

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

„Wdrożenie systemów OSS/BSS wraz ze zwirtualizowaną infrastrukturą obliczeniową”

znak postępowania: **ZZ.2131.599.2018.TKI [OSE-S] [OSE-B] [OSE-D] [OSE2019]**

Spis treści

1. Wprowadzenie	5
1.1. Koncepcja OSE	5
2. Definicje	7
3. Architektura biznesowa Operatora OSE	11
3.1. Architektura danych operatora OSE	12
3.2. Katalog produktów Ogólnopolskiej Sieci Edukacyjnej	14
3.3. Główne procesy operatora OSE	17
3.4. Proces zarządzania produktami OSE	18
3.5. Proces obsługi klienta	30
3.6. Proces technicznej obsługi	35
3.7. Proces realizacji usług	42
3.8. Proces utrzymania sieci, usług i systemów	49
3.9. Proces współpracy z operatorami	55
3.10. Proces zarządzania bezpieczeństwem	66
3.11. Proces rozwoju OSS/BSS	74
3.12. Proces wsparcia OSE	84
3.13. Proces marketingu i komunikacji	100
4. Sieć OSE	102
4.1. Sieć szkolna	103
4.2. Sieć dostępowa	106
4.3. Sieć szkieletowa	107
4.4. Koncepcja świadczenia usługi dla szkoły	109
5. Bezpieczeństwo OSE	111
5.1. Architektura Infrastruktury Bezpieczeństwa	112
6. Platforma Operatora OSE	114

6.1 Warstwa aplikacyjna.....	117
6.1.1. Funkcjonalności obszaru OSS	119
6.1.2. Funkcjonalności obszaru BSS	125
6.2. Warstwa infrastruktury	128
6.2.1. Wstęp.....	128
6.2.2. Założenia techniczne	129
6.2.3. Ośrodki przetwarzania danych	131
6.2.4. Skalowalność systemu	132
6.2.5. Magazyn danych.....	133
6.2.6. Architektura sieci.....	134
6.3. Koncepcja wdrożenia POOSE.....	142
6.3.1. Wdrożenie warstwy aplikacyjnej.....	144
6.3.2. Wdrożenie infrastruktury	152
7. Opis przedmiotu zamówienia	159
7.1. Opis ogólny	159
7.1.1. Beneficjenci systemu OSS/BSS	160
7.1.2. Informacje mające wpływ na architekturę rozwiązania.....	162
7.2. Opis funkcjonalności dla obszarów biznesowych.....	185
7.2.1. Proces zarządzania produktami OSE	185
7.2.2. Proces obsługi klienta	188
7.2.3. Proces obsługi technicznej	192
7.2.4. Proces realizacji usług.....	202
7.2.5. Proces utrzymania sieci, usług i systemów.....	208
7.2.6. Proces współpracy z operatorami	211
7.2.7. Proces zarządzania bezpieczeństwem OSE	216
7.2.8. Proces rozwoju OSS/BSS.....	219
7.2.9. Proces wsparcia OSE.....	222
7.2.10. Proces marketingu i komunikacji.....	234
7.3. Opis funkcjonalności dla całego rozwiązania	235
7.3.1. Silnik Procesów Biznesowych	235
7.3.1. Uwierzytelnianie i autoryzacji dla użytkowników wewnętrznych i dla partnerów OSE.....	236
7.3.2. Automatyzacja, integracja i elastyczność całości rozwiązania	240
7.3.3. Centralny System Raportowy	242
7.3.4. Integracja z systemami zewnętrznymi	244
7.3.5. Rozwiązanie musi spełniać następujące wysokopoziomowe wymagania:	251

7.3.6. Rozwiązanie musi spełniać następujące wymagania regulacyjne	254
7.4. Opis funkcjonalności dla obszaru OSS	254
7.4.1. Monitorowanie infrastruktury i usług OSE (Fault & Availability oraz Performance Management)	255
7.4.2. Zarządzanie konfiguracją (Config Manager)	287
7.4.3. Provisionig	292
7.4.4 Aktywator Usług (wdrażany w Fazie 1 wdrożenia)	303
7.4.5. Inwentaryzacja OSE (Inventory)	305
7.5. Opis funkcjonalności dla obszaru BSS	312
7.5.1. Obszar Centrum Kontaktu	312
7.5.2. Obszar Zarządzania Klientami	319
7.5.3. Obszar Zarządzania Partnerami	321
7.5.4. Obszar Rozliczeń	322
7.5.5. Obszar Łańcuch Dostaw	325
7.5.6. Obszar Katalog Produktów	326
7.5.7. Obszar Zarządzania dokumentami	327
7.5.8. Obszar Zarządzania przedsiębiorstwem	328
7.6. Środowisko testowe	329
7.7. Infrastruktura dla systemów OSS/BSS	329
7.8. Platforma wirtualizacyjna - wymagania funkcjonalne	331
7.8.1 Wirtualizacja mocy obliczeniowej	331
7.8.2 Moduł wirtualizacji przestrzeni dyskowej	333
7.8.3 Moduł wirtualizacji funkcji sieciowych	336
7.8.4 Moduł monitorowania i zarządzania pojemnością i efektywnością platformy	337
7.8.5 Moduł zarządzania cyklem życia platformy	343
7.8.6 Moduł zbierania zbieranie logów z infrastruktury	343
7.9. Opis infrastruktury wirtualizacyjnej	344
7.9.1 Infrastruktura dla środowiska produkcyjnego	344
7.9.2 Wymagania ilościowe warstwy oprogramowania	345
7.9.3 Wymagania ogólne dla warstwy sprzętowej dla serwerów w węzłach centralnych	346
7.9.4 Wymagania ogólne dla warstwy sprzętowej dla serwerów w regionach	350
7.10. Obiektowy system składowania danych	354
7.11 Backup i Archiwizacja	360
7.11.1 Backup i Archiwizacja - Deduplikatory	362
7.11.2 Backup i Archiwizacja - Wymagane funkcjonalności oprogramowania do zabezpieczania danych ..	366
7.11.3 Backup i Archiwizacja - Wymagania dotyczące backupu serwerów (Data Center)	366

7.11.4 Backup i Archiwizacja - Wymaga funkcjonalności – dotyczących monitorowania, raportowania oraz przeszukiwania backupów.....	369
7.11.5 Backup i Archiwizacja - Wymaga funkcjonalności – dotyczy rozwiązań Continuous Data Protection dla środowisk wirtualnych	370
7.12. Wymagania wdrożeniowe	372
7.12.1. Zakres prac dla Fazy 0.....	372
7.12.2. Zakres prac dla Fazy 1.....	372
7.12.3. Zakres prac dla Fazy 2.....	379
7.12.4. Zakres prac dla Fazy 3.....	382
7.12.5. Zakres prac dla Fazy 4.....	385
7.12.6. Zakres prac dla Fazy 5.....	387

1. Wprowadzenie

Ogólnopolska Sieć Edukacyjna ma na celu zapewnienie dostępu do szybkiego, bezpiecznego Internetu dla szkół. OSE jest publiczną siecią telekomunikacyjną, opartą o istniejącą infrastrukturę szerokopasmową wybudowaną w ramach inwestycji komercyjnych oraz dofinansowanych ze środków publicznych w ramach Programu Operacyjnego Polska Cyfrowa. Za uruchomienie i utrzymanie Sieci, oraz w szczególności za dostarczenie szkołom usługi dostępu do Internetu o symetrycznej przepustowości co najmniej 100 Mb/s wraz z kompleksowymi usługami bezpieczeństwa sieciowego, w tym ochrony przed zagrożeniami dla prawidłowego rozwoju uczniów, odpowiedzialny jest Operator OSE.

Operatorem OSE został NASK - Państwowy Instytut Badawczy (zwany dalej „NASK”), nadzorowany przez Ministra Cyfryzacji.



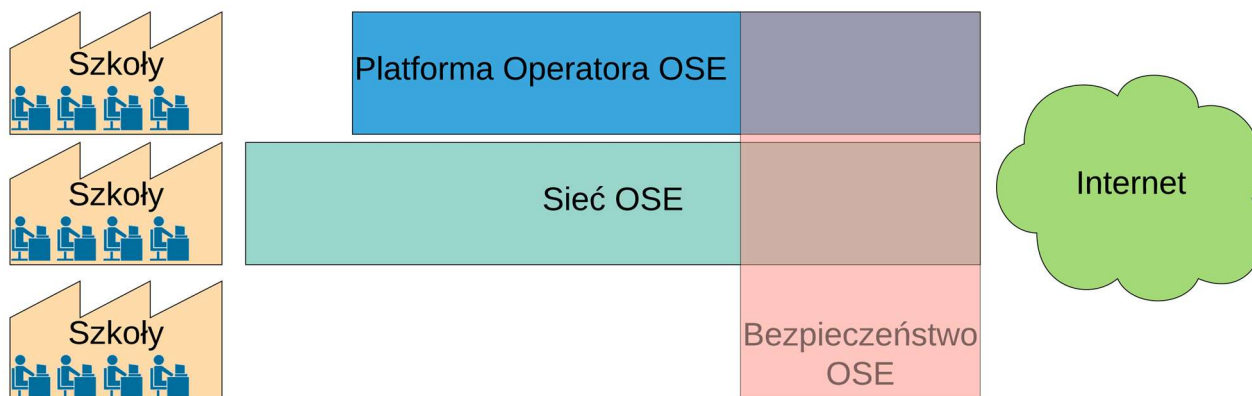
W Polsce istnieje 25 015 szkół zlokalizowanych w 19 500 lokalizacjach. Podstawowym zadaniem OSE ma być zapewnienie szkołom w Polsce możliwości dostępu do bezpiecznego Internetu i zasobów edukacyjnych wraz z szeregiem usług powiązanych, w tym:

- 1) Zapewnienie usług dostępu do sieci Internet o przepływności minimum 100 Mb/s symetrycznie,
- 2) Zapewnienie usług bezpieczeństwa umożliwiających ochronę użytkowników,
- 3) Zapewnienie dostawcom treści edukacyjnych dostępu do użytkowników sieci OSE.
- 4) Umożliwienia wspomagania procesu kształcenia w szkole.

W ramach budowy OSE planuje się uruchomienie sieci rozległej transmisji danych, systemów bezpieczeństwa wraz z systemami wsparcia obejmującymi m.in. systemy zarządzania tożsamością, OSS, BSS, SIEM jak również urządzenia abonenckie (CPE), przełączniki, AP sieci bezprzewodowej. Usługi obejmować będą swoim zasięgiem terytorium Polski. Sieć OSE, zbudowana będzie z węzłów zlokalizowanych na terenie 16 województw.

1.1. Koncepcja OSE

NASK, jako operator OSE zapewniający dostęp do internetu dla szkół realizuje swoje działania w oparciu o trzy podstawowe obszary:



1. Sieć OSE - Infrastruktura telekomunikacyjna wykorzystywana do świadczenia przez Operatora OSE usług dostarczanych klientom (takich jak m.in. dostęp do internetu). Dostęp szkolny do internetu jest realizowany w czterech podstawowych wariantach:

- a. OSE - operator dostępowy odpowiada jedynie za łącze do szkoły, instalację i konfigurację punktu dostępowego realizuje operator OSE i on dostarcza wszystkie urządzenia,
 - b. POPC - instalacja punktu dostępowego w szkole i dostarczenie łącza dostępowego ze szkoły do sieci szkieletowej jest w odpowiedzialności beneficjenta POPC, operator OSE odpowiada jedynie za konfigurację punktu dostępowego i ewentualną rozbudowę o dodatkowe urządzenia (np. switchy)
 - c. MAN - punkt dostępowy i sieć dostępową jest w odpowiedzialności OPS/szkoły, w odpowiedzialności operatora OSE może znaleźć się agregacja pomiędzy łączami dostępowymi a siecią szkieletową, operator OSE odpowiada za usługę, ale MAN realizuje wszelkie prace związane z konfiguracją punktu dostępowego w szkole.
 - d. ODN - punkt dostępowy jest w odpowiedzialności OPS / szkoły, część łącza jest w odpowiedzialności ODN, a część w odpowiedzialności OSE, przebieg łącza jest wydłużony o dodatkowy węzeł - Powiatowy Punkt Wymiany Ruchu
2. Platforma Operatora OSE - platforma złożona z komponentów informatycznych, których celem jest wsparcie wszelkiej działalności NASK, jako Operatora OSE (w tym m.in. zarządzanie infrastrukturą sieciową, działania sprzedażowe czy rozliczanie wydatków) składające się z dwóch typów komponentów:
- a. Systemy OSE - systemy informatyczne tworzone lub rozwijane na potrzeby operatora OSE
 - b. Systemy NASK - systemy informatyczne wykorzystywane w ramach podstawowej działalności NASK PIB, które zostaną zintegrowane z rozwiązaniem na potrzeby OSE
3. Bezpieczeństwo OSE - komponenty warstwy sieciowej, sprzęt oraz oprogramowanie, których celem jest zapewnienie bezpieczeństwa teleinformatycznego sieci OSE oraz jej użytkownikom.

2. Definicje

Definicja	Wyjaśnienie
ADC (Application Delivery Controller)	system realizujący równomierne rozłożenie obciążenia na Urządzenia należące do Systemów ADC, NG Firewall, inspekcji ruchu SSL/TLS
Administratorzy OSE	komórka organizacyjna odpowiadająca za utrzymanie sieci OSE
Beneficjent POPC	przedsiębiorca telekomunikacyjny będący beneficjentem działania POPC 1.1, budujący łącza światłowodowe do jednostek oświatowych
Centralny Węzeł Bezpieczeństwa	węzeł Bezpieczeństwa zlokalizowany w Węźle Centralnym dostarczający mechanizmy ochrony Zasobów obliczeniowych OSE
Lokalizacja węzła / Kolokacja	miejsce fizyczne, powierzchnia kolokacyjna, w którym pracuje Węzeł sieci / Węzeł Bezpieczeństwa.
Węzeł agregacyjny	węzeł do którego dołączone są łącza dostępne do szkół, węzeł ten nie ma bezpośredniego połączenia do sieci Internet
Węzeł bezpieczeństwa	zestaw Urządzeń wraz z Oprogramowaniem, realizujących funkcje bezpieczeństwa (m.in. dekrypcja SSL, funkcjonalność IPS, NG Firewall itd.). Zamawiający wyróżnia dwa typy Regionalny Węzeł Bezpieczeństwa oraz Centralny Węzeł Bezpieczeństwa
Węzeł szkieletowy	węzeł zapewniający przeniesienie ruchu z węzłów agregacyjnych do sieci Internet, a także inżynierię ruchu, na styku sieci OSE z Internetem
Węzeł sieci	zespół urządzeń pracujących w jednej lokalizacji, zapewniających komunikację użytkownikom sieci (Szkołom) z siecią Internet. Węzeł wraz z innymi węzłami, z którymi jest połączony za pośrednictwem łączy szkieletowych, stanowi sieć OSE. Częścią węzła są Regionalne i Centralne Węzły Bezpieczeństwa.
Partner serwisowy	podmiot realizujący usługi techniczne w jednostkach oświatowych w zakresie podłączania szkół do OSE oraz serwisowania na terenie szkoły świadczonych przez OSE usług
Dostawca łącza dostępowego	przedsiębiorca telekomunikacyjny budujący łącza światłowodowe do jednostek oświatowych, także Beneficjent POPC, dzierżawiący je na rzecz operatora OSE
Operator Agregujący	przedsiębiorca telekomunikacyjny, zbierający od Dostawców łączy dostępowych łącza do jednostek oświatowych, agregujący je w warstwie Ethernet oraz oddający operatorowi OSE w Węźle Agregacyjnym
Operator Sieci Regionalnej	operator sieci dostępowych zapewniający obsługę informatyczną dla jednostek edukacyjnych. Szkoły zgłaszają wszelkie problemy do OSR, który ewentualnie przekazuje je do OSE. OSR to sieci miejskie (MAN) i sieć Ośrodka Doskonalenia Nauczycieli (ODN).
Dostawca sieci szkieletowej	przedsiębiorca telekomunikacyjny, udostępniający swoją infrastrukturę na potrzeby budowy szkieletu OSE, czyli łączy pomiędzy węzłami OSE
Dostawca kolokacji	podmiot świadczący na rzecz Zamawiającego usługi kolokacji w centrum przetwarzania danych, w którym zlokalizowany jest Węzeł centralny i/lub Węzeł agregacyjny sieci OSE

Definicja	Wyjaśnienie
Jednostka oświatowa	placówka edukacyjna należąca do systemu oświaty w Polsce, w szczególności szkoła podstawowa, gimnazjum, szkoły ponadgimnazjalne, policealne, artystyczne, inne szkoły specjalne i placówki oświatowo-wychowawcze oraz opiekuńcze z wyłączeniem szkół dla dorosłych
Operator OSE	przedsiębiorca telekomunikacyjny świadczący usługi dostępu do Internetu za pośrednictwem OSE na rzecz Jednostek edukacyjnych, Operator OSE odpowiada za podłączanie Jednostek Oświatowych, a następnie obsługuje je na bazie wewnętrznych i zewnętrznych struktur organizacyjnych, zawierających między innymi Centrum Kontaktu, Centrum Zarządzania Siecią oraz Centrum Zarządzania Bezpieczeństwem;
Centralny Węzeł Bezpieczeństwa	Węzeł Bezpieczeństwa zlokalizowany w Węźle Centralnym, zapewniający ochronę Zasobów obliczeniowych OSE
IdP (Identity Provider)	system służący do tworzenia, utrzymywania i udostępniania tożsamości dla celów uwierzytelniania i autoryzacji dla zewnętrznych podmiotów.
Infrastruktura bezpieczeństwa	
LDAP (Lightweight Directory Access Protocol)	protokół przeznaczony do korzystania z usług katalogowych. Jest to również nazwa własna usługi katalogowej przechowującej informacje o użytkownikach i ich atrybutach.
System NG Firewall(NGFW – Next Generation Firewall)	System kontrolujący dostęp do sieci w oparciu o polityki, klasyfikujące ruch bazujący na informacjach pozyskanych z protokołów działających w 4 i 7 warstwie OSI, z wykorzystaniem mechanizmów statefull packet inspection, intrusion prevention system, application control, antivirus.
Portal OSE	portal umożliwiający obsługę usług w sieci OSE, w tym zgłaszanie problemów technicznych, zmian w zakresie świadczonych usług, kreowanie i modyfikowanie kont Użytkowników Sieci OSE oraz ich parametrów
Radius	Remote Authentication Dial In User Service – usługa zdalnego uwierzytelniania użytkowników, używana głównie z systemami telekomunikacyjnymi. Zdefiniowana w następujących RFC: RFC 2865, RFC2866, RFC3579
Regionalny Węzeł Bezpieczeństwa	węzeł Bezpieczeństwa zlokalizowany w Węźle Regionalnym i obsługujący Szkoły podłączone do danego Węzła Regionalnego.
SAML (Język Security Assertion Markup Language)	protokół służący do wymiany danych uwierzytelniania i autoryzacji w domenach zabezpieczeń. W modelu domeny SAML dostawca tożsamości jest specjalnym typem urzędu uwierzytelniania. Dostawca tożsamości SAML jest jednostką systemową, która wydaje zapewnienie uwierzytelniania w połączeniu z profilem SSO SAML. Strona ufająca, która zużywa te zapewnienie uwierzytelniania, jest nazywana dostawcą usług SAML.
Ustawa OSE	ustawa z dnia 27 października 2017 r. o Ogólnopolskiej Sieci Edukacyjnej
Użytkownicy Sieci OSE	użytkownicy usług Sieci OSE w tym m.in. : uczniowie, nauczyciele, pracownicy administracyjni oraz inni upoważnieni przez administratora danych usług Sieci OSE
Zasoby obliczeniowe OSE	infrastruktura serwerowa udostępniona w celu zapewnienia mocy obliczeniowej t.j. procesory, pamięć RAM, przestrzeń dyskowa wybudowana na potrzeby systemów i usług

Definicja	Wyjaśnienie
	OSE. Zasoby są umieszczone w dwóch węzłach centralnych OSE w lokalizacjach: Warszawa i Poznań.
PWR (Punkt Wymiany Ruchu)	Punkt Wymiany Ruchu internetowego (IX - z ang. Internet eXchange Point) to miejsce, gdzie operatorzy, przedsiębiorcy telekomunikacyjni (w rozumieniu Ustawy Prawo Telekomunikacyjne) i dostawcy treści i usług internetowych wymieniają się ruchem IP pomiędzy swoimi sieciami.
PPWR (Powiatowy Punkt Wymiany Ruchu)	Regionalny PWR pośredniczący w ruchu pomiędzy węzłem abonenckim a PWR-em w sieciach ODN.
MAN	Sieć miejska - operatorzy sieci regionalnych w rejonach miejskich
ODN	Ośrodek Doskonalenia Nauczycieli - jeden z Operatorów Sieci Regionalnych obsługujących szkoły.
RADIUS	Remote Authentication Dial In User Service – usługa zdalnego uwierzytelniania użytkowników, używana głównie z systemami telekomunikacyjnymi. Zdefiniowana w następujących RFC: RFC 2865, RFC2866, RFC3579
SNMP	<p>Rodzina protokołów sieciowych wykorzystywanych do zarządzania urządzeniami sieciowymi i serwerami za pośrednictwem sieci IP.</p> <p>Do transmisji wiadomości SNMP wykorzystywany jest głównie protokół UDP: standardowo port 161 wykorzystywany jest do wysyłania i odbierania żądań, natomiast port 162 wykorzystywany jest do przechwytywania sygnałów <i>trap</i> od urządzeń.</p> <p>Protokół znany jest i wykorzystywany w następujących wersjach</p> <p>SNMPv1 – pierwsza wersja, która została opublikowana w 1988 roku w dokumencie RFC 1067 (z późniejszymi zmianami w RFC 1098 oraz RFC 1157. W tej wersji protokołu bezpieczeństwo oparte jest na tak zwanych <i>communities</i>, które są pewnego rodzaju nieszyfrowanymi hasłami umożliwiającymi zarządzanie urządzeniem.</p> <p>SNMPv2 – eksperymentalna wersja protokołu, określana także SNMPv2c, opisana w dokumencie RFC 1901</p> <p>SNMPv3 – obsługująca uwierzytelnianie oraz szyfrowaną komunikację wykorzystującą szyfrowanie SHA i MD5</p>
SSH	<p>Standard protokołów szyfrowania komunikacji typu klient-serwer, a także serwer-klient</p> <p>Protokoły z rodziny SSH korzystają zwykle z portu 22 protokołu TCP.</p> <p>Protokół SSH jest zaimplementowany na warstwie aplikacji modelu OSI w ramach połączenia TCP. Protokół SSH jest opisany szczegółowo w RFC 4251 i 4254.</p>
SYSLOG	<p>Program, który umożliwia rejestrowanie zachodzących zdarzeń przy pomocy scentralizowanego mechanizmu logowania. Działa on na porcie 514 udp / tcp.</p> <p>Cały mechanizm jest opisany w następujących RFC 5424 i 3164</p>
VRF	Technologia pozwalająca koegzystować wielu instancjom tablic routingu na tym samym routerze w tym samym czasie.

Definicja	Wyjaśnienie
	Głównym aspektem tej funkcjonalności jest separacja wirtualnych tablic routingu wobec siebie bez potrzeby zastosowania wielu ruterów.
VPN	Tunel, przez który płynie ruch w ramach sieci prywatnej pomiędzy klientami końcowymi, za pośrednictwem publicznej sieci (takiej jak Internet) w taki sposób, że węzły tej sieci są przezroczyste dla przesyłanych w ten sposób pakietów. Można opcjonalnie kompresować lub szyfrować przesyłane dane w celu zapewnienia lepszej jakości lub większego poziomu bezpieczeństwa. Określenie "wirtualna" oznacza, że sieć ta istnieje jedynie, jako struktura logiczna działająca w rzeczywistości w ramach sieci publicznej, w odróżnieniu od sieci prywatnej, która powstaje na bazie specjalnie dzierżawionych w tym celu łącz. Pomimo takiego mechanizmu działania stacje końcowe mogą korzystać z VPN dokładnie tak, jak gdyby istniało pomiędzy nimi fizyczne łącze prywatne. Rozwiązania oparte na VPN stosowane są np. w sieciach korporacyjnych firm, których zdalni użytkownicy pracują ze swoich domów na niezabezpieczonych łączach. Wirtualne Sieci Prywatne charakteryzują się dość dużą efektywnością, nawet na słabych łączach (dzięki kompresji danych) oraz wysokim poziomem bezpieczeństwa (ze względu na szyfrowanie).
SMTP	Protokół internetowy wykorzystywany do przekazywania poczty elektronicznej w Internecie. Standard został zdefiniowany w dokumencie RFC 821, a następnie zaktualizowany w 2008 roku w dokumencie RFC 5321.
SIP	SIP współgra z kilkoma innymi protokołami i jest zaangażowany jedynie w część sygnalizacyjną sesji komunikacyjnej. SIP występuje, jako nośnik Session Description Protocol (SDP), który opisuje transportowane multimedia w sieci, np. używane porty IP, używany kodek itp. Pierwsza zaproponowana wersja standardu (SIP 2.0) została zdefiniowana w RFC 2543. Protokół następnie uszczegółowiono w RFC 3261, jakkolwiek wiele implementacji używa wskazówek z tymczasowych wersji próbnych (ang. <i>draft</i>).
SIEM	system tożsamy z funkcjami Log Management (LM) odpowiedzialny za logowanie zdarzeń z urządzeń sieciowych, systemów operacyjnych oraz aplikacji. System LM posiada funkcjonalności takie jak: zbieranie logów, agregację logów, retencję logów oraz przeszukiwanie, raportowanie i tworzenie reguł korelacyjnych
SWG (Security Web Gateway)	System zapewniający funkcje ochrony użytkownika sieci OSE związane z potencjalnym dostępem do treści nielegalnych i szkodliwych w Internecie.

3. Architektura biznesowa Operatora OSE

NASK Państwowy Instytut Badawczy funkcjonując, jako Operator Ogólnopolskiej Sieci Edukacyjnej realizuje te same działania jak każdy inny operator telekomunikacyjny, jednakże w sposób dopasowany do specyfiki OSE. Celem działania operatora jest świadczenie usług dostarczanych na bazie sieci teleinformatycznej. W związku ze świadczeniem usług operator musi realizować wiele funkcjonalności powiązanych z całym cyklem życia produktu od tworzenia jego koncepcji poprzez wdrażanie i dostarczanie klientom, aż po jego wycofanie. Kluczowym elementem działania każdego operatora jest jego katalog produktów określający wartości (produkty), jakie oferuje swoim klientom, sposób ich oferowania i dostarczania, sposób ich realizacji (czy na bazie własnych zasobów, czy też partnerów), sposób rozliczeń się z klientami. Dodatkowo należy pamiętać, że operator telekomunikacyjny jest przedsiębiorcą i w związku z tym realizuje wszelkie działania związane z prowadzeniem przedsiębiorstwa, takie jak finanse, księgowość, gospodarka magazynowa, zarządzanie IT itp. Całość funkcjonowania Operatora OSE oraz jego podział na poszczególne obszary biznesowe można opisać wykorzystując mapę procesów przedsiębiorstwa telekomunikacyjnego zdefiniowanego przez TMForum w ramach eTOM. Poniżej znajduje się diagram mapy biznesowej dla Operatora OSE.

Marketing & Sprzedaż	1. Proces zarządzania produktami OSE	2. Proces obsługi klienta					10. Proces marketingu i komunikacji
Produkty							
Klienci			3. Proces technicznej obsługi			7. Proces zarządzania bezpieczeństwem	
Usługi				4. Proces realizacji usług			
Zasoby					5. Proces utrzymania sieci, usług i systemów		
Partnerzy						6. Proces współpracy z operatorami	
Przedsiębiorstwo						8. Proces rozwoju OSS/BSS	9. Proces wsparcia OSE

Procesy biznesowe

Operator OSE znajduje się w trakcie definiowania procesów biznesowych oraz tworzenia dla nich wsparcia informatycznego. Z uwagi na te uwarunkowania procesy biznesowe można podzielić na trzy kategorie:

1. Procesy wdrożone - procesy biznesowe, jakie już zostały zdefiniowane i dla których zostało wdrożone (lub będzie wdrożone w najbliższym czasie) wsparcie informatyczne w ramach systemów przejściowych. Dla tych procesów konieczne będzie przeprowadzenie analizy biznesowej, aby dostosować je / zoptymalizować przy wdrożeniu docelowej platformy OSS/BSS. Dla tych procesów niezbędne jest zadbanie o zapewnienie ciągłości ich realizacji oraz migracji danych z zakończonych instancji procesów.
2. Procesy zdefiniowane - procesy, jakie obecnie zostały określone i zdefiniowane z mniejszą lub większą szczegółowością, ale nie ma dla nich żadnego wsparcia informatycznego. Ma ono zostać dopiero

zapewnione na docelowych systemach OSS/BSS. Dla tych procesów konieczne będzie przeprowadzenie dogłębnej analizy biznesowej, aby je w pełni zdefiniować i wdrożyć dla nich oczekiwane, efektywne i optymalne wsparcie biznesowe. W ramach analizy tych procesów należy kierować się najlepszymi praktykami branżowymi uwzględniając jednocześnie specyfikę biznesową OSE.

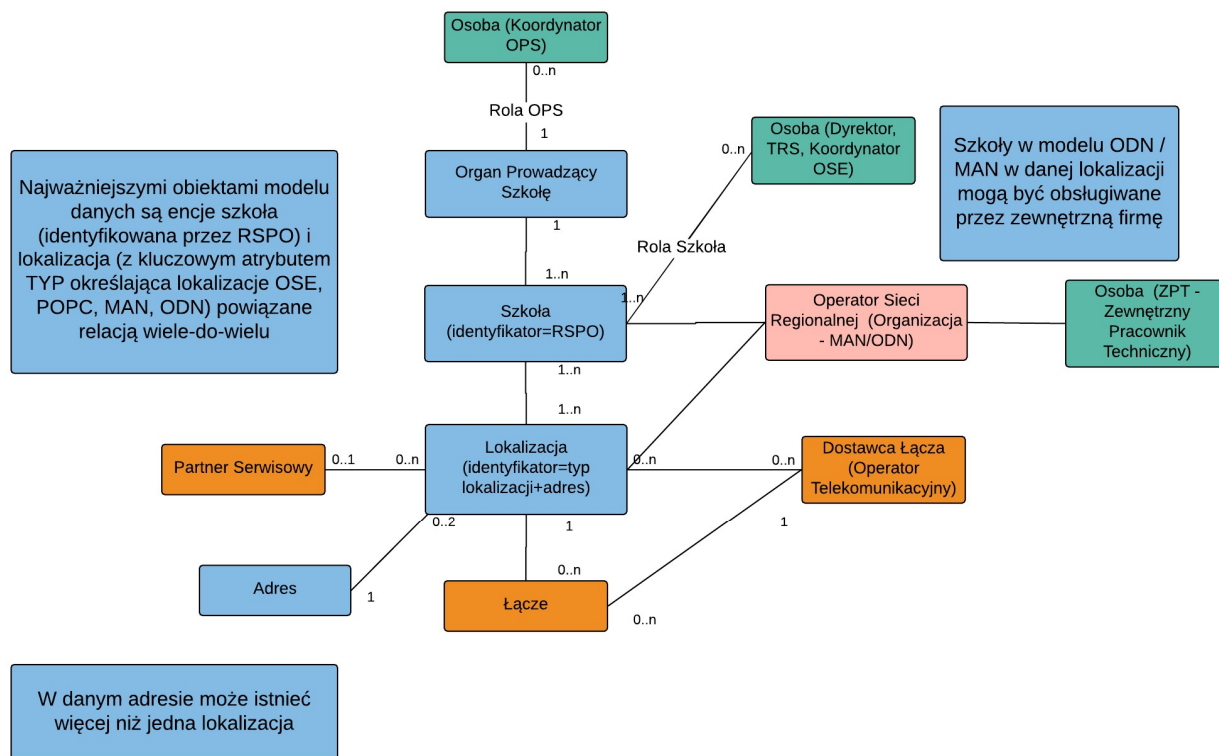
3. Procesy niezdefiniowane - procesy biznesowe, które obecnie nie zostały określone / wytypowane. Zostaną one zidentyfikowane w trakcie realizacji wdrożenia OSS/BSS przez zespół operatora OSE lub zespół odpowiedzialny za realizację wdrożenia. Dla tych procesów konieczne będzie przeprowadzenie pełnej analizy biznesowej i zaprojektowania ich w oparciu o najlepsze praktyki branżowe uwzględniając jednocześnie specyfikę biznesową OSE.

Konfiguracja biznesowa

W ramach opisu architektury biznesowej znajdują się informacje dotyczące konfiguracji (i modeli danych) wykorzystywanej w procesach biznesowych, takich jak np. konfiguracja katalogu produktów, SLA zgłoszeń, procesów obsługowych czy reklamacyjnych. Należy założyć, iż podane w dokumencie konfiguracje są przykładowe i ich celem jest jedynie przekazanie zakresu wymaganych danych, struktury biznesowego modelu danych oraz skali i złożoności zagadnienia. Konieczne będzie przeprowadzenie prac analitycznych celem opracowania i wdrożenia poprawnej konfiguracji dla docelowej platformy OSS/BSS.

3.1. Architektura danych operatora OSE

W ramach kompleksowej realizacji zadań / procesów związanych z zapewnieniem bezpiecznego dostępu do internetu konieczne jest operowanie na dużej ilości różnorodnych danych. Poniżej znajduje się diagram ogólnego modelu danych w obszarze BSS.



Procesy realizowane w obszarze BSS koncentrują się wokół dwóch podstawowych obiektów:

- Szkoły - placówki edukacyjnej, będącej klientem Operatora OSE

- Lokalizacji - czyli miejsca świadczenia usług

Pomiędzy szkołą a lokalizacją zachodzi relacja wiele-do-wielu - wiele szkół może być w jednej lokalizacji, ale również jedna szkoła może występować w wielu lokalizacjach.

Osoby

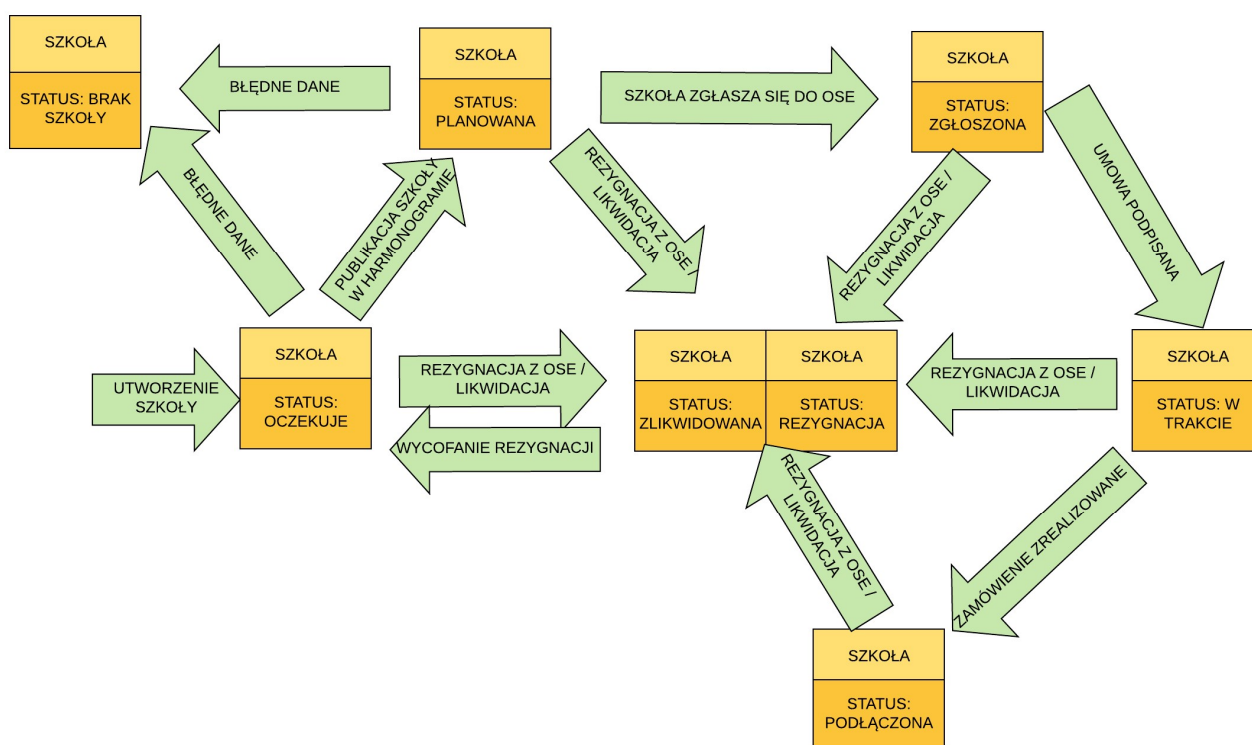
Za zapewnienie dostępu do internetu dla szkoły odpowiedzialny jest Organ Prowadzący Szkołę, osobą go reprezentującą w procesach biznesowych jest Koordynator OPS.

Szkołę w kontaktach z OSE reprezentuje Dyrektor i jest on użytkownikiem odpowiedzialnym za administrację pozostałymi użytkownikami OSE w szkole. W procesach biznesowych występują w roli użytkowników jeszcze Techniczny Reprezentant Szkoły (TRS) oraz Koordynator OSE. Dyrektor jest odpowiedzialny za zarządzanie bazą użytkowników dla swojej szkoły. Należy zwrócić uwagę, że poszczególne osoby mogą być użytkownikami w wielu szkołach. Np. dana osoba może być TRS-em w więcej niż jednej szkole.

Szkoła

Wszystkie główne procesy operatora OSE realizowane są w kontekście szkoły. Zanim możliwe będzie pozyskanie szkoły musi zostać wstępnie przygotowana infrastruktura telekomunikacyjna, dopiero szkoła w ramach harmonogramu może uzyskać możliwość zgłoszenia się do OSE.

Cykl życia szkoły



Po zgłoszeniu szkoły do OSE Dyrektor jest odpowiedzialny za zarządzanie użytkownikami, tworzenie odpowiednich kont dla użytkowników, którzy będą mieli uprawnienia do zarządzania usługami OSE i zgłaszaniem ewentualnych problemów. Szkoła jest nadzorowana przez Organ Prowadzący Szkołę w ramach, którego jest wyznaczona osoba w roli Koordynatora OPS.

W przypadku szkół w lokalizacjach obsługiwanych przez Operatora Sieci Regionalnej (MAN / ODN) użytkownicy szkolni nie mogą zgłaszać problemów technicznych bezpośrednio do operatora OSE,

problemy muszą być zgłaszane do Operatorów Sieci Regionalnych i dopiero ich pracownicy po weryfikacji mogą zgłaszać ewentualne problemy do Operatora OSE.

Lokalizacja

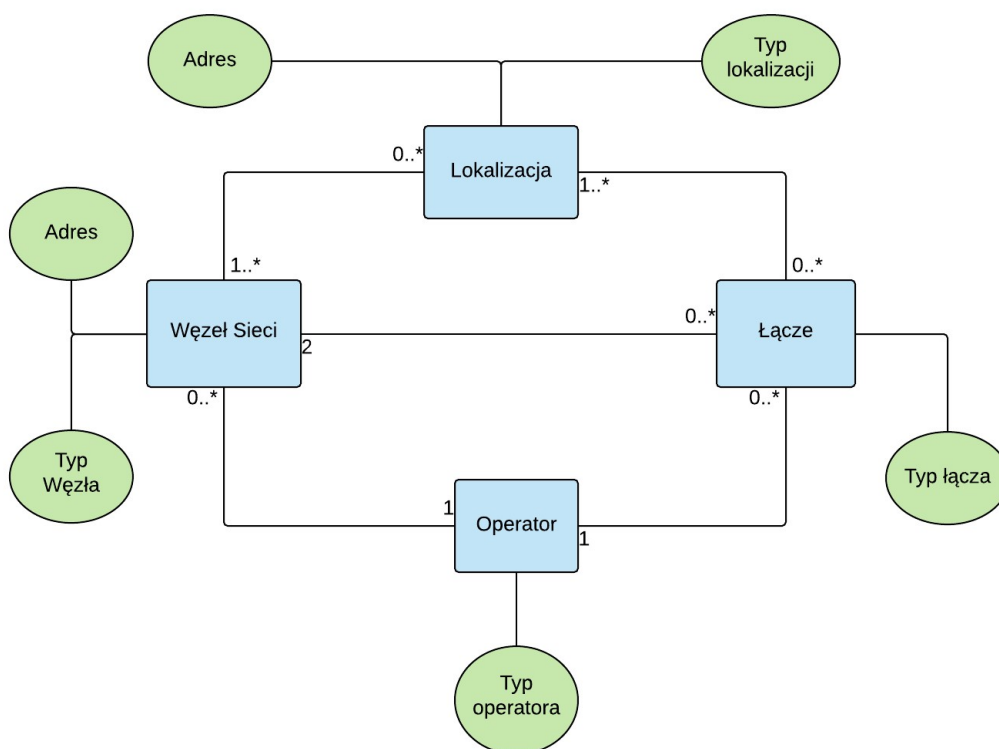
Główną encją danych, wokół której koncentrują się działania związane z usługami OSE jest lokalizacja, grupująca wszystkie szkoły znajdujące się pod jednym adresem i podłączane w tym samym modelu świadczenia usług (OSE / POPC / MAN / ODN).

Dla każdej lokalizacji jest określony Partner Serwisowy odpowiedzialny za realizację prac w szkołach. W przypadku szkół ODN / MAN jego rolę może pełnić NASK lub Operator Sieci Regionalnej (OSR).

Dla każdej lokalizacji jest z góry określony przebieg łącza sieci dostępowej, czyli wskazani operatorzy odpowiedzialni za łącza pomiędzy poszczególnymi punktami wraz ze wskazaniem odpowiedzialnego za łącze (OSE / OSR).

Łącza dostępne

Kolejnym istotnym elementem modelu danych jest obszar łączy dostępowych, czyli infrastruktury sieciowej służącej do połączenia węzła abonenckiego w szkole z węzłem agregacyjnym sieci szkieletowej.



W przeciwieństwie do tradycyjnego modelu operatora telekomunikacyjnego gdzie przebieg jest wyznaczany w momencie podłączenia (lub wywiadu technicznego), w przypadku OSE zanim szkoła będzie miała możliwość zgłoszenia się do OSE przebieg łącz dla lokalizacji zostaje wcześniej ustalony, czyli z góry wiadomo, jaki operator dostarczy, jakie łącza, które będą przechodzić przez jasno określone węzły sieci.

3.2. Katalog produktów Ogólnopolskiej Sieci Edukacyjnej

Założenia

1. Katalog produktów Operatora OSE jest samodzielnym bytem w żaden sposób niepowiązany z innymi katalogami, jakie istnieją bądź będą istnieć w ramach NASK PIB.
2. Wsparcie dla zarządzania katalogiem produktów realizowane jest w ramach systemów Platformy Operatora OSE.
3. W ramach OSE, jeżeli jest wymagany dodatkowy produkt, to klient zawsze musi samodzielnie wyrazić chęć włączenia / nabycia produktu. Nie będzie żadnych produktów dodatkowych, które zostaną dodane do zamówienia na etapie realizacji w sposób automatyczny.

Produkty OSE

Nazwa	Opis produktu	Model rozliczeniowy	Ograniczenia techniczne	Ograniczenia biznesowe	Produkty składowe	Produkty Wymagane	Instalacja Aktywacja
Produkty główne							
Internet OSE	Dostęp do Internetu poprzez sieć szkieletową OSE o prędkości synchronicznej 100Mb/s na bazie komercyjnie istniejących łączy operatorów	Abonament, instalacja, cena rozdzielną dla regionów	Dostępność łącza w lokalizacji Dostępność partnera serwisowego w lokalizacji	Minimalny czas pomiędzy rezygnacją a ponownym podłączeniem (konfiguracja)	Urządzenie CPE (tylko dla jednej szkoły w lokalizacji), ·Urządzenie AP, ·Urządzenie SW		Instalacja łącza (operator) ·Instalacja punktu dostępowego (partner serwisowy) ·Instalacja VLAN
Internet OSE POPC	Dostęp do Internetu poprzez sieć szkieletową OSE o prędkości synchronicznej 100Mb/s na bazie łączy budowanych w ramach POPC				Urządzenie AP, Urządzenie SW		Instalacja łącza (operator) ·Instalacja punktu dostępowego (operator) ·Rozbudowa punktu dostępowego (partner serwisowy) ·Instalacja VLAN
Internet OSE MAN	Dostęp do Internetu poprzez sieć szkieletową OSE o prędkości synchronicznej 100Mb/s na dostępie zapewnianego przez OPS przy wykorzystaniu sieci miejskich (MAN)		Dostępność łącza w lokalizacji		Urządzenie CPE (opcjonalnie dla jednej szkoły w lokalizacji)		Instalacja punktu dostępowego (szkoła) (opcja) ·Instalacja VLAN (opcja)
Internet OSE ODN	Dostęp do Internetu poprzez sieć szkieletową OSE o prędkości synchronicznej 100Mb/s na bazie łączy znajdujących się w ODN przy wykorzystaniu też łączy komercyjnych operatorów		Dostępność łącza w lokalizacji, dostępność ODN w lokalizacji Dostępność partnera serwisowego w lokalizacji				Instalacja punktu dostępowego (szkoła) (opcja) ·Instalacja VLAN (opcja)

Nazwa	Opis produktu	Model rozliczeniowy	Ograniczenia techniczne	Ograniczenia biznesowe	Produkty składowe	Produkty Wymagane	Instalacja Aktywacja
Podwyższona Prędkość	Zwiększenie prędkości internetu powyżej 100Mb/s w paczkach po 50Mb/s (n paczek). Produkt płatny na podstawie wyceny od dostawcy łącza.	Abonament, instalacja, cena rozdzielna dla regionów	Do maksymalnej przepustowości łącza	Maksymalnie liczba miesięcznych aktywacji		Internet OSE lub Internet OSE POPC lub Internet OSE MAN lub Internet OSE ODN	Dostosowanie przepustowości łącza
Ochrona przed szkodliwym oprogramowaniem	Zaawansowana ochrona sieci szkolnej przed włamaniami i złośliwym oprogramowaniem. Uwaga: Produkt wymaga zgody na inspekcję ruchu szyfrowanego SSL.	Abonament, instalacja		Maksymalnie liczba miesięcznych aktywacji	System zapobiegania włamań (IPS), ·Antywirus (AV), ·Certyfikat SSL	[Internet OSE lub Internet OSE POPC lub Internet OSE MAN lub Internet OSE ODN] i CPE OSE	Instalacja certyfikatu SSL Instalacja oprogramowania IPS Instalacja oprogramowania AV
Ochrona użytkownika OSE	Zaawansowana ochrona użytkowników szkolnych na kilku poziomach bezpieczeństwa poprzez filtrowanie treści. Uwaga: Produkt wymaga zgody na inspekcję ruchu szyfrowanego SSL	Abonament, instalacja		Maksymalnie liczba miesięcznych aktywacji	Certyfikat SSL	[Internet OSE lub Internet OSE POPC lub Internet OSE MAN lub Internet OSE ODN] i Ochrona przed szkodliwym oprogramowaniem	Ustawienie poziomu filtracji
Wsparcie Techniczne Szkoły	Wsparcie techniczne dla szkoły w rozwiązywaniu problemów IT niepowiązanych z OSE. Produkt o ograniczonej dostępności – indywidualnie negocjowany.	Użycie		Maksymalna liczba użyć miesięcznie / rocznie (konfiguracja)		Internet OSE lub Internet OSE POPC	Wizyta partnera serwisowego we wskazanym terminie
Rekonfiguracja Sieci Szkolnej	Dostosowanie istniejącej sieci szkolnej do dostępu do internetu w ramach OSE	Użycie		Dostępna opcjonalnie dla instalacji w lokalizacjach OSE i POPC. Niedostępne w lokalizacjach MAN		Internet OSE lub Internet OSE POPC	Wizyta partnera serwisowego we wskazanym terminie
Monitorowanie zachowań	Monitorowanie zachowań i wykrywanie potencjalnych zagrożeń wynikających z zachowań odbiegających od prawidłowego profilu a także w wyniku porównania zachowań z profilem potencjalnych zagrożeń	Abonament		Maksymalnie liczba miesięcznych aktywacji			Instalacja certyfikatu SSL

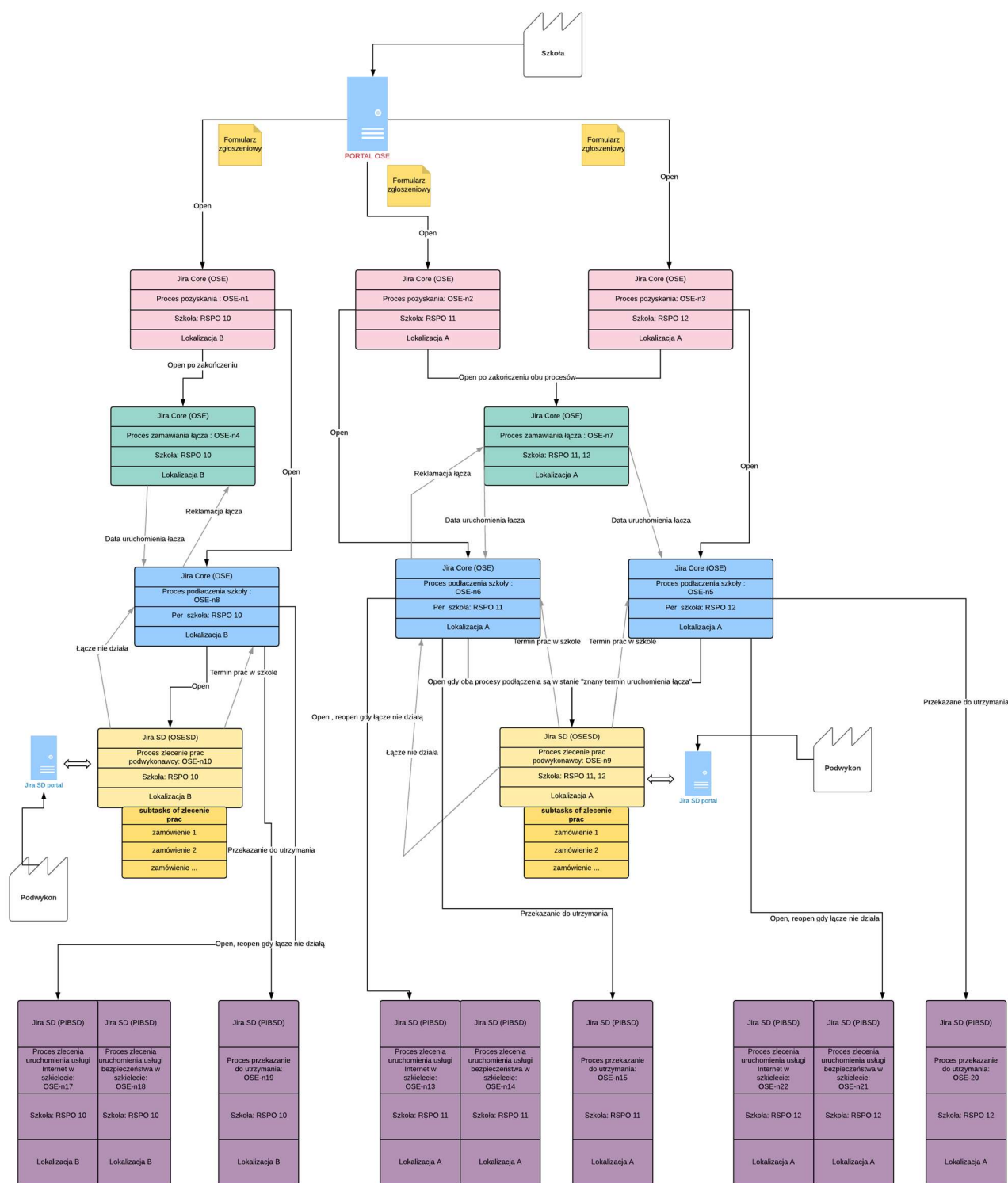
Nazwa	Opis produktu	Model rozliczeniowy	Ograniczenia techniczne	Ograniczenia biznesowe	Produkty składowe	Produkty Wymagane	Instalacja Aktywacja
Bezpieczeństwo użytkownika mobilnego	Aplikacja oferująca funkcjonalność filtrowania treści na urządzeniu końcowym ucznia.	Abonament	Dostępność aplikacji na platformie mobilnej klienta	Maksymalnie liczba miesięcznych aktywacji	Certyfikat SSL	Internet OSE lub Internet OSE POPC lub Internet OSE MAN	Instalacja certyfikatu SSL Pobranie i instalacja oprogramowania Aktywacja konta
Produkty składowe							
Urządzenie CPE	Zakończenie sieci telekomunikacyjnej znajdujące się u klienta.						
Urządzenie AP	Urządzenie dostępne (wyposażone w moduł WIFI)						
Urządzenie SW	Przełącznik sieciowy						
Rekonfiguracja Sieci Szkolnej	Dostosowanie istniejącej sieci szkolnej do dostępu do internetu w ramach OSE						
System zapobiegania włamaniom (IPS)	System zapobiegający włamaniom do sieci komputerowej						
Antywirus (AV)	Ochrona przed złośliwym oprogramowaniem						
Certyfikat SSL	Certyfikat SSL						

Oferty w ramach Ogólnopolskiej Sieci Edukacyjnej

W poszczególnych kanałach dostępowych powinny się pokazywać jedynie oferty dostępne dla wybranego klienta (zawierające produkty dostępne w związku z konkretną lokalizacją klienta), co oznacza konieczność wcześniejszej identyfikacji klienta. Głównym czynnikiem determinującym dostępność ofert jest lokalizacja, na podstawie, której wiadomo, jaki operator będzie świadczyć dostęp do internetu oraz w jakim modelu OSE/ POPC / MAN./ ODN (Dla części lokalizacji może nie być dostępnego żadnego operatora, ale powinna być znana data dostępności produktów).

3.3. Główne procesy operatora OSE

Jednym z głównych zadań, jakie są postawione przed operatorem OSE jest realizacja połączeń a następnie obsługa poszczególnych szkół skupionych w lokalizacjach. Całość procesów związanych z połączeniem szkoły (oraz modyfikacją usługi dostępu) jest zdekomponowana na procesy, które są realizowane wokół różnych encji: szkół, lokalizacji, partnerów serwisowych. Powoduje to konieczność zapewnienia odpowiedniej orkiestracji przebiegu zamówień. Poniżej została zaprezentowana poglądowa mapa przebiegu procesów i ich wzajemnej synchronizacji.

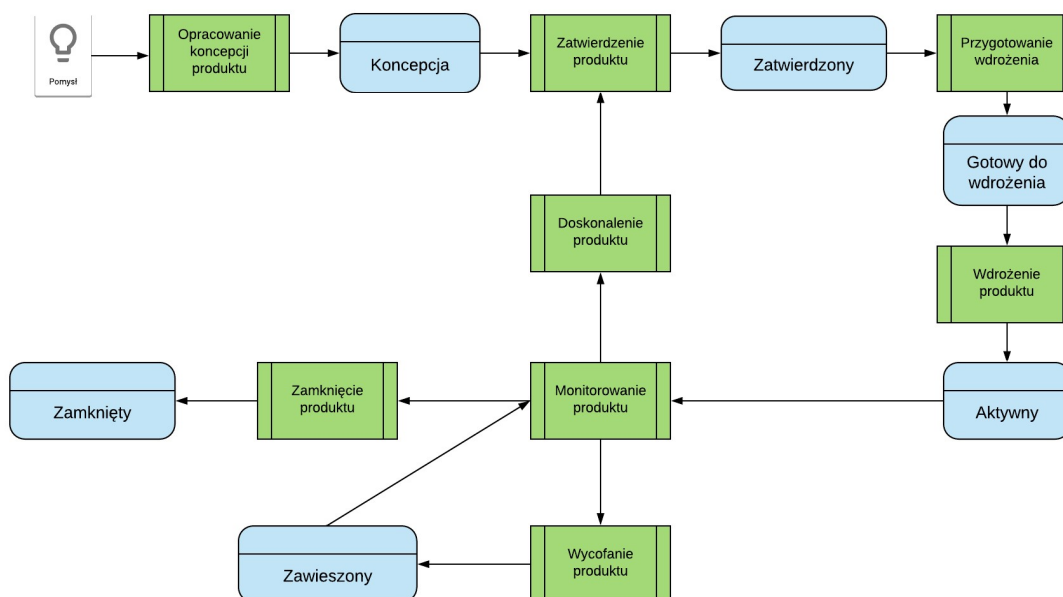
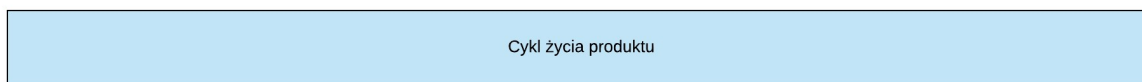
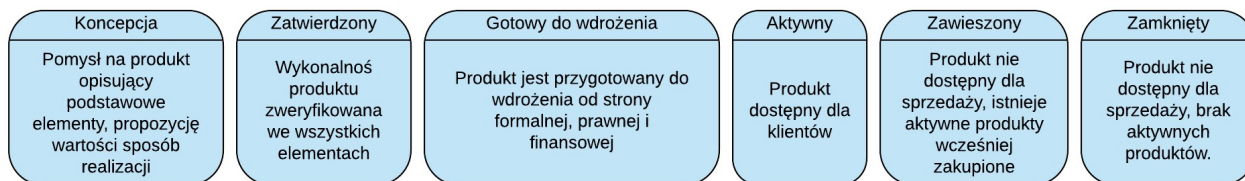


Powyżej wskazane procesy zostaną szczegółowo zaprezentowane w ramach opisu poszczególnych obszarów biznesowych.

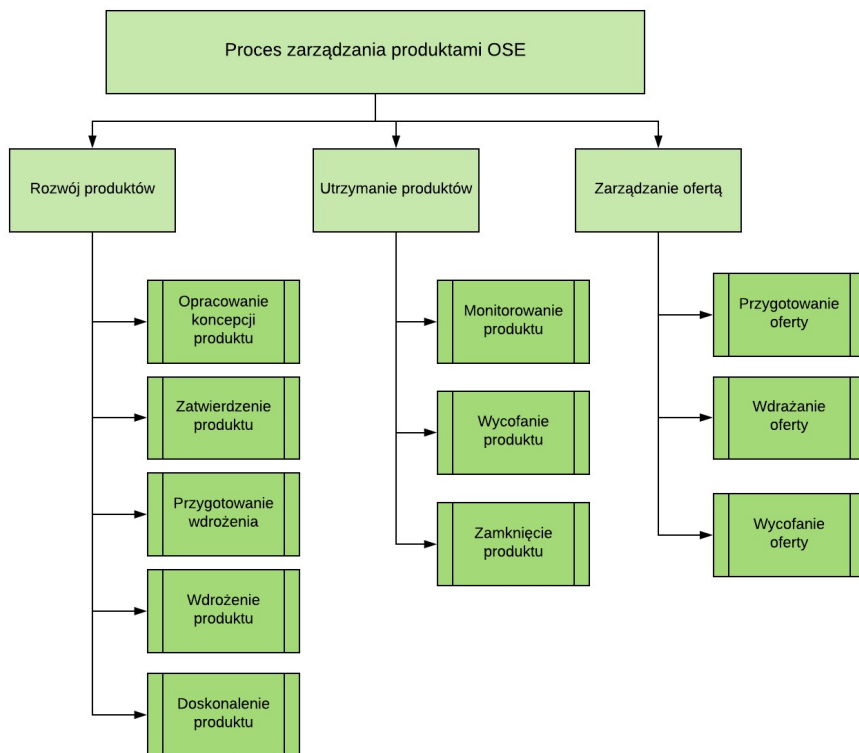
3.4. Proces zarządzania produktami OSE

Obszar adresuje zagadnienia związane z zarządzaniem katalogiem produkt i ofert.

Cykl życia produktu



Hierarchia procesów biznesowych

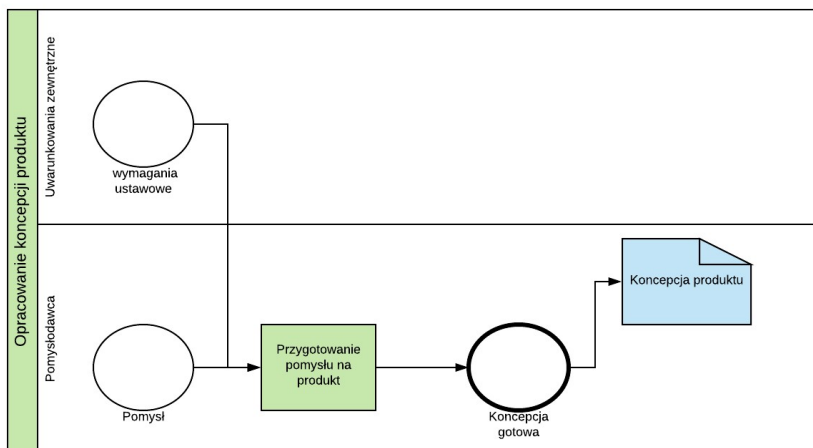


Procesy biznesowe

Opracowanie koncepcji produktu (proces zdefiniowany)

Cel procesu	Przygotowanie pomysłu na nowy produkt
Inicjacja	
Dane wejściowe	Pomysły, wymagania (np. ustawowe)
Dane wyjściowe	Koncepcja produktu
KPI	

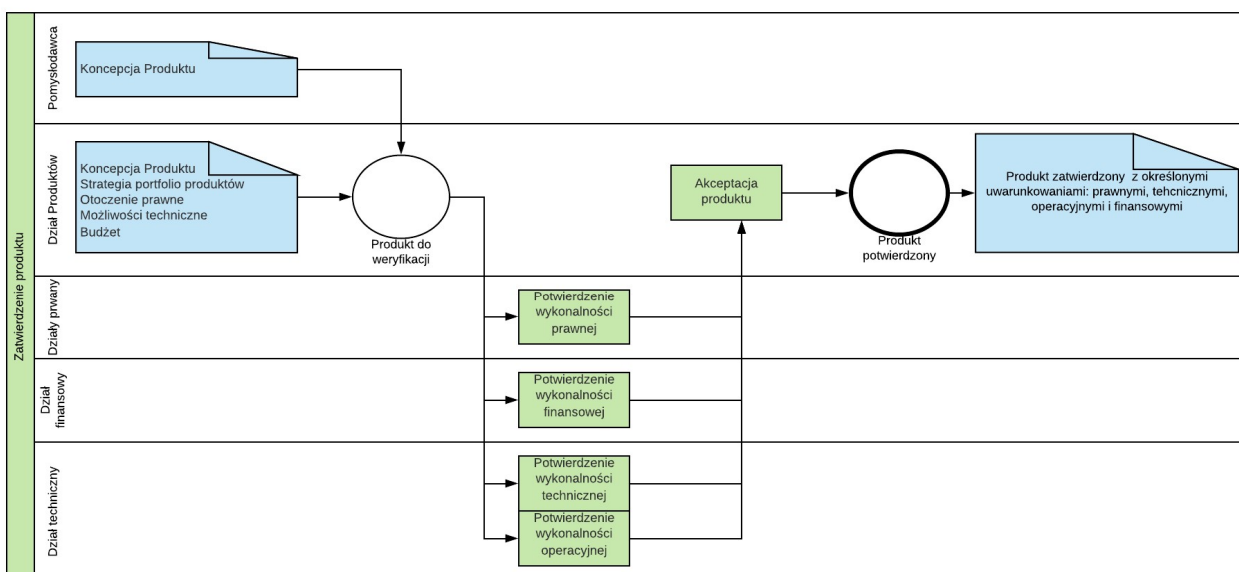
Diagram procesu



Zatwierdzenie produktu (proces zdefiniowany)

Cel procesu	Potwierdzenie możliwości realizacji produktu (studium wykonalności)
Inicjacja	Zatwierdzona koncepcja produktu
Dane wejściowe	Koncepcja Produktu Strategia portfolio produktów Otoczenie prawne Możliwości techniczne Budżet
Dane wyjściowe	Definicja produktu (m.in. funkcjonalność, kryteria jakości) wraz z określonymi uwarunkowaniami
KPI	

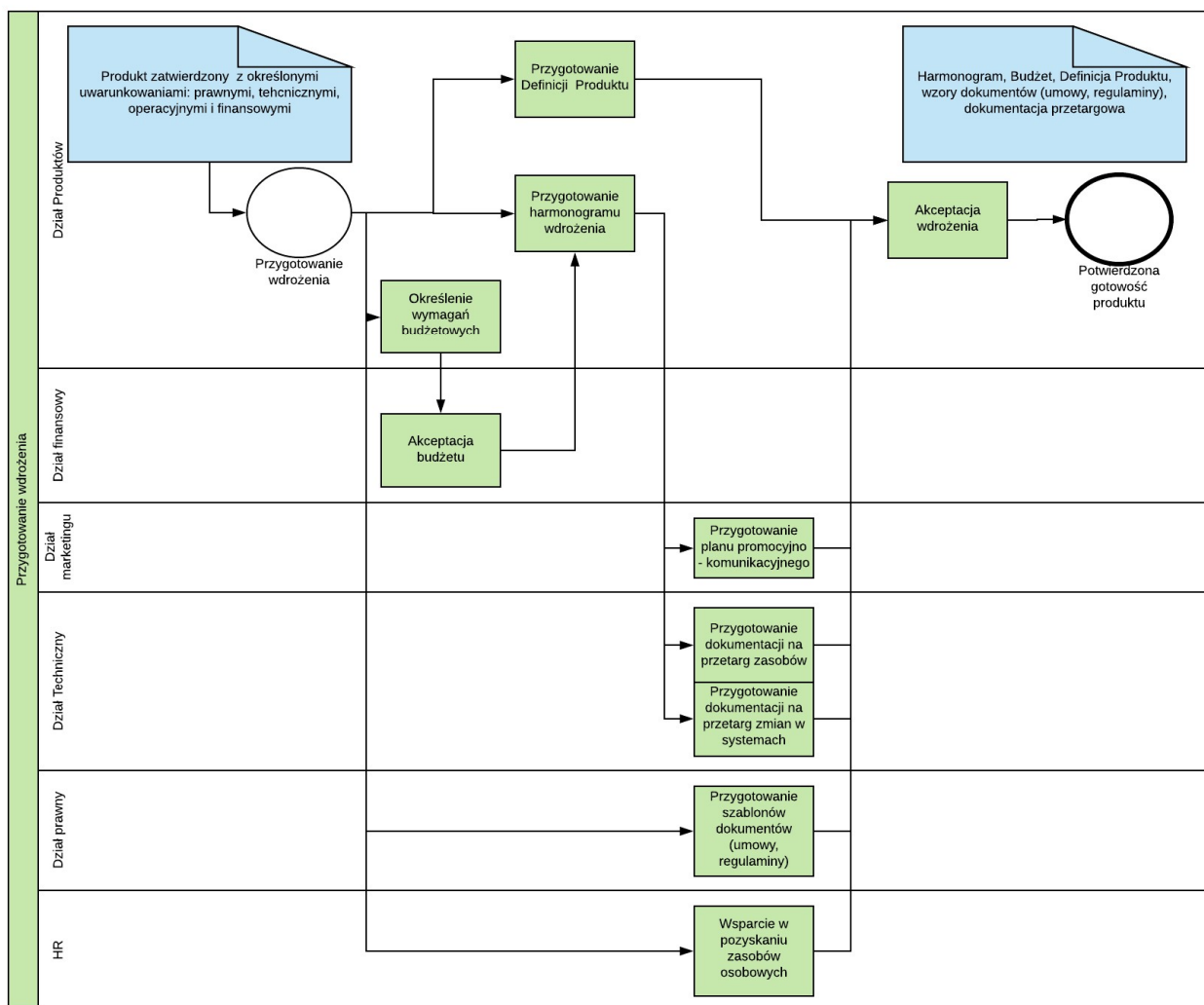
Diagram procesu



Przygotowanie wdrożenia (proces zdefiniowany)

Cel procesu	Przygotowanie nowego produktu do produkcyjnego wykorzystania
Inicjacja	
Dane wejściowe	Definicja produktu Wymagania prawne Wymagania zmian w systemach Wymagania techniczne Wymagania zasobowe
Dane wyjściowe	Gotowe dokumenty Umowne Harmonogram wdrożenia nowego produktu Zaakceptowany budżet Plan promocyjno-komunikacyjny Przygotowana dokumentacja do przetargów
KPI	

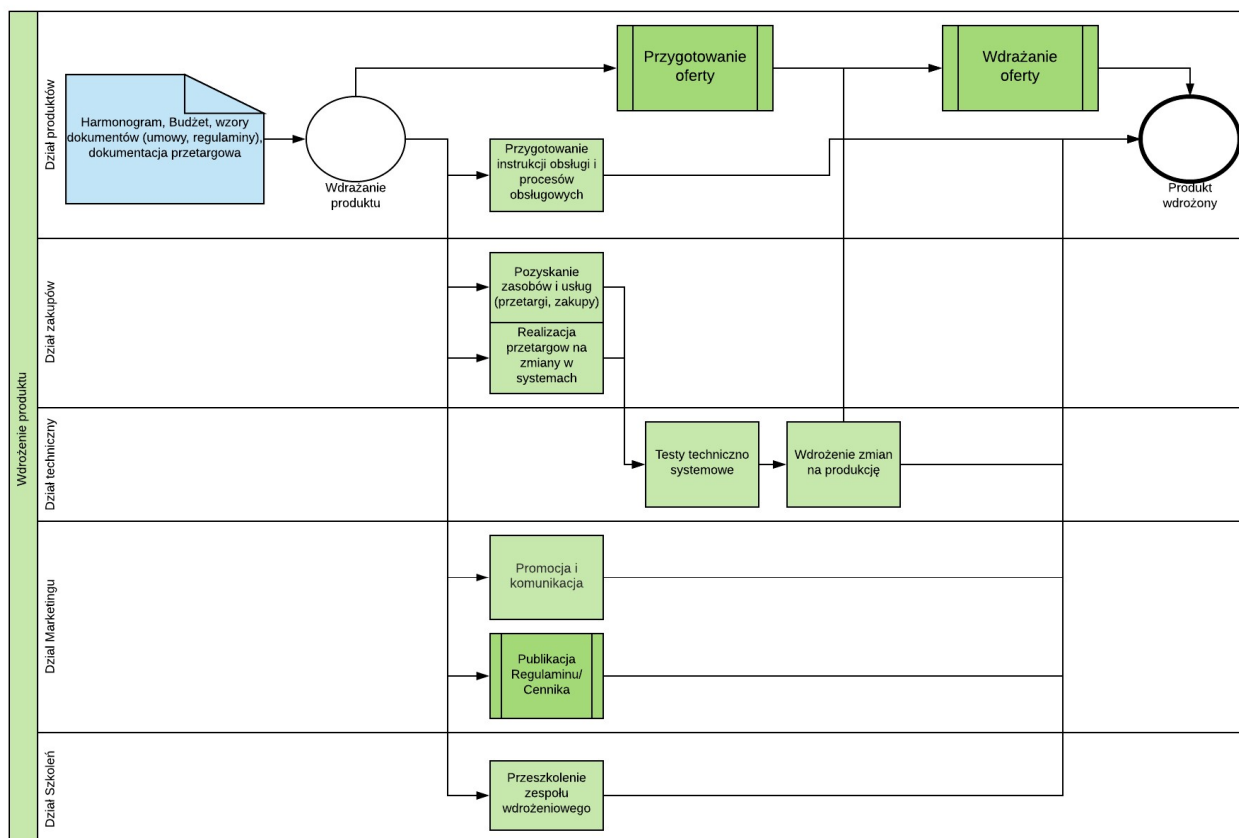
Diagram procesu



Wdrożenie produktu (proces zdefiniowany)

Cel procesu	Wdrożenie produktu do produkcyjnego wykorzystania
Inicjacja	
Dane wejściowe	<p>Gotowe dokumenty Umowne</p> <p>Harmonogram wdrożenia nowego produktu</p> <p>Zaakceptowany budżet</p> <p>Plan promocyjno-komunikacyjny</p> <p>Przygotowana dokumentacja do przetargów</p>
Dane wyjściowe	Wdrożony produkt
KPI	

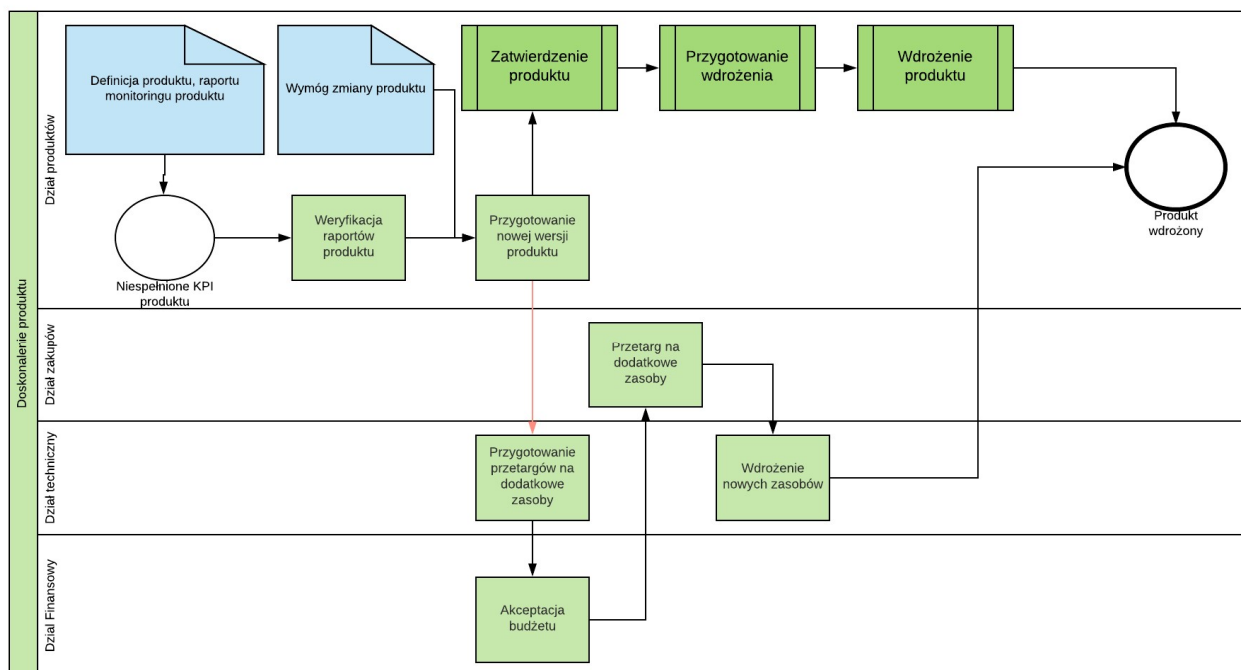
Diagram procesu



Dokształcanie produktu (proces zdefiniowany)

Cel procesu	Ulepszanie produktu, dostosowanie do wymagań prawnych
Inicjacja	Pomysł na rozwój produktu Zmian wymogów prawnych Niespełnione KPI produktu
Dane wejściowe	Definicja produktu Raporty dla produktu
Dane wyjściowe	Produkt wdrożony
KPI	

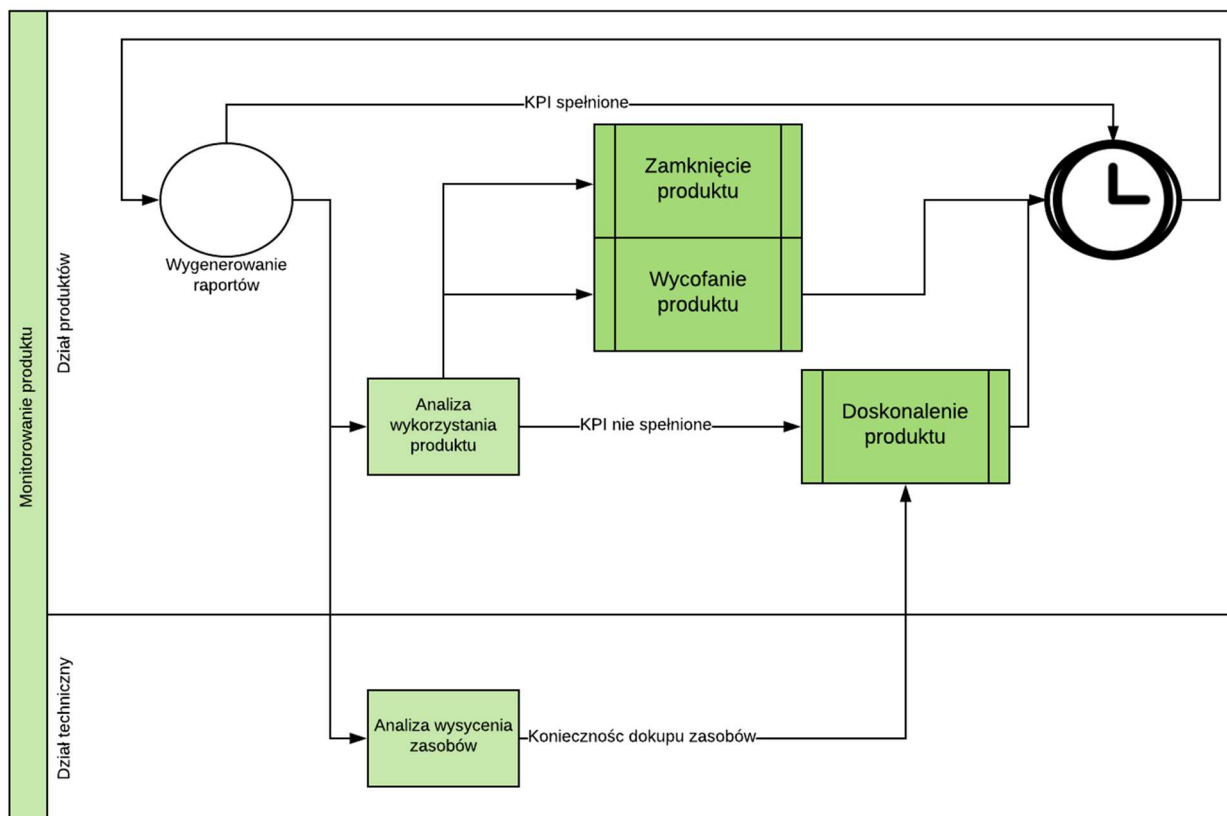
Diagram procesu



Monitorowanie produktu (proces zdefiniowany)

Cel procesu	Weryfikacja wykorzystania produktu oraz stopnia wykorzystania zasobów niezbędnych do działania produktu
Inicjacja	Wdrożony produkcyjnie produkt
Dane wejściowe	Definicja produktu
Dane wyjściowe	Raporty użycia produktu Raporty jakości produktu Raporty satysfakcji Użytkowników
KPI	Liczba produktów/ usług per typ/ wariant Liczba podpisanych umów Liczba Użytkowników % zadowolonych Użytkowników % dotrzymania SLA per usługa Stabilność usług (liczba awarii per m-c)

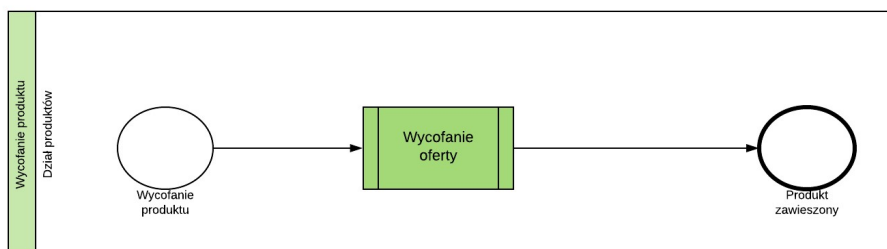
Diagram procesu



Wycofanie produktu (proces zdefiniowany)

Cel procesu	Wycofanie produktu z portfolio
Inicjacja	Doskonalenie produktu, monitorowanie produktu
Dane wejściowe	Definicja produktu
Dane wyjściowe	Zmiana ofert
KPI	

Diagram procesu

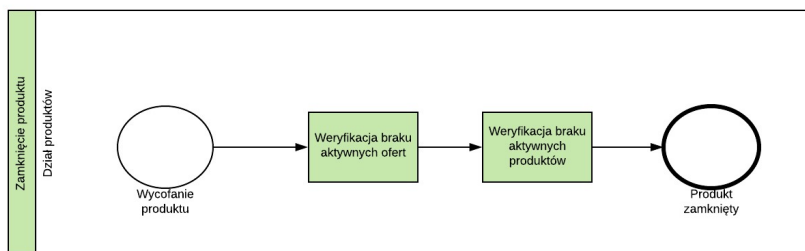


Zamknięcie produktu (proces zdefiniowany)

Cel procesu	Zakończenie obsługi produktu
--------------------	------------------------------

Inicjacja	Monitorowanie produktu
Dane wejściowe	Definicja produktu
Dane wyjściowe	Definicje ofert
KPI	

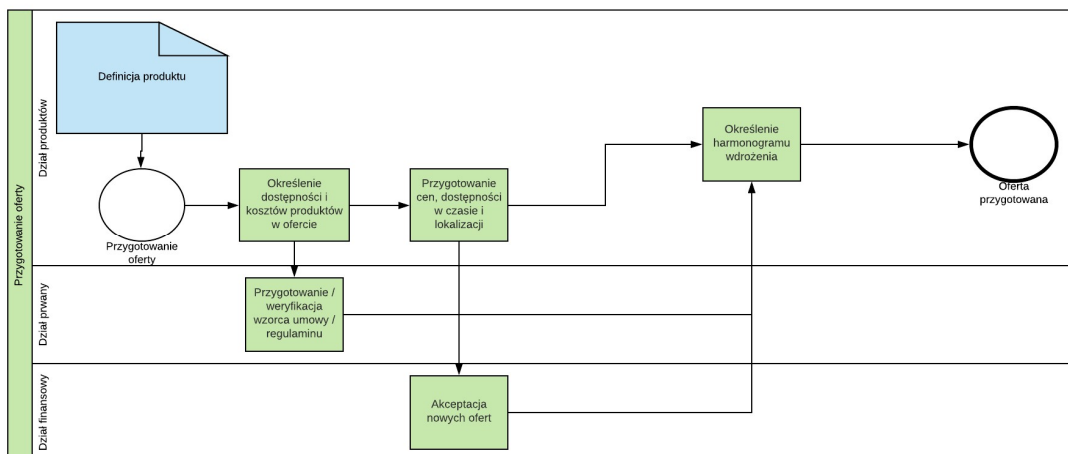
Diagram procesu



Przygotowanie oferty (proces zdefiniowany)

Cel procesu	Przygotowanie nowych warunków ofertowych
Inicjacja	Monitorowanie produktu, przygotowanie produktu do wdrożenia
Dane wejściowe	Definicja produktu
Dane wyjściowe	Katalog ofert
KPI	

Diagram procesu

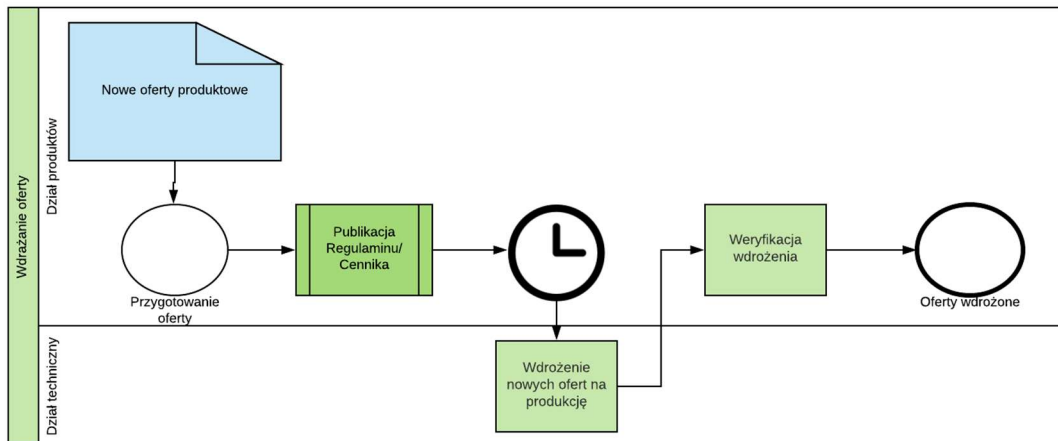


Wdrażanie oferty (proces zdefiniowany)

Cel procesu	Udostępnienie nowych warunków ofertowych dla klientów
Inicjacja	Przygotowane nowe oferty
Dane wejściowe	Definicja produktu, katalog ofert, plan komunikacyjny

Dane wyjściowe	Katalog ofert
KPI	

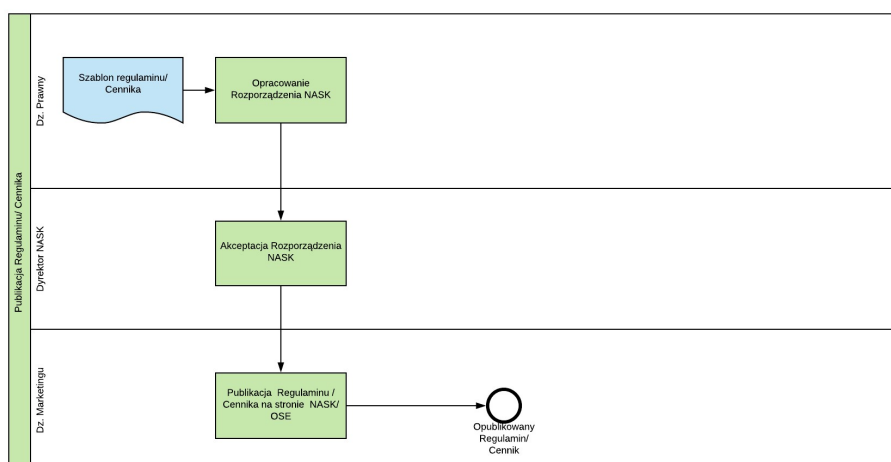
Diagram procesu



Publikacja Regulaminu/ Cennika (proces zdefiniowany)

Cel procesu	Wypełnienie obowiązku operatora telekomunikacyjnego
Inicjacja	Wprowadzenie nowego regulaminu/ cennika Zmiana istniejącego regulaminu/ cennika
Dane wejściowe	Nowy/ zmieniony Regulamin/ Cennik
Dane wyjściowe	Opublikowany Regulamin/ Cennik
KPI	

Diagram procesu

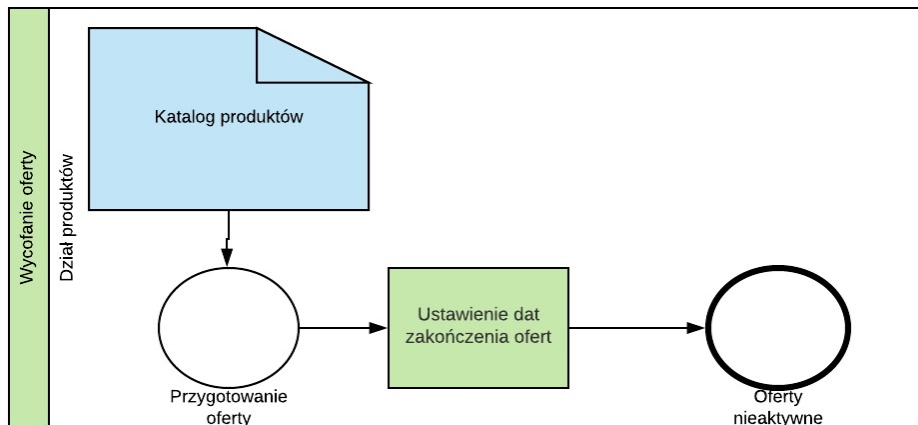


Wycofanie oferty (proces zdefiniowany)

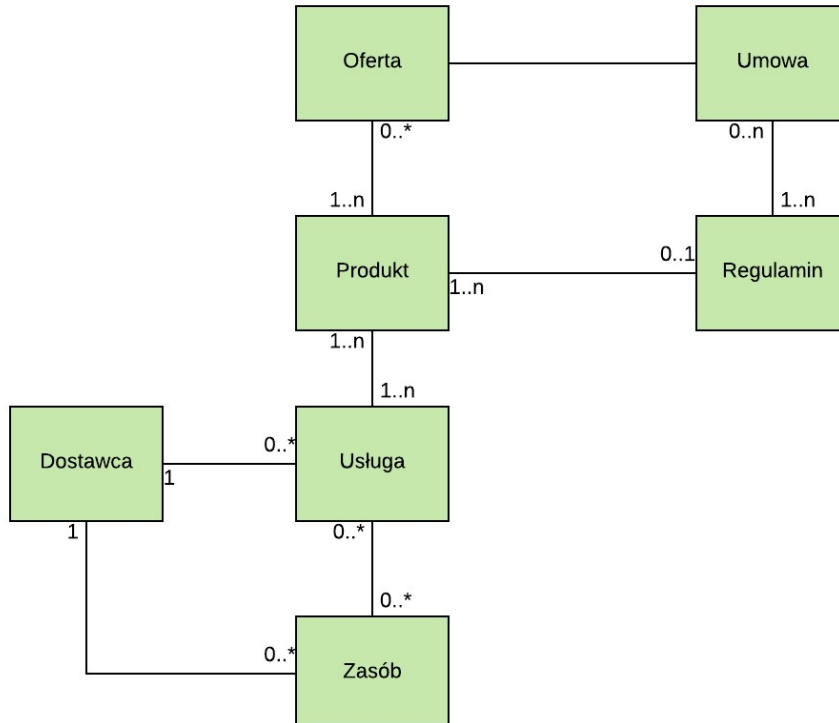
Cel procesu	Wycofanie ofert z dostępności
--------------------	-------------------------------

Inicjacja	Monitorowanie produktu, doskonalenie produktu
Dane wejściowe	Definicja produktu, katalog ofert
Dane wyjściowe	Katalog ofert
KPI	

Diagram procesu



Model danych



Produkt określa wartość oferowaną klientowi i charakteryzuje się następującymi atrybutami:

- Nazwa / Nazwa handlowa
- Opis

- Parametry produktu
- Produkty składowe
- Sposób rozliczania produktu / naliczania opłat za produkt
- Zależności techniczne produktu (jakie inne produkty są wymagane lub się wykluczają)
- Ograniczenia techniczne produktu
- Ograniczenia biznesowe produktu
- Usługi instalacji / deinstalacji
- Powiązanie z regulaminem korzystania z produktu

Oferta określa warunki dostępności produktu i charakteryzuje się następującymi atrybutami:

- Nazwa techniczna / handlowa
- Opis oferty
- Produkty wchodzące w skład oferty (ich wymagalność)
- Okres czasu, w jakim jest dostępna w sprzedaży oferta (może być bezterminowo)
- W jakich kanałach oferta jest dostępna
- W jakich lokalizacjach jest dostępna oferta
- Warunki cenowe oferty
- Powiązanie z wzorcem umowy dla oferty

Usługa określa techniczną realizację produktu i charakteryzuje się następującymi atrybutami:

- Nazwa usługi
- Jakim elementem produktu jest usługa (aktywacja, realizacja, dezaktywacja, modyfikacja)
- Powiązanie z zasobami wymaganymi do realizacji usługi
- Powiązanie z dostawcą usługi
- Cenę usługi u dostawcy / koszt realizacji

3.5. Proces obsługi klienta

Obszar adresuje bezpośrednią obsługę klienta

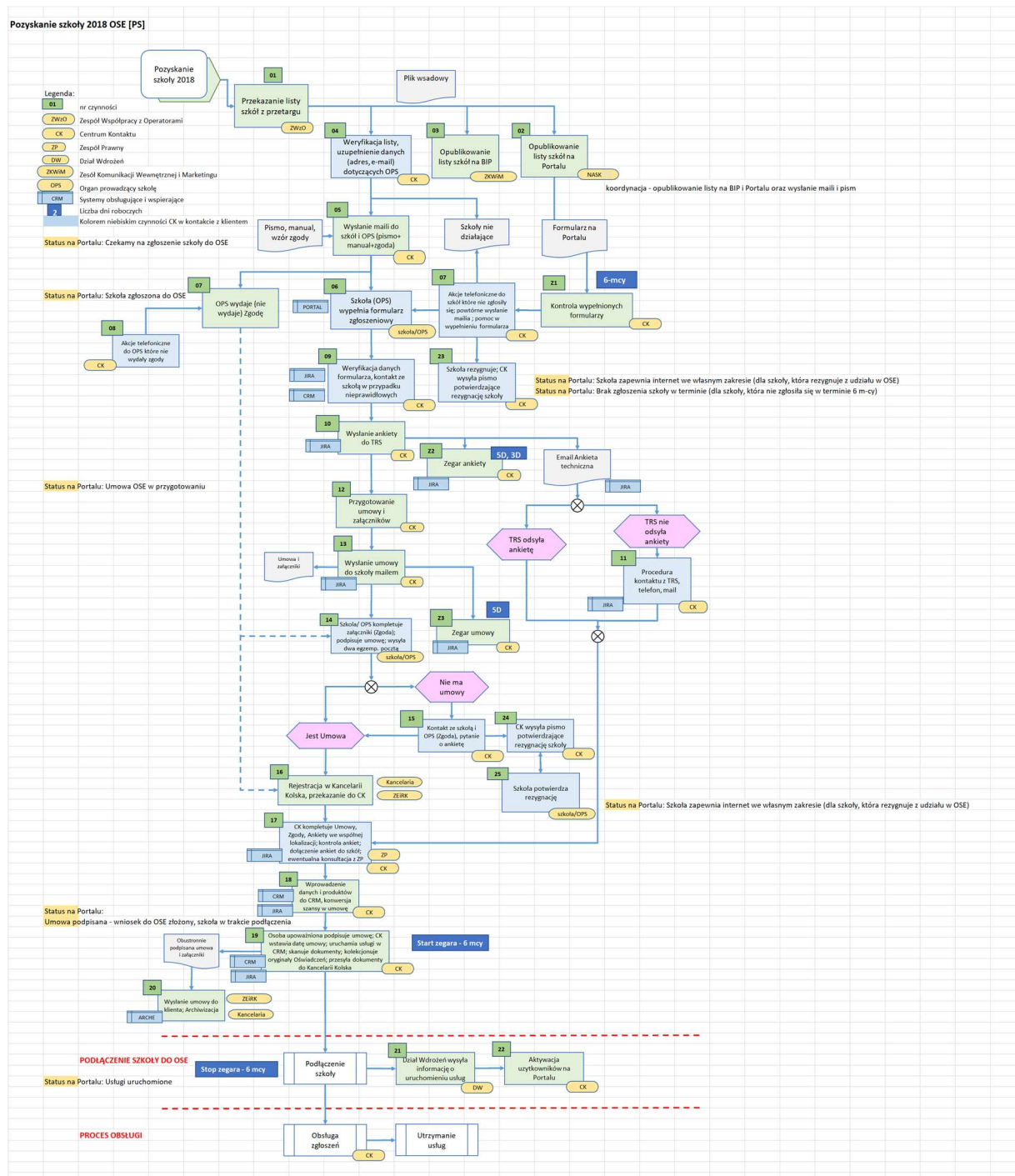
Procesy biznesowe

Proces pozyskania szkoły (proces wdrożony)

Cel procesu	Pozyskanie nowej szkoły do podłączenia do sieci OSE
Inicjacja	Przetarg dla operatorów na łącza dla szkół
Dane wejściowe	Lista szkół z przetargu
Dane wyjściowe	

Załącznik nr 1.3 - Diagram procesu pozyskania szkoły

Proces obecnie zaimplementowany i doskonalony (diagram poglądowy)



Proces zmiana umowy, usługi (proces wdrożony)

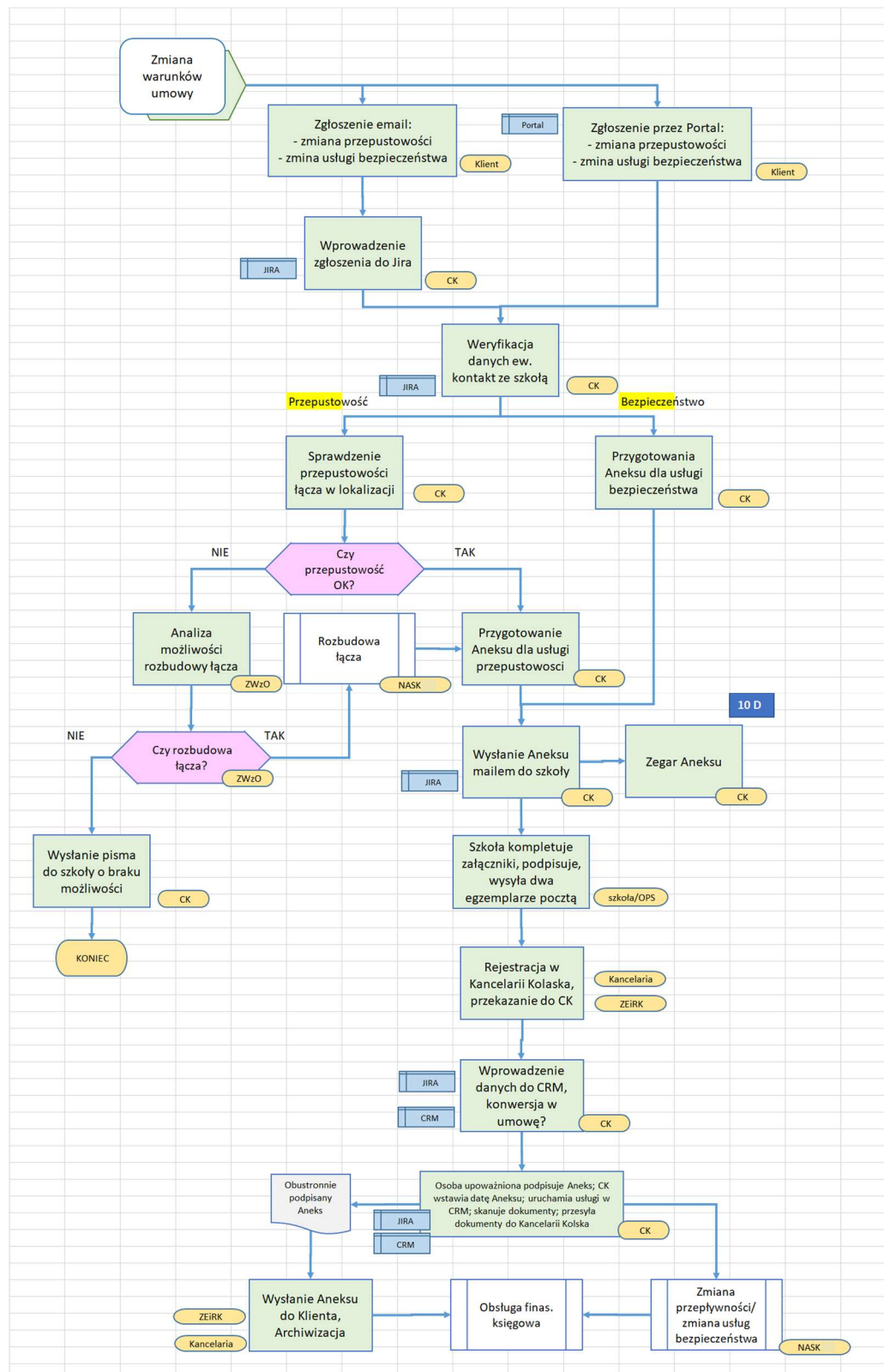
Cel procesu	Zmiana warunków umowy / parametrów usług
Inicjacja	Zgłoszenie przez szkołę zmiany przepustowości lub zamiany usług bezpieczeństwa
Dane wejściowe	Zamówienie zmiany parametrów usług

Dane wyjściowe

KPI

Załącznik nr 1.2 - Diagram procesu zmiana umowy, usługi

Proces obecnie zaimplementowany i doskonalony (diagram poglądowy)



Proces reklamacyjny (proces wdrożony)

Cel procesu	Obsługa reklamacji dotyczących: <ul style="list-style-type: none">• Niedotrzymania z winy NASK określonego w Umowie terminu rozpoczęcia świadczenia Usług OSE,• Niewykonania lub nienależytego wykonania Usług OSE• Nieprawidłowego obliczenia należności z tytułu świadczenia Usług OSE
Inicjacja	Zgłoszenie reklamacji dostarczone przez szkołę jednym z kanałów: <ul style="list-style-type: none">• telefonicznym• ustnym• pisemnym• elektronicznym
Dane wejściowe	Opis reklamacji
Dane wyjściowe	Odpowiedź na reklamację
KPI	

Załącznik nr 1.1 - Diagram procesu reklamacji

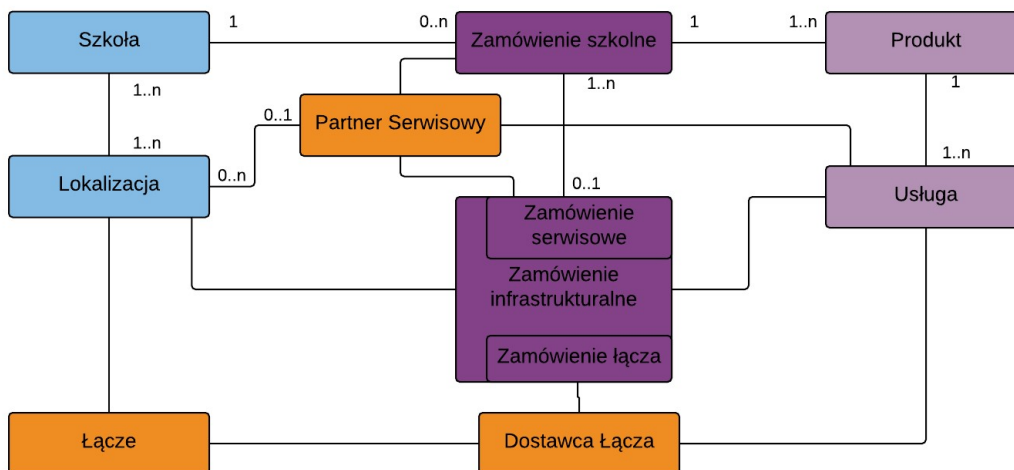
Proces obecnie zaimplementowany i doskonalony (diagram poglądowy)

[illegible]

Model danych

Istotną rolę pełnią osoby przypisane do szkoły (dyrektor, TRS, koordynator) lub OPS. W poszczególnych procesach biznesowych ich dane kontaktowe wykorzystywane są do komunikacji automatycznej (np. email) lub ręcznej (telefon).

