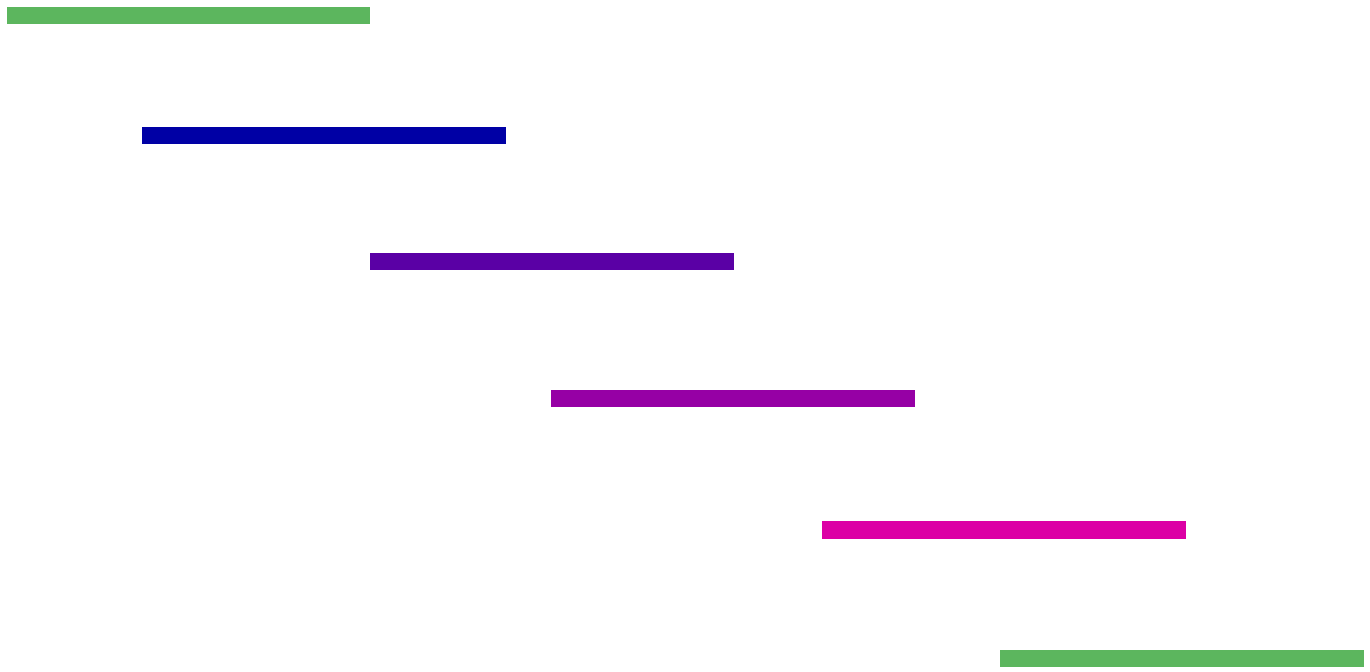
# Raport z przeglądu systemu ePUAP

centralny ośrodek informatyki

Warszawa, dn. 24.03.2016 r.

# Plan prezentacji

| | |
|---|---|
| **Wprowadzenie** | slajdy 2 - 4 |
| **Funkcjonalności** | slajdy 5 - 8 |
| **Infrastruktura** | slajdy 9 - 11 |
| **Bezpieczeństwo** | slajdy 12 - 14 |
| **Organizacja** | slajdy 15 - 17 |
| **Plan działania** | slajdy 18 - 24 |



# Podstawa i przyjęte założenia

**Podstawa formalna przeglądu:**

1. Pismo MC z dnia 29.02.2016 r. znak SAS.512.2.2016
2. Pismo COI z dnia 10 marca 2016 r. znak COI.0500.5.2016
3. Statut prac COI z dnia 31 grudnia 2015 r.

**Założenia przeglądu:**

1. Status przygotowania COI do utrzymania systemu ePUAP
2. Rekomendacje działań wynikające z przeglądu
3. Przygotowany przez COI Raport z audytu ePUAP

**Ograniczenia:**

1. Krótki czas przeglądu
2. Brak możliwości sprawdzenia wszystkich funkcjonalności (system produkcyjny)
3. Przestoje / niedostępności systemu (awaryjne / administracyjne)
4. Zaangażowanie zespołu w bieżące zadania (np. CEPIK)

**Termin:**

Data przejęcia systemu przez COI: 4 kwietnia 2016 r.

