zarządzania ITmed Sp. z o.o.
Nizielski & Borys Consulting Sp. z o.o.

Spis treści

1. Przedmiot zamówienia

Przedmiotem zamówienia jest przeprowadzenie audytu zewnętrznego projektu o nazwie „Podkarpacki System Informacji Medycznej" „PSIM" współfinansowanego ze środków Unii Europejskiej z Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Państwa w ramach Regionalnego Programu Operacyjnego Województwa Podkarpackiego na lata 2007-2013 na podstawie Uchwały.

2. Zakres rzeczowy podlegający audytowi zewnętrznemu

Zakres rzeczowy projektu o nazwie „Podkarpacki System Informacji Medycznej" „PSIM", podlegającego audytowi zewnętrznemu:

2.1. Przedmiotem projektu jest budowa systemu informatycznego pn.: "Podkarpacki System Informacji Medycznej" „PSIM", którego bezpośrednim Beneficjentem będzie Województwo Podkarpackie oraz ośmiu partnerów – wymienionych poniżej podmiotów leczniczych:

1) Specjalistyczny Psychiatryczny Zespół Opieki Zdrowotnej im. prof. Antoniego Kępińskiego w Jarosławiu,
2) Wojewódzki Szpital Podkarpacki im. Jana Pawła II w Krośnie,
3) Wojewódzki Szpital im. Św. Ojca Pio w Przemyślu,
4) Podkarpackiego Centrum Chorób Płuc w Rzeszowie,
5) Wojewódzki Szpital Specjalistyczny im. Fryderyka Chopina w Rzeszowie,
6) Szpital Wojewódzki nr 2 im. Świętej Jadwigi Królowej w Rzeszowie,
7) Wojewódzki Szpital im. Zofii z Zamoyskich Tarnowskiej w Tarnobrzegu,
8) Wojewódzki Podkarpacki Szpital Psychiatryczny im. prof. Eugeniusza Brzezickiego w Żurawicy.

2.2. Podkarpacki System Informacji Medycznej zgodnie z założeniami zawartymi we wniosku o dofinansowanie będzie systemem teleinformatycznym, służącym gromadzeniu, analizie i udostępnianiu zasobów cyfrowych z udzielonymi lub planowanymi świadczeniami opieki zdrowotnej w placówkach służby zdrowia.

2.3. System PSIM będzie miał budowę dwupoziomową obejmującą:

Warstwę regionalną - zlokalizowaną w RCIM, która pełni funkcję integrującą dla Systemu PSIM do którego zostaną podłączone Lokalne systemy informatyczne Partnerów Projektu i Podmiotów leczniczych.

Warstwa regionalna, będzie również posiadać potencjał do podłączenia do systemów informatycznych ogólnokrajowych, które są w fazie tworzenia.

Warstwę lokalną - zlokalizowaną u Partnerów Projektu posiadających Lokalne systemy informatyczne.

Szczegółowy opis Systemu PSIM dostępny jest w dokumentacji przetargowej na wybór Generalnego Wykonawcy (Budowa i wdrożenie Podkarpackiego Systemu Informacji Medycznej: http://www.bip.podkarpackie.pl/index.php/zamowienia-publiczne/dostawy/123-budowa-i-wdrozenie-podkarpackiego-systemu-informacji-medycznej).

3. Cel, zakres i sposób wykonania audytu zewnętrznego Projektu PSIM

3.1. Cel Audytu zewnętrznego Projektu PSIM

Celem przeprowadzenia Audytu zewnętrznego Projektu PSIM jest wydanie przez zewnętrznego audytora opinii w zakresie:

1) poprawności danych liczbowych i opisowych zawartych w dokumentach związanych z realizowanym Projektem PSIM,
2) realizacji wydatków i uzyskania założonych efektów związanych z audytowanym Projektem PSIM, zgodnie z wymaganiami zwartymi w Decyzji o dofinansowanie,
3) działań zarządczych oraz organizacyjnych prowadzonych w Projekcie PSIM,
4) poprawności procedur utrzymaniowych Systemu PSIM oraz polityki bezpieczeństwa RCIM, które opracowane zostaną przez Administratora RCIM,
5) zgodności elementów systemu ze zidentyfikowanymi wymaganiami bezpieczeństwa oraz regulacjami prawnymi,
6) zidentyfikowanych i oszacowanych ryzyk bezpieczeństwa.

3.2. Obszary tematyczne Audytu zewnętrznego

Audyt zewnętrzny Projektu PSIM został podzielony na dwa obszary tematyczne:

3.2.1. Obszar dotyczący organizacji, zarządzania, finansów oraz realizacji Projektu PSIM.

3.2.2. Obszar dotyczący bezpieczeństwa Systemu PSIM.

3.3. Etapy techniczne realizacji Audytu zewnętrznego

Realizacja Audytu zewnętrznego podzielona została na 4 Etapy techniczne:

3.3.1. ET 1 - Audyt cząstkowy organizacyjno – finansowo – zarządczy, w trakcie trwania projektu, zakończony raportem wstępnym (Raport ET1).

3.3.2. ET 2 – Audyt bezpieczeństwa – iteracja pierwsza, zakończony raportem z audytu bezpieczeństwa (Raport ET2).

3.3.3. ET 3 – Audyt bezpieczeństwa – iteracja druga, zakończony raportem finalnym z Audytu bezpieczeństwa (Raport ET3).

3.3.4. ET 4– audyt organizacyjno – finansowo – zarządczy na koniec Projektu PSIM, zakończony raportem finalnym (Raport ET4).

