Pytanie 1.
Jaka jest szacunkowa liczba pracowników odpowiedzialnych za obszar IT (administratorów IT)?

W PFRON w Departamencie Teleinformatyki zadania administracji Systemem Teleinformatycznym podzielone są pomiędzy:

1. *Administratorów Infrastruktury Teleinformatycznej - administrowanie serwerami do poziomu systemów operacyjnych, zasobami pamięci masowej, urządzeniami aktywnymi sieci LAN (w tym administrowanie oprogramowaniem firmware urządzeń).*
2. *Administratorzy oprogramowania aplikacyjnego i bazodanowego.*
3. *Administratorzy oprogramowania i sprzętu na stanowiskach pracy, w tym usług Active Directory.*

LP	*Administratorzy*	*Liczba Osób*
1	*Administratorów Infrastruktury Teleinformatycznej*	*5*
2	*Administratorzy oprogramowania aplikacyjnego i bazodanowego*	*5*
3	*Administratorzy oprogramowania i sprzętu na stanowiskach pracy*	*4*

PFRON posiada podpisane umowy serwisu pogwarancyjnego dla urządzeń i oprogramowania elementów infrastruktury teleinformatycznej, umowy wsparcia technicznego (maintenance) dla oprogramowania aplikacyjnego i bazodanowego.

Pytanie 2.
Jaka jest liczba utrzymywanych systemów teleinformatycznych objętych zakresem audytu (np. aplikacja WWW, gruby klient, cienki klient) ?

W PFRON wykorzystywane są trzy systemy dedykowane obsługujące zadania ustawowe Funduszu. Systemy te przetwarzają dane osobowe i wrażliwe dane osobowe:

1. *System Obsługi Dofinansowań i Refundacji SODIR wspiera zadanie wypłaty dofinansowań i refundacji zgodnie z zpisami* ustawy *z dnia 27 sierpnia 1997 roku o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych (Dz. U. z 2011 r. Nr 127, poz. 721, ze zm.), a także Rozporządzeniami Wykonawczymi.*
   - *W obszarze Back-End system działa w architekturze trójwarstwowej w oparciu o oprogramowanie Oracle (Oracle WebLogic i Oracle DataBase Enterprise Edition) działające na serwerach zlokalizowanych w Biurze Funduszu w Warszawie, al. Jana Pawła II 13. Obszar Back-End systemu SODiR1 składa się z dwóch podsystemów: Podsystemu Centralnego i Podsystemu Finansowego. W obszarze Back-End System SODiR zawiera 2 046 tabel, 769 widoków, 450 pakietów funkcji i procedur, 43 funkcje, 94 procedury. W tabelach zdefiniowano około 21 000 kolumn.*

- *w obszarze Front-End system działa w architekturze trójwarstwowej w oparciu o oprogramowanie aplikacyjne Jboss i bazy danych PostgreSQL działające na serwerach w siedzibie hostingodawcy.*

2. *System Ewidedencji i Poboru Wpłat Neo wspiera realizację przez PFRON zadań z zakresu obsługi pracodawców zobowiązanych do dokonywania obowiązkowych wpłat na Fundusz lub zwolnionych z tych wpłat – wynikających z ustawy z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych (Dz.U. z 2011 r. Nr 127, poz. 721, z późn. zm.).*
   - *W obszarze Back-End system działa w architekturze trójwarstwowej w oparciu o serwery aplikacyjne Oracle WebLogic i bazę danych RDBMS Informix działające na serwerach zlokalizowanych w Biurze Funduszu w Warszawie, al. Jana Pawła II 13. Baza danych systemu Neo w obszarze Front-End zawiera 566 tabel, 44 widoki, 21 funkcji i 19 procedur. W tabelach zdefiniowano około 8 100 kolumn.*
   - *W obszarze Front-End (system e-PFRON2) system działa w architekturze trójwarstwowej w oparciu o serwer WWW i oprogramowanie PHP, framework Symfony2 oraz bazę PostgreSQL działające w na serwerach w Biurze Funduszu w Warszawie, al. Jana Pawła II 13.*