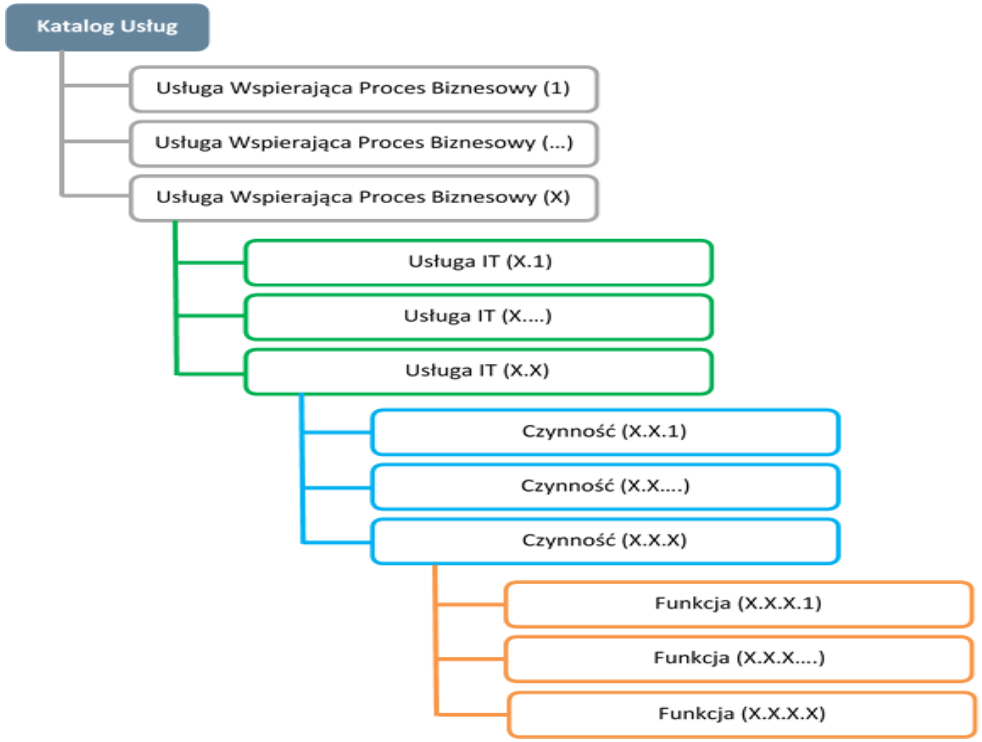
# Status poszczególnych obszarów przeglądu

