Lp WKR	Typ	Opis
1.1	Administracja - ogólne	System ITSM musi umożliwiać definiowanie nowych oraz modyfikowanie istniejących przepływów pracy (ang. workflow) dla wszystkich implementowanych procesów przy użyciu interfejsu graficznego działające na zasadzie przeciągnij i upuść oraz zaawansowanych narzędzi przy czym modyfikacja musi być możliwa do realizacji przez Użytkownika Systemu z odpowiednim poziomem uprawnień.
1.2	Administracja - ogólne	System ITSM musi umożliwić tworzenie klonów istniejących workflow ich wersjonowanie oraz dynamiczne podmienianie z poziomu konsoli Użytkownika Systemu z odpowiednim poziomem uprawnień.
1.3	Administracja - ogólne	System ITSM musi umożliwiać Administratorowi definiowanie i klonowanie nieograniczonej liczby kompletnych: 1) przepływów pracy (ang. workflow) dla wszystkich implementowanych procesów, 2) formularzy (formatek),
1.4	Administracja - ogólne	System ITSM musi umożliwiać Administratorowi definiowanie i klonowanie nieograniczonej liczby kompletnych grup Operatorów i Użytkowników.
1.5	Administracja - ogólne	System ITSM musi umożliwiać automatyczne przypisywanie Incydentu, Wniosku o usługę, Zmiany, Problemu, Wydania do określonego Operatora lub grupy Operatorów, na podstawie zdefiniowanych przez Administratora kryteriów.
1.6	Administracja - ogólne	System ITSM musi umożliwiać automatyczną realizację rekordów spełniających kryteria definiowane w workflow przez Administratora.
1.7	Administracja - ogólne	System ITSM musi umożliwiać automatyczne wyznaczanie gwarantowanego czasu realizacji rekordów (Wnioski, Incydenty, Problemy, Zmiany itd..) na podstawie wymagań SLA z możliwością modyfikacji przez Operatora.
1.8	Administracja - ogólne	System ITSM musi umożliwiać konfiguracjeę przepływów pracy w tym pozwalać na zatrzymywanie zegarka SLA/OLA przy zdefiniowanych warunkach.
1.9	Administracja - ogólne	System ITSM musi umożliwiać przypisanie wielu zadań powiązanych z rekordem/Zgłoszeniem do różnych grup.
1.10	Administracja - ogólne	Automatyzacja Procesów: System ITSM musi umożliwiać automatyzację procesów związanych z zamawianiem i świadczeniem usług, takich jak tworzenie zadań, powiadomienia, aktualizacje statusów.
1.11	Administracja - ogólne	Proces Akceptacji: System ITSM musi umożliwiać definiowanie procesów akceptacji dla zamówień usług, w tym wieloetapowych zatwierdzeń.
1.12	Administracja - ogólne	System ITSM musi umożliwiać Administratorowi definiowanie na podstawie statusu usługi, priorytetu, progów eskalacyjnych, automatycznych powiadomień e-mail wysyłanych do Użytkowników, Operatorów i innych osób i grup, zawierających co najmniej: 1) dowolny tekst, 2) wybrane dane Incydentu, Wniosku o usługę, Problemu, Zmiany, Wydania, elementu konfiguracji, 3) link do Incydentu, Wniosku o usługę, Problemu, Zmiany, Wydania, elementu konfiguracji.
1.13	Administracja - ogólne	System ITSM musi umożliwiać przypisanie adresów email do usług zdefiniowanych w KU, w celu interaktywnej komunikacji z użytkownikiem poprzez wskazany adres email.
1.14	Administracja - ogólne	System ITSM musi umożliwiać Administratorowi konfigurowanie kryteriów automatycznego powiadamiania Operatora poprzez wiadomość e-mail o zdarzeniach w Systemie ITSM, co najmniej o: 1) przypisaniu bądź aktualizacji dla Incydentu, Wniosku o usługę, Zmiany, Problemu, Wydania, Elementu konfiguracji. 2) zagrożeniu przekroczenia oraz o przekroczeniu gwarantowanego czasu rozwiązania, 3) powiadamianie Operatorów o progach eskalacyjnych (np. 25% czasu (data). 50% (data), 75% (data), 100% deadline(data)) wynikających z SLA dla usługi).
1.15	Administracja - ogólne	System ITSM musi zapewniać możliwość wysyłania pojedynczych oraz masowych wiadomości e-mail w formacie TXT, HTML w sposób automatyczny lub manualny (przez Operatora). Sposób wysyłania ww. powiadomień do definiowania przez Administratora.
1.16	Administracja - ogólne	System ITSM musi umożliwiać wysyłanie do Użytkowników automatycznych powiadomień dotyczących zmian statusów Incydentów, Wniosków o Usługę, Zmian (co najmniej faktu zarejestrowania, akceptacji, wstrzymania realizacji oraz faktu rozwiązania Wniosku o usługę) przy czym zawartość powiadomienia oraz warunki wysłania muszą być możliwe do zdefiniowania przez Administratora.
1.17	Administracja - ogólne	System ITSM musi umożliwiać automatyczną eskalację hierarchiczną (pionową w ramach struktury organizacyjnej), według kryteriów konfigurowanych przez Administratora, przy czym kryterium to powinno obejmować co najmniej upływ czasu realizacji rekordu w stosunku do czasu gwarantowanego. Eskalacja powinna polegać na przekazaniu zdefiniowanym osobom lub rolom określonego zakresu informacji o rekordzie przy czym lista osób (ról) i zakres informacji muszą być możliwe do zdefiniowania przez Administratora.
1.18	Administracja - ogólne	System ITSM musi umożliwiać wysyłanie do Użytkowników końcowych automatycznych powiadomień dotyczących zmian statusów na Zgłoszeniu przy czym zawartość powiadomienia oraz warunki wysłania muszą być możliwe do zdefiniowania przez Administratora.
1.19	Administracja - ogólne	System ITSM musi posiadać wewnętrzne mechanizmy archiwizacji rekordów, polegajace na ich migracji na dedykowany serwer/y
1.20	Administracja - ogólne	System musi umożliwiać definiowanie czasu po jakim rekordy zostaną zarchiwizowane.
1.21	Administracja - ogólne	System musi umożliwiać definiowanie dostępu osobom do rekordów zarchiwizowanych.

1.22	Administracja - ogólne	System ITSM musi zachowywać ciągłość numeracji wszystkich rekordów a) z zachowaniem informacji co się zadziało z rekordem jeśli ostatecznie nie został utworzony (np. jeśli Incydent nie został zapisany to w logach będzie możliwość weryfikacji dlaczego wpis tego Incydentu nie widnieje na liście) lub b) System ITSM nadaje numer rekordu dopiero po jego zapisaniu w systemie.
1.23	Administracja - ogólne	System ITSM musi umożliwiać Operatorowi łączenie (tworzenie zależności i relacji) pomiędzy rekordami (Incydentami, Wnioskami o usługę, Problemami, Zmianami, Wydaniami, Elementami konfiguracji itd.) w dowolnym momencie po ich zarejestrowaniu, przy czym powinien istnieć mechanizm ułatwiający wyszukiwanie oraz łączenie.
1.24	Administracja - ogólne	System ITSM musi umożliwiać Operatorowi bezpośrednie przechodzenie pomiędzy Incydentami, Wnioskami o usługę, Problemami, Zmianami, Wydaniami, elementami konfiguracji połączonymi w relacje.
1.25	Administracja - ogólne	System ITSM musi umożliwiać stosowanie kodów rozwiązania (kategorii rozwiązania dostarczającej informację do analizy w celach zarządczych, np. rozwiązany, odrzucony, obejście) dla Incydentów, Wniosków o usługę, Problemów oraz Zmian, przy czym musi istnieć możliwość konfigurowania kodów rozwiązania przez Administratora.
1.26	Administracja - ogólne	System ITSM musi umożliwiać Administratorowi graficzne definiowanie nowych formularzy, ich modyfikowanie i duplikowanie. Budowa formularza powinna odbywać się na zasadzie przeciągnij i upuść. System ITSM musi umożliwiać oznaczanie, które formularze i ich elementy są widoczne, edytowalne i/lub obowiązkowe dla zdefiniowanych ról. (np. Incydent Manager może edytować priorytet niezależnie od statusu incydentu, a inne role nie mogą go edytować w innym statusie niż "nowe")
1.27	Administracja - ogólne	System ITSM musi umożliwiać automatyczne zarządzanie zawartością pól formularza na podstawie informacji z Systemu ITSM np. automatyczne uzupełnienie informacji o przypisanym sprzęcie, licencjach Zgłaszającego, przy czym reguły wypełniania pól muszą być możliwe do definiowania przez Administratora.
1.28	Administracja - ogólne	System ITSM musi umożliwiać grupowanie rekordów, wykonywanie operacji masowych na tych rekordach w Systemie ITSM (przynajmniej w zakresie Incydentów, Wniosków o usługę, Elementów konfiguracji, Użytkowników) oraz nawigowanie między nimi z poziomu widoku Operatora i Administratora.
1.29	Administracja - ogólne	System ITSM musi umożliwiać Operatorom lub zdefiniowanym rolom, definiowanie przypomnień dotyczących Incydentów, Wniosków o usługę, Problemów, Zmian, Wydań. (np. dodanie flagi do rekordu, komunikat systemowy)
1.30	Administracja - ogólne	System ITSM musi mieć możliwość nadawania przez Administratora Operatorom, Użytkownikom uprawnień do wykonywania różnych akcji zdefiniowanych przez Administratora opierających się o modyfikacje parametrów, atrybutów i ich odczyt, dodawanie i usuwanie zapisów, w ramach Incydentów, Wniosków o usługę, Problemów, Zmian, Wydań, bazy konfiguracji (CMDB).
1.31	Administracja - ogólne	System ITSM musi umożliwiać Użytkownikowi i Operatorowi dołączanie do rekordów załączników w postaci plików zewnętrznych (co najmniej formaty PDF, DOC, DOCX, XLS, XLSX, GIF, JPG, BMP, TXT, PPT, PPTX, ZIP).
1.32	Administracja - ogólne	System ITSM musi umożliwiać rejestrację Incydentów, Wniosków o usługę, Problemów, Zmian poprzez następujące kanały: 1) automatycznie poprzez e-mail, 2) ręcznie przez Operatora, 3) ręcznie przez zgłaszającego poprzez Portal użytkownika, 4) System/moduł SAM/HAM 5) automatycznie na podstawie informacji z innego systemu zewnętrznego np. z systemu monitoringu, CMP, etc. 6) automatyczne powiadomienia/alert z modułu zarządzania zdarzeniami,
1.33	Administracja - ogólne	System ITSM musi umożliwiać stosowanie kodów typów objawów (ang. symptom types) w klasyfikacji zgłoszeń, dostarczających informacje służące do identyfikacji potencjalnych przyczyn wystąpienia zdarzenia lub problemu do analizy przyczyn źródłowych (ang. Root cause analysis RCA) , przy czym musi istnieć możliwość konfigurowania kodów typów objawów przez Administratora.
1.34	Administracja - ogólne	System ITSM powinien umożliwiać wczytanie z pliku np. pliku płaskiego: Incydentów, Wniosków o usługę, Problemów, Zmian, Elementów konfiguracji, Użytkowników.
1.35	Administracja - ogólne	System ITSM musi posiadać możliwość tworzenia nowych rekordów poprzez duplikacje istniejących.
1.36	Administracja - ogólne	System ITSM musi umożliwiać operacje masowe na rekordach (relacjonowanie, zmiana grupy odpowiedzialnej etc.)
1.37	Administracja - ogólne	System ITSM musi umożliwiać jednoczesny dostęp do danych wielu Użytkownikom, z zapewnieniem integralności danych wynikających z ich działań. Rekord w Systemie ITSM edytowany przez jedną osobę w czasie rzeczywistym blokuje możliwość edycji dla innych osób z wyświetleniem personalizowanego komunikatu lub pola zmodyfikowane na rekordzie w trakcie edycji przez innego użytownika są odpowiednio zaznaczone w czasie rzeczywistym. Dodatkowo wszelkie zmiany pojawiają się w czasie rzeczywistym w dzenniku aktywności widocznym bezpośrednio na rekordzie
1.38	Administracja - ogólne	System ITSM musi umożliwiać jednoczesne zamykanie wszystkich podrzędnych Zgłoszeń poprzez zamknięcie Zgłoszenia nadrzędnego.
1.39	Administracja - Bezpieczeństwo	System ITSM musi umożliwiać wydzielenie wszystkich informacji w zakresie zdefiniowanej jednostki organizacyjnej, zapewniając pełną izolację danych, kont oraz personalizacje paneli Użytkowników w podziale na Klientów (multi-Tenant).

1.40	Administracja - ogólne	System ITSM powinien dawać Operatorom możliwość dostosowywania/modyfikacji layout'u/dashboardu/portletu etc. bez konieczności angażowania Administratora systemu.
1.41	Administracja - ogólne	System ITSM musi posiadać w standardzie realizację wszystkich zadań przypisanych do Administratora w GUI bez zmian kodu źródłowego i prac programistycznych.
1.42	Administracja - ogólne	System ITSM musi zapewniać możliwość tworzenia kalendarzy dostępności Operatorów oraz możliwość definiowania zastępstw, aby w przypadku skierowania Incydentu, Wniosku o usługę, Problemu, Zmiany, Wydania lub powiązanych zleceń do osoby niedostępnej, sygnalizowana była niedostępność takiej osoby lub następowało automatyczne przekierowanie do osoby zastępującej lub możliwość wskazania grupy i masowe przepięcie ww. obiektów na grupę.
1.43	Administracja - ogólne	System ITSM musi zapewniać mechanizmy pozwalające na centralne zarządzanie kontami oraz uprawnieniami Administratorów, Operatorów, Użytkowników.
1.44	Administracja - ogólne	System ITSM musi umożliwiać tworzenie przez Administratora grup Administratorów, Operatorów, Użytkowników niezależnych od struktury organizacyjnej
1.45	Administracja - ogólne	System ITSM musi mieć możliwość nadawania przez Administratora Operatorom, Użytkownikom uprawnień do widoczności danych, przeglądania danych bez możliwości ich modyfikacji.
1.46	Administracja - ogólne	System ITSM musi zapewniać definiowanie wielopoziomowej struktury organizacyjnej ręcznie oraz poprzez import danych w odpowiednim formacie, dla Operatorów i Użytkowników. System ITSM musi umożliwiać odczytywanie i odtwarzanie struktury organizacyjnej na podstawie danych pochodzących z systemów zewnętrznych np. Active Directory.
1.47	Administracja - ogólne	System ITSM musi umożliwiać definiowanie przez Administratora uprawnień i przypisanie ich do użytkowników lub grup użytkowników.
1.48	Administracja - ogólne	System ITSM musi posiadać możliwość zarządzania przez Operatorów tabelami rekordów (np. listą Incydentów, Zmian itd.) tj. możliwość ukrywania i odkrywania kolumn, możliwość sortowania danych w tabeli po wskazanej kolumnie, możliwość filtrowania danych po każdej kolumnie, możliwość eksportu danych do pliku XLSX.
1.49	Administracja - Bezpieczeństwo	System ITSM musi zapewniać stosowanie mechanizmów uwierzytelniania Administratorów, Operatorów, Użytkowników. Logowanie SSO z dodatkowym zabezpieczeniem 2FA (MS Authenticator)
1.50	Administracja - Bezpieczeństwo	System ITSM musi zapewniać możliwość ustawienia przez Administratora ilości i długości czasu trwania sesji, po której System ITSM samoczynnie wyloguje bezczynnego Administratora, Operatora, Użytkownika.
1.51	Administracja - ogólne	System ITSM musi zapewniać rejestrację i śledzenie historii dokonywanych modyfikacji i zapisów w Systemie ITSM, ze wskazaniem osób dokonujących modyfikacji oraz dat i godzin modyfikacji dla Użytkowników posiadających odpowiednie uprawnienia.
1.52	Administracja - ogólne	System ITSM musi umożliwiać Operatorom wyszukiwanie Incydentów, Wniosków o usługę, Problemów, Zmian, Wydań, Elementów konfiguracji, usług, użytkowników, informacji w repozytorium wiedzy przy użyciu słów kluczowych, ciągów znaków w tym niepełnych wyrazów, fragmentów tekstu z użyciem operatorów logicznych (I, LUB, ORAZ).
1.53	Administracja - ogólne	System ITSM musi umożliwiać automatyczne zarejestrowanie Użytkownika na podstawie informacji z wiadomości e-mail oraz innych zintegrowanych systemów.
1.54	Administracja - ogólne	System ITSM musi umożliwiać przeprowadzenie badań satysfakcji poprzez udostępnienie Użytkownikom ankiety zawierającej pytania i pola umożliwiające umieszczenie lub wybranie odpowiedzi. Ankiety muszą być możliwe do konfigurowania przez Administratora i uruchamiane z poziomu dowolnego obiektu w Systemie ITSM (Incydent, Wniosek o usługę, Problem, Zmiana, Usługa, Użytkownik, lub jednostka organizacyjna Użytkownika)
1.55	Administracja - ogólne	System ITSM musi wspierać procesy zgodnie ITIL 3 lub wyższym, które System ITSM musi wspierać, podlegają zakupowi i wdrożeniu: : 1) Zarządzanie Zasobami i Konfiguracją, 2) Zarządzanie Incydentami, 3) Zarządzanie Zmianą, 4) Zarządzanie Poziomem Świadczenia Usługi, 5) Zarządzanie Katalogiem Usług, 6) Realizacja Wniosków, 7) Zarządzanie Zdarzeniami, 8) Zarządzanie Ciągłością, 9)Zarządzanie Ryzykiem 10)Zarządzanie Dostawcami (Umowami) 11) Zarządzanie Licencjami, Procesy zgodne z ITIL 3 lub wyższym, które System ITSM musi wspierać ale nie podlegają zakupowi i wdrożeniu: 12) Zarządzanie Problemami, 13) Zarządzanie Dostępnością, 14) Zarządzanie Pojemnością 15) Zarządzanie Wiedzą. 16) Zarządzanie Wydaniami i Wdrożeniami,
1.56	Administracja - ogólne	System ITSM musi pozwalać na jednoznaczną identyfikacje i raportowanie grup wsparcia odpowiedzialnych za przekroczenia SLA na poszczególnych rekordach
1.57	Administracja - ogólne	System ITSM musi umożliwiać blokowanie zamknięcia rekordu w sytuacji, gdy pozostają otwarte zlecenia związane z danym rekordem oraz pozostają niewypełnione wymagane pola informacyjne rekordu.

1.58	Administracja - ogólne	System ITSM powinien posiadać funkcjonalność pobierania danych (np. numeru telefonu) z narzędzia call center i rozpoczęcie rejestracji Zgłoszenia podstawiając odpowiedniego użytkownika (np. na podstawie nr. tel)
1.59	Administracja - ogólne	System ITSM musi umożliwiać wyszukanie Wniosku o usługę, Incydentu po Operatorze, który go utworzył.
1.60	Administracja - ogólne	System ITSM musi umożliwiać wstrzymanie (zamrożenie) naliczania czasów SLA w rekordach (np. Incydentów, Wniosków o usługę, Zmian) i powiązanych z nimi obiektach/rekordach w sposób bezpośredni przez Operatora lub pośrednio na podstawie ustawionego statusu, przy czym zapewniona musi być automatyczna aktualizacja gwarantowanego czasu rozwiązania.
1.61	Administracja - ogólne	System ITSM powinien umożliwiać komunikację ze Zgłaszającym z możliwością wstrzymania czasu SLA na rekordzie i automatycznego wznowienia po otrzymaniu komunikacji zwrotnej. (np. wysłanie pytania powoduje zmianę statusu rekordu na stop SLA i po odpowiedzi wznowienie SLA)
1.62	Administracja - ogólne	System ITSM musi umożliwiać kierowanie zleceń pracy dla Incydentów, Wniosków o usługę, Problemów oraz Zmian do osób i grup opiniujących ze zdefiniowanym czasem realizacji.
1.63	Administracja - ogólne	System ITSM musi zapewniać graficzny widok zależności w celu identyfikacji które usługi są dotknięte przez Incydent
1.64	Administracja - Infrastruktura	System ITSM musi posiadać możliwość budowy kopii środowiska produkcyjnego 1:1 (test dev)
1.65	Administracja - Infrastruktura	System ITSM musi umożliwiać odtworzenie środowiska test dev na podstawie środowiska produkcyjnego
1.66	Administracja - Infrastruktura	System ITSM powinien składać się z trzech niezależnych środowisk: produkcyjne, testowe, developerskie.
1.67	Realizacja Wniosków o usługę	System ITSM musi posiadać gotowy formularz Wniosku o usługę (SR)z możliwością modyfikacji layout'u oraz pól przez Operatora obsługującego Zarządzanie Wnioskami.
1.68	Realizacja Wniosków o usługę	Zgłaszanie wniosków: System ITSM powinien umożliwiać zgłaszanie wniosków poprzez różne kanały, takie jak Portal Użytkownika, e-mail czy przez Operatora.
1.69	Realizacja Wniosków o usługę	Przypisywanie wniosków: System ITSM powinien umożliwiać automatyczne przypisywanie wniosków do odpowiednich osób/grup wsparcia na podstawie warunków definiowanych w workflow.
1.70	Realizacja Wniosków o usługę	Ocena poziomu usług: System ITSM powinien umożliwiać zbieranie opinii i ocen od użytkowników na temat jakości i satysfakcji z realizacji wniosku.
1.71	Realizacja Wniosków o usługę	Automatyczne odpowiedzi i powiadomienia: Wymaganie dotyczące automatycznej odpowiedzi na wniosek oraz wysyłania powiadomień o postępie jego rozwiązania.
1.72	Realizacja Wniosków o usługę	System ITSM powinien umożliwiać przypisywanie wnioskom w zależności od ich rodzaju odpowiednich czasów SLA i OLA.
1.73	Realizacja Wniosków o usługę	Historia wniosków: Wymaganie dotyczące prowadzenia historii wszystkich wniosków, wraz z informacjami na temat ich statusu, czasu rozwiązania i innych szczegółów.
1.74	Realizacja Wniosków o usługę	Monitorowanie czasu reakcji: System ITSM powinien umożliwiać monitorowanie czasu SLA i OLA oraz identyfikację opóźnień w ich obsłudze.
1.75	Realizacja Wniosków o usługę	SLA dla realizacji usług: Wymaganie dotyczące definiowania i zarządzania SLA dla procesu realizacji wniosków, określających oczekiwane czasy reakcji i rozwiązania.
1.76	Realizacja Wniosków o usługę	Umożliwienie użytkownikom zgłaszania wielu wniosków w ramach jednego formularza, co po złożeniu automatycznie wygeneruje oddzielne wnioski dla każdej zgłoszonej usługi lub sprawy (rozszycie zgłoszenia masowego na pojedyncze wnioski)
1.77	Realizacja Wniosków o usługę	Raportowanie i analiza danych: Wymaganie dotyczące generowania raportów i analizy danych dotyczących obsługi wniosków w celu identyfikacji trendów, obszarów wymagających ulepszeń i oceny efektywności procesu zarządzania realizacją.
1.78	Zarządzanie Incydentami	System ITSM musi posiadać gotowy formularz Incydentu z możliwością modyfikacji layout'u oraz pól przez Operatora obsługującego Zarządzanie Incydentami.
1.79	Zarządzanie Incydentami	Rejestracja Incydentów: System ITSM musi umożliwiać rejestrację incydentów poprzez różne kanały: e-mail, portal użytkownika, przez Operatora, automatycznie na podstawie monitoringu systemów zewnętrznych.
1.80	Zarządzanie Incydentami	Kategoryzacja i Priorytetyzacja: System ITSM musi umożliwiać kategoryzację i priorytetyzację incydentów zgodnie z modelem ITIL v4, bazując na pilności i wpływie, z możliwością ręcznej modyfikacji przez Operatora.
1.81	Zarządzanie Incydentami	Automatyczne Powiadomienia: System ITSM musi umożliwiać automatyczne wysyłanie powiadomień e-mail o zmianach statusu incydentu, przypisania do operatora, zagrożeniach przekroczenia SLA.
1.82	Zarządzanie Incydentami	Przypisywanie Incydentów: System ITSM musi umożliwiać automatyczne przypisywanie incydentów do odpowiednich operatorów lub grup na podstawie zdefiniowanych kryteriów.
1.83	Zarządzanie Incydentami	Eskalacja: System ITSM musi wspierać eskalację funkcjonalną i hierarchiczną incydentów, w oparciu o konfigurowalne kryteria, takie jak czas realizacji w stosunku do SLA.
1.84	Zarządzanie Incydentami	Śledzenie Incydentów: System ITSM musi umożliwiać operatorom śledzenie incydentu od momentu jego rejestracji do rozwiązania, w tym po przekazaniu incydentu do innego operatora lub grupy.
1.85	Zarządzanie Incydentami	Zarządzanie SLA: System ITSM musi umożliwiać automatyczne wyznaczanie i śledzenie SLA dla incydentów.
1.86	Zarządzanie Incydentami	Przegląd i Analiza: System ITSM musi umożliwiać przeglądanie historii incydentów, w tym wszystkich działań podjętych w celu rozwiązania incydentu oraz ich efektywności.
1.87	Zarządzanie Incydentami	Raportowanie: System ITSM musi oferować zaawansowane narzędzia raportowania incydentów, umożliwiając generowanie raportów dotyczących liczby incydentów, czasu rozwiązania, zgodności z SLA, itd.
1.88	Zarządzanie Incydentami	Kody Rozwiązania: System ITSM musi umożliwiać stosowanie i konfigurowanie kodów rozwiązania dla incydentów, takich jak rozwiązany, odrzucony, obejście, itp.

1.89	Zarządzanie Incydentami	Relacje między Rekordami: System ITSM musi umożliwiać tworzenie i zarządzanie relacjami między incydentami a innymi rekordami, takimi jak wnioski o usługę, problemy, zmiany, elementy konfiguracji.
1.90	Zarządzanie Incydentami	Automatyzacja Procesów: System ITSM musi umożliwiać automatyzację wybranych procesów związanych z zarządzaniem incydentami, takich jak automatyczne przypisywanie, eskalacja, powiadomienia.
1.91	Zarządzanie Incydentami	Załączniki: System ITSM musi umożliwiać dołączanie załączników do incydentów, w formatach takich jak PDF, DOC, XLS, JPG, itp.
1.92	Zarządzanie Incydentami	Blokowanie Zamknięcia Rekordów: System ITSM musi umożliwiać blokowanie zamknięcia incydentu, jeśli związane z nim pola wymagane są niewypełnione.
1.93	Zarządzanie Incydentami	Wstrzymanie SLA: System ITSM musi umożliwiać wstrzymanie naliczania czasu SLA w incydentach na podstawie ustawionego statusu lub działań operatora.
1.94	Zarządzanie Incydentami	Ankiety Satysfakcji: System ITSM musi umożliwiać przeprowadzanie badań satysfakcji użytkowników po rozwiązaniu incydentu, z możliwością konfigurowania ankiet przez administratora.
1.95	Zarządzanie Incydentami	Wyszukiwanie i Filtrowanie: System ITSM musi umożliwiać operatorom wyszukiwanie i filtrowanie incydentów przy użyciu słów kluczowych, ciągów znaków, oraz operatorów logicznych.
1.96	Zarządzanie Incydentami	Historia Działań: System ITSM musi rejestrować i śledzić historię działań związanych z każdym incydentem, w tym modyfikacje, przypisania, eskalacje.
1.97	Zarządzanie Incydentami	Rejestrowanie Działań: System musi umożliwiać rejestrowanie wszystkich działań podjętych w celu rozwiązania incydentu.
1.98	Zarządzanie Incydentami	Współpraca: System powinien wspierać funkcje współpracy, takie jak czat i grupy dyskusyjne, dla lepszej komunikacji między zespołami.
1.99	Zarządzanie Katalogiem Usług	System ITSM musi umożliwiać definiowanie uprawnień Użytkownikom do Katalogu usług, co pozwoli na publikowanie usług w katalogu dla określonych grup użytkowników oraz ukrywanie ich przed innymi.
1.100	Zarządzanie Katalogiem Usług	System ITSM musi umożliwiać tworzenie jednego lub więcej katalogów usług, które pozwalają użytkownikom wnioskować o usługę na zasadzie samoobsługi.
1.101	Zarządzanie Katalogiem Usług	System ITSM musi zapewnić kreator pozycji katalogowych w intuicyjnym GUI, które umożliwia Menadżerowi Katalogu Usług tworzenie, utrzymywanie i publikowanie pozycji katalogowych (bez angażowania Administratora).
1.102	Zarządzanie Katalogiem Usług	System ITSM musi umożliwiać użytkownikom i Operatorom wyszukiwania i filtrowania usług w katalogu na podstawie różnych kryteriów, takich jak słowa kluczowe, kategorie, poziom wsparcia.
1.103	Zarządzanie Katalogiem Usług	System ITSM musi posiadać gotowe rekordy usług z możliwością modyfikacji layout'u oraz pól przez Operatora obsługującego Zarządzanie Katalogiem Usług.
1.104	Zarządzanie Katalogiem Usług	System ITSM musi posiadać możliwość tworzenie szablonów pozycji Katalogu Usług.
1.105	Zarządzanie Katalogiem Usług	Tworzenie i Zarządzanie Usługami: System ITSM musi umożliwiać tworzenie, edytowanie i usuwanie rekordów usług w katalogu usług.
1.106	Zarządzanie Katalogiem Usług	Kategoryzacja Usług: System ITSM musi umożliwiać kategoryzację usług według zdefiniowanych kategorii, takich jak rodzaj usługi, dział, poziom wsparcia itp.
1.107	Zarządzanie Katalogiem Usług	Definiowanie Atrybutów Usługi: System ITSM musi umożliwiać definiowanie szczegółowych atrybutów dla każdej usługi, takich jak opis, właściciel usługi, SLA, koszty, warunki świadczenia itp.
1.108	Zarządzanie Katalogiem Usług	Zarządzanie SLA: System ITSM musi umożliwiać definiowanie, śledzenie i zarządzanie umowami o poziomie usług (SLA) związanych z poszczególnymi usługami.
1.109	Zarządzanie Katalogiem Usług	Automatyczne Powiadomienia: System ITSM musi umożliwiać wysyłanie automatycznych powiadomień o zmianach w usługach, takich jak aktualizacje, przestoje, zmiany warunków świadczenia.
1.110	Zarządzanie Katalogiem Usług	Monitorowanie i Raportowanie: System ITSM musi oferować narzędzia do monitorowania i raportowania o wykorzystaniu usług, ich popularności, kosztach oraz poziomach zgodności z SLA.
1.111	Zarządzanie Katalogiem Usług	Oceny i Opinie: System ITSM musi umożliwiać użytkownikom ocenianie i wyrażanie opinii na temat świadczonych usług.
1.112	Zarządzanie Katalogiem Usług	Integracja z innymi Procesami ITSM: System ITSM musi umożliwiać integrację katalogu usług z innymi procesami ITSM, takimi jak zarządzanie incydentami, zmianami, problemami i zasobami.
1.113	Zarządzanie Katalogiem Usług	Historia Zmian Usług: System ITSM musi rejestrować i udostępniać historię zmian wprowadzonych w usługach, w tym zmiany atrybutów, publikacji i statusów.
1.114	Zarządzanie Katalogiem Usług	Zarządzanie Dokumentacją: System ITSM musi umożliwiać przechowywanie i zarządzanie dokumentacją związanych z usługami, taką jak umowy, opisy techniczne, instrukcje.
1.115	Zarządzanie Katalogiem Usług	Wizualizacja zależności: Wyświetlanie zależności między różnymi usługami, aby Operatorzy mogli zrozumieć, jak usługi są powiązane.
1.116	Zarządzanie Katalogiem Usług	Dostępność informacji: Zapewnienie aktualnych informacji o dostępności usług, w tym statusu i godzin dostępności.
1.117	Zarządzanie Katalogiem Usług	Opisy usług: Możliwość dodawania szczegółowych opisów do każdej usługi w katalogu, aby użytkownicy mieli pełne zrozumienie oferowanych usług.
1.118	Zarządzanie Katalogiem Usług	Powiadomienia: Wysyłanie powiadomień użytkownikom o zmianach w usługach dostępnych w katalogu oraz o awariach lub przerwach w świadczeniu usług.
1.119	Zarządzanie Poziomem Usług	System ITSM musi umożliwiać tworzenie list Klientów usług (organizacji korzystających z usług), przy czym dla każdego Klienta rejestrowane powinny być co najmniej: 1) nazwa, 2) adres korespondencyjny, 3) osoba kontaktowa, 4) telefon i e-mail kontaktowy, 5) powiązane umowy SLA, 6) powiązane usługi.