3.4. Szczegółowy opis przedmiotu zamówienia

Szczegółowy zakres realizacji zadań w poszczególnych etapach jest następujący:

3.4.1. Etap techniczny 1

ET 1 - audyt cząstkowy organizacyjno – finansowo – zarządczy, który obejmuje kompleksową analizę dokumentacji, przebiegu oraz działań realizowanych i planowanych do realizacji ze szczególnym uwzględnieniem realizacji przyjętych celów Projektu PSIM wskazanych we Wniosku o dofinansowanie i realizacji postanowień Uchwały nr 7/123/10 Zarządu Województwa Podkarpackiego w Rzeszowie z dnia 28 grudnia 2010 r. w sprawie decyzji o realizacji projektu własnego współfinansowanego z Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Podkarpackiego na lata 2007-2013 Na audyt cząstkowy organizacyjno – finansowo – zarządczy składają się:

3.4.1.1. Audyt organizacji Projektu PSIM w ET1 musi obejmować kompleksowy przegląd organizacyjno – zarządczy projektu w szczególności:

3.4.1.1.1. realizowanych procesów zarządzania Projektem,

3.4.1.1.2. kompletności i jakości dokumentacji zarządczej, w tym sprawozdań z postępu prac w projekcie,

3.4.1.1.3. terminów realizacji działań projektowych,

3.4.1.1.4. prowadzonych działań w zakresie informacji i promocji (w tym stosowanie wytycznych RPO WP oraz zapisów Uchwały),

3.4.1.1.5. wdrożenia uwag/rekomendacji/zaleceń z przeprowadzonych kontroli w projekcie,

3.4.1.1.6. prowadzenia archiwum dokumentacji projektowej (w wersji papierowej oraz elektronicznej) – w zakresie kompletności wymaganej dokumentacji projektowej,

3.4.1.1.7. analiza spełnienia wymagań określonych w polskich oraz międzynarodowych regulacjach prawnych – jako minimalne należy przyjąć dokumenty odniesienia wskazane w Rozdziale 4.

3.4.1.2. Audyt finansowo - księgowy Projektu PSIM ET1, który musi obejmować co najmniej:

3.4.1.2.1. weryfikacja Harmonogramu rzeczowo – finansowego Projektu PSIM w kontekście rozliczania środków UE,

3.4.1.2.2. weryfikacja ewidencji księgowej prowadzonej na potrzeby Projektu PSIM,

3.4.1.2.3. weryfikacja poprawności i terminowości składania wniosków o płatność oraz ich zgodność z księgami rachunkowymi Zamawiającego w części dotyczącej projektu,

3.4.1.2.4. weryfikacja czy ponoszone wydatki są kwalifikowane,

3.4.1.2.5. analiza kosztów Projektu pod kątem zgodności z obowiązującym budżetem i innymi dokumentami tworzonymi w ramach Projektu.

3.4.1.3. Audyt rzeczowej realizacji Projektu PSIM w ET 1, który musi obejmować co najmniej:

3.4.1.3.1. weryfikację kompletności dokumentacji postępowań o udzielenie zamówień publicznych w Projekcie PSIM,

3.4.1.3.2. weryfikację terminowości i jakości realizacji zadań (zgodnie z podpisanymi Umowami) przez Wykonawców, ,

3.4.1.3.3. weryfikację postępu prac w zakresie realizacji wskaźników projektu,

3.4.1.3.4. weryfikację postępu prac w zakresie realizacji wskaźników produktów.

3.4.1.4. Audytor zobowiązany jest do przedstawienia w ramach ET1 w terminie wskazanym w Umowie zaleceń dla jednostek integrowanych z RCIM w zakresie opracowania lub aktualizacji oraz wdrożenia polityk bezpieczeństwa w warstwie lokalnej. W ramach zadania Audytor zobowiązany jest do:

3.4.1.4.1. Przygotowania dokumentu z referencyjnymi wytycznymi do opracowania bądź aktualizacji polityk bezpieczeństwa u Partnerów Projektu oraz jednostek integrowanych z RCIM

3.4.1.4.2. Opracowane wytyczne muszą wynikać z wdrożenia oraz wykorzystania przez pracowników tych podmiotów (Partnerów Projektu oraz jednostek medycznych integrowanych z RCIM) Systemu PSIM oraz obowiązujących przepisów prawa

3.4.1.4.3. Wytyczne będą opracowane na podstawie SIWZ, dokumentacji Systemu PSIM oraz wiedzy i doświadczenia Audytora

3.4.1.4.4. Wytyczne muszą uwzględniać aspekty organizacyjne oraz techniczne dedykowane dla jednostek integrowanych z RCIM.

3.4.1.5. W wyniku zadań wskazanych w pkt. 3.4.1.1 - 3.4.1.3. Audytor zobowiązany jest do przedstawienia **Raportu wstępnego z przeprowadzonych czynności wraz z wnioskami oraz rekomendacjami (Raport ET1)**.

