



Polska Agencja Żeglugi Powietrznej

**ZAPYTANIE O INFORMACJĘ CENOWĄ
(RFI)**

Zakup i wdrożenie platformy do zarządzania procesami IT

dla

Polskiej Agencji Żeglugi Powietrznej

Warszawa, 22 marca 2017r.

I. Informacje ogólne

1. Zamawiający: Polska Agencja Żeglugi Powietrznej („PAŻP”/„Agencja”)
ul. Wieżowa 8, 02-147 Warszawa
tel. +48 22 574 53 51
2. Prowadzący sprawę: Jacek Pęczek, jacek.peczek@pansa.pl
3. Godziny kontaktu: 8.00 - 15.00 w dni robocze
4. Przedmiot zapytania:
 - 4.1 Dostawa licencji dla Narzędzia klasy ITSM oraz Oprogramowanie Pozostałego na sprzęcie zamawiającego;
 - 4.2 Uruchomienie w Narzędziu ITSM wybranych procesów zgodnych z ITIL:
 - Zarządzanie Incydentami wraz z funkcją Service Desk,
 - Realizację wniosków,
 - Zarządzanie problemami,
 - Zarządzanie zmianami,
 - Zarządzanie komponentami Usług i Konfiguracją, wraz z bazą CMDB,
 - Zarządzanie Poziomem Usług,
 - Zarządzanie Bazą Wiedzy,
 - Mierzenie i raportowanie usług.
 - 4.3 Asysta techniczna na okres 36 miesięcy od dnia przekazania do eksploatacji narzędzia.
5. Cel zapytania:

W związku z planowaną realizacją wdrożenia w organizacji nowego narzędzia wspierającego zarządzanie wybranymi procesami zgodnie z ITIL, audytu legalności posiadanego oprogramowania i asysty technicznej dla zakupionego rozwiązania.

W celu rzetelnego oszacowania wartości planowanego przedmiotu zamówienia, PAŻP zwraca się z uprzejmą prośbą o przedstawienie szacunkowej wyceny wykonania przedmiotu zapytania.

Niniejsze zapytanie nie stanowi oferty w rozumieniu art. 66 ustawy Kodeks cywilny, jak również nie jest ogłoszeniem w rozumieniu ustawy kodeks Cywilny lub Prawo zamówień publicznych.

6. Własność dokumentu: Niniejszy dokument stanowi własność PAŻP.
Kopiowanie i rozpowszechnianie tego dokumentu, w całości lub częściowo, w jakiegokolwiek formie, jest zabronione bez uprzedniej, pisemnej zgody PAŻP.
7. Termin odpowiedzi: **Do dnia 03.04.2017r.**
8. Język odpowiedzi: Język polski
9. Wycena: Wszystkie ceny należy podawać jako wartości netto w polskich złotych. Odpowiedź na niniejsze RFI należy złożyć na Formularzu, którego wzór został dołączony do niniejszego zapytania jako Załącznik nr 4.
10. Koszty: Odpowiedź na RFI jest przygotowywana na wyłączny koszt odpowiadającego.
11. Zastrzeżenia: Informacje zawarte w niniejszym RFI mogą być wykorzystane jedynie zgodnie z ich przeznaczeniem, tj. w celu przygotowania odpowiedzi na zapytanie o informację.

II. Przedmiot zapytania

Oczekuje się, że odpowiadający wykorzystując swoją wiedzę i doświadczenie, najlepszą praktykę oraz sprawdzone narzędzia i metodologię, dokona wyceny zakupu i wdrożenia platformy do zarządzania procesami IT w PAŻP.

Przyszłe zamówienie obejmie:

1. Dostawę licencji dla Narzędzia klasy ITSM oraz Oprogramowania Pozostałego niezbędnego do realizacji projektu instalowanego na sprzęcie zamawiającego;
2. Uruchomienie w Narzędziu ITSM wybranych procesów zgodnych z ITIL:
 - a. Zarządzanie Incydentami wraz z funkcją Service Desk,
 - b. Realizację wniosków,
 - c. Zarządzanie problemami,
 - d. Zarządzanie zmianami,
 - e. Zarządzanie komponentami Usług i Konfiguracją, wraz z bazą CMDB,
 - f. Zarządzanie Poziomem Usług,
 - g. Zarządzanie Bazą Wiedzy,
 - h. Mierzenie i raportowanie usług.

Oferowany System ITSM musi spełniać wymagania określone w załączniku nr 1 do zapytania.

3. Przedmiot zamówienia realizowany będzie w pięciu etapach:
 - a. Etap I – Przygotowanie projektu wdrożenia Systemu ITSM,
 - b. Etap II - Przygotowanie procesów i usług,
 - c. Etap III - Dostosowanie systemu do potrzeb Zamawiającego,
 - d. Etap IV - Dostawa licencji,
 - e. Etap V - Wdrożenie systemu.
4. W ramach realizacji przedmiotu Umowy Wykonawca zobowiązuje się do:
 - a. wykonania projektu wdrożenia systemu klasy ITSM w PAŻP
 - b. weryfikacji obecnie wdrożonych procesów i usług i zaproponowania zmian pozwalających na optymalne dostosowanie procesów i usług do implementacji w oferowanym narzędziu.
 - c. konfiguracji Platformy Sprzętowej zapewnionej do projektu przez zamawiającego w lokalizacji Polskiej Agencji Żeglugi Powietrznej w Warszawie przy ul. Wieżowej 8.
 - d. dostarczenia, instalacji oraz konfiguracji Narzędzia ITSM wraz z wymaganymi licencjami oraz niezbędną dokumentacją,
 - e. wdrożenia procesów (opis procesów dostarczony przez Zamawiającego, lub zaproponowany przez Wykonawcę) oraz funkcji zarządzania usługami IT zgodnie z opracowanym przez Wykonawcę i zaakceptowanym przez Zamawiającego Projektem Technicznym.
 - f. zapewnienia niezawodnego działania Systemu ITSM zgodnie z Projektem Technicznym.
 - g. przeprowadzenia prac zgodnie z przedstawionym przez Zamawiającego Zakresem Projektu Wdrożeniowego.

- h. przeprowadzania przeglądów i asyst Systemu ITSM,
- i. wdrożenia Systemu ITSM w sposób gwarantujący współpracę z obecnymi systemami informatycznymi Zamawiającego wyszczególnionymi w Załączniku nr 1 do zapytania punkt 2.5.
- j. przeniesienia praw do korzystania z wykonanych w ramach Umowy Utworów (m.in. Dokumentacji i Kastomizacji),
- k. udzielenia Gwarancji i rękojmi na System ITSM na warunkach określonych w załączniku nr 2 do RFI),
- l. dostarczenia Wsparcia producenta Systemu ITSM na okres 36 miesięcy od daty podpisania Protokołu Odbioru Umowy,
- m. przeprowadzenia Szkoleń,
- n. dostarczenia Dokumentacji.

III. Zestawienie wymagań wobec treści odpowiedzi na RFI

1. W odpowiedzi na niniejsze RFI należy przedstawić informację cenową obejmującą poszczególne ceny jednostkowe zgodnie z Załącznikiem nr 3, z zachowaniem kolejności tytułów poszczególnych punktów.
2. Wszystkie ceny należy podawać jako wartości netto w polskich złotych.
3. Pytający zakłada, że wszystkie informacje udzielone przez oferenta są prawdziwe i wiarygodne.

IV. Opis sposobu udzielania wyjaśnień

1. Ewentualne pytania dotyczące przedmiotowego zapytania należy kierować drogą elektroniczną na e-mail: **jacek.peczek@pansa.pl**
2. PAŻP zastrzega sobie prawo do nieudzielania odpowiedzi na pytania wykraczające poza zakres niniejszego zapytania.

V. Załączniki

1. Załącznik nr 1- Wymagania na Narzędzie ITSM w PAŻP
2. Załącznik nr 2 - Gwarancja dla Systemu ITSM
3. Załącznik nr 3 – Formularz wyceny

Załącznik nr 1- Wymagania na Narzędzie ITSM w PAŻP

Spis treści

1. Słownik pojęć	8
2. Wymagania na System ITSM	11
2.1. Założenia	11
2.2. Architektura	12
2.3. Bezpieczeństwo	14
2.4. Administracja	15
2.5. Integracja z systemami zewnętrznymi	17
3. Wymagania w zakresie funkcji i procesów	18
3.1. Funkcja Service Desk	18
3.2. Proces Zarządzanie Incydentami	19
3.3. Proces Realizacji Wniosków	21
3.4. Proces Zarządzanie Problemami	22
3.5. Proces Zarządzanie Zmianami	24
3.6. Proces Zarządzanie Komponentami Usług i Konfiguracją	26
3.7. Proces Zarządzanie Poziomem Usług	31
3.8. Proces Zarządzanie Bazą Wiedzy	32
4. Wymagania na mierzenie i raportowanie Usług	34
4.1. Zarządzanie Incydentami	34
4.2. Funkcja Service Desk	35
4.3. Zarządzanie Zmianami	36
4.4. Zarządzanie Poziomem Usług	36
4.5. Zarządzanie Komponentami usług i Konfiguracją	37

1. Słownik pojęć

Nazwa / skrót	Opis
Administrator Systemu	Osoba odpowiedzialna za utrzymanie i administrację Systemu ITSM.
Asset	Ogólnie pojęte aktywa, o których informacje są przetwarzane przez System ITSM, w szczególności sprzęt komputerowy, oraz licencje oprogramowania.
Baza CMDB	ang. <i>Configuration Management Data Base</i> – Baza Konfiguracji Baza danych zawierająca wszystkie istotne szczegóły dotyczące elementu konfiguracji oraz szczegóły istotnych powiązań między nimi.
Baza Wiedzy	Baza zawierająca informacje o Incydentach, Problemach i Znanych Błędach. Używana jest do wyszukiwania rozwiązań dla nowych Incydentów w celu skrócenia czasu ich rozwiązania.
Baza Znanych Błędów	Baza zawierająca informacje o wszystkich Znanych Błędach. Tworzona jest przez proces Zarządzania Problemami i wykorzystywana przez ten proces oraz Proces Zarządzania Incydentami.
Element Konfiguracji (EK)	Komponent infrastruktury lub element, który będzie objęty nadzorem Zarządzania konfiguracją. Mogą one znacznie różnić się złożonością, rozmiarem lub typem. Elementem Konfiguracji może być cały system, wliczając w to sprzęt, oprogramowanie i dokumentację lub też jeden moduł lub drobny komponent sprzętowy.
Eskalacja Hierarchiczna	Przekazanie informacji o przebiegu obsługi rozwiązywania Problemu na kolejny szczebel zarządczy.
Eskalacja Funkcjonalna / Eskalacja funkcyjna	Przekazanie Problemu do innej Grupy Wsparcia posiadającej większą wiedzę i doświadczenie w obszarze, którego dotyczy przekazywany Problem.
Grupa Wsparcia	Grupy (stałe, kompetencyjne, zadaniowe) pracowników IT realizujące obsługę zgłoszeń oraz zadań/projektów.
Incydent	Każde zdarzenie, które nie należy do standardowej operacji Usługi IT i które powoduje lub może powodować przerwę w dostarczaniu tej usługi lub redukcję jej jakości.