1.120	Zarządzanie Poziomem Usług	System ITSM musi posiadać gotowe rekordy usług z możliwością modyfikacji layout'u oraz pól przez Operatora obsługującego Zarządzanie Poziomem Usług.
1.121	Zarządzanie Poziomem Usług	Monitorowanie i raportowanie: System ITSM musi zapewniać monitorowanie i raportowanie na bieżąco poziomów usług w odniesieniu do ustalonych SLA dla: 1) Incydentów, 2) Wniosków o usługę, 3) Problemów, 4) Zmian.
1.122	Zarządzanie Poziomem Usług	System ITSM musi umożliwiać wykorzystanie informacji szczegółowych określonych wymaganiami (regułami) SLA co najmniej do: 1) zautomatyzowania procesu monitorowania i raportowania poziomu usług; 2) śledzenia i analizy trendów.
1.123	Zarządzanie Poziomem Usług	System ITSM musi umożliwiać rejestrację wyników przeglądów SLA np. poprzez dedykowane rekordy do Audytów SLA Usług, zawierające wartości SLA zdefiniowane jako zakontraktowane, wartości SLA faktyczne w danym okresie, etc. Dodatkowo rekordy audytu SLA powinny posiadać miejsce na SIP (service improvement plan)oraz możliwość tworzenia work orderów (zleceń pracy) zrelacjonowanych do danego rekordu audytowego.
1.124	Zarządzanie Poziomem Usług	Definicja SLA: System ITSM musi umożliwiać definiowanie i zarządzanie poziomami usług (SLA) dla usług.
1.125	Zarządzanie Poziomem Usług	Określanie SLA: System ITSM powinien umożliwiać określanie gwarantowanych parametrów usług, takich jak dostępność, terminowości itp.
1.126	Zarządzanie Poziomem Usług	Powiadomienia: System ITSM musi umożliwiać automatyczne generowanie alertów i powiadomień w przypadku zagrożenia naruszenia ustalonych SLA i jego przekroczenia.
1.127	Zarządzanie Poziomem Usług	System ITSM powinien umożliwiać automatyczne generowanie raportów i zestawień dotyczących realizacji SLA dla różnych grup interesariuszy.
1.128	Zarządzanie Umowami (w procesie Zarządzania Dostawcami)	System ITSM musi posiadać funkcje powiadamiania o określonych zdarzeniach związanych z realizacją umów, np.: zakończenie okresu gwarancji, przy pomocy powiadomień e-mail do określonych osób. Zasady uruchomienia powiadomień, wartości parametrów oraz lista osób powiadamianych muszą być możliwe do skonfigurowania przez Operatora lub Administratora.
1.129	Zarządzanie Umowami (w procesie Zarządzania Dostawcami)	System ITSM musi posiadać możliwość tworzenia bazy adresowej dostawców, obejmującej co najmniej: 1) nazwę przedsiębiorstwa oraz NIP 2) osobę kontaktową, 3) adres korespondencyjny, 4) telefon i e-mail kontaktowy, 5) powiązanie z umowami, 6) kategorię dostaw, 7) sumę wielkości kontraktów posiadanych z Zamawiającym,
1.130	Zarządzanie Umowami (w procesie Zarządzania Dostawcami)	System ITSM musi posiadać możliwość rejestracji określonych parametrów umów z dostawcami, w tym co najmniej: 1) daty zawarcia umowy, 2) daty zakończenia umowy, 3) Data końca wsparcia 4) wartości umowy, 5) statusu umowy, 6) właściciela umowy, 7) czasu dostawy, 8) terminu i modelu płatności, 9) czasu reakcji w ramach serwisu, 10) czasu naprawy w ramach serwisu oraz dodawanie załączników w postaci plików zewnętrznych (co najmniej formaty PDF, DOC, DOCX, XLS, XLSX, GIF, JPG, BMP, TXT, PPT, PPTX, ZIP) przez Operatora.
1.131	Zarządzanie Umowami (w procesie Zarządzania Dostawcami)	Centralne repozytorium kontraktów: System ITSM powinien zawierać centralne repozytorium, w którym przechowywane są wszystkie umowy i kontrakty z dostawcami usług IT.
1.132	Zarządzanie Umowami (w procesie Zarządzania Dostawcami)	Analiza ryzyka kontraktowego: Analiza dostawcy pod kątem wywiązywania się z warunków umowy (np. weryfikacja SLA, kary umowne) umożliwiająca ocenę ryzyka związaną z potencjalnymi konsekwencjami dla organizacji oraz podejmowania działań zapobiegawczych.
1.133	Zarządzanie Umowami (w procesie Zarządzania Dostawcami)	Śledzenie ocen dostawców: Wymaganie dotyczące śledzenia ocen dostawców na podstawie takich czynników jak jakość usług, terminowość dostaw oraz elastyczność w reagowaniu na zmiany.
1.134	Zarządzanie Umowami (w procesie Zarządzania Dostawcami)	Kategoryzacja dostawców: System ITSM powinien umożliwiać kategoryzację dostawców w zależności od ich roli, znaczenia strategicznego oraz oceny wydajności.
1.135	Zarządzanie Umowami (w procesie Zarządzania Dostawcami)	Weryfikacja umów SLA: Wymaganie dotyczące weryfikacji zgodności umów z dostawcami z ustalonymi poziomami usług (SLA) oraz wymaganiami organizacji.
1.136	Zarządzanie Umowami (w procesie Zarządzania Dostawcami)	Zarządzanie zmianami w umowach: System ITSM powinien umożliwiać zarządzanie zmianami w istniejących umowach, w tym renegocjację warunków oraz przedłużanie terminów.
1.137	Zarządzanie Umowami (w procesie Zarządzania Dostawcami)	Zarządzanie kosztami: Wymaganie dotyczące monitorowania i kontrolowania kosztów związanych z umowami i kontraktami, w tym oceny opłacalności poszczególnych dostawców.
1.138	Zarządzanie Umowami (w procesie Zarządzania Dostawcami)	Zarządzanie życiowym cyklem kontraktu: System ITSM powinien umożliwiać kompleksowe zarządzanie cyklem życia kontraktu, począwszy od jego inicjacji, poprzez egzekucję, aż do zakończenia.
1.139	Zarządzanie Umowami (w procesie Zarządzania Dostawcami)	Zarządzanie SLA dostawców: System ITSM musi umożliwiać zarządzanie relacjami z dostawcami zgodnie z ustalonymi SLA.
1.140	Zarządzanie Wiedzą	System ITSM musi być w stanie tworzyć i utrzymywać wiele wersji artykułu wiedzy

1.141	Administracja - Portal Użytkownika	System ITSM musi posiadać interfejs wielojęzykowy w tym w polskiej wersji językowej i angielskiej z możliwością wyboru przez Użytkownika Systemu.
1.142	Administracja - Portal Użytkownika	System ITSM musi być dostępny z poziomu przeglądarki internetowej w ich najnowszych wersjach, bez konieczności instalowania komponentów trzecich lub plug-in. Aplikacja ITSM ma być wpierana przez popularne przeglądarki na różnych systemach: Windows, MAC OS, Linux w szczególności Google Chrome, Mozilla FireFox oraz Safari co najmniej w wersji aktualnej na dzień składania ofert.
1.143	Administracja - Portal Użytkownika	System ITSM musi posiadać portal samoobsługowy (Portal Użytkownika) umożliwiający zamawianie usług, rejestrowanie Zgłoszeń, sprawdzanie przypisanych Zasobów (w tym sprzętu fizycznego i licencji), odczytywanie komunikatów i ogłoszeń, i informację o wszystkich rekordach dotyczących Użytkownika końcowego.
1.144	Administracja - Portal Użytkownika	System ITSM musi umożliwiać publikowanie przez Administratora i Operatora w Portalu Użytkownika ogłoszeń, w tym umieszczanie artykułów, plików do pobrania oraz odnośników do stron internetowych.
1.145	Administracja - Portal Użytkownika	System ITSM musi zapewniać mechanizmy powiązania artykułów bazy wiedzy z Incydentami w celu redukcji ilość zgłoszeń, np. poprzez wyświetlanie odpowiednich artykułów wiedzy w trakcie tworzenia incydentu przez Operatora lub Użytkownika końcowego.
1.146	Administracja - Portal Użytkownika	Portal Użytkownika musi umożliwiać automatyczne przypisanie incydentu lub wniosku o usługę do odpowiedniej kategorii na podstawie zdefiniowanych reguł.
1.147	Administracja - Portal Użytkownika	Portal Użytkownika musi umożliwiać śledzenie statusu zgłoszonych incydentów i wniosków o usługi w czasie rzeczywistym.
1.148	Administracja - Portal Użytkownika	Portal Użytkownika musi umożliwiać użytkownikowi przeglądanie historii zgłoszeń oraz przeszukiwanie archiwalnych incydentów i wniosków.
1.149	Administracja - Portal Użytkownika	Portal Użytkownika musi umożliwiać użytkownikowi zamknięcie zgłoszenia lub jego ponowne otwarcie w przypadku nierozwiązania problemu.
1.150	Administracja - Portal Użytkownika	Portal Użytkownika musi umożliwiać wysyłanie powiadomień e-mail o zmianie statusu zgłoszenia oraz o nowych komentarzach dodanych do zgłoszenia przez operatorów.
1.151	Administracja - Portal Użytkownika	Portal Użytkownika musi umożliwiać dwustronną komunikację między użytkownikiem a operatorem poprzez dodawanie komentarzy do zgłoszenia.
1.152	Administracja - Portal Użytkownika	Portal Użytkownika musi umożliwiać użytkownikom końcowym skonfigurowanie preferencji powiadomień (np. powiadomienia e-mail, powiadomień systemowych, itp.).
1.153	Administracja - Portal Użytkownika	Portal Użytkownika musi umożliwiać personalizację interfejsu użytkownika (np. układ widżetów, kolorystyka, dostępne opcje menu).
1.154	Administracja - Portal Użytkownika	Portal Użytkownika musi być dostępny na urządzeniach mobilnych poprzez responsywny design lub dedykowaną aplikację mobilną.
1.155	Administracja - Bezpieczeństwo	Portal Użytkownika musi integrować się z systemem Single Sign-On (SSO) Zamawiającego, umożliwiając użytkownikom logowanie za pomocą jednego zestawu poświadczeń.
1.156	Administracja - Integracja	Portal Użytkownika musi umożliwiać integrację z narzędziami do komunikacji (np. Microsoft Teams) w celu powiadamiania użytkowników o aktualizacjach zgłoszeń.
1.157	Administracja - Portal Użytkownika	Portal Użytkownika musi zawierać moduł bazy wiedzy, umożliwiający użytkownikom dostęp do artykułów, FAQ i instrukcji rozwiązania najczęstszych problemów.
1.158	Administracja - Portal Użytkownika	Portal Użytkownika musi umożliwiać użytkownikom wyszukiwanie artykułów bazy wiedzy za pomocą wyszukiwarki tekstowej i filtrowania kategorii.
1.159	Administracja - Portal Użytkownika	Portal Użytkownika musi wspierać mechanizmy samoobsługowe, umożliwiając użytkownikom resetowanie hasła, aktualizację danych kontaktowych i inne operacje bez konieczności zgłaszania incydentu dla Użytkowników spoza Active Directory .
1.160	Administracja - Bezpieczeństwo	Portal Użytkownika musi zapewniać bezpieczeństwo danych poprzez szyfrowanie połączeń SSL/TLS.
1.161	Administracja - Portal Użytkownika	Portal Użytkownika musi umożliwiać administratorom konfigurowanie uprawnień dostępu dla różnych grup użytkowników.
1.162	Administracja - Raportowanie	System ITSM musi posiadać wbudowany mechanizm raportowania na podstawie danych z Systemu ITSM – umożliwiający tworzenie dowolnych raportów w systemie ITSM, korzystanie/modyfikowanie z predefiniowanych raportów (dotyczące wszystkich wdrożonych procesów/modułów). Użytkownik Systemu może definiować własne zaawansowane raporty z dostępnych elementów (w zależności od przypisanej roli w Systemie) z użyciem dedykowanego interfejsu na zasadach np. "przeciągnij i upuść" bez konieczności pisania zaawansowanych zapytań do bazy .
1.163	Administracja - Raportowanie	System ITSM musi umożliwiać generowanie raportów w różnych formatach, takich jak PDF, CSV, XLSX, HTML.
1.164	Administracja - Raportowanie	System ITSM musi zapewniać możliwość udostępniania raportów innym użytkownikom lub grupom, zgodnie z ich uprawnieniami.
1.165	Administracja - Raportowanie	System ITSM powinien umożliwiać wizualne prezentowanie danych raportowych w formie graficznej tj. wykresy, grafy, trendy, tabelaryczne itd. aby ułatwić analizę danych.
1.166	Administracja - Raportowanie	System ITSM musi umożliwiać planowanie i harmonogramowanie raportów, tak aby można było je generować automatycznie w określonych interwałach czasowych.
1.167	Administracja - Raportowanie	System ITSM powinien umożliwiać generowanie cyklicznych raportów na podstawie zdefiniowanych reguł.
1.168	Administracja - Raportowanie	System ITSM musi umożliwiać generowanie zapytań w języku obsługującym bazę danych.
1.169	Administracja - Raportowanie	System ITSM powinien umożliwiać definiowanie adresatów, do których wysyłane będą mailowo raporty cykliczne
1.170	Administracja - Raportowanie	Raporty powinny być dostępne w czasie rzeczywistym i umożliwiać natychmiastowe przeglądanie najnowszych danych.
1.171	Administracja - Raportowanie	Raporty powinny być konfigurowalne, co pozwoli użytkownikom na dostosowanie ich do własnych potrzeb i preferencji.

1.172	Administracja - Raportowanie	System ITSM musi zapewniać możliwość tworzenia raportów opartych na różnych źródłach danych, takich jak rekordy Incydentów, Wniosków o usługę, Problemy, Zmiany, Wydania, Elementy konfiguracji itp.
1.173	Administracja - Raportowanie	System ITSM musi umożliwiać filtrowanie danych raportów na podstawie różnych kryteriów, takich jak data, status, priorytet itp.
1.174	Administracja - Raportowanie	Raporty powinny być skalowalne, aby umożliwić zarówno ogólny przegląd danych, jak i bardziej szczegółowe analizy.
1.175	Administracja - Raportowanie	System ITSM musi oferować wbudowane szablony raportów, które użytkownicy mogą łatwo dostosować do własnych potrzeb.
1.176	Administracja - Raportowanie	Raporty powinny być interaktywne, co umożliwi użytkownikom wykonywanie różnych operacji, takich jak sortowanie, grupowanie i zmiana widoku danych.
1.177	Administracja - Raportowanie	Raporty powinny być zoptymalizowane pod kątem wydajności, aby szybko generować i wyświetlać duże ilości danych.
1.178	Administracja - Raportowanie	System ITSM musi zapewniać mechanizmy śledzenia i audytu raportów, aby monitorować, kto je generuje, udostępnia i przegląda.
1.179	Administracja - Integracja	Integracja z rozwiązaniami jak Microsoft Azure Active Directory, czy LDAP Zakres integracji: Automatyzacja zarządzania użytkownikami i dostępami, synchronizacja uprawnień. Dane potrzebne: Informacje o użytkownikach, grupach, rolach, uprawnieniach. Cel: Centralne zarządzanie dostępem, zwiększenie bezpieczeństwa.
1.180	Administracja - Integracja	System ITSM musi zapewniać dwukierunkową integrację z serwerem poczty elektronicznej, co najmniej MS Exchange oraz protokoły SMTP i IMAP. Zakres integracji System ITSM musi umożliwiać: 1. Automatyczne tworzenie i aktualizowanie zgłoszeń na podstawie wiadomości e-mail. 2. Wysyłanie powiadomień e-mail o zmianach statusów zgłoszeń i innych ważnych wydarzeniach. 3.Odbieranie e-maili i automatyczne przypisywanie ich do istniejących zgłoszeń. 4. Możliwość komunikacji z użytkownikami poprzez e-mail bezpośrednio z poziomu systemu ITSM. 5. Obsługę załączników do e-maili, które mogą być dołączane do zgłoszeń. Dane potrzebne Dane o użytkownikach poczty: 1. Adresy e-mail nadawców i odbiorców. 2. Korespondencja e-mailowa (treść wiadomości, tematy, daty). 3. Załączniki do wiadomości. Dane o zgłoszeniach w ITSM: 1. Identyfikatory zgłoszeń. 2. Statusy zgłoszeń. 3. Historia komunikacji i notatek w zgłoszeniach. 4. Informacje o przydzielonych zasobach i personelu.
1.181	Administracja - Integracja	System ITSM musi umożliwiać integrację poprzez: 1) API 2) usługi sieciowe (Web Services), 3) dokumenty w formacie XML, 4) e-mail, 5) płaskie pliki tekstowe. 6) interfejsy bazodanowe 7) PowerShell 8) SSH 9) ODBC/JDBC 10) LDAP
1.182	Administracja - Integracja	Integracja z narzędziami monitorującymi: System ITSM musi być w stanie integrować się z różnymi narzędziami monitorującymi w celu zbierania danych o zdarzeniach min. Kibana, Monit24, Nagios Core, Nagios XI, VMWare Aria Operations, Zabbix. Narzędzia, z którymi potrzebna będzie integracja na etapie wdrożenia to: Nagios Core, Nagios XI, Zabbix. Zakresem danych są alerty, lub pojęcia równoważne, z wymienionych systemów zawierające nazwę hosta/systemu, nazwę/typ alertu, opcjonalną wartość oraz opcjonalny komentarz/opis.

1.183	Administracja - Integracja	i pozwala na odczytanie następujących danych: Dane, jakie API musi zwracać dla zgłoszenia: Dane wejściowe: numer zgłoszenia Dane wyjściowe: - Dane zgłoszenia: - Użytkownik (zgłaszający) - Tytuł zgłoszenia - Usługa - Pilność - Wpływ - Priorytet - Rodzaj zgłoszenia - Kanał - Grupa odpowiedzialna - Odpowiedzialny - Id grupy przekazującej zgłoszenie - Id osoby przekazująca zgłoszenie - Problem nadrzędny - Status zgłoszenia: - Status - Zamrożone do - Data wpłynięcia - Data utworzenia - Gwarantowana data reakcji - Gwarantowana data rozwiązania - Data zamknięcia - Czas realizacji - Czas realizacji w godz. roboczych
1.184	Administracja - Integracja	i pozwala na odczytanie następujących danych: Dane, jakie API musi zwracać dla wniosku o zmianę: Dane wejściowe: numer zmiany Dane wyjściowe: - Dane zmiany: - Tytuł - Wnioskujący - Usługa - Typ zmiany - Kategoria - Pilność - Priorytet - Wnioskowane przez - Wytwórca merytoryczny zmiany - Menadżer zmiany - Aktualnie odpowiedzialny - Obiekt nadrzędny - Ocena ryzyka zmiany - Pakiet dystrybucyjny zmiany - Status zmiany: - Stan - Zamrożona do - Data utworzenia - Wymagana data opinii wewnętrznej - Wymagana data opinii CAB - Data zamknięcia - Etap - Planowana data rozpoczęcia wdrożenia

1.185	Administracja - Integracja	i pozwala na odczytanie następujących danych: Lista zgłoszeń: Dane wejściowe: poniższe kryteria filtrowania w liczbie jeden lub więcej. Jeśli sprecyzowano więcej niż jeden filtr interesują nas tylko zgłoszenia, które spełniają WSZYSTKIE sprecyzowane kryteria: - Zgłaszający użytkownik (nazwa lub email) - Grupa użytkownika zgłaszającego - Status - Zakres dat zgłoszenia - Odpowiedzialny - Historyczny odpowiedzialny - Grupa odpowiedzialna - Historyczna grupa odpowiedzialna Wyjście: - Tytuł - Wnioskujący - Usługa - Kanał, którym spłynęło - Typ zmiany - Kategoria - Pilność - Priorytet - Stan - Data zgłoszenia - Data zamknięcia (jeśli już zamknięte, jeśli nie to `null` lub brak odpowiadającego tej wartości klucza) Lista wniosków o zmianę: Dane wejściowe: poniższe kryteria filtrowania w liczbie jeden lub więcej. Jeśli sprecyzowano więcej niż jeden filtr interesują nas tylko zgłoszenia, które spełniają WSZYSTKIE sprecyzowane kryteria: - Zgłaszający użytkownik (nazwa lub email)
1.186	Administracja - Integracja	Integracja systemu ITSM z Microsoft System Center Configuration Manager (SCCM) Zakres integracji System ITSM musi umożliwiać: 1. Automatyczne importowanie i synchronizację danych o zasobach IT z SCCM. 2. Monitorowanie stanu i zdrowia zasobów zarządzanych przez SCCM. 3. Wykorzystanie danych SCCM do zarządzania cyklem życia zasobów w systemie ITSM. 4. Automatyczne tworzenie zgłoszeń w ITSM na podstawie alertów i raportów generowanych przez SCCM. 5. Przeprowadzanie zdalnych operacji na urządzeniach, takich jak instalacja oprogramowania czy aktualizacje, z poziomu ITSM przy użyciu funkcji SCCM. Dane potrzebne Dane o zasobach IT: 1. Informacje o urządzeniach (komputery, serwery, urządzenia mobilne). 2. Dane o zainstalowanym oprogramowaniu i jego wersjach. 3. Statusy i konfiguracje urządzeń. 4. Informacje o zgodności urządzeń z politykami bezpieczeństwa. Dane o użytkownikach: 1. Informacje o przypisanych użytkownikach do poszczególnych urządzeń. 2. Historia działań związanych z zasobami. Dane o alertach i incydentach: 1. Alerty o problemach sprzętowych lub programowych. 2. Raporty o niezgodności z politykami bezpieczeństwa. 3. Informacje o automatycznych działaniach naprawczych.
1.187	Administracja - Bezpieczeństwo	Nie może być formalnych ograniczeń na testowanie pod kątem bezpieczeństwa systemu ITSM.
1.188	Administracja - Bezpieczeństwo	System ITSM musi umożliwiać integracje z systemami do uwierzytelniania wieloskładnikowego (MFA).
1.189	Administracja - Bezpieczeństwo	System ITSM musi umożliwiać definiowanie ról dostępu do informacji w zależności od autoryzacji Użytkownika Systemu .
1.190	Administracja - Bezpieczeństwo	System ITSM musi zapobiegać nieautoryzowanemu dostępowi do Systemu ITSM poprzez wbudowane mechanizmy bezpieczeństwa.
1.191	Administracja - Bezpieczeństwo	W przypadku lokalnej bazy użytkowników System ITSM musi udostępniać mechanizm wymuszający ich kontrolę np. w postaci minimalnej długości hasła, maksymalnego czasu ważności hasła, historii haseł (wymuszenie unikalności haseł), złożoności hasła.
1.192	Administracja - Bezpieczeństwo	System ITSM musi umożliwiać integrację z zewnętrznymi dostawcami w przypadku tworzenia zewnętrznych tożsamości za pomocą protokołów SAML, LDAP, Kerberos, NTLM.
1.193	Administracja - Bezpieczeństwo	Zamawiający nie dopuszcza udostępniania, przekazywania danych z Systemu ITSM poza infrastrukturę Zamawiającego bez jego wiedzy i zgody.
1.194	Administracja - Bezpieczeństwo	System ITSM musi zapewniać bezpieczeństwo komunikacji. Przesyłane dane muszą być zabezpieczone i szyfrowane za pomocą protokołu TLS w wersji co najmniej 1.2. System musi wspierać TLS wersję 1.3.
1.195	Administracja - Bezpieczeństwo	System ITSM musi zapewniać logowanie (lokalne i do systemu SIEM), przeglądanie i raportowanie zdarzeń systemowych (audytowych) wg zadanych kryteriów umożliwiających identyfikację czasu, konta użytkownika, rodzaju i sposobu wykonania czynności na danym obiekcie.

1.196	Administracja - Bezpieczeństwo	System ITSM musi zapewniać logowanie (lokalne i do systemu SIEM), przeglądanie i raportowanie zdarzeń systemowych (audytowych) w zakresie prób nieautoryzowanego dostępu, niepoprawnego i poprawnego logowania.
1.197	Administracja - Bezpieczeństwo	System ITSM musi posiadać funkcjonalność anonimizacji danych osobowych (zgodnie z przepisami RODO) w sposób uniemożliwiający powiązanie "zdarzenia" (zgłoszenie, działanie, operacja itp.) z użytkownikiem, jednocześnie niezakłócający ciągłości działania systemu.
1.198	Administracja - Bezpieczeństwo	System ITSM musi mieć możliwość przechowywanych danych w sposób zaszyfrowany.
1.199	Administracja - Bezpieczeństwo	System ITSM musi posiadać funkcjonalność przeglądania logów systemowych i innych zdarzeń za pomocą filtrów.
1.200	Administracja - Bezpieczeństwo	System ITSM musi pozwalać na przesyłanie logów z zarejestrowanych zdarzeń do zewnętrznego serwera logów za pomocą protokołu syslog.
1.201	Administracja - Bezpieczeństwo	System ITSM musi posiadać oddzielną witrynę dla pracowników firmy, osób współpracujących, kontrahentów itp. służącą do składania anonimowych wniosków (obsługa Sygnalistów) bez konieczności logowania się i pozostawiania jakichkolwiek danych osobowych.
1.202	Administracja - Bezpieczeństwo	System ITSM musi posiadać funkcjonalność tworzenia i odzyskiwania kopii zapasowej danych.
1.203	Administracja - Bezpieczeństwo	System ITSM musi zapewniać Sygnaliście możliwość weryfikacji statusu sprawy oraz korespondowania w jej zakresie poprzez użycie wygenerowanego podczas składania wniosku jednorazowego tokena.
1.204	Administracja - Infrastruktura	Wykonawca określi wymagania dla środowiska ITSM (ilość serwerów, systemy operacyjne, bazy danych i inne). Środowisko musi być skalowalne, dawać możliwość zwiększenia wydajności poprzez rozbudowę infrastruktury, np. serwerów (w szczególności poprzez dodanie procesorów, pamięci RAM, zwiększenie liczby serwerów).
1.205	Administracja - Infrastruktura	Dane generowane przez system ITSM powinny być zbierane w jednolitym jeziorze danych, do którego wszystkie moduły systemu posiadają dostęp i możliwość przeszukiwania danych w identyczny sposób. Zastosowana technologia jeziora danych musi być wspierana przez producenta oprogramowania ITSM. Jeżeli wykorzystanie go wymaga dodatkowych licencji, należy je dostarczyć na rekomendowaną dla tego wdrożenia pojemność. Funkcjonalność ta musi być niezależna od głównej bazy danych rozwiązania.
1.206	Administracja - Infrastruktura	Technologia jeziora danych musi wspierać przeszukiwanie i analizę danych za pomocą co najmniej następujących języków danych: SQL, Python, R, Java. Dodatkowo, powinno umożliwiać integrację z narzędziami klasy Business Intelligence (takimi jak Power BI, Qlik, Tableau).
1.207	Administracja - Infrastruktura	System ITSM musi spełniać parametry RTO = 4 godziny, RPO = 5 minut. Architektura Systemu ITSM powinna zapewnić dostępność systemu na poziomie 99,8%, bez wliczania ustalanych wcześniej przerw serwisowych.
1.208	Administracja - Infrastruktura	Środowisko produkcyjne systemu ITSM powinno zostać zainstalowane w dwóch równolegle pracujących ośrodkach.
1.209	Administracja - Infrastruktura	System ITSM powinien zapewniać procedury naprawcze na wypadek wystąpienia Awarii, umożliwiające przywrócenie Systemu ITSM do stanu sprzed Awarii, na podstawie kryteriów zdefiniowanych przez Administratora. Rozwiązanie dla serwerów aplikacyjnych i bazodanowych.
1.210	Administracja - Infrastruktura	System ITSM musi umożliwiać tworzenie całkowitych, przyrostowych kopii bezpieczeństwa Systemu ITSM (automatyczne oraz manualne) i danych w trybie on-line oraz zapewniać procedurę przywracania Systemu ITSM z kopii bezpieczeństwa po Awarii. W tym zakresie system ITSM powinien umożliwiać współpracę z wiodącymi systemami kopii zapasowej (np. Veeam, Commvault, Networker)
1.211	Zarządzanie Zdarzeniami	System ITSM musi zapewnić zbieranie logów zdarzeń, backup logów, filtrowanie logów wg rodzajów, definiowanie zasad wykrywania incydentów na podstawie alertów, logów, definiowanie wymagań dotyczących monitorowania działań administratorskich.
1.212	Zarządzanie Zdarzeniami	System ITSM musi umożliwiać automatyczne zarejestrowanie Incydentu powiązanego z Elementem konfiguracji (CI) na podstawie alertu z narzędzi monitoringu. W przypadku próby zarejestrowania kolejnego Incydentu wywołanego tym samym alertem dotyczącym tego samego CI system ma informować o istnieniu otwartego Incydentu, z możliwością zarejestrowania kolejnego Incydentu dla tego Elementu konfiguracji. W celu osiągnięcia tej funkcjonalności wymagana jest integracja Systemu ITSM poprzez API HTTP umożliwiające komunikację w formatach XML oraz JSON.
1.213	Zarządzanie Zdarzeniami	System ITSM musi umożliwiać automatyczne rozwiązanie i zamknięcie Incydentu na podstawie alertu z systemu zewnętrznego lub narzędzi monitorowania o przywróceniu prawidłowych parametrów usługi. Integracja ta ma być dostępna w postaci API dostępnego przez HTTP przyjmującego i zwracającego dane w formacie XML oraz JSON.
1.214	Zarządzanie Zdarzeniami	Automatyczne powiadomienia: System ITSM powinien automatycznie generować powiadomienia o zdarzeniach do odpowiednich użytkowników lub grup.
1.215	Zarządzanie Zdarzeniami	Eskalacja zdarzeń: System ITSM musi umożliwiać automatyczną eskalację zdarzeń, które nie zostały rozwiązane w ustalonym czasie.
1.216	Zarządzanie Zdarzeniami	Rejestracja zdarzeń: System ITSM powinien automatycznie rejestrować wykryte zdarzenia o określonych kryteriach, wraz z ich szczegółami. Te kryteria to: tytuł, priorytet, host (może być jako flara w tytule), treść.
1.217	Zarządzanie Zdarzeniami	Przekształcanie zdarzeń w incydenty: System ITSM powinien umożliwiać przekształcanie wykrytych zdarzeń w incydenty do dalszego procesowania.
1.218	Zarządzanie Zdarzeniami	Integracja z narzędziami monitorującymi: System ITSM musi być w stanie integrować się z różnymi narzędziami monitorującymi w celu zbierania danych o zdarzeniach min. Kibana, Monit24, Nagios Core, Nagios XI, VMWare Aria Operations, Zabbix. Narzędzia, z którymi potrzebna będzie integracja na etapie wdrożenia to: Nagios Core, Nagios XI, Zabbix. Zakresem danych są alerty, lub pojęcia równoważne, z wymienionych systemów zawierające nazwę hosta/systemu, nazwę/typ alertu, opcjonalną wartość oraz opcjonalny komentarz/opis.

1.219	Zarządzanie Zdarzeniami	i pozwala na odczytanie następujących danych: Dane, jakie API musi zwracać dla zgłoszenia: Dane wejściowe: numer zgłoszenia Dane wyjściowe: - Dane zgłoszenia: - Użytkownik (zgłaszający) - Tytuł zgłoszenia - Usługa - Pilność - Wpływ - Priorytet - Rodzaj zgłoszenia - Kanał - Grupa odpowiedzialna - Odpowiedzialny - Id grupy przekazującej zgłoszenie - Id osoby przekazująca zgłoszenie - Problem nadrzędny - Status zgłoszenia: - Status - Zamrożone do - Data wpłynięcia - Data utworzenia - Gwarantowana data reakcji - Gwarantowana data rozwiązania - Data zamknięcia - Czas realizacji - Czas realizacji w godz. roboczych
1.220	Zarządzanie Zdarzeniami	i pozwala na odczytanie następujących danych: Dane, jakie API musi zwracać dla wniosku o zmianę: Dane wejściowe: numer zmiany Dane wyjściowe: - Dane zmiany: - Tytuł - Wnioskujący - Usługa - Typ zmiany - Kategoria - Pilność - Priorytet - Wnioskowane przez - Wytwórca merytoryczny zmiany - Menadżer zmiany - Aktualnie odpowiedzialny - Obiekt nadrzędny - Ocena ryzyka zmiany - Pakiet dystrybucyjny zmiany - Status zmiany: - Stan - Zamrożona do - Data utworzenia - Wymagana data opinii wewnętrznej - Wymagana data opinii CAB - Data zamknięcia - Etap - Planowana data rozpoczęcia wdrożenia

1.221	Zarządzanie Zdarzeniami	i pozwala na odczytanie następujących danych: Lista zgłoszeń: Dane wejściowe: poniższe kryteria filtrowania w liczbie jeden lub więcej. Jeśli sprecyzowano więcej niż jeden filtr interesują nas tylko zgłoszenia, które spełniają WSZYSTKIE sprecyzowane kryteria: - Zgłaszający użytkownik (nazwa lub email) - Grupa użytkownika zgłaszającego - Status - Zakres dat zgłoszenia - Odpowiedzialny - Historyczny odpowiedzialny - Grupa odpowiedzialna - Historyczna grupa odpowiedzialna Wyjście: - Tytuł - Wnioskujący - Usługa - Kanał, którym spłynęło - Typ zmiany - Kategoria - Pilność - Priorytet - Stan - Data zgłoszenia - Data zamknięcia (jeśli już zamknięte, jeśli nie to `null` lub brak odpowiadającego tej wartości klucza) Lista wniosków o zmianę: Dane wejściowe: poniższe kryteria filtrowania w liczbie jeden lub więcej. Jeśli sprecyzowano więcej niż jeden filtr interesują nas tylko zgłoszenia, które spełniają WSZYSTKIE sprecyzowane kryteria: - Zgłaszający użytkownik (nazwa lub email)
1.222	Zarządzanie Zdarzeniami	System ITSM musi umożliwiać ręczne i automatyczne utworzenie Incydentu na podstawie zdarzenia w Systemie ITSM. Oba obiekty powinny być ze sobą zrelacjonowane.
1.223	Administracja - Integracja	Integracja pomiędzy nowym ITSM a Atmosferą ITSM musi posiadać możliwość integracji z obecnym systemem ITSM Atmosfera w celu przesyłania danych w sposób cykliczny i na żądanie z nowego ITSM do ITSM Atmosfera. Celem wymagania jest obsługa procesu Zarządzania Zmianą w ITSM Atmosfera oraz realizacja procesu Zarządzania Konfiguracją w nowym ITSM Przesyłane będą informację: - Zmiana statusu zlecenia pracy w nowym ITSM będzie wyzwalaczem zmiany statusu RFC w ITSM Atmosfera. Integracja będzie odbywać się poprzez API ITSM Atmosfera (API jest obecnie na etapie planowania) zdolnego do przyjęcia wszystkich wymienionych powyżej informacji lub poprzez komunikację z bazą danych ITSM Atmosfera za pośrednictwem proxy.
1.224	Administracja - Integracja	Integracja pomiędzy ITSM Atmosfera a nowym ITSM. ITSM musi posiadać możliwość integracji z obecnym systemem ITSM Atmosfera w celu przesyłania danych w sposób cykliczny i na żądanie z ITSM Atmosfera do nowego ITSM. Celem wymagania jest 1. Obsługa procesu Zarządzania Zmianą w ITSM Atmosfera oraz realizacja procesu Zarządzania Konfiguracją w nowym ITSM. 2. Budowanie relacji CI - Usługa w CMDB Przesyłane będą dane: 1. Przesyłane będą informacje z RFC (wybrane zakładki z RFC). Wyzwalaczem będzie status RFC w ITSM Atmosfera do utworzenia zlecenia pracy w nowym ITSM. (np. Status RFC 'do aktualizacji CMDB' w systemie Atmosfera jest wyzwalaczem zlecenia pracy do zespołu Zarzadzania Konfiguracja. Zmiana statusu zlecenia pracy na zrealizowane wyzwala zmianę statusu RFC na "potwierdzona/odrzucona aktualizacja" 2. Przesyłane i aktualizowane będą Katalogi Usług z ITSM Atmosfera do nowego ITSM na potrzeby utrzymania bazy CMDB w nowym ITSM Integracja będzie odbywać się poprzez API ITSM Atmosfera (API jest obecnie na etapie planowania) zdolnego do przyjęcia wszystkich wymienionych powyżej informacji lub poprzez komunikację z bazą danych ITSM Atmosfera za pośrednictwem proxy.
1.225	Administracja - Integracja	System ITSM musi posiadać interfejs API do integracji z co najmniej jednym silnikiem antywirusowym dla załączanych plików (np. Microsoft Defender).

1.226	Administracja - ogólne	System musi posiadać wewnętrzne mechanizmy archiwizacji rekordów (m. in. assety, dokumenty) historycznych lub niepotrzebnych.
1.227	Zarządzanie Zmianą	System powinien zapewnić możliwość rejestrowania Wniosków o Zmianę za pomocą interfejsu WWW.
1.228	Zarządzanie Zmianą	System musi umożliwiać kompletne śledzenie cyklu życia Zmiany z możliwością dodawania i modyfikacji szczegółów w każdym kroku cyklu.
1.229	Zarządzanie Zmianą	System musi umożliwiać modyfikowanie istniejących oraz definiowanie nowych przepływów workflow dla procesu Zarządzania Zmianami przy użyciu interfejsu graficznego przez administratora systemu.
1.230	Zarządzanie Zmianą	System musi umożliwiać, w ramach przepływów workflow, definiowanie warunków przejścia pomiędzy kolejnymi krokami przepływu przez administratora systemu.
1.231	Zarządzanie Zmianą	System musi umożliwiać modyfikowanie istniejących oraz definiowanie nowych formularzy dla procesu Zarządzania Zmianami przez administratora systemu.
1.232	Zarządzanie Zmianą	System musi umożliwiać tworzenie i modyfikowanie pól, list, hierarchii, powiązań dla procesu Zarządzania Zmianami przez administratora systemu.
1.233	Zarządzanie Zmianą	System musi umożliwiać automatyczne wypełnianie pól formularza na podstawie innych informacji w systemie, przy czym reguły wypełnienia pól muszą być możliwe do definiowania przez administratora systemu.
1.234	Zarządzanie Zmianą	System musi umożliwiać konfigurowanie pól formularzy jako odblokowanych lub zablokowanych do edycji manualnej, przy czym konfiguracja musi być możliwa dla administratora systemu.
1.235	Zarządzanie Zmianą	System musi umożliwiać dołączanie do zapisów załączników w postaci plików zewnętrznych (co najmniej formaty PDF, DOC, DOCX, XLS, XLSX, GIF, JPG, BMP, TXT, ZIP) z możliwością wersjonowania oraz archiwizacji wersji poprzednich.
1.236	Zarządzanie Zmianą	System musi zapewniać wysyłanie wiadomości e-mail w formacie TXT oraz HTML.
1.237	Zarządzanie Zmianą	System musi umożliwiać graficzne prezentowanie zestawień zmian wraz z informacją co najmniej o: a) ich statusie oraz b) czasie realizacji oraz c) ewentualnym przekroczeniu czasu realizacji przy czym musi istnieć możliwość konfigurowania widoku tego zestawienia przez administratora systemu.
1.238	Zarządzanie Zmianą	System musi umożliwiać łączenie (tworzenie relacji) incydentów, zapytań o usługę, problemów i zmian w dowolnym momencie po ich zarejestrowaniu.
1.239	Zarządzanie Zmianą	System powinien umożliwiać łączenie (tworzenie relacji) incydentów, zapytań o usługę, problemów i zmian przy użyciu interfejsu graficznego, ułatwiającego wyszukiwanie i wykonywanie operacji łączenia.
1.240	Zarządzanie Zmianą	System musi umożliwiać tworzenie raportów w zakresie dowolnych zarejestrowanych w systemie danych, przy czym musi istnieć możliwość definiowania tych raportów przez administratora systemu.
1.241	Zarządzanie Zmianą	System musi zapewniać możliwość tworzenia kalendarzy dostępności operatorów oraz możliwość definiowania zastępstw, aby w przypadku skierowania zmiany lub powiązanych zleceń do osoby niedostępnej, następowało przekierowanie do osoby zastępującej.
1.242	Zarządzanie Zmianą	System musi zapewniać integralność danych oraz uniemożliwiać jednoczesną modyfikację zapisów w systemie przez więcej niż jedną osobę.
1.243	Zarządzanie Zmianą	System musi zapewniać rejestrację i śledzenie historii zmian zapisów w systemie, ze wskazaniem osób dokonujących modyfikacji oraz dat i godzin modyfikacji.
1.244	Zarządzanie Zmianą	System musi zapewniać zgodność stosowanych pojęć z biblioteką dobrych praktyk ITIL v4.
1.245	Zarządzanie Zmianą	a) unikalnego numeru, b) nazwy zmiany, c) typu zmiany, d) kategorii zmiany, e) opisu zakresu zmiany, f) osoby definiującej zakres (wytwórca merytoryczny zmiany), i jego jednostki organizacyjnej, g) osoby inicjującej zmianę i jej jednostki organizacyjnej, h) osoby zgłaszającej zmianę i jej jednostki organizacyjnej, i) właściciela zmiany, j) grupy usług oraz usługi, k) statusu, l) daty i godziny nadania statusu, m) osoby nadającej status, n) priorytetu, o) powiązanych elementów konfiguracji, p) jednostek organizacyjnych lub grup użytkowników objętych zmianą, q) planowanego kosztu, r) oceny ryzyka, s) planu wdrożenia i wycofania, t) daty i godziny rejestracji, u) planowanej daty i godziny wprowadzenia, v) podstawy zmiany, w) wpływu implementacji zmiany na dostępność usług, wydajność, architekturę, bezpieczeństwo oraz konfigurację systemu, x) wykonawcy zmiany, y) informacji o zależnościach z innymi zmianami, z) linku do pakietu dystrybucyjnego, aa) terminu akceptacji zmiany,

1.246	Zarządzanie Zmianą	System musi umożliwiać rejestrację zmian powiązanych z incydentami, problemami oraz zmian niepowiązanych z incydentami i problemami.
1.247	Zarządzanie Zmianą	System musi umożliwiać wysyłanie powiadomień o zarejestrowaniu zmiany do inicjującego oraz zgłaszającego zmianę, przy czym musi istnieć możliwość definiowania treści powiadomień przez administratora systemu.
1.248	Zarządzanie Zmianą	System musi umożliwiać tworzenie zbiorczego harmonogramu zmian pozwalającego na graficzne prezentowanie zmian wg przyjętego kryterium obejmującego co najmniej: a) typ, b) kategorię, c) priorytet, d) grupę usług, e) usługę, f) element konfiguracji, g) status, h) zakres dat realizacji, w skali czasu.
1.249	Zarządzanie Zmianą	System powinien umożliwiać definiowanie okien serwisowych oraz powiadamianie o konfliktach pomiędzy terminami okien serwisowych a terminami zmian (nakładania się terminów) spełniających określone kryteria, obejmujące co najmniej: a) klienta, b) grupa usług, c) usługa, d) typ zmiany, e) wartość ryzyka zmiany. f) element konfiguracji
1.250	Zarządzanie Zmianą	System musi umożliwiać tworzenie grup zatwierdzających zmianę, przy czym powinno być możliwe utworzenie co najmniej 100 różnych grup CAB.
1.251	Zarządzanie Zmianą	System musi umożliwiać kierowanie zmian do akceptacji CAB wielokrotnie w ramach obsługi danej zmiany.
1.252	Zarządzanie Zmianą	System musi umożliwiać kierowanie zmian do akceptacji CAB w formie zleceń ze zdefiniowanym czasem realizacji.
1.253	Zarządzanie Zmianą	System musi umożliwiać tworzenie zleceń (tasks) związanych z daną zmianą do realizacji przez innych operatorów systemu, przy czym dla każdego zlecenia musi być możliwe wskazanie co najmniej: a) zakresu prac, b) terminu realizacji, c) priorytetu zmiany, d) osoby realizującej. System musi umożliwiać automatyczne powiadamianie określonej grupy osób poprzez e-mail o zdarzeniach w systemie, co najmniej o: a) upływającym czasie realizacji zmiany lub zlecenia (procent pozostającego czasu, ilość pozostającego czasu), b) o przypisaniu zmiany lub zlecenia, c) o modyfikacjach w zapisach zmiany. przy czym powinna istnieć możliwość konfigurowanie grupy powiadamianej oraz kryteriów powiadamiania przez administratora systemu.
1.254	Zarządzanie Zmianą	System powinien umożliwiać odrębny widok historii zmian statusu lub filtrowanie historii zapisu zmiany w sposób umożliwiający wyodrębnienie wyłącznie modyfikacji statusu.
1.255	Zarządzanie Zmianą	System musi umożliwiać wstrzymanie (zamrożenie) czasu realizacji zmiany.
1.256	Zarządzanie Zmianą	System musi umożliwiać wyliczanie czasu realizacji zmiany i zleceń powiązanych z daną zmianą przez poszczególne grupy wsparcia co najmniej: a) poprzez wyliczenie maksymalnego czasu realizacji oraz b) poprzez wyliczenie sumarycznego czasu realizacji (suma czasu wszystkich operatorów - czasochłonność).
1.257	Zarządzanie Zmianą	System musi umożliwiać zdefiniowanie listy zmian standardowych oraz umożliwiać przypisanie do poszczególnych zmian standardowych zdefiniowanych przebiegów workflow.
1.258	Zarządzanie Zmianą	System musi umożliwiać prezentowanie w widoku danej zmiany planowanego terminu realizacji incydentu lub problemu powiązanego z daną zmianą.
1.259	Zarządzanie Zmianą	System musi umożliwiać wykonanie co najmniej następujących akcji Menadżera Zmian dla procesowania zmiany: a) przyjęcie, b) odrzucenie, c) potrzeba uzupełnienia przez zlecającego.
1.260	Zarządzanie Zmianą	System musi umożliwiać wykonanie co najmniej następujących akcji członków CAB dla zleceń akceptacji zmiany: a) przyjęcie, b) odrzucenie, c) potrzeba uzupełnienia.

1.261	Zarządzanie Zmianą	System powinien umożliwiać wysyłanie członkom CAB w momencie generowania zleceń o akceptację, wiadomości e-mail zawierających określone informacje z zapisu zmiany oraz aktywne linki pozwalające zrealizować operacje akceptacji, odrzucenia lub prośby o uzupełnienie, bez bezpośredniego dostępu do systemu.
1.262	Zarządzanie Zmianą	System musi umożliwiać zdefiniowanie statusów dla zleceń (task) powiązanych ze zmianą, przy czym statusy te powinny obejmować co najmniej: a) zarejestrowanie, b) przyjęcie do realizacji, c) częściową realizację, d) całkowitą realizację (w przypadku zleceń na wdrożenie zmiany status powinien uwzględniać powodzenie realizacji, niepowodzenie lub wycofanie zmiany).
1.263	Zarządzanie Zmianą	System powinien umożliwiać importowanie zgłoszeń zmian do systemu przy zastosowaniu plików o określonej strukturze i formacie, co wykorzystywane ma być przy braku możliwości rejestracji zmian bezpośrednio w systemie.
1.264	Zarządzanie Zmianą	System powinien umożliwiać integrację z klientem FTP w celu pobrania pakietu dystrybucyjnego.
1.265	Zarządzanie Zmianą	System musi umożliwić budowanie reguł oceny i akceptacji Zmiany.
1.266	Zarządzanie Zmianą	System powinien udostępniać interfejs do akceptacji Wniosków o Zmianę, których realizacja jest uzależniona od akceptacji wskazanych osób lub grup.
1.267	Zarządzanie Zmianą	System powinien umożliwiać pobieranie informacji potrzebnych w cyklu obsługi Zmiany bezpośrednio z bazy np. Incydentów.
1.268	Zarządzanie Zmianą	System musi umożliwiać zdefiniowanie alarmów powiadamiających o krytycznych momentach w procesie realizacji Zmiany np. zbliżający się termin wykonania zadania.
1.269	Zarządzanie Zmianą	Powinna istnieć możliwość przypisania lub zmiany przypisania do osoby, grupy lub dostawcy.
1.270	Zarządzanie Zmianą	System powinien umożliwiać definiowanie aktywności lub zadań w cyklu realizacji Zmian, pozwalających na rozdzielenie przypisania obsługi Zmiany do specjalisty, grupy lub dostawcy.
1.271	Zarządzanie Zmianą	System musi umożliwiać kontrolę procesu Zarządzania Zmianami od momentu wpłynięcia Wniosku o Zmianę, poprzez akceptację, planowanie, przegląd, koordynację implementacji aż do rozliczania kosztów realizacji.
1.272	Zarządzanie Zmianą	System powinien zapewnić możliwość ustalanie przeglądów Zmian po zdefiniowanym okresie od wdrożenia.
1.273	Zarządzanie Zmianą	System powinien zapewnić łatwą identyfikację Incydentów (i docelowo również Problemów), które wynikły z wprowadzenia danej Zmiany.
1.274	Zarządzanie Zmianą	System musi umożliwiać prosty dostęp do informacji o planowanych Zmianach w infrastrukturze – powinien zapewnić możliwość zautomatyzowanego informowania innych procesów o bieżących i planowanych Zmianach.
1.275	Zarządzanie Zmianą	System powinien posiadać funkcjonalność obsługi Zmian masowych.
1.276	Zarządzanie Zmianą	System powinien umożliwiać automatyczne rejestrowanie rekordu Zmiany dla nieautoryzowanych zmian Elementów Konfiguracji.
1.277	Zarządzanie Zmianą	System powinien zapewnić możliwość łatwego powiązania Elementów Konfiguracji z Wnioskami o Zmianę i Zmianami. System powinien umożliwić dostęp z poziomu formatki Zmiany do szczegółowych danych Elementów Konfiguracji.
1.278	Zarządzanie Zmianą	Zakończenie Zmiany powinno wywoływać modyfikacje atrybutów Elementu Konfiguracji w bazie CMDB.
1.279	Zarządzanie Zmianą	System powinien powiadamiać o pojawieniu się wniosku o Zmianę który dotyczy elementu, już podlegającego zmianie.
1.280	Zarządzanie Zmianą	Narzędzie powinno posiadać funkcjonalność automatycznej oceny wpływu planowanej Zmiany na infrastrukturę.
1.281	Zarządzanie Zmianą	Proponowane rozwiązanie powinno umożliwiać proaktywne powiadamianie członków Rady ds. Zmian o zmianach mających wpływ na krytyczne komponenty usług.
1.282	Zarządzanie Zmianą	Proponowane rozwiązanie powinno umożliwiać rejestrowanie notatek z działań Rady ds. Zmian oraz decyzji podejmowanych przez to ciało.
1.283	Zarządzanie Zmianą	System powinien udostępniać interfejs do akceptacji, odrzucenia lub zmiany harmonogramu dla Zmiany podczas spotkania Rady ds. Zmian.
1.284	Zarządzanie Zmianą	Harmonogram przyszłych Zmian musi być prezentowany w formie graficznej z możliwością podejrzenia szczegółów danej Zmiany.
1.285	Zarządzanie Zmianą	System musi udostępniać możliwość samodzielnego budowania raportów w oparciu o bieżące potrzeby Zamawiającego.
1.286	Zarządzanie Zmianą	Narzędzie musi udostępniać graficzne narzędzie do projektowania raportów.
1.287	Zarządzanie Zmianą	System musi posiadać mechanizm do uruchamiania raportów na bazie zadanego harmonogramu i przesyłania wyników pocztą elektroniczną.
1.288	Zarządzanie Zmianą	Narzędzie musi posiadać możliwości zabezpieczające przed uruchomieniem raportów zwracających za dużą liczbę rekordów.
1.289	Zarządzanie Zmianą	System 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.
1.290	Zarządzanie Zmianą	System musi posiadać wbudowaną funkcjonalność graficznego prezentowania wybranych metryk. Uprawnieni użytkownicy powinni mieć możliwość definiowania własnych metryk.
1.291	Zarządzanie Zmianą	Narzędzie musi mieć możliwość definiowania graficznej reprezentacji zestawu danych.
1.292	Zarządzanie Zmianą	System powinien udostępniać narzędzia typu drill-down, umożliwiające dokładną analizę przedstawianych wykresów graficznych.
1.293	Zarządzanie Zmianą	System powinien posiadać możliwość definiowania dashboardów dla użytkowników i umieszczania na nich zestawień, metryk, graficznych reprezentacji wybranych danych.

1.294	Zarządzanie Zmianą	System powinien udostępniać możliwość przesyłania raportów na żądanie, za pomocą poczty elektronicznej (system odpowiada na odpowiednio sformatowany e-mail wiadomością zwrotną z żądanymi danymi).
1.295	Zarządzanie Zmianą	Narzędzie powinno umożliwiać definiowanie uprawnień do raportów.
1.296	Zarządzanie Zmianą	W celach wydajnościowych powinna istnieć możliwość osadzenia motoru raportów na oddzielnej maszynie.
1.297	Zarządzanie Zmianą	Oferowany System musi mieć możliwość prezentowania co najmniej następujących raportów: - Liczba Wniosków o Zmianę zarejestrowanych w danym okresie czasu; - Liczba Wniosków o Zmianę zamkniętych w danym okresie czasu; - Liczba Wniosków o Zmianę w danym okresie czasu w podziale na poszczególne statusy jego obsługi; - Liczba Wniosków o Zmianę w podziale na poszczególne Usługi IT.

Lp WKR	Typ	Opis
2.1	Administracja - Bezpieczeństwo	Baza musi mieć możliwość nadawania przez Administratora/Operatorom, uprawnień Użytkownikom do widoczności danych, przeglądania danych bez możliwości ich modyfikacji.
2.2	Administracja - Bezpieczeństwo	Baza musi mieć możliwość definiowania przez Administratora profili użytkowników, w ramach których będą określanie poziomy widoczności elementów bazy oraz uprawnienia do modyfikacji CI jak i relacji. Profil widoczności musi dawać możliwość określenia poziomu widoczności dla każdego atrybutu CI jak i rekordu w bazie. System musi umożliwiać definiowanie profili w podziale na możliwe do wykonania akcje takie jak, tworzenie nowych obiektów (insert), aktualizację dancy (update), odczyt (read). Konfiguracja musi także dawać możliwość określania funkcjonalności systemu dostępnych w ramach profilu.
2.3	Administracja - Bezpieczeństwo	Baza musi posiadać zabezpieczoną (szyfrowanie ruchu) komunikację pomiędzy integrowanymi aplikacjami a CMDB w oparciu o aktualne standardy na rynku.
2.4	Administracja - Bezpieczeństwo	Baza musi zapewniać możliwość ustawienia przez Administratora ilości i długości czasu trwania sesji, po której baza samoczynnie wyloguje bezczynnego Administratora, Operatora, Użytkownika.
2.5	Administracja - Bezpieczeństwo	System musi mieć możliwość wydzielenia oddzielnej instacji, działającej na oddzielnej infrastrukturze.
2.6	Administracja - Bezpieczeństwo	Baza musi umożlwiać przeprowadzenie testów bezpieczeństwa przez podmiot trzeci posiadający odpowiednie kompetencje i doświadczenie bez wsparcia Wykonawcy.
2.7	Administracja - Bezpieczeństwo	Baza musi umożlwiać korzystanie z uwierzytelniania wieloskładnikowego (MFA).
2.8	Administracja - Bezpieczeństwo	Baza musi umożliwiać definiowanie ról dostępu do informacji w zależności od rodzaju i autoryzacji Użytkownika Systemu i zapobiegać nieautoryzowanemu dostępowi poprzez wbudowane mechanizmy bezpieczeństwa. Jeśli baza zarządza hasłami lokalnego Użytkownika , powinien udostępniać mechanizm wymuszający ich kontrolę np. w postaci minimalnej długości hasła, maksymalnego czasu ważności hasła, historii haseł (wymuszenie unikalności haseł), złożoności hasła.
2.9	Administracja - Bezpieczeństwo	Baza musi umożliwiać integrację z zewnętrznymi dostawcami w przypadku tworzenia zewnętrznych tożsamości za pomocą protokołów SAML, OpenID, LDAP, OAuth 2.0, Kerberos.
2.10	Administracja - Bezpieczeństwo	Zamawiający nie dopuszcza udostępniania, przekazywania danych z bazy poza infrastrukturę Zamawiającego bez jego wiedzy i zgody.
2.11	Administracja - Bezpieczeństwo	Baza musi zapewniać bezpieczeństwo komunikacji. Przesyłane dane muszą być zabezpieczone i szyfrowane za pomocą protokołu TLS w wersji co najmniej 1.2 oraz system musi wspierać wersję 1.3.
2.12	Administracja - Bezpieczeństwo	Baza musi zapewniać logowanie, przeglądanie i raportowanie zdarzeń systemowych wg zadanych kryteriów (zakresu) umożliwiających identyfikację czasu, osoby, rodzaju i sposobu wykonania czynności na danym obiekcie oraz prób nieautoryzowanego dostępu w tym sposób umożliwiający odtwarzanie historii aktywności Użytkowników Systemu .
2.13	Administracja - Bezpieczeństwo	Baza musi posiadać funkcjonalność anonimizacji danych osobowych (zgodnie z przepisami RODO) w sposób uniemożliwiający powiązanie "zdarzenia" (działanie, operacja itp.) z użytkownikiem, jednocześnie niezakłócający ciągłosci działania systemu.
2.14	Administracja - Bezpieczeństwo	Baza musi mieć możliwość szyfrowania przechowywanych danych.
2.15	Administracja - Bezpieczeństwo	Baza musi posiadać funkcjonalność przeglądania logów systemowych i innych zdarzeń za pomocą filtrów.
2.16	Administracja - Bezpieczeństwo	Baza musi pozwalać na przesyłanie logów ze zdarzeń do zewnętrznego serwera logów za pomocą protokołu syslog.
2.17	Administracja - Bezpieczeństwo	Baza musi zapewniać stosowanie mechanizmów uwierzytelniania Administratorów, Operatorów, Użytkowników. Logowanie SSO z dodatkowym zabezpieczeniem 2FA (MS Authenticator)
2.18	Administracja - Bezpieczeństwo	System musi zapewniać mechanizmy do zarządzania i audytowania urządzeń zapory sieciowej, takie jak możliwość tworzenia raportów audytowych zapory sieciowej.
2.19	Administracja - Infrastruktura	Baza CMDB musi umożliwiać tworzenie całkowitych, przyrostowych kopii bezpieczeństwa (automatyczne oraz manualne) i danych w trybie on-line oraz zapewniać procedurę przywracania CMDB z kopii bezpieczeństwa po Awarii. W tym zakresie system CMDB powinien umożliwiać współpracę z wiodącymi systemami kopii zapasowej (np. Veeam, Commvault, Networker)
2.20	Administracja - Infrastruktura	Dostawca musi określić wymagania infrastrukturalne dla płynnego działania bazy o parametrach: 1 mln CI, generowania raportów agregowanych z całej bazy w czasie krótszym niż 3 min, jednoczesnej pracy 500 użytkowników bez widocznych spowolnień systemu. Przy ilości operacji X/min
2.21	Administracja - Infrastruktura	System musi skalować się do wielkości bazy 5 mln CI z zachowaniem parametrów wydajnościowych opisanych w pkt A1.1
2.22	Administracja - Infrastruktura	Wykonawca określi wymagania dla środowiska CMDB (ilość serwerów, systemy operacyjne, bazy danych i inne). Środowisko musi być skalowalne, dawać możliwość zwiększenia wydajności poprzez rozbudowę infrastruktury, np. serwerów (w szczególności poprzez dodanie procesorów, pamięci RAM, zwiększenie liczby serwerów).
2.23	Administracja - Infrastruktura	CMDB musi posiadać możliwość instalacji na platformie konteneryzacyjnej (np. Kubernetes, Openshift). Zamawiający dopuszcza rozwiązanie, w którym główna baza danych nie jest skonteneryzowana.
2.24	Administracja - Infrastruktura	Środowisko produkcyjne bazy musi umożliwiać instalację w dwóch równolegle pracujących ośrodkach.
2.25	Administracja - Infrastruktura	Baza musi zapewniać procedury naprawcze na wypadek wystąpienia Awarii, umożliwiające przywrócenie bazy do stanu sprzed Awarii, na podstawie kryteriów zdefiniowanych przez Administratora. Rozwiązanie dla serwerów aplikacyjnych i bazodanowych.
2.26	Administracja - Infrastruktura	Baza powinna składać się z trzech niezależnych środowisk: produkcyjne, testowe, developerskie.
2.27	Administracja - Infrastruktura	Dane generowane przez bazę powinny być zbierane w jednolitym jeziorze danych, do którego wszystkie moduły systemu posiadają dostęp i możliwość przeszukiwania danych w identyczny sposób. Zastosowana technologia jeziora danych musi być wspierana przez producenta oprogramowania. Jeżeli wykorzystanie go wymaga dodatkowych licencji, należy je dostarczyć na rekomendowaną dla tego wdrożenia pojemność. Funkcjonalność ta musi być niezależna od głównej bazy danych rozwiązania.

2.28	Administracja - Infrastruktura	Technologia jeziora danych musi wspierać przeszukiwanie i analizę danych za pomocą co najmniej następujących języków danych: SQL, Python, R, Java. Dodatkowo, powinno umożliwiać integrację z narzędziami klasy Business Intelligence (takimi jak Power BI, Qlik, Tableau).
2.29	Administracja - Infrastruktura	Baza musi spełniać parametry RTO = 4 godziny, RPO = 5 minut. Architektura Bazy powinna zapewnić dostępność systemu na poziomie 99,8%, bez wliczania ustalanych wcześniej przerw serwisowych.
2.30	Administracja - Integracja	Integracja pomiędzy bazą CMDB a Discovery/SAM/HAM Baza musi umożliwiać utworzenie Elementów konfiguracji pochodzących z różnych źródeł; na podstawie danych z pliku, narzędzi automatycznego wykrywania elementów infrastruktury (Discovery/SAM/HAM), wprowadzanych ręcznie. W przypadku elementów wykrytych przez (Discovery/SAM/HAM) system musi automatycznie je sklasyfikować oraz wypełnić pola atrybutów dostępnymi informacjami. Celem wymagania jest możliwość wykonywania audytów zgodności pomiędzy informacjami pochodzącymi z Discovery a znajdującymi się w CMDB. Dodatkowo w przypadku wykrycia CI, zależy nam na automatyzacji części procesu tworzenia nowego CI.
2.31	Administracja - Integracja	Integracja pomiędzy bazą CMDB a Discovery/SAM/HAM Baza musi automatycznie przyjmować i wykorzystywać informacje o znacznikach oprogramowania. Celem jest wykorzystanie potencjału znaczników w celu budowania relacji pomiędzy CI oraz mapowaniem CI względem usług z katalogu usług. Wykrywane mają być m, in. aplikacje stworzone przez zamawiającego.
2.32	Administracja - Integracja	Integracja pomiędzy bazą CMDB a Discovery/SAM/HAM Baza musi umożliwiać zbieranie danych z różnych źródeł (Discovery, Monitoring, SCCM, pliki płaskie) celem zasilenia CMDB z możliwością ustalania priorytetów źródeł i korelowania danych z tych źródeł (wieloźródłowość). Celem jest możliwość wykorzystania wielu źródeł informacji do uzupełniania/aktualizacji bazy CMDB
2.33	Administracja - Integracja	Integracja pomiędzy bazą CMDB a Discovery/SAM/HAM Baza musi posiadać mechanizmy do automatycznego tworzenia relacji/zależności elementów konfiguracji z usługami, umowami w oparciu o znaczniki oprogramowania oraz analizę ruchu sieciowego. Celem jest automatyzacja tworzenia relacji pomiędzy CI oraz relacji pomiędzy CI a usługami.
2.34	Administracja - Integracja	Integracja pomiędzy bazą CMDB a Discovery/SAM/HAM Baza musi umożliwić rekoncyliację danych o Elementach konfiguracji pochodzących z różnych źródeł i definiować dowolnie reguły pozwalające na ich analizę. Reguły rekoncyliacji muszą być możliwe do definiowania dla każdej klasy oraz każdego atrybutu. System musi umożliwiać priorytetyzację źródeł. Celem jest umożliwienie operatorowi definiowanie reguł na podstawie których będą rozstrzygane rozbieżności w informacjach pochodzących z dwóch źródeł a dotyczących jednego atrybutu w konkretnym CI
2.35	Administracja - Integracja	Integracja pomiędzy bazą CMDB a Discovery/SAM/HAM Baza musi umożliwiać automatyczne przenoszenie wartości z rekordów w systemach SAM/HAM do atrybutów CI. Operator musi mieć możliwość ustalenia które atrybuty CI mają podlegać w. w. przenoszeniu. Celem jest uniknięcie pracy manualnej w przypadku zmian CI wykonanych przez operatorów systemu SAM/HAM. Zmiana taka powinna automatycznie przenieść się do CMDB. Operatorzy CMDB powinni mieć możliwość definiowania, które atrybuty podlegają automatycznej aktualizacji
2.36	Administracja - Integracja	Integracja pomiędzy bazą CMDB a Discovery/SAM/HAM Baza CMDB musi posiadać możliwość integracji z innymi systemami jak : HAM , SAM, Discovery. Poprzez integracje musi istnieć możliwość przesyłania wszystkich informacji przechowywanych w HAM , SAM, Discovery. Celem wymagania jest uniknięcie sytuacji w której nie wszystkie informacje zbierane przez Discovery/SAM/HAM mogą być automatycznie importowane do CMDB w postaci rzeczywistych elementów konfiguracji, podlegających dalszej weryfikacji przez operatora.

2.37	Administracja - Integracja	Integracja pomiędzy bazą CMDB a repozytoriami producentów sprzętu Baza CMDB automatycznie pobiera informacje o dacie end of life sprzętu produkowanego przez: IBM Cisco Microsoft APPLE DELL HP Oracle Celem wymagania jest ograniczenie manualnej pracy operatora związanej z ustaleniem i uzupełnieniem daty EOL
2.38	Administracja - Integracja	Integracja pomiędzy bazą CMDB a Discovery/SAM/HAM Baza CMDB musi przydzielać poziom krytyczności danego CI w kontekście świadczonej usługi na podstawie danych dostarczonych przez Discovery/HAM/SAM. Poziom krytyczności musi być dodatkowo zatwierdzony przez operatora. Celem wymagania jest zautomatyzowanie procesu w wyniku którego zostanie określony poziom krytyczności (zatwierdzony przez operatora) danego CI pod kątem usługi z uwzględnieniem że jeden CI może być elementem składowym wielu usług jednocześnie.
2.39	Administracja - Integracja	Integracja pomiędzy bazą CMDB a bazą ITSM Atmosferą. Założenia: 1. Proces zmiany (wniosków RFC) będzie realizowany w ITSM Atmosfera 2. Bazą CMDB referencyjną będzie nowa baza która jest przedmiotem zamówienia 3. Zespół zarządzający konfiguracją będzie otrzymywał zlecenie pracy w nowym ITSM dotyczące modyfikacji/utworzenia CI. Zlecenie pracy będzie wywoływane statusem RFC w ITSM Atmosfera. Zamkniecie zlecenia pracy będzie wywoływało zmianę statusu RFC w ITSM Atmosfera Cel: 1. Celem jest przeniesienie danych z nowego CMDB do CMDB Atmosfera w sposób cykliczny i na żądanie. 2. Zrelacjonowanie RFC z CI (który zostanie utworzony w nowym CMDB w wyniku zmiany) w CMDB Atmosfera.
2.40	Administracja - Integracja	Integracja pomiędzy bazą CMDB a Atmosferą Baza CMDB musi posiadać możliwość integracji z obecnym systemem ITSM Atmosfera w celu przesyłania danych w sposób cykliczny i na żądanie z nowej bazy CMDB do ITSM Atmosfera. Przesyłane będą informacje: -Atrybuty CI mające swoje odpowiedniki w ITSM Atmosfera -Relacje pomiędzy CI np. relacja pomiędzy aplikacją a VM -Informacje o nowo wykrytych CI (przesyłane będą dane w zakresie atrybutów rejestrowanych w ITSM Atmosfera) -Informacje o zmianie w atrybucie CI Integracja będzie odbywać się poprzez API ITSM Atmosfera (API jest obecnie na etapie planowania) zdolnego do przyjęcia wszystkich wymienionych powyżej informacji lub poprzez komunikację z bazą danych ITSM Atmosfera za pośrednictwem proxy. Celem wymagania jest synchronizacja pomiędzy CMDB Atmosfera a nowym CMDB tak aby w obu bazach znajdowały się identyczne informacje (w zakresie atrybutów ITSM Atmosfera). Synchronizacja będzie jednokierunkowa, informacje będą przesyłane jedynie z nowej bazy do bazy w ITSM Atmosfera.
2.41	Administracja - Integracja	Baza CMDB musi umożliwiać integrację poprzez: 1) API 2) usługi sieciowe (Web Services), 3) dokumenty w formacie XML, 4) e-mail, 5) płaskie pliki tekstowe. 6) interfejsy bazodanowe 7) PowerShell 8) SSH 9) ODBC/JDBC 10) LDAP

2.42	Administracja - Integracja	Integracja systemu ITSM z Microsoft System Center Configuration Manager (SCCM) Zakres integracji Baza musi umożliwiać: 1. Automatyczne importowanie i synchronizację danych o zasobach IT z SCCM. 2. Monitorowanie stanu i zdrowia zasobów zarządzanych przez SCCM. 3. Wykorzystanie danych SCCM do zarządzania cyklem życia zasobów w systemie ITSM. Dane potrzebne Dane o zasobach IT: 1. Informacje o urządzeniach (komputery, serwery, urządzenia mobilne). 2. Dane o zainstalowanym oprogramowaniu i jego wersjach. 3. Statusy i konfiguracje urządzeń. 4. Informacje o zgodności urządzeń z politykami bezpieczeństwa. Dane o użytkownikach: 1. Informacje o przypisanych użytkownikach do poszczególnych urządzeń. 2. Historia działań związanych z zasobami. Celem jest wykorzystanie SCCM jako systemu wspierającego Discovery/Monitoring.
2.43	Administracja - Ogólno funkcjonalne	Baza musi umożliwiać Operatorom wyszukiwanie Elementów konfiguracji przy użyciu słów kluczowych, ciągów znaków w tym niepełnych wyrazów, fragmentów tekstu z użyciem operatorów logicznych (I, LUB, ORAZ).
2.44	Administracja - Ogólno funkcjonalne	Baza musi posiadać możliwość zarządzania przez Operatorów tabelami CI tj. możliwość ukrywania i odkrywania kolumn, możliwość sortowania danych w tabeli po wskazanej kolumnie, możliwość filtrowania danych po każdej kolumnie, możliwość eksportu danych do pliku XLSX.
2.45	Administracja - Raportowanie	Baza musi umożliwiać tworzenie raportów w zakresie zmian w konfiguracji Elementów konfiguracji bez konieczności pisania zapytań w języku bazy danych i udostępniać gotowy interfejs do budowania takich raportów.
2.46	Administracja - Raportowanie	Baza musi umożliwiać tworzenie dowolnych raportów w zakresie określonych przez Operatora na podstawie atrybutów, relacji/zależności, umów, CI. Przy czym musi istnieć możliwość zapisu takiego raportu w pliku zewnętrznym w formacie co najmniej jeden z wymienionych : XLS,XLSX,PDF,CSV. Musi istnieć możliwość generowania takich wielu raportów jednym zleceniem dla zadanej grupy Elementów konfiguracji np. raport utworzony CI w danym miesiącu, przy czym raporty były by podzielone ze względu na usługę i reprezentowane jako oddzielny plik do pobrania. Musi być również możliwość pisania zapytań bezpośrednio w bazie danych. W języku obsługującym bazę danych. Z możliwością zapisania zapytania jako szablonu w celu późniejszego wykorzystania.
2.47	Administracja - Raportowanie	Baza musi umożliwiać operatorowi, poprzez interfejs graficzny, tworzenie złożonych zapytań w bazie CMDB. Interfejs graficzny musi odzwierciedlać aktualną strukturę bazy CMDB. System musi umożliwiać zapisanie szablonu raportu.
2.48	Administracja - Raportowanie	System musi mieć możliwość definiowania harmonogramu generowania raportów.
2.49	Administracja - Raportowanie	Wynik zapytań do bazy danych musi być prezentowany w formie tabeli w systemie oraz musi być możliwy do pobrania w formie pliku.
2.50	Administracja - Raportowanie	W przypadku generowania raportów, operator musi mieć możliwość filtrowania rekordów nie tylko po wartości ale także po zakresie wartości. Np. CI z zakresu dat, CI o wartości RAM poniżej X itd.
2.51	Administracja - Raportowanie	Zapisane szablony raportów muszą umożliwiać definiowanie filtrów ustalanych trwale, definiowane każdorazowo w momencie zlecenia raportu oraz filtrów względnych np. raport za ostatni miesiąc/kwartał/rok.
2.52	Administracja - Raportowanie	Szablony raportów muszą podlegać pod reguły grup widoczności. Udostępnieniem musi zarządzać operator oraz administrator
2.53	Administracja - Wdrożenie	W przypadku infrastruktury o wyższym poziomie klauzuli niejawności, dostawca pozyska niezbędne poświadczenia bezpieczeństwa we własnym zakresie.
2.54	Baza CMDB - Ogólne - prezentacja treści	Baza CMDB musi umożliwiać prezentację graficzną bazy CMDB, która zawiera Elementy konfiguracji, relacje i zależności pomiędzy Elementami konfiguracji, relacje i zależności pomiędzy Elementami konfiguracji a Usługami, Incydentami, Zmianami itp...
2.55	Baza CMDB - Ogólne - prezentacja treści	Baza CMDB musi umożliwiać prezentację graficzną , która zawiera : 1. Elementy konfiguracji powiązane z konkretnym zleceniem pracy wraz z relacjami. Przykład: zlecenie pracy dotyczy utworzenia 10 nowych VM na 5 różnych serwerach. Widok graficzny z poziomu zlecenia pracy przedstawiałby wspomniane VM wraz z relacjami/zależnościami do innych CI.
2.56	Baza CMDB - Ogólne - prezentacja treści	Możliwość nawigacji z poziomu CI, umowy, usługi pomiędzy elementami nadrzędnymi i podrzędnymi oraz powiązanymi/zależnymi. Np. na stronie elementu konfiguracji poprzez jedno kliknięcie operator jest w stanie przejść do elementu nadrzędnego jak i podrzędnego oraz powiązanego/zależnego.
2.57	Baza CMDB - Ogólne - prezentacja treści	Baza musi dawać Operatorom możliwość dowolnego dostosowywania/modyfikacji layout'u/dashboardu/portletu etc. bez konieczności angażowania Administratora systemu. Również musi być możliwość zapisywania wielu widoku/restartowanie go do ustawień początkowych. Musi być możliwość wyboru indywidualnego widoku domyślnego.
2.58	Baza CMDB - Ogólne - prezentacja treści	Baza musi umożliwiać Operatorowi płynne (kilka kliknięć) przechodzenie pomiędzy elementami konfiguracji połączonymi w relacje. Np. Z poziomu CI operator ma dostęp do listy powiązanych CI. Lista ta może być filtrowana. Jednym kliknięciem operator jest w stanie przejść do wylistowanego CI.
2.59	Baza CMDB - Ogólne - prezentacja treści	W przypadku gdy lista CI będzie wyświetlana na wielu stronach, operator musi mieć możliwości bezpośredniego przejścia do dowolnej strony z listy
2.60	Baza CMDB - Ogólne - prezentacja treści	Baza CMDB musi umożliwiać pracę na minimum 5 zakładkach w jednej przeglądarce jednocześnie, funkcjonalność ta musi działać niezależnie od przeglądarki internetowej.

2.61	Baza CMDB - Ogólne - prezentacja treści	Baza CMDB musi informować operatora o tym że inny operator jest na danym CI wraz z informacją o nazwie operatora.
2.62	Baza CMDB - Ogólne - prezentacja treści	Baza musi mieć możliwość wyszukiwanie CI po każdym z dostępnych atrybutów oraz relacji. Lista wyników musi być modyfikowalna w taki sposób że operator może wybrać dowolny atrybut jako kolumnę na liście wyników.
2.63	Baza CMDB - Ogólne - prezentacja treści	Historia zmian CI powinna zwierać informacje o dacie zmiany, źródle zmiany, wartości przed zmianą oraz po zmianie. Historia musi być widoczna dla wszystkich operatorów zarządzających CMDB. Historia zmian musi być rejestrowana dla wszystkich rekordów w bazie.
2.64	Baza CMDB - Ogólne - prezentacja treści	Widok graficzny relacji musi być konfigurowalny w taki sposób, aby operator mógł zobaczyć wybrane atrybuty powiązanych CI
2.65	Baza CMDB - Ogólne - prezentacja treści	Administrator musi mieć możliwość modyfikacji układu prezentowanych atrybutów w oknie CI
2.66	Baza CMDB - Ogólne - struktura bazy	Baza musi być wyposażona w gotową i całkowicie edytowalną klasyfikację (minimum 2-stopniową tj. odpowiedniki typu podtyp w ITSM Atmosfera) dla Elementów konfiguracji (klasy CI) wraz z predefiniowanymi atrybutami dla poszczególnych klas oraz relacjami pomiędzy elementami. Wymienione wyżej szablony muszą być edytowalne przez Administratora i Operatora.
2.67	Baza CMDB - Ogólne - struktura bazy	Baza CMDB musi posiadać gotową i edytowalną klasyfikację elementów konfiguracji odzwierciedlające wszystkie typy i podtypy CI wypisane w zakładce "Typy i podtypy CI w Atmosfera". Edycja musi być możliwa przez Administratora i Operatora.
2.68	Baza CMDB - Ogólne - struktura bazy	Baza musi umożliwiać tworzenie nowych atrybutów Elementów konfiguracji, przy czym musi istnieć możliwość definiowania tych atrybutów przez Administratora i Operatora.
2.69	Baza CMDB - Ogólne - struktura bazy	Baza musi umożliwiać tworzenie nowych klas Elementów konfiguracji, przy czym musi istnieć możliwość definiowania tych klas przez Administratora i Operatora.
2.70	Baza CMDB - Ogólne - struktura bazy	Baza musi umożliwiać Administratorowi i Operatorowi definiowanie relacji/zależności (np. "zależy od", "wspiera", "cześć", "zawiera", "połączone z", "hostowany przez", "dostarcza", "wykorzystuje", "zarządzany przez", "własność").
2.71	Baza CMDB - Ogólne - struktura bazy	Baza musi posiadać możliwość wprowadzenia i dowolnej modyfikacji umów na zakup, serwis i utrzymanie sprzętu. Oraz budowanie relacji umów/usług serwisowych z każdym CI oraz usługami z katalogu usług (tworzenie relacji musi być możliwe z poziomu CI jak i umowy, usługi). Umowa musi być reprezentowana jako jeden nadrzędny obiekt składający się z kilku podrzędnych, reprezentujących poszczególne usługi serwisowe. Usługi serwisowe musza mieć możliwości definiowania indywidualnych danych kontaktowych, czasów realizacji, harmonogramu dostępności.
2.72	Baza CMDB - Ogólne - struktura bazy	Baza musi zachowywać ciągłość numeracji wszystkich rekordów Baza nadaje numer rekordu dopiero po jego zapisaniu w systemie.
2.73	Baza CMDB - Ogólne - struktura bazy	Baza musi umożliwiać definiowanie przez operatora wszystkich atrybutów wymaganych do wypełnienia przy zapisie danego typu obiektu w bazie oraz uniemożliwiać zarejestrowanie elementu bez wypełnienia tych pól.
2.74	Baza CMDB - Ogólne - struktura bazy	Baza CMDB musi mieć możliwość definiowania Właściciela Biznesowego i Technicznego dla CI. Możliwość dodania kilku właścicieli z każdej kategorii.
2.75	Baza CMDB - Ogólne - struktura bazy	Administrator musi mieć możliwość definiowania zasad maskowania pola w atrybucie. Np. ile znaków ma być widocznych w danym polu.
2.76	Baza CMDB - Ogólne - zarządzanie CI	Administrator musi mieć możliwość definiowania nowych wartości słownika.
2.77	Baza CMDB - Ogólne - zarządzanie CI	Administrator musi mieć możliwość edytowania wartości domyślnych dla atrybutów. Typu danych w atrybucie. Długości pola w atrybucie.
2.78	Baza CMDB - Ogólne - zarządzanie CI	Administrator musi mieć możliwość definiowania wartości domyślnych dla atrybutów. Typu danych w atrybucie. Długości pola w atrybucie.
2.79	Baza CMDB - Ogólne - zarządzanie CI	Modyfikacja wartości ze słownika jakiegokolwiek parametru/atrybutu/usługi/umów/klasyfikacji może zostać wykonane, bez uprzedniego wykasowywania w.w. wartości z atrybutu CI. Zmiana statusu wartości słownikowej na nieaktywną nie wywołuje zmiany wartości (tej dezaktywowanej ze słownika)w atrybucie w CI. Po dezaktywacji wartości ze słownika, w CI pozostaje nadal wartość zdezaktywowana. W przypadku modyfikacji wartości w słowniku, zmodyfikowane zostaną automatycznie wartości w atrybutach CI. W przypadku modyfikacji słownika wartości która jest wykorzystywana w CI, baza powinna poinformować operatora o tym fakcie.
2.80	Baza CMDB - Ogólne - zarządzanie CI	Baza musi udostępniać mechanizmy wspierające realizację audytu zgodności informacji(pochodzących z różnych źródeł (Discovery/SAM/HAM) o stanie Elementu konfiguracji w CMDB ze stanem faktycznym potwierdzonym przez Operatora, możliwość modyfikowania dowolnej informacji przez uprawnionego Operatora przy zachowaniu historii zmian oraz możliwości określenia przyczyny zmiany oraz źródła informacji (operator lub system zintegrowany).
2.81	Baza CMDB - Ogólne - zarządzanie CI	Baza musi umożliwiać Operatorowi tworzenie nowych Elementów Konfiguracji poprzez wykorzystanie jako szablonu Elementów konfiguracji już zarejestrowanych. W momencie tworzenia szablonu musi istnieć możliwość wyboru jakie atrybuty relacje/zależności zostaną przeniesione.

2.82	Baza CMDB - Ogólne - zarządzanie CI	Baza musi posiadać mechanizmy umożliwiające wsparcie utrzymania zdrowej Bazy Konfiguracji (CMDB), w tym wskaźniki takie jak: * Wykrywanie osieroconych (niepowiązanych lub takich które nie są zrelacjonowane, zgodnie z predefiniowanym szablonem relacji) elementów * Wykrywanie duplikatów * oraz wykrywanie brakujących danych w wskazanych jako wymagane w CMDB. Baza powinna posiadać gotowy przepływ pracy do zarządzania wykrytymi anomaliami.
2.83	Baza CMDB - Ogólne - zarządzanie CI	Baza musi umożliwiać zarządzanie relacjami dla wielu elementów jednocześnie. Tworzenie relacji pomiędzy wszystkimi rekordami bazy musi być możliwe z poziomu każdego rekordu. Przykładowo po wyszukaniu incydentu jest możliwość powiązania go z wieloma CI które mogą być wyszukane w oddzielnym okienku.
2.84	Baza CMDB - Ogólne - zarządzanie CI	Baza musi umożliwiać Operatorowi łączenie oraz modyfikowanie (tworzenie zależności i relacji) pomiędzy wszystkimi rekordami (Incydentami, Wnioskami o usługę, Problemami, Zmianami, Wydaniami, Elementami konfiguracji, umowami itd.) bez konieczności zmiany statusu.
2.85	Baza CMDB - Ogólne - zarządzanie CI	baza musi umożliwiać grupowanie rekordów w oparciu o atrybuty, klasyfikacje, relacje oraz wykonywanie operacji masowych na tych rekordach w bazie (przynajmniej w zakresie Elementów konfiguracji, Umów serwisowych Użytkowników) oraz nawigowanie między nimi z poziomu widoku Operatora i Administratora.
2.86	Baza CMDB - Ogólne - zarządzanie CI	Operator musi mieć możliwość zarządzania CI poprzez edytowanie każdego atrybutu, statusu, relacji.
2.87	Baza CMDB - Ogólne - zarządzanie CI	Baza musi posiadać mechanizm automatycznej aktualizacji każdego atrybutu/relacji/zależności w wielu Elementach Konfiguracji(dla każdego typu/podtypu CI) na podstawie pliku wsadowego. Dostawca jest zobowiązany do dostarczenia dokładnej instrukcji oraz pliku testowego/edytowalnego do wykorzystania przez operatora bazy cmdb. Identyczny mechanizm musi być dostępny dla tworzenia nowych CI.
2.88	Baza CMDB - Ogólne - zarządzanie CI	System musi mieć możliwość definiowania reguł nadawania nr ID nowym CI np. ID CI wypełniany z listy słownikowej według reguły indexu co automatycznie wypełnia atrybuty. Przykładowo - w polu identyfikator wyzwalane są 3 słowniki, wybór wartości z 3 słowników tworzy jednocześnie identyfikator CI oraz wypełnia atrybuty.
2.89	Baza CMDB - Ogólne - zarządzanie CI	Baza musi umożliwiać autoryzowanie rzeczywistego elementu konfiguracji w prosty sposób (kilka kliknięć). System musi umożliwiać masową autoryzację rzeczywistych elementów konfiguracji np. poprzez zaznaczenie checkboxu na liście rzeczywistych CI a następnie jednym kliknięciem przycisku "Autoryzuj".
2.90	Baza CMDB - Ogólne - zarządzanie CI	Wykryte przez discovery zmiany w CI muszą być w prosty sposób możliwe do naniesienia na autoryzowane CI.

Lp WKR	Typ	Opis
3.1	Administracja - Bezpieczeństwo	System nie może przechowywać żadnych danych logowania i hasła (nawet zaszyfrowanych) na końcowym punkcie inwentaryzowanym.
3.2	Administracja - Bezpieczeństwo	System musi umożliwiać definiowanie numeru portu, na którym odbywa się komunikacja z agentami.
3.3	Administracja - Bezpieczeństwo	System musi posiadać funkcjonalność zapobiegania nieautoryzowanemu dostępowi poprzez wbudowane mechanizmy bezpieczeństwa.
3.4	Administracja - Bezpieczeństwo	System musi umożliwiać obsługę niezależnych instancji, wydzielenie wszystkich informacji w zakresie zdefiniowanej jednostki organizacyjnej, zapewniając pełną izolację danych, kont oraz personalizacje paneli Użytkowników w podziale na Klientów (multi-Tenant).
3.5	Administracja - Bezpieczeństwo	System musi zapewniać stosowanie mechanizmów uwierzytelniania Administratorów, Operatorów. Logowanie SSO z dodatkowym zabezpieczeniem 2FA (MS Authenticator)
3.6	Administracja - Bezpieczeństwo	System musi umożlwiać przeprowadzenie testów bezpieczeństwa przez podmiot trzeci posiadający odpowiednie kompetencje i doświadczenie bez wsparcia Wykonawcy.
3.7	Administracja - Bezpieczeństwo	System musi umożlwiać korzystanie z uwierzytelniania wieloskładnikowego (MFA).
3.8	Administracja - Bezpieczeństwo	System musi umożliwiać definiowanie ról dostępu do informacji w zależności od rodzaju i autoryzacji Użytkownika Systemu i zapobiegać nieautoryzowanemu dostępowi do Systemu poprzez wbudowane mechanizmy bezpieczeństwa. Jeśli System zarządza hasłami lokalnego Użytkownika Systemu powinien udostępniać mechanizm wymuszający ich kontrolę np. w postaci minimalnej długości hasła, maksymalnego czasu ważności hasła, historii haseł (wymuszenie unikalności haseł), złożoności hasła.
3.9	Administracja - Bezpieczeństwo	System musi umożliwiać integrację z zewnętrznymi dostawcami w przypadku tworzenia zewnętrznych tożsamości za pomocą protokołów SAML, OpenID, LDAP, OAuth 2.0, Kerberos.
3.10	Administracja - Bezpieczeństwo	Zamawiający nie dopuszcza udostępniania, przekazywania danych z Systemu poza infrastrukturę Zamawiającego bez jego wiedzy i zgody.
3.11	Administracja - Bezpieczeństwo	System musi zapewniać bezpieczeństwo komunikacji. Przesyłane dane muszą być zabezpieczone i szyfrowane za pomocą protokołu TLS w wersji co najmniej 1.2 oraz system musi wspierać wersję 1.3.
3.12	Administracja - Bezpieczeństwo	System musi zapewniać logowanie, przeglądanie i raportowanie zdarzeń systemowych wg zadanych kryteriów (zakresu) umożliwiających identyfikację czasu, osoby, rodzaju i sposobu wykonania czynności na danym obiekcie oraz prób nieautoryzowanego dostępu w tym sposób umożliwiający odtwarzanie historii aktywności Użytkowników Systemu .
3.13	Administracja - Bezpieczeństwo	System musi posiadać funkcjonalność anonimizacji danych osobowych (zgodnie z przepisami RODO) w sposób uniemożliwiający powiązanie "zdarzenia" (zgłoszenie, działanie, operacja itp.) z użytkownikiem, jednocześnie niezakłócający ciągłosci działania systemu.
3.14	Administracja - Bezpieczeństwo	System musi mieć możliwość szyfrowania przechowywanych danych.
3.15	Administracja - Bezpieczeństwo	System musi posiadać funkcjonalność przeglądania logów systemowych i innych zdarzeń za pomocą filtrów.
3.16	Administracja - Bezpieczeństwo	System musi pozwalać na przesyłanie logów ze zdarzeń do zewnętrznego serwera logów za pomocą protokołu syslog.
3.17	Administracja - Bezpieczeństwo	System musi zapewniać komunikację platformy z oprogramowaniem agenta za pośrednictwem serwera pośredniczącego (kolektora), którego zadaniem jest miedzy innymi ograniczenie komunikacji pomiędzy podsieciami oraz agregowanie danych przesyłanych do platformy.
3.18	Administracja - Bezpieczeństwo	System musi umożliwiać definiowanie numeru portu, na którym odbywa się komunikacja z agentami.
3.19	Administracja - Bezpieczeństwo	System musi posiadać funkcjonalność tworzenia i odzyskiwania kopii zapasowej danych.
3.20	Administracja - Bezpieczeństwo	System musi posiadać zabezpieczoną (szyfrowanie ruchu) komunikację pomiędzy agentem a Systemem w oparciu o aktualne standardy na rynku.
3.21	Administracja - Infrastruktura	System musi umożliwiać definiowanie przez Administratora uprawnień i przypisanie ich do użytkowników lub grup użytkowników.
3.22	Administracja - Infrastruktura	System musi posiadać możliwość budowy kopii środowiska produkcyjnego 1:1 (test dev)
3.23	Administracja - Infrastruktura	System musi umożliwiać odtworzenie środowiska test dev na podstawie środowiska produkcyjnego
3.24	Administracja - Infrastruktura	System ITSM powinien składać się z trzech niezależnych środowisk: produkcyjne, testowe, developerskie.
3.25	Administracja - Infrastruktura	Wykonawca określi wymagania dla środowiska (ilość serwerów, systemy operacyjne, bazy danych i inne). Środowisko musi być skalowalne, dawać możliwość zwiększenia wydajności poprzez rozbudowę infrastruktury, np. serwerów (w szczególności poprzez dodanie procesorów, pamięci RAM, zwiększenie liczby serwerów).
3.26	Administracja - Infrastruktura	Środowisko musi posiadać możliwość instalacji na platformie konteneryzacyjnej (np. Kubernetes, Openshift). Zamawiający dopuszcza rozwiązanie, w którym główna baza danych nie jest skonteneryzowana.
3.27	Administracja - Infrastruktura	Dane generowane przez system powinny być zbierane w jednolitym jeziorze danych, do którego wszystkie moduły systemu posiadają dostęp i możliwość przeszukiwania danych w identyczny sposób. Zastosowana technologia jeziora danych musi być wspierana przez producenta oprogramowania ITSM. Jeżeli wykorzystanie go wymaga dodatkowych licencji, należy je dostarczyć na rekomendowaną dla tego wdrożenia pojemność. Funkcjonalność ta musi być niezależna od głównej bazy danych rozwiązania.
3.28	Administracja - Infrastruktura	Technologia jeziora danych musi wspierać przeszukiwanie i analizę danych za pomocą co najmniej następujących języków danych: SQL, Python, R, Java. Dodatkowo, powinno umożliwiać integrację z narzędziami klasy Business Intelligence (takimi jak Power BI, Qlik, Tableau).
3.29	Administracja - Infrastruktura	System musi spełniać parametry RTO = 4 godziny, RPO = 5 minut. Architektura Systemu powinna zapewnić dostępność systemu na poziomie 99,8%, bez wliczania ustalanych wcześniej przerw serwisowych.

3.30	Administracja - Infrastruktura	Środowisko produkcyjne systemu musi umożliwiać instalację w dwóch równolegle pracujących ośrodkach.
3.31	Administracja - Infrastruktura	System musi zapewniać procedury naprawcze na wypadek wystąpienia Awarii, umożliwiające przywrócenie Systemu do stanu sprzed Awarii, na podstawie kryteriów zdefiniowanych przez Administratora. Rozwiązanie dla serwerów aplikacyjnych i bazodanowych.
3.32	Administracja - Infrastruktura	System musi umożliwiać tworzenie całkowitych, przyrostowych kopii bezpieczeństwa Systemu (automatyczne oraz manualne) i danych w trybie on-line oraz zapewniać procedurę przywracania Systemu z kopii bezpieczeństwa po Awarii. W tym zakresie system powinien umożliwiać współpracę z wiodącymi systemami kopii zapasowej (np. Veeam, Commvault, Networker)
3.33	Administracja - Integracja	System musi umożliwiać integrację poprzez: 1) API 2) usługi sieciowe (Web Services), 3) dokumenty w formacie XML, 5) płaskie pliki tekstowe. 6) interfejsy bazodanowe 7) PowerShell 8) SSH 9) ODBC/JDBC 10) LDAP
3.34	Administracja - Integracja	W przypadku braku konektorów wymaganych w celu integracji, dostawca zobowiązany jest dostarczać i utrzymywać dany konektor.
3.35	Administracja - Integracja	System musi zapewniać automatyczną aktualizację (zakładanie, dezaktywowanie, uzupełnianie danych) kont Użytkowników z wykorzystaniem Active Directory oraz innych baz LDAP.
3.36	Administracja - Integracja	1. Konfiguracja konektorów do integracji w celu wymiany danych. * Microsoft Active Directory – pobieranie istniejących danych do Systemu ITSM, obsługa trybu logowania mix-modę (lokalne oraz domenowe), możliwość obsługi większej ilości domen * Microsoft SCCM - parametry sprzętowe i oprogramowanie
3.37	Administracja - Ogólno funkcjonalne	System musi umożliwiać automatyczne zbieranie danych o infrastrukturze z wykorzystaniem mechanizmu pozwalającego na definiowanie harmonogramu skanowania Zasobów, w celu ograniczenia nadmiernego ruchu pomiędzy podsieciami w ramach infrastruktury.
3.38	Administracja - Ogólno funkcjonalne	System musi mieć wbudowany mechanizm wykrywania i powiadamiania o bieżących zmianach w infrastrukturze oraz wykorzystywanego oprogramowania, tj. historia zmian widoczna w systemie w postaci automatycznego oznaczania lub wyróżnienia zasobu.
3.39	Administracja - Ogólno funkcjonalne	System musi pokazywać aktualną strukturę rozłożenia maszyn wirtualnych oraz klastrów.
3.40	Administracja - Ogólno funkcjonalne	System powinien zapewnić integracje z CMDB w zakresie pobrania i synchronizacji danych.
3.41	Administracja - Ogólno funkcjonalne	System powinien dawać Operatorom możliwość dostosowywania/modyfikacji layout'u/dashboardu/portletu etc. bez konieczności angażowania Administratora systemu.
3.42	Administracja - Ogólno funkcjonalne	System musi posiadać w standardzie realizację wszystkich zadań przypisanych do Administratora w GUI bez zmian kodu źródłowego i prac programistycznych,
3.43	Administracja - Ogólno funkcjonalne	System musi zapewniać mechanizmy pozwalające na centralne zarządzanie kontami oraz uprawnieniami Administratorów, Operatorów.
3.44	Administracja - Ogólno funkcjonalne	System musi umożliwiać tworzenie przez Administratora grup Administratorów, Operatorów Systemu niezależnych od struktury organizacyjnej.
3.45	Administracja - Ogólno funkcjonalne	System musi mieć możliwość nadawania przez Administratora Operatorom, Użytkownikom uprawnień do widoczności danych, przeglądania danych bez możliwości ich modyfikacji.
3.46	Administracja - Ogólno funkcjonalne	System musi mieć możliwość nadawania Operatorom, przez Administratora uprawnień do wykonywania różnych akcji zdefiniowanych przez Administratora opierających się o modyfikacje parametrów i ich odczyt, dodawanie i usuwanie zapisów.
3.47	Administracja - Ogólno funkcjonalne	System musi zapewniać możliwość ustawienia przez Administratora ilości i długości czasu trwania sesji, po której System samoczynnie wyloguje bezczynnego Administratora, Operatora.
3.48	Administracja - Ogólno funkcjonalne	System musi zapewniać rejestrację i śledzenie historii dokonywanych modyfikacji i zapisów w Systemie , ze wskazaniem osób dokonujących modyfikacji oraz dat i godzin modyfikacji dla Użytkowników posiadających odpowiednie uprawnienia.
3.49	Administracja - Ogólno funkcjonalne	System musi umożliwiać Operatorom wyszukiwanie rekordów przy użyciu słów kluczowych, ciągów znaków w tym niepełnych wyrazów, fragmentów tekstu z użyciem operatorów logicznych (I, LUB, ORAZ).
3.50	Administracja - Ogólno funkcjonalne	System musi umożliwiać definiowanie przez Administratora uprawnień i przypisanie ich do użytkowników lub grup użytkowników.
3.51	Administracja - Ogólno funkcjonalne	System musi umożliwiać jednoczesny dostęp do danych wielu Użytkownikom, z zapewnieniem integralności danych wynikających z ich działań. Rekord w Systemie edytowany przez jedną osobę w czasie rzeczywistym blokuje możliwość edycji dla innych osób z wyświetleniem personalizowanego komunikatu lub pola zmodyfikowane na rekordzie w trakcie edycji przez innego użytkownika są odpowiednio zaznaczone w czasie rzeczywistym. Dodatkowo wszelkie zmiany pojawiają się w czasie rzeczywistym w dzienniku aktywności widocznym bezpośrednio na rekordzie
3.52	Administracja - Ogólno funkcjonalne	System musi posiadać możliwość zarządzania przez Operatorów tabelami rekordów tj. możliwość ukrywania i odkrywania kolumn, możliwość sortowania danych w tabeli po wskazanej kolumnie, możliwość filtrowania danych po każdej kolumnie, możliwość eksportu danych do pliku XLSX.

3.53	Discovery - Ogólne	System musi mieć wbudowany mechanizm automatycznego wykrywania środowiska IT (discovery) pozwalający na rozpoznanie konfiguracji komputerów, serwerów i oprogramowania z wykorzystaniem protokołów: * SNMP, * WMI * SSH, * HTTP / HTTPS * ICMP oraz w ramach gotowych konektorów integracyjnych do rozwiązań: * MS SCCM, * System ILMT v.9, * VMware vCenter, * Microsoft Hyper-V, * KVM, * MS Intune, * MS AZURE, * M365.
3.54	Discovery - Ogólne	System musi posiadać wbudowany mechanizm automatycznego wykrywania środowiska IT (discovery) pozwalający na rozpoznaniem konfiguracji środowiska cloud (wraz z rozpoznaniem aplikacji na nich uruchomionych) dla takich środowisk jak: * Kubernetes, * GCP, * AWS, * Oracle Cloud * MS AZURE
3.55	Discovery - Ogólne	System musi umożliwiać wykrywanie infrastruktury IT bez użycia agentów, co umożliwia identyfikację parametrów maszyny i zainstalowanego oprogramowania.
3.56	Discovery - Ogólne	System powinien mieć mechanizmy oparte na agentach do wykrywanie infrastruktury IT środowisk serwerowych i komputerów.
3.57	Discovery - Ogólne	System musi dostarczać wykrywanie baz danych Oracle, nie używając żadnych komponentów agenta (w tym binarnych plików agenta), wyłącznie korzystając z technologii bez agentowych, w tym wykrywania danych takich jak SID, katalog instalacyjny, wersja, Oracle home, edycja, nazwa, porty TCP.
3.58	Discovery - Ogólne	System musi posiadać mechanizm wykrywania zasobów oparty na tagach w celu automatycznego tworzenia relacji pomiędzy CI.
3.59	Discovery - Ogólne	System musi posiadać funkcje pomagające w wykrywaniu relacji między Elementami konfiguracji na podstawie funkcji opartych na ruchu sieciowym.
3.60	Discovery - Ogólne	System musi umożliwiać śledzenie zasobów i elementów konfiguracji (CI) wraz z relacjami i automatyczną synchronizacją między nimi w razie potrzeby (zainicjowanie procesu wykrywania infrastruktury przez operatora, poza harmonogramem).
3.61	Discovery - Ogólne	System powinien posiadać mechanizm skanowania infrastruktury, który umożliwia pobieranie danych o elementach konfiguracji w czasie rzeczywistym, bez wpływu na wydajność sieci lub skanowanych elementów. Powinien także zapewniać automatyczne wykrywanie zmian w infrastrukturze teleinformatycznej (Discovery), w tym identyfikację elementów konfiguracji oraz zasilanie bazy konfiguracji (CMDB) danymi dotyczącymi utworzonych lub zmodyfikowanych elementów konfiguracji.
3.62	Discovery - Ogólne	System musi umożliwiać Operatorowi łatwe przechodzenie pomiędzy wykrytymi elementami oraz ich filtrowanie.
3.63	Discovery - Ogólne	System musi umożliwiać grupowanie rekordów, wykonywanie operacji masowych na tych rekordach w Systemie oraz nawigowanie między nimi z poziomu widoku Operatora i Administratora.
3.64	Discovery - Ogólne	System musi wykrywać infrastrukturę IT wypisaną w zakładce "Lista sprzętów IT"
3.65	Discovery - Ogólne	Integracja pomiędzy bazą CMDB a Discovery/SAM/HAM Baza musi umożliwić rekoncyliację danych o Elementach konfiguracji pochodzących z różnych źródeł i definiować dowolnie reguły pozwalające na ich analizę. Reguły rekoncyliacji muszą być możliwe do definiowania dla każdej klasy oraz każdego atrybutu. System musi umożliwiać priorytetyzację źródeł. Celem jest umożliwienie operatorowi definiowanie reguł na podstawie których będą rozstrzygane rozbieżności w informacjach pochodzących z dwóch źródeł a dotyczących jednego atrybutu w konkretnym CI
3.66	Discovery - Ogólne	System musi posiadać mechanizm pozwalający na uniknięcie tworzenia wielu kopii rzeczywistych elementów konfiguracji tak aby kolejne skany infrastruktury nie tworzyły kolejnych rzeczywistych elementów konfiguracji reprezentujących jeden CI. Operator musi mieć możliwość definiowania reguł identyfikacji i porównania nowo tworzonych rzeczywistych elementów konfiguracji z już istniejącymi.

Lp WKR	Typ	Opis
4.1	Administracja - Backup	System musi posiadać funkcjonalność tworzenia i odzyskiwania kopii zapasowej danych.
4.2	Administracja - Bezpieczeństwo	System musi umożliwiać integrację z zewnętrznymi systemami przechowującymi dane uwierzytelniające dla wykrywanych systemów, takich jak CyberArk lub podobne.
4.3	Administracja - Bezpieczeństwo	System musi umożliwiać obsługę niezależnych instancji, wydzielenie wszystkich informacji w zakresie zdefiniowanej jednostki organizacyjnej, zapewniając pełną izolację danych, kont oraz personalizacje paneli Użytkowników w podziale na Klientów (multi-Tenant).
4.4	Administracja - Bezpieczeństwo	System musi umożlwiać przeprowadzenie testów bezpieczeństwa przez podmiot trzeci posiadający odpowiednie kompetencje i doświadczenie bez wsparcia Wykonawcy.
4.5	Administracja - Bezpieczeństwo	System musi umożlwiać korzystanie z uwierzytelniania wieloskładnikowego (MFA).
4.6	Administracja - Bezpieczeństwo	System musi umożliwiać definiowanie ról dostępu do informacji w zależności od rodzaju i autoryzacji Użytkownika Systemu i zapobiegać nieautoryzowanemu dostępowi do Systemu poprzez wbudowane mechanizmy bezpieczeństwa. Jeśli System zarządza hasłami lokalnego Użytkownika Systemu powinien udostępniać mechanizm wymuszający ich kontrolę np. w postaci minimalnej długości hasła, maksymalnego czasu ważności hasła, historii haseł (wymuszenie unikalności haseł), złożoności hasła.
4.7	Administracja - Bezpieczeństwo	System musi umożliwiać integrację z zewnętrznymi dostawcami w przypadku tworzenia zewnętrznych tożsamości za pomocą protokołów SAML, OpenID, LDAP, OAuth 2.0, Kerberos.
4.8	Administracja - Bezpieczeństwo	Zamawiający nie dopuszcza udostępniania, przekazywania danych z Systemu poza infrastrukturę Zamawiającego bez jego wiedzy i zgody.
4.9	Administracja - Bezpieczeństwo	System musi zapewniać bezpieczeństwo komunikacji. Przesyłane dane muszą być zabezpieczone i szyfrowane za pomocą protokołu TLS w wersji co najmniej 1.2 oraz system musi wspierać wersję 1.3.
4.10	Administracja - Bezpieczeństwo	System musi zapewniać logowanie, przeglądanie i raportowanie zdarzeń systemowych wg zadanych kryteriów (zakresu) umożliwiających identyfikację czasu, osoby, rodzaju i sposobu wykonania czynności na danym obiekcie oraz prób nieautoryzowanego dostępu w tym sposób umożliwiający odtwarzanie historii aktywności Użytkowników Systemu.
4.11	Administracja - Bezpieczeństwo	System musi posiadać funkcjonalność anonimizacji danych osobowych (zgodnie z przepisami RODO) w sposób uniemożliwiający powiązanie "zdarzenia" (zgłoszenie, działanie, operacja itp.) z użytkownikiem, jednocześnie niezakłócający ciągłosci działania systemu.
4.12	Administracja - Bezpieczeństwo	System musi mieć możliwość szyfrowania przechowywanych danych.
4.13	Administracja - Bezpieczeństwo	System musi posiadać funkcjonalność przeglądania logów systemowych i innych zdarzeń za pomocą filtrów.
4.14	Administracja - Bezpieczeństwo	System musi pozwalać na przesyłanie logów ze zdarzeń do zewnętrznego serwera logów za pomocą protokołu syslog.
4.15	Administracja - Bezpieczeństwo	System musi posiadać oddzielną witrynę dla pracowników firmy, osób współpracujących, kontrahentów itp. służącą do składania anonimowych wniosków (obsługa Sygnalistów) bez konieczności logowania się i pozostawiania jakichkolwiek danych osobowych.
4.16	Administracja - Bezpieczeństwo	System musi umożliwiać definiowanie numeru portu, na którym odbywa się komunikacja z agentami.
4.17	Administracja - Bezpieczeństwo	System musi posiadać zabezpieczoną (szyfrowanie ruchu) komunikację pomiędzy agentem a Systemem w oparciu o aktualne standardy na rynku.
4.18	Administracja - Bezpieczeństwo	System musi zapewniać stosowanie mechanizmów uwierzytelniania Administratorów, Operatorów, Użytkowników. Logowanie SSO z dodatkowym zabezpieczeniem 2FA (MS Authenticator)
4.19	Administracja - Bezpieczeństwo	System musi posiadać interfejs API do integracji z co najmniej jednym silnikiem antywirusowym dla załączanych plików (np Microsoft Defender).
4.20	Administracja - Infrastruktura	Środowisko produkcyjne systemu musi umożliwiać instalację w dwóch równolegle pracujących ośrodkach.
4.21	Administracja - Infrastruktura	Wykonawca określi wymagania dla środowiska (ilość serwerów, systemy operacyjne, bazy danych i inne). Środowisko musi być skalowalne, dawać możliwość zwiększenia wydajności poprzez rozbudowę infrastruktury, np. serwerów (w szczególności poprzez dodanie procesorów, pamięci RAM, zwiększenie liczby serwerów).
4.22	Administracja - Infrastruktura	Środowisko musi posiadać możliwość instalacji na platformie konteneryzacyjnej (np. Kubernetes, Openshift). Zamawiający dopuszcza rozwiązanie, w którym główna baza danych nie jest skonteneryzowana.
4.23	Administracja - Infrastruktura	Dane generowane przez system powinny być zbierane w jednolitym jeziorze danych, do którego wszystkie moduły systemu posiadają dostęp i możliwość przeszukiwania danych w identyczny sposób. Zastosowana technologia jeziora danych musi być wspierana przez producenta oprogramowania . Jeżeli wykorzystanie go wymaga dodatkowych licencji, należy je dostarczyć na rekomendowaną dla tego wdrożenia pojemność. Funkcjonalność ta musi być niezależna od głównej bazy danych rozwiązania.
4.24	Administracja - Infrastruktura	Technologia jeziora danych musi wspierać przeszukiwanie i analizę danych za pomocą co najmniej następujących języków danych: SQL, Python, R, Java. Dodatkowo, powinno umożliwiać integrację z narzędziami klasy Business Intelligence (takimi jak Power BI, Qlik, Tableau).
4.25	Administracja - Infrastruktura	System musi spełniać parametry RTO = 4 godziny, RPO = 5 minut. Architektura Systemu powinna zapewnić dostępność systemu na poziomie 99,8%, bez wliczania ustalanych wcześniej przerw serwisowych.
4.26	Administracja - Infrastruktura	System musi zapewniać procedury naprawcze na wypadek wystąpienia Awarii, umożliwiające przywrócenie Systemu do stanu sprzed Awarii, na podstawie kryteriów zdefiniowanych przez Administratora. Rozwiązanie dla serwerów aplikacyjnych i bazodanowych.

4.27	Administracja - Infrastruktura	System musi umożliwiać tworzenie całkowitych, przyrostowych kopii bezpieczeństwa Systemu (automatyczne oraz manualne) i danych w trybie on-line oraz zapewniać procedurę przywracania Systemu z kopii bezpieczeństwa po Awarii. W tym zakresie system powinien umożliwiać współpracę z wiodącymi systemami kopii zapasowej (np. Veeam, Commvault, Networker)
4.28	Administracja - Infrastruktura	System powinien składać się z trzech niezależnych środowisk: produkcyjne, testowe, developerskie.
4.29	Administracja - Infrastruktura	System musi posiadać możliwość budowy kopii środowiska produkcyjnego 1:1 (test dev)
4.30	Administracja - Infrastruktura	System musi umożliwiać odtworzenie środowiska test dev na podstawie środowiska produkcyjnego
4.31	Administracja - Integracja	System musi umożliwiać utworzenie assetów pochodzących z różnych źródeł; na podstawie danych z pliku , narzędzi automatycznego wykrywania elementów infrastruktury (Discovery) lub wprowadzanych ręcznie.
4.32	Administracja - Integracja	System musi prezentować przypisane do użytkownika zasoby w Portalu użytkownika (w ITSM).
4.33	Administracja - Integracja	System musi umożliwiać integrację z systemem ITSM w zakresie wszystkich informacji przechowywanych w HAM.
4.34	Administracja - Integracja	System musi automatycznie pobierać dane o użytkownikach z konta AD lub z innych systemów do zarządzania kontami. Synchronizacja musi się odbywać co 24 godziny z możliwością wymuszenia synchronizacji natychmiastowej przez operatora bazy.
4.35	Administracja - Integracja	System musi integrować się z bazą CMDB w zakresie wszystkich informacji dotyczących danego assetu
4.36	Administracja - Integracja	System musi zapewniać automatyczną aktualizację (zakładanie, dezaktywowanie, uzupełnianie danych) kont Użytkowników z wykorzystaniem Active Directory oraz innych baz LDAP.
4.37	Administracja - Integracja	System musi zapewniać dwukierunkową integrację z serwerem poczty elektronicznej, co najmniej MS Exchange oraz protokoły SMTP i IMAP.
4.38	Administracja - Integracja	System musi umożliwiać integracje z systemem Discovery
4.39	Administracja - Integracja	System musi umożliwiać integrację poprzez: 1) API 2) usługi sieciowe (Web Services), 3) dokumenty w formacie XML, 4) e-mail, 5) płaskie pliki tekstowe. 6) interfejsy bazodanowe 7) PowerShell 8) SSH 9) ODBC/JDBC 10) LDAP
4.40	Administracja - Integracja	1. Konfiguracja konektorów do integracji w celu wymiany danych. * Microsoft Active Directory – pobieranie istniejących danych do Systemu , obsługa trybu logowania mix-modę (lokalne oraz domenowe), możliwość obsługi większej ilości domen * Microsoft SCCM - parametry sprzętowe i oprogramowanie * MS Teams - zakładanie zgłoszeń
4.41	Administracja - Integracja	Integracja systemu z Microsoft System Center Configuration Manager (SCCM) Zakres integracji System musi umożliwiać: 1. Automatyczne importowanie i synchronizację danych o zasobach IT z SCCM. 2. Monitorowanie stanu i zdrowia zasobów zarządzanych przez SCCM. 3. Wykorzystanie danych SCCM do zarządzania cyklem życia zasobów w systemie . 4. Automatyczne tworzenie zgłoszeń w na podstawie alertów i raportów generowanych przez SCCM. 5. Przeprowadzanie zdalnych operacji na urządzeniach, takich jak instalacja oprogramowania czy aktualizacje, z poziomu przy użyciu funkcji SCCM. Dane potrzebne Dane o zasobach IT: 1. Informacje o urządzeniach (komputery, serwery, urządzenia mobilne). 2. Dane o zainstalowanym oprogramowaniu i jego wersjach. 3. Statusy i konfiguracje urządzeń. 4. Informacje o zgodności urządzeń z politykami bezpieczeństwa. Dane o użytkownikach: 1. Informacje o przypisanych użytkownikach do poszczególnych urządzeń. 2. Historia działań związanych z zasobami. Dane o alertach i incydentach: 1. Alerty o problemach sprzętowych lub programowych. 2. Raporty o niezgodności z politykami bezpieczeństwa. 3. Informacje o automatycznych działaniach naprawczych.

4.42	Administracja - ogólne	System ITSM musi posiadać wewnętrzne mechanizmy archiwizacji rekordów, polegające na ich migracji na dedykowany serwer/y
4.43	Administracja - ogólne	System musi umożliwiać definiowanie czasu po jakim rekordy zostaną zarchiwizowane.
4.44	Administracja - ogólne	System musi umożliwiać definiowanie dostępu osobom do rekordów zarchiwizowanych.
4.45	Administracja - Ogólno funkcjonalne	System musi umożliwiać Administratorowi graficzne definiowanie nowych formularzy, ich modyfikowanie i duplikowanie. Budowa formularza powinna odbywać się na zasadzie przeciągnij i upuść. System musi umożliwiać oznaczanie, które formularze i ich elementy są widoczne, edytowalne i/lub obowiązkowe.
4.46	Administracja - Ogólno funkcjonalne	System musi umożliwiać automatyczne zarządzanie zawartością pól formularza na podstawie informacji z Systemu np. automatyczne uzupełnienie informacji o przypisanym sprzęcie, przy czym reguły wypełniania pól muszą być możliwe do definiowania przez Administratora.
4.47	Administracja - Ogólno funkcjonalne	System musi zapewniać definiowanie wielopoziomowej struktury organizacyjnej ręcznie oraz poprzez import danych w odpowiednim formacie, dla Operatorów i Użytkowników. System musi umożliwiać odczytywanie i odtwarzanie struktury organizacyjnej na podstawie danych pochodzących z systemów zewnętrznych np. Active Directory.
4.48	Administracja - Ogólno funkcjonalne	System musi mieć możliwość nadawania przez Administratora Operatorom, Użytkownikom uprawnień do widoczności danych, przeglądania danych bez możliwości ich modyfikacji.
4.49	Administracja - Ogólno funkcjonalne	System musi mieć możliwość nadawania Operatorom, Użytkownikom przez Administratora uprawnień do wykonywania różnych akcji zdefiniowanych przez Administratora opierających się o modyfikacje parametrów, atrybutów i ich odczyt, dodawanie i usuwanie zapisów, w ramach assetów.
4.50	Administracja - Ogólno funkcjonalne	System musi umożliwiać definiowanie przez Administratora uprawnień i przypisanie ich do użytkowników lub grup użytkowników.
4.51	Administracja - Ogólno funkcjonalne	System musi zapewniać możliwość ustawienia przez Administratora ilości i długości czasu trwania sesji, po której System samoczynnie wyloguje bezczynnego Administratora, Operatora, Użytkownika.
4.52	Administracja - Ogólno funkcjonalne	System musi posiadać wewnętrzne mechanizmy archiwizacji rekordów (m. in. assety, dokumenty) historycznych lub niepotrzebnych.
4.53	Administracja - Ogólno funkcjonalne	System musi zachowywać ciągłość numeracji wszystkich rekordów System nadaje numer assetu dopiero po jego zapisaniu w systemie.
4.54	Administracja - Ogólno funkcjonalne	System powinien dawać Operatorom możliwość dostosowywania/modyfikacji layout'u/dashboardu/portletu etc. bez konieczności angażowania Administratora systemu.
4.55	Administracja - Ogólno funkcjonalne	System musi posiadać w standardzie realizację wszystkich zadań przypisanych do Administratora w GUI bez zmian kodu źródłowego i prac programistycznych,
4.56	Administracja - Ogólno funkcjonalne	System musi umożliwiać definiowanie nowych oraz modyfikowanie istniejących przepływów pracy (ang. workflow) dla wszystkich implementowanych procesów przy użyciu interfejsu graficznego działające na zasadzie przeciągnij i upuść oraz zaawansowanych narzędzi przy czym modyfikacja musi być możliwa do realizacji przez Użytkownika Systemu z
4.57	Administracja - Ogólno funkcjonalne	System musi umożliwić tworzenie klonów istniejących workflow ich wersjonowanie oraz dynamiczne podmienianie z poziomu konsoli Użytkownika Systemu z odpowiednim poziomem uprawnień.
4.58	Administracja - Ogólno funkcjonalne	System musi umożliwiać Operatorowi łatwe przechodzenie pomiędzy assetami i obiektami powiązanymi.
4.59	Administracja - Ogólno funkcjonalne	System musi umożliwiać definiowanie przez Administratora atrybutów wymaganych do wypełnienia w zapisie danego typu obiektu w Systemie oraz uniemożliwiać zarejestrowanie elementu bez wypełnienia tych pól.
4.60	Administracja - Ogólno funkcjonalne	System musi umożliwiać grupowanie rekordów, wykonywanie operacji masowych na tych rekordach w Systemie oraz nawigowanie między nimi z poziomu widoku Operatora i Administratora.
4.61	Administracja - Ogólno funkcjonalne	System musi umożliwiać Administratorowi definiowanie i klonowanie nieograniczonej liczby kompletnych: 1) przepływów pracy (ang. workflow) dla wszystkich implementowanych procesów, 2) formularzy (formatek), 3) grup Operatorów i Użytkowników.
4.62	Administracja - Ogólno funkcjonalne	System musi zapewniać mechanizmy pozwalające na centralne zarządzanie kontami oraz uprawnieniami Administratorów, Operatorów, Użytkowników.
4.63	Administracja - Ogólno funkcjonalne	System musi umożliwiać tworzenie przez Administratora grup Administratorów, Operatorów, Użytkowników Systemu niezależnych od struktury organizacyjnej.
4.64	Administracja - Ogólno funkcjonalne	System musi umożliwiać Użytkownikowi i Operatorowi dołączanie do zapisów załączników w postaci plików zewnętrznych (co najmniej formaty PDF, DOC, DOCX, XLS, XLSX, GIF, JPG, BMP, TXT, PPT, PPTX, ZIP).
4.65	Administracja - Ogólno funkcjonalne	System musi umożliwiać automatyczną realizację rekordów spełniających kryteria definiowane w workflow przez Administratora.
4.66	Administracja - Ogólno funkcjonalne	System musi umożliwiać jednoczesny dostęp do danych wielu Operatorom, z zapewnieniem integralności danych wynikających z ich działań. Rekord w Systemie edytowany przez jedną osobę w czasie rzeczywistym blokuje możliwość edycji dla innych osób z wyświetleniem personalizowanego komunikatu lub pola zmodyfikowane na rekordzie w trakcie edycji przez innego użytkownika są odpowiednio zaznaczone w czasie rzeczywistym. Dodatkowo wszelkie zmiany pojawiają się w czasie rzeczywistym w dzienniku aktywności widocznym bezpośrednio na rekordzie
4.67	Administracja - Ogólno funkcjonalne	System musi posiadać możliwość zarządzania przez Operatorów tabelami rekordów (np. listą Incydentów, Zmian itd.) tj. możliwość ukrywania i odkrywania kolumn, możliwość sortowania danych w tabeli po wskazanej kolumnie, możliwość filtrowania danych po każdej kolumnie, możliwość eksportu danych do pliku XLSX.
4.68	Administracja - Raportowanie	System musi umożliwiać raportowanie stanu posiadania i wykorzystania zasobów w sposób dowolnie konfigurowany przez operatora, tak aby możliwe było m. in. zaobserwowanie tempa zużycia przestrzeni dyskowej.
4.69	Administracja - Raportowanie	System musi umożliwiać tworzenie raportów w zakresie określonych przez Operatora atrybutów danego assetu, przy czym musi istnieć możliwość zapisu takiego raportu w pliku zewnętrznym w formacie co najmniej, XLS, XLSX oraz PDF. Musi istnieć możliwość masowego generowania takich raportów dla zadanej grupy assetów.

4.70	Administracja - Raportowanie	System musi posiadać wbudowany mechanizm raportowania na podstawie danych z Systemu – umożliwiający tworzenie dowolnych raportów w systemie , korzystanie/modyfikowanie z predefiniowanych raportów (dotyczące wszystkich wdrożonych procesów/modułów). Użytkownik Systemu może definiować własne zaawansowane raporty z dostępnych elementów (w zależności od przypisanej roli w Systemie) z użyciem dedykowanego interfejsu na zasadach np. "przeciągnij i upuść" bez konieczności pisania zaawansowanych zapytań do bazy .
4.71	Administracja - Raportowanie	System musi umożliwiać generowanie raportów w różnych formatach, takich jak PDF, CSV, XLSX, HTML.
4.72	Administracja - Raportowanie	System musi zapewniać możliwość udostępniania raportów innym użytkownikom lub grupom, zgodnie z ich uprawnieniami.
4.73	Administracja - Raportowanie	System powinien umożliwiać wizualne prezentowanie danych raportowych w formie graficznej tj. wykresy, grafy, trendy, tabelaryczne itd.
4.74	Administracja - Raportowanie	System musi umożliwiać planowanie i harmonogramowanie raportów, tak aby można było je generować automatycznie w określonych interwałach czasowych.
4.75	Administracja - Raportowanie	Raporty powinny być dostępne w czasie rzeczywistym i umożliwiać natychmiastowe przeglądanie najnowszych danych.
4.76	Administracja - Raportowanie	Raporty powinny być konfigurowalne, co pozwoli użytkownikom na dostosowanie ich do własnych potrzeb i preferencji.
4.77	Administracja - Raportowanie	System musi umożliwiać filtrowanie danych raportów na podstawie wszystkich atrybutów opisujących asset
4.78	Administracja - Raportowanie	Raporty powinny być skalowalne, aby umożliwić zarówno ogólny przegląd danych, jak i bardziej szczegółowe analizy.
4.79	Administracja - Raportowanie	System musi oferować wbudowane szablony raportów, które użytkownicy mogą łatwo dostosować do własnych potrzeb.
4.80	Administracja - Raportowanie	Raporty powinny być interaktywne, co umożliwi użytkownikom wykonywanie różnych operacji, takich jak sortowanie, grupowanie i zmiana widoku danych.
4.81	Administracja - Raportowanie	Raporty powinny być zoptymalizowane pod kątem wydajności, aby szybko generować i wyświetlać duże ilości danych.
4.82	Administracja - Raportowanie	Raporty powinny być dostępne w trybie online i offline, aby użytkownicy mogli je przeglądać zarówno w czasie rzeczywistym, jak i poza siecią.
4.83	Administracja - Raportowanie	System musi zapewniać mechanizmy śledzenia i audytu raportów, aby monitorować, kto je generuje, udostępnia i przegląda.
4.84	Baza CMDB/HAM -Ogólne	System musi udostępniać mechanizmy wspierające realizację audytu zgodności informacji o stanie CI ze stanem faktycznym potwierdzonym przez Operatora, co najmniej poprzez możliwość nadpisania informacji przez uprawnionego Operatora przy zachowaniu historii zmian oraz możliwości określenia przyczyny zmiany oraz źródła informacji.
4.85	Baza CMDB/HAM -Ogólne	System musi dawać możliwość dowolnego tworzenia własnych modeli zasobów sprzętowych.
4.86	Baza CMDB/HAM -Ogólne	System musi posiadać możliwość tworzenia dowolnego nowego magazynu do celów przechowywania elementów sprzętowych.Wraz z wykazem informacji kto jest osób odpowiedzialną za dany magazyn. Również musi istnieć możliwość modyfikowania magazynów każdego parametru opisującego magazyn poprzez operatora który posiada odpowiednie uprawnienia.
4.87	HAM - Ogólne	System musi umożliwiać definiowane nowych atrybutów, typów i podtypy, assetów.
4.88	HAM - Ogólne	System powinien automatycznie klasyfikować odkryte CI oraz uzupełnić atrybuty dostępnymi informacjami.
4.89	HAM - Ogólne	System musi umożliwiać przypisanie zdefiniowanych w nim zasobów do Użytkowników
4.90	HAM - Ogólne	System musi umożliwiać predykcję wyczerpania zasobów, przy czym Administrator i Operator muszą mieć możliwość zdefiniowania co najmniej: 1) progów (liczba, procent, data), 2) Użytkowników informowanych o przekroczeniu progu.
4.91	HAM - Ogólne	System musi wspierać poprzez wysyłania komunikacji do określonych operatorów informacji o stanach magazynowych.
4.92	HAM - Ogólne	System musi posiadać możliwości dowolnej obsługi transferów sprzętu między magazynami.
4.93	HAM - Ogólne	System musi posiadać możliwość podglądu przypisanych do użytkownika zasobów sprzętowych poprzez Portal ale także z użyciem urządzeń mobilnych.
4.94	HAM - Ogólne	System musi posiadać możliwość obsługi poniższych czynności z użyciem gotowych przepływów pracy oraz z zastosowaniem urządzeń mobilnych przez osoby odpowiedzialne za sprzęt: * Spis z natury * Inwentaryzacja wskazanych lokalizacji Zamawiającego * Zdanie sprzętu przez użytkownika * Odbiór sprzętu przez użytkownika * Przyjęcie na magazyn * Wydanie z magazynu * Złomowanie sprzętu, * Onboarding / Offboarding zasobu sprzętowego dla użytkownika, * Podmiana sprzętu uszkodzonego, * Rezerwacje sprzętu, * Obsługę wniosków RMA (Return merchandise authorization).
4.95	HAM - Ogólne	System musi posiadać możliwość podglądu dla Osoby odpowiedzialnej za zasoby sprzętowe wszystkich niezbędnych zadań w ramach jednej przestrzeni roboczej, uwzględniając takie elementy jak: Posiadane zinwentaryzowane zasoby sprzętowe, możliwość zarządzania modelami zasobów, informacje na temat statusów zamówionych elementów sprzętowych.
4.96	HAM - Ogólne	System musi posiadać mechanizm normalizacji danych o sprzęcie (producent, model, typ urządzenia, Data GA (General Avilability - Data wejścia produktu na rynek), Data końca życia (End of Life), Data końca sprzedaży (End of Sale).

4.97	HAM - Ogólne	System musi dostarczyć gotową bazę części sprzętowych (Part Number) o wielkości min.1 500 000 pozycji.
4.98	HAM - Ogólne	System musi posiadać jedno miejsce do wyszukania wszystkich dostępnych w systemie modeli sprzętu oraz numerów części sprzętowych (Part Number) dostępnych w ramach zinwentaryzowanego środowiska oraz w ramach gotowej dostarczonej z rozwiązaniem bazy numerów części sprzętowych (Part Number).
4.99	HAM - Ogólne	System musi umożliwiać zapis i śledzenie informacji o każdym assecie, od momentu zamówienia, do momentu wycofania z użycia, z zachowaniem informacji historycznych oraz z uwzględnieniem wartości zasobów oraz osoby dokonującej zmiany.
4.100	HAM - Ogólne	System musi umożliwiać Operatorowi tworzenie nowych assetów poprzez kopiowanie, duplikowanie assetów już zarejestrowanych w Systemie z możliwością wyboru pól podlegających kopiowaniu. Dodawanie assetów z plików w formacie co najmniej, XLS, XLSX.
4.101	HAM - Ogólne	Możliwość wypełnienia formularzy przekazanych przez operatora o dane z systemu. Formularz po wypełnieniu danymi musi być edytowalny i możliwy do wydrukowania. Formaty które muszą być obsługiwane to : PDF DOC xls. .
4.102	HAM - Ogólne	Możliwość zaciągania informacji do bazy na podstawie skanu dokumentu przygotowanego przez operatora. Z możliwością korekty danych przed zatwierdzeniem aktualizacji.
4.103	Ham - ogólne	System musi generować alerty w przypadku zbliżającej się daty końca obowiązywania umowy serwisowej. Alert powinien mieć swój workflow w systemie jak i być wysyłany w postaci maila do osoby zarządzającej daną umową. Warunki alertu musza być w całości edytowalne (czas do końca umowy który generuje alert, lista dystrybucyjna, lista umów objętych danym typem alertu).
4.104	Ham - ogólne	System musi posiadać możliwość wprowadzenia i dowolnej modyfikacji umów na zakup, serwis i utrzymanie sprzętu. Oraz budowanie relacji umów/usług serwisowych z każdym assetem . Umowa musi być reprezentowana jako jeden nadrzędny obiekt składający się z kilku podrzędnych, reprezentujących poszczególne usługi serwisowe. Usługi serwisowe musza mieć możliwości definiowania indywidualnych danych kontaktowych, czasów realizacji, harmonogramu dostępności.
4.105	HAM - Ogólne	System musi posiadać możliwość zarządzania przez Operatorów tabelami rekordów tj. możliwość ukrywania i odkrywania kolumn, możliwość sortowania danych w tabeli po wskazanej kolumnie, możliwość filtrowania danych po każdej kolumnie, możliwość eksportu danych do pliku XLSX.
4.106	HAM - Ogólne	System musi zapewniać rejestrację i śledzenie historii dokonywanych modyfikacji i zapisów w Systemie , ze wskazaniem osób dokonujących modyfikacji oraz dat i godzin modyfikacji dla Użytkowników posiadających odpowiednie uprawnienia.
4.107	HAM - Ogólne	System musi umożliwiać Operatorom wyszukiwanie assetów, użytkowników, przy użyciu słów kluczowych, ciągów znaków w tym niepełnych wyrazów, fragmentów tekstu z użyciem operatorów logicznych (I, LUB, ORAZ).
4.108	Ham - Ogólne	System musi umożliwiać pracę na minimum 5 zakładkach w jednej w przeglądarce jednocześnie, funkcjonalność ta musi działać niezależnie od przeglądarki internetowej.

Lp WKR	Typ	Opis
5.1	Administracja - ogólne	System ITSM musi posiadać wewnętrzne mechanizmy archiwizacji rekordów, polegajace na ich migracji na dedykowany serwer/y
5.2	Administracja - ogólne	System musi umożliwiać definiowanie czasu po jakim rekordy zostaną zarchiwizowane.
5.3	Administracja - ogólne	System musi umożliwiać definiowanie dostępu osobom do rekordów zarchiwizowanych.
5.4	SAM	System musi monitorować i zarządzać dostępnym na rynku oprogramowaniem wykorzystywanym przez Klientów w zakresie rozwiązań oferowanych przez producentów m.in.: a) Oracle, b) Microsoft, c) IBM, d) VMware, e) Red Hat, f) Cisco,
5.5	SAM	System musi wykrywać, monitorować, analizować zgodność licencyjną i zarządzać licencjami oprogramowania poniższych producentów z uwzględnieniem metryk licencyjnych i specyfiki produktów wykorzystywane przez Klientów minimum w zakresie: a) Oracle – Database Standard / Enterprise; Opcje DB: Turning Pack, Partitioning, Real Application Cluster; Oracle OLAP; Oracle Weblogic, Oracle Java SE, Oracle Java JVM, Oracle MySQL – metryki licencyjne Processor, NUP, b) Microsoft – Windows Server Standard/Datacenter; System Center Datacenter; Core Infrastructure Server Suite Datacenter; MS SQL Standard/Enterprise; MS Exchange; MS SCCM; licencje dostępowe CAL na użytkownika/urządzenie, Windows 10/11 , MS Office, c) IBM – Websphere, DB2, Tivoli, Spectrum Protect, QRadar, Security Access Manager, Web Content, WebPortal – posiadane metryki licencyjne PVU, RVU, AU, TB, d) VMware – vCenter Server; vSphere; e) Linux – Red Hat Linux, Suse Linux, Oracle Linux, Euro Linux, CentOS, f) Red Hat – CloudForms, Red Hat Virtualization Suite, OpenStack Platform, Red Hat Ceph Storage, Smart Management, Red Hat Ansible Tower with Ansible Engine, Red Hat JBoss, RedHat MySQL, g) Cisco – rozwiązania sieciowe, h) Adobe, i) SAP, j) SAS, k) Symantec.
5.6	SAM	Wykonawca będzie zobowiązany wprowadzić do Systemu SAM przekazane mu przez Zamawiającego dane w formie rejestrów o nabytych licencjach w podziale na producentów oprogramowania, typ oprogramowania wraz ze wskazaniem modeli licencjonowania oraz warunków licencyjnych i obowiązujących umów.
5.7	SAM	System musi posiadać możliwość przechowywania dokumentów świadczących o nabytych prawach do licencji lub posiadać mechanizm pozwalający na referowanie do systemu w którym takie informacje są przechowywane.
5.8	SAM	System SAM powinien zapewniać: 1) Dostarczanie bazy wzorców oprogramowania. Baza wzorców – wbudowany i aktualizowany na bieżąco moduł interpretacji danych, wzorce aplikacji, warunki licencyjne, metryki licencyjne, prawa do wersji (upgrade, downgrade), informacje o wsparciu technicznym oprogramowania. 2) Aktualizację bazy wzorców umów licencyjnych oprogramowania w module rozpoznawania oprogramowania. 3) Aktualizację bazy wzorców w zakresie warunków licencji, metryk licencyjnych, EOL, EOS oraz posiadać mechanizm normalizacji danych o oprogramowaniu (producent, wersja, edycja), a także dostarczać danych o: Dacie końca życia (End of Life), Data końca wsparcia (End of Support). oraz musi posiadać: a. Repozytorium danych do rejestrowania i zarządzania Zasobami. b. Interfejs dla użytkowników w zależności od roli w procesie. c. Wbudowane dedykowane mechanizmy analizy dla kluczowych technologii: Oracle, Microsoft, VMware, Red Hat, IBM. d. Wbudowane mechanizmy raportowania na poziomie platformy.
5.9	SAM	System SAM musi posiadać gotową bazę wzorców oprogramowania o wielkości min. 300 000 pozycji oraz SKU/PN dla oprogramowania o wielkości min. 1 500 000 pozycji.
5.10	SAM	System SAM musi mieć możliwość dodawania nowych wzorców licencyjnych.
5.11	SAM	Wszystkie funkcjonalności Systemu SAM muszą być dostępne bez konieczności tworzenia nowego oprogramowania, wykorzystywania innych rozwiązań produktowych odrębnych producentów, zapytań do bazy danych czy zaimplementowania przez Wykonawcę (dostepne z "pudełka").
5.12	SAM	System musi posiadać wbudowany mechanizm umożliwiający zarządzanie licencjami dostępów do aplikacji webowych.
5.13	SAM	System musi posiadać możliwość pełnego skanowania środowiska Zamawiającego za pośrednictwem dedykowanego Agenta instalowanego na hostach do zbierania danych ze środowiska w odniesieniu do systemów operacyjnych wykorzystywanych w ramach platformy. W przypadku braku możliwości użytkowania dedykowanego Agenta, moduł musi posiadać możliwość skanowania środowiska w sposób bez agentowy.

5.14	SAM	Dedykowany agent musi posiadać funkcjonalność monitorowania trendów wykorzystywania oprogramowania m.in. w zakresie czasu uruchomienia oraz okresu aktywnego korzystania z oprogramowania, użytkownika korzystającego z oprogramowania.
5.15	SAM	Instalacja agenta musi odbywać się w sposób zdalny nie zakłócający pracy serwera wirtualnego, fizycznego lub stacji roboczej. Dodatkowo zakończenie instalacji nie może wymagać restartu maszyny na której jest instalowany agent.
5.16	SAM	System musi zapewnić automatyczny mechanizm aktualizacji wersji agenta. Deinstalacja, instalacja lub aktualizacja nowej wersji agenta nie wymaga dodatkowego nakładu pracy ze strony Zamawiającego.
5.17	SAM	Agent musi być zgodny w zakresie instalacji oraz zbierania danych minimum wobec systemów operacyjnych: Microsoft, IBM, Linux (Red Hat, SUSE, Oracle, etc….), Vmware, Unix, MacOS.
5.18	SAM	Agent powinien posiadać funkcjonalność pracy w środowisku wirtualnym i zbierać dane dotyczące struktury wirtualnej (Struktura klastrów).
5.19	SAM	Wdrożony System musi umożliwiać bieżącą weryfikację zgodności zainstalowanego oprogramowania w odniesieniu do wykorzystywanych przez Zamawiającego technologii oraz dostępnych typów i modeli licencjonowania : a. Oprogramowanie stanowiące platformę Zamawiającego, b. Oprogramowanie do wirtualizacji serwerów, c. Systemy operacyjne (desktop i serwer), d. Oprogramowanie warstwy pośredniej (middleware), e. Oprogramowanie bazodanowe, f. Oprogramowanie specjalistyczne, branżowe, g. Oprogramowanie własne (wytworzone aplikacje), h. Oprogramowanie open source, i. Oprogramowanie deweloperskie, j. Oprogramowanie standardowe (popularne aplikacje na stacje robocze instalowane w środowisku desktopowych systemów operacyjnych Windows, Linux, MacOS).
5.20	SAM	Automatyczne zbieranie danych o zainstalowanym oprogramowaniu w infrastrukturze z wykorzystaniem mechanizmu pozwalającego na definiowanie harmonogramu skanowania oraz liczby bezpośrednich sesji pomiędzy platformą a skanowanymi Zasobami, w celu ograniczenia nadmiernego ruchu pomiędzy podsieciami w ramach infrastruktury.
5.21	SAM	System SAM powinien automatycznie zbierać informacje o korzystaniu z danej aplikacji, czasie jej wykorzystania a zbieranie danych powinno być oparte zarówno na serwerach fizycznych, jak i wirtualnych. Informacje zbierane powinny zawierać dane dotyczące rozpoczęcia korzystania z aplikacji, średnie statystyki użytkowania i datę instalacji oraz ścieżkę instalacji oprogramowania.
5.22	SAM	System musi mieć wbudowany mechanizm monitorowania i powiadamiania o bieżących zmianach w infrastrukturze oraz wykorzystywanego oprogramowania, tj. historia zmian widoczna w systemie w postaci automatycznego oznaczania lub wyróżnienia zasobu nie spełniającego warunku licencyjnego.
5.23	SAM	Wykrywanie i inwentaryzacja infrastruktury powinna odbywać się automatycznie z opcją manualnego dodawania elementów (np.: pasywnych elementów sieci, drukarek, urządzeń offline itp.).
5.24	SAM	System musi pokazywać aktualną strukturę rozłożenia maszyn wirtualnych oraz klastrów.
5.25	SAM	System musi umożliwiać definiowanie list dozwolonego i niedozwolonego oprogramowania w oparciu o wzorce.
5.26	SAM	System musi posiadać Bazę wzorców wykorzystującą znaczniki oprogramowania według norm ISO/IEC 19770-2 i ISO/IEC 19770-3.
5.27	SAM	System musi rozróżniać w ramach jednego produktu różne modele licencjonowania w ramach jednego środowiska, np. produkt Oracle Database w metryce NUP i Processor. Rozróżnienie polega na możliwości zarządzania licencjami w dwóch różnych modelach, a nie jedynie wykrywania modelu przez moduł SAM.
5.28	SAM	Wsparcie i automatyzację zgodności licencyjnej dla istniejących form licencjonowania opartych o metrykę licencjonowania: na użytkownika, na urządzenie, na instalację, na dostęp, na procesor, na rdzeń, subskrypcja, wirtualizacja, w oparciu o całkowitą liczbę użytkowników / równoległych użyć / urządzeń oraz upgrade / downgrade oprogramowania, Terminal Server i zarządzania aplikacjami w oparciu o określoną wartość, która została zdefiniowana przez Zamawiającego.
5.29	SAM	System musi posiadać wbudowany mechanizm stałego rozpoznawania niezidentyfikowanych aplikacji niezależnie od dostawcy, typu lub wielkości automatycznie rozpoznawać i identyfikować zainstalowane oprogramowanie niezależnie od producenta na podstawie plików, rejestrów lub innych stosowanych metod do identyfikacji. Dla specyficznych rozwiązań (będących poza Bazą wzorców) Zamawiający musi mieć możliwość manualnej klasyfikacji oprogramowania do grupy i określenia modelu licencjonowania oraz pozostałych parametrów opisujących licencje.
5.30	SAM	Dane publikowane przez producenta o wycofywaniu produktów oraz wygasającym wsparciu (Software Maintenance) mają być pobierane i dostarczane w ramach Bazy wzorców na potrzeby generowania raportów (dane dostarczane w paczce z możliwością manualnego importu do modułu SAM bez dostępu do Internetu).
5.31	SAM	Zasilanie i aktualizacja Bazy wzorców musi odbywać się w sposób automatyczny (za pośrednictwem Internetu) oraz z plików płaskich dostarczanych przez producenta Systemu SAM (w okresie aktywnego wsparcia technicznego).
5.32	SAM	System musi umożliwiać weryfikację dostarczanych przez producenta danych w pliku (zakres musi być otwarty i dostępny do analizy)

5.33	SAM	Mechanizm Bazy wzorców musi umożliwiać rozpoznanie zainstalowanego oprogramowania pod kątem atrybutów: 1. Oprogramowanie wymaga licencji lub oprogramowanie jest darmowe (nie wymaga licencji), 2. Wersji i edycji oprogramowania, stanowi część pakietów (bundling), 3. Stanowi upgrade lub downgrade bazując na wprowadzonych danych do bazy o prawach licencyjnych.
5.34	SAM	System musi posiadać mechanizm analizujący zainstalowane oprogramowanie pod kątem cyklu życia produktu (edycji, wersji lub paczki) wg danych producenta oprogramowania i okresu obowiązywania wsparcia technicznego dla kluczowego oprogramowania.
5.35	SAM	System musi umożliwiać zbieranie danych o zainstalowanym oprogramowaniu IBM z serwera ILMT. Komunikacja musi przebiegać za pośrednictwem REST API (Web Service). Niedopuszczalna jest komunikacja na poziomie bazy danych serwera ILMT. Dane z serwera ILMT powinny być pobierane jedynie za pośrednictwem dedykowanych konektorów, a sposób przekazywania danych z serwera ILMT do Systemu SAM musi być zgodny z warunkami licencji IBM (umowa IBM Passport Advantage) zachowując zgodność licencyjną.
5.36	SAM	System musi posiadać panel menadżerski, który będzie zawierał informacje o aktualnym stanie posiadanych i zainstalowanych licencji (w formie bilansu). Panel menadżerski będzie posiadał co najmniej następujące widoki: a. niedobór licencji, b. nadwyżka licencji, c. bilans licencji, d. informacją o koszcie/wartości oraz stopniu amortyzacji licencji, e. wartość utrzymania licencji w definiowanym okresie czasu.
5.37	SAM	System musi posiadać mechanizm interpretujący na podstawie wprowadzonych danych finansowych możliwe oszczędności lub koszty z tytułu utrzymywania licencji, ROI, TCO.
5.38	SAM	Repozytorium danych musi umożliwiać zarządzanie Zasobami, dokumentami, dostawcami oraz umowami licencyjnymi minimum w zakresie: a. przechowywania informacji o warunkach handlowych (produkty, typy licencji oraz ich wartość), b. umożliwia przypisywanie komputerów, licencji i użytkowników do struktury organizacyjnej i centrów kosztów oraz Klientów, c. mechanizm zarządzania umowami musi być powiązany z Zasobami w bazie danych Modułu SAM (wielopoziomowe powiązania i relacje pomiędzy umową a Zasobami oraz parametrami zasobu), d. zarządzanie licencjami zgodnie z faktycznym wykorzystaniem Zasobów przez centra kosztów czy klient wykorzystujący System, e. Umowy licencyjne oraz zakupowe muszą być powiązane z produktami wykrytymi w środowisku Zamawiającego, f. przechowywania informacji o umowach serwisowych, które przypisane zostaną do osób odpowiedzialnych, g. dodawanie historycznych informacji na temat posiadanych licencji, obejmujących co najmniej informacje o nr umowy, dacie zawarcia i wygasania umowy, informacje o licencjach bazowych (upgrade) oprogramowania, h. musi umożliwiać odczytywanie informacji o lokalizacjach, strukturze organizacyjnej, centrach kosztów/klientów, użytkownikach i Zasobach z zewnętrznych systemów poprzez integrację, i. Umożliwia ręczne wprowadzanie danych w celu aktualizacji informacji o licencjach oraz kontraktach, j. Umożliwia wprowadzanie zasad licencjonowania specyficznych dla danej umowy logiki licencyjnej do indywidualnych umów licencyjnych, k. Umożliwia przetwarzanie manualnie wprowadzonych danych.
5.39	SAM	Repozytorium danych musi przechowywać umowy licencyjne wraz z ich warunkami handlowymi (produkty, typy licencji oraz ich wartość) powiązanych z produktami wykrytymi w środowisku Zamawiającego.
5.40	SAM	System SAM musi zapewniać możliwość wprowadzenia następujących umów licencyjnych: * dla Adobe - Generic, Enterprise Term License Agreement (ETLA), Cumulative Licensing Program (CLP), Transactional Licensing Program (TLP), Value Incentive Plan (VIP), * dla IBM - Generic, Enterprise License Agreement (ELA), Internattional Program License Agreement (IPLA), IBM Customer Agreement (ICA), IBM Unlimited License Agreement (IULA), * dla Microsoft - Generic, Enterprise Agreement, Enterprise Enrollment, Enterprise Subscription Agreement, Microsoft Products and Services Agreement (MPSA), Open License, Open Value, Open Value Subscription, Select Enrollment, Select License, Select Plus, * dla Oracle - Generic, Unlimited License Agreement (ULA), * dla Vmware - Generic, Enterprise License Agreement (ELA), Enterprise Purchasing Program (EPP), Volume Purchasing Program (VPP), * pozostali producenci - Generic, Enterprise License Agreement (ELA).
5.41	SAM	System SAM musi posiadać możliwość przechowywania informacji o powiązaniach między Zasobami m.in. stacjami roboczymi, serwerami z historią konfiguracji, parametrów technicznych i pełnym skanowaniem sprzętu a oprogramowaniem.
5.42	SAM	Dla każdego Zasobu powinno być możliwe przechowywanie załączonych kopii dokumentów m.in. faktur, certyfikatów, umów, zestawień, plików w dowolnych formatach.
5.43	SAM	Repozytorium danych musi posiadać możliwość oznaczania oprogramowania w zakresie: wykorzystywania przez oprogramowanie danych osobowych, status opisujący stan Zasobu (utylizacja, wyłączenie z użytkowania), cele wykorzystywania oprogramowania (np. w ramach istniejącego systemu).

5.44	SAM	Repozytorium danych powinno posiadać funkcjonalność automatycznego wysyłania powiadomień drogą elektroniczną (wiadomość e-mail) do osób odpowiedzialnych w przypadku zbliżania się terminu zakończenia kontraktu (np. 6 miesięcy przed datą zakończenia umowy).
5.45	SAM	System SAM musi posiadać wbudowany interfejs umożlwiający zarządzanie typem/rodzajem pola w określonym formacie (np. dodanie pola tekstowego, liczbowego z wyborem: obowiązkowy – nieobowiązkowy).
5.46	SAM	Umożliwiać zaczytanie danych o posiadanych kontraktach i licencjach z zewnętrznego źródła danych w tym z plików płaskich, np. Excel, .csv.
5.47	SAM	System oprócz możliwości wprowadzenia licencji w ramach dedykowanego formularza, musi posiadać kreator wprowadzania licencji, który poprzez zadanie odpowiednich pytań ułatwia operatorowi systemu jej wprowadzenie. Pytania zadawane w ramach kreatora to m.in.: Czy wprowadzania licencja jest dla oprogramowania on-premise czy SaaS?, Czy dostępne jest SKU / PN dla wprowadzanej licencji?, Jaki jest typ licencji - Perpetual czy Subskrypcja?, Jak jest typu umowy w jakiej licencje jest zakupiona?, Jaka jest metryka licencji?, Jaki jest koszt zakupu jednostkowy dla licencji?, Kto jest właścicielem licencji? itp.
5.48	SAM	Repozytorium musi posiadać mechanizm analityczny wykonujący automatyczną weryfikacją zgodności licencyjnej poprzez porównywanie danych. Obliczanie zgodność licencyjnej z danymi pochodzącymi z inwentaryzacji powinno dokonywać się automatycznie.
5.49	SAM	System musi posiadać funkcjonalność klasyfikacji oprogramowania m.in. wpisanie pozycji na czarną listę oprogramowania. Wskazane przez administratora Systemu SAM oprogramowanie w określonej wersji i edycji będzie zaznaczone jako niedopuszczone do instalacji, odbiegające od standardów, np. gry komputerowe.
5.50	SAM	System musi umożliwiać bez agentową inwentaryzację środowiska, np. za pomocą pliku płaskiego. Musi również umożliwiać wbudowaną identyfikację i monitorowanie środowisk lub urządzeń przy użyciu rozwiązań w zależności od uwarunkowań technicznych oraz decyzji Zamawiającego m.in. za pomocą dedykowanego agenta platformy, agenta innych rozwiązań kluczowych producentów np. Microsoft SCCM i bez użycia agenta np. z pliku płaskiego (w sytuacjach urządzeń wydzielonych).
5.51	SAM	System powinien zapewniać integracje pomiędzy swoimi modułami w zakresie zapewnienia referencji do dokumentów świadczących o posiadanych uprawnieniach licencyjnych oraz umowach.
5.52	SAM	W ramach realizacji zamówienia Wykonawca dokona parametryzacji System SAM umożliwiających zarządzanie Zasobami i zgodnością licencyjną w oparciu o specyfikę Zasobów oraz wymagania zdefiniowane przez Zamawiającego w dokumencie OPZ.
5.53	SAM	Wykonawca dokona parametryzacji platformy minimum w zakresie procesów zarządzania licencjami Zamawiającego: a) Utworzenie profili użytkowników i uprawnień w odniesieniu do ról w procesie platformy. b) Ustawienie dedykowanych pól w platformie pod kątem specyfiki zarządzanego oprogramowania. c) Utworzenie widoków i raportów w zależności od uprawnień użytkowników. d) Przygotowanie widoków do eksportu i importu danych. e) Przygotowanie szablonów zbierania danych standardowych, np. import manualny Zasobów sprzętowych. f) Uzgodnienie procesu zbierania danych dotyczących instalacji, których nie można importować automatycznie (licencje dostępowe, środowisko wirtualne itp.). W przypadku braku odpowiednich formalnych uregulowań utworzenie procedury na potrzeby Zamawiającego.
5.54	SAM	System SAM musi posiadać jedno miejsce do wyszukania wszystkich dostępnych w systemie wzorców oprogramowania oraz SKU / Part Number dostępnych w ramach zinwentaryzowanego środowiska oraz w ramach gotowej dostarczonej z rozwiązaniem bazy wzorców.
5.55	SAM	System SAM musi posiadać graficzny kalendarz odnowień dla posiadanych licencji subskrypcyjnych.
5.56	SAM	System SAM musi posiadać możliwość definiowania celów dla procesu Zarządzania oprogramowaniem i licencjami (SAM) z możliwością przypisywania do celów zadań dla zespołu ds. licencji oraz możliwością śledzenia postępów realizacji założonych celów.
5.57	SAM	System SAM musi mieć możliwość obsługi rozliczania licencji dla Microsoft z zastosowaniem modelu BYOL (Bring Your Own License) dla środowisk Azure.
5.58	SAM	System SAM musi mieć możliwość wykrywania aplikacji używanych w ramach środowisk kontenerowych Kubernates celem wsparcia w ramach rozliczania licencji na oprogramowanie.
5.59	SAM	System SAM musi zapewnić mechanizmy wykonujące projekcję kosztów rozwiązań on-premise związane z ich migracją do chmury publicznej, wraz z podaniem obecnych kosztów CAPEX oraz szacowanych kosztów chmury (OPEX), a także rekomendacjami z zakresie instancji jakie w środowisku cloud będą wymagane.
5.60	SAM	System SAM powinien zapewniać panel nawigacyjny optymalizacji SaaS, umożliwiający analizę użytkowania i optymalizację wielu instancji.
5.61	SAM	System SAM powinien zapewniać gotowe definicje pakietów licencyjnych do zarządzania i optymalizacji subskrypcji.
5.62	SAM	System SAM powinien zawierać rekomendacje licencji dla oprogramowania min.: * Microsoft * IBM * Red HAT * Oracle * VMWare * Cisco
5.63	SAM	System SAM musi posiadać możliwość korzystania z urządzeń mobilnych typu tablet/telefon z systemami operacyjnymi Android i IOS.

5.64	SAM	System SAM musi mieć wbudowany mechanizm automatycznego wykrywania środowiska IT (discovery) pozwalający na rozpoznanie konfiguracji komputerów, serwerów i oprogramowania z wykorzystaniem protokołów: * SNMP, * WMI, * SSH, * HTTP / HTTPS, * ICMP oraz w ramach gotowych konektorów integracyjnych do rozwiązań: * MS SCCM, * System ILMT v.9, * VMware vCenter, * Microsoft Hyper-V, * KVM, * MS Intune, * MS AZURE, * M365. * ILS (IBM License Service)
5.65	SAM	System SAM musi umożliwiać przypisanie zdefiniowanych w nim zasobów do Użytkowników oraz prezentację tych danych.
5.66	SAM	System SAM musi automatycznie przyjmować i wykorzystywać informacje o znacznikach oprogramowania.
5.67	SAM	System SAM musi posiadać możliwość wprowadzenia i zarządzania umowami na zakup i wsparcie oprogramowaniem.
5.68	SAM	System SAM powinien dawać Operatorom możliwość dostosowywania/modyfikacji layout'u/dashboardu/portletu etc. bez konieczności angażowania Administratora systemu.
5.69	SAM	System SAM musi posiadać interfejs wielojęzykowy w tym w polskiej wersji językowej i angielskiej z możliwością wyboru przez Użytkownika Systemu.
5.70	SAM	System SAM musi być dostępny z poziomu przeglądarki internetowej w ich najnowszych wersjach, bez konieczności instalowania komponentów trzecich lub plug-in. System ma być wpierany przez popularne przeglądarki na różnych systemach: Windows, MAC OS, Linux w szczególności Google Chrome, Mozilla FireFox oraz Safari co najmniej w wersji aktualnej na dzień składania ofert.
5.71	SAM	System SAM musi umożliwiać przypisanie zdefiniowanych w nim zasobów licencyjnych do Użytkowników oraz ich prezentację
5.72	SAM - Administracja Bezpieczeństwo	System musi posiadać funkcjonalność zapobiegania nieautoryzowanemu dostępowi poprzez wbudowane mechanizmy bezpieczeństwa.
5.73	SAM - Administracja Bezpieczeństwo	Zamawiający nie dopuszcza udostępniania, przekazywania danych z Systemu poza infrastrukturę Zamawiającego bez jego wiedzy i zgody.
5.74	SAM - Administracja Bezpieczeństwo	System musi zapewniać logowanie, przeglądanie i raportowanie zdarzeń systemowych wg zadanych kryteriów (zakresu) umożliwiających identyfikację czasu, osoby, rodzaju i sposobu wykonania czynności na danym obiekcie oraz prób nieautoryzowanego dostępu w tym sposób umożliwiający odtwarzanie historii aktywności Użytkowników Systemu.
5.75	SAM - Administracja Bezpieczeństwo	System musi mieć możliwość szyfrowania przechowywanych danych.
5.76	SAM - Administracja Bezpieczeństwo	System musi posiadać funkcjonalność przeglądania logów systemowych i innych zdarzeń za pomocą filtrów.
5.77	SAM - Administracja Bezpieczeństwo	System musi pozwalać na przesyłanie logów ze zdarzeń do zewnętrznego serwera logów za pomocą protokołu syslog.
5.78	SAM - Administracja Bezpieczeństwo	System musi zapewniać komunikację platformy z oprogramowaniem agenta za pośrednictwem serwera pośredniczącego (kolektora), którego zadaniem jest miedzy innymi ograniczenie komunikacji pomiędzy podsieciami oraz agregowanie danych przesyłanych do platformy.
5.79	SAM - Administracja Bezpieczeństwo	System musi posiadać funkcjonalność tworzenia i odzyskiwania kopii zapasowej danych.
5.80	SAM - Administracja Bezpieczeństwo	System musi posiadać zabezpieczoną (szyfrowanie ruchu) komunikację pomiędzy agentem a Systemem w oparciu o aktualne standardy na rynku.
5.81	SAM - Administracja Bezpieczeństwo	System musi zapewniać możliwość przenoszenia danych do innych systemów Zamawiającego (dane w powszechnie uznanym formacie)
5.82	SAM - Administracja Infrastruktura	Wykonawca określi wymagania dla środowiska SAM (ilość serwerów, systemy operacyjne, bazy danych i inne). Środowisko musi być skalowalne, dawać możliwość zwiększenia wydajności poprzez rozbudowę infrastruktury, np. serwerów (w szczególności poprzez dodanie procesorów, pamięci RAM, zwiększenie liczby serwerów).
5.83	SAM - Administracja Infrastruktura	System SAM musi umożliwiać tworzenie przez Administratora grup Administratorów, Operatorów, Użytkowników Systemu ITSM niezależnych od struktury organizacyjnej.
5.84	SAM - Administracja Infrastruktura	System SAM musi mieć możliwość nadawania przez Administratora Operatorom, Użytkownikom uprawnień do widoczności danych, przeglądania danych bez możliwości ich modyfikacji.
5.85	SAM - Administracja Infrastruktura	System SAM musi zapewniać możliwość ustawienia przez Administratora ilości i długości czasu trwania sesji, po której System SAM samoczynnie wyloguje bezczynnego Administratora, Operatora, Użytkownika.
5.86	SAM - Administracja Infrastruktura	System SAM musi zapewniać rejestrację i śledzenie historii dokonywanych modyfikacji i zapisów w Systemie SAM, ze wskazaniem osób dokonujących modyfikacji oraz dat i godzin modyfikacji dla Użytkowników posiadających odpowiednie uprawnienia.
5.87	SAM - Administracja Infrastruktura	System SAM musi umożliwiać Operatorowi dołączanie załączników w postaci plików zewnętrznych (co najmniej formaty PDF, DOC, DOCX, XLS, XLSX, GIF, JPG, BMP, TXT, PPT, PPTX, ZIP).
5.88	SAM - Administracja Infrastruktura	System SAM musi umożliwiać definiowanie przez Administratora uprawnień i przypisanie ich do użytkowników lub grup użytkowników.

5.89	SAM - Administracja Infrastruktura	System SAM musi umożliwiać jednoczesny dostęp do danych wielu Użytkownikom, z zapewnieniem integralności danych wynikających z ich działań. Rekord w Systemie SAM edytowany przez jedną osobę w czasie rzeczywistym blokuje możliwość edycji dla innych osób z wyświetleniem personalizowanego komunikatu lub pola zmodyfikowane na rekordzie w trakcie edycji przez innego użytownika są odpowiednio zaznaczone w czasie rzeczywistym. Dodatkowo wszelkie zmiany pojawiają się w czasie rzeczywistym w dzienniku aktywności widocznym bezpośrednio na rekordzie
5.90	SAM - Administracja Infrastruktura	System SAM musi zapewniać logowanie, przeglądanie i raportowanie zdarzeń systemowych wg zadanych kryteriów (zakresu) umożliwiających identyfikację czasu, osoby, rodzaju i sposobu wykonania czynności na danym obiekcie oraz prób nieautoryzowanego dostępu w tym sposób umożliwiający odtwarzanie historii aktywności Użytkowników Systemu SAM.
5.91	SAM - Administracja Infrastruktura	System SAM musi zapewniać komunikację platformy z oprogramowaniem agenta za pośrednictwem serwera pośredniczącego (konektora), którego zadaniem jest miedzy innymi ograniczenie komunikacji pomiędzy podsieciami oraz agregowanie danych przesyłanych do platformy.
5.92	SAM - Administracja Infrastruktura	Środowisko musi posiadać możliwość instalacji na platformie konteneryzacyjnej (np. Kubernetes, Openshift). Zamawiający dopuszcza rozwiązanie, w którym główna baza danych nie jest skonteneryzowana.
5.93	SAM - Administracja Infrastruktura	Środowisko produkcyjne Systemu musi umożliwiać instalację w dwóch równolegle pracujących ośrodkach.
5.94	SAM - Administracja Infrastruktura	System musi zapewniać procedury naprawcze na wypadek wystąpienia Awarii, umożliwiające przywrócenie Systemu do stanu sprzed Awarii, na podstawie kryteriów zdefiniowanych przez Administratora. Rozwiązanie dla serwerów aplikacyjnych i bazodanowych.
5.95	SAM - Administracja Infrastruktura	System musi umożliwiać tworzenie całkowitych, przyrostowych kopii bezpieczeństwa Systemu (automatyczne oraz manualne) i danych w trybie on-line oraz zapewniać procedurę przywracania Systemu z kopii bezpieczeństwa po Awarii. W tym zakresie system powinien umożliwiać współpracę z wiodącymi systemami kopii zapasowej (np. Veeam, Commvault, Networker)
5.96	SAM - Administracja Integracja	System SAM musi posiadać konektory do integracji: * Active Directory, * System ILMT v.9, * VMware vCenter, * MS SCCM, * M365, * MS Intune. * baza danych SQL * IBM DB2 * Oracle DB, * System ILS (IBM License Service) Dane w platformie muszą być na bieżąco aktualizowane w oparciu o dane z wyżej wymienionych systemów wykorzystywanych przez Zamawiającego podlegających integracji.
5.97	SAM - Administracja Integracja	System powinien zapewnić integracje z CMDB w zakresie pobrania i synchronizacji danych dotyczących minimum: Assetów sprzętowych, typu środowiska (dev/test/prod), nazwy systemu informatycznego, właściciela systemu, grupy administrującej, krytyczności systemu , kategorii systemu ze względu na poufność.
5.98	SAM - Administracja Integracja	1. Integracja z niżej wymienionymi systemami w celu monitorowania licencji: * System ILMT v.9, * VMware vCenter, * Microsoft Hyper-V, * KVM, * System ILS (IBM License Service)
5.99	SAM - Administracja ogólno funkcjonalne	System musi umożliwiać Administratorowi graficzne definiowanie nowych formularzy, ich modyfikowanie i duplikowanie. Budowa formularza powinna odbywać się na zasadzie przeciągnij i upuść. System musi umożliwiać oznaczanie, które formularze i ich elementy są widoczne, edytowalne i/lub obowiązkowe dla zdefiniowanych ról. (np. Incydent Manager może edytować priorytet niezależnie od statusu incydentu, a inne role nie mogą go edytować w innym statusie niż "nowe")
5.100	SAM - Administracja ogólno funkcjonalne	System musi umożliwiać definiowanie przez Administratora atrybutów wymaganych do wypełnienia w zapisie danego typu obiektu w Systemie oraz uniemożliwiać zarejestrowanie elementu bez wypełnienia tych pól.
5.101	SAM - Administracja ogólno funkcjonalne	System musi umożliwiać przypisanie adresów email do usług zdefiniowanych w KU, w celu interaktywnej komunikacji z użytkownikiem poprzez wskazany adres email.
5.102	SAM - Administracja ogólno funkcjonalne	System musi umożliwiać Operatorom lub zdefiniowanym rolom, definiowanie przypomnień dotyczących Incydentów, Wniosków o usługę, Problemów, Zmian, Wydań. (np. dodanie flagi do rekordu, komunikat systemowy
5.103	SAM - Administracja ogólno funkcjonalne	System musi zapewniać mechanizmy pozwalające na centralne zarządzanie kontami oraz uprawnieniami Administratorów, Operatorów, Użytkowników, Klientów Systemu .
5.104	SAM - Administracja ogólno funkcjonalne	System musi umożliwiać tworzenie przez Administratora grup Administratorów, Operatorów, Użytkowników Systemu niezależnych od struktury organizacyjnej.
5.105	SAM - Administracja ogólno funkcjonalne	System musi mieć możliwość nadawania przez Administratora Operatorom, Użytkownikom uprawnień do widoczności danych, przeglądania danych bez możliwości ich modyfikacji.
5.106	SAM - Administracja ogólno funkcjonalne	System musi zapewniać rejestrację i śledzenie historii dokonywanych modyfikacji i zapisów w Systemie, ze wskazaniem osób dokonujących modyfikacji oraz dat i godzin modyfikacji dla Użytkowników posiadających odpowiednie uprawnienia.

5.107	SAM - Administracja ogólno funkcjonalne	System musi zapewniać definiowanie wielopoziomowej struktury organizacyjnej ręcznie oraz poprzez import danych w odpowiednim formacie, dla Operatorów i Użytkowników. System musi umożliwiać odczytywanie i odtwarzanie struktury organizacyjnej na podstawie danych pochodzących z systemów zewnętrznych np. Active Directory.
5.108	SAM - Administracja ogólno funkcjonalne	System musi umożliwiać blokowanie zamknięcia rekordu w sytuacji, gdy pozostają otwarte zlecenia związane z danym rekordem oraz pozostają niewypełnione wymagane pola informacyjne rekordu.
5.109	SAM - Administracja ogólno funkcjonalne	System musi posiadać możliwość tworzenia nowych rekordów poprzez ich duplikacje zarejestrowanych w Systemie.
5.110	SAM - Administracja ogólno funkcjonalne	System musi umożliwiać Operatorowi łatwe przechodzenie pomiędzy obiektami, elementami konfiguracji połączonymi w relacje.
5.111	SAM - Administracja ogólno funkcjonalne	System musi składać się z niezależnych środowisk: produkcyjnego, testowego
5.112	SAM - Administracja Raportowanie	System musi umożliwiać zarządzanie, monitorowanie, raportowanie i weryfikację wykorzystywanych licencji oraz urządzeń komputerowych (m.in. serwery fizyczne i wirtualne, stacje robocze, pozostałe urządzenia IT) w ramach platformy
5.113	SAM - Administracja Raportowanie	System musi posiadać wbudowany mechanizm analizy zgromadzonych danych o posiadanych prawach licencyjnych oraz zainstalowanego oprogramowania na podstawie, których dokonuje kalkulacji i generuje zestawienia niedoborów licencyjnych oraz kosztów związanych z koniecznością ich uzupełnienia w podziale min. na: a. producenta, b. produkt, c. metrykę licencjonowania, d. typ oprogramowania, e. wartość finansową, f. trend zmian (niedobory, nadwyżki) w danym okresie czasu, g. Klientów, w których licencje są wykorzystywane.
5.114	SAM - Administracja Raportowanie	System musi posiadać możliwość generowania zestawienia oprogramowania z wygasającym wsparciem oraz produktami niewspieranymi przez producenta oprogramowania zainstalowanego w zależności od edycji i wersji produktu.
5.115	SAM - Administracja Raportowanie	System musi posiadać wbudowany mechanizm raportowania w ramach interfejsu. Niedopuszczalne jest wyłączne definiowanie zapytań na poziomie bazy danych w zakresie generowania podstawowych raportów wprowadzonych danych do portalu: a. Udostępnienie automatycznych raportów na żądanie zawierających informacje o statusie zgodności licencji, instalacji oprogramowania. b. Na podstawie danych w portalu o Zasobach, Zamawiający może utworzyć raport o dowolnym zakresie (przy zachowaniu relacji elementów w bazie). c. Cykliczne importowanie danych od ostatniego bilansu licencji – dotyczy danych, które zostały zebrane od czasu ostatniego bilansu licencji i stanowią podstawę do wygenerowania nowego bilansu licencji. d. Umożliwia importowanie szablonów na potrzeby ręcznego zbierania danych. e. Umożliwia definiowania własnych raportów oraz modyfikowania istniejących z poziomu interfejsu portalu bez konieczności ustawiania zapytań do bazy danych. f. Umożliwia eksport danych bezpośrednio w interfejsie portalu do popularnych formatów: Excel, .csv, .pdf.
5.116	SAM - Administracja Raportowanie	Dostęp do generowania raportów powinien być zapewniony dla dowolnej liczby użytkowników, nie może być ograniczony ze względu na licencje.
5.117	SAM - Administracja Raportowanie	System musi posiadać domyślnie zdefiniowane i dostępne na „jedno kliknięcie” raporty umożliwiające weryfikację licencyjną.
5.118	SAM - Administracja Raportowanie	System SAM Musi umożliwiać import raportu z Microsoft License Statement (MLS), import raportu z systemu ILMT (automatyczny i manualny) oraz z sytemu ILS (IBM License Service)
5.119	SAM - Administracja Raportowanie	System SAM powinien zapewnić zdefiniowane i dostępne raporty minimum w podziale na: a. producentów i typy rozwiązań Zasobów, b. umów licencyjnych (wartość kontraktów, zakres Zasobów powiązanych, czasy obowiązywania, dostawcy, okres obowiązywania wsparcia technicznego, potencjalne oszczędności w ramach umowy), c. wg parametrów sprzętowych (np. typ procesora, numery seryjne, TCO wg organizacji, zestawienie komputerów i ich szczegółowych parametrów technicznych), d. wg pozostałych danych zarejestrowanych w bazie (ostatni użytkownik, status i czas użytkowania Zasobu przez użytkownika, wykryte nowe pozycje w bazie), e. wg parametrów licencji (typy licencjonowania, czas obowiązywania licencji, licencje nieprzypisane do Zasobów, okresowe statystyki), f. wg parametrów oprogramowania (czarna lista oprogramowania, w podziale na jednostki, użytkowników, sprzęt, bundling oprogramowania, oprogramowanie poza zdefiniowanym standardem), g. zgodności licencyjnej – per organizacja, komórka organizacyjna, wg producenta (bilans licencyjny, brak potwierdzonych licencji), wg użytkownika (powiązane licencje, sprzęt, Zasoby, dostępy).

5.120	SAM - Administracja Raportowanie	Zakres danych o środowisku i licencjach w portalu musi być wystarczający do przygotowania raportu kontroli w trakcie oficjalnego audytu zgodności licencyjnej wg metodyki producenta oprogramowania m.in. a. Oracle Server Worksheet (OSW) (oprogramowanie typu DB, Middleware), b. Microsoft Volume Licensing Service Center (oprogramowanie klienckie, serwerowe, deweloperskie, dostępowe) (raport wdrożenia oprogramowania), c. IBM Passport Advantage (licencje PVU, TB, RVU, AU) (raport wdrożenia oprogramowania), d. VMware Enterprise License Agreement (raport wdrożenia oprogramowania). e. Red Hat f. Cisco
5.121	SAM - Administracja Raportowanie	System SAM powinien prezentować w raportach zgodności licencyjnej, cen zakupu, brakujących licencji oraz wartości nadwyżek niewykorzystywanych (niezainstalowanych), a zakupionych przez Zamawiającego licencji.
5.122	SAM - Administracja Raportowanie	System SAM powinien posiadać mechanizm masowego exportu oraz importu danych pozwalających na szybkie pobranie danych oraz zasilenie narzędzia (masowe zasilenie danymi). Dodatkowo system powinien posiadać zidentyfikowane szablony niezbędne do wykonania zasilenia danymi.
5.123	SAM - Administracja Raportowanie	Inwentaryzacja środowiska polega na automatycznym zebraniu danych licencyjnych poprzez narzędzia platformy z infrastruktury IT Zamawiającego. Jeżeli nie jest możliwa automatyczna identyfikacja (np. urządzenia pracujące w wydzielonych sieciach LAN lub odłączone od sieci) to platforma powinna umożliwić ręczne wprowadzenie danych, w tym zasilanie z plików płaskich (z formatem dowolnym, min. dokument Excel lub .csv).
5.124	SAM - Administracja Raportowanie	System umożliwia definiowanie procesów kontroli zgodności i zarządzania oprogramowaniem.
5.125	SAM - Administracja Raportowanie	System SAM musi mieć możliwość pozyskiwania informacji o zasobach z narzędzi dedykowanych do tych działań oraz raportowanie użycia zasobów w tym licencji.
5.126	SAM - Administracja Raportowanie	System SAM musi umożliwiać eksport raportu do pliku zewnętrznego w co najmniej dwóch wymienionych formatów: XLSX, CSV, PDF, XML.
5.127	SAM - Administracja Raportowanie	System SAM powinien posiadać możliwość definiowania raportu z możliwością udostępnienia go określonej grupie Operatorów.
5.128	SAM - Administracja Raportowanie	System SAM powinien umożliwiać wizualne prezentowanie danych raportowych w formie graficznej tj. wykresy, grafy, trendy, tabelaryczne itd.
5.129	SAM - Administracja Raportowanie	System SAM powinien umożliwiać generowanie cyklicznych powiadomień email na podstawie zdefiniowanych raportów.
5.130	SAM - Administracja Raportowanie	System SAM powinien umożliwiać generowanie powiadomień email w czasie rzeczywistym dla odchyleń (zdefiniowane działania).
5.131	SAM - Administracja Raportowanie	System SAM musi mieć możliwość monitorowania i raportowania użycia zasobów w tym licencji.
5.132	SAM - Administracja Raportowanie	System SAM musi umożliwiać alertowanie odnośnie aktywacji Usług, które spowodują przekroczenie wolumenu licencyjnego na poziomie jednostki organizacyjnej.
5.133	SAM - Administracja Raportowanie	System SAM musi umożliwiać predykcję wyczerpania zasobów, w tym licencji przy czym Administrator i Operator muszą mieć możliwość zdefiniowania co najmniej: 1) progów (liczba, procent, data), 2) Użytkowników informowanych o przekroczeniu progu.

Lp WKR	Typ	Opis
6.1	Administracja - Bezpieczeństwo	System musi umożlwiać przeprowadzenie testów bezpieczeństwa przez podmiot trzeci posiadający odpowiednie kompetencje i doświadczenie bez wsparcia Wykonawcy.
6.2	Administracja - Bezpieczeństwo	System musi umożlwiać korzystanie z uwierzytelniania wieloskładnikowego (MFA).
6.3	Administracja - Bezpieczeństwo	System musi umożliwiać definiowanie ról dostępu do informacji w zależności od rodzaju i autoryzacji Użytkownika Systemu i zapobiegać nieautoryzowanemu dostępowi do Systemu poprzez wbudowane mechanizmy bezpieczeństwa. Jeśli System zarządza hasłami lokalnego Użytkownika Systemu powinien udostępniać mechanizm wymuszający ich kontrolę np. w postaci minimalnej długości hasła, maksymalnego czasu ważności hasła, historii haseł (wymuszenie unikalności haseł), złożoności hasła.
6.4	Administracja - Bezpieczeństwo	Zamawiający nie dopuszcza udostępniania, przekazywania danych z Systemu poza infrastrukturę Zamawiającego bez jego wiedzy i zgody.
6.5	Administracja - Bezpieczeństwo	System musi zapewniać bezpieczeństwo komunikacji. Przesyłane dane muszą być zabezpieczone i szyfrowane za pomocą protokołu TLS w wersji co najmniej 1.2 oraz system musi wspierać wersję 1.3.
6.6	Administracja - Bezpieczeństwo	System musi zapewniać logowanie, przeglądanie i raportowanie zdarzeń systemowych wg zadanych kryteriów (zakresu) umożliwiających identyfikację czasu, osoby, rodzaju i sposobu wykonania czynności na danym obiekcie oraz prób nieautoryzowanego dostępu w tym sposób umożliwiający odtwarzanie historii aktywności Użytkowników Systemu.
6.7	Administracja - Bezpieczeństwo	System musi mieć możliwość szyfrowania przechowywanych danych.
6.8	Administracja - Bezpieczeństwo	System musi posiadać funkcjonalność przeglądania logów systemowych i innych zdarzeń za pomocą filtrów.
6.9	Administracja - Bezpieczeństwo	System musi pozwalać na przesyłanie logów ze zdarzeń do zewnętrznego serwera logów za pomocą protokołu syslog.
6.10	Administracja - Bezpieczeństwo	System musi posiadać oddzielną witrynę dla pracowników firmy, osób współpracujących, kontrahentów itp. służącą do składania anonimowych wniosków (obsługa Sygnalistów) bez konieczności logowania się i pozostawiania jakichkolwiek danych osobowych.
6.11	Administracja - Bezpieczeństwo	System musi zapewniać komunikację platformy z oprogramowaniem agenta za pośrednictwem serwera pośredniczącego (kolektora), którego zadaniem jest miedzy innymi ograniczenie komunikacji pomiędzy podsieciami oraz agregowanie danych przesyłanych do platformy.
6.12	Administracja - Bezpieczeństwo	System musi umożliwiać definiowanie numeru portu, na którym odbywa się komunikacja z agentami.
6.13	Administracja - Bezpieczeństwo	System musi posiadać funkcjonalność tworzenia i odzyskiwania kopii zapasowej danych.
6.14	Administracja - Bezpieczeństwo	System musi posiadać zabezpieczoną (szyfrowanie ruchu) komunikację pomiędzy agentem a Systemem w oparciu o aktualne standardy na rynku.
6.15	Administracja - Bezpieczeństwo	System musi zapewniać możliwość przenoszenia danych do innych systemów Zamawiającego (dane w powszechnie uznanym formacie)
6.16	Administracja - Bezpieczeństwo	System musi umożliwiać integrację z zewnętrznymi systemami przechowującymi dane uwierzytelniające dla wykrywanych systemów, takich jak CyberArk lub podobne.
6.17	Administracja - Bezpieczeństwo	System nie może przechowywać żadnych danych logowania i hasła (nawet zaszyfrowanych) na końcowym punkcie inwentaryzowanym.
6.18	Administracja - Infrastruktura	Wykonawca określi wymagania dla środowiska (ilość serwerów, systemy operacyjne, bazy danych i inne). Środowisko musi być skalowalne, dawać możliwość zwiększenia wydajności poprzez rozbudowę infrastruktury, np. serwerów (w szczególności poprzez dodanie procesorów, pamięci RAM, zwiększenie liczby serwerów).
6.19	Administracja - Infrastruktura	Środowisko musi posiadać możliwość instalacji na platformie konteneryzacyjnej (np. Kubernetes, Openshift). Zamawiający dopuszcza rozwiązanie, w którym główna baza danych nie jest skonteneryzowana.
6.20	Administracja - Infrastruktura	System musi spełniać parametry RTO = 4 godziny, RPO = 5 minut. Architektura Systemu powinna zapewnić dostępność systemu na poziomie 99,8%, bez wliczania ustalanych wcześniej przerw serwisowych.
6.21	Administracja - Infrastruktura	Środowisko produkcyjne Systemu musi umożliwiać instalację w dwóch równolegle pracujących ośrodkach.
6.22	Administracja - Infrastruktura	System musi zapewniać procedury naprawcze na wypadek wystąpienia Awarii, umożliwiające przywrócenie Systemu do stanu sprzed Awarii, na podstawie kryteriów zdefiniowanych przez Administratora. Rozwiązanie dla serwerów aplikacyjnych i bazodanowych.
6.23	Administracja - Infrastruktura	System musi umożliwiać tworzenie całkowitych, przyrostowych kopii bezpieczeństwa Systemu (automatyczne oraz manualne) i danych w trybie on-line oraz zapewniać procedurę przywracania Systemu z kopii bezpieczeństwa po Awarii. W tym zakresie system powinien umożliwiać współpracę z wiodącymi systemami kopii zapasowej (np. Veeam, Commvault, Networker)
6.24	Administracja - Infrastruktura	Wszystkie komponenty systemu muszą być zainstalowane na infrastrukturze zamawiającego, a dane nie mogą być przechowywane i przetwarzane poza infrastrukturą zamawiającego np. w zewnętrznym środowisku chmurowym.
6.25	Administracja - Integracja	System musi zapewniać automatyczną aktualizację (zakładanie, dezaktywowanie, uzupełnianie danych) kont Użytkowników z wykorzystaniem Active Directory oraz innych baz LDAP.
6.26	Administracja - Integracja	System musi zapewniać dwukierunkową integrację z serwerem poczty elektronicznej, co najmniej MS Exchange oraz protokoły SMTP i IMAP.

6.27	Administracja - Integracja	System musi umożliwiać integrację poprzez: 1) API 2) usługi sieciowe (Web Services), 3) dokumenty w formacie XML, 4) e-mail, 5) płaskie pliki tekstowe. 6) interfejsy bazodanowe 7) PowerShell 8) SSH 9) ODBC/JDBC 10) LDAP
6.28	Administracja - Integracja	System musi posiadać następujące gotowe natywne konektory do systemów monitorowania infrastruktury, jak: * Nagios, * Grafana, * Dyntrace, * Azure Monitor, * Zabbix Pozwalające na pobieranie informacji na temat zrejestrowanych w tych systemach zdarzeń (Event) nieprawidłowego działania infrastruktury monitorowanej u Zamawiającego.
6.29	Administracja - Integracja	1. Konfiguracja konektorów do integracji w celu wymiany danych. * Microsoft Active Directory – pobieranie istniejących danych do Systemu, obsługa trybu logowania mix-modę (lokalne oraz domenowe), możliwość obsługi większej ilości domen * Poczta elektroniczna – przekazywanie zgłoszeń poprzez email do systemu * Microsoft SCCM - parametry sprzętowe i oprogramowanie * MS Teams - zakładanie zgłoszeń 2. Testy komunikacji i wymiany danych z ww. narzędziami. 3. Weryfikację działania przepływów pracy w Systemie, inicjowanych przez zintegrowane systemy.
6.30	Administracja - ogólne	System musi posiadać wewnętrzne mechanizmy archiwizacji rekordów (CI, INC, Wnioski, RFC, dokumenty) historycznych lub niepotrzebnych.
6.31	Administracja - ogólne	System musi umożliwiać obsługę niezależnych instancji, wydzielenie wszystkich informacji w zakresie zdefiniowanej jednostki organizacyjnej, zapewniając pełną izolację danych, kont oraz personalizacje paneli Użytkowników w podziale na Klientów (multi-Tenant).
6.32	Administracja - ogólne	System musi zachowywać ciągłość numeracji wszystkich rekordów a) z zachowaniem informacji co się zadziało z rekordem jeśli ostatecznie nie został utworzony (np. jeśli Incydent nie został zapisany to w logach będzie możliwość weryfikacji dlaczego wpis tego Incydentu nie widnieje na liście) lub b) System nadaje numer rekordu dopiero po jego zapisaniu w systemie.
6.33	Administracja - ogólne	System powinien dawać Operatorom możliwość dostosowywania/modyfikacji layout'u/dashboardu/portletu etc. bez konieczności angażowania Administratora systemu.
6.34	Administracja - ogólne	System musi umożliwiać definiowanie nowych oraz modyfikowanie istniejących przepływów pracy (ang. workflow) dla wszystkich implementowanych procesów przy użyciu interfejsu graficznego działające na zasadzie przeciągnij i upuść oraz zaawansowanych narzędzi przy czym modyfikacja musi być możliwa do realizacji przez Użytkownika Systemu z odpowiednim poziomem uprawnień.
6.35	Administracja - ogólne	System musi umożliwiać Operatorowi łatwe przechodzenie pomiędzy obiektami, elementami konfiguracji połączonymi w relacje.
6.36	Administracja - ogólne	System musi zapewniać - możliwość ręcznego i automatycznego przypomnienia o konieczności aktualizacji danych dotyczących procesu, list kontaktowych, analiz, etc.; - możliwość automatycznej dystrybucji list kontrolnych i kwestionariuszy
6.37	Administracja - ogólne	System musi zapewniać możliwość przypisania adresów email, w celu interaktywnej komunikacji z użytkownikiem poprzez wskazany adres email
6.38	Administracja - ogólne	System musi umożliwiać grupowanie rekordów (np zadań w planie, ocen ryzyka) wykonywanie operacji masowych na tych rekordach w Systemie oraz nawigowanie między nimi z poziomu widoku Operatora i Administratora.
6.39	Administracja - ogólne	System musi zapewniać mechanizmy pozwalające na centralne zarządzanie kontami oraz uprawnieniami Administratorów, Operatorów, Użytkowników, Klientów Systemu.
6.40	Administracja - ogólne	System musi zapewniać stosowanie mechanizmów uwierzytelniania Administratorów, Operatorów, Użytkowników. Logowanie SSO z dodatkowym zabezpieczeniem 2FA (MS Authenticator)
6.41	Administracja - ogólne	System musi zapewniać możliwość ustawienia przez Administratora ilości i długości czasu trwania sesji, po której System samoczynnie wyloguje bezczynnego Administratora, Operatora, Użytkownika.
6.42	Administracja - ogólne	System musi zapewniać rejestrację i śledzenie historii dokonywanych modyfikacji i zapisów w Systemie, ze wskazaniem osób dokonujących modyfikacji oraz dat i godzin modyfikacji dla Użytkowników posiadających odpowiednie uprawnienia.
6.43	Administracja - ogólne	System musi umożliwiać Użytkownikowi i Operatorowi dołączanie do zapisów załączników w postaci plików zewnętrznych (co najmniej formaty PDF, DOC, DOCX, XLS, XLSX, GIF, JPG, BMP, TXT, PPT, PPTX, ZIP). System musi posiadać interfejs API do integracji z co najmniej jednym silnikiem antywirusowym dla załączanych plików (np Microsoft Defender).
6.44	Administracja - ogólne	System musi umożliwiać Operatorom i Użytkownikom wyszukiwanie rekordów, obiektów, usług, użytkowników, informacji w repozytorium wiedzy przy użyciu słów kluczowych, ciągów znaków w tym niepełnych wyrazów, fragmentów tekstu z użyciem operatorów logicznych (I, LUB, ORAZ).
6.45	Administracja - ogólne	System musi umożliwiać zarejestrowanie Użytkownika na podstawie informacji z wiadomości e-mail oraz automatycznie z innych zweryfikowanych wewnętrznie i zintegrowanych systemów.

6.46	Administracja - ogólne	System musi wspierać co najmniej procesy ITIL® : 10) Zarządzanie Ciągłością Działania,
6.47	Administracja - ogólne	System musi zapewniać możliwość wysyłania pojedynczych oraz masowych wiadomości e-mail w formacie TXT, HTML w sposób automatyczny lub manualny (przez Operatora) z możliwościa ustawienia interwałów czasowych umożliwiających ponowne syłanie tej samj wiadomości. Sposób wysyłania ww. powiadomień do definiowania przez Administratora.
6.48	Administracja - ogólne	System musi zapewniać definiowanie wielopoziomowej struktury organizacyjnej ręcznie oraz poprzez import danych w odpowiednim formacie, dla Operatorów i Użytkowników. System musi umożliwiać odczytywanie i odtwarzanie struktury organizacyjnej na podstawie danych pochodzących z systemów zewnętrznych np. Active Directory.
6.49	Administracja - ogólne	System musi umożliwiać definiowanie przez Administratora uprawnień i przypisanie ich do użytkowników lub grup użytkowników.
6.50	Administracja - ogólne	System musi umożliwiać wysyłanie do Użytkowników automatycznych powiadomień dotyczących zmian statusów w zdarzeniach, procesach (do których zostali przypisani lub biorą udział), przy czym zawartość powiadomienia oraz warunki wysłania muszą być możliwe do zdefiniowania przez Administratora. System musi zapewniać - możliwość ręcznego i automatycznego przypomnienia o konieczności aktualizacji danych dotyczących procesu, list kontaktowych, analiz, etc.; - możliwość automatycznej dystrybucji list kontrolnych i kwestionariuszy - możliwość akceptacji wyników zgodnie z modelem uprawnień i roli użytkownika
6.51	Administracja - ogólne	System musi umożliwiać automatyczną eskalację hierarchiczną (pionową w ramach struktury organizacyjnej), według kryteriów konfigurowanych przez Administratora, przy czym kryterium to powinno obejmować co najmniej upływ czasu realizacji rekordu/zadania w stosunku do czasu zaplanowanego. Eskalacja powinna polegać na przekazaniu zdefiniowanym osobom lub rolom określonego zakresu informacji o rekordzie/ zadaniu przy czym lista osób (ról) i zakres informacji muszą być możliwe do zdefiniowania przez Administratora.
6.52	Administracja - ogólne	System powinien składać się z trzech niezależnych środowisk: produkcyjne, testowe, developerskie.
6.53	Administracja - ogólne	System musi zapewniać mechanizm jednoczesnego dostępu do danych dla wielu użytkowników, z zastrzeżeniem, że rekord edytowany przez jedną osobę w czasie rzeczywistym blokuje możliwość edycji dla innych osób przy jednoczesnym wyświetlaniu komunikatu o edycji rekordu
6.54	Administracja - Portal Użytkownika	System musi posiadać interfejs wielojęzykowy w tym w polskiej wersji językowej i angielskiej z możliwością wyboru przez Użytkownika Systemu. System powinien posiadać intuicyjny interfejs wraz z mechanizmami podpowiedzi (samouczków) prowadzących użytkownika przez poszczególne, ekrany / widoki/ formularze i zakładki.
6.55	Administracja - Portal Użytkownika	System musi być dostępny z poziomu przeglądarki internetowej w ich najnowszych wersjach, bez konieczności instalowania komponentów trzecich lub plug-in. Aplikacja ma być wspierana przez popularne przeglądarki na różnych systemach: Windows, MAC OS, Linux w szczególności Google Chrome, Mozilla FireFox oraz Safari co najmniej w wersji aktualnej na dzień składania ofert.
6.56	Administracja - Raportowanie	System musi zapewniać: - możliwość elastycznego raportowania – opracowanie widoków dynamicznych, szablonów dokumentacji - możliwość opracowania przekrojowych raportów analitycznych - możliwość definiowania za pomocą kreatora szablonów raportu, planów, procedur, etc. - możliwość customizacji layoutu danego raportu (kolorystyka, znaki graficzne / logo - wbudowany mechanizm raportowania z predefiniowanymi wzorcami jak i z możliwością tworzenia własnych raportów
6.57	Administracja - Raportowanie	System musi umożliwiać eksport raportu do pliku zewnętrznego w co najmniej dwóch wymienionych formatach: XLSX, CSV, PDF, XML.
6.58	Administracja - Raportowanie	System musi umożliwiać wizualne prezentowanie danych raportowych w formie graficznej tj. wykresy, grafy, trendy, tabelaryczne itd.
6.59	Administracja - Raportowanie	System powinien umożliwiać generowanie cyklicznych powiadomień email na podstawie zdefiniowanych raportów.
6.60	Administracja - Raportowanie	System powinien umożliwiać generowanie powiadomień email w czasie rzeczywistym dla odchyleń (zdefiniowane działania).
6.61	Administracja - Raportowanie	System musi zapewniać możliwość ustawienia mierników KPI oraz mierzenia ich efektywności (opcjonalnie).
6.62	GRC	Wymagane jest, aby funkcjonalność systemu do zarządzania ryzykiem w bezpieczeństwie informacji, zarządzania ryzykiem w ciągłości działania oraz zarządzania analizą wpływu na biznes była zgodna z aktualnie obowiązującymi następującymi normami: PN-EN ISO/IEC 27001, PN-EN ISO/IEC 22301, PN-EN ISO/IEC 27005; PN-EN ISO/IEC 31000 lub równoważnymi.
6.63	GRC	System musi być zgodny z aktualnymi wymaganiami Krajowego Systemu Cyberbezpieczeństwa oraz dyrektywy NIS2.
6.64	GRC	Wymagane jest, aby System był aktualizowany i modyfikowany na bieżąco, co do zgodności z obowiązującymi przepisami prawa oraz wewnętrznymi aktami prawnymi i regulaminami COI w okresie objętym wsparciem przez Dostawcę systemu.
6.65	GRC	System musi posiadać logiczne i funkcjonalne mechanizmy umożliwiające zarządzanie ryzykiem w bezpieczeństwie informacji, zarządzanie ryzykiem w ciągłości działania, zarządzanie analizą wpływu na biznes, takie jak powiązanie z bazą aktywów (CI), informacjami dotyczącymi zarządzania incydentami.

6.66	GRC	System musi posiadać możliwość szczegółowego określenia zasobów, w tym: 20.5.1. Identyfikację zasobu, opis i tworzenie listy procesów, podprocesów (w tym biznesowych, wspierających i innych); 20.5.2. Możliwość opracowania „workflow" w celu uzyskiwania akceptacji i zatwierdzania danych na różnych poziomach uprawnień użytkowników;
6.67	GRC	System musi zapewniać realizację wszystkich zadań wynikających z procesu zarządzania ryzykiem w bezpieczeństwie informacji (w aspekcie identyfikacji, analizy, ewaluacji, postępowania z ryzykiem, monitorowania, komunikacji) i generować stosowne dokumenty i raporty
6.68	GRC	System musi zapewniać realizację wszystkich zadań wynikających z procesu zarządzania analizą wpływu na biznes (BIA) – (kontekst, usługi, procesy, rodzaje wpływów i kryteria oddziaływania, szacowanie strat zakłóceń, wymagania wznowienia usług, priorytety odtwarzania, minimalne zasoby do utrzymania ciągłości, zależności priorytetowych działań) i generować stosowne dokumenty i raporty
6.69	GRC	System musi zapewniać realizację wszystkich zadań wynikających z procesu zarządzania ryzykiem w ciągłości działania (identyfikacji, analizy, ewaluacji, postępowania z ryzykiem, monitorowania, komunikacji) i generować stosowne dokumenty i raporty
6.70	GRC	System musi zapewniać zaimplementowane i opisane metodyki oraz umożliwiać tworzenie i definiowanie metodyk zarządzania ryzykiem w oparciu o różne wzory i mechanizmy dostosowane do obszarów i kontekstu podstawowych atrybutów takich jak poufność, integralność dostępność oraz niezawodność i rozliczalność (w obszarze ciągłości działania). W szczególności System musi zapewniać dowolne agregowanie aktywów organizacji wprowadzonych do Systemu, stosowanie wobec w/w agregacji innych metodyk zarządzania ryzykiem w celu odwzorowania specyficznych procesów biznesowych
6.71	GRC	System musi zapewniać wprowadzanie i utrzymywanie kompletnego, spójnego i aktualnego rejestru aktywów oraz import aktywów z innych baz
6.72	GRC	System musi zapewniać wypełnianie i generowanie metryk / paszportów zasobu zawierającego minimum: - nazwę - typ - właściciela - zasoby podrzędne i nadrzędne (z wyraźnym rozgraniczeniem) - umiejscowienie
6.73	GRC	System musi zapewniać wskazanie właścicieli: podmiotów wewnętrznych i zewnętrznych odpowiedzialnych za np. dostarczenie, utrzymania, nadzór, serwisowanie lub wsparcie aktywów
6.74	GRC	System musi zapewniać wskazanie działań związanych z danym aktywem (np. czasowe wyłączenie, serwis, audyt) oraz zapewnić komunikację zdarzeń, przypomnienia i raportowanie
6.75	GRC	System musi zapewniać możliwość zgłaszania w systemie przez użytkowników propozycji zmiany, uwag i ryzyk do modelu i obiektów z poziomu systemu (z możliwością dołączania dokumentów przez użytkownika do zgłaszanej propozycji) oraz za pomocą wbudowanego workflow automatyzować przebieg zmiany (opiniowania, zatwierdzania, wdrażania)
6.76	GRC	System musi zapewniać kokpity menadżerskie prezentujące syntetycznie wyniki analizy BIA, analizy ryzyka (w tym bezpieczeństwa informacji).
6.77	GRC	System musi zapewniać możliwość rozpoczęcia wskazanych czynności dla wszystkich procesów w wybranym terminie
6.78	GRC	System musi zapewniać możliwość wysłania automatycznego powiadomienia do wybranych osób/ról dla zdefiniowanego workflow (poczta elektroniczna), m.in. przypomnienia o nadchodzących terminach, nowych ryzykach, incydentach, zdarzeniach, przekroczeniach poziomów ryzyk poza zdefiniowany poziom; możliwość weryfikacji kompletności/statusu realizacji poszczególnych zadań w zdefiniowanych punktach kontrolnych (np.: nieaktualna analiza, brak danych) – w definiowalnych interwałach czasowych
6.79	GRC	System musi zapewniać możliwość podglądu danych historycznych z poprzednich wersji (listy kontaktowe, listy procesów/zasobów, etc.) wraz z możliwością porównywania danych
6.80	GRC	System musi zapewniać możliwość śledzenia, przeglądu pobierania danych historycznych, np. już wykonanego szacowania i analizy ryzyka w szczególności każdego ryzyka z osobna, wykonanej analizy BIA
6.81	GRC	System musi zapewniać możliwość weryfikacji przez użytkownika (wykonującego ocenę) jak również przez zarządzających oceną ryzyka/ analizą BIA statusu swojego zadania/wszystkich zadań (dot. zarządzającego oceną) oraz wglądu do treści wykonanej oceny/ zadania
6.82	GRC	W obszarze zarządzania ryzykiem w bezpieczeństwie informacji, w tym wykonywania analizy ryzyka System musi zapewniać zautomatyzowany proces analizy ryzyka w oparciu o zidentyfikowane i ocenione zasoby z uwzględnieniem procesów realizowanych z ich udziałem
6.83	GRC	W obszarze zarządzania ryzykiem w bezpieczeństwie informacji, w tym wykonywania analizy ryzyka System musi zapewniać możliwość samodzielnego dostosowania i określenia skali ocen oraz progów prawdopodobieństwa i wpływu (dla ryzyka oraz szansy)
6.84	GRC	W obszarze zarządzania ryzykiem w bezpieczeństwie informacji, w tym wykonywania analizy ryzyka System musi zapewniać możliwość przeprowadzenia klasyfikacji informacji
6.85	GRC	W obszarze zarządzania ryzykiem w bezpieczeństwie informacji, w tym wykonywania analizy ryzyka System musi zapewniać możliwość przeprowadzenia identyfikacji i oceny zasobów (odpowiedzialnych za przetwarzanie informacji)
6.86	GRC	W obszarze zarządzania ryzykiem w bezpieczeństwie informacji, w tym wykonywania analizy ryzyka System musi zapewniać predefiniowany katalog zagrożeń
6.87	GRC	W obszarze zarządzania ryzykiem w bezpieczeństwie informacji, w tym wykonywania analizy ryzyka System musi zapewniać możliwość porównania ryzyka dla danego zidentyfikowanego zasobu / procesu

6.88	GRC	W obszarze zarządzania ryzykiem w bezpieczeństwie informacji, w tym wykonywania analizy ryzyka System musi zapewniać identyfikację technicznych, osobowych, naturalnych i realnych ryzyk dla dowolnej lokalizacji wraz z ich oceną i wpływem
6.89	GRC	W obszarze zarządzania ryzykiem w bezpieczeństwie informacji, w tym wykonywania analizy ryzyka System musi zapewniać identyfikację i pomiar potencjalnych zagrożeń dla dowolnej informacji, lokalizacji informacji, zasobu, w którym przetwarzana jest informacjalub i obiektu.
6.90	GRC	W obszarze zarządzania ryzykiem w bezpieczeństwie informacji, w tym wykonywania analizy ryzyka System musi zapewniać dokonywanie oceny ryzyka (w tym szans) przy pomocy wprowadzonych skal ocen
6.91	GRC	W obszarze zarządzania ryzykiem w bezpieczeństwie informacji, w tym wykonywania analizy ryzyka System musi zapewniać powiązanie zdarzenia materializacji ryzyka z poszczególnymi ryzykami
6.92	GRC	W obszarze zarządzania ryzykiem w bezpieczeństwie informacji, w tym wykonywania analizy ryzyka System musi zapewniać określenie sposobu postępowania z ryzykiem
6.93	GRC	W obszarze zarządzania ryzykiem w bezpieczeństwie informacji, w tym wykonywania analizy ryzyka System musi zapewniać zarządzania zadaniami określonymi po przeprowadzeniu analizy ryzyka
6.94	GRC	W obszarze zarządzania ryzykiem w bezpieczeństwie informacji, w tym wykonywania analizy ryzyka System musi zapewniać dostosowanie do wymagań wybranej metodyki przeprowadzenia analizy ryzyka wraz z oceną
6.95	GRC	W obszarze zarządzania ryzykiem w bezpieczeństwie informacji, w tym wykonywania analizy ryzyka System musi zapewniać opracowanie raportu pokazującego prawdopodobieństwo i dotkliwość zagrożeń
6.96	GRC	W obszarze zarządzania ryzykiem w bezpieczeństwie informacji, w tym wykonywania analizy ryzyka System musi zapewniać opracowanie planu postępowania z ryzykiem (listy kontrolne, zadania/kroki, śledzenie statusów, powiadamianie odbiorców, itp.)
6.97	GRC	W obszarze zarządzania ryzykiem w bezpieczeństwie informacji, w tym wykonywania analizy ryzyka System musi zapewniać automatyzację planowania działań wynikających z analizy ryzyka z określeniem ról i odpowiedzialności. Poprzez mechanizmy workflow obsługiwać proces realizacji działań wynikających z planu postępowania z ryzykiem (powiadomienie o zadaniu, okresowe raportowanie, zrealizowanie zadania wraz ze wskazaniem wyników, ocenę skuteczności działań)
6.98	GRC	W obszarze zarządzania ryzykiem w bezpieczeństwie informacji, w tym wykonywania analizy ryzyka System musi zapewniać zarządzanie planami ciągłości działania w postaci repozytorium planów. Repozytorium planów ma mieć drzewiastą postać, a każdy plan ma posiadać odrębna metrykę, która umożliwia zarządzanie zmianą i komunikację planu dla wskazanych obiektów struktury organizacyjnej (komórka, stanowisko, osoba)
6.99	GRC	W obszarze zarządzania ryzykiem w bezpieczeństwie informacji, w tym wykonywania analizy ryzyka System musi zapewniać powiązanie incydentu z ryzykiem (rozszerzenie o moduł zarządzania incydentami).
6.100	GRC	W obszarze zarządzania ryzykiem w bezpieczeństwie informacji, w tym wykonywania analizy ryzyka System musi zapewniać powiązanie incydentu z procesem oraz zasobem (w przyszłości rozszerzenie o moduł zarządzania incydentami)
6.101	GRC	W obszarze zarządzania ryzykiem w bezpieczeństwie informacji, w tym wykonywania analizy ryzyka System musi zapewniać agregację ryzyk (integrację i powiązanie) w ramach hierarchii ryzyk
6.102	GRC	W obszarze zarządzania ryzykiem w bezpieczeństwie informacji, w tym wykonywania analizy ryzyka System musi zapewniać generowanie mapy ryzyka i reakcji na ryzyko
6.103	GRC	W obszarze zarządzania analizą wpływu na biznes BIA System musi zapewniać modelowanie diagramów procesów przynajmniej w dwóch notacjach: - BPMN, - EPC.
6.104	GRC	W obszarze zarządzania analizą wpływu na biznes BIA System musi zapewniać przeprowadzenie procesu identyfikacji kontekstu organizacji, usług, procesów, działań wspierających dostarczanie wyrobów i usług (w tym zasobów, wartości zasobów), niezbędnego do przeprowadzenia analizy BIA
6.105	GRC	W obszarze zarządzania analizą wpływu na biznes BIA System musi zapewniać przeprowadzenie procesu identyfikacji rodzajów wpływu i kryteriów oddziaływania
6.106	GRC	W obszarze zarządzania analizą wpływu na biznes BIA System musi zapewniać wykonanie analizy wpływu na biznes (BIA) dla procesów poprzez mechanizmy samooceny skutków przestoju przez właścicieli procesów
6.107	GRC	W obszarze zarządzania analizą wpływu na biznes BIA System musi zapewniać przeprowadzenie BIA w kontekście wielu kryteriów skutku i czasu
6.108	GRC	W obszarze zarządzania analizą wpływu na biznes BIA System musi zapewniać możliwość wskazania jakie zasoby są niezbędne do realizacji usługi, procesów i wykazanie ich na karcie oceny/procesu w celu utrzymania ciągłości działania.
6.109	GRC	W obszarze zarządzania analizą wpływu na biznes BIA System musi zapewniać określenie oraz automatyzować wyliczenie czasów wymaganych wznowienia usług: RTO, RPO, MTPD (o ile taka funkcjonalność występuje w Systemie)
6.110	GRC	W obszarze zarządzania analizą wpływy na biznes BIA System musi zapewniać przeprowadzenie procesu określania procesów krytycznych/ określania priorytetów odtwarzania procesów
6.111	GRC	W obszarze zarządzania analizą wpływu na biznes BIA System musi zapewniać określenie zależności i współzależności priorytetowych działań
6.112	GRC	W obszarze zarządzania analizą wpływu na biznes BIA System musi zapewniać mechanizm okresowego przeglądu analizy BIA, pozwalający na zautomatyzowanie ponownej oceny w kolejnym okresie
6.113	GRC	W obszarze zarządzania ryzykiem w ciągłości działania System musi zapewniać zautomatyzowany proces analizy ryzyka w oparciu o zasoby z uwzględnieniem procesów realizowanych z ich udziałem

6.114	GRC	W obszarze zarządzania ryzykiem w ciągłości działania System musi zapewniać możliwość samodzielnego dostosowania i określenia skali ocen oraz progów prawdopodobieństwa i wpływu (dla ryzyka oraz szansy)
6.115	GRC	W obszarze zarządzania ryzykiem w ciągłości działania System musi zapewniać predefiniowany katalog zagrożeń
6.116	GRC	W obszarze zarządzania ryzykiem w ciągłości działania System musi zapewniać inwentaryzację wszystkich zasobów niezbędnych do utrzymania ciągłości działania
6.117	GRC	W obszarze zarządzania ryzykiem w ciągłości działania System musi zapewniać klasyfikację i wycenę zasobów (określenie ich istotności, warości)
6.118	GRC	W obszarze zarządzania ryzykiem w ciągłości działania System musi zapewniać dokonywanie oceny ryzyka (w tym szans) przy pomocy wprowadzonych skal ocen
6.119	GRC	W obszarze zarządzania ryzykiem w ciągłości działania System musi zapewniać powiązanie zdarzenia materializacji ryzyka z poszczególnymi ryzykami
6.120	GRC	W obszarze zarządzania ryzykiem w ciągłości działania System musi zapewniać stworzenie karty procesu, za pomocą dedykowanego elektronicznego formularza elektronicznego, z prezentacją ryzyk oraz zasobów wykorzystywanych w procesie
6.121	GRC	W obszarze zarządzania ryzykiem w ciągłości działania System musi zapewniać określenie sposobu postępowania z ryzykiem
6.122	GRC	W obszarze zarządzania ryzykiem w ciągłości działania System musi zapewniać możliwość zarządzania zadaniami określonymi po przeprowadzeniu analizy ryzyka
6.123	GRC	W obszarze zarządzania ryzykiem w ciągłości działania System musi zapewniać dostosowanie do wymagań wybranej metodyki przeprowadzenia analizy ryzyka wraz z oceną
6.124	GRC	W obszarze zarządzania ryzykiem w ciągłości działania System musi zapewniać możliwość opracowania raportu pokazującego prawdopodobieństwo i dotkliwość zagrożeń
6.125	GRC	W obszarze zarządzania ryzykiem w ciągłości działania System musi zapewniać opracowanie planu postępowania z ryzykiem (listy kontrolne, zadania/kroki, śledzenie statusów, powiadamianie odbiorców, itp.)
6.126	GRC	W obszarze zarządzania ryzykiem w ciągłości działania System musi zapewniać automatyzację planowania działań wynikających z analizy ryzyka z określeniem ról i przypisanych odpowiedzialności. Poprzez mechanizmy workflow obsługiwać proces realizacji działań wynikających z planu postępowania z ryzykiem (powiadomienie o zadaniu, okresowe raportowanie, zrealizowanie zadania wraz ze wskazaniem wyników, ocenę skuteczności działań)
6.127	GRC	W obszarze zarządzania ryzykiem w ciągłości działania System musi zapewniać zarządzanie planami ciągłości działania w postaci repozytorium planów. Repozytorium planów ma mieć drzewiastą postać, a każdy plan ma posiadać odrębna metrykę, która umożliwia zarządzanie zmianą i komunikację planu dla wskazanych obiektów struktury organizacyjnej (komórka, stanowisko, osoba)
6.128	GRC	W obszarze zarządzania ryzykiem w ciągłości działania System musi zapewniać powiązanie incydentu z ryzykiem po wdrożeniu modułu zarządzania Incydentami.
6.129	GRC	W obszarze zarządzania ryzykiem w ciągłości działania System musi zapewniać agregację ryzyk (integrację i powiązanie) w ramach hierarchii ryzyk; generowanie map ryzyka i reakcji na ryzyko
6.130	GRC - Zarządzanie Wiedzą	Instrukcja obsługi dla użytkowników i administratorów w systemie – poza dostarczoną w wersji PDF – powinna być dodatkowo (jeżeli to możliwe) zaszyta w systemie w formie „dymków" lub podpowiedzi