Zakres Raportu ET1 musi zawierać co najmniej:

3.4.1.5.1. Streszczenie dla Kierownictwa

3.4.1.5.2. podstawowe informacje o Beneficjencie i partnerach projektu oraz realizowanym przez nich projekcie PSIM: nazwa, adres, NIP i REGON Beneficjenta oraz partnerów, numer i tytuł projektu, numer Uchwały oraz ewentualnych aneksów, krótki opis projektu, całkowitą wartość projektu, w tym całkowitą wartość wydatków kwalifikowalnych, poziom procentowy i kwotę dofinansowania;

3.4.1.5.3. nazwa, adres, NIP i REGON Wykonawcy przeprowadzającego audyt zewnętrzny Projektu PSIM;

3.4.1.5.4. imiona i nazwiska audytorów zewnętrznych przeprowadzających audyt zewnętrzny Projektu PSIM i określenie uprawnień audytorów;

3.4.1.5.5. oświadczenie audytora zewnętrznego projektu oraz osób wykonujących czynności audytu zewnętrznego projektu o niezależności od audytowanych podmiotów oraz o zachowaniu poufności i nienaruszaniu tajemnic określonych w odrębnych przepisach, w tym tajemnicy przedsiębiorstwa;

3.4.1.5.6. cele audytu;

3.4.1.5.7. data rozpoczęcia i zakończenia audytu zewnętrznego Projektu PSIM w zakresie ET1;

3.4.1.5.8. wykaz dokumentów, które w trakcie audytu stanowiły źródło informacji i stanowiły podstawę badania;

3.4.1.5.9. zakres przedmiotowy i podmiotowy audytu zewnętrznego Projektu PSIM w zakresie ET1;

3.4.1.5.10. podjęte działania i zastosowane techniki audytu, w tym informację o metodzie doboru i wielkości próby do badania oraz charakterystyka przyjętych metod pracy

3.4.1.5.11. wskazanie wartości kwot poddanych badaniu;

3.4.1.5.12. ustalenia stanu faktycznego, w tym:

- jego ocenę,
- wskazanie stwierdzonych ewentualnych problemów, zagrożeń w trakcie realizacji Projektu PSIM wraz ze wskazaniem ich przyczyn, wagi oraz czy jakikolwiek z tych problemów ma charakter powtarzalny, a także uwagi i wnioski w sprawie usunięcia stwierdzonych uchybień, rekomendacje oraz zalecenia, jak również wymagane działania naprawcze, usprawniające i zapobiegawcze (jeżeli są możliwe do wdrożenia w Projekcie PSIM);
- opis obszarów funkcjonujących w sposób poprawny;

3.4.1.5.13. zwięzły opis działań audytowanego podmiotu w obszarze objętym audytem oraz ocenę adekwatności i skuteczności systemu zarządzania i kontroli w obszarze działalności audytowanych podmiotów objętych audytem, w szczególności:

- zgodność - w badanym zakresie - realizacji projektu z Uchwałą i obowiązującymi przepisami prawa oraz procedurami w ramach RPO WP na lata 2007 - 2013, w tym: wskazanie i opis funkcjonowania posiadanych procedur wewnętrznych Beneficjenta (dokumentów);
- opis ścieżki audytu Beneficjenta w zakresie finansowo-księgowym;
- opis prawidłowości klasyfikacji wydatków według kategorii i źródeł finansowania;
- stosowanie przepisów w zakresie zamówień publicznych;
- księgowanie wydatków poniesionych w ramach realizowanego projektu ujętych w złożonych wnioskach o płatność, ocenę kwalifikowalności wydatków, sposób ich dokumentowania i prowadzenia odrębnej ewidencji księgowej (deklarowane wydatki znajdują odzwierciedlenie w zapisach księgowych i dokumentach wspierających prowadzonych przez Beneficjenta oraz są zgodne z zasadami wspólnotowymi i krajowymi);
- analiza terminowości występowania, uzyskiwania i wydatkowania środków na realizację projektu;
- wiarygodność części sprawozdawczych wniosków beneficjenta o płatność z zakresem rzeczowym projektu;
- sposób monitorowania projektu (osiągania celu projektu);
- zgodność z ustalonymi przez MRR (Ministerstwo Rozwoju Regionalnego), IZ (Instytucję Zarządzającą), IW (Instytucję Wdrażającą) wymogami dotyczącymi informacji i promocji projektu;
- sposób przechowywania, udostępniania i archiwizacji dokumentacji zgromadzonej w ramach projektu;

3.4.1.5.14. zaprezentowanie wyników badania, w których stwierdzono nieprawidłowości;

3.4.1.5.15. określenie nieprawidłowości w działalności audytowanego podmiotu oraz analizę ich przyczyn i skutków;

3.4.1.5.16. zalecenia w sprawie usunięcia stwierdzonych nieprawidłowości w działalności audytowanych podmiotów;

3.4.1.5.17. ogólną opinię o projekcie, stanowiącą element sprawozdania, wydaną na podstawie ustaleń zawartych w sprawozdaniu; powody odmowy wydania opinii, z uwagi na okoliczności, które uniemożliwiają jej sformułowanie oraz zawierającą informację o stwierdzonym istotnym naruszeniu prawa wspólnotowego lub krajowego bądź procedur obowiązujących w ramach RPO WP na lata 2007 - 2013 (jeżeli zaistnieje);podpisy każdego z audytorów zewnętrznych przeprowadzających audyt zewnętrzny Projektu PSIM;

3.4.1.5.18. miejsce i datę dzienną sporządzenia oraz podpisania Raportu ET1.