Nazwa / skrót	Opis
ITIL	ang. <i>Information Technology Infrastructure Library</i> Biblioteka najlepszych praktyk zarządzania IT będąca własnością Agencji UK Cabinet Office działającej przy rządzie brytyjskim.
Menedżer Bazy Wiedzy	Osoba administrująca wpisami w Bazie Wiedzy, akceptująca propozycje wpisów do Bazy Wiedzy.
Obejście (ang. <i>work-around</i>)	Metoda stosowana w celu jak najszybszego przywrócenia normalnego, tj. zgodnego z opisem, działania Usługi IT w przypadku zaistnienia Incydentu, polegająca na zastosowaniu tymczasowego rozwiązania.
OLA (Operational Level Agreement)	Umowa opisująca parametry usługi technicznej (wewnętrznej) dostarczanej przez jednostki podległe Zastępcy Dyrektora Biura Administracyjnego ds. IT.
Operator IT	Osoba zajmująca się rozwiązywaniem Incydentów, Problemów oraz Wniosków o Usługę w ściśle określonym obszarze kompetencji. Mogą być to pracownicy I, II Linii Wsparcia.
Pilność	Miara określająca pożądaną szybkość działania, na przykład wypracowania rozwiązania Incydentu lub Problemu albo podjęcia decyzji o wdrożeniu zmiany i jej zrealizowania.
Priorytet	Jest to główny parametr określający pierwszeństwo do obsługi dla danego Incydentu lub Problemu.
Priorytet użytkownika	Priorytet określany przez użytkownika rejestrującego zgłoszenia, w zgłoszeniach generowanych automatycznie równy wartości Priorytetu.
Problem	Nieznana, ukryta przyczyna co najmniej jednego Incydentu.
Proces	Logiczny ciąg czynności, który prowadzi do spełnienia oczekiwań odbiorcy procesu (zewnętrznego lub wewnętrznego) poprzez dostarczenie mu produktów w postaci: wyrobów, usług, dokumentacji lub informacji. Procesy są powtarzalne (realizowane cyklicznie), zużywają zasoby (kapitał, zasoby ludzkie, czas, materiały, wyposażenie) a w efekcie ich działania powstaje wartość dodana.
Proces ITSM	Jeden z procesów opisanych w bibliotece ITIL
Rada ds. Zmian (CAB)	Grupa osób odpowiedzialna za sprawne i rzetelne sporządzanie rekomendacji odnośnie przedstawianych jej Wniosków o Zmianę.

Nazwa / skrót	Opis
Rada ds. Pilnych Zmian (ECAB)	Grupa osób podejmująca decyzje w zakresie Zmian Pilnych.
RfC (Request for Change)	Wniosek o Zmianę zgodnie z wytycznymi biblioteki ITIL Formularz lub ekran zastosowany do zapisu szczegółów żądania zmian w dowolnym Elemencie Konfiguracji w Usłudze IT lub infrastrukturze.
Service Desk	Jeden punkt kontaktu dla użytkowników przy zakłóceniach w działaniu Usługi IT, zgłaszaniu Wniosków o Usługę, a nawet niektórych kategorii Wniosków o Zmianę.
SLA (Service Level Agreement)	Pisemne uzgodnienie między dostawcą Usług IT i klientem, w którym są udokumentowane Usługi IT oraz uzgodnione poziomy Usług IT.
System ITSM / Narzędzie ITSM	Narzędzie informatyczne wspierające procesy zdefiniowane w ramach zarządzania Usługami IT.
UC (Underpinning Contract)	Umowa opisująca zobowiązania zewnętrznego dostawcy Usługi IT (usługa zewnętrzna) w celu zagwarantowania warunków zawartych w OLA lub SLA.
Usługa IT	Usługa IT to sposób dostarczania Klientowi narzędzi umożliwiających uzyskanie rezultatów biznesowych, których oczekuje. Klient nie bierze na siebie kosztów i ryzyk związanych z dostarczaniem Usługi IT.
Użytkownik	Osoba uprawniona do zgłaszania Zgłoszeń w Systemie ITSM.
Wniosek o Usługę	Formalna prośba użytkownika o dostarczenie czegoś - na przykład, prośba o informację lub poradę, o reset hasła lub dostarczenie stacji roboczej dla nowego pracownika.
Wniosek o Zmianę	Patrz RfC
Wpływ	Miara określająca stopień naruszenia przez Incydent gwarantowanego w umowie poziomu Usługi IT.
Zadania	Zestaw czynności wykonywanych w ramach obsługi zgłoszeń.
Zgłoszenie	Incydent, Wniosek o Usługę
Znany Błąd	To Problem, dla którego przyczyna wystąpienia Incydentu (ów) została zdiagnozowana i zostało opracowane rozwiązanie tymczasowe (Obejście) lub trwałe.

2. Wymagania na System ITSM

2.1. Założenia

2.1.1. Opis wymagań

1. Oferowane rozwiązanie musi zapewniać wsparcie implementacji funkcji i procesów:
 - Funkcja Service Desk,
 - Proces Zarządzanie Incydentami,
 - Proces Realizacja Wniosków,
 - Proces Zarządzanie Problemami,
 - Proces Zarządzanie Zmianami,
 - Proces Zarządzanie Komponentami Usług i Konfiguracją,
 - Proces Zarządzanie Poziomem Usług,
 - Proces Zarządzanie Katalogiem Usług,
 - Mierzenie i raportowanie Usług.
2. Wykonawca musi zaoferować przedstawić system, który będzie działał optymalnie na wyspecyfikowanym przez zamawiającego infrastrukturze.
3. System ITSM musi umożliwiać obsługę min. 2000 zgłoszeń miesięcznie.

2.1.2. Licencje

1. Liczba wymaganych licencji
 - a. 15 licencji dla Operatorów IT jednoczesnych,
 - b. 10 licencji dla Operatorów IT nazwanych.

2. Maintenance

Licencje muszą być objęte co najmniej 36 miesięcznym wsparciem producenta (maintenance).

W ramach maintenance Zamawiający może zgłaszać Wady Systemu ITSM całodobowo – 24 godziny na dobę, 7 dni w tygodniu, 365 dni w roku (366 w przypadku lat przestępnych) do serwisu producenta oprogramowania lub serwisu autoryzowanego przez producenta. Zgłoszenie Wady może być dokonywane w postaci: zgłoszenia telefonicznego, za pomocą faksu, z wykorzystaniem serwisu WWW w języku polskim, lub za pomocą poczty elektronicznej.

2.1.3. Użytkownicy

Licencje powinny zapewniać możliwość pracy użytkownikom w liczbach wymienionych w tabeli:

	Nazwa użytkowników/procesu	Liczba osób użytkujących proces	Liczba osób zarządzających procesem*
1	Użytkownicy końcowi (zgłaszanie incydentów, wniosków o usługę, przeszukiwanie bazy wiedzy)	min. 2.000 osób	4 operatorów
2	Zarządzenie Incydentami	30 operatorów	4 operatorów
2.1	I linia Wsparcia (funkcja Service Desk)	10 operatorów	n.d.
2.2	II linia Wsparcia (Administratorzy systemów informatycznych)	20 operatorów	n.d.
3	Zarządzanie Problemami	30 operatorów	4 operatorów
4	Zarządzanie Poziomem Usług	15 operatorów	3 operatorów
5	Zarządzanie Konfiguracją	4 operatorów	3 operatorów
6	Zarządzanie Zmianami	5 operatorów	3 operatorów
7	Zarządzanie Bazą Wiedzy	5 operatorów	2 operatorów

Tabela 1. Liczba pracowników korzystających z narzędzia ITSM

* przez zarządzanie procesem rozumie się m.in. modyfikowanie 'workflow' procesu, modyfikowanie formatek i formularzy, modyfikowanie słowników itp.

- Wykonawca przedstawi możliwe sposoby licencjonowania (w tym także dostępność w modelu Application Service Provider) oraz ceny licencji w przypadku konieczności dokupienia ich w przyszłości. W szczególności dla różnej liczby użytkowników, w podziale co 100 użytkowników oraz w wersji nielimitowanej w aspekcie liczby użytkowników, o ile istnieje taka możliwość.
- Dostarczone licencje na System ITSM powinny również umożliwić zamawiającemu uruchomienie dodatkowej instancji Systemu (testowej).

2.2. Architektura

2.2.1. Opis wymagań

- System ITSM powinien posiadać polską wersję językową. Dopuszczalne jest rozwiązanie, w którym wersja polska dotyczy tylko opcji dla: Użytkowników, Operatorów IT i ról zarządzających procesami, a panel administratora posiada wyłącznie angielską wersję językową.
- System ITSM musi gwarantować zapewnienie wysokiej dostępności.
- System powinien zapewniać informacje o logowaniu wszystkich aktywności realizowanych na zgłoszeniach oraz elementach konfiguracji (kto i co zmienił),

ze szczególnym uwzględnieniem czynności mających wpływ na kluczowe parametry usługi. System powinien jednocześnie gwarantować historię działania Użytkownika oraz Operatora IT w ramach jednego zalogowania.

4. System ITSM musi posiadać trójwarstwową architekturę (baza danych, serwer aplikacji, interfejs klienta).
5. System ITSM musi zapewniać możliwość pracy na platformie sprzętowej o następujących parametrach będącej w posiadaniu pytającego:

Serwery obsługujące środowiska produkcyjne jak i testowe będą pracowały pod nadzorem wirtualizatora firmy Microsoft – Hyper-V o poniższych parametrach:

Serwer: Serwer PowerEdge M630 E5-2690v3 – 2 CPU

Procesor	Intel Xeon E5-2690 v3
Ilość rdzeni/CPU	12
Taktowanie procesora	3,5 / 2,6 GHz
RAM dla serwera aplikacyjnego	16 GB
RAM dla serwera SQL	32 GB
Przestrzeń na dysku dla serwera aplikacyjnego	min 100GB
Przestrzeń na dysku dla serwera SQL	min 400GB

6. Pytający w przypadku gdy oferowane narzędzie będzie wymagało platformy systemowej Microsoft Windows Server zapewni odpowiednie licencje systemu operacyjnego oraz CAL, umożliwiające korzystanie z Systemu ITSM.
7. W przypadku gdy oferowane narzędzie wymaga platformy bazodanowej Microsoft SQL Server (dopuszczalna wersja 2013 lub wyższa), Pytający zapewni odpowiednie licencje systemu bazodanowego oraz CAL, umożliwiające korzystanie z Systemu ITSM
8. Rozwiązanie musi być skalowalne, w przypadku potrzeby zwiększenia wydajności, poprzez zwiększenie liczby serwerów w warstwie aplikacji oraz baz danych.
9. Dostęp do funkcjonalności systemu dla Użytkowników musi być realizowany za pośrednictwem standardowej przeglądarki WWW (co najmniej *MS Internet Explorer* w wersji 11 lub nowszej, *Firefox* w wersji 52.0 lub nowszej). System powinien umożliwiać zrealizowanie tej funkcjonalności bez konieczności instalacji dodatkowych pluginów do przeglądarek
10. Dostęp do funkcjonalności systemu dla Operatorów IT musi być realizowany za pośrednictwem przeglądarki WWW (co najmniej *MS Internet Explorer* w wersji 11 lub nowszej, *Firefox* w wersji 52.0 lub nowszej).
11. Dostęp do funkcjonalności systemu dla administratorów systemu może być realizowany za pośrednictwem przeglądarki WWW (co najmniej *MS Internet Explorer* w wersji 11 lub nowszej, *Firefox* w wersji 52.0 lub nowszej) lub dedykowanej aplikacji działającej pod kontrolą systemu MS Windows 8.1 lub wyższej.