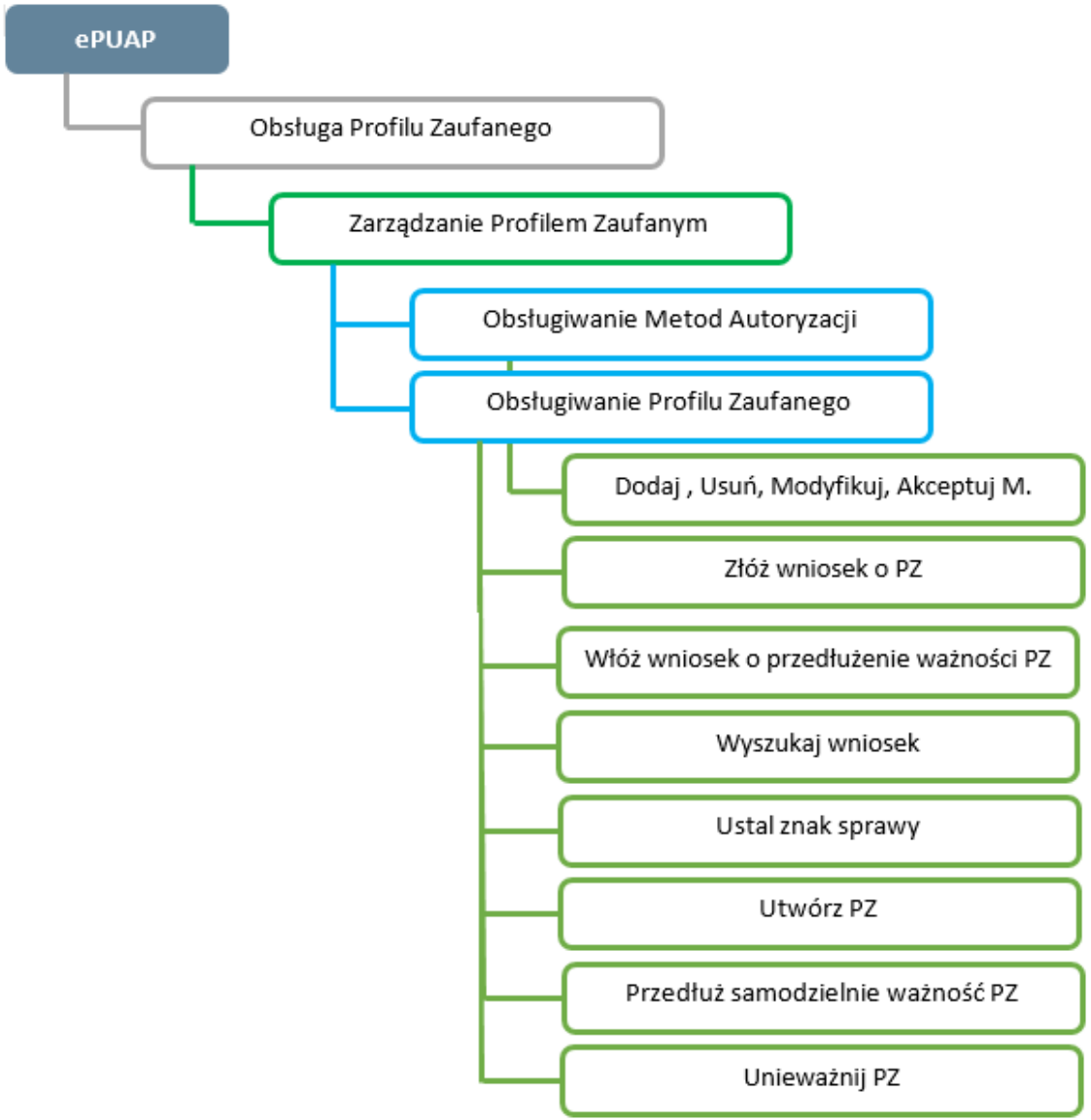
| Obszar | Status | Komentarz |
|---|---|---|
| **Funkcjonalność**  | Zidentyfikowane i przetestowane funkcjonalności (83%) | Brak kompletnego „katalogu usług”, brak wszystkich opisów funkcjonalnych (niektóre funkcjonalności „odkrywane” w ramach testów), brak potwierdzenia poziomu świadczonych usług SLA (niejasne kryteria przydziału kategorii „utrudnienia” i „niedostępność” – niedostępność PZ jest kategoryzowana, jako „utrudnienie”) i monitoringu wydajności funkcjonalności i użyteczności. Brak spójności pomiędzy środowiskami produkcyjnymi i testowymi. Braki dokumentacyjne/ eksploatacyjne. |
| **Infrastruktura**  | Przejmowana infrastruktura pozwala na funkcjonowanie systemów po wykonaniu niezbędnych konfiguracji, a docelowo migracji na ZIR | Złożona architektura systemu, urozmaicona nieaktualnymi systemami i serwerami oraz brakiem krytycznych procedur administracyjnych. Niezbędne jest wykonanie konfiguracji, a w szczególności strojenia baz danych oraz serwerów aplikacyjnych. |
| **Bezpieczeństwo**  | Obecne rozwiązania wymagają znaczących i natychmiastowych korekt | W krótkim okresie należy rozwiązać podstawowe problemy związane z bezpieczeństwem (konfiguracja, zarządzanie kontami administracyjnymi, aktualizacja oprogramowania – ssh, http). W średniej i długiej perspektywie, doprowadzenie systemu do oczekiwanego poziomu bezpieczeństwa będzie wymagało znaczących zmian w konfiguracjach, systemach, jak i samej architekturze (temat powiązany z obszarem Infrastruktura). |
| **Organizacja**  | Zagrożenie braku ciągłości osobowej do czasu zbudowania kompetencji w COI | W krótkim czasie konieczność zrekrutowania osób do COI celem zapewnienia osobowej ciągłości działania, przejście z aplikacji OTRS na kompleksową aplikację ITSM. Budowa kompetencji po stronie MC (właścicielstwo biznesowe) oraz COI (utrzymanie, rozwój ) Pilne uruchomienie linii wsparcia (Service Desk, Utrzymanie, Zespoły administratorów infrastruktury, aplikacji, analityków biznesowych, testów funkcjonalnych. Niezbędne wypracowanie procedur obsługi użytkowników (indywidualnych, instytucjonalnych).Obszar kluczowy dla całości utrzymania i przyszłego rozwoju systemu. |

# Obszar Funkcjonalności

**Aplikacje poddane testom funkcjonalności w ramach przeglądu:**

- ePUAP - elektroniczna Platforma Usług Administracji Publicznej
- SG BIP - SG Biuletyn Informacji Publicznej
- PAP - Publikator Elektronicznych Aktów Prawnych