3.4.2. Etap techniczny 2

ET 2 to audyt bezpieczeństwa - pierwsza iteracja, który co najmniej obejmuje:

3.4.2.1. Testy bezpieczeństwa Systemu PSIM, w ramach których Audytor zobowiązany jest do:

3.4.2.1.1. analizy rozwiązań technologicznych w obszarze bezpieczeństwa w kontekście spełnienia wymagań funkcjonalnych oraz pozafunkcjonalnych (zgodnie z SIWZ na GW) na System PSIM w zakresie objętym audytem, które zostaną zastosowane przez Generalnego Wykonawcę zgodnie z Dokumentacją projektową,

3.4.2.1.2. przygotowania scenariuszy testów bezpieczeństwa, które podlegać będą akceptacji Zamawiającego zgodnie z procedurą wskazaną w Umowie,

3.4.2.1.3. weryfikacji gotowości środowiska testowego przygotowanego przez Generalnego Wykonawcę zgodnie z wymaganiami określonymi przez Wykonawcę na potrzeby testów bezpieczeństwa,

3.4.2.1.4. weryfikacja poprawności i kompletności Dokumentacji Systemu PSIM dostarczonej przez Generalnego Wykonawcę w zakresie bezpieczeństwa zgodnie z przedmiotem audytu,

3.4.2.1.5. przeprowadzenia testów bezpieczeństwa obejmujących testy podatności Oprogramowania aplikacyjnego (e-Usługi) i Oprogramowania warstwy integracji, oraz konfigurację i parametryzację sprzętu serwerowego oraz sprzętu sieciowego aktywnego, w szczególności:

- określenie podatności i odporności na stosowane formy ataków, zgodnie z zaleceniami OWASP[1] Top 10 2013[2] (lub późniejszymi jeśli zostaną opublikowane w trakcie trwania realizacji przedmiotu zamówienia),

[1] OWASP (ang. *The Open Web Application Security Project*) należy przez to rozumieć organizację non – profit, która prowadzi działania na rzecz poprawy bezpieczeństwa oprogramowania
[2] https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

- zweryfikowanie możliwości podsłuchu danych wymienianych pomiędzy klientem, a serwerem systemu,
- zweryfikowanie odporności serwerów aplikacji na wprowadzanie niepoprawnych danych, w tym z wykorzystaniem fuzzingu,
- zweryfikowanie mechanizmów zapewniających integralność (weryfikacja możliwości dokonania nieautoryzowanych modyfikacji danych), poufność (weryfikacja możliwości nieautoryzowanego dostępu do danych), rozliczalność przetwarzanych przez system informacji (weryfikacja czy aktywności użytkowników są monitorowane),
- zweryfikowanie wykorzystywanej polityki haseł (w tym weryfikacja nadawanie haseł, weryfikacja siły stosowanych haseł, weryfikacja częstotliwość zmiany haseł, weryfikacja restartowania haseł),
- identyfikacji obecność mechanizmów pozwalających na eskalację uprawnień użytkowników (np. pliki suid w systemach Unix),
- zweryfikowanie konfiguracji mechanizmów logowania zdarzeń,
- badanie podatności systemów informatycznych (aplikacji) wchodzących w skład systemu PSIM dostępnych z sieci Internet,
- badanie podatności urządzeń sieciowych.

3.4.2.2. Testy bezpieczeństwa muszą być prowadzone wg co najmniej następujących typów:

3.4.2.2.1. testy penetracyjne wskazanych zasobów wykonywane metodą white-box,

3.4.2.2.2. testy bezpieczeństwa styku sieci Zamawiającego i Partnerów Projektu z siecią Internet,

3.4.2.2.3. testy bezpieczeństwa aplikacji wytworzonych i dostarczonych przez Generalnego Wykonawcę.

3.4.2.3. W trakcie prowadzenia Testów bezpieczeństwa Audytor zobowiązany jest do wprowadzania na bieżąco zidentyfikowanych Wad z testów do System zgłaszania i przyjmowania uwag oraz Wad zgodnie z kategoryzacją wg Załącznika nr 11 do SIWZ. Do Systemu zgłaszania i przyjmowania uwag oraz Wad muszą być wprowadzane następujące informacje:

3.4.2.3.1. Opis każdej zidentyfikowanej Podatności (w tym błędów w dokumentacji) oraz Luk bezpieczeństwa wykrytych w trakcie testów.

3.4.2.3.2. Opis każdej wykrytej Podatności musi zawierać:

- kategoryzację krytyczności zgłoszonej podatności wraz z analizą ryzyka oraz wpływu na audytowany System,
- analizę przypadku,

- identyfikację sprzętu serwerowego lub aktywnego sprzętu sieciowego, którego dotyczy,
- szczegółowy opis przeprowadzenia badania wraz z opisem problemu i jego możliwe skutki. Opis powinien zawierać przykłady (np. wizualizacja również poprzez obrazy w postaci printscrean, zrzuty logów, itd.),
- opisu Podatności wraz ze wskazaniem możliwych zagrożeń skutków ich wykorzystania.

3.4.2.4. W ET2 Audytor zobowiązany jest do zaproponowania i uzgodnienia z Zamawiającym metodyki szacowania ryzyk bezpieczeństwa oraz identyfikacja i ocena zidentyfikowanych ryzyk.