12. Rozwiązanie powinno umożliwiać realizację importu danych obejmującą możliwość ładowania plików w formacie: CSV oraz XML.
13. Rozwiązanie powinno umożliwiać realizację eksportu danych w formatach: CSV oraz XML.
14. Rozwiązanie powinno umożliwiać wymianę danych pomiędzy Systemem ITSM a innymi aplikacjami z wykorzystaniem usług sieciowych *Web Service*.
15. Rozwiązanie powinno umożliwić logiczne wydzielenie części systemu na potrzeby świadczenia przez Zamawiającego Usługi Service Desk.
16. Rozwiązanie powinno pozwolić na badanie wykorzystania poszczególnych funkcjonalności systemu ITSM obejmująca m.in. częstotliwość wykorzystywania poszczególnych funkcjonalności.
17. System ITSM powinien powodować zamknięcie sesji nieaktywnych, ale tylko dla zdefiniowanych ról z uwzględnieniem zapewnienia wymogu dowolnej konfiguracji czasu, po którym sesja będzie automatycznie zamykana z opcją ponownego szybkiego wznowienia.

2.3. Bezpieczeństwo

2.3.1. Opis wymagań

1. Rozwiązanie musi posiadać mechanizm definiowania profili użytkowników, które wykorzystywane są między innymi do zabezpieczenia przed nieuprawnionym dostępem do Systemu ITSM i poszczególnych jego funkcji.
2. Prawa w Systemie ITSM muszą się opierać na poziomie dostępu do odpowiednich profili zdefiniowanych dla grup Użytkowników oraz ich ról w obsługiwanych procesach.
3. Dostosowywanie uprawnień Użytkowników i definiowanie ograniczeń dostępu musi być funkcjonalnością dostępną Administratorowi Systemu.
4. Rozwiązanie musi zapewniać możliwość uwierzytelniania Użytkowników poprzez integrację z bazą LDAP w tym z Active Directory firmy Microsoft, Zamawiającego.
5. Rozwiązanie musi zapewniać możliwość oznaczania Użytkowników korzystających z rozwiązania bezpośrednio w Systemie ITSM w przypadku, gdy Użytkownik nie korzysta z bazy LDAP (Active Directory firmy Microsoft).
6. Rozwiązanie musi zawierać funkcjonalność rejestrowania dostępu Użytkownika i Administratora Systemu do aplikacji oraz ich działań w aplikacji (Dziennik zdarzeń).
7. Rozwiązanie musi umożliwiać szyfrowanie informacji przesyłanych między serwerem i stacją roboczą Użytkownika Systemu ITSM. W przypadku dostępu przez WWW rozwiązanie musi umożliwiać korzystanie z bezpiecznego połączenia przez HTTPS.

8. Rozwiązanie musi umożliwiać zrealizowanie wszystkich wymagań stawianych przed systemami przetwarzającymi dane osobowe zgodnie z Ustawą o ochronie Danych Osobowych.

2.4. Administracja

2.4.1. Opis wymagań

1. System ITSM musi umożliwiać dodawanie przez Administratora Systemu nowych pól do formularzy, bez konieczności zmian w kodzie aplikacji.
2. Rozwiązanie musi umożliwiać dodawanie reguł i akcji umożliwiających wykonanie operacji typu:
 - a. wysłanie wiadomości pocztą elektroniczną,
 - b. zmiana wartości dowolnego pola (w momencie przekroczenia ustalonego czasu rozwiązania zgłoszenia oraz innych zdefiniowanych punktów kontrolnych).
3. Rozwiązanie musi umożliwiać nadawanie Operatorom IT uprawnień pozwalających na rejestrację, edycję, usuwanie i odczytywanie poszczególnych typów danych przechowywanych w systemie (np.: zgłoszenie, informacja na tablicy ogłoszeń, zasób IT). Ponadto tablica ogłoszeń powinna mieć funkcje *flash* (przemieszczających się na stronie, dynamicznych, dobrze widocznych (zauważalnych) komunikatów, a nie statycznego komunikatu.
4. System ITSM musi zapewnić elastyczne definiowanie struktur organizacyjnych:
 - a. wewnętrzne i zewnętrzne Grupy Wsparcia,
 - b. grupy Użytkowników końcowych (hierarchia organizacji).
5. Rozwiązanie musi zapewnić przypisanie do osoby informacji o jej:
 - a. lokalizacji,
 - b. danych kontaktowych (nr tel., e-mail),
 - c. przynależności w strukturze organizacyjnej,
 - d. dostarczanych Usługach IT,
 - e. przypisanych Elementach Konfiguracji,
 - f. umowach SLA oraz poziomach i warunkach Usług IT świadczonych danej osobie.
6. Oferowane rozwiązanie musi umożliwiać dodawanie nowych pól do tabel dla repozytoriów danych o typach:

Lp.	Typ danych	Opis
1	Tekstowe	Pole umożliwiające wprowadzanie i przechowywanie ciągu dowolnych znaków alfanumerycznych
2	Numeryczne	Pole umożliwiające wprowadzanie i przechowywanie całkowitych wartości liczbowych
3	Daty	Pole umożliwiające wprowadzanie i przechowywanie wartości określających daty i czasy
4	Wielo-wierszowe	Pole umożliwiające wprowadzanie i przechowywanie wielu wierszy ciągu dowolnych znaków alfanumerycznych
5	Logiczne	Pole umożliwiające wprowadzanie i przechowywanie wartości prawda / fałsz
6	Obiekt	Pole umożliwiające wprowadzanie i przechowywanie załączników

7. Oferowane rozwiązanie musi umożliwić dodawanie nowych pól (kontrolek) do formularzy interfejsu o typach:

Lp.	Typ pola	Opis
1	Tekstowe	Pole umożliwiające wprowadzanie i prezentację ciągu dowolnych znaków alfanumerycznych
2	Daty	Pole umożliwiające wprowadzanie i prezentację wartości określających daty i czasy. Pole umożliwiające: – Manualne wprowadzenie daty według zdefiniowanego formatu – Automatyczne wprowadzenie daty poprzez wybór z kalendarza Data/czas będą prezentowane na formularzu zgodnie ze zdefiniowanym przez administratora formatem.
3	Wielowierszowe	Pole umożliwiające wprowadzanie i prezentację wielu wierszy ciągu dowolnych znaków alfanumerycznych.
4	Combo Box	Pole listy rozwijanej. Umożliwiające wybór jednej z wielu zdefiniowanych wartości.
5	Check Box	Pole umożliwiające wprowadzanie i przechowywanie wartości prawda/fałsz
6	Aktywne łącze	Pole tekstowe umożliwiające automatyczne wprowadzenie danych poprzez odniesienie się do referencyjnego repozytorium
7	Obiekt	Pole umożliwiające wprowadzanie i prezentację załączników

2.5. Integracja z systemami zewnętrznymi

2.5.1. Opis wymagań

Poniżej wskazane zostały zewnętrzne źródła danych, z którymi powinien integrować się System ITSM:

1. Active Directory firmy Microsoft,
 - a. Integracja polegająca na zasileniu Systemu ITSM danymi o pracownikach Zamawiającego (m.in. imię, nazwisko, nr pracownika, komórka organizacyjna, lokalizacja, e-mail, telefon, nazwa konta użytkownika w AD)
 - b. Zasilenie systemu inicjalne – informacje o ok. 2000 pracownikach Zamawiającego.
 - c. Synchronizacja danych dokonywana raz na dobę

System ITSM powinien umożliwiać automatyczne odnotowywanie informacji o identyfikatorze użytkownika wprowadzającego dane osobowe do systemu, oraz dacie pierwszego wprowadzenia danych do systemu, podczas importu lub synchronizacji danych, a także wykonanie raportu zawierającego te informacje.

2. System do ewidencji sprzętu informatycznego eAudytor firmy BTC, oraz System do ewidencji księgowej ORACLE EBS wersja 11i (moduł ST - środki trwałe),
 - a. Zasilenie inicjalne systemu danymi o sprzęcie informatycznym z systemu eAudytor firmy BTC – ok. 5.500 sztuk
 - b. Opcjonalna integracja z system ORACLE EBS wersja 11i, w zakresie danych o środkach trwałych
 - c. Docelowo możliwość integracji po przez web service z systemem finansowo księgowym (moduł ST - środki trwałe). System zostanie wyłoniony w przygotowywanym postępowaniu zakupowym.
3. System musi umożliwiać integrację z Microsoft System Center 2012 Configuration Manager.
4. System musi umożliwiać integrację z Microsoft SharePoint 2013 i wyżej.
5. System musi zapewniać informację o zasobach (w tym zasobach ludzkich) na podstawie danych z Active Directory Niezbędna jest aktualizacja danych o ludziach, ich kontaktach, adresach e-mail.
6. System musi zapewnić możliwość wykorzystania Web Serwisów do integracji z innymi systemami.