3. *System Obsługi Finansowej PFRON SOF2 wspiera obsługę zdarzeń finansowych w obszarze głównej księgi rachunkowej, kadr i płac, ewidencji środków majątkowych, obsługi dofinansowań i pozyczek oraz windykacji cywilno-prawnej. System działa w architekturze trójwarstwowej w oparciu o oprogramowanie Oracle (Oracle WebLogic i Oracle DataBase Enterprise Edition) działające na serwerach zlokalizowanych w Biurze Funduszu w Warszawie, al. Jana Pawła II 13. Baza danych systemu SOF2 zawiera 2 659 tabel, 845 widoków, 505 pakietów funkcji i procedur, 198 funkcji, 65 procedur i 2 joby. W tabelach zdefiniowano około 7 700 kolumn.*

Fundusz wykorzystuje także następujące aplikacje działające w architekturze trójwarstwowej:

1. *Aplikacja PAWOR oparta o serwer PHP i bazę danych MySQL zintegrowana z bazą danych SODiR wspierająca windykację administracyjna należności z tytułu udzielonych przez PFRON dofinansowań i refundacji. Aplikacja PAWOR w warstwie bazodanowej jest zrealizowana przez 54 tabele, 4 widoki, 74 funkcje i 6 procedur.*
2. *Aplikacja KIKW oparta o serwer PHP i bazę danych MySQL zintegrowana z bazą danych SODiR i wykorzystująca serwer plików wspierająca działania Departamentu Kontroli i Windykacji – prowadzenie kontroli, korespondencja z kontrolowanymi podmiotami, protokoły kontroli. Aplikacja KIKW w warstwie bazodanowej jest zrealizowana przez 184 tabele, 10 funkcji i 6 procedur.*
3. *Aplikacja SWKZ/PADIR wspiera działania kontrolerów PFRON w prowadzeniu w siedzibie pracodawcy kontroli zgodności z prawem uzyskanych środków finansowych z PFRON. Aplikacja w części centralnej jest aplikacją oparta o serwer PHP i bazę MySQl i jest zintegrowana z bazą danych systemu SODiR1. W części wspierającej pracę kontrolerów PFRON w terenie aplikacja działa w architekturze trójwarstwowej w środowisku opartym o WMAPSERWER. Aplikacja SWKZ/PADIR przetwarza dane osobowe. Aplikacja SWKZ/PADIR w warstwie bazodanowej jest zrealizowana przez 133 tabel, 3 widoki, 58 funkcji i 10 procedur.*

Ponadto Fundusz wykorzystuje około 40 aplikacji stworzonych w oparciu o LotusDomino. Część z tych aplikacji przetwarza dane osobowe. Część aplikacje stworzona w oparciu o oprogramowanie LotusDomino jest dostępna przez przeglądarkę internetową. W oparciu o oprogramowanie LotusDomino działa także w PFRON poczta elektroniczna.

Dodatkowo PFRON utrzymuje stronę internetową Funduszu www.pfron.org.pl działającą w oparciu o silniki CMS Typo3 oraz stronę informacyjną serwisu e=pfron2 https://pracodawca.e-pfron.pl/login opartą o system CMS Joomla.

Pytanie 3.
Jaka jest liczba serwerów fizycznych / serwerów wirtualnych objętych zakresem audytu?

Liczba serwerów fizycznych – 40
Liczba serwerów wirtualnych - 48

Pytanie 4.
Jaka jest liczba pomieszczeń serwerowni / lokalnych punktów dystrybucyjnych objętych zakresem audytu?