# Obszar Funkcjonalności

**Sposób przeprowadzenia testów i wyniki:**

- Identyfikacja usług, funkcjonalności
- Testowanie poszczególnych funkcjonalności z poziomu czynności i funkcji z perspektywy usług
- Przetestowanie przez COI funkcji z perspektywy użyteczności

| | Ilość zidentyfikowanych funkcjonalności | Ilość wykonanych testów | Testy – Perspektywa katalogu usług | | Testy – Perspektywa użyteczności | | Łączna ilość uwag do wykonanych testów |
|---|---|---|---|---|---|---|---|
| | | | Pozytywne | Negatywne | Pozytywne | Negatywne | |
| **BIP** | 152 | 147 | 145 | 2 | 132 | 15 | 63 |
| **PAP** | 39 | 31 | 24 | 7 | 21 | 10 | 10 |
| **ePUAP** | 204 | 150 | 144 | 6 | 131 | 19 | 40 |
| **Σ** | 395 | 328 | 313 | 15 | 284 | 44 | 113 |

# Obszar Funkcjonalności

| Spostrzeżenia | Rekomendacje |
|---|---|
| Zdefiniowany katalog usług stanowiący załącznik do umowy utrzymaniowej MC – COI jest niekompletny | • Należy dokonać pełnego, kompleksowego rozpoznania funkcjonalności w ramach przejmowanych systemów |
| Wykonanie części testów było niemożliwe z powodu braku środowisk testowych, dostępów do nich lub znaczących różnic w stosunku do środowisk produkcyjnych | • Należy wdrożyć brakujące środowiska testowe oraz zaktualizować istniejące do postaci referencyjnych, a następnie stworzyć wyczerpujące scenariusze testowe, pozwalające jednoznacznie określić faktycznie występujące błędy |
| Dotychczasowe warunki SLA były subiektywne, niejasno określone | • Należy uzgodnić warunki SLA pomiędzy MC a COI w oparciu o bibliotekę ITIL i normę ISO 20000-1<br>• W negocjowanej aktualnie umowie pomiędzy MC a COI zaproponowano poziomy SLA |
| Do podjęcia decyzja w zakresie odpowiedzialności i obsługi przez COI w kwestii nieprzetestowanych lub zwracających błędy funkcji | • Należy uzgodnić w umowie sposób i tryb realizacji tego typu zgłoszeń |

# Obszar Funkcjonalności

## Zidentyfikowane inicjatywy

**Inicjatywy krótkoterminowe**

- F1 – Przygotowanie opisu procesu zarządzania poziomem usług
- F2 – Opracowanie szablonu raportu poziomów świadczenia usług
- F3 – Analiza funkcjonalności ePUAP vs. obywatel.gov.pl

---

**Inicjatywy średnio- i długoterminowe**

- F4 – Ustalenie po stronie MC kompletnego katalogu usług i funkcjonalności
- F5 – Uzgodnienie z MC warunków SLA i zbudowanie kompletnego sytemu raportowego
- F6 – Opracowanie 100% brakujących opisów funkcji wykazanych w katalogu usług
- F7 – Kolekcjonowanie danych dot. dostępności i wydajności celem określenia mierników
- F8 – Określenie docelowych wartości mierników wydajności
- F9 – Uruchomienie mechanizmów monitorowania wydajności
- F10 – Stworzenie referencyjnych środowisk testowych
- F11 – Uruchomienie procesu zarządzania poziomem usług w zakresie parametrów wydajnościowych

# Obszar Infrastruktura

**Przeglądowi poddano infrastrukturę systemową środowisk testowych, deweloperskich i produkcyjnych systemów:**

- ePUAP
- PAP
- SS DIP
- SG BIP

---

**Badaniu poddano krytyczne elementy systemu:**

- Infrastruktura sieciowa
- Serwery bazodanowe
- Baza danych DB2
- Serwery aplikacyjne
- Serwery LDAP
- WebServices