3. Wymagania w zakresie funkcji i procesów

3.1. Funkcja Service Desk

3.1.1. Wymagania w zakresie Funkcji Service Desk

1. Możliwość rejestracji zgłoszeń przy pomocy wiadomości e-mail, która automatycznie generuje zapis Incydentu w Systemie ITSM (realizowane przez system bezpośrednio lub pośrednio za pomocą dodatkowych modułów/rozwiązań).
2. Możliwość automatycznej rejestracji Zgłoszeń z systemów monitorujących pracę określonych urządzeń np.: serwerów, urządzeń sieciowych, UPS.
3. Możliwość definiowania ról oraz zakresu ich uprawnień.
4. Zapewnienie przez system elastycznego mechanizmu notyfikacji, pozwalającego definiować reguły powiadomień dla przypisanych operatorów w zależności od parametrów zgłoszenia.
5. Możliwość zdefiniowania wewnętrznych alarmów informujących o sytuacjach takich jak: przekroczona liczba przekazania zgłoszenia, zbliżający się termin rozwiązania, brak podjęcia przez linie wsparcia, itp.
6. Możliwość w Zgłoszeniach i Wnioskach o Zmianę dołączania i przechowywania załączników w dowolnym formacie (w szczególności w formacie: PDF, DOC, DOCX, XLS, XLSX, JPG, GIF, TIFF, BMP).
7. Zapewnienie przez system pól obligatoryjnych zgłoszenia:
 - a. data i godzina Zgłoszenia,
 - b. unikalny identyfikator Zgłoszenia (generowany automatycznie),
 - c. Wpływ i Pilność,
 - d. priorytet Zgłoszenia (definiowany na podstawie Wpływu i Pilności),
 - e. kategoria Zgłoszenia,
 - f. temat Zgłoszenia,
 - g. pełny opis Zgłoszenia,
 - h. zgłaszający, użytkownik, odpowiedzialny i grupa realizująca zgłoszenie,
 - i. jednostka organizacyjna zgłaszającego,
 - j. nr telefonu zgłaszającego,
 - k. Element Konfiguracji (lub też grupa Elementów Konfiguracji), którego dotyczy Zgłoszenie, w tym informacji o usłudze,
 - l. status Zgłoszenia.
8. Możliwość definiowania pól wypełnianych automatycznie przez system:
 - a. priorytet Zgłoszenia,
 - b. data i godzina rejestracji Zgłoszenia,
 - c. data i godzina przekazania Zgłoszenia do odpowiedniej Grupy Wsparcia,
 - d. data i godzina realizacji,
 - e. data i godzina zamknięcia,
 - f. kontrola zadeklarowanych parametrów realizacji.
9. Możliwość przypisania do zgłoszenia Elementu Konfiguracji (lub grupy Elementów) użytkowanego przez Zgłaszającego lub innego zasobu, z którym związane jest dane

Zgłoszenie. Lista Elementów Konfiguracji będących w posiadaniu Zgłaszającego musi być dostępna podczas rejestracji Zgłoszenia.

10. Możliwość zmiany przypisanego do Zgłoszenia Elementu Konfiguracji lub dodanie nowego Elementu Konfiguracji w czasie obsługi Zgłoszenia;
11. Możliwość sprawnego zarządzania kalendarzem z uwzględnieniem:
 - a. dni świadczenia usługi dla każdej usługi zgodnie z deklarowanymi czasami ich wsparcia (z uwzględnieniem dni świątecznych),
 - b. planowanych przerw w działaniu Usług,
 - c. harmonogramu wszystkich zmian,
 - d. zależności i wzajemnego wpływu planowanych oraz realizowanych czynności, ułatwiających koordynację wszelkich aktywności w ramach codziennej pracy.
12. Możliwość sprawnego dystrybuowania ankiet drogą mailową do wybranej grupy Użytkowników.
13. Możliwość zastosowania różnych formularzy rejestracji zgłoszenia w zależności od kategorii zgłoszenia. Kategoryzacja zgłoszeń powinna zależeć od miejsca zajmowanego w strukturze organizacyjnej hierarchii (nie wszystkie kategorie powinny być dostępne dla każdego zgłaszającego).

3.2. Proces Zarządzanie Incydentami

3.2.1. Wymagania w zakresie procesu Zarządzania Incydentami

1. Możliwość zgłaszania Incydentów z różnych źródeł:
 - a. strona WWW,
 - b. e-mail z oznaczeniem, jakim kanałem zgłoszenia zostały zgłoszone,
 - c. komunikaty z systemu monitorowania,
 - d. aplikacja biznesowa,
 - e. ręcznie przez pracownika Service Desk.
2. Możliwość generowania automatycznej informacji zwrotnej potwierdzającą przyjęcie i rozwiązanie Incydu. Możliwość tworzenia szablonów korespondencji przez administratora systemu.
3. Możliwość automatycznego tworzenia incydu na podstawie alertu wysłanego przez system monitorowania infrastruktury teleinformatycznej).
4. Możliwość zdefiniowania Priorytetu Incydu poprzez określenie Wpływu i Pilności. Dostępne parametry Wpływu i Pilności muszą być definiowane przez Administratora Systemu w module administracyjnym.
5. Możliwość kategoryzacji i klasyfikacji Incydu, w co najmniej 3-poziomowej hierarchicznej strukturze.
6. Możliwość przekazywania Incydentów do wielu Grup Wsparcia; przypisywanie zadań do wielu Grup Wsparcia.
7. Realizacja Incydentów za pomocą Zadań.
8. Możliwość tworzenia eskalacji hierarchicznej i funkcjonalnej dla Incydentów z uwzględnieniem możliwości postępu prac nad zgłoszeniami pomimo eskalacji.

9. Możliwość dowolnego modyfikowania listy statusów z określeniem, które z nich mają wpływać na czas realizacji.
10. Możliwość tworzenia nadrzędności i podrzędności Incydentów ze Zgłoszeniami w dowolnej konfiguracji.
11. Możliwość wyboru Usługi, na którą wpływa Incydent podczas rejestracji Zgłoszenia.
12. Możliwość przekazywania Incydentów do zewnętrznych organizacji wsparcia.
13. Możliwość sortowania i grupowania Incydentów, które wpływają na dany Element Konfiguracji.
14. Możliwość sortowania i grupowania Incydentów zgłoszonych przez tę samą grupę Użytkowników.
15. Możliwość automatycznego określenia osób przypisanych do realizacji Incydentów na podstawie kategorii.
16. Ograniczenie możliwości otwierania, modyfikacji i zamykania Incyduentu tylko do określonych w procesie ról.
17. Mechanizm umożliwiający przypisanie Incydentów do określonej Grupy Wsparcia oraz możliwość pobrania przez dowolnego pracownika tej grupy Incyduentu z listy. Pobranie Incyduentu z listy powoduje automatyczne jego przypisanie do osoby pobierającej.
18. Umożliwienie obsługi tzw. 'masowych Incydentów' (incydenty takie same, lecz pochodzące od różnych użytkowników) poprzez podłączanie ich do jednego głównego Incyduentu. W podglądzie Incyduentu musi się pojawić informacja o podpiętych Incydentach. Rozwiązanie głównego Incyduentu musi automatycznie rozwiązywać powiązane z nim Incydenty i gdy zostanie zamknięty główny incydent system zamyka również incydenty z nim powiązane (zgrupowane).
19. System nie może pozwolić na zamknięcie zgłoszenia w przypadku gdy pozostają otwarte zlecenia związane z danym zgłoszeniem jak i w przypadku gdy pozostają niewypełnione a wymagane do wypełnienia, pola na formularzu zgłoszenia – walidacja kompletności danych na formularzach zgłoszeń.
20. Możliwość dostępu do informacji z procesu Zarządzania Zmianami, takich jak kalendarz Zmian planowanych czy historia Zmian.
21. Możliwość przeglądania i oszacowania, czy planowane Zmiany mogą dostarczyć rozwiązania istniejącego Incyduentu.
22. Dostęp do Bazy Wiedzy w celu wsparcia diagnozy Incyduentu i jego rozwiązania – preferowany dostęp z funkcjonalnością zapewniającą informację o rozwiązaniach zastosowanych w analogicznych sytuacjach.
23. Możliwość definiowania filtrów dostępu do grup Incydentów, np. raportowanie Incydentów o przekroczonym czasie rozwiązania.
24. Możliwość bieżącego monitorowania statusów Incydentów, dostarczająca wiarygodnych informacji o rzeczywistym czasie ich realizacji (uwzględniające wszelkie przestoje czasowe w realizacji zgłoszenia).
25. Możliwość tworzenia Problemów, Wniosków o Usługę i Wniosku o Zmianę, Zgłoszeń serwisowych (są to zgłoszenia do dostawców zewnętrznych), zadań z poziomu Incyduentu;

26. Możliwość informowania Użytkowników zgłaszających oraz pracowników Service Desk o bieżących pracach i awariach, tzw. *hot news* – informacje z ostatniej chwili.
27. Możliwość zakładania blokad, żeby nie tworzyły się zgłoszenia podczas planowanych prac serwisowych.
28. Funkcjonalność umożliwiająca zablokowanie możliwości zamknięcia zgłoszenia otwartego w wyniku monitorowania do czasu, gdy sytuacja nie ulegnie naprawie.

Podsumowując: System ITSM w obszarze Zarządzania Incydentami powinien umożliwiać sprawne zarządzanie całym cyklem życia Incydentu, które pozwala na precyzyjne określanie czasów realizacji w rozbiciu na poszczególne statusy zgłoszenia, jak i zbiorczo dla całości, z uwzględnieniem zmian priorytetów Incydentów oraz innych atrybutów zgłoszenia takich jak Grupa Wsparcia, usługa, kategoria. Pomiar musi uwzględniać przedziały czasowe, w których obsługa Incydentu była wstrzymana po stronie Operatorów IT np.: oczekiwanie na informacje od Użytkownika.

System ITSM musi umożliwiać Operatorom IT wstrzymanie prac nad Incydentem. Wstrzymanie prac musi spowodować zawieszenie mierzenia czasu rozwiązania Incydentu. Wznowienie prac nad incydentem może być aktywowane przez tego samego lub innego Operatora IT. Zarówno zawieszenie jak i odwieszenie Incydentu musi być powiązane z wymogiem podania powodu zawieszenia jak i odwieszenia incydentu przez osobę dokonującą tej operacji.

3.3. Proces Realizacji Wniosków

3.3.1. Wymagania w zakresie procesu Realizacji Wniosków

1. Możliwość zgłaszania Wniosków o usługę z różnych źródeł:
 - a. strona WWW,
 - b. e-mail,
 - c. ręcznie przez pracownika Service Desk.
2. Możliwość definiowania szablonów dla wszystkich Wniosków o usługę rejestrowanych automatycznie.
3. Możliwość tworzenia i wykorzystania szablonów dla typowych Wniosków o usługę.
4. Możliwość definiowania i zaimplementowania standardowej listy wniosków o usługę.
5. Zapewnienie przez system pól obligatoryjnych Wniosku o usługę:
 - a. data i godzina Wniosku o usługę,
 - b. unikalny identyfikator Wniosku o usługę (generowany automatycznie),
 - c. Wpływ i Pilność,
 - d. priorytet Wniosku o usługę (definiowany na podstawie Wpływu i Pilności),
 - e. kategoria Wniosku o usługę,
 - f. temat Wniosku o usługę,
 - g. pełny opis Wniosku o usługę,
 - h. zgłaszający, użytkownik, odpowiedzialny i grupa realizująca Wniosek o usługę,
 - i. jednostka organizacyjna zgłaszającego,
 - j. nr telefonu zgłaszającego,

- k. element konfiguracji (lub też grupa elementów konfiguracji), którego dotyczy Wniosek o usługę, w tym informacji o usłudze,
 - l. status Wniosku o usługę.
6. Możliwość automatycznego wypełniania niektórych pól (np. czas obsługi) na podstawie SLA.
 7. Możliwość dodawania załączników do Wniosków o usługę w dowolnym formacie (w szczególności w formacie: PDF, DOC, DOCX, XLS, XLSX, JPG, GIF, TIGG, BMP).
 8. Możliwość eskalacji Wniosku o usługę (hierarchicznej i funkcjonalnej).
 9. Realizacja eskalacji Wniosku o usługę nie powinna mieć wpływu na dostępność Wniosku dla jego właściciela (musi on być w stanie kontynuować śledzenie postępu prac nad Wnioskiem o usługę).
 10. Możliwość rejestracji wszystkich czynności związanych z danym Wnioskiem. Historia musi być dostępna dla operatorów systemu.
 11. Możliwość definiowania zadań, planowanego czasu ich realizacji, oraz przypisanie osoby lub grupy odpowiedzialnej za ich realizację.
 12. Możliwość powiązania Wniosków o usługę z elementami konfiguracji w CMDB.
 13. Możliwość utworzenia Wniosku o usługę z poziomu Incydentu.
 14. Możliwość wyszukiwania zarejestrowanych Wniosków o usługę po wybranym parametrze.
 15. Możliwość zdefiniowania różnych dróg kierowania Wniosków o usługę oraz ich akceptacji (workflow) w zależności od rodzaju wniosku.