Fundusz dysponuje dwoma serwerowniami mieszczącymi się w budynku Biura PFRON w Warszawie, al. Jana Pawła II 13. W każdym oddziale Funduszu i lokalizacjach w Warszawie istnieją punkty dystrybucyjne sieci LAN/WAN. Adresy oddziałów i lokalizacji zawiera tabela poniżej:

Oddział/Lokalizacja	***Lokalizacja***
Dolnośląski	*ul. Szewska 6/7, 50-053 Wrocław*
Kujawsko-Pomorski	*ul. Szosa Chełmińska 30, 87-100 Toruń*
Lubelski	*ul. W. Kunickiego, 20-422 Lublin*
Lubuski	*ul. Bohaterów Westerplatte 11, 65-034 Zielona Góra*
Łódzki	*ul. Kilińskiego 169, 90-353 Łódź*
Małopolski	*ul. Na Zjeździe 11, 30-527 Kraków*
Mazowiecki	*ul. Grójecka 19/25, 02-021 Warszawa*
Opolski	*ul. Katowicka 55, 45-061 Opole*
Podkarpacki	*ul. Rejtana 10, 35-310 Rzeszów*
Podlaski	*ul. Fabryczna 2, 15-483 Białystok*
Pomorski	*ul. Grunwaldzka 184, 80-266 Gdańsk*
Śląski	*pl. Grunwaldzki 8-10/8, 40-950 Katowice*
Świętokrzyski	*Al. IX Wieków Kielc 3, 25-516 Kielce*
Warmińsko-Mazurski	*ul. A. Mickiewicza 21/23, 10-508 Olsztyn*
Wielkopolski	*ul. Lindego 4, 60-573 Poznań*
Zachodniopomorski	*al. Powstańców Wielkopolskich 33, 70-111 Szczecin*
Lokalizacja Amew Invest	*al. Jana Pawła II 11, 00-828 Warszawa*
Lokalizacja Sienna	*ul. Sienna 63 ,00-820 Warszawa*
Lokalizacja Kolejowa	*ul. Kolejowa 19/21, 01-217 Warszawa*
Biuro PFRON	*al. Jana Pawła II 13, 00-828 Warszawa*

Pytanie 5.
Jaka jest liczba urządzeń sieciowych z rozbiciem na poszczególne typy (zapora sieciowa, trasownik, przełącznik) objętych zakresem audytu?

Zapora sieciowa : 6
Trasownik : 23
Przełącznik : 74

Pytanie 6.
Czy w organizacji wytwarza się oprogramowanie?

Tak, w organizacji wytwarza się oprogramowanie.

Pytanie 7.
Czy w organizacji zdefiniowano i wdrożono formalne dokumenty w zakresie bezpieczeństwa informacji? Jeżeli tak, proszę podać ich zakres przedmiotowy (np. obszar ochrony fizycznej, obszar teleinformatyki, zarządzanie incydentami, itd.)?

W PFRON opracowano:
1. *Polityka bezpieczeństwa danych osobowych*
2. *Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych*

Aktualna wersja tych dokumentów obowiązuje od 31 lipca 2015 r.

Pytanie 8.
W ramach pkt. 4 Zapytania ofertowego na usługę audytu bezpieczeństwa teleinformatycznego Zamawiający określił wymagania dla osób w zakresie posiadanych certyfikatów. Zgodnie z zapytaniem Zamawiający wymaga certyfikatu CISM lub CISA lub CISSP lub CEH lub certyfikatów równoważnych dla każdego powyższych. Czy Zamawiający dopuści jako równoważny certyfikat OSCP (Offensive Security Certified Professional), https://www.offensive-security.com/information-security-certifications/oscp-offensive-security-certified-professional/ dla certyfikatu CISSP lub CISA lub CISM? Certyfikat OSCP potwierdza praktyczne umiejętności w zakresie prowadzenia audytów oraz testów bezpieczeństwa ze szczególnym uwzględnieniem testów penetracyjnych. Osoby posiadające ten certyfikat, muszą poprzez wskazanie wad symulowanych środowisk informatycznych, udowodnić swoje kompetencje w wymiarze praktycznym.