# Obszar Infrastruktura

| Spostrzeżenia | Rekomendacje |
|---|---|
| Przekazane i badane procedury administracyjne nie były testowane przy odbiorach i w większości przypadków są bezużyteczne w codziennych czynnościach utrzymaniowych | • Należy stworzyć procedury od nowa, bazując na rzeczywistej pracy administratorów i aktualizować je przy kolejnych zmianach (inicjatywach) |
| Zastosowana, skomplikowana architektura wpływa negatywnie na stabilność działania systemów oraz czas usuwania awarii | • Należy zaktualizować oprogramowanie na serwerach do wersji zapewniających stabilność działania oraz wsparcie techniczne<br>• Należy rozpatrzyć, i tam, gdzie to możliwe, wykorzystać mechanizmy wirtualizacji |
| Błędy w konfiguracji serwerów, aplikacji, a także w samej architekturze negatywnie wpływają na bezpieczeństwo i wydajność systemów | • Należy wdrożyć poprawki w konfiguracjach |
| Nieprawidłowa konfiguracja serwerów bazodanowych oraz brak wymaganych struktur (indeksy) powodowały niską wydajność warstwy bazodanowej, częste awarie i negatywny odbiór użytkowników | • Należy przeprowadzić strojenie serwerów bazodanowych (część prac wykonano podczas przeglądu) |
| W związku z realizacją 16 programów regionalnych w 4 obszarach (e-Zdrowie, e-Administracja, e-Kultura i e-Edukacja) spodziewany jest znaczy wzrost e-Usług publicznych korzystających z Profilu Zaufanego | • Należy monitorować obciążenie PZ<br>• Zaplanowanie potencjalnej rozbudowy infrastruktury |

# Obszar Infrastruktura

## Zidentyfikowane inicjatywy

| | |
|---|---|
| **Inicjatywy krótkoterminowe** | • I1 – Skatalogowanie procedur administracyjnych i ich opracowanie<br>• I2 – Aktualizacja serwerów i aplikacji (w tym ich konfiguracji)<br>• I3 – Poprawienie kodu aplikacji (niezbędne zmiany)<br>• I4 – Przygotowanie koncepcji nowego Profilu Zaufanego |
| **Inicjatywy średnio- i długoterminowe** | • I5 – Uruchomienie nowego Profilu Zaufanego*<br>• I6 – Wirtualizacja serwerów<br>• I7 – Migracja infrastruktury ePUAP na środowisko Zintegrowanej Infrastruktury Rejestrów<br>• I8 – Optymalizacja kosztów utrzymania (licencje, infrastruktura itp.)<br>• I9 – Wdrożenie systemu zarządzania tożsamością |

* Uruchomienie nowego Profilu Zaufanego jest przewidziane w Programie B, jako odrębny projekt

# Obszar Bezpieczeństwo

**Przegląd bezpieczeństwa systemów został poddany testom w wymienionych obszarach :**

| | Obszar | Komentarz |
|---|---|---|
|  | **Rekonesans środowiska produkcyjnego** | Zidentyfikowano domeny mające przekierowanie na domenę ePUAP, domeny epuap.gov.pl – serwery DNS znajdują się w tej samej podsieci, a dodatkowo nie są niezależnymi systemami rozlokowanymi w różnych lokalizacjach. |
|  | **Testy konfiguracji i zarządzania konfiguracją** | Wymagania dot. tworzonych kont i haseł, konfiguracje urządzeń i aplikacji wymagają natychmiastowej interwencji. Zidentyfikowano błędy w WebServices. |
|  | **Testy zarządzania tożsamością** | Nie zidentyfikowano problemów. |
|  | **Testy procesu zarządzania sesją** | Zidentyfikowano jeden niekrytyczny przypadek, który należy poddać dalszym testom. |
|  | **Testy walidacji pól wejściowych** | Zidentyfikowano jedną podatność związaną z modyfikacją przesyłanych plików xml. Podatność należy poddać dalszym testom, ponieważ istnieje ryzyko, że jest ona poważna. |
|  | **Testy słabej kryptografii** | Nie zidentyfikowano problemów. |
|  | **Testy interfejsu klienta** | Należy przeprowadzić analizę i rekonfigurację routerów brzegowych i zweryfikować możliwość podatności przez strony trzecie poprzez podszywanie pod domeny, usługi/ profil klienta. |

# Obszar Bezpieczeństwo

| Spostrzeżenia | Rekomendacje |
|---|---|
| Aplikacje i urządzenia nie są zaktualizowane do najnowszych wersji, są niejednorodnie skonfigurowane | • Routery brzegowe i systemy bezpieczeństwa wymagają aktualizacji i rekonfiguracji<br>• Konfiguracja serwerów i aplikacji |
| Nie stwierdzono obecności Polityki Bezpieczeństwa Systemów | • Opracowanie i wdrożenie PBS<br>• Konfiguracja serwerów i aplikacji zgodnie z PBS<br>• Regularne przeglądy systemów pod kątem bezpieczeństwa |
| Wymagana optymalizacja środowiska ePUAP | • Weryfikacja realnego obciążenia wynikającego z uruchomionych usług i zabezpieczeń<br>• Optymalizacja środowiska pod kątem eliminacji luk bezpieczeństwa i zagrożeń<br>• Uruchomienie monitoringu incydentów bezpieczeństwa |