3.4. Proces Zarządzanie Problemami

3.4.1. Wymagania w zakresie procesu Zarządzania Problemami

1. System ITSM musi umożliwiać rejestrowanie Problemów.
2. Rozwiązanie musi umożliwiać tworzenie Problemów na podstawie zarejestrowanych Incydentów (jednego bądź wielu).
3. Rozwiązanie musi umożliwiać, podczas rejestracji Problemu, pobranie części danych z rekordów Incydentów, na podstawie których rejestrowany jest Problem.
4. Rozwiązanie musi zapewniać możliwość powiązania zarejestrowanych Incydentów z Problemem, jak również powiązań pomiędzy Problemami.
5. Rozwiązanie musi umożliwiać rejestrowanie Znanych Błędów.
6. Rejestracja Znanych Błędów musi odbywać się na podstawie zarejestrowanych Problemów. System musi umożliwiać, podczas rejestracji Znanego Błędu, pobranie części danych z rekordów Problemu, na podstawie którego Znany Błąd jest rejestrowany.
7. W momencie rejestracji Znanego Błędu, Problem, na podstawie którego rejestrowany jest Znany Błąd, musi od razu zostać z nim powiązany, co może być realizowane poprzez zmianę statusu Problemu. Musi również istnieć możliwość powiązania Problemów z już zarejestrowanymi Znanymi Błędami.
8. Rozwiązanie powinno umożliwiać, w czasie rejestracji, przypisanie do Problemu Elementu Konfiguracji (lub Grupy EK), z którym związany jest dany Problem. Jeżeli

Problem rejestrowany jest na podstawie Incydentu, wówczas System ITSM musi podpowiadać Elementy Konfiguracji przypisane do Incydentu. Lista Elementów Konfiguracji musi być pobierana z Bazy CMDB (ang. *Configuration Management DataBase*).

9. Rozwiązanie musi umożliwiać, w czasie rejestracji, przypisanie do Problemu i Znanego Błędu Usługi lub Usług, której dotyczy, jak również umożliwiać zmianę tego przypisania w trakcie jego obsługi.
10. Rozwiązanie musi umożliwiać śledzenie postępu prac nad Problemami i Znanymi Błędami poprzez interfejs WWW.
11. Rozwiązanie musi zapewniać Operatorom IT z poszczególnych Grupach Wsparcia dostęp do Problemów przypisanych do danej Grupy Wsparcia poprzez interfejs WWW.
12. Rozwiązanie musi zapewniać możliwość kategoryzacji Problemów i Znanych Błędów zgodnie ze zdefiniowaną przez Administratora Systemu listą kategorii.
13. Listę kategorii musi tworzyć Administrator Systemu. Podczas tworzenia listy kategorii Administrator Systemu musi posiadać możliwość zdefiniowania również nazwy Grup Wsparcia oraz listy Operatorów IT, dla których będą przypisywane Problemy i Znane Błędy. Lista kategorii musi być spójna dla Incydentów, Problemów i Znanych Błędów.
14. Rozwiązanie musi posiadać mechanizm umożliwiający przypisanie Problemów i Znanych Błędów do określonej Grupy Wsparcia (grupa Operatorów IT) oraz możliwość pobrania przez dowolnego pracownika tej grupy Problemu lub Znanego Błędu z listy. Pobranie Problemu lub Znanego Błędu z listy powoduje automatyczne jego przypisanie do osoby pobierającej.
15. Rozwiązanie musi posiadać mechanizm wysyłania powiadomienia pocztą elektroniczną do wszystkich Operatorów IT w danej Grupie Wsparcia w przypadku przypisania Problemu lub Znanego Błędu na tę grupę.
16. Przekazanie Problemu lub Znanego Błędu do innej Grupy Wsparcia lub do innego Operatora IT Grupy Wsparcia musi być powiązane z koniecznością utworzenia komentarza wewnętrznego (widocznego tylko dla Operatora IT) przez osobę przekazującą.
17. Rozwiązanie musi zapewniać możliwość automatycznego zdefiniowania Priorytetu Problemu poprzez określenie Wpływu i Pilności. Dostępne parametry Wpływu i Pilności muszą być definiowane przez Administratora Systemu w module administracyjnym.
18. Dla uprawnionych Operatorów IT w Grupie Wsparcia, system musi umożliwiać ręczną zmianę przypisanego Priorytetu.
19. Rozwiązanie musi umożliwiać dołączenie do Problemu i Znanych Błędów załączników w dowolnym formacie.
20. Rozwiązanie musi posiadać mechanizm automatycznego informowania Operatora IT, który zarejestrował Problem lub Znany Błąd, o zmianie jego statusu oraz postępach prac, zgodnie z parametrami i warunkami zdefiniowanymi przez Administratora Systemu.
21. Rozwiązanie musi posiadać mechanizm automatycznego informowania Operatorów IT w danej Grupie Wsparcia o przypisaniu Problemu lub Znanego Błędu, zmianie jego

statusu oraz wpływającym czasie realizacji, zgodnie z parametrami i warunkami zdefiniowanymi przez Administratora Systemu.

22. Rozwiązanie musi posiadać możliwość definiowania i edycji nazw statusów Problemów i Znanych Błędów.
23. System musi umożliwiać śledzenie zmian historii cyklu Problemu i Znanego Błędu. Przy czym treść Problemu/Znanego Błędu po zarejestrowaniu powinna być nieedytowalna. Wszelkie zmiany powinny być rejestrowane, jako elementy dodatkowe, dopisywane w trakcie realizacji, z wyspecyfikowaniem daty edycji i danych edytującego. Historia cyklu Problemu lub Znanego Błędu powinna umożliwiać oddzielnie prezentowanie komentarzy merytorycznych, dodawanych załączników oraz komentarzy wewnętrznych, wprowadzanych przez Operatorów IT realizujących Zgłoszenie.
24. Rozwiązanie musi umożliwiać zaawansowane wyszukiwanie Problemów lub Znanych Błędów po dowolnym ich polu.
25. Rozwiązanie musi prezentować Operatorom IT w Service Desk oraz w Grupach Wsparcia wolumen aktualnie przypisanych do nich Problemów i Znanych Błędów, np. z podziałem na Priorytet, kategoryzację itp.
26. Rozwiązanie musi umożliwiać generowanie Wniosków o Zmianę, jak również powiązanie Problemów i Znanych Błędów z tymi wnioskami.
27. Rozwiązanie musi zapewniać możliwość zamknięcia wszystkich Incydentów „podpiętych” pod Problem w przypadku jego rozwiązania.

3.5. Proces Zarządzanie Zmianami

3.5.1. Wymagania w zakresie procesu Zarządzania Zmianami

1. Możliwość rejestrowania Wniosków o Zmianę;
2. Zapewnienie przez system pól obligatoryjnych Wniosku:
 - a. data i godzina Wniosku o Zmianę,
 - b. unikalny identyfikator Wniosku o Zmianę (generowany automatycznie),
 - c. Wpływ i Pilność Zmiany,
 - d. priorytet Wniosku o Zmianę (definiowany na podstawie Wpływu i Pilności),
 - e. kategoria Wniosku o Zmianę,
 - f. typ Zmiany,
 - g. temat Wniosku o Zmianę,
 - h. pełny opis Wniosku o Zmianę,
 - i. opis wyniku testów Zmiany,
 - j. Zgłaszający, użytkownik, odpowiedzialny i grupa realizująca Wniosek o Zmianę,
 - k. termin/terminy wykonania zmiany,
 - l. Element Konfiguracji (lub też grupa Elementów Konfiguracji), którego dotyczy Wniosek o Zmianę, w tym informacji o usłudze, oraz Elementy Konfiguracji (w szczególności systemy informatyczne) na które Zmiana ma wpływ
 - m. status Wniosku o Zmianę.
3. Możliwość definiowania nowych kategorii Zmian (grup Zmian o wspólnej ścieżce obsługi);

4. Możliwość definiowania zadań w ramach procesu;
5. Możliwość definiowania ról oraz zakresu ich uprawnień;
6. Możliwość budowania reguł oceny i akceptacji Zmiany poprzez budowanie drzewa decyzyjnego przypisując odpowiednio osoby z bazy Użytkowników systemu. Poprzez konsolę, Operator IT pełniący odpowiednią rolę w procesie, musi mieć wgląd do wybranych informacji z Wniosku o Zmianę i możliwość podjęcia decyzji, takich jak: zaakceptowanie, do uzupełnienie, odrzucenie. Po pozytywnej akceptacji przez wszystkie osoby ze ścieżki Wniosek o Zmianę musi przejść do realizacji;
7. Z przesłaniem utworzonego Wniosku o Zmianę do osoby lub zespołu realizującego, musi istnieć możliwość powiązania akcji wysłania powiadomienia poprzez system oraz za pomocą e-maila do wskazanej osoby lub zespołu realizującego, z informacją o pojawieniu się nowego Wniosku o Zmianę.
8. Możliwość monitorowania wprowadzania zadań i zmian stanowiących odpowiedź na Wnioski o zmianę, w tym szczegółów wykonawczych oraz terminów realizacji.
9. Możliwość zdefiniowania, jakie Zmiany (na podstawie typów) wymagają akceptacji.
10. Możliwość przekazywania Wniosku o Zmianę do osób pełniących odpowiednie role zdefiniowane w procesie;
11. Możliwość generowania automatycznych powiadomień do uczestników procesu, zróżnicowanych w zależności od pełnionej roli i statusu Wniosku o Zmianę;
12. Możliwość tworzenia Harmonogramu Zmian, który integrowałaby wszystkie kluczowe aktywności procesu Zarządzania Zmianami z uwzględnieniem planowanych przerw wynikających z prac realizowanych w ramach procesu Zarządzania Incydentami;
13. Możliwość ustalanie przeglądów Zmian po definiowalnym okresie od wdrożenia;
14. Możliwość łatwego (zautomatyzowanego) informowania innych procesów o bieżących i planowanych Zmianach;
15. Możliwość załączenia do danej Zmiany dokumentu zawierającego procedury wycofania instalacji;
16. Możliwość zarejestrowania szczegółowych planów w zmianie, planu wdrożenia Zmiany oraz planu cofnięcia Zmiany.
17. Możliwość tworzenia powiązań nadrzędności i podrzędności zadań, Wniosków o Zmianę;
18. Możliwość tworzenia zadań/ zleceń z poziomu Wniosku o Zmianę;
19. Możliwość łatwej identyfikacji Incydentów (i docelowo również Problemów), które wynikły z wprowadzenia danej Zmiany;
20. Możliwość powiązania Zmiany z Incydentami i Problemami;
21. Możliwość zamykania Incydentów (w przyszłości także docelowo Problemów i Znanych Błędów), gdy powiązana z nimi Zmiana zostanie wdrożona. Zamykanie automatyczne powinno się odbywać wyłącznie po akceptacji upoważnionej osoby;
22. Możliwość tworzenia interfejsów do innych procesów, z precyzyjnym określeniem, w jakich czynnościach danych podprocesów istnieje wymiana informacji lub występują czynności zależne;
23. Możliwość dystrybuowania Harmonogramu Zmian do Service Desk-u i Grup Wsparcia;