3.4.2.5. W wyniku realizacji zadań wskazanych w pkt. 3.4.2.1 - 3.4.2.2 Audytor zobowiązany jest do przedstawienia Raportu ET2, który obejmować musi co najmniej:

3.4.2.5.1. Streszczenie dla Kierownictwa;

3.4.2.5.2. Opis metodyki przeprowadzenia audytu bezpieczeństwa, wraz z informacją o wykorzystanych narzędziach;

3.4.2.5.3. Osoby audytujące (imiona oraz nazwiska);

3.4.2.5.4. Oświadczenie audytora zewnętrznego projektu oraz osób wykonujących czynności audytu zewnętrznego projektu o niezależności od audytowanych podmiotów oraz o zachowaniu poufności i nienaruszaniu tajemnic określonych w odrębnych przepisach, w tym tajemnicy przedsiębiorstwa;

3.4.2.5.5. Terminy przeprowadzania czynności audytorskich (dd.mm.rrrr – dd.mm.rrrr);

3.4.2.5.6. Lokalizacje przeprowadzonych czynności audytorskich;

3.4.2.5.7. Przeprowadzone czynności audytorskie (wykaz weryfikowanej dokumentacji, wywiady z pracownikami Zamawiającego oraz przedstawicielami Zespołu Bezpieczeństwa Generalnego Wykonawcy, testy, itd.);

3.4.2.5.8. Wykaz dokumentów, które w trakcie audytu bezpieczeństwa stanowiły źródło informacji i stanowiły podstawę badania;

3.4.2.5.9. Wyniki przeprowadzonego audytu (w tym wynik: analizy dokumentacji oraz wywiadów, audytu wizyjnego, itd.) ze szczególnym uwzględnieniem podatności zidentyfikowanych w trakcie testów bezpieczeństwa, które odnotowane zostaną w Raporcie z testów bezpieczeństwa, którego minimalny zakres informacyjny przedstawiono poniżej:

a. Wyniki każdego z przypadków testowych zgodnie z zaakceptowanymi scenariuszami testów

b. Szczegółową listę wszystkich zidentyfikowanych Podatności (w tym błędów bądź braków w dokumentacji) oraz Luk bezpieczeństwa wykrytych w trakcie testów wraz z opisem przeprowadzonych działań naprawczych przeprowadzonych przez Generalnego Wykonawcę. Każda z Podatności oraz Luk bezpieczeństwa musi być identyfikowana poprzez numer zgłoszenia w Systemie zgłaszania i przyjmowania uwag i Wad.
c. Opis każdej wykrytej Podatności z uwzględnieniem:
   - kategoryzacja krytyczności zgodnie z Załącznikiem nr 11 do SIWZ zgłoszonych podatności wraz z analizą ryzyka oraz wpływu na audytowany System PSIM,
   - analiza przypadku,
   - sprzętu serwerowego lub aktywnego sprzętu sieciowego, którego dotyczy,
   - szczegółowy opis przeprowadzenia badania wraz z opisem problemu i jego możliwe skutki. Opis powinien zawierać przykłady (np. wizualizacja również poprzez obrazy w postaci printscrean, zrzuty logów, itd.),
   - opisu Podatności wraz ze wskazaniem możliwych zagrożeń skutków ich wykorzystania,
   - rekomendacje w zakresie planu działań naprawczych w zależności od zidentyfikowanych Podatności oraz przypisanych im kategorii krytyczności,
   - podsumowanie.

3.4.2.5.10. Raport z testów bezpieczeństwa musi zostać przekazany Zamawiającemu w 3 dniu roboczym po zakończeniu testów bezpieczeństwa. Raport musi być podpisany przez osoby uczestniczące w testach po stronie Audytora.

3.4.3. Etap techniczny 3

ET 3 to audyt bezpieczeństwa – iteracja druga, która obejmuje:

3.4.3.1. Weryfikację polityki bezpieczeństwa dla RCIM.

3.4.3.2. Aktualizację scenariuszy testów bezpieczeństwa z ET 2.

3.4.3.3. Weryfikacja zaktualizowanych dokumentów projektowych opracowanych przez GW oraz Administratora RCIM, które są wynikiem zmian wprowadzonych w Systemie w wyniku zidentyfikowanych Podatności w trakcie testów bezpieczeństwa (w ET 2 oraz ET 3).

3.4.3.4. Re-testy - weryfikacja wprowadzonych przez GW działań wynikających ze zgłoszonych Podatności (w tym luk bezpieczeństwa) w Systemie PSIM zgodnie

z zakresem ET 2 (pkt. 3.4.2.1.5). Audytor zobowiązany będzie do przeprowadzenia maksymalnie 3 iteracji re-testów w ramach ET 3.

3.4.3.5. W trakcie prowadzenia Testów bezpieczeństwa (każdej z iteracji w ramach re-testów) Audytor zobowiązany jest do wprowadzania na bieżąco zidentyfikowanych Wad z testów do system zgłaszania i przyjmowania uwag oraz Wad zgodnie z kategoryzacją wg Załącznika nr 12 do SIWZ. Do Systemu zgłaszania i przyjmowania uwag oraz Wad muszą być wprowadzane następujące informacje:

3.4.3.5.1. Opis każdej zidentyfikowanej Podatności (w tym błędów w dokumentacji) oraz Luk bezpieczeństwa wykrytych w trakcie testów.