# Obszar Bezpieczeństwo

## Zidentyfikowane inicjatywy

| | |
|---|---|
| **Inicjatywy krótkoterminowe** | • B1 – Weryfikacja i poprawa konfiguracji urządzeń w niezbędnym, możliwym w krótkiej perspektywie<br>• B2 – Aktualizacja systemów operacyjnych, oprogramowania układowego, usług zainstalowanych na poszczególnych serwerach<br>• B3 – Opracowanie i wdrożenie podstawowych standardów bezpieczeństwa<br>• B4 – Uruchomienie monitoringu 24h bezpieczeństwa środowiska produkcyjnego |
| **Inicjatywy średnio- i długoterminowe** | • B5 – Eliminacja luk bezpieczeństwa (konfiguracja i wymiana urządzeń)<br>• B6 – Ponowne przeprowadzenie pełnych testów bezpieczeństwa<br>• B7 – Opracowanie Polityki Bezpieczeństwa Systemów<br>• B8 – Rozważenie i podjęcie decyzji dot. wdrożenia systemu klasy SIEM (ang. Security Information and Event Management)<br>• B9 – Opracowanie planów Business Continuity Plan i Disaster Recovery Plan |

# Obszar Organizacja

**Ze względu na kluczową rolę tego obszaru dla realizacji pozostałych, duża część złożonych zagadnień musi być opracowana po stronie COI w krótkim okresie:**

- Powołanie Linii wsparcia (Service Desk, administratorzy, analitycy, testerzy)
- Zastąpienie obecnego systemu OTRS na Service Desk COI
- Opracowanie kompletnych procedur obsługi incydentów, problemów, zarządzania zmianą, pojemności i katalogiem usług wg praktyk ITIL

---

**Prace po stronie COI wymagają niezwłocznego wskazania  właściciela biznesowego projektu po stronie MC, decydującego m.in. o:**

- Wypracowaniu modelu współpracy
- Weryfikacji i potwierdzeniu utrzymywanych funkcjonalności systemu
- Uzgadnianiu i weryfikacji zapisów SLA
- Uruchomieniu nowego Profilu Zaufanego

# Obszar Organizacja

| Spostrzeżenia | Rekomendacje |
|---|---|
| W dostarczonej dokumentacji nie zawarto opisu wskaźników SLA dla incydentów zewnętrznych | • Należy opracować wskaźniki SLA, które pozwolą na jednoznaczną interpretację zapisów umowy |
| Brak dokumentacji związanej ze zgłaszaniem incydentów zewnętrznych | • Należy opracować kompleksową dokumentację (z uwzględnieniem procesów obsługi incydentów klienta instytucjonalnego i indywidualnego) |
| Brak katalogów usług dla poszczególnych projektów | • Należy opracować katalogi poszczególnych usług biznesowych |
| Brak procedur transferu zleceń na wyższe poziomy linii wsparcia | • Należy opracować procedury przekazywania zleceń na wyższe poziomy linii wsparcia, oraz realizacji tych zleceń na wszystkich poziomach |
| Budowa kompetentnego zespołu wsparcia | • Przejęcie części pracowników z CCA<br>• Rekrutacja niezbędnych zasobów na brakujące wakaty |

# Obszar Organizacja

## Zidentyfikowane inicjatywy

| | |
|---|---|
| **Inicjatywy krótkoterminowe** | • O1 – Powołanie Linii wsparcia – z uwzględnieniem opracowania procedur<br>• O2 – Wdrożenie ITSM Atmosfera zamiast OTRS<br>• O3 – Wskazanie właściciela biznesowego po stronie MC<br>• O4 – Budowa zespołu wsparcia (cz. 1 – Service Desk, administratorzy infrastruktury, administratorzy aplikacji i analitycy biznesowi) |
| **Inicjatywy średnio- i długoterminowe** | • O5 – Wypracowanie zasad współpracy i struktur organizacyjnych dla docelowego modelu ePUAP po stronie MC i COI<br>• O6 – Weryfikacja wypracowanych standardów i narzędzi<br>• O7 – Szkolenia merytoryczne i miękkie dla zespołu wsparcia<br>• O8 – Budowa bazy wiedzy<br>• O9 – Budowa zespołu wsparcia (docelowego) |

# Plan działania – co i jak chcemy realizować


Wszystkie inicjatywy zidentyfikowane w poszczególnych obszarach zostały przypisane do krótko- lub długoterminowych działań.