Widok zamówienie



3.6. Proces technicznej obsługi

Obszar adresuje zagadnienia związane z częścią techniczną dotyczącą procesów obsługi klienta

Procesy biznesowe

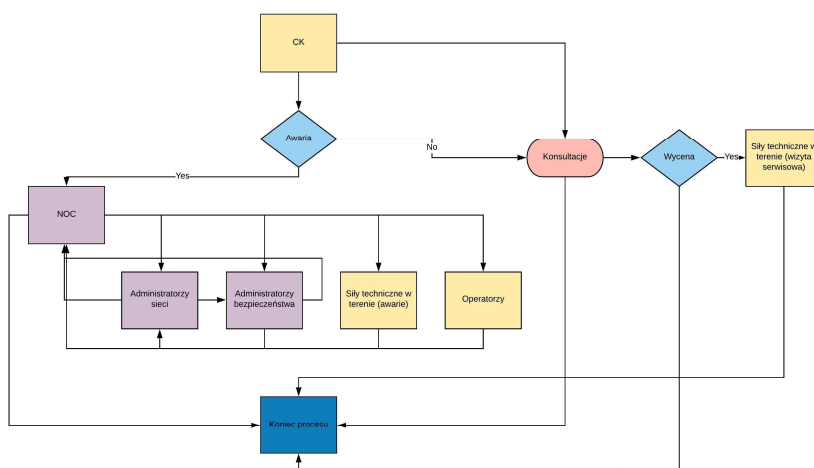
Proces obsługi zgłoszenia w szkole (proces wdrożony)

Cel procesu	Obsługa zgłoszenia dla szkoły
Inicjacja	zgłoszenie wystawione na Portalu OSE przez szkołę lub przez 1 linię wsparcia w imieniu Szkoły bezpośrednio w systemie TT (obecnie Jira SD) (wpisywana jest tylko szkoła)
Dane wejściowe	opis zgłoszenia
Dane wyjściowe	zamknięcie zgłoszenia
KPI	

Diagram procesu obsługi zgłoszenia w szkole

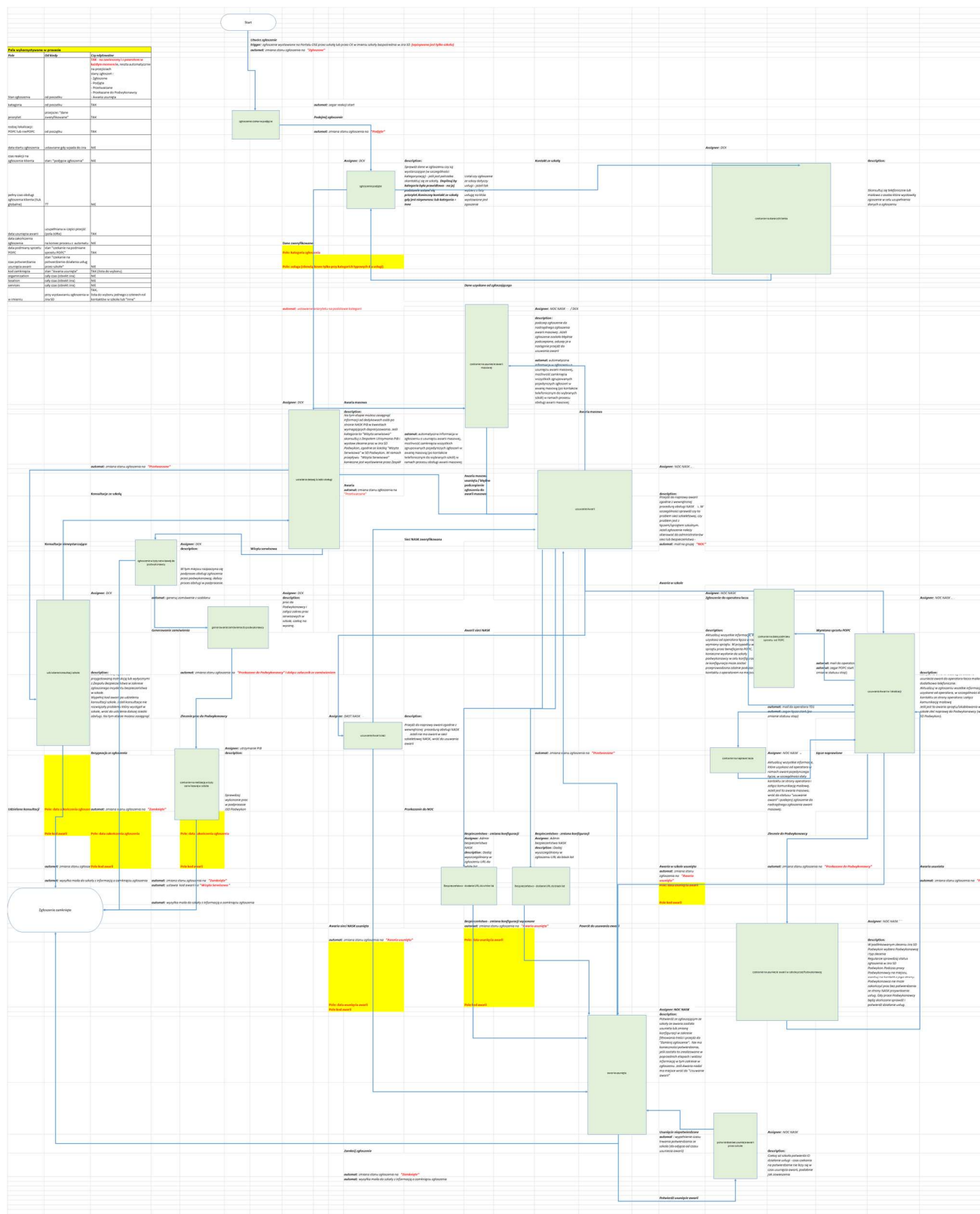
Uproszczona wersja procesu (diagram poglądowy).

Wersja rozszerzona jako dodatkowy diagram



Załącznik nr 1.4 - Diagram procesu obsługi zgłoszenia w szkole

Proces obecnie wdrożony (diagram poglądowy)



Proces obsługi zgłoszenia u podwykonawcy (proces wdrożony)

Cel procesu	Obsługa zgłoszenia u podwykonawcy
--------------------	-----------------------------------

Pola wykorzystywane w procesie obsługi zgłoszeń szkolnych	Uwagi
	<ul style="list-style-type: none"> - Zawieszone - Przetwarzane - Przekazane do Podwykonawcy - Awaria usunięta - Zamknięte
kategoria	
priorytet	
rodzaj lokalizacji: POPC lub niePOPC	
data startu zgłoszenia	
czas reakcji na zgłoszenie klienta	
pełny czas obsługi zgłoszenia klienta (SLA globalne)	
data usunięcia awarii	
data zakończenia zgłoszenia	
data podmiany sprzętu POPC	
czas potwierdzania usunięcia awarii	
kod zamknięcia	lista do wyboru
organization	
location	
services	
w imieniu	lista do wyboru jednego z czterech ról kontaktów w szkole lub "inne"

Pola wykorzystywane w procesie obsługi zgłoszeń u podwykonawcy	Uwagi
Stan zgłoszenia	Stany zgłoszenia: <ul style="list-style-type: none"> - Zlecone - Podjęte - Zawieszone - Przetwarzane - Wykonane - Brak akceptacji wizyty serwisowej
kategoria (pobrana z Issue nadrzędnego)	
priorytet (pobraną z Issue nadrzędnego)	

Pola wykorzystywane w procesie obsługi zgłoszeń u podwykonawcy	Uwagi
czas reakcji na zlecenie od NASK	
liczba godzin w ramach wizyty serwisowej	
czas obsługi zlecenia przez Podwykonawcę	
data wizyty w szkole	
TRS/dyr./koordynator OSE	

Kategoria zgłoszenia	Czy awaria usług OSE	Priorytet	Do kogo kieruje CK/NOC	Wyświetlane na portalu (do wyboru przez szkołę)	Dymek z wyjaśnieniem na Portalu OSE
Konsultacja	nie	3	nie dotyczy, zgłoszenie realizowane przez CK	tak	x
Brak dostępu do internetu	tak	2	admin siec + podwykon	tak	x
Wolne działanie internetu	tak	2	admin siec	tak	x
Awaria sieci NASK	tak	2	admin siec		
Awaria usługi TD	tak	2	admin siec + operator		
Awaria urządzenia CPE POPC	tak	2	NOC + operator + podwykon		
Awaria urządzenia CPE NASK	tak	2	NOC + podwykon		
Awaria urządzenia AP POPC	tak	2	NOC + operator + podwykon		
Awaria urządzenia AP NASK	tak	2	NOC + podwykon		
Awaria urządzenia Przetątnik Sieciowy	tak	2	NOC + podwykon		
Awaria okablowania	tak	2	NOC + podwykon	tak	x
Uszkodzenie szafki POPC	tak	3	NOC + operator		
Uszkodzenie szafki NASK	tak	3	NOC + podwykon		
Inne	nie	3	konieczna zmiana na inną kategorię przez CK	tak	x
Wizyta serwisowa	nie	3	NASKPIB + podwykon		
Bezpieczeństwo - nieprawidłowe filtrowanie	nie	3	NOC + admin bezpieczeństwa	tak	x
Bezpieczeństwo - dodanie url do black list	nie	3	NOC + admin bezpieczeństwa	tak	x
Bezpieczeństwo - dodanie url do white list	nie	3	NOC + admin bezpieczeństwa	tak	x
Bezpieczeństwo - zgłoszenie incydentu	tak	2	NASKPIB + konsultacje z zespołem bezpieczeństwa PIB	tak	x
Grupa "Utrzymanie PIB" może w każdej chwili dodać komentarz do każdego zgłoszenia					

Kategoria zgłoszenia	Czy awaria usług OSE	Priorytet	Do kogo kieruje CK/NOC	Wyświetlane na portalu (do wyboru przez szkołę)	Dymek z wyjaśnieniem na Portalu OSE
Grupy wsparcia CK, NOC oraz podwykonawcy posiadają 1 dedykowany adres mailowy (podwykonawcy terenowi poza domeną NASK) na który przychodzą notyfikacje mailowe o pojawieniu się zgłoszenia na grupie.					

Kody zamknięcia zgłoszenia (obligatoryjne, nie można zamknąć zgłoszenia bez wypełnienia)	
Nazwa kodu	Opis, co kod oznacza
Brak awarii	zgłoszenie nie jest awarią
Awaria z winy klienta	awaria
Awaria masowa - operator	awaria mająca wpływ na brak usług w wielu lokalizacjach (miejsce powstania sieć dostępową)
Awaria masowa - sieć szkieletowa NASK	awaria mająca wpływ na brak usług w wielu lokalizacjach (miejsce powstania sieć szkieletowa)
Awaria masowa - brak usług bezpieczeństwa	awaria mająca wpływ na brak usług w wielu lokalizacjach (miejsce powstania systemy bezpieczeństwa)
Awaria w lokalizacji	awaria w wyniku, której usługi OSE nie były dostępne we wszystkich szkołach w lokalizacji, również w przypadku, gdy 1 lokalizacja = 1 szkoła
Awaria w szkole	awaria w wyniku, której usługi OSE nie były dostępne tylko w 1 szkole. Do wyboru jedynie, gdy w lokalizacji jest > 1 szkoła
Wizyta Serwisowa	zgłoszenie zakończone wizytą serwisową - nie jest to awaria
Brak akceptacji Wizyty Serwisowej	zgłoszenie niezrealizowane w związku z brakiem akceptacji wyceny Podwykonawcy
Awaria masowa	awaria mająca wpływ na brak usług w wielu lokalizacjach (miejsce powstania sieć szkieletowa, sieć dostępową, usługi bezpieczeństwa)
Filtrowanie / url - zaakceptowane	jedynie w przypadku posiadania usługi OSE Plus
Filtrowanie / url - odrzucone	jedynie w przypadku posiadania usługi OSE Plus
Bezpieczeństwo - konsultacja	konsultacja ze szkołą w przypadku zgłoszenia w szkole incydentu bezpieczeństwa (wirusy, ransomware) - wsparcie zdalne przez CKPIB na podstawie dokumentu zdefiniowanego przez Zespół Bezpieczeństwa PIB
Prace planowe	awaria zgłoszona w trakcie prac planowych, o których szkoła została poinformowana

Nazwa SLA	Moment wejścia w stan z Workflow lub moment wykonania akcji, od którego ma zostać uruchomiony zegar	Moment wejścia w stan z Workflow lub moment wykonania akcji, od którego ma zostać zatrzymany zegar	Jaką wartość ma SLA w formacie 1d, 2h 30m, 45m lub wpisana data zakończenia zegara	Typ kalendarza do SLA (24/7 lub 8/5)	Lista stanów z workflow wyłączonych z pomiaru (Stany, w których zegar zostanie zapauzowany)	Czy ma być wysyłane powiadomienie o terminie przekroczenia?	Czas przed,/po jakim czasie od końca założonego SLA ma zostać wysłane powiadomienie	Wysyłka do
zegar reakcji	stan "czekanie na podjęcie zgłoszenia"	stan "zgłoszenie podjęte"	2	9 (8:00-17:00)/5(pn-pt)		tak		szkoła
główny zegar usunięcia awarii	stan "czekanie na podjęcie zgłoszenia"	stan "awaria usunięta"	28	9 (8:00-17:00)/5(pn-pt)	wpisanie w stan zgłoszenia = "zawieszone"	tak, 4 notyfikacje w następujących cyklach: <ul style="list-style-type: none"> • 1 notyfikacja po 8h roboczych (grupa wsparcia, na której jest zgłoszenie) • 2 notyfikacja po 8h roboczych (grupa wsparcia, na której jest zgłoszenie) • 3 notyfikacja po 6h roboczych (grupa wsparcia, na której jest zgłoszenie) • 4 notyfikacja po 6h roboczych (grupa wsparcia, na której jest zgłoszenie + eskalacja do Utrzymanie PIB) 		grupa wsparcia, na której aktualnie znajduje się zgłoszenie
zegar weryfikacji CK	stan "zgłoszenie podjęte"	stan "usuwanie awarii"	4	9 (8:00-17:00)/5(pn-pt)	wpisanie w stan zgłoszenia = "zawieszone"			ck
zegar weryfikacji NOC	stan "usuwanie awarii"	przejście "Zlecenie do Podwykonawcy" lub przejście "Zlecenie do POPC" lub przejście "Zlecenie do operatora łącza" lub stan "Awaria usunięta"	4	9 (8:00-17:00)/5(pn-pt)	wpisanie w stan zgłoszenia = "zawieszone"			noc
zegar POPC	stan "czekanie na datę podmiiany sprzętu"	stan "usuwanie awarii w lokalizacji"	24	24/5				
zegar łącza	stan "czekanie na naprawę łącza"	stan "usuwanie awarii w lokalizacji"	24	24/5				
zegar Podwykonawcy - usuwanie awarii	stan "czekanie na usunięcie awarii w szkole przez Podwykonawcę"	stan "usuwanie awarii w lokalizacji"	8	9 (8:00-17:00)/5(pn-pt)	wpisanie w stan zgłoszenia = "zawieszone"			

Nazwa SLA	Moment wejścia w stan z Workflow lub moment wykonania akcji, od którego ma zostać uruchomiony zegar	Moment wejścia w stan z Workflow lub moment wykonania akcji, od którego ma zostać zatrzymany zegar	Jaką wartość ma SLA w formacie 1d, 2h 30m, 45m lub wpisana data zakończenia zegara	Typ kalendarza do SLA (24/7 lub 8/5)	Lista stanów z workflow wyłączonych z pomiaru (Stany, w których zegar zostanie zapauzowany)	Czy ma być wysyłane powiadomienie o terminie przekroczenia?	Czas przed,/po jakim czasie od końca założonego SLA ma zostać wysłane powiadomienie	Wysyłka do
zegar Podwykonawcy - wizyta serwisowa	stan "czekanie na wykonanie serwisu w szkole"	stan "usuwanie awarii w lokalizacji"	16	9 (8:00-17:00)/5(pn-pt)	wpisanie w stan zgłoszenia = "zawieszone"			

Nazwa SLA	Moment wejścia w stan z Workflow lub moment wykonania akcji, od którego ma zostać uruchomiony zegar	Moment wejścia w stan z Workflow lub moment wykonania akcji, od którego ma zostać zatrzymany zegar	Jaką wartość ma SLA w formacie 1d, 2h 30m, 45m lub wpisana data zakończenia zegara	Typ kalendarza do SLA (24/7 lub 8/5)	Lista stanów z workflow wyłączonych z pomiaru (Stany, w których zegar zostanie zapauzowany)
zegar reakcji	stan "zlecenie wystawione"	stan "obsługa zgłoszonej awarii"	2h	9 (8:00-17:00)/5(pn-pt)	
zegar wykonania zgłoszenia - awarie	stan "obsługa zgłoszonego zlecenia"	przejścia: "Potwierdzone (dokumentacja ta sama)" lub "Potwierdzone (dokumentacja nowa)"	8h	9 (8:00-17:00)/5(pn-pt)	stan "zgłoszenie zawieszone"
zegar wykonania zgłoszenia - wizyty serwisowe	stan "obsługa zgłoszonego zlecenia"	przejścia: "Potwierdzone (dokumentacja ta sama)" lub "Potwierdzone (dokumentacja nowa)"	16h	9 (8:00-17:00)/5(pn-pt)	stan "zgłoszenie zawieszone"
zegar przekazanie terminu wizyty w szkole	stan "obsługa zgłoszonego zlecenia"	wypełnienie pola "Data wizyty w szkole"	2h	9 (8:00-17:00)/5(pn-pt)	stan "zgłoszenie zawieszone"
zegar przekazania nowej dokumentacji	stan "potwierdź wykonanie zlecenia"	stan "Zlecenie wykonane"	3 dni robocze	9 (8:00-17:00)/5(pn-pt)	
zegar potwierdzenia przyjęcia zamówienia szczegółowego	stan "potwierdzenie wizyty serwisowej"	stan "obsługa zgłoszonego zlecenia"	2h	9 (8:00-17:00)/5(pn-pt)	

3.7. Proces realizacji usług

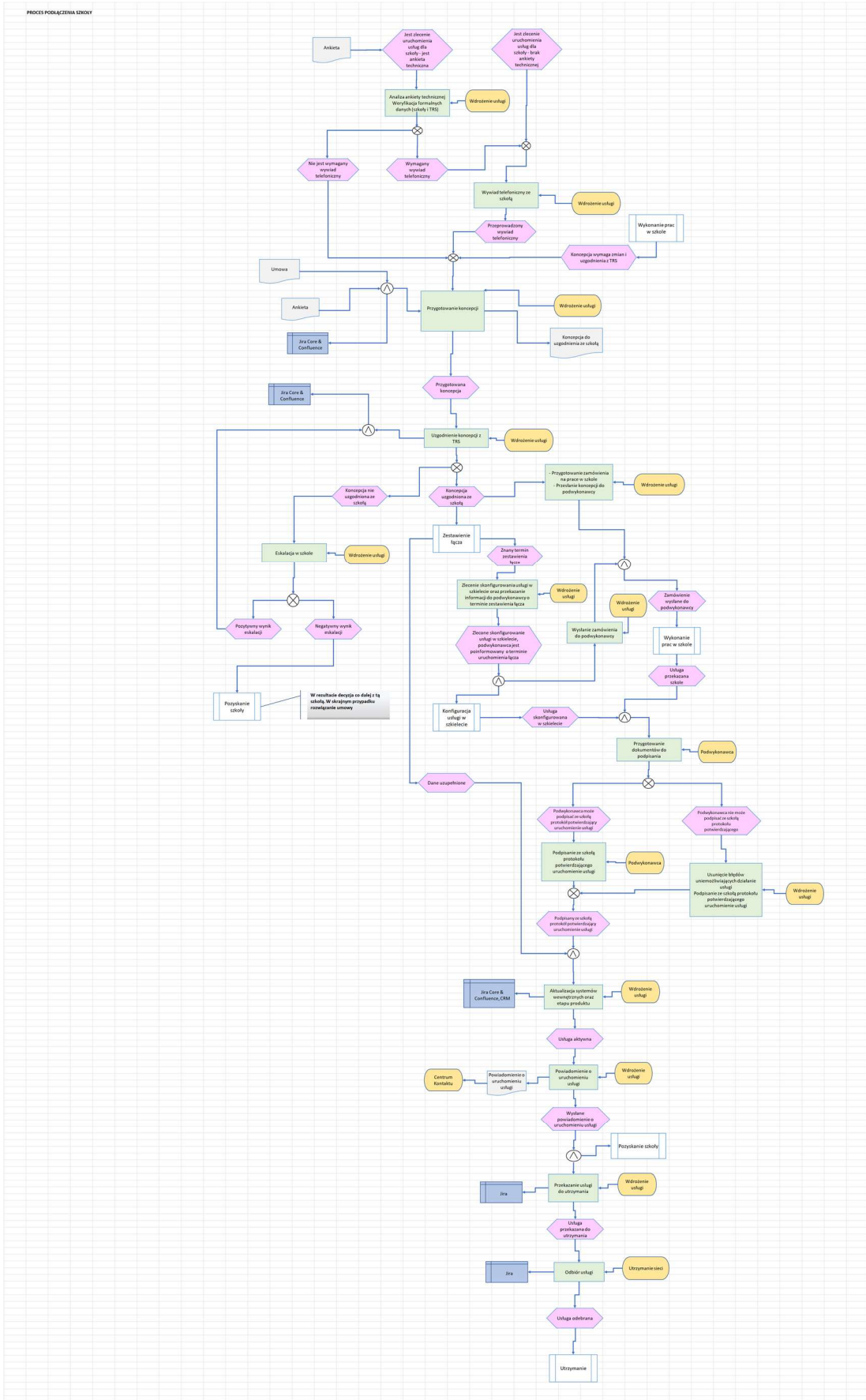
Obszar adresuje wsparcie dostarczania usług dla szkół

Procesy biznesowe

Podłączenie szkoły (proces wdrożony)

Cel procesu	Podłączenie szkoły do sieci OSE
Inicjacja	Zlecenie uruchomienia usługi
Dane wejściowe	Zlecenie uruchomienia usługi, opcjonalnie ankieta techniczna
Dane wyjściowe	Dokumentacja powykonawcza
KPI	

Załącznik nr 1.6 - Diagram procesu podłączenie szkoły
Proces wdrożony (diagram poglądowy)

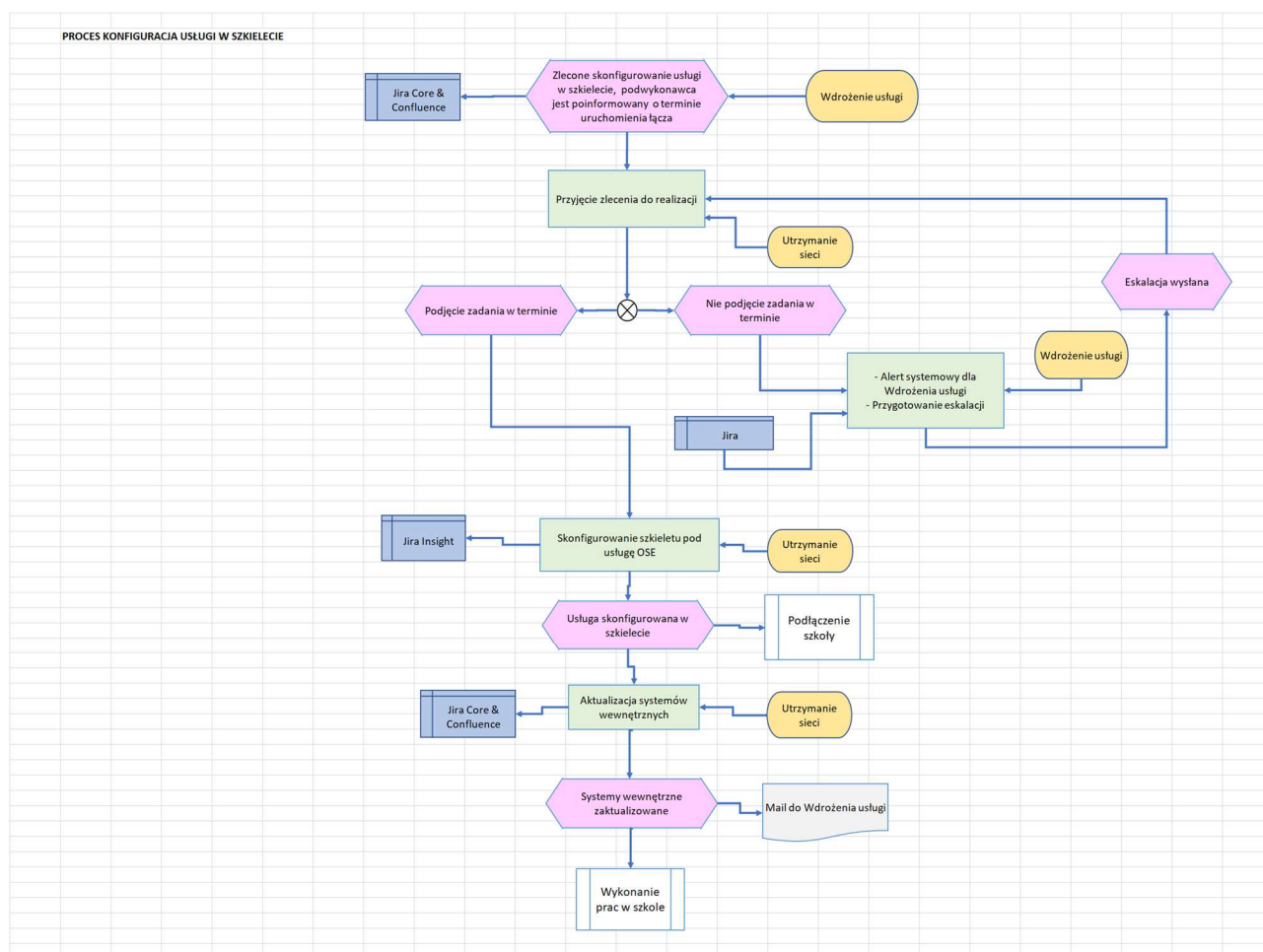


Konfiguracja usług w szkielecie (proces wdrożony)

Cel procesu	Konfiguracja zasobów i usług w sieci szkieletowej na potrzeby działania usług w lokalizacji / szkole
Inicjacja	Zlecenie konfiguracji usług w szkielecie
Dane wejściowe	Zlecenie konfiguracji usług w szkielecie
Dane wyjściowe	
KPI	

Załącznik nr 1.7 - Diagram procesu konfiguracja usług w szkielecie

Proces wdrożony (diagram poglądowy)



Wykonanie prac w szkole (proces wdrożony)

Cel procesu	Realizacja prac technicznych w lokalizacji / szkole
Inicjacja	Zamówienie wysłane do podwykonawcy / partnera serwisowego
Dane wejściowe	Zamówienie na prace w lokalizacji

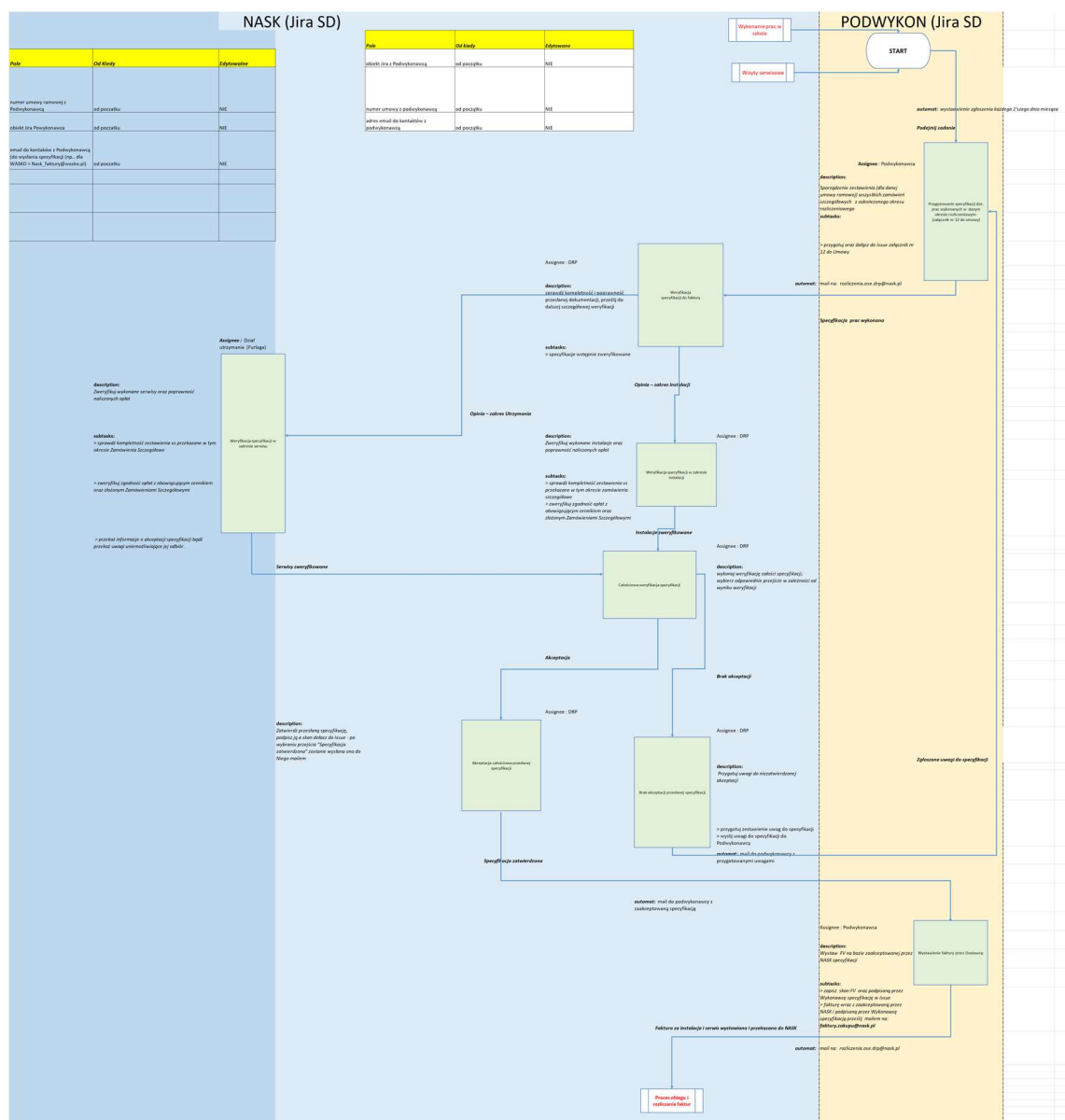
Rozliczenia z podwykonawcami (proces wdrożony)

Cel procesu	Rozliczenie pracy realizowanej przez podwykonawcę / partnera serwisowego
Inicjacja	Wykonanie prac w szkole
Dane wejściowe	Dokumentacja powykonawcza
Dane wyjściowe	Faktura
KPI	

Załącznik nr 1.9 - Diagram procesu rozliczenia z podwykonawcami

Załącznik nr 1.9 - Diagram procesu rozliczenia z podwykonawcami

Proces wdrożony (diagram poglądowy)



Gospodarka magazynowa (proces wdrożony)

Cel procesu	Zarządzanie gospodarką magazynową urzędzeń
Inicjacja	Ręczne uruchamianie procesu
Dane wejściowe	
Dane wyjściowe	
KPI	

[Załącznik nr 1.10 - Diagram procesu gospodarka magazynowa](#)

Załącznik nr 1.10 - Diagram procesu gospodarka magazynowa

Proces wdrożony (diagram poglądowy)

Strona 48 z 387

3.8. Proces utrzymania sieci, usług i systemów

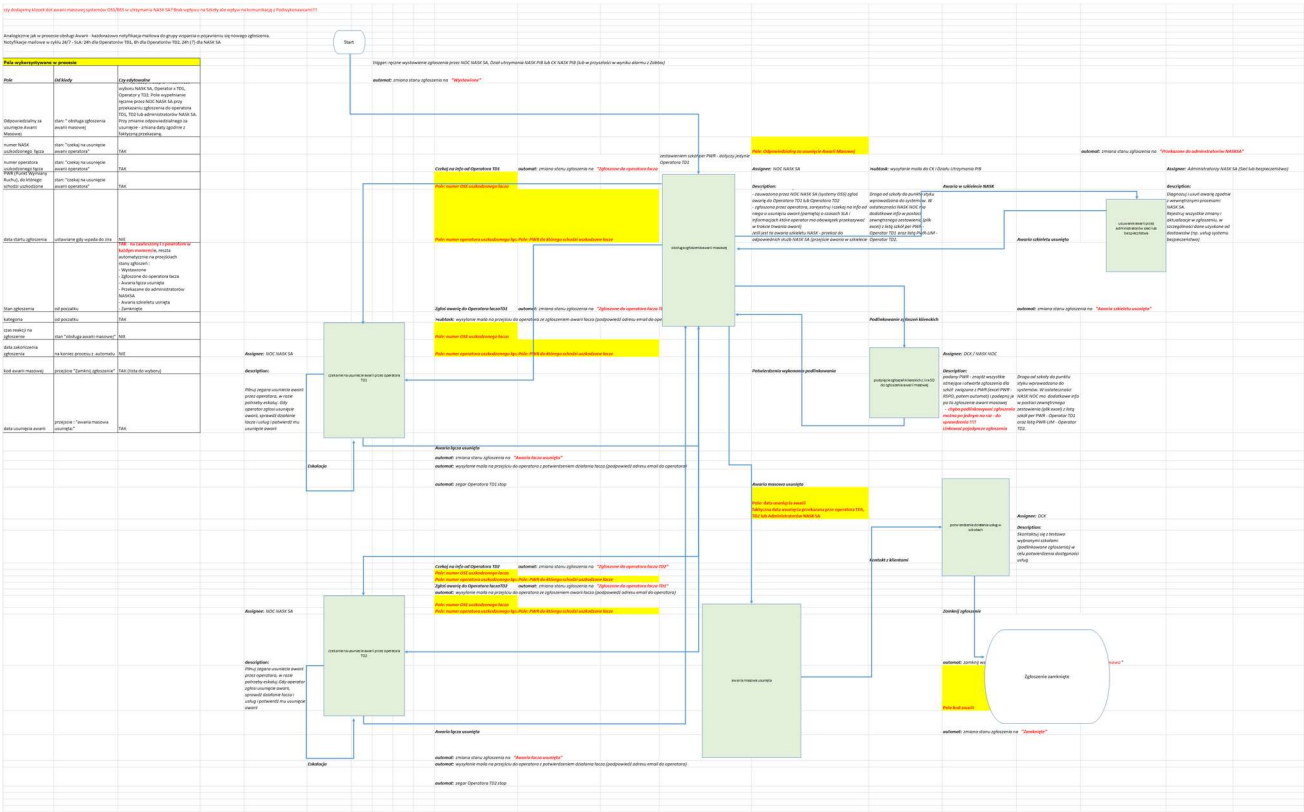
Obszar adresuje zagadnienia związane z utrzymaniem sieci, usług dostarczanych klientom oraz systemów, aplikacji i infrastruktury

Procesy biznesowe

Obsługa awarii masowej (proces wdrożony)

Cel procesu	Obsługa awarii masowych
Inicjacja	Wystąpienie awarii masowej
Dane wejściowe	
Dane wyjściowe	
KPI	

Załącznik nr 1.11 - Diagram procesu awarii masowych
Proces wdrożony



Procedury obsługowe

Załącznik nr 7 do Umowy

Procedura obsługi Awarii Masowych

Informowanie o pracach planowych i awariach na sieci Operatora

- Operator będzie informował OSE o Pracach Planowych oraz Awariach Masowych pocztą elektroniczną pod adres wskazany w Załączniku nr 3 do Umowy.

- Operator do wiadomości elektronicznej dołączy plik Excel, o następującym formacie:

Zakładka: Awaria Masowa	Zakładka: Prace Planowe
<p>Kolumny:</p> <ul style="list-style-type: none"> Adres Budynku Szkoły Współrzędne geograficzne Budynku Szkoły Data wystąpienia Awarii Masowej Czy znana przyczyna Awarii Masowej (Tak/Nie) Planowana data usunięcia awarii Objawy ID PWR, na którym Usługa TD jest niedostępna. 	<p>Kolumny:</p> <ul style="list-style-type: none"> Adres Budynku Szkoły Współrzędne geograficzne Budynku Szkoły Planowana data rozpoczęcia Planowana data zakończenia Opis prac Status

- Dane z pkt. 2 będą aktualizowane i przysyłane przez Operatora do OSE co 2h dla Awarii Masowych i co 12h dla Prac Planowych.

III. Obsługa Awarii Masowej

- Proces obsługi Awarii Masowej realizowany jest zgodnie z zapisami pkt 2-4, Informacje o Awariach będą przekazywane zgodnie z procedurą stanowiącą Załącznik Nr 7 do Umowy.
- Operator po wykryciu Awarii Masowej przez służby techniczne, będzie informował OSE w czasie do 6 (sześciu) godzin od zdiagnozowania o zaistniałej sytuacji.
- Wiadomość będzie zawierała załącznik z listą ID Łączy Abonenckich objętych Awarią Masową. Komunikat będzie zawierał dodatkowo następujące informacje:
 - ID Łączy Abonenckich;
 - Data wystąpienia Awarii;
 - Planowana data usunięcia Awarii;
 - Opis Awarii.
- Operator co 4 (cztery) godziny w przedziale czasowym 0:00 – 23:59 będzie informował OSE w formie elektronicznej za pośrednictwem adresu poczty elektronicznej wskazanego w Załączniku nr 3 do Umowy o statusie Łączy Abonenckich objętych Awarią Masową.
- Zamknięcie statusu Awarii Masowej będzie dotyczyło pełnej listy Łączy Abonenckich, dla których Awaria Masowa została usunięta.
- OSE potwierdza Operatorowi fakt usunięcia Awarii Masowej.
- W sytuacji wystąpienia Awarii Masowej OSE nie będzie zgłaszał do Operatora pojedynczych informacji o Awarii Łączy Abonenckich, wchodzących w skład węzła sieci telekomunikacyjnej objętego Awarią Masową.
- Wyciążanie bonifikat/odszkodowań w systemach rozliczeniowych będzie realizowane na zasadach ogólnych określonych w Umowie.

§ 6

Zasady współpracy w zakresie Awarii

- Wykonawca i Zamawiający współpracują przy lokalizacji, diagnostyce i usuwaniu Awarii.
- Strona odpowiedzialna za usunięcie Awarii usuwa ją według własnych procedur technicznych i dostępnych środków.
- Wykonawca umożliwi Zamawiającemu przeprowadzenie diagnostyki Usługi w każdym momencie trwania Umowy.
- Wykonawca i Zamawiający wzajemnie i bezzwłocznie powiadamiają się o wystąpieniu Awarii.
- Po usunięciu Awarii Wykonawca niezwłocznie powiadomi Zamawiającego o usunięciu Awarii.
- Wykonawca prowadzi rejestr zgłoszeń Awarii.
- W przypadku stwierdzenia przez Wykonawcę Awarii, za którą odpowiedzialny jest Zamawiający, Wykonawca nie ponosi odpowiedzialności za przekroczenie czasu usuwania Awarii.
- Wykonawca zapewnia przyjmowanie zgłoszeń Awarii, które będzie dostępne 24 (dwadzieścia cztery) godziny na dobę, 7 (siedem) dni w tygodniu, we wszystkie dni w roku.
- Czas usunięcia Awarii nie może przekroczyć 6 (sześciu) godzin od momentu dokonania Zgłoszenia Awarii przez OSE.
- W celu uniknięcia wątpliwości do czasu Awarii nie jest wliczany czas gdy Usługa jest świadczona za pomocą rozwiązania zapasowego (protekcja).
- Wykonawca przesyła Zamawiającemu informację o usunięciu Awarii.

Obsługa prac planowych (proces wdrożony)

Cel procesu	Obsługa prac planowych
Inicjacja	Przygotowanie pracy planowej
Dane wejściowe	

Pola wykorzystywane w procesie obsługi awarii masowej

Pole	Uwagi
Odpowiedzialny za usunięcie Awarii Masowej	Możliwość wyboru NASK, Operator x TD1, Operator y TD2. Pole wypełnianie ręcznie przez NOC przy przekazaniu zgłoszenia do operatora TD1, TD2 lub administratorów NASK. Przy zmianie odpowiedzialnego za usunięcie - zmiana daty zgodnie z faktyczną przekazaną.
numer NASK uszkodzonego łącza	
numer operatora uszkodzonego łącza	
PWR (Punkt Wymiany Ruchu), do którego schodzi uszkodzone łącze	
data startu zgłoszenia	
Stan zgłoszenia	stany zgłoszeń : - Wystawione - Zgłoszone do operatora łącza - Awaria łącza usunięta - Przekazane do administratorów NASK - Awaria szkieletu usunięta - Zamknięte - Zawieszony
kategoria	
czas reakcji na zgłoszenie	
data zakończenia zgłoszenia	
kod awarii masowej	
data usunięcia awarii	

Operatorzy TD1 (szkoła - PWR):

komunikacja z operatorami mailowo i telefonicznie - na poziomie operacyjnym NOC

awaria masowa - awaria minimum 1 węzła sieci telekomunikacyjnej

informacje przekazywane przez Operatora TD1 - arkusz "TD1 - zał. dot. obsługi awarii m"

Operatorzy TD2 (PWR - LIM):

komunikacja z operatorami mailowo i telefonicznie - na poziomie operacyjnym NOC.

awarie tylko masowe --> w efekcie brak usług we wszystkich szkołach zebranych w danym PWR

Operatorzy TD1 (szkoła - PWR):

połączenie między TD1 a TD2 - przełącznica światłowodowa ODF zlokalizowana w PWR w miejscu wskazanym przez Operatora TD1. Za transmisję punktu styku w ODF TD1 do punktu styku w LIM (NASK) odpowiada Operator TD2

w systemie JIRA należy wprowadzić wszystkich operatorów TD1 i TD2 wraz z kontaktami wynikającymi z umów NASK PIB - Operator TD1 lub TD2

Kategoria awarii masowej

Awaria łącza - Operator TD1

Awaria łącza - Operator TD2

Awaria sieci szkieletowej NASK

Awaria urządzeń szkieletowych (sieć)

Awaria urządzeń szkieletowych (bezpieczeństwo)

Awaria systemu bezpieczeństwa

Inne

Kod awarii masowej

uszkodzony światłowód

zasilanie w PWR

awaria routera NASK

awaria switcha NASK

zasilanie w węźle NASK

błędna konfiguracja na urządzeniu sieciowym

błędna konfiguracja na urządzeniu bezpieczeństwa

awaria systemu bezpieczeństwa

Kody zamknięcia zgłoszenia

Nazwa kodu

Brak awarii

Awaria łącza - Operator TD1

Awaria łącza - Operator TD2

Awaria szkieletu NASK - sieć

Kody zamknięcia zgłoszenia

Awaria szkieletu NASK - bezpieczeństwo

Nazwa SLA	Moment wejścia w stan z Workflow lub moment wykonania akcji, od którego ma zostać uruchomiony zegar	Moment wejścia w stan z Workflow lub moment wykonania akcji, od którego ma zostać zatrzymany zegar	Jaką wartość ma SLA w formacie 1d, 2h 30m, 45m lub wpisana data zakończenia zegara	Typ kalendarza do SLA (24/7 lub 8/5)
zegar reakcji	start Issue	stan "obsługa awarii masowej"	??	24/7
główny zegar usunięcia awarii	stan "obsługa awarii masowej"	stan "awaria masowa usunięta"	?? Inne zegary w zależności od operatora TD1, TD2, NASK	24/7
zegar operatora TD1	stan "czekaj na info od operatora1"	stan "obsługa awarii masowej"	24	24/7
zegar operatora TD2	stan "czekaj na info od operatora2"	stan "obsługa awarii masowej"	6	24/7
zegar bezpieczeństwo				24/7

Pola wykorzystywane w procesie obsługi prac planowych

Pole	Uwagi
Podmiot zgłaszający	
Termin rozpoczęcia prac	
Planowany czas trwania prac	
Termin zakończenia prac (automat)	
Pole: Dane kontaktowe	
Stan zgłoszenia	stany zgłoszeń : <ul style="list-style-type: none">- Wystawione- Przetwarzane- Zrealizowane- Zamknięte- Zawieszony

Nazwa SLA	Moment wejścia w stan z Workflow lub moment wykonania akcji, od którego ma zostać uruchomiony zegar	Moment wejścia w stan z Workflow lub moment wykonania akcji, od którego ma zostać zatrzymany zegar	Jaką wartość ma SLA w formacie 1d, 2h 30m, 45m lub wpisana data zakończenia zegara	Typ kalendarza do SLA (24/7 lub 8/5)	Lista stanów z workflow wyłączonych z pomiaru (Stany, w których zegar zostanie zapauzowany)	Czy ma być wysyłane powiadomienie o terminie przekroczenia?	Czas przed/po jakim czasie od końca założonego SLA ma zostać wysłane powiadomienie	Wysyłka do
zegar informacji do szkół			3 dni (przed rozpoczęciem prac)	24/7				

3.9. Proces współpracy z operatorami

Procesy biznesowe

Założenia (na podstawie Modelu Wymiany Danych)

OSE będzie przysyłać jedno zamówienie łączy do jednej lokalizacji Szkoły. OSE nie zamawia kilku łączy do jednej lokalizacji. Oznacza to, iż jeśli Operator otrzyma od OSE więcej niż jedno zamówienie do danej lokalizacji, powinien je odrzucić formalnie (zgodnie z umową operator ma 2DR na weryfikację formalną). Odrzucenie zamówienia powinno być wykonane zgodnie z Rozdziałem 3 – Weryfikacja Formalna.

W przypadku usług aktywnych, tj. szkoła już działa w sieci OSE, OSE będzie zamawiać zwiększenie przepływności o dodatkowe 50/50Mbps zgodnie z ofertą Operatora składając nowe Zamówienie do Operatora. Zamówienie będzie wyglądać dokładnie tak samo, jak Zamówienie na łącze – będzie jedynie zmienione względem niego w zakresie liczby zamawianych 50/50Mbps. Zamówienie otrzyma nowy numer ewidencyjny OSE

Dokumentem uzupełniającym Model Wymiany Danych (MWD) są wytyczne do kreowania VLAN oraz tabela konfiguracji CPE (dla Beneficjentów POPC).

OSE będzie przysyłać Zamówienia za pomocą e-mail. E-mail będzie zawierał:

- w treści e-mail - dane dotyczące zamówienia.
- w załączniku - Zamówienie w formie pliku word, z polami edytowalnymi.
- w załączniku - skan Zamówienia podpisanego przez upoważnionych przedstawicieli OSE oraz skan Oświadczenia podpisanego przez przedstawicieli Szkoły

Oryginały w formie papierowej: zamówień i oświadczeń będą przysyłane pod wskazany w umowie adres Operatora, do pierwszego dnia roboczego każdego miesiąca.

Zestawienie łączy (proces wdrożony)

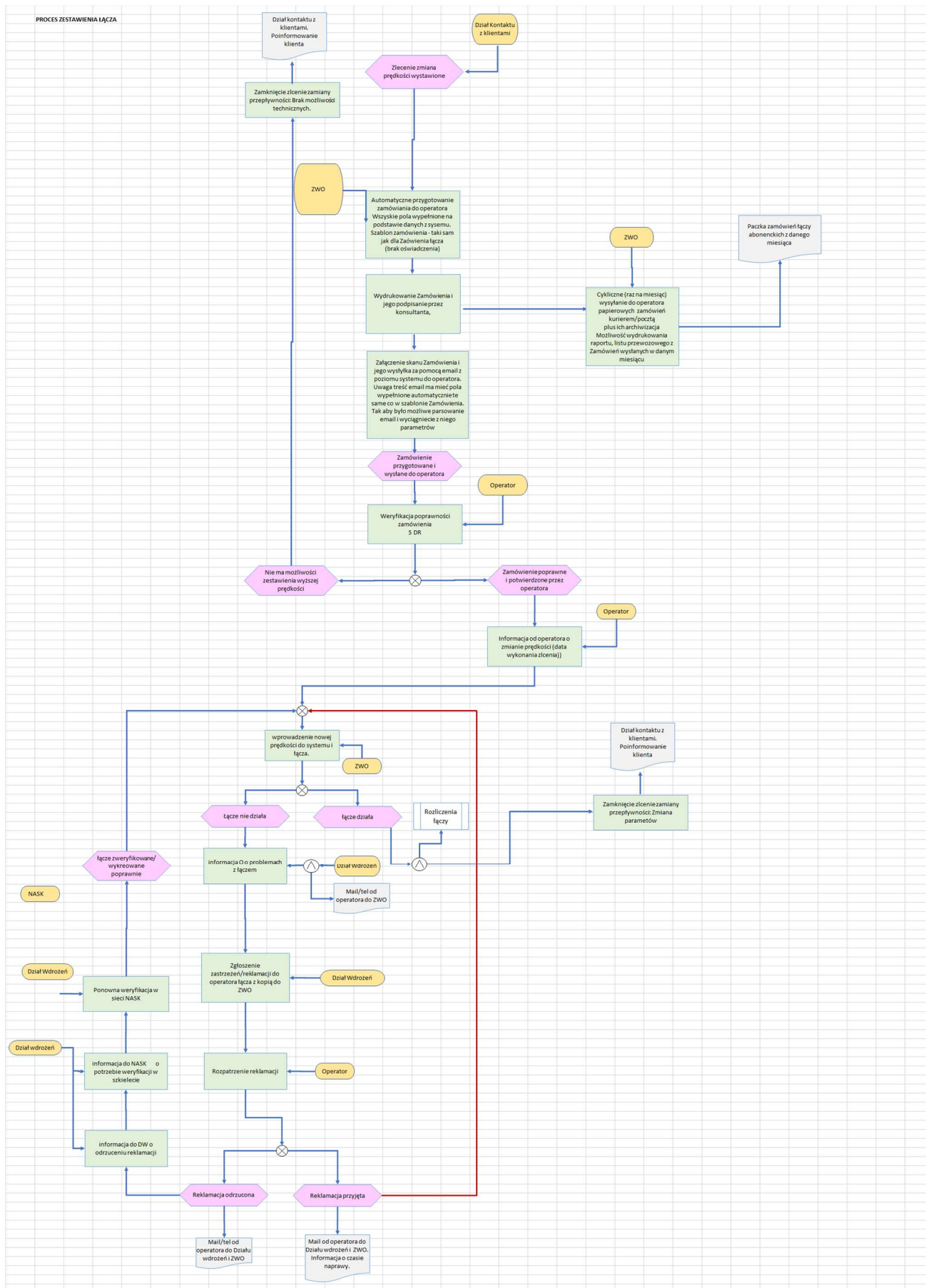
Cel procesu	Podłączenie szkoły przez operatora dostępowego
--------------------	--

Zmiana szybkości łącza (proces wdrożony)

Cel procesu	Zmiana prędkości łącza dostępowego
Inicjacja	Zamówienie na zmianę prędkości łącza
Dane wejściowe	Zamówienie na zmianę prędkości łącza
Dane wyjściowe	
KPI	

Załącznik nr 1.14 - Diagram procesu zmiana szybkości łącza

Proces wdrożony (diagram poglądowy)



Szczegółowy opis procesu komunikacji z operatorami

Rozpoczęcie procesu realizacji Usługi TD do Budynku Szkoły

- E-mail będzie przesyłany z adresu: mail.ose@nask.pl
- Tytuł e-mail będzie zawierał: unikalny numer ewidencyjny danego zamówienia.
- E-mail każdorazowo będzie dotyczył tylko jednej lokalizacji. Każde zamówienie na lokalizację jest równoznaczne z osobnym e-mail.
- Każde zamówienie będzie zawierać dwa unikalne ID: Numer RSPO, ID Adresu:
 - Numer RSPO Szkoły – jest to unikalny numer przypisany do danej Szkoły w danej lokalizacji.

Uwaga! W danej lokalizacji może być więcej niż jedna Szkoła, dlatego pomimo, iż Zamówienie będzie wystawiane tylko do jednej Szkoły, tj. podawany będzie tylko jeden Numer RSPO, to do tego Zamówienia będą załączone Oświadczenia w formie papierowej dla każdej Szkoły znajdującej się w Budynku Szkoły (np. 2). Numer RSPO umożliwia OSE odnalezienie Szkoły w systemach OSE oraz w harmonogramie dla Szkół publikowanym przez OSE.

- ID Adresu – jest to unikalny numer przypisany do danego adresu (lokalizacji Szkoły). ID Adresu mieści się również w tabelach służących do składania ofert przez Operatorów w postępowaniu przetargowym NASK, gdzie jest nazwane **ID_2017**. ID Adresu umożliwia jednoznaczną identyfikację rekordu w postępowaniu przetargowym, również dla przypadków oczywistych omyłek w adresie wynikających z:
 - dekomunizacji nazw ulic: zmiana adresu wynika ze zmiany nazwy ulicy.
 - omyłkowego numeru budynku np. 5 na 5C.

Uwaga! W przypadku, w którym zmiana adresu na zamówieniu nie została uzgodniona pomiędzy OSE a Operatorem przed złożeniem Zamówienia przez OSE, należy w weryfikacji formalnej (2DR) wskazać, czy Operator akceptuje wykonanie zamówienia, czy je odrzuca (niezgodność adresu z ofertą) – zwłaszcza w przypadku zmiany numeru budynku Szkoły. OSE każdorazowo stara się wychwycić zmiany adresów przy zawieraniu umowy ze Szkołą, dlatego też przypadki składania Zamówień na inne adresy przy wykorzystaniu tego samego ID_2017 nie powinny wystąpić.

Weryfikacja formalna

W terminie 2 (dwóch) DR od otrzymania przez Operatora Zamówienia dokonywana jest weryfikacja formalna i w przypadku, gdy Zamówienie i/lub Oświadczenie nie spełnia wymogów formalnych, Operator w powyższym terminie zwraca się w formie elektronicznej do OSE o uzupełnienie lub poprawienie Zamówienia i/lub Oświadczenia. W przypadku, gdy Zamówienie i Oświadczenie spełniają wymogi formalne, są przyjmowane przez Operatora do realizacji a Operator wysyła do OSE potwierdzenie przyjęcia Zamówienia do realizacji.

- Operator ma 2 dni robocze na ewentualne odrzucenie danego Zamówienia i tym samym wstrzymanie biegu jego realizacji.
- Potwierdzenie lub odrzucenie zamówienia powinno zostać wykonane za pomocą e-mail w odpowiedzi na email OSE z Zamówieniem bez zmiany tematu e-mail, tj. wymagane jest nie edytowanie tematu, a jedynie kliknięcie „odpowiedź”.
- Operator ma dwie opcje udzielenia odpowiedzi:
 - Potwierdzenie przyjęcia realizacji zamówienia: Należy udzielić odpowiedzi: „Potwierdzamy przyjęcie Zamówienia do realizacji”.
 - Odrzucenie formalne Zamówienia. Należy udzielić odpowiedzi zgodnej z poniższym słownikiem:
 - 01 – Zamówienie nie dotyczy Operatora. Błąd wskazania Operatora.

Przykład: brak możliwości identyfikacji lokalizacji – brak ID_Adresu na liście lokalizacji w Umowie.

- 02 – Zamówienie złożone przed datą gotowości zawartą w Umowie.

Rozpoczęcie procesu realizacji Usługi TD do Budynku Szkoły

- 03- Kolejne Zamówienie dotyczące tego samego adresu. Usługa TD jest nieaktywna i w trakcie realizacji (wcześniejsze Zamówienie zostało przyjęte).
- 04 – Zamówienie na adres niezgodny z Umową, Operator nie wykona instalacji do innego adresu.

Przykład: zmiana numeru domu na niezgodny z Umową.

- 05 – Brak możliwości Technicznych.

Przykład: Operator posiada wiedzę na etapie weryfikacji formalnej, że Zamówienia nie zrealizuje ze względu na brak możliwości Technicznych. Taki kod i odpowiedź przerywa proces Zamawianie łącza. Dalsza komunikacja będzie odbywać się już pomiędzy osobami wskazanymi w Umowie.

W przypadku negatywnej weryfikacji Zamówienia, OSE ma 3 Dni Robocze na poprawienie Zamówienia. Poprawienie Zamówienia będzie wykonane poprzez wystawienie nowego Zamówienia z nowym numerem ewidencyjnym. Termin realizacji Usługi TD będzie biegł z datą złożenia nowego Zamówienia. Format e-mail poprawionego Zamówienia będzie identyczny jak Zamówienia pierwotnego, jednakże zawarte w nim informacje zostaną zmienione.

Weryfikacja możliwości technicznych realizacji Zamówienia

Po przyjęciu do realizacji Zamówienia dotyczącego łącza Abonenckiego, Operator dokonuje weryfikacji możliwości technicznych świadczenia Usługi TD na danym łączy Abonenckim i w terminie 10 (dziesięciu) DR od przyjęcia Zamówienia do realizacji przekazuje pisemnie OSE informację o wyniku weryfikacji możliwości technicznych (istnieniu bądź braku technicznych możliwości realizacji Zamówienia). W przypadku braku technicznych możliwości realizacji Zamówienia, Operator podaje przyczynę oraz Strony podejmują negocjacje w celu wypracowania alternatywnej możliwości realizacji Usługi TD. W przypadku braku znalezienia alternatywnego rozwiązania podłączenia Usługi TD przez Operatora do Budynku Szkoły, Strony pisemnie zawrą aneks mający na celu usunięcie Adresu Budynku Szkoły z Listy lokalizacji Szkół.

- W przypadku pozytywnej weryfikacji technicznej nie należy przysyłać komunikacji do OSE i należy przejść do etapu przesłania Parametrów technicznych usługi.

W przypadku negatywnej weryfikacji technicznej należy udzielić odpowiedzi na pierwotny e-mail z Zamówieniem danej Usługi TD oraz przesłać na adres e-mail wskazany w umowie informacje o braku możliwości technicznych realizacji zamówienia. Wysłanie odpowiedzi przerywa bieg realizacji Zamówienia i dalsza korespondencja odbywa się pomiędzy właściwymi osobami wskazanymi w Umowie.

Parametry techniczne usługi – data jej realizacji.

Operator na 10 (dziesięć) DR przed realizacją Usługi TD, przekaże OSE drogą elektroniczną (poczta elektroniczna) informacje o:

1. Dacie i planowanej godzinie rozpoczęcia realizacji Usługi TD na łączy Abonenckim;
2. parametrach Usługi TD, w szczególności numerach VLAN oraz PWR, na którym Usługa TD będzie dostępna.
3. Typie i modelu Urządzenia CPE, które zamierza zainstalować wraz z jego numerem seryjnym oraz adresem MAC.
4. Typie i modelu Urządzenia Wi Fi, które zamierza zainstalować wraz z jego numerem seryjnym oraz adresem MAC.

Rozpoczęcie procesu realizacji Usługi TD do Budynku Szkoły

- Operator przesyła zestaw danych w odpowiedzi na e-mail z Zamówieniem Usługi TD bez zmiany tematu e-mail. Operator nie może do treści email wstawiać danych innej / innych Usług/i TD. Każdorazowo jedna odpowiedź z parametrami dotyczy jednej Usługi TD.
- Operator, na co najmniej 10 DR przed realizacją Usługi TD w odpowiedzi na e-mail z Zamówieniem (bez zmiany tematu) powinien udzielić następującej odpowiedzi:
 1. Data planowanego rozpoczęcia Instalacji: [rrrr.mm](#).dd HH:MM
 2. Informacja VLAN:
 - a. i. Mapowanie VLAN: VLAN mgmt: XXXXX (VLAN zarządzanie), VLAN data: yyyyyyy VLAN data: zzzzzz, VLAN data:, w zależności ile VLAN zostało zamówione przez OSE oraz sposobu realizacji.
 - b. ii. Stosowanie QinQ na PWR: SVLAN dla danej szkoły: XXXXXX.
 3. ID_PWR: wskazać nazwę PWR zgodną z nazwą w Umowie. W przypadku, w którym na danym PWR są dwa lub więcej interfejsów – należy dodatkowo wskazać ID ODF/portu routera w zależności o fizycznego punktu styku.
 4. TYP i MODEL CPE: xx wraz z jego numerem seryjnym oraz adresem MAC.

Uwaga: Dotyczy Beneficjentów POPC i łączy realizowanych w programie POPC.

1. TYP I MODEL AP: xx wraz z jego numerem seryjnym oraz adresem MAC.

Uwaga: Dotyczy Beneficjentów POPC i łączy realizowanych w programie POPC.

Informacje dodatkowe

Informacje dodatkowe umożliwiają sprawne podłączenie sieci LAN do OSE, w tym wyposażenie szkoły w CPE z właściwym rodzajem interface do łącza Operatora:

Numer	lista:
1	GPON - 1GE RJ45
2	Radio - 1GE RJ45
3	CPE - 1GE RJ45
4	Switch - 1GE RJ 45
5	CPE - 1GE SFP-LC
6	Switch - 1GE SFP-LC
7	2J ST/UPC,
8	2J SC/UPC,
9	2J SC/APC 8,
10	2J FC/UPC,
11	2J FC/APC 8,

Rozpoczęcie procesu realizacji Usługi TD do Budynku Szkoły

12	2J LC/UPC,
13	2J LC/APC 8,
14	2J E2000/UPC,
15	2J E2000/APC,
16	2J MU/UPC,
17	2J MU/APC,
18	2J DIN/UPC,
19	2J DIN/APC 8,
20	2J MTRJ.
21	1J ST/UPC,
22	1J SC/UPC,
23	1J SC/APC 8,
24	1J FC/UPC,
25	1J FC/APC 8,
26	1J LC/UPC,
27	1J LC/APC 8,
28	1J E2000/UPC,
29	1J E2000/APC,
30	1J MU/UPC,
31	1J MU/APC,
32	1J DIN/UPC,
33	1J DIN/APC 8,
34	1J MTRJ.

TYP REALIZACJI ŁĄCZA

Nowe - Nowe łącze, brak działających usług na łączu

Istniejące - Przełączenie istniejącej usługi – należy rozłączyć działającą Usługę w Szkole

Odbiór Usługi TD – błędy w jej konfiguracji

W terminie 14 (czternastu) dni od dnia realizacji Zamówienia, OSE ma prawo zgłosić zastrzeżenie do technicznej realizacji Zamówienia (Interwencja). Zgłoszona uwaga powinna być bezpośrednio związana z brakiem możliwości uruchomienia usługi dla Abonenta. Po wpłynięciu zgłoszenia do Operatora realizowana jest weryfikacja techniczna Usługi TD mająca na celu wykrycie i usunięcie ewentualnego błędu technicznego leżącego po stronie Operatora.

Rozpoczęcie procesu realizacji Usługi TD do Budynku Szkoły

Za termin rozpoczęcia świadczenia Usługi TD na danym Łączu Abonenckim przyjmuje się datę następującą w terminie 14 (czternastu) dni kalendarzowych od daty realizacji Zamówienia. Jeżeli w terminie 14 (czternastu) dni kalendarzowych od daty realizacji Zamówienia, OSE zgłosi zastrzeżenia, co do realizacji, i będą one zasadne, to data ta będzie przesunięta do czasu ostatecznego zakończenia realizacji Zamówienia.

- Komunikacja będzie odbywać się za pomocą e-mail. OSE prześle na adres wskazany w umowie zastrzeżenia do realizacji technicznej. Podając każdorazowo Adres_ID i RSPO danej Szkoły, do której było wystawione zamówienie. Informacja będzie zawierała również parametry techniczne, jakimi posługuje się OSE w celu ich weryfikacji.
- W przypadku przekroczenia 14-dniowego terminu, OSE zgłosi do Operatora Awarię za pomocą poczty elektronicznej na adres funkcyjny z Umowy.

Odbiór Usługi TD następuje automatycznie 14 dni od daty realizacji Zamówienia, o ile data ta nie zostanie przesunięta w wyniku zgłoszonej Interwencji technicznej.

Model danych

Definicje:

Szkoła – zgodnie z ustawą z dnia 27 października 2017 r. o Ogólnopolskiej Sieci Edukacyjnej (Dz.U. z 2017r.,poz.2184) jest to szkoła w rozumieniu art. 2 pkt 2 ustawy z dnia 14 grudnia 2016 r. – Prawo oświatowe (Dz. U. z 2017 r. poz. 59 i 949), z wyjątkiem szkół dla dorosłych.

Usługa TD – usługa Transmisji Danych,

Łącze Abonenckie - stanowi:

a) segment linii kablowej podziemnej, linii kablowej nadziemnej lub kanalizacji kablowej wraz z kablem telekomunikacyjnym, zawarty między złączem rozgałęźnym a zakończeniem tych linii lub kanalizacji w obiekcie budowlanym,

b) system bezprzewodowy łączący instalację wewnętrzną obiektu budowlanego z węzłem publicznej sieci telekomunikacyjnej umożliwiający korzystanie w obiekcie budowlanym z publicznie dostępnych usług telekomunikacyjnych.

Na Łączu Abonenckim świadczona jest Usługa TD przez Operatora.

Awaria - stan techniczny sieci lub jej elementów uniemożliwiający świadczenie Usług TD, a poprzez to, uniemożliwiający świadczenie Usług abonenckich.

Interwencja techniczna - zastrzeżenie do technicznej realizacji Zamówienia (Interwencja)

Atrybuty przypisane do adresu / lokalizacji

Nazwa pola:	Przykładowa wartość	Uwagi
ID_2016	9100000003211459	unikalne ID

Nazwa pola:	Przykładowa wartość	Uwagi
duplikaty 2016 --> 2017	NIE	
ID_2017	9633010	unikalne ID
GML_ID	4508226	
ID_PODMIOT_SZKOŁA RSPO	31042,31092	może być kilka numerów RSPO - do 20 na lokalizacji
województwo	PODLASKIE	
powiat	SOKÓLSKI	
gmina	NOWY DWÓR	
SIMC	0037612	
miejsowość	NOWY DWÓR	
ULIC	08828	
ULICA	UL. KOLEJOWA	
NR_DOMU	2	
X92	800421	współrzędne
Y92	650404	współrzędne
POPC2/ NIE POPC	POPC	
Operator dostarczający łącze	MDO Projekt	
Punkt Wymiany Ruchu (PWR) z Operatorem		
Data zaktualizowana rekordu		
Zmiana adresu (1 - TAK, 0 - NIE) - czy nastąpiła zmiana adresu na ID_2017	0	
Sposób zakończenia łącza w Szkole - słownik zdefiniowany		
model CPE		
model AP (WiFi)		
model switch		
Czy objęta przetargiem	TAK	
Nr paczki przetargowej	60	
Zwycięzca przetargu	MDO	

Nazwa pola:	Przykładowa wartość	Uwagi
Proponowany PWR	Al. Jerozolimskie 65/79, Warszawa	
Data, po której można złożyć zamówienie	30.10.2018	
Nr Harmonogramu	2	numer prezentujący numer harmonogramu i publikacji
Abonament miesięczny netto	218	
Opłata instalacyjna netto	398	
Opłata 50/50 MB netto	98	
Opłata 50/50 MB brutto	120,54	
możliwa data podłączenia z harmonogramu	43434	
data aktywacji łącza		
data zmiany przepływności łącza		
ID_łącza		
VLAN		może być kilkanaście na adresie.

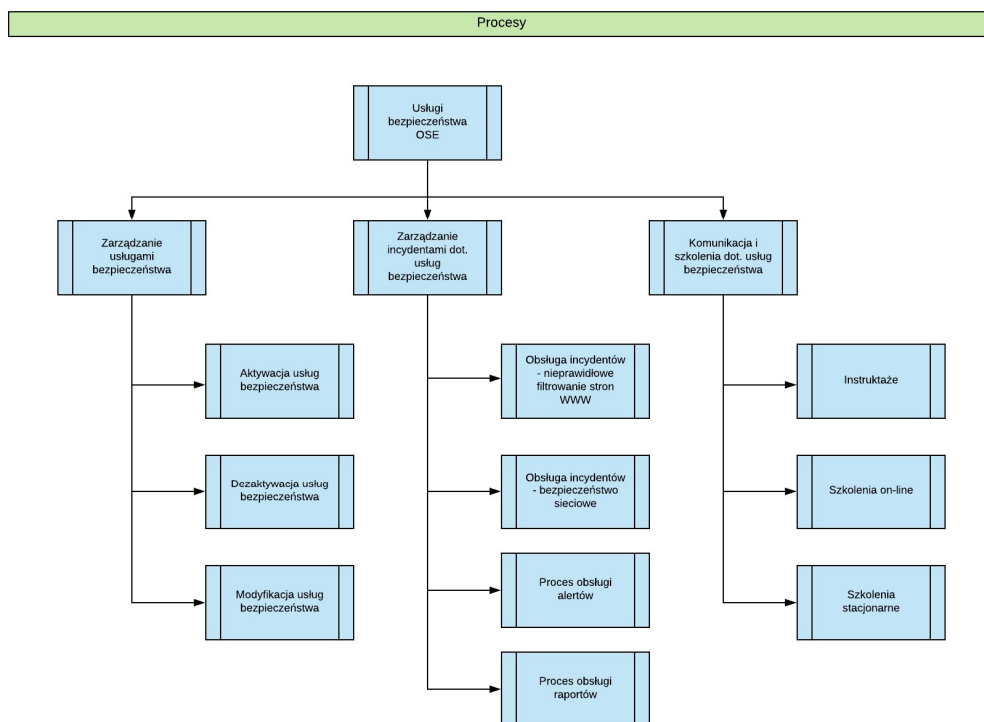
Atrybuty przypisane do szkoły:

Nazwa pola	Przykładowa wartość	Uwagi
id_2016	1000000003643441	w tym zestawieni nie jest to ID unikalne. Wiele szkół na adresie
id_2017	2570340	w tym zestawieni nie jest to ID unikalne. Wiele szkół na adresie
ID_PODMIOT_szkoła RSPO	2874	Unikalne - numer RSPO
TYP_PODMIOTU	Szkoła podstawowa	
TERC	1212062	
WOJEWODZTWO	(12) MAŁOPOLSKIE	
POWIAT	(1212) olkuski	
GMINA	(121206) Trzyciąż Gm	
SIMC	0339916	
MIEJSCOWOSC	Trzyciąż	
ULIC	99999	

Nazwa pola	Przykładowa wartość	Uwagi
ULICA		
NR_DOMU	70	
NR_MIESZKANIA		
KOD_POCZTOWY	32-353	
województwo	MAŁOPOLSKIE	
powiat	OLKUSKI	
gmina	TRZYCIAŹ	
SIMC	0339916	
miejsowość	TRZYCIAŹ	
ULIC	99999	
ULICA		
NR_DOMU	70	
X92	555500	
Y92	271409	
hiperlink lokalizacja		
Data dodania szkoły do systemu		
Data aktywacji łącza w danej szkole		
Data zmiany rekordu		
liczba uczniów		
osobny LAN (tak/nie)		

3.10. Proces zarządzania bezpieczeństwem

Hierarchia procesów biznesowych



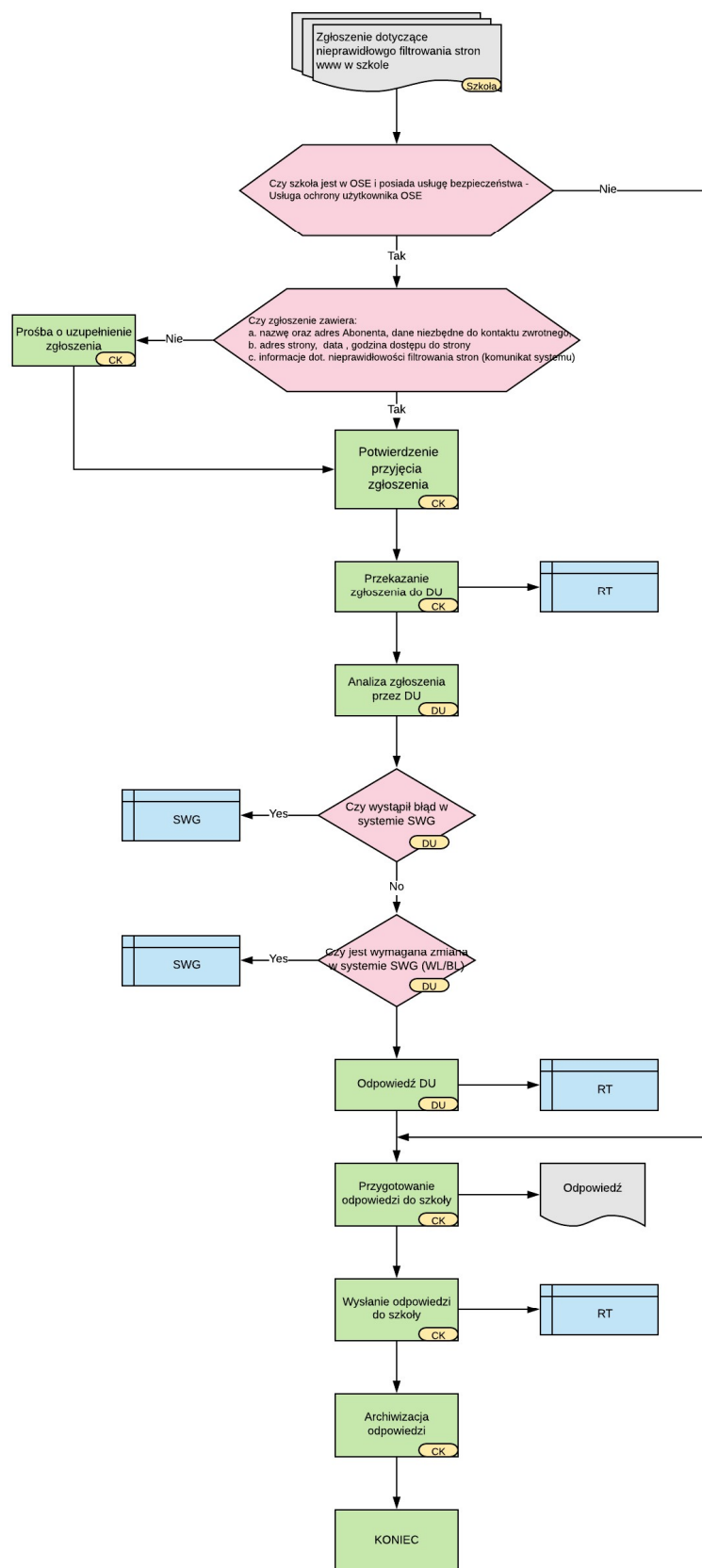
Procesy biznesowe

Proces obsługi zgłoszeń incydentów bezpieczeństwa ze szkół w OSE

Nieprawidłowe filtrowanie stron www (proces zdefiniowany)

Cel procesu	Obsługa incydentów pochodzących ze szkół w OSE związanych z nieprawidłowym filtrowaniem stron www
Inicjacja	Zgłoszenie nieprawidłowego filtrowania strony www
Dane wejściowe	Dane abonenta, adres strony, data i godzina dostępu do strony, informacje dot. nieprawidłowości
Dane wyjściowe	Odpowiedź do szkoły
KPI	Czas obsługi

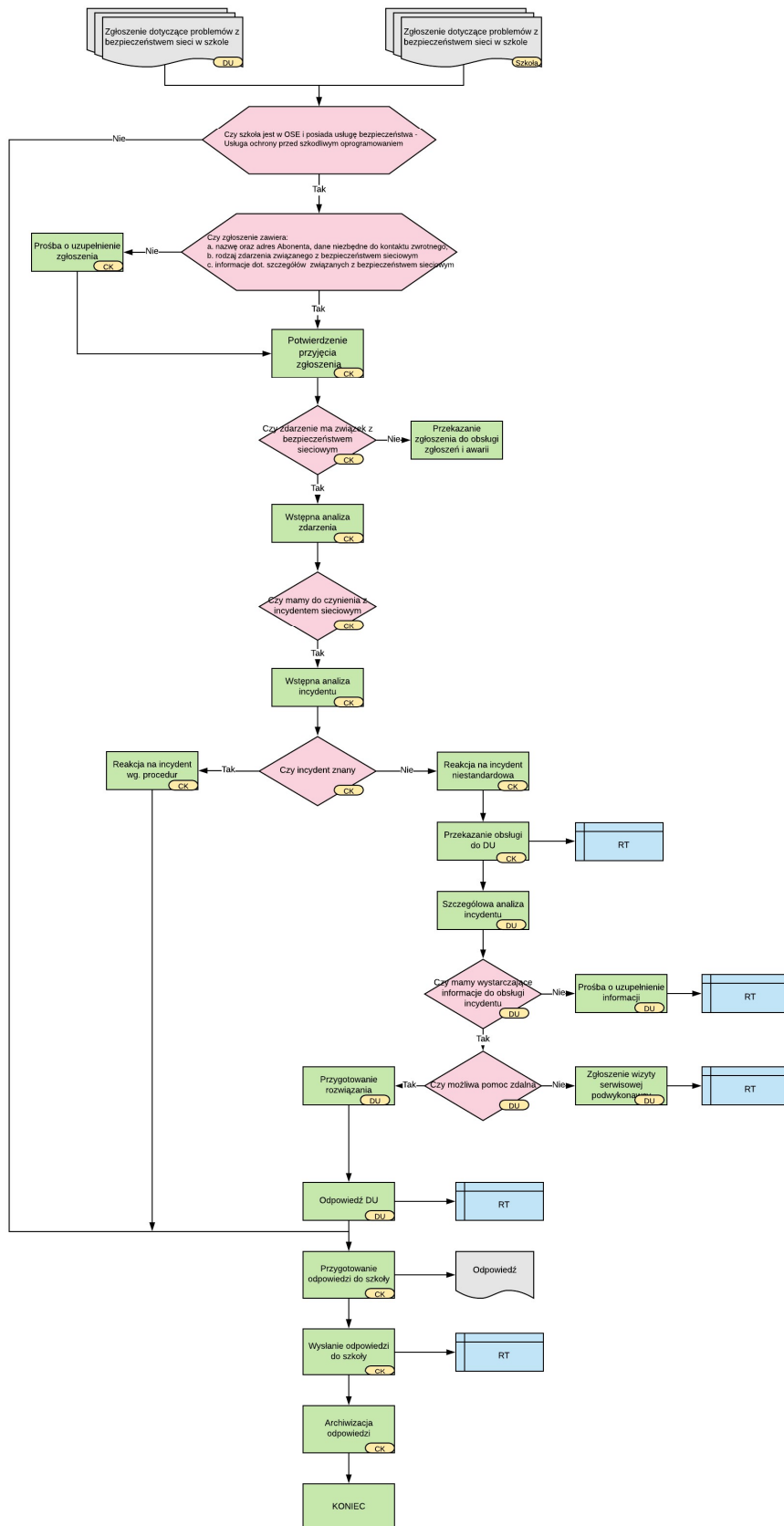
Załącznik nr 1.15 - Diagram procesu obsługi incydentów ze szkół - nieprawidłowe filtrowanie stron WWW



Incydenty sieciowe (proces zdefiniowany)

Cel procesu	Obsługa incydentów pochodzących ze szkół w OSE związanych z bezpieczeństwem sieci w szkole
Inicjacja	Zgłoszenie zdarzenia związanego z bezpieczeństwem sieci w szkole
Dane wejściowe	Dane abonenta, informacje dot. szczegółów nieprawidłowości związanych z bezpieczeństwem sieci
Dane wyjściowe	Odpowiedź do szkoły
KPI	Czas obsługi

Załącznik nr 1.16 - Diagram procesu obsługa incydentów ze szkół - bezpieczeństwo sieciowe



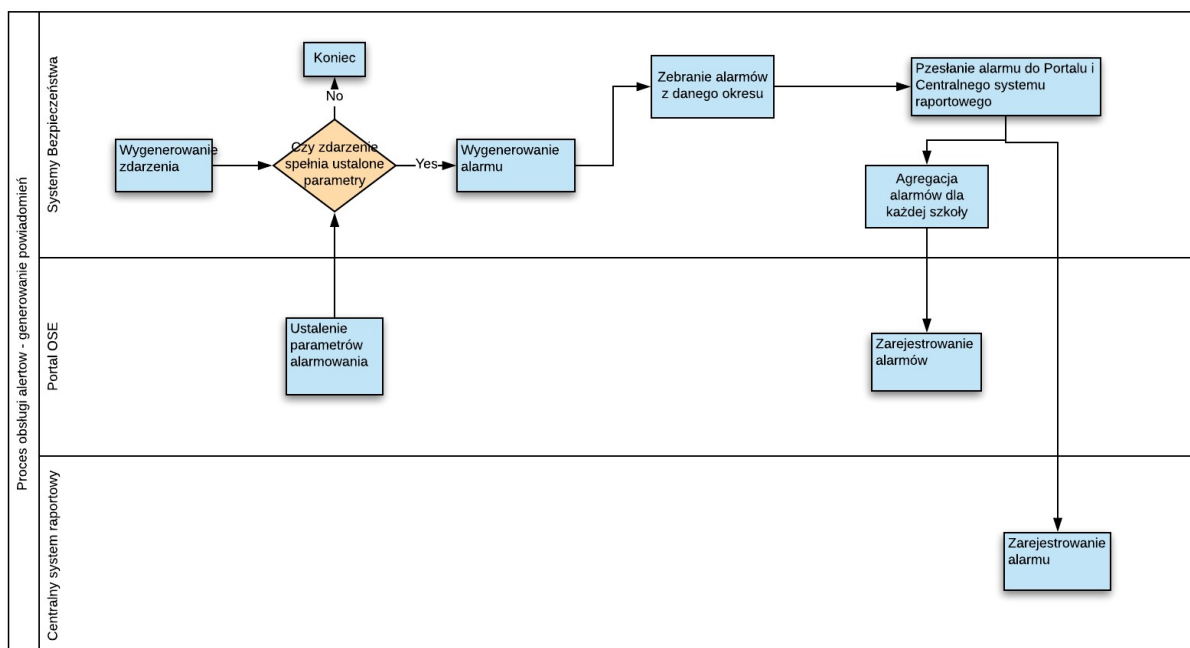
Proces obsługi alertów i raportów

Proces obsługi alertów - generowanie powiadomień (proces zdefiniowany)

Cel procesu	Dostarczanie szkołom informacji dotyczącej przekroczenia ustalonych parametrów ochrony zapewnianych przez usługi bezpieczeństwa
Inicjacja	Ustalenie parametrów powiadomień dotyczących ochrony zapewnianych przez usługi bezpieczeństwa
Dane wejściowe	Zdarzenia pochodzące z systemów bezpieczeństwa OSE
Dane wyjściowe	Alerty na portalu OSE
KPI	Czas obsługi

Diagram procesu

Proces obsługi alertów - generowanie powiadomień



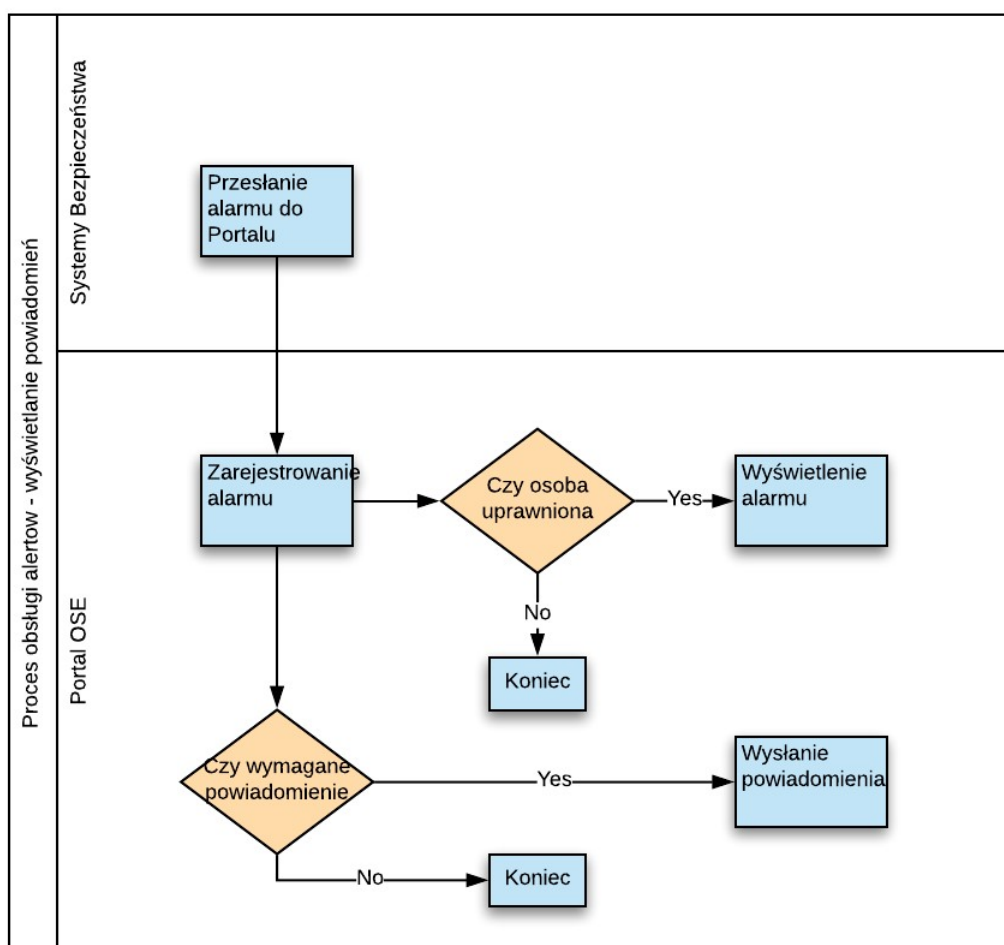
Proces obsługi alertów - wyświetlanie powiadomień (proces zdefiniowany)