3.4.3.5.2. Opis każdej wykrytej Podatności musi zawierać:

- kategoryzację krytyczności zgłoszonej podatności wraz z analizą ryzyka oraz wpływu na audytowany System,
- analizę przypadku,
- identyfikację sprzętu serwerowego lub aktywnego sprzętu sieciowego, którego dotyczy,
- szczegółowy opis przeprowadzenia badania wraz z opisem problemu i jego możliwe skutki. Opis powinien zawierać przykłady (np. wizualizacja również poprzez obrazy w postaci printscrean, zrzuty logów, itd.),
- opisu Podatności wraz ze wskazaniem możliwych zagrożeń skutków ich wykorzystania.

3.4.3.6. Weryfikacja Procedur utrzymaniowych (w tym weryfikacja wykonywania, testowania i odtwarzania kopii zapasowej, procedur monitoringu systemu oraz procedury związanych z operacyjnym utrzymaniem systemu PSIM np. procedura zmian planowych), opracowanych przez Administratora RCIM wraz z niezbędnymi rekomendacjami modyfikacji w opracowanych procedurach,

3.4.3.7. W wyniku realizacji zadań wskazanych w pkt. 3.4.3.1 - 3.4.3.6 Audytor zobowiązanych jest do przedstawienia Raportu ET3, który obejmować musi co najmniej:

3.4.3.7.1. Streszczenie dla Kierownictwa;

3.4.3.7.2. Opis metodyki przeprowadzenia audyt bezpieczeństwa, wraz z informacją o wykorzystanych narzędziach;

3.4.3.7.3. Osoby audytujące;

3.4.3.7.4. Terminy przeprowadzenia czynności audytorskich (dd.mm.rrrr – dd.mm.rrrr);

3.4.3.7.5. Lokalizacje przeprowadzonych czynności audytorskich;

3.4.3.7.6. Wynik analizy polityki bezpieczeństwa RCIM oraz Procedur utrzymaniowych wraz z niezbędnymi rekomendacjami wprowadzenia zmian;

3.4.3.7.7. Wyniki testów bezpieczeństwa przedstawiony w Raporcie z testów bezpieczeństwa, którego minimalny zakres przedstawiony został poniżej:

a. Wyniki każdego z przypadków testowych zgodnie z zaakceptowanymi scenariuszami testów
b. Szczegółową listę wszystkich zidentyfikowanych (wraz z numerem zgłoszenia z Systemu zgłaszania i przyjmowania uwag i Wad) Podatności (w tym błędów bądź braków w dokumentacji) oraz Luk bezpieczeństwa wykrytych w trakcie testów wraz z opisem przeprowadzonych działań naprawczych przeprowadzonych przez Generalnego Wykonawcę,
c. Opis każdej wykrytej Podatności z uwzględnieniem:
   - kategoryzacja krytyczności zgodnie z Załącznikiem nr 12 do SIWZ zgłoszonych podatności wraz z analizą ryzyka oraz wpływu na audytowany System PSIM,
   - analiza przypadku,
   - sprzętu serwerowego lub aktywnego sprzętu sieciowego, którego dotyczy,
   - szczegółowy opis przeprowadzenia badania wraz z opisem problemu i jego możliwe skutki. Opis powinien zawierać przykłady (np. wizualizacja również poprzez obrazy w postaci printscrean, zrzuty logów, itd.),
   - opisu Podatności wraz ze wskazaniem możliwych zagrożeń skutków ich wykorzystania,
   - rekomendacje w zakresie planu działań naprawczych w zależności od zidentyfikowanych Podatności oraz przypisanych im kategorii krytyczności,
   - podsumowanie.

3.4.3.7.8. Raport z testów bezpieczeństwa musi zostać przekazany Zamawiającemu w 3 dniu roboczym po zakończeniu danej iteracji testów bezpieczeństwa w ramach ET3. Raport musi być podpisany przez osoby uczestniczące w testach po stronie Audytora.

3.4.3.7.9. Listę wszystkich zidentyfikowanych Podatności (w tym błędów bądź braków w dokumentacji) oraz Luk bezpieczeństwa wykrytych w trakcie testów wraz z opisem przeprowadzonych działań naprawczych przeprowadzonych przez Generalnego Wykonawcę.

3.4.4. Etap techniczny 4

ET 4 – audyt organizacyjno – finansowo – zarządczy na koniec Projektu PSIM, który obejmuje kompleksową analizę Projektu PSIM wraz z etapem rozliczenia rzeczowego oraz finansowego Projektu. Zakres Etapu technicznego 4 obejmuje:

3.4.4.1. Audyt organizacyjno – finansowo – zarządczy na koniec Projektu PSIM ma na celu:

3.4.4.1.1. weryfikację czy rekomendacje wskazane w Raporcie ET 1 zostały wdrożone w Projekcie PSIM oraz czy pozytywnie wpłynęły na przebieg projektu w obszarze organizacyjno – finansowo – zarządczym,

3.4.4.1.2. uzupełnienie przeglądu przeprowadzonego w ET 1 o weryfikację odpowiadającą swym zakresem ET 1 dla okresu od zakończenia ET 1 do zakończenia realizacji Projektu PSIM,