Zamawiający dopuści jako równoważny do certyfikatu CISM lub CISA lub CISSP lub CEH certyfikat OSCP.

Pytanie 9.
Ile webaplikacji będzie podlegało testom?

Wykaz aplikacji zawiera odpowiedź na pytanie 2.

Pytanie 10.

Ile łącznie pól formularzy zawierają wymienione wyżej aplikacje?

LP	System	Szacunkowa liczba formularzy służacych do wprowadzania danych	Szacunkowa liczba pól do wprowadzania danych *	Uwagi
1.	System SODiR – obszar Front-End	65	2 925	Liczba pól zależna od typu dokumentu
2.	System SODiR – obszar Back-End	110	3 225	Wartości szacunkowe
3.	System Neo – obszar Front-End	80	4 500	Liczba pól zależna od typu dokumentu
4.	System Neo – obszar Back-End	1 000	7 500	Bez formatek precyzujących kryteria wyszukiwania
3.	System obsługi finansowej SOF2	574	2 870	Przyjęto, że każdy formularz służy średnio do wprowadzenia 5 pól
4.	Aplikacja Pawor	4	20	
5.	Aplikacja KIKW	10	50	
6.	Aplikacja SWKZ/PADIR	10	Do 2 000 pól	Formularze do rejestracji danych mogą być tworzone dynamicznie (rejestry błędów)
7.	Aplikacje LotusDomino **	400	Do 8 000 pól	Wartość szacunkowa

*) Wartość szacunkowa. Błąd około 10 % . Nie uwzględniono pól wprowadzanych przy tworzeniu kryteriów wyszukiwania

**) Wartości szacunkowe dla około 40 aplikacji

Pytanie 11.

Jakie role w webaplikacjach mają zostać przetestowane, czy są to: gość, użytkownik, administrator, czy występują też inne np. moderator, redaktor i czy mają zostać przetestowane? Czy każda aplikacja ma taki sam zestaw ról? Jeśli nie, prosimy o wyszczególnienie.

Uprawnienia do systemów SODiR1 w obszarze Back-End , Neo w obszarze Back-End i SOF2 przyznawane są w sposób hierarchiczny. Poziom najwyższy to lokalizacja. Ten poziom został zaimplementowany tylko w systemie SODiR1 w obszarze Back-End Podsystemu Centralnego. Poziom lokalizacji określa uprawnienia do danych dla pracodawców z określonego województwa. Poniżej poziomu lokalizacji zdefiniowany jest poziom modułu uprawnień. Termin „moduł" został wprowadzony w systemie SODiR1w obszarze Back-End Podsystemu

Centralnego. W obszarze Back – End systemu Neo poziom ten nosi nazwę „kategorii", zaś w systemie SOF2 i w systemie SODIR1 w obszarze Back-End w Podsystemie Finansowym nazwę „węzła". W ramach modułu (odpowiednio kategorii lub węzła) definiowane są uprawnienia (dla Neo to odpowiednio bramka, zaś dla SOF2 i SODIR1 w obszarze Back-End dla Podsystemu Finansowego to grupa). Uprawnienie (bramki, grupy) definiują prawa do poszczególnych obiektów bazy danych. W systemie SODiR1 w obszarze Back-End w Podsystemie Centralnym predefiniowane uprawnienia w ramach modułu to: czytelnik, operator, administrator i koordynator.
Dla aplikacji PAWOR, KIKW, SWKZ/PADIR najwyższym poziomem uprawnień jest moduł. Dla każdego modułu utworzone są następujące predefiniowane uprawnienia: czytelnik, użytkownik, kierownik i administrator.
Uprawnienia dla beneficjentów do systemu SODIR1 w obszarze Front-End są nadawane na pisemny wniosek beneficjenta. W systemie SODIR1 w obszarze Front-End isntnieje tylko jeden rodzaj uprawnień.
Uprawnienia dla pracodawców do systemu Neo w obszarze Front-End (system e-PFRON2) są nadawane na pisemny wniosek pracodawcy. Realizacja wniosku polega na nadaniu roli Administratora wskazanej we wniosku osobie. Administrator może zakładać innych użytkowników systemu dla danego pracodawcy przypisując im predefiniowane role „użytkownika" lub „pracownika". Dla pracowników PFRON w systemie Neo w obszarze Front-End (System e-PFRON2) istnieją predefiniowane uprawnienia Administratora, Operatora i Operatora-tylko do odczytu.
Uprawnienia do aplikacji LotusDomino są nadawane przy wykorzystaniu mechanizmu serwera LotusDomino.
Podsumowując, liczba testowanych ról musi być określona indywidualnie w zależności od systemu. W ofercie proszę podać cenę przetestowania 10 grup uprawn/uprawnień/bramek.