24. Możliwość dostępu z poziomu formatki Wniosku o Zmianę do szczegółowych danych o Elementach Konfiguracji;
25. Możliwość identyfikacji różnych Wniosków o Zmianę, które odnoszą się do tego samego Elementu Konfiguracji;
26. Możliwość dołączenia załączników do Wniosku o Zmianę w różnych formatach;
27. Możliwość integracji procesu Zarządzania Zmianami z rozwiązaniami do Zarządzania Komponentami Usług i Konfiguracją;
28. Możliwość definiowania ról/osób akceptujących Zmiany danej kategorii (grup Zmian o wspólnej ścieżce obsługi);
29. Możliwość delegowania uprawnień osób akceptujących zmiany;
30. Możliwość wymuszania kolejności wykonywania zaplanowanych zadań w ramach procesu;
31. Możliwość symulowanie wpływu niedostępności Elementu Konfiguracji na inne Elementy Konfiguracji, w tym usługi zdefiniowane w bazie CMDB (ang. *Configuration Management Data Base*), w postaci graficznej – diagram zależności;

3.6. Proces Zarządzanie Komponentami Usług i Konfiguracją

3.6.1. Wymagania w zakresie procesu Zarządzania Komponentami Usług i Konfiguracją

1. Potrzeba budowy docelowego mechanizmu, który umożliwiałby obserwację: Elementów Konfiguracji, ich atrybutów oraz relacji między poszczególnymi elementami – możliwość kompleksowego śledzenia wszelkich pojawiających się zmian;
2. Potrzeba utrzymywania pełniej historii zgłoszeń związanych z poszczególnymi Elementami Konfiguracji;
3. Możliwość przydzielania praw modyfikacji Operatorom IT z dokładnością do poszczególnych atrybutów Elementów Konfiguracji.
4. Możliwość rejestrowania wszystkich Elementów Konfiguracji infrastruktury informatycznej w różnych rodzinach i klasach. Jako rodziny rozumiemy na przykład:
 - Usługa biznesowa z klasami,
 - Usługa techniczna,
 - Aplikacja z klasami: Biznesowa, Narzędziowa, Serwer Aplikacyjny,
 - Baza danych z klasami,
 - Klaster z klasami: Sprzętowy, Aplikacyjny,
 - Partycja z klasami: Wirtualna, Sprzętowa,
 - Serwer z klasami: np. Windows, HP-UX, AIX, Linux,
 - Komputer osobisty z klasami: Stacjonarny, Notebook,
 - Sieć z klasami: Sieć LAN/WAN, Sieć SAN, Switch.
5. Możliwość tworzenia relacji jeden-jeden, jeden-wielu, wiele-wielu na kilku poziomach pomiędzy Elementami Konfiguracji. Poprzez relację rozumiemy:
 - Element Konfiguracji jest komponentem innego Elementu Konfiguracji,
 - Element Konfiguracji wpływa na inny Element Konfiguracji,

- Element Konfiguracji należy do innego Elementu Konfiguracji,
 - Element Konfiguracji zależy od innego Elementu Konfiguracji.
6. Możliwość przeglądu Elementów Konfiguracji i powiązań pomiędzy nimi w postaci graficznej z możliwością filtrowania wyświetlanych informacji (np. po typie relacji);
 7. Możliwość zagnieżdżania Elementów Konfiguracji – Element Konfiguracji traktowany, jako „kontener” zawierający inne Elementy Konfiguracji;
 8. Możliwość śledzenia cyklu życia danego Elementu Konfiguracji – od pojawienia się, przez przesunięcia, modyfikacje danych, serwis i utrzymanie do likwidacji. Dodatkowo musi istnieć dostęp do pełnej historii cyklu życia danego Elementu Konfiguracji (kiedy i kto zmieniał status Elementu Konfiguracji);
 9. Możliwość pozyskania z oferowanego rozwiązania pełnej informacji o aktualnym statusie danego Elementu Konfiguracji;
 10. Dane o Elementach Konfiguracji muszą być dostępne dla Incydentów, Problemów i Wniosków o Zmiany w trybie on-line;
 11. Możliwość łatwego definiowania filtrów dla wszechstronnych przeszukiwań i raportowania;
 12. Baza CMDB musi mieć możliwość definiowania własnych, niestandardowych klas Elementów Konfiguracji;
 13. Baza CMDB musi posiadać mechanizm automatycznego wprowadzania danych pochodzących z różnych źródeł (wprowadzanych ręcznie, z narzędzi automatycznego wykrywania infrastruktury);
 14. Baza CMDB musi mieć możliwość definiowania Usług IT, na które składają się elementy technologiczne i logiczne;
 15. Baza CMDB musi posiadać otwarty interfejs umożliwiający korzystanie z zawartych w niej danych przez oprogramowanie zewnętrzne;
 16. System ITSM powinien mieć możliwość zapisywania w logach (dla potrzeb audytowych) wszystkich modyfikacji dokonywanych na elementach konfiguracji;
 17. System ITSM powinien zapewniać powiązanie informacji o Użytkowniku z przypisanymi do niego środkami trwałymi – powiązanie ewidencji księgowej środków trwałych z ewidencją realizowaną przez dział zarządzania licencjami oprogramowaniem i sprzętem informatycznym;
 18. System ITSM musi wspomagać zarządzanie licencjami oprogramowania (Manager Licencji)
 - a. System musi umożliwiać prowadzenie ewidencji posiadanych licencji na oprogramowanie komputerowe.
 - b. System musi pozwalać na ewidencjonowanie licencji o różnych sposobach licencjonowania:
 - Licencjonowanie na urządzenie,
 - Licencjonowanie na serwer,
 - Licencjonowanie licencji dostępowych (CAL),
 - Licencjonowanie licencji zabezpieczonych kluczami sprzętowymi,
 - Licencjonowanie w chmurze (SaaS),
 - Licencjonowanie na użytkownika,

- Licencjonowanie na procesor,
 - Licencjonowanie pakietów.
- c. System musi automatycznie dokonywać analizy zainstalowanych programów komputerowych w porównaniu z licencjami zakupionymi.
- d. System musi posiadać bazę treści umów licencyjnych dla programów komputerowych w ilości minimalnej 5000 szt. i ostatniej dacie aktualizacji nie starszej niż 30 dni.
- e. System musi automatycznie uwzględniać i rozliczać licencje typu Upgrade i Downgrade oraz komponenty programów.
- f. System musi automatycznie uwzględniać i rozliczać licencje w przypadku kiedy oprogramowanie zostało zainstalowane na dwóch komputerach (stacjonarny i przenośny), gdzie użytkownikiem głównym jest ten sam pracownik.
- g. System musi automatycznie uwzględniać i rozliczać licencje na systemy operacyjne w modelu OEM oraz musi być wrażliwy na przypadek kiedy system operacyjny zakupiony został z innym komputerem a zainstalowany na innym. W takim przypadku system musi pokazać nieprawidłowość automatycznie.
- h. System musi być wrażliwy na licencje po terminie i nie powinien ich uwzględniać w analizach rozliczeniowych.
- i. System musi szczegółowo prezentować pozycje rozliczenia licencji w rozbiciu na komputer, ilość instalacji, kopii oprogramowania, przypisanych licencji do komputerów i wykorzystanych licencji.
- j. System musi oferować możliwość tworzenia wielu (bez ograniczeń) różnych rozliczeń licencji np. dla całej firmy, dla określonego działu, dla określonej lokalizacji itp.
19. System ITSM powinien generować identyfikatory sprzętu lub korzystać z identyfikatorów z systemów zewnętrznych (Identyfikatory sprzętu)
20. System ITSM powinien umożliwiać dodawanie, modyfikację i usuwanie informacji o jednostkach organizacyjnych dla różnych poziomów hierarchii;
21. System ITSM powinien umożliwiać definiowanie hierarchii organizacyjnej, tj. powiązania między poszczególnymi jednostkami organizacyjnymi;
22. System ITSM powinien rejestrować dane jednostek organizacyjnych, przynajmniej:
- Nazwa
 - Dane adresowe
 - Dane kontaktowe (telefon, faks, email)
 - Dyrektor/kierownik/naczelnik jednostki
 - Jednostka nadrzędna
23. System powinien umożliwiać wyświetlenie powiązanych informacji dotyczących danej jednostki organizacyjnej, przynajmniej:
- Lista pracowników w jednostce
 - Lista Asset-ów w jednostce
 - Lista jednostek podrzędnych
 - Lista zgłoszonych problemów z jednostki

24. System powinien umożliwiać przypisanie użytkownika do jednej z jednostek organizacyjnych.
25. System powinien umożliwiać wyświetlenie powiązanych informacji dotyczących użytkownika, przynajmniej:
 - Pełna historia kontaktów z użytkownikiem
 - Lista Asset-ów, z których użytkownik korzysta
 - Lista wygenerowanych przez użytkownika zgłoszeń

W kontekście zarządzania zasobami (Asset Management):