Cel procesu	Dostarczanie szkołom informacji dotyczącej przekroczenia ustalonych parametrów ochrony zapewnianych przez usługi bezpieczeństwa
Inicjacja	Ustalenie parametrów powiadomień dotyczących ochrony zapewnianych przez usługi bezpieczeństwa
Dane wejściowe	Zdarzenia pochodzące z systemów bezpieczeństwa OSE

Dane wyjściowe	Alerty na portalu OSE
KPI	Czas obsługi

Diagram procesu

Proces obsługi alertów - wyświetlanie powiadomień



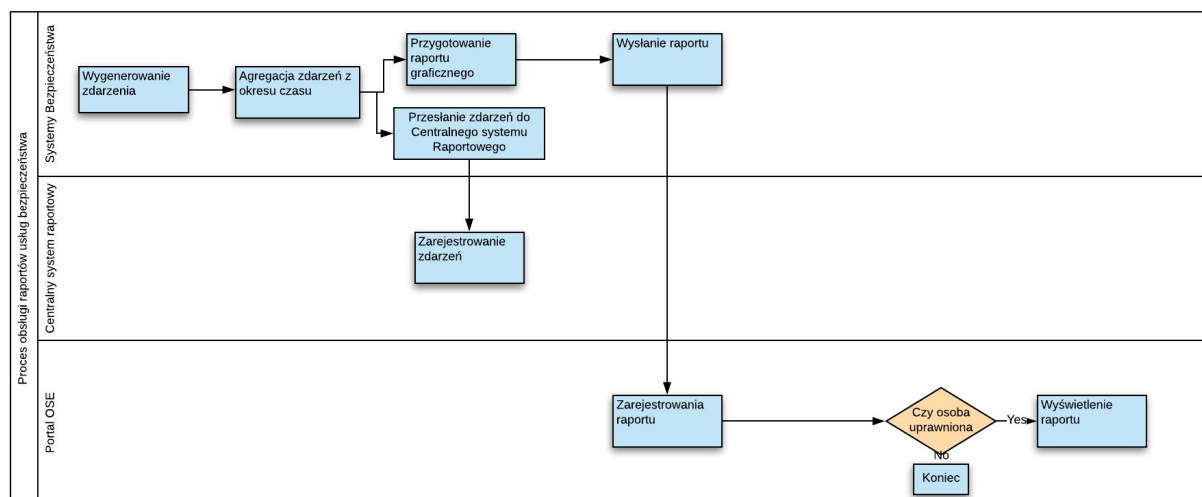
Proces obsługi raportów usług bezpieczeństwa (proces zdefiniowany)

Cel procesu	Dostarczanie szkołom informacji dotyczącej statystyk działania usług bezpieczeństwa
Inicjacja	Ustalenie parametrów dotyczących raportów
Dane wejściowe	Zdarzenia pochodzące z systemów bezpieczeństwa OSE
Dane wyjściowe	Raporty na portalu OSE

KPI	Czas obsługi
-----	--------------

Diagram procesu

Proces obsługi raportów usług bezpieczeństwa



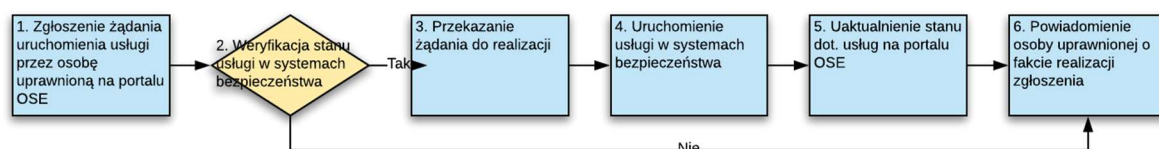
Proces zarządzania produktami bezpieczeństwa

Aktywacja usług bezpieczeństwa OSE (proces zdefiniowany)

Cel procesu	Aktywacja usług bezpieczeństwa OSE przez osobę uprawnioną w szkole
Inicjacja	Zgłoszone żądanie aktywacji usługi bezpieczeństwa OSE
Dane wejściowe	Żądanie aktywacji usługi bezpieczeństwa OSE
Dane wyjściowe	Zmiana statusu dot. usługi na portalu OSE
KPI	Czas obsługi

Diagram procesu

Aktywacja usług bezpieczeństwa OSE



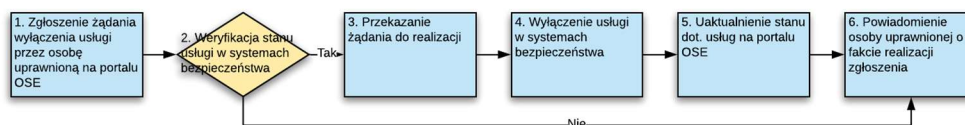
Dezaktywacja usług bezpieczeństwa OSE (proces zdefiniowany)

Cel procesu	Dezaktywacja usług bezpieczeństwa OSE przez osobę uprawnioną w szkole
Inicjacja	Zgłoszone żądanie dezaktywacji usługi bezpieczeństwa OSE

Dane wejściowe	Żądanie dezaktywacji usługi bezpieczeństwa OSE
Dane wyjściowe	Zmiana statusu dot. usługi na portalu OSE
KPI	Czas obsługi

Diagram procesu

Dezaktywacja usług bezpieczeństwa OSE

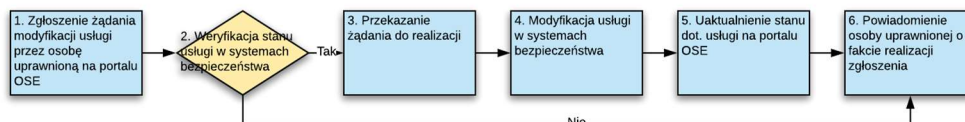


Modyfikacja usługi ochrony użytkownika OSE (proces zdefiniowany)

Cel procesu	Modyfikacja usługi ochrony użytkownika OSE przez osobę uprawnioną w szkole
Inicjacja	Zgłoszone żądanie modyfikacji usługi ochrony użytkownika OSE
Dane wejściowe	Żądanie modyfikacji usługi ochrony użytkownika OSE
Dane wyjściowe	Zmiana statusu dot. usługi na portalu OSE
KPI	Czas obsługi

Diagram procesu

Modyfikacja usługi ochrony użytkownika OSE



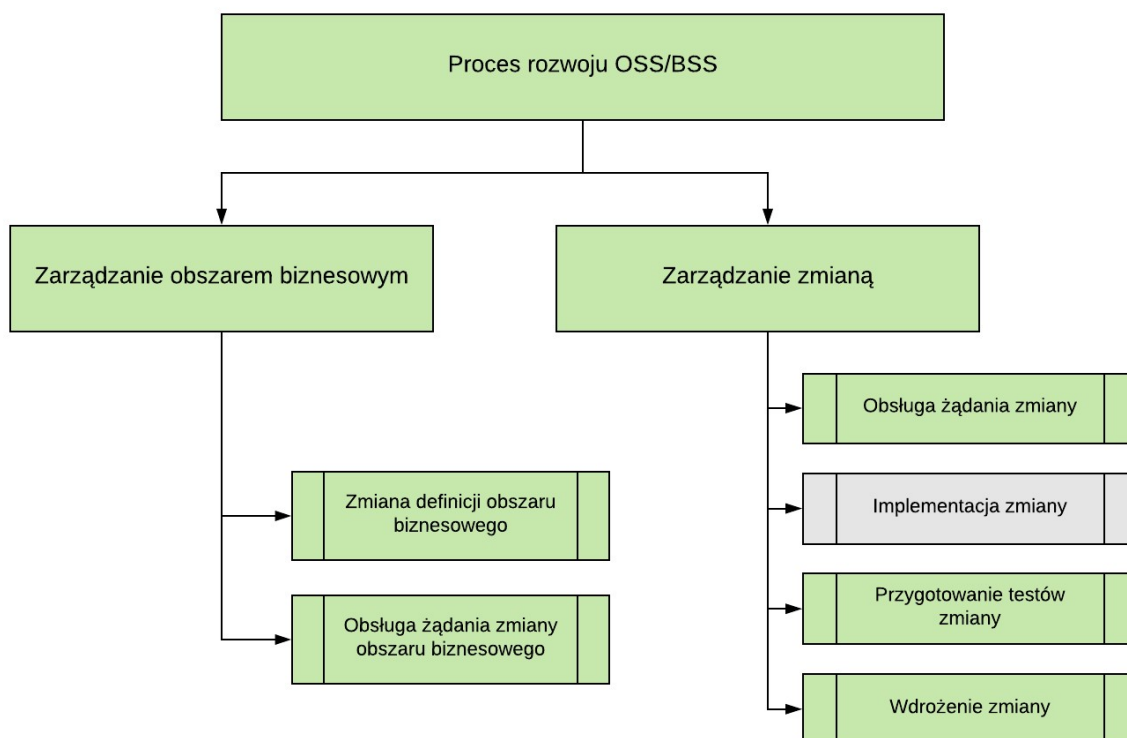
Proces zarządzania komunikacją i szkoleniami dot. usług bezpieczeństwa (proces zdefiniowany)

Cel procesu	Przekaz informacji i wiedzy dotyczącej usług bezpieczeństwa OSE
Inicjacja	Potrzeba przekazania informacji i/lub wiedzy dotyczącej usług bezpieczeństwa OSE
Dane wejściowe	Zmiany dotyczące usług bezpieczeństwa OSE
Dane wyjściowe	Informacje i wiedza dotyczące usług bezpieczeństwa OSE
KPI	Czas obsługi

3.11. Proces rozwoju OSS/BSS

Obszar adresuje zagadnienia związane z procesami dotyczącymi rozwoju Platformy Operatora OSE

Hierarchia procesów biznesowych

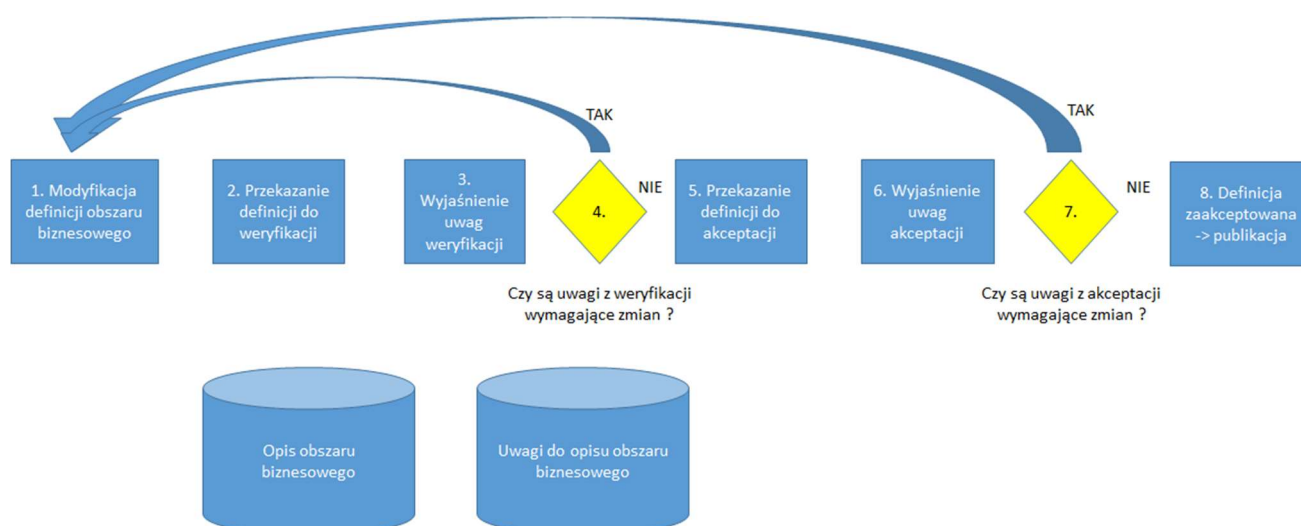


Procesy biznesowe

Zmiana definicji obszaru biznesowego (proces zdefiniowany)

Cel procesu	Zmiana definicji obszaru biznesowego (zmiana zakresu, procesów lub jakichkolwiek innych danych opisujących obszar biznesowy)
Inicjacja	Zaakceptowane żądanie zmiany definicji obszaru biznesowego
Dane wejściowe	Definicja obszaru biznesowego
Dane wyjściowe	Definicja obszaru biznesowego
KPI	Czas akceptacji zmiany - od przedstawienia w status "do akceptacji" (rozpoczęcia procesu akceptacji) do momentu przedstawienia w status zaakceptowany
Wykorzystywane systemy	JIRA, TREE (Confluence)

Diagram procesu



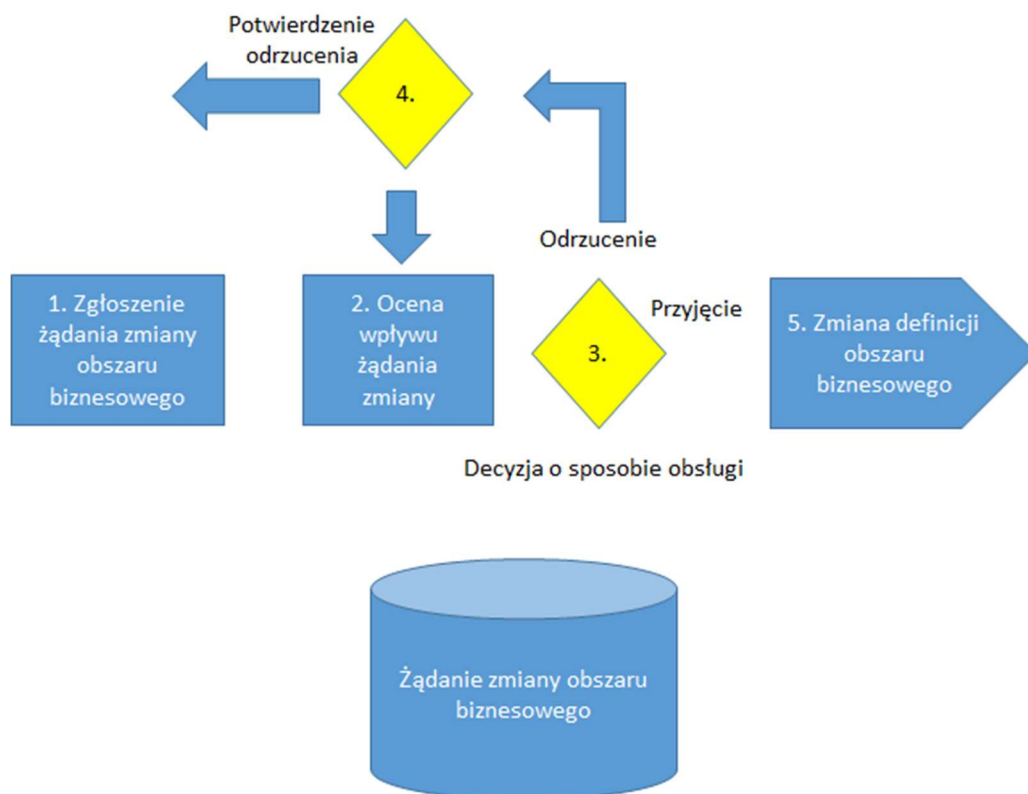
Krok	Opis kroku
1. Modyfikacja definicji obszaru biznesowego	Zmiana definicji obszaru biznesowego realizowana przez właściciela biznesowego w ramach repozytorium → Tree, lub wprowadzenie nowej definicji dla nieistniejącego obszaru biznesowego.
2. Przekazanie definicji do weryfikacji	Zgłoszenie nowej wersji definicji obszaru biznesowego do weryfikacji, wysłanie maila lub zaproszenie na spotkanie osób weryfikujących. Prezentacja definicji i zebranie uwag.
3. Wyjaśnienie uwag weryfikacji	Wyjaśnienie wszystkich uwag zgłoszonych w ramach weryfikacji, dostarczenie odpowiedzi, zaproponowanie modyfikacji bieżącego opisu obszaru biznesowego
4. Czy są uwagi z weryfikacji wymagające zmian	Jeżeli w wyniku weryfikacji konieczne są zmiany należy się cofnąć do kroku modyfikacji definicji obszaru biznesowego, w przeciwnym przypadku można przejść do kolejnego kroku
5. Przekazanie definicji do akceptacji	Wygenerowanie eksportu definicji obszaru biznesowego z repozytorium (tree) do dokumentu WORD. Utworzenie zlecenia JIRA, załączenie eksportu definicji do zlecenia JIRA i przekazanie zlecenia do akceptującego. Umieszczenie linka do zadania akceptacyjnego JIRA na stronie repozytorium (TREE).
6. Wyjaśnienie uwag akceptacji	Zebranie i wyjaśnienie wszystkich uwag wynikających z akceptacji (w JIRA)
7. Czy są uwagi z akceptacji wymagające zmian	Jeżeli uwagi z akceptacji wymagają zmian w definicji obszaru biznesowego należy się cofnąć do kroku modyfikacji definicji obszaru biznesowego, w przeciwnym przypadku można przejść do kolejnego kroku
8. Definicja zaakceptowana → publikacja	Po zaakceptowaniu definicji przez akceptującego, eksport w formacie WORD należy umieścić w repozytorium na stronie głównej dla wszystkich obszarów biznesowych.

Obsługa żądania zmiany obszaru biznesowego (proces zdefiniowany)

Cel procesu	Obsługa uwagi zgłoszonej do zaakceptowanego wcześniej opisu obszaru biznesowego (lub nieistniejącego - inicjalne żądanie zmiany)
--------------------	--

Inicjacja	Zgłoszona uwaga / żądanie zmiany definicji obszaru biznesowego
Dane wejściowe	Żądanie zmiany obszaru biznesowego
Dane wyjściowe	
KPI	Czas obsługi żądania zmiany - od zgłoszenia żądania zmiany / uwagi do momentu przyjęcia lub odrzucenia
Wykorzystywane systemy	JIRA, TREE (Confluence)

Diagram procesu



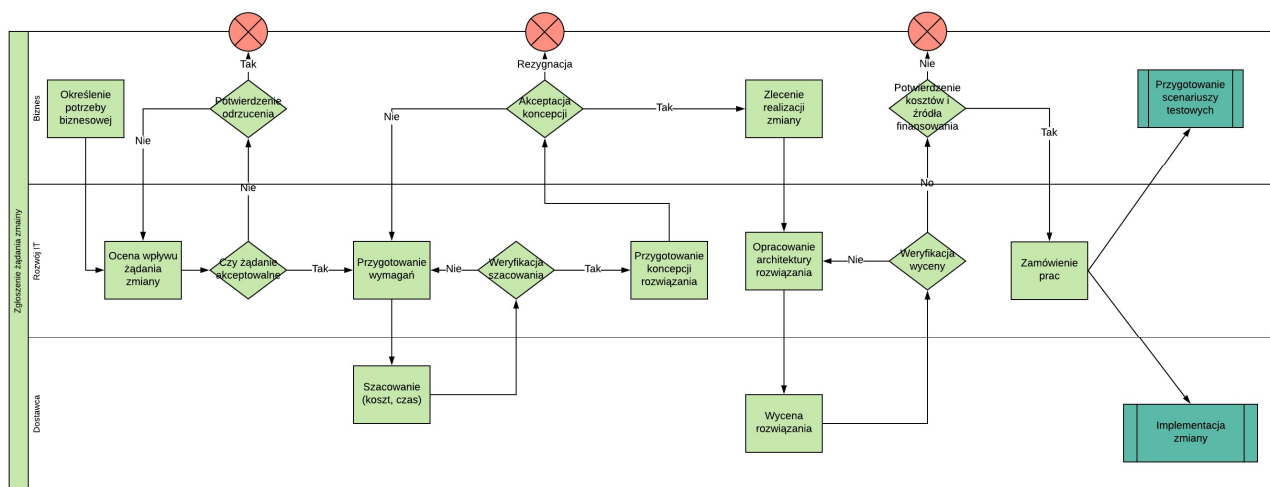
Krok	Opis kroku
1. Zgłoszenie żądania zmiany obszaru biznesowego	Wprowadzenie zgłoszenia żądania modyfikacji definicji obszaru biznesowego do systemu JIRA przez zgłaszającego. W zgłoszeniu powinny być informacje określające cel realizacji zmiany, co jest do zmiany, korzyści wynikające z modyfikacji, oraz w miarę możliwości oszacowanie kosztów realizacji zmiany.
2. Ocena wpływu żądania zmiany	Zgłoszenie trafia do właściciela biznesowego, który analizuje wpływ zmian. Ocenia wartość wynikającą ze zmiany, określa czas wymagany do realizacji zmiany oraz potencjalne koszty (dotyczące również zmian w aplikacjach). Szacowanie kosztów powinno zawierać zarówno koszty finansowe, zaangażowania zasobów oraz czasu koniecznego do realizacji zmiany.
3. Decyzja o sposobie obsługi	Właściciel biznesowy podejmuje decyzję o ewentualnej realizacji żądania zmiany (przejdzie do kolejnego kroku w realizacji) lub odrzuca żądanie zmiany (przejdzie do kroku potwierdzenia odrzucenia)

Krok	Opis kroku
4. Potwierdzenie odrzucenia	Akceptujący dla obszaru biznesowego potwierdza odrzucenie żądania zmiany, bądź zgłasza uwagi do analizy oceny wpływu cofa żądanie zmiany ponownie do kroku oceny wpływu żądania zmiany
5. Zmiana definicji obszaru biznesowego	Żądanie zmiany zostaje przekazane do procesu <u>Zmiany definicji obszaru biznesowego</u>

Obsługa żądania zmiany (proces zdefiniowany)

Cel procesu	Obsługa biznesowego żądania zmiany
Inicjacja	Żądanie dostarczenia / zmiany funkcjonalności biznesowej
Dane wejściowe	Zbiór wymagań dla żądania zmiany
Dane wyjściowe	
KPI	Czas obsługi żądania zmiany - od zgłoszenia żądania zmiany do pozytywnego zakończenia testów akceptacyjnych

Diagram procesu

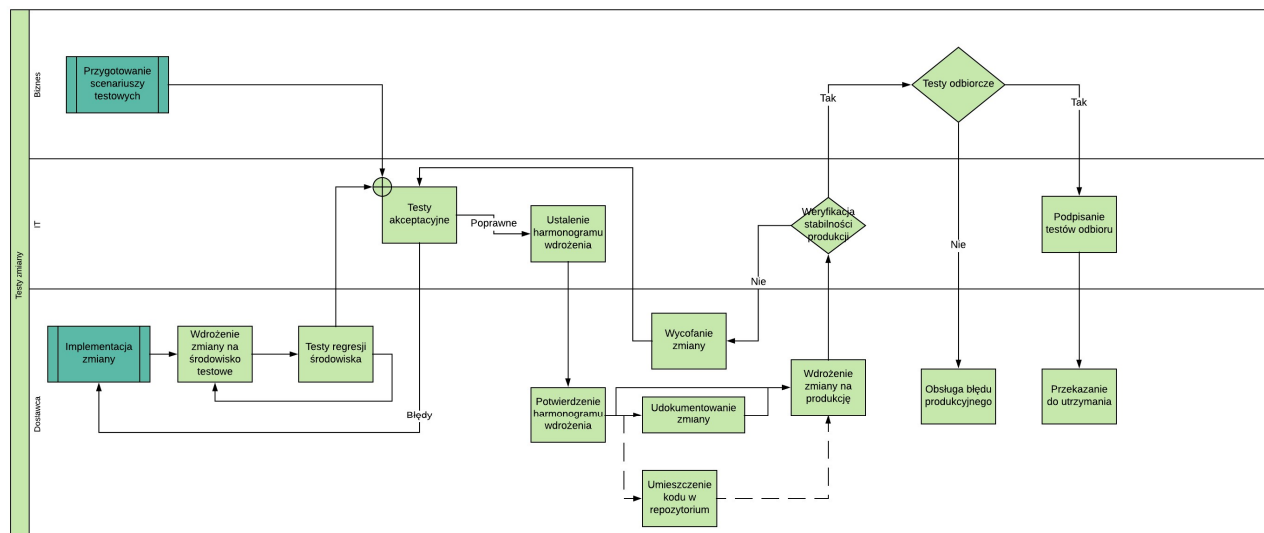


Wdrożenie zmiany (proces zdefiniowany)

Cel procesu	Wdrożenie zmiany na produkcję
Inicjacja	Implementacja zmiany, przygotowanie scenariuszy testowych
Dane wejściowe	Scenariusze testowe
Dane wyjściowe	

KPI	Jakość dostarczonego rozwiązania = $\frac{\text{Liczba scenariuszy testów akceptacyjnych}}{(\text{Liczba podejść do testów akceptacyjnych} * \text{Suma dla wszystkich podejść} (\text{nr testu akceptacyjnego} * (\text{ilość błędu w danym podejściu testowym} + 1)))}$
------------	---

Diagram procesu



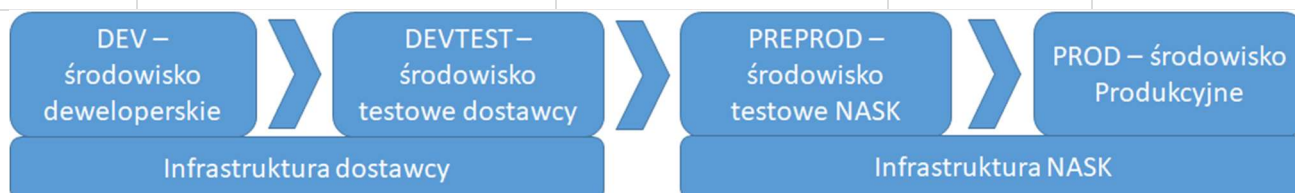
Zarządzanie środowiskami IT (proces zdefiniowany)

Cel procesu	Zarządzania środowiskami IT na potrzeby rozwoju i utrzymania Platformy Operatora OSE
--------------------	--

Środowiska

Środowisko	Definicja	Integracja z siecią	Lokalizacja	Odpowiedzialność
Środowisko deweloperskie (DEV)	Środowisko służące do rozwoju oprogramowania, zawierające wyłącznie systemy dostawcy oprogramowania. Po stronie dostawcy jest zaślepienie integracji z otoczeniem oraz przygotowanie symulacji wywołań z systemów nienależących do jego środowiska	Brak sieci	Infrastruktura dostawcy oprogramowania	Dostawca oprogramowania
Środowisko testów wewnętrznych (DEVTEST)	Środowisko służące do testów po stronie dostawcy, nie zawierające systemów innych dostawców. Po stronie dostawcy jest zaślepienie integracji z otoczeniem oraz przygotowanie symulacji wywołań z systemów nienależących do jego środowiska.	Brak sieci	Infrastruktura dostawcy oprogramowania	Dostawca oprogramowania
Środowisko testów	Środowisko służące realizacji testów akceptacyjnych. Zawierające wersje	Na potrzeby testów można wykorzystać TestLab, po	Infrastruktura NASK	Firma utrzymująca oprogramowanie

Środowisko	Definicja	Integracja z siecią	Lokalizacja	Odpowiedzialność
akceptacyjnych (PREPROD)	testowe systemów o ile istnieją. Środowisko nie jest zintegrowane z siecią (integracja będzie przygotowywane w incydentalnych przypadkach). Po stronie dostawcy POOSE jest przygotowanie emulatorów/symulatorów dla systemów niewystępujących w środowisku testowym.	wcześniejszych ustaleniach. Dla bardziej złożonych testów należy zestawić połączenie z produkcyjną siecią poprzez interfejs z tzw. WhiteList, który będzie przepuszczał wywołania do sieci jedynie dla wskazanych (skonfigurowanych) numerów / lokalizacji.		
Środowisko produkcyjne (PROD)	Środowisko zapewniające produkcyjne działanie systemów, w pełni zintegrowane.	Pełna integracja z siecią oparta o mechanizm tzw. BlackList - lokalizacje testowe, dla których wywołania nie będą wysyłane do sieci.	Infrastruktura NASK	Firma utrzymująca oprogramowanie

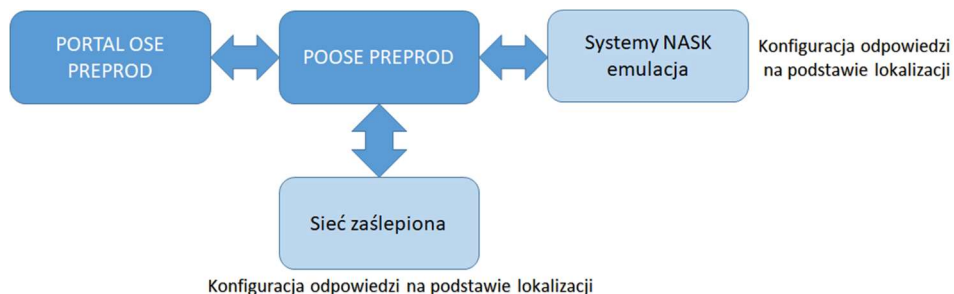


Warianty realizacja testów akceptacyjnych

Na środowisku produkcyjnym (PROD) należy zapewnić konfigurację testowego partnera serwisowego oraz testowego operatora dostępowego (np. NASK TEST, z kontem pocztowym NASK), aby umożliwić realizację testów bez konieczności angażowania zasobów spoza NASK.

Na środowisku testowym (PREPROD) należy zapewnić skonfigurowanie testowych operatorów (z adresami email w NASK), aby umożliwić realizację testów bez konieczności angażowania zasobów spoza NASK.

Wariant 1. minimalny



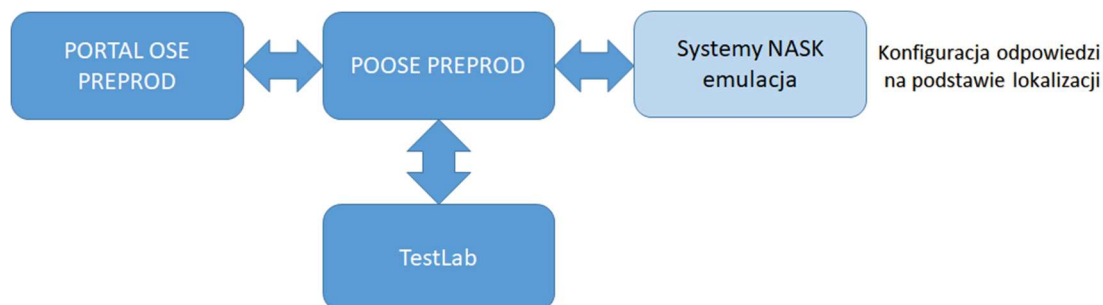
Ustawienia konfiguracji

Zmienna	Wartość
Environment	Test

Ustawienia konfiguracji

Network	None
---------	------

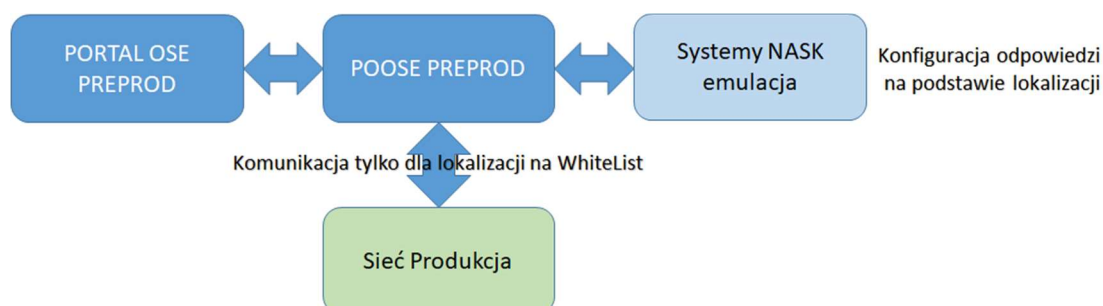
Wariant 2. z TestLab



Ustawienia konfiguracji

Zmienna	Wartość
Environment	Test
Network	Test

Wariant 3. z siecią produkcyjną



Ustawienia konfiguracji

Zmienna	Wartość
Environment	Test
Network	Prod

Wariant 4. testy produkcyjne



Ustawienia konfiguracji	
Zmienna	Wartość
Environment	Prod
Network	Prod

Emulatory systemów na potrzeby środowiska testów akceptacyjnych

W celu umożliwienia realizacji testów akceptacyjnych należy przygotować narzędzia symulujące działanie systemów niewystępujących w środowisku.

Dla każdej integracji wychodzącej z POOSE należy przygotować odpowiednią symulację wywołań pozwalającą na skonfigurowanie odpowiedzi w następujący sposób:

- Dla każdej integracji powinien istnieć identyfikator (np. lokalizacja)
- Musi być możliwe skonfigurowanie odpowiedzi w ramach każdego wywołania dla wybranego identyfikatora (np. dla lokalizacji A odpowiedź poprawna, parametry X,Y; dla lokalizacji B odpowiedź negatywna parametr Z; itp.)
- Musi być możliwe skonfigurowanie odpowiedzi domyślnej dla przypadków wywołań z identyfikatorem niewystępującym w konfiguracji

Dla każdej integracji przychodzącej do POOSE musi być możliwe przygotowanie wzorca wywołania z możliwością podmiany identyfikatora w wywołaniu.

Zarządzanie dokumentacją architektury IT (proces zdefiniowany)

Cel procesu	Zarządzania dokumentacją architektury IT na potrzeby rozwoju i utrzymania Platformy Operatora OSE
--------------------	---



Do udokumentowania POOSE należy wykorzystać TREE (Confluence NASK PIB). Do zamodelowania architektury POOSE należy wykorzystać narzędzie SPARX Enterprise Architect zapewniając jednocześnie jego integrację z TREE, tak, aby wszelkie zmiany w modelach powodowały aktualizację dokumentacji na TREE.

Model danych

Obiekt	Definicja obszaru biznesowego
Fiszka obszaru biznesowego	[Typ złożony] Metryka opisująca w sposób jednoznaczny obszar biznesowy
Wymagania obszaru biznesowego	[Typ złożony] Wymagania dla wskazanego obszaru biznesowego określające sposób realizacji procesów będących w zakresie prac

Obiekt	Fiszka obszaru biznesowego
Nazwa	Jednoznaczna nazwa obszaru zgodnie z przygotowanym wcześniej podziałem
Właściciel biznesowy	Osoba odpowiedzialna za obszar
Data aktualizacji	Data ostatniej zmiany statusu
Status	Obecny status opisu obszaru (Roboczy / W akceptacji / Zaakceptowany)
Weryfikujący	Osoby weryfikujące zakres i koncepcje dotyczące obszaru biznesowego
Akceptujący	Osoby odpowiedzialne za akceptację zakresu, wymagań i procesów dla obszaru
Data akceptacji	Data ostatniej akceptacji opisu obszaru biznesowego
Zakres	Zakres pokrycia funkcjonalnego obszaru zgodnie z przygotowanym wcześniej podziałem
Lista procesów	Lista procesów realizowanych w ramach obszaru

Obiekt	Wymaganie obszaru biznesowego
Diagramy procesów biznesowych	schemat dla każdego procesu (uwzględniając role i ograniczenia) wraz z określeniem KPI
Struktura danych	opis struktur danych wykorzystywanych w ramach każdego z procesów (z określeniem danych wejściowych i wyjściowych dla procesów)
Raporty	opisanie wymagań raportowych dla poszczególnych procesów
Wymagania funkcjonalne	wymagania funkcjonalne właściwe dla obszaru biznesowego
Wymagania нефункционалне	pozostałe wymagania (niefunkcjonalne) dla obszaru biznesowego

Obiekt	Uwaga do opisu obszaru biznesowego
Nr.	Unikalny numer porządkowy uwagi
Nazwa	Ogólna nazwa (nagłówek) uwagi
Wskazanie do definicji	Wskazanie elementu definicji, do którego odnosi się uwaga

Obiekt	Uwaga do opisu obszaru biznesowego
Treść	Treść uwagi do opisu obszaru biznesowego
Status	Status uwagi (Zgłoszona, W trakcie, Odrzucona, Rozwiązana, Zamknięta)
Data zgłoszenia	Data zgłoszenia uwagi
Data zmiany statusu	Ostatnia data zmiany statusu

Obiekt	Raport
Nazwa	Jednoznaczna nazwa raportu
Procesy	Lista procesów, dla jakich raport jest przygotowywany
Dane	Lista pól wraz z opisem dla raportu (oraz ewentualne formuły dla wyliczeń)
Format	Forma prezentacji raportu

Obiekt	Żądanie zmiany obszaru biznesowego
Numer	Unikalny numer żądania zmiany w formacie ZZ.O.X gdzie O jest numerem obszaru a X jest kolejnym numerem żądania zmiany
Nazwa	Nazwa żądania zmiany obszaru biznesowego
Zgłaszający	Zgłaszający żądanie zmiany obszaru biznesowego
Data zgłoszenia	Data zgłoszenia żądania zmiany
Status	Status żądania zmiany (Zgłoszone, W trakcie, Zakończone, Odrzucone)
Data zmiany statusu	Ostatnia zmiana daty statusu żądania zmiany
Obszar	Obszar biznesowy, którego dotyczy żądanie zmiany
Przypisany	Osoba przypisana do żądania zmiany
Treść	Treść żądania zmiany
Wpływ	Ocena wpływu na projekt z podziałem na dwie składowe - harmonogram i budżet

3.12. Proces wsparcia OSE

Hierarchia procesów biznesowych

Umowy kosztowe nie PZP, podNASK (proces wdrożony)

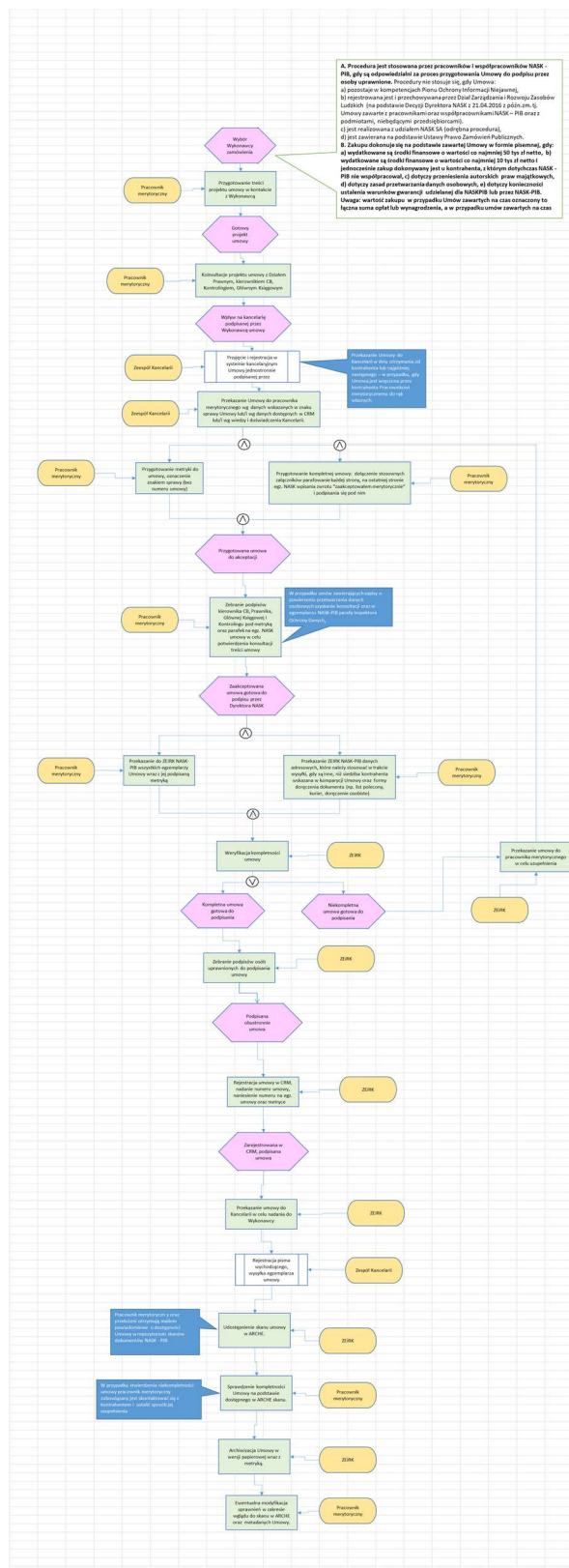
Cel procesu	Obsługa umów kosztowych nie PZP, podNASK
Inicjacja	
Dane wejściowe	
Dane wyjściowe	

Załącznik nr 1.18 - Diagram procesu obsługa umów kosztowych niePZP podNASK

Proces wdrożony (diagram poglądowy)

Załącznik nr 1.19 - Diagram procesu obsługa umów kosztowych niePZP nieNASK

Proces wdrożony (diagram poglądowy)

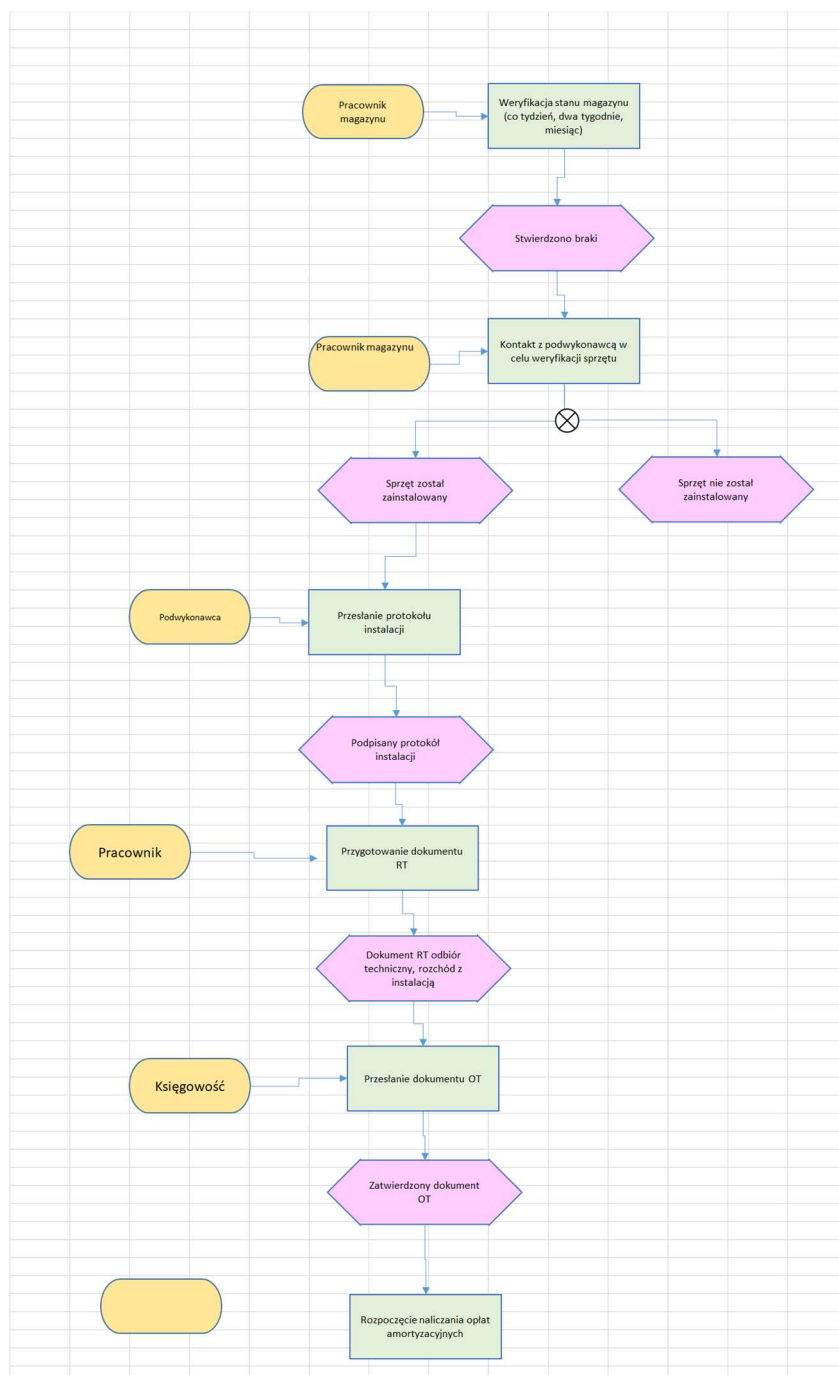


Przyjęcie środka trwałego (proces wdrożenia)

Cel procesu	Obsługa przyjęcia środka trwałego
Inicjacja	
Dane wejściowe	
Dane wyjściowe	

Załącznik nr 1.20 - Diagram procesu obsługa przyjęcia środka trwałego

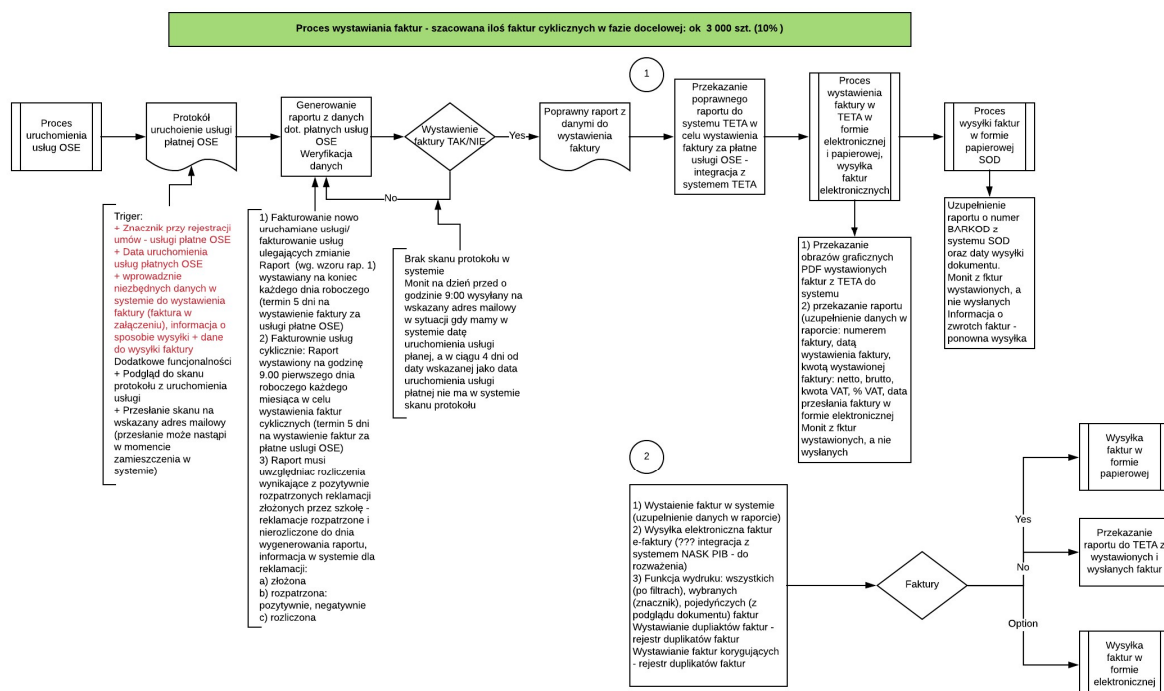
Proces wdrożony (diagram poglądowy)



Faktury przychodowe (proces wdrożony)

Cel procesu	Obsługa faktur przychodowych
Inicjacja	
Dane wejściowe	
Dane wyjściowe	

Diagram procesu



Proces windykacji przedsądowej (proces zdefiniowany)

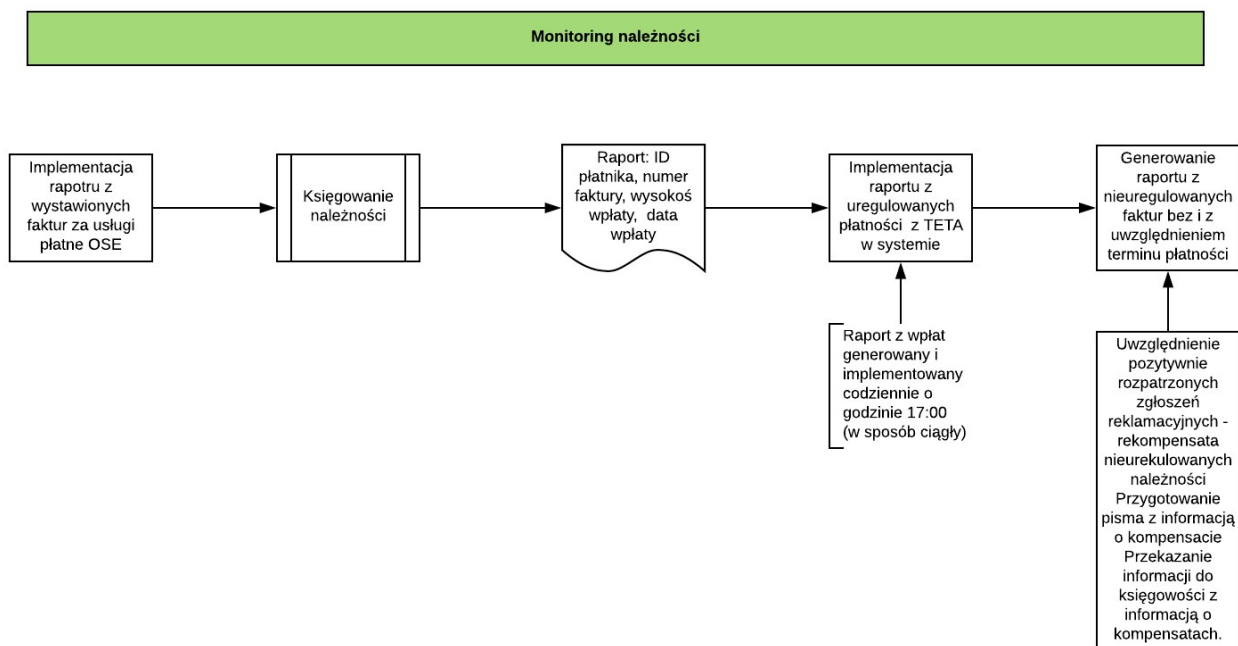
Cel procesu	Realizacja procesu windykacji przedsądowej
Inicjacja	
Dane wejściowe	
Dane wyjściowe	

Diagram procesu

Proces monitoring należności (proces zdefiniowany)

Cel procesu	Monitorowanie rozliczeń
Inicjacja	
Dane wejściowe	
Dane wyjściowe	

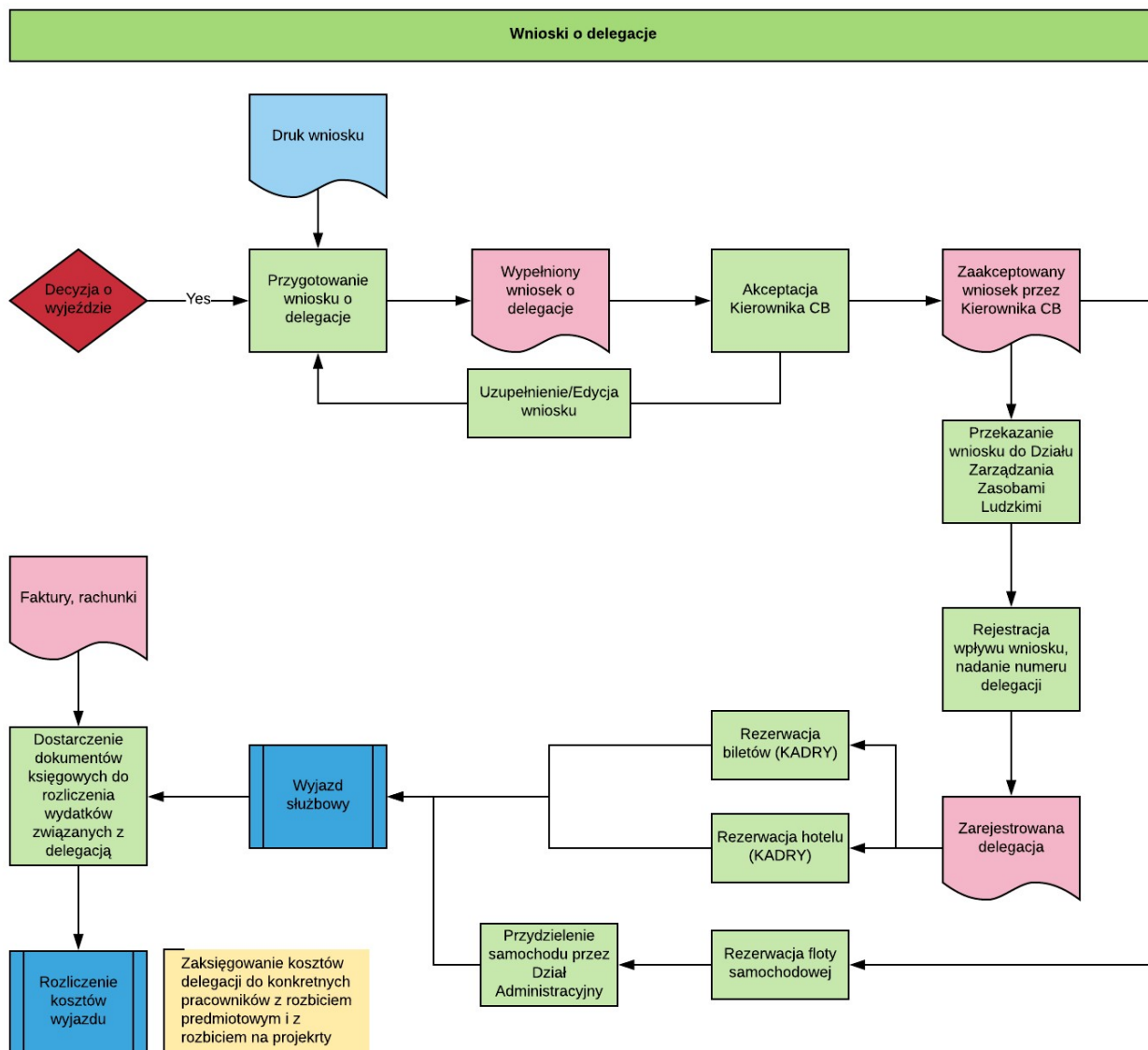
Diagram procesu



Proces wnioski o delegację (proces zdefiniowany)

Cel procesu	Przyjmowanie i obsługa wniosków o delegację
Inicjacja	
Dane wejściowe	
Dane wyjściowe	

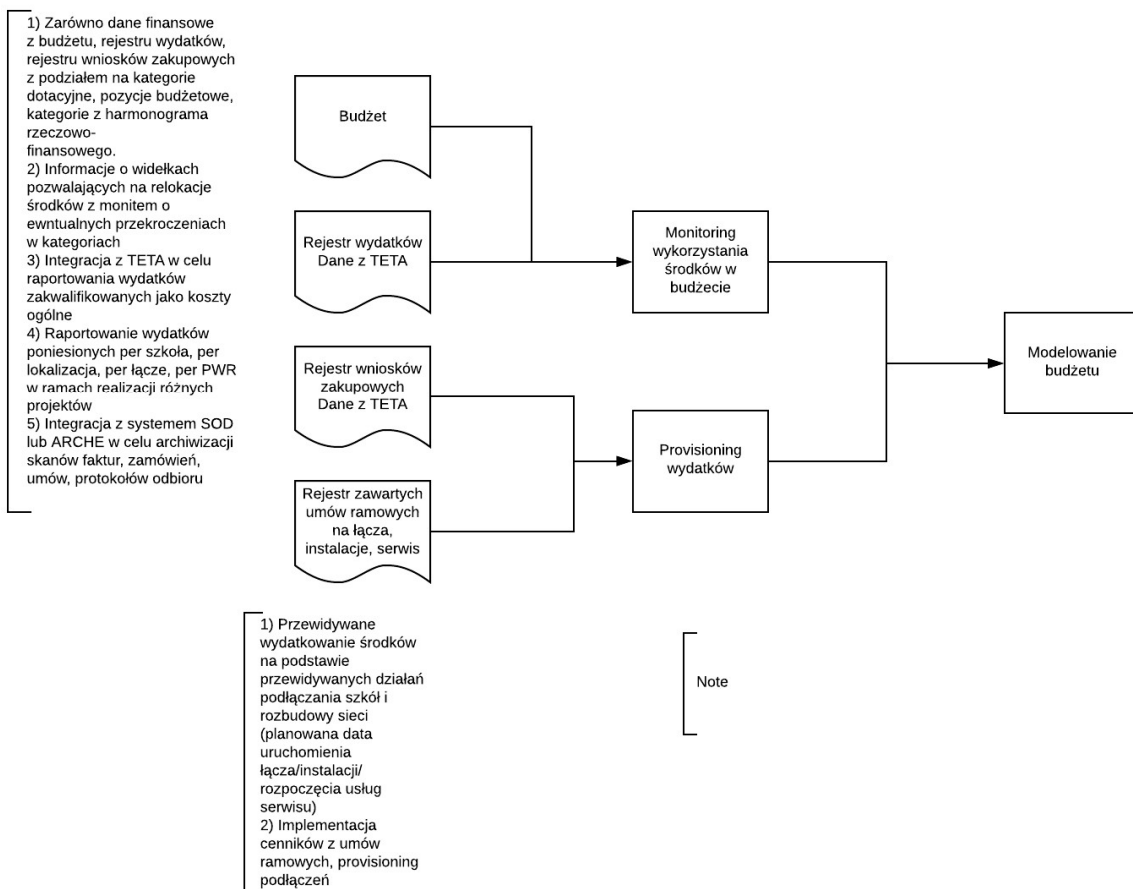
Diagram procesu



Proces monitorowanie budżetu (proces zdefiniowany)

Cel procesu	Raportowanie, monitorowanie budżetu, alokacja wydatków
Inicjacja	
Dane wejściowe	
Dane wyjściowe	

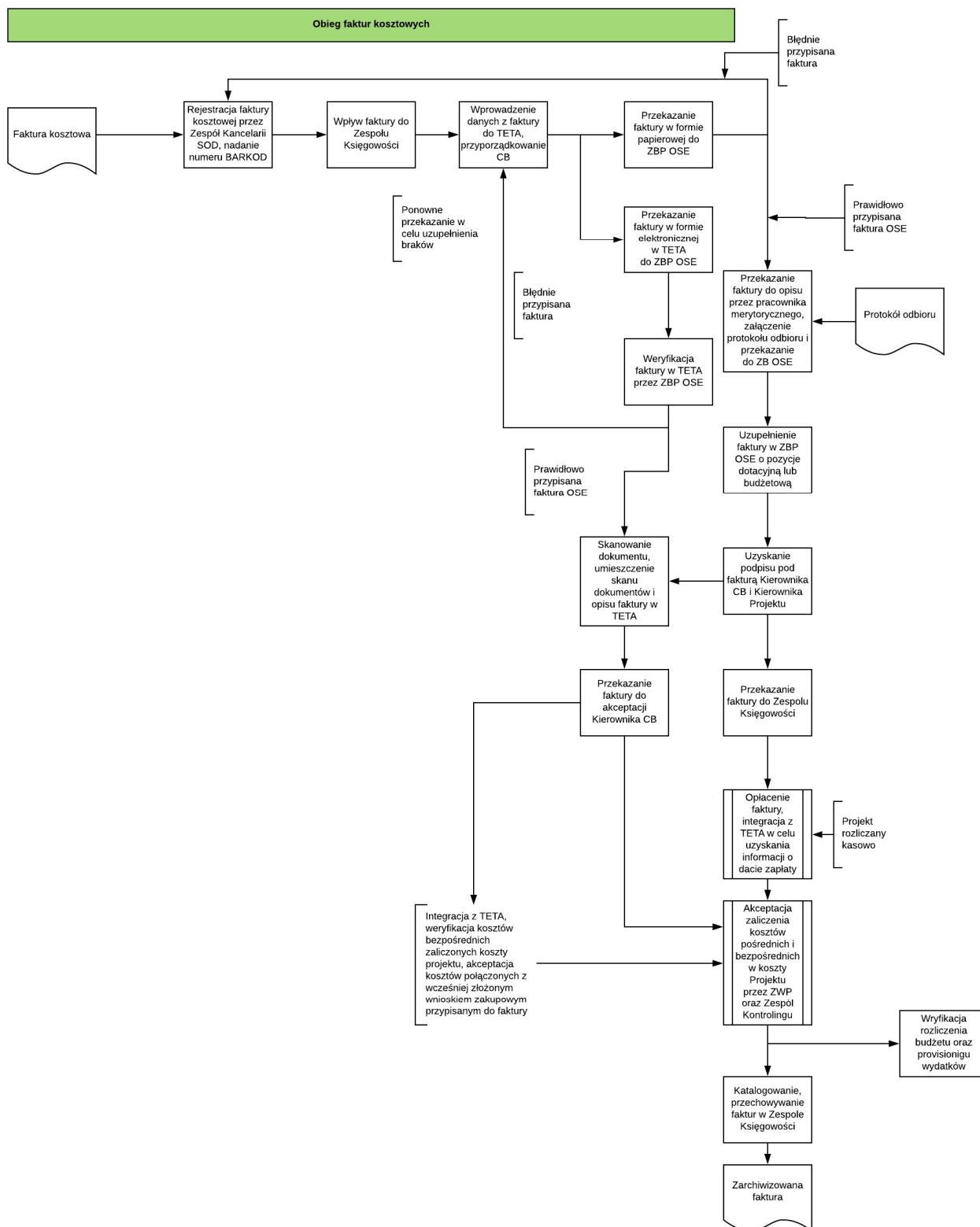
Diagram procesu



Proces obsługa faktur kosztowych (proces zdefiniowany)

Cel procesu	Obsługa faktur kosztowych
Inicjacja	
Dane wejściowe	
Dane wyjściowe	

Diagram procesu



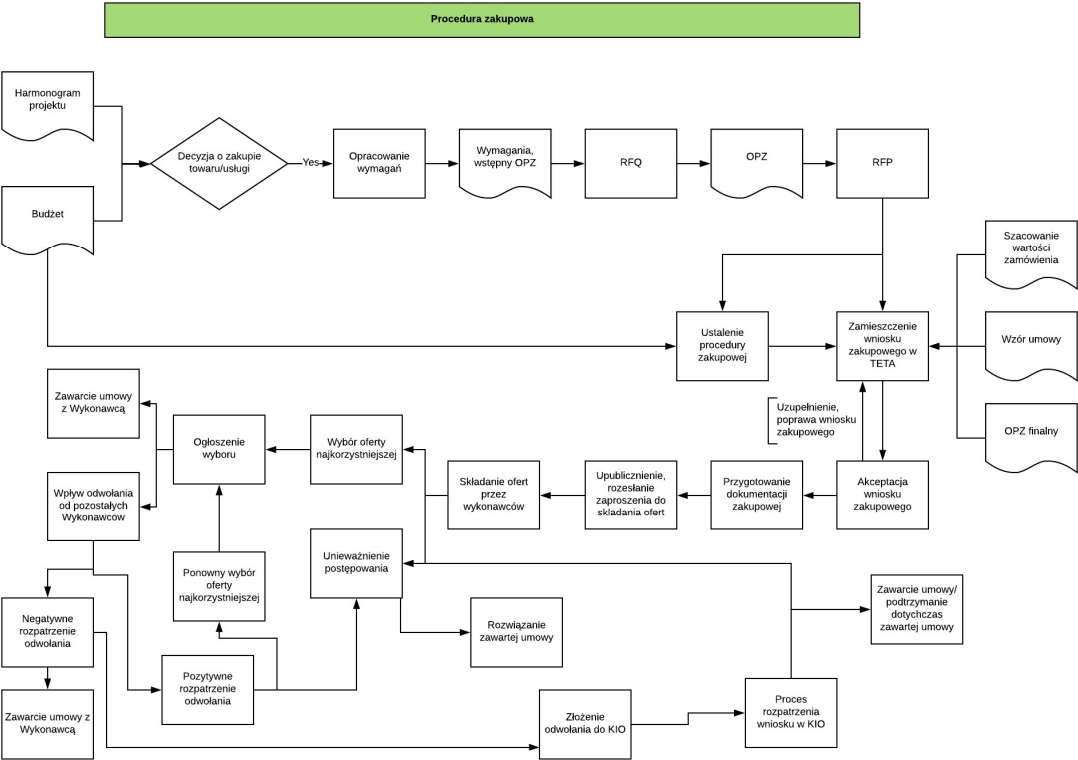
Proces procedura zakupowa (proces zdefiniowany)

Cel procesu

Obsługa zakupów

Inicjacja	
Dane wejściowe	
Dane wyjściowe	

Diagram procesu

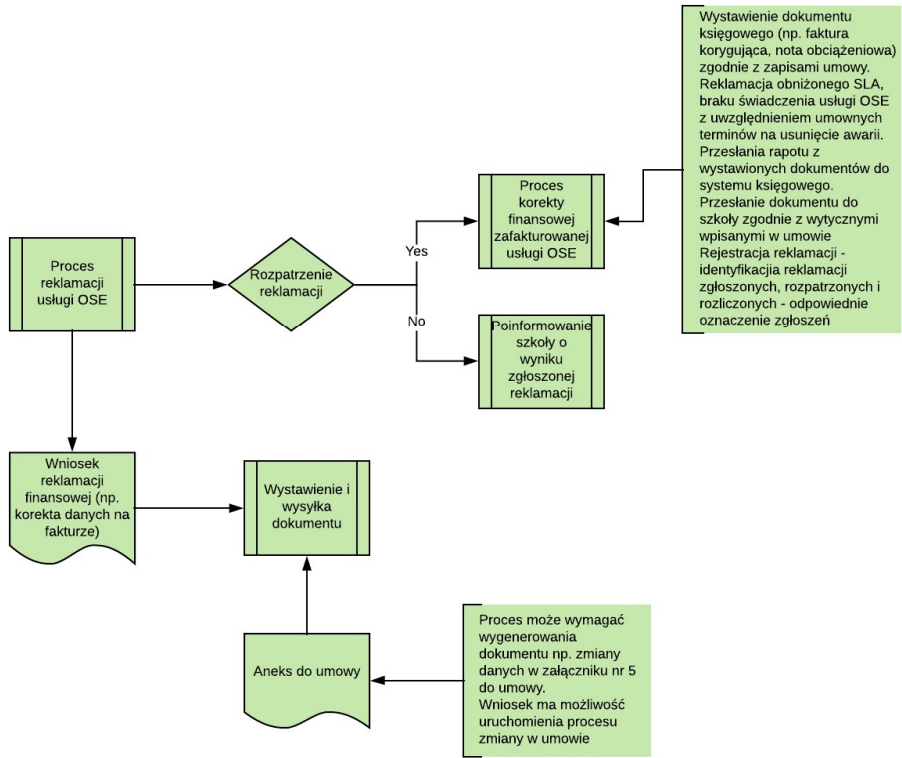


Proces zamówienia na dostawę sprzętu (proces zdefiniowany)

Cel procesu	Zamawiania sprzętu
Inicjacja	
Dane wejściowe	
Dane wyjściowe	

Diagram procesu

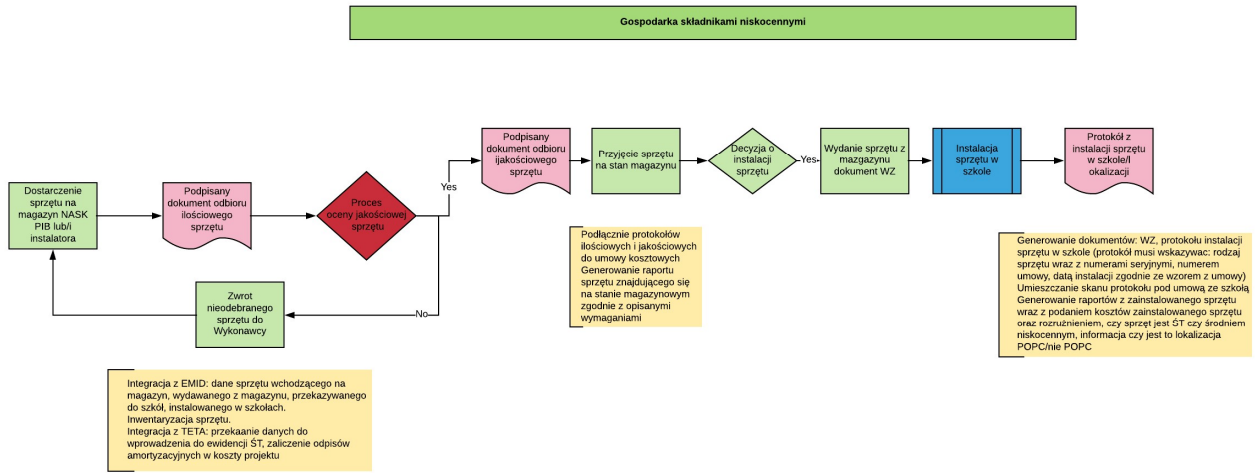
Reklamacja usługi OSE, a dokumenty finansowe



Proces gospodarka składnikami niskocennymi (proces zdefiniowany)

Cel procesu	Obsługa niskocennych materiałów / sprzętów
Inicjacja	
Dane wejściowe	
Dane wyjściowe	

Diagram procesu



Model danych

W okresie przejściowym dla Umów Przychodowych zawartych ze Szkołami w ramach projektu OSE na etapie konwersji Szansy w Umowę należy wprowadzić metadane:

Kontrahent	(wypełniony automatycznie z Szansy)
Przedmiot umowy	Usługi dla Szkół_OSE
Typ umowy	Przychodowe telekomunikacyjne TDG
Kategoria	Szkoły OSE
Data zawarcia	(data zawarcia z treści umowy)
Okres obowiązywania	czas nieokreślony (jeśli tak zawierane są umowy)
Strona Umowy	NASK PIB (alternatywą jest NASK SA lub NASK PIB/SA - tu nie dotyczy)
Obsługa w	NASK PIB
Opiekun umowy	Osoba odpowiedzialna za zawarcie i realizację Umowy, czyli wskazani pracownicy Centrum Kontakt, którzy będą konwertować Szanse w Umowę i wypełniać powyższe metadane dot. Umowy

Pola, które wypełnia ZEIRK

Obowiązuje od	data wprowadzona na podstawie otrzymanej w oryginale obustronnie podpisanej umowy i protokołu - w niektórych przypadkach tj. powyżej 100Mbps powstaje faktura
Data doręczenia do NASK	data dostarczenia do NASK - Kolska obustronnie podpisanej umowy w oryginale
Data doręczenia do ZEIRK	data dostarczenia umowy do Zespołu ZEIRK
Znak sprawy	

3.13. Proces marketingu i komunikacji

Obszar adresuje zagadnienia związane ze wsparciem działań związanych z zarządzaniem marką takich jak marketing i komunikacja

Procesy biznesowe

Zarządzanie szablonem komunikacji mailowej

Cel procesu	Konfiguracja stopki dla wiadomości email wysyłanych w ramach procesów operatora OSE
Inicjacja	Przygotowanie nowej wersji stopki dla wiadomości email

Dane wejściowe	
Dane wyjściowe	
KPI	Czas od aktywacji nowej wersji stopki w konfiguracji do jej gotowości wysyłania w komunikacji mailowej

4. Sieć OSE

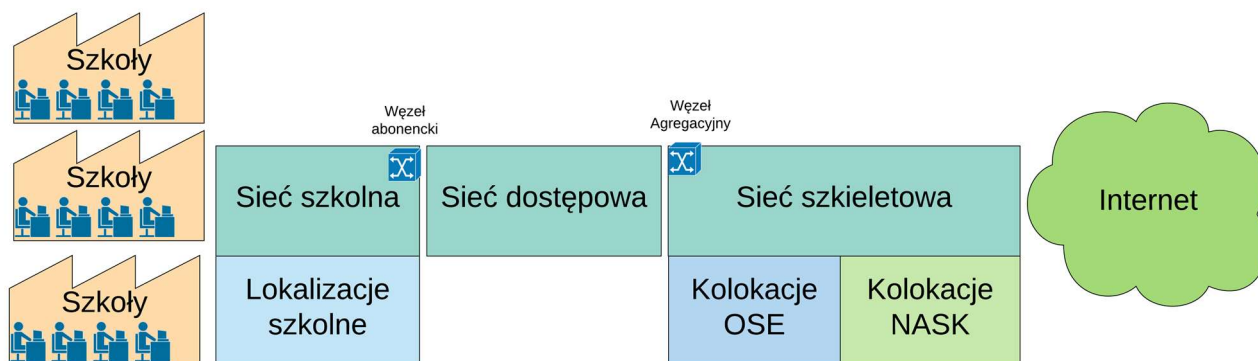
Podstawowym zadaniem OSE ma być zapewnienie jednostkom oświatowym w Polsce możliwości dostępu do bezpiecznego Internetu i zasobów edukacyjnych z przepustowością nie mniejszą niż 100Mb/s (symetrycznie).

Analizując różnice w sposobie realizacji podłączenia poszczególnych lokalizacji, w jakich znajdują się jednostki oświatowe, należy wskazać na istnienie trzech zasadniczych grup, tj. lokalizacje obecnie już będące w zasięgu sieci szerokopasmowej (część z nich już korzysta z dostępu do sieci Internet), lokalizacje planowane do podłączenia w ramach prywatnych inwestycji operatorów telekomunikacyjnych oraz lokalizacje podłączane w ramach POPC, działanie 1.1.

Dostępność lokalizacji (gotowość do podłączenia) będzie rozłożona w czasie zgodnie z poniższym harmonogramem:

	jednostka	2018	2019	2020	2021
Podłączenia w roku	lokalizacje	1 500	11 200	6 178	634
W OSE na koniec roku	lokalizacje	1 500	12 700	18 878	19 512

W celu świadczenia usług szerokopasmowego dostępu do internetu niezbędne jest zapewnienie odpowiedniej infrastruktury telekomunikacyjnej łączącej szkołę / lokalizację (wraz z jej siecią i sprzętem informatycznym) do zasobów sieci internet. Cały przebieg tzw. Sieci OSE możemy podzielić na trzy segmenty zgodnie z poniższym rysunkiem.



Wyodrębnić możemy następujące segmenty sieci OSE:

- Sieć szkolna - infrastruktura sieciowa znajdująca się w lokalizacjach szkolnych, której celem jest zapewnienie łączności dla urządzeń w szkole (zarówno klienckich jak i elementów sieciowych) z punktem dostępowym (CPE). Punkt styku sieci szkolnej z otoczeniem nazywany jest węzłem abonenckim. Zapewnienie odpowiedniej kolokacji dla infrastruktury szkolnej znajduje się w odpowiedzialności placówki szkolnej i jej dyrektora.
- Sieć dostępową - infrastruktura sieciowa dostarczana przez innych operatorów telekomunikacyjnych zapewniająca łączność pomiędzy lokalizacją szkolną a siecią szkieletową.
- Sieć szkieletowa - Infrastruktura sieciowa zapewniająca łączność pomiędzy węzłami sieci OSE oraz siecią OSE a siecią Internet. Sieć szkieletowa będzie znajdować się po części w ramach kolokacji dzierżawionych od podmiotów zewnętrznych a w pewnej części w kolokacji NASK

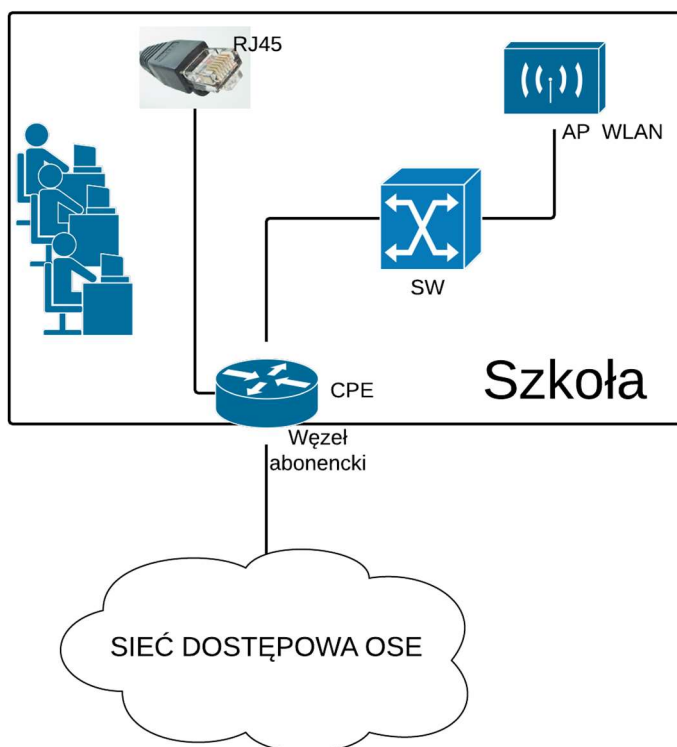
Istnieją cztery modele podłączania szkół do sieci szkieletowej:

1. OSE (standardowy) - szkoły podłączane i konfigurowane w ramach OSE
 - a. rozdzielenie prac w sieci dostępowej i szkolnej
 - b. operator sieci dostępowej doprowadza jedynie zakończenie do lokalizacji szkolnej
 - c. prace w szkole realizowane są przez Operatora OSE
 - d. Obsługa dla szkoły jest świadczona przez OSE
2. POPC - podłączenie szkół będzie realizowane w ramach I Osi priorytetowej Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 „Powszechny dostęp do szybkiego internetu”
 - a. w takim przypadku instalacja punktu dostępowego będzie realizowana przez beneficjenta POPC, zapewnia on również urządzenia CPE i AP
 - b. dodatkowo instalacja będzie rozszerzana przez Operatora OSE o urządzenia SW.
 - c. Obsługa dla szkoły jest świadczona przez OSE (za serwis CPE odpowiada beneficjent POPC)
3. MAN (Sieci Miejskie) - w szkole istnieje już łącze dostarczane w ramach sieci miejskiej
 - a. w szkole nie będzie realizowanych żadnych prac poza opcjonalnym dodaniem CPE dostarczanego przez Operatora OSE - modyfikacja sieci w ramach odpowiedzialności dyrektora szkoły
 - b. Obsługa dla szkoły jest świadczona przez Operatora Sieci Regionalnej (MAN), który dalej ewentualnie zgłasza problemy od OSE
 - c. Na potrzeby części prac w sieci szkolnej może zostać przypisany przez OSE Partner Serwisowy
4. ODN (Ośrodek Doskonalenia Nauczycieli) - szkoła posiada infrastrukturę gotową do podłączenia do sieci
 - a. Operator sieci dostępowej doprowadza zakończenie do lokalizacji szkolnej (inny niż ODN, łącza zamawiane bezpośrednio przez operatora OSE)
 - b. Podłączenie istniejącej w szkole infrastruktury sieciowej do doprowadzonego łącza jest w odpowiedzialności szkoły
 - c. Operator OSE może opcjonalnie dostarczyć dodatkowe CPE - modyfikacja sieci w ramach odpowiedzialności dyrektora szkoły
 - d. Obsługa dla szkoły jest świadczona przez Operatora Sieci Regionalnej (MAN), który dalej ewentualnie zgłasza problemy od OSE
 - e. Na potrzeby części prac w sieci szkolnej może zostać przypisany przez OSE Partner Serwisowy

4.1. Sieć szkolna

Sieci lokalne w jednostkach oświatowych, co do zasady, nie będą w ramach podłączania do OSE modernizowane, jednakże zakłada się możliwość przeprowadzenia ograniczonych prac rekonfiguracyjnych w celu umożliwienia korzystania z dostarczonych usług. Decyzja o wykonywaniu tych prac będzie podejmowana ad hoc, podczas wizyty partnera serwisowego.

Architektura sieci szkolnej z perspektywy OSE przedstawiona jest na poniższym obrazku:



Infrastruktura telekomunikacyjna doprowadzana jest przez operatorów do poszczególnych lokalizacji, w jakich znajdują się szkoły. Należy jednakże zauważyć, że pomiędzy szkoła a lokalizacją zachodzi relacja wiele do wielu. Oznacza to, iż w lokalizacji może występować wiele szkół, lub szkoła może znajdować się w wielu lokalizacjach. Dodatkowo zdarzają się sytuacje, iż szkoła w danej lokalizacji posiada więcej niż jeden budynek. Mogą się również zdarzyć sytuacje, że pod jednym adresem znajdują się będą szkoły o różnym modelu podłączania, czyli w danym adresie może występować więcej niż jedna lokalizacja (lokalizacja grupuje szkoły w jednym adresie podłączane i obsługiwane w tym samym modelu podłączania).

Za fizyczną instalacją oraz konfiguracją urządzeń w jednostce oświatowej, a także przełączenie sieci lokalnej, odpowiadać będzie partner serwisowy. Rolą partnera serwisowego będzie wsparcie jednostki oświatowej podczas uruchomienia, a także późniejsza opieka nad dostarczonymi przez OSE usługami. Proces instalacji urządzeń brzegowych w jednostkach oświatowych będzie realizowany z wykorzystaniem narzędzi automatyzujących konfigurację sprzętu pod kątem konkretnych potrzeb sieci lokalnej i świadczonych usług.

Obsługa techniczna jednostki oświatowej będzie świadczona w zakresie dostarczanych przez OSE usług oraz obsługi urządzenia dostępowego CPE. Dla wszystkich tych usług powstanie jeden punkt kontaktu (tzw. SPOC – Single Point of Contact) odpowiedzialny za przyjmowanie zgłoszeń. Podstawowym kanałem komunikacyjnych z operatorem OSE będzie Portal Usługowy, wspierany przez infolinię telefoniczną (CallDesk).

Dla lokalizacji OSE/POPC szkoła będzie obsługiwana przez Operatora OSE, w przypadku lokalizacji MAN / ODN szkoła będzie obsługiwana przez Operatora Sieci Regionalnej, który dopiero po wstępnej analizie będzie przekazywał problemy do Operatora OSE.

Podstawowym założeniem jest, iż w przypadku, gdy szkoła występuje w więcej niż jednej lokalizacji lub ma więcej niż jeden budynek w tej samej lokalizacji podłączenie jest realizowane wyłącznie do jednego

budynku w podstawowej lokalizacji. Wyjątkiem od tej reguły jest sytuacja, gdy druga lokalizacja jest objęta interwencją POPC 1.1 – wtedy beneficjent POPC w ramach oddzielnych prac podłącza drugą lokalizację.

Poniższa tabela szczegółowo rozpisuje dostępne warianty realizacji i sposób zapewnienia sprzętu w lokalizacji

Model podłączenia	Liczba lokalizacji	Liczba budynków	Liczba szkół	CPE	SW	AP	Uwagi
OSE	1	1	1	1szt. dostarcza OSE	1szt. dostarcza OSE	1szt. dostarcza OSE	
POPC	1	1	1	1szt. dostarcza POPC	1szt. dostarcza OSE	1szt. dostarcza POPC	
OSE	1	2	1	1szt. dostarcza OSE	1szt. dostarcza OSE	1szt. dostarcza OSE	Instalacja wykonywana wyłącznie w jednym budynku
POPC	1	2	1	1szt. dostarcza POPC	1szt. dostarcza OSE	1szt. dostarcza POPC	Instalacja wykonywana wyłącznie w jednym budynku
OSE	1	1	2+	1szt. dostarcza OSE	1+sz. dostarcza OSE	2+sz. dostarcza OSE	Zależnie od projektu 1SW na wszystkie szkoły, albo każda szkoła będzie miała własny switch
POPC	1	1	2+	1szt. dostarcza POPC	2+sz. dostarcza OSE	1szt. dostarcza POPC 1+sz. dostarcza OSE	Zależnie od projektu 1SW na wszystkie szkoły, albo każda szkoła będzie miała własny switch W ramach POPC dostarczany jest jeden komplet sprzętu (CPE+AP) per lokalizacja
OSE	1	2	2	1szt. dostarcza OSE	1+sz. dostarcza OSE	2+sz. dostarcza OSE	Zależnie od projektu 1SW na wszystkie szkoły, albo każda szkoła będzie miała własny switch
POPC	1	2	2	1szt. dostarcza POPC	2+sz. dostarcza OSE	1szt. dostarcza POPC 1+sz. dostarcza OSE	Zależnie od projektu 1SW na wszystkie szkoły, albo każda szkoła będzie miała własny switch W ramach POPC dostarczany jest jeden komplet sprzętu (CPE+AP) per lokalizacja
OSE	2	2	1	1szt. dostarcza OSE	1szt. dostarcza OSE	1szt. dostarcza OSE	Instalacja wykonywana wyłącznie w jednym budynku / lokalizacji
POPC	2	2	1	2szt. dostarcza POPC	2szt. dostarcza OSE	2szt. dostarcza POPC	Wyłącznie, gdy lokalizacja jest objęta interwencją POPC, w przeciwnym przypadku podłączana jest wyłącznie jedna lokalizacja (sprzęt po 1 szt.)
MAN	*	*	n	0-n dostarcza OSE	0-n dostarcza OSE	0-n dostarcza OSE	Możliwe dostarczenie urządzeń OSE do szkół. Operator Sieci Regionalnej (MAN) może pełnić rolę Partnera Serwisowego, dostarczenie urządzeń może być realizowane przez Operatora OSE, ewentualnie zostanie wybrany zewnętrzny partner serwisowy (jak dla lokalizacji OSE/POPC)

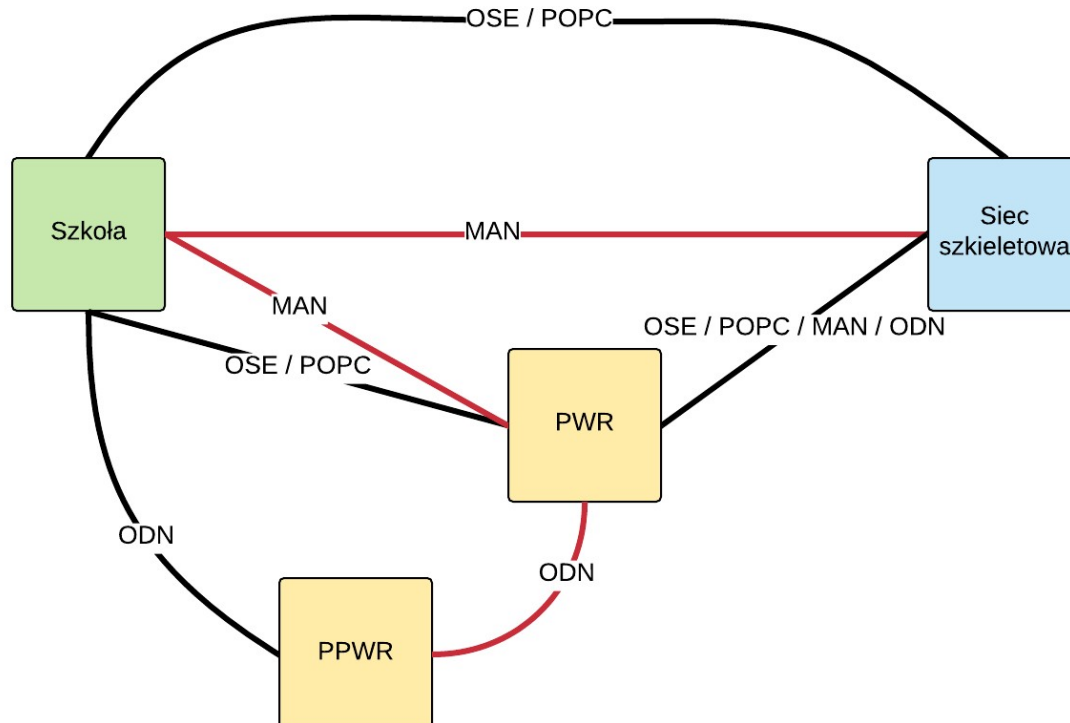
Model podłączenia	Liczba lokalizacji	Liczba budynków	Liczba szkół	CPE	SW	AP	Uwagi
ODN	*	*	n	0-n dostarcza OSE	0-n dostarcza OSE	nie dotyczy	Możliwe dostarczenie urządzeń OSE do szkół. Operator Sieci Regionalnej (ODN) może pełnić rolę Partnera Serwisowego, dostarczenie urządzeń może być realizowane przez Operatora OSE, ewentualnie zostanie wybrany zewnętrzny partner serwisowy (jak dla lokalizacji OSE/POPC)

Urządzenia dostępne CPE

Kluczowym elementem sieci szkolnej z punktu widzenia systemu OSS będą urządzenia dostępne - CPE. System provisioningu musi zarządzać zdalnie konfiguracją tych urządzeń - w przypadku urządzeń zarządzanych przez OSE, lub wysłać mailowo konfigurację urządzeń do Operatora Sieci Regionalnej (w przypadku urządzeń będących własnością MAN / ODN). Należy zwrócić uwagę na dużą możliwą różnorodność urządzeń. O ile urządzenia kupowane przez Operatora OSE będą znane z dużym wyprzedzeniem (można, więc będzie przygotować dla nich profile konfiguracji z dużym zapasem czasowym), to w przypadku urządzeń dostarczanych przez beneficjentów POPC model urządzenia będzie znany z 1-2 tygodniowym wyprzedzeniem. Provisioning musi, więc zapewniać szybkie i elastyczne dodawanie nowych modeli urządzeń do konfiguracji.

4.2. Sieć dostępowa

Połączenie pomiędzy lokalizacją szkolną (węzeł abonencki) a siecią szkieletową OSE (węzeł agregacyjny) realizowana jest za pośrednictwem tzw. sieci dostępowej. Możliwe warianty realizacji połączenia w sieci szkieletowej zależą od modelu podłączenia szkoły / lokalizacji.



Wyróżniamy następujące przebiegi łącz w sieci dostępowej:

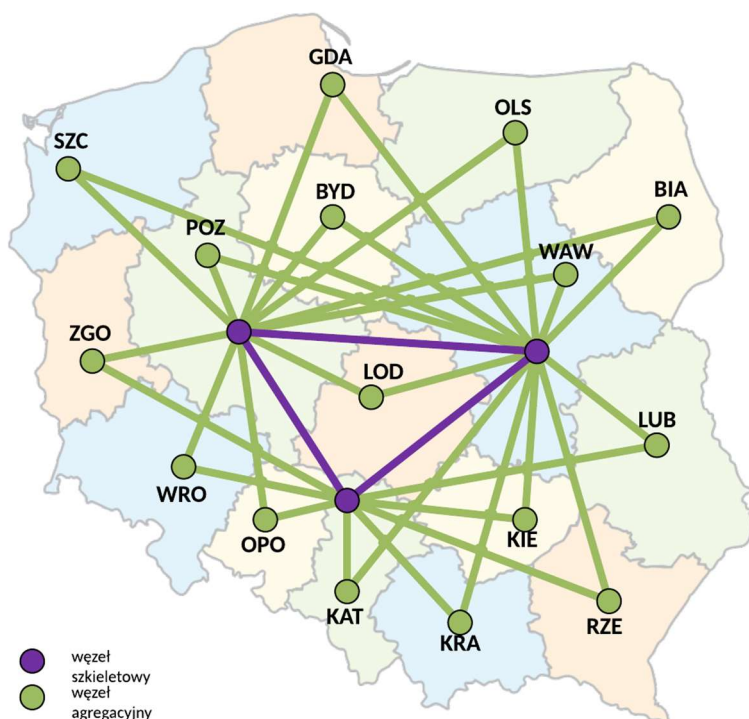
Model Podłączenia	Przebieg łącza	Odpowiedzialność za łącze
OSE / POPC	Węzeł abonencki → Węzeł agregacyjny	Operator OSE
OSE / POPC	Węzeł abonencki → PWR → Węzeł agregacyjny	Operator OSE
MAN	Węzeł abonencki → Węzeł agregacyjny	Operator Sieci Regionalnej (MAN)
MAN	Węzeł abonencki → PWR → Węzeł agregacyjny	Operator Sieci Regionalnej (MAN)
ODN	Węzeł abonencki → PPWR → PWR → Węzeł agregacyjny	Za łącze PPWR→PWR odpowiada Operator Sieci Regionalnej (ODN) Za pozostały przebieg odpowiada operator OSE

Konfiguracja sieci dostępowej

Za konfigurację po stronie sieci dostępowej będzie odpowiedzialny operator zapewniający łącze zarówno dla łącz zarządzanych przez OSE, jak i pozostałych (MAN / ODN). W procesie zamawiania łącza konieczne jest, więc przekazanie pełnej konfiguracji, jaka ma być ustawiona dla łącza. Z uwagi na fakt braku aktywnych urządzeń OSE w sieci dostępowej monitoring łączy musi być realizowany na jej brzegach (węzeł abonencki w szkole i węzeł agregacyjny w sieci szkieletowej). Aby było możliwe szybkie analizowanie i rozwiązywanie problemów w systemach odpowiedzialnych za Trouble Ticketing muszą być informacje o całym przebiegu łącza wraz z informacją o operatorach odpowiedzialnych za poszczególne odcinki.

4.3. Sieć szkieletowa

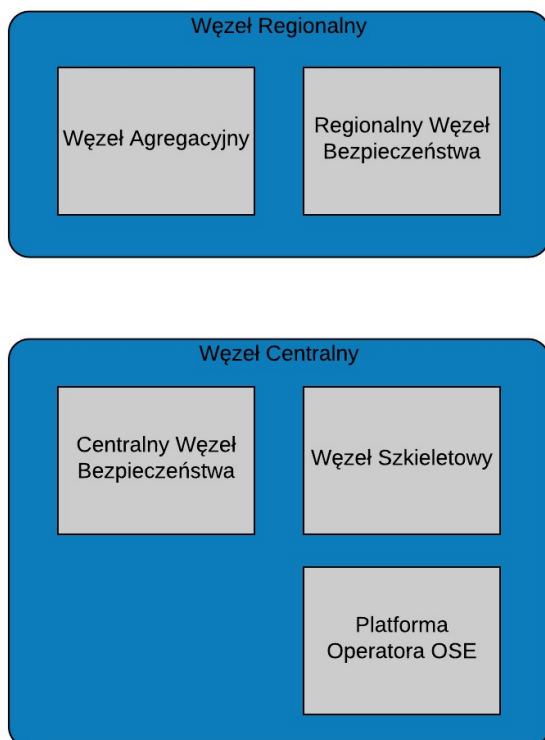
W zakresie sieci szkieletowej operator OSE będzie opierał się na łączach dzierżawionych od operatorów telekomunikacyjnych, nie jest rozważana budowa własnej infrastruktury kablowej. Przeprowadzony przez NASK Dialog Techniczny z operatorami telekomunikacyjnymi wskazał na potrzebę budowy 16 węzłów OSE, zlokalizowanych w miastach wojewódzkich, w celu agregowania ruchu z jednostek oświatowych z terenu całego kraju (węzły agregacyjne). 3 spośród tych węzłów powinny pełnić również rolę węzłów centralnych (węzły szkieletowe). Pozostałe węzły będą połączone do węzłów centralnych. Lokalizacje węzłów zostanie wybrana przez NASK Państwowy Instytut Badawczy w ramach odrębnych, wewnętrznych procesów zakupowych, w wyniku, których zostaną wyłonieni dostawcy Usług kolokacji w poszczególnych centrach przetwarzania danych. Zamawiający planuje również objęcie wszystkich "kolokacji" jednym, wspólnym systemem zarządzania.