Pytanie 12.
Ile jest hostów/IP w sieci? W tym:
12.1 Ile serwerów bazodanowych?
12.2 Ile serwerów plikowych?
12.3 Ile serwerów aplikacyjnych?

Liczba hostów, w tym stacji roboczych i drukarek to około 1 500.
W PFRON istnieje około 20 logicznych lub fizycznych hostów, na których działają bazy danych, 1 logiczny serwer plików, około 15 serwerów aplikacyjnych. Powyższe liczby obejmują zarówno instancje produkcyjne, jak i testowe.

Pytanie 13.
Ile występuje podsieci?

W PFRON w oddziałów i lokalizacjach wyszczególnionych w odpowiedzi na Pytanie 4 wynosi około 80.

Pytanie 14.

Uprzejmie prosimy o informację dot. ilości (sztuk) komponentów wymienionych w pkt 2.1. Zapytania ofertowego, wchodzących w zakres testów i audytów.

LP	***Systemy i warstwy poddane testowaniu i audytowi***	*Liczba*	*Uwagi*
1.	*Systemy CMS/aplikacje www*	*Około 20 aplikacji*	*W oszacowaniu uwzględniono aplikacje LotusDomino dostępne przez przeglądarkę.*
2.	*Sieciowe urządzenia brzegowe*	*6*	
3.	*Routery ekranujące i bramy*	*21*	
4.	*Systemy firewall*	*6*	
5.	*Serwery Proxy*	*2*	
6.	*Usługi VPN*		
7.	*Systemy antywirusowe*	*1*	*System Kaspersky EndPoint Security*
8.	*Systemy tworzenia i odtwarzania kopii zapasowych*	*1*	*HP DataProtector*
9.	*Serwery aplikacji,*	*13*	*Serwy PHP, Oracle Web Logic*
10.	*Systemy monitorowania dostępności*	*1*	*Oprogramowanie Zabbix – agenci zainstalowani na około 10 serwerach*
11.	*Serwery DNS*	*4*	
12.	*Serwery i usługi poczty elektronicznej*	*1*	*1 serwer WMWare i system LotusDomino*
13.	*Systemy operacyjne*	*6*	*HP-UX, RedHat Linux, Debian Linux,MS Windows Serwers, MS Windows XP, MS Windows 7, MS Windows 10*
14.	*Systemy baz danych*	*4*	*Informix, Oracle, PostgreSQL, MySQL*
15.	*System usług katalogowych(Active Directory),*	*1*	
16.	*Warstwy dostępowe do usług bankowości elektronicznej*	*1*	*Dostęp do aplikacji BG@24BIZNES*
17.	*System obiegu dokumentów*	*1*	*Aktualnie wdrażany EZD-POW*
18.	*Usługi dostępu do danych dedykowane dla urządzeń mobilnych oraz konfiguracje urządzeń mobilnych*	*1*	*Lotus Notes Traveler*

19.	*Usługi udostępniane dla użytkowników systemów wspierających realizowanie statutowych zadań PFRON*	*2*	*System SODIR1 obszar Front-End, System Neo obszar Front-End*

Pytanie 15.
Czy zestaw zadań określony w pkt. 2.1 Zapytania ofertowego, należy powielić i zrealizować we wszystkich oddziałach Funduszu.

W oddziałach i lokalizacjach wyszczególnionych w odpowiedzi na Pytanie 4 należy wykonać ocenę bezpieczeństwa fizycznego infrastruktury teleinformatycznej oraz przeprowadzić testy nieuprawnionego dostępu do systemów i aplikacji PFRON poprzez stacje robocze tam zlokalizowane.

Pytanie 16.
Uprzejmie prosimy o uściślenie, listy oddziałów objętych audytem i testami.

Listę oddziałów zawiera odpowiedź na Pytanie 4.

Pytanie 17.
Czy Zamawiający uzna za równoważny dla CISM - certyfikat CRISC.
Nie.

Pytanie 18.
Punkt 4 Zapytania ofertowego - Czy Wykonawca prawidłowo rozumie, iż Zmawiający oczekuje wykazania, iż poszczególni pracownicy Wykonawcy uczestniczyli w min. 3 audytach systemów teleinformatycznych czyli łącznie 6 audytów (przy zespole 2 - osobowy) a dodatkowo należy przedstawić referencję wydane na te poszczególne osoby?

Osoby, wskazane w ofercie mogły w przeszłości uczestniczyć w tych samych audytach. Stąd wskazana w pytaniu liczba 6 koniecznych audytów jest liczbą maksymalną.
Ponadto Zamawiający dopuszcza przedstawienie dokumentów potwierdzających wykonanie przez Wykonawcę w ciągu ostatnich trzech lat trzech audytów bezpieczeństwa systemów teleinformatycznych w zakresie, o którym mowa w pkt. 4. Dokumenty te muszą być wystawione przez podmiot, na rzecz którego usługa audytu została wykonana. Dodatkowo w takim przypadku Wykonawca przedstawi dokumenty potwierdzające udział pracowników Wykonawcy w tych audytach.

Pytanie 19.
Miejsce i termin składani ofert - uprzejmie prosimy o przedłużenie terminu składania ofert min. do 25.05.2017r. Wykonawcy zależy na przygotowaniu rzeczowej oferty, która w odpowiedni sposób będzie adresować potrzeby Klienta.

Zamawiający przedłuża termin składania ofert do 29.05.2017 do godz.12.00. Jednocześnie, Zamawiający zastrzega sobie prawo do nie udzielania odpowiedzi na pytania, które zostaną dostarczone do Zamawiającego po godz. 12.00 dnia 19.05.2017.

Pytanie 20.
Zwracam się z zapytaniem, czy Zamawiający dopuści do udziału w postępowaniu 2 osoby z w wymaganymi certyfikatami (każda z nich posiada po jednym, różnym certyfikacie), i które w ostatnim roku wykonały co najmniej 1 audyt systemów teleinformatycznych?

Obecne warunki ograniczają udział konkurencji w przetargu. Uniemożliwiają również Zamawiającemu uzyskanie większej ilości ofert, które mogą okazać się bardziej atrakcyjne cenowo.
Z kolei zakres tematyczny poświadczony certyfikatami:
- **CISM: Certified Information Security Manager**
- **CISA: Certified Information System Auditor**
- **CISSP: Certified Information System Security Professional**
- **CEH: Certified Ethical Hacker**

jest zbliżony do siebie, a główna różnica polega na tym, iż wydawane są przez inne jednostki certyfikujące, dlatego wiedza uzyskana i potwierdzona jednym z w/w certyfikatów jest wystarczająca na przeprowadzenie usługi na wysokim poziomie.

Zamawiający, z zastrzeżeniem odpowiedzi na pytanie 8, podtrzymuje wymagania opisane w pkt. 4 Zapytania ofertowego.

Dyrektor Departamentu
ds. Teleinformatyki
Damian Dyndo