26. System powinien pozwalać na dodawanie, modyfikowanie i usuwanie Asset-ów (sprzętu lub oprogramowania), z których korzystają użytkownicy.
27. System powinien pozwalać rejestrować dane Asset-ów, przynajmniej:
 - Nazwa i opis
 - Typ, model, wersja
 - Kod producenta
 - Numer seryjny
 - Numer inwentarzowy
 - Dodatkowy identyfikator
 - Grupa
 - Informacje o gwarancji
 - Informacje o serwisie zewnętrznym
 - Lokalizacja
28. System powinien pozwalać powiązać Asset z użytkownikami, którzy z niego korzystają.
29. System powinien umożliwiać dodawanie i usuwanie dokumentacji dotyczącej Asset-u w formie załączników w dowolnym formacie.
30. System powinien rejestrować dokonywane zmiany lokalizacji Asset-u.
31. System powinien umożliwiać dodawanie informacji o dokonanych naprawach, modyfikacjach, konserwacjach i kosztach tych działań oraz wspierać przechowywanie informacji o historii Asset-u
32. System musi przechowywać informacje o dostępnych częściach zamiennych i sprzęcie zamiennym.
 - system musi umożliwiać wprowadzenie do systemu części zamiennych
 - system musi umożliwiać raportowanie dostępności części zamiennych po grupach
33. System powinien umożliwiać dodawanie, modyfikację i usuwanie informacji o Operatorach IT.
34. System powinien pozwalać rejestrować dane Operatorów IT, przynajmniej:
 - Imię i nazwisko
 - Dane kontaktowe (telefon, faks, email)
 - Jednostka organizacyjna
 - Dodatkowe dane kontaktowe (przynajmniej inny nr telefonu)
 - Informacje dodatkowe (stanowisko, zespół wsparcia, przełożony)
35. System powinien umożliwiać wyświetlenie powiązanych informacji dotyczących Operatorów IT, tj.:
 - Lista zgłoszeń obsługiwanych aktualnie przez Operatora IT

- Lista zgłoszeń obsługiwanych do tej pory przez Operatora IT
 - Pełna historia kontaktów z Operatorem IT
 - Lista zadań do realizacji
 - Lista zrealizowanych zadań
 - Plan pracy Operatora IT
 - Charakterystyka kompetencji Operatora IT
 - Obszar (lista jednostek organizacyjnych i Asset-ów) obsługiwany przez Operatora IT
36. System powinien pozwalać dodawać, modyfikować i usuwać informacje o Grupach Wsparcia. System powinien umożliwiać rejestrowanie danych dot. Grup Wsparcia, przynajmniej:
- Nazwa
 - Lider
 - Członkowie
37. System powinien pozwalać wyświetlić powiązane informacje dotyczące Grupy Wsparcia, przynajmniej:
- Lista wspieranych zasobów
 - Lista członków Grupy Wsparcia
 - Lista zgłoszeń obsługiwanych przez członków Grupy Wsparcia.
 - Lista zadań realizowanych przez członków Grupy Wsparcia.
38. Obszar (lista jednostek organizacyjnych) obsługiwany przez Grupę Wsparcia.
39. System powinien pozwalać dodawać, modyfikować i usuwać informacje o partnerach.
40. System powinien umożliwiać rejestrowanie danych o partnerach handlowych, przynajmniej:
- Nazwa
 - Dane adresowe
 - Dane kontaktowe do serwisu partnera (telefon, faks, email)
 - Dodatkowe adresy i dane kontaktowe (przynajmniej adres magazynu, inny nr telefonu, faksu)
41. System powinien pozwalać wyświetlić powiązane z partnerem informacje, przynajmniej:
- Lista osób kontaktowych partnera
 - Lista zgłoszeń przypisanych do partnera
42. System powinien umożliwiać rejestrowanie danych osób kontaktowych, przynajmniej:
- Imię i nazwisko
 - Dane kontaktowe
 - Informacja dodatkowe (stanowisko, dział, przełożony)
 - Dodatkowe dane kontaktowe (przynajmniej inny nr telefonu, faksu)

3.7. Proces Zarządzanie Poziomem Usług

3.7.1. Wymagania w zakresie procesu Zarządzania Poziomem Usług

1. Możliwość definiowania różnych poziomów świadczonej usługi, przy czym dla każdego rodzaju Usługi IT powinna istnieć możliwość przyporządkowania parametrów danego rodzaju Usługi IT do konkretnych Umów OLA i UC;
2. Możliwość definiowania parametrów dla poziomu Usługi IT, w tym przynajmniej:
 - a. czas Reakcji,
 - b. czas Rozwiązania,
 - c. dostępność Usługi IT;
3. Możliwość sprawnego zarządzania całym cyklem życia Usługi, pozwalająca na precyzyjne określenie czasów zdefiniowanych w umowach SLA z uwzględnieniem uzasadnionych przestoju w realizacji zgłoszeń
4. Możliwość dodawania, modyfikacji i usuwania umów:
 - a. umowa z odbiorcą usług IT (Umowa SLA),
 - b. umowa między jednostkami organizacyjnymi (Umowa OLA),
 - c. umowa serwisowa z partnerem/dostawcą/podwykonawcą (Umowa UC).
5. Możliwość rejestrowania danych umowy z dostawcą zewnętrznym, w tym przynajmniej:
 - a. stron umowy,
 - b. okresu obowiązywania umowy,
 - c. Lista Asset-ów objętych umową
 - d. obowiązujących terminów realizacji;
 - e. płatności (planowane i zrealizowane),
 - f. informacji dodatkowych (przynajmniej kary umowne, informacje finansowe, automatyczne przedłużanie umowy),
 - g. kar za niedotrzymanie umowy;
6. Wspomaganie przestrzegania ustalonych w umowach reżimów czasowych i jakościowych poprzez monitorowanie;
7. Możliwość tworzenia dowolnej liczby kalendarzy czasu pracy np.:
 - a. pn-pt od 7:00 do 15:00,
 - b. pn-sob od 7:00 do 19:00,
 - c. 24 x 7,
 - d. inne dowolne godziny pracy w tygodniu;
8. Możliwość tworzenia wyjątków w kalendarzach pracy w postaci definiowania świąt i dni wolnych od pracy samodzielnie przez Administratora Systemu;
9. Możliwość monitorowania parametrów na podstawie wskaźników wyznaczonych dla innych systemów (np. czas odpowiedzi aplikacji, dostępność i wydajność usług infrastruktury IT);
10. Możliwość zdefiniowania dowolnej ścieżki przypomnień/powiadomień i eskalacji:
 - a. wysłanie wiadomości do wybranej osoby, grupy,
 - b. wykonanie modyfikacji obiektu np. – zapalenie flagi informującej, że nastąpiła eskalacja hierarchiczna, przepisanie zgłoszenia do innej grupy, uruchomienie zewnętrznej aplikacji;

11. Możliwość uruchamiania przypomnień/powiadomień i eskalacji w zadanym etapie czasu, jaki jest do dyspozycji, wyrażając procentowo czas, po jakim ma być uruchamiana eskalacja wraz ze wskazaniem medium, jakim powinny zostać wysłane powiadomienia (email, sms, alarm wywołujący „ręczną” obsługę telefoniczną przez Operatorów IT w I linii Wsparcia - Service Desk);
12. Możliwość kontroli wskaźników jakości Usług IT opisanych w Umowach SLA związanych z procentową dostępnością Usług IT lub Elementów Konfiguracji;
13. Możliwość zdefiniowania formularzy dla wzorca Karty Usługi;
14. Możliwość definiowania filtrów dla przeszukiwania i raportowania;
15. Możliwość definiowania i edycji statusów Usług IT;
16. Możliwość powiązania warunków oferowanych w Katalogu Usług z warunkami Umów SLA.
17. Możliwość budowania i przeglądania graficznego modelu usługi.
18. Możliwość graficznej reprezentacji osiągniętych poziomów usługi.
19. Możliwość wizualizacji poprawności lub nie pracy danego elementu usługi i propagowania się wpływu danego elementu na funkcjonowanie innych elementów.

3.8. Proces Zarządzanie Bazą Wiedzy

3.8.1. Wymagania w zakresie procesu Zarządzania Bazą Wiedzy

1. System musi umożliwiać obsługę wpisów oraz dostęp do Bazy Wiedzy za pomocą interfejsu WWW.
2. System musi umożliwiać dostęp do Bazy Wiedzy oraz wyszukiwanie informacji dla Operatorów IT w poszczególnych Grupach Wsparcia pracujących nad rozwiązaniem danego Incydentu.
3. System musi umożliwiać dostęp do Bazy Wiedzy oraz wyszukiwanie informacji dla Operatorów IT w poszczególnych Grupach Wsparcia pracujących nad rozwiązaniem Problemu czy Znanego Błędu.
4. Rozwiązanie musi zapewnić możliwość tworzenia wpisów do Bazy Wiedzy na podstawie bieżących Zgłoszeń.
5. Rozwiązanie musi zapewnić możliwość tworzenia wpisów do Bazy Wiedzy na podstawie Problemów, a w szczególności wpisywania Obejść znalezionych podczas rozwiązywania Problemu.
6. Baza Wiedzy musi posiadać mechanizm umożliwiający Zarządzającemu Bazą Wiedzy akceptację nowych i zmienionych wpisów.
7. Baza Wiedzy musi posiadać mechanizm definiowania grupy Operatorów IT oraz użytkowników, dla których dany wpis ma być dostępny.
8. Baza Wiedzy musi posiadać mechanizmy zaawansowanego wyszukiwania wpisów po słowach kluczowych i z wykorzystaniem kategorii wpisów.
9. Baza Wiedzy musi umożliwiać Zarządzającemu Bazą Wiedzy definiowanie kategorii i obszarów wiedzy.
10. Baza Wiedzy musi umożliwiać Zarządzającemu Bazą Wiedzy definiowanie ról w narzędziu oraz przypisywanie do zdefiniowanych ról kont Użytkowników.

11. Proponowane rozwiązanie musi inteligentnie pozycjonować wyniki przeszukania Bazy Wiedzy prezentując wyniki najbardziej trafne, jako pierwsze.
12. System musi udostępniać Zarządzającemu Bazą Wiedzy narzędzie do przeglądania dokumentów z Bazy Wiedzy oczekujących na akceptację.
13. Musi istnieć możliwość dołączania załączników (np. dokumenty, zdjęcia, rysunki, linki do stron www) do tworzonych dokumentów w Bazie Wiedzy.
14. System musi umożliwiać zliczanie liczby odwiedzin dla poszczególnych artykułów.
15. System musi umożliwiać dokonywanie oceny przydatności danego artykułu przez czytelnika.
16. System musi umożliwiać Zarządzającemu Bazą Wiedzy przeglądanie autorów artykułów pod kątem liczby artykułów oraz ocen przydatności.
17. System musi umożliwiać zarządzanie czasem życia artykułów.
18. Baza Wiedzy musi posiadać mechanizmy wyszukiwania pełno tekstowego, po słowach kluczowych (Tag-ach) oraz przypisanych do artykułu kategoriach.