3.4.4.1.3. zdefiniowanie rekomendacji (na podstawie zebranych informacji o projekcie PSIM oraz wiedzy i doświadczenia zespołu Audytora zewnętrznego) dla organizacji prowadzącej oraz zarządzającej Projektem PSIM (UMWP) dla kolejnych projektów prowadzonych przez Urząd

3.4.4.1.4. uzyskanie oceny, na podstawie zgromadzonych dowodów, pozwalającej stwierdzić, czy realizacja Projektu PSIM przebiegała zgodnie z prawem, procedurami oraz Uchwałą i wnioskiem o dofinansowanie projektu, a wydatki poniesione w ramach Projektu PSIM, zostały prawidłowo zaliczone do wydatków kwalifikowanych lub niekwalifikowanych, zgodnie z założeniami przyjętymi w/w dokumentach;

3.4.4.2. Audytor jako wynik prac w ET 4 musi opracować Raport ET4, w którym przedstawione zostaną wszystkie czynności zrealizowane w ramach audytu organizacyjno – finansowo – zarządczego wraz z wynikami przeglądu i analiz oraz wydana zostanie opinia o przebiegu projektu PSIM:

- opinia pozytywna bez zastrzeżeń lub
- opinia pozytywna z zastrzeżeniami (wykaz uchybień) lub
- opinia negatywna (wykaz nieprawidłowości).

Opinia wydana po zakończeniu audytu zewnętrznego Projektu PSIM powinna także wskazywać wszelkie odstępstwa i ograniczenia w stosunku do celu i zakresu audytu zewnętrznego Projektu PSIM.

Raport końcowy z przeprowadzonego audytu (Raport ET4) musi co najmniej zawierać:

3.4.4.2.1. Streszczenie dla Kierownictwa

3.4.4.2.2. podstawowe informacje o Beneficjencie i partnerach projektu oraz realizowanym przez nich projekcie PSIM: nazwa, adres, NIP i REGON Beneficjenta oraz partnerów, numer i tytuł projektu, numer Uchwały

oraz ewentualnych aneksów, krótki opis projektu, całkowitą wartość projektu, w tym całkowitą wartość wydatków kwalifikowalnych, poziom procentowy i kwotę dofinansowania;

3.4.4.2.3. nazwa, adres, NIP i REGON Wykonawcy przeprowadzającego audyt zewnętrzny Projektu PSIM;

3.4.4.2.4. imiona i nazwiska audytorów zewnętrznych przeprowadzających audyt zewnętrzny Projektu PSIM i określenie uprawnień audytorów;

3.4.4.2.5. oświadczenie audytora zewnętrznego projektu oraz osób wykonujących czynności audytu zewnętrznego projektu o niezależności od audytowanych podmiotów oraz o zachowaniu poufności i nienaruszaniu tajemnic określonych w odrębnych przepisach, w tym tajemnicy przedsiębiorstwa;

3.4.4.2.6. cele audytu;

3.4.4.2.7. data rozpoczęcia i zakończenia audytu zewnętrznego Projektu PSIM;

3.4.4.2.8. zakres przedmiotowy i podmiotowy audytu zewnętrznego Projektu PSIM;

3.4.4.2.9. wykaz dokumentów, które w trakcie audytu stanowiły źródło informacji i stanowiły podstawę badania;

3.4.4.2.10. podjęte działania i zastosowane techniki audytu, w tym informację o metodzie doboru i wielkości próby do badania;

3.4.4.2.11. wskazanie wartości kwot poddanych badaniu;

3.4.4.2.12. ocenę realizacji projektu PSIM;

3.4.4.2.13. zwięzły opis działań audytowanego podmiotu w obszarze objętym audytem oraz ocenę adekwatności i skuteczności systemu zarządzania i kontroli w obszarze działalności audytowanych podmiotów objętych audytem, w szczególności:

- zgodność - w badanym zakresie - realizacji projektu z Uchwałą i obowiązującymi przepisami prawa oraz procedurami w ramach RPO WP na lata 2007 - 2013, w tym: wskazanie i opis funkcjonowania posiadanych procedur wewnętrznych Beneficjenta (dokumentów);
- opis ścieżki audytu Beneficjenta w zakresie finansowo-księgowym;
- opis prawidłowości klasyfikacji wydatków według kategorii i źródeł finansowania;
- stosowanie przepisów w zakresie zamówień publicznych;

- księgowanie wydatków poniesionych w ramach realizowanego projektu ujętych w złożonych wnioskach o płatność, ocenę kwalifikowalności wydatków, sposób ich dokumentowania i prowadzenia odrębnej ewidencji księgowej (deklarowane wydatki znajdują odzwierciedlenie w zapisach księgowych i dokumentach wspierających prowadzonych przez Beneficjenta oraz są zgodne z zasadami wspólnotowymi i krajowymi);
- analiza terminowości występowania, uzyskiwania i wydatkowania środków na realizację projektu;
- wiarygodność części sprawozdawczych wniosków beneficjenta o płatność z zakresem rzeczowym projektu;
- sposób monitorowania projektu (osiągania celu projektu);
- zgodność z ustalonymi przez MRR (Ministerstwo Rozwoju Regionalnego), IZ (Instytucję Zarządzającą), IW (Instytucję Wdrażającą) wymogami dotyczącymi informacji i promocji projektu;
- sposób przechowywania, udostępniania i archiwizacji dokumentacji zgromadzonej w ramach projektu;