Na podstawie zidentyfikowanych inicjatyw powołane zostaną projekty:

**Projekt A** - dla krótkoterminowych działań mających na celu przygotowanie do przejęcia w COI, a następnie eksploatacji w początkowym okresie systemu ePUAP w COI.

**Projekt / Program B** - dla długoterminowych działań mających na celu:

- wypracowanie docelowego rozwiązania,
- architektury systemowej,
- odpowiednich funkcjonalności,
- analizę User Experience.

Obydwa projekty, w szczególności Projekt/ Program B powinny być realizowane i nadzorowane przez MC, jako właściciela biznesowego.

# Przypisanie inicjatyw do projektów

| | Organizacja | Funkcjonalności | Infrastruktura | Bezpieczeństwo |
|---|---|---|---|---|
| Projekt A (do 3M) | O1, O2, O3, O4 | F1, F2, F3 | I1, I2, I3, I4 | B1, B2, B3, B4 |
| Projekt B (powyżej 3M) | O5, O6, O7, O8, O9 | F4, F5, F6, F7, F8, F9, F10, F11 | I5, I6, I7, I8, I9 | B5, B6, B7, B8, B9 |

# Projekt A

**Zapewnienie bieżącej eksploatacji i utrzymania przejmowanych systemów poprzez :**

### Organizacja

- Powołanie Linii wsparcia (Service Desk, Zespoły Utrzymania, Administratorzy)
- Zapewnienie ciągłości biznesowej po stronie MC (wskazanie właściciela biznesowego)

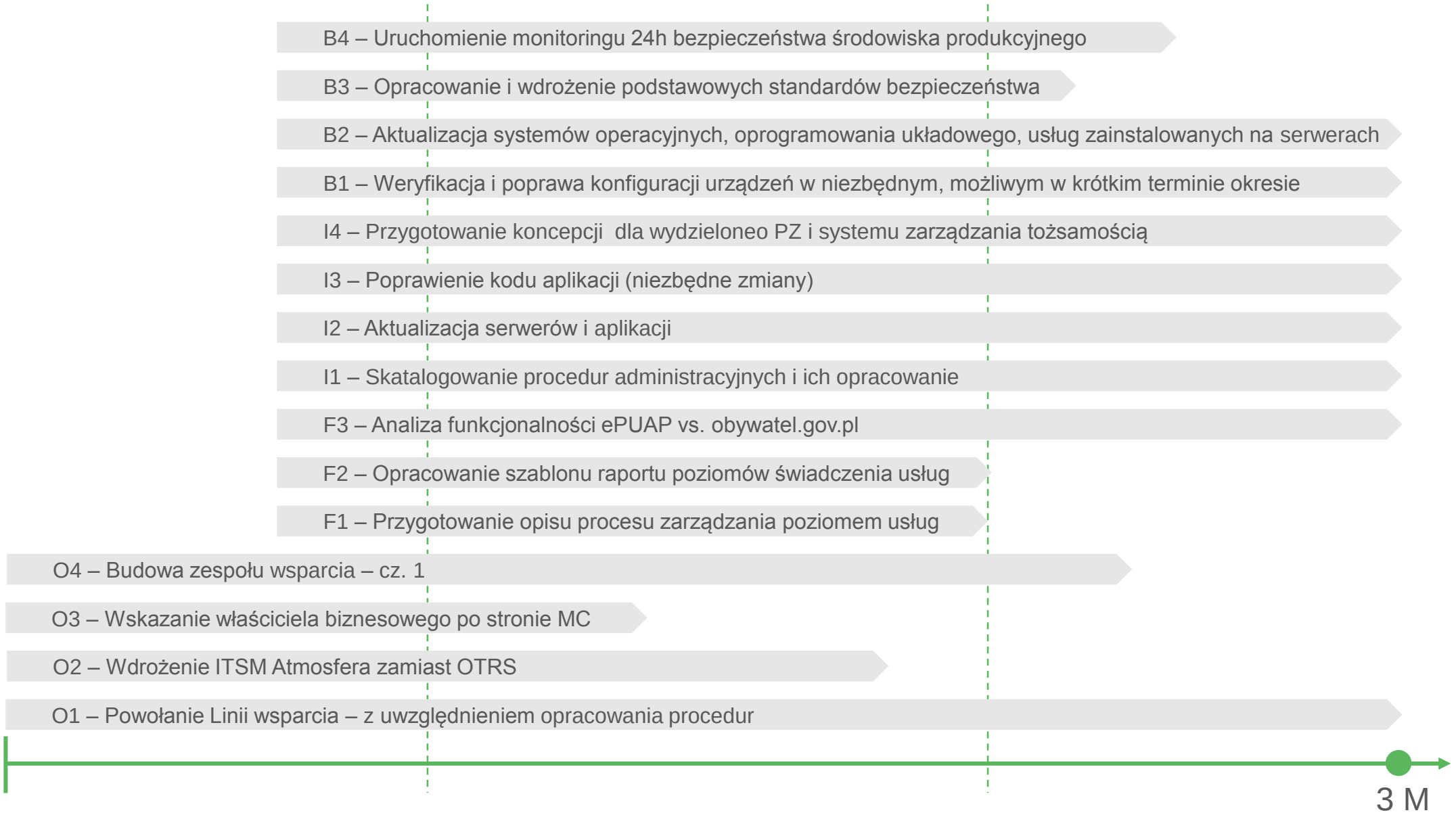
### Technologia (Infrastruktura i Bezpieczeństwo)