4. Wymagania na mierzenie i raportowanie Usług

Należy zwrócić uwagę na kilka kluczowych obszarów podczas budowy docelowego mechanizmu raportowania:

1. System ITSM musi udostępniać możliwość samodzielnego budowania raportów w oparciu o bieżące potrzeby Zamawiającego.
2. Narzędzie ITSM musi udostępniać graficzne narzędzie do projektowania raportów.
3. System ITSM musi posiadać mechanizm do uruchamiania raportów na bazie zadanego harmonogramu i przesyłania wyników pocztą elektroniczną, a także możliwość exportu do pliku xls, csv bez wysyłania pocztą elektroniczną.
4. Narzędzie ITSM powinien posiadać możliwości zabezpieczające przed uruchomieniem raportów zwracających za dużą liczbę rekordów, możliwość konfiguracji wartości progowej i ewentualnie włączenie generowania raportu z dużą liczbą rekordów po powtórnym zaakceptowaniu ostrzeżenia.
5. System ITSM musi posiadać możliwości definiowania prostych raportów ad-hoc przez użytkowników końcowych z możliwością ich zapisania do kolejnego użycia. Raportowanie ad-hoc powinno umożliwiać wybór danych tworzących kolumny raportu, kolumny do grupowania i sortowania.
6. System ITSM powinien posiadać wbudowaną funkcjonalność graficznego prezentowania wybranych metryk. Uprawnieni Operatorzy IT powinni mieć możliwość definiowania własnych metryk.
7. Narzędzie ITSM powinno mieć możliwość definiowania graficznej reprezentacji zestawu danych, wykresy kołowe, kolumnowe, słupkowe itp..
8. System ITSM powinien udostępniać narzędzia typu drill-down, umożliwiające dokładną analizę przedstawianych wykresów graficznych.
9. System ITSM powinien posiadać możliwość definiowania dashboardów dla użytkowników i umieszczania na nich zestawień, metryk oraz graficznych reprezentacji wybranych danych, które to będą udostępniane na stronie SelfService. Powinna być możliwość tworzenia osobnych dashboardów dla grup np. menadżerów danego poziomu, dla pracowników danego poziomu, dla dyrektorów, dowolna personalizacja. Każdy pracownik na swoim dashboardzie musi mieć dostęp do informacji o przypisanym do niego sprzęcie z zasobów IT.
10. Narzędzie ITSM powinno umożliwiać definiowanie uprawnień do raportów.
11. Narzędzie ITSM musi zawierać bazowo zdefiniowane raporty jak i musi mieć możliwość definiowania dodatkowych raportów, w zależności od potrzeb po stronie PAŻP

4.1. Zarządzanie Incydentami

Zestawienie raportów wspierających osoby odpowiedzialne za realizację procesu:

1. Liczba Incydentów zgłoszonych w danym okresie czasu;
2. Liczba Incydentów zamkniętych w danym okresie czasu;
3. Liczba Incydentów rozwiązanych w zadeklarowanych czasach realizacji w podziale na poszczególnych Operatorów IT;

4. Liczba Incydentów z przekroczeniami czasów realizacji uwzględniająca wszelkie przestoje przy realizacji zgłoszeń;
5. Liczba Incydentów rozwiązanych przez poszczególnych Operatorów IT;
6. Liczba reklamacji zgłoszonych przez Użytkowników dotyczących rozwiązania Incydentów. Przez reklamację rozumie się zgłoszenie przez Użytkownika zastrzeżeń do jakości przedstawionego rozwiązania i brak akceptacji dla zamknięcia Incydu, w określonym przedziale czasowym od zakończenia Incydu np. 48h. Oznacza to w praktyce potrzebę dalszych prac nad zgłoszeniem do czasu przygotowania rozwiązania, które satysfakcjonuje Użytkownika i zostanie przez niego zaakceptowane;
7. Liczba Incydentów zgłoszonych w danym okresie czasu w podziale na poszczególne Usługi IT;
8. Liczba Incydentów zgłoszonych w danym okresie czasu w podziale na poszczególne Elementy Konfiguracji.
9. Procentowa ilość zgłoszeń zrealizowanych w terminie podziale na kategorie/typy i priorytety
10. Procentowa ilość zgłoszeń rozwiązanych przez Operatorów Service Desk
11. Procentowa ilość zgłoszeń skategoryzowanych nieprawidłowo
12. Średni czas potrzebny na realizację zgłoszenia w podziale na kategorie/typy i priorytety
13. Procent oraz ilość reklamacji w raportowanym okresie.

4.2. Funkcja Service Desk

Zestawienie raportów wspierających osoby odpowiedzialne za realizację procesu:

1. Liczba i historia zgłoszeń w podziale na:
 - a. Całkowitą liczbę zgłoszeń,
 - b. Zgłoszenia o danym statusie,
 - c. Zgłoszenia według kategorii,
 - d. Zgłoszenia podjęte przez poszczególnych Operatorów IT w Service Desk,
 - e. Zgłoszenia w podziale na medium, za pomocą którego dokonano zgłoszenie.
2. Liczba zgłoszeń w danym okresie czasu z podziałem na kategorię zgłoszenia.
3. Średni czas rozwiązania zgłoszeń w danym okresie w podziale na Operatorów IT rozwiązujących.
4. Liczba reklamacji zgłoszonych przez Użytkowników.
5. Liczba i historia zgłoszeń rozwiązanych w zdefiniowanych w Umowach parametrach:
 - a. Zgłoszenia z prezentacją poszczególnych progów kontrolnych,
 - b. Zgłoszenia w zadanym okresie,
 - c. Zgłoszenia rozwiązane,
 - d. Zgłoszenia zamknięte,
 - e. Zgłoszenia w podziale na Operatorów IT rozwiązujących zgłoszenie z prezentacją czasu rozwiązania,

- f. Zgłoszenia w podziale na Operatorów IT rejestrujących zgłoszenie z prezentacją czasu reakcji.
6. Liczba i historia zgłoszeń o przekroczonych parametrach zdefiniowanych w Umowach:
 - a. Zgłoszenia z prezentacją poszczególnych progów kontrolnych,
 - b. Zgłoszenia w zadanym okresie,
 - c. Zgłoszenia rozwiązane,
 - d. Zgłoszenia zamknięte,
 - e. Zgłoszenia w podziale na Operatorów IT rozwiązujących zgłoszenie z prezentacją czasu rozwiązania, Zgłoszenia w podziale na Operatorów IT rejestrujących zgłoszenie z prezentacją czasu reakcji.

4.3. Zarządzanie Zmianami

Zestawienie raportów wspierających osoby odpowiedzialne za realizację procesu:

1. Liczba Wniosków o Zmianę zarejestrowanych w danym okresie czasu (standardowo raportowane miesięcznie).
2. Liczba Wniosków o Zmianę zamkniętych w danym okresie czasu (standardowo raportowane miesięcznie).
3. Liczba Wniosków o Zmianę w danym okresie czasu (standardowo raportowane miesięcznie) w podziale na poszczególne statusy jego obsługi.
4. Liczba Wniosków o Zmianę w podziale na poszczególne Usługi IT.
5. Ilość zmian powiązanych z Bura Informatyki (procentowo, w stosunku do wszystkich zmian) zamkniętych w danym okresie czasu.
6. Ilość zrealizowanych z sukcesem zmian (procentowo, w stosunku do wszystkich zmian) zamkniętych w danym okresie czasu.
7. Ilość zrealizowanych z sukcesem zmian standardowych (procentowo, w stosunku do wszystkich zrealizowanych z sukcesem zmian) zamkniętych w danym okresie czasu.
8. Ilość zrealizowanych z sukcesem i w terminie zmian (procentowo, w stosunku do wszystkich zrealizowanych z sukcesem zmian) zamkniętych w danym okresie czasu.
9. Ilość niezatwierdzonych zmian (procentowo, w stosunku do wszystkich zaakceptowanych zmian, które zostały zrealizowane) zamkniętych w danym okresie czasu.

4.4. Zarządzanie Poziomem Usług

Zestawienie raportów wspierających osoby odpowiedzialne za realizację procesu:

1. Liczba zdefiniowanych Usług IT.
2. Liczba dotrzymanyh i niedotrzymanyh zdefiniowanych parametrów świadczenia Usług IT (liczba przekroczeń celów SLA dla poszczególnej usługi).

4.5. Zarządzanie Komponentami usług i Konfiguracją

Zestawienie raportów wspierających osoby odpowiedzialne za realizację procesu:

1. Lista Elementów Konfiguracji, które uległy zmianie w danym okresie czasu.
2. Procentowa ilość zgłoszeń powiązanych z CI (jednostką konfiguracji) w podziale na kategorie i typy/podtypy/rodzaje.
3. Procentowa ilość zgłoszeń z nieaktualnym CI (jednostką konfiguracji) w podziale na kategorie i typy/podtypy/rodzaje.
4. Ilość wyjątków w bazie CMDB wynikających z przeprowadzonego audytu.
5. Ilość nieautoryzowanych CI w przedsiębiorstwie. Nieautoryzowane CI to taka jednostka konfiguracji, która znajduje się w przedsiębiorstwie, natomiast nie jest zarejestrowana w bazie CMDB.

Załącznik nr 2 - Gwarancja dla Systemu ITSM

1. Wykonawca udzieli Zamawiającemu 36 miesięcznej Gwarancji na System ITSM liczony od daty podpisania Protokołu Odbioru Umowy.
2. Wykonawca w ramach udzielonej Gwarancji udzieli Gwarancji na zmiany w Systemie ITSM wykonane w ramach opieki serwisowej oraz na wszelkie usługi Wykonawcy objęte Umową i produkty powstałe w wyniku jej realizacji.
3. W ramach Gwarancji Wykonawca będzie zobowiązany do:
 - a. Usuwania Wad Systemu ITSM:
 - i. Awarie
 - Czas Reakcji: 2 godziny zegarowe
 - Czas Naprawy: 24 godziny zegarowe
 - Czas przyjmowania zgłoszeń: 7 dni w tygodniu, 24 godziny na dobę,
 - ii. Błędy Krytyczne
 - Czas Reakcji: 4 godziny zegarowe,
 - Czas Naprawy: 48 godziny zegarowe,
 - Czas przyjmowania zgłoszeń: 7 dni w tygodniu, 24 godziny na dobę,
 - iii. Błędy Niekrytyczne
 - Czas Reakcji: 8 Godzin Roboczych,
 - Czas Naprawy/Obejścia: 7 dni kalendarzowych, czas naprawy w przypadku zastosowania Obejścia 30 dni kalendarzowych,
 - Czas przyjmowania zgłoszeń: 7 dni w tygodniu, 24 godziny na dobę.
 - b. Dostarczania, nie rzadziej niż raz na 3 miesiące, wykazu rekomendowanych wersji Oprogramowania Pozostałego zapewniającego prawidłowe działanie Systemu ITSM.

**Załącznik nr 3 – Formularz wyceny**

LP	Element wyceny	Cena netto w PLN	UWAGI
1	Projekt wdrożenia systemu ITSM		
2	Przygotowanie procesów i usług		
3	Licencje jednoczesne operatora IT		
4	Licencje nazwane operatora IT		
5	Dokupienie 1 szt. Licencji jednoczesnej Operatora IT		
6	Dokupienie 1 szt. Licencji nazwanej Operatora IT		
7	Usługa maintenance na okres 36 miesięcy		
8	Usługa wdrożenia systemu		