3.4.4.2.14. zaprezentowanie wyników badania, w których stwierdzono nieprawidłowości;

3.4.4.2.15. ogólną opinię o projekcie, stanowiącą element sprawozdania, wydaną na podstawie ustaleń zawartych w sprawozdaniu; powody odmowy wydania opinii, z uwagi na okoliczności, które uniemożliwiają jej sformułowanie oraz zawierającą informację o stwierdzonym istotnym naruszeniu prawa wspólnotowego lub krajowego bądź procedur obowiązujących w ramach RPO WP na lata 2007 - 2013 (jeżeli zaistnieje); rekomendacje dla przyszłych projektów, które prowadzone będą w UMWP;

3.4.4.2.16. podpisy każdego z audytorów zewnętrznych przeprowadzających audyt zewnętrzny Projektu PSIM;

3.4.4.2.17. miejsce i datę dzienną sporządzenia oraz podpisania sprawozdania z audytu zewnętrznego Projektu PSIM.

3.5. Forma przekazania Raportów

3.5.1. Raport ET1 zostanie dostarczony do siedziby Zamawiającego i przekazany w 2 egzemplarzach w formie papierowej oraz w formie elektronicznej (doc oraz pdf) na płycie CD/DVD w terminie wskazanym w Umowie.

3.5.2. Raport ET2 oraz Raport ET3, które są wynikiem audytu bezpieczeństwa zostaną dostarczone do siedziby Zamawiającego i przekazane w 2 egzemplarzach w formie papierowej oraz w formie elektronicznej (.doc oraz .pdf) na płycie CD/DVD w terminie wskazanym w Umowie.

3.5.3. Raport końcowy z audytu zewnętrznego (ET4) Projektu PSIM którego elementem koniecznym jest opinia o projekcie, zostanie dostarczony do siedziby Zamawiającego i przekazany w 3 egzemplarzach w formie papierowej oraz w formie elektronicznej (.doc oraz .pdf) na płycie CD/DVD w terminach wskazanych w Umowie.

3.5.4. Wszystkie strony Raportów ET 1 – ET 4 z Audytu zewnętrznego Projektu PSIM powinny być ponumerowane i parafowane przez audytorów zewnętrznych oraz Zamawiającego.

3.5.5. Raporty ET1 – ET4 powinny w sposób bezstronny, kompletny, zrozumiały, jednoznaczny, jasny, rzetelny, zwięzły i zgodny ze stanem faktycznym przedstawiać wyniki Audytu zewnętrznego Projektu PISM (ustalenia, wnioski oraz rekomendacje).

3.5.6. Wnioski i opinie zawarte w Raportach ET1 – ET4 z Audytu zewnętrznego powinny wynikać w szczególności z przeprowadzanych analiz, ocen, weryfikacji dokumentacji oraz testów bezpieczeństwa. Potwierdzenie i opinia zawarta przez audytorów zewnętrznych w sprawozdaniu dotyczy m.in. dokumentów, kwot i informacji odnoszących się do Projektu PSIM istniejących do momentu przeprowadzenia audytu zewnętrznego Projektu PSIM (tj. daty złożenia Raportu do akceptacji Zamawiającego).

3.5.7. Zamawiający będzie miał prawo do odniesienia się do otrzymanej treści Raportów i opinii zgodnie z zasadami określonymi we wzorze umowy stanowiącym Załącznik Nr 7 do SIWZ.

4. Dokumenty odniesienia

1) rozporządzenie Rady (WE) nr 1083/2006 z dnia 11 lipca 2006r ustanawiającym przepisy ogólne dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego oraz Funduszu Spójności i uchylającym rozporządzenie nr 1260/1999,

2) rozporządzenie (WE) nr 1081/2006 Parlamentu Europejskiego i Rady z dnia 5 lipca 2006r w sprawie Europejskiego Funduszu Rozwoju Regionalnego i uchylającym rozporządzenie (WE) nr 1783/1999,
3) rozporządzenie Komisji (WE) nr 1828/2006 z dnia 8 grudnia 2006r ustanawiające szczegółowe zasady wykonania rozporządzenia Rady (WE) nr 1083/2006 ustanawiającego przepisy ogólne dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego oraz Funduszu Spójności oraz rozporządzenia (WE) nr 1080/2006 w sprawie Europejskiego Funduszu Rozwoju Regionalnego,
4) ustawa z dnia 6 grudnia 2006 r o zasadach prowadzenia polityki rozwoju (Dz.U. 2006 nr 227, poz. 1658 z późn. zm.),
5) ustawa z dnia 29 stycznia 2004r Prawo zamówień publicznych (tj. Dz. U. 2007 nr 223, poz.1655 z póz.zm.),
6) ustawa z dnia 29 września 1994r o rachunkowości (Dz. U. 1994 nr 121 poz. 591 z póz. zm.),
7) Regionalny Programem Operacyjnym Województwa Podkarpackiego na lata 2007-2013
8) Szczegółowy Opis Priorytetów Regionalnego Programu Operacyjnego Województwa Podkarpackiego na lata 2007-2013
9) wytyczne Instytucji Zarządzającej Regionalnym Programem Operacyjnym Województwa Podkarpackiego na lata 2007-2013
10) ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych
11) ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne
12) Polska Norma PN-ISO/IEC 27001
13) Raporty i zalecenia CERT.GOV.PL
14) rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024)