- Zapewnienie ciągłości funkcjonowania i podniesienie poziomu bezpieczeństwa infrastruktury i systemów ePUAP

### Funkcjonalności

- Przygotowanie procesu zarządzania poziomem usług i raportu poziomu świadczenia usług (SLM)

# Projekt A – planowana roadmapa



# Projekt B

**Wypracowanie i realizacja docelowego modelu dla ePUAP poprzez :**

## Organizacja

- Wypracowanie współpracy biznesowej pomiędzy MC (właściciel biznesowy), a COI
- Wypracowanie struktur organizacyjnych / projektowych dla docelowego modelu ePUAP

## Technologia (Infrastruktura i Bezpieczeństwo)

- Wypracowanie docelowej architektury systemu i modelu bezpieczeństwa z uwzględnieniem ePUAP

## Funkcjonalności

- Stworzenie kompletnego katalogu usług i docelowej wizji dla systemu ePUAP (z uwzględnieniem roli i funkcji PZ)

# Projekt/ Program B – wstępna roadmapa

B9 – Opracowanie planów Business Continuity Plan i Disaster Recovery Plan
B8 – Rozważenie i podjęcie decyzji dot. wdrożenia systemu klasy SIEM (ang. Security Information and Event Management)
B7 – Opracowanie Polityki Bezpieczeństwa Systemów
B6 – Ponowne przeprowadzenie pełnych testów bezpieczeństwa
B5 – Eliminacja luk bezpieczeństwa (konfiguracja i wymiana urządzeń)
I9 – Wdrożenie docelowego PZ i systemu zarządzania tożsamością
I8 – Optymalizacja kosztów utrzymania (licencje, infrastruktura itp.)
I7 – Migracja infrastruktury ePUAP na środowisko Zintegrowanej Infrastruktury Rejestrów
I6 – Wirtualizacja serwerów
**I5 – Uruchomienie nowego Profilu Zaufanego – jako osobny projekt w Programie B**
F11 – Uruchomienie procesu zarządzania poziomem usług w zakresie parametrów wydajnościowych
F10 – Stworzenie referencyjnych środowisk testowych
F9 – Uruchomienie mechanizmów monitorowania wydajności
F8 – Określenie docelowych wartości mierników wydajności
F7 – Kolekcjonowanie danych dot. dostępności i wydajności celem określenia mierników
F6 – Opracowanie 100% brakujących opisów funkcji wykazanych w katalogu usług
F5 – Uzgodnienie z MC warunków SLA
F4 – Ustalenie po stronie MC kompletnego katalogu usług i funkcjonalności
O9 – Budowa zespołu wsparcia (docelowego)
O8 – Budowa bazy wiedzy
O7 – Szkolenia merytoryczne i miękkie dla zespołu wsparcia
O6 – Weryfikacja wypracowanych standardów i narzędzi
O5 – Wypracowanie zasad współpracy i struktur organizacyjnych

3 M
6 M

# Kluczowe czynniki sukcesu

| | |
|---|---|
| Zapewnienie zasobów osobowych dla utrzymania i rozwoju systemu | |
| Doprecyzowanie zasad współpracy pomiędzy MC i COI | • Wskazanie właściciela biznesowego po stronie MC<br>• Wypracowanie modelu współpracy i rozliczeń pomiędzy MC i COI<br>• Wypracowanie skutecznych struktur zarządzania projektami A i B |
| Uzgodnienie docelowej wizji i funkcjonalności dla ePUAP | • Zakres realizacji projektów zależny od decyzji biznesowych MC<br>• Decyzje związane z architekturą Profilu Zaufanego – zmiany wpłyną na integrację e-Usług z PZ |
| Wyeliminowanie zależności od zewnętrznych podmiotów | |

# Dziękujemy za uwagę

centralny
ośrodek
informatyki