Węzły sieci

W sieci OSE będą dwa funkcjonalne rodzaje węzłów:

- Węzeł Regionalny składa się z Węzła Agregacyjnego, do którego będą dołączone łącza ze szkół, oraz z Regionalnego Węzła Bezpieczeństwa.
- Węzeł Centralny, składa się z Węzła Szkieletowego, do którego będą dołączone Węzły Agregacyjne. Węzły te będą także zapewniały łączność do sieci Internet oraz zapewnią połączenie z Zasobami obliczeniowymi OSE. Centralny Węzeł Bezpieczeństwa będzie zlokalizowany tylko w dwóch Węzłach Centralnych.



Węzły Szkieletowe będą zlokalizowane w tych samych miejscach, co Węzły Agregacyjne, za wyjątkiem węzła WAW / WAW Core, w którym Węzeł Agregacyjny będzie umieszczony w innej lokalizacji niż Węzeł Szkieletowy (oba węzły będą zlokalizowane na terenie Warszawy). Urządzenia pełniące funkcje obu węzłów będą oddzielne.

Każdy węzeł OSE wyposażony zostanie w urządzenia sieciowe, Infrastrukturę bezpieczeństwa, przełączniki sieci lokalnej, systemy OSS/BSS (węzły centralne) oraz w urządzenia sieci zarządzania, zapewniające dostęp administracyjny do wszystkich urządzeń zlokalizowanych w węźle.

Przełączniki sieci lokalnej będą zainstalowane w każdym z węzłów. Przełączniki te będą obsługiwały urządzenia zainstalowane w węzłach, w szczególności urządzenia Węzła Bezpieczeństwa, systemy zbierania i retencji logów telekomunikacyjnych oraz systemy komputerowe, na których będą posadowione systemy OSS/BSS sieci OSE.

Konfiguracja sieci szkieletowej:

Zadaniem systemu odpowiedzialnego za provisioning będzie automatyczna konfiguracja urządzeń w sieci szkieletowej (zarówno urządzeń typowo sieciowych jak i urządzeń bezpieczeństwa). Pomimo iż architektura sieci szkieletowej będzie się charakteryzować minimalną zmiennością to jednakże dla komponentu Service Order Manager dużym wyzwaniem będzie choreografia skonfigurowania poszczególnych elementów sieci. SOM będzie musiał potrafić dla każdego zlecenia aktywacji / modyfikacji / usługi przeprowadzić proces automatycznej zmiany konfiguracji urządzeń w sieci szkieletowej wykorzystując komponenty Element Manager dostarczane wraz z urządzeniami sieciowymi lub konfiguruje urządzenia bezpośrednio przy użyciu interfejsu udostępnianego przez te urządzenia. Cały proces konfiguracji usług musi być zamodelowany w SOM.

4.4. Koncepcja świadczenia usługi dla szkoły

W szkołach zainstalowane będą urządzenia CPE, świadczące usługi dla sieci lokalnych w szkołach.

Na urządzeniach tych lokalne adresy IPv4 z pul prywatnych zgodnych z RFC1918 / BCP5 translowane są (NAT 1:1) do adresów z puli 100.64.0.0/10 (Shared Address Space zgodnie z RFC6598 / BCP153). Jednocześnie dla klientów IPv6 zaalokowana jest pula adresów GUA z puli przydzielonej dla sieci OSE przez RIPE (w sieci OSE nie będą używane adresy prywatne IPv6).

Ruch od urządzeń CPE umieszczonych w szkołach przenoszony jest przez łącza, w technologii Ethernet, operatorów agregujących do Węzłów Agregacyjnych sieci OSE, gdzie jest oddawany do urządzeń agregujących sieci OSE na interfejsach 10GE oraz 1GE. Ruch do każdego urządzenia CPE jest oddawany na oddzielnych VLANach, przy następujących założeniach:

- każda szkoła jest terminowana na oddzielnym VLANie lub VLANach,
- z każdej szkoły może być skreowanych kilka VLANów (do pięciu), przy czym każdy z nich terminowany jest po stronie szkoły w oddzielnym VRF, a od strony sieci OSE każdy traktowany jest, jako oddzielne łącze z własną adresacją i routingiem; Separacja VLANów tworzona jest na potrzeby kreowania różnych usług, w tym usług posiadających różne polityki bezpieczeństwa;
- ruch zarządzania do urządzenia CPE jest oddzielony od ruchu produkcyjnego szkoły obsługiwanej przez to CPE i terminowany jest na oddzielnym VLANie,
- ww. VLANy mogą być oddane w jednym z dwóch modeli:
 - jako VLAN z pojedynczym tagowaniem, zgodnie ze standardem IEEE 802.1q lub,
 - jako VLAN z podwójnym tagowaniem, zgodnie ze standardem IEEE 802.1ad, przy czym ruch z pojedynczej szkoły ma wspólny S-TAG oraz EtherType = 0x88a8.

Ruch odebrany w Węźle Agregacyjnym kierowany jest do Węzła Bezpieczeństwa.

Następnie odebrany ruch z Regionalnego Węzła Bezpieczeństwa kierowany jest do Węzłów Szkieletowych, a następnie do sieci Internet. Pomiędzy Węzłem Bezpieczeństwa, a wyjściem do sieci Internet ruch IPv4 przechodzi przez instancję CG-NAT, gdzie jest translowany do publicznych adresów IPv4 przydzielonych dla sieci OSE.

Separacja ruchu

Ruch zarządzania (zarówno dla urządzeń CPE jak też urządzeń sieci OSE) traktowany jest, jako ruch zaufany i jest oddzielony od ruchu produkcyjnego do / ze szkół. Separacja tego ruchu w sieci OSE powinna nastąpić na poziomie VFR, logical system lub podobnym (tj. zapewniającym separację tablic routingu oraz wykluczającym wzajemny dostęp do ruchu z poszczególnych strumieni).

QoS

W sieci OSE wdrożony będzie QoS z następującymi założeniami:

- klasyfikacja odbywa się na urządzeniu agregacyjnym sieci OSE,
- najwyższy priorytet w sieci ma ruch z klasy Network Control, obejmujący ruch kontrolny protokołów routingu (IGP, BGP, MPLS, itd.) – ruch ma zagwarantowane 3% pasma na interfejsach szkieletowych sieci (tj. interfejsach pomiędzy urządzeniami sieci OSE bez uwzględnienia urządzeń CPE);
- ruch w klasie MGMT (ruch zarządzania, w szczególności ruch do / z systemów OSS, ruch sesji terminalowych do urządzeń sieciowych, ruch do kolektorów logów) – ruch ma zagwarantowane 5% pasma na interfejsach sieci (w tym na interfejsach pomiędzy urządzeniami sieci OSE a urządzeniami CPE);

- ruch w klasie BE (Best Effort) obejmujący ruch produkcyjny do / ze szkół – ruch ma zagwarantowane 50% pasma na wszystkich interfejsach;
- w sieci OSE musi być przygotowana możliwość uruchomienia ruchu w klasach:
 - VOICE – ruch priorytetowy – nie więcej niż 5% pasma;
 - INTVIDEO (Interactive Video) – ruch gorszy niż NC a lepszy niż MGMT – zagwarantowane 20% pasma;
 - scavenger (less-than best-effort) – ruch bez gwarancji pasma.

5. Bezpieczeństwo OSE

W sieci OSE będą dwa funkcjonalne rodzaje węzłów:

- Węzeł Regionalny składa się z Węzła Agregacyjnego, do którego będą dołączone łącza ze szkół, oraz z Regionalnego Węzła Bezpieczeństwa.
- Węzeł Centralny, składa się z Węzła Szkieletowego, do którego będą dołączone Węzły Agregacyjne. Węzły te będą także zapewniały łączność do sieci Internet oraz zapewnią połączenie z Zasobami obliczeniowymi OSE. Centralny Węzeł Bezpieczeństwa będzie zlokalizowany tylko w dwóch Węzłach Centralnych.

Węzły Centralne mogą być zlokalizowane w tych samych Obiektach, co Węzły Regionalne, ale Urządzenia pełniące funkcje obu węzłów będą oddzielne.

Każdy węzeł OSE wyposażony zostanie w urządzenia sieciowe, elementy Infrastruktury bezpieczeństwa, przełączniki sieci lokalnej, systemy OSS/BSS zlokalizowanych w węźle oraz w urządzenia sieci zarządzania, zapewniające dostęp administracyjny do wszystkich Urządzeń zlokalizowanych w Węźle.

Każdy z 16 Regionalnych Węzłów Bezpieczeństwa będzie zawierać komponenty realizujące podstawowe funkcjonalności, m.in:

- zapewnianie bezpieczeństwa teleinformatycznego użytkownikom sieci OSE,
- wykrywanie i zapobieganie włamaniom poprzez wykrywanie i blokowanie ataków sieciowych w czasie rzeczywistym,
- wykrywanie i blokowanie zdefiniowanych aplikacji webowych,
- monitorowanie ruchu sieciowego i zapisywanie najważniejszych wydarzeń do logu.

Dwa Centralne Węzły Bezpieczeństwa będą zawierać komponenty realizujące funkcjonalności ochrony Zasobów obliczeniowych OSE, tzn. będą:

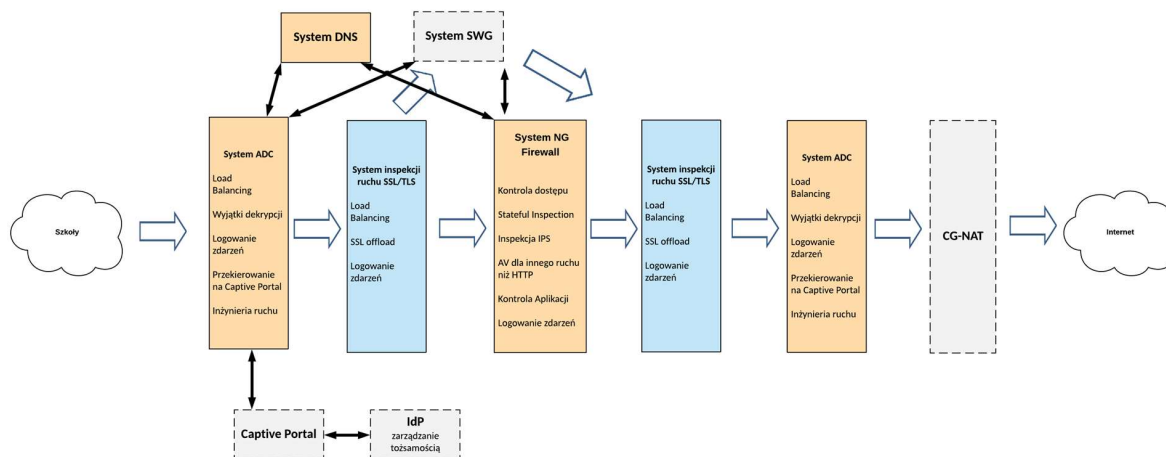
- zapewniać bezpieczeństwo teleinformatyczne Zasobów obliczeniowych OSE i systemów wsparcia
- wykrywać i zapobiegać włamaniom poprzez wykrywanie i blokowanie ataków sieciowych w czasie rzeczywistym

Ponad to w każdym Regionalnym Węźle Bezpieczeństwa zostaną zainstalowane mechanizmy ochrony użytkownika sieci OSE, realizowane w oparciu o systemy klasy SWG.

5.1. Architektura Infrastruktury Bezpieczeństwa

Architektura Infrastruktury bezpieczeństwa składa się z Systemu ADC, Systemu inspekcji SSL/TLS, Systemu NG Firewall, Systemu DNS, Systemu zarządzającego oraz Systemu SWG.

Poniżej zaprezentowano schemat blokowy przepływu danych w Regionalnych Węzłach Bezpieczeństwa. Schemat zawiera systemy Zamawiającego, składające się na Infrastrukturę bezpieczeństwa.



Koncepcja przepływu danych

- Cały ruch (100%) od CPE, po przejściu przez Węzeł agregacyjny, przechodzi przez System ADC, który dokonuje deszyfracji SSL wewnątrz lub z wykorzystaniem Urządzeń dedykowanych. Inspekcji podlega 100% ruchu SSL/TLS z pominięciem wybranych domen, pobranych z pól SNI i CN certyfikatu, należących do kategorii treści określonych przez Zamawiającego. Informację na temat kategorii, do jakiej należy dana domena, System ADC uzyska poprzez współpracę z Systemem DNS.
- Po dokonaniu deszyfracji, cały ruch zostanie przekierowany do Systemu NG Firewall, gdzie będą zdefiniowane polityki dotyczące ruchu warstwy 3 / 4 i uruchomione zostaną funkcjonalności IPS (100% ruchu), AV (9% ruchu - inspekcji AV będzie podlegał ruch niezwiązany z ruchem webowym HTTP/HTTPS) i Kontroli aplikacji (100% ruchu). W przypadku, kiedy będzie to żądanie do serwisów web (HTTP, HTTPS), System przekieruje cały taki ruch do Systemu SWG.
- Po dokonaniu inspekcji treści, ruch jest kierowany ponownie do Systemu ADC, lub na urządzeniu dedykowanym do obsługi ruchu SSL/TLS, w celu ponownej szyfracji SSL.
- Ruch wychodzi z Regionalnego Węzła Bezpieczeństwa i kierowany jest zgodnie z tablicą routingu Węzła szkieletowego. W przypadku potrzeby skierowania ruchu do sieci Internet, przed opuszczeniem Węzła Centralnego, dokonywana jest translacja CGNAT do adresacji publicznej.
- Ruch zarządzania (zarówno dla CPE jak też urządzeń sieci OSE) traktowany jest, jako ruch zaufany i jest oddzielony od ruchu produkcyjnego do / ze szkół. Separacja tego ruchu w sieci OSE powinna nastąpić na poziomie VFR, logical system lub podobnym.

Systemy Wsparcia

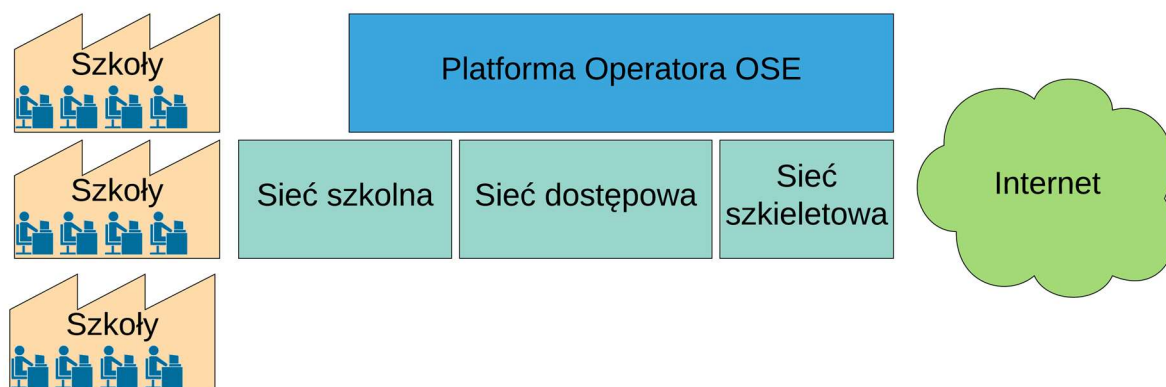
Zamawiający planuje większość procesów realizować w sposób zautomatyzowany. Systemy i infrastruktura objęte zostaną zintegrowane z centralnymi systemami nadzorującymi działanie wszystkich elementów sieci OSE.

6. Platforma Operatora OSE

Platforma Operatora OSE (POOSE) służy do wsparcia działalności NASK PIB, jako operatora telekomunikacyjnego w obszarze Ogólnopolskiej Sieci Edukacyjnej.

Systemy nadzoru OSE muszą zapewniać Operatorowi OSE możliwość spełniania wszystkich jego obowiązków i zadań wynikających z ustawy o OSE. Zgodnie z Art. 5 ustawy o OSE do zadań Operatora OSE należy:

- przygotowanie OSE w sposób umożliwiający świadczenie z jej wykorzystaniem usług, bezpiecznego dostępu do internetu, jej eksploatację, utrzymanie, usuwanie awarii, modernizację oraz nadzór nad jej funkcjonowaniem;
- świadczenie szkole usługi szerokopasmowego dostępu do Internetu o symetrycznej przepustowości co najmniej 100 Mb/s;
- świadczenie szkole usług bezpieczeństwa teleinformatycznego, obejmujących ochronę przed szkodliwym oprogramowaniem oraz monitorowanie zagrożeń i bezpieczeństwa sieciowego;



Dodatkowo NASK PIB, jako Operator OSE realizujący projekt OSE również przy dofinansowaniu z projektów unijnych musi przy wykorzystaniu platformy nadzoru OSE móc spełnić następujące wymagania:

- Kwalifikowalność wydatków
- Kontrola projektu
- Sprawozdawczość, rozliczenie projektu i jego dokumentacja
- Promowanie i znakowanie produktów projektu
- Zapewnienie trwałości projektu

Główne zadania stawiane POOSE są następujące:

- Obsługa klientów (szkół)
- Prowadzenie działalności operatora telekomunikacyjnego
- Zarządzanie i rozliczanie prac partnerów serwisowych
- Zarządzanie i rozliczanie dostawców sprzętu

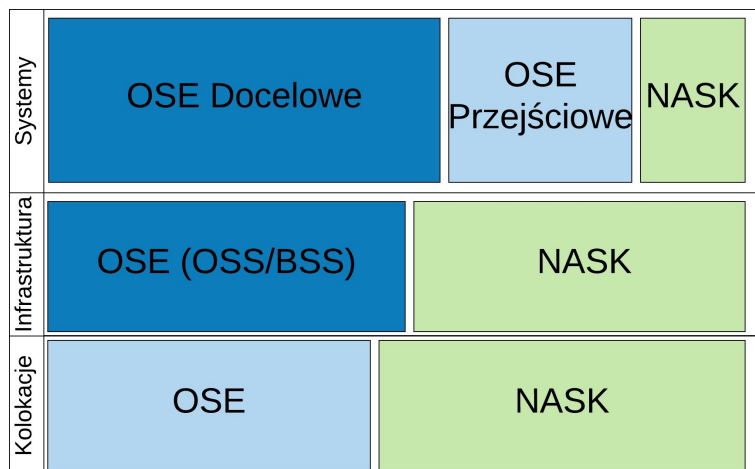
- Zarządzanie i rozliczanie usług operatorów sieci dostępowej / agregacyjnej / szkieletowej
- Monitorowanie sieci i systemów bezpieczeństwa OSE (**monitorowaniem bezpieczeństwa w OSE zajmuje się głównie system SIEM, którego wdrożenie nie jest przedmiotem niniejszego postępowania**)
- Zarządzanie punktami dostępu w szkołach
- Zarządzanie bezpieczeństwem w ramach dedykowanego Portalu bezpieczeństwa
- Wsparcie rozliczania projektu OSE
- Integracja z systemami zewnętrznymi (Portal OSE, Element Managers OSE, SIEM OSE, Centralny System Tożsamości OSE, system magazynowy NASK PIB, System Finansowo-księgowy NASK PIB, Sugar CRM)

Architektura referencyjna

W ramach Platformy Operatora OSE wyróżniamy 3 główne obszary:

- Systemy informatyczne wspierające realizację działań operatora OSE,
- Infrastrukturę umożliwiającą działanie systemów POOSE,
- Kolokacje, w których znajdować się będzie infrastruktura

Obszary te dzielą się na segmenty zgodnie z poniższym rysunkiem:

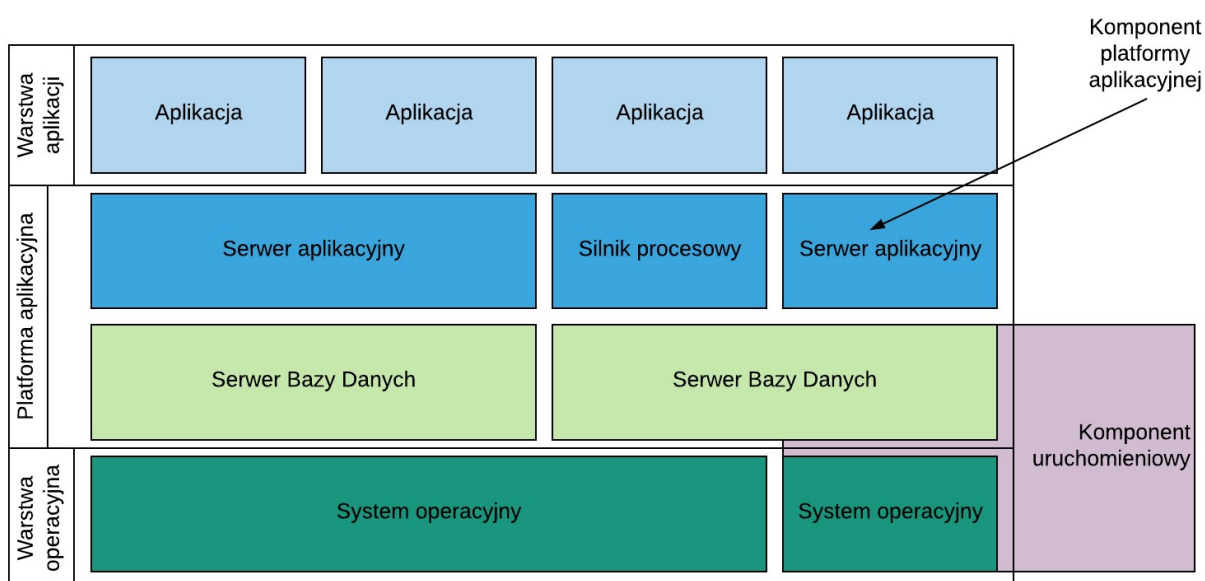


- W obszarze NASK (Systemy, Infrastruktura, Kolokacje) znajduje się wszystkie elementy architektury IT wykorzystywane w bieżącej działalności NASK, jakie po ewentualnym dostosowaniu będą wykorzystywane (zintegrowane) w ramach Platformy Operatora OSE.
- W obszarze OSE (Kolokacje), znajdują się wszystkie elementy, które już powstały lub powstają poza obecnym postępowaniem (OSS/BSS), ale są dedykowane wyłącznie na potrzeby OSE.
- OSE przejściowe to wszelkie oprogramowanie na potrzeby OSE, jakie już powstało lub będzie powstawać poza obecnym postępowaniem przetargowym
- OSE Docelowe, czyli systemy wsparcia i zarządzania są to aplikacje, które mają zostać dostarczone w ramach obecnego postępowania i zintegrowane z innymi elementami Platformy Operatora OSE. Zostaną one osadzone na infrastrukturze OSE (OSS/BSS)

- Infrastruktura OSE (OSS/BSS) jest to dedykowana na potrzeby operatora OSE warstwa sprzętowa dostarczana w ramach tego postępowania przetargowego, która ma umożliwić również funkcjonowanie części systemom OSE NASK. Zostanie ona umiejscowiona zarówno w kolokacjach NASK jak i kolokacjach OSE.

Złożoność architektury

Wygoda użytkowania rozwiązania, koszty związane z jego utrzymaniem oraz rozwojowe są wprost proporcjonalne do złożoności samego rozwiązania. Im bardziej złożona architektura tym większe będą wymagania kompetencyjne do zespołu zajmującego się utrzymaniem, również większa pracochłonność związana z realizacją poszczególnych prac operacyjnych. Aby ograniczyć koszty związane z pracami konieczne jest wskazanie maksymalnego dopuszczalnego stopnia złożoności rozwiązania. Celem poprawnego wyliczenia złożoności konieczne jest zapewnienie odpowiedniego modelu referencyjnego.



Złożoność architektura składa się z następujących elementów:

- Różnorodność komponentów - ilość różnych komponentów realizujących funkcjonalności tej samej warstwy (np. różne silniki baz danych, lub różne wersje serwerów aplikacyjnych)
- Różnorodność relacji - ilość różnych relacji pomiędzy komponentami różnych warstw (np. dla tej samej bazy różne wersje systemu operacyjnego)
- Integracje - ilość i skomplikowanie integracji pomiędzy komponentami tej samej warstwy.

Zbudowanie pełnego modelu złożoności wymaga dużej pracy w ramach organizacji oraz weryfikacji na poziomie architektury korporacyjnej i strategii biznesowej. W związku z tym na potrzeby oceny rozwiązań przyjęty zostanie uproszczony zakładający, iż największy wpływ na złożoność ma architektura platformy aplikacyjnej, mniejszy wpływ ma wielość aplikacji, a najmniejszy ilość systemów operacyjnych. We wzorze zostaną wykorzystane następujące współczynniki:

- aplikacja - Samodzielnie funkcjonujący komponent programistyczny posiadający interfejs graficzny udostępniany dla użytkownika oraz określony model własności i licencjonowania. Aplikacja może się składać z modułów pochodzących od jednego dostawcy i dostarczanych w ramach jednego modelu

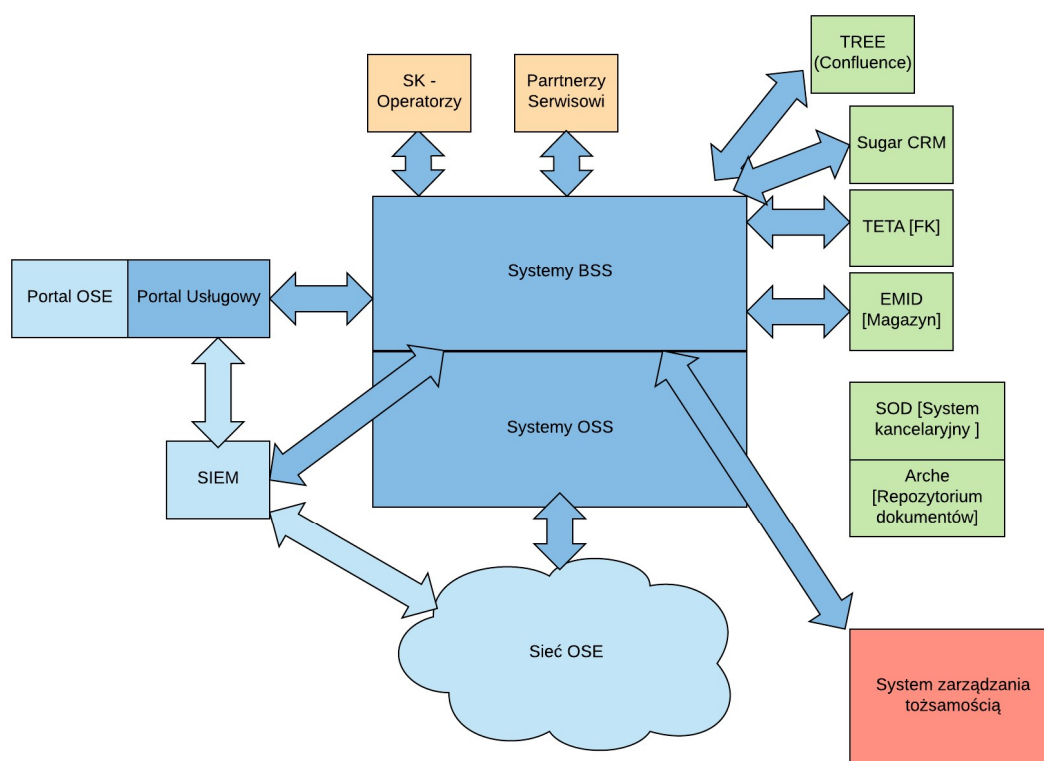
licencji. Jeżeli "dodatki" do aplikacji dostarczane są przez innego producenta lub posiadają inny model licencjonowania traktowane są, jako oddzielne aplikacje.

- komponent platformy aplikacyjnej - komponent programistyczny będący środowiskiem do funkcjonowania aplikacji taki jak serwer aplikacyjny, serwer bazy danych itp. W przypadku, gdy dany komponent występuje w różnych wersjach oprogramowania to traktowany jest, jako oddzielne komponenty platformy aplikacyjnej.
- komponent uruchomieniowy - połączenie komponentu platformy aplikacyjnej z warstwą operacyjną (czyli systemem operacyjnym). W sytuacji, gdy dany serwer bazy danych uruchamiany jest na dwóch różnych systemach operacyjnych liczony jest, jako dwa komponenty uruchomieniowe.

Współczynnik złożoności jest iloczynem ilości aplikacji z ilością komponentów uruchomieniowych uwzględniając odpowiednie współczynniki wagowe.

6.1 Warstwa aplikacyjna

Wysokopoziomowy model Platformy Operatora OSE:



Portal OSE - Wizytówka Ogólnopolskiej Sieci Edukacyjnej, platforma informacyjna udostępniająca treści edukacyjne, umożliwiającą również oferowanie dodatkowej wartości / usług / produktów dostępnych dla użytkowników OSE.

Portal Usługowy - aplikacja dla klientów sieci OSE (dla szkół i ich pracowników) służąca do zarządzania produktami OSE (w tym usług bezpieczeństwa), zamawiania usług, obsługi posprzedażowej, jako kanał Self-Service. Służy ona do zarządzania usługami, prezentacją stanu usług oraz innych informacji związanych z tymi usługami. Poprzez Portal Usługowy jest również realizowane zgłaszanie szkół do OSE.

SIEM - aplikacja do zbierania, monitorowania i analizy logów bezpieczeństwa. Przygotowująca raporty dla dyrektorów szkół udostępniane na Portalu Usługowym. Zakładana jest ograniczona integracja OSS/BSS z systemem SIEM

System Zarządzania Tożsamością - system do zarządzania tożsamością [m.in](#) użytkowników systemów POOSE oferujący funkcjonalność Single-Sign-On. Na obecnym etapie prac system jest jeszcze w fazie planowania

System Kancelaryjny, SOD (rejestr dokumentów), Arche (Repozytorium dokumentów) - systemy wspierające procesy obiegu dokumentów w NASK-PIB, Zakładana jest integracja wyłącznie na poziomie procesów biznesowych.

EMID - system magazynowy NASK-PIB. Zakładana jest ograniczona integracja z systemem, celem zasilania i aktualizacji informacji na podstawie zmian w obszarze POOSE.

TETA - system finansowy-księgowy NASK-PIB. Zakładane jest, iż pełna sprawozdawczość finansowo-księgowa będzie realizowana w oparciu o system TETA, w związku, z czym konieczna będzie integracja na poziomie zagregowanych danych finansowo-księgowych, oraz synchronizacja bazy kontrahentów.

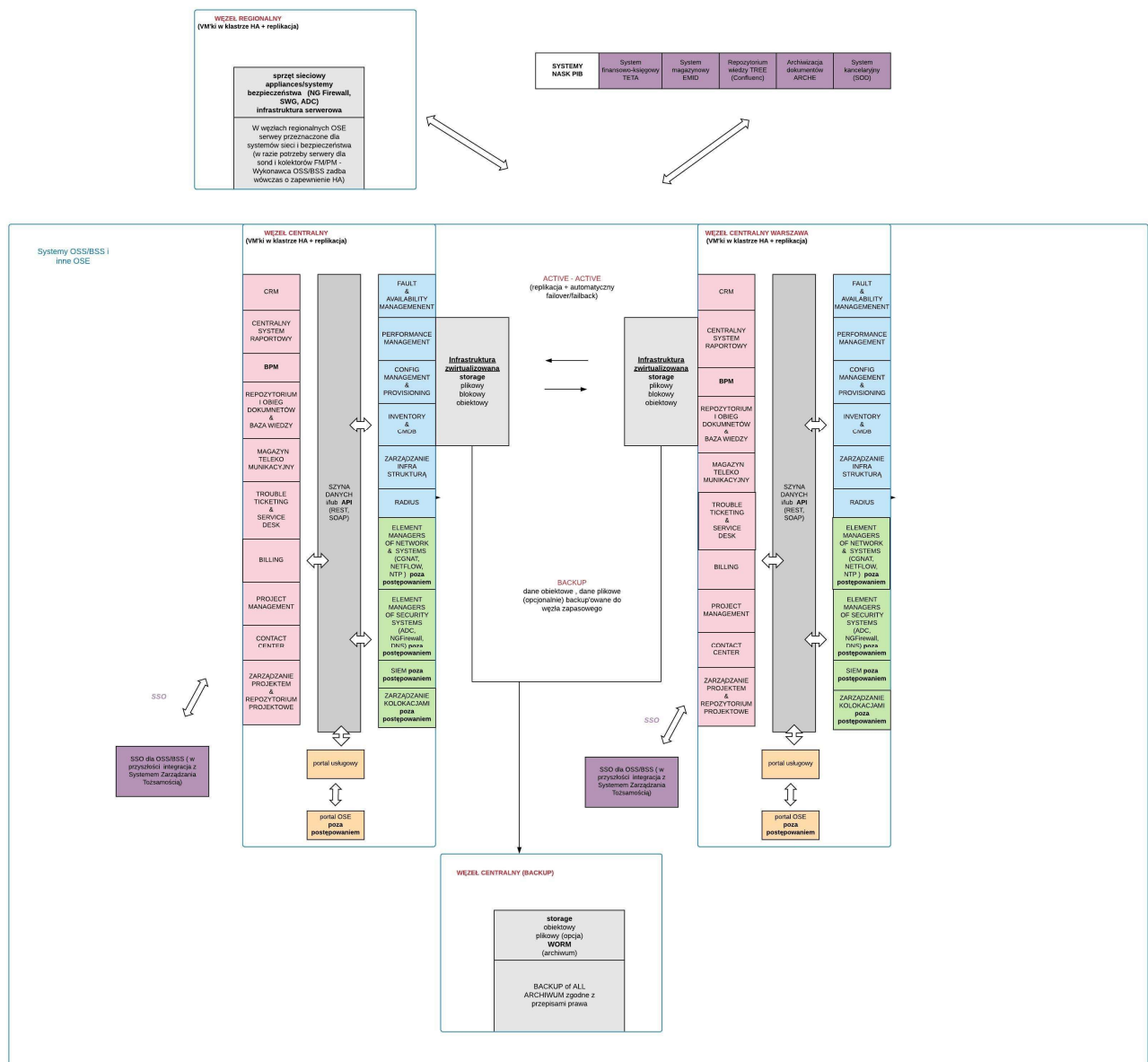
SugarCRM - system do obsługi klientów NASK-PIB. Zakładana jest integracja w obszarze umów.

TREE - platforma Confluence służąca do zarządzania i wymiany wiedzy. Zakładana jest realizacja części rozwiązania na platformie (baza wiedzy), oraz dodatkowo integracja z repozytorium architektonicznym.

SK - Operatorzy - kanał komunikacyjny z operatorami łączy dostępowych i agregacyjnych wykorzystywany w procesie zamawiania / modyfikacji łącz oraz w procesach reklamacji i TT. Domyślnie komunikacja będzie realizowana w oparciu o email.

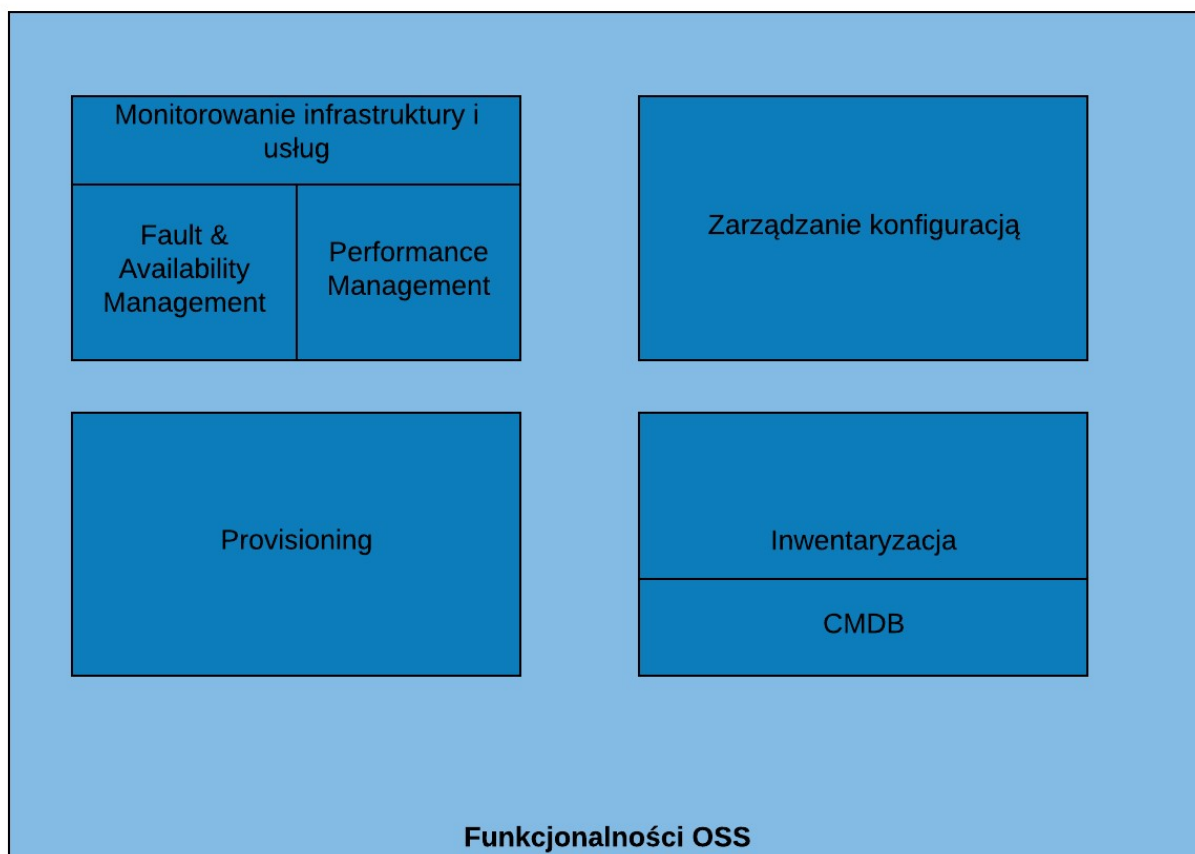
Partnerzy Serwisowi - Kanał komunikacyjny służący do informowania (notyfikowaniu) o zleceniach partnerów serwisowych. Zakładane jest, iż procesy będą realizowane wyłącznie w oparciu o systemy OSS/BSS umożliwiając jednakże wysyłanie powiadomień do systemów partnerów.

Większy poziom szczegółowości POOSE widać na poniższym rysunku:



6.1.1. Funkcjonalności obszaru OSS

Wymagane w ramach przedmiotu zamówienia systemy obszaru OSS zostały zgrupowane wokół funkcjonalności zgodnie z poniższym rysunkiem:



Fault & availability management - wsparcie pracy zespołów NOC, SOC i IT w zakresie utrzymania sieci, usług i systemów OSE.

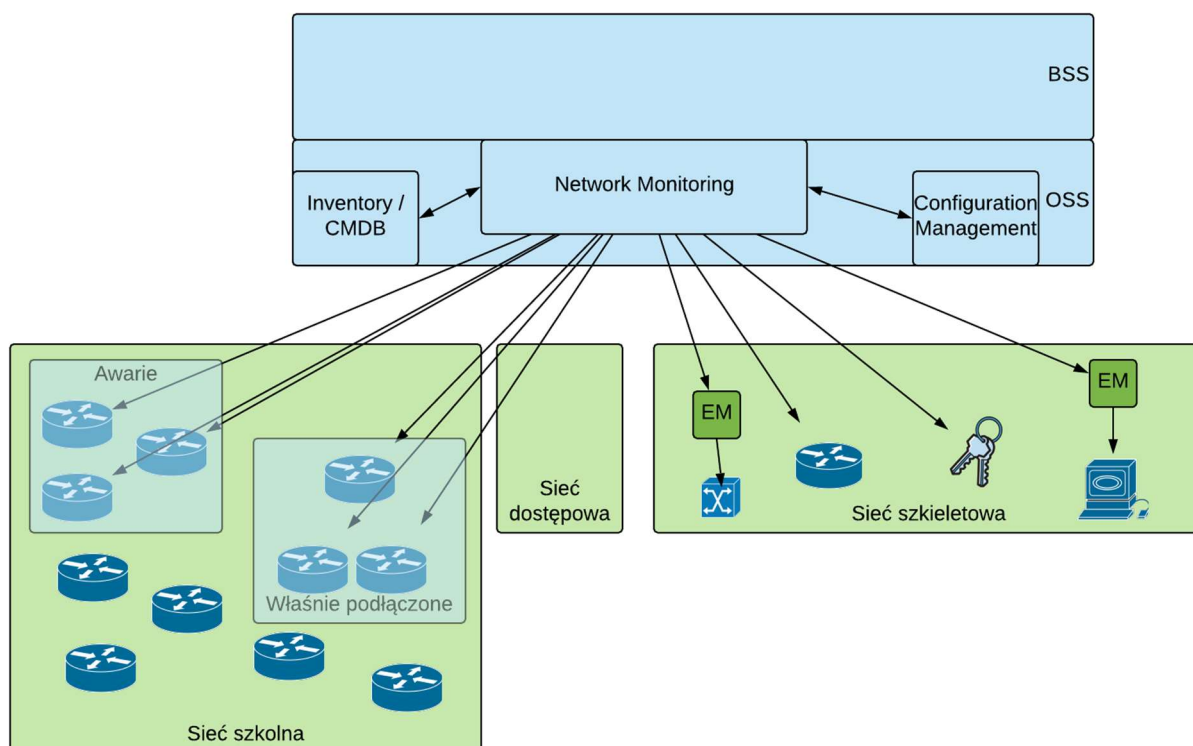
Należy pamiętać przy tym o uwarunkowaniach związanych z monitorowaniem sieci OSE

W przypadku sieci szkieletowej wymagany jest standardowy / pełny monitoring wszystkich elementów sieci. W ramach rozwiązania OSS powinna zostać dostarczona platforma zapewniająca pełen widok na sieć szkieletową, usługi bezpieczeństwa, portal, inne elementy OSE i zapewniająca pełną widoczność wszystkich problemów. W szczególności należy zwrócić uwagę na to, że system OSS, jako system parasolowy dla wszystkich innych systemów dziedzinowych obsługiwany będzie przez stosunkowo niewielki zespół NOC i musi zapewnić szybką analizę stanu sieci (zwłaszcza w sytuacji awarii), zatem jedną z pryncypialnych funkcjonalności, jakie system ma posiadać jest RCA (Route Cause Analysis).

W przypadku sieci szkolnej z uwagi na potencjalną ilość urządzeń zakładane jest monitorowanie w następującym zakresie:

- W ramach podłączenia i przez pewien czas po podłączeniu monitorowane będą urządzenia CPE (fault & availability) oraz CPE, SW, AP (performance)
- W przypadku problemów / awarii i przy decyzji, że niezbędna jest dodatkowa diagnoza będzie włączany monitoring urządzenia CPE (fault & availability) oraz urządzeń CPE, AP, SW (performance). W tych okresach alarmy z CPE będą kierowane przez SIEM do systemu FM oraz w tych okresach system PM będzie pobierał dane performance'owe do statystyk z urządzeń CPE, SW i AP (z tych ostatnich dwóch po odpowiedni przekonfigurowaniu tych urządzeń)

- Dodatkowo niezbędny jest monitoring ruchu w kontekście VLANów szkoły, całej szkoły oraz lokalizacji - zakłada się, że ruch per VLAN będzie zbierany z subinterface'u urządzenia szkieletowego w węźle OSE oraz zebrane dane odpowiednio sumowane by otrzymać ruch per szkoła i per lokalizacja



Z uwagi na:

- uwarunkowania techniczne - wiele różnych modeli stawianych w szkołach urządzeń i związana z tym implementacja MIB w systemie FM versus to, że informacje w SYSLOG są wystarczające i bez dodatkowego nakładu pracy
- logistyczne - jedynie CPE jest w pełni zarządzane przez operatora OSE, a urządzenia SW i AP są przekazywane szkole w jej administrację

operator rezygnuje ze zbierania trap'ów SNMP z urządzeń stawianych w szkole, wysyłane będą wyłącznie logi z urządzenia CPE (SYSLOG) i do systemu monitoringu będą one trafiać za pośrednictwem systemu bezpieczeństwa SIEM (zintegrowanego z OSS).

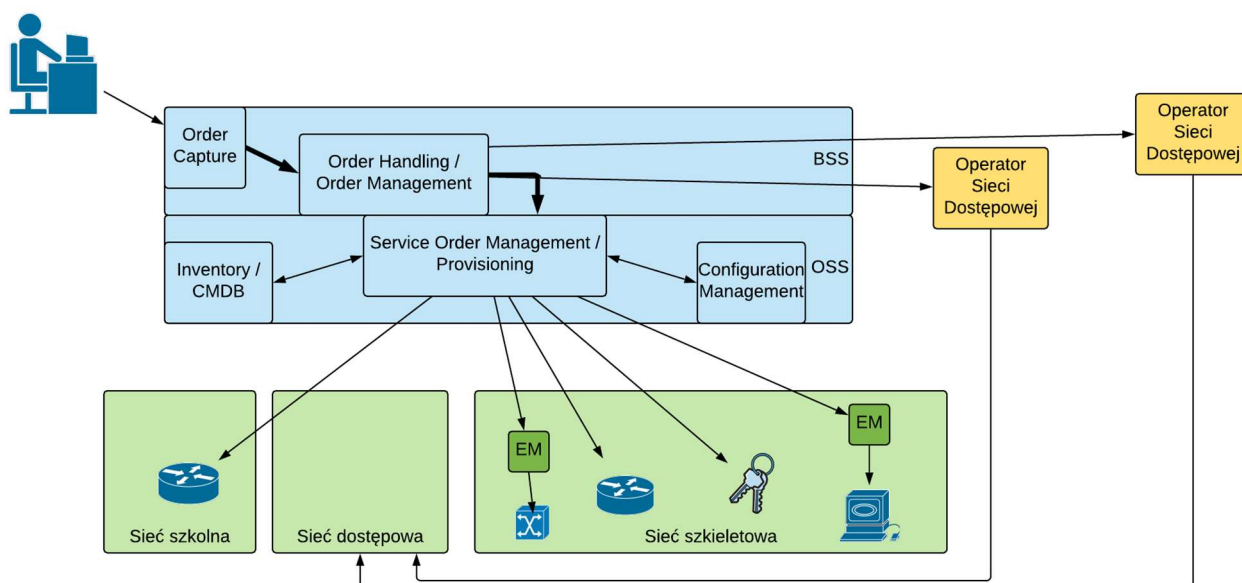
Performance management - swoją funkcjonalnością ma wspierać procesy utrzymania sieci, usług i systemów OSE a w szczególności monitorować wydajność urządzeń i wykorzystanie zasobów sieci OSE.

Zarządzanie konfiguracją - zarządzanie konfiguracją (w tym backupy i wersjonowanie) masowej ilości urządzeń OSE - większość tych urządzeń to heterogeniczny sprzęt instalowany w szkołach w różnorodnych modelach i z różnorodną konfiguracją (zależną od producenta sprzętu). System Config Manager musi objąć swym zasięgiem zarówno sprzęt sieciowy jak i urządzenia bezpieczeństwa OSE w węzłach regionalnych i centralnych. Zarządzaniem konfiguracjami i backupowaniem serwerów OSE ma być realizowane przez dedykowany system do zarządzania infrastrukturą serwerową dostarczony przez Wykonawcę razem z tą infrastrukturą.

Provisioning - automatyzacja procesów obejmuje szereg działań, które są tożsame z provisioningiem niezbędnych konfiguracji w systemach i na sprzęcie OSE a także usług w systemach, co oznacza, co najmniej:

- uzupełnienie/implementacja konfiguracji urządzenia CPE w szkole i urządzeń szkieletowych przy pomocy automatycznych skryptów/polityk itp.,
- uzupełnienie konfiguracji urządzeń w Config Manager (wyzwolenie zaciągnięcia nowej konfiguracji urządzenia, potem cykliczna kontrola zmian w konfiguracji),
- uzupełnienie danych w systemach OSS/BSS dotyczących inwentaryzacji zasobów i stanów magazynowych,
- uruchomienie odpowiednich pomiarów jakości sieci i zbierania zdarzeń i alarmów (Fault & Availability Management),
- uruchomienie odpowiednich pomiarów performance'owych i ruchu w szkielecie i pomiarów ruchu generowanego przez szkoły (performance Management)
- uruchomienie pomiarów urządzeń CPE w okresie 3 tygodni od podłączenia szkoły do OSE
- uruchomienie monitoringu łącz,
- uruchomienie monitoringu świadczonych usług OSE (co najmniej dostęp do internetu i bezpieczeństwa),
- inicjowanie automatycznego procesu generowania statystyk i cyklicznych raportów (w szczególności inicjowanie w SIEM generowania raportów bezpieczeństwa dla danej szkoły i przekazywanie ich na portal usługowy/ CSR)

W architekturze platformy operatora OSE w domenie OSS konieczne jest zapewnienie funkcjonalności związanej z realizacją konfiguracji oraz zmian konfiguracji na urządzeniach sieciowych i urządzeniach/systemach bezpieczeństwa w szkielecie a także urządzeń CPE w szkołach, czyli tzw. docelowy provisioning usług. Z uwagi na specyfikę sieci OSE działania te będą dotyczyć sieci szkolnej i docelowej sieci szkieletowej, zgodnie z poniższym obrazkiem.



Oba te obszary mają charakterystyczne dla nich wyzwania.

W sieci szkolnej provisioning będzie w miarę prostym i standardowym działaniem, jednakże wyzwaniem będzie zapewnienie obsługi różnych modeli urządzeń. O ile przypadku lokalizacji OSE dostępne modele urządzeń będą znane wcześniej (zostaną zakupione w oddzielnym przetargu) to w przypadku lokalizacji POPC lista dostępnych modeli urządzeń może się zmieniać dynamicznie, gdyż za ich dostarczenie odpowiada beneficjent POPC na podstawie własnych uwarunkowań. Natomiast dla modeli podłączenia MAN / ODN w podstawowym wariancie to na Operatorach Sieci Regionalnych (OSR) spoczywa obowiązek zapewnienia i skonfigurowania urządzeń dostępowych (CPE) w sieci szkolnej. W takiej sytuacji po stronie operatora OSE będzie jedynie przygotowanie konfiguracji i przesłanie jej do OSR. W pewnych sytuacjach może się zdarzyć, że będą tam dostawiane urządzenia OSE, należy wtedy zapewnić możliwość ich automatycznej konfiguracji.

Provisioning usług sieciowych i bezpieczeństwa (firewalling) na urządzeniach w szkołach w trakcie podłączenia szkoły do OSE będzie obejmował:

- przygotowanie konfiguracji urządzeń CPE, SW, AP
- w zależności od możliwości danego modelu CPE
 - przygotowanie konfiguracji w formie pliku do wgrania na urządzenie w celu przekazania do Podwykonawcy wykonującego instalację w szkole
 - automatyczne załadowanie docelowej konfiguracji CPE na urządzenie po nawiązaniu łączności z urządzeniem posiadającym inicjalną konfigurację
 - automatyczne załadowanie docelowej konfiguracji CPE na urządzenie z zastosowaniem mechanizmu ZTP (Zero Touch Provisioning)
- w przypadku urządzeń SW i AP
 - przygotowanie konfiguracji w formie pliku do wgrania na urządzenie w celu wysyłki mailem do Podwykonawcy wykonującego instalację w szkole

Należy założyć, co najmniej, że w trakcie "życia usługi" w ramach procesu zmian usług na urządzeniach CPE będą mogły ulegać zmianie:

- parametry związane z przepustowością łącza
- przydzielone adresy publicznych
- inne elementy konfiguracji (w ramach masowych zmian konfiguracji wspólnej dla wszystkich CPE)

Architektura sieci szkieletowej będzie bardziej skomplikowana, chociaż dużym ułatwieniem będzie zamknięty i dobrze znany katalog urządzeń sieciowych. Przed provisioningiem będzie stało zadanie właściwego skonfigurowania wszystkich urządzeń w sieci szkieletowej. Dla części urządzeń dostępne będzie oprogramowanie zarządcze (element manager) jednakże nie można założyć, iż będzie to dla wszystkich urządzeń, w związku, z czym konieczna może być bezpośrednia komunikacja z urządzeniami.

W przypadku potrzeby realizacji provisioningu przy użyciu element manager'a należy założyć wykorzystanie udokumentowanego API producenta tego systemu.

W przypadku provisioningu urządzeń sieciowych w sieci szkieletowej OSE Masowe użycie provisioningu usług sieciowych w szkielecie sieci będzie miało miejsce w trakcie

procesu podłączania szkoły do OSE i będzie obejmowało:

- konfigurację parametrów L2
- konfigurację adresacji IPv4 / IPv6
- konfigurację routingu statycznego w stronę szkoły
- konfigurację QoS na łączu

W przypadku provisioningu urządzeń i systemów bezpieczeństwa w sieci szkieletowej OSE również ułatwieniem będzie znany katalog urządzeń i systemów oraz fakt, że każde z urządzeń będzie posiadać element manager'y. Realizacja provisioningu usług bezpieczeństwa w szkielecie OSE zakłada użycie udokumentowanego API producenta do systemów i do element manager'ów. Provisioning ten jednak komplikuje mnogość tych systemów i operacji, które trzeba na nich wykonać w celu konfiguracji usługi.

Proces podłączenia szkoły zakłada dodanie adresu podsieci IP, wydzielonego z puli 100.64.0.0/10 (Shared Address Space zgodnie z RFC6598 / BCP153) i przydzielonego do danej szkoły, do predefiniowanych na etapie wdrożenia polityk skonfigurowanych na systemach dostarczonych w ramach Infrastruktury bezpieczeństwa (ADC, NGFW, DNS, SWG) oraz inicjacja generowania raportów bezpieczeństwa w SIEM

Proces zmiany konfiguracji usług zakłada modyfikację parametrów polityk zdefiniowanych per szkoła na poszczególnych systemach, w tym w szczególności choć nie wyłącznie:

- Na systemie ADC:
 - Wyjątki definiujące, jaki ruch ma nie podlegać dekrypcji SSL, np. na podstawie źródłowych lub docelowych adresów IP, adresów URL zawartych w parametrach certyfikatu (pola: SNI lub CN)
- Na systemie NGFW:
 - Tworzenie dedykowanych polityk per szkoła blokujących lub przepuszczających ruch z/do zadanych adresów IP, nawiązywany na określonych portach TCP/UDP
 - Włączanie i wyłączanie ruchu mailowego (m. in. protokoły IMAP, POP3) wychodzącego i przychodzącego z/do danej szkoły z analizy antywirusowej
- Na systemie DNS:
 - Włączenie / wyłączenie lub zmiana listy kategorii treści przypisanych do polityk określających poziom ochrony użytkowników OSE
- Na systemie SWG:
 - Tworzenie dedykowanych polityk per szkoła
 - Dodawanie i usuwanie kategorii blokowanych, skonfigurowanych w polityce dla danej szkoły
 - Dodawanie i usuwanie zawartości statycznych list, zawierających adresu URL, definiujących wyjątki od polityki blokowania dla danej szkoły

- Włączanie i wyłączanie ruchu mailowego (protokoły HTTP i HTTPS) wychodzącego i przychodzącego z/do danej szkoły z analizy antywirusowej
- Na systemie SIEM:
 - Generowanie raportu dla danej szkoły, na podstawie predefiniowanych przez Zamawiającego szablonów
 - Określenie harmonogramu generowania raportów dla danej szkoły

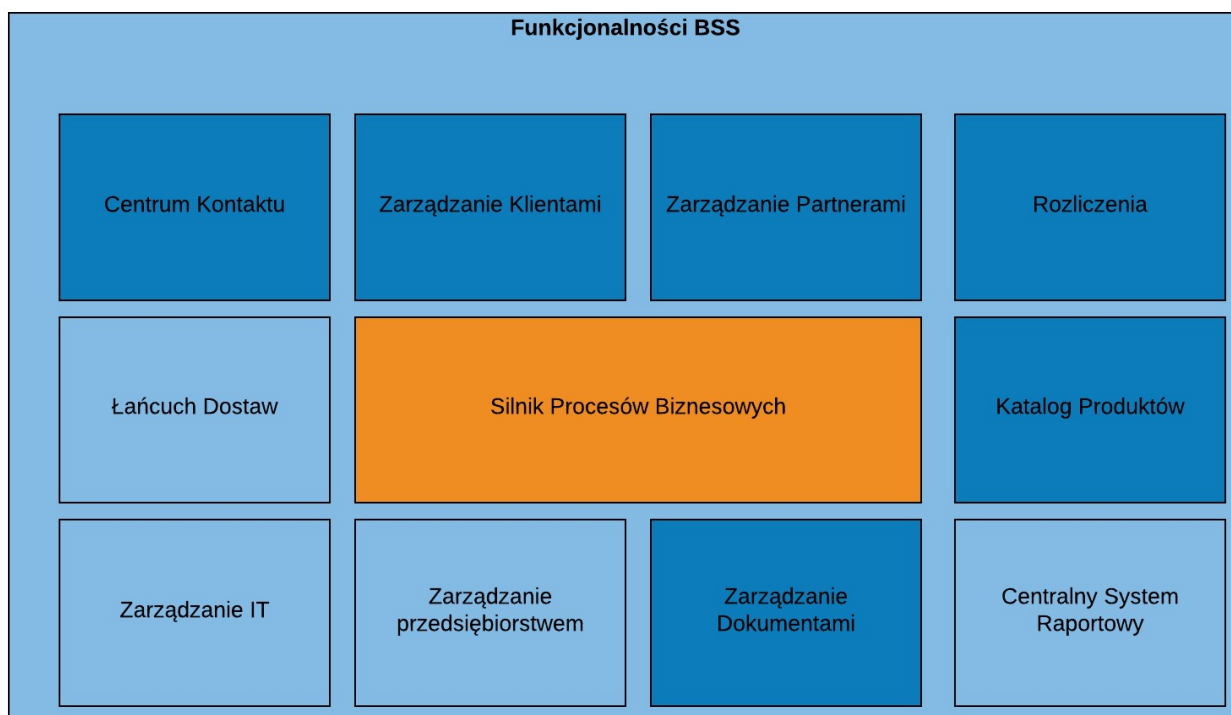
Na etapie Projektu Technicznego Zamawiający doprecyzuje listę i szczegółowy zakres procesów podlegających automatyzacji na dostarczanej przez Wykonawcę Infrastrukturze bezpieczeństwa.

Inwentaryzacja - zbieranie i udostępnianie wszelkich informacji na temat zasobów sieci OSE - zaczynając od informacji technicznych (zarówno o zasobach aktywnych jak i pasywnych, zarówno o zasobach będących własnością Operatora OSE jak i beneficjentów POPC a także o na temat zasobów dzierżawionych jak łącza czy kolokacje) kończąc na informacjach na temat świadczonych usług i ich parametrach. Obiektami w systemie Inwentaryzacji będą, co najmniej:

- serwery i systemy w centrach kolokacyjnych,
- łącza dzierżawione w szkielecie, łącza agregacyjne i dostępne do jednostek oświatowych,
- lokalizacje węzłów szkieletowych (regionalnych i centralnych),
- sprzęt kolokacyjny OSE umiejscowionym w lokalizacjach węzłów,
- sprzęt i systemy sieciowe i bezpieczeństwa zainstalowane w węzłach OSE (dane szczegółowe, np. hardware, software, licencje, serwis itp.),
- lokalizacje jednostek oświatowych (dane teleadresowe, partner serwisowy obsługujący szkołę, operator łącza podłączającego szkołę itp.),
- sprzęt zainstalowany w danej jednostce oświatowej,
- połączenia pomiędzy urządzeniami,
- katalog dostępnych typów urządzeń i producentów,
- katalog dostępnego oprogramowania,
- katalog świadczonych usług (powiązanie z zasobami technicznymi sieci OSE, parametry usług, powiązanie między usługami)

6.1.2. Funkcjonalności obszaru BSS

Oczekiwane w rozwiązaniu systemu obszaru BSS możemy zgrupować wokół funkcjonalności zgodnie z poniższym rysunkiem:



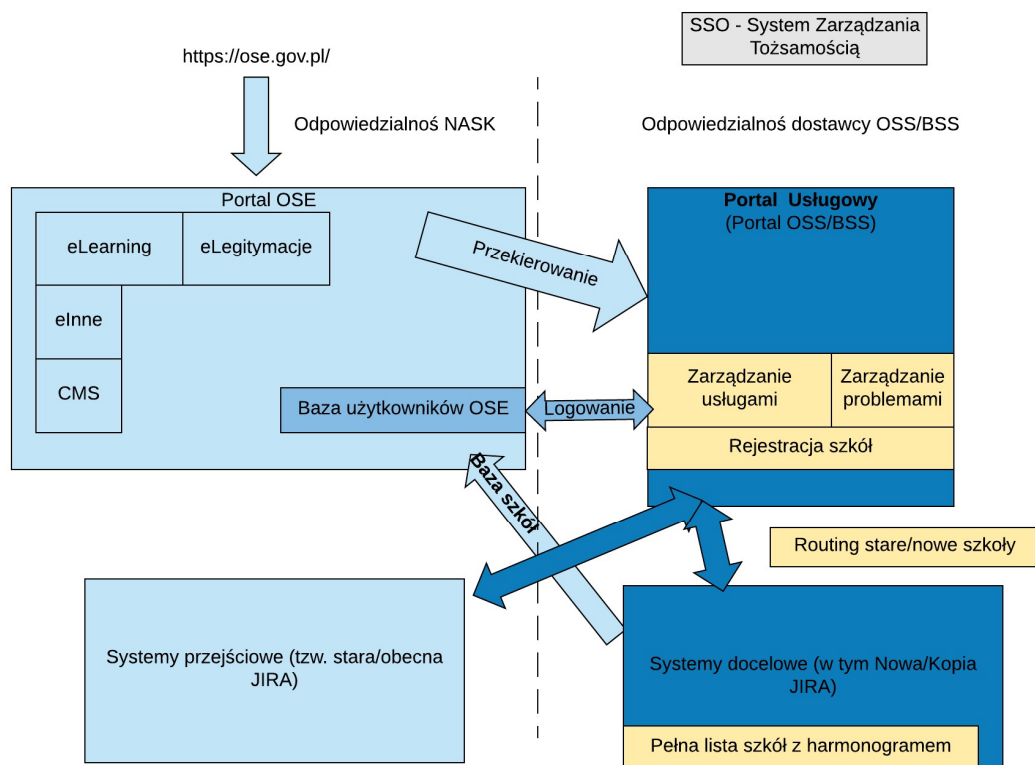
Centrum Kontaktu - obszar funkcjonalny odpowiedzialny za wsparcie działań związanych z kontaktem z klientami poprzez wszelkie kanały komunikacyjne takie jak. np. IVR czy Call Center.

W tym obszarze szczególnie istotny jest obszar Portalu

W architekturze platformy operatora OSE w domenie Portali (obszar samoobsługowy klienta) znajduje się komponent Portal OSE pełniący rolę oferujący następujące funkcjonalności:

- rejestracji szkół
- zarządzania usługami OSE, zgłaszanie problemów
- zarządzania użytkownikami OSE
- platforma usług dodatkowych opartych o OSE dla osób korzystających z OSE (uczniowie, nauczyciele).

W modelu docelowym funkcjonalności zostaną rozdzielona na dwa komponenty zgodnie z poniższym rysunkiem.



Portal OSE pełniący rolę "wizytówki" świata OSE będzie punktem wejściowym i będzie odpowiedzialny za prezentację treści dotyczących OSE (zarówno dostępnych dla wszystkich jak i dedykowanych do konkretnych użytkowników OSE). Portal OSE będzie również platformą udostępniania usług opartych o OSE a także miejscem zarządzania wszystkimi użytkownikami OSE. Będzie również odpowiedzialny za przekierowywanie użytkowników do Portalu Usługowego.

Portal Usługowy będzie komponentem dedykowanym do samoobsługi klientów / użytkowników usług OSE umożliwiając również rejestrację nowych szkół. Za pośrednictwem Portalu Usługowego będzie również dostępna funkcjonalność do zgłaszania problemów.

W pośrednich etapach wdrożenia będzie również odpowiedzialny za kierowanie komunikacji do właściwej grupy systemów (przejściowych lub docelowych).

Katalog Produktów - obszar funkcjonalny odpowiedzialny za wsparcie wszelkich działań związanych z zarządzaniem produktami, cyklem życia produktów, ofertami, cennikami, monitorowaniem produktów, zapewnieniem odpowiednich zasobów dla produktów.

Zarządzanie Klientami - podstawowy obszar funkcjonalny wspierający realizację wszelkich działań skoncentrowanych na klientach, zarządzaniem informacją o kliencie, jego produktach, umowach, realizacja procesów dostarczania produktów (order management)

Zarządzanie Partnerami - obszar funkcjonalny wspierający zarządzanie relacjami i kontaktami z partnerami takimi jak operatorzy czy partnerzy serwisowi, zarządzanie pracami (workforce management)

Rozliczenia - obszar grupujący funkcjonalności związane z rozliczeniami z klientami i partnerami, rozliczanie produktów, rozliczanie zamówień od partnerów i dostawców, zarządzanie należnościami, windykację

Zarządzanie Dokumentami - obszar funkcjonalny wspierający zarządzanie dokumentami, składowanie, generowanie, udostępnianie, zarządzanie wzorcami dokumentów, archiwizację

Centralny System Raportowy - funkcjonalność odpowiedzialna za generowania wszystkich raportów: finansowych, operacyjnych, SLA, rozliczeniowych, performance'owych a także raportów bezpieczeństwa w szkołach.

Łańcuch Dostaw - obszar funkcjonalny do wsparcia procesów logistycznych i magazynowych

Zarządzanie IT - zarządzanie zasobami informatycznymi przedsiębiorstwa, środowiskami IT, procesami rozwoju i utrzymania systemów

Zarządzanie Przedsiębiorstwem - zarządzanie przedsiębiorstwem, prowadzenie finansów i rozliczeń przedsiębiorstwa, zarządzanie wiedzą i kapitałem ludzkim

Silnik Procesów Biznesowych - kluczowy komponent wspierający realizację procesów we wszystkich obszarach funkcjonalnych

6.2. Warstwa infrastruktury

6.2.1. Wstęp

Wymagane jest dostarczenie infrastruktury aplikacyjno-sprzętowej, która będzie się składać na środowisko uruchomieniowe oraz dodatkowo będzie dostarczała zasobów dla środowisk testowych. Głównym celem istnienia zwirtualizowanej infrastruktury obliczeniowej jest zapewnienie zasobów dla:

- systemów OSS/BSS
- portalu OSE
- przechowywanie danych blokowych i obiektowych
- wirtualnej sieci – SDN
- backupu środowiska i systemu odtwarzania po awarii
- systemu zarządzania tożsamością
- systemów zarządzania, monitorowania chmury i opcjonalnie automatyzacji
- system klasy SIEM (Security Information and Event)
- innych systemów wspierających infrastrukturę OSE

Pozostałe wymagania dla dostawcy przy projektowaniu środowiska:

- zapewnienie odpowiedniej mocy obliczeniowej i powierzchni do składowania danych dla powyższych systemów jak również dla systemów pomocniczych;
- wysoka skalowalność rozwiązania i efektywne wykorzystanie zasobów sprzętowych poprzez implementację środowiska na platformie zwirtualizowanej;
- zapewnienie wysokiej dostępności, integralności i poufności informacji przechowywanych w środowisku;
- efektywne przechowywanie i analiza logów pochodzących z różnych źródeł

- automatyzacja i efektywne wykonywanie kopii zapasowych zapewniających możliwość odtworzenia systemu oraz bezstratnego odtworzenia danych i dokumentów na wypadek katastrofy (Disaster Recovery Plan);
- możliwości zapewnienia niezmienności przechowywanych danych;
- uproszczenie zarządzania infrastrukturą, przechowywaniem danych, bezpieczeństwem i wprowadzaniem zmian w infrastrukturze;
- zapewnienie odpowiedniej ilości licencji na oprogramowanie w infrastrukturze.

Założeniem projektu architektury jest maksymalna integracja systemów w ramach platformy i uproszczenie procesów dokonywania zmian w systemach. Zbudowanie środowiska, które zminimalizuje ilości administratorów potrzebnych do utrzymania go. Służyć temu ma uruchomienie wszystkich możliwych elementów odpowiedzialnych za obsługę, nadzorowanie i zarządzanie infrastrukturą w formie maszyn wirtualnych na zasobach chmury, a także ujednolicenie technologii używanej do budowy środowiska.

6.2.2. Założenia techniczne

Wymagana jest architektura zbudowana w modelu chmury prywatnej. Architektura musi zakładać, że infrastruktura obliczeniowa ma być rozciągniętą pomiędzy dwoma centralnymi aktywnymi ośrodkami przetwarzania danych (**OPD**) – OPD1 i OPD2, trzeci centralny ośrodek (OPD3) będzie pełnił rolę świadka oraz miejsca przechowywania kopii zapasowych wraz z archiwum. Architektura zakłada również 16 regionalnych ośrodków przetwarzania danych, z których każdy będzie podłączony do centralnych OPD. Środowiska w regionalnych ośrodkach będą różnej wielkości, ich rozmiar będzie dostosowany do potrzeb systemów SIEM i ściśle uzależniony od ilości logów zbieranych w danym regionie. Trzy regionalne ośrodki danych będą mieściły się w tych samych centrach danych, co centralne ośrodki przetwarzania danych. W celu zapewnienia odpowiedniej ciągłości działania, **OPD** będą znacznie oddalone od siebie w celu zminimalizowania wpływu zdarzeń losowych na ciągłość działania systemu. Pomiędzy wybranymi centrami będzie dostępna wydajna sieć umożliwiająca synchronizację i replikację krytycznych danych.

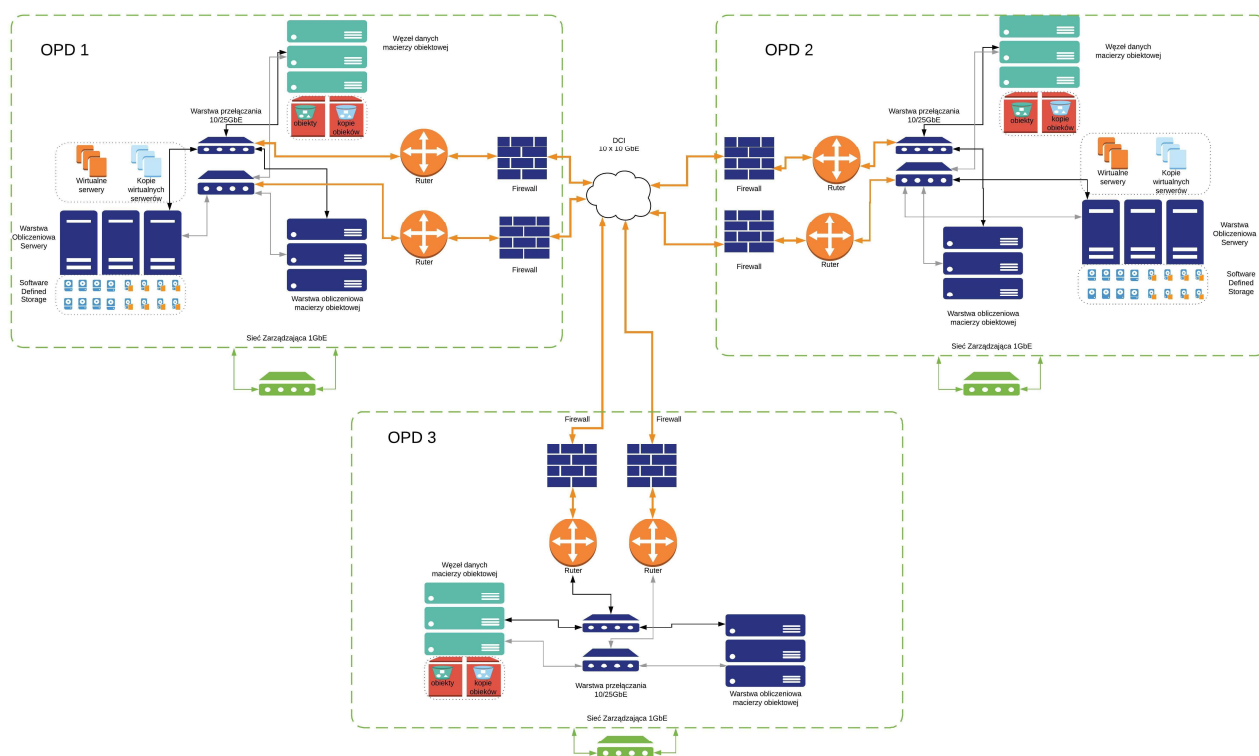
Wymagana jest taka architektura rozwiązania, która zminimalizuje nakłady pracy ludzkiej związanej z procesem utrzymania i integracji stosu obliczeniowego, sieciowego, pamięci masowych oraz wirtualizacji. Wymaga się użycia rozwiązań pozwalających zautomatyzować zarządzanie infrastrukturą. Poniżej zebrano główne założenia techniczne infrastruktury chmury obliczeniowej, które dostawca musi spełnić w kontekście infrastruktury obliczeniowej:

1. Infrastruktura chmury obliczeniowej ma być jak najbardziej zintegrowana i prosta w zarządzaniu oraz odporna na awarie, musi obejmować zarówno warstwę sprzętową, jak i część niezbędnego oprogramowania.
2. Możliwe wszystkie systemy muszą być uruchamiane, jako maszyny wirtualne.
3. Infrastruktura zostanie tak zaplanowana, aby zapewnić pełną ciągłość działania w przypadku całkowitej awarii jednego z dwóch głównych węzłów OPD1 i OPD2.
4. Wszystkie typy danych będą chronione poziomem nadmiarowości min. N+1
5. Wdrożone rozwiązanie informatyczne musi pracować w architekturze redundantnej. Replikacja musi być zrealizowana w taki sposób, dwa główne ośrodki (OPD1 i OPD2) mogły korzystać z systemów

storage, na których uruchomione będą usługi produkcyjne - czyli np. połowa zasobów dyskowych musi być dostępna w każdym OPD, reszta musi być wykorzystana na replikację.

6. Architektura rozwiązania musi umożliwiać przełączenie przetwarzania pomiędzy węzłami przetwarzania danych – z jednego głównego OPD do drugiego i odwrotnie.
7. Rozwiązanie infrastruktury chmury obliczeniowej w ramach głównych OPD musi posiadać funkcjonalność, która pozwala na zautomatyzowany failover oraz failback infrastruktury maszyn wirtualnych w przypadku wystąpienia awarii jednego z głównych OPD.
8. *Wdrażane rozwiązanie informatyczne chmury obliczeniowej musi umożliwiać ochronę przetwarzanych w nim danych, w tym gwarantować ich:*
 - *rozliczalność - zapewniać możliwość rozliczenia osoby, która uzyskała dostęp do informacji na podstawie mechanizmów identyfikacji i uwierzytelnienia*
 - *ochronę przed nieautoryzowanymi, nieprzewidywalnymi, niezamierzonymi modyfikacjami informacji,*
 - *ochronę poufności informacji np. danych osobowych,*
 - *zachowanie spójności danych,*
 - *zapewniać dostęp do informacji.*
9. Rozwiązanie musi wspierać proces automatycznego logowania (SSO) jak i manualnego (za pomocą loginu i hasła).
10. Rozwiązanie musi posiadać mechanizmy kontroli dostępu, możliwość budowy zasad oraz polityk w zakresie haseł.
11. Planowane do wdrożenia rozwiązanie informatyczne chmury obliczeniowej musi wspierać architekturę, która zapewni, że awaria jednego elementu rozwiązania informatycznego chmury obliczeniowej dostępnego w ramach pojedynczego OPD nie powoduje niedostępności usługi/rozwiązania informatycznego chmury obliczeniowej, a jedynie spadek jej wydajności. Warunek ten nie musi zostać spełniony, jeżeli awarii ulega ostatni element danego typu.
12. Przyjęto, że każdy system programowy i możliwie każdy sprzętowy wykorzystywany w chmurze musi posiadać natywne API, lub umożliwiać automatyzację procesów m.in. poprzez integrację z systemami OSS i BSS.
13. Dostęp do rozwiązania infrastruktury obliczeniowej dla administratorów musi być możliwy m.in. za pośrednictwem przeglądarki internetowej (np. połączenie szyfrowane SSL).
14. Architektura rozwiązania informatycznego chmury obliczeniowej musi umożliwiać tworzenie klastra wysokiej dostępności (HA) w obrębie OPD oraz pozwalać na wdrożenie mechanizmu niezawodności (DR) pomiędzy OPD 1 i 2.

Modelowa infrastruktura chmury obliczeniowej jest przedstawiona na poniższym schemacie. Poszczególne części opisane są w kolejnych akapitach.



6.2.3. Ośrodki przetwarzania danych

Wymaga się dostarczenia Infrastruktury opartej o trzy główne ośrodki przetwarzania danych, zrealizowanej, jako klastry, jak i 16 wysoko dostępnych ośrodków regionalnych.

Planowana infrastruktura obliczeniowa ma być rozdzielona na dwa aktywne ośrodki przetwarzania danych (OPD1 i OPD2). W każdym z tych ośrodków będzie dostępna równoważna infrastruktura sieciowa. Odpowiednia przepustowość zarówno do WAN, jak i sieci pomiędzy OPD będą zapewnione przez OSE. OPD1 i OPD2 będą miejscem przechowywania kopii zapasowych środowiska na potrzeby zapewnienia ciągłości działania po awarii OPD. W szczególności:

- kopie zapasowe maszyn wirtualnych wraz z ich konfiguracją i obrazami wraz z archiwum,
- konfigurację wirtualnych centrów danych zawierającą konfigurację sieci, storage-u, automatyzację, logi, konfigurację wirtualizatorów etc..
- kopie zapasowe plików i obiektów,
- backup baz danych aplikacji wraz z katalogami użytkowników i ich uprawnieniami,
- backup systemów zarządzających, monitorujących, raportujących, bezpieczeństwa, konfigurację urządzeń fizycznych (przełączników, ruterów, firewall-i)

Trzeci ośrodek przetwarzania danych (OPD3) nie będzie posiadał infrastruktury obliczeniowej, SDS jak również SDN. Ośrodek ten będzie posiadał część obiektowego systemu przetwarzania danych.

Dla zapewnienia efektywnego, bezpiecznego, a także szybkiego przesyłania i składowania danych pomiędzy ośrodkami, dostawca powinien wykorzystać systemy zapewniające mechanizmy deduplikacji, kompresji i szyfrowania danych.

System przechowywania danych blokowych musi znajdować się w OPD1 i OPD2 i być wykorzystywany możliwie tylko do udostępniania danych dla systemów wirtualizacji.

Dane plikowe (Plik) i blokowe (Blok) z OPD1 będą replikowane do OPD2 a z OPD2 do OPD1. Infrastruktura serwerowa musi zostać zaprojektowana w taki sposób, aby zapewnić działanie systemu przy awarii jednego fizycznego serwera w klastrze (nadmiarowość N+1), jak również w przypadku awarii całego ośrodka OPD (odtworzenie po awarii – Disaster Recovery). Dla zapewnienia większej elastyczności, odporności na awarie sprzętu, lepszego wykorzystania zasobów serwerowych, a także automatyzację zadań administracyjnych należy zastosować technologie wirtualizacji zasobów obliczeniowych i sieciowych, jak również wirtualizacji zasobów przechowujących dane.

Infrastruktura obliczeniowa musi zostać zrealizowana, jako zestaw klastrów lokalnych w obu centralnych OPD (OPD1 i OPD2). Rozwiązanie musi posiadać mechanizmy wysokiej dostępności (HA) wbudowane w oprogramowanie zarządzające środowiskiem wirtualnym.

We wszystkich centralnych ośrodkach OPD musi zostać rozproszony system archiwum opartego o obiektowy system przechowywania plików (Obiekt + WORM), do którego przesyłane będą dane przeznaczone do składowania długoterminowego. Dane archiwalne będą składowane na tym samym urządzeniu, które obsługuje dane aktywne. Separacja powinna zostać wykonana za pomocą mechanizmów programowych. Dodatkowo dla zapewnienia wysokiego bezpieczeństwa danych archiwalnych, dane te powinny mieć możliwość zabezpieczenia technologią WORM - Write once read many, która pozwoli na zapisanie informacji na urządzeniu, ale nie pozwoli jej usunąć lub zmodyfikować.

6.2.4. Skalowalność systemu

Budowane środowisko powinno być stworzone na platformie sprzętowej o wydajności i poziomie bezpieczeństwa odpowiednim dla powyższych założeń. Istotne jest, aby środowisko było możliwie uniwersalne, otwarte na potencjalne zmiany, przy jednoczesnym zachowaniu wsparcia wielu technologii. W warstwie fizycznej należy wyróżnić komponenty:

- komponenty infrastruktury sieciowej,
- serwery zapewniające moc obliczeniową chmury i bezpieczne przechowywanie danych,
- zasoby storage pozwalające na bezpieczne przechowywanie danych,
- systemy bezpieczeństwa oraz systemy monitorowania i zarządzania infrastrukturą.

Wymagane jest, aby budowa infrastruktury została oparta o tzw. „building blocks” w kontekście całości architektury, dotyczy to również sieci. Sieć powinna być zaprojektowana taki sposób, aby wymagana rozbudowa zasobów serwerowych lub storage była łatwo policzalna i nie wymagała ciągłych zmian w rdzeniu sieci. Narzędzia oraz procesy zastosowane w rozwiązaniu, służące do zarządzania infrastrukturą, powinny działać w sposób całkowicie zintegrowany i holistyczny. Rozwiązanie powinno posiadać budowę modułową, i charakteryzować się dużą elastycznością w tworzeniu połączeń konfiguracyjnych poszczególnych komponentów. Poszczególne elementy systemu powinny być zwirtualizowane, przy zachowaniu przez infrastrukturę fizyczną wymaganej zdolności do przeprowadzania dynamicznych zmian przy zapewnieniu wysokiej niezawodności. Konstrukcji rozwiązania powinna umożliwiać eliminowanie jednorazowych prac projektowych i łatwą i szybką wymianę uszkodzonych modułów wymienić bez konieczności wyłączania całego systemu. Rozwiązania ma łączyć w sobie elastyczność systemów ogólnego przeznaczenia i środowisk przetwarzania w chmurze oraz prostotę dedykowanego urządzenia (ew. bloku). Oznaczać się możliwością szybkiego tworzenia, wdrażania i zmian pod kątem aplikacji za

pomocą sprawdzonych wzorców. Aktualizacje wersji wszystkich komponentów powinny być realizowane możliwie dla całego modułu i w prosty sposób.

Wymagane jest, aby środowiska w regionalnych centrach danych zapewniały wysoką dostępność na wypadek awarii jednego serwera.

6.2.5. Magazyn danych

Magazyn danych blokowych

Dostęp do blokowej powierzchni dyskowej zarówno w węzłach centralnych jak i w regionach powinien opierać się na koncepcji Software Defined Storage, która pozwala stworzyć współdzieloną przestrzeń dyskową z zasobów bezpośrednio wbudowanych w serwery. Zasoby serwerowe i dedykowane wirtualne serwery posłużą do udostępniania przestrzeni blokowej i plikowej. Rozwiązanie musi umożliwiać łatwe skalowanie wertykalne jak i horyzontalne. Przestrzeń ta będzie przeznaczona do składowania wirtualnych maszyn wraz z obrazami środowiska wirtualnego.

Storage ten musi zapewnić niskie czasy odpowiedzi dla dostępu do danych, jak również możliwość dużej ilości odczytów i zapisów (IOPS). System powinien zapewnić również wielką łatwość i elastyczność w tworzeniu przestrzeni danych o różnym stopniu zabezpieczenia jak i prędkości odczytu i zapisu. Rozwiązanie powinno pozwolić w przyszłości, na co najmniej dziesięciokrotny wzrost pojemności wraz z zapewnieniem par HA (wysokiej dostępności). System SDS powinien mieć możliwość skalowania do kilkudziesięciu serwerów (każdy zawierający kilkadziesiąt dysków) i uzyskanie całkowitej pojemności rzędu PB petabajtów.

Magazyn danych obiektowych.

Preferowanym rozwiązaniem do długoterminowego przechowywania i zabezpieczania danych jak i dla funkcjonalności archiwum danych jest obiektowy system przetwarzania danych. Obiektowy oznacza, że operujemy na poziomie obiektów (a nie plików), na które składają się: dane, metadane systemowe i metadane własne oraz polityki (np. retencja, replikacja, wersjonowanie, tiering). Metadane własne pozwalają na opisanie zawartości lub kontekstu obiektów oraz użycie tych informacji w tworzeniu polityk.

Rozwiązanie storage-u obiektowego musi posiadać funkcjonalność WORM („Write Ones Read Many”) gwarantującą niezmiennność raz zapisanych danych dla wybranych obszarów pamięci obiektowej. Dodatkowo storage obiektowy musi zapewnić funkcjonalność archiwum, w którym można zdefiniować politykę przechowywania danych (retencji) zapewniającą niezmiennność danych przez cały czas życia archiwum lub zdefiniowany okres ich przechowywania, niemożliwość skasowania danych, także przez operatora (administratora), niezmiennność metadanych (opisów/ metryk) opisujących dane po ich wprowadzeniu, śledzenie zmian w danych i metadanych oraz śledzenie dostępu do danych. Replikacja powinna odbywać w technologii geograficznie rozproszonego klastra urządzeń - Global Access Topology, pracujących w trybie aktywny-aktywny. Obiekty (jednostki archiwalne) muszą być przechowywane w minimum dwóch punktach. Kopie powinny zostać tworzone automatycznie w oparciu o zdefiniowane polityki bezpieczeństwa. System pamięci obiektowej nie może posiadać pojedynczego punktu awarii (one point of failure) i działać w trybie HA (wysokiej dostępności) a RPO = 0.

Rozwiązanie powinno zapewnić niezmiennność oraz bezpieczeństwo danych po przez takie mechanizmy jak: WORM, replikację w ramach szyfrowanego kanału, system kluczy „hash”, klucz dla każdego obiektu przechowywanego w pamięci, weryfikacja spójności klucza w trakcie czasu życia obiektu w pamięci,

retencję, wersjonowanie, bezpowrotne niszczenie danych, mechanizm migracji na nową generację sprzętu przy zachowaniu polityk i łańcucha dozoru, sprawdzanie spójności danych.

6.2.6. Architektura sieci

Ze względu na dużą skalę przedsięwzięcia, ilość serwerów wirtualnych, instancji i ich środowisk, które należy zaimplementować i nadzorować w obszarze zarządzania infrastrukturą zwirtualizowaną należy zastosować technologię SDN (Software Defined Network), aby zapewnić:

- Niezależność rozwiązania od fizycznej struktury sieci:
 - Sieć fizyczna może być oparta o różne urządzenia sieciowe,
 - Nowe usługi uruchomione w warstwie wirtualnej nie wymagają konfiguracji warstwy fizycznej;
- Rozciągnięcie sieci na oba węzły OPD1 i OPD2 z możliwością dołączenia 16 węzłów regionalnych;
- Skalowalność środowiska;
- Programowe i częściowo automatyczne zarządzanie całością topologii sieciowej;
- Izolację środowisk:
 - mikro segmentacja środowiska,
 - błędy w konfiguracji jednego środowiska nie wpływają na inne.
- Możliwość zapewnienia wysokiej dostępności usług i wdrożenia mechanizmu Disaster Recovery ciągłości biznesowej w zakresie infrastruktury OSE:
 - możliwość migracji maszyn wirtualnych bez przebudowy polityk,
 - awaria w środowisku wirtualnym nie przenosi się na środowisko fizyczne,
 - brak wpływu awarii sprzętu/węzła na usługę.
- Zwiększenie bezpieczeństwa całego rozwiązania poprzez:
 - zwiększenie bezpieczeństwa transmisji danych
 - granulowanie polityk bezpieczeństwa
 - automatyzację tworzenia polityk bezpieczeństwa.

Ze względu na założenia przyjęte w architekturze sieci data center wyklucza się użycie technologii Fiber Chanel i InfiniBand.

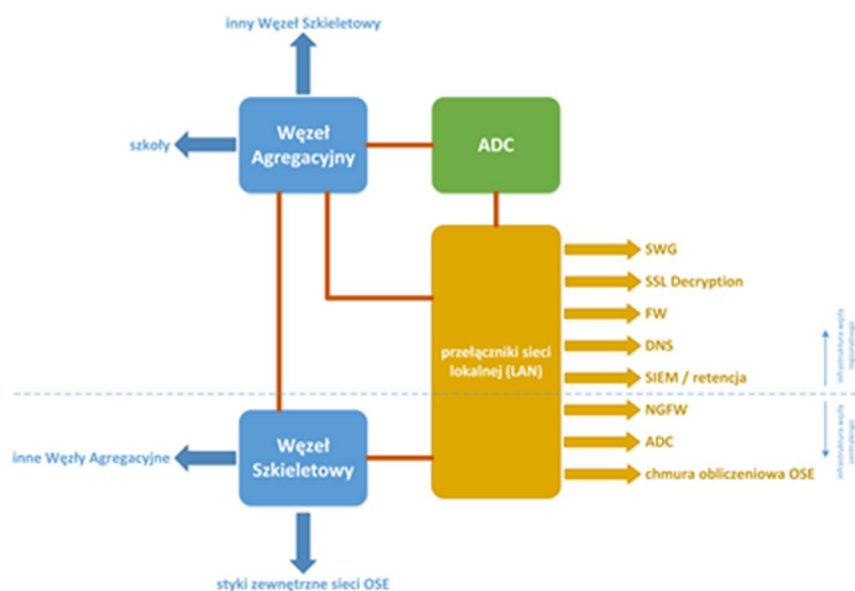
Przełączniki odpowiedzialne za realizację agregacji datacenter będą wdrożone w każdym z OPD min. dwa urządzenia zapewniające HA dla ruchu sieciowego. Sieć agregacyjna w obrębie OPD będzie umożliwiać skalowanie horyzontalne zasobów obliczeniowych, przy równoczesnym zapewnieniu zbliżonych do siebie opóźnień i takiej samej ilości przełączeń na warstwie sieciowej. Architektura sieci w OPD będzie zrealizowana w zgodzie z paradygmatem Closs'a - Leaf and Spine. Infrastruktura fizyczna zapewni wsparcie dla technologii SDN – m. in. obsługa Jumbo Frames, niezbędne Protokoły Routingu i Multicast.

Przełączniki sieci lokalnej dla węzłów centralnych jak i regionalnych zostaną zapewnione przez Zamawiającego wraz z siecią szkieletową i agregacyjną. Poniżej zamieszczone są wymagania specyficzne jak i szczegółowe dla przełączników sieci lokalnej, które zostaną wymagane w osobnym przetargu.

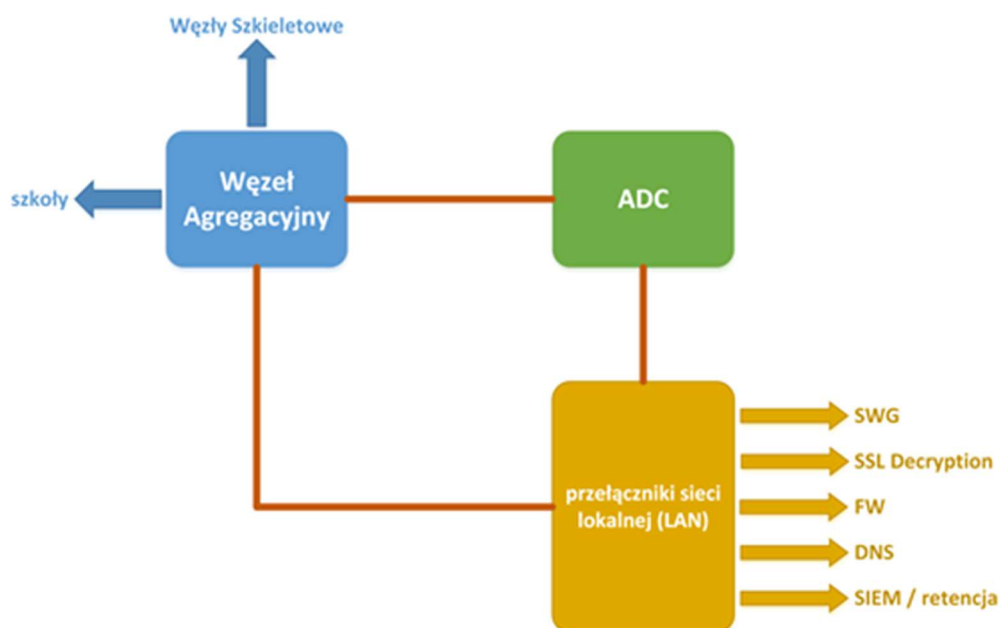
Wymagania na przełączniki sieci lokalnej

Przełączniki sieci lokalnej będą zainstalowane w każdym z węzłów. Przełączniki te będą obsługiwały urządzenia zainstalowane w węzłach, w szczególności urządzenia Węzła Bezpieczeństwa, systemy zbierania i retencji logów telekomunikacyjnych oraz infrastruktury obliczeniowej, na której będą posadowione systemy OSS/BSS i sieć OSE.

Struktura połączeń poszczególnych elementów Węzła Centralnego i Regionalnego przedstawiona jest poniżej:



Struktura połączeń Węzła Centralnego



Struktura połączeń Węzła Regionalnego

W dalszej części punktu słowa przełącznik oraz urządzenie używane są wymiennie.

Wszystkie przełączniki muszą spełniać następujące wymagania:

1. Wymagania ogólne

1.1. Wszystkie oferowane przełączniki (wraz z zainstalowanym na nich oprogramowaniem) muszą pochodzić od jednego producenta.

1.1.1. Wykonawca musi być oficjalnym sprzedawcą w Polsce oferowanych urządzeń.

1.1.2. Wykonawca musi mieć możliwość świadczenia autoryzowanego przez producenta serwisu gwarancyjnego.

1.2. Urządzenie musi być przystosowane do instalacji w standardowych 19" szafach teleinformatycznych (EIA-310-D, IEC 60297). Urządzenie musi posiadać wszystkie elementy potrzebne do zainstalowania go w szafie.

1.2.1. Urządzenie musi umożliwiać zapewnić możliwość montażu w szafie teleinformatycznej o głębokości 1000mm, tj. głębokość i konstrukcja urządzenia muszą zapewnić w szafie o takiej głębokości dołączenie zasilania, przewodów światłowodowych oraz miedzianych przy zapewnieniu wymaganych profili zginania przewodów.

1.3. Urządzenie musi być wyposażone w zasilacze dostosowane do napięcia przemiennego 230V. Dostarczone urządzenie będzie wyposażone w odpowiednią liczbę kabli zasilających pozwalających na podłączenie wszystkich zasilaczy, w jakie jest wyposażone urządzenie do standardowych gniazd zasilających.

1.3.1. Dostarczone zasilacze muszą umożliwiać dołączenie urządzenia do dwóch niezależnych obwodów zasilających (dwa zestawy gniazd) oraz poprawną pracę urządzenia w pełnej, wymaganej przez Zamawiającego, konfiguracji z wykorzystaniem zasilania z jednego obwodu, przy zachowaniu pełnej funkcjonalności urządzenia.

1.3.2. Dostarczone urządzenie musi umożliwiać pracę z pełną funkcjonalnością w pełnej, wymaganej przez Zamawiającego, konfiguracji przy wyłączeniu, co najmniej jednego zasilacza.

1.4. Urządzenie musi poprawnie pracować w temperaturze otoczenia od 5 do 40 °C.

1.5. Urządzenie musi poprawnie pracować przy wilgotności powietrza od 10% do 80% zakładając brak występowania zjawiska kondensacji pary wodnej.

1.6. Urządzenie musi umożliwiać możliwość instalacji, wymiany lub zamiany poszczególnych modułów (takich jak np. zasilacze, wentylatory, karty z interfejsami sieciowymi, moduły optyczne typu SFP / XFP / itd.) w trakcie pracy urządzenia (ang. hot-swap).

1.7. Wszystkie wymagane funkcjonalności muszą być dostępne w jednej, komercyjnie dostępnej wersji oprogramowania, tj. wersji oferowanej wszystkim klientom. Wersja ta musi być wersją rekomendowaną przez producenta. Niedopuszczalne jest wytwarzanie wersji oprogramowania wyłącznie na potrzeby Zamawiającego, nieoferowanej innym klientom.

1.8. Dokumentacja do urządzenia (w tym oprogramowania) musi być dostępna w całości w języku polskim lub angielskim. Dokumentacja musi być dostarczona w formie elektronicznej, w formacie ogólnodostępnym (PDF, DOC, DOCX, ODF, HTML) lub dostępna na stronie producenta urządzenia (jeżeli dostęp do tej dokumentacji wymaga autoryzacji Wykonawca zapewni do niej dostęp dla wskazanych pracowników Zamawiającego lub podmiotów wskazanych przez Zamawiającego). W przypadku dokumentacji on-line musi istnieć możliwość jej pobrania do przeglądania off-line.

1. Wymagania na interfejsy

2.1. Interfejsy 1GE, 10 GE, 25 GE, 40GE i 100GE muszą być zgodne z właściwą dla danego typu interfejsu normą IEEE 802.3.

2.2. Karty liniowe lub moduły urządzenia zawierające interfejsy przeznaczone do obsadzenia modułami optycznymi (ang. transceiver), muszą współpracować z modułami optycznymi (zgodnymi z ogólnie przyjętymi normami właściwymi dla danego typu interfejsu), pochodzącymi od różnych producentów^[1]. Instalacja modułów optycznych pochodzących od innych producentów nie może powodować utraty, ograniczenia lub zawieszenia gwarancji na urządzenie ani ograniczeń w świadczeniu usług serwisowych

Wykorzystywanie modułów optycznych innych producentów nie może wymagać restartu urządzenia ani nie może powodować konieczności wykonania prac serwisowych, utrzymaniowych lub konfiguracyjnych (dopuszczalne jest jednorazowe uruchomienie funkcjonalności dla całego urządzenia umożliwiające korzystanie z ww. wkładek instalowanych w dowolnym momencie).

2.3. Dostarczone moduły optyczne muszą umożliwiać możliwość sprawdzenia mocy odbieranego sygnału, tj. muszą wspierać funkcjonalność digital diagnostics monitoring (DDM)^[2] zgodną z SFF-8472 (Digital Diagnostics Monitoring, Digital Optical Monitoring) lub równoważne

2.4. Urządzenie musi obsługiwać ramki Ethernet o wielkości, co najmniej 9100B.

2.5. Wszystkie interfejsy liniowe zainstalowane w urządzeniu (bezpośrednio w chassis lub na kartach interfejsów) muszą być odblokowane. Oznacza to, że nie mogą posiadać żadnych blokad umożliwiających ich wykorzystanie dopiero po wprowadzeniu jakiegokolwiek licencji, klucza, kodu lub innego mechanizmu odblokowującego. Dotyczy to wszystkich interfejsów znajdujących się fizycznie w oferowanym urządzeniu.

2.6. Urządzenie musi wspierać pojedyncze i podwójne tagowanie ramek ethernet (zgodnie ze standardem IEEE 802.1q i IEEE 802.1ad).

2.7. Przełącznik musi wspierać agregację łączy ethernet zgodną ze standardem 802.3ad (LACP).

2.7.1.Przełącznik musi umożliwiać utworzenie nie mniej niż 64 interfejsów zagregowanych.

2.7.2.Przełącznik musi umożliwiać tworzenie grup LAG składających się, z co najmniej 8 interfejsów składowych, przy czym nie może być ograniczeń, co do lokalizacji tych interfejsów na kartach interfejsów (dla urządzeń modularnych), zaś dla urządzeń wirtualnych zbudowanych z wielu urządzeń składowych musi być zapewniona możliwość składania interfejsów umieszczonych w różnych urządzeniach fizycznych (MC-LAG).

1. Zarządzanie i monitorowanie urządzeń

3.1. Wszystkie opcje konfiguracyjne muszą być możliwe do zmiany z wykorzystaniem interfejsu tekstowego (ang. Command Line Interface = CLI).

3.1.1.Cała konfiguracja urządzenia musi być zapisywana do pojedynczego pliku tekstowego.

Plik ten musi być w formacie umożliwiającym jego bezpośrednie odczytanie przez administratora oraz jego bezpośrednią edycję (tj. przy użyciu dowolnego edytora tekstu np. vi, notepad++).

3.1.2.Urządzenie musi zapewniać minimum dwustopniowe zatwierdzanie komend (wprowadzenie komendy, aktywacja konfiguracji),

3.1.3.Urządzenie musi zapewniać możliwość cofnięcia zmian konfiguracji,

3.1.4.Urządzenie musi zapewniać możliwość tworzenia punktów kontrolnych konfiguracji i ich odtwarzania,

3.1.5.Urządzenie musi zapewniać możliwość tworzenia i przywracania kopii zapasowych konfiguracji,

3.1.6.CLI urządzenia (generowane komunikaty i wydawane komendy) musi bazować na języku angielskim lub polskim (dopuszczalne jest stosowanie skrótów lub nazw własnych mających jednak za bazę języki polski lub angielski).

3.2. Urządzenie musi zapewniać możliwość współpracy z serwerami autoryzacji TACACS+ i RADIUS (zgodnie z RFC2865), w szczególności przy umożliwianiu dostępu do CLI), bez konieczności tworzenia lokalnej informacji o każdym użytkowniku wraz z przypisaniem użytkownika do odpowiedniej grupy na podstawie informacji otrzymanych z serwera autoryzującego.

3.3. Urządzenie musi wspierać RADIUS Accounting zgodnie z RFC2866 umożliwiający rejestrowanie, co najmniej następujących zdarzeń: informacji o logowaniu i wylogowaniu się administratora, wydaniu komendy (wraz z jej treścią), zapisania konfiguracji.

3.4. Urządzenie musi umożliwiać komunikację z urządzeniem za pomocą protokołu SNMPv2 (RFC1901) zgodnie z MIB-2 (RFC1213) oraz SNMPv3 (RFC2570).

3.4.1.Dane zbierane przy wykorzystaniu protokołu SNMP muszą być identyczne z danymi, jakie można zebrać przez CLI.

3.4.2.Urządzenie musi pozwalać na zbieranie następujących statystyk przez protokół SNMP w sposób niepowodujący znacznego obciążenia procesorów urządzenia z cyklicznością 1 pobranie danych na 5 minut:

- statystyki ruchu dla interfejsów fizycznych,
- statystyki ruchu dla interfejsów logicznych,
- statystyki zajętości tablic MAC,

- statystyki przypisania adresów MAC do VLAN,
- informacje o wykorzystaniu kolejek,
- statystyki dla ACL.

3.5. Urządzenie musi wspierać mechanizm SNMP Trap (STD 62).

3.6. Urządzenie musi oferować interfejs programowy do współpracy z aplikacjami (API lub SDK). Wymagana jest obsługa NETCONF (RFC 6241, Network Configuration Protocol), za pomocą którego możliwe będzie konfigurowanie urządzenia oraz sprawdzanie jego stanu (stan interfejsów, protokołów, liczniki pakietów/ramek itd.)

3.7. Urządzenie musi zapewniać możliwość tworzenia wielu poziomów dostępu do urządzenia (nie mniej niż czterech – full-access, read-only, różne poziomy ograniczenia dostępu, np. operator 1 / 2 linii wsparcia, systemy provisioningu ograniczone do wybranych funkcjonalności).

3.8. Urządzenie musi zapewniać możliwość uwierzytelniania administratora poprzez klucz SSH.

3.9. Na urządzeniu musi być możliwość wyłączenia dostępu terminalowego przy wykorzystaniu protokołów nieszyfrowanych (telnet).

3.10. Urządzenie musi mieć możliwość zdalnej aktualizacji oprogramowania.

3.10.1. Urządzenie musi mieć zaimplementowany mechanizm ISSU (In Service Software Upgrade) zapewniający aktualizację oprogramowania bez przerywania pracy urządzenia (dopuszczalna jest przerwa w pracy kart liniowych nie dłuższa niż 0,5s niewpływająca na działanie protokołów routingu).

3.11. Urządzenie musi posiadać port terminalowy do dołączenia konsoli (RS-232).

3.12. Urządzenie musi posiadać dodatkowy port typu Ethernet (10/100/1000 lub 10/100), za pomocą którego możliwe będzie zarządzanie urządzeniem poza pasmem (ang. out-of-band management = OOB). Opcją alternatywną jest możliwość skonfigurowania jednego z portów, jako portu OOB (port musi mieć styk 1000Base-T lub 10/100/1000).

3.13. Urządzenie musi obsługiwać mechanizm syslog, pozwalający na przesyłanie informacji o zarejestrowanych przez urządzenie zdarzeniach do zdalnego serwera syslog.

3.14. Urządzenie musi obsługiwać protokół NTP.

3.15. Urządzenie musi obsługiwać IPFIX lub NetFlow (wersje 5 i 9) dla IPv4, IPv6.

3.16. Urządzenie musi mieć możliwość tworzenia list kontroli dostępu (ACL) dla IPv4 i IPv6.

3.16.1. Muszą być dostępne liczniki trafień w poszczególne wpisy list.

3.16.2. Listy kontroli dostępu muszą mieć długość nie mniejszą niż 500 wpisów.

3.16.3. Urządzenie musi mieć możliwość założenia ACL na każdym interfejsie logicznym w kierunku wejściowym i wyjściowym. Dotyczy to jednoczesnego założenia ACL na wszystkich skonfigurowanych interfejsach, przy czym każdy interfejs może mieć inną listę kontroli dostępu.

3.16.4. Listy ACL IPv4 i IPv6 nie mogą się wykluczać, tj. urządzenie musi umożliwiać aktywację obu typów na interfejsie logicznym.

1. Architektura urządzeń

4.1. Przełączniki muszą mieć architekturę modułarną. Za urządzenie modułarne Zamawiający uznaje urządzenie, który umożliwia rozbudowę o nowe, dodatkowe lub wymianę istniejących na nowsze

elementy składowe, poprzez ich instalację w odpowiednich slotach przeznaczonych na moduły sprzętowe, takie jak interfejsy liniowe, matryce przełączające, karty procesorowe, itd. Nie dotyczy to wymiennych wkładek optycznych.

4.1.1. Każdy oferowane urządzenie musi mieć takie wyposażenie, aby wszystkie elementy istotne z punktu widzenia pracy urządzenia miały nadmiarowość (jako elementy istotne Zamawiający uznaje wszystkie elementy konieczne dla prawidłowej pracy urządzenia, tj. zasilacze, wentylatory, karty procesorowe, matryce przełączające, itd. z wyłączeniem kart interfejsów liniowych). Wszystkie urządzenia mogące mieć zainstalowane elementy nadmiarowe będą niewyposażone. Prosimy o opisanie sposobu realizacji wymogu nadmiarowości w oferowanych urządzeniach.

4.2. Dopuszczalne jest zaoferowanie urządzeń wirtualizowanych, zbudowanych z wielu urządzeń składowych (w szczególności z urządzeń o stałej konfiguracji), przy następujących założeniach:

4.2.1. Połączenie urządzeń będzie zrealizowane w sposób nieograniczający wydajności (sumaryczna przepustowość połączeń pomiędzy dowolnymi urządzeniami wchodzącymi w skład zestawu, jak również wydajność poszczególnych urządzeń nie może być niższa niż wymagana wydajność urządzenia),

4.2.2. Zapewnione i dostarczone będą wszystkie elementy konieczne do połączenia zespołu urządzeń,

4.2.3. Wszystkie elementy zestawu będą spełniały wymagania związane z zarządzaniem,

4.2.4. Do oferty zostanie dołączony szczegółowy opis zespołu, obejmujący schematy połączeń, określenie, które elementy zestawu odpowiadają za poszczególne funkcjonalności itp.

4.2.5. Wymagania dotyczące niezawodności dla urządzeń modularnych związane z przełączeniem kart procesorowych będą zachowane dla przełączenia urządzeń master (kontrolujących urządzenie wirtualne).

4.3. Architektura oferowanego urządzenia musi zapewniać bezstratne przełączanie pakietów pomiędzy dowolnymi dwoma interfejsami bez żadnych ograniczeń wydajnościowych przy założeniu, że wszystkie porty pracują z pełną wydajnością (tj. nadają i odbierają pakiety z pełną prędkością interfejsu).

4.3.1. Jeżeli karty interfejsów liniowych mają ograniczenia wydajnościowe (nadszyskrypcja), to do ilości interfejsów wymaganych liczone mogą być tylko interfejsy zapewniające pracę bez ograniczeń wydajnościowych. Pozostałe interfejsy, mimo że nie są zaliczane do interfejsów wymaganych, nie mogą mieć wprowadzonych żadnych blokad (muszą być dostępne do wykorzystania bez konieczności zakupu dodatkowych licencji, itd.).

1. Wymagania na funkcjonalności przełączania

5.1. Przełącznik musi obsługiwać protokoły RSTP i MSTP.

5.2. Przełącznik musi obsługiwać protokół PVSTP lub równoważny (umożliwiający utworzenie oddzielnego drzewa rozpinającego (ag, spanning tree) dla każdego skonfigurowanego VLANu).

5.3. Przełącznik musi obsługiwać mechanizm typu BUM (Broadcast/Unknown/Multicast) storm control.

5.4. Przełącznik musi obsługiwać protokół LLDP Link Layer Discovery Protocol (LLDP) zgodnie z IEEE 802.1ab.

5.5. Przełącznik musi obsługiwać jednocześnie, co najmniej 4 000 sieci VLAN.

5.6. Przełącznik musi zapewniać wsparcie dla sieci VXLAN,

5.6.1. Przełącznik musi spełniać funkcjonalność VXLAN L2 Gateway,

5.6.2. Przełącznik musi spełniać funkcjonalność VXLAN L3 Gateway,

5.6.3. Przełącznik musi wspierać EVPN, w tym EVPN multihoming.

5.7. Przełącznik musi obsługiwać tablicę MAC o pojemności 128 000 wpisów

5.8. Przełącznik musi zapewniać wsparcie dla IPv4 oraz IPv6.

5.8.1. Przełącznik musi obsługiwać tablice routingu o pojemności, co najmniej 32 000 prefixów dla każdego z protokołów IPv4 i IPv6.

5.8.2. Przełącznik musi obsługiwać tablice ARP o wielkości 16 000 adresów,

5.8.3. Przełącznik musi obsługiwać tablice ND (neighbor discovery) o wielkości 16 000 adresów.

5.9. Przełącznik musi obsługiwać protokół BGP.

5.10. Przełącznik musi obsługiwać protokół OSPF.

5.11. Przełącznik musi obsługiwać protokół ISIS.

5.12. Przełącznik musi obsługiwać VRRP v2 i v3.

W każdym z węzłów muszą być następujące ilości portów [\[MM1\]](#) w przełącznikach:

węzeł	100GE	40GE	10GE / 25GE	wkładki 10GE
WAW	4	68	316	229
KAT	4	62	174	96
POZ	3	37	260	194
KRA	3	35	94	28
RZE	2	29	98	52
LUB	2	26	98	52
WRO	2	26	100	54
LOD	2	26	104	58
GDA	2	26	98	52
TOR	2	23	94	48
SZC		23	90	44
OLS		20	86	50
KIE		20	80	44
BIA		20	80	44
OPO		17	60	34
ZGO		17	64	38

gdzie:

- 100GE – porty 100GE wyposażone w optykę w standardzie 100GBase-SR4,

- 40GE – porty 40GE wyposażone w optykę 40GBase-SR4, w węźle WAW 2 wkładki muszą być typu 40GBase-LR4,

Dla połączeń do Urządzeń Agregacyjnych, w węzłach WAW, KAT, POZ, KRA, RZE, LUB, WRO, LOD, GDA, TOR, jest możliwa zamiana 2 portów 40GE na 8 portów 10GE. W węźle WAW oznacza to wymianę optyki 40GBase-LR4 (2 wkładki) na optykę 10GBase-LR.

- 10GE /25GE – porty 10GE lub 10GE / 25GE (porty o zmiennej prędkości pracy), porty bez wkładek,
- wkładki 10GE – ilość wkładek 10GBase-SR do instalacji w przełączniku,

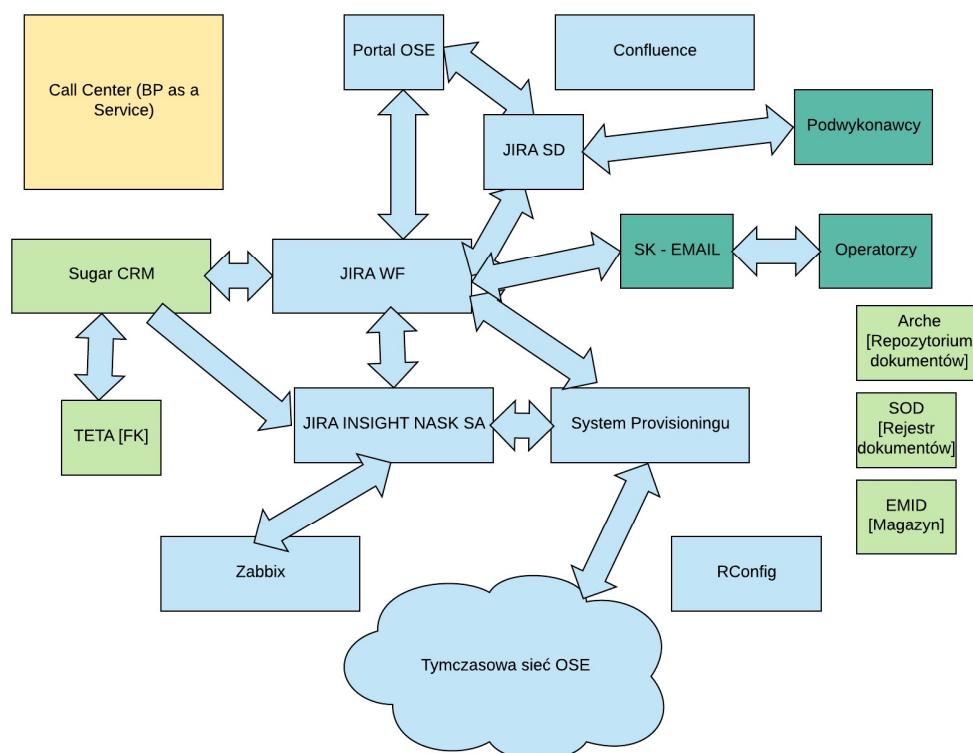
W każdym z węzłów porty 40GE oraz 10GE / 25GE muszą być umieszczone równomiernie, na co najmniej dwóch kartach interfejsów (w przypadku urządzeń modularnych) lub na co najmniej dwóch urządzeniach składowych (w przypadku urządzeń wirtualizowanych zbudowanych z wielu urządzeń składowych). Należy przyjąć, że każde urządzenie końcowe (serwer) wyposażone jest w dwa identyczne porty (40GE lub 25GE lub 10GE) i każdy z tych portów musi być dołączony do portu przełącznika zlokalizowanym na innej karcie / urządzeniu.

[1] W przypadku, gdy wykorzystanie modułów optycznych pochodzących od innych producentów, wymaga wykonania dodatkowych czynności polegających na rekonfiguracji urządzenia, Wykonawca zobowiązany jest przedstawić szczegółową dokumentację techniczną, zawierającą informację na temat sposobu ich przeprowadzenia.

[2] Funkcjonalność często określaną również, jako digital optical monitoring (DOM).

6.3. Koncepcja wdrożenia POOSE

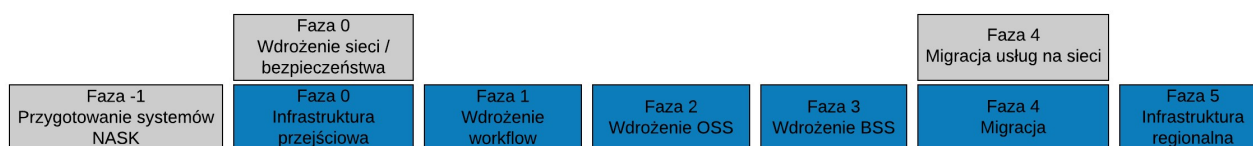
Celem umożliwienia świadczenia usług OSE zgodnie z wymaganiami ustawowymi w okresie poprzedzającym zbudowanie kompletnej platformy przygotowane zostało i wdrożone rozwiązanie przejściowe, które obecnie jest ciągle rozwijane. Funkcjonuje ono w oparciu o systemy dedykowane dla OSE jak również systemy NASK już wcześniej istniejące. Wszystko to funkcjonuje we współpracy z tymczasową siecią OSE.



Pomimo iż obecnie systemy te nie zapewniają pełnego wsparcia, to podlegając ciągłemu rozwojowi spełniają istotną rolę w procesach biznesowych Operatora OSE w ramach procesów pozyskiwania i podłączania szkół. Zbierają też, gromadzą i przetwarzają dane związane z działalnością OSE, które będą również niezbędne w przyszłości. Część tych systemów zostanie wykorzystana również w docelowym rozwiązaniu, jednakże pozostałe zostaną zastąpione w ramach systemów wsparcia i zarządzania (OSS/BSS).

Wdrożenie rozwiązania docelowego dla Operatora OSE będzie realizowane w wielu fazach, aby wyeliminować ryzyko problem/awarii mogących mieć wpływ na ciągłość funkcjonowania procesów biznesowych jednocześnie zapewniając szybki przyrost oczekiwanych funkcjonalności biznesowych i oczekiwaną wydajność i niezawodność procesów biznesowych. Wdrażanie rozwiązania w warstwie aplikacyjnej zależy również od tego jak będą wdrażane i rozwijane zdolności / funkcjonalności w innych obszarach (sieci, infrastrukturze, bezpieczeństwie).

Wdrożenia OSS/BSS będzie się składać z następujących faz:

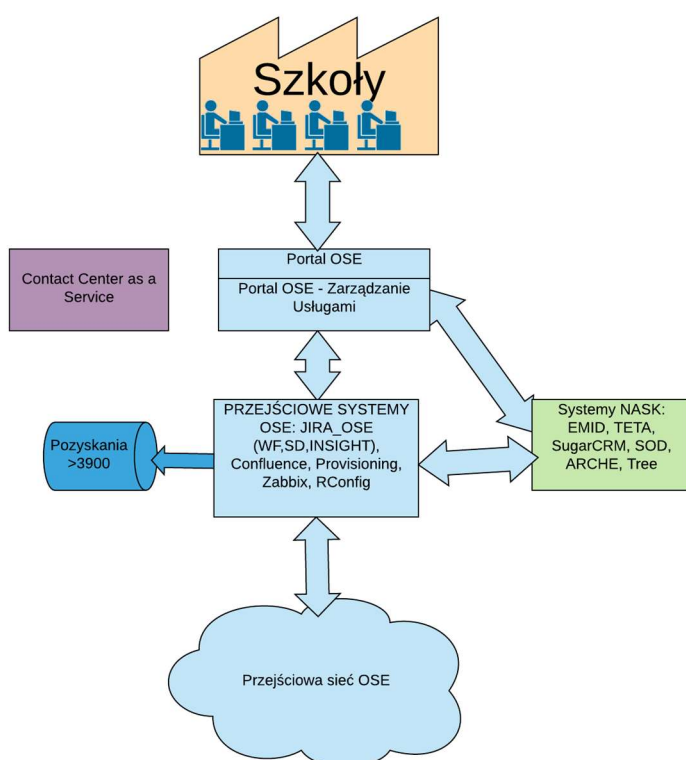


Punktem startowym do rozpoczęcia wdrożenia będzie bieżąca architektura systemowa, czyli obecnie wdrożone tymczasowe rozwiązanie.

6.3.1. Wdrożenie warstwy aplikacyjnej

Stan bieżący - Start

Z uwagi na ograniczenia systemowe jak i organizacyjne pojemność systemów przejściowych jak i przejściowej sieci szkieletowej w zakresie limitu obsługiwanych szkół jest ograniczona. W związku z tym w systemach zostaną zaimplementowane ograniczenia, które zablokują przetwarzanie zleceń po procesie pozyskania w sytuacji przekroczenia limitu pozyskanych szkół. Zostanie zmodyfikowany proces pozyskania szkoły tak, aby po ostatnim kroku (umowa podpisana) przed przejściem do kolejnego procesu (podłączania szkoły) była sprawdzana ilość szkół już podłączonych lub w trakcie podłączania. Jeżeli liczba takich szkół przekroczy limit zgodnie z konfiguracją (wstępnie ustawiony na 3900) to proces zostanie wstrzymany.

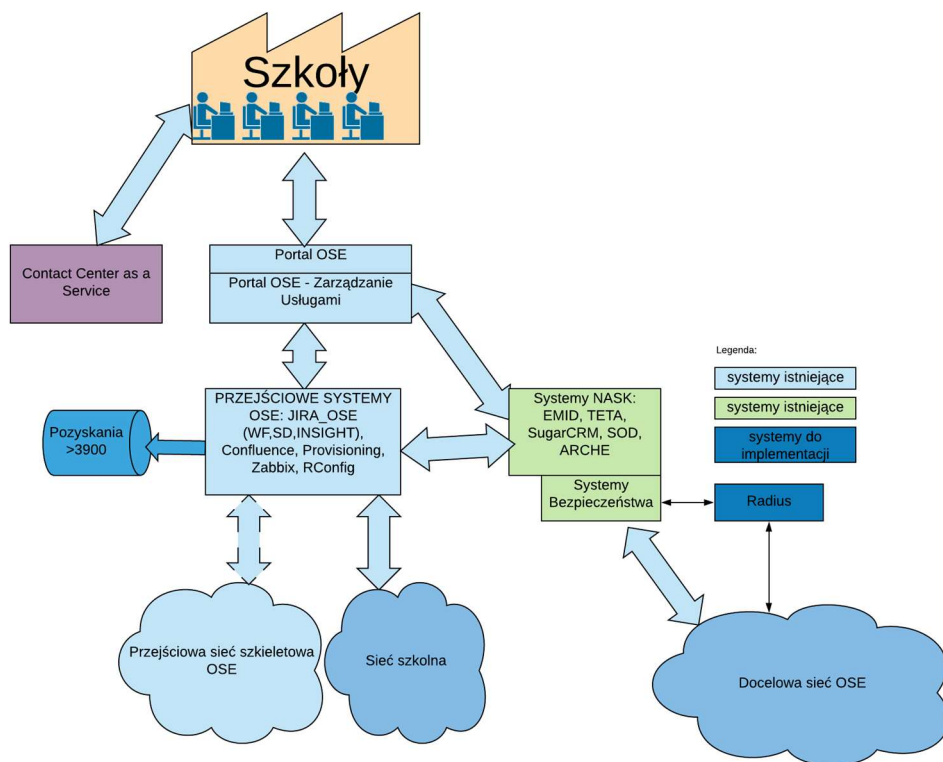


Uwaga: Wyjątkiem będzie sytuacja, gdy proces będzie dotyczył szkoły w lokalizacji, która już została podłączona (dołączenie kolejnej szkoły w lokalizacji). Dla takich sytuacji proces nie będzie wstrzymywany.

Cel realizacji fazy: Przygotowanie środowiska do wdrożenia docelowych systemów.

Faza 0 - Wdrożenie sieci i bezpieczeństwa

W celu zapewnienia odpowiedniej jakości usług dostępu do internetu dla ciągle rosnącej liczby użytkowników konieczne jest zbudowanie sieci szkieletowej o odpowiednich parametrach wydajnościowych. Dodatkowo uruchomienie sieci szkieletowej wymaga też zapewnienia odpowiednich systemów bezpieczeństwa. Oba elementy znajdują się poza zakresem przetargu. Do autoryzacji użytkowników (administratorów) na urządzeniach sieciowych zostanie wykorzystany system Radius. Na tym etapie w sieci szkieletowej nie będzie jeszcze realizowanego podłączania żadnych szkół.



W ramach realizacji OSS/BSS w etapie tym przeprowadzone zostaną następujące działania:

- dostarczenie infrastruktury na potrzeby systemów sieci i bezpieczeństwa (może być wykorzystane rozwiązanie tymczasowe oparte o centrum danych dostawcy)
- instalacja serwera Radius na potrzeby systemów sieci i bezpieczeństwa

Faza ta umożliwi weryfikację gotowości produkcyjnej sieci i systemów bezpieczeństwa.

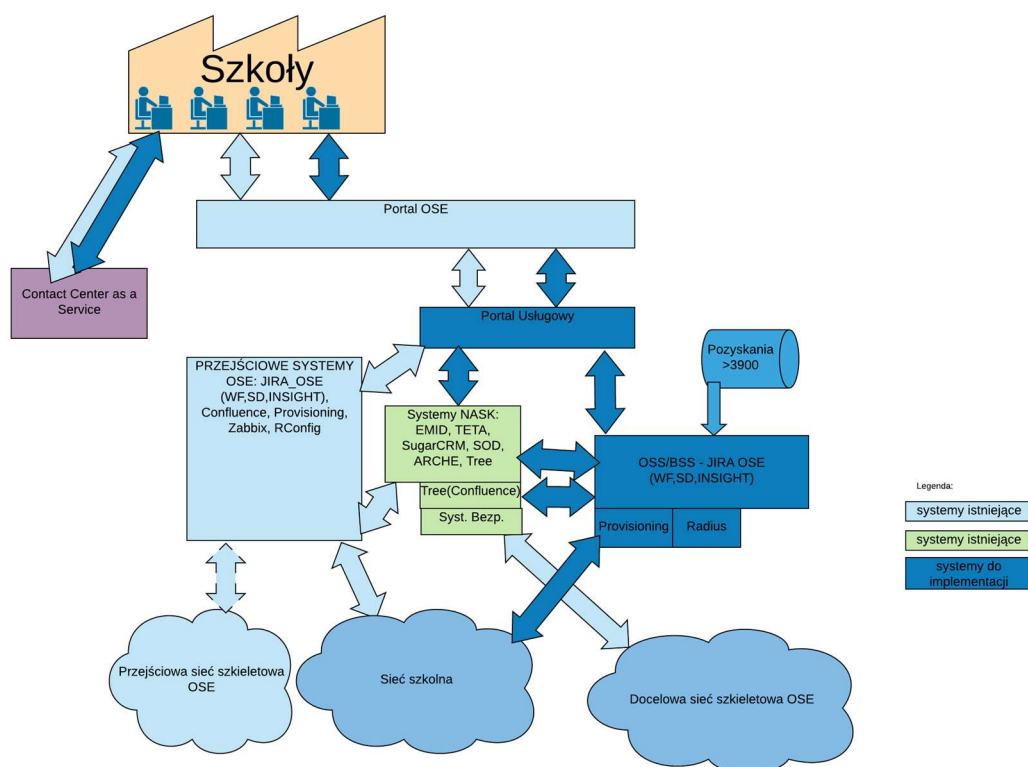
Cel realizacji fazy: Zapewnienie środowiska do funkcjonowania sieci docelowej i systemów bezpieczeństwa

Faza 1 - Wdrożenie workflow

W roku 2019 nastąpi znaczący wzrost podłączanych szkół, co znacznie podniesie wymagania wydajnościowe dla systemów operatora OSE. Z uwagi na fakt, iż przygotowanie i wdrożenie nawet części systemów OSS/BSS wymaga pewnego czasu w ramach etapu przejściowego zostanie stworzona kopia systemów przejściowych (m.in JIRA WF, SD, Insight) i umieszczona w środowisku OSS/BSS umożliwiając obsługę części procesów w tym środowisku realizującym potrzeby pod względem wydajności. Po stronie dotychczasowych systemów rozwijanych przez NASK zostanie przygotowany odpowiedni routing, aby ruch mógł zostać przekierowany do nowej instancji systemów. Rejestracja szkół będzie kierowana do systemów przejściowych, jeżeli dotyczy szkoły w lokalizacji gdzie są już podłączone szkoły w systemach przejściowych lub w przeciwnym przypadku do systemów docelowych.

Dodatkowo w fazie tej zostanie wdrożona funkcjonalność umożliwiająca aktywację usług na docelowej sieci szkieletowej OSE, czyli aktywator.

W ramach prac tej fazy obszar portali zostanie rozdzielony na dwa komponenty - Portal OSE będący wizytówką OSE, oraz Portal Usługowy zapewniający funkcjonalności samoobsługowe do zarządzania usługami OSE.



W zakresie prac OSS/BSS zostaną zrealizowane następujące zadania:

- zostanie rozbudowana infrastruktura OSS/BSS (aby zrealizować zwiększone wymagania pojemnościowe wynikające z większej liczby systemów i realizowanych procesów)
- wdrożenia nowych systemów (jako kopia obecnie istniejących) - zostaną przeniesione wszystkie funkcjonalności procesów (bez migracji danych klientów). Należy uwzględnić konieczność inicjalnego zasilenia systemów konfiguracją oraz danymi ewidencyjnymi (bazą szkół i lokalizacji) niezbędnymi do realizacji procesów biznesowych. Nowe systemy w celu dostarczania usług w sieci będą wykorzystywać kopię istniejącego systemu provisioningu. Rozwój i utrzymanie nowych systemów będzie znajdować się w odpowiedzialności dostawcy OSS/BSS.
- zostanie zrealizowana migracja wstrzymanych procesów pozyskania (wstrzymanych z uwagi na przekroczenie limitu połączenia). Migracja będzie dotyczyć wyłącznie procesów, które zostały wstrzymane na ostatnim kroku procesu pozyskania. Jeżeli proces będzie się znajdował w innym kroku to najpierw musi on zostać dokończony w przejściowych systemach, a dopiero wtedy będzie mógł zostać zmigrowany.
- wdrożony zostanie również Portal Usługowy realizujący integrację zarówno z systemami przejściowymi jak i docelowymi. W momencie wdrożenia musi on zapewniać, co najmniej następujące funkcjonalności:
- rejestracja szkół (na bazie istniejącej w Portalu OSE funkcjonalności) wraz z kierowaniem rejestracji do właściwej grupy systemów
- logowanie użytkowników szkolnych - umożliwiając przejście do części dostępnej dla zalogowanych użytkowników osobom posiadającym uprawnienia
- wyświetlanie usług - prezentacja stanu i parametrów usług posiadanych przez szkołę, do której jest przypisany zalogowany użytkownik.

- obsługa zgłoszeń - funkcjonalność dostępna dla zalogowanych użytkowników umożliwiającą zarządzanie zgłoszeniami (awarie, incydenty bezpieczeństwa, konsultacje itp.) do operatora OSE
- routing komunikacji do właściwej JIRY (przejęciowej lub docelowej)
- zlecenia usługowe - aktywacja, modyfikacja, dezaktywacja usług
- obsługa usług bezpieczeństwa (alerty, raporty, zarządzanie parametrami)
- *Wraz z wdrożeniem Portalu Usługowego na Portalu OSE funkcjonalności te zostaną wyłączone oraz zostanie ustawione przekierowanie do Portalu Usługowego. (w zakresie prac po stronie zamawiającego)*
- Portal OSE zostanie przeniesiony na tymczasową infrastrukturę OSS/BSS.
- System Zarządzania Budżetem zostanie przeniesiony na tymczasową infrastrukturę OSS/BSS.
- zostanie wdrożony wspólny widok na JIRY przejęciową i docelową umożliwiający użytkownikom biznesowym na operowanie danych z obu środowisk na jednym ekranie (użytkownikom zarówno z centrum kontaktu, utrzymania, DRP jak również jeden wspólny widok dla parterów serwisowych na JIRA SD)
- zostanie wdrożone narzędzie do łączenia raportów pochodzących z obu środowisk (przejęciowego i docelowego) tak, aby na wyjściu otrzymywać jeden spójny raport łączący dane raportowe z obu środowisk.
- w ramach funkcjonalności OSS wdrożony zostanie Aktywator - komponent z obszaru OSS umożliwiający provisioning usług na urządzeniach sieci szkieletowej (zarówno w zakresie urządzeń sieciowych jak i urządzeń bezpieczeństwa) umożliwiający pełną aktywację usług. Na tym etapie prac nie jest oczekiwana funkcjonalność umożliwiająca modyfikację usług.
- obecne rozwiązanie Contact Center (w formie usługi) zostanie zintegrowane z systemami docelowymi

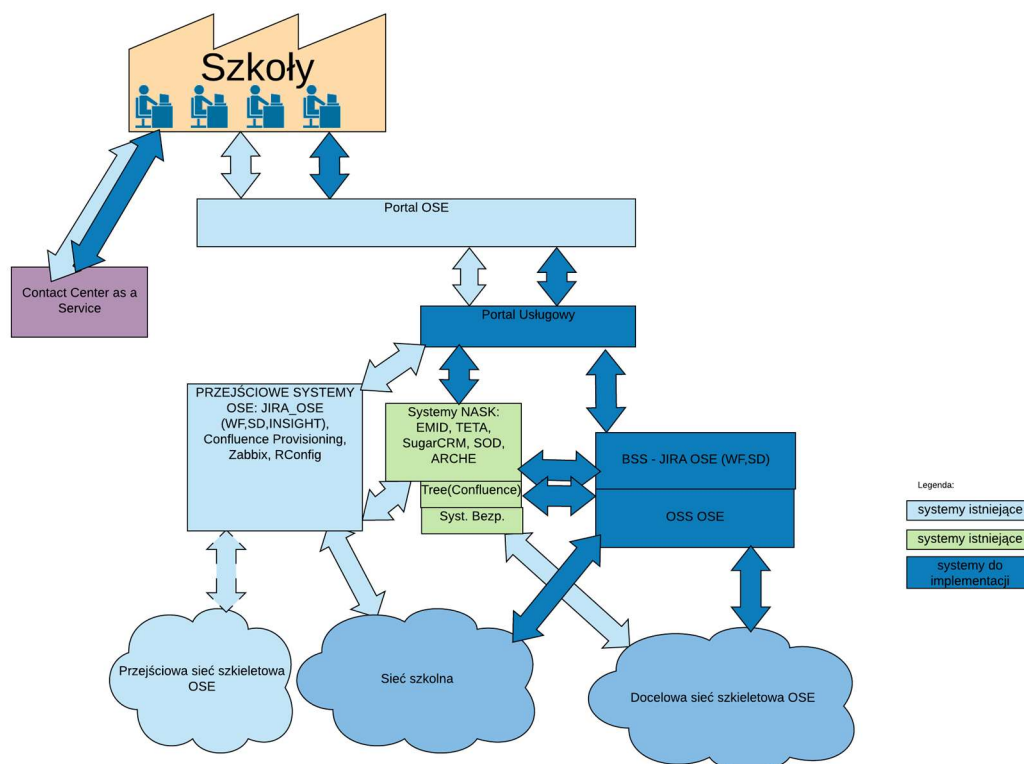
W etapie tym nie ma dostarczonego monitoringu docelowej sieci szkieletowej (musi on być realizowany przez dostawcę sieci szkieletowej), a provisioning jest ograniczony wyłącznie do urządzeń CPE w sieci szkolnej.

Cel realizacji fazy: Zapewnienie środowiska o wystarczającej wydajności i odpowiednim utrzymaniu w zakresie realizacji procesów OSE ze szczególnym uwzględnieniem procesów pozyskania i podłączenia.

Faza 2 - Wdrożenie OSS

Po ustabilizowaniu się nowych systemów JIRA zostaną wdrożone do nowego środowiska wszystkie funkcjonalności z obszaru OSS (zastępując również część OSS-ową realizowaną przez JIRA Insight, provisioning, aktywator). Systemy JIRA nowego środowiska zostaną zintegrowane z nowo wdrożonym rozwiązaniem OSS i jednocześnie odłączone od starego systemu provisioningu. W ramach swoich prac

dostawca OSS/BSS będzie zobowiązany do migracji danych z systemu JIRA Insight do docelowego



rozwiązania.

W ramach Fazy 2 zostaną zrealizowane następujące działania:

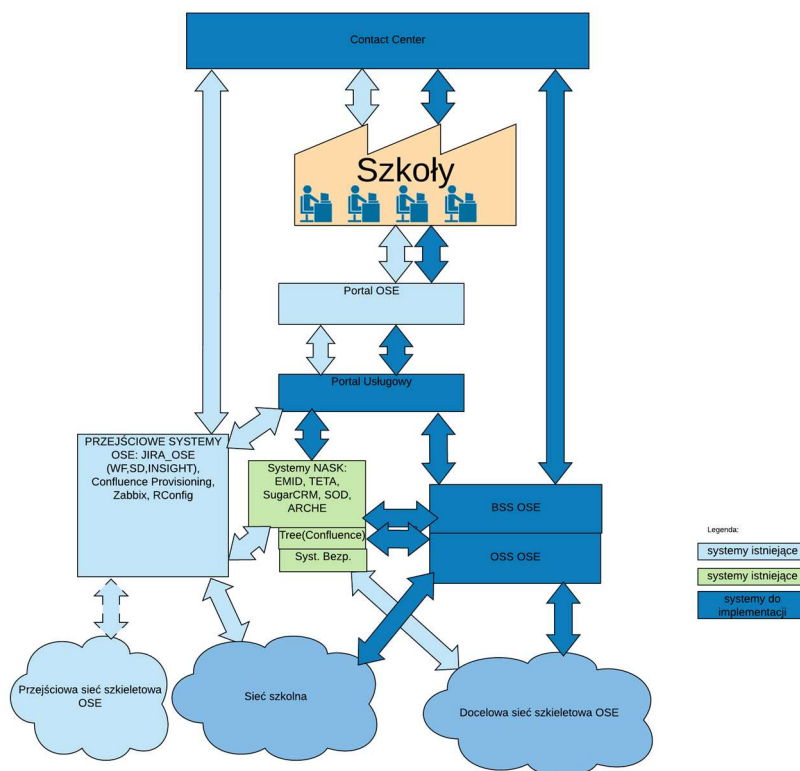
- wdrożenie infrastruktury "chmurowej" zgodnej z docelowymi wymaganiami i migracja systemów
- tymczasowe rozwiązania do aktywacji zostaną zastąpione docelowym provisioningiem
- wdrożony zostanie pełen monitoring docelowej sieci OSE
- wdrożone zostaną wszystkie elementy rozwiązanie obszaru OSS (telemetria na tym etapie jest opcjonalna)
- zmigrowane zostaną dane z wyłączanych systemów do docelowego rozwiązania
- uruchomienie SSO dla systemów OSS

Faza musi zostać zrealizowana nie później niż 2 miesiące po fazie pierwszej.

Cel realizacji fazy: Zapewnienie odpowiednio wydajnego środowiska realizującego wszystkie podstawowe funkcjonalności związane z zarządzaniem usługami ściśle zintegrowanego z docelową siecią OSE i w pełni zautomatyzowanego.

Faza 3 - Wdrożenie BSS

Kolejny etapem wdrażania OSS/BSS przez dostawcę będzie uruchomienie wszystkich funkcjonalności obszaru BSS w docelowym środowisku wraz z integracją ich z pozostałymi systemami NASK OSE i NASK. Od tego momentu środowisko OSS/BSS będzie odpowiedzialne za pełną obsługę procesów biznesowych zgodnie z docelowym modelem.



W ramach etapu wdrożenia BSS zostaną zrealizowane następujące działania:

- zastąpienie kopii systemów przejściowych przez docelowe rozwiązanie w obszarze BSS
- optymalizacja już zamplementowanych procesów biznesowych i dostosowanie ich do architektury docelowych systemów
- migracja do systemów BSS wszelkich danych niezbędnych do obsługi klientów, podłączonych przy wykorzystaniu docelowych systemów OSS (czyli od wdrożenia Fazy 2)
- wdrożenie pozostałych wyspecyfikowanych procesów biznesowych (a wcześniej niezaimplementowanych)
- wdrożenie na portalu usługowym pełnej obsługi klienta (m.in obsługi finansowej) i zapewnienie integracji z BSS-em
- wdrożenie docelowego Contact Center wraz z integracją z systemami przejściowymi
- dołączenie systemów BSS do SSO

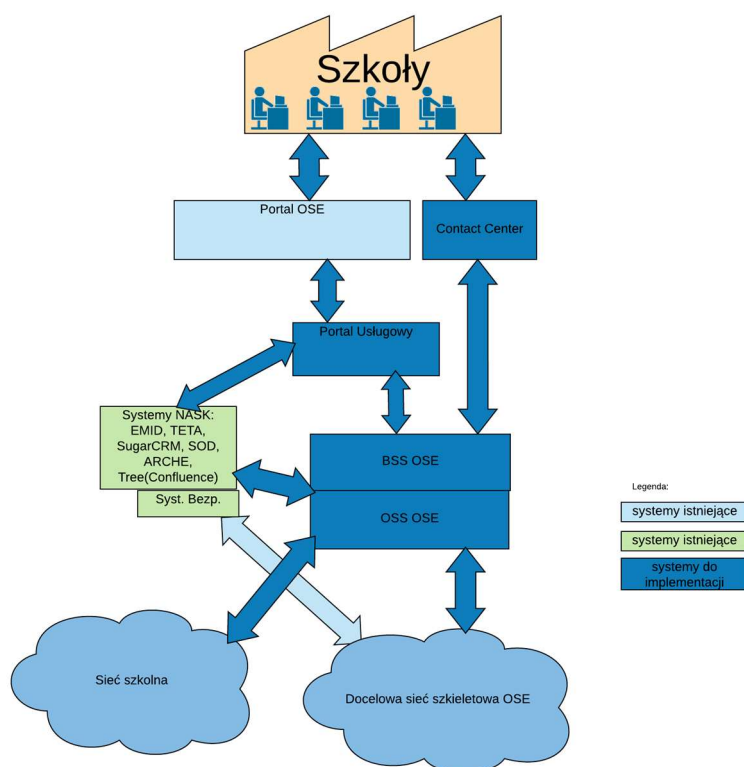
Od tego momentu środowisko OSS/BSS powinno już posiadać pełną funkcjonalność zgodnie z wymaganiami, aby wspierać wszystkie procesy Operatora OSE.

Faza musi być zrealizowana nie później niż 2 miesiące po fazie drugiej.

Cel realizacji fazy: zapewnienie zautomatyzowane zintegrowanego środowiska (docelowe rozwiązanie) realizującego wszystkie wymagane funkcjonalności.

Faza 4 - Migracja

Ostatnim krokiem w procesie wdrażania OSS/BSS będzie migracja klientów z rozwiązania przejściowego do docelowego, co doprowadzi do wyłączenia (całkowitego lub tylko zaprzestania wykorzystania w ramach działań operatora OSE) systemów, które nie są planowane do architektury docelowej.



Migracja będzie dotyczyć zarówno danych z obszaru BSS jak i OSS. Po zakończeniu migracji wszystkich danych zostaną również odłączone integracje z systemami nieplanowanymi do pracy w środowisku docelowym. Migracja musi być realizowana równolegle w systemach OSS/BSS oraz na sieci szkieletowej.

Faza nie może trwać dłużej niż 2 miesiące.

Cel realizacji fazy: zapewnienie jednego środowiska do obsługi OSE.

Faza 5 - Infrastruktura regionalna

Po zakończeniu wdrażania systemów OSS/BSS i zmigrowaniu wszystkich szkół do systemów docelowych do dostarczenia pozostanie jedynie infrastruktura dla systemów sieci i bezpieczeństwa w pozostałych węzłach regionalnych (infrastruktura dla węzłów centralne oraz części regionalnych zostanie dostarczona we wcześniejszych fazach). Harmonogram dostarczania infrastruktury obliczeniowej będzie dostosowywany do harmonogramu dostępności poszczególnych węzłów regionalnych.

Cel realizacji fazy: zapewnienie infrastruktury dla wszystkich węzłów regionalnych

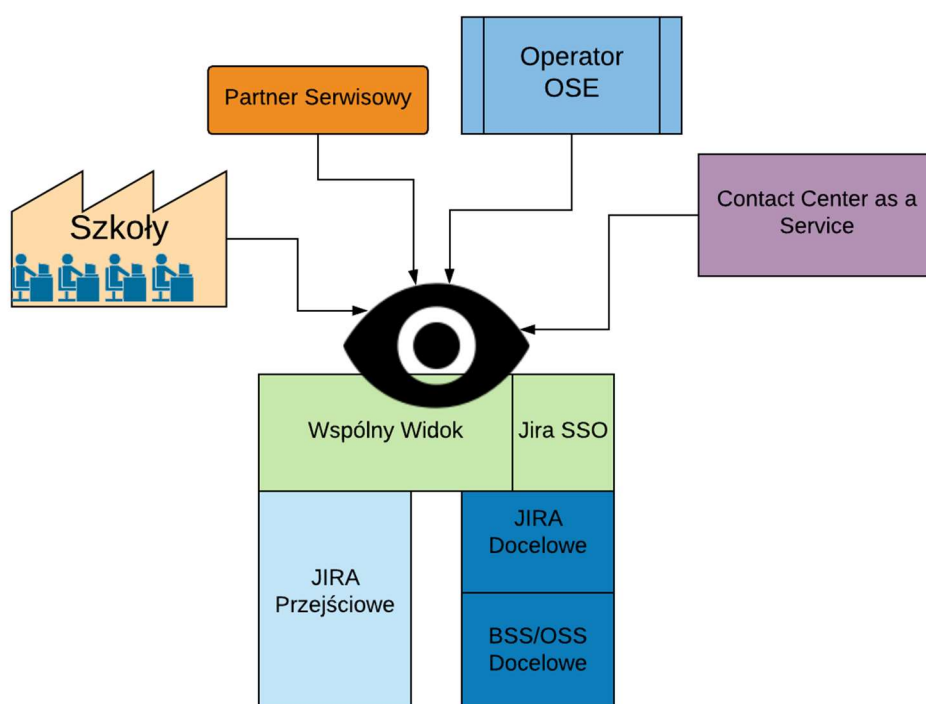
Koegzystencja

Wdrożenie systemów OSS/BSS będzie realizowane wieloetapowo, zanim dokończymy wdrożenie będziemy w sytuacji, gdy będą istniały dwie grupy systemów - docelowe i przejściowe. Część szkół będzie obsługiwana w jednej grupie systemów, natomiast druga część szkół w drugiej grupie systemów. Taka sytuacja będzie miała miejsce od wdrożenia kopii systemów BSS/OSS w fazie pierwszej aż do zakończenia migracji danych w fazie czwartej. Dla jasności obrazu zakładane jest, że przyporządkowanie szkół do poszczególnych grup systemów bazuje na podstawie lokalizacji. Do momentu wdrożenia pierwszej fazy wszystkie szkoły/lokalizacje podłączane są w systemach przejściowych (docelowe nie istnieją), o ile nie zostanie przekroczony limit szkół. Systemy przejściowe na podstawie różnych uwarunkowań mogą obsługiwać maksymalnie 4000 szkół, jako szkołę obsługiwaną należy rozumieć taką, która podpisała umowę z OSE i rozpoczął się dla niej proces podłączania. Jeżeli w systemach przejściowych zostanie

osiągnięty limit to zostanie wstrzymane przekazywanie szkół do podłączania po podpisaniu umowy. Wszelkie szkoły wstrzymane zostaną już podłączone w systemach docelowych po ich wdrożeniu.

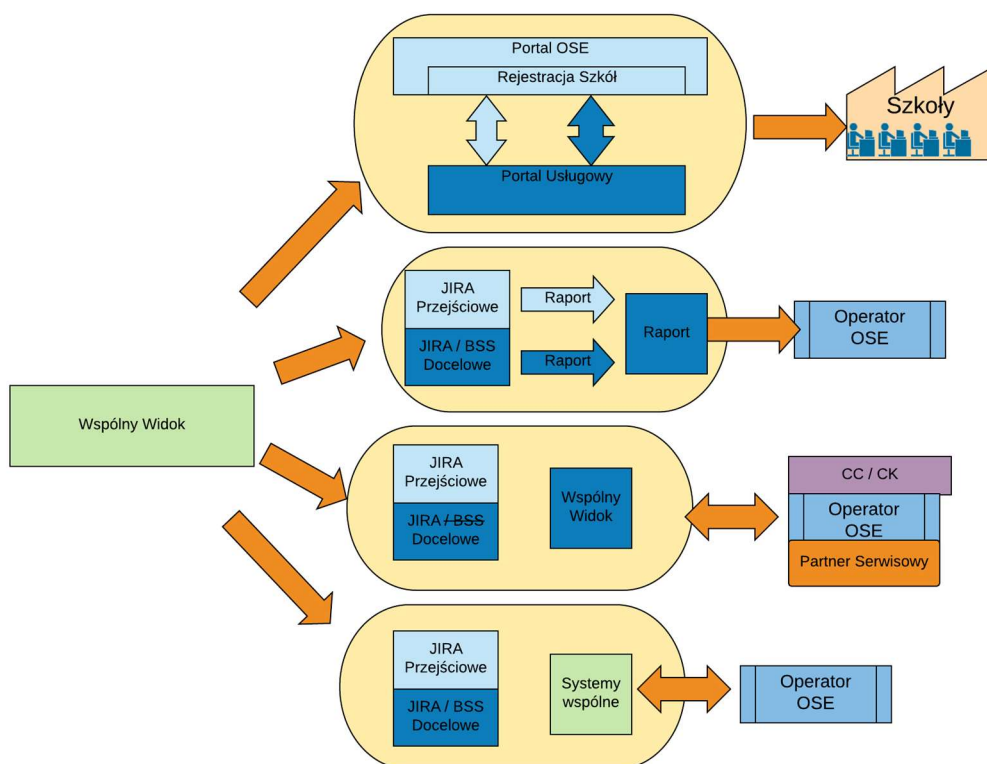
Od momentu wdrożenia wszystkie nowe podłączenia szkół będą kierowane do systemów docelowych. Jedynym wyjątkiem od tej reguły będzie sytuacja, gdy do podłączenia do OSE zgłosi się szkoła w lokalizacji, w której inne szkoły są obsługiwane w systemach przejściowych. W takiej sytuacji szkoła ta zostanie również podłączona w systemach przejściowych, aby zachować spójność obsługi w ramach lokalizacji.

Celem zminimalizowania problemów wynikających z posiadania dwóch grup systemów obsługujących klientów OSE tam, gdzie to możliwe zostanie przygotowany wspólny widok i zostanie zainstalowany moduł Jira SSO w celu jednokrotnego logowania użytkownika w dowolnej instancji Jira i utrzymania sesji pomiędzy instancjami.



W trakcie weryfikacji możliwości budowy wspólnego ujednoliconego widoku wyróżnione zostały następujące cztery obszary, dla których przygotowane zostaną rozwiązania:

- widok dla klientów
- raporty
- widok dla pracowników / partnerów
- systemy wspólne

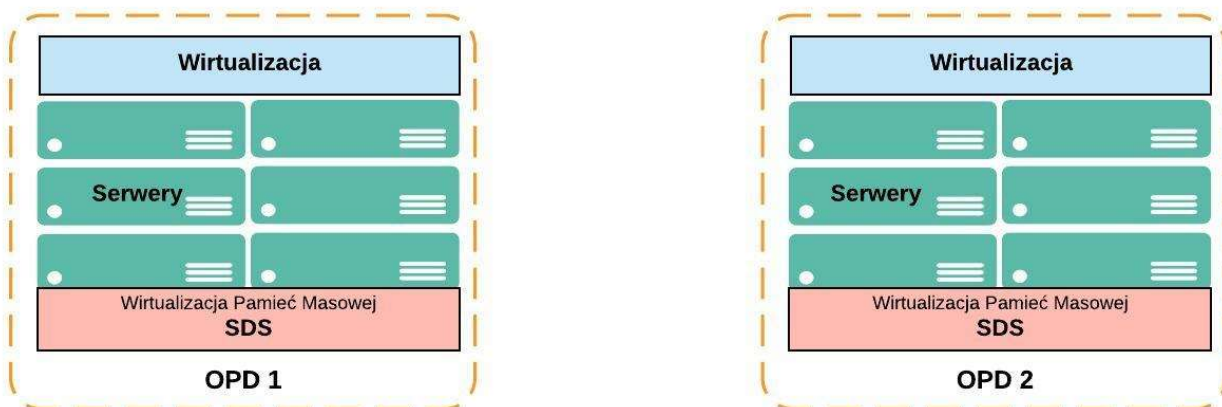


- W obszarze widoku dla klienta rozwiązanie zostanie zrealizowane w ramach Portalu Usługowego, który zapewni, aby rejestracja szkół była kierowana do właściwych systemów oraz aby dla zalogowanych klientów pobierać dane przypisanych do nich szkół z właściwej grupy systemów.
- Zostanie zapewnione jednokrotne logowanie pomiędzy instancjami systemu Jira oraz utrzymanie sesji użytkownika pomiędzy nimi (Dostawca powinien wdrożyć moduł/plugin SSO dla systemu Jira).
- W przypadku raportów zapewniona zostanie funkcjonalność do łączenia raportów pochodzących z dwóch grup systemów w jeden spójny raport.
- W sytuacji wykorzystywania przez pracowników lub partnerów systemów do realizacji zadań zostaną przygotowane odpowiednie komponenty umożliwiające prezentację danych pochodzących z obu grup systemów na jednym widoku / komponencie. Rozwiązanie ma zapewnić jeden punkt wejścia - zebranie zadań na wspólnym ekranie, chociaż dalsze działania biznesowe będą już realizowane we właściwej grupie systemów. Takie rozwiązanie będzie funkcjonować jedynie w sytuacji, gdy w obu grupach systemów w warstwie BSS rozwiązanie będzie oparte o systemy JIRA, czyli od pierwszej fazy do trzeciej fazy. Po wdrożeniu trzeciej fazy (docelowych systemów BSS) takie rozwiązanie byłoby zbyt kosztowne w stosunku do oferowanych korzyści, w związku z tym konieczne będzie korzystanie z oddzielnych grup systemów.
- W przypadku systemów wspólnych rozwiązanie umożliwiający wspólną prezentację systemów zostanie przeanalizowane i dostarczone poza wdrożeniem OSS/BSS

6.3.2. Wdrożenie infrastruktury

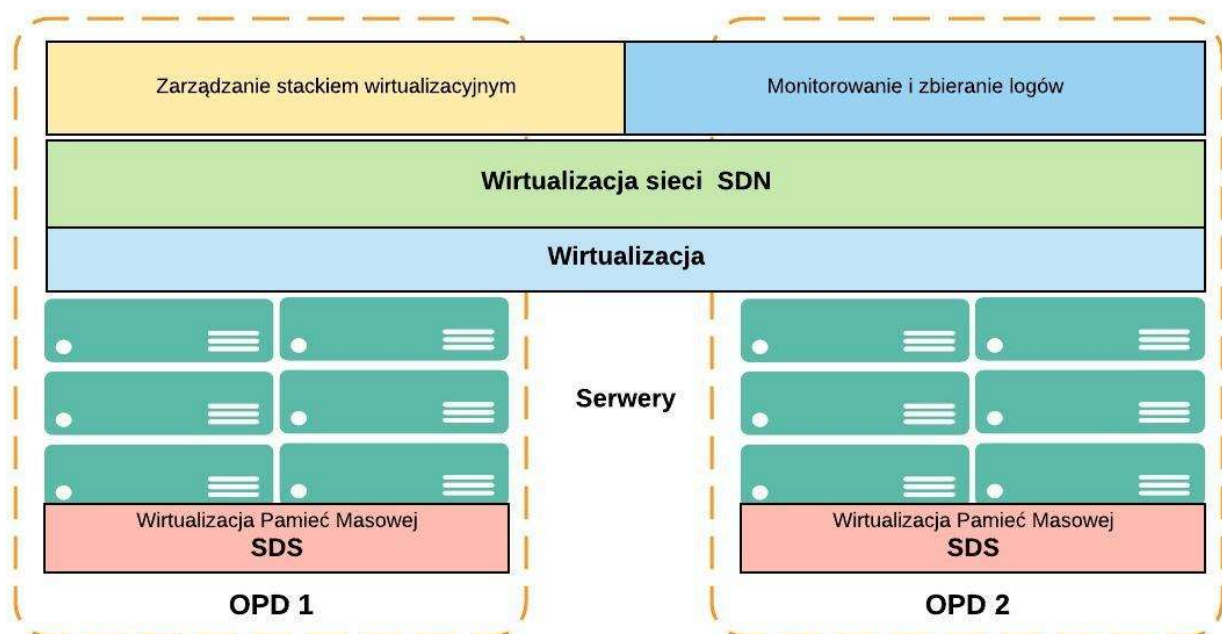
Faza 0 - Instalacja sprzętu pod wirtualizację

W tej fazie w dwóch głównych ośrodkach przetwarzania danych (Warszawa i Poznań) dostawca instaluje serwery i podłącza je do zainstalowanej już sieci LAN. Instalowana zostaje warstwa wirtualizacyjnej mocy obliczeniowej wraz z wirtualizacją przestrzeni dyskowej SDS.



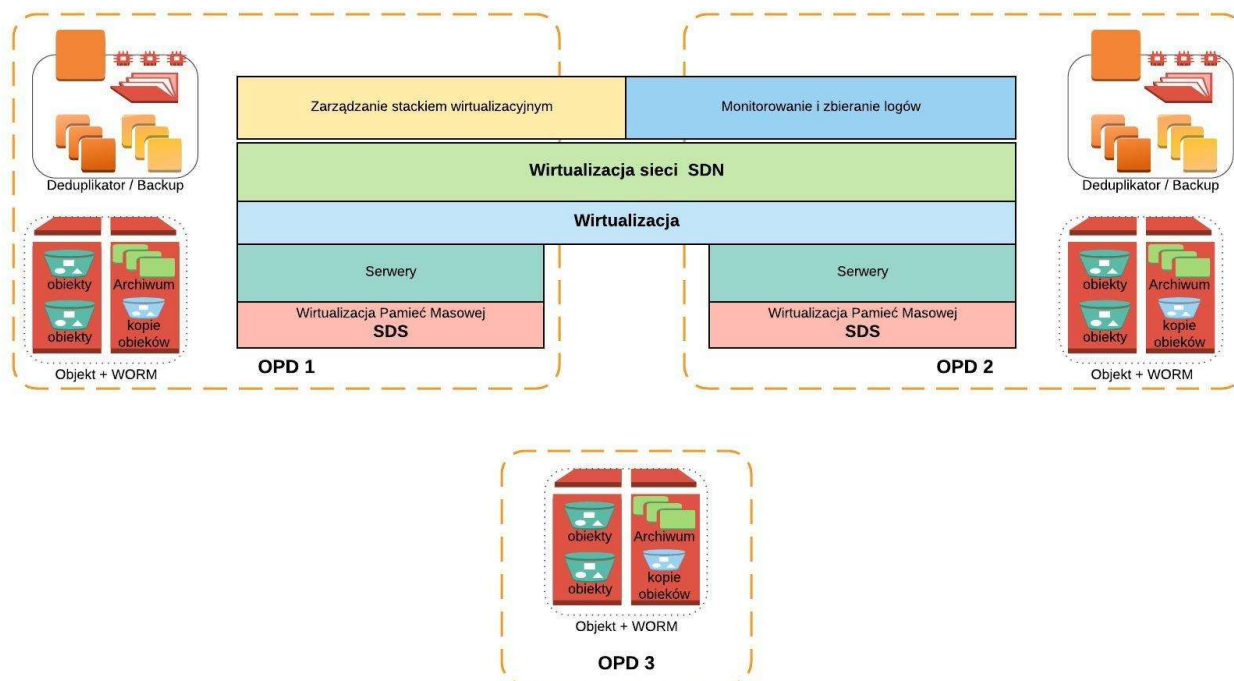
Faza 0 - Instalacja zarządzającej warstwy wirtualizacji, wirtualnej sieci wraz z monitorowaniem i kolekcja logów.

W tej fazie dostawca instaluje moduły zarządzania pojemnością i efektywnością platformy, a także moduł zbierania logów z infrastruktury. Instalowana zostaje warstwa wirtualizacji funkcji sieciowych.



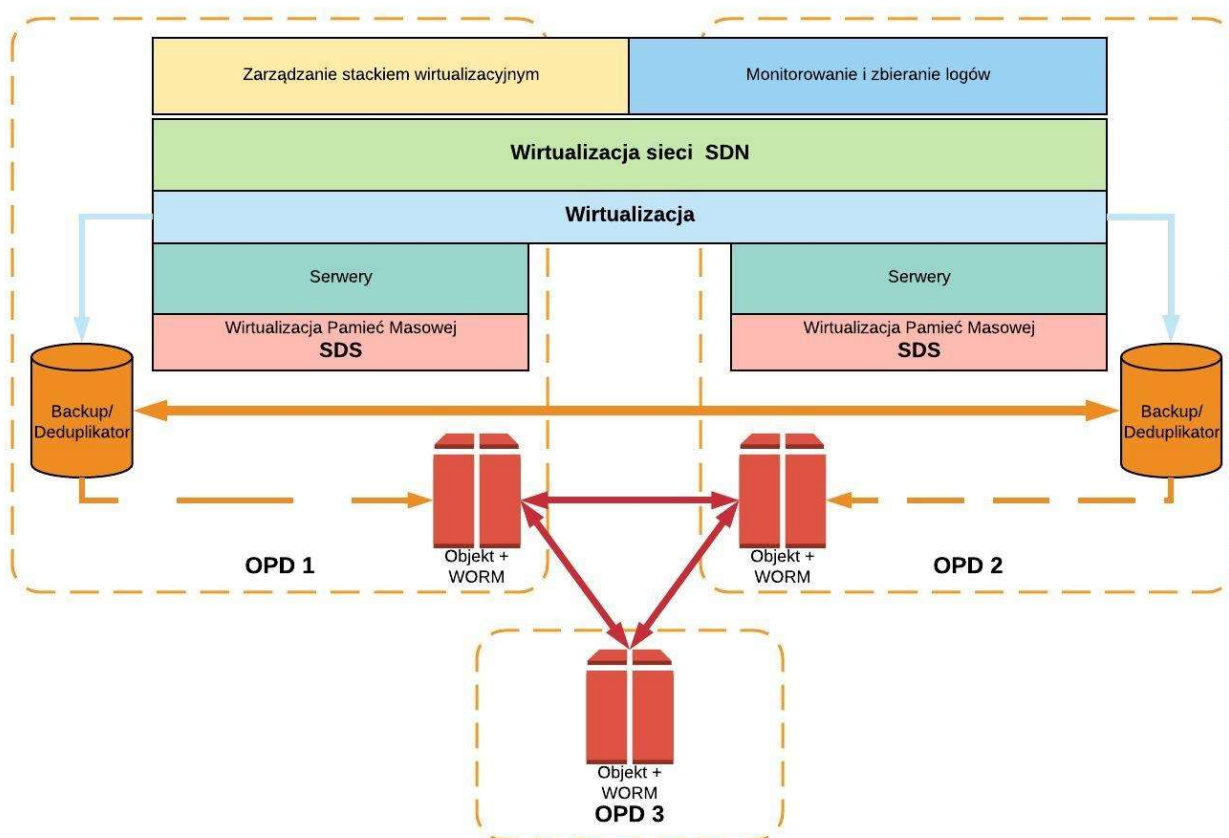
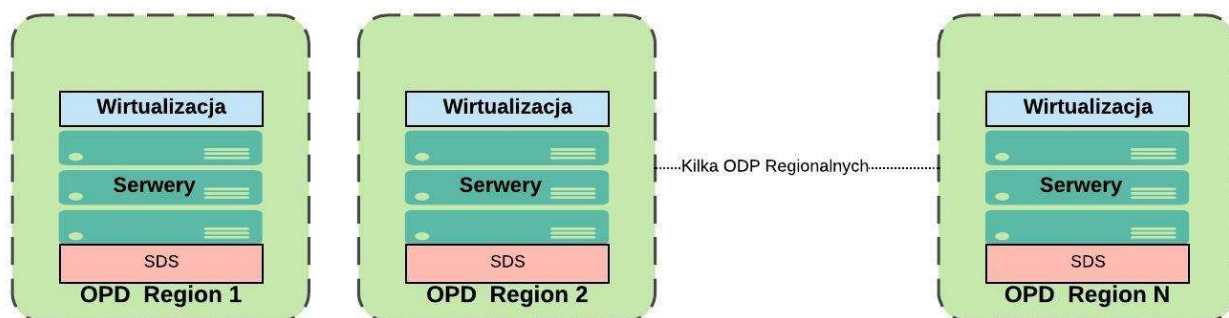
Faza 0 - Instalacja systemu backup wraz z obiekowym systemem składowania danych.

W tej fazie dostawca instaluje rozwiązania do backup-u wraz z deduplikatorami jak również system odtwarzania po awarii. W trzech głównych ośrodkach przetwarzania danych zainstalowany zostaje system obiektowego składowania danych.



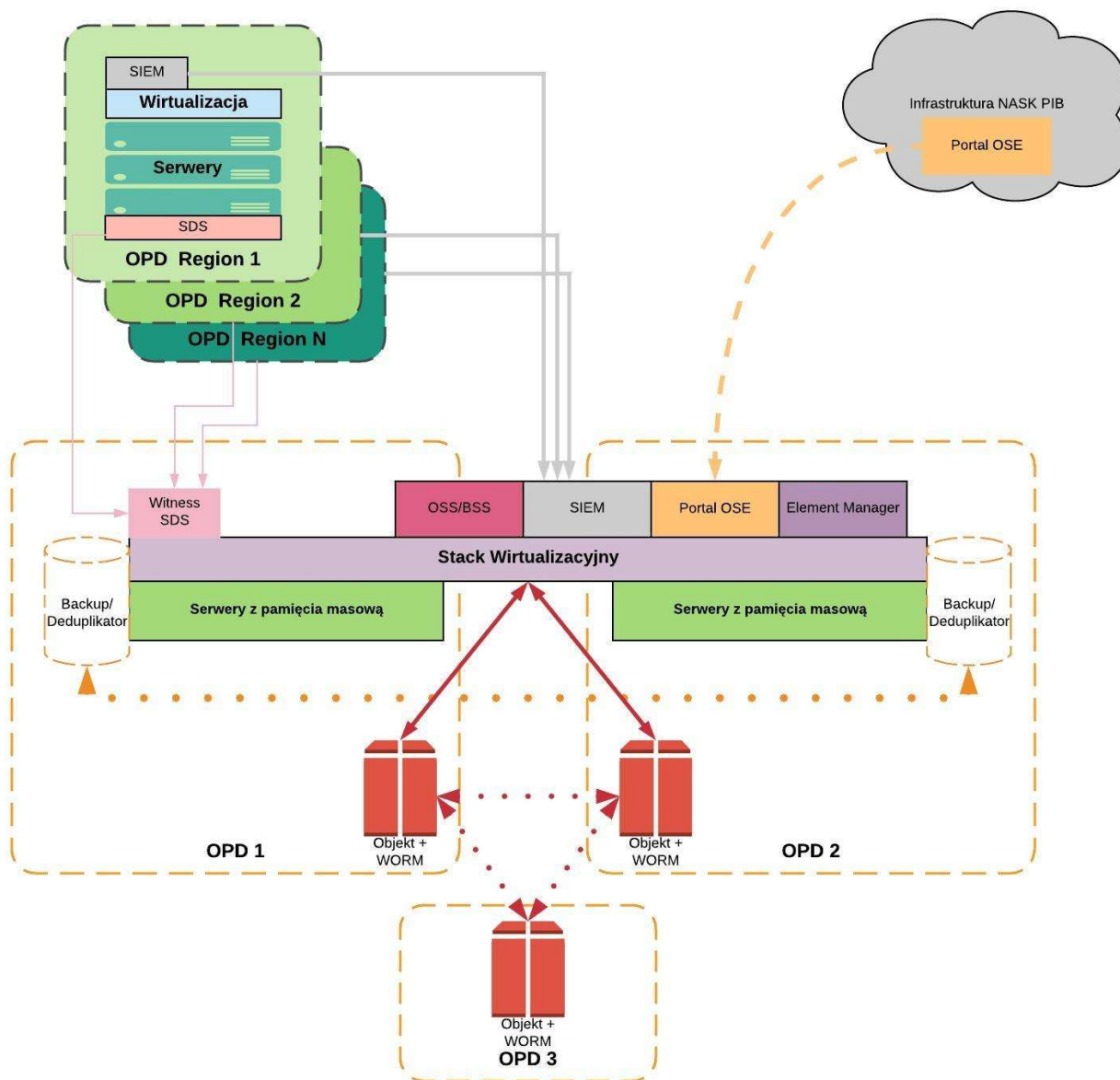
Faza 0 - Instalacja regionalnych ośrodków przetwarzania danych i konfiguracja systemów backup i DR

W tej fazie w 8 regionalnych ośrodkach przetwarzania danych (w tym 3 centralnych ośrodkach pełniących podwójną rolę) dostawca instaluje serwery i podłącza je do zainstalowanej już sieci LAN. Instalowana zostaje warstwa wirtualizacyjnej mocy obliczeniowej wraz z wirtualizacją przestrzeni dyskowej SDS. Skonfigurowana zostaje replikacja pomiędzy ośrodkami dla systemów backupowych/deduplikatorów. Skonfigurowane zostaje rozproszenie danych na trzy ośrodki w obiektowym systemie składowania danych. Skonfigurowane zostaje archiwum dla backupu na obiektowym systemie składowania danych.



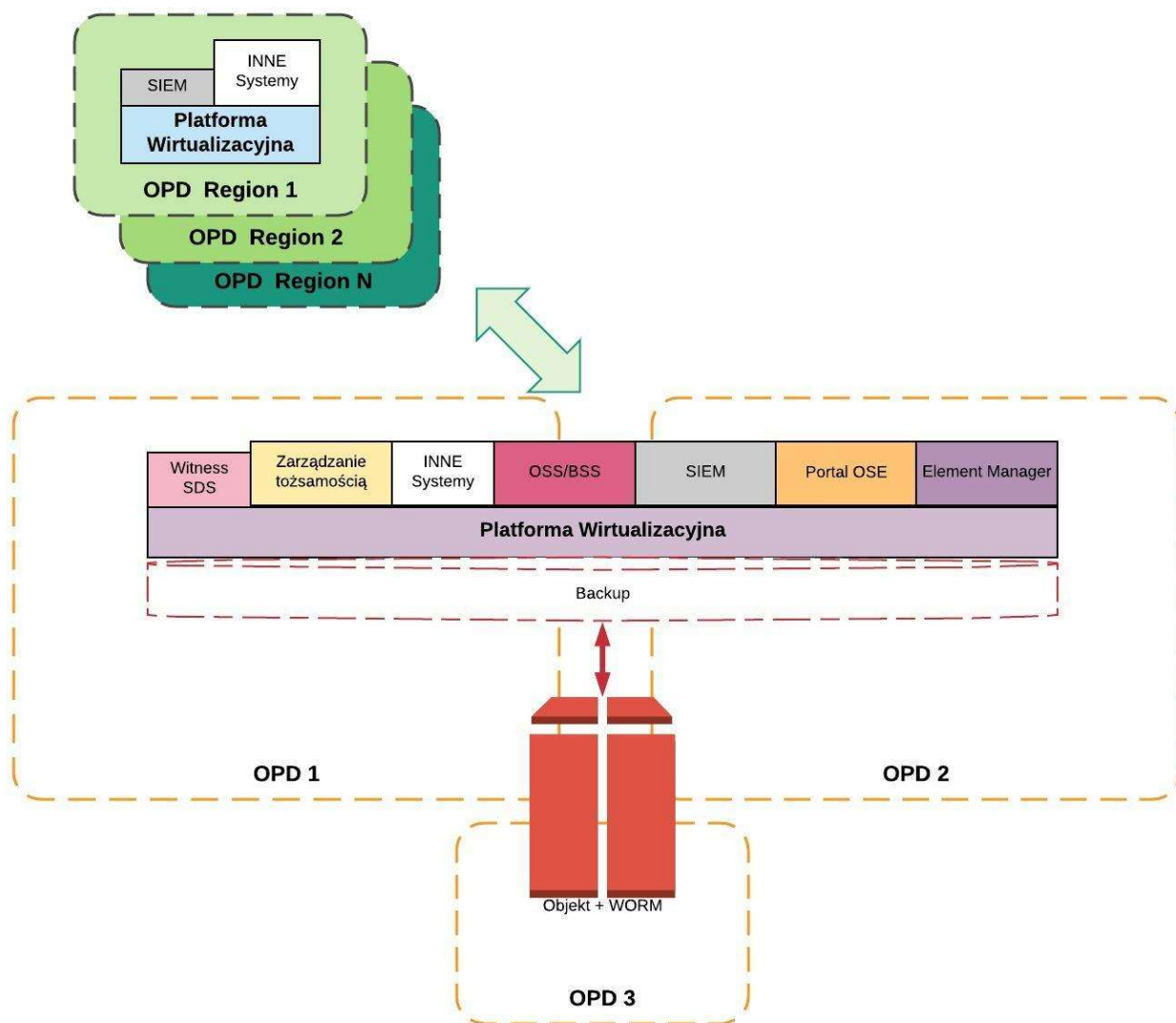
Faza 2 - Gotowość platformy do instalowania i migrowania aplikacji.

Na centralnej platformie wirtualizacyjnej instalowane zostają systemy OSS/BSS, SIEM, Element Manager, przemieszczany zostaje portal OSE. Część systemów jest integrowana z obiektywnym systemem składowania danych. System SIEM jest instalowany w regionalnych centrach przetwarzania danych.



Faza 3 - Gotowość platformy do instalowania dodatkowych systemów i aplikacji.

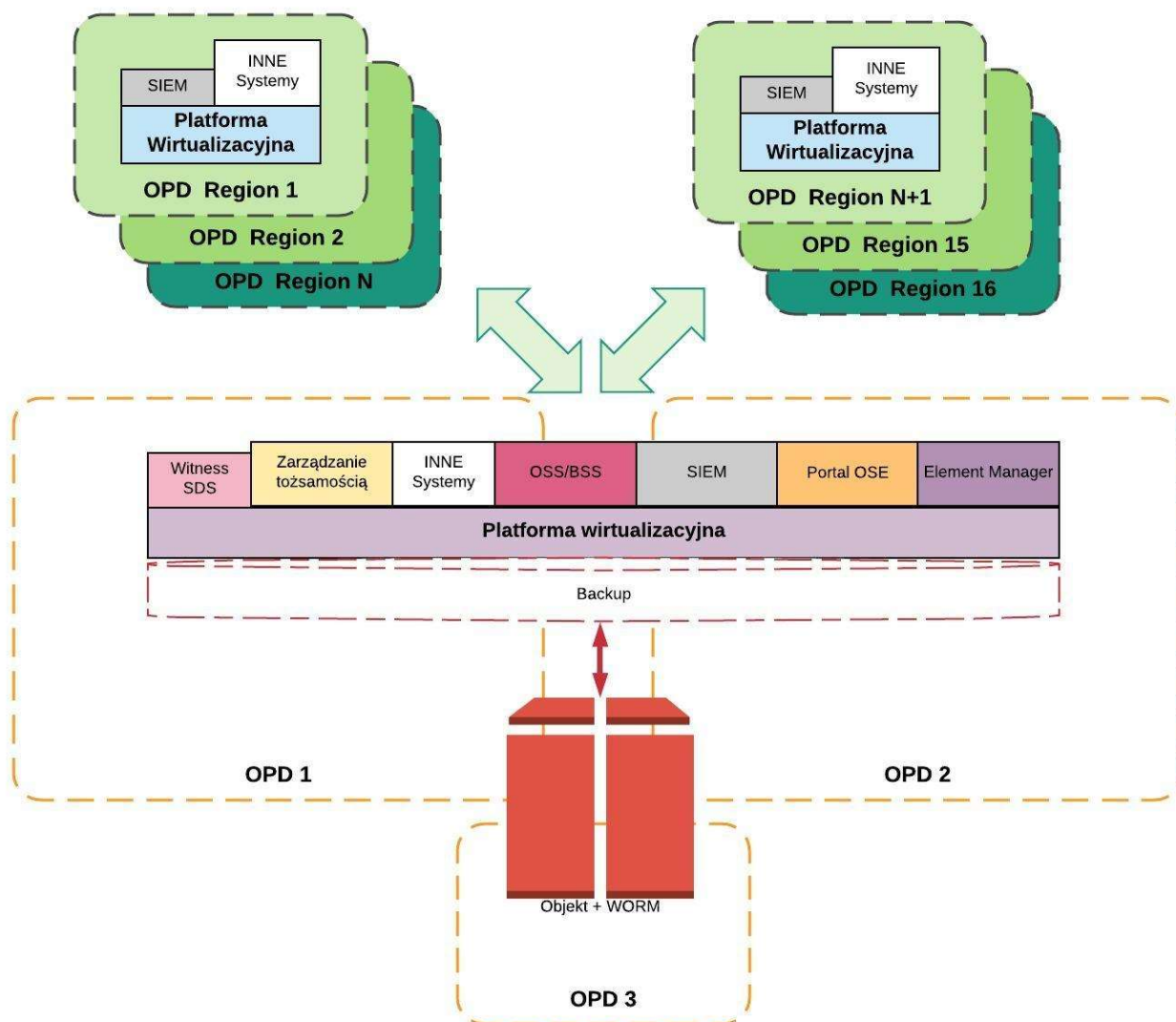
Na centralnej platformie wirtualizacyjnej zainstalowany zostaje system zarządzania tożsamością i pomocnicze systemy. W regionalnych centrach przetwarzania danych zainstalowane zostają serwery NTP, DHCP i inne systemy pomocnicze.



Faza 3 - Instalacja pozostałych regionalnych centrów danych.

W tej fazie w pozostałych 11 regionalnych ośrodkach przetwarzania danych dostawca instaluje serwery i podłącza je do zainstalowanej już sieci LAN. 4 z tych ośrodków będą podłączane na początku 2020 roku.

W dołączonych regionalnych ośrodkach przetwarzania danych zainstalowane zostają systemy pomocnicze i SIEM.



7. Opis przedmiotu zamówienia

7.1. Opis ogólny

Przedmiotem zamówienia jest wdrożenie Systemów OSS/BSS (zwanymi dalej Systemami lub Rozwiązaniem) zgodnie z przedstawionymi w dokumencie fazami i uwarunkowaniami wdrożenia, dotyczącymi uruchomienia kopii funkcjonalnej istniejących u Zamawiającego systemów Jira WF, SD, Insight wraz z dostawą, instalacją i uruchomieniem infrastruktury serwerowej, migracjami i przełączeniem usług z rozwiązania tymczasowego na rozwiązanie docelowe Zamawiającego oraz wykonaniem integracji ze wskazanymi systemami Zamawiającego. W ramach realizacji przedmiotu zamówienia Wykonawca jest zobowiązany do:

- wykonania projektu architektury Systemów OSS/BSS uwzględniającego wszystkie fazy wdrożenia (Projekt techniczny Systemów) zgodnie z wymaganiami Zamawiającego zawartymi w niniejszym dokumencie i z uwzględnieniem informacji zawartych w dostarczonych dokumentach oraz na bazie analizy środowiska operacyjnego i biznesowego Operatora OSE
- wykonania szczegółowego projektu architektury infrastruktury serwerowej (Projekt techniczny infrastruktury) dla Systemów OSS/BSS
- wdrożenia (dostawy, instalacji, konfiguracji i uruchomienia) niezbędnej infrastruktury serwerowej dla Systemów OSS/BSS umożliwiającej maksymalne ich zautomatyzowanie, integrację i niezawodność, zgodnie z wykonanym wcześniej przez Wykonawcę i zaakceptowanym przez Zamawiającego Projektem technicznym, obejmującego wszystkie założone fazy a także na bazie doświadczeń z faz wdrożenia 1 - 2, przeprowadzenie analizy biznesowej i implementacji ustalonych procesów biznesowych OSE
- wdrożenia rozwiązania „pod klucz” (zwanego dalej Rozwiązaniem lub Systemami OSS/BSS) obejmującego zarówno obszar systemów nadzoru klasy OSS (Operation Support System), obszar systemów klasy BSS (Business Support System), elementy systemów Enterprise Management oraz integrację z systemami Zamawiającego, zgodnie z wykonanym wcześniej przez Wykonawcę i zaakceptowanym przez Zamawiającego Projektem technicznym
- dostarczenia infrastruktury serwerowej dla pozostałych systemów Zamawiającego wdrożonych na potrzeby OSE, niebędących częścią niniejszego postępowania (wymagania odnośnie wymiarowania tej infrastruktury zostały przedstawione w punkcie opisującym wymagania dla infrastruktury zwirtualizowanej)
- integracji Systemów OSS/BSS z systemami Zamawiającego, wskazanymi przez Zamawiającego, wdrożonymi na potrzeby projektu OSE oraz z systemami NASK
- przeprowadzenie instruktaży dla pracowników Zamawiającego, zgodnie z wymaganiami opisanymi w załączniku "Zakres Instruktażu"
- przygotowanie i uruchomienie środowiska testowego pod kolejne etapy wdrożenia Systemów OSS/BSS, jak również do wykorzystania w pracach rozwojowych rozwiązania w przyszłości
- wykonanie Planu Testów
- przeprowadzenie testów przy udziale Zamawiającego

- dostarczenie dokumentacji poszczególnych modułów i dokumentacji powykonawczej całego rozwiązania
- świadczenie usług gwarancyjnych dla dostarczonych urządzeń i oprogramowania, zgodnie z wymaganiami Zamawiającego
- zapewnienie usług wsparcia producenckiego oraz wsparcia dla wdrożonego rozwiązania (systemy i infrastruktura) zgodnie z wymaganiami Zamawiającego
- świadczenie usługi utrzymania i administrowania Systemami OSS/BSS oraz systemami będącymi kopią funkcjonalną systemów Zamawiającego, a także infrastrukturą serwerową w ramach wdrożonego rozwiązania w okresie przejściowym na warunkach opisanych w niniejszym dokumencie
- po okresie przejściowym przekazanie utrzymania firmie, która w ramach outsourcingu IT będzie utrzymywać infrastrukturę i systemy OSE
- przygotowanie Planów kolejnych migracji
- migracje zarządzania usługami i procesami OSE z obecnych przejściowych systemów OSS/BSS NASK poprzez systemy będącymi kopią części systemów NASK aż do rozwiązania docelowego wdrożonego w wyniku niniejszego postępowania, z uwzględnieniem wszystkich faz wdrożenia oraz migracji danych
- świadczenie usługi Asysty technicznej

Systemy muszą zostać wdrożone zgodnie z wymaganiami Zamawiającego zawartymi w niniejszym dokumencie RFP. Wszystkie wymagania i parametry, w tym techniczne, funkcjonalne i wydajnościowe zawarte w niniejszym dokumencie mają charakter obligatoryjny. Wykonawca zobowiązany jest do spełnienia wymagań obligatoryjnych w ramach ceny oferowanego rozwiązania.

Wykonawca jest zobowiązany do zaproponowania Rozwiązania optymalnego pod względem jak najmniejszej ilości komponentów różnych producentów.

7.1.1. Beneficjenci systemu OSS/BSS

Podane poniżej liczby osób obsługujących sieć OSE ukazują plany NASK w zakresie zasobów osobowych. Należy przyjąć, że systemy OSS/BSS dostarczone przez Wykonawcę w ramach zakupionych licencji będą musiały obsłużyć podaną poniżej w tabeli liczbę użytkowników korzystających z podanych funkcjonalności. Zamawiający będzie mógł zmieniać ilość zamawianych licencji na użytkowników zgodnie z wyceną tych licencji i zgodnie ze swoim zapotrzebowaniem w danym momencie (o ile licencjonowanie systemów OSS/BSS będzie oparte na ilości użytkowników).

Funkcje POOSE i systemów współpracujących	Dział Centrum Kontaktów 35 osób	Dział Realizacji Podłączeń 35 osób	Dział współpracy z Operatorami 6 osób	Dział utrzymania (NOC & SOC) 80 osób (NASK + outsourcing)	Zespół Obsługi Incydentów Bezpieczeństwa 6 osób	Dział IT (rozwój i utrzymanie OSS/BSS & infrastrukturą serwerową) 28 osób (NASK + outsourcing)	Partnerzy serwisowi max 100 firm	Zespół Projektu OSE & Zespół wsparcia projektu 8 osób	Kadra zarządzająca 8 osób	Szkoła ca. 25tys.
---	---	--	---	---	---	--	--	---	-------------------------------------	-----------------------------

Single Sign On	X	X	X	X	X	X	X	X	X	
Fault & Performance Management (liczba jednoczesnych użytkowników = 60)		X	X	X		X				
Config Management (liczba jednoczesnych użytkowników = 60)		X		X		X				
Service & Config Provisionig (liczba jednoczesnych użytkowników = 60)		X		X		X				
Zarządzanie wirtualizacją i orkestracją w DC (liczba jednoczesnych użytkowników = 40)				X		X				
Inventaryzacja sieci i usług (liczba jednoczesnych użytkowników = 120)	X	X	X	X		X				
Zarządzanie relacjami z klientem (liczba jednoczesnych użytkowników = 70)	X	X				X				
Workflow (liczba jednoczesnych użytkowników = 200)	X	X	X	X	X	X	X	X	X	
Trouble Ticketing & ServiceDesk (liczba jednoczesnych użytkowników = 150)	X	X	X	X	X	X	X			
Repozytorium dokumentów (liczba jednoczesnych użytkowników = 50)	X	X	X	X	X	X		X	X	
Dostęp do raportów RO (liczba jednoczesnych użytkowników = 100)	X	X	X	X	X	X	X	X	X	X
Bilingowanie świadczonych usług (liczba jednoczesnych użytkowników = 60)	X			X				X	X	X
Bilingowanie świadczonych dla OSE usług przez dostawców i partnerów (liczba jednoczesnych użytkowników = 60)		X	X	X		X			X	
Rozliczanie dostawców i partnerów (liczba jednoczesnych użytkowników = 100)		X	X	X		X	X		X	
Rozliczanie projektu OSE (liczba jednoczesnych użytkowników = 5)								X	X	
Generowanie raportów (operacyjnych, projektowych, finansowych) (liczba jednoczesnych użytkowników = 100)	X	X	X	X		X		X		

Wielokanałowy kontakt z klientem (liczba jednoczesnych użytkowników = 30)	X				X					
Gospodarowanie magazynem sprzętu OSE (liczba jednoczesnych użytkowników = 80)		X		X		X	X			
SIEM (<i>zakup poza POOSE</i>)				X		X				
Element Managers dla urządzeń sieciowych w szkieletcie OSE (<i>zakup poza POOSE</i>)				X		X				
Element Managers dla systemów bezpieczeństwa : ADC, NGFW, SWG, DNS Filtering , SIEM (<i>zakup poza POOSE</i>)				X						
Portal Usługowy	X			X	X	X				X
Portal OSE dla klienta końcowego (<i>poza POOSE</i>)	X				X	X				X
System FK NASK PIB (<i>poza POOSE</i>)								X		
System magazynowy NASK PIB (<i>poza POOSE</i>)		X								

7.1.2. Informacje mające wpływ na architekturę rozwiązania

Rozwiązanie musi uwzględniać ilościowy rozkład elementów sieci, harmonogram jej wzrostu zapewniając odpowiednią wydajność funkcjonalności systemowych

I SIEĆ SZKIELETOWA

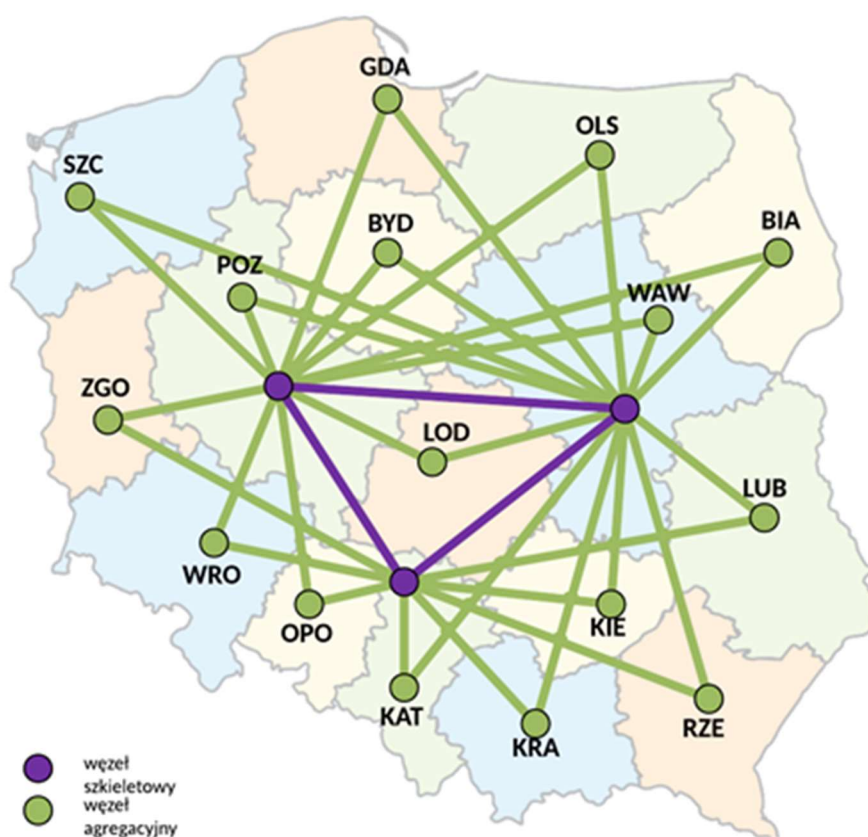
województwo	węzeł	liczba dołączonych szkół
mazowieckie	WAW	3 806
śląskie	KAT	3 447
wielkopolskie	POZ	2 184
małopolskie	KRA	2 157
łódzkie	LOD	1 553
dolnośląskie	WRO	1 424
pomorskie	GDA	1 363
lubelskie	LUB	1 348

województwo	węzeł	liczba dołączonych szkół
podkarpackie	RZE	1 328
kujawsko-pomorskie	TOR	1 194
warmińsko-mazurskie	OLS	1 132
zachodniopomorskie	SZC	942
świętokrzyskie	KIE	921
podlaskie	BIA	921
lubuskie	ZGO	712
opolskie	OPO	582
suma		25 014

Harmonogram wdrożenia typów węzłów OSE	
Typ	Przewidywana data wdrożenia węzła OSE
Węzeł Centralny 1:	02.04.2019
Węzeł Centralny 2:	02.04.2019
Węzeł Centralny 3:	16.04.2019
Węzeł Regionalny 1:	02.04.2019
Węzeł Regionalny 2:	02.04.2019
Węzeł Regionalny 3:	24.04.2019
Węzeł Regionalny 4:	01.05.2019
Węzeł Regionalny 5:	15.05.2019
Węzeł Regionalny 6:	27.08.2019
Węzeł Regionalny 7:	03.09.2019
Węzeł Regionalny 8:	10.09.2019
Węzeł Regionalny 9:	15.09.2019
Węzeł Regionalny 10:	20.09.2019
Węzeł Regionalny 11:	25.09.2019
Węzeł Regionalny 12:	30.09.2019
Węzeł Regionalny 13:	05.10.2019

Harmonogram wdrożenia typów węzłów OSE	
Węzeł Regionalny 14:	10.10.2019
Węzeł Regionalny 15:	15.10.2019
Węzeł Regionalny 16:	20.10.2019

Schemat połączeń Węzłów Agregacyjnych i Węzłów Szkieletowych jest pokazany poniżej.



W każdym **Węźle Szkieletowym Węzła Centralnego** będą m. in. styki do operatorów zewnętrznych oferujących wymianę ruchu. Ilości interfejsów będą następujące:

węzły centralne	ilość interfejsów			
	100GE	40GE	10GE	1GE
WAW-Core	15	6	15	10
POZ-Core	6	2	10	10
KAT-Core	8	4	10	10

Każdy **Węzeł Agregacyjny Węzła Regionalnego** wyposażony będzie w następujące ilości portów agregujących ruch do / ze szkół:

węzły regionalne	minimalna ilość interfejsów	
	10GE	1GE
WAW	30	45
KAT	24	15
KRA	12	20
POZ	15	15
RZE	8	35
LUB	8	35
WRO	10	20
LOD	10	15
GDA	10	15
TOR	8	20
SZC	6	15
OLS	8	15
KIE	6	15
BIA	6	15
OPO	5	15
ZGO	5	15

Sieć szkieletowa	
Węzły	3 Węzły Centralne , 16 Węzłów Regionalnych dostarczane będą : <ul style="list-style-type: none"> • stopniowo przez cały rok 2019

Sieć szkieletowa

	<ul style="list-style-type: none"> • przybliżony planowany czas wdrożenia pierwszego węzła centralnego : 02.04.2019 <p>W sieci OSE będą dwa rodzaje Węzłów:</p> <ul style="list-style-type: none"> • Węzły Regionalne, w których skład będą wchodzić Węzły Agregacyjne (do których będą dołączone łącza ze szkół) oraz Regionalne Węzły Bezpieczeństwa. • Węzły Centralne, w których skład będą wchodzić Węzły Szkieletowe, Centralne Węzły Bezpieczeństwa oraz Zasoby Obliczeniowe OSE (będące platformą dla systemów OSS / BSS). Do Węzłów Szkieletowych dołączone będą Węzły Agregacyjne. Węzły te będą także zapewniały łączność do sieci Internet. • Węzły Szkieletowe będą zlokalizowane w tych samych miejscach, co Węzły Agregacyjne, za wyjątkiem węzła WAW / WAW Core, w którym Węzeł Agregacyjny będzie umieszczony w innej lokalizacji niż Węzeł Szkieletowy (oba węzły będą zlokalizowane na terenie Warszawy). Urządzenia pełniące funkcje obu węzłów będą oddzielne, za wyjątkiem przełączników sieci lokalnej, które będą świadczyć usługi na rzecz zarówno Węzła Agregacyjnego jak i Węzła Szkieletowego.
Łącza	<p>40 łączy szkieletowych, czyli łączy pomiędzy węzłami OSE</p> <p>20 łączy tranzytowych, czyli łączy z wyjściem z sieci OSE do Internetu – łącza są obecnie w procesie postępowania zakupowego (zostaną dookreślone w momencie jego zakończenia)</p>
Urządzenia sieci	<p>Sumarycznie około 130-150 urządzeń (licząc również instancje wirtualne na urządzeniach, należy założyć o 1/3 więcej)</p> <p>urządzenia w węźle centralnym : router, router reflektor, shadow router</p> <p>urządzenia w węźle agregacyjnym : router, przełącznik LAN, shadow router</p> <p>sieć LAN w węźle do 3 urządzeń fizycznych</p> <p>sieć MGMT w węźle : router, switch, terminal serwer</p> <p>w agregacji ~10 prefixów IPv4, 1 prefix IPv6 (+ globalne tablice routingu - w sumie ok. 1M)</p> <p>instancje wirtualnych nie mniej niż 3 w węźle agregacyjnym (obecnie w przypadku uruchomienia usług VPN ~10k VRF w sieci + ~50k prefixów)</p>
Ilość modeli provisionowanych urządzeń	ok. 20 typów (agregacja , szkielet, LAN, zarządzanie)
Systemy	Dwie instancje (primary + secondary) systemów Element Manager do integracji
Szafy w kolokacjach	we wszystkich węzłach OSE w sumie 59 szaf,
Monitorowanie	<p>~100 tys. łączy (logicznych w sumie szkieletowych i dostępowych)</p> <p>~20 tys. łączy fizycznych</p> <p>około 130 urządzeń (należy założyć nawet max. 150 urządzeń)</p>
Ilość raportów ze statystyk	~25 rodzajów raportów (na pewno 95-percentyl, ruch w GNR, ruch na interfejsach szkieletowych i tranzytowych (średni w godzinach roboczych, max, 95 percentyl)),

Sieć szkieletowa

	statystyki z protokołów routingu (BGP), opóźnienia i straty na łączach, statystyki z CG-NAT, raporty z systemów bezpieczeństwa na temat stron odfiltrowanych w wyniku działania systemu filtracji treści (raporty dla dyrektorów szkół) aproksymacja zasobów dla innych, które pojawią z czasem
Konfiguracje	dla urządzeń szkieletowych / agregacyjnych 50 historycznych (rolowane + 5 punktów przywracania konfiguracji)
Wersje oprogramowania	jedna wersja per urządzenie (czyli dwie - aktualna i kandydująca) - ok. 10 typów urządzeń
Liczba portów	<ul style="list-style-type: none">• fizycznych tyle ile łącz• logicznych szkieletowych ~10 w agregacji , ~100 w szkielecie• logicznych do szkół ~145 tys. w tym :<ul style="list-style-type: none">○ 5 VLAN'ów per szkoła = 5 * 25 tys. = 125 tys.○ jeden VLAN zarządzający do lokalizacji = 1 * 20 tys = 20 tys.

II SIEĆ DOSTĘPOWA

Liczba łącz dostępowych w relacjach PWR (Punkt Wymiany Ruchu) - lokalizacja szkolna :

Ilość uruchomionych na dany rok

Łączy	Dostępowe - około 19-20 tysięcy, dostarczane w ramach harmonogramu podłączania szkół: 2018 - 1,5 tys. 2019 – 12,7 tys. 2020 – 19 tys. 2021 - 19,5 tys.
-------	--

Liczba łącz agregacyjnych w relacjach węzeł OSE - PWR (Punkt Wymiany Ruchu) :

Województwo	Punkt Styku	Docelowa Liczba 10GE	Docelowa liczba 1GE2
MAZOWIECKIE	Warszawa	15	32
LUBELSKIE	Lublin	4	25
PODLASKIE	Białystok	4	4
MAŁOPOLSKIE	Kraków	9	13
ŚLĄSKIE	Katowice	16	4
KUJAWSKO-POMORSKIE	Bydgoszcz	5	7
POMORSKIE	Gdańsk	6	5
WIELKOPOLSKIE	Poznań	10	4
WARMIŃSKO-MAZURSKIE	Olsztyn	5	4
OPOLSKIE	Opole	2	8
ŁÓDZKIE	Łódź	7	4
ŚWIĘTOKRZYSKIE	Kielce	4	4
ZACHODNIOPOMORSKIE	Szczecin	4	5
LUBUSKIE	Zielona Góra	3	4
DOLNOŚLĄSKIE	Wrocław	6	8
PODKARPACKIE	Rzeszów	4	24
Razem		104	155

III SIEĆ SZKOLNA

Liczba podłączeń w danym roku							Liczba podłączeń do końca danego roku					
Rok	Liczba lokalizacji	Liczba szkół	Ilość CPE	Ilość SW	Ilość AP	Łączna ilość urządzeń	Liczba lokalizacji	Liczba szkół	Ilość CPE	Ilość SW	Ilość AP	Łączna ilość urządzeń
2018	1 500	2 250	1 500	2 250	2 250	6 000	1 500	2 250	1 500	2 250	2 250	6 000

Liczba podłączeń w danym roku							Liczba podłączeń do końca danego roku					
2019	11 200	16 800	11 200	16 800	16 800	44 800	12 700	19 050	12 700	19 050	19 050	50 800
2020	6 300	5 450	6 300	5 450	5 450	17 200	19 000	24 500	19 000	24 500	24 500	68 000
2021	500	500	500	500	500	1 500	19 500	25 000	19 500	25 000	25 000	69 500
RAZEM	19 500	25 000	19 500	25 000	25 000	69 500	19 500	25 000	19 500	25 000	25 000	69 500

Sieć szkolna				
Szafy	Szafy w lokalizacjach szkolnych - jedna na lokalizację			
Urządzenia	jedno CPE na lokalizację, jeden SW i jeden AP na szkołę na szkołę średnio 1,5 prefixu IPv4, 1 prefix IPv6 jeden VRF na szkołę			
Ruch sieciowy	Węzeł agregacyjny	Ruch do szkół		Ruch ze szkół
		<i>pasmo</i>	<i>pakiety</i>	<i>pasmo</i>
		<i>[Mb/s]</i>	<i>[kpps]</i>	<i>[Mb/s]</i>
				<i>[kpps]</i>
	WAW	160 990	55 531	58 610
	KAT	145 810	50 293	53 080
	POZ	92 380	31 865	33 630
	KRA	91 240	31 471	33 220
	LOD	65 690	22 659	23 920
	WRO	60 240	20 777	21 930
	GDA	57 650	19 887	20 990
	LUB	57 020	19 668	20 760
	RZE	56 170	19 376	20 450
	TOR	50 510	17 421	18 390

Sieć szkolna

	OLS	47 880	16 516	17 430	6 013
	SZC	39 850	13 744	14 510	5 004
	KIE	38 960	13 438	14 180	4 892
	BIA	38 960	13 438	14 180	4 892
	ZGO	30 120	10 388	10 960	3 782
	OPO	24 620	8 492	8 960	3 092
Monitorowanie	<p>ilość monitorowanych (availability) urządzeń szkolnych (ICMP) przez pierwsze 3 tygodnie od podłączenia lokalizacji szkolnej do OSE oraz w wyniku niezbędnej diagnostyki ad hoc :</p> <p>~ 25 tys. (AP +SW) + 19,5 tys. CPE = ~70 tys. (przy założeniu monitorowania SW i AP)</p> <p>ilość monitorowanych łącz fizycznych w lokalizacji szkolnej (przy założeniu 1,5 szkoły na lokalizację szkolną) : ~ 3,5</p> <p>ilość urządzeń szkolnych wysyłających alarmy (tylko SYSLOG i via SIEM) przez pierwsze 3 tygodnie od podłączenia lokalizacji szkolnej do OSE oraz w wyniku niezbędnej diagnostyki ad hoc (pomiar na urządzeniach szkolnych) : ~19,5 tys. (tylko CPE)</p>				
Ilość statystyk	<p>ruch z lokalizacji szkolnej / szkoły / VLANu szkoły zbierany po stronie szkieletu sieci - na subinterface'ach urządzeń sieciowych w węzłach OSE (per szkoła do 5 VLAN), co daje statystyk ruchu z max. następującej liczby łącz:</p> <p>25 tys. * 5 subinterface (per VLAN) + 19,5 tys. 1 subinterface (VLAN zarządzający) ~= 145 tys. statystyk</p> <p>Poniższe statystyki zbierane po stronie lokalizacji szkolnej przez pierwsze 3 tygodnie od podłączenia lokalizacji szkolnej do OSE oraz w wyniku niezbędnej diagnostyki ad hoc :</p> <p>CPE: ~2,5 statystyki łącza, 1 RAM, 1 CPU SW: 2 statystyki łącza AP: 1 łącze, 1 ilość użytkowników WLAN</p>				
Konfiguracje	1 bazowa (moment instalacji), 3 punkty przywracania konfiguracji, 5 rolowanych				

Modele urządzeń instalowanych w szkole (provisioning CPE)

lista na dzień opublikowania RFP - będzie się sukcesywnie powiększać

Modele CPE	Modele SW	Modele AP
------------	-----------	-----------

Modele urządzeń instalowanych w szkole (provisioning CPE)**lista na dzień opublikowania RFP - będzie się sukcesywnie powiększać**

FortiGate-81E-POE		FortiAP-221C
FortiGate-101E		FortiAP-221E
Firewall Huawei USG6320	Huawei S1720-10GW-2P-E	Huawei AP4050DN
Huawei USG6330 AC	DCN S4600-28P-SI-R2	
MikroTik CCR1009-7G-1C-1S+		Access Point Ubiquiti UniFi AC Long Range

Usługi

Ilość rodzajów usług uruchamianych w sieci OSE	<p>~10 rodzajów z wariantami w tym:</p> <ul style="list-style-type: none">• Internet 100Mbps• Internet powyżej 100Mbps• IPSEC• VLAN (wiele wariantów: INET, NO SECURITY, WLAM PUBLIC, inne)• Internet via MAN/ODN (agregacja dostępu dla wielu szkół)• inne
Monitorowanie	<p>ilość monitorowanych usług:</p> <p>~25 tys. usług dostępu do Internetu x 3 VPN (Standard, Security, Public WLAN) = ~75 tys.</p> <p>~50 tys. usług VPN (dodatkowe 2 VPN na przyszłe usługi),</p> <p>~20 tys. MGMT</p> <p>ilość dodatkowych relacji pomiarowych: poniżej 1 tys.</p>

ilość monitorowanych szkół jednocześnie w związku z nadzorem przez pierwsze 3 tygodnie po podłączeniu szkół do OSE

Parametry	Wszystkie urządzenia	Uwagi	Samo CPE (Fault, tylko monitoring per lokalizacja)
Ilość tyg. monitorowania szkoły	3	wymóg biznesowy	3

ilość monitorowanych szkół jednocześnie w związku z nadzorem przez pierwsze 3 tygodnie po podłączeniu szkół do OSE			
Ilość szkół podłączanych dziennie (szczyt trwający przez 3 tygodnie)	150	nie 200 (jak wymóg biznesowy) bo pik nie będzie nigdy trwał non-stop 3 tygodnie , więc średnio mniej szkół w tych 3 tyg. założenie: 1,5 szkoły na lokalizację	100
przybliżona ilość dni monitorowanych w tygodniu	6	6 a nie 7 bo w weekendy szkoły nie będą podłączane i nie będą zakładane nowe monitoringi	6
Ilość podłączeń przez 21 dni (podłączenia przez 7 dni w tygodniu)	2700		1800
Ilość urządzeń na podłączenie	2,5	SW + AP + CPE (0,5 bo CPE jest per lokalizacja, więc per szkoła mniej niż 1)	1
max ilość urządzeń równolegle monitorowanych	6750		1800
ilość monitorowanych szkół jednocześnie w związku z awariami			
Parametry	Wszystkie urządzenia	Uwagi	Samo CPE (Fault)
Ilość urządzeń w szkołach (w przybliżeniu)	70 000	20 tys. lokalizacji * CPE + 25 tys. szkół * (SW+AP)	20 000
Współczynnik awarii (w skali miesiąca)	1,50%	założenie	1,50%
Wyliczenia	Wszystkie urządzenia	Jednostka	Samo CPE (Fault)
Ilość awarii w miesiącu	1050	urządzenia	300
Długość okresu monitoringu diagnostycznego	2	tygodnie	2

ilość monitorowanych szkół jednocześnie w związku z nadzorem przez pierwsze 3 tygodnie po podłączeniu szkół do OSE			
Sumaryczny czas monitoringu w miesiącu	2100	tygodnie (suma z wszystkich urzędzeń)	600
Średnia ilość urzędzeń równoległe monitorowanych	525	urzędzenia	150
Wniosek : w roku 2019, 2020 i 2021 przyjąć 7000 urzędzeń równoległe monitorowanych, od 2022 roku 1000 urzędzeń równoległe monitorowanych (nie ma podłączeń nowych szkół, ale mogą być zmiany lokalizacji szkół, stąd liczba większa niż 525)			

Rozwiązanie musi uwzględniać architekturę obszaru bezpieczeństwa zapewniając odpowiednią wydajność i zasoby do obsługi

IV URZĄDZENIA BEZPIECZEŃSTWA W SZKIELECIE

Urządzenia	
ilość monitorowanych urzędzeń/systemów	ok 400 urzędzeń razem w węzłach bezpieczeństwa (centralnych i regionalnych) Monitorowanie: <ul style="list-style-type: none"> • pasywne (SNMP TRAP, SYSLOG) • aktywne (ICMP, SNMP.)
ilość provisionowanych modeli urzędzeń bezpieczeństwa w szkielecie	ok 20 typów (agregacja, szkielet, LAN, zarządzanie)
ilość wersji software dla wszystkich urzędzeń bezpieczeństwa	Zalecane jest, aby wszędzie była ta sama wersja softu - ok 10 typów urzędzeń

Urządzenia

ilość integracji z systemami bezpieczeństwa	<p>Zakłada się, że ilość Element Managerów w obszarze bezpieczeństwa, z którymi niezbędne są integracje będzie następująca :</p> <ul style="list-style-type: none"> • 18 Element Managerów do ADC (Application Delivery Controler, 16 węzłów regionalnych i 2 węzły centralne) • 16 Element Managerów do SWG (Security Web Gateway, 16 węzłów regionalnych) • 18 Element Managerów do NG Firewall (16 węzłów regionalnych i 2 węzły centralne) • 2 instancje Element Managera do Systemu Zarządzania Tożsamością (w dalszych etapach projektu OSE) • 2 instancje Element Managera SIEM (2 węzły centralne) • 2 instancje DNS (2 węzły centralne) <p>Integracje zakładają:</p> <ul style="list-style-type: none"> • provisioning i modyfikację usług bezpieczeństwa • forwardowanie logów z urządzeń CPE w szkołach via SIEM • wysyłanie alarmów z urządzeń/systemów bezpieczeństwa do OSS Fault Management • zbieranie statystyk performance'owych z urządzeń/systemów bezpieczeństwa do OSS Performance Management • wysyłanie raportów bezpieczeństwa do Centralnego Systemu Raportowego • wysyłanie/pobieranie plików z raportami i plików graficznych ze statystykami do/przez portalu usługowego OSE
sposoby integracji	<p>Sposoby i poziomy integracji docelowych systemów OSS/BSS z urządzeniami i systemami bezpieczeństwa:</p> <ul style="list-style-type: none"> • wymiana danych standardowymi mechanizmami typu REST API • wymiana plików (TXT, CSV, XML, JSON) • wymiana plików graficznych • plików raportowych (PDF, XLS)

Usługi

ilość polityk bezpieczeństwa	maksymalnie 15 per szkoła
ilość urządzeń podłączonych do serwera RADIUS	urządzenia CPE + urządzenia sieciowe + urządzenia bezpieczeństwa ~ 20 tys. + 130 + 400 = 20,5 tys.

Usługi	
ilość autoryzacji na dobę w serwerze RADIUS	~ 300
Funkcjonalności usług w regionalnych węzłach bezpieczeństwa	<ul style="list-style-type: none"> • Zapewnienie bezpieczeństwa teleinformatycznego użytkownikom sieci OSE • Wykrywanie i zapobieganie włamaniom poprzez wykrywanie i blokowanie ataków sieciowych w czasie rzeczywistym. • Zabezpieczanie bazujące na adresacji sieciowej, użytkownikach oraz zawartości transmitowanej poprzez sieć teleinformatyczną. • Mechanizmy ochrony użytkowników przed zaawansowanymi zagrożeniami oraz mechanizmy kontroli aplikacji webowych. • Mechanizmy autoryzacji i autentykacji użytkowników i mapowania ich do adresu IP. • Monitorowanie ruchu sieciowego i zapisywanie najważniejszych zdarzeń do logu. • Mechanizmy przypisania polityk kontroli treści użytkownikom. • Mechanizmy ochrony użytkownika sieci OSE, realizowane w oparciu o systemy klasy SWG
Funkcjonalności usług w centralnych węzłach bezpieczeństwa	<ul style="list-style-type: none"> • Zapewnienie bezpieczeństwa teleinformatyczne zasobów obliczeniowych i systemów wsparcia • Wykrywanie i zapobieganie włamaniom poprzez wykrywanie i blokowanie ataków sieciowych w czasie rzeczywistym

Monitorowanie	
dzienna ilość alarmów z systemów bezpieczeństwa	około 2000 z urządzeń w węzłach bezpieczeństwa plus alarmy typu Fault z urządzeń w szkole (tylko CPE) - forwarding z SIEM (założenie zbierania logów 3 tyg. po podłączeniu szkoły do OSE i ad. hoc w razie niezbędnej diagnostyki)
ilość statystyk z urządzeń/systemów bezpieczeństwa (per węzeł centralny/regionalny)	z węzłów centralnych ok 20 z węzłów regionalnych ok 100
raporty z systemów bezpieczeństwa dla dyrektorów szkół (przekazywane do Centralnego systemu Raportowego i na Portal Usługowy z systemów bezpieczeństwa)	<ol style="list-style-type: none"> 1. Ochrona użytkownika OSE <ol style="list-style-type: none"> a. Alerty zdarzeń prób wejść na strony z kategorii niedozwolonych (szczególnie nielegalnych)

- b. Alerty zdarzeń prób wyszukiwania informacji dotyczących kategorii niedozwolonych (szczególnie nielegalnych)
- c. Alerty zdarzeń wejść na strony oraz prób wyszukiwania informacji o charakterze odbiegającym od normy (identyfikacja zjawisk typu Challenge, Fake news itp.)
- d. Alerty zdarzeń wykrytych zjawisk związanych z cyberprzemocą
- e. Raporty ukazujące globalne informacje o sposobie wykorzystania Internetu w szkole
- f. Raporty obejmujące wykryte w danym okresie czasu zdarzenia przedstawione powyżej.

2. Ochrona przed szkodliwym oprogramowaniem

- a. Alerty zdarzeń wykrytego szkodliwego oprogramowania
- b. Alerty zdarzeń wykrytych ataków sieciowych (w tym ataki typu DDoS)
- c. Alerty zdarzeń wykrytych prób komunikacji z serwerami C&C (Command&Control, czyli serwerami, które zarządzają działaniem wirusa na komputerach)
- d. Alerty zdarzeń wykrytych prób komunikacji o charakterze odbiegającym od normy
- e. Alerty zdarzeń wykrytych prób komunikacji z adresami IP w internecie o podejrzaną reputację
- f. Raporty ukazujące globalne informacje o sposobie wykorzystania Internetu w szkole
- g. Raporty obejmujące wykryte w danym okresie czasu zdarzenia przedstawione powyżej.

3. Ochrona infrastruktury

- a. Alerty zdarzeń wykrytych prób komunikacji z serwerami C&C (Command&Control, czyli serwerami, które zarządzają działaniem wirusa na komputerach)
- b. Alerty zdarzeń wykrytych prób komunikacji o charakterze odbiegającym od normy

Monitorowanie

	<ul style="list-style-type: none">c. Alerty zdarzeń wykrytych prób komunikacji z adresami IP w internecie o podejrzaną reputacjęd. Raporty ukazujące globalne informacje o sposobie wykorzystania Internetu w szkolee. Raporty obejmujące wykryte w danym okresie czasu zdarzenia przedstawione powyżej.
--	--

V ALARMY

Alarmy SIEĆ SZKIELETOWA

założenie: 1400 alarmów dziennie na urządzenie szkieletowe (sieciowe i bezpieczeństwa)

<i>Maksymalna ilość urządzeń sieci we wszystkich węzłach</i>	<i>Maksymalna ilość urządzeń bezpieczeństwa w węźle</i>	<i>Liczba Centralnych Węzłów Bezpieczeństwa</i>	<i>Liczba Regionalnych Węzłów Bezpieczeństwa</i>	<i>SIEĆ ilość urządzeń</i>	<i>SIEĆ średnia ilość alarmów w na dzień</i>	<i>BEZPIECZEŃSTWO ilość urządzeń/systemów</i>	<i>BEZPIECZEŃSTWO średnia ilość alarmów na dzień</i>	<i>Łączna średnia ilość alarmów w na dzień</i>	<i>Łączna średnia ilość alarmów w w roku</i>
150	22	2	16	150	210 000	396	554 400	764 400	279 006 000

Alarmy SIEĆ SZKOLNA (dane z zakładki "ilość urządzeń w szkole" - SAMO CPE)

założenie: 20 alarmów na jedno CPE (dziennie)

<i>Rok</i>	<i>Ilość urządzeń CPE na raz monitorowanych</i>	<i>Ilość alarmów na dzień</i>	<i>Łączna ilość alarmów w roku</i>
2019	1 950	39 000	14 235 000
2020	1 950	39 000	14 235 000
2021	1 950	39 000	14 235 000
2022	150	3 000	1 095 000

Alarmy SIEĆ SZKIELETOWA + SZKOLNA

Rok	Łączna ilość alarmów dziennie (razem)	EPH - Events per Hour (razem)	EPS - Events per Second (razem)
2019	803 400	33 475,00	9,30
2020	803 400	33 475,00	9,30
2021	803 400	33 475,00	9,30
2022	767 400	31 975,00	8,88

VI STATYSTYKI**Statystyki performance'owe SIEĆ SZKIELETOWA**

założenie: ok. 25 statystyk na urządzenie sieciowe, ok. 25 statystyk na urządzenie bezpieczeństwa w węźle centralnym, 50 statystyk na urządzenie w węźle regionalnym

Maksymalna ilość urządzeń sieci we wszystkich węzłach	Maksymalna ilość urządzeń bezpieczeństwa w węźle	Liczba Centralnych Węzłów Bezpieczeństwa	Liczba Regionalnych Węzłów Bezpieczeństwa	SIEĆ ilość urządzeń	SIEĆ ilość statystyk	BEZPIECZEŃSTWO ilość urządzeń/systemów	BEZPIECZEŃSTWA ilość statystyk	Ilość statystyk razem
150	22	2	16	150	3 750	396	18 700	22 450

Statystyki performance'owe SIEĆ SZKOLNA

założenie: max 10 statystyk na jedno urządzenia w szkole

Rok	Ilość urządzeń w szkole równolegle monitorowanych	Ilość statystyk ze szkoły
2019	7 000	70 000
2020	7 000	70 000
2021	7 000	70 000
2022	1 000	10 000

Statystyki ruchu (całość)				
Rok	ilość dostępowych łącz fizycznych	ilość szkół	ilość max dostępowych łącz logicznych	ca. ilość statystyk ruch (szkielet, agregacja, dostęp)
2019	12 700	19 050	107 950	108 060
2020	19 000	24 500	141 500	141 610
2021	19 500	25 000	144 500	144 610
2022	19 500	25 000	144 500	144 610

Rozwiązanie musi uwzględniać uwarunkowania aplikacyjne w zakresie ilości użytkowników, realizowanych procesów, przetwarzanych danych i harmonogramu rozwoju zapewniając odpowiednią wydajność systemów, dostępność funkcjonalności i zasoby do przechowywania i przetwarzania danych

VII APLIKACJE

Użytkownicy systemów	
ilość użytkowników systemów OSS	~do 20-25 jednoczesnych użytkowników (NOC,SOC), do 50 nazwanych użytkowników Dział Realizacji Podłączy: 30-35 użytkowników Zespół Utrzymania: do 30 nazwanych użytkowników
ilość użytkowników w obszarze TT	Dział Realizacji Podłączy : 30-40 osób Zespół Obsługi Incydentów Bezpieczeństwa: 6 użytkowników Zespół Utrzymania: do 100 nazwanych użytkowników (wraz z Działem Centrum Kontakt), jednoczesnych użytkowników do 72
Ilość użytkowników w ramach dostępu do Portalu Usługowego	max 25 000 szkół, w każdej szkole nazwanych 4-5 ról użytkowników funkcyjnych (pracowników/współpracowników szkoły), ~ 100 000 użytkowników nazwanych
Ilość użytkowników w obszarze SD	Dział Realizacji Podłączy 30-40 osób Zespół utrzymania: do 75 nazwanych (bez podwykonawców w terenie)

Użytkownicy systemów	
	Zewnętrzni: maksymalnie 100 partnerów serwisowych - dedykowani pracownicy, różne ilości w ramach partnera
Ilość użytkowników w obszarze magazynowym	Dział Realizacji Podłączeń: 30-40 osób Zespół Utrzymania: do 20 nazwanych użytkowników Pracownicy podwykonawców (do 100 użytkowników)
Ilość użytkowników w obszarze centrum kontaktu	Agenci CC (+ 2 supervisor) 2019: 23 2020: 34 2021: 35 Zespół utrzymania: na tę chwilę brak decyzji, co do korzystania z IVR przez NOC i SOC Zespół Obsługi Incydentów Bezpieczeństwa: 6 (1 supervisor) Dział Realizacji Podłączeń: 30-35 agentów; do 5 supervisorów.
Ilość administratorów systemów OSS/BSS	~20 (wydzielona część Zespołu Utrzymania)

Procesy biznesowe	
Produkty	Okolo 10 głównych, dowolna ilość parametrów
Ilość procesów biznesowych OSE	<p>Obecnie zdefiniowanych ok. 55, w tym najważniejsze procesy operacyjne (uruchomione lub w trakcie uruchamiania):</p> <ul style="list-style-type: none"> • pozyskania szkoły • podłączenia szkoły • zamawiania łącz • obsługi zgłoszeń • obsługi zmian w usłudze (w szczególności zmian parametrów usług bezpieczeństwa) • obsługi awarii masowych • obsługi prac planowych • zlecenia prac w szkole do podwykonawcy • zlecenia prac w szkielecie OSE • obsługi reklamacji • rozliczeń z podwykonawcami • gospodarki magazynowej

Procesy biznesowe	
	<p>Planowanych 70 - procesy (workflow) do wdrożenia przez Wykonawcę w ramach wdrożenia lub w ramach utrzymania w okresie 5 lat</p> <p>Należy założyć, że procesy są ze sobą powiązane zależnościami wpływającymi na przebieg procesów oraz wspólnymi dokumentami.</p> <p>Zamawiający oczekuje od Wykonawcy zarówno implementacji nowych/ modyfikowania działających procesów jak i wsparcia Wykonawcy przy tworzeniu przez Zamawiającego nowych procesów</p>
Obszar pozyskania	<p>W peek-u 200 szkół w procesie rozpoczynanych się jednego dnia</p> <p>W peeku 150 zamówień na łączu rozpoczynanych się jednego dnia</p> <p>Masowe podpisywanie umów 100 sztuk w ramach jednego spotkania</p> <p>Uwaga: W sytuacji problemów z systemami, lub partnerami zewnętrznymi (np. operatorami) liczba zamówień może ulec spiętrzeniu</p>
średnia ilość zgłoszeń obsługi ze szkół dziennie (inicjowanych przez szkołę po podpisaniu umowy na portalu OSE lub w Centrum Kontaktu)	<p>90% w godz. 7:00-15:00</p> <p>Liczba zgłoszeń:</p> <p>2019: 25400</p> <p>2021: 37756</p> <p>2021: 39022</p>
średnia ilość zleceń wystawianych partnerom	<p>Miesięcznie 1000-1200 zleceń - w procesie zlecenia prac podwykonawcom</p> <p>Miesięcznie (docelowo po wszystkich podłączeniach) ok 700-1000 zleceń - w procesie obsługi zgłoszeń</p>
Faktury	<p>faktury przychodowe - tyle, co szkół do ca. 25000</p> <p>faktury kosztowe - większość to faktury za łączu (19,5 tys.) + faktury od poddostawcy (zbiorczo miesięcznie per województwo) + inne projektowe</p>

Szacowana ilość zgłoszeń i ilość pracowników (agentów,supervisorów) w Centrum Kontaktu OSE					
Rok		2018	2019	2020	2021
Liczba lokalizacji szkolnych		1 500	12 700	18 878	19 512
% zgłoszeń obsługiwanych przez zmianę 7-15, pon-pt	90%				
Liczba zgłoszeń na lokalizację/miesiąc	2				
Liczba zgłoszeń - zmiana 7-15		2 700	22 860	33 980	35 122
Liczba zgłoszeń - zmiana 15-21		300	2 540	3 776	3 902

Szacowana ilość zgłoszeń i ilość pracowników (agentów, supervisorów) w Centrum Kontaktów OSE

średni czas obsługi zgł. w CallDesk (h)	0,15				
Czas obsługi zgłoszeń CallDesk przypadający na zmianę 7-15, pon-pt (h/miesiąc)		405	3 429	5 097	5 268
Czas obsługi zgłoszeń CallDesk przypadający na zmianę 7-15, pon-pt (h/miesiąc)		45	381	566	585
średnia liczba h pracy 1 zmiany pn-pt CallDesk w miesiącu	168				
Liczba personelu CallDesk na zmianie 7-15 , pn-pt		2	20	30	31
Liczba personelu CallDesk na zmianie 15-21, pn-pt		1	3	4	4
Liczba personelu CallDesk - suma dla zmian pn-pt		3	23	34	35

Dokumenty

ilość typów dokumentów per szkoła	<p>Dokumenty generowane w kontekście szkoły (docelowo tyle ile szkół, czyli 25 tys. per każdy dokument poniżej):</p> <ul style="list-style-type: none"> • ankieta techniczna • umowa • 7 załączników do umowy • koncepcja techniczna • protokół odbioru usług • protokół z-o instalacji i urządzeń (plus zmiany po serwisie/wymianie sprzętu – należy dodać 5-10%) • dokumentacja powykonawcza (może być aktualizowana po serwisie/wymianie sprzętu – należy dodać 5%) • dodatkowy kosztorys prac (można przyjąć dla 30-50% przypadków) • wyceny wizyt serwisowych (zakładamy, że 10-20% szkół jednorazowo skorzysta z takiego serwisu) • faktura przychodowa • faktura korekcyjna (po uznaniu reklamacji) • faktura kosztowa (zbiorcza do miesięcznej specyfikacji od podwykonawcy) • aneksy (zmiany w usługach – należy założyć, że aneksy pojawią się dla 5% szkół) <p>Należy przy wymiarowaniu założyć, że dokumenty będą wersjonowane - średnio do 3 wersji na dokument oraz konieczność masowego wydruku dokumentów</p>
ilość dokumentów per lokalizacja szkolna	<p>Dokumenty w kontekście lokalizacji szkolnej (docelowo tyle ile lokalizacji szkolnych, czyli 19,5 tys. per każdy dokument poniżej):</p> <ul style="list-style-type: none"> • zamówienie łącza • dodatkowe zamówienia na upgrade łącza (należy założyć dla 10% szkół) • zamówienie na prace do Podwykonawcy przy podłączeniu szkoły do OSE (może ich być więcej, gdy będą domawiane niestandardowe prace instalacyjne)

Dokumenty	
	<ul style="list-style-type: none"> • dokumentacja powykonawcza <p>Należy przy wymiarowaniu założyć, że dokumenty będą wersjonowane - średnio do 3 wersji na dokument oraz konieczność masowego wydruku dokumentów</p>
ilość typów dokumentów w standardowych procesach operatora telekomunikacyjnego	<ul style="list-style-type: none"> • protokoły odbiorów ilościowych (dostawa do magazynu) • protokoły odbiorów jakościowych (dostawa do magazynu) • listy S/N i MAC adres urządzeń od dostawców sprzętu (przed dostawą do magazynu) • listy S/N i MAC adres urządzeń beneficjentów POPC • protokoły przekazania-zwrotu urządzeń (z magazynu NASK do magazynu podwykonawcy i w drugą stronę) • karty gwarancyjne (per urządzenie) • faktury (per dostawa) • faktury za dzierżawę kolokacji (miesięcznie) • dokumenty związane z prowadzeniem projektu <p>Należy przy wymiarowaniu założyć, że dokumenty będą wersjonowane - średnio do 3 wersji na dokument oraz konieczność masowego wydruku dokumentów.</p> <p>Należy również przyjąć extra zasoby na dodatkową pulę dokumentów nieprzewidzianych w momencie powstawania niniejszego dokumentu - 10%</p>
ile typów dokumentów będzie generowana	ilość typów: kilkanaście (formaty, co najmniej DOC, PDF, XLS) : dokumenty umowne, zlecenia prac na instancję/serwis, zamówienia na łącza
ilość skanów per szkoła	<ul style="list-style-type: none"> • protokół odbioru usług • protokół z-o instalacji i urządzeń (plus zmiany po serwisie/wymianie sprzętu – należy dodać 5-10%) • kosztorys extra prac (dla 20% szkół)
ilość skanów per lokalizacja szkolna	<ul style="list-style-type: none"> • dokumentacja powykonawcza będzie zawierać zdjęcia
ilość skanów w standardowych procesach operatora telekomunikacyjnego	<p>Per podwykonawca:</p> <ul style="list-style-type: none"> • podpisana specyfikacja (co miesiąc) 1-2 per umowa ramowa z podwykonawcą • faktury za prace instalacyjne - tyle, co specyfikacji • raporty miesięczne zbierające wszystkie zamówienia szczegółowe - tyle co faktur • wyceny wizyt serwisowych przedstawiane przez podwykonawców (kilka miesięcznie)

Dokumenty

	<p>Per dostawa sprzętu (zakładane jest 120 dostaw):</p> <ul style="list-style-type: none">• zamówienie• protokół ilościowy• protokół jakościowy• karty gwarancyjne• faktura <p>Należy założyć, że część skanów trafi również do centralnego repozytorium skanów NASK (ARCHE)</p>
Raporty	<p>Obecnie opisanych jest około 80 typów raportów wynikających z procesów biznesowych - raporty opisane są w części dokumentu nt. wymagań procesów biznesowych oraz wymagań na systemy OSS.</p> <p>Zakładane jest, że docelowo typów raportów będzie około 200 (raporty operacyjne z działania sieci, raporty z procesów biznesowych, raporty bezpieczeństwa dla dyrektorów szkół, raporty projektowe - w tym rozliczenia projektu do Ministerstwa Cyfryzacji i rozliczenia dotacji unijnych)</p> <p>Zakładane jest kilkanaście formatów raportów (w tym standardowe formaty: XLS, DOC, PDF, XML, JSON, HTML, TXT, inne)</p>

Kontrahenci

Szkoły	docelowo około 25000 szkół , każda szkoła ma OPS (Organ Prowadzący Szkołę) , Jeden OPS może prowadzić kilka szkół
Dostawcy łącz	20-30 operatorów łącz (operatorzy są wybierani sukcesywnie w ramach kolejnych postępowań zakupowych na kolejne województwa w Polsce, zatem jest to liczba przybliżona)
Podwykonawcy	Maksymalnie 100 - podwykonawcy są wybierani w ramach kolejnych postępowań zakupowych na podwykonawstwo OSE w kolejnych województwach, zatem ich liczba nie jest obecnie znana; umowy z Podwykonawcami mogą ulegać zmianom (rozwiązywanie umowy/podpisywanie umów z nowymi Podwykonawcami), zatem zakładamy, że łączna liczba Podwykonawców nie będzie większa niż 100
Liczba magazynów	<p>Kilka magazynów fizycznych, magazyny wirtualne dla każdego partnera (maksymalnie 100, bo tyłu maksymalnie partnerów jest zakładanych).</p> <p>Magazyny wirtualne pozwalają na to by fizycznie sprzęt był magazynowany u Podwykonawcy, ale ewidencja sprzętu jest w jednym systemie magazynowym NASK - dzięki wirtualnym instancjom magazynowym Podwykonawca ma wgląd w przypisaną tylko jemu pulę sprzętu, za który odpowiada i może na bieżąco sprawdzać swoje stany magazynowe pod kątem zaplanowanych prac w szkołach, Jednocześnie NASK ma wgląd we wszystkie magazyny wirtualne i ich stany po całości dla wszystkich Podwykonawców.</p>

Kontakt z operatorem OSE	
ile rodzajów kontaktów (do szkoły/OPS/partnerów OSE)	szkoły: 4 role, szkoła, OPS = 6-8 partnerzy: zamówienia, awarie, faktury ,handlowy , techniczny itp. : ca. 6-8 Razem: do 20
formy kontaktu	telefon (w tym IVR), mail, chat
ile rozmów dziennie/tygodniowo/miesięcznie	1000 dziennie/5000 tygodniowo/20 000 miesięcznie - szacunkowo średni czas trwania rozmowy to 3,5 minuty
ile rozmów nagrywanych, jak długo trzymamy nagrania ("on-line", "w archiwum")	nagrania czasu dostępne "od ręki – do 3 miesięcy wstecz nagrania dostępne "na życzenie" – do roku wstecz
ile scenariuszy IVR	komunikat dzienny, nocny, po godzinach pracy, skrócone godziny pracy (przyjmijmy do 6 scenariuszy)
ile maili dziennie/tygodniowo/miesięcznie, ile akcji mailingowych w planach	100 dziennie/500 tyg/2000 miesięcznie, 3 akcje mailingowe tygodniowo

Integracje	
Ilość integracji w ramach sieci/systemów OSE	~ 67 (część powielana per węzeł OSE)
ilość integracji z systemami NASK PIB	6 - 7 systemów
Ilość typów	17-18 typów integracji
repozytoria dokumentów	wszystkie niezbędne w ramach Rozwiązania + system FK, magazyn, system kancelaryjny
źródła danych raportowych	Magazyn NASK, system FK, CRM NASK

7.2. Opis funkcjonalności dla obszarów biznesowych

Wykonawca jest zobowiązany do spełnienia poniższych wymagań w poszczególnych obszarach wsparcia procesów Operatora OSE

7.2.1. Proces zarządzania produktami OSE

Nr wymagania	Treść wymagania
O1.F1	Rozwiązanie musi udostępniać panel do zarządzania konfiguracji produktów, ofert, cenników (m.in. definicja parametrów)

Nr wymagania	Treść wymagania
O1.F2	Rozwiązanie musi być zawierać repozytorium zdefiniowanych produktów wraz z obowiązującym statusem życia produktu.
O1.F3	Rozwiązanie musi wspierać workflow do zarządzania procesami dot. produktu wraz z możliwością definiowania limitów czasowych, alertów o opóźnieniu, ryzyku opóźnienia.
O1.F4	Rozwiązanie musi wspierać przeprowadzanie badań satysfakcji Użytkownika (mail/ ankieta/ Pop Up itp.) przez definiowanie wywiadu, analizę i raportowanie ich wyników
O1.F5	Na docelowej platformie BSS należy wdrożyć proces "Opracowanie koncepcji produktu" na podstawie definicji opisanej w ramach rozdziału "Architektura biznesowa operatora OSE". Należy przeprowadzić analizę biznesową celem opracowania definicji procesu oraz określenia dla niego konfiguracji biznesowej uwzględniając najlepsze praktyki branżowe oraz specyfikę operatora OSE.
O1.F6	Na docelowej platformie BSS należy wdrożyć proces "Zatwierdzenie produktu" na podstawie definicji opisanej w ramach rozdziału "Architektura biznesowa operatora OSE". Należy przeprowadzić analizę biznesową celem opracowania definicji procesu oraz określenia dla niego konfiguracji biznesowej uwzględniając najlepsze praktyki branżowe oraz specyfikę operatora OSE.
O1.F7	Na docelowej platformie BSS należy wdrożyć proces "Przygotowanie wdrożenia" na podstawie definicji opisanej w ramach rozdziału "Architektura biznesowa operatora OSE". Należy przeprowadzić analizę biznesową celem opracowania definicji procesu oraz określenia dla niego konfiguracji biznesowej uwzględniając najlepsze praktyki branżowe oraz specyfikę operatora OSE.
O1.F8	Na docelowej platformie BSS należy wdrożyć proces "Wdrożenie produktu" na podstawie definicji opisanej w ramach rozdziału "Architektura biznesowa operatora OSE". Należy przeprowadzić analizę biznesową celem opracowania definicji procesu oraz określenia dla niego konfiguracji biznesowej uwzględniając najlepsze praktyki branżowe oraz specyfikę operatora OSE.
O1.F9	Na docelowej platformie BSS należy wdrożyć proces "Dokształcanie produktu" na podstawie definicji opisanej w ramach rozdziału "Architektura biznesowa operatora OSE". Należy przeprowadzić analizę biznesową celem opracowania definicji procesu oraz określenia dla niego konfiguracji biznesowej uwzględniając najlepsze praktyki branżowe oraz specyfikę operatora OSE.
O1.F10	Na docelowej platformie BSS należy wdrożyć proces "Monitorowanie produktu" na podstawie definicji opisanej w ramach rozdziału "Architektura biznesowa operatora OSE". Należy przeprowadzić analizę biznesową celem opracowania definicji procesu oraz określenia dla niego konfiguracji biznesowej uwzględniając najlepsze praktyki branżowe oraz specyfikę operatora OSE.
O1.F11	Na docelowej platformie BSS należy wdrożyć proces "Wycofanie produktu" na podstawie definicji opisanej w ramach rozdziału "Architektura biznesowa operatora OSE". Należy przeprowadzić analizę biznesową celem opracowania definicji procesu oraz określenia dla niego konfiguracji biznesowej uwzględniając najlepsze praktyki branżowe oraz specyfikę operatora OSE.
O1.F12	Na docelowej platformie BSS należy wdrożyć proces "Zamknięcie produktu" na podstawie definicji opisanej w ramach rozdziału "Architektura biznesowa operatora OSE". Należy przeprowadzić analizę biznesową celem opracowania definicji procesu oraz określenia dla niego konfiguracji biznesowej uwzględniając najlepsze praktyki branżowe oraz specyfikę operatora OSE.
O1.F13	Na docelowej platformie BSS należy wdrożyć proces "Przygotowanie oferty" na podstawie definicji opisanej w ramach rozdziału "Architektura biznesowa operatora OSE". Należy przeprowadzić analizę

Nr wymagania	Treść wymagania
	biznesową celem opracowania definicji procesu oraz określenia dla niego konfiguracji biznesowej uwzględniając najlepsze praktyki branżowe oraz specyfikę operatora OSE.
O1.F14	Na docelowej platformie BSS należy wdrożyć proces "Wdrażanie oferty" na podstawie definicji opisanej w ramach rozdziału "Architektura biznesowa operatora OSE". Należy przeprowadzić analizę biznesową celem opracowania definicji procesu oraz określenia dla niego konfiguracji biznesowej uwzględniając najlepsze praktyki branżowe oraz specyfikę operatora OSE.
O1.F15	Na docelowej platformie BSS należy wdrożyć proces "Publikacja Regulaminu/ Cennika" na podstawie definicji opisanej w ramach rozdziału "Architektura biznesowa operatora OSE". Należy przeprowadzić analizę biznesową celem opracowania definicji procesu oraz określenia dla niego konfiguracji biznesowej uwzględniając najlepsze praktyki branżowe oraz specyfikę operatora OSE.
O1.F16	Na docelowej platformie BSS należy wdrożyć proces "Wycofanie oferty" na podstawie definicji opisanej w ramach rozdziału "Architektura biznesowa operatora OSE". Należy przeprowadzić analizę biznesową celem opracowania definicji procesu oraz określenia dla niego konfiguracji biznesowej uwzględniając najlepsze praktyki branżowe oraz specyfikę operatora OSE.

Rozwiązanie musi zapewniać wystarczającą wydajność dla procesów zgodnie z poniższymi parametrami

L.p.	Nazwa procesu	Ilość dzienna / miesięczna uruchomień procesu	Uwagi
1	Opracowanie koncepcji produktu	5 / 50	
2	Zatwierdzenie produktu	10 / 100	
3	Przygotowanie wdrożenia	10 / 100	
4	Wdrożenie produktu	5 / 50	
5	Doskonalenie produktu	40 / 1500	
6	Monitorowanie produktu	40 / 1500	
7	Wycofanie produktu	10 /100	
8	Zamknięcie produktu	10 /100	
9	Przygotowanie oferty	40 / 1500	
10	Wdrażanie oferty	40 / 1500	
11	Publikacja Regulaminu/ Cennika	10 /100	
12	Wycofanie oferty	10 /100	

Wymagania w zakresie raportowania:

Lista raportów

L.p.	(Na potrzeby umieszczenia na stronie https://ose.gov.pl/regulations)
1	Cennik ofert przygotowanych do wdrożenia
2	Cennik do aktualnie obowiązujących ofert
3	Aktualnie obowiązujące regulaminy
4	Nowe wersje regulaminów
	Raporty produktu
5	Liczba użytkowników per produkt/ parametr produktu
6	Liczba użytkowników per oferta
7	Liczba użytkowników per cennik
8	Przekroczone SLA per typ usług
9	Przychody należne per produkt
10	Przychody zafakturowane per produkt
	Raporty cyklu życia produktu
11	Historia zmian statusu per produkt
12	Raport produktów per status

7.2.2. Proces obsługi klienta

Nr wymagania	Treść wymagania
O2.F1	Proces "Pozyskania szkoły" musi umożliwiać nadawanie automatyczne i ręczne numerów umów. Musi być możliwość nadawania podwójnej numeracji umowy - dedykowana numeracja OSE oraz ogólnofirmowa numeracja NASK
O2.F2	Proces musi wspierać nadawanie statusów zgłoszeniom jak i poszczególnym obiektom istotnym w kontekście sprawy. Statusy muszą być możliwe do zmiany automatycznie i ręcznie w procesie. Statusy muszą mieć możliwość wpływania na przebieg i status procesu (np. jego anulowanie) oraz na przebieg i statusy procesów powiązanych.
O2.F3	W ramach obiegu dokumentów w poszczególnych procesach musi być możliwe oznaczanie powrotu i daty powrotu wybranych dokumentu. Musi być również możliwość datowania określonych zdarzeń w procesie. Daty muszą mieć możliwość wpływania na przebieg procesu oraz zegary ustawione w procesie celem jego eskalacji.
O2.F4	Musi być możliwe dodanie do sprawy dodatkowej notatki do edycji w dowolnym momencie.
O2.F5	W ramach procesu pozyskania szkoły na Portalu OSE muszą zostać założone 4 konta na dla 4 ról : - dyrektor szkoły - TRS

Nr wymagania	Treść wymagania
	<ul style="list-style-type: none"> - koordynator OSE - koordynator OSE z OPS (wyłącznie dla pierwszej szkoły podlegającej pod danego OPS)
O2.F6	Proces musi zapewnić automatyczne generowanie dokumentów umownych i ich numerację według podanego przez Zamawiającego szablonu. Proces musi też wspierać możliwość wydruku tych dokumentów - sugerowana jest możliwość wydruków masowych z poziomu repozytorium dokumentów. Repozytorium to musi być dostępne z poziomu procesu.
O2.F7	W procesie pozyskania szkoły po kroku zgłoszeniu szkoły, musi być automatycznie wysyłana ankieta techniczna na adres e mail TRS a i Dyrektora (o ile są ustawione adresy email)
O2.F8	Rozwiązanie musi umożliwiać seryjną wysyłkę spersonalizowanych wiadomości e-mail do wielu odbiorców - na podstawie szablonu wiadomości część treści statyczna (identyczna dla wszystkich odbiorców) i część treści dynamiczna (podmieniana treścią charakterystyczną dla każdego z odbiorców, na podstawie jego danych - np adresowych czy osobowych). Seryjna wysyłka musi być realizowana, jako oddzielne email-e na każdy adres mailowy.
O2.F9	Rozwiązanie musi zawierać Centralne Repozytorium Dokumentów. Na CRD należy stworzyć odpowiednią strukturę do przechowywania danych. Na najwyższym poziomie struktury powinny być poszczególne OPS-y, na kolejnym poziomie szkoły przyporządkowane do OPS-ów, a pod szkołami konkretne sprawy lub zamówienia. Dokumenty powinny być zapisywane w najniższym poziomie struktury. Np. jeżeli dokument dotyczy OPS to struktura będzie zaczynała się od OPS, poniżej będzie numer sprawy dla danego OPS i dopiero w tym katalogu zostanie zapisany dokument.
O2.F10	Rozwiązanie musi zawierać narzędzie do badania satysfakcji Klienta (szablony ankiet, pytań, graficzna i liczbową prezentacja danych, segmentacja odpowiedzi). Narzędzie musi umożliwiać masową wysyłkę do szkół linków do ankiet, wypełnianie ich online, uniemożliwiając wypełnienie ankiety więcej niż raz przez każdą szkołę. Rozwiązanie musi umożliwiać raportowanie i analizę wyników ankiet.
O2.F11	<p>Rozwiązanie musi zawierać funkcjonalność do zarządzania bazą ewidencji szkół i lokalizacji. W ramach funkcjonalności musi być możliwe zarówno ładowanie danych z pliku jak i ręczna edycja danych. Funkcjonalności te muszą obejmować następujące encje:</p> <p>OPS</p> <p>Lokalizacja</p> <p>Szkoła</p> <p>Rozwiązanie musi być zintegrowane z Portalem OSE zapewniając synchronizację zmian danych w trybie online.</p>
O2.F12	Musi być zapewnione automatyczne wysłanie drugiej ankiety technicznej po zakończeniu czasu zegara ankiety; uruchomienie zegar dla drugiej ankiety; automatyczne wysłanie trzeciej ankiety technicznej po zakończeniu czasu zegara drugiej ankiety;
O2.F13	Należy zapewnić automatyczne zapisywanie do pliku txt lub xls lub innego danych ze spraw / zadań "zapisanie zgody dot. przetwarzania danych osobowych w zewnętrznej bazie" - dane osobowe osób z formularza zgłoszeniowego
O2.F14	Należy zapewnić konfiguracyjne możliwość przekierowania maili otrzymywanych w ramach procesu pozyskania szkoły na skrzynkę ckose@nask.pl lub inną jaka zostanie wskazana w konfiguracji
O2.F15	Należy zapewnić przekazywanie informacji o mailach wysłanych, które nie dotarły do adresata

Nr wymagania	Treść wymagania
O2.F16	Należy zapewnić możliwość przejścia "kroku wysłania umowy" bez wysłania umowy (pominięcia kroku)
O2.F17	Rozwiązanie musi umożliwiać wyszukiwanie szkół na podstawie parametrów takich jak region, lokalizacja(adres), OPS, partner serwisowy, operator dostępowy, status szkoły. W wyniku wyszukiwania rozwiązanie musi wyświetlać listę znalezionych szkół jednocześnie pokazując szkoły w różnych kolorach zależnie od statusu szkoły. W ramach otrzymanej listy musi być możliwe zaznaczanie/odznaczanie szkół zarówno pojedynczo jak wszystkich. Dla zaznaczonych szkół musi być możliwe masowe przeprowadzenie następujących akcji: masowa (seryjna) wysyłka maili wysyłka ankiet do badania satysfakcji
O2.F18	Należy zapewnić automatyzację powiązania zamówień szkolnych z zamówieniami dla lokalizacji. Tworzenie i powiązanie zamówień dla lokalizacji powinno być zależne od rodzaju produktów w zamówieniu i akcji na tych produktach (konieczność zamówienia dla lokalizacji powinna wynikać z konfiguracji produktów w katalogu produktów)
O2.F19	Rozwiązanie musi umożliwiać skonfigurowanie kolorów przypisanych do poszczególnych statusów szkół. Na podstawie konfiguracji szkoły powinny być oznaczane kolorem przy wyświetlaniu ich na listach (zarówno w wyniku wyszukiwania, jak i w widokach dla innych obiektów, z którymi powiązane są szkoły - takich jak lokalizacje czy OPS)
O2.F20	Na docelowej platformie BSS należy wdrożyć proces "Proces reklamacyjny" na podstawie przebiegu procesu w systemie JIRA osadzonym w docelowym środowisku. Po stronie dostawcy rozwiązania znajduje się odpowiedzialność za analizę przebiegu procesu (wraz z konfiguracją) oraz jego dostosowanie do architektury docelowych systemów. W ramach analizy biznesowej należy uwzględnić najlepsze praktyki branżowe oraz specyfikę operatora OSE.
O2.F21	Na docelowej platformie BSS należy wdrożyć proces "Proces zmiana umowy, usługi" na podstawie przebiegu procesu w systemie JIRA osadzonym w docelowym środowisku. Po stronie dostawcy rozwiązania znajduje się odpowiedzialność za analizę przebiegu procesu (wraz z konfiguracją) oraz jego dostosowanie do architektury docelowych systemów. W ramach analizy biznesowej należy uwzględnić najlepsze praktyki branżowe oraz specyfikę operatora OSE.
O2.F22	Na docelowej platformie BSS należy wdrożyć proces "Proces pozyskania szkoły" na podstawie przebiegu procesu w systemie JIRA osadzonym w docelowym środowisku. Po stronie dostawcy rozwiązania znajduje się odpowiedzialność za analizę przebiegu procesu (wraz z konfiguracją) oraz jego dostosowanie do architektury docelowych systemów. W ramach analizy biznesowej należy uwzględnić najlepsze praktyki branżowe oraz specyfikę operatora OSE.
O2.F23	Rozwiązanie musi umożliwiać rejestrowanie zgód udzielonych przez osoby kontaktowe (w różnych rolach) ze szkoły i z OPS zarówno poprzez przechowywanie skanu dokumentu jak i poprzez przechowywanie stanu poszczególnych zgód w bazie danych
O2.F24	Rozwiązanie musi zawierać katalog zgód (definicja zgody wraz określeniem poziomu, na jakim jest wyrażana: szkoła, OPS, osoba, produkt)

Rozwiązanie musi zapewniać wystarczającą wydajność dla procesów zgodnie z poniższymi parametrami

L.p.	Nazwa procesu	Ilość dzienna / miesięczna uruchomień procesu	Uwagi
1	Proces reklamacyjny	195/ 3900	90% w godz. 7:00-15:00
2	Proces zmiana umowy, usługi	800 / 10000	
3	Proces pozyskania szkoły	200 / 2000	

Wymagania w zakresie raportowania:

Lista raportów

1. Raport "Statusy" (zawiera wszystkie szkoły)
Numer harmonogramu
Numer RSPO
Status szkoły
Dane adresowe szkoły (nazwa szkoły, ulica, miasto)
Dane osób kontaktowych (dyrektor, TRS, itd) - imię, nazwisko, telefon
Dane kontaktowe OPS
Status – ostatni status sprawy
Czy jest ankieta?
Przekroczony zegar ankiety
Czy jest umowa?
Przekroczony zegar umowy
2. Raport „Dokumenty”
Numer RSPO
Dane adresowe szkoły (nazwa szkoły, ulica, miasto)
Dane osób kontaktowych (dyrektor, TRS, itd) - imię, nazwisko, telefon
Dane kontaktowe OPS
Status – ostatni status sprawy
Lista dokumentów (dokumenty wysyłane/ dokumenty podpisane u klienta, data odesłania)
Umowa o świadczenie publiczne dostępnych usług telekomunikacyjnych w Ogólnopolskiej Sieci Edukacyjnej
Zgoda Organu Prowadzącego
Wzór protokołu Zd. Odb.
Regulamin świadczenia publicznie dostępnych usług telekomunikacyjnych w Ogólnopolskiej Sieci Edukacyjnej

1. Raport "Statusy" (zawiera wszystkie szkoły)
Cennik usług w ramach Ogólnopolskiej Sieci Edukacyjnej
Zamówienie
Warunki świadczenia usługi OSE (SLA)
Oświadczenie
Aneks
Lista brakujących dokumentów + data
Komentarz z notatki
3. Raport formularz zgłoszeniowy dane osobowe
Dane osób kontaktowych (TRS, koordynator, itd.) - imię i nazwisko, telefon, mail
osoba podpisująca protokół (imię i nazwisko, telefon, mail)
data
godzina
4. Raport formularz kontaktowy dane osobowe
Imię, Nazwisko
adres e mail
telefon
data, godzina
treść zgody

7.2.3. Proces obsługi technicznej

Nr wymagania	Treść wymagania
O3.F1	Rozwiązanie musi wysyłać maile do szkół z aktualizacją statusów danego zgłoszenia na adres email osoby zgłaszającej. Musi być możliwe indywidualne skonfigurowanie dla każdej szkoły oddzielnie czy mają być wysyłane maile w przypadku dowolnej zmiany statusu zgłoszenia, czy tylko w przypadku zamknięcia zgłoszenia, czy też w ogóle nie mają być wysyłane notyfikacje o zmianie statusu. Domyślnie musi być ustawione wysyłanie maili dla wszystkich zmian statusu. Konfiguracja musi być dostępna do zmiany zarówno poprzez wystawienia API dla portalu OSE jak i bezpośrednio w systemach obsługi klienta w rozwiązaniu.
O3.F2	Należy zaimplementować funkcjonalność do weryfikacji liczby roboczogodzin partnerów serwisowych w ramach wizyt serwisowych na terenie danego województwa, uzależniona od szacowanej liczby lokalizacji do podłączenia w danych województwie zgodnie z wzorem: 30*LL*(X/1000)

Nr wymagania	Treść wymagania
	<p>gdzie:</p> <p>LL – szacowana liczba Lokalizacji do podłączenia na obszarze objętym Umową,</p> <p>X=0,2 w 2018 roku,</p> <p>X=0,6 w 2019 roku,</p> <p>X=1 w 2020 roku,</p> <p>X=1 w 2021 roku,</p> <p>X=1 w 2022 roku,</p> <p>przy czym liczba roboczogodzin, do których wykonania będzie zobowiązany Wykonawca bez dodatkowych opłat w ramach Ryczaftu za Serwis nie może być mniejsza dla wszystkich Lokalizacji (w ramach danego województwa) niż 8 roboczogodzin w Okresie rozliczeniowym.</p>
O3.F3	Rozwiązanie musi zawierać narzędzia do badania satysfakcji Klienta w procesie obsługi umożliwiając wysyłanie linków do ankiet online, przeprowadzanie ankiet poprzez system IVR oraz przeprowadzanie ankiet za pośrednictwem poczty elektronicznej.
O3.F4	Rozwiązanie musi zapewniać monitorowanie rozliczeń finansowych i prac ze szkołą (systemowe pilnowanie i sygnalizacja wykorzystania kwoty z umowy, przekroczenia ilości bezpłatnych wizyt serwisowych, terminów na weryfikację specyfikacji prac- alarmy, powiadomienia, eskalacje)
O3.F5	Rozwiązanie musi zawierać Centralne Repozytorium Dokumentów. Na CRD należy stworzyć odpowiednią strukturę do przechowywania danych. Na najwyższym poziomie struktury powinny być poszczególne OPS-y, na kolejnym poziomie szkoły przyporządkowane do OPS-ów, a pod szkołami konkretne sprawy lub zamówienia. Dokumenty powinny być zapisywane w najniższym poziomie struktury. Np. jeżeli dokument dotyczy OPS to struktura będzie zaczynała się od OPS, poniżej będzie numer sprawy dla danego OPS i dopiero w tym katalogu zostanie zapisany dokument.
O3.F6	Rozwiązanie musi udostępniać bezpieczne API do pobierania informacji przez dostawców o ich niezamkniętych zleceniach. Zapewniając możliwość weryfikacji dostawcy / partnera, udostępnianie wyłącznie informacji o zgłoszeniach niezamkniętych przypisanych do danego dostawcy / partnera.
O3.F7	Rozwiązanie musi zapewnić elastyczne narzędzie do raportowania umożliwiające dostosowanie i tworzenie raportów przez użytkowników biznesowych bez konieczności prac implementacyjnych
O3.F8	Rozwiązanie musi zapewnić możliwość zebrania maksymalnie dużej liczby informacji o awarii w szkole w ramach systemów kontaktu z klientem (np. chatbot, IVR etc.) aby wyeliminować konieczność dodatkowego kontaktu z klientem. Zebranie informacji musi być realizowane w ramach zgłaszania awarii / reklamacji przez klienta. Systemy muszą umożliwiać wykorzystywanie skryptów z zestawami pytań w strukturze drzewa, tak, aby na podstawie odpowiedzi automatycznie wybierać / podpowiadać kolejne pytania.
O3.F9	W rozwiązaniu w jednym miejscu muszą być zebrane i widoczne wszelkie informacje niezbędne do realizacji procesów utrzymaniowych m in. Szkoła z RSPO, adresem, lokalizacja szkoły (popc, niepopc), usługi w szkole, konfiguracja, vlany, urządzenia (NASK / beneficjentów POPC), osoby w konkretnych rolach po stronie szkoły wraz z mailem i tel (Dyrektor, TRS, koordynator OSE w szkole etc), operator łączy dostępowego, PWR, operator łączy agregacyjnego, styk z NASK.
O3.F10	Rozwiązanie musi umożliwiać wyszukanie i wyświetlenie na jednym ekranie wszystkich szkół w konkretnym PWR, z możliwością przejścia do ekranu dla wybranej szkoły
O3.F11	Na docelowej platformie BSS należy wdrożyć proces "Proces obsługi zgłoszenia w szkole" na podstawie przebiegu procesu w systemie JIRA osadzonym w docelowym środowisku. Po stronie

Nr wymagania	Treść wymagania
	dostawcy rozwiązania znajduje się odpowiedzialność za analizę przebiegu procesu (wraz z konfiguracją) oraz jego dostosowanie do architektury docelowych systemów. W ramach analizy biznesowej należy uwzględnić najlepsze praktyki branżowe oraz specyfikę operatora OSE.
O3.F12	Na docelowej platformie BSS należy wdrożyć proces "Proces obsługi zgłoszenia u podwykonawcy" na podstawie przebiegu procesu w systemie JIRA osadzonym w docelowym środowisku. Po stronie dostawcy rozwiązania znajduje się odpowiedzialność za analizę przebiegu procesu (wraz z konfiguracją) oraz jego dostosowanie do architektury docelowych systemów. W ramach analizy biznesowej należy uwzględnić najlepsze praktyki branżowe oraz specyfikę operatora OSE.
O3.F13	Rozwiązanie musi wykorzystywać w procesie zgłaszania problemów przez użytkowników informacje o pracach planowych i awariach masowych. W przypadku zgłoszenia w dowolnym kanale dotyczącego usługi dotkniętej awarią masową lub pracą planową należy poinformować użytkownika o przyczynie problemów z usługą i ewentualnym możliwym terminie zakończenia prac / usunięcia problemu. W kanałach automatycznych (np. IVR) użytkownik powinien otrzymać od razu informacje.

Rozwiązanie musi zapewniać wystarczającą wydajność dla procesów zgodnie z poniższymi parametrami

L.p.	Nazwa procesu	Ilość dzienna / miesięczna uruchomień procesu	Uwagi
1	Proces obsługi zgłoszenia w szkole	195/ 3900	90% w godz. 7:00-15:00
2	Proces obsługi zgłoszenia u podwykonawcy	400 / 5000	

Wymagania w zakresie raportowania:

Lista raportów

Raporty szkoły	
1.	<p>Ticketsy OSE zbiorczo (JIRA SD)</p> <p>Generowany ad-hoc z możliwością eksportu do xls/csv</p>
	<p>Warunki:</p> <p>bazujący na ticketach w systemie</p> <p>wybór zakresu dat (cykl dzienny, tygodniowy, miesięczny, kwartalny)</p> <p>zamknięte/otwarte/wszystkie zgłoszenia (awarie i wizyty serwisowe) w systemie</p> <p>SLA - zegar globalny zgłoszenia (przekroczone / nieprzekroczone / wszystkie)</p>
	<p>Dane w raporcie:</p> <p>dane szkoły (nazwa, adres, lokalizacja POPC/niePOPC, zgłaszający etc.)</p> <p>temat zgłoszenia</p> <p>kategoria</p> <p>źródło zgłoszenia (portal / CK)</p>

Raporty szkoły

nazwa kodu zamknięcia (ważne w kontekście np. awarii zgłoszonych podczas prac planowych, braku awarii etc)
 lokalizacja OSE, POPC, MAN
 usługa darmowa / płatna
 grupa wsparcia (dla zamkniętych kto rozwiązał, dla otwartych, na jakiej aktualnie jest zgłoszenie)
 SLA (wszystkie zegary)
 priorytet zgłoszenia

2 Tickety OSE per zgłaszający/szkoła (JIRA SD)
 Generowany ad-hoc z możliwością eksportu do xls/csv.

Warunki:
 -bazujące na ticketach w systemie
 -wybór zakresu dat (cykl dzienny, tygodniowy, miesięczny, kwartalny)
 -zamknięte/otwarte/wszystkie zgłoszenia w systemie
 -SLA - zegar globalny zgłoszenia (przekroczone / nieprzekroczone / wszystkie)
 - wybór po szkole (nazwa, rspo)

Dane w raporcie:
 -dane szkoły (nazwa, adres, lokalizacja POPC/niePOPC, zgłaszający etc.)
 -temat zgłoszenia
 -kategoria
 -źródło zgłoszenia (portal / CK)
 -nazwa kodu zamknięcia (ważne w kontekście np. awarii zgłoszonych podczas prac planowych, braku awarii etc)
 -lokalizacja POPC, niePOPC
 -usługa darmowa / płatna (>100mb)
 -grupa wsparcia (dla zamkniętych kto rozwiązał, dla otwartych, na jakiej aktualnie wisi zgłoszenie)
 -SLA (wszystkie zegary)
 - priorytet

3 Szkoły z przekroczonym SLA (JIRA SD)
 Generowany automatycznie 1 dnia miesiąca za poprzedni miesiąc w formie xls/csv

Warunki:
 -szkoły z usługą płatną (podstawa do naliczenia kary umownej)
 -pozostałe szkoły w celach statystycznych
 -szkoły z uwzględnioną przez NASK reklamacją
 -nie zawierające zgłoszeń zarejestrowanych jako 'prace planowe', 'brak awarii', 'wizyta serwisowa' etc (zamykane z oddzielnym kodem awarii)
 -cykl miesięczny (pełny miesiąc rozliczeniowy)
 -opłata za usługę w terminie/w opóźnieniu (dla szkół nie płacących w terminie za usługi OSE nie płaci kar umownych)
 -Dostępność Usługi = $(COR - CA) / COR * 100\%$ gdzie:
 COR – łączny czas w Okresie Rozliczeniowym;
 CA – łączny czas wszystkich potwierdzonych przez NASK Awarii w Godzinach Roboczych w Okresie Rozliczeniowym;
 - 96% < DU
 WAŻNE – panowanie nad kalendarzem w systemie (dni robocze, święta etc)

Raporty szkoły

	<p>Dane w raporcie:</p> <ul style="list-style-type: none"> -dane szkoły (nazwa, adres, typ lokalizacji OSE / POPC / MAN) -liczba zgłoszeń awarii -łączny czas usuwania awarii -SLA miesięczne dla szkoły -kwota do zapłaty przez OSE na rzecz Szkoły za poprzedni miesiąc
4	<p>Parametry jakościowe dla lokalizacji</p> <p>Generowany ad-hoc z możliwością eksportu do xls/csv.</p>
	<p>Warunki:</p> <p>bazujące na statystykach sieci</p> <p>dla konkretnej lokalizacji</p> <p>Dodatkowe informacje techniczne</p>
	<p>Dane w raporcie:</p> <ul style="list-style-type: none"> • dane jak w statystykach SPIDS dla szkół z pilotażu (przykład) <p>- informacja o przekroczeniu</p>
5	<p>Bezpieczeństwo – najpopularniejsze treści</p> <p>Raport dedykowany dla Dyrektorów Szkół publikowany na portalu OSE</p> <p>(na podstawie założeń z obszaru bezpieczeństwa – zakres może ulec zmianie)</p> <p>Generowany automatycznie 1 dnia miesiąca za poprzedni miesiąc na szablonie dokumentów OSE.</p>
	<p>Warunki:</p> <p>3 wykresy z wyszczególnieniem:</p> <ol style="list-style-type: none"> 1. TOP 10 – kategorii dozwolonych, przepuszczonych, zgodnie z polityką filtrowania 2. TOP 10 – kategorii niedozwolonych, zablokowanych, zgodnie z polityką filtrowania 3. TOP 10 – najpopularniejszych stron www
	<p>Dane dostępne na każdym z wykresów to nazwa kategorii i liczba wejść na strony w danej kategorii w ostatnim miesiącu.</p>
6	<p>Zgłoszenia OSE (portal OSE)</p> <p>Raport dedykowany dla Szkół publikowany na portalu OSE.</p> <p>Widoczny w portalu po zalogowaniu do modułu serwisowego dla wszystkich użytkowników powiązanych z daną szkołą (Dyrektor, TRS, koordynator OSE w szkole etc)</p>
	<p>Warunki:</p> <ul style="list-style-type: none"> - wszystkie zgłoszenia stworzone przez szkołę lub CK w imieniu szkoły - dane zbiorczo z możliwością podziału na miesiące - zamknięte / w toku
	<p>Dane w raporcie:</p> <ul style="list-style-type: none"> - numer zgłoszenia - status (portalowy) - temat zgłoszenia - opis zgłoszenia - data zgłoszenia

Raporty szkoły

	<ul style="list-style-type: none">- data rozwiązania (jeśli zamknięte)- opis rozwiązania (jeśli zamknięte)
RAPORTY GRUPY WSPARCIA	
7	<p>Tickety zamknięte dla grupy wsparcia (JIRA SD)</p> <p>Generowany ad-hoc z możliwością eksportu do xls/csv.</p>
	<p>Warunki:</p> <ul style="list-style-type: none">- wybór po grupie wsparcia- wybór zakresu dat (cykl dzienny, tygodniowy, miesięczny)- zamknięte zgłoszenia w systemie- wszystkie kategorie lub zdefiniowana kategoria
	<p>Dane w raporcie:</p> <ul style="list-style-type: none">- kategoria- temat- opis zgłoszenia- opis zamknięcia- daty- SLA - zegar globalny zgłoszenia (przekroczone, nieprzekroczone)- czas reakcji (globalny)- awaria / brak awarii- osoba zamykająca zgłoszenie
8	<p>Tickety zamknięte dla grupy wsparcia - suma (JIRA SD)</p> <p>Generowany ad-hoc z możliwością eksportu do xls/csv.</p>
	<p>Warunki:</p> <ul style="list-style-type: none">- wybór po grupie wsparcia- wybór zakresu dat (cykl dzienny, tygodniowy, miesięczny)- zamknięte zgłoszenia w systemie- wszystkie kategorie lub zdefiniowana kategoria
	<p>Dane w raporcie:</p> <ul style="list-style-type: none">- liczba zgłoszeń (awarie / brak awarii)- liczba zgłoszeń (przeterminowane / nieprzeterminowane)
9	<p>Tickety otwarte dla grupy wsparcia (JIRA SD)</p> <p>Generowany ad-hoc z możliwością eksportu do xls/csv.</p>
	<p>Warunki:</p> <ul style="list-style-type: none">- wybór po grupie wsparcia- wybór zakresu dat (cykl dzienny, tygodniowy, miesięczny)- zamknięte zgłoszenia w systemie- wszystkie kategorie lub zdefiniowana kategoria
	<p>Dane w raporcie:</p> <ul style="list-style-type: none">- kategoria- temat- opis zgłoszenia

Raporty szkoły

	<ul style="list-style-type: none"> - daty - SLA - zegar globalny zgłoszenia (przekroczone, nieprzekroczone) - SLA – czas pozostały (gdy nieprzekroczone) - czas reakcji (globalny) - awaria / brak awarii - osoba obsługująca zgłoszenie
RAPORTY PODWYKONAWCY	
10	<p>Tickety zamknięte dla podwykonawców (JIRA SD)</p> <p>Generowany ad-hoc z możliwością eksportu do xls/csv.</p> <p>Podwykonawcy potencjalnie różni w zakresie województwa (specyficzna grupa wsparcia)</p>
	<p>Warunki:</p> <ul style="list-style-type: none"> - wybór po podwykonawcy - wybór w ramach 1 lub wielu województw - wybór zakresu dat (cykl dzienny, tygodniowy, miesięczny) - zamknięte zgłoszenia w systemie - wszystkie kategorie lub zdefiniowana kategoria
	<p>Dane w raporcie:</p> <ul style="list-style-type: none"> - województwo - szkoła (dane adresowe etc) - kategoria - temat - opis zgłoszenia - daty - SLA - zegar globalny zgłoszenia (przekroczone, nieprzekroczone) - czas reakcji (podwykonawcy) - awaria / brak awarii (kod zamknięcia zgłoszenia)
11	<p>Tickety otwarte dla podwykonawców (JIRA SD)</p> <p>Generowany ad-hoc z możliwością eksportu do xls/csv.</p> <p>Podwykonawcy potencjalnie różni w zakresie województwa (specyficzna grupa wsparcia)</p>
	<p>Warunki:</p> <ul style="list-style-type: none"> - wybór po podwykonawcy - wybór w ramach 1 lub wielu województw - wybór zakresu dat (cykl dzienny, tygodniowy, miesięczny) - zamknięte zgłoszenia w systemie - wszystkie kategorie lub zdefiniowana kategoria
	<p>Dane w raporcie:</p> <ul style="list-style-type: none"> - województwo - szkoła (dane adresowe etc) - kategoria - temat - opis zgłoszenia - daty - SLA - zegar globalny zgłoszenia (przekroczone, nieprzekroczone)

Raporty szkoły

	<ul style="list-style-type: none"> - czas reakcji (podwykonawcy) - awaria / wizyta serwisowa
12	<p>Liczba wizyt serwisowych dla województwa (JIRA SD)</p> <p>Generowany ad-hoc z możliwością eksportu do xls/csv.</p> <p>Podwykonawcy potencjalnie różni w zakresie województwa (specyficzna grupa wsparcia)</p>
	<p>Warunki:</p> <ul style="list-style-type: none"> - wybór po podwykonawcy - wybór w ramach konkretnego województwa - miesięczny, wybór konkretnego miesiąca - zamknięte zgłoszenia w systemie - kategoria 'wizyta serwisowa'
	<p>Dane w raporcie:</p> <ul style="list-style-type: none"> -liczba godzin zrealizowanych w ramach w wizyt serwisowych w danym województwie w danym miesiącu
13	<p>Kary umowne dla podwykonawcy (JIRA SD)</p> <p>Generowany ad-hoc z możliwością eksportu do xls/csv.</p> <p>Podwykonawcy potencjalnie różni w zakresie województwa (specyficzna grupa wsparcia)</p>
	<p>Warunki:</p> <ul style="list-style-type: none"> - wybór po podwykonawcy - wybór w ramach konkretnego województwa - miesięczny, wybór konkretnego miesiąca - zamknięte zgłoszenia w systemie - zlecenia usunięcia awarii z przekroczonym czasem SLA - zlecenia wizyt serwisowych z przekroczonym czasem SLA
	<p>Dane w raporcie:</p> <ul style="list-style-type: none"> - nr zgłoszenia - dane szkoły - SLA dla zgłoszenia (awarie 8h roboczych, wizyty serwisowe 16h roboczych – od momentu zgłoszenia – zegar SLA Podwykonawcy) - SLA przekroczone per zgłoszenie (w godzinach) - przekroczone SLA (awarie) <ul style="list-style-type: none"> • SLA przekroczone > 25% • SLA przekroczone < 25% - przekroczone SLA (wizyty serwisowe) <ul style="list-style-type: none"> • SLA przekroczone > 18h • SLA przekroczone < 18h
RAPORTY OPERATORZY TD1 (SZKOŁA – PWR)	
14	<p>Zgłoszenia awarii łącz do operatorów (JIRA SD)</p> <p>Generowany ad-hoc z możliwością eksportu do xls/csv.</p> <p>Operatorzy odpowiedzialni za transmisję lokalizacja Szkoły – PWR.</p> <p>Komunikacja mailowa i telefoniczna przez NOC – wszelkie informacje wprowadzane do JIRA SD.</p> <p>Dla części lokalizacji Operator TD1 odpowiada w całości za łącze ze szkoły do punktu styku z NASK (z pominięciem przesiadki w PWR)</p> <p>W przypadku lokalizacji POPC – sprzęt (CPE, AP, Szafka) to własność operatorów.</p>

Raporty szkoły

	<p>Warunki:</p> <ul style="list-style-type: none"> - wybór operatora TD1 - wybór zakresu dat (cykl miesięczny) - zamknięte/otwarte zlecenia w systemie - wszystkie kategorie lub zdefiniowana kategoria
	<p>Dane w raporcie:</p> <ul style="list-style-type: none"> - nr zgłoszenia - szkoła (dane adresowe etc) - PWR - kategoria - temat - opis zgłoszenia - daty (zlecenia, zamknięcia etc) - SLA - zegar Operatora TD1 awaria 24h w dni robocze (przekroczone, nieprzekroczone) - czas reakcji (zegar Operatora TD1)
15	<p>Zgłoszenia awarii masowych łącz do operatorów (JIRA SD)</p> <p>Generowany ad-hoc z możliwością eksportu do xls/csv.</p> <p>Operatorzy odpowiedzialni za transmisję lokalizacja Szkoły – PWR.</p> <p>Awaria masowa – awaria minimum 1 węzła.</p> <p>Komunikacja mailowa i telefoniczna przez NOC – wszelkie informacje wprowadzane do JIRA SD.</p> <p>Dla części lokalizacji Operator TD1 odpowiada w całości za łącze ze szkoły do punktu styku z NASK (z pominięciem przesiadki w PWR)</p> <p>W przypadku lokalizacji POPC – sprzęt (CPE, AP, Szafka) to własność operatorów.</p>
	<p>Warunki:</p> <ul style="list-style-type: none"> - wybór operatora TD1 - wybór zakresu dat (cykl miesięczny) - zamknięte/otwarte zlecenia w systemie - wszystkie kategorie lub zdefiniowana kategoria
	<p>Dane w raporcie:</p> <ul style="list-style-type: none"> - nr zgłoszenia - szkoła (dane adresowe etc) - PWR - kategoria - temat - opis zgłoszenia - daty (zlecenia, zamknięcia etc) - SLA - zegar Operatora TD1 awaria masowa 24h w dni kalendarzowe (przekroczone, nieprzekroczone) - czas reakcji (zegar Operatora TD1)
16	<p>Dostępność usługi</p> <p>Generowany ad-hoc z możliwością eksportu do xls/csv.</p> <p>Gwarantowana dostępność 99,5% w ujęciu rocznym</p>
	<p>Warunki:</p> <ul style="list-style-type: none"> - wybór operatora TD1 - wybór zakresu dat (cykl miesięczny, kwartalny, roczny)

Raporty szkoły

	Dane w raporcie: <ul style="list-style-type: none">- dostępność usługi (%)
17	Wymienione urządzenia przez Operatora (POPC) Generowany ad-hoc z możliwością eksportu do xls/csv. Operatorzy odpowiedzialni za transmisję lokalizacja Szkoły – PWR. Komunikacja mailowa i telefoniczna przez NOC – wszelkie informacje wprowadzane do JIRA SD. W przypadku lokalizacji POPC – sprzęt (CPE, AP, Szafka) to własność operatorów.
	Warunki: <ul style="list-style-type: none">- wybór operatora TD1- wybór zakresu dat (cykl miesięczny, kwartalny, roczny)
	Dane w raporcie: <ul style="list-style-type: none">- nr zgłoszenia- szkoła (dane adresowe etc)- urządzenie (CPE/AP)- kategoria- temat- opis zgłoszenia- daty (zlecenia, zamknięcia etc)- SLA - zegar Operatora TD1- czas reakcji (zegar Operatora TD1)
RAPORTY OPERATORZY TD2 (PWR – LIM)	
18	Zgłoszenia awarii łącz do operatorów (JIRA SD) Generowany ad-hoc z możliwością eksportu do xls/csv. Operatorzy odpowiedzialni za transmisję lokalizacja PWR – NASK (od ODF operatora TD1 w ramach PWR) Komunikacja mailowa i telefoniczna przez NOC – wszelkie informacje wprowadzane do JIRA SD.
	Warunki: <ul style="list-style-type: none">- wybór operatora TD2- wybór zakresu dat (cykl miesięczny)- zamknięte/otwarte zlecenia w systemie- wszystkie kategorie lub zdefiniowana kategoria
	Dane w raporcie: <ul style="list-style-type: none">- nr zgłoszenia- PWR- temat- opis zgłoszenia- daty (zlecenia, zamknięcia etc)- SLA - zegar Operatora TD2 awaria masowa 6h (przekroczone, nieprzekroczone)- czas reakcji (zegar Operatora TD2)
19	Dostępność usługi Generowany ad-hoc z możliwością eksportu do xls/csv. Gwarantowana dostępność 99,1% w ujęciu rocznym

Raporty szkoły

	Warunki: <ul style="list-style-type: none">- wybór operatora TD2- wybór zakresu dat (cykl miesięczny)
	Dane w raporcie: <ul style="list-style-type: none">- wynik

7.2.4. Proces realizacji usług

Nr wymagania	Treść wymagania
O4.F1	<p>W ramach procesu podłączenia jednej lub wielu szkół w lokalizacji. Lokalizacja = miejsce z jednym adresem, w którym mieści się szkoła lub szkoły. Rozwiązanie powinno umożliwiać przechodzenie z ekranu szkoły do ekranu lokalizacji i odwrotnie. Na ekranie (szkoły / lokalizacji) musi być widać ile szkół jest w lokalizacji. Rozwiązanie musi umożliwiać grupowanie zadań:</p> <ul style="list-style-type: none">- akceptacji koncepcji podłączenia szkoły -> możliwość wystania jednej koncepcji dla wielu szkół w lokalizacji;- zamówienie łączy do lokalizacji -> jedno zlecenie obejmujące wszystkie szkoły w lokalizacji. <p>Identyfikacja szkoły po RSPO i numerze umowy.</p>
O4.F2	<p>Rozwiązanie musi zapewniać generowanie zleceń na podstawie szablonów, zlecenie prac, odbiory prac, pilnowanie czasów, alarmy przed zbliżającymi się czasami i po upływie terminu wykonania; procedura eskalacji (Podłączenie szkoły, Konfiguracja usług w szkole, Wykonanie prac w szkole). Rozwiązanie musi umożliwić generowanie zamówień pobierając dane o:</p> <ul style="list-style-type: none">- podwykonawcy (nazwa i dane adresowe);- numerze umowy ramowej;- pozycjach cennikowych;- cenach;- adresie lokalizacji;- szkołach w lokalizacji (RSPO, nazwy);- osobach kontaktowych w szkołach (Techniczni Reprezentanci Szkół - TRS). <p>Rozwiązanie musi nadawać numerację dla zamówień wg ustalonego klucza - na podstawie konfiguracji (np. numer umowy ramowej_rodzaj prac_kolejny numer zamówienia).</p> <p>Rozwiązanie musi umożliwiać generowanie raportów cyklicznych ze złożonych zamówień ze wszystkimi polami z zamówienia, np. data, podwykonawca, numer umowy ramowej, lokalizacja, szkoły, zakres prac, kwota, itp.</p>
O4.F3	<p>W procesie rozliczenia z podwykonawcami musi być widoczna informacja (na zasadzie listy) o stanie skompletowania dokumentacji od podwykonawcy umożliwiając weryfikację postępów i kompletności pracy.</p>
O4.F4	<p>Potwierdzenia z realizacji poszczególnych zamówień (potwierdzenia należytego wykonania zamówień) muszą być zebrane w jednym miejscu i stanowić rozpoczęcie procesu rozliczenia z podwykonawcami.</p>

Nr wymagania	Treść wymagania
O4.F5	Należy zapewnić monitorowanie kompletności dokumentacji lub stanu realizacji zadań względem zapisów z umowy (rozwiązanie musi na tej podstawie generować alarmy, eskalacje, mierzyć KPI, „SLA” na poszczególnych czynnościach/procesach)
O4.F6	Należy zapewnić monitorowanie procesu fakturowania (systemowe pilnowanie i sygnalizacja wykorzystania kwoty z umowy, przekroczenia ilości bezpłatnych wizyt serwisowych, terminów na weryfikację specyfikacji prac- alarmy, powiadomienia, eskalacje)
O4.F7	Musi być dostępny podgląd oraz pobieranie informacji nt. otrzymanych faktur, statusu realizacji płatności, wysyłki duplikatów. Możliwość opisu faktur oraz ich przekazania dalej na ścieżce akceptacyjnej w formie elektronicznej.
O4.F8	Musi być zapewniona możliwość zmian w systemie osób zaangażowanych w proces np. gdy zmiana umowy nie wymaga aneksowania Umowy („przyjazne” profilowanie uprawnień do modyfikacji tych informacji– nie tylko modyfikacje realizowane via admin)
O4.F9	Rozwiązanie musi zapewniać możliwość ustawiania zastępstw dla wszystkich lub pojedynczych spraw
O4.F10	Muszą być widoczne informacje nt. realizowanych dostaw sprzętu (nr zamówienia, dane nadawcy, dane odbiorcy, miejsce i daty dostarczenia, zamówienie podgląd zamówień, przedmiot i status zamówienia)
O4.F11	Rozwiązanie musi zawierać możliwość zbierania zamówień od podwykonawców na sprzęt (np. formatki pobierające podstawowe informacje z systemu/umowy- np.: nr umowy, rodzaj zamawianego sprzętu, itd
O4.F12	Rozwiązanie musi udostępniać szybki podgląd dokumentacji: zawarta umowa, dane kontaktowe czy np.: aktualny cennik podwykonawcy, ale również dokumentacji powykonawczej, faktur- wymagany profilowany dostęp
O4.F13	Rozwiązanie musi umożliwiać wprowadzanie informacji o zasobach technicznych wykorzystywanych do podłączenia szkoły oraz możliwość sprawdzenia zasobów z poziomu szkoły lub lokalizacji.
O4.F14	Rozwiązanie musi zapewniać : wymianę dokumentacji (zamówienia, protokoły odbiorcze) możliwość realizacji w formie elektronicznej, archiwizację dokumentów (Umowy oraz załączniki) z możliwością przekazywania ich do zdefiniowanych obszarów np. do Kancelarii, ZEIRK, magazynu czy innych podmiotów NASK/Podwykonawców/Dostawców, akceptację otrzymanych faktur- opisanie oraz przekazanie do zapłaty.
O4.F15	Rozwiązanie musi zapewniać w ramach Provisioningu urządzeń - minimalizację ręcznej konfiguracji urządzeń
O4.F16	Rozwiązanie musi zawierać narzędzie do zarządzania adresacją IP
O4.F17	Rozwiązanie musi zawierać pulpit zarządczy - wyświetlanie danych z różnych systemów i procesów w jednym miejscu
O4.F18	Rozwiązanie musi zawierać narzędzie do szybkiej komunikacji wewnętrznej

Nr wymagania	Treść wymagania
O4.F19	Rozwiązanie musi uwzględniać mechanizm nadawania nazw urządzeniom wg ustalonego algorytmu, jaki zostanie przekazany po podpisaniu umowy.
O4.F20	Rozwiązanie musi umożliwiać rozliczenia z podwykonawcami na podstawie ustalonego klucza (np. BAid, numer umowy ze szkołą, poz. budżetowa) i danych w systemach generowanie opisów do faktur.
O4.F21	Rozwiązanie musi zawierać repozytorium dokumentów podzielone na typy, np. protokoły z-o instalacji i przekazania sprzętu, protokoły z-o usługi, koncepcje podłączenia szkoły, dokumentacje powykonawcze, itp. Repozytorium dokumentów musi zostać zrealizowane w ramach Tree Confluence (NASK)
O4.F22	Rozwiązanie musi na podstawie dokumentu "Zasady doboru pasma łączy od węzła OSE do szkół" zawierać kalkulatora do wyliczania pasma koniecznego do zamówienia u dostawcy łączy. Z kalkulatora powinno korzystać też DWO na etapie zamawiania łączy. Dane potrzebne do wyliczeń powinny być pobierane z formularza wypełnianego przez szkołę (docelowo może z ankiety technicznej). Dokument zostanie przekazany po podpisaniu umowy.
O4.F23	Narzędzie musi cechować wysoka ergonomiczność
O4.F24	Należy zapewnić skuteczny sposób informowania o opóźnieniach (inny niż powiadomienia mailowe lub wyskakujące okienka)
O4.F25	Na docelowej platformie BSS należy wdrożyć proces "Podłączenie szkoły" na podstawie przebiegu procesu w systemie JIRA osadzonym w docelowym środowisku. Po stronie dostawcy rozwiązania znajduje się odpowiedzialność za analizę przebiegu procesu (wraz z konfiguracją) oraz jego dostosowanie do architektury docelowych systemów. W ramach analizy biznesowej należy uwzględnić najlepsze praktyki branżowe oraz specyfikę operatora OSE.
O4.F26	Na docelowej platformie BSS należy wdrożyć proces "Konfiguracja usług w szkole" na podstawie przebiegu procesu w systemie JIRA osadzonym w docelowym środowisku. Po stronie dostawcy rozwiązania znajduje się odpowiedzialność za analizę przebiegu procesu (wraz z konfiguracją) oraz jego dostosowanie do architektury docelowych systemów. W ramach analizy biznesowej należy uwzględnić najlepsze praktyki branżowe oraz specyfikę operatora OSE.
O4.F27	Na docelowej platformie BSS należy wdrożyć proces "Wykonanie prac w szkole" na podstawie przebiegu procesu w systemie JIRA osadzonym w docelowym środowisku. Po stronie dostawcy rozwiązania znajduje się odpowiedzialność za analizę przebiegu procesu (wraz z konfiguracją) oraz jego dostosowanie do architektury docelowych systemów. W ramach analizy biznesowej należy uwzględnić najlepsze praktyki branżowe oraz specyfikę operatora OSE.
O4.F28	Na docelowej platformie BSS należy wdrożyć proces "Rozliczenia z podwykonawcami" na podstawie przebiegu procesu w systemie JIRA osadzonym w docelowym środowisku. Po stronie dostawcy rozwiązania znajduje się odpowiedzialność za analizę przebiegu procesu oraz jego dostosowanie do architektury docelowych systemów.
O4.F29	Na docelowej platformie BSS należy wdrożyć proces "Gospodarka magazynowa" na podstawie przebiegu procesu w systemie JIRA osadzonym w docelowym środowisku. Po stronie dostawcy rozwiązania znajduje się odpowiedzialność za analizę przebiegu procesu (wraz z konfiguracją) oraz jego dostosowanie do architektury docelowych systemów. W ramach analizy biznesowej należy uwzględnić najlepsze praktyki branżowe oraz specyfikę operatora OSE.

Nr wymagania	Treść wymagania
O4.F30	Rozwiązanie musi zawierać w ramach funkcjonalności "Kalendarz Montera" funkcjonalność "Kalendarz zaplanowanych instalacji" – narzędzie, z którego wynikać będą zaplanowane instalacje na dany dzień, tydzień, miesiąc, z możliwością wyraportowania lokalizacji i szkół (RSPO). Narzędzie musi umożliwiać wyświetlanie wyników z możliwością filtrowania według regionów, partnerów serwisowych, operatorów dostępowych, rodzajów lokalizacji.
O4.F31	Rozwiązanie musi zapewniać ergonomiczną i prostą funkcjonalność dołączania załączników do zleceń / zgłoszeń w ramach spraw lub powiązanych ze sprawami. Mechanizm musi umożliwiać dodawanie załączników w ramach jednego kroku bez konieczności wykonywania kroków pośrednich takich jak np. zapis na dysku.
O4.F32	Rozwiązanie musi umożliwiać wyświetlanie dashletów/raportów dla zadanych RSPO zgodnie z informacjami w wymaganiach raportowych
O4.F33	Pracownicy partnerów powinni mieć możliwość zarządzania sprzętem przypisanym do magazynów ich partnerów (wirtualnych). Widoczność magazynów i sprzętu w magazynach powinna być ograniczona dla pracowników partnerów wyłącznie do sprzętu/magazynu przypisanego do tego partnera.
O4.F34	Rozwiązanie musi zawierać funkcjonalność łańcucha dostaw umożliwiając śledzenie przebiegu procesu dostarczania sprzętu od momentu jego zakupu aż do dostarczenia do magazynu partnera, a następnie możliwość weryfikacji działań realizowanych na sprzęcie przez partnera takich jak wykorzystanie, wymiana, uszkodzenia, zwroty.

Rozwiązanie musi zapewniać wystarczającą wydajność dla procesów zgodnie z poniższymi parametrami

L.p.	Nazwa procesu	Ilość dzienna / miesięczna uruchomień procesu	Uwagi
1	Podłączenie szkoły	200 / 2000	
2	Konfiguracja usług w szkielecie	800 / 10000	
3	Wykonanie prac w szkole	400 / 5000	
4	Rozliczenia z podwykonawcami	400 / 5000	
5	Gospodarka magazynowa	200 / 2000	

Wymagania w zakresie raportowania:

Lista raportów

1.	<p>ilość szkół i lokalizacji zleconych do podłączenia i podłączonych (w podziale na szkoły i lokalizacje, poszczególne harmonogramy);</p> <p>wraz z raportem lista szkół podłączonych (RSPO, nazwa, dane adresowe wraz z gminą i powiatem); lokalizacji podłączonych;</p> <p>częstotliwość - na żądanie</p>																		
	<p>W raporcie powinna znaleźć się lista planowanych szkół (RSPO, nazwa, dane adresowe wraz z gminą i powiatem) i lokalizacji do podłączenia ze wskazaniem w którym tygodniu planowane jest podłączenie (np.. T32 2018).</p>																		
	<table><tr><td></td><td>Zadanie</td><td>Opis</td></tr><tr><td>1.</td><td>Szkoły do podłączenia</td><td>Ilość szkół zleconych do DRP</td></tr><tr><td>2.</td><td>Zlecone do zestawienia łączy</td><td>Ilość spraw zleconych do DWO i w trakcie realizacji przez DWO</td></tr><tr><td>3.</td><td>Przygotowanie podłączenia</td><td>Od ilości zleconych szkół do DRP odjęcie poz. 2 i 4</td></tr><tr><td>4.</td><td>Zlecone podłączenia (do podwykonawców)</td><td>Ilość spraw zleconych do podwykonawców i w trakcie realizacji przez</td></tr><tr><td>5.</td><td>Szkoły podłączone</td><td>Ilość szkół podłączonych</td></tr></table>		Zadanie	Opis	1.	Szkoły do podłączenia	Ilość szkół zleconych do DRP	2.	Zlecone do zestawienia łączy	Ilość spraw zleconych do DWO i w trakcie realizacji przez DWO	3.	Przygotowanie podłączenia	Od ilości zleconych szkół do DRP odjęcie poz. 2 i 4	4.	Zlecone podłączenia (do podwykonawców)	Ilość spraw zleconych do podwykonawców i w trakcie realizacji przez	5.	Szkoły podłączone	Ilość szkół podłączonych
	Zadanie	Opis																	
1.	Szkoły do podłączenia	Ilość szkół zleconych do DRP																	
2.	Zlecone do zestawienia łączy	Ilość spraw zleconych do DWO i w trakcie realizacji przez DWO																	
3.	Przygotowanie podłączenia	Od ilości zleconych szkół do DRP odjęcie poz. 2 i 4																	
4.	Zlecone podłączenia (do podwykonawców)	Ilość spraw zleconych do podwykonawców i w trakcie realizacji przez																	
5.	Szkoły podłączone	Ilość szkół podłączonych																	
2.	<p>Bieżący status realizacji podłączeń z podziałem na opublikowane harmonogramy (kolejność kolumn do ustalenia)</p>																		
	<p>ID</p> <p>Data publikacji harmonogramu</p> <p>Lokalizacja (Id, adres)</p> <p>RSPO</p> <p>Szkoła (nazwa, adres, status)</p> <p>Dane kontaktowe (TRS, Dyrektor, opiekun) - imię, nazwisko, email, telefon</p> <p>Dostęp OSE - status usługi,</p> <p>status sprawy pozyskania</p> <p>Status sprawy podłączenia</p> <p>Numer umowy</p> <p>Czy przyszło zlecenie do DRP</p> <p>Osoba odpowiedzialna z DRP</p> <p>Planowany tydzień podłączenia</p> <p>Data uruchomienia</p> <p>Nazwa OPS</p> <p>Możliwy termin świadczenia usług</p> <p>Operator dostępowy</p>																		
3	<p>Czas analizy ankiety technicznej w ujęciu na pracownika i ogółem; wyliczanie czasów dla godzin roboczych, obliczanie średniej, mediany</p>																		
4	<p>Czas przygotowania Koncepcji podłączenia szkoły w ujęciu na pracownika i ogółem; wyliczanie czasów dla godzin roboczych, obliczanie średniej, mediany</p>																		
5	<p>Czas zestawienia łączą; w ujęciu na operatora i ogółem; wyliczanie czasów dla dni kalendarzowych, roboczych, obliczanie średniej, mediany</p>																		

1.	<p>ilość szkół i lokalizacji zleconych do podłączenia i podłączonych (w podziale na szkoły i lokalizacje, poszczególne harmonogramy);</p> <p>wraz z raportem lista szkół podłączonych (RSPO, nazwa, dane adresowe wraz z gminą i powiatem); lokalizacji podłączonych;</p> <p>częstotliwość - na żądanie</p>
6	Czas przekazania usługi do utrzymania (od daty aktywacji usługi do przekazania do utrzymania) w ujęciu na pracownika i ogółem; wyliczanie czasów dla godzin roboczych, obliczanie średniej, mediany
7	Wykaz zamówień przekazanych do podwykonawców w ujęciu na podwykonawcę, rodzaj zamówień (instalacje, serwis), przeniesienie do rekordu raportu wszystkich danych dot. konkretnego zamówienia, np.. Data, numer umowy, numer zamówienia, wykaz prac, kwoty, itp.
8	Czas realizacji zamówień przez podwykonawcę; w ujęciu na podwykonawcę i ogółem; uwzględniający rodzaj zleconych prac; wyliczanie czasów dla dni kalendarzowych, roboczych, obliczanie średniej, mediany
9	Rozliczenia z podwykonawcami - lista zleconych zamówień, z numerami umów ramowych, z numerami zamówień, zakresem, kwotą, adnotacją czy prace odebrane, czy wystawiona faktura, numer faktury
10	Informacja na temat realizacji KPI/ dotrzymywania „SLA” przez podwykonawców (np.: per umowa ramowa, ekipa podwykonawcy - o ile będzie możliwe wskazywanie ekip wykonujących prace)
11	Badanie satysfakcji Szkół vs. realizację instalacji/serwis/usuwanie awarii
12	Informacje dot. zgłaszanego zapotrzebowania na sprzęt przez podwykonawców w podziale na podwykonawcę, rodzaj sprzętu
13	Możliwość generowania raportów (na żądanie) po poszczególnych statusach za dowolnie zdefiniowany okres.
14	Automatyczne wyliczenia możliwych do zastosowania kar finansowych za brak lub nienależyte wykonanie umowy/opóźnienia w realizacji zamówień instalacji/usuwanie awarii- wynikające wprost z zapisów umowy.
15	Wykaz zasobów przypisanych do szkoły lub lokalizacji (zasoby sieciowe, sprzętowe, łącza)
16	Możliwość definiowania nowych raportów w oparciu o pola w bazie danych
17	Raport dla zadanych RSPO
	<p>Warunki dla raportu:</p> <p>Dla różnych zestawów RSPO, np. łącza INEI gotowe w pierwszej kolejności, łącza MDO gotowe, łącza NEXERY gotowe w pierwszej kolejności, itp.</p> <p>Dane:</p> <p>Szkoła (RSPO, status, nazwa, dane adresowe)</p> <p>Przepustowość</p> <p>Rodzaj lokalizacji (OSE, POPC, MAN)</p> <p>Nr umowy</p> <p>Zamówienie (data, numer)</p> <p>Osoba realizująca z DRP</p> <p>Status koncepcji (przygotowana, zaakceptowana)</p>

1.	<p>ilość szkół i lokalizacji zleconych do podłączenia i podłączonych (w podziale na szkoły i lokalizacje, poszczególne harmonogramy);</p> <p>wraz z raportem lista szkół podłączonych (RSPO, nazwa, dane adresowe wraz z gminą i powiatem); lokalizacji podłączonych;</p> <p>częstotliwość - na żądanie</p>
	Zamówienie (czy u podwykonawcy, numer, planowana data instalacji)

7.2.5. Proces utrzymania sieci, usług i systemów

Nr wymagania	Treść wymagania
O5.F1	Należy zapewnić regularne aktualizacje OS, systemów w zakresie bezpieczeństwa oraz wersji oprogramowania poprzedzone testami (również regresji) na środowiskach preprod. Wersjonowanie, możliwość przywrócenia poprzedniej wersji
O5.F2	Rozwiązanie musi zawierać proaktywny monitoring urządzeń w szkieletach, punktów styku, usług w szkołach i dostępności systemów. Wizualizacja geograficzna, śledzenie alarmów, thresholdy etc. Wykresy zależności online między awarią a jej wpływem na inne części infrastruktury. FM w zakresie usług klienckich oraz infrastruktury OSE.
O5.F3	Rozwiązanie musi zawierać narzędzia do ewidencji zasobów, narzędzia klasy DCIM
O5.F4	Rozwiązanie musi zapewniać automatyzację procesu informowania szkół o możliwych niedostępnościach usług w wyniku prac planowych. Rejestracja pracy planowej na dowolnym elemencie infrastruktury sieciowej OSE musi skutkować wysłaniem odpowiednich powiadomień do szkół, na które praca planowa będzie miała dostęp.
O5.F5	Rozwiązanie musi umożliwiać zbieranie i aktualizację wszelkich informacji o wszystkich podwykonawcach występujących we wszystkich procesach + poziomy uprawnień, nadawanie dostępu etc - ewidencja zasobów
O5.F6	Rozwiązanie musi zawierać platformę do wymiany informacji między podmiotami / podwykonawcami w ramach procesów obsługowych
O5.F7	Rozwiązanie musi uwzględniać podwykonawców inni niż realizujący prace w szkołach (utrzymanie sieci, systemów bezpieczeństwa, NOC ...)
O5.F8	Rozwiązanie musi umożliwiać zgłaszanie przez pracowników / współpracowników NASK ticketów do podwykonawców realizujących procesy utrzymaniowe w zakresie dostępności narzędzi obsługowych (zgodnie z SLA w zakresie podpisanych umów)
O5.F9	Na docelowej platformie BSS należy wdrożyć proces "Obsługa awarii masowej" na podstawie przebiegu procesu w systemie JIRA osadzonym w docelowym środowisku. Po stronie dostawcy rozwiązania znajduje się odpowiedzialność za analizę przebiegu procesu (wraz z konfiguracją) oraz jego dostosowanie do architektury docelowych systemów. W ramach analizy biznesowej należy uwzględnić najlepsze praktyki branżowe oraz specyfikę operatora OSE.

Nr wymagania	Treść wymagania
O5.F10	Na docelowej platformie BSS należy wdrożyć proces "Obsługa prac planowych" na podstawie przebiegu procesu w systemie JIRA osadzonym w docelowym środowisku. Po stronie dostawcy rozwiązania znajduje się odpowiedzialność za analizę przebiegu procesu (wraz z konfiguracją) oraz jego dostosowanie do architektury docelowych systemów. W ramach analizy biznesowej należy uwzględnić najlepsze praktyki branżowe oraz specyfikę operatora OSE.
O5.F11	Rozwiązanie musi zapewniać przechowywanie informacji o pracach planowych (kto i kiedy zgłosił, jakich elementów i w jakim okresie dotyczy) oraz udostępniać te informacje użytkownikom za pośrednictwem Portalu Usługowego i w komponencie CRM, a także w procesach obsługi zgłoszeń.
O5.F12	Rozwiązanie musi zapewniać przechowywanie informacji o awariach masowych (kto i kiedy wykrył, jakich elementów dotyczyło, w jakim okresie powodowało problemy) oraz udostępniać te informacje w komponencie CRM, a także w procesach obsługi zgłoszeń.

Rozwiązanie musi zapewniać wystarczającą wydajność dla procesów zgodnie z poniższymi parametrami

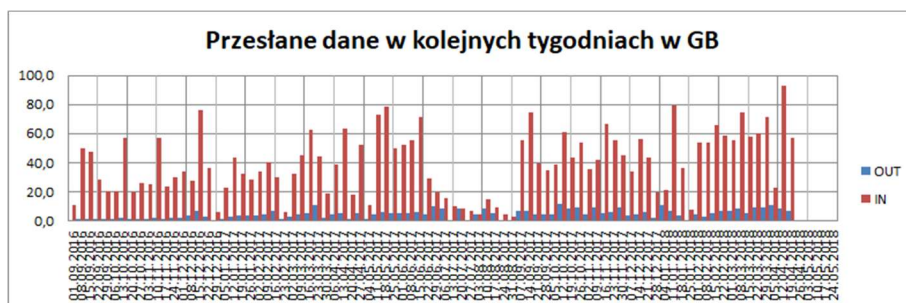
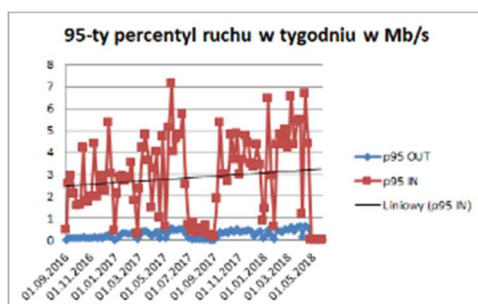
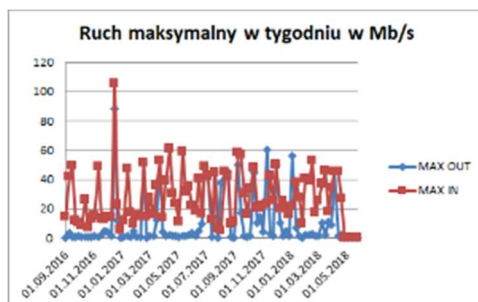
L.p.	Nazwa procesu	Ilość dzienna / miesięczna uruchomień procesu	Uwagi
1	Obsługa awarii masowej	50 / 1000	
2	Obsługa prac planowych	50 / 1000	

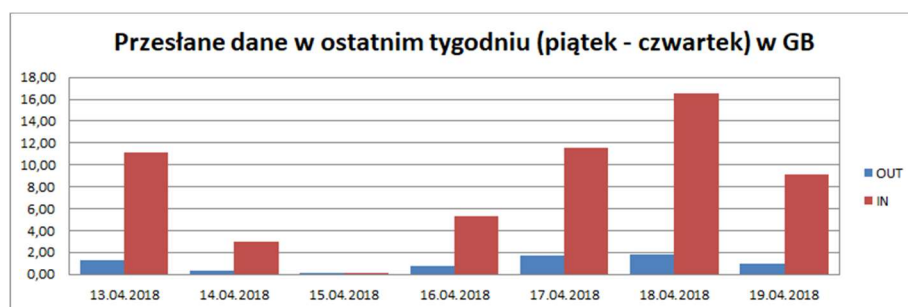
Wymagania w zakresie raportowania:

L.p.	Parametr	Wartość
1.	ID z bazy	
2.	Nazwa szkoły	
3.	województwo	
4.	liczba uczniów	
5.	Uwagi	
6.	Założenie (z próbki ruchu)	
7.	% ruchu w GNR:	30%
8.	Maksymalny w tygodniu, średni ruch w Godzinie Największego Ruchu w kierunku od szkoły w Mb/s (estymacja)	
	Transfer danych w GB	

L.p.	Parametr	Wartość
9.	Maksymalny w tygodniu, średni ruch w Godzinie Największego Ruchu w kierunku do szkoły w Mb/s (estymacja)	
10.	Maksymalna, dzienna ilość danych przesłana w kierunku od szkoły w ostatnim tygodniu	
11.	Maksymalna, dzienna ilość danych przesłana w kierunku do szkoły w ostatnim tygodniu	
12.	Maksymalna, dzienna ilość danych przesłana w kierunku od szkoły od początku obserwacji	
13.	Maksymalna, dzienna ilość danych przesłana w kierunku do szkoły od początku roku szk. 2016/7.	
14.	Średnia, dzienna ilość danych przesłana w kierunku od szkoły od początku obserwacji	
15.	Średnia, dzienna ilość danych przesłana w kierunku do szkoły od początku roku szk. 2016/7.	
16.	Ilość danych przesłana w całym ostatnim tygodniu w kierunku od szkoły	
17.	Ilość danych przesłana w całym ostatnim tygodniu w kierunku do szkoły	

Raportowanie dla każdej ze szkół:





7.2.6. Proces współpracy z operatorami

Nr wymagania	Treść wymagania
O6.F1	Rozwiązanie musi umożliwiać wyszukiwanie po adresie łącznie z podpowiadanie, po nazwie szkoły, numerze RSPO (unikalny numer szkoły), ID_lokalizacji (unikalny numer lokalizacji). Wyszukiwanie powinno być łatwe bez konieczności wskazywania, po jakim atrybucie ma następować wyszukiwanie.
O6.F2	<p>Rozwiązanie musi zawierać statusy zleceń i umożliwiać łatwy wybór tych zleceń zamówienia łączy, które są w danym statusie. Przykładowe statusy:</p> <ul style="list-style-type: none"> a.1. Zlecone wystawienie zamówienia do operatora na łącze a.2. Zlecone wystawienie zamówienia do operatora na zmianę przepływności a.3. Zlecone inne działanie z operatorem a.4. Zamówienie na łącze wysłane do operatora a.5. Zamówienie na zmianę przepływności wysłanego do operatora a.6. Uzyskano odpowiedź: brak dostarczenia email a.7. Uzyskano odpowiedź: Błąd formalny – zamówienie wymaga poprawy a.8. Uzyskano odpowiedź: Potwierdzono przyjęcie Zamówienia (automatyczny status po 2DR (dniach roboczych) od daty wysyłki zamówienia do operatora. a.9. Uzyskano odpowiedź: Przesłane parametry Usługi Zamówienie łączy a.10. Uzyskano odpowiedź: Przesłano potwierdzenie zwiększenia przepływności łączy a.11. Brak załadowania parametrów łączy – błąd w strukturze danych w email – podejmij a.12. Minął termin odbioru łączy: 14DR od daty z punktu a.8. dokonaj aktywacji lub zgłoś problem a.13. łączy do szkoły aktywne – brak wykonania instalacji sieci w szkole a.14. łączy do szkoły aktywne – szkoła podłączona do OSE (wykonana instalacja w szkole, łączy sprawne) a.15. łączy do szkoły aktywne – problem z uruchomieniem łączy (Awaria po stronie operatora) a.16. Inny status: błąd – sprawdź, na jakim etapie wystąpił błąd.
O6.F3	Zamówienie do operatora ma być wypełniane automatycznie na podstawie danych przechowywanych w systemie – zgodnie z załączonym wzorem zamówieniem.
O6.F4	Rozwiązanie musi sprawdzić i dokonać kolekcjonowania wszystkich Szkół pod danym adresem – tym samym wyliczyć według algorytmu zamawianą przepływność, liczbę VLAN.
O6.F5	Rozwiązanie musi sprawdzać czy pod wskazanym adresem nie zostało już wcześniej wystawione zamówienie na łącze. Moduł musi odrzucić próbę zamówienia drugiego łączy na danym adresie pomimo, iż będzie inna szkoła. W takim przypadku musi być możliwość zamknięcia zlecenia bez przejścia przez wysyłkę zamówienia.

Nr wymagania	Treść wymagania
O6.F6	Rozwiązanie musi umożliwiać wydrukowanie automatycznie wypełnionego zamówienia (w formie pliku edytowalnego np. word), następnie po jego podpisaniu przez upoważnioną osobę musi istnieć możliwość jego załączenia w formie scan (pdf) do obiektu/zlecenia zamówienia. System musi przechowywać zarówno edytowalną wersję wygenerowanego zamówienia jak i załączony przez użytkownika scan (pdf).
O6.F7	Rozwiązanie musi umożliwiać wysyłkę email bezpośrednio z systemu, załączając scan pdf. Wysyłka email musi być realizowana ze wskazanej skrzynki email innej niż do ogólnego kontaktu z operatorem. Treść email musi być zgodna z załączonym dokumentem: treść email. Co więcej treść email musi zawierać pola wypełnione automatycznie, w tym samym formacie, aby umożliwić operatorowi jego parsowanie.
O6.F8	Adresy email operatorów muszą być przechowywane i w zależności od operatora danego łącza automatycznie się wybierać w pole do. Na podstawie danych z systemu.
O6.F9	Rozwiązanie musi automatycznie przetworzyć otrzymany przez operatora komunikat - rozpoznać odpowiedź: i.1. Błąd formalny – zmienić status zlecenia na a.7. i przejść z powrotem do etapu wysyłki zamówienia. i.2. Potwierdzone przesłane parametry – zmienić status na a.9 oraz automatycznie na podstawie treści email pobrać parametry usługi do systemu: i.2.1. Model CPE i.2.2. Model AP Wi Fi i.2.3. Numery VLAN i.2.4. Data podłączenia łącza. i.2.5. Podczepić numery VLAN pod łącze, które założone zostałyby automatycznie. Rozpoznanie łącza odbyłoby się po numerze RSPO oraz ID_2017 w zależności od struktury obiektów w systemie. i.3. Inna treść email lub brak możliwości pasowania wszystkich niezbędnych parametrów. System musi zmienić status i dokonać walidacji liczby zamawianych VLAN z liczbą otrzymanych VLAN. Status musi zmienić się na a.11. System musi umożliwić ręczne wpisanie (nawet nowych) lub skorygowanie parametrów VLAN, Model CPE, Model AP
O6.F10	Rozwiązanie musi zmienić status na „zamówienie niewykonane w terminie” w przypadku, w którym brak jest odpowiedzi operatora w terminie 60 DR od daty wysłania email z Zamówieniem.
O6.F11	Rozwiązanie musi ustawić automatycznie datę podłączenia łącza i przekazać zlecenie do Działu Podłączenia Usług w celu rozpoczęcia procesu budowy sieci we szkole. Uwaga dział realizacji podłączenia Usług w szkole musi otrzymać zlecenie dotyczące budowy sieci w szkole dopiero po otrzymaniu od operatora parametrów lub w przypadku ręcznej obsługi (ręcznego wypełnienia parametrów) przekazania do tego działu zlecenia.
O6.F12	Musi istnieć możliwość wystawienia zlecenia na zmianę przepływności łącza przez centrum kontaktu z klientami.
O6.F13	Proces zamówienia nowej przepływności jest prawie taki sam jak proces zamawiania łącza. Również następuje wysyłka Zamówienia za pomocą email. Należy jednak dopasować temat email do nowego rodzaju zamówienia. Przy zmianie prędkości, zamówienie powinno mieć wygenerowany nowy numer zamówienia, przy czym musi on być połączony z numerem oryginalnego zamówienia na dane łącze (lub zamówienie musi być w inny sposób powiązane z zamówieniem na łącze).

Nr wymagania	Treść wymagania
O6.F14	Rozwiązanie musi umożliwiać, aby zamówienie na zmianę przepływności na danym łączu może być wystawiane wielokrotnie na danym adresie.
O6.F15	Rozwiązanie musi umożliwiać wysyłkę email bezpośrednio z systemu, załączając scan pdf zamówienia na zmianę przepływności. Wysyłka email powinna być realizowana ze wskazanej skrzynki email innej niż do ogólnego kontaktu z operatorem, ale tej samej co dla Zamawiania łącza. Treść email musi być zgodna z załączonym dokumentem: treść email. Co więcej treść email powinna zawierać pola wypełnione automatycznie, w tym samym formacie, aby umożliwić operatorowi jego parsowanie.
O6.F16	Adresy email operatorów muszą być przechowywane i w zależności od operatora danego łącza automatycznie się wybierać w pole do. Na podstawie danych z systemu
O6.F17	Rozwiązanie musi automatycznie przetworzyć otrzymany przez operatora komunikat - rozpoznać odpowiedź: g.1. Błąd formalny – zmienić status zlecenia na a.7. i przejść z powrotem do etapu wysyłki zamówienia na zmianę przepływności. g.2. Brak możliwości technicznych g.3. Zlecenie wykonano.
O6.F18	Rozwiązanie ma zmienić status na „zamówienie niewykonane w terminie” w przypadku, w którym brak jest odpowiedzi operatora w terminie SDR od daty wysłania email z Zamówieniem na zmianę przepływności
O6.F19	Po otrzymaniu odpowiedzi od operatora ma wystawić się zlecenie na kontakt z klientem – lub automatyczne wysłanie do szkoły email. Przepływność zmieniona dnia:..... (6DR+data wysłania email). Potwierdź wyższą przepływność.
O6.F20	Łączą rozumiane, jako relacja pomiędzy lokalizacją Szkoły a Punktem Styku PWR muszą być ładowane automatycznie na podstawie pliku txt, excel ze zdefiniowanymi polami. Łączą muszą być w systemie automatycznie utworzone, przy czym mogą mieć statusy: łączą planowane do uruchomienia, uruchomione – utrzymane parametry, zlikwidowane. Statusy łączą zależą od obsługi Zamówień tj. po przejściu przez proces zamawiania łącza status musi zostać zmieniony z „planowane” na uruchomione
O6.F21	Zmiany przepływności łącza automatycznie mają zmienić atrybut – przepływność danego łącza.
O6.F22	Pod łączę za pomocą ID adresu lub RSPO muszą być podczipione numery VLAN otrzymane od operatora w procesie zestawienia łącza. System muszą parsować treść email otrzymywanego od operatora i parsować numery VLAN, typ urządzeń CPE, AP, oraz inne dane.
O6.F23	Na danym łączu data jego uruchomienia musi ustawiać się sama w zależności od zdefiniowanego jednoznacznego algorytmu.
O6.F24	Rozwiązanie musi rzucać całą strukturę danych wraz ze statusami do bazy – tworzenie shadow, łącznie z ID zamówienia i wszystkimi atrybutami lokalizacji (Adres,ID). Raz dziennie.
O6.F25	Rozwiązanie przy zdefiniowanym algorytmie dla niektórych łącz o przepływności powyżej 100Mbps musi wystawiać automatycznie faktury dla Szkoły i wysyłać je email na wskazany adres email.
O6.F26	Rozwiązanie musi umożliwiać przechowywanie danych operatorów, w szczególności dane spółki oraz dane kontaktowe (email, telefon) do kilkunastu procesów, jakie są realizowane pomiędzy OSE a

Nr wymagania	Treść wymagania
	<p>Operatorem. Wykaz danych, jakie powinny być przechowywane z możliwością ich edycji:</p> <ul style="list-style-type: none"> a.1. Nazwa operatora a.2. NIP a.3. Dane kontaktowe do: <ul style="list-style-type: none"> a.3.1. Zamówienie na usługę a.3.2. Zamówienie na rezygnację z usługi i zmianę opcji usługi a.3.3. Uruchomienie i modyfikacja PWR a.3.4. Likwidacja PWR a.3.5. Migracja PWR a.3.6. Wykaz osób uprawnionych do podpisu zamówień a.3.7. Projekty techniczne a.3.8. Reklamacje finansowe a.3.9. Potwierdzenie odbioru zamówień Usługa TD a.3.10. Błędy formalne zamówień a.3.11. Informacja o dacie realizacji zamówienia a.3.12. Potwierdzenie realizacji zamówienia a.3.13. Potwierdzenie realizacji modyfikacji a.3.14. Potwierdzenie realizacji dezaktywacji a.3.15. Interwencje dotyczące realizacji usługi a.3.16. Zgłoszenia uszkodzeń, awarii i przerw w świadczeniu usługi a.3.17. Zgłoszenia awarii PWR oraz prace planowe a.3.18. Reklamacje operatorskie
O6.F27	Dane danego operatora powinny być przypisywane na podstawie danych wsadowych do danej lokalizacji. Istnieje konieczność możliwości zmiany danego operatora obsługującego daną lokalizację.
O6.F28	Rozwiązanie musi umożliwiać edycję danych operatora i zmianę danych kontaktowych.
O6.F29	<p>Rozwiązanie musi umożliwiać przechowywanie i edycję trzech typów łączy:</p> <ul style="list-style-type: none"> a.1. Łącza dostępne: łącza do szkoły do PWR przypisane do lokalizacji i ładowane zgodnie z punktem 3a. Lokalizacji węzłów PWR będzie około 80. a.2. Łącza tranzytowe: łącza od PWR do węzła OSE, łącza te mogą być wprowadzana ręcznie, przy czym wybór lokalizacji węzłów (punktów styku) musi być osłownikowany a lokalizacja rozumiana nie tylko przez adres, ale również lokalizację w budynku (nr pomieszczenia czy szafa). Lokalizacji węzłów OSE będzie 16. a.3. Łącza Szkieletowe: łącza pomiędzy węzłami sieci OSE. Łącza te mogą być wprowadzone ręcznie poprzez wskazanie ich lokalizacji.
O6.F30	Rozwiązanie musi automatycznie na podstawie danych od operatora (w email) przypisywać łącza do PWR do danego łącza tranzytowego. Tak, aby istniała możliwość wyświetlenia, w jaki sposób jest zestawione łącze End2End do węzła OSE.
O6.F31	Do łączy od szkół do PWR muszą być automatycznie przypisane VLANY z możliwością ich edycji.
O6.F32	Na docelowej platformie BSS należy wdrożyć proces "Zestawienie łącza" na podstawie przebiegu procesu w systemie JIRA osadzonym w docelowym środowisku. Po stronie dostawcy rozwiązania znajduje się odpowiedzialność za analizę przebiegu procesu (wraz z konfiguracją) oraz jego

Nr wymagania	Treść wymagania
	dostosowanie do architektury docelowych systemów. W ramach analizy biznesowej należy uwzględnić najlepsze praktyki branżowe oraz specyfikę operatora OSE.
O6.F33	Na docelowej platformie BSS należy wdrożyć proces "Zmiana szybkości łącza" na podstawie przebiegu procesu w systemie JIRA osadzonym w docelowym środowisku. Po stronie dostawcy rozwiązania znajduje się odpowiedzialność za analizę przebiegu procesu (wraz z konfiguracją) oraz jego dostosowanie do architektury docelowych systemów. W ramach analizy biznesowej należy uwzględnić najlepsze praktyki branżowe oraz specyfikę operatora OSE.

Rozwiązanie musi zapewniać wystarczającą wydajność dla procesów zgodnie z poniższymi parametrami

L.p.	Nazwa procesu	Ilość dzienna / miesięczna uruchomień procesu	Uwagi
1	Zestawienie łącza	200 / 2000	
2	Zmiana szybkości łącza	400 / 5000	

Wymagania w zakresie raportowania:

W celu rozliczeń z operatorami wymagany jest następujący raport:

- Identyfikator Łącza nadany przez NASK ID_2017 (identyfikator łącza i lokalizacji)
- Identyfikator Łącza nadany przez Operatora (jego nazewnictwo – pole puste, jeśli brak)
- Identyfikator Zamówienia służący do zamówienia danego łącza. System nie powinien mieć kilku identyfikatorów zamówienia przypisanych do jednego łącza (jeśli ma wybiera najnowszy).
- Identyfikator Zamówienia służący do zmiany przepływności.
- Data przesłania email o dacie instalacji przez operatora.
- Data aktywacji usługi – uruchomienia płatności. W przypadku braku awarii będzie to +14 dni od daty instalacji łącza przez Operatora (daty podanej przez operatora).
- Data wykonania i ukończenia budowy sieci przez Dział Realizacji Usług (wykonania sieci LAN w szkole i sprawdzenia łącza).
- Przepływność łącza.
- Liczba płatnych 50/50Mbps wyliczanych na podstawie algorytmu. Uwaga będzie to wymagało raportu per lokalizacja przy agregacji przepływności z poszczególnych szkół.
- Dokładny Adres
- Współrzędne geograficzne.
- Cena za łącze standard 100/100Mbps według cennika
- Cena za dodatkową opcję 50/50Mbps według cennika

- Cena za instalację usługi.
- Wyliczona wartość abonamentu w danym miesiącu: dla aktywacji w środku miesiąca 1/30 abonamentu za dzień. Uwzględnione awarie, jeśli przekroczone SLA 24/5 dla danego zdarzenia awarii.
- Atrybut POPC/Nie POPC
- Pełna nazwa operatora łącza
- Pełna nazwa PWR (punktu styku).

7.2.7. Proces zarządzania bezpieczeństwem OSE

Nr wymagania	Treść wymagania
O7.F1	Rozwiązanie musi zapewniać realizację procesu obsługi zgłoszeń incydentów bezpieczeństwa ze szkół OSE zgodnie z przebiegiem procesu technicznej obsługi zgłoszeń dla szkół (obszar 3) uwzględniając jednocześnie rozszerzenia funkcjonalności wynikające z wymagań bezpieczeństwa (obszar 7).
O7.F2	Rozwiązanie musi zapewnić możliwość stworzenia i korzystania z bazy scenariuszy wspomagających prowadzić proces obsługi incydentów bezpieczeństwa
O7.F3	Rozwiązanie musi zapewnić możliwość stworzenia i korzystania z bazy wiedzy dotyczącej rozwiązanych już wcześniej incydentów bezpieczeństwa
O7.F4	Rozwiązanie musi zapewnić możliwość zmian w usługach tylko osobom upoważnionym
O7.F5	Portal OSE musi zapewnić możliwość delegowania uprawnień do wprowadzania zmian w usługach przez Dyrektora na inną osobę (do zrealizowania poza rozwiązaniem)
O7.F6	Rozwiązanie musi zapewnić możliwość wymuszenia max. ilości zmian w usługach bezpieczeństwa w założonym okresie czasu
O7.F7	Rozwiązanie musi zapewnić możliwość raportowania wykonywanych przez osoby upoważnione zmian (kto, kiedy, co)
O7.F8	Rozwiązanie musi zapewnić możliwość generowania dashboard'u z aktualnym ogólnym stanem bezpieczeństwa w szkole dla osób upoważnionych, dane do dashboard'u zostaną dostarczone przez systemy bezpieczeństwa OSE
O7.F9	Rozwiązanie musi zapewnić możliwość generowania raportów tylko osobom upoważnionym
O7.F10	Portal OSE musi zapewnić możliwość delegowania uprawnień do generowania raportów przez Dyrektora na inną osobę (do zrealizowania poza rozwiązaniem)
O7.F11	Rozwiązanie musi zapewnić możliwość wymuszenia max. ilości generowanych raportów w założonym okresie czasu
O7.F12	Rozwiązanie musi zapewnić możliwość wymuszenia max. długości okresu, za jaki raport może zostać wygenerowany
O7.F13	Rozwiązanie musi zapewnić możliwość raportowania wykonywanych przez osoby upoważnione raportów (kto, kiedy, co)

Nr wymagania	Treść wymagania
O7.F14	Na docelowej platformie BSS należy wdrożyć proces "Nieprawidłowe filtrowanie stron www" na podstawie definicji opisanej w ramach rozdziału "Architektura biznesowa operatora OSE". Należy przeprowadzić analizę biznesową celem opracowania definicji procesu oraz określenia dla niego konfiguracji biznesowej uwzględniając najlepsze praktyki branżowe oraz specyfikę operatora OSE.
O7.F15	Na docelowej platformie BSS należy wdrożyć proces "Incydenty sieciowe" na podstawie definicji opisanej w ramach rozdziału "Architektura biznesowa operatora OSE". Należy przeprowadzić analizę biznesową celem opracowania definicji procesu oraz określenia dla niego konfiguracji biznesowej uwzględniając najlepsze praktyki branżowe oraz specyfikę operatora OSE.
O7.F16	Na docelowej platformie BSS należy wdrożyć proces "Aktywacja usług bezpieczeństwa OSE" na podstawie definicji opisanej w ramach rozdziału "Architektura biznesowa operatora OSE". Należy przeprowadzić analizę biznesową celem opracowania definicji procesu oraz określenia dla niego konfiguracji biznesowej uwzględniając najlepsze praktyki branżowe oraz specyfikę operatora OSE.
O7.F17	Na docelowej platformie BSS należy wdrożyć proces "Dezaktywacja usług bezpieczeństwa OSE" na podstawie definicji opisanej w ramach rozdziału "Architektura biznesowa operatora OSE". Należy przeprowadzić analizę biznesową celem opracowania definicji procesu oraz określenia dla niego konfiguracji biznesowej uwzględniając najlepsze praktyki branżowe oraz specyfikę operatora OSE.
O7.F18	Na docelowej platformie BSS należy wdrożyć proces "Modyfikacja usługi ochrony użytkownika OSE" na podstawie definicji opisanej w ramach rozdziału "Architektura biznesowa operatora OSE". Należy przeprowadzić analizę biznesową celem opracowania definicji procesu oraz określenia dla niego konfiguracji biznesowej uwzględniając najlepsze praktyki branżowe oraz specyfikę operatora OSE.
O7.F19	Na portalu OSE musi być udostępniona funkcjonalność do zarządzania usługą "Ochrona użytkownika OSE" umożliwiając: Wybór listy kategorii blokowanych treści Tworzenie białej listy: URLe nieblokowane Tworzenie czarnej listy: URLe blokowane Tworzenie białej listy dla aplikacji mobilnych (wybór z listy), /zgodnie z polityką aplikacji niedające prawa do rozszycia SSL (większość) są blokowane/ Decyzja o analizie ruchu pocztowego (blokada, ochrona, brak kontroli) Ustalenie poziomu alarmowania.
O7.F20	Na portalu OSE musi być udostępniona funkcjonalność do zarządzania usługą "Ochrona przed szkodliwym oprogramowaniem" umożliwiając: Włączenie dla Poczty elektronicznej Włączenie dla Pobieranie plików z sieci Internet Tworzenie białej listy: URLe nieblokowane Ustalenie poziomu alarmowania
O7.F21	Na portalu OSE musi być udostępniona funkcjonalność do zarządzania usługą "Ochrona infrastruktury OSE" umożliwiając: Wprowadzanie niestandardowych zmian w konfiguracji sieci OSE: -Tworzenie listy adresów i portów sieciowych nieblokowanych -Tworzenie listy adresów i portów sieciowych blokowanych Ustalenie poziomu alarmowania

Nr wymagania	Treść wymagania
O7.F22	Portal OSE musi umożliwiać otrzymywanie raportów z systemów bezpieczeństwa dotyczących zarejestrowanych alarmów na usługach bezpieczeństwa, alarmy te muszą być wyświetlane uprawnionym użytkownikom (dyrektorom) od razu po zalogowaniu. Musi być również możliwość przeglądania alarmów w osobnej zakładce.
O7.F23	Centralny System Raportowy musi umożliwiać odbieranie z systemów bezpieczeństwa danych o zarejestrowanych alarmach oraz zapewniać funkcjonalności do tworzenia raportów w oparciu o przekroje szkół, lokalizacji (regionów), rodzajów podłączeń.
O7.F24	Portal OSE musi umożliwiać otrzymywanie statystyk ukazujące globalne informacje o sposobie wykorzystania Internetu w szkole oraz obejmujących wykryte w danym okresie czasu zdarzenia / alarmy w postaci plików graficznych. Portal OSE musi zawierać funkcjonalność do wyświetlania statystyk bezpieczeństwa dostępnych w postaci plików graficznych.
O7.F25	Centralny system Raportowy musi zapewniać funkcjonalność otrzymywania statystyk raportowych z systemów bezpieczeństwa pokazujących globalne informacje o wykorzystaniu internetu w szkołach.
O7.F26	Na docelowej platformie BSS należy wdrożyć proces "Proces obsługi alertów - generowanie powiadomień" na podstawie definicji opisanej w ramach rozdziału "Architektura biznesowa operatora OSE". Należy przeprowadzić analizę biznesową celem opracowania definicji procesu oraz określenia dla niego konfiguracji biznesowej uwzględniając najlepsze praktyki branżowe oraz specyfikę operatora OSE.
O7.F27	Na docelowej platformie BSS należy wdrożyć proces "Proces obsługi alertów - wyświetlanie powiadomień" na podstawie definicji opisanej w ramach rozdziału "Architektura biznesowa operatora OSE". Należy przeprowadzić analizę biznesową celem opracowania definicji procesu oraz określenia dla niego konfiguracji biznesowej uwzględniając najlepsze praktyki branżowe oraz specyfikę operatora OSE.
O7.F28	Na docelowej platformie BSS należy wdrożyć proces "Proces obsługi raportów usług bezpieczeństwa" na podstawie definicji opisanej w ramach rozdziału "Architektura biznesowa operatora OSE". Należy przeprowadzić analizę biznesową celem opracowania definicji procesu oraz określenia dla niego konfiguracji biznesowej uwzględniając najlepsze praktyki branżowe oraz specyfikę operatora OSE.
O7.F29	Na docelowej platformie BSS należy wdrożyć proces "Proces zarządzania komunikacją i szkoleniami dot. usług bezpieczeństwa" na podstawie definicji opisanej w ramach rozdziału "Architektura biznesowa operatora OSE". Należy przeprowadzić analizę biznesową celem opracowania definicji procesu oraz określenia dla niego konfiguracji biznesowej uwzględniając najlepsze praktyki branżowe oraz specyfikę operatora OSE.

Rozwiązanie musi zapewniać wystarczającą wydajność dla procesów zgodnie z poniższymi parametrami

L.p.	Nazwa procesu	Ilość dzienna / miesięczna uruchomień procesu	Uwagi
1	Nieprawidłowe filtrowanie stron www	100 / 1000	

L.p.	Nazwa procesu	Ilość dzienna / miesięczna uruchomień procesu	Uwagi
2	Incydenty sieciowe	200 / 1000	
3	Aktywacja usług bezpieczeństwa OSE	200 / 2000	
4	Dezaktywacja usług bezpieczeństwa OSE	200 / 1000	
5	Modyfikacja usług bezpieczeństwa OSE	200 / 1000	
6	Proces obsługi alertów - generowanie powiadomień	2 / 35	
7	Proces obsługi alertów - wyświetlanie powiadomień	25 000 / 500 000	
8	Proces obsługi raportów usług bezpieczeństwa	2 / 35	

Wymagania w zakresie raportowania:

Raporty będą generowane na żądanie Dyrektora szkoły, do ustalenia możliwa częstotliwość generowania raportów, okres danych objętych raportem, czas potrzebny na przygotowanie raportu oraz format raportu

Raport dotyczący monitorowania zagrożeń i bezpieczeństwa sieciowego zawierający następujące dane:

- wykryte zagrożenia zawiązane ze złośliwym oprogramowaniem w szkole
- wykryte ataki sieciowe na sieci szkół

Raport dotyczący monitorowania zagrożeń i przypadków naruszeń bezpieczeństwa użytkowników OSE zawierający następujące dane:

- TOP 10 kategorii **dozwolonych, przepuszczonych**, zgodnie z polityką filtrowania
- TOP 10 kategorii **niedozwolonych, zablokowanych**, zgodnie z polityką filtrowania
- TOP 10 najpopularniejszych stron www
- TOP 10 najpopularniejszych aplikacji www
- TOP 10 najpopularniejszych aplikacji mobilnych
- TOP 10 zablokowanych aplikacji mobilnych

7.2.8. Proces rozwoju OSS/BSS

Wymagana jest realizacja następujących wymagań:

Nr wymagania	Treść wymagania
O8.F1	W trakcie weryfikacji lub akceptacji opisu obszaru biznesowego można zgłaszać wyłącznie uwagi do elementów zmodyfikowanych od poprzedniej akceptacji. Wszelkie uwagi do opisu obszaru biznesowego dotyczące elementów już zaakceptowanych muszą być zgłaszane, jako nowe żądania zmiany.
O8.F2	Przyjęcie żądania zmiany do zakresu wymaga zgody / akceptacji właściciela biznesowego obszaru
O8.F3	Wszelkie integracje z siecią muszą być wyposażone w odpowiednie mechanizmy (whiteList i blackList) umożliwiające testowanie: <ul style="list-style-type: none"> - rozpoznawanie na podstawie konfiguracji, czy środowisko jest produkcyjne czy testowe - w przypadku środowiska testowego, wywołania do sieci są realizowane wyłącznie dla lokalizacji skonfigurowanych na whiteList, dla pozostałych zwracany jest zawsze sukces wraz z ewentualnym zestawem standardowych danych - w przypadku środowiska produkcyjnego sprawdzana jest blackList i dla lokalizacji na niej występujących nierealizowane jest wywołanie do sieci a jedynie zwracany jest komunikat o sukcesie wraz ze standardowym zestawem parametrów
O8.F4	Należy zapewnić narzędzia dla zarządzania konfiguracją zarówno środowisk testowych jak i produkcyjnych (CMDB)
O8.F5	Należy zapewnić wsparcie dla procesów zarządzania i utrzymania platformą POOSE, w tym min: <ul style="list-style-type: none"> - monitorowania systemów i środowisk - obsługa zgłoszeń użytkowników systemów (dotyczących zarówno problemów jak i zgłoszeń administracyjnych takich jak dodawanie użytkowników czy modyfikacja uprawnień)
O8.F6	Repozytorium opisu obszarów biznesowych powinno być zrealizowane w oparciu o platformę Confluence NASK PIB, należy, więc zapewnić integracje narzędzi dostarczanych w ramach przetargu z tą platformą
O8.F7	Proces akceptacji zmian opisu obszaru biznesowego powinien być zrealizowany w oparciu o narzędzie klasy workflow JIRA NASK PIB, należy, więc zapewnić w ramach projektu jego odpowiednią konfigurację
O8.F8	Należy dostarczyć systemy zarówno dla środowiska produkcyjnego jak i środowiska testowego. Aplikacje nie mogą mieć rozróżniać, na jakim typie środowiska pracują, z wyjątkiem integracji z siecią, która na podstawie konfiguracji musi uwzględniać blackListy i whiteListy.
O8.F9	Należy udokumentować architekturę POOSE w ramach SPARX Enterprise Architect opisując m.in. : <ul style="list-style-type: none"> - procesy biznesowe wspierane przez POOSE - model danych - wszystkie systemy POOSE (uwzględniając również podział na moduły) - integrację między poszczególnymi systemami (modułami) - procesy systemowe realizowane w ramach POOSE
O8.F10	Należy utworzyć bazę wiedzy POOSE na platformie TREE (Confluence NASK PIB) wykorzystując architekturę udokumentowaną w ramach SPARX Enterprise Architect, oraz co najmniej: <ul style="list-style-type: none"> - instrukcje stanowiskowe - dokumentację wdrożeniową - dokumentację administracyjną

Nr wymagania	Treść wymagania
	- dokumentację środowisk testowych - pozostałą dokumentację POOSE
O8.F11	Należy stworzyć integrację pomiędzy Sparx EA oraz TREE, umożliwiając aktualizowanie bazy wiedzy POOSE na TREE w wyniku zmian opisu architektury na SPARX EA
O8.F12	Należy zapewnić przeszkolenie zespołu POOSE (do 15 osób) w obszarze modelowania architektury przy wykorzystaniu narzędzia Sparx Enterprise Architect w zakresie wykorzystywanym w projekcie POOSE
O8.F13	Należy utworzyć i skonfigurować repozytorium architektury POOSE w ramach narzędzia Sparx EA w zakresie potrzebnym do dokumentowania projektu POOSE.
O8.F14	Należy zapewnić 4 licencji "floating" dla bieżącej wersji narzędzia Sparx Enterprise Architect dla zespołu zamawiającego oraz odpowiednią ilość licencji dla zespołu dostawcy. Licencje minimum w edycji "Unified".
O8.F15	Na docelowej platformie BSS należy wdrożyć proces "Zmiana definicji obszaru biznesowego" na podstawie definicji opisanej w ramach rozdziału "Architektura biznesowa operatora OSE". Należy przeprowadzić analizę biznesową celem opracowania definicji procesu oraz określenia dla niego konfiguracji biznesowej uwzględniając najlepsze praktyki branżowe oraz specyfikę operatora OSE.
O8.F16	Na docelowej platformie BSS należy wdrożyć proces "Obsługa żądania zmiany obszaru biznesowego" na podstawie definicji opisanej w ramach rozdziału "Architektura biznesowa operatora OSE". Należy przeprowadzić analizę biznesową celem opracowania definicji procesu oraz określenia dla niego konfiguracji biznesowej uwzględniając najlepsze praktyki branżowe oraz specyfikę operatora OSE.
O8.F17	Na docelowej platformie BSS należy wdrożyć proces "Obsługa żądania zmiany" na podstawie definicji opisanej w ramach rozdziału "Architektura biznesowa operatora OSE". Należy przeprowadzić analizę biznesową celem opracowania definicji procesu oraz określenia dla niego konfiguracji biznesowej uwzględniając najlepsze praktyki branżowe oraz specyfikę operatora OSE.
O8.F18	Na docelowej platformie BSS należy wdrożyć proces "Wdrożenie zmiany" na podstawie definicji opisanej w ramach rozdziału "Architektura biznesowa operatora OSE". Należy przeprowadzić analizę biznesową celem opracowania definicji procesu oraz określenia dla niego konfiguracji biznesowej uwzględniając najlepsze praktyki branżowe oraz specyfikę operatora OSE.
O8.F19	Na docelowej platformie BSS należy wdrożyć proces "Zarządzanie środowiskami IT" na podstawie definicji opisanej w ramach rozdziału "Architektura biznesowa operatora OSE". Należy przeprowadzić analizę biznesową celem opracowania definicji procesu oraz określenia dla niego konfiguracji biznesowej uwzględniając najlepsze praktyki branżowe oraz specyfikę operatora OSE.

Rozwiązanie musi zapewniać wystarczającą wydajność dla procesów zgodnie z poniższymi parametrami

L.p.	Nazwa procesu	Ilość dzienna / miesięczna uruchomień procesu	Uwagi
1	Zmiana definicji obszaru biznesowego	4 / 20	

L.p.	Nazwa procesu	Ilość dzienna / miesięczna uruchomień procesu	Uwagi
2	Obsługa żądania zmiany obszaru biznesowego	4 / 20	
3	Obsługa żądania zmiany	2 / 10	
4	Wdrożenie zmiany	10/15	

Wymagania w zakresie raportowania:

1.	Postęp przygotowania definicji obszarów biznesowych
Procesy	Zmiana obszaru biznesowego
Dane	Liczba wszystkich obszarów biznesowych, liczba obszarów w podziale na poszczególne statusy.
Format	Raport kołowy (pie chart)
2.	Obsługa żądania zmiany
Procesy	Obsługa żądania zmiany, Wdrożenie zmiany
Dane	Wszystkie żądania zmiany z podziałem na różne statusy (zaakceptowane, odrzucone, w trakcie), informacja o koszcie i czasie realizacji
Format	Tabela z możliwością sortowania
3.	Wdrożone rozwiązania
Proces	Wdrożenie zmiany
Dane	Wszystkie wdrożone żądania zmiany, budżety, czas realizacji, czas wdrożenia (implementacja + testy + wdrożenie), ilość zgłoszonych błędów w procesie testowania

7.2.9. Proces wsparcia OSE

Nr wymagania	Treść wymagania
O9.F1	Rozwiązanie musi zapewnić synchronizację wykazu umów podpisanych przez NASK PIB (z bazą kontrahentów NASK w Sugar CRM)
O9.F2	Rozwiązanie musi realizować rejestrację umów zgodnie z wykazem metadanych dla umów przychodowych OSE

Nr wymagania	Treść wymagania
O9.F3	Rozwiązanie musi wykorzystywać dane wprowadzone z formularza portalu OSE do generowania umowy
O9.F4	Rozwiązanie musi zapewniać automatyzację nadawanie numeru umowy OSE w systemach OSS/BSS oraz w systemie Sugar CRM
O9.F5	Rozwiązanie musi umożliwiać nadanie numeru (podwójna rejestracja) na podstawie generowanych raportów z Sugar CRM
O9.F6	Rozwiązanie musi zawierać funkcjonalność do weryfikacji kompletności dokumentacji w procesach podpisania umowy: - wymaganie oznaczenia braku w dokumentacji Umowy (lista z możliwością wyboru kilku pozycji) - możliwość wysłania maila do szkoły z informacją o zdiagnozowanych brakach
O9.F7	Rozwiązanie musi umożliwiać: - pobieranie skanów dokumentów z Arche po numerze rejestracyjnym sprawy/Barcode - przy rejestracji dokumentów wymagane jest przekazanie informacji do zdefiniowanych odbiorców (zespołów) o stanie dokumentu na podstawie Skanów systemu SOD (coś w stylu: elektroniczny obieg umów przychodowych) – wpływ brakujących załączników do umowy, skanów protokołów odbioru sprzętu, protokołu instalacji sprzętu w szkole, protokołu uruchomienia, zawieszenia, usług OSE
O9.F8	Rozwiązanie musi umożliwiać w procesie wypowiedzenia umowy: - generowanie dokumentu wypowiadającego umowę (na podstawie danych klienta i umowy zarejestrowanych w systemach) - przesłanie informacji do utrzymania ws. weryfikacji przepustowości łącza oraz w razie potrzeby przesłanie informacji do DWO w celu zlecenia modyfikacji łącza (rezygnacja szkoły może zmniejszyć zapotrzebowanie na łącze) - generowanie raportu z terminem zakończenia świadczenia usługi + protokół do ZEIRK
O9.F9	Rozwiązanie musi zapewniać w procesie wystawiania faktur: -przesyłanie skanów podpisanych protokołów uruchomienia płatnych usług OSE, lub protokołu zmian w płatnych usługach OSE (protokołu zakończenia płatnych usług OSE) w forma zdjęcie lub skanu na adres mailowy (do ustalenia) w celu wystawienia faktury, faktury korygującej oraz zamieszczenie tego skanu w systemie. Dodatkowo wprowadzenie linku do ARCHE w momencie wpływu oryginału na kancelarię NASK i przesłania skanu z SOD do ARCHE. - wysyłka e-faktur, zbieranie adresów mailowych do wysyłania e-faktur (dodatkowe pole) - wystawienie zgłoszeń do systemu rozliczeniowego z danymi faktur za usługi płatne (faktury na druku OSE)
O9.F10	W rozwiązaniu należy zaimplementować raporty z systemu FK o terminach zapłaty za faktury przez szkoły
O9.F11	W rozwiązaniu należy zaimplementować raporty usług do zawieszenia, usług do zamknięcia. - generowanie ticketów do DCK o przygotowanie wypowiedzenia usług płatnych, pisemnych informacji o zawieszeniu usługi - automatyczne generowanie stosownych dokumentów, po zatwierdzeniu przez Kierownika DCK
O9.F12	W rozwiązaniu należy zapewnić: - generowanie ticketów do DCK o przygotowanie wypowiedzenia usług płatnych, pisemnych

Nr wymagania	Treść wymagania
	<p>informacji o zawieszeniu usługi</p> <ul style="list-style-type: none"> - automatyczne generowanie stosownych dokumentów, po zatwierdzeniu przez Kierownika DCK
O9.F13	<p>Rozwiązanie musi zapewnić następujące raporty w obszarze umów:</p> <ul style="list-style-type: none"> - wygenerowanie raportu zawartych umów implementowanego do CRM NASK - generowanie raportu zawartych (obustronnie podpisanych) umów OSE (raport 1) - generowanie raportu „Umów OSE w podpisie” (raport 2)- zawiera umowy wysłane do szkół celem podpisania - generowanie raportu „Niekompletnych umów OSE” zawartych (obustronnie podpisanych) jednak z brakami wraz ze wskazaniem rodzaju braku - generowanie comiesięcznych raportów z „Wystawionych zamówień dla umowy [NR UMOWY],”(podany numer umowy) - raport ze sprzedanych produktów OSE płatnych i bezpłatnych (raport)
O9.F14	<p>Rozwiązanie musi zapewnić następujące raporty w obszarze rozliczeń z podwykonawcami:</p> <ul style="list-style-type: none"> - generowanie comiesięcznego raportów „Wykonane instalacje”/ „Szkoly w utrzymaniu”, kosztów wynikających z umowy/ zamówienia z podziałem - na źródło finansowania, nr umowy, lokalizację, województwo, lokalizację POPC, nie POPC, uwzględniającego złożone reklamacje - generowanie opisów do faktur za łączą, instalacje, serwis – ze wskazaniem umowy ze szkołą, lokalizacji i kwoty brutto, miesiąca wydatku – implementacja raportów do TETA - generowanie prognozowanych wydatków związanych ze świadczonymi usługami na podstawie planowanych instalacji w okresie miesięcznym, kwartalnym i rocznym - raporty z zainstalowanego sprzętu (szafy) przez podwykonawców w systemie - raport z protokołów podpisanych w danym miesiącu per rodzaj usługi (instalacja usługi płatne/instalacje usługi bezpłatne/ przekazanie do utrzymania)
O9.F15	<p>Rozwiązanie musi zapewnić</p> <ul style="list-style-type: none"> - generowanie raportów z planowanych instalacji w celu oszacowania wielkości zamówienia - generowanie raportów z zamówionego sprzętu, wydane z magazynu, zainstalowanego sprzętu (szkoła, data instalacji, rodzaj sprzętu – według nw. wariantów) - generowanie raportów protokołów uruchomienia usługi/instalacji sprzętu - generowanie dokumentów OT z zainstalowanych ŚT
O9.F16	<p>Rozwiązanie musi umożliwiać:</p> <ul style="list-style-type: none"> - automatyczne generowanie druków delegacji - implementacja wydatków związanych z delegacjami dot. wyjazdów do szkół, lokalizacji, punktów kolokacyjnych (powiązanie wydatków z konkretnymi szkołami – o ile jest to możliwe (ceny hoteli, biletów, kosztów delegacji itp.)
O9.F17	<p>Rozwiązanie musi umożliwiać:</p> <ul style="list-style-type: none"> - generowanie miesięcznego raportu Kadrowego z informacją o wysokości miesięcznego dochodu, możliwość wprowadzenia podziału finansowania, prognozowanie rocznych wydatków dot. wynagrodzeń z informacją o terminie wypłaty wynagrodzenia (raport kasowy), datą zatrudnienia i rozwiązania umowy o pracę (przeniesienie kart pracy i zatrudnienia - raport z wykazem wyposażenia oraz innymi kosztami pracowniczymi, np. szkoleniami, do rozważenia czy dofinansowanie do zakupu okularów też wliczać) - wskazanie odpowiednich uprawnień dla osób korzystających
O9.F18	<p>Na docelowej platformie BSS należy wdrożyć proces "Obieg dokumentów przychodzących" na podstawie definicji opisanej w ramach rozdziału "Architektura biznesowa operatora OSE". Należy</p>

Nr wymagania	Treść wymagania
	przeprowadzić analizę biznesową celem opracowania definicji procesu oraz określenia dla niego konfiguracji biznesowej uwzględniając najlepsze praktyki branżowe oraz specyfikę operatora OSE.
O9.F19	Na docelowej platformie BSS należy wdrożyć proces "Umowy kosztowe nie PZP, podNASK" na podstawie definicji opisanej w ramach rozdziału "Architektura biznesowa operatora OSE". Należy przeprowadzić analizę biznesową celem opracowania definicji procesu oraz określenia dla niego konfiguracji biznesowej uwzględniając najlepsze praktyki branżowe oraz specyfikę operatora OSE.
O9.F20	Na docelowej platformie BSS należy wdrożyć proces "Umowy kosztowe nie PZP, nie NASK" na podstawie definicji opisanej w ramach rozdziału "Architektura biznesowa operatora OSE". Należy przeprowadzić analizę biznesową celem opracowania definicji procesu oraz określenia dla niego konfiguracji biznesowej uwzględniając najlepsze praktyki branżowe oraz specyfikę operatora OSE.
O9.F21	Na docelowej platformie BSS należy wdrożyć proces "Przyjęcie środka trwałego" na podstawie definicji opisanej w ramach rozdziału "Architektura biznesowa operatora OSE". Należy przeprowadzić analizę biznesową celem opracowania definicji procesu oraz określenia dla niego konfiguracji biznesowej uwzględniając najlepsze praktyki branżowe oraz specyfikę operatora OSE.
O9.F22	Na docelowej platformie BSS należy wdrożyć proces "Faktury przychodowe" na podstawie definicji opisanej w ramach rozdziału "Architektura biznesowa operatora OSE". Należy przeprowadzić analizę biznesową celem opracowania definicji procesu oraz określenia dla niego konfiguracji biznesowej uwzględniając najlepsze praktyki branżowe oraz specyfikę operatora OSE.
O9.F23	Na docelowej platformie BSS należy wdrożyć proces "Proces windykacji przedsądowej" na podstawie definicji opisanej w ramach rozdziału "Architektura biznesowa operatora OSE". Należy przeprowadzić analizę biznesową celem opracowania definicji procesu oraz określenia dla niego konfiguracji biznesowej uwzględniając najlepsze praktyki branżowe oraz specyfikę operatora OSE.
O9.F24	Na docelowej platformie BSS należy wdrożyć proces "Proces windykacji sądowej" na podstawie definicji opisanej w ramach rozdziału "Architektura biznesowa operatora OSE". Należy przeprowadzić analizę biznesową celem opracowania definicji procesu oraz określenia dla niego konfiguracji biznesowej uwzględniając najlepsze praktyki branżowe oraz specyfikę operatora OSE.
O9.F25	Na docelowej platformie BSS należy wdrożyć proces "Proces monitoring należności" na podstawie definicji opisanej w ramach rozdziału "Architektura biznesowa operatora OSE". Należy przeprowadzić analizę biznesową celem opracowania definicji procesu oraz określenia dla niego konfiguracji biznesowej uwzględniając najlepsze praktyki branżowe oraz specyfikę operatora OSE.
O9.F26	Na docelowej platformie BSS należy wdrożyć proces "Proces wnioski o delegacje" na podstawie definicji opisanej w ramach rozdziału "Architektura biznesowa operatora OSE". Należy przeprowadzić analizę biznesową celem opracowania definicji procesu oraz określenia dla niego konfiguracji biznesowej uwzględniając najlepsze praktyki branżowe oraz specyfikę operatora OSE.
O9.F27	Na docelowej platformie BSS należy wdrożyć proces "Proces monitorowanie budżetu" na podstawie definicji opisanej w ramach rozdziału "Architektura biznesowa operatora OSE". Należy przeprowadzić analizę biznesową celem opracowania definicji procesu oraz określenia dla niego konfiguracji biznesowej uwzględniając najlepsze praktyki branżowe oraz specyfikę operatora OSE.
O9.F28	Na docelowej platformie BSS należy wdrożyć proces "Proces obsługa faktur kosztowych" na podstawie definicji opisanej w ramach rozdziału "Architektura biznesowa operatora OSE". Należy

Nr wymagania	Treść wymagania
	przeprowadzić analizę biznesową celem opracowania definicji procesu oraz określenia dla niego konfiguracji biznesowej uwzględniając najlepsze praktyki branżowe oraz specyfikę operatora OSE.
O9.F29	Na docelowej platformie BSS należy wdrożyć proces "Proces procedura zakupowa" na podstawie definicji opisanej w ramach rozdziału "Architektura biznesowa operatora OSE". Należy przeprowadzić analizę biznesową celem opracowania definicji procesu oraz określenia dla niego konfiguracji biznesowej uwzględniając najlepsze praktyki branżowe oraz specyfikę operatora OSE.
O9.F30	Na docelowej platformie BSS należy wdrożyć proces "Proces zamówienia na dostawę sprzętu" na podstawie definicji opisanej w ramach rozdziału "Architektura biznesowa operatora OSE". Należy przeprowadzić analizę biznesową celem opracowania definicji procesu oraz określenia dla niego konfiguracji biznesowej uwzględniając najlepsze praktyki branżowe oraz specyfikę operatora OSE.
O9.F31	Na docelowej platformie BSS należy wdrożyć proces "Proces dostawa sprzętu" na podstawie definicji opisanej w ramach rozdziału "Architektura biznesowa operatora OSE". Należy przeprowadzić analizę biznesową celem opracowania definicji procesu oraz określenia dla niego konfiguracji biznesowej uwzględniając najlepsze praktyki branżowe oraz specyfikę operatora OSE.
O9.F32	Na docelowej platformie BSS należy wdrożyć proces "Proces zawieranie umów przychodowych OSE" na podstawie definicji opisanej w ramach rozdziału "Architektura biznesowa operatora OSE". Należy przeprowadzić analizę biznesową celem opracowania definicji procesu oraz określenia dla niego konfiguracji biznesowej uwzględniając najlepsze praktyki branżowe oraz specyfikę operatora OSE.
O9.F33	Na docelowej platformie BSS należy wdrożyć proces "Proces reklamacja usług OSE" na podstawie definicji opisanej w ramach rozdziału "Architektura biznesowa operatora OSE". Należy przeprowadzić analizę biznesową celem opracowania definicji procesu oraz określenia dla niego konfiguracji biznesowej uwzględniając najlepsze praktyki branżowe oraz specyfikę operatora OSE.
O9.F34	Na docelowej platformie BSS należy wdrożyć proces "Proces gospodarka składnikami niskocennymi" na podstawie definicji opisanej w ramach rozdziału "Architektura biznesowa operatora OSE". Należy przeprowadzić analizę biznesową celem opracowania definicji procesu oraz określenia dla niego konfiguracji biznesowej uwzględniając najlepsze praktyki branżowe oraz specyfikę operatora OSE.

Rozwiązanie musi zapewniać wystarczającą wydajność dla procesów zgodnie z poniższymi parametrami

L.p.	Nazwa procesu	Ilość dzienna / miesięczna uruchomień procesu	Uwagi
1	Obieg dokumentów przychodzących	800 / 4000	
2	Umowy kosztowe nie PZP, podNASK	800 / 4000	
3	Umowy kosztowe nie PZP, nie NASK	800 / 4000	
4	Przyjęcie środka trwałego	800 / 4000	
5	Faktury przychodowe	2000 / 4000	

L.p.	Nazwa procesu	Ilość dzienna / miesięczna uruchomień procesu	Uwagi
6	Proces windykacji w OSE	100 / 500	

Wymagania w zakresie raportowania:

1. Raport „Faktury do wystawienia” jest podstawą do fakturowania płatnych usług OSE; *dot. PROCESU: faktury przychodowe*

Lp.	Zakres danych
1.	Dane odbiorcy faktury: pełna nazwa kontrahenta, ulica, numer, kod-pocztowy, miejscowość numer NIP RSPO
2.	Faktura elektroniczna: Tak Nie
3.	Dane, na które należy wysłać fakturę Adres @ (jeśli wysyłka elektroniczna =TAK) Adres wysyłki faktury (jeśli wysyłka elektroniczna =NIE) pełna nazwa kontrahenta, ulica, numer, kod-pocztowy, miejscowość
4.	Termin uruchomienia usługi
5.	Nazwa usługi i parametry usługi
6.	Typ rozliczenia: Opłata jednorazowa Opłata abonamentowa
7.	Okres rozliczeniowy: miesięczny
8.	Wynagrodzenie: określenie stawki podatku, kwoty netto za usługę, waluta: PLN
9.	Status windykacyjny Abonenta: zalega / nie zalega z płatnością
10.	Wysokość Kary Umownej (jeśli status: nie zalega z płatnością)

11.	Sposób obciążania opłatą: z góry do 5-go dnia miesiąca, lub w przypadku pierwszego miesiąca, w którym uruchomiona jest usługa: w terminie do 5-ciu dni od uruchomienia usługi
12.	Znacznik "usługa płatna" - ustawiany dla wszystkich usług płatnych, dostępu do internetu pow. 100 MB/s.

2. Raport „Wystawione faktury” jest podstawą do weryfikacji i monitorowania wystawionych faktur za płatne usługi OSE; *dot. PROCESU: faktury przychodowe*

Lp.	Zakres danych
1.	Data wystawienia faktury
	Dane odbiorcy faktury: pełna nazwa kontrahenta, ulica, numer, kod-pocztowy, miejscowość numer NIP RSPO
	Adres świadczenia usługi ulica, numer, kod-pocztowy, miejscowość
2.	Faktura elektroniczna: Tak Nie
3.	Termin uruchomienia usługi
4.	Nazwa usługi i parametry usługi
5.	Typ rozliczenia: Opłata jednorazowa Opłata abonamentowa
6.	Okres rozliczeniowy: miesięczny
7.	Wynagrodzenie: określenie stawki podatku, kwoty netto za usługę, waluta: PLN
8.	Sposób obciążania opłatą: z góry do 5-go dnia miesiąca, lub w przypadku pierwszego miesiąca, w którym uruchomiona jest usługa: w terminie do 5-ciu dni od uruchomienia usługi
9.	Termin płatności
10.	Adres e-mail w przypadku, gdy faktura elektroniczna = Tak

Dla powyższego ma być zapewniona możliwość raportowania:

- w skali: miesiąca, roku (pojedynczych lat), całego okresu trwania usługi
- z podziałem na rodzaj świadczonych odpłatnie usług
- per szkołę (RSPO), lokalizację (adres świadczenia usługi)

3. Raport - Umowy OSE; dot. PROCESU: Umowy kosztowe

Lp.	Zakres danych
1.	Nazwa Kontrahenta
2.	Nr zamówienia postępowania zakupowego (jeśli dotyczy)
3.	Data zawarcia Umowy
4.	Okres trwania Umowy: oznaczony (wartość), nieoznaczony
5.	Numer Umowy
6.	Projekty, których dotyczy
7.	Data wygaśnięcia Umowy (dla Umowy na czas oznaczony)

4. Raport - ŚT do amortyzacji dot. PROCESU: Przyjęcie ŚT

Lp.	Zakres danych
1.	Nazwa Kontrahenta
2.	Numer Umowy
3.	Data zawarcia Umowy
4.	Opis ŚT
5.	Ilość
6.	Wartość
7.	Nr dokumentu OT
8.	Data rozpoczęcia amortyzacji

5. Raport - Braki magazynowe dot. PROCESU: Przyjęcie ŚT

Lp.	Zakres danych
1.	Nazwa Kontrahenta

2.	Numer Umowy
3.	Data zawarcia Umowy
4.	Opis ŚT
5.	Ilość sztuk
6.	Ilość braków (szt)
7.	Nr dokumentu OT

6. Raport - zadłużenie Abonentów OSE; dot. PROCESU: Windykacja w OSE

Lp.	Zakres danych
1.	Nazwa szkoły
2.	NIP
3.	RSPO
4.	Wysokość zadłużenia
5.	Nr niepłaconej faktury/ faktur
6.	Adres e-mail szkoły
7.	Termin płatności (najstarszy w przypadku zaległości z kilku okresów rozliczeniowych)

7. Raport - Wezwania do zapłaty do wystawienia (Abonenci OSE); dot. PROCESU: Windykacja w OSE

Lp.	Zakres danych
1.	Dane odbiorcy faktury: pełna nazwa szkoły ulica, numer, kod-pocztowy, miejscowość numer NIP RSPO
2.	Wysokość zadłużenia
3.	Nr niepłaconej faktury/ faktur
4.	Adres e-mail szkoły
5.	Termin płatności (najstarszy w przypadku zaległości z kilku okresów rozliczeniowych)

8. Raport - Lista szkół do zawieszenia płatnych usług OSE; dot. PROCESU: Windykacja w OSE

Lp.	Zakres danych
1.	Dane odbiorcy faktury: pełna nazwa szkoły ulica, numer, kod-pocztowy, miejscowość numer NIP RSPO
2.	Nazwa Usługi (dodatkowa przepustowość)
3.	Adres świadczenia usługi ulica, numer, kod-pocztowy, miejscowość
4.	Termin płatności (najstarszy w przypadku zaległości z kilku okresów rozliczeniowych)
5.	Status windykacyjny Abonenta: zalega z płatnością ponad 21 dni

9. Raport - Usługi płatne OSE do wypowiedzenia dot. PROCESU: Windykacja w OSE

Lp.	Zakres danych
1.	Dane odbiorcy faktury: pełna nazwa szkoły ulica, numer, kod-pocztowy, miejscowość numer NIP RSPO
2.	Nazwa Usługi (dodatkowa przepustowość)
3.	Adres świadczenia usługi ulica, numer, kod-pocztowy, miejscowość
4.	Termin płatności (najstarszy w przypadku zaległości z kilku okresów rozliczeniowych)
5.	Status windykacyjny Abonenta: zalega z płatnością ponad 21 dni
6.	Wysokość zadłużenia
7.	Status usługi: zawieszona- windykacja
8.	Data zawieszenia usługi

10. Raport- zaangażowanie zasobów osobowych w OSE; dot. PROCESU: Rozliczanie projektu

Lp.	Zakres danych
-----	---------------

1.	Nazwa projektu
2.	Imię i nazwisko pracownika
3.	% zaangażowania
4.	Data powierzenia obowiązków: START
5.	Data powierzenia obowiązków: KONIEC

Raport per projekt/ per Pracownik (do weryfikacji, czy nie przekracza 100% zaangażowania pracując w kilku projektach)

11. Raport - rozliczenie dotacji celowej z MC; dot. PROCESU: *Rozliczanie projektu*

wg Załącznika nr 3 do Umowy Celowej;

12. Raport - rozliczenie dotacji z CPPC; dot. PROCESU: *Rozliczanie projektu*

w trakcie ustalania (trwa proces weryfikacji wniosków o dofinansowanie)

13. Raport Usługi Płatne

Lp.	Zakres danych
1	Nazwa Płatnika Ulica Płatnika Nr. domu Płatnika Nr. lokalu płatnika Kod pocztowy Płatnika Miejscowość Płatnika NIP Płatnika RSPO Szkoły ID Abonenta
2	Adres świadczenia usługi Faktura elektroniczna: TAK, NIE Adres e-mail Odbiorcy (wypełnione, gdy TAK faktura elektroniczna) Nazwa Odbiorcy Ulica Odbiorcy Nr. domu Odbiorcy Nr. lokalu Odbiorcy Kod pocztowy Odbiorcy Miejscowość Odbiorcy ID Odbiorcy
3	Data uruchomienia usługi Nazwa usługi: Dostęp o zwiększonej przepustowości Parametry usługi - Prędkość Miesiąc świadczenia usługi Początek okresu świadczenia usługi w danym miesiącu: data uruchomienia lub początek miesiąca Koniec okresu świadczenia usługi w danym miesiącu: koniec miesiąca Pierwsza faktura: TAK, NIE Typ rozliczenia: Pierwsza faktura, Zmieniona opłata (aneks do umowy); Opłata abonamentowa (kolejna

Lp.	Zakres danych
	faktura) Kwota netto Stawka VAT Kwota brutto Okres rozliczeniowy: Miesięczny
4	Informacja o złożonej reklamacji: Złożona, rozpatrywana, uznana reklamacja, reklamacja nieuznana Kwota netto uznanej reklamacji Stawka Vat uznanej reklamacji Kwota brutto uznanej reklamacji Data uznania reklamacji Miesiąc uznanej reklamacji Kwota netto - Kwota netto uznanej reklamacji Stawka Vat Kwota brutto - Kwota netto uznanej reklamacji
5	Numer faktury Data sprzedaży Miejsce wystawienia faktury Data wystawienia faktury Forma płatności: Przelew Ilość dni do zapłaty: 21 Termin płatności Wartość netto Stawka Vat Wartość brutto Data wysyłki faktury Informacja o wysokości nieuregulowanych płatnościach

KPI

1) Zakupy:

- Śr czas procesu zakupowego od ogłoszenia do otwarcia ofert
- Śr czas procesu zakupowego od ogłoszenia do rozstrzygnięcia
- % unieważnionych przetargów
- Terminowość przetargów (brak przedłużeń)

2) Faktury przychodowe

- Terminowość wystawiania faktur (% wystawionych faktur w ciągu regulaminowego czasu na wystawienie faktury w stosunku do wszystkich wystawionych w okresie rozliczeniowym faktur)

- % zafakturowania opłat jednorazowych (liczba wystawionych faktur za opłaty jednorazowe w stosunku do liczby uruchomionych usług w danym okresie rozliczeniowym z uwzględnieniem czasu na wystawienie faktury)
- % Faktur elektronicznych (% faktur wystawionych elektronicznie w stosunku do wszystkich wystawionych faktur w okresie rozliczeniowym)
- Terminowość płatności faktur przychodowych OSE (liczba) - stosunek liczby faktur opłaconych w terminie do wszystkich wystawionych faktur w okresie rozliczeniowym (%)
- Terminowość płatności faktur przychodowych OSE (wartość) - stosunek wartości faktur opłaconych w terminie do wartości wszystkich wystawionych faktur w okresie rozliczeniowym (%)

3) Faktury kosztowe OSE

- Terminowość płatności faktur kosztowych OSE (liczba) - stosunek liczby faktur opłaconych w terminie do wszystkich otrzymanych faktur w okresie rozliczeniowym (%)
- Terminowość płatności faktur kosztowych OSE (wartość) - stosunek wartości faktur opłaconych w terminie do wartości wszystkich otrzymanych faktur w okresie rozliczeniowym (%)
- % opłaconych faktur (liczba) - stosunek liczby faktur opłaconych do wszystkich otrzymanych faktur liczone na dany moment (%), dla całego CB i w podziale na projekty
- % opłaconych faktur (wartość) - stosunek wartości faktur opłaconych do wartości wszystkich otrzymanych faktur liczone na dany moment (%), dla całego CB i w podziale na projekty
- Księgowanie faktur - liczba zaksięgowanych faktur OSE do liczby wszystkich otrzymanych faktur OSE (%)

7.2.10. Proces marketingu i komunikacji

Wymagana jest realizacja następujących wymagań:

Nr wymagania	Treść wymagania
O10.F1	Należy zapewnić możliwość konfigurowania stopki dla wszelkiej komunikacji mailowej realizowanej przez systemy operatora OSE. Konfiguracja musi umożliwiać przechowywanie historii wykorzystywanych stopek wraz z informacją o datach, w jakich były aktywne.
O10.F2	Należy zapewnić, aby szablony dokumentów wykorzystywane do generowania dokumentów mogły zawierać znaki graficzne związane z marką NASK PIB
O10.F3	Konfiguracja stopki w komunikacji mailowej powinna umożliwiać ustawienie zarówno części tekstowej jak i graficznej i być dostępna dla uprawnionych użytkowników biznesowych
O10.F4	Musi być możliwe ustawienie w konfiguracji daty (i czasu), od jakiego ma obowiązywać nowy wzór stopki.
O10.F5	Musi być możliwe natychmiastowe włączenie nowego szablonu (stopki) komunikacji mailowej

Nr wymagania	Treść wymagania
O10.F6	Na ekranach logowania musi być możliwość wyświetlenia logo OSE z pliku graficznego na podstawie informacji z konfiguracji. Musi być możliwa obsługa plików graficznych w formacie .jpg, .bmp, .gif, .png.
O10.F7	Zastosowanie nowego (lub zmiana istniejącego) szablonu dokumentu lub stopki dla komunikacji mailowej musi być możliwe do realizacji bez konieczności jakichkolwiek prac administracyjnych (np. restartu serwera, wyczyszczenia cache itp.)

7.3. Opis funkcjonalności dla całego rozwiązania

7.3.1. Silnik Procesów Biznesowych

Podstawą realizacji procesów biznesowych w systemach OSE jest Silnik Procesów Biznesowych, który musi spełniać następujące wymagania

Nr wymagania	Treść wymagania
O41.F1	Silnik procesów biznesowych musi zawierać funkcjonalność lejka umożliwiającą ograniczenie ilości jednoczesnego przetwarzania procesów w kontekście poszczególnych wywoływanych integracji. Musi być możliwość skonfigurowania ilości wywołań dla każdego interfejsu z systemem w liczbie wywołań na sekundę / minutę. W przypadku spiętrzenia procesów umożliwi to stopniowe - kontrolowane rozładowywanie zatorów w procesach.
O41.F2	Rozwiązanie musi zawierać funkcjonalności dostosowujące przetwarzanie do wydajności ograniczając liczbę jednoczesnych wywołań / wykonań procesów do zadanego limitu (procesów i lub obciążenia systemu).
O41.F3	Rozwiązanie musi umożliwiać nadawanie priorytetów procesom (definicjom procesów) a następnie przetwarzanie instancji (uruchomień) procesów zgodnie z priorytetami od najwyższego do najniższego.
O41.F4	Rozwiązanie musi umożliwiać manualne nadawanie priorytetów instancjom procesów zarówno pojedynczym jak i grupowe na podstawie odpowiednich filtrów. Następnie instancje powinny być przetwarzane od zgodnie z priorytetem od najwyższego do najniższego.
O41.F5	Rozwiązanie musi zawierać funkcjonalność do monitorowania przetwarzania procesów umożliwiające zarówno śledzenie stanu obecnego jak i trendów. Wyniki monitorowania muszą być prezentowane w formie graficznej pozwalając na weryfikację poziomu i trendu zamówień uwzględniając odpowiednie przekroje zamówień (filtry) (np. regionalne, czy typu procesów)
O41.F6	Rozwiązanie musi umożliwić konfigurację alarmów w ramach monitorowania procesów. Alarmy muszą być możliwe do ustawienia zarówno dla przypadków przekroczenia poziomu (np. oczekujących zamówień dla regionu) jak i w przypadku wystąpienia trendów (np. lawinowo rosnącego poziomu procesów oczekujących, co w ciągu np. godziny może doprowadzić do poziomu przekraczającego wydajność systemu)

Nr wymagania	Treść wymagania
O41.F7	Rozwiązanie musi zawierać mechanizm do obsługi błędów przetwarzania pozwalający na skonfigurowanie zachowań dla konkretnych błędów (np.. Błąd A zatrzymuje zamówienie, błąd B ponowienie kroku)
O41.F8	Rozwiązanie musi zawierać mechanizm umożliwiający masowe wznawianie błędnych zamówień np. Po usunięciu błędu, lub po modyfikacji zawartości zamówień - poprzez wskazanie błędu, dla jakiego wznowić zamówienia.
O41.F9	Rozwiązanie musi zawierać funkcjonalność umożliwiającą modyfikację zawartości pojedynczych zamówień z poziomów GUI jak również do masowej modyfikacji błędnych zamówień zgrupowanych w ramach filtra (np.. Kodu błędu)
O41.F10	Silnik Procesów Biznesowych musi zawierać graficzny edytor umożliwiający tworzenie i modyfikowanie procesów biznesowych. W sytuacji, gdy proces można zrealizować w oparciu o istniejące interfejsy / funkcjonalności operacja taka musi być możliwa do przeprowadzenia przez użytkownika biznesowego bez konieczności modyfikacji kodu.

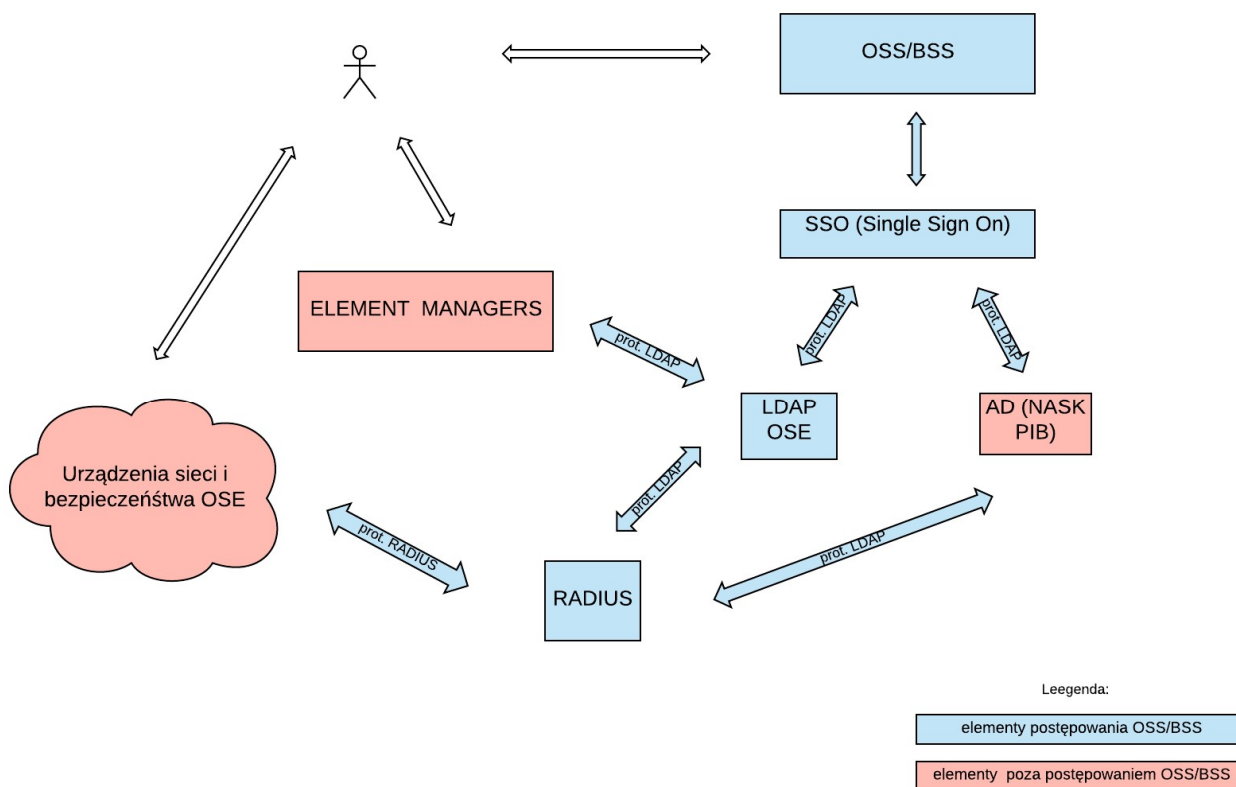
7.3.1. Uwierzytelnianie i autoryzacji dla użytkowników wewnętrznych i dla partnerów OSE

Wdrożenie systemów OSS/BSS wraz infrastrukturą musi zapewnić uwierzytelnienie i autoryzację użytkowników systemów OSS/BSS oraz uwierzytelnienie użytkowników Element Manager'ów do urządzeń sieci i bezpieczeństwa, użytkowników systemów bezpieczeństwa (np. SIEM i SWG) oraz w dostępie do urządzeń OSE. Funkcjonalność pojedynczego logowania SSO musi być zapewniona w dostępie do systemów OSS/BSS. System SSO musi być zintegrowany z katalogiem użytkowników Zamawiającego AD (Active Directory) oraz z dedykowanym katalogiem użytkowników dla partnerów OSE (np. LDAP) również zaimplementowanym przez Wykonawcę.

W ramach systemu uwierzytelnienia i autoryzacji Wykonawca jest zobowiązany do wdrożenia serwera autoryzacji do urządzeń sieciowych i urządzeń bezpieczeństwa w sieci szkieletowej OSE oraz do urządzeń CPE w lokalizacjach szkolnych (serwer Radius). Serwer ten musi być zintegrowany z ww. repozytoriami AD i LDAP.

W ramach wdrożenia sieci OSE planowane jest w przyszłości wdrożenie centralnego systemu uwierzytelniania użytkowników wewnętrznych i zewnętrznych operatora OSE - System Zarządzania Tożsamością (kupowany w oddzielnym postępowaniu zakupowym). W związku z tym należy zagwarantować zdolność techniczną Rozwiązania do przełączenia w łatwy sposób na korzystanie z tego systemu.

Architektura systemu uwierzytelnienia i autoryzacji użytkowników OSE przedstawiona jest na schemacie poniżej:



Zatem muszą być spełnione poniższe wymagania :

Nr wymagania	Treść wymagania
O42.F1	Wszystkie systemy w ramach Rozwiązania lub Rozwiązanie, jako całość musi zapewnić uwierzytelnianie i autoryzację użytkowników z uwzględnieniem grup i ról użytkowników (zgodnie z metodą RBAC - Role Based Access Control) oraz dostęp tylko do tych zasobów, do których użytkownicy mają uprawnienia.
O42.F2	Wszystkie systemy w ramach Rozwiązania będą korzystać z jednego systemu autoryzacji i uwierzytelniania zwanym dalej Systemem Autoryzacji, który jest wymagany, jako integralna część oferowanego Rozwiązania.
O42.F3	Wszystkie systemy Rozwiązania mają zdolność korzystania z zewnętrznego systemu autoryzacji (potencjalnie dostarczonego w przyszłości przez Zamawiającego) wraz z funkcjonalnością SSO na podstawie standardów wymienionych w O42.F5 i O42.F15.
O42.F4	System Autoryzacji w Rozwiązaniu musi być przeznaczony do autoryzacji użytkowników OSE w tym pracowników NASK i partnerów NASK. Zamawiający nie przewiduje użytkowania Systemu

Nr wymagania	Treść wymagania
	Autoryzacji na potrzeby portalu usługowego OSE; System Autoryzacji i utrzymania sesji (Single Sign On) służyć ma dla potrzeb wewnętrznych użytkowników systemów BSS/OSS. Nie jest planowane użycie modułu SSO Rozwiązania na potrzeby Portalu OSE jednak Zamawiający nie blokuje takiej możliwości Wykonawcy, jeśli uzna on ją za konieczną w architekturze Rozwiązania.
O42.F5	System Autoryzacji umożliwi autoryzację się również zewnętrznym elementom dla Rozwiązania, takim jak Element Managery oraz urządzenia bezpieczeństwa. System Autoryzacji musi umożliwić komunikację z systemami zewnętrznymi poprzez a) moduł Radius będący częścią rozwiązania b) bezpośrednio protokołem LDAP. Nie jest wymagane przeniesienie sesji bez powtórного logowania dla urządzeń zewnętrznych.
O42.F6	Zamawiający może w przyszłości podjąć decyzję o wprowadzeniu zewnętrznego System Tożsamości OSE (SSO). Rozwiązanie powinno być otwarte na taką możliwość i zapewniać możliwość przezroczystego uwierzytelniania swoich użytkowników i administratorów za pomocą mechanizmu typu Single Sign On przy wykorzystaniu protokołu SAML w wersji 2.0. Profile SAML SSO muszą wspierać przynajmniej: Web Browser SSO Profile Enhanced Client or Proxy (ECP) Profile Identity Provider Discovery Profile Single Logout Profile Name Identifier Management Profile
O42.F7	Rozwiązanie musi umożliwiać Zamawiającemu upload pliku xml zawierającego metadane serwera służącego, jako Identity Provider (IdP) lub umożliwiać pobranie takiego pliku bezpośrednio z serwera IdP. Po wgraniu takiego pliku System musi odbierać tokeny protokołu SAML ze skonfigurowanego serwera IdP i na ich podstawie wykonywać uwierzytelnianie użytkowników.
O42.F8	Rozwiązanie musi umożliwiać obsługę skonfigurowanych po stronie IdP i zdefiniowanych przez Zamawiającego pól, które nie wchodzą w skład domyślnej konfiguracji tokenu SAML (custom attributes)
O42.F9	Użytkownicy systemów Jira WF, Jira SD, Jira Insight, które mają być uruchomione w fazie 1 wdrożenia i działać aż do fazy 2 wdrożenia muszą być autoryzowani i uwierzytelniani przy pomocy istniejącego u Zamawiającego systemu Active Directory (AD) .
O42.F10	Dostawca zainstaluje wybrany przez siebie moduł Jira SSO tylko na potrzeby instancji systemu Jira i przeprowadzi niezbędne prace integracyjne między instancjami.
O42.F11	System autoryzacji musi umożliwiać tworzenie i zarządzanie: rolami, zasobami, aplikacjami, grupami użytkowników
O42.F12	Każdy niezależny system zamawianego Rozwiązania (poza portalem OSE) powinna wspierać funkcjonalność „Single-Sign-On” polegającej na jednorazowej autoryzacji w Systemie Autoryzacji tylko jeden raz w trakcie trwania sesji użytkownika niezależnie z ilu aplikacji oferowanego rozwiązania będzie korzystał.
O42.F13	System Autoryzacji musi umożliwiać tworzenie i zarządzanie: rolami, zasobami, aplikacjami, grupami użytkowników
O42.F14	System Autoryzacji musi definiować typy dostępu do zasobu: odczyt/zmiana/usunięcie/inne

Nr wymagania	Treść wymagania
O42.F15	System Autoryzacji musi wspierać przynajmniej jeden z następujących standardów: <ul style="list-style-type: none"> • SAML 2.0 • OAuth • OpenID
O42.F16	System Autoryzacji musi w bezpieczny i zaszyfrowany sposób przechowywać dane użytkowników i ich hasła
O42.F17	System Autoryzacji musi umożliwiać definiowanie polityk zarządzania hasłami
O42.F18	Polityki tworzenia haseł Systemu Autoryzacji powinny móc zawierać ograniczenia i wymuszenia, co do kategorii stosowanych znaków i ich ilości (minimalna ilość znaków specjalnych, cyfr itd.)
O42.F19	Polityki zarządzania hasłami Systemu Autoryzacji powinny wymuszać zmianę hasła po upływie konfigurowalnego w systemie czasu
O42.F20	Polityki zarządzania hasłami Systemu Autoryzacji powinny uniemożliwiać zmianę hasła na jedno z X haseł poprzednich, gdzie X powinno być konfigurowalne
O42.F21	Polityki zarządzania zmianą hasła oraz złożoności hasła (dwa powyższe punkty) mogą być aplikowane per grupa użytkowników
O42.F22	System Autoryzacji musi posiadać bezpieczną procedurę tworzenia hasła początkowego, jego przekazania użytkownikowi i wymuszenia zmiany po pierwszym użyciu.
O42.F23	System Autoryzacji musi mieć możliwość wymuszenia zmiany hasła dla danego użytkownika lub grupy użytkowników na żądanie administratora systemu.
O42.F24	System Autoryzacji musi dostarczać silnik zarządzania politykami - regułami dostępu
O42.F25	Silnik zarządzania politykami musi umożliwiać definicję zasobów, aplikacji, uprawnień, typów uprawnień.
O42.F26	Silnik zarządzania politykami musi umożliwiać dodawanie uprawnień do danych zasobów i aplikacji na podstawie: <ul style="list-style-type: none"> - grup użytkowników - zakresów IP - typu klienta (przeglądarka, aplikacja mobilna itd.)
O42.F27	Silnik zarządzania politykami musi umożliwiać stworzenie dowolnej ilości polityk
O42.F28	System Autoryzacji musi udostępniać API dla systemów zewnętrznych umożliwiające autentykację i zapytania o uprawnienia do zasobów
O42.F29	System Autoryzacji musi móc obsługiwać więcej niż jedno repozytorium grup i użytkowników, w szczególności mogą to być jednocześnie repozytoria typu: <p>LDAP</p> <p>AD</p> <p>SQL</p>
O42.F30	System Autoryzacji musi umożliwiać dodawanie, usuwanie i modyfikację użytkowników i grup w dowolnym z podłączonych repozytoriów

Nr wymagania	Treść wymagania
O42.F31	System Autoryzacji musi umożliwiać wyszukiwanie grup, użytkowników, aplikacji, uprawnień i zasobów według wzajemnych relacji takich jak: użytkownicy z danej grupy, użytkownicy z przydzielonym uprawnieniem do danego zasobu, grupa zasobów per system itd.
O42.F32	Delegowani użytkownicy powinni móc zarządzać całością uprawnień dla grup i użytkowników do wybranych aplikacji i zasobów; Delegacja uprawnień administracyjnych per aplikacja/obszar aplikacji.
O42.F33	Delegowani użytkownicy powinni móc tworzyć grupy i nowych użytkowników
O42.F34	Delegowani użytkownicy powinni móc tworzyć zasoby w ramach aplikacji.
O42.F35	System Autoryzacji musi definiować następujące typy dostępu do zasobów, operacji i aplikacji: - użytkownik może dokonać operacji na danym zasobie tylko, jeśli ma wprost przydzielone uprawnienie do działania na tym zasobie - użytkownik może dokonać operacji na danym zasobie za zgodą innego użytkownika (model jednorazowej akceptacji przez przełożonego); wielostopniowa autoryzacja operacji
O42.F36	System Autoryzacji musi umożliwiać procedurę czasowej delegację uprawnień z jednego użytkownika na drugiego za zgodą użytkownika trzeciego (transfer uprawnień na czas urlopu)
O42.F37	System Autoryzacji musi umożliwiać czasowe blokowanie kont przez administratorów oraz ich odblokowywanie.
O42.F38	System Autoryzacji musi umożliwiać czasowe blokowanie kont z zadanej grupy użytkowników przez administratorów oraz ich podobne odblokowywanie
O42.F39	System Autoryzacji musi przechowywać logi pełnej historii zdarzeń takich, jak (ale nieograniczonych do): logowanie i próby logowania, operacje na zasobach – typu odczyt, modyfikacja, zapis, modyfikacje uprawnień użytkowników, dodawanie grup i użytkowników, kasowanie obiektów, autoryzacje do konkretnych aplikacji.
O42.F40	Logi powinny przechowywać typ klienta, z którego dokonywano w/w operacji, login name, adres IP/hostname źródłowy, czas/timestamp logowania (próby udane i nieudane), timestamp dokonywanych operacji
O42.F41	Parametry przechowywane w logach powinny być konfigurowalne
O42.F42	System musi umożliwiać raportowanie dostępu i operacji z filtrowaniem per zasób, aplikacja, grupa, zakres czasowy itp.

7.3.2. Automatyzacja, integracja i elastyczność całości rozwiązania

Sposoby i poziomy integracji docelowego stosu systemów OSS/BSS z systemami i urządzeniami OSE i NASK, elastyczność Rozwiązania oraz automatyzacja zarówno integracji jak i wewnętrznych procesów Rozwiązania musi być maksymalna ze względu na skalę sieci OSE i potencjalną złożoność funkcjonalności, jaką sieć OSE będzie udostępniać.

Identyfikator wymagania	Treść wymagania
O43.F1	Rozwiązanie musi się cechować maksymalnym stopniem automatyzacji zadań zarówno w obszarze technicznej obsługi sieci jak i w obszarze procesów biznesowych - w szczególności zadań związanych z podłączaniem szkół do OSE jak i utrzymywaniem świadczonych usług OSE a także komunikacji z partnerami NASK i ich rozliczaniem
O43.F2	Z punktu widzenia Operatora OSE Rozwiązanie ma być spójną platformą systemową i aplikacyjną, wewnętrznie integrującą wszystkie wymagane funkcjonalności
O43.F3	Dostawca musi dostarczyć w ramach Rozwiązania kompletną platformę, co oznacza dopasowane środowisko aplikacyjne, systemowe, wirtualizacyjne i sprzętowe tak by spełniało wszystkie wymagania Zamawiającego
O43.F4	Rozwiązanie musi pozwalać na elastyczne definiowanie, co najmniej następujących elementów: <ul style="list-style-type: none"> - scenariuszy provisioningu - scenariuszy pomiarów - urządzeń OSE stawianych w szkole - urządzeń szkieletowych - systemów sieciowych i bezpieczeństwa - łącz fizycznych i logicznych - usług świadczonych przez OSE i usług wewnętrznych w ramach systemów nadzoru operatora OSE - workflow dla procesów biznesowych - statystyk i raportów - pól dla danych wykorzystywanych w systemach OSS i BSS - słowników stosowanych w systemach OSS/BSS - szablonów dokumentów - kampanii mailingowych
O43.F5	Rozwiązanie musi być gotowe na komunikację z urządzeniami OSE przy użyciu standardowych mechanizmów : <ul style="list-style-type: none"> - SNMP - Syslog - Netconf - Telnet - SSH - HTTP - REST API - pliki standardowe TXT, CSV XML (np. pliki konfiguracyjne)
O43.F6	Rozwiązanie musi być gotowe na integracje przy użyciu standardowych mechanizmów integracji z systemami : <ul style="list-style-type: none"> - Element Managerami urządzeń sieciowych i bezpieczeństwa, - systemami bezpieczeństwa i sieci (SIEM, SWG, DNS, anty-DDos) - systemami zewnętrznymi (NASK OSE) - przy pomocy protokołu SNMP - przy pomocy protokołu Syslog - poprzez wymianę plików w standardowych formatach (co najmniej CSV, JSON, XML) - poprzez API (co najmniej REST API, SOAP)

Identyfikator wymagania	Treść wymagania
O43.F7	<p>Docelowe Rozwiązanie musi być gotowe na integracje przy użyciu standardowych mechanizmów integracji i komunikacji z obecnymi systemami BSS Zamawiającego:</p> <ul style="list-style-type: none"> - pliki w standardowych formatach (co najmniej CSV, JSON, XML, XLS) - co najmniej REST API i SOAP - HTTP/HTTPS np. przekierowanie stron - na poziomie baz danych (ODBC, JDBC, skrypty SQL, inne) - na poziomie wymiany poczty elektronicznej (protokół SMTP)
O43.F8	<p>Rozwiązanie zaimplementowane przez Wykonawcę w fazie 1 i 2 wdrożenia, oparte na systemach Jira WF, Jira SD oraz Jira Insight, Provisioning musi zapewniać integrację z systemami OSS i BSS Zamawiającego w szczególności w zakresie BSS z systemami :</p> <ul style="list-style-type: none"> - sugarCRM, - Portal OSE, - Emid, - Teta, - Reporting Services, - Contact Center Alvafox (system poza NASK - usługa świadczona Zamawiającemu przez Dostawcę usługi)
O43.F9	<p>W ramach integracji w fazach 1-2 wdrożenia Rozwiązanie musi zapewniać użycie, co najmniej następujących mechanizmów:</p> <ul style="list-style-type: none"> - REST API , SOAP - plików o standardowych formatach (np. CSV, JSON, XML, XLS) - na poziomie baz danych (ODBC, JDBC, skrypty SQL, inne) - na poziomie wymiany poczty elektronicznej (protokół SMTP) - skryptów integracyjnych NASK - skryptów integracyjnych napisanych przez Wykonawcę
O43.F10	<p>Rozwiązanie musi zapewniać płynną skalowalność, dla co najmniej 20-to krotnego zwiększenia liczby użytkowników systemów, co oznacza, że przy liniowym zwiększaniu zasobów infrastrukturalnych proporcjonalnie do przyrostu użytkowników nie wystąpi spadek wydajności.</p>

7.3.3. Centralny System Raportowy

Centralny System Raportowy OSE będzie wykorzystywany do generowania wszystkich raportów : finansowych, operacyjnych, SLA, rozliczeniowych, performance'owych a także raportów bezpieczeństwa w szkołach. Część z tych raportów będzie znana na etapie ogłoszenia postępowania zakupowego w i zaimplementowana zgodnie z harmonogramem wdrożenia a część będzie powstawała ad hoc. zgodnie z potrzebami operatora OSE.

Identyfikator wymagania	Treść wymagania
O45.F1	Centralny System Raportowy (CSR) musi być narzędziem w formie hurtowni danych do elastycznego generowania raportów bazujących na danych z systemów OSS i BSS oraz pozwalającym na prowadzenie analizy biznesowej.
O45.F2	Funkcjonalność Centralnego Systemu Raportowego musi umożliwiać zaplanowanie uruchomienia raportów na wskazaną datę i czas, z możliwością cyklicznego uruchamiania raportów, co wskazany okres czasu w dniach, miesiącach, latach.
O45.F3	Funkcjonalność CSR musi umożliwiać konfiguracyjne zdefiniowanie sposobu dostarczenia raportu do użytkowników poprzez: <ul style="list-style-type: none"> - zdefiniowanie odbiorców raportu - zdefiniowanie sposobu dostarczenia (raport poprzez email, notyfikacja poprzez email - raport dostępny w systemie, raport dostępny w systemie)
O45.F4	CSR musi zawierać panel (GUI) umożliwiający konfigurację sposobu uruchamiania i dostarczania raportów.
O45.F5	CSR musi umożliwiać samodzielne tworzenie raportów przez użytkowników biznesowych przy wykorzystaniu odpowiedniego panelu użytkownika (GUI)
O45.F6	Wykonawca na etapie postępowania zakupowego otrzyma listę zdefiniowanych już raportów oraz liczbę nowych raportów, które mogą pojawić się do implementacji w trakcie wdrożenia i utrzymania powdrożeniowego Rozwiązania i które Wykonawca będzie musiał skonfigurować. Wymaganie to nie blokuje możliwości konfigurowania raportów w okresie powdrożeniowym przez uprawnionych użytkowników systemu oraz zamawianie kolejnych raportów w cenach wynikających z oferty.
O45.F7	Rozwiązanie musi być tak zaimplementowane by Centralny System Raportowy miał wbudowaną możliwość pobierania danych z innych elementów Rozwiązania (poprzez ETL) , co najmniej : <ul style="list-style-type: none"> - dane z systemu Fault Management - dane z systemu Performance Management - dane z systemu Inventory - dane z systemów BSS (obszar CRM, obszar PRM, obszar Service Desk, Trouble Ticketing, rozliczenia, zamówienia, produkty) - dane pośrednio uzyskane z systemów zintegrowanych z systemami BSS: - dane na temat rozliczeń z partnerami OSE (dostawcy sprzętu, dostawcy łącz, podwykonawcy) - dane na temat zamówień (łącz i prac u podwykonawców) - dane na temat faktur przychodowych i kosztowych oraz ich rozliczeń - dane na temat stanów magazynowych
O45.F8	Centralny System Raportowy musi pozwalać na zasilanie go danymi do raportu pochodzącymi z systemów OSE NASK i NASK na wiele różnych sposobów: <ul style="list-style-type: none"> - zasilanie batchowe z plików płaskich - zasilanie przy użyciu API Systemu - zasilanie na poziomie bazy danych (ODBC, JDPC, skrypty SQL, inne)
O45.F9	Centralny System Raportowy musi mieć możliwość pobierania przez niego danych z zewnątrz, (z systemów w ramach Rozwiązania jak i z systemów Zamawiającego) poprzez : <ul style="list-style-type: none"> - integrację na poziomie baz danych - pobieranie jednorazowe oraz cykliczne

Identyfikator wymagania	Treść wymagania
	- integrację na poziomie wymiany plików w standardowych formatach W ramach pobierania musi być możliwa transformacja danych źródłowych do modelu docelowego (ETL).
O45.F10	Centralny System Raportowy musi mieć możliwość definiowania przez administratora szablonów szaty graficznej a w szczególności logo do wykorzystania w raportach
O45.F11	Centralny System Raportowy powinien zapewnić przechowywanie danych historycznych (nieaktualnych) przez co najmniej 3 lata od ich zmiany, natomiast w przypadku danych finansowych przez co najmniej 5 lat.
O45.F12	Centralny System Raportowy musi przechowywać, co najmniej dane wskazane w architekturze danych operatora OSE oraz wymagane do generowania wyspecyfikowanych raportów.

7.3.4. Integracja z systemami zewnętrznymi

Aby pokazać złożoność i mnogość integracji systemu OSS/BSS z systemami NASK OSE i NASK poniżej wylistowane zostały niezbędne do implementacji integracje z konkretnymi systemami :

systemy NASK OSE

- do 18 Element Managerów do ADC (w 16 węzłach regionalnych i w 2 centralnych)
- do 16 Element Managerów do systemu SWG (w 16 węzłach regionalnych)
- do 18 Element Managerów do systemów NG Firewall (w 16 węzłach regionalnych i w 2 węzłach centralnych)
- 2 instancje Element Managera do urządzeń sieciowych (w 2 węzłach centralnych - jedna zapasowa, zakładamy jednego producenta)
- 2 instancje Element Managera do Systemu Zarządzania Tożsamością (w 2 węzłach centralnych, implementacja w dalszych etapach projektu, zakup Systemu Zarządzania Tożsamością w odrębnym postępowaniu zakupowym)
- 2 instancje Element Managera do SIEM (w 2 węzłach centralnych) - w przypadku SIEM istotny jest fakt, że w ramach SIEM będzie uruchomiony System Retencji Logów i że logi spływające z CPE do tego systemu będą forwardowane z niego do do Systemu Fault Managemet
- 2 instancje Element Managera do systemu DNS (w 2 węzłach centralnych)
- 2 instancje Portalu OSE (w 2 węzłach centralnych - jedna zapasowa)
- 2 instancje Systemu Zarządzania Kolokacjami (zakup systemu w odrębnym postępowaniu zakupowym, jedna zapasowa)
- 2 instancje systemu anti-DDoS (w 2 węzłach centralnych, system developowany przez pracowników NASK PIB)
- 1 instancja Jira

systemy NASK PIB

- sugarCRM (system crm'owy NASK PIB)

- Teta (system finansowo-księgowy NASK PIB)
- Emid (system magazynowy NASK PIB)
- Confluence Tree (system z bazą wiedzy NASK PIB)
- Active Directory (repozytorium użytkowników - pracownicy NASK PIB)
- Reporting Services (centralny system raportowy NASK PIB)

Podobszar / Proces	Identyfikator wymagania	Treść wymagania
Integracja Portal OSE	O44.F1	Rozwiązanie (Portal Usługowy) musi zostać zintegrowane z Portalem OSE w ramach następujących obszarów: - Użytkownicy (Tworzenie, Edycja danych, zarządzanie rolami) - integracja danych użytkowników, dla których bazą master jest Portal OSE - Szkoły (Pobieranie informacji) - bazą master jest system CRM Rozwiązania - Logowanie - w ramach logowania na Portalu Usługowym dokonywana jest weryfikacja użytkownika i hasła w Portalu OSE, w odpowiedzi przesyłana jest lista szkół użytkownika i jego role w poszczególnych szkołach
Integracja Portal OSE	O44.F2	Rozwiązanie (Portal Usługowy) musi być zintegrowane z Portalem OSE na poziomie synchronizacji użytkowników Portalu OSE. Portal Usługowy musi posiadać bazę użytkowników, która jest podzbiorem bazy użytkowników Portalu OSE - użytkownicy ci są zapisywani w obszarze CRM, jako osoby kontaktowe w szkołach z uwzględnieniem ról tych użytkowników (co najmniej: dyrektor, techniczny reprezentant szkoły, koordynator OSE w szkole, koordynator OSE w OPS) i ich uprawnień w stosunku do inicjowanych procesów biznesowych. W szczególności musi być możliwość automatycznego : - zakładania z procesów biznesowych OSE użytkowników na Portalu OSE (i z niego na Portalu Usługowym) - zakładania/modyfikacji osób kontaktowych w CRM w wyniku zakładania/modyfikacji użytkowników na Portalu OSE. Portal OSE jest miejscem zarządzania danymi do logowania dla użytkowników (login, hasło, przypisanie wszystkich ról do szkół)
Integracja Portal OSE	O44.F3	W przypadku danych zesłownikowanych wymienianych między Portalem OSE a Rozwiązaniem musi być zapewniona implementacja w Rozwiązaniu istniejących już w środowisku Operatora OSE słowników oraz gotowość na elastyczne definiowanie kolejnych słowników
Integracja Portal OSE	O44.F4	Rozwiązanie musi umożliwiać integrację z Portalem OSE poprzez standardowe protokoły i otwarte mechanizmy integracyjne oraz osadzanie raportów z systemów OSS/BSS w Portalu OSE. Muszą być wspierane następujące mechanizmy integracji:

Podobszar / Proces	Identyfikator wymagania	Treść wymagania
		<ul style="list-style-type: none"> - pliki w standardowych formatach (co najmniej CSV, JSON, XML, HTML) - REST API, SOAP - osadzanie gotowych raportów i plików graficznych - na poziomie baz danych : dostęp z poziomu dedykowanego użytkownika, ODBC, JDBC, skrypty SQL <p>Preferowanym sposobem integracji jest REST API i wymiana plików Portal OSE oparty jest na bazie Postgres</p>
Integracja EMID	O44.F5	<p>Rozwiązanie musi zostać zintegrowane z systemem EMID umożliwiając aktualizację danych magazynowych na podstawie działań realizowanych w Rozwiązaniu. Należy uwzględnić ewentualną możliwość niedostępności systemu EMID umożliwiając dosłanie informacji po ponownej dostępności systemu (wykorzystując interfejsy asynchroniczne).</p>
Integracja EMID	O44.F6	<p>Rozwiązanie musi umożliwiać integrację z systemem EMID poprzez standardowe protokoły i otwarte mechanizmy integracyjne. Muszą być wspierane następujące mechanizmy integracji:</p> <ul style="list-style-type: none"> - wymiana plików w standardowych formatach (co najmniej XLS, CSV, JSON, XML) - Webservices - na poziomie baz danych : dostęp do tabel z widokami z poziomu dedykowanego użytkownika -przy pomocy wymiany poczty elektronicznej w procesie biznesowym do osób będącymi uprawnionymi użytkownikami systemu Emid <p>Preferowanym sposobem integracji jest dostęp na poziomie baz danych i wymiana plików</p> <p>system EMID jest zaimplementowany na bazie MSSQL</p>
Integracja TETA	O44.F7	<p>Należy zapewnić integrację z systemem TETA wysyłając dane wystawionych dokumentów finansowych umożliwiając realizację procesów związanych z ustawą o rachunkowości w tym systemie. Należy uwzględnić ewentualną możliwość niedostępności systemu TETA umożliwiając dosłanie informacji po ponownej dostępności systemu (wykorzystując interfejsy asynchroniczne).</p>
Integracja TETA	O44.F8	<p>Należy zapewnić integrację z systemem TETA umożliwiając synchronizację bazy kontrahentów w oparciu o przetwarzanie batchowe i interfejsy asynchroniczne.</p>
Integracja TETA	O44.F9	<p>Rozwiązanie musi zostać integrowane z systemem TETA przy użyciu mechanizmów integracyjnych wspieranych przez Teta .</p> <p>W celach integracji należy przyjąć następujące założenia :</p>

Podobszar / Proces	Identyfikator wymagania	Treść wymagania
		<ul style="list-style-type: none"> - integracja na poziomie plików o standardowych formatach (co najmniej TXT, CSV, XLS, XML) - integracja na poziomie baz danych : TETA posiada wtyczki do standardowych baz danych (też via ODBC, JDBC), dostęp do tabel z widokami z poziomu dedykowanego użytkownika - przy pomocy wymiany poczty elektronicznej w procesie biznesowym do osób będącymi uprawnionymi użytkownikami systemu Teta - integracja via centralny system raportowy Zamawiającego "Reporting Services" <p>system Teta jest zaimplementowany na bazie Oracle</p>
Integracja TETA	O44.F10	Należy zapewnić integrację z systemem TETA pobierając dane dotyczące wpłat i ich alokacji na należności. Należy uwzględnić ewentualną możliwość niedostępności systemu TETA umożliwiając dostanie informacji po ponownej dostępności systemu (wykorzystując interfejsy asynchroniczne).
Integracja Sugar CRM	O44.F11	<p>Rozwiązanie musi zostać zintegrowane z systemem SugarCRM w ramach następujących obszarów:</p> <ul style="list-style-type: none"> - Umowy (synchronizacja danych, zarządzanie numeracją, usługi na umowie) - Kontrahenci (synchronizacja danych) - Użytkownicy (synchronizacja danych) <p>system sugarCRM jest zaimplementowany w bazie MySQL</p>
Integracja Sugar CRM	O44.F12	<p>W Fazie 1 Rozwiązanie musi zostać integrowane z systemem sugarCRM przy użyciu mechanizmów integracyjnych używanych pierwotnym rozwiązaniu Zamawiającego (integracja sugarCRM -Jira).</p> <p>W zakresie integracji docelowych systemów BSS z sugarCRM muszą być możliwe następujące standardowe mechanizmy integracji:</p> <ul style="list-style-type: none"> - integracja via API, co najmniej REST API - integracja przy pomocy plików wsadowym do sugar CRM w standardowych formatach (co najmniej XLS) - integracja via centralny system raportowy Zamawiającego "Reporting Services" - integracja przy pomocy wymiany poczty elektronicznej w procesie biznesowym do osób będącymi uprawnionymi użytkownikami systemu sugarCRM
Integracja Element Managers - bezpieczeństwo	O44.F13	<p>Rozwiązanie musi umożliwiać integrację z Element Managera' mi systemów bezpieczeństwa (NGFW, ADC, inne) poprzez standardowe protokoły i otwarte mechanizmy integracyjne:</p> <ul style="list-style-type: none"> - poprzez API (co najmniej REST API) - poprzez wymianę plików w standardowych formatach (co najmniej TXT, CSV, XML, JSON)

Podobszar / Proces	Identyfikator wymagania	Treść wymagania
Integracja Element Managers - bezpieczeństwo	O44.F14	<p>Rozwiązanie musi zapewniać provisioning usług i konfiguracji systemów bezpieczeństwa na systemach NGFW, SWG, ADC, DNS z wykorzystaniem dedykowanych Element Managerów i interfejsów REST API lub modyfikacji plików płaskich (pliki konfiguracyjne zapisane na sieciowym zasobie dyskowym), co najmniej w zakresie:</p> <ul style="list-style-type: none"> -Tworzenia i modyfikacji polityk bezpieczeństwa -Zmiany polityk bezpieczeństwa dla szkoły -> usunięcie jednego adresu IP z polityki A i dodanie go do polityki B -Dodawania wyjątków do polityk bezpieczeństwa -Włączania / wyłączania poszczególnych usług dla określonych przez zakres adresów IP <p>Dokładny opis scenariusza aktywacji usług bezpieczeństwa jest opisany w rozdziale pt. "Wymagania dla obszaru OSS"</p>
Integracja Element Managers - bezpieczeństwo	O44.F15	<p>Musi być zapewniona integracja wbudowanej w Rozwiązanie funkcjonalności Fault Management w zakresie odbierania alarmów z urządzeń, systemów bezpieczeństwa oraz Element Manager'ów za pomocą protokołów/mechanizmów:</p> <ul style="list-style-type: none"> - SYSLOG - SNMP trap - forwardowanie alarmów (np. z CPE przez SIEM)
Integracja Element Managers - bezpieczeństwo	O44.F16	<p>Musi być zapewniona integracja wbudowanej w Rozwiązanie funkcjonalności Performance Management z urządzeniami i systemami bezpieczeństwa - komunikacja protokołem SNMP ver. 2c lub ver. 3 , muszą być monitorowane co najmniej następujące parametry:</p> <ul style="list-style-type: none"> - CPU – Idle time - CPU – Percentage spent on processes in the user space - CPU – Percentage spent on process in the system space - Memory – Total Free - Memory – Total Real - Memory – Avail. Swap - Storage – disk usage
Integracja Element Managers - bezpieczeństwo	O44.F17	<p>Rozwiązanie musi zapewniać dla systemu SWG monitoring działania usługi poprzez:</p> <ul style="list-style-type: none"> - monitoring polegający na cyklicznym wykonywaniu zapytania HTTP GET na stronę podaną przez Zamawiającego i podlegającą filtracji stronę WWW oraz sprawdzenie czy pojawia się strona blokowania, - monitoring polegający na wykonywaniu zapytania HTTP GET na podaną przez Zamawiającego stronę WWW i weryfikacja certyfikatu, którym podpisana jest ww. strona. Parametry certyfikatu powinny być tożsame z certyfikatem wgranym na systemie SWG
Integracja SIEM	O44.F18	<p>Rozwiązanie musi zapewnić integrację funkcjonalności Service Desk z systemem SIEM, co najmniej w zakresie wystawiania nowych zgłoszeń w systemie ServiceDesk na podstawie incydentów</p>

Podobszar / Proces	Identyfikator wymagania	Treść wymagania
		pojawiających się w systemie SIEM (poprzez API oraz wysyłanie maila na określony adres)
Integracja SIEM	O44.F19	Musi być zapewniona integracja wbudowanej w Rozwiązanie funkcjonalności Fault Management w zakresie odbierania alarmów na temat działania i dostępności sieci z SIEM za pomocą protokołów/mechanizmów: <ul style="list-style-type: none"> - SYSLOG - SNMP trap - forwardowanie alarmów zebranych z urządzeń CPE w szkołach (tylko SYSLOG)
Integracja SIEM	O44.F20	System musi być zintegrowany w kontekście przekazywania cyklicznych zagregowanych danych i/lub raportów do CSR (Centralny system Raportowy) i/lub do portalu usługowego (będących częścią Rozwiązania) : <ul style="list-style-type: none"> - na temat aspektów bezpieczeństwa dla dyrektorów w kontekście szkoły (np. alarmy, statystyki zablokowanych stron itp.) - na temat danych dotyczących rozkładu ruchu w sieci OSE (pochodzące z Netflow i analizowane przez SIEM) - przy pomocy wymiany danych standardowymi mechanizmami typu REST API - przy pomocy wymiany plików (TXT, CSV, XML, JSON) - przy pomocy wymiany plików graficznych - przy pomocy plików raportowych (PDF, XLS)
Integracja SIEM	O44.F21	Musi być zapewniona integracja wbudowanej w Rozwiązanie funkcjonalności Performance Management z systemem SIEM - komunikacja protokołem SNMP ver. 2c lub ver. 3 , muszą być monitorowane, co najmniej następujące parametry: <ul style="list-style-type: none"> - CPU – Idle time - CPU – Percentage spent on processes in the user space - CPU – Percentage spent on process in the system space - Memory – Total Free - Memory – Total Real - Memory – Avail. Swap - Storage – disk usage
Integracja Element Managers -Sieć	O44.F22	Rozwiązanie musi umożliwiać integrację z Element Managerami szkieletowych urządzeń sieciowych poprzez standardowe protokoły i otwarte mechanizmy integracyjne. Rozwiązanie musi zostać zintegrowane przy założeniach : <ul style="list-style-type: none"> - integracja z Element Managerami odbywa się poprzez API - integracja m. in. służy uruchomieniu provisioningu usług i ich konfiguracji na szkieletowych urządzeniach sieciowych - w przypadku, gdy niemożliwy jest provisioning bezpośrednio na szkieletowych urządzeniach sieciowych należy wykorzystać dedykowane funkcje Element Managerów dostępne poprzez interfejsy API lub poprzez modyfikację plików konfiguracyjnych

Podobszar / Proces	Identyfikator wymagania	Treść wymagania
		<ul style="list-style-type: none"> - możliwość odbierania alarmów poprzez protokoły syslog i snmp trap (forwardowanie) a także możliwość pobierania alarmów poprzez udostępnione API Element Managera - odbieranie wyników pomiarów performance'owych poprzez udostępnione API Element Managera - zarządzanie pomiarami w relacjach E2E zakładanych na ruterach shadow via Element Manager (zakładanie pomiarów i pobieranie wyników pomiarów - w szczególności w postaci raportów zaciąganych do Centralnego Systemu Raportowego)
Integracja Element Managers	O44.F23	Rozwiązanie musi zapewniać możliwość integracji wbudowanej funkcjonalności IPAM wraz z danymi z obszaru CRM z pozostałymi systemami OSE (w szczególności z SIEM) za pomocą REST API. System musi zapewniać możliwość wzbogacania danych w innych systemach OSE na podstawie adresu IP - wydobywanie z systemu BSS nazwy szkoły, lokalizacji, danych kontaktowych dyrektora szkoły na podstawie tego adresu IP.
Integracja TREE Confluence	O44.F24	Należy zapewnić integrację repozytorium architektonicznego Sparx Enterprise Architect z TREE Confluence umożliwiając odświeżanie informacji na Tree na podstawie zmian w EA. Rozwiązanie powinno umożliwiać odświeżanie, co najmniej następujących danych: <ul style="list-style-type: none"> - procesów biznesowych (modeli wraz z opisami kroków) - systemów / modułów (modeli wraz z opisami) - integracji pomiędzy modułami / systemami - diagramów sekwencji (modeli wraz z opisami kroków) - modeli klas / danych (modeli wraz z opisami)
Integracja z partnerami	O44.F25	Rozwiązanie musi udostępniać API w obszarze zleceń dla partnerów umożliwiające w sposób bezpieczny na pobieranie przez partnerów ich zleceń. Funkcjonalność musi ograniczać dostęp jedynie do niezamkniętych zleceń odpytującego partnera. Musi być zapewniona unikalna identyfikacja odpytującego partnera oraz rejestracja wszelkich pobrań danych. Należy udostępnić API jedynie do wyszukiwania i pobierania zleceń, bez możliwości modyfikacji danych.
Integracja ze storag'em obiekowym	O44.F26	Rozwiązanie musi mieć możliwość integracji ze storagem obiekowym przy pomocy protokołu REST API lub S3 w celu potencjalnego składowania danych statystycznych
Integracja z systemem zarządzania środowiskiem kolokacyjnym	O44.F27	Rozwiązanie musi zostać zintegrowane z zewnętrznym systemem zarządzania/monitorowania środowiskiem kolokacyjnym. Zamawiający zamierza jednym spójnym systemem objąć wszystkie centra kolokacyjne OSE. Należy założyć standardowe protokoły i otwarte mechanizmy integracyjne - co najmniej: <ul style="list-style-type: none"> - REST API - wymiana plików o standardowych formatach (TXT, CSV, XML, JSON, XLS)

Podobszar / Proces	Identyfikator wymagania	Treść wymagania
Integracja POCZTA ELEKTRONICZNA	O44.F28	Rozwiązanie musi być zintegrowane z systemem pocztowym NASK (niezbędne pod kontem, co najmniej powiadomień oraz raportowania)
Integracja anty-DDoS	O44.F29	Rozwiązanie musi być zintegrowane z systemem anty-DDoS implementowanym przez NASK PIB, co najmniej w zakresie : - odbierania z systemu anty-DDoS alarmów (SNMP Trap, Syslog) - monitorowania (availability & performance) systemu anty-DDoS (SNMP) - automatycznego zakładania ticketów w systemie OSS/BSS w wyniku alarmu na temat wykrytego ataku na sieć OSE - automatyczne akcje w wyniku alarmu na temat wykrytego ataku na sieć OSE (mail, wykonanie skryptu w shell)
Integracja Active Directory	O44.F30	system SSO implementowany przez Wykonawcę musi być zintegrowany z systemem Active Directory Zamawiającego w celu uwierzytelniania w dostępie do wspieranych przez SSO systemów użytkowników będących pracownikami NASK PIB
Integracja Reporting Services	O44.F31	Rozwiązanie musi być zintegrowany z centralnym systemem raportowym Zamawiającego (Reporting Services) wykorzystywanym do zbierania danych raportowych z różnych systemów NASK PIB. Integracja może mieć na celu pozyskiwanie danych np. z systemów Teta i sugarCRM i potencjalnie innych w przyszłości. system musi umożliwiać integrację: - na poziomie baz danych - na poziomie wymiany plików w standardowych formatach (TXT, CSV, XLS, XML, JSON) system Reporting Services jest zaimplementowany na bazie MSSQL

7.3.5. Rozwiązanie musi spełniać następujące wysokopoziomowe wymagania:

Identyfikator wymagania	Treść wymagania
O46.F1	Platforma Operatora OSE (POOSE) musi umożliwiać interakcję pomiędzy wszystkimi uczestnikami sieci OSE (w tym pracownikami NASK PIB, partnerami NASK PIB oraz klientami końcowymi)
O46.F2	POOSE musi wspierać zarządzanie umowami i usługami świadczonymi jednostkom oświatowym;
O46.F3	POOSE musi umożliwiać inwentaryzację infrastruktury sieciowej i serwerowej sieci OSE (w tym urządzeń aktywnych i pasywnych sieci OSE, urządzeń bezpieczeństwa, łączы dzierżawionych i własnych, urządzeń OSE zainstalowanych w centrach danych i w dzierżawionych miejscach kolokacyjnych)

Identyfikator wymagania	Treść wymagania
O46.F4	POOSE musi umożliwiać inwentaryzację świadczonych usług w powiązaniu z inwentaryzacją infrastruktury sieci OSE z uwzględnieniem graficznej prezentacji inwentaryzowanych elementów
O46.F5	POOSE musi zapewnić funkcjonalność Fault & Performance Management infrastruktury OSE
O46.F6	POOSE musi umożliwiać provisioning konfiguracji urządzeń CPE oraz konfigurację urządzeń szkieletowych w ramach provisioningu usług (urządzenia sieciowe i bezpieczeństwa) POOSE musi również umożliwiać hurtowe zmiany konfiguracji na wielu ww. urządzeniach na raz (mechanizm musi wspierać wybór konfigurowanych urządzeń zarówno z poziomu systemu jak i wsadowo z pliku CSV)
O46.F7	POOSE musi umożliwić zarządzanie konfiguracją i oprogramowaniem urządzeń sieci OSE z uwzględnieniem wersjonowania i archiwizacji danych
O46.F8	POOSE musi wspierać zarządzanie centrami danych rozlokowanych w węzłach sieci OSE
O46.F9	POOSE musi prezentować działanie sieci i usług OSE w postaci statystyk z uwzględnieniem różnych grup docelowych (NOC/SOC OSE, partnerzy OSE, klienci końcowi)
O46.F10	POOSE musi umożliwiać generowanie (w tym automatyczne) i prezentację raportów z różnych - aspektów funkcjonowania operatora OSE: - działanie sieci - działanie usług - rozliczenia usług OSE - rozliczenie partnerów NASK PIB (co najmniej: dostawcy łącz, dostawcy kolokacji, podwykonawcy, - outsorsing IT) - rozliczenia kosztów ponoszonych w projekcie z uwzględnieniem wymogów raportowych dotacji budżetowych i unijnych - wskaźniki osiągnięcia celów projektowych
O46.F11	Rozwiązanie musi cechować się niezawodnością - systemy nadzoru powinny pracować w trybie wysokiej dostępności, powinna być zapewniona pełna funkcjonalność przy awarii pojedynczego elementu czy węzłów centralnych (funkcjonalność Data Recovery)
O46.F12	POOSE musi współpracować z heterogeniczną infrastrukturą sieciową (w szczególności w szkołach)
O46.F13	POOSE musi wspierać maksymalną automatyzację wszystkich procesów operatora OSE ze szczególnym naciskiem na procesy dostarczania usług OSE i zarządzania usługami OSE
O46.F14	Rozwiązanie musi zapewniać skalowalność - co oznacza rozwiązanie w pełni funkcjonalne a jednocześnie optymalne wydajnościowo bez względu na ilość podłączonych do OSE szkół
O46.F15	dostęp dla użytkowników systemów OSS/BSS do poszczególnych funkcjonalności POOSE powinien być możliwy zarówno z poziomu poszczególnych aplikacji serwujących daną funkcjonalność (z uwzględnieniem SSO) jak również z poziomu centralnego FrontEnd'u (portal Web/strona WW dostępne przy użyciu protokołu HTTP/HTTPS) zgodnie z założonym profilem użytkownika (po przejściu uwierzytelnienia i autoryzacji)
O46.F16	dostęp do POOSE musi być możliwy przy pomocy standardowych przeglądarek Web zarówno z poziomu urządzeń stacjonarnych jak i mobilnych (w szczególności dotyczy to dostępu dla podwykonawców/partnerów serwisowych)

Identyfikator wymagania	Treść wymagania
O46.F17	w pełni funkcjonalne Rozwiązane ale o mniejszej wydajności niż Rozwiązanie produkcyjne musi być uruchomione w środowisku testowym zaimplementowanym przez Dostawcę
O46.F18	Całość infrastruktury (zarówno na potrzeby OSS/BSS jak i innych projektów OSE) musi zostać umiejscowiona w kolokacjach NASK lub dzierżawionych przez NASK w ramach projektu OSE
O46.F19	Po zakończeniu ostatniej fazy wdrożenia całe rozwiązanie warstwy aplikacyjnej musi zostać osadzone na infrastrukturze dostarczanej w ramach rozwiązania i umiejscowionej w kolokacjach NASK (własnych lub dzierżawionych). Nie dopuszczalne jest umieszczenie jakiegokolwiek części rozwiązania poza infrastrukturą i/lub kolokacjami NASK (własnymi lub dzierżawionymi).
O46.F20	Wprowadzanie i modyfikacji danych adresowych w Rozwiązaniu musi być weryfikowane na zgodność z bazą TERYT. Baza TERYT jest podstawą dla danych adresowych w Rozwiązaniu. Dostarczenie i aktualizacja bazy Teryt pozostaje w gestii Wykonawcy
O46.F21	<p>Rozwiązanie musi być spójnie, dobrze zintegrowane oraz o w miarę niskiej złożoności / różnorodności architektonicznej. Na podstawie zdefiniowanej w rozdziale "6.Koncepcja systemów nadzoru (Platforma Operatora OSE)" złożoności architektury dla rozwiązania, współczynnik złożoności wyliczony dla następującego wzoru $\text{Złożoność} = \text{ilość aplikacji} \wedge \text{waga (1)} * \text{ilość komponentów uruchomieniowych} \wedge \text{waga (2)}$ musi mieć wartość nie większą niż 4000.</p> <p>Aplikacja - samodzielnie funkcjonujący komponent programistyczny posiadający interfejs graficzny udostępniany dla użytkownika oraz określony model własności i licencjonowania. Aplikacja może się składać z modułów pochodzących od jednego dostawcy i dostarczanych w ramach jednego modelu licencji. Jeżeli moduły do aplikacji dostarczane są przez innego producenta lub posiadają inny model licencjonowania traktowane są, jako oddzielne aplikacje.</p> <p>Komponent platformy aplikacyjnej - komponent programistyczny będący środowiskiem do funkcjonowania aplikacji taki jak serwer aplikacyjny, serwer bazy danych itp. W przypadku, gdy dany komponent występuje w różnych wersjach oprogramowania to traktowany jest, jako oddzielne komponenty platformy aplikacyjnej.</p> <p>Komponent uruchomieniowy - połączenie komponentu platformy aplikacyjnej z warstwą operacyjną (czyli systemem operacyjnym). W sytuacji, gdy dany serwer bazy danych uruchamiany jest na dwóch różnych systemach operacyjnych liczony jest, jako dwa komponenty uruchomieniowe.</p>
O46.F22	Rozwiązanie w zakresie funkcjonalności przeznaczonej dla klientów i partnerów OSE musi zapewniać odpowiedni stopień bezpieczeństwa, czyli wykazywać brak podatności z listy „OWASP Top Ten” oraz brak błędów typu „High” i „Critical” w testach penetracyjnych. Wykonawca jest odpowiedzialny za weryfikację poziomu bezpieczeństwa we własnym zakresie. Zamawiający przed dopuszczeniem rozwiązania na produkcję przeprowadzi we własnym zakresie testy bezpieczeństwa. Wykonawca jest zobowiązany do przygotowania środowiska i zapewnienia wsparcia w realizacji testów przez zamawiającego lub firmę, której zamawiający zleci realizację tych prac.
O46.F23	Rozwiązanie musi być zwymiarowane zgodnie z informacjami zawartymi w rozdziale "Informacje mające wpływ na architekturę Rozwiązania"
O46.F24	Wszystkie funkcjonalności Rozwiązania muszą być udokumentowane w postaci dokumentacji technicznej użytych technologii i zastosowanych rozwiązań (w szczególności wszystkich

Identyfikator wymagania	Treść wymagania
	używanych API). Dokumentacja ta musi być przekazana Zamawiającemu na etapie akceptacji dokumentu LLD. W przypadku, gdy funkcjonalność jest wytwarzana na etapie wdrożenia musi ona zostać udokumentowana i uzupełniona w przekazanej Zamawiającemu dokumentacji technicznej przez Wykonawcę. Dokumentacja techniczna musi być odpowiednio uporządkowana tak by była możliwość jej łatwego przeszukiwania.
O46.F25	W przypadku zastosowania gotowego oprogramowania dokumentacja producenta tego oprogramowania musi zostać dołączona do dokumentacji technicznej całego Rozwiązania

7.3.6. Rozwiązanie musi spełniać następujące wymagania regulacyjne

Nr wymagania	Treść wymagania
O47.F1	Sposób działania Rozwiązania jest zgodny z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (RODO).
O47.F2	Rozwiązanie musi udostępniać rejestr czynności przetwarzania danych osobowych.
O47.F3	Rozwiązanie musi udostępniać rejestr zgód na przetwarzanie danych osobowych zawierający informacje o udzieleniu lub cofnięciu zgód na przetwarzanie danych, jak również zgód na przesyłanie informacji handlowych wraz z historią ich udzielenia.
O47.F4	Rozwiązanie musi udostępniać rejestr upoważnień przetwarzania danych osobowych wraz z informacją o tym, kto w danej firmie i firmach zależnych i współpracujących otrzymał prawo do wglądu w dane osobowe, w jakim zakresie i na jaki okres
O47.F5	Rozwiązanie musi udostępniać rejestr naruszeń przetwarzania danych osobowych.
O47.F6	Rozwiązanie musi udostępniać raport z przetwarzanymi danymi osobowymi dostarczany dla osoby fizycznej dostarczany na jej wyraźną prośbę.
O47.F7	Rozwiązanie musi wspierać możliwość trwałego usunięcia danych osobowych na żądanie osoby uprawnionej, pod warunkiem, że w systemie nie istnieją dokumenty, których przechowywanie jest wymagane prawnie
O47.F8	Rozwiązanie musi zapisywać listę działań użytkowników Rozwiązania w tym zapisywać informacje o tym, jakie czynności wykonywał użytkownik i jakich zmian w danych osobowych czy jakich wydruków dokonywał.

7.4. Opis funkcjonalności dla obszaru OSS

7.4.1. Monitorowanie infrastruktury i usług OSE (Fault & Availability oraz Performance Management)

Systemy monitorowania sieci OSE powinny obejmować dwie poniższe domeny systemów, które realizują zadania modelu zarządzania siecią telekomunikacyjną FCAPS (Fault, Configuration, Accounting, Performance, Security):

- Fault & Availability Management (FM) – moduł pozwalający na wykrywanie i kontrolowanie awarii i usterek występujących w OSE poprzez ciągłe monitorowanie wszystkich elementów systemu, aktywne monitorowanie ich dostępności oraz odbiór i przetwarzanie zdarzeń pasywnych z monitorowanej infrastruktury.
- Performance Management (PM) – moduł pozwalający na monitorowanie w sposób ciągły wydajności wszystkich elementów systemu OSE i przekazywanie informacji na temat wykrytych problemów do systemu FM.

Obydwie ww. domeny monitoringu muszą być zaprojektowane warstwowo tak by wyodrębnić warstwy funkcjonalne, które pozwolą uelastyczyć architekturę systemu monitorowania - warstwy te obejmują:

- warstwę kolekcji danych – odpowiedzialnej za udostępnienie interfejsów południowych i pobieranie danych z elementów monitorowanej infrastruktury. Realizowane są tu również zadania wstępnej filtracji i normalizacji danych, konfiguracji trybu i sposobu monitorowania elementów, jak również zadania związane z wykrywaniem infrastruktury sieciowej i włączaniem jej do struktur monitorowania;
- warstwę agregacji i przetwarzania – odpowiedzialnej za procesowanie, korelację i składowanie kolekcjonowanych danych w ramach centralnego repozytorium. W warstwie tej realizowane są również zadania związane z analizą danych, ich korelacją, integracją z innymi systemami OSS/BSS oraz wspomaganiem obsługi operatorskiej (m. in. automatycznymi eskalacjami);
- warstwę prezentacji – realizującej zadania związane z szeroko pojętym raportowaniem stanu monitorowanej infrastruktury, zarówno w formie prezentacji w czasie rzeczywistym, jak i udostępnianiem raportów historycznych czy predykcji użycia sieci w formie trendów. W ramach tej warstwy umieszczamy również zadania związane z przydzielaniem odpowiednich poziomów dostępu użytkownikom systemu w zależności od ich roli w strukturach organizacyjnych zapewniały możliwość pracy w modelu z rozproszoną kolekcją zdarzeń i danych wydajnościowych. Systemy powinny zapewnić możliwość uruchamiania zewnętrznych, względem modułów centralnych, **kolektorów** danych wydajnościowych i **sond** kolekcjonujących zdarzenia pasywne.

Wymaga się, aby systemy Fault & Availability oraz Performance Management zapewniały możliwość pracy w modelu z rozproszoną kolekcją zdarzeń i danych wydajnościowych. Systemy powinny zapewnić możliwość uruchamiania zewnętrznych, względem modułów centralnych, kolektorów danych wydajnościowych i sond kolekcjonujących zdarzenia pasywne.

Kolektory i sondy mają agregować zebrane dane i przekazywać je do systemu centralnego. Taka architektura zapewnia następujące korzyści:

- rozłożenie obciążenia systemu związanego ze znaczną ilością monitorowanych urządzeń/systemów;
- buforowanie danych na poziomie kolektorów/sond i odciążenie centralnych systemów;

- możliwość filtracji szumu informacyjnego na poziomie sond;
- optymalizację pracy systemu poprzez wstępne procesowanie i normalizację zdarzeń na poziomie sond/kolektorów;
- zwiększoną elastyczność konfiguracji systemu poprzez możliwość dostosowywania parametrów poszczególnych kolektorów/sond do specyfiki monitorowanego segmentu sieci;
- skalowalność horyzontalną i możliwość prostej rozbudowy systemu poprzez dołożenie dodatkowych sond/kolektorów i/lub instancji systemu centralnego.

W szczególności obydwa systemy muszą mieć możliwość integracji z systemami typu Element Managers w celu pobierania alarmów oraz pobierania danych performance'owych. NASK planuje wdrożenie wielu Element Manager'ów : w obszarze sieciowym, w obszarze bezpieczeństwa , w obszarze zarządzania infrastrukturą serwerową oraz w obszarze zarządzania środowiskiem kolokacyjnym. Operator OSE będzie kolokował swoje urządzenia w 16tu centrach kolokacyjnych w całej Polsce - jedno centrum danych będzie własnością NASK a pozostałe będą dzierżawione od dostawców kolokacji. W celu sprawnego monitorowania środowiska kolokacyjnego (dzierżawione szafy z niezbędnymi czujnikami parametrów środowiska) zostanie wdrożony wspólny system zarządzania, który swym zasięgiem obejmie wszystkie kolokacje - zarówno centrum kolokacyjne NASK jak i pozostałe centra (dzierżawione szafy).

Obydwa systemy muszą w wygodny sposób prezentować zbierane informacje tak, aby w szybki sposób można było wyszukiwać przyczynę awarii oraz wyszukiwać stosowne statystyki i raporty pomimo dużej ilości danych pochodzących z wszystkich urządzeń OSE - w szczególności z rozbiciem tych informacji na logiczne i geograficzne obszary a także per jednostki oświatowe i świadczone im usługi. System Performance Management musi być ściśle zintegrowany z częścią Fault & Availability Management, obydwa systemy w ramach Rozwiązania mają być prezentowane w uspojnionym jednym logowaniem interface'ie graficznym.

Podstawowe funkcje wymagane w warstwie prezentacji to:

- własny, spójny interfejs operatorski i administracyjny,
- podstawowym interfejsem systemu ma być aplikacja webowa, stanowiąca konsolę operatorsko-administracyjną,
- interfejs systemu ma umożliwiać dostosowywanie widoków, dashboardów, etc. do specyficznych wymagań użytkowników,
- interfejs webowy systemu powinien być przystosowany do jego wykorzystania w ramach NOC i SOC operatora OSE
- dostępność udokumentowanego API systemu, które pozwoli na pobranie odpowiednich danych za pomocą aplikacji/systemu odpowiedzialnego za wystawienie danych np. do portalu OSE
- natywny interfejs webowy systemu monitorowania powinien być wspierany przez popularne przeglądarki internetowe

Istotnym aspektem warstwy prezentacji systemów jest mechanizm raportowy, który musi mieć możliwość generowania raportów w swoim natywnym mechanizmie, ale również być źródłem danych dla Centralnego Systemu raportowania, gdzie raporty typowo technicznych aspektów będą mogły być porównane z aspektami biznesowymi. Zwłaszcza w przypadku systemu Performance Management tych raportów będzie bardzo dużo i muszą one spełniać szereg wymagań a w szczególności:

- system musi udostępniać predefiniowane zestawy raportów, na przykład grupowane ze względu na typy dostępnych monitorów, typ raportu, usługę. Przykładowe predefiniowane raporty:
 - Raporty prezentujące statystyki ruchu sieciowego (m. in. użycie interfejsów, opóźnienia, jitter);
 - Raporty dostępności za określony czas;
 - Raporty porównawcze np. tego samego typu raportu dla dwóch różnych elementów, pozwalających na analizę wskaźników wydajnościowych w tym samym okresie pomiaru;
 - Raport wszystkich wskaźników monitorowanych na danym typie elementu;
 - Raporty typu Top N według różnych kryteriów;
 - Raporty typu inventory korzystające z zasobów określonych w ramach procesu automatycznego wykrywania sieci;
- system powinien umożliwiać definiowanie harmonogramów dla automatycznego generowania raportów oraz ich udostępniania, np. poprzez email;
- użytkownicy systemu musi mieć możliwość tworzenia własnych raportów, udostępniania ich w postaci szablonów innym użytkownikom. Narzędzie służące tworzeniu raportów powinno posiadać intuicyjny graficzny interfejs;
- generowanie raportów w standardowych formatach np. PDF, CSV oraz XLS
- szablony raportów udostępniane w ramach systemu (domyślne i utworzone przez użytkowników) powinny zapewniać parametryzację, np. określenie zakresu czasowego, czy listy interfejsów.

7.4.1.1 Funkcjonalność Fault & Availability Management

Celem systemu Fault & Availability Management jest wsparcie pracy zespołów NOC, SOC i IT w zakresie utrzymania sieci, usług i systemów OSE. System musi być elastyczny i pozwalać na monitorowanie zarówno działania szkieletu sieci OSE jak i sieci agregacyjnej i dostępowej a także heterogenicznych urządzeń OSE instalowanych w sieci LAN w szkołach.

System Fault Management ma pozwalać na zbieranie alarmów (pasywny monitoring) wygenerowanych bezpośrednio przez urządzenia i systemy sieciowe w szkieletcie OSE oraz w jednostkach oświatowych, przez systemy w centrach kolokacji, aplikacje czy dowolne elementy infrastruktury teleinformatycznej potrafiące poinformować system nadrzędny (Fault Management) o swoim stanie, natomiast System Availability Management pozwoli na sprawdzanie dostępności urządzeń i usług (aktywne monitorowanie) w szczególności systemy te będą monitorować:

- wszystkie urządzenia sieciowe sieci szkieletowej zainstalowane w węzłach centralnych i szkieletowych
- infrastruktura serwerowa, systemowa i aplikacyjna w centrach danych (jak SGW, Portal OSE, inne)
- urządzenia OSE w szkołach

- urządzenia i elementy sieci zarządzania (np. szafy serwerowe - integracja poprzez system zarządzania kolokacją)
- systemy typu Element Management nadzorujące urządzenia sieciowe i bezpieczeństwa
- dedykowane systemy sieciowe i systemy bezpieczeństwa (jak SIEM, NGFirewall, CGNAT) w węzłach regionalnych

W przypadku systemu Fault Management bardzo ważną rolę odgrywa wspomniana wyżej warstwa agregacji i przetwarzania, która odpowiedzialna jest za procesowanie, korelację i składowanie kolekcjonowanych danych w ramach centralnego repozytorium. W warstwie tej realizowane są głównie zadania związane z analizą danych, ich korelacją, integracją z innymi systemami OSS/BSS oraz wspomaganie obsługi operatorskiej. Centralne repozytorium zdarzeń powinno zapewniać następujące główne funkcjonalności w zakresie przetwarzania danych:

- podstawową korelację zdarzeń:
 - deduplikację, czyli identyfikację alarmów dotyczącą dokładnie tego samego zdarzenia i przechowywanie go w repozytorium jako jednego rekordu,
 - automatyczną korelację ON/OFF, czyli parowanie zdarzeń, które oznaczają wystąpienie awarii i jej zakończenie,
 - filtrację, automatyczne usuwanie z repozytorium alarmów na podstawie zdefiniowanego kryterium,
 - eskalację – automatyczne powiadomienia wywoływane na podstawie alarmów (opisane szczegółowo w dalszej części dokumentu).
- automatyczne wykonywanie akcji (np. skryptu) na podstawie zarejestrowanych zdarzeń pozwalające na automatyczne wykonywanie akcji naprawczych takich jak np. restart usługi czy restart portu urządzenia. Wywołanie akcji może być realizowane poprzez integrację z systemem Config Manager i wykorzystanie zadań konfiguracyjnych zdefiniowanych w tym systemie;
- mechanizmy archiwizacji zdarzeń aktywnych w bazie zdarzeń historycznych;
- diagnostykę i monitoring wydajności przetwarzania zdarzeń/alarmów.

Podobnie bardzo istotnym elementem systemu Fault Management jest możliwość analizy kolekcjonowanych danych i ich korelacja. W przypadku infrastruktury OSE spodziewana jest kolekcja bardzo znaczącej ilości danych i z tego względu ważne jest aby system udostępniał, co najmniej zestaw poniższych podstawowych automatyzacji, które pozwalają na efektywną analizę danych:

- deduplikacja – grupowanie komunikatów dotyczących dokładnie tego samego zdarzenia w ramach jednego rekordu. W ramach funkcjonalności pożądaną jest, aby grupowane rekordy otrzymały znaczniki, takie jak czasy pierwszego i ostatniego wystąpienia zdarzenia, liczba wystąpień;
- automatyczna korelacja ON/OFF polegająca na parowaniu zdarzeń informujących o zaistnieniu awarii oraz o jej zakończeniu. Zdarzenia podlegające korelacji są przechowywane jeszcze przez określony czas w ramach centralnej bazy, jednak docelowo są automatycznie usuwane. Powinny być jednak zawsze dostępne w ramach bazy alarmów historycznych;
- filtrację zdarzeń – funkcjonalność realizowana już w warstwie kolekcji systemu, ale również w warstwie przetwarzania pozwalająca na grupowanie zdarzeń zgodnie z określonymi potrzebami, np. w przypadku zdarzeń tzw. bezstanowych, które nie podlegają korelacji ON/OFF, a mimo wszystko

powinny być odnotowane i zaprezentowane użytkownikom systemu lub system powinien umożliwiać ich automatyczne usuwanie z repozytorium, np. po potwierdzeniu przez operatora albo poprzez możliwość definiowania czasu przechowywania takiego zdarzenia z systemu;

- kategoryzację danych – funkcjonalność, która zapewni możliwość oznaczania i agregowania kolekcjonowanych zdarzeń w ramach zdefiniowanych w systemie grup i/lub kategorii, na przykład przydzielanie urządzeń i ich zdarzeń do odpowiednich rejonów geograficznych lub wedle kryteriów organizacyjnych;
- wzbogacanie zdarzeń w zakresie informacji dostępnych w pozostałych systemach OSS/BSS (w szczególności Inventory i CRM)

Bardzo użyteczną funkcjonalnością związaną z monitorowaniem awarii w sieci jest funkcjonalność automatycznego wykrywania topologii sieci i związanego z tym mechanizmu wykrywania przyczyny pierwotnej awarii (RCA - Route Cause Analysis). Ta wymagana funkcjonalność będzie ograniczać ilość zdarzeń generowanych w systemie w przypadku awarii (zwłaszcza awarii masowych). Funkcjonalność automatycznego wykrywania sieci wraz z funkcją RCA oraz z możliwością prezentacji topologii sieci z różnej perspektywy np. widoki topologii warstwy 2 lub 3 dostępne są w ramach dedykowanych aplikacji realizujących funkcje Topology Management. Zakłada się, że dostarczone Rozwiązanie powinno mieć tę funkcjonalność zaimplementowaną przynajmniej w obszarze węzłów OSE.

Założenia dotyczące architektury pomiarów

1. W zakresie Fault & Availability Management sieć szkieletowa OSE, czyli wszystkie urządzenia w węzłach centralnych i regionalnych OSE (zarówno urządzenia sieciowe jak i urządzenia i systemy bezpieczeństwa oraz serwery) będą wysyłać pewne spectrum syslogów i trapów SNMP (zdefiniowane na etapie HLD). Zakłada się również uruchomienie monitoringu przy pomocy RTT ICMP dostępności urządzeń (na adres loopback) , portów fizycznych i logicznych (na adresy skonfigurowane na portach) jak również przy pomocy protokołu TCP dostępności usług (odpowiedzi pakietów wysłanych do zdefiniowany port TCP) z częstotliwością, co najmniej 300 sekund. W przypadku braku dostępności generowany jest alarm do systemu Fault & Availability Management (brak dostępności będzie wynikać z założonych kryteriów zdefiniowanych na poziomie HDL).
2. W przypadku urządzeń zainstalowanych w szkole trapy SNMP nie będą wysyłane, natomiast pakiety syslog będą przesyłane tylko z CPE i tylko w okresach 3 tygodni po podłączeniu szkoły/lokalizacji szkolnej do sieci OSE oraz w przypadkach niezbędnej diagnostyki zgłoszonych przez szkołę problemów. Logi te będą przesyłane do systemu SIEM pełniącego między innymi rolę Systemu Retencji Logów ze względu na ograniczoną funkcjonalność urządzeń CPE (brak możliwości wysyłania logów do dwóch Fault Managerów jednocześnie). Syslogi istotne ze względu na utrzymanie urządzeń (zdefiniowane na etapie HLD) będą następnie przekierowywane z SIEM do systemu Fault & Availability Management. Aktywny monitoring CPE przy pomocy pakietów RTT ICMP będzie prowadzony również tylko w okresach 3 tygodni po podłączeniu szkoły/lokalizacji szkolnej do sieci OSE oraz w przypadkach niezbędnej diagnostyki zgłoszonych przez szkołę problemów. W przypadku urządzeń SW i AP monitoring taki będzie aktywowany w przypadku zgłoszonych problemów ze szkoły i po decyzji operatora OSE i skonfigurowaniu dostępu do tych urządzeń by był możliwy, zatem tylko w szczególnych przypadkach. Zakłada się częstotliwość pomiarów RTT ICMP na poziomie 300 sekund.

Można szacunkowo założyć, że takich monitorowanych urządzeń w danym momencie w skali całej sieci OSE będzie dotyczyło około 1000 szkół.

Wymagania funkcjonalne

Podobszar	Nr Wymagania	Treść wymagania
Szczególne wymagania pod kątem monitorowania dostępności sieci szkieletowej oraz łącz agregacyjnych i dostępowych	O11.F1	system musi monitorować dostępność (aktywny monitoring RTT ICMP) wszystkich aktywnych interface'ów fizycznych i logicznych na urządzeniach szkieletowych uwzględniając również rutery logiczne oraz instancje VRF
Szczególne wymagania pod kątem monitorowania dostępności sieci szkieletowej oraz łącz agregacyjnych i dostępowych	O11.F2	system musi odbierać wysyłane do niego z urządzeń sieciowych i urządzeń/systemów bezpieczeństwa zainstalowanych w sieci szkieletowej trapy SNMP v2c, v3
Szczególne wymagania pod kątem monitorowania dostępności sieci szkieletowej oraz łącz agregacyjnych i dostępowych	O11.F3	system musi odbierać logi SYSLOG (zgodne z RFC 5424) wysyłane do niego z urządzeń sieciowych i urządzeń/systemów bezpieczeństwa zainstalowanych w sieci szkieletowej, należy założyć, że urządzenia będą logowały zdarzenia z severity co najmniej warning (warning i bardziej krytyczne)
Szczególne wymagania pod kątem monitorowania dostępności sieci szkieletowej oraz łącz agregacyjnych i dostępowych	O11.F4	system musi przyjmować alarmy generowane w wyniku przekroczeń progów założonych na pomiarach performance'owych zarówno pobieranych z urządzeń przy pomocy protokołu SNMP z dowolnych urządzeń OSE jak i jako strumień danych telemetrycznych ze szkieletowych urządzeń OSE, które będą wspierać technologię telemetry
Szczególne wymagania pod kątem monitorowania dostępności urządzeń w sieci LAN w szkołach	O11.F5	system musi mieć możliwość odbierania i odpowiedniego interpretowania wysyłanych do niego trap'ów SNMP v2c, v3 z urządzeń zainstalowanych w szkołach (CPE, Switch , Acces Point wi-fi) - potencjalnie operator OSE może zdecydować w dowolnym momencie projektu, że incydentalnie trapy SNMP będą wysyłane z urządzeń zainstalowanych w szkołach
Szczególne wymagania pod kątem monitorowania	O11.F6	urządzenia CPE w szkołach będą wysyłać logi typu SYSLOG (zgodne z RFC 5424) do systemu Retencji Logów (docelowo będącego częścią systemu SIEM) co najmniej z obszarów DHCP i NAT, stan urządzenia itp. ponieważ funkcjonalność CPE (kupowane sukcesywnie w

Podobszar	Nr Wymagania	Treść wymagania
dostępności urządzeń w sieci LAN w szkołach		<p>przetargach i dostarczane przez beneficjentów POCP) może nie pozwalać na przesyłanie logów SYSLOG równolegle do dwóch odbiorców : Fault Managera i Systemu SIEM/ Retencji Logów :</p> <ul style="list-style-type: none"> - system musi wspierać otrzymywanie/pobieranie logów SYSLOG z Systemu SIEM/Retencji Logów (severity z poziomu warning i bardziej krytyczne) na temat stanu urządzeń CPE - należy założyć, że standardową metodą jest dostarczanie danych do systemu OSS FM przez SIEM, natomiast konieczność pobierania przez system OSS FM z SIEM należy traktować, jako podejście rezerwowe na wypadek problemów z metodą standardową
Szczególne wymagania pod kątem monitorowania dostępności urządzeń w sieci LAN w szkołach	O11.F7	<p>system musi odbierać pakiety syslog przesyłane z CPE w okresach 3 tygodni po podłączeniu szkoły/lokalizacji szkolnej do sieci OSE oraz w przypadkach niezbędnej diagnostyki (należy założyć średnio do 2 tygodni) zgłoszonych przez szkołę problemów (logi te będą przesyłane do FM via system SIEM pełniący też rolę systemu Retencji Logów);</p> <p>należy uwzględnić wymiarowanie przedstawione w rozdz. "Informacje mające wpływ na architekturę Rozwiązania"</p>
Szczególne wymagania pod kątem monitorowania dostępności urządzeń w sieci LAN w szkołach	O11.F8	<p>system musi prowadzić aktywny monitoring dostępności urządzenia CPE przy pomocy pakietów RTT ICMP w okresach 3 tygodni po podłączeniu szkoły/lokalizacji szkolnej do sieci OSE oraz w przypadkach niezbędnej diagnostyki (należy założyć średnio do 2 tygodni) zgłoszonych przez szkołę problemów;</p> <p>należy uwzględnić wymiarowanie przedstawione w rozdz. "Informacje mające wpływ na architekturę Rozwiązania"</p>
Szczególne wymagania pod kątem monitorowania dostępności sieci szkieletowej oraz łącz agregacyjnych i dostępowych	O11.F9	<p>system musi jednoznacznie identyfikować urządzenia po adresie (np. loopback) i dokonywać jego translacji na nazwę urządzenia by prezentować alarmy per nazwa urządzenia celem prostszej identyfikacji źródła alarmu (schemat nazewnictwa urządzeń będzie zdefiniowany przez Zamawiającego na etapie wdrożenia - należy założyć, że w nazwach urządzeń będą zaszyte informacje terytowe)</p>
Szczególne wymagania pod kątem monitorowania dostępności urządzeń w sieci LAN w szkołach	O11.F10	<p>standardowo urządzenia OSE w szkołach typu Switch i Access Pointy wi-fi nie będą wysyłać logów SYSLOG i trapów SNMP do systemu, jednakże system musi być gotowy na ich odbieranie ad. hoc. w miarę potrzeb w celu diagnostyki tych urządzeń (należy założyć średnio do 2 tygodni)</p>
Szczególne wymagania pod kątem monitorowania urządzeń infrastruktury serwerowej	O11.F11	<p>system musi umożliwiać integrację z dedykowanym systemem zarządzania infrastrukturą serwerową (będącą częścią Rozwiązania) na poziomie odbierania logów SYSLOG (zgodnie z FRC 5424) i trapów NSMP (v2c, v3) a także na poziomie standardowych mechanizmów integracji (co najmniej REST API, pliki w formatach CSV, TXT, XML, JSON) celem prezentowania najważniejszych alarmów dla NOC/SOC</p>

Podobszar	Nr Wymagania	Treść wymagania
		w jednym miejscu, czyli w systemie typu umbrella (Fault Management)
Wymagania całościowe	O11.F12	alarmy, które trafiają do systemu Fault Management muszą być raportowane do operatorów w NOC przy założeniu różnej gradacji alarmów (np. operator III linii widzi tylko alarmy krytyczne) oraz grupowania alarmów (np. operatorzy systemów bezpieczeństwa widzą tylko alarmy dotyczące bezpieczeństwa lub wydzielona część NOC widzi tylko alarmy z danego obszaru geograficznego sieci OSE)
Wymagania całościowe	O11.F13	system musi zapewniać możliwość generowania raportów zbiorczych, które będą dostępne np. dla kierowników operatora OSE
Wymagania całościowe	O11.F14	system musi wspierać implementację architektury rozproszonej – możliwość kolekcji danych poprzez wydzielone dedykowane moduły programowe (sondy)
Wymagania całościowe	O11.F15	celem mniejszego obciążania łącz pomiędzy węzłami OSE system musi zostać zaimplementowany w architekturze rozproszonej by kolekcja zdarzeń znajdowała się jak najbliżej źródła zdarzenia; należy uwzględnić architekturę zapewniającą to, że logiczne warstwy systemu wymagające większej wydajności i niezawodności (warstwa prezentacji i przetwarzania danych) były ulokowane w węzłach centralnych
Wymagania całościowe	O11.F16	system musi mieć możliwość monitorowania działania sieci OSE w sposób pasywny (odbieranie alarmów) jak również w sposób aktywny (wysyłanie pakietów RTT ICMP, badanie dostępności dedykowanych portów TCP, inne) - w wyniku przekroczenia zadanych parametrów pomiarów (np. czas odpowiedzi, wielkość strat pakietów, wielkość opóźnienia) generowany jest alarm z poziomu tegoż systemu (Fault & Availability Management)
Wymagania całościowe	O11.F17	system musi odbierać alarmy wygenerowane przez system Performance Management (w ramach Rozwiązania będącego przedmiotem zamówienia) a także z dowolnego systemu OSE przy zachowaniu standardowych formatów odbieranych pakietów (SNMP Trap i SYSLOG)
Wymagania całościowe	O11.F18	sondy odbierające alarmy muszą mieć możliwość filtracji kolekcjonowanych danych
Wymagania całościowe	O11.F19	sondy odbierające alarmy muszą normalizować odebrane alarmy i mieć możliwość formatowania danych
Wymagania całościowe	O11.F20	sondy odbierające alarmy muszą zapewnić mechanizmy wzbogacania alarmów bazując na prostych strukturach danych zapisywanych, co najmniej w plikach płaskich oraz w danych z bazy CMDB

Podobszar	Nr Wymagania	Treść wymagania
Wymagania całościowe	O11.F21	system musi mieć funkcjonalność elastycznego logowania parametrów pracy sond oraz zdarzeń (alarmów) w formie nieprzetworzonej
Wymagania całościowe	O11.F22	sondy muszą zapewniać mechanizm buforowania danych w przypadku utraty komunikacji z innymi komponentami systemu przez okres 36 godzin
Wymagania całościowe	O11.F23	sondy muszą zapewniać możliwość konfiguracji częstotliwości pollingu per monitorowany element i/lub typ elementu, co najmniej z częstotliwością 300 sekund
Wymagania całościowe	O11.F24	system musi mieć możliwość dostosowywania parametrów poszczególnych sond do specyfiki monitorowanego elementu
Wymagania całościowe	O11.F25	system musi posiadać skalowalność horyzontalną i możliwość prostej rozbudowy systemu poprzez dołożenie dodatkowych sond i/lub instancji systemu centralnego
Wymagania całościowe	O11.F26	zaimplementowane w systemie sondy muszą mieć możliwość odbierania przesyłanym do nich pakietów SNMP trap (v2c, v3) oraz pakietów SYSLOG (zgodnie z RFC 5424)
Wymagania całościowe	O11.F27	<p>system musi posiadać udokumentowane API w zakresie kolekcji danych, za pomocą którego możliwa będzie integracja systemu z elementami infrastruktury przy wykorzystaniu innych protokołów niż SNMP, SYSLOG - co najmniej REST API, protokoły TCP/UDP, odczyt plików płaskich, telnet/ssh</p> <p>monitoring aktywny musi w zakresie monitorowania dostępności (Availability Management) spełniać następujące wymagania:</p> <ul style="list-style-type: none"> - wysyłanie pakietów ICMP echo (sprawdzenie osiągalności urządzenia, sygnalizowanie przekroczenia zadanego poziomu strat pakietów / opóźnień) - wysyłanie zapytań SNMP o wskazany OID (porównanie wyniku z zadaną wartością liczbową lub tekstową) - wysyłanie zapytań SQL do wskazanej bazy danych, porównanie wyniku z zadaną wartością liczbową lub tekstową - badanie dostępności stron Web poprzez weryfikację czasów odpowiedzi na zapytania HTTP/HTTPS i porównywanie ich z zadanymi wartościami liczbowymi oraz weryfikację zwracanych kodów błędów - badanie czasów pobierania stron Web, transferu plików przy pomocy protokołu FTP/TFTP/HTTP - wysyłanie pakietów TCP/UDP (sprawdzenie, czy możliwe jest połączenie się na zadany port), alarmowanie braku odpowiedzi (np. timeout, connection refused) oraz przekroczeń oczekiwanego czasu odpowiedzi, w szczególności sprawdzanie usług : <ul style="list-style-type: none"> - SMTP, POP3, IMAP - DNS

Podobszar	Nr Wymagania	Treść wymagania
		<ul style="list-style-type: none"> - SSL, SSH, TELNET - SIP - możliwość wykonywania pomiarów w konkretnych relacjach pomiarowych z użyciem protokołów pomiarowych typu Two-Way : TWAMP (zgodnie z RFC 5357) lub/i przy użyciu rozwiązań producenckich (np. Cisco IP SLA, Juniper RPM, Huawei NQA, Alcatel SAA) bezpośrednio z systemu lub poprzez API do Element Managera do urządzeń sieciowych (kupowany w oddzielnym postępowaniu zakupowym)
Wymagania całościowe	O11.F28	monitoring pasywny musi wykorzystywać, co najmniej protokoły SNMP i Syslog, należy założyć możliwość implementacji innych interfejsów integracji, np. z wykorzystaniem API
Wymagania całościowe	O11.F29	w zakresie monitoringu pasywnego system musi zapewnić domyślną obsługę zdarzeń, dla których nie zdefiniowano żadnych reguł przetwarzania, aby uniknąć sytuacji, w której informacja o awarii dotychczas nierozpoznanej i niezdefiniowanej w systemie nie zostanie przetworzona i zaprezentowana użytkownikom
Wymagania całościowe	O11.F30	system musi zapewniać metody eskalacji: <ul style="list-style-type: none"> - akcje automatyczne, co najmniej: - uruchomienie zewnętrznego skryptu - wysyłanie wiadomości email - wysyłanie wiadomości SMS
Wymagania całościowe	O11.F31	system musi mieć możliwość konfiguracji powiadamiania/eskalacji dla grupy monitorowanych elementów jak i niezależnie dla każdego monitorowanego elementu konfiguracja eskalacji musi opierać się, co najmniej na: <ul style="list-style-type: none"> - typach zdarzeń/alarmów, dla których wysyłane jest powiadomienie - przedziałach czasowych, w których wysyłane jest powiadomienia (wsparcie dla kalendarza roboczego i nieroboczego - definiowanie kalendarza)
Wymagania całościowe	O11.F32	system musi zapewniać możliwość kreowania powiadomienia/eskalacji na podstawie pól alarmu (np. czas wystąpienia zdarzenia, nazwa monitorowanego elementu, opis zdarzenia) oraz dodawania własnych treści (np. dodatkowy opis wyjaśniający zdarzenie)
Wymagania całościowe	O11.F33	system musi umożliwiać integrację z zewnętrznymi systemami typu Element Managers w celu kolekcji danych o awariach, zdarzeniach - system musi być gotowy na możliwość pobierania danych z Element Manager'ów z obszaru sieci, bezpieczeństwa, z systemów zarządzania infrastrukturą serwerową (część Rozwiązania) oraz środowiskiem kolokacyjnym poprzez API (API zostanie udokumentowane przez dostawców ww. Element Managerów i systemów)

Podobszar	Nr Wymagania	Treść wymagania
Wymagania całościowe	O11.F34	system musi zapewniać integrację z systemem Inventory sieci OSE celem, co najmniej identyfikacji źródeł alarmów oraz celem ich wzbogacania
Wymagania całościowe	O11.F35	system musi zapewniać agregację informacji o stanach poszczególnych elementów w ramach zdefiniowanej usługi, tak, aby na podstawie parametrów pracy jej elementów składowych określić jej aktualny status
Wymagania całościowe	O11.F36	systemu musi w sposób automatyczny udostępniać swoje dane (zdarzenia/alarmy) w miarę potrzeb pozostałym elementom zaimplementowanym w Rozwiązaniu
Wymagania całościowe	O11.F37	system musi umożliwiać automatyczne wykrywanie topologii sieci na poziomie warstwy 3 i 2 modelu ISO/OSI i prezentację jej w sposób graficzny
Wymagania całościowe	O11.F38	system musi umożliwiać kreowanie imiennych użytkowników o różnych poziomach dostępu (np. ReadOnly, ReadWrite, Admin etc.)
Wymagania całościowe	O11.F39	widoki wyświetlane przez użytkowników systemu nie mogą się generować dłużej niż przez 5 sekund
Wymagania całościowe	O11.F40	system musi umożliwiać tworzenie grup użytkowników, np. w celu kreowania większych pakietów uprawnień dla wielu użytkowników, dla których wymagany jest jednakowy poziom dostępu
Wymagania całościowe	O11.F41	system musi mieć możliwość definiowania ról/profilu, które przypisane do użytkowników lub ich grup będą warunkować różne poziomy dostępu (np. dostęp do panelu administracyjnego) i różne uprawnienia (np. wykonywanie operacji zapisu) w ramach systemu
Wymagania całościowe	O11.F42	system musi mieć możliwość restrykcji prezentacji elementów monitorowanej infrastruktury w celu: <ul style="list-style-type: none"> - ograniczenia dostępu użytkownikom tylko do ich infrastruktury (np. dla partnera OSE w danym regionie) - wyświetlania jedynie tych elementów, za które dany użytkownik jest odpowiedzialny
Wymagania całościowe	O11.F43	system musi udostępniać interfejsy integracji pozwalających m.in. na integrację z: <ul style="list-style-type: none"> - elementami i/lub systemami sieciowymi w celu kolekcji danych o awariach (np. z Element Manager'ów) - zewnętrznymi źródłami danych w celu wzbogacania informacji o awariach
Wymagania całościowe	O11.F44	system musi wspierać konfigurację korelacji obsługi zdarzeń z wykorzystaniem informacji o zależnościach funkcjonalnych między elementami infrastruktury OSE, musi być również możliwość dopisywania korelacji "ręcznie", Wykonawca w ramach wdrożenia wykona co najmniej 15 korelacji.

Podobszar	Nr Wymagania	Treść wymagania
Wymagania całościowe	O11.F45	<p>system musi mieć możliwość budowy interfejsów integracji do innych systemów OSS/BSS lub też szyny danych, tak aby umożliwić:</p> <ul style="list-style-type: none"> - publikację danych systemu (eventów, alarmów, kolekcjonowanych metryk) w zewnętrznych systemach, np. szynie danych monitorowaną przez system typu BPM - wykorzystywanie danych z systemów zewnętrznych do wzbogacania i korelacji zdarzeń. System powinien umożliwiać wzbogacanie alarmów o informacje pobrane z zewnętrznych źródeł danych typu Inventory (np. nazwy klienta, nazwy urządzenia) - eksport danych do systemów zewnętrznych, na przykład w celach raportowych, prezentacji statystyk - współpracę systemu w ramach zdefiniowanych procesów operacyjnych, np. obsługa zgłoszeń serwisowych - eskalację informacji o zidentyfikowanych awariach - integrację z systemami typu Trouble Ticketing umożliwiającą automatyczne i półautomatyczne kreowanie/aktualizację/zamykanie zgłoszeń na podstawie zarejestrowanych alarmów
Wymagania całościowe	O11.F46	<p>system musi zapewniać podstawową korelację zdarzeń:</p> <ul style="list-style-type: none"> - deduplikację, czyli identyfikację alarmów dotyczącą dokładnie tego samego zdarzenia i przechowywanie go w repozytorium, jako jednego rekordu (w szczególności flap'owanie interface'ów) - filtrację i automatyczne usuwanie z repozytorium alarmów na podstawie zdefiniowanego kryterium - kategoryzację danych - możliwość oznaczania i agregowania kolekcjonowanych zdarzeń w ramach zdefiniowanych w systemie grup i/lub kategorii - eskalację z alarmu – automatyczne powiadomienia wywoływane na podstawie alarmu i jego zidentyfikowanej treści - wzbogacanie zdarzeń w zakresie informacji dostępnych w systemach zewnętrznych
Wymagania całościowe	O11.F47	system musi zapewniać automatyczną korelację zdarzeń ON/OFF, czyli parowanie zdarzeń, które oznaczają wystąpienie awarii i jej zakończenie (zastosowanie np. dla flapowania interface'ów)
Wymagania całościowe	O11.F48	system musi zapewniać automatyczne wykonywanie akcji (np. skryptu) na podstawie zarejestrowanych zdarzeń/alarmów
Wymagania całościowe	O11.F49	system musi zapewniać mechanizmy archiwizacji zdarzeń/alarmów aktywnych w bazie zdarzeń/alarmów historycznych
Wymagania całościowe	O11.F50	system musi posiadać mechanizmy umożliwiające diagnostykę i monitorowanie wydajności przetwarzania alarmów

Podobszar	Nr Wymagania	Treść wymagania
Wymagania całościowe	O11.F51	podstawowym interfejsem systemu musi być aplikacja webowa, stanowiąca konsolę operatorsko-administracyjny
Wymagania całościowe	O11.F52	system musi zapewnić możliwość integracji z CSR (Centralny System Raportowy) celem przekazania danych do raportów, w szczególności np. dane parametrów jakościowych szkieletu OSE (opóźnienia, straty pakietów itp.) mają być ostatecznie prezentowane w Portalu Usługowym
Wymagania całościowe	O11.F53	system musi udostępniać informację typu audytowego pozwalającego na weryfikację działań użytkowników zawierającą, co najmniej następujące danych: <ul style="list-style-type: none"> - czas logowania użytkownika - adres/hostname źródłowy - niepoprawne próby logowania - błędy wykonywania działań w ramach interfejsu użytkownika, ze wskazaniem danych użytkownika - inne informacje wspomagające diagnostykę i identyfikację naruszeń bezpieczeństwa system wymagany czas przechowywania danych audytowych to 12 miesięcy
Wymagania całościowe	O11.F54	system musi posiadać predefiniowane widoki prezentujące stan monitorowanej infrastruktury; widoki te powinny jednak umożliwiać modyfikację, a także powinna być możliwość kreowania nowych widoków, także w oparciu o te istniejące
Wymagania całościowe	O11.F55	system musi umożliwiać konfigurację własnych stron prezentacji (zespołu widoków), które równocześnie mogłyby zostać przypisane konkretnym użytkownikom lub grupom użytkowników
Wymagania całościowe	O11.F56	system musi posiadać: <ul style="list-style-type: none"> - zestaw predefiniowanych elementów wizualizacyjnych, za pomocą, których użytkownik może budować złożone widoki (dashboardsy) : - listy/tabele zdarzeń - różnego typu wykresy pozwalające na prezentację danych ilościowych i statystycznych (np. grafy, pie-chart'y, histogramy - mapy topologii oraz mapy budowane statycznie z możliwością podłożenia mapy bitowej lub wektorowej, jako tło pod mapę sieć - możliwość budowy struktury hierarchicznej, pozwalającej na przejście „od ogółu do szczegółu” (tzw. funkcjonalność „drill-down”); funkcjonalność ta ma pozwalać na budowę ogólnych widoków prezentujących w sposób wysokopoziomowy aktualny stan monitorowanej sieci, jednocześnie pozwalać na szybkie wyświetlenie widoków bardziej szczegółowych, np. dotyczących konkretnej monitorowanej lokalizacji - możliwość zdefiniowania zindywidualizowanych map/widoków

Podobszar	Nr Wymagania	Treść wymagania
		użytkowników umożliwiających przeglądanie fragmentów monitorowanej sieci
Wymagania całościowe	O11.F57	<p>lista alarmów dostępna w systemie musi zapewniać następujące funkcjonalności:</p> <ul style="list-style-type: none"> - możliwość filtracji prezentowanych alarmów - odpowiednie oznaczanie różnych priorytetów alarmów, np. poprzez zróżnicowaną kolorystykę - sortowanie listy alarmowej według prezentowanych kolumn - możliwość kreowania widoków alarmów poprzez wyświetlanie wybranych atrybutów w formie osobnych kolumn listy - możliwość dynamicznego przeszukiwania listy
Wymagania całościowe	O11.F58	<p>elementy warstwy prezentacji muszą pozwalać na wykonywanie z ich poziomu kontekstowych akcji (uzależnione od uprawnień użytkownika, konfigurowalne per profil/grupa/użytkownik) :</p> <ul style="list-style-type: none"> - potwierdzanie alarmu - usuwanie alarmu - zmiana priorytetu alarmu - przypisanie użytkownika
Wymagania całościowe	O11.F59	<p>system w zakresie prezentacji musi zapewniać funkcjonalności raportowe związane zarówno z obsługą zdarzeń bieżących jak i historycznych i zapewniać następujące funkcje:</p> <ul style="list-style-type: none"> - prezentacja danych w formach tabelarycznych i graficznych z możliwością agregowania (grupowania) danych - predefiniowane raporty dostępne per element, grupa elementów - możliwość generowania porównawczych raportów zbiorczych, np. w celu określenia najbardziej awaryjnych elementów bądź typów elementów - eksport raportów do plików w popularnych formatach (co najmniej CSV, XLS, TXT) - możliwość kreowania własnych raportów <p>wymagany czas przechowywania zdarzeń historycznych to 12 miesięcy</p> <p>wymagany czas przechowywania raportów to 12 miesięcy</p>
Wymagania całościowe	O11.F60	<p>system musi zapewniać mechanizmy kontroli swojego działania umożliwiające :</p> <ul style="list-style-type: none"> - przeprowadzanie diagnostyki funkcjonowania systemu (troubleshooting) - dynamiczne serwisy logowania i śledzenia konfigurowane w trakcie działania system - przeprowadzanie weryfikacji czynności wykonywanych przez użytkowników systemu

Podobszar	Nr Wymagania	Treść wymagania
		- podgląd dziennika zdarzeń systemowych oraz akcji podejmowanych przez użytkownika (np. dodanie bądź usunięcie obiektu)
Wymagania całościowe	O11.F61	system musi mieć możliwość wykonywania kompletnego backupu konfiguracji systemu oraz zbieranych danych wraz z możliwością bezproblemowego odtworzeni
Wymagania całościowe	O11.F62	system musi mieć możliwość uruchomienia odrębnej, niezależnej instancji testowej systemu bez dodatkowych kosztów licencji lub przy wykorzystaniu licencji ze środowiska produkcyjnego
Wymagania całościowe	O11.F63	system musi posiadać wsparcie producenta lub/i społeczności w zakresie integrowanych typów urządzeń a także rozwoju funkcjonalności pod kątem nowych technologii i nowych typów urządzeń przez cały okres obowiązywania Umowy
Wymagania całościowe	O11.F64	system musi zapewniać automatyczny provisioning pomiarów (Availability) oraz możliwości poprawnego odbioru alarmów w wyniku provisioningu nowej usługi w sieci OSE (w systemie provisioningu będącego integralną częścią Rozwiązania
Wymagania całościowe	O11.F65	system musi mieć możliwość czasowego wyłączenia powiadomień/eskalacji dla danej osoby (np. w czasie urlopu) lub dla pojedynczego monitorowanego elementu lub grupy elementów
Wymagania całościowe	O11.F66	system musi zapewniać funkcjonalności RCA (root cause analysis) - analiza źródłowej przyczyny awarii musi opierać się również na topologii sieci
Wymagania całościowe	O11.F67	system musi zapewniać funkcjonalność Topology Managment (przynajmniej w obszarze węzłów OSE i sieci szkieletowej
Wymagania całościowe	O11.F68	system musi posiadać dedykowany silnik korelacji i możliwość definiowania własnych automatyzacji i korelacji
Wymagania całościowe	O11.F69	system musi mieć możliwość budowy integracji z systemem provisioningu w kierunku do systemu provisioningu pozwalającą na automatyczne wywoływanie akcji naprawczych
Wymagania całościowe	O11.F70	elementy warstwy prezentacji muszą pozwalać na wykonywanie z ich poziomu kontekstowych akcji (uzależnione od uprawnień użytkownika, konfigurowalne per profil/grupa/użytkownik) : - dodawanie komentarzy do alarmu - tworzenie zgłoszenia w systemie SD - uruchamianie skryptu (np. z akcją naprawczą)
Wymagania całościowe	O11.F71	system musi mieć możliwość ustalania harmonogramów dla automatycznego generowania i dystrybucji raportów albo w ramach OSS lub/i przy wykorzystaniu Centralnego Systemu Raportowego

Podobszar	Nr Wymagania	Treść wymagania
Wymagania całościowe	O11.F72	system musi wspierać funkcjonalność okien serwisowych, które mają wpływ na pozostałe elementy systemu (np. nie wystawiania alarmów z pomiarów Availability w trakcie trwania okna): <ul style="list-style-type: none"> - możliwość definiowania okien serwisowych - definiowanie okien serwisowych w wyniku integracji z procesem biznesowym (działu utrzymania) - prezentacja graficzna w raportach i statystykach - dostępność historii
Wymagania całościowe	O11.F73	system musi mieć możliwość integracji z mapami online, np. OpenStreetMap czy Google Maps

7.4.1.2 Funkcjonalność Performance Management

System Performance Management swoją funkcjonalnością ma wspierać procesy utrzymania sieci, usług i systemów OSE a w szczególności monitorować wydajność urządzeń i wykorzystanie zasobów sieci OSE.

System Performance Management ma pozwalać na zbieranie danych związanych z wydajnością urządzeń w szkieletcie OSE i w jednostkach oświatowych, z systemów w centrach kolokacji, także aplikacji i świadczonych w sieci OSE service'ów oraz obciążenia ruchem łącz szkieletowych i dostępowych. Zakres monitorowania obejmował będzie te same elementy infrastruktury, co system Fault & Availability Management. System ma monitorować dużą ilość różnorodnych urządzeń, łącz i systemów, parametrów itp. W celu prezentacji tych danych będą generowane automatycznie statystyki oraz raporty. Ze względu na dużą ilość danych wydajność bazy danych jak i wszelkie zaimplementowane mechanizmy bazodanowe i graficzne muszą gwarantować odpowiednią wydajność.

Rozwiązanie musi wygodnie prezentować statystyki i raporty z pomiarów a także umożliwiać tworzenie widoków w różnych aspektach zainteresowania i dla różnych grup użytkowników.

Muszą być prezentowane, co najmniej:

- statystyk on-line i raporty z jakości działania sieci i usług OSE (opóźnienia, straty, jittery, dostępność urządzeń i serwisów),
- statystyki i raporty parametrów ruchowych w szkieletcie OSE oraz na łączach do szkół (konieczne badanie ruchu per VLAN szkolny - szkoła może mieć jednocześnie do 5 VLAN),
- statystyki i raporty wydajności serwerów i urządzeń sieciowych (CPU, RAM itp.)
- statystyki i raporty środowiskowe (temperatura w urządzeniach, temperatura w szafach kolokacyjnych itp.)
- raporty z pomiarów jakości sieci w relacjach pomiędzy węzłami OSE

System musi zapewnić następujące główne funkcjonalności związane z kolekcją danych:

- monitoring sieci w warstwie 2 i 3 modelu ISO/OSI;

- monitoring przy użyciu wielorakich protokołów: ICMP, SNMP, RPING, HTTP, HTTPS oraz opcjonalnie OAM
- monitoring w relacjach pomiarowych E2E przy użyciu protokołów typu Two-Way: TWAMP lub/i rozwiązań producenckich (np. Juniper RPM, Cisco IP SLA Monitoring, Huawei NQA, Alcatel SAA) bezpośrednio z systemu lub poprzez API do Element Managera do urządzeń sieciowych (kupowany w oddzielnym postępowaniu zakupowym);
- współpraca systemu monitoringu z ruterami shadow bezpośrednio lub via Element Manager do urządzeń sieciowych
- monitoring parametrów jakościowych (opóźnienia, straty, jittery w warstwie IP) w szczególności mierzone/wyliczane w okresach dostępności
- monitoring aplikacji, systemów operacyjnych, urządzeń serwerowych i sieciowych; ze względu na spodziewaną różnorodność typów elementów