INNOWACYJNA GOSPODARKA
NARODOWA STRATEGIA SPÓJNOŚCI

pl.ID

UNIA EUROPEJSKA
EUROPEJSKI FUNDUSZ
ROZWOJU REGIONALNEGO

# Ministerstwo Spraw Wewnętrznych

# Raport z ekspertyzy IT projektu pl.ID

*Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1„Społeczeństwo informacyjne – budowa elektronicznej administracji"*

**Historia zmian dokumentu**

| Nr wersji | Data | Autor zmiany | Opis zmiany |
|---|---|---|---|
| 1.11 | 19.12.2014 | Andrzej Tyrowicz | Drobne poprawki Zamawiającego do wersji końcowej |
| 1.10 | 19.12.2014 | Andrzej Tyrowicz | Autopoprawka z uzupełnieniem listy dokumentów |
| 1.00 | 19.12.2014 | Andrzej Tyrowicz | Finalna edycja do dostawy |
| 0.99 | 19.12.2014 | Jerzy Niepostyn | Przegląd jakości przed dostawą |
| 0.93 | 19.12.2014 | Andrzej Tyrowicz | Uzupełnienia i edycja przed dostawą |
| 0.92 | 19.12.2014 | Jerzy Niepostyn | Uzupełnienia metodyki budowy oprogramowania |
| 0.91 | 18.12.2014 | Andrzej Tyrowicz | Wprowadzone uwagi Zamawiającego do wersji 0.9 |
| 0.9 | 18.12.2014 | Andrzej Tyrowicz | Draft dostawy dla Zamawiającego, |
| 0.52 | 17.12.2014 | Andrzej Tyrowicz | Uzupełnienie obserwacji, wniosków i rekomendacji |
| 0.45 | 15.12.2014 | Jerzy Niepostyn | Uzupełnienie obserwacji i rekomendacji |
| 0.40 | 12.12.2014 | Jerzy Niepostyn | Uporządkowanie i aktualizacja do pierwszego draftu |
| 0.30 | 11.12.2014 | Jerzy Niepostyn | Uzupełnienie dokumentu od pozostałych ekspertów |
| 0.20 | 4.12.2014 | Jerzy Niepostyn | Utworzenie dokumentu |

**Lista dystrybucyjna**

| LP | Imię i nazwisko | Rola w procesie / Stanowisko |
|---|---|---|
| 1. | Tomasz Szubiela | Sponsor projektu pl.ID, Podsekretarz Stanu MSW |
| 2. | Anna Siejda | Z-ca Dyrektora Departament Ewidencji Państwowych MSW |
| 3 | Wojciech Żukowski | Radca Ministra, Departament Ewidencji Państwowych MSW |
| 4. | Dariusz Czerniawski | Ekspert w Departamencie Ewidencji Państwowych MSW |
| 5. | Przemysław Kuna | Ekspert w Departamencie Teleinformatyki MSW |

**Zatwierdzone**

| Data | Imię i nazwisko | Rola w procesie / stanowisko | Podpis |
|---|---|---|---|
| 19.12.2014 | Jerzy Niepostyn | Ekspert ds. Wdrożeń | |
| 19.12.2014 | Dariusz Czerniawski | Ekspert ds. ew. | |
| | | | |
| | | | |
| | | | |
| | | | |



*Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1„Społeczeństwo informacyjne – budowa elektronicznej administracji"*

**Spis treści**




*Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1„Społeczeństwo informacyjne – budowa elektronicznej administracji"*

# Wykaz użytych skrótów oraz symboli

| Skrót | Znaczenie |
|---|---|
| BIA | Business Impact Analysis[1] |
| BUSC | Baza Urzędów Stanu Cywilnego – komponent SRP |
| CEPIK | Centralna Ewidencja Pojazdów i Kierowców – system zewnętrzny do SRP |
| CRS | Centralny Rejestr Sprzeciwów |
| COI | Centralny Ośrodek Informatyki Ministerstwa Spraw Wewnętrznych |
| DEP | Departament Ewidencji Państwowych, właściciel biznesowy SRP |
| OEWiUDO | Ogólnokrajowa Ewidencja Wydanych i Unieważnionych Dowodów Osobistych |
| PESEL | Powszechny System Ewidencji Ludności |
| RDO | Rejestr Dowodów Osobistych – komponent SRP |
| RPO | Recovery Point Objective,[2] |
| RTO | Recovery Time Objective [3] |
| SRP | System Rejestrów Państwowych – zespół współdziałających systemów PESEL, BUSC, RDO, RWPiDP, SOP |
| SOP | System Odznaczeń Państwowych – komponent SRP |
| UML | Unified Modelling Language |
| Umowa | Umowa Nr 679/DEP/4.8./2014 z 4 grudnia 2014 r. |
| | |

[1] *Wiki: Business impact analysis (BIA) differentiates critical (urgent) and non-critical (non-urgent) organization functions/activities. (Analiza wpływu biznesowego wprowadza rozróżnienie pomiędzy krytycznych i niekrytycznymi funkcjami/czynnościami organizacji).*

[2] *Wiki: "RPO", is defined as the maximum targeted period in which data might be lost from an IT service due to a major incident. (Maksymalny okres utraty danych w wyniku incydentu)*

[3] *Wiki: "RTO" is the targeted duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity. (Maksymalny okres czasu, w którym po niespodziewanym przerwaniu proces musi być ponownie dostępny w celu uniknięcia nieakceptowalnych konsekwencji)*



*Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1„Społeczeństwo informacyjne – budowa elektronicznej administracji"*

# Streszczenie dla Kierownictwa

Dokument niniejszy pt. „Raport z ekspertyzy IT projektu pl.ID" jest wynikiem ekspertyzy IT dokumentacji udostępnionej przez Zamawiającego. Celem raportu było przedstawienie beneficjentom ekspertyzy IT odpowiedzi na pytania w zakresie poprawności realizacji projektu pl.ID w aspekcie wymagań funkcjonalnych, wydajnościowych, zarządzania zmianą, ryzykiem oraz ciągłością działania. Ekspertyza IT obejmowała swoim zakresem ocenę wspomnianych wyżej aspektów wyłącznie w odniesieniu do systemu pl.ID.

Na główne pytania ekspertyzy udzielono jednoznacznie niepozytywnych odpowiedzi. Na podstawie zgromadzonych obserwacji i przedstawionych dla nich wniosków wypracowano rekomendacje przedstawione tabelarycznie w grupach dla każdego z pytań postawionych przed ekspertyzą (zgromadzono je w rozdziale 5.). Główne zagrożenia wynikające z niewprowadzenia rekomendacji to :

1) Niekontrolowanie wydłużony proces implementacji i faktycznego wdrażania SRP.
2) Niezapewnienie świadczenia wymaganego poziomu usług przez wdrożony SRP;
3) Przerwy w świadczeniu usług przez SRP, ciągłości działania całości lub bardzo wielu elementów krytycznych systemów państwa w zakresie bezpieczeństwa i ochrony zdrowia i zakłócenia funkcjonowania praktycznie wszystkich systemów państwa.
4) Długotrwałe przerwy w świadczeniu wszelkich usług przez System Rejestrów Państwowych;
5) Powiększanie skutków dowolnej awarii SRP;
6) Niegospodarność wyrażająca się nieuzasadnionymi i nadmiernymi kosztami inwestycyjnymi i utrzymaniowymi infrastruktury SRP;
7) Nieskuteczność i nieefektywność wprowadzania zalecanych rozwiązań organizacyjnych w COI.

Najistotniejsze obserwacje, wnioski i rekomendacje związane są z brakiem widocznych procedur zapewnienia jakości oprogramowania i zarządzania zmianami oraz z niezapewnieniem ciągłości działania.

W dotychczasowych pracach nad projektem pl.ID Wykonawca systemu poświęcił dużo uwagi i zasobów projektowych zapewnieniu bezpieczeństwa oraz zagadnieniom architektonicznym. Niestety, jak zazwyczaj zdarza się w przypadku systemów budowanych wewnątrz organizacji, bardzo trudno jest zapewnić niezbędny poziom jakości i pielęgnowalności (ang. *maintainability*)[4] oprogramowania. Ten właśnie aspekt powoduje teraz niekontrolowane w istocie opóźnienia w procesie akceptacji i nadchodzącym wdrażaniu systemu. W udostępnionych dokumentach oraz w strukturach organizacyjnych i projektowych brakuje wydzielenia ról i przypisania odpowiedzialności za zapewnienie jakości. Zdaniem Wykonawcy ekspertyzy pomijanie szeroko pojętej jakości w projekcie pl.ID jest źródłową przyczyną większości napotykanych obecnie i nadchodzących problemów. Wprowadzanie

[4] *Za testerzy.pl:* ***pielęgnowalność****: Łatwość, z którą oprogramowanie może być modyfikowane w celu naprawy defektów, dostosowania do nowych wymagań, modyfikowane w celu ułatwienia przyszłego utrzymania lub dostosowania do zmian zachodzących w jego środowisku. [ISO 9126]*


Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1„Społeczeństwo informacyjne – budowa elektronicznej administracji"

najbardziej nowatorskich architektur, technologii i metodyk nie może odbywać się bez zapewnienia niezbędnej jakości rozwiązań budowanych dla kilkudziesięciu milionów obywateli i praktycznie wszystkich składowych informacyjnych państwa i gospodarki. Dlatego też warunkiem niezbędnym uporządkowania procesu wytwórczego w projekcie pl.ID jest jak najszybsze wydzielenie testowania QA[5] w COI oraz poddanie testowania akceptacyjnego w MSW[6] sprawdzonym i bezwzględnie przestrzeganym zasadom zapewniania jakości. Wykorzystywanie użytkowników końcowych Zamawiającego do testowania w procesie wytwórczym pod hasłem testów akceptacyjnych jest nieakceptowalne z wielu względów. Najważniejsze z nich to szybko postępująca utrata motywacji pracowników i wiarygodności obydwu partnerów oraz nieunikniona niska jakość uzyskanego kodu. Testy akceptacyjne mogą zostać rozpoczęte tylko po potwierdzonym wewnętrznym protokołem jakości zakończeniu kolejnej fazy procesu wytwórczego systemu. W warunkach obrotu gospodarczego niekontrolowalnie rosnące koszty wytwórcze, kary umowne za odrzucane dostawy i trudności w zapewnieniu płynności przedsiębiorstwa wynikłe z przeciągających się odbiorów są wystarczającą stymulacją dla wprowadzania reżimu zapewnienia jakości i wydzielenia roli QA. Prawidłową praktyką jest poddanie wytwarzania i wdrażania systemów informatycznych wewnątrz organizacji lub instytucji również takim samym reżimom zarządzania projektem i zapewnienia jakości po stronie zamawiającego jak kontraktowanie ich na zewnątrz. Wymaga to zatem wytworzenia kompetencji QA również po stronie MSW[7]. W ostatnim okresie MSW podjął także prawidłowe działania zmierzające do uporządkowania prac nad wdrożeniem, jak przesunięcie czasu wdrożenia, zablokowanie rozpoczęcia testowania wydajności systemu przed jego akceptacją, czy zaproponowanie wdrożenia systemu od uruchomienia jego prototypu (części).

Zarządzanie zmianami jest immanentną składową zarządzania projektem i zapewnienia jakości. Zmiana (szczególnie biznesowa wynikająca ze zmiany prawno/proceduralnej) nie powinna być postrzegana przez Wykonawcę systemu jako największe ryzyko[8] projektowe. Zmiana otoczenia prawnego budowanego oprogramowania jest oczywistym atrybutem

---

[5] FAT – Factory Acceptance Testing – sprawdzenie jakości u wytwórcy PRZED PRZEKAZANIEM oprogramowania do testów akceptacyjnych użytkownika UAT. Wymaga zbudowania kultury organizacyjnej wokół procesu QA odseparowanego od testowania w procesie wytwórczym oprogramowania.

[6] UAT – User Acceptance Testing – testowanie przez użytkowników końcowych Zamawiającego formalnie dostarczonych dostaw (opatrzonych protokołami FAT) w STAŁYCH, udokumentowanych i ściśle kontrolowanych warunkach (tzw. zamrożenie wersji oprogramowania i konfiguracji sprzętowo/programowych platform na czas prowadzenia testów). Wyniki UAT nie powinny zasadniczo odbiegać od rezultatów prawidłowo przeprowadzonych i udokumentowanych FAT co do liczby i kategorii zidentyfikowanych niezgodności.

[7] Możliwe tu jest zarówno wyszkolenie własnych pracowników (w średniej perspektywie nawet do poziomu certyfikowanego audytora jakości) jak i (w krótszym terminie) wynajęcie zewnętrznych ekspertów jakości oprogramowania.

[8] W Planie Ryzyka COI zmiana prawna jest umieszczona jako największe ryzyko projektu pl.ID. Jest to niezrozumiałe tym bardziej wobec przyjęcia zwinnej metodyki wytwórczej SCRUM z założenia najbardziej dostosowanej do częstych zmian.


*Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1„Społeczeństwo informacyjne – budowa elektronicznej administracji"*

projektu i powinna być objęta adekwatnym procesem rozpoczynającym się od zgłoszenia (RFC). By wprowadzanie zmian nie stanowiło zagrożenia, ale było rutynową składową zarządzania, niezbędne jest faktyczne sprawowane właścicielstwo biznesowe projektu oraz funkcjonowanie Rady ds. Zmiany na poziomie organizacji lub Komitetu Sterującego Projektu[9]. COI dysponuje zatwierdzoną procedurą zarządzania zmianą, jednak Wykonawca ekspertyzy nie zidentyfikował żadnych śladów wskazujących na jej faktyczne wykorzystywanie. Niestosowanie zarządzania zmianą do złożonych projektów z reguły znacznie obniża wydajność i jakość oprogramowania oraz bezpieczeństwo.

Krytycznym elementem w prowadzonych jak dotąd pracach projektowych jest migracja dotychczasowych zasobów informacyjnych rejestrów państwowych będących w gestii MSW. Zagadnienia migracji w udostępnionych dokumentach (przede wszystkim w projektach technicznych BUSC) zostały potraktowane bardzo zdawkowo. Nie było to przedmiotem ekspertyzy, jednak Wykonawca ekspertyzy rekomenduje tu opracowanie dwustopniowe adekwatnej strategii migracji, a po jej uzgodnieniu przez właścicieli biznesowych, także planu i niezbędnych narzędzi do przeprowadzenia migracji oraz wsparcia użytkowników końcowych. Zdaniem Wykonawcy ekspertyzy w przypadku referencyjnych rejestrów państwowych jest to zagadnienie najwyższej wagi. Wobec nowej, różniącej się od dotychczasowej struktury danych we wdrażanym SRP nie tylko nie będzie możliwe automatyczne przemigrowanie obecnych zawartości rejestrów, ale niezbędne będzie także uspójnianie oraz uzupełnienie nowych baz (szczególnie BUSC) o szereg danych z dokumentacji papierowej USC i EWiUDO. Zagadnienie migracyjne wymaga, zdaniem Wykonawcy ekspertyzy, utworzenia struktur podprojektowych po stronie MSW oraz przygotowania właśnie przez nie niezbędnych strategii i planów. COI powinien wytworzyć (i wyczerpująco przetestować) narzędzia służące temu wg wymagań ekspertów biznesowych MSW, by maksymalnie zautomatyzować czynności migracyjne i wspomóc uzupełnianie danych[10]. Zestawienie kategoryzacji obserwacji dla 4 obszarów ekspertyzy określonych w Umowie przedstawia poniższa tabela:

| Obszar ekspertyzy | L. uwag krytycznych | L. uwag poważnych |
|---|---|---|
| Wymogi funkcjonalne SRP (pyt. 1.) | 4 | 6 |
| Wymogi wydajnościowe SRP (pyt. 2.) | 6 | 1 |
| Zarządzanie zmianą w rozumieniu ITIL (pyt. 3.) | 1 | 6 |
| Zarządzanie ryzykiem i ciągłością (pyt. 4.) | 6 | 1 |

[9] W celu podejmowania decyzji o priorytecie lub odrzuceniu wniosku o zmianę (RfC - *Request for Change*).

[10] Utworzone struktury podprojektowe powinny dogłębnie przestudiować doświadczenia z dużych migracji i czyszczenia danych w CEPiK, PZU oraz prawno-proceduralną organizację migracji Nowej Księgi Wieczystej w celu wyeliminowania znanych już nieprawidłowości oraz adekwatnego zaadresowania obiektywnych problemów i zagadnień proceduralno-prawnych jeszcze przed rozpoczęciem ograniczonego lokalizacyjnie wdrożenia pilotowego SRP.


*Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1„Społeczeństwo informacyjne – budowa elektronicznej administracji"*

# 1. WSTĘP

## 1.1. Wprowadzenie

Dokument „Raport z ekspertyzy IT projektu pl.ID" ma na celu umożliwienie użytkownikom właścicielom systemu informacyjnego w Ministerstwie Spraw Wewnętrznych uzupełnienie istniejącej dokumentacji i poprawienie sposobu oraz metod realizacji projektu pl.ID. Niniejszy dokument został wytworzony zgodnie z Umową Nr 679/DEP/4.8./2014 z 4 grudnia 2014 r. na przeprowadzenie ekspertyzy IT projektu pl.ID i przedstawia ocenę dokumentacji udostępnionej na dzień sporządzenia raportu.

Zgodnie z Umową ekspertyza ma na celu uzyskanie odpowiedzi na następujące pytania:

a. Czy zakontraktowane wymogi funkcjonalne Systemu Rejestrów Państwowych zostały dostarczone i mają odwzorowanie w dokumentacji technicznej?
b. Czy wymogi wydajnościowe Systemu Rejestrów Państwowych są adekwatne do systemu tej skali i czy zostały potwierdzone poprawnie przeprowadzonymi testami?
c. Czy system zarządzania zmianą po stronie wytwórcy Systemu Rejestrów Państwowych jest adekwatny w rozumieniu ITIL?
d. Czy zarządzanie ryzykiem i ciągłością działania po stronie wytwórcy Systemu Rejestrów Państwowych jest adekwatne w rozumieniu norm ISO 22301 i ISO 31000?

Niniejsza ekspertyza obejmuje następujące informacje:

a) jednoznaczne odpowiedzi na pytania wymienione wyżej;
b) ocenę stanu organizacyjnego po stronie wykonawcy oprogramowania i systemu SRP w badanych obszarach (poziom dojrzałości – *maturity level*);
c) rekomendacje.

Sposób przygotowania ekspertyzy:
Zgodnie z Umową niniejsza ekspertyza zostało przygotowana wyłącznie na podstawie dokumentacji dostarczonej Wykonawcy ekspertyzy. W pracach Wykonawcy ekspertyzy uczestniczyli eksperci zgodnie z ofertą, na podstawie której została zawarta ww. Umowa. Eksperci nie uczestniczyli w żadnych spotkaniach poza własnym gronem, dotyczących realizacji projektu p.ID oraz nie prowadzili rozmów z uczestnikami zespołu projektowego.

## 1.2. Własność dokumentu

Niniejszy dokument stanowi podstawę do dyskusji nad zaprezentowanymi w nim wnioskami zespołu ekspertów zewnętrznych dotyczącymi zakresu, jakości i podejścia ze strony COI, jednostki Ministerstwa Spraw Wewnętrznych do realizacji, wdrożenia, utrzymania i rozwoju Systemów Rejestrów Państwowych wyłącznie w aspekcie projektu pl.ID.

Niniejsza ekspertyza powinna być czytana i analizowana w całości, gdyż opieranie się tylko na jej poszczególnych częściach może prowadzić do błędnych wniosków. Wyrwane z całości kontekstu części Raportu mogą być całkowicie nieadekwatne dla celów innych badań lub analiz.

Dokument jest przeznaczony dla kierownictwa MSW.


Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1„Społeczeństwo informacyjne – budowa elektronicznej administracji"

# 2. OGÓLNY OPIS PRZEGLĄDU

## 2.1. Cel przeglądu

Celem przeglądu było zebranie i uporządkowanie obserwacji oraz przedstawienie wniosków stanowiących podstawę do zarekomendowania działań dla procesów projektowania, wdrożenia, utrzymania i rozwoju systemu pl.ID. Cel ten zrealizowany został poprzez:

- przeprowadzenie analizy udostępnionej dokumentacji projektowej projektu pl.ID;
- przeprowadzenie analizy budowania i implementacji rozwiązań technologii informatycznej w trakcie realizacji projektu pl.ID;
- przeanalizowanie istniejących rozwiązań w zakresie monitorowania i zarządzania wymaganiami projektu pl.ID;
- przeprowadzenie oceny kompletności i jakości udostępnionej dokumentacji;
- wypracowanie wniosków wynikających z przeprowadzonego przeglądu, dających podstawy co do przedstawienia rekomendacji w zakresie dalszego postępowania przy opracowaniu i wdrożeniu projektu pl.ID.

## 2.2. Otoczenie projektu pl.ID

Załącznik 2 zawiera tabelarycznie przedstawione kalendarium zdarzeń, które do tej pory miały miejsce, związanych z realizacją projektu pl.ID. Jak dotychczas projekt miał 11 Ministrów i Właścicieli Programu (Wiceministrów SW i MAiC) oraz był realizowany w 3 instytucjach (MSW, CPI i COI). Zmianie podlegały założenia, cele strategiczne, zakres, daty wdrożenia, budżet (nawet w skali dziesięciokrotnej), podejście strategiczne, architektura, technologie oraz metody wytwórcze, a przede wszystkim zespoły zarządzające i wykonawcze. Ze względu na niedostatki uruchomionej funkcjonalności kilkakrotnie przesuwano wejście w życie niezbędnych wprowadzających regulacji prawnych. Przegląd dotyczy wyłącznie ostatniej fazy projektu pl.ID prowadzącej do wdrożenia Systemu Rejestrów Państwowych wg nowego podejścia, mającego zapewnić funkcjonalność przewidywaną do wprowadzenia w życie w r. 2015.

W okresie od czerwca 2014 MSW podjął także prawidłowe działania zmierzające do uporządkowania prac nad wdrożeniem, jak przesunięcie czasu wdrożenia, zablokowanie rozpoczęcia testowania wydajności systemu przed jego akceptacją [68], czy zaproponowanie wdrożenia systemu od uruchomienia jego prototypu[11] (części).

[11] Wykonawca ekspertyzy potwierdza tutaj prawidłowość podejścia przyjętego w ostatnim okresie ze strony MSW: **obecny stan pl.ID rzeczywiście należy zakwalifikować jako prototyp systemu.** O pilotażu można mówić tylko w przypadku, gdy system jest już gotowy (tzn. pomyślnie przeszedł pełne testy akceptacyjne użytkownika funkcjonalne i wydajności (UAT)), a początkowe ograniczenie lokalizacyjne służy wypracowaniu najlepszych praktyk organizacyjnych dla jego wdrożenia na skalę ogólnopolską.


*Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1„Społeczeństwo informacyjne – budowa elektronicznej administracji"*

# 2.3. Założenia przeglądu

## 2.3.1.Zakres przeglądu

Zakresem przeglądu zostały objęte wyłącznie dokumenty udostępnione przez MSW i COI pod kątem:

- realizacji projektu pl.ID w zakresie zarządzania zmianą, ciągłością oraz ryzykiem,
- oceny jakościowej niektórych produktów utworzonych w trakcie realizacji projektu pl.ID,
- oceny podejścia do budowy oprogramowania i zarządzania wymaganiami w projekcie.

Wykaz dokumentacji poddanej przeglądowi zawiera Tabela 1 w rozdziale 2.3.3 Źródła informacji.

## 2.3.2.Punkt odniesienia do oceny Systemu

Przegląd jest działaniem kontrolnym, którego istotą jest weryfikacja zgodności faktycznego stanu jakiegoś obiektu (obszaru, dziedziny, procesu) ze stanem wcześniej zdefiniowanym /oczekiwanym.

W dokumencie [70] otrzymanym z COI stwierdzono, że budowa oprogramowania w trakcie realizacji projektu pl.ID wykorzystuje metodyki zwinne (Agile) przede wszystkim SCRUM.

W związku z powyższym, Zespół Ekspertów przyjął jako punkt odniesienia, wybrane i dopasowane przez ekspertów do charakteru, zakresu i skali projektu pl.ID, ogólne standardy zdefiniowane w uznanych metodykach formalnych inżynierii oprogramowania, poparte tzw. „dobrymi praktykami", czyli sprawdzonymi doświadczeniami wyniesionymi z innych przedsięwzięć tego typu.

W ocenie wyników przeglądu wykorzystano zalecenia metodyki COBIT (w wersji 4.0), a także standard ISO/IEC 12207:2008, ISO/IEC 42010:2011, ISO 22301, ISO 31 000. Każdą obserwację zaklasyfikowano do jednej z niżej przedstawionych dziedzin COBIT zdefiniowanych dla badania systemów informatycznych:

1. Pozyskanie i implementacja oprogramowania (*ang. AI – Acquisition and Implementation*)
2. Dostawa i wsparcie (*ang. DS – Delivery and Support*)
3. Monitorowanie i ocena (*ang. M - Monitoring*).

W ocenie projektu pl.ID uwzględniono także odpowiednie obszary zdefiniowane dla standardu ISO/IEC 12207:2008:

1. Procesy umowy (Agreement)
2. Procesy organizacyjne (Organizational Project- Enabling Processes)
3. Procesy zarządzania przedsięwzięciem (Project)
4. Procesy techniczne (Technical)
5. Procesy specyfikujące oprogramowanie (SW Specific Processes) *(tylko w zakresie wynikającym z udostępnionej dokumentacji)*


*Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1„Społeczeństwo informacyjne – budowa elektronicznej administracji"*

Ponadto uwzględniono również ocenę jakościową, w tym:

1. Stosowania standardów.
2. Spójności produktów.
3. Zapewnienia rozliczalności wymagań (*ang. traceability*).
4. Udokumentowania zmian.
5. Użyteczności (zrozumiałość, kompletność opisu, przydatność operacyjna).

## 2.3.3.Źródła informacji

Głównym źródłem informacji dla oceny Zespołu Ekspertów była Tabela 1., przedstawiająca całą dokumentację udostępnioną przez MSW i COI.

***Tabela 1. Wykaz udostępnionej dokumentacji stanowiącej źródła przeglądu***

| Tytuł dokumentu lub nazwa pliku | Wersja | Data dokumentu |
|---|---|---|
| 1. Studium Wykonalności Projektu pl.ID | do wersji 2.0 | styczeń 2013 r. |
| 2. Harmonogram wysokopoziomowy realizacji projektu - załącznik do umowy | załącznik nr 3 do aneksu nr 2 do umowy nr 4/DSiA/2013 | 27 czerwca 2014 r. |
| 3. Harmonogram szczegółowy projektu pl.ID | brak | lipiec 2013 r. |
| 4. Projekt Wysokopoziomowej Architektury Systemów Rejestrów Państwowych | 1.2 | 18 kwietnia 2013 r. |
| 5. Architektura Systemu Rejestrów Państwowych, wersja: 4.0 - załącznik do Projektu technicznego | 4.0 | 12 maja 2013 r. |
| 6. Analiza prac modernizacyjnych BUSC oraz koncepcja przebudowy i modernizacji BUSC | 1.3 | 4 września 2013 r. |
| 7. Analiza kierunków modernizacji SRP | 1.3 | 17 września 2013 r. |
| 8. Analiza związana z realizacją Systemu Odznaczeń Państwowych | 1.3 | 18 września 2013 r. |
| 9. Analiza związana z realizacją Centralnego Rejestru Sprzeciwów | 1.3 | 19 września 2013 r. |
| 10. Specyfikacja interfejsu komunikacyjnego pomiędzy Rejestrem Dowodów Osobistych (RDO) a Systemem Personalizacji Dokumentów (SPD) | 1.4 | 12 lipca 2013 r. |
| 11. Analiza wstępna budowy Rejestrów Dowodów Osobistych | 3.0 | 10 października 2013 r. |
| 12. Dokumentacja powykonawcza na dostawę urządzeń do Podstawowego Centrum Przetwarzania Danych i Zapasowego Centrum Przetwarzania Danych w zakresie Centralnej Magistrali Serwisowej | 1.0 | 9 grudnia 2013 r. |
| 13. Projekt techniczny PESEL (SRP) - etap I | 3.0 | 29 listopada 2013 r. |
| 14. Projekt techniczny PESEL (SRP) - etap II | 2.0 | 6 grudnia 2013 r. |
| 15. Projekt techniczny SOP | 2.0 | 6 grudnia 2013 r. |
| 16. Projekt techniczny CRS | 2.0 | 9 grudnia 2013 r. |
| 17. Projekt techniczny Rejestru Dowodów Osobistych - etap I | 2.0 | 2 grudnia 2013 |
| 18. Projekt techniczny Rejestru Dowodów Osobistych - | 3.0 | 10 lutego 2014 r. |



*Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1„Społeczeństwo informacyjne – budowa elektronicznej administracji"*

| | | |
|---|---|---|
| etap II | | |
| 19. Projekt techniczny modernizowanej Bazy Usług Stanu Cywilnego | 2.0 | 5 grudnia 2013 r. |
| 20. Koncepcja realizacji i uruchomienia projektu e-usług związanych z SRP rozumianym jako rejestr PESEL, rejestr SOP, rejestr BUSC, rejestr RDO i rejestr CRS | 2.0 | 7 października 2013 r. |
| 21. Koncepcja dokumentów (drukowanych i elektronicznych) powiązanych z ewidencją ludności i aktami stanu cywilnego (SRP) w zakresie architektury informacji i projektów graficznych | 2.0 | 8 października 2013 r. |
| 22. Koncepcja realizacji platformy e-usług dedykowanej dla MSW | 1.0 | 5 grudnia 2013 r. |
| 23. Analiza kierunków optymalizacji ZMOKU | 1.3 | 18 września 2013 r. |
| 24. Projekt techniczny optymalizacji ZMOKU (Źródło) etap I | 3.0 | 29 listopada 2013 r. |
| 25. Projekt techniczny optymalizacji ZMOKU (Źródło) etap II | 2.0 | 6 grudnia 2013 r. |
| 26. w sprawie przygotowań do przejęcia projektu pl.ID polska ID karta | 3/DSIA/2013/WKiMP | 23 stycznia 2013 r. |
| 27. w sprawie realizacji projektu "pl.ID" | 4/DSiA/2013 | 25 lutego 2013 r. |
| 28. aneks nr 1 do umowy w sprawie realizacji projektu "pl.ID" | | 13 lutego 2014 r. |
| 29. aneks nr 2 do umowy w sprawie realizacji projektu "pl.ID" | | 27 czerwca 2014 r. |
| 30. w przedmiocie przetwarzania danych osobowych | 7/DSiA/2013 | 4 listopada 2013 r. |
| 31. w sprawie wykonywania przez Centrum Personalizacji Dokumentów MSW zadań w zakresie projektu Rejestr Dowodów Osobistych w ramach projektu pl.ID | | 21 listopada 2013 r. |
| 32. aneks nr 1 do porozumienia w sprawie wykonywania przez Centrum Personalizacji Dokumentów MSW zadań w zakresie projektu Rejestr Dowodów Osobistych w ramach projektu pl.ID | | 3 maja 2014 r. |
| 33. w sprawie rozwiązania porozumienia o realizacji "Projektu pl.ID - Polska ID karta" - przejęcie projektu przez MSW | | 12 kwietnia 2013 r. |
| 34. dofinansowanie nr POIG.07.01.00-00-003/08-00 w ramach 7 osi priorytetowej "Społeczeństwo informacyjne - budowa elektronicznej administracji" Programu Operacyjnego innowacyjna Gospodarka 2007-2013 | | 3 czerwca 2009 |
| 35. aneks nr 1 do umowy o dofinansowanie | | 16 kwietnia 2010 r. |
| 36. aneks nr 2 do umowy o dofinansowanie | | 23 listopada 2011 r. |
| 37. aneks nr 3 do umowy o dofinansowanie | | 17 września 2012 r. |
| 38. aneks nr 4 do umowy o dofinansowanie | | 26 czerwca 2013 r. |
| 39. aneks nr 5 do umowy o dofinansowanie | | 24 lutego 2014 r. |
| 40. zarządzenie w sprawie ustalenia struktury zarządzania projektem „pl.ID" | zarządzenie nr 43 MSW | 15 maja 2013 r. |
| 41. zarządzenie zmieniające zarządzenie w sprawie ustalenia struktury zarządzania projektem „pl.ID" | zarządzenie nr 2 MSW | 22 stycznia 2014 r. |
| 42. zarządzenie zmieniające zarządzenie w sprawie ustalenia struktury zarządzania projektem „pl.ID" | zarządzenie nr 21 MSW | 12 czerwca 2014 r. |


*Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1„Społeczeństwo informacyjne – budowa elektronicznej administracji"*

| | | |
|---|---|---|
| 43. zarządzenie w sprawie powołania Zespołu do spraw wdrożenia „Systemu Rejestrów Państwowych" w ramach projektu „pl.ID" | zarządzenie nr 30 MSW | 5 listopada 2014 r. |
| 44. regulamin organizacyjny MSW - tekst jednolity | zarządzenie nr 4 MSW | 9 grudnia 2011 r. |
| 45. statut Centralnego Ośrodka Informatyki | zarządzenie nr 48 MSW | 26 listopada 2010 r. |
| 46. zmiana statutu Centralnego Ośrodka Informatyki | zarządzenie nr 33 MSW | 17 maja 2012 r. |
| 47. zmiana statutu Centralnego Ośrodka Informatyki | zarządzenie nr 27 MSW | 15 lutego 2013 r. |
| 48. zmiana statutu Centralnego Ośrodka Informatyki | zarządzenie nr 28 MSW | 22 lutego 2013 r. |
| 49. Raport wyników testów akceptacyjnych komponentu RDO etap I | 1.0 | 10 grudnia 2013 r. |
| 50. Zestawienie zgłoszeń zarejestrowanych podczas testów akceptacyjnych RDO etap I | 1.0 | 6 grudnia 2013 r. |
| 51. Raport wyników testów akceptacyjnych komponentu PESEL oraz CMOKU etap I | 1.0 | 29 listopada 2013 r. |
| 52. Raport wyników testów akceptacyjnych komponentu CRS | 1.0 | 28 lipca 2014 r. |
| 53. Raport wyników testów akceptacyjnych komponentu SOP | 1.0 | 22 października |
| 54. Protokół odbioru produktu Zlecenia nr 25 - prace programistyczne PESEL etap I | | 9 grudnia 2013 r. |
| 55. Protokół odbioru produktu Zlecenia nr 26 - prace programistyczne CMOKU etap I | | 10 grudnia 2013 r. |
| 56. Protokół odbioru produktu Zlecenia nr 32 - prace programistyczne RDO etap I | | 10 grudnia 2013 r. |
| 57. Protokół odbioru produktu Zlecenia nr 36 - prace programistyczne CRS etap I | | 7 października 2014 r. |
| 58. Scenariusze testów wydajnościowych i obciążeniowych | 1.3 | 14 listopada 2014 r. |
| 59. Plan wdrożenia | 1.0 (2 pliki: pdf+mpp) | październik 2014 r. |
| 60. Definicja błędów | brak (2 pliki: word + pdf) | |
| 61. Studium wykonalności | 3.1 (plik word) | 20 maja 2013 r. |
| 62. Harmonogram wysokopoziomowy | do aneksu 1 do umowy nr 4 | luty 2014 r. |
| 63. Zrzut bazy Mantis | | 15 grudnia 2014 r. |
| 64. Zrzut ekranu ITSM | | 15 grudnia 2014 r. |
| 65. Ostatnie statystyki retestów | | 10 grudnia 2014 r. |
| 66. Scenariusze testów wydajnościowych i obciążeniowych | | 12 grudnia 2014 r. |
| 67. Dashboard | 9 plików | |
| 68. Stan oprogramowania SRP po testach regresji w dniach 26-30.11.2014 r. | | 1 grudnia 2014 r. |
| 69. Projekt wysokopoziomowej architektury SRP | 4.0 | 5 grudnia 2013 r. |
| 70. Odpowiedz_COI_w_sprawie_ekspertyzy | pdf | 2 grudnia 2014 |
| 71. Analiza ryzyka do planu dzialalnosci COI na 2014 | pdf | |
| 72. analiza ryzyka do planu dzialalnosci na 2013 | pdf | |
| 73. Plan postepowania z ryzykiem w roku 2014 | pdf | |
| 74. Wyniki oceny ryzyka 2013 | pdf | |
| 75. Zidentyfikowane ryzyka na 2014 r. | pdf | 12 marca 2014 |


*Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1„Społeczeństwo informacyjne – budowa elektronicznej administracji"*

| | | | |
|---|---|---|---|
| 76. | Backlog BUSC | xls | 8 grudnia 2014 |
| 77. | Backlog Common | xls | 8 grudnia 2014 |
| 78. | Backlog RDO | xls | 8 grudnia 2014 |
| 79. | Backlog SOP | xls | 8 grudnia 2014 |
| 80. | Backlog CORE | xls | 8 grudnia 2014 |
| 81. | Backlog PESEL | xls | 8 grudnia 2014 |
| 82. | Backlog CRS | xls | 8 grudnia 2014 |
| 83. | Instrukcja przetwarzania danych osobowych | pdf | 5 grudnia 2014 |
| 84. | Instrukcja zarzadzania systemami infrmatycznymi DO | pdf | 5 grudnia 2014 |
| 85. | Polityka Bezpieczeństwa Danych Osobowych | pdf | 5 grudnia 2014 |
| 86. | Zarządzenie_polityka bezpieczenstwa | pdf | 26 lutego 2014 |
| 87. | Regulamin zamowień Publicznych | pdf | 1 sierpnia 2012 |
| 88. | Zarządzenie_zmiana reg. ZP | pdf | 16 kwietnia 2014 |
| 89. | Zarzadzenie Dyrektora_Wprowadzenie TP | pdf | 28 grudnia 2012 |
| 90. | Zarzadzenie Dyrektora_Zmiana TP | pdf | 23 sierpnia 2013 |
| 91. | InstrukcjaZarzadzaniaZmiana | pdf | 1 lipca 2013 |
| 92. | 2014-11-28_Instrukcja_Zarzadzania_Zmiana_SI_CEPiK | pdf | 1 rudnia 2014 |
| 93. | ProceduraZarzadzaniaZmiane | pdf | 19 czerwca 2012 |
| 94. | 2014-09-01_Procedura_Zarzadzania_Zmiana | pdf | 5 września 2014 |
| 95. | Proces wytwarzania oprogramowania | pdf | |
| 96. | proces-planowania-wydajnosci-systemu | pdf | |
| 97. | Regulamin Organizacyjny | pdf | 2014 |
| 98. | sposob-wersjonowania-aplikacji | pdf | |
| 99. | Struktura | pdf | 8 grudnia 2014 |
| 100. | Zarzadzenie Dyrektora_Kontrole w COIf | pdf | 21 marca 2013 |
| 101. | Zarzadzenie Dyrektora_Wyliczanie kosztow w projektach | pdf | 26 marca 2014 |
| 102. | Zarzadzenie Dyrektora_Zarzadzanie ryzykiem | pdf | 17 grudnia 2013 |
| 103. | Instrukcja - brak w folderze zarządzenia | pdf | |
| 104. | Zarzadzenie zmieniające Regulamin Organizacyjny | pdf | 3 czerwca 2014 |
| 105. | Zarządzenie_zespół wdrożeniowy SRP | pdf | 17 listopada 2014 |
| 106. | Nowe podejście - brak w folderze zarządzenia | pdf | luty 2013 |
| 107. | Zarzadzenie 62_2014 - brak w folderze zarządzenia | pdf | 15 lipca 2014 |
| 108. | 2_Kategoryzacja błedów_ITSM | pdf | |
| 109. | 6_Zrzuty ekranu z ITSM | Outlook | |



*Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1„Społeczeństwo informacyjne – budowa elektronicznej administracji"*

# 3. OCENA SPOSOBU REALIZACJI PROJEKTU

W niniejszym rozdziale przedstawiono ocenę wybranych aspektów związanych z realizacją i rozwojem projektu pl.ID. Analiza Zespołu Ekspertów skupiła się wokół zagadnień związanych z uzyskaniem odpowiedzi na zapytania przedstawione we Wprowadzeniu do niniejszego opracowania.

Poniżej przedstawiono opis poszczególnych obszarów oceny Projektu pl.ID wyznaczonych Umową na realizację ekspertyzy oraz obserwacje eksperckie z poszczególnych dziedzin metodyki COBIT.

W każdej z części przedstawiono wykaz obserwacji - spostrzeżeń usterek i nieprawidłowości lub uwag ekspertów. Dla każdej obserwacji określony został stopień wpływu na jakość i efektywność funkcjonowania systemu oraz sformułowany wniosek. Ma to na celu umożliwienie Zamawiającemu przeprowadzenie własnej oceny zagrożeń wynikających z niedostatków poszczególnych obszarów Projektu pl.ID zidentyfikowanych przez ekspertów. W dalszej części ekspertyzy zebrano łącznie rekomendacje opracowane na podstawie wypracowanych wniosków i doświadczeń ekspertów związanych ze stosowaniem norm przywołanych w Umowie oraz dobrych praktyk budowy i utrzymania oprogramowania z uwzględnieniem specyfiki administracji publicznej.

Wyniki analizy przeprowadzonej dla udostępnionej dokumentacji zostały ujęte w tabelach z obserwacjami o następującej strukturze:

*Tabela 2. Definicja sposobu opisu oceny Zespołu Ekspertów*

| „Identyfikator i nazwa obserwacji" – **Identyfikuje, czego dotyczy obserwacja odnośnie zapisów ujętych w dokumentacji.** | |
|---|---|
| **Kategoria** | „Kategoria" – Określa istotność obserwacji, definiuje stopień wpływu ocenianego elementu lub aspektu danego obszaru na jakość systemu oraz związane z tym zagrożenia.<br>Kategoria określa więc poziom istotności obserwacji i może przyjąć następujące wartości:<br>• **Krytyczna** - problem opisywany w obserwacji ma znaczenie krytyczne, jego wpływ na jakość Systemu jest zasadnicza, nierozwiązanie problemu może spowodować poważne trudności w dalszej eksploatacji lub rozwoju Systemu.<br>• **Poważna** - problem opisywany w obserwacji jest poważny, znacząco obniża jakość systemu, nierozwiązany może skutkować zakłóceniami w eksploatacji i utrudnieniami w procesie w dalszej eksploatacji lub rozwoju systemu.<br>• **Drobna** - problem opisywany w obserwacji ma mało istotne znaczenie, jego wpływ na jakość systemu jest niski. Rozwiązanie problemu jest pożądane, ale jego brak nie powinien istotnie utrudniać dalszej eksploatacji lub rozwoju systemu. |
| **Dziedzina COBIT/12207** | Określenie jednej z dziedzin COBIT:<br>P – Planning and Organization (Planowanie i organizacja)<br>AI – Acquisition and Implementation (Pozyskanie i implementacja oprogramowania)<br>DS – Delivery and Support (Dostawa i wsparcie) |


*Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1„Społeczeństwo informacyjne – budowa elektronicznej administracji"*

| | |
|---|---|
| | M – Monitoring (Monitorowanie i ocena)<br>Określenie jednego z obszarów ISO IEC 12207:2008:<br>A - Agreement (Procesy umowy)<br>O - Organizational Project- Enabling Processes (Procesy organizacyjne)<br>PR - Project (Procesy zarządzania przedsięwzięciem)<br>T - Technical (Procesy techniczne)<br>SW - SW Specific Processes (Procesy specyfikujące oprogramowanie). |
| **Opis obserwacji** | „Opis obserwacji" – W tym wierszu znajduje się opisowa część obserwacji. Krótki opis charakteryzuje i wyjaśnia, czego dotyczy obserwacja. |
| **Wniosek** | Konkretne odniesienie do obserwacji. |

# 3.1. Wymogi funkcjonalne SRP

Architektura systemu informatycznego opisuje sposób realizacji systemu informatycznego jak i uzasadnienie zastosowanych rozwiązań (ISO/IEC 42010:2011). Architekturę systemu należy opisywać w osobnych perspektywach oddzielając od siebie zagadnienia związane z funkcjonalnością, technologiami, środowiskiem programistycznym, czy zainstalowanym sprzętem teleinformatycznym, czyli uwypuklenia pewnych aspektów systemu, przy jednoczesnym pominięciu innych. Perspektywy stanowią mechanizm umożliwiający rozdzielenie różnych aspektów systemu w trakcie tworzenia, rozwoju lub analizowania architektury. Typowe perspektywy architektoniczne to[12]: perspektywa biznesowa, perspektywa przypadków użycia, perspektywa projektowa (logiczna), perspektywa implementacyjna, perspektywa procesowa, czy perspektywa fizyczna (wdrożeniowa). Ponadto jednym z najważniejszych rezultatów opisu architektury systemu jest opracowanie odpowiedniej sekwencji, czy kolejności powiązanych ze sobą modeli tak, by możliwe było zarówno śledzenie zasadności zastosowania określonych elementów (ang. *traceability*) jak i zapewnienie kompletności i spójności (ang. *consistency*) opisu całej architektury.

Niespójności architektury powstają pomiędzy modelami opisującymi ten sam system z różnych punktów widzenia i używających wspólnych elementów[13]. Wspólny element może być inaczej interpretowany w różnych modelach. Zatem system jest spójny, gdy interpretacja elementów w różnych modelach jest taka sama.

Kompletność opisu architektury systemu (wystarczający zestaw modeli) nie zawsze jest oczywista. Jednakże zgodnie z koncepcją Johna Gero[14] opis dowolnego systemu (artefaktu) powinien posiadać informacje o jego funkcjonalności, strukturze i zachowaniu, by taki projekt systemu mógł być zrealizowany. Zatem wydaje się oczywiste, że rozwiązania w zakresie budowy systemów informatycznych, w których nie bierze się pod uwagę tych trzech

[12] Tutaj: model perspektyw architektonicznych 4+1 – podstawa USDP (Unified Software Development Process).
[13] Spanoudakis, G., Zisman, A.: Inconsistency management in software engineering: Survey and open research issues. In S. K. Chang (Ed.), Handbook of software engineering and knowledge engineering, 1, 329-380. London: World Scientific Publishing Co, 1999
[14] Gero, J. S. (1990). Design prototypes: a knowledge representation schema for design, AI Magazine, 11(4): 26-36.

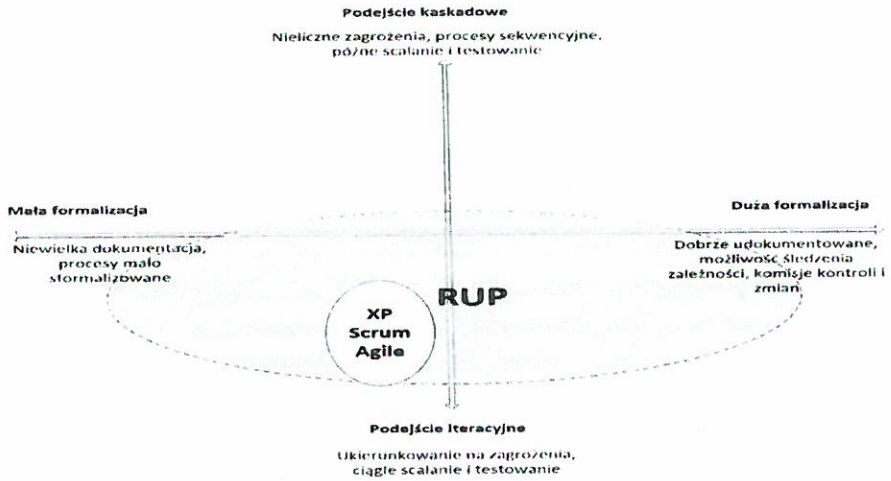

Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1„Społeczeństwo informacyjne – budowa elektronicznej administracji"

wymiarów, tzn. funkcjonalności, struktury i zachowania systemu, zgodnie z koncepcją FSB[15] Johna Gero, skazane są na niepowodzenie. Zazwyczaj braki modeli opisujących konkretne wymiary muszą zostać zrekompensowane w trakcie implementacji oprogramowania, a niekiedy nawet w trakcie wdrażania systemu.

W trakcie prac nad oceną modeli projektu pl.ID posłużono się metodyką Unified Software Development Process[16] (zwaną również Unified Process), której centralnym punktem odniesienia jest model perspektyw architektonicznych 4+1[17]. Metodyka USDP (UP) dotyczy przede wszystkim budowy oprogramowania, a zatem opisuje tzw. dyscypliny wspierające proces budowy oprogramowania (zarządzanie projektem, zarządzanie konfiguracjami i zmianami, przygotowywanie środowiska, wdrożenie). Metodykę USDP (UP) można rozpatrywać z jednej strony jako strukturę statyczną (sposób opisywania metodyki oraz kluczowe pojęcia takie, jak role, czynności, artefakty, dyscypliny itd.). Z drugiej zaś strony USDP (UP) można rozpatrywać jako strukturę dynamiczną (przebieg realizacji projektu). Struktura dynamiczna USDP (UP) opisuje tworzenie iteracyjne systemu informatycznego, czyli przebieg działań związany z procesem wytwórczym, gdzie uwzględnia się etapy, kamienie milowe, iteracje, jak również czynniki, które mają wpływ na przebieg procesu wytwórczego. W trakcie realizacji projektu każdy wykonawca posługuje się w dużej mierze modelami. Metodyka USDP (UP) dopuszcza dobieranie odpowiednich modeli do konkretnych zastosowań przy produkcji oprogramowania, pozostawiając wykonawcy decyzję co do poziomu szczegółowości poszczególnych modeli. Zbiór konkretnych modeli tworzy razem jedną z tzw. Perspektyw architektury oprogramowania (model perspektyw 4+1). Metodyka USDP niestety nie pokazuje kolejności tworzenia poszczególnych modeli, czy ich wynikania, natomiast wskazuje konkretne diagramy UML[18], za pomocą których można opisać architekturę budowanego systemu informatycznego. Końcowym wynikiem prac nad architekturą systemu powinien być diagram wdrożenia (UML) systemu informatycznego.
Poniżej zestawiono porównanie innych popularnych metodyk budowy oprogramowania z Rational Unified Process, która to metodyka jest komercyjnym odpowiednikiem Unified Software Development Process (Unified Process).

[15] FSB - Functionality – Structure – Behaviour – funkcjonalność, struktura, zachowanie
[16] The Unified Software Development Process, Ivar Jacobson, Grady Booch, James Rumbaugh, Rational Software Corporation, Addison-Wesley 1999.
[17] Philippe Kruchten, Architectural Blueprints—The "4+1" View Model of Software Architecture, Philippe Kruchten Rational Software Corp., Paper published in IEEE Software 12 (6) November 1995, pp. 42-50
[18] Unified Modeling Language: Superstructure, version 2.4.1, formal/2012-05-06. Patrz również: ISO/IEC 19505-2:2012 (UML 2.4.1 Superstructure)


Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1„Społeczeństwo informacyjne – budowa elektronicznej administracji"




Porównanie RUP (UP) z innymi metodykami budowy oprogramowania

Bardzo istotnym elementem budowy oprogramowania zgodnie z metodyką Unified Software Development Process (Unified Process) jest budowa prototypu (inicjalna część systemu), która w trakcie kolejnych iteracji rozbudowywana jest do finalnego systemu. W trakcie kolejnych iteracji testowane są poszczególne wymogi funkcjonalne i niefunkcjonalne systemu, co pozwala skutecznie śledzić postępy budowy oprogramowania, a nawet je kontrolować. Warto wskazać, iż ideę budowy prototypu zaproponowano 22 października [Analiza scenariuszy uruchomienia systemu PL_ID.pdf, Uruchomienie pilotażowe – str. 4], co jest zbieżne z założeniami metodyki Unified Software Development Process.

W dalszej części podrozdziału przedstawiono obserwacje Zespołu Ekspertów wynikające z analizy dokumentacji projektu pl.ID.

| **1. Brak scenariuszy testów akceptacyjnych** | |
|---|---|
| **Kategoria** | • Krytyczna |
| **Dziedzina COBIT/12207** | AI – Pozyskanie i implementacja oprogramowania<br>SW – specyfikacja oprogramowania |
| **Opis obserwacji** | W trakcie analizy całości udostępnionej dokumentacji Projektu pl.ID nie udało się zidentyfikować w specyfikacjach opisu scenariuszy testów akceptacyjnych. |
| **Wniosek** | Ze względu na brak informacji o scenariuszach testów akceptacyjnych nie można ocenić, co jest przedmiotem testów akceptacyjnych. Zatem należy stwierdzić, iż zakontraktowane wymogi funkcjonalne Systemu Rejestrów Państwowych nie zostały dostarczone i nie mają odwzorowanie w dokumentacji technicznej, gdyż tylko testy akceptacyjne umożliwiają w wiarygodny sposób udowodnić dostarczenie wymogów funkcjonalnych. |

| **2. Wybrane scenariusze testowania są niereprezentatywne** | |
|---|---|
| **Kategoria** | • Krytyczna |
| **Dziedzina COBIT/12207** | COBIT:<br>M – Monitoring (Monitorowanie i ocena)<br>ISO IEC 12207:2008:<br>T - Technical (Procesy techniczne) |


*Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1„Społeczeństwo informacyjne – budowa elektronicznej administracji"*

| | |
|---|---|
| **Opis obserwacji** | W trakcie analizy dokumentacji Projektu pl.ID ustalono, iż do testowania całego systemu wybrano w zakresie:<br>1- BUSC: 77 funkcjonalności [9_dashboard_plid_?.pdf], gdy zidentyfikowano 34 procesy [6_Analiza BUSC.pdf] i 64 przypadki użycia [19_PT BUSC\PT BUSC.pdf]<br>2- RDO: 84 funkcjonalności [9_dashboard_plid_?.pdf], gdy zidentyfikowano 7 procesów [11_Analiza RDO.pdf] i 39 przypadków użycia [17_PT RDO etap I.pdf, 18_PT RDO etap II.pdf]<br>3- SOP: 73 funkcjonalności [9_dashboard_plid_?.pdf], gdy zidentyfikowano 9 procesów [8_Analiza SOP.pdf] i 17 przypadków użycia [15_PT SOP.pdf]<br>4- CRS: 33 funkcjonalności [9_dashboard_plid_?.pdf], gdy zidentyfikowano 8 procesów [9_Analiza CRS.pdf] i 22 przypadki użycia [16_PT CRS\PT CRS.pdf.pdf]<br>5- PESEL: 47 funkcjonalności [9_dashboard_plid_?.pdf], gdy zidentyfikowano 59 procesów [7_Analiza SRP.pdf] i 72 przypadki użycia [13_PT PESEL etap I.pdf, 14_PT PESEL etap II\PT PESEL SRP etap II.pdf]<br>Uwaga!<br>Brak powiązania analizy i projektu ZMOKU z innymi częściami systemu pl.ID, gdy zidentyfikowano 2 procesy [23_Analiza optymalizacji ZMOKU.pdf] i 63 przypadki użycia [25_PT ZMOKU etap II\PT ZMOKU etap II.pdf] |
| **Wniosek** | Na podstawie udostępnionych dokumentów można stwierdzić, iż testy akceptacyjne nie są reprezentatywne w stosunku do pełnej funkcjonalności systemu, gdyż nie odpowiadają zaprojektowanym i opisanym w dokumentacji przypadkom użycia, bądź/i procesom.<br>Brak pełnej reprezentacji scenariuszy testowych wprowadza ryzyko ograniczonej wiarygodności ich wyników.<br>Brak odpowiedniości pomiędzy procesami, przypadkami użycia i przypadkami testowymi ogranicza wiarygodność co do poprawności i rzetelności tej części dokumentacji pl.ID.<br>Jednocześnie brak informacji na temat danych, na jakich przeprowadza się testy akceptacyjne. Brak testów na danych rzeczywistych jeszcze bardziej zmniejsza wiarygodność wyniku testów akceptacyjnych. |

## 3. Wymagania funkcjonalne i niefunkcjonalne we wszystkich dokumentach analitycznych i projektowych nie zawierają określeń liczby użytkowników ani miar intensywności korzystania z systemu SRP

| | |
|---|---|
| **Kategoria** | • Krytyczna |
| **Dziedzina COBIT/12207** | AI – Pozyskanie i implementacja oprogramowania<br>SW – specyfikacja oprogramowania |
| **Opis obserwacji** | W trakcie analizy udostępnionej dokumentacji Projektu pl.ID nie udało się zidentyfikować w specyfikacjach wymagań funkcjonalnych i niefunkcjonalnych [6, 7, 8, 9, 10, 11] oraz w projektach technicznych [13, 14, 15, 16, 17, 18, 19, 24, 25] określenia liczbowego:<br>1- liczby lokalizacji,<br>2- liczby maksymalnej/średniej użytkowników w poszczególnych rolach,<br>3- liczby równoczesnych stanowisk pracy,<br>4- wolumetryki[23] akcji z systemem dziennej/okresowej/rocznej, szczytowych aktywności,<br>5- granicznych czasów reakcji systemu dla określonych funkcjonalności.<br>Na podstawie udostępnionej dokumentacji nie można stwierdzić czy przy |

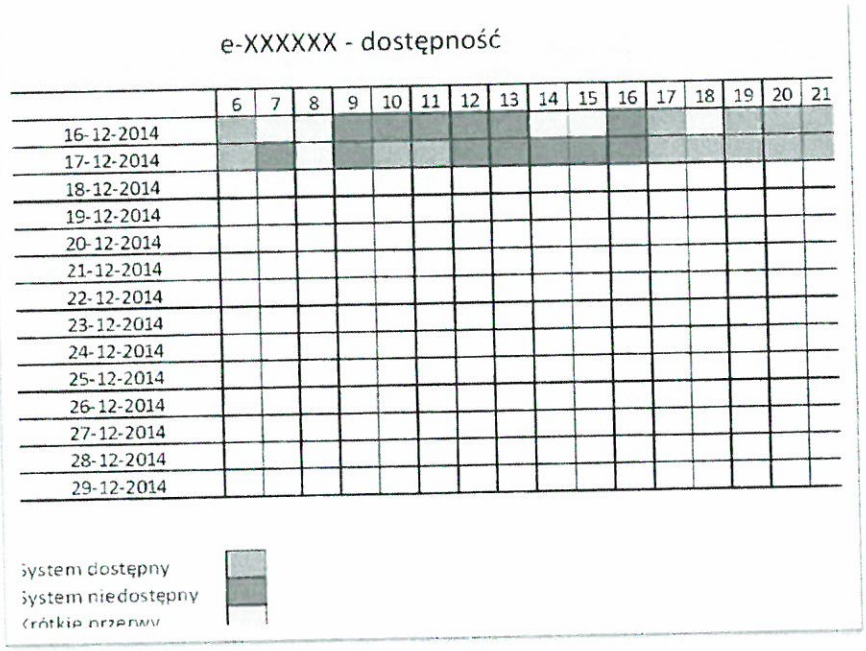

Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1„Społeczeństwo informacyjne – budowa elektronicznej administracji"

budowie projektu pl.ID posługiwano się oszacowaniami wymaganych przepływów informacji i, wynikającymi z nich niezbędnymi własnościami wydajnościowymi wprowadzanej architektury rozwiązań dla poszczególnych komponentów informatycznych oraz minimalnymi wymaganiami dla sieci teleinformatycznych i urządzeń.

Dokumenty projektowe zawierają natomiast opisy projektowanych zasobów sprzętowych i wykorzystywanych funkcji technicznych bez jakiegokolwiek odniesienia ich do niezbędnych zasobów dla:

1- dotychczasowego obciążenia pracą zastępowanych i funkcjonujących obecnie rozwiązań,
2- okresu rozruchu i wdrażania systemu wraz z działaniami migracyjnymi oraz
3- przewidywanych szczytowych obciążeń w związku z wprowadzaniem nowych dowodów osobistych i paszportów, planowanych zmian w obowiązku meldunkowym itd., itp.

Dla zobrazowania znaczenia adekwatnego określenia liczbowego metryk zapotrzebowania dla poszczególnych funkcjonalności poniżej zaprezentowano autentyczny przykład z monitorowania niedostępności web'owego systemu informatycznego pochodzący z ostatnich dni z sektora administracji publicznej na poniższym rysunku[19]. Widać braki w dostępności systemu spowodowane wzmożonym obciążaniem bazy danych przez zapytania zewnętrzne w godzinach rozpoczęcia dnia pracy i popołudniowego szczytu rozliczania dokumentów finansowych




[19] *Sytuacja ta została spowodowana niedawnym wprowadzeniem niedostatecznie przemyślanych zmian związanych z pośpiesznym uruchomieniem usługi elektronicznej bez przeanalizowania skutków (por. rozdział 3.3* Zarządzanie zmianą w rozumieniu ITIL, *dotyczący zarządzania zmianą i BIA) oraz zwiększonego obciążenia systemu pochodzącego od zewnętrznie generowanych usług elektronicznych.*


*Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1„Społeczeństwo informacyjne – budowa elektronicznej administracji"*

| | |
|---|---|
| **Wniosek** | W udostępnionych dokumentach analitycznych i projektowych dotyczących SRP: PESEL, BUSC, RDO, CRS, SOP znajdują się listy wymagań funkcjonalnych stanowiące transpozycje funkcjonalności określonej w podstawach prawnych wraz z procedurami pracy. Bez odniesienia się do oczekiwanych wydajności i czasu reakcji nie można jednak potwierdzić ani ich faktycznego dostarczenia ani wymaganej adekwatnej wydajności.<br>W dokumencie [SCENARIUSZE TESTÓW WYDAJNOŚCIOWYCH I OBCIĄŻENIOWYCH, SYSTEMU REJESTRÓW PAŃSTWOWYCH, Numer wersji: 1.5., Data ostatniej aktualizacji: 2014-12-12 – dokument 66] w części metodycznej zostały już zamieszczone takie ogólne warunki oraz wymagania wydajnościowe. |

## 4. Stan zidentyfikowanych niezgodności nie odpowiada protokołom akceptacyjnym przeprowadzonych odbiorów

| | |
|---|---|
| **Kategoria** | • Krytyczna |
| **Dziedzina COBIT/12207** | AI – Pozyskanie i implementacja oprogramowania<br>SW – specyfikacja oprogramowania |
| **Opis obserwacji** | Udostępniona dokumentacja zawiera szereg protokołów akceptacji potwierdzających dostarczone funkcjonalności systemu podpisanych przez Wykonawcę systemu w październiku br. W plikach JIRA [76, 77, 78, 79, 80, 81, 82] wytworzonych 8.12.2014 dla poszczególnych komponentów SRP znajdują się następujące liczby zidentyfikowanych niezgodności wraz z ich aktualnym statusem. Poniżej zestawiono liczności niezgodności dla wybranych 3 statusów: zarejestrowane; poddane „przeglądowi kodu" (zgodnie z dokumentem COI Proces wytwarzania oprogramowania[95] c należałoby uznać za stan odpowiadający spełnieniu przynajmniej funkcjonalnych wymagań jakościowych); oraz w testowaniu: |

| *Komponent SRP* | *Niezgodności* | *Przegląd kodu* | *Test* |
|---|---|---|---|
| **PESEL** | **225** | **1** | **19** |
| **BUSC** | **466** | **11** | **0** |
| **Common** | **114** | **2** | **17** |
| **Core** | **234** | **4** | **1** |
| **RDO** | **644** | **6** | **29** |
| **SOP** | **119** | **0** | **4** |
| **CRS** | **52** | **0** | **2** |
| **łącznie** | **1854** | **24** | **72** |

Czyli łącznie na 1854 zidentyfikowane dotąd nieprawidłowości tylko 24 obsłużono do poziomu „Przeglądu Kodu"[20], a w testowaniu znajduje się dalsze 72. Pozostałe 1758 nie są jeszcze w ogóle obsłużone. Gdyby te liczby nanosić regularnie (np. cotygodniowo) na wykres kalendarzowy można z dużym prawdopodobieństwem wskazać jeszcze kilkanaście miesięcy niezbędnych do ustabilizowania systemu i doprowadzenia go do używalności funkcjonalnej (bez uwzględniania różnych kategorii nieprawidłowości).

[20] W metodyce wytwórczej oprogramowania przyjętej w COI [95] status „przegląd kodu" oznacza fragment kodu o jakości kwalifikującej do ponownego wykorzystywania przez innych deweloperów, o ile przegląd ten przebiegnie pomyślnie.



*Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1„Społeczeństwo informacyjne – budowa elektronicznej administracji"*

**Wniosek**

1. **Na podstawie tak wyglądającej statystyki wewnętrznej Wykonawcy systemu należy stwierdzić, że wymagane funkcjonalności nie zostały wytworzone, a zatem i nie mogły być uznane za dostarczone.**

Biorąc pod uwagę kategorię zakwalifikowania znacznej liczby niezgodności jako „Major", co oznacza zgodnie z metodyką przyjętą w COI[21] brak kompatybilności pomiędzy wydaniami, istnieje znaczące ryzyko, że systemu nie da się ustabilizować w przewidywalnej przyszłości. Przy braku kompatybilności bowiem należy oczekiwać ponownego pojawiania się niezgodności poprzednio już obsłużonych.

To zjawisko potwierdza udostępniony dokument z retestowania [7_Ostatnie statystyki retestów_10.12.2014 – dokument 65] gdzie, przykładowo m.in. dla komponentu BUSC: *„..Zamknięto 18 błędów o statusie poważny, 25 błędów o statusie poważny ponownie otwarto; z uwagi na awarię serwera - testy zakończyły się o 17.30.; Zgłoszono 10 nowych błędów: 4 poważnych / 4 średnich /1 niskie. Ponadto pozostało do retestu: 1 poważnych i 63 średnie."*

Dla komponentu PESEL odpowiednio:

| PESEL | Ogółem | Poważny | Średni |
|---|---|---|---|
| Do retestu | 38 | 22 | 16 |
| Zamknięto | 18 | 8 | 10 |
| Ponownie otwarto | 5 | 4 | 1 |
| Do uszczegółowienia | 3 | 3 | 0 |

Dla komponentu RDO: *„wykonano retest 27 zgłoszeń, 10 zgłoszeń zostało zamkniętych - błędy naprawione.; 1 zgłoszenie zostało odrzucone za zgodą stron; 1 zgłoszenie wymaga konsultacji wewnątrz MSW; 15 zgłoszeń zostało ponownie otwartych - błędy nie zostały naprawione lub pojawiły się nowe błędy związane z testowaną funkcjonalnością.;*

*Stan ogólny błędów zgłoszonych w RDO na zakończenie 10.12.2014: wszystkich zgłoszonych błędów: 454; zamknięte zgłoszenia: 315; otwarte po stronie COI: 73; otwarte po stronie MSW: 66."*

2. **Testy wewnętrzne Wykonawcy systemu nie gwarantują zidentyfikowania i usunięcia większości niezgodności PRZED przekazaniem kodu użytkownikom do testowania akceptacyjnego. Zarządzanie jakością kodu (QA) w COI nie jest wystarczające. Z punktu widzenia dobrych praktyk wykorzystywanie personelu Zamawiającego do prowadzenia *de facto* testów wewnętrznych u Wykonawcy systemu nie jest dopuszczalne i prowadzi do obniżenia jakości kodu, demotywacji po stronie personelu Zamawiającego oraz korozji wiarygodności COI jako wytwórcy kodu. Przerzuca to także znaczącą część kosztów opracowania oprogramowania na Zamawiającego.**
3. **Niedostateczna jakość wytwarzanego kodu ani niedostatek procedur jakości QA po stronie COI nie figuruje w Planie Ryzyka COI [72, 73, 74, 75, 71] ani też w Analizie Ryzyka w Studium Wykonalności [61].**
4. **Struktury projektowe po stronie COI oraz MSW nie zawierają**

[21] Wg metody wytwórczej oprogramowania SCRUM stosowanej w COI [Proces wytwarzania oprogramowania – dokument 95, str. 7/27 (brak numeracji stron i statusu zatwierdzenia)] status niezgodności (issue) oznaczony jako „Major" oznacza, że *„Wersja "major" jest używana do określania zmian niekompatybilnych wstecznie lub przełomowych względem publicznego API aplikacji. Wszystkie narzędzia produkowane wewnętrznie lub zewnętrznie powinny precyzyjnie określać wersję "major" aplikacji, gdyż ma to krytyczny wpływ na ich działanie oraz kompatybilność."*



*Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1„Społeczeństwo informacyjne – budowa elektronicznej administracji"*

| | |
|---|---|
| | **wydzielonego i niezależnego od pionowej hierarchii stanowiska/roli QA.[40, 41, 42, 43, 97, 99]** |

| **5. Wprowadzające w błąd opisy czynności wykonywane w tzw. procesach biznesowych** | |
|---|---|
| **Kategoria** | • Poważna |
| **Dziedzina COBIT/12207** | AI – Pozyskanie i implementacja oprogramowania<br>SW – specyfikacja oprogramowania |
| **Opis obserwacji** | W P001.01 Proces sporządzania aktu urodzenia [Dokument PT BUSC.pdf - 19] pokazano czynność o nazwie „Podanie w systemie BUSC daty sporządzenia karty urodzenia ...", po której nie następuje przejście do czynności wykonywanej przez BUSC, co powoduje dezorientację dewelopera kodu co do czynności wykonywanych przez system BUSC. Jednocześnie w projekcie technicznym BUSC zaprojektowano przypadek użycia PU-BUSC-1, który *de facto* implementuje przytoczoną wcześniej czynność procesu P001.01. |
| **Wniosek** | Bardzo duże prawdopodobieństwo braku identyfikacji, opracowania i zaimplementowania wszystkich niezbędnych przypadków użycia w opisanych tzw. procesach biznesowych. |

| **6. „Wymagania funkcjonalne" opisane w sposób wieloznaczny** | |
|---|---|
| **Kategoria** | • Poważna |
| **Dziedzina COBIT/12207** | AI – Pozyskanie i implementacja oprogramowania<br>SW – specyfikacja oprogramowania |
| **Opis obserwacji** | [Projekt techniczny modernizowanej Bazy Usług Stanu Cywilnego - 19] Id: P001.01.W.01 „Możliwość sporządzenia aktu w dowolnym trybie", nie informuje jakie mogą być tryby sporządzenia aktu, zatem wprowadza możliwość niejednoznacznego opisu tzw. „procesu biznesowego", co w konsekwencji może uniemożliwić prawidłową identyfikację wszystkich niezbędnych przypadków użycia w tzw. „procesie biznesowym" |
| **Wniosek** | Bardzo duże prawdopodobieństwo braku identyfikacji, opracowania i zaimplementowania wszystkich niezbędnych przypadków użycia w opisanych tzw. wymaganiach funkcjonalnych, co może prowadzić do ich nieuwzględnienia przy testowaniu akceptacyjnym systemu. |

| **7. Brak opisów wszystkich aktorów[22] występujących w tzw. procesach biznesowych** | |
|---|---|
| **Kategoria** | • Poważna |
| **Dziedzina COBIT/12207** | AI – Pozyskanie i implementacja oprogramowania<br>SW – specyfikacja oprogramowania |
| **Opis obserwacji** | W P001.01 Proces sporządzania aktu urodzenia [19] pokazano aktora o nazwie „elementy pozasystemowe procesu", który to aktor nigdzie nie jest opisany |

[22] Aktor - wyróżniony szereg kategorii osób, bądź systemów wykonujących konkretne zadania w ramach procesów biznesowych realizowanych w systemie informacyjnym pl.ID.



*Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1„Społeczeństwo informacyjne – budowa elektronicznej administracji"*

| | |
|---|---|
| **Wniosek** | Bardzo duże prawdopodobieństwo braku identyfikacji, opracowania i zaimplementowania wszystkich niezbędnych ról (uprawnień) wchodzących w interakcję ze zidentyfikowanymi przypadkami użycia w opisanych tzw. procesach biznesowych, co może prowadzić do ich nieuwzględnienia przy testowaniu akceptacyjnym systemu. |

| **8. Niejednoznaczne opisy aktorów występujących w tzw. procesach biznesowych** | |
|---|---|
| **Kategoria** | • Poważna |
| **Dziedzina COBIT/12207** | AI – Pozyskanie i implementacja oprogramowania<br>SW – specyfikacja oprogramowania |
| **Opis obserwacji** | W P001.01 Proces sporządzania aktu urodzenia [19] pokazano aktora o nazwie „kierownik USC lub urzędnik USC z odpowiednią rolą" oraz aktora o nazwie „kierownik USC", przy czym z tzw. „procesu biznesowego" wynika, iż są to różni aktorzy, gdyż wykonują różne czynności a dotyczy to tego samego zakresu uprawnień. |
| **Wniosek** | Bardzo duże prawdopodobieństwo braku identyfikacji, opracowania i zaimplementowania wszystkich niezbędnych ról (uprawnień) lub nadmiarowych ról wchodzących w interakcję ze zidentyfikowanymi przypadkami użycia w opisanych tzw. procesach biznesowych, co może prowadzić do duplikowania i redundancji poszczególnych części scenariuszy w różnych przypadkach użycia. |

| **9. Brak opisu scenariuszy poszczególnych przebiegów w tzw. procesie biznesowym** | |
|---|---|
| **Kategoria** | • Poważna |
| **Dziedzina COBIT/12207** | AI – Pozyskanie i implementacja oprogramowania<br>SW – specyfikacja oprogramowania |
| **Opis obserwacji** | Brak wizualizacji przypadków użycia – np. 3.1.1. Przypadek użycia nr 1. Kalendarz kierownika USC - rejestracja daty, do której wymagane jest zgłoszenie urodzenia - PU - BUSC – 1 [19] |
| **Wniosek** | **Brak wizualizacji przypadku użycia zwiększa prawdopodobieństwo pominięcia alternatywnych przebiegów scenariusza, co w konsekwencji może spowodować brak niezbędnych funkcjonalności w systemie informatycznym**, co może prowadzić do ich nieuwzględnienia przy testowaniu akceptacyjnym systemu albo utraty użyteczności lub zawieszeń systemu.. |

| **10. W trakcie testowania używane są trzy różne systemy rejestracji błędów: Jira, Mantis, Atmosfera** | |
|---|---|
| **Kategoria** | • Poważna |
| **Dziedzina COBIT/12207** | AI – Pozyskanie i implementacja oprogramowania<br>SW – specyfikacja oprogramowania |
| **Opis obserwacji** | W trakcie analizy testów stwierdzono, iż w ich trakcie używane są jednocześnie trzy różne systemy rejestracji błędów: Jira, Mantis, Atmosfera,[49, 50, 51, 52, 53, 63, 64, 60, 70, 76, 77, 78, 79, 80, 81, 82, 108, 109] |


*Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1„Społeczeństwo informacyjne – budowa elektronicznej administracji"*

| | |
|---|---|
| **Wniosek** | **Brak ujednoliconego systemu rejestracji i zarządzania informacjami o błędach i ich stanie może spowodować wzrost komplikacji procedur testowych, sztuczne zaniżanie liczby błędów oraz zwiększenie czasu niezbędnego na przeprowadzenie testów.** |

## 3.2. Wymogi wydajnościowe SRP

Wymagania dotyczące wydajności systemu informatycznego można ocenić na podstawie takich charakterystyk systemu jak:

- czas oczekiwania na reakcję systemu w określonych przypadkach użycia,
- dopuszczalne obciążenie sieci,
- ilość użytkowników jednocześnie korzystających z systemu,
- ilość jednoczesnych transakcji,
- akceptowalny poziom obniżenia wydajności systemu w określonym przedziale czasu,
- wykorzystanie zasobów (np. miejsce na dysku),
- uwarunkowania związane ze sprzętem komputerowym przeznaczonym do obsługi systemu.

Jednakże pierwszorzędnym zagadnieniem powinna być ocena wydajności związana z czasami oczekiwania przez użytkowników na reakcję systemu informatycznego. Zatem kluczowym zagadnieniem przy pomiarze wydajności jest prawidłowe określenie planu testów wydajnościowych oraz scenariuszy.

Poniżej zestawiono obserwacje związane z udostępnionym przez Zamawiającego planem testów [58 - Dokument: „COI_PLID_Scenariusze testów wydajnościowych i obciążeniowych SRPv1_3.docx" z dnia 14 listopada 2014 r.]. W trakcie realizacji ekspertyzy Zamawiający udostępnił powyższy dokument w wersji 1.5 [66], który już częściowo adresuje niektóre z zagadnień wymienionych powyżej. Wykonawca ekspertyzy pozostawił jednak częściowo inicjalne rekomendacje, gdyż właśnie ich wstępne sformułowanie i przekazanie do DEP stało się impulsem w celu ulepszenia przez COI początkowo udostępnionej wersji 1.3 dokumentu.

| **1. Brak wiarygodnych oszacowań na wymagania wydajnościowe** | |
|---|---|
| **Kategoria** | • Poważna |
| **Dziedzina COBIT/12207** | AI – Pozyskanie i implementacja oprogramowania<br>SW – specyfikacja oprogramowania |
| **Opis obserwacji** | W dokumencie [20130418_Projekt wysokopoziomowej architektury SRP_1.2.pdf] „Oszacowanie wymagań wydajnościowych serwerów" wykonano opierając się na aktualnych doświadczeniach związanych z eksploatacją systemu PESEL2 oraz dokumencie pt. „Koncepcja optymalizacji architektury SRP" opracowany na zlecenie CPI przez Sygnity w ramach projektu pl.ID (Załącznik nr. 3 do Projektu)" – str. 71. |


*Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1„Społeczeństwo informacyjne – budowa elektronicznej administracji"*

| | |
|---|---|
| **Wniosek** | **Nie daje się potwierdzić wiarygodności przyjętych założeń architektonicznych wpływających na wyliczenia niezbędnej wydajności. Brak informacji o ilości przetwarzanych danych, o jednostkach danych (pakiety ? żądania http ?), brak jest oszacowania wolumetryki.[23]** |

| **2. Brak informacji o konfiguracji środowiska do pomiaru testów wydajnościowych** | |
|---|---|
| **Kategoria** | • Krytyczna |
| **Dziedzina COBIT/12207** | COBIT:<br>M – Monitoring (Monitorowanie i ocena)<br>ISO IEC 12207:2008:<br>T - Technical (Procesy techniczne) |
| **Opis obserwacji** | W trakcie analizy dokumentacji Projektu pl.ID nie udało się zidentyfikować w specyfikacjach dotyczących planów testów:<br>1- Czy aplikacja do testowania bada poszczególne komponenty systemu, czy też uruchamia przeglądarkę, czy też jedynie wysyła żądania http?<br>2- Przez jakie łącza telekomunikacyjne będą prowadzone testy (gruby/cienki klient)?<br>3- Zastosowane narzędzie/aplikacji do testowania (z opisów testów wynika, iż zastosowano narzędzie JMeter, natomiast z dokumentacji projektowej wynika, iż do testów wydajnościowych zostanie zastosowane narzędzie SOAPUI [dokument 12_Specyfikacja Techniczna - Centralna Magistrala Serwisowa.pdf, str. 59 [12]]<br>4- Z ilu stanowisk będą realizowane testy wydajnościowe (z opisu testów wynika, iż prawdopodobnie testy planuje się uruchomić tylko z jednego komputera, co potwierdzono w rozmowach)<br>5- Na jakich danych przeprowadzane są testy (jakie dane zawierają bazy danych ?) i jakiej wielkości są to dane (porównywalne z z rzeczywistymi bazami danych) ? |
| **Wniosek** | Na podstawie udostępnionych dokumentów nie jest zatem możliwe jednoznaczne udzielenie odpowiedzi dotyczące poprawności planowanych testów.<br>Brak informacji o środowisku do realizacji testów wydajnościowych wprowadza ryzyko ograniczonej wiarygodności ich wyników.<br>W zaktualizowanej wersji opisu testów wydajnościowych ([66 - SCENARIUSZE TESTÓW WYDAJNOŚCIOWYCH I OBCIĄŻENIOWYCH, SYSTEMU REJESTRÓW PAŃSTWOWYCH, Numer wersji: 1.5., Data ostatniej aktualizacji: 2014-12-12]) znajduje się więcej informacji o środowisku do realizacji testów wydajnościowych, jednakże nadal brak informacji związanych z punktami wyspecyfikowanymi w wierszu „Opis obserwacji".<br>Jednocześnie brak informacji na temat danych, na jakich przeprowadza się testy wydajnościowe. Brak testów na danych rzeczywistych jeszcze bardziej zmniejszy wiarygodność wyniku testów wydajnościowych. |

[23] Wolumetryka opisuje wielkość i zakres przestrzeni pamięci stałej do przechowania i przetwarzania danych w systemie IT.


*Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1„Społeczeństwo informacyjne – budowa elektronicznej administracji"*

| 3. Wybrane scenariusze testowania są niereprezentatywne | |
|---|---|
| **Kategoria** | • Krytyczna |
| **Dziedzina COBIT/12207** | COBIT:<br>M – Monitoring (Monitorowanie i ocena)<br>ISO IEC 12207:2008:<br>T - Technical (Procesy techniczne) |
| **Opis obserwacji** | W trakcie analizy dokumentacji Projektu pl.ID [4, 5, 6, 7, 8, 9, 10, 11, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25] ustalono, iż:<br>1- Do testowania całego systemu wybrano 6 scenariuszy<br>2- Liczba scenariuszy zidentyfikowanych w dokumentacji pl.ID: 72 (SRP) + 64 (BUSC) + 17 (SOP) + 22 (CRS) + 39 (RDO) = 214, a z raportu z testów wynika, iż jest 314 funkcjonalności do testowania [9_dashboard_plid_?.pdf].<br>3- Brak odniesienia scenariuszy testowych do istniejących oznaczeń tzw. procesów biznesowych, czy przypadków użycia. |
| **Wniosek** | Na podstawie udostępnionych dokumentów można stwierdzić, iż testy wydajnościowe nie są reprezentatywne w stosunku do pełnej funkcjonalności systemu.<br>Brak pełnej reprezentacji scenariuszy testowych wprowadza ryzyko ograniczonej wiarygodności ich wyników.<br>W zaktualizowanej wersji opisu testów wydajnościowych ([66 - SCENARIUSZE TESTÓW WYDAJNOŚCIOWYCH I OBCIĄŻENIOWYCH, SYSTEMU REJESTRÓW PAŃSTWOWYCH, Numer wersji: 1.5., Data ostatniej aktualizacji: 2014-12-12]) nadal brak informacji związanych z punktami wyspecyfikowanymi w wierszu „Opis obserwacji". |

| 4. Zbyt duże założone czasy uzyskania odpowiedzi systemu | |
|---|---|
| **Kategoria** | • Krytyczna |
| **Dziedzina COBIT/12207** | COBIT:<br>M – Monitoring (Monitorowanie i ocena)<br>ISO IEC 12207:2008:<br>T – Technical (Procesy techniczne) |
| **Opis obserwacji** | W trakcie analizy dokumentacji Projektu pl.ID ustalono [dokumenty ], iż:<br>1- Średni czas reakcji systemu na żądanie użytkownika może dochodzić do 25s (ST-04)<br>2- Średni czas reakcji systemu na żądanie WebService może dochodzić do 10s (ST-09) |


*Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1„Społeczeństwo informacyjne – budowa elektronicznej administracji"*

| | |
|---|---|
| **Wniosek** | Na podstawie udostępnionych dokumentów wynika, iż założone parametry czasowe dotyczące reakcji systemu na żądania użytkowników, bądź systemów zewnętrznych są zbyt duże, by wydajność systemu była akceptowana przez użytkowników[24]. Przykład czasów reakcji systemu osiąganych już w 2008 roku: http://download.microsoft.com/download/7/0/1/701e1196-918d-4b4d-a18d-81781f78af21/MSCRM4_0_Skalowalnosc_i_Wydajnosc.pdf.<br>W zaktualizowanej wersji opisu testów wydajnościowych ([SCENARIUSZE TESTÓW WYDAJNOŚCIOWYCH I OBCIĄŻENIOWYCH, SYSTEMU REJESTRÓW PAŃSTWOWYCH, Numer wersji: 1.5., Data ostatniej aktualizacji: 2014-12-12]) podtrzymane są wielkości kwestionowane w punktach wyspecyfikowanych w wierszu „Opis obserwacji". |

| **5. Zbyt małe założone wielkości dla jednocześnie działających użytkowników systemu** | |
|---|---|
| **Kategoria** | • Krytyczna |
| **Dziedzina COBIT/12207** | COBIT:<br>M – Monitoring (Monitorowanie i ocena)<br>ISO IEC 12207:2008:<br>T – Technical (Procesy techniczne) |
| **Opis obserwacji** | W trakcie analizy dokumentacji Projektu pl.ID ustalono, iż:<br>1- System może poprawnie obsłużyć co najwyżej 500 użytkowników jednocześnie pracujących (ST-10)<br>2- Brak uzasadnienia (wiarygodnego źródła), iż 1 wątek symuluje wielu użytkowników, a nie tylko jednego użytkownika (ST-10)<br>3- W systemie będzie pracowało około 15 tys. użytkowników (konsultacje z pracownikami MSW)<br>4- Dla 15 tys. użytkowników należy założyć prawdopodobieństwo wystąpienia sytuacji, w której jednocześnie działa 30%[25] użytkowników.<br>5- Należy też określić oczekiwane, szczytowe oraz maksymalne obciążenie systemu SRP związane ze świadczeniem usług elektronicznych dla pozostałych podłączonych instytucji i organizacji. |
| **Wniosek** | Na podstawie udostępnionych dokumentów oraz uzyskanych informacji wynika, iż założone parametry czasowe dotyczące jednocześnie działających użytkowników są zbyt małe, by wydajność systemu mogła być wiarygodnie zweryfikowana.<br>W zaktualizowanej wersji opisu testów wydajnościowych ([66 - SCENARIUSZE TESTÓW WYDAJNOŚCIOWYCH I OBCIĄŻENIOWYCH, SYSTEMU REJESTRÓW PAŃSTWOWYCH, Numer wersji: 1.5., Data ostatniej aktualizacji: 2014-12-12]) podtrzymane są wielkości kwestionowane w punktach wyspecyfikowanych w wierszu „Opis obserwacji". |

| **6. Zbyt małe założone wielkości dla liczby działających użytkowników systemu i usług WebService w ciągu doby** | |
|---|---|
| **Kategoria** | • Krytyczna |
| **Dziedzina** | COBIT:<br>M – Monitoring (Monitorowanie i ocena) |

[24] http://www.nngroup.com/articles/website-response-times/ - użytkownicy są w stanie bez irytacji reagować do max. 8 sekund; http://searchsoftwarequality.techtarget.com/tip/Acceptable-application-response-times-vs-industry-standard.
[25] http://perfwork.wordpress.com/2012/02/01/estimating-maximum-users-that-an-application-can-support/


*Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1„Społeczeństwo informacyjne – budowa elektronicznej administracji"*

| | |
|---|---|
| **COBIT/12207** | ISO IEC 12207:2008:<br>T – Technical (Procesy techniczne) |
| **Opis obserwacji** | W trakcie analizy dokumentacji Projektu pl.ID [58, 66] ustalono, iż:<br>Parametr „Constant Throughput Timer" ustalono na 181,25/min, co oznacza, iż średnio w ciągu doby przewiduje się obsługę około 3 zdarzeń na sekundę związanych z obsługą żądania użytkownika, bądź usługi WebService, przy czym nie uzasadniono tego parametru. |
| **Wniosek** | Na podstawie udostępnionych dokumentów oraz uzyskanych informacji wynika, iż wartość parametru „Constant Throughput Timer" jest zbyt mała, gdyż pozostałe parametry zakładają obsługę w jednej sekundzie co najmniej 100 użytkowników, bądź 100 usług WebService. Zatem wartość parametru „Constant Throughput Timer" na poziomie 3 zdarzeń na sekundę jest zbyt mała.<br>W zaktualizowanej wersji opisu testów wydajnościowych ([66 - SCENARIUSZE TESTÓW WYDAJNOŚCIOWYCH I OBCIĄŻENIOWYCH, SYSTEMU REJESTRÓW PAŃSTWOWYCH, Numer wersji: 1.5., Data ostatniej aktualizacji: 2014-12-12]) podtrzymane są wielkości kwestionowane w wierszu „Opis obserwacji". |

| **7. Brak informacji o wynikach zakończenia scenariuszy** | |
|---|---|
| **Kategoria** | • Krytyczna |
| **Dziedzina COBIT/12207** | COBIT:<br>M – Monitoring (Monitorowanie i ocena)<br>ISO IEC 12207:2008:<br>T – Technical (Procesy techniczne) |
| **Opis obserwacji** | W trakcie analizy dokumentacji Projektu pl.ID [58, 66] ustalono, iż:<br>Specyfikacja testów wydajnościowych nie podaje jakim rezultatem kończą się poszczególne scenariusze, co może spowodować spadek wiarygodności takich testów. |
| **Wniosek** | Na podstawie udostępnionych dokumentów wynika, iż brak informacji o wynikach zakończenia scenariuszy testowych może oznaczać, iż zaniedbano taki parametr planu testów. Zatem wyniki testów, w których wszystkie scenariusze kończą się niepowodzeniem (np. błędem systemu) nie będą reprezentatywne dla wszystkich testów, a tym samym nie będą wiarygodne.<br>W zaktualizowanej wersji opisu testów wydajnościowych ([66 - SCENARIUSZE TESTÓW WYDAJNOŚCIOWYCH I OBCIĄŻENIOWYCH, SYSTEMU REJESTRÓW PAŃSTWOWYCH, Numer wersji: 1.5., Data ostatniej aktualizacji: 2014-12-12]) nadal brak informacji opisanych w wierszu „Opis obserwacji". |

# 3.3. Zarządzanie zmianą w rozumieniu ITIL

**Poniżej przedstawiono Obserwacje i Wnioski związane z Zarządzaniem Zmianą.**

| **1. Brak udokumentowania procesu Zarządzania Zmianą w obszarze utrzymania usług w COI** | |
|---|---|
| **Kategoria** | • Poważne |
| **Dziedzina ITIL** | Service Transition |
| **Opis obserwacji** | W trakcie analizy przekazanej dokumentacji nie stwierdzono formalnego udokumentowania funkcjonowania procesu. Przekazane dokumenty nie |



*Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1„Społeczeństwo informacyjne – budowa elektronicznej administracji"*

| | |
|---|---|
| | stwierdzają, że proces jest spójny i występuje w organizacji. Nie można jednoznacznie stwierdzić, że proces jest powtarzalny. Nie można stwierdzić, że występuje zaangażowanie w proces zarządzania zmianą ze strony organizacji, zarządu i personelu. Zgodnie z pismem COI-ZPLID.0500.25.2014 [70] punkty 1d, 1e nie stwierdzają, czy zmiana jest dokonywania w oparciu o dobre praktyki zawarte w bibliotekach ITIL. [109]<br>Stwierdzono obecność w Pionie Eksploatacji systemów Procedury [94] oraz Instrukcji Zarządzania Zmianą od 2012 z ostatnią aktualizacją z jesieni 2014 [92]. |
| **Wniosek** | Zgodnie z dokumentami Procedurą (COI) oraz Instrukcją zarządzania zmianą (CEPIK2) można stwierdzić istnienie dobrych praktyk w części utrzymywanych usług w COI. Brak jednak formalnie zatwierdzonych reguł dla całej organizacji może powodować brak zarządzania w pełnym spektrum działalności COI.<br>**Brak kompleksowego podejścia może skutkować powstawaniem ryzyka zmian nieprzemyślanych, jak i, w przypadku wystąpienia błędów, brak możliwości powrotu do konfiguracji pierwotnej. W konsekwencji może to prowadzić do zatrzymania usług.** |

| **2. Nie można stwierdzić jednoznacznie, że występuje gwarancja zapisania wszelkich zmian w elementach konfiguracji i sprawnego nimi zarządzania w obszarze utrzymania usług w COI.** | |
|---|---|
| **Kategoria** | • Poważne |
| **Dziedzina ITIL** | Service Transition |
| **Opis obserwacji** | Zgodnie z przekazanymi dokumentami nie można stwierdzić, że zmiany są planowane i kontrolowane oraz rozumie się ich wpływ. Zaobserwowano brak zapewnienia, że istnieją plany naprawy. Zgodnie z pismem COI-ZPLID.0500.25.2014 zaobserwowano, że organizacja posiada system klasy ITSM w którym są prowadzone zmiany [63, 64, 108, 109]. Na podstawie dostarczonych dowodów nie można jednoznacznie stwierdzić, że proces Zarzadzania Zmianą został zaimplementowany zgodnie z ITIL, przekazana informacja jest niewystarczająca. |
| **Wniosek** | Brak nadzoru nad procesem oraz uwzględniania wszystkich zmian powodują niejednoznaczność i możliwość konfliktu zmian w elementach konfiguracji. Przykładowo, zmiany w systemach mogą się nałożyć ze zmianami prowadzonymi w obszarze sieci i sparaliżować realizację jednego z zadań, a co w konsekwencji może doprowadzić do dłuższego przestoju świadczonej usługi. |

| **3. Nie można stwierdzić jednoznacznie, że zmiany podlegają wewnętrznej autoryzacji i podejmowanie decyzji o zmianach są adekwatne w obszarze utrzymania usług w COI.** | |
|---|---|
| **Kategoria** | • Poważne |
| **Dziedzina ITIL** | Service Transition |
| **Opis obserwacji** | Zgodnie z przekazanymi dokumentami nie można stwierdzić, że zmiany są autoryzowane i podejmowanie decyzji o zmianach, jest poprzedzone analizą ryzyka. Nie stwierdzono prowadzenia analizy ryzyka w obszarze utrzymania usług dla zmian. Zgodnie z pismem COI-ZPLID.0500.25.2014 [70] niema informacji, czy w ramach organizacji występuje proces planowania i kontrolowania zmian.<br>Stwierdzono obecność w Pionie Eksploatacji Systemów Procedury oraz Instrukcji Zarządzania Zmianą. W ramach przekazanych dokumentów na str.19 |


*Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1„Społeczeństwo informacyjne – budowa elektronicznej administracji"*

| | |
|---|---|
| | [94] Procedury Zarządzania Zmianą nie stwierdzono procesu autoryzacji zmiany. |
| **Wniosek** | Brak autoryzacji zmian może prowadzić do niekontrolowanych zmian. Przykładem takiego działania jest wgranie poprawki systemowej w systemie produkcyjnym bez wcześniejszego uzgodnienia i akceptacji. Wgranie takiej poprawki może spowodować zatrzymanie świadczenia usługi. |

| **4. Nie można stwierdzić jednoznacznie, że role/odpowiedzialności w zakresie prowadzenia zmiany są zaadresowane.** | |
|---|---|
| **Kategoria** | • Poważne |
| **Dziedzina ITIL** | Service Transition |
| **Opis obserwacji** | Zgodnie z przekazanymi dokumentami nie można stwierdzić, że zgodnie z ITIL są wytworzone role dla procesu zmiany.<br>Stwierdzono obecność w Pionie Eksploatacji systemów Procedury [94] oraz Instrukcji Zarządzania Zmianą [92]. |
| **Wniosek** | Brak zdefiniowania ról oraz odpowiedzialności w procesie zarządzania zmianą może doprowadzić do niezapewnienia należytej obsługi zmiany. Taki stan rzeczy może rzutować na jakość wykonanej zmiany i uniemożliwiać zachowanie powtarzalności procesu. W konsekwencji braki te mogą być szkodliwe dla usług i uniemożliwić skuteczne przeprowadzenie Zmiany. |

| **5. Brak Zarządzania Zmianą w obszarze wytwarzania Systemu Rejestrów Państwowych u wykonawcy systemu COI.** | |
|---|---|
| **Kategoria** | • Krytyczna |
| **Dziedzina ITIL** | Service Transition |
| **Opis obserwacji** | W trakcie analizy przekazanej dokumentacji „5_Projekt wysokopoziomowej architektury SRP" [4] nie stwierdzono formalnego udokumentowania procesu.<br>W w/w dokumencie w punkcie 3.8 mowa jest o wytworzeniu procedury wdrażania zmian po wdrożeniu produkcyjnym systemu. W ramach przekazanych dokumentów można wyszczególnić poszczególne zlecenia, oraz ich odbiór jako elementów systemu. Wskazuje na to również przekazany harmonogram projektu. |
| **Wniosek** | Zważywszy na fakt, że elementy systemu, podlegają cząstkowemu odbiorowi oraz brak jest wewnętrznych regulacji w zakresie zarządzania zmianą (nie stwierdzono w obszarze wytwarzania SRP) – zgodnie z przekazaną wiedzą nie występuje Zarządzanie zmianą w projekcie w rozumieniu bibliotek ITIL.<br>Brak funkcjonującego procesu może skutkować przerwaniem funkcjonowania oddanych elementów systemu lub nie spójność w elementach systemu. W konsekwencji również może doprowadzić do braku zgodności dokumentacji systemu ze stanem faktycznym. Taki stan rzeczy może doprowadzić do uniemożliwienia MSW samodzielnego rozwoju lub dowolnego dysponowania SRP. |



*Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1„Społeczeństwo informacyjne – budowa elektronicznej administracji"*

# 3.4. Zarządzanie ryzykiem i ciągłością

Poniżej przedstawiono Obserwacje i Wnioski związane z Zarządzaniem Zmianą.

| **1. Brak zdefiniowanej polityki SZCD (Systemu Zarządzania Ciągłością Działania) (p. 5.3 normy ISO 22301:2012)[28]** | |
|---|---|
| **Kategoria** | • Krytyczna |
| **Dziedzina ISO 22301** | Polityka |
| **Opis obserwacji** | Zgodnie z normą kierownictwo instytucji winno ustanowić politykę ciągłości działania, która jest dostępna formie udokumentowanej, zakomunikowana, dostępna dla osób zaangażowanych w proces oraz podlega przeglądom. Nie stwierdzono dokumentu tego typu w przekazanych materiałach. Brak formalnego opracowania polityki może spowodować nieadekwatną odpowiedź na zdarzenie kryzysowe i niezdolność organizacji do pełnienia powierzonych zadań. |
| **Wniosek** | **Norma 22301 wymaga utworzenie formalnej polityki SZCD. Brak dokumentu oznacza niespełnienie podstawowego wymogu normy.** |

| **2. Brak zdefiniowanych granic SZCD (p. 4.3.2 normy ISO 22301:2012)[28]** | |
|---|---|
| **Kategoria** | • Krytyczne |
| **Dziedzina ISO 22301** | Zakres SZCD |
| **Opis obserwacji** | Zgodnie z normą zakres powinien być dostępny w formie udokumentowanej informacji. Nie stwierdzono udokumentowanego zakresu SZCD. Stwierdzono w dokumencie „5_Projekt wysokopoziomowej architektury SRP" [4] w punkcie 3.7 następujący element SZCD: „winien być zgodnie z w/w dokumentem wytworzony dokument „Procedury awaryjne (DR)"" – brak tego dokumentu w woluminie dokumentów przekazanych. Brak zdefiniowania obszarów do odtworzenia wewnętrznych oraz zewnętrznych w rozumieniu celów organizacji może spowodować załamanie się możliwości ich realizacji, a co za tym idzie, paraliż funkcjonowania. Przez zewnętrze należy tu rozumieć cele postawione COI przez MSW, a wnętrze to cele niezbędne dla funkcjonowania COI. Przypadek taki będzie miał miejsce np. gdy COI nie zapewni procedur odtworzeniowych, gdy aktualni administratorzy systemu są niedostępni lub nie stawią się do pracy z dowolnego powodu.<br>Nie zidentyfikowano udokumentowania analizy wpływu BIA (Business Impact Analysis), co uniemożliwia wyselekcjonowanie procesów krytycznych (zdefiniowanie obszarów) oraz określenie odpowiednich czasów odtworzeniowych w zakresie systemów teleinformatycznych (RTO) oraz punktu odtworzenia (RPO). |
| **Wniosek** | **COI nie wykazuje spełniania normy ISO 22301 p.4.3.2** |

| **3. Brak zdefiniowanych ról, odpowiedzialności i uprawnień w organizacji dla SZCD. (p. 5.4 normy ISO 22301:2012)[28]** | |
|---|---|
| **Kategoria** | • Krytyczne |
| **Dziedzina ISO 22301** | Role SZCD |


*Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1„Społeczeństwo informacyjne – budowa elektronicznej administracji"*

| | |
|---|---|
| **Opis obserwacji** | Zaobserwowano brak zdefiniowania sztabu kryzysowego w organizacji oraz zespołów odtworzeniowych. Brak zdefiniowanych ról w planie oraz odpowiedzialności uniemożliwia skuteczną reakcję na zdarzenie kryzysowe oraz paraliżuje komunikację i zarządzanie zdarzeniem. Sytuacja taka to np. brak informacji kto ma podjąć działanie gdy jeden z komponentów systemu nie działa poza godzinami pracy. Brak tego elementu (sztabu kryzysowego) oznacza niezdolność w organizacji odtworzenia procesów krytycznych wewnętrznych oraz zewnętrznych. |
| **Wniosek** | **COI nie wykazuje spełniania normy ISO 22301 p.5.4.** |

| **4. Brak zdefiniowanej ścieżki komunikacji (p. 7.4 normy ISO 22301:2012)** [28] | |
|---|---|
| **Kategoria** | • Poważne |
| **Dziedzina ISO 22301** | Komunikacja |
| **Opis obserwacji** | Zaobserwowano brak zdefiniowania osób odpowiedzialnych za komunikację wewnątrz, jak i na zewnątrz organizacji . Brak zdefiniowania komunikacji w zakresie zdarzeń kryzysowych może spowodować zmniejszenie wiarygodności COI, a co może skutkować nadwątleniem zaufania do administracji publicznej. |
| **Wniosek** | **COI nie wykazuje spełniania normy ISO 22301 p.7.4.** |

| **5. Brak wykazania zaangażowania kierownictwa organizacji w SZCD (p. 5.2 normy ISO 22301:2012)** [28] | |
|---|---|
| **Kategoria** | • Krytyczne |
| **Dziedzina ISO 22301** | Przywództwo, zaangażowanie kierownictwa |
| **Opis obserwacji** | Nie zidentyfikowano dowodów zaangażowania kierownictwa organizacji w ustalenie polityki i celów SZCD, brak jest formalnego zatwierdzenia Planu oraz dowodów zapewnienia zasobów niezbędnych dla działania SZCD. Brak jednoznacznego zaangażowania może skutkować niewłaściwym podejściem ze strony personelu. Sytuacja taka to np. wysłanie na urlop krytycznych zasobów ludzkich niezbędnych do funkcjonowania COI w tym samym terminie i co za tym idzie paraliż w szczególności w realizacji celów. |
| **Wniosek** | Kierownictwo organizacji nie jest zaangażowane w SZCD zgodnie z wymogiem normy 22301.<br>**COI nie wykazuje spełniania normy ISO 22301 p.5.2.** |

| **6. Brak oceny wpływu biznesowego i oceny ryzyka (p. 8.2 normy ISO 22301:2012)** [28] | |
|---|---|
| **Kategoria** | • Krytyczne |
| **Dziedzina ISO 22301** | Analiza wpływu biznesowego i oceny ryzyka |
| **Opis obserwacji** | Nie udało się zidentyfikować w udostępnionej dokumentacji ustanowionego, wdrożonego i utrzymywanego formalnego i udokumentowanego procesu analizy wpływu biznesowego (BIA) oraz oceny ryzyka, brak definicji kryteriów i oceny potencjalnego wpływu incydentu zakłócającego działanie, brak dokumentów systematycznej analizy oraz ustalania priorytetów przy postępowaniu z ryzykiem, |



*Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1„Społeczeństwo informacyjne – budowa elektronicznej administracji"*

| | |
|---|---|
| | brak dokumentów oceny ryzyka. Braki zdefiniowania w/w elementów, czyli przeprowadzenia BIA (analiza wpływu na biznes) oraz prawidłowej oceny ryzyka, czyli określenie uzasadnionego prawdopodobieństwa i wpływu uniemożliwiają skuteczne zapobieganie zdarzeniom lub ograniczanie ich skutków. Również może to prowadzić do podjęcia nieadekwatnych działań, a co za tym idzie nieracjonalnych wydatków w obszarze ciągłości działania. Przykładem takiego działania może być nieracjonalne wydatkowanie środków na zasoby ludzkie, czyli zabezpieczenie odpowiednich kompetencji. |
| **Wniosek** | **COI nie wykazuje spełniania normy ISO 22301 p.8.2** |

| **7. Brak przeglądów zarządzania SZCD (p. 9.3 normy ISO 22301:2012)** [28] | |
|---|---|
| **Kategoria** | • Krytyczne |
| **Dziedzina ISO 22301** | Monitorowanie, pomiar, analiza i ocena |
| **Opis obserwacji** | Nie zidentyfikowano dowodów określenia metod monitorowania, pomiarów, analizy i oceny, brak dowodów dokonywania przeglądów SZCD organizacji. Brak prowadzenia pomiarów oraz przeglądów Systemu Zarządzania Ciągłości Działania prowadzi do nieadekwatnego reagowania organizacji na zmieniające się otoczenie. Przykładem takiego zdarzenia będzie np. śmierć technologiczna istotnego komponentu infrastruktury (obrazując to jest wycofanie się producenta np. Microsoftu ze wsparcia systemu operacyjnego np. Windows XP). |
| **Wniosek** | **COI nie wykazuje spełniania normy ISO 22301 p.9.3.** |


*Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1„Społeczeństwo informacyjne – budowa elektronicznej administracji"*

# 4. REKOMENDACJE

Zalecenia i rekomendacje zostały podzielone na cztery grupy zgodnie ze strukturą Umowy:

1. Rekomendacje działań do zrealizowania w zakresie realizacji zakontraktowanych wymogów funkcjonalnych.
2. Rekomendacje działań do zrealizowania w zakresie realizacji wymagań wydajnościowych.
3. Rekomendacje działań do zrealizowania w zakresie zarządzania zmianą w rozumieniu ITIL.
4. Rekomendacje działań do zrealizowania w zakresie zarządzania ciągłością działania.

## 4.1. Działania w zakresie realizacji zakontraktowanych wymogów funkcjonalnych

**W związku z powyższymi obserwacjami i wnioskami rekomenduje się:**

| Lp. | Rekomendacja | Możliwe skutki zaniechania |
|---|---|---|
| 1. | Każde wymaganie funkcjonalne powinno być zaopatrzone w wyczerpującą metrykę charakterystyk liczbowych.<br>Każdy biznesowy przypadek użycia (związany z jednym lub więcej wymaganiami funkcjonalnymi) należy opisać co najmniej jednym przypadkiem użycia, na podstawie którego opracowany powinien być co najmniej jeden przypadek (scenariusz) testowy z miernikiem/miernikami badającymi spełnienie powyższych metryk liczbowych dla przynajmniej wszystkich kluczowych wymagań funkcjonalnych.<br>Pokazanie powyższych powiązań i mapowania stosownych elementów (procesy biznesowe -> przypadki użycia -> przypadki testowe) uwiarygodnia proces przekazania produktów oprogramowania. | **Niezapewnienie świadczenia wymaganego poziomu usług przez SRP** |
| 2. | Należy wdrożyć zasady Zarządzania Jakością Oprogramowania po stronie COI oraz po stronie MSW. W COI powinien powstać specjalizowany zespół testujący **niezależny** od Kierownika Projektu pl.ID. Testy akceptacyjne komponentów mogą się zacząć **jedynie** po pomyślnym przejściu FAT (Factory Acceptance Tests)[5] korzystnie potwierdzonym podpisem certyfikowanego audytora QA. Na czas prowadzenia testów akceptacyjnych wersja oprogramowania i konfiguracja sprzętowo programowa środowiska **MUSZĄ** być zamrożone. Podobnie po stronie MSW należałoby formalnie | **SRP stał się wysoce złożonym komponentem struktury informacyjnej państwa. Jego zawodność skutkowałaby przerwaniem ciągłości działania całości lub bardzo wielu elementów krytycznych systemów bezpieczeństwa i ochrony zdrowia.** |



Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1„Społeczeństwo informacyjne – budowa elektronicznej administracji"

| | | |
|---|---|---|
| | utworzyć zadaniową strukturę QA. Ułatwiłoby to uzgadnianie kategorii identyfikowanych niezgodności oraz planowanie kolejnych wydań oprogramowania Kierownik QA powinien przedstawiać wyniki przeglądów jakości Sponsorowi projektu bez względu na podporządkowanie hierarchiczne. | |
| 3. | Należy dokonać szczegółowego przeglądu dokumentacji analitycznej w szczególności przypadków użycia (obecnie ich liczba wydaje się zbyt duża)[26] i konsekwentnie architektury rozwiązania oprogramowania w celu uproszczenia struktury i zmniejszenia stopnia złożoności kodu. | **j.w.** |
| 4. | Niezbędne jest opracowanie mapowania zaprojektowanych przypadków użycia na odpowiadające im czynności w tzw. procesach w celu wyeliminowania możliwości pominięcia opracowania i zaimplementowania wszystkich niezbędnych przypadków użycia. | **Wydłużony proces implementacji i wdrażania SRP.** |
| 5. | Opisy tzw. „wymagań funkcjonalnych" powinny zawierać jednoznaczne i enumeratywne tryby, czy sposoby działania/zmiany stanów obiektów, bądź dokumentów | **j.w.** |
| 6. | Niezbędne jest opracowanie listy aktorów występujących w tzw. procesach biznesowych w celu wyeliminowania możliwości pominięcia opracowania i zaimplementowania wszystkich niezbędnych ról i uprawnień, które powinny być zaimplementowane w systemie informatycznym. | **j.w.** |
| 7. | Należy opracować wizualizację przypadków użycia za pomocą np. diagramu aktywności UML w celu identyfikacji i kompletacji wszystkich niezbędnych przebiegów alternatywnych w scenariuszu celem identyfikacji wszystkich niezbędnych funkcjonalności w systemie informatycznym. | **j.w.** |

## 4.2. Działania w zakresie realizacji wymagań wydajnościowych

**W związku z powyższymi obserwacjami i wnioskami rekomenduje się:**

[26] Przyjmuje się zazwyczaj, że średnio skomplikowany system daje się opisać przy użyciu 30-40 przypadków użycia. Systemy operacyjne (jako przykład bardzo złożonego produktu) zawierają od 200 do 2000 tys. przypadków użycia. Ok. 70 przypadków użycia opisanych dla wymagań funkcjonalnych w BUSC wydaje się przesadnie dużo, co może prowadzić do zbytniej komplikacji kodu i ograniczenia jego re-używalności (podstawowy paradygmat SOA).



*Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1„Społeczeństwo informacyjne – budowa elektronicznej administracji"*

| Lp. | Rekomendacja | Możliwe skutki zaniechania |
|---|---|---|
| 1. | Należy opisać wyczerpująco i kompletnie środowisko do przeprowadzenia testów w celu wyeliminowania niejednoznaczności przy interpretacji wyników testów wydajnościowych.<br>W planach testów należy uwzględnić przeprowadzenie tzw. testów rozproszonych, czyli testów na kilku, jak nie kilkunastu stanowiskach równocześnie.<br>W przypadku zastosowania innych narzędzi, aniżeli przewidzianych w dokumentacji projektowej należy bezwzględnie ten fakt zaznaczyć oraz zaktualizować stosowny fragment dokumentacji. | **Niezapewnienie wymaganego poziomu dostępności usług SRP** |
| 2. | Należy zaprojektować testy wydajnościowe uwzględniając kompletny zestaw tzw. procesów biznesowych i przypadków użycia.<br>W planach testów należy wykorzystać oznaczenia i identyfikatory opracowanych i zaprojektowanych tzw. procesów biznesowych i przypadków użycia.<br>Po uzyskaniu pozytywnych wyników należy je powtórzyć w kompletnym środowisku pracy, tj. z uwzględnieniem faktycznych sieci teletransmisyjnych i realnych urządzeń dla typowych instalacji gminnych. | **j.w.** |
| 3. | Należy zaprojektować testy wydajnościowe uwzględniając maksymalny czas reakcji systemu na żądanie użytkownika (do 7 sekund), w przeciwnym przypadku istnieje duże prawdopodobieństwo szybkiego przeciążenia systemu poprzez zwielokrotnienie tych samych żądań użytkowników. | **j.w.** |
| 4. | Należy zaprojektować testy wydajnościowe uwzględniając maksymalny czas reakcji systemu na żądanie WebService (time-out na granicy części sekundy), w przeciwnym przypadku większość systemów zewnętrznych będzie przerywała komunikację wskutek zwyczajowych ustawień czasów time-out dla usług WebService na poziomie ułamka sekundy. | **j.w.** |
| 5. | Należy zaprojektować testy wydajnościowe uwzględniając 5 000 jednocześnie działających użytkowników w systemie.<br>Należy zaprojektować testy wydajnościowe uwzględniając takie progi użytkowników w systemie jak: 1, 10, 100, 500, 1000, 2000, 3000, 4000, 5000 itd., a następnie zidentyfikować punkt, w którym dalsze zwiększanie liczby jednocześnie pracujących użytkowników powoduje „załamanie" systemu.<br>Należy zaprojektować testy wydajnościowe dla testu | **j.w.** |


*Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1„Społeczeństwo informacyjne – budowa elektronicznej administracji"*

| | | |
|---|---|---|
| | ST-11 uwzględniając takie progi zdarzeń w systemie jak: 3, 10, 100, itd, a następnie zidentyfikować punkt, w którym dalsze zwiększanie liczby jednocześnie obsługiwanych zdarzeń powoduje „załamanie" systemu. | |
| **6.** | Należy zaprojektować scenariusze testowe, by mieć pewność iż kończą się one sukcesem. | **j.w.** |

## 4.3. Działania w zakresie zarządzania zmianą w rozumieniu ITIL

Zgodnie z definicją metodyki ITIL, celem procesu Zarządzania Zmianą jest wdrożenie zatwierdzonych zmian sprawnie i przy zachowaniu ryzyka możliwego do zaakceptowania z punktu widzenia zarówno istniejących, jak i nowych, przyszłych usług IT. Proces ten wymusza na jego uczestnikach myślenie proaktywne. Wyszczególnia się główne cele procesu zarządzania zmianą:

- odpowiadanie na wszelkie zmiany biznesowe względem potrzeb organizacji, przy jednoczesnym maksymalizowaniu wartości(lub użyteczności w sektorze publicznym) oraz redukcji incydentów, awarii i wymuszonych przeróbek;
- reagowanie na wnioski o zmianę (ang. RFC), tak aby powiązać usługi z potrzebami organizacji;
- zapewnienie, że zmiany zostaną zapisane i ocenione oraz, że autoryzowane zmiany otrzymają odpowiedni priorytet i zostaną zaplanowane, przetestowane, wdrożone i zarchiwizowane w zorganizowany sposób;
- optymalizacja całkowitego ryzyka biznesowego.

Zakres działania zarządzania zmianą obejmuje wszelkie zmiany wprowadzone do elementów konfiguracji usług, przez cały cykl życia procesu. Proces zarządzania zmianą dotyczy zmian zarówno w zakresie fizycznych komponentów takich jak np. serwery, jak i wirtualnych takich jak bazy danych, umowy, kontrakty. Proces ten swoim działaniem obejmuje także pięć składników procesu projektowania usług:

- rozwiązania usługowe
- narzędzia i systemy informowania kierownictwa
- struktury technologiczne oraz kierownicze
- procesy
- systemy i metody pomiarów

**Do głównych działań podejmowanych w ramach całego procesu zarządzania zmianą należą:**

- planowanie i kontrolowanie zmian
- zrozumienie wpływów zmian
- udzielanie autoryzacji zmianom i podejmowanie decyzji o zmianach
- tworzenie harmonogramu zmian i wydań
- komunikacja z interesariuszami
- zapewnienie, że istnieją plany napraw
- raporty kontrolne i miernicze


*Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1„Społeczeństwo informacyjne – budowa elektronicznej administracji"*

- ciągły rozwój procesu

**Główne czynności w procesie pojedynczej zmiany:**

- stworzenie i zapisanie RFC
- oszacowanie i ocena zmian
- określenie kto powinien być zaangażowany w proces oceny
- ocena wpływu na biznes, kosztów, zagrożeń oraz zysków
- autoryzacja zmian, gdy jest to możliwe
- przekazanie wiadomości o zmianie wszystkim interesariuszom
- koordynowanie procesu wdrażania zmian
- przegląd efektów i zamknięcie procesu

Proces ten winien być spisany w dokumencie formalnym obowiązującym w organizacji oraz zatwierdzony, jako obowiązujący, dla systemów tak i wewnętrznych, jak i zewnętrznych.

**Wejściem w procesie jest:**

- Dokument formalny np. polityka zarządzania zmianą;
- RFC lub propozycja zmiany
- plany zmian, przekazań, wydań, testów, ocen i napraw
- obecny harmonogram zmian lub przewidywana niedostępność usługi
- raporty z rezultatami testów i ocen okresowych
- konfiguracja odniesienia (podstawa dla przyszłych wersji, wydań zmian)

**Wyjściem z procesu jest:**

- odrzucone lub anulowane RFC
- autoryzowane zmiany lub propozycje zmian
- wprowadzenie zmian w usługach lub infrastrukturze w rezultacie autoryzowanych zmian
- nowe, zmienione lub wyrzucone elementy konfiguracji (do elementów konfiguracji zaliczają się zazwyczaj usługi informatyczne, sprzęt, oprogramowanie, budynki, ludzie oraz formalna dokumentacja, taka jak na przykład dokumentacja procesu oraz umowy o gwarantowanym poziomie świadczenia usług)
- zaktualizowany harmonogram zmian
- autoryzowane plany zmian
- raporty i zapisy zmian

**Podstawowe wyzwania dla procesu:**

- Zapewnienie, że każda zmiana zostanie zapisana i zarządzana.
- W procesie zarządzania zmianą, należy wiedzieć, czy przyspieszanie zmian, podniesie wartość firmy i będzie miało dobry wpływ na nią.
- W niektórych organizacjach, gdzie zarządzanie zmianami obejmuje tylko autoryzację zmian operacyjnych, zmiana w prawdziwy, pełnowartościowy proces zarządzania zmianą, zaangażowany w każdy inny proces zarządzania usługą, może być bardzo trudny.
- W dużych organizacjach znaczącym wyzwaniem może być akceptowanie i archiwizowanie zmian, zachodzących na wielu poziomach autoryzacji, ale potrzebnych do efektywnego zarządzania zmianami i komunikowania się w zakresie wprowadzonych zmian.


*Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1,Społeczeństwo informacyjne – budowa elektronicznej administracji"*

**W związku z powyższym rekomenduje się:**

| Lp. | Rekomendacja | Możliwe skutki zaniechania |
|---|---|---|
| 1. | Dobrą praktyką jest zbudowanie polityki lub procedury zarządzania zmianą w procesie utrzymania systemów teleinformatycznych w obszarze działalności COI oraz jej formalne zatwierdzenie, jako standard obowiązujący w organizacji.<br>Proces winien być udokumentowany i zarządzany. Proces powinien objąć wszystkie systemy/usługi i formalne zatwierdzenie jednolitych zasad w obszarze Zarządzania Zmianą. | **Długotrwała utrata świadczenia wszelkich usług przez System Rejestrów Państwowych** |
| 2 | Wymagane jest zbudowanie Polityki zarządzania zmianą w systemach teleinformatycznych w obszarze działalności COI z uwzględnieniem zagwarantowania zapisania wszelkich zmian w elementach konfiguracji i sprawnego nimi zarządzania. Optymalnym rozwiązaniem byłoby wytworzenie jednolitych zasad formalnych i implementacja ich w narzędziu ITSM. | **j.w.** |
| 3 | Wymagane jest zbudowanie Polityki zarządzania zmianą w systemach teleinformatycznych w obszarze działalności COI obejmującą zakresem planowanie i kontrolowanie. Pozwoli to na uniknięcie nieoczekiwanych przerw i zmniejszenie wpływu zmiany na aktualnie świadczone usługi. Przedstawioną procedurę oraz instrukcję należy dostosować do całej organizacji i formalnie zatwierdzić, aby obowiązywała dla wszystkich usług, w szczególności krytycznych świadczonych przez COI. | **j.w.** |
| 4 | Zgodnie z ITIL wymagane jest wytworzenie odpowiedzialności oraz role dla podprocesów w ramach zarządzania zmianą. Dobrą praktyką jest wytworzenie macierzy zgodnie z modelem RACI. Między innymi wytworzenie roli: menadżera ds. zmiany, Rada ds. zmian, Rada ds. zmian pilnych, Operator IT oraz Analityk techniczny. W szczególności istotne jest faktyczne wytworzenie ról odpowiedzialności zarządczej oraz odpowiedzialności zgodnie z ITIL. Odpowiednie zaadresowanie ról i odpowiedzialności może skutecznie przeciwdziałać zdarzeniom niepożądanym, jak np. nieoczekiwany przestój w świadczeniu usług, czy niekorzystny wpływ na integralność danych. | **j.w.** |
| 5. | Zważywszy na to, że dwa kluczowe Piony (Pion Eksploatacji Systemów oraz Pion Rozwoju Systemu) funkcjonują w zakresie Zarządzania Zmianą na odrębnych zasadach zachodzi potrzeba wypracowania jednolitego podejścia do przedmiotowego procesu. | **j.w.** |



*Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1„Społeczeństwo informacyjne – budowa elektronicznej administracji"*

| | | |
|---|---|---|
| | Niespójność w/w zakresie może mieć negatywny wpływ na całość wytwarzanego środowiska. | |
| 6. | Rekomenduje się pilne wytworzenie i wprowadzenie Zarządzania zmianą zważywszy na fakt przekazania elementów systemu do eksploatacji. Zmiany winny być zarządzane i dokumentowane. Brak prawidłowego zarządzania zmianą ma wpływ bezpośredni na inne procesy ITIL, takie jak:<br>▪ zarządzanie wiedzą;<br>▪ ocena zmiany;<br>▪ zarządzanie zasobami i konfiguracją usługi;<br>▪ planowanie i wsparcie przekazania;<br>▪ walidację i testowanie usługi.<br>W kontekście braku zarządzania zmianą zagrożone są krytyczne czynniki sukcesu w zakresie przedmiotowego procesu: odpowiadanie na RFC, optymalizację ryzyka biznesowego oraz gwarancja zapisania wszelkich zmian w elementach konfiguracji i sprawnego nimi zarządzania. | **j.w.** |

## 4.4. Działania w zakresie zarządzanie ryzykiem i ciągłością działania

Zgodnie z normą ISO 22301:2012 określającą wymagania dotyczące ustanawiania skutecznego Systemu Zarządzania Ciągłością Działania (SZCD) każda organizacja powinna określić zewnętrzne i wewnętrzne kwestie, które mają dla niej znaczenie i które wpływają na jej zdolność do osiągnięcia zamierzonych wyników SZCD. Przy ustanawianiu, wdrażaniu i utrzymywaniu SZCD organizacja powinna określić i udokumentować:

a) Swoje działalności, funkcje, usługi, wyroby, partnerstwa, łańcuchy dostaw, relacje z zainteresowanymi stronami oraz potencjalny wpływ związany z incydentami zakłócającymi jej działanie
b) Powiązania między polityką ciągłości działania a celami i innymi politykami organizacji, w tym z jej ogólna strategią zarządzania ryzykiem
c) Akceptowany poziom ryzyka (tzw. apetyt na ryzyko) dla organizacji.

W udostępnionych materiałach nie można odnaleźć żadnych dokumentów potwierdzających zrozumienie przez kierownictwo wytwórcy SRP wagi problematyki SZCD. W szczególności nie przedstawiono udokumentowanych polityk i procedur związanych z tym obszarem.

W zakresie zarządzania ryzykiem udostępnione dokumenty odnoszą się do planu działalności organizacji, np. Analiza ryzyka do planu działalności COI na rok 2013 i Analiza ryzyka do planu działalności COI na rok 2014[102, 73, 72, 71, 74, 75] i dotyczą ryzyk związanych z nieosiągnięciem przez organizację zaplanowanych celów, zamiast do zagadnień zarządzania ciągłością działania i ryzykami funkcjonowania samej organizacji.[27]

[27] Zdaniem Wykonawcy ekspertyzy ostatnie SW projektu pl.ID [61] zawierało prawidłowo przygotowaną i wiarygodną analizę ryzyka. Nie została ona jednak odzwierciedlona w Planie Ryzyka COI w części pl.ID, nie


Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1„Społeczeństwo informacyjne – budowa elektronicznej administracji"

**W związku z powyższym rekomenduje się:**

| Lp. | Rekomendacja | Możliwe skutki zaniechania |
|---|---|---|
| 1. | Wymagane jest opracowanie formalne Polityki Systemu Zarządzania Ciągłością Działania, pozwoli to na jasne i jednoznaczne reagowanie na zdarzenia i zachowanie ciągłości świadczenia usług oraz realizację postawionych celów.[28] | **Odniesienie do minimalnych wymagań dla systemów teleinformatycznych i ich powiązanie z normami ISO opisano w Załączniku 1.** |
| 2. | Rekomendowane jest przeprowadzenie analizy BIA[1] z interesariuszami (również uwzględniając MSW – jako cele zewnętrzne) i wyselekcjonowanie procesów krytycznych (czyli zdefiniowanie obszaru) oraz określenie odpowiednich czasów odtworzeniowych w zakresie systemów teleinformatycznych (RTO)[3] oraz punktu odtworzenia (RPO)[2]. Kolejnym krokiem byłoby zaakceptowanie wskazanych parametrów przez Właścicieli Biznesowych, czyli MSW. Winno być to ujęte w zatwierdzonym planie SZCD. | **Niezapewnienie wymaganego poziomu usług SRP lub niegospodarność wyrażająca się nieuzasadnionymi i nadmiernymi kosztami inwestycyjnymi i utrzymaniowymi infrastruktury SRP** |
| 3. | Wymagane jest zaadresowanie odpowiednio ról w planie odtworzeniowym oraz zakomunikowanie tego w organizacji. Zdefiniowanie w/w pozwoli skutecznie przeciwdziałać awariom i efektywnie nimi zarządzać. Winno być to ujęte w zatwierdzonym planie SZCD. | **Przerwy w świadczeniu usług przez SRP i funkcjonowaniu praktycznie wszystkich systemów państwa.** |
| 4. | Zdefiniowanie osób odpowiedzialnych za komunikację oraz autoryzację komunikatów jest istotne w trakcie procesu przywracania organizacji do funkcjonowania po zdarzeniu kryzysowym. Winno być to ujęte w zatwierdzonym planie SZCD. | **Powiększanie skutków dowolnej awarii i przerwy w świadczeniu usług SRP** |
| 5. | Wymagane jest zaangażowanie kierownictwa organizacji w budowę SZCD i powiązanie go z celami biznesowymi organizacji (np. wypełnianie zleconych zadań przez MSW) oraz zakomunikowanie tego w organizacji. Osoby będące w najwyższym kierownictwie i posiadające inne istotne role kierownicze w COI powinny wspierać swoim autorytetem SCZD. | **Nieskuteczność i nieefektywność wypracowanych rozwiązań.** |

zidentyfikowano również odpowiedniego Planu działań ograniczających lub zapobiegających tym ryzykom ani estymacji adekwatnego budżetu przeznaczonego na takie działania.

[28] Norma 22301 nie w pełni stosuje się do przedmiotowego systemu. W Krajowych Radach Interoperacyjności występuje bezpośrednie odwołanie do innych norm wg Rozp. RM §20 p.3: „Wymagania określone w ust. 1 i 2 uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą, w tym:
1) PN-ISO/IEC 17799 – w odniesieniu do ustanawiania zabezpieczeń;
2) PN-ISO/IEC 27005 – w odniesieniu do zarządzania ryzykiem;
3) PN-ISO/IEC 24762 – w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania."


*Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1„Społeczeństwo informacyjne – budowa elektronicznej administracji"*

| | | |
|---|---|---|
| **6.** | COI powinien ustanowić, wdrożyć i utrzymywać formalny i udokumentowany proces oceny skutków zakłócenia działalności wspomagających dostarczanie produktów i usług, w tym dostawców, partnerów outsourcingowych i innych istotnych zainteresowanych stron. Korzyścią z prowadzenia prawidłowej oceny ryzyka jest racjonalny dobór środków do potrzeb, co za tym idzie efektywne zarządzanie budżetem w obszarze ciągłości organizacji np. wyliczanie ROSI (Return on Security Investment). | **Niezapewnienie wymaganego poziomu usług SRP lub niegospodarność wyrażająca się nieuzasadnionymi i nadmiernymi kosztami inwestycyjnymi i utrzymaniowymi infrastruktury SRP** |
| **7.** | Najwyższe kierownictwo powinno dokonywać przeglądów SZCD dla COI w zaplanowanych okresach czasu, organizacja powinna dokonywać oceny efektów działania SZCD, opracować procedury monitorowania efektywności SZCD. Prowadzenie w/w i ciągłe doskonalenie SZCD pozwala na efektywne reagowanie na zmiany w otoczeniu COI. | **Nieskuteczność i nieefektywność wypracowanych rozwiązań.** |


*Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1„Społeczeństwo informacyjne – budowa elektronicznej administracji"*

# 5. PODSUMOWANIE WNIOSKÓW Z EKSPERTYZY

Zgodnie z Umową ekspertyza powinna zawierać następujące odpowiedzi i informacje:

| | |
|---|---|
| Czy zakontraktowane wymogi funkcjonalne Systemu Rejestrów Państwowych zostały dostarczone i mają odwzorowanie w dokumentacji technicznej? | Zgodnie z udostępnioną dokumentacją COI i MSW na dzień dostarczenia ekspertyzy, a w szczególności z brakiem opisów scenariuszy prowadzonych testów akceptacyjnych zakontraktowane wymogi funkcjonalne **NIE ZOSTAŁY DOSTARCZONE, gdyż brak informacji co jest przedmiotem testów akceptacyjnych**. Kolejnym dowodem na powyższą odpowiedź jest fakt, iż obecnie zarejestrowanych jest kilkaset niezgodności, z których duża część ma kategorię „poważne" czyli funkcjonalności niemożliwe do prawidłowego wykonania. Oznacza to, iż testy akceptacyjne przeprowadza się raczej intuicyjnie i niezgodnie z opracowaną wcześniej dokumentacją projektu pl.ID. Dotyczy to przede wszystkim kluczowych referencyjnych części systemu czyli PESEL, BUSC i RDO. |
| Czy wymogi wydajnościowe Systemu Rejestrów Państwowych są adekwatne do systemu tej skali i czy zostały potwierdzone poprawnie przeprowadzonymi testami? | Na podstawie udostępnionej dokumentacji należy stwierdzić, iż wymogi wydajnościowe Systemu Rejestrów Państwowych obecnie **NIE SĄ ADEKWATNE DO SYSTEMU TEJ SKALI** i nie zostały potwierdzone poprawnie przeprowadzonymi testami. Zaproponowane przez COI testy wydajnościowe nie oddają ani złożoności środowiska, ani nie są reprezentatywne dla faktycznie oczekiwanych obciążeń. Nie są znane również ich wyniki. |
| Czy system zarządzania zmianą po stronie wytwórcy Systemu Rejestrów Państwowych jest adekwatny w rozumieniu ITIL? | System zarządzania zmianą po stronie wytwórcy SRP **NIE JEST ADEKWATNY W ROZUMIENIU ITIL.** Jedyny dokument opisujący taki system nie jest zatwierdzony, nie zidentyfikowano również dowodów potwierdzających jego stosowanie. Udostępnione dokumenty organizacyjne COI i metodyki projektowe (również niezatwierdzone) nie dają dowodów na jakiekolwiek wdrożenie praktyk ITIL. |
| Czy zarządzanie ryzykiem i ciągłością działania po stronie wytwórcy Systemu Rejestrów | Zarządzanie ryzykiem po stronie wytwórcy SRP **NIE JEST ADEKWATNE W ROZUMIENIU NORM ISO22301 I ISO31000**. Brak jest dokumentów SZCD. |



*Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1„Społeczeństwo informacyjne – budowa elektronicznej administracji"*

| | |
|---|---|
| Państwowych jest adekwatne w rozumieniu norm ISO 22301 i ISO 31000? | Plany ryzyka nie spełniają wymagań norm. |
| Ocena stanu organizacyjnego po stronie wykonawcy oprogramowania i systemu SRP w badanych obszarach (poziom dojrzałości – *maturity level*); | Ze względu na niezidentyfikowanie i nieudokumentowanie procesów biznesowych związanych z wytwarzaniem oprogramowania, zapewnieniem jakości, zapewnieniem ciągłości działania i zarządzaniem ryzykiem poziom dojrzałości w obszarze **wg COBIT należy określić jako „2"** (powtarzalny lecz intuicyjny)[29]. Istnieją minimalne metryki związane ze śledzeniem liczby zidentyfikowanych niezgodności w kodzie. Istnieje zatwierdzona procedura zarządzania zmianą, ale nie zidentyfikowano udokumentowania jej stosowania. |
| Rekomendacje. | Rekomendacje wypracowane na podstawie obserwacji dokumentów i wniosków przedstawiono tabelarycznie w rozdziale w grupach dla każdego z pytań postawionych przed ekspertyzą. Niewprowadzenie rekomendacji będzie prowadzić do akceptowania poniższych zagrożeń:<br>1) Niezapewnienie świadczenia wymaganego poziomu usług przez SRP;<br>2) Przerwanie w świadczeniu usług przez SRP i ciągłości działania całości lub bardzo wielu elementów krytycznych systemów bezpieczeństwa i ochrony zdrowia oraz zakłóceń funkcjonowania praktycznie wszystkich systemów państwa;<br>3) Wydłużenie procesu implementacji i wdrażania SRP<br>4) Powiększanie skutków dowolnej awarii SRP;<br>5) Długotrwała przerwa w świadczeniu wszelkich usług przez System Rejestrów Państwowych;<br>6) Niegospodarność wyrażająca się nieuzasadnionymi i nadmiernymi kosztami inwestycyjnymi i utrzymaniowymi infrastruktury SRP;<br>7) Nieskuteczność i nieefektywność wypracowanych rozwiązań organizacyjnych w COI. |

[29] Maturity level określono wg COBIT:
http://www.isaca.org/Knowledge-Center/cobit/Documents/COBIT-4.1-Polish-version.pdf
**2 Powtarzalne lecz intuicyjne** gdy
Stosowane są podobne podejścia do tworzenia procedur i dokumentacji, jednak nie są one oparte na zorganizowanym podejściu lub metodyce. Nie ma jednolitego podejścia do tworzenia procedur użytkowania i obsługi. Materiały szkoleniowe są opracowywane przez pojedyncze osoby lub zespoły projektowe, a ich jakość zależy od zaangażowanych osób. Jakość procedur i wsparcia dla użytkowników waha się od złej do bardzo dobrej przy niewielkiej spójności i integracji w ramach organizacji. Realizowane lub wspierane są programy szkoleniowe dla strony biznesowej i użytkowników, ale nie ma ogólnego planu ich realizacji.


*Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1„Społeczeństwo informacyjne – budowa elektronicznej administracji"*

# 6. ZAŁĄCZNIK 2. KRAJOWE RAMY INTEROPERACYJNOŚCI A NORMY.

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 określa, że:

§ 20. 1. Podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.
2. Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań:
1) zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;
2) utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację; Dziennik Ustaw – 7 – Poz. 526
3) przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;
4) podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;
5) bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4;
6) zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:
a) zagrożenia bezpieczeństwa informacji,
b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna, c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich;
7) zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:
a) monitorowanie dostępu do informacji,
b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;
8) ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;
9) zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;
10) zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;
11) ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;
12) zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:
a) dbałości o aktualizację oprogramowania,


Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1„Społeczeństwo informacyjne – budowa elektronicznej administracji"

b) minimalizowaniu ryzyka utraty informacji w wyniku awarii,
c) ochronie przed błędami, utratą, nieuprawnioną modyfikacją,
d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,
e) zapewnieniu bezpieczeństwa plików systemowych,
□f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,
g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,
h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;
13) bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących;
14) zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.
3. Wymagania określone w ust. 1 i 2 uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą, w tym:
1) PN-ISO/IEC 17799 – w odniesieniu do ustanawiania zabezpieczeń;
2) PN-ISO/IEC 27005 – w odniesieniu do zarządzania ryzykiem;
3) PN-ISO/IEC 24762 – w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.

**Norma ISO/IEC** 24762 - międzynarodowa norma dostarczająca wskazówek dotyczących ochrony informacji i usług technologii komunikacyjnej z zakresu disaster recovery (ang. ICT Disaster Recovery, ICT DR) jako część zarządzania ciągłością biznesu (ang. Business Continuity Management). Standard ten stosuje się zarówno do wewnętrznych, jak i zewnętrznych (ang. in-house & outsourced) dostawców usług IT.
ISO/IEC 24762:2008 określa:

- wymagania dotyczące implementacji, obsługi, monitorowania i utrzymywania usług oraz urządzeń ICT DR,
- zdolności, które powinni mieć zewnętrzni dostawcy usług ICT DR (ang. *outsourced ICT DR*), jak również praktyki, za którymi powinni podążać, aby zapewnić podstawowe środowiska operacyjne bezpieczeństwa i ułatwić organizacji wysiłki skupione na naprawie (ang. *recovery efforts*);
- wytyczne odnośnie wyboru miejsca naprawy (ang. *recovery site*);
- wytyczne dotyczące dostawców usług ICT DR w celu stałego ich doskonalenia.

ISO 24762 został utworzony w celu zdefiniowania tego, co niezależne organizacje powinny oferować w ramach usług disaster recovery. Standard służy jako schemat dla organizacji takich jak firmy hot site i cold site, firmy zarządzające usługami, dostawcy usług kolokacji i alternatywni dostawcy powierzchni roboczej. Obejmuje szeroki zakres kwestii, którymi powinni zająć się sprzedawcy, aby upewnić się, że ich propozycje usług są chronione. Włącza się w to przedsiębiorstwa budowlane, środki bezpieczeństwa, ochronę usług infrastrukturalnych takich jak energia, woda i telekomunikacja, jak również kontrole środowiskowe. Dla porównania, istnieje również inny standard ISO, mianowicie ISO/IEC 27031, który skupia się na disaster recovery IT użytkownika końcowego. Porównanie tych dwóch standardów wskazuje na to, że ISO 24762 skupia się bardziej szczegółowo na kwestiach technologicznych, którymi powinien zajmować się sprzedawca DR (ang. DR


Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1„Społeczeństwo informacyjne – budowa elektronicznej administracji"

vendor). ISO/IEC 27031 przypomina bardziej pięciopoziomowy schemat opisujący działania IT DR, które powinny być włączone jako część programu ciągłości biznesowej na poziomie przedsiębiorstwa.

Zapewnienie ciągłości działania organizacji polega na zapewnieniu skutecznej realizacji planów strategicznych organizacji. Poprzez analizę kluczowych procesów i zaangażowanych w nie zasobów, poznajemy punkty krytyczne, najbardziej narażone na zagrożenia zewnętrzne i wewnętrzne. Podstawą metodyczną wdrożenia zarządzania ciągłością działania (BCP, BCMS) są BS 25999, ISO 22301 oraz dobre praktyki z zakresu zarzadzania kryzysowego i budowy planów awaryjnych.

Analiza BIA (Business Impact Analysis) jest źródłem informacji na temat tego, co jest krytyczne dla funkcjonowania organizacji, jakie procesy, zasoby są niezbędne do realizacji produktu, czy usługi.

Analiza ryzyka realizowana dla punktów krytycznych daje odpowiedzi, w jaki sposób zabezpieczyć funkcjonowanie organizacji. Odpowiedzi: co i kto zagraża naszym procesom, zasobom, realizowanym działaniom, łańcuchowi dostaw, współpracownikom, umożliwiają wdrożenie działań prewencyjnych, podnoszących odporność na sytuacje krytyczne. Oczywiście zabezpieczenie się przed wszystkimi możliwymi zagrożeniami jest ze względów organizacyjnych i kosztowych niemożliwe.

Zarządzanie ciągłością działania zapewnia nam jednak narzędzia reagowania w sytuacji kryzysowej, w postaci: minimalnej akceptowalnej konfiguracji oraz planów ciągłości działania / planów odtworzeniowych. Minimalna akceptowalna konfiguracja to poziom dostępności zasobów niezbędny do realizowania procesu w minimalnym akceptowalnym poziomie. Plany ciągłości działania oraz Plany odtworzeniowe to zbiór działań podejmowanych w sytuacjach kryzysowych niezbędnych do zabezpieczenia zasobów organizacji i umożliwiających jak najsprawniejsze odtworzenie działalności po awarii.

Norma ISO 22301 :2012 określa wymagania dotyczące ustanawiania skutecznego Systemu Zarządzania Ciągłością Działania (SZCD), który powinien składać się z następujących elementów:

a) Polityki,
b) Osób o zdefiniowanym zakresie odpowiedzialności
c) Procesów zarządzania dotyczących:
    1. Polityki,
    2. Planowania
    3. Wdrażania i funkcjonowania
    4. Oceny efektywności
    5. Przeglądów zarządzania
    6. Doskonalenia.
d) Dokumentacji stanowiącej dowody, które można zbadać w drodze audytu
e) Jakichkolwiek procesów zarządzania działania istotnych dla organizacji.

Norma ISO24762 obejmuje wytyczne dla jednego szczegółowego procesu (odtwarzanie po katastrofie) całego holistycznego Systemu Zarządzania Ciągłością Działania definiowanego zgodnie z normą ISO 22301.


*Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1„Społeczeństwo informacyjne – budowa elektronicznej administracji"*

# 7. ZAŁĄCZNIK 2. HISTORIA PROJEKTU PL.ID

| Data | Zdarzenie | Najważniejsze skutki, Właściciele Programu, osoby odpowiedzialne za realizację. |
|---|---|---|
| **Wrzesień 2005** | podpisanie umowy pomiędzy Ministerstwem Spraw Wewnętrznych i Administracji a Ministerstwem Nauk i Szkolnictwa Wyższego na dofinansowanie projektu PESEL2, | Zakres i harmonogram projektu – koniec przewidziany na 31.12.2007<br>Minister SWiA – Ryszard Kalisz |
| Maj 2006 | Dokument Podstawowy dokument programowy PESEL2 | Opis sposobu budowy nowych i integracji istniejących systemów informatycznych, koncepcja budowy referencyjnego rejestru ewidencji ludności ZSI PESEL2, rejestry urzędów stanu cywilnego, portale informacyjne. Podział na 2 etapy – etap1 – projekt PESEL2, etap 2 – projekt pl.ID<br>Podsekretarz Stanu Piotr Piętak<br>Realizacja projektu MSWiA |
| Sierpień 2006 | Utworzenie Biura Projektu | Prace planistyczne, organizacyjne, pierwsze postępowania przetargowe<br>Realizacja projektu MSWiA |
| Grudzień 2006 | Podpisanie Aneksu do umowy o dofinansowanie | Zmniejszenie kwoty projektu do 167 mln zł |
| Październik 2007 | Podpisanie Aneksu do umowy o dofinansowanie | Zmniejszenie kwoty projektu do 126 mln zł |
| IV kw 2007 | Plan naprawczy projektu | Przebudowa założeń, ograniczenie zakresu<br>Podsekretarz Stanu Grzegorz Bliźniuk |
| Grudzień 2007 | Podpisanie Aneksu do umowy o dofinansowanie | Zmniejszenie kwoty projektu do 31 mln zł, ograniczenie liczby usług do dwóch |
| 30.09.2008 | Zakończenie projektu PESEL2 | Odbiór pierwszego etapu przedsięwzięcia, przeniesienie niezrealizowanych zadań do projektu pl.ID<br>Minister SWiA – Grzegorz Schetyna |
| Październik 2008 | Rozpoczęcie prac nad projektem pl.ID | Cel strategiczny – wprowadzenie elektronicznego dowodu tożsamości z funkcją uwierzytelnienia od 01.07.2011 |
| 03.06.2009 | Podpisanie umowy o dofinansowanie projektu pl.ID nr POIG.07.01.00-00-003/08-00 między Ministrem SW a Ministrem RR | Budżet – 370 mln zł, Zamknięcie projektu 31.12.2013<br>Minister MSWiA Grzegorz Schetyna, pełnomocnik MSWiA Andrzej Machnacz, Realizacja Projektu - CPI |
| 16.04.2010 | Aneks nr 1do umowy o dofinansowanie | Zmiana formalna (treść preambuły) wynikająca z zakwalifikowania projektu jako projektu indywidualnego POIG |



*Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1„Społeczeństwo informacyjne – budowa elektronicznej administracji"*

| | | |
|---|---|---|
| 23.11.2011 | Aneks nr 2 do umowy o dofinansowanie | Zmiana wskaźników produktu i rezultatu<br>Minister SW – Jerzy Miller<br>Dyrektor CPI – Zbigniew Olejniczak |
| 08.02.2012 | Porozumienie między MSW a MAiC w sprawie realizacji projektu | Deklaracja współpracy między MSW a MAiC, Zastępca Dyrektora CPI Rafał Magryś od 1 marca 2012 r.– osoba odpowiedzialna za realizację projektu pl.ID |
| 21.03.2012 | Decyzja KRMC o zmianie zakresu realizacji projektu (rezygnacja z wydawania wielofunkcyjnego elektronicznego powszechnego dokumentu tożsamości) | 1. przesunięcie terminu wdrożenia elektronicznego dowodu osobistego, do czasu:<br>a. przeprowadzenia testów, które będą mogły potwierdzić pełną integrację rejestrów państwowych,<br>b. opracowania jednolitej polityki w zakresie uwierzytelniania obywateli w systemach teleinformatycznych<br>administracji publicznej, na podstawie której będzie możliwe precyzyjne określenie niezbędnych funkcjonalności<br>elektronicznego dowodu osobistego, w tym także<br>rozstrzygnięcie celowości wprowadzania kolejnej metody uwierzytelniania – podpisu osobistego,<br>c. nowelizacji ustawy o dowodach osobistych, która będzie uwzględniała wymagania wynikające z opracowanej polityki w zakresie uwierzytelniania, a także będzie zgodna ze znowelizowaną dyrektywą 1999/93/WE ws. wspólnotowych ram prawnych dla podpisów elektronicznych |
| 17.09.2012 | Aneks nr 3 do umowy o dofinansowanie | Zmiana zakresu projektu, rezygnacja z wydawania elektronicznego dowodu osobistego |
| 11.10.2012 | Pismo Ministra SW do Ministra RR – wniosek o przeniesienie realizacji projektu z CPI do COI | Rozpoczęcie formalnego procesu przeniesienia realizacji projektu z CPI do COI |
| 12.10.2012 | Rekomendacja KS projektu o przeniesienie realizacji z CPI do COI | Rozpoczęcie formalnego procesu przeniesienia realizacji projektu z CPI do COI |
| 19.10.2012 | Pismo Ministra SW do Dyrektora COI zlecający przygotowanie do przejęcia projektu | Rozpoczęcie formalnego procesu przygotowania COI do realizacji projektu<br>Podsekretarz Stanu Roman Dmowski |
| 23.01.2013 | Umowa między Ministrem SW a Dyrektorem COI w sprawie przygotowań do przejęcia projektu | Przygotowanie do realizacji projektu przez COI |


*Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1„Społeczeństwo informacyjne – budowa elektronicznej administracji"*

| | | |
|---|---|---|
| 25.02.2013 | Umowa między Ministrem SW a Dyrektorem COI o realizacji projektu pl.ID | Powierzenie COI przez Ministra SW realizacji projektu pl.ID<br>Podsekretarz Stanu Rafał Magryś |
| 12.04.2013 | Porozumienie między MAiC, MSW i CPI | Rozwiązanie KS projektu, odwołanie kierownika projektu, rozwiązanie porozumienia z 08.02.2012 r., określenie procesu przejmowania projektu i zakresu prac realizowanych dotąd przez CPI |
| 26.06.2013 | Aneks nr 4 do umowy o dofinansowanie | Zmiana budżetu projektu – 294 mln zł, zmiana terminu realizacji – 31.03.2015 |
| 13.02.2014 | Aneks nr 1do umowy między Ministrem SW a Dyrektorem COI | Aktualizacja harmonogramu – wydłużenie terminów realizacji poszczególnych zadań<br>Podsekretarz Stanu – Rafał Magryś |
| 24.02.2014 | Aneks nr 5 do umowy o dofinansowanie | Zmiana nazewnictwa CMOKU na ŹRÓDŁO<br>Podsekretarz Stanu – Rafał Magryś |
| 27.06.2014 | Aneks nr 2 do umowy między Ministrem SW a Dyrektorem COI | Aktualizacja harmonogramu – wydłużenie terminu realizacji poszczególnych zadań<br>Podsekretarz Stanu – Tomasz Szubiela |
| 16.12.2014 | Nowelizacja ustawy o dowodach osobistych, ewidencji ludności i przepisów Prawa o aktach stanu cywilnego | Przesunięcie z 1 stycznia na 1 marca 2015 terminu wdrożenia nowego systemu SRP<br>Podsekretarz Stanu – Tomasz Szubiela |

Koniec dokumentu


*Przedmiot zamówienia współfinansowany przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka 2007-2013 – Działanie 7.1„Społeczeństwo informacyjne – budowa elektronicznej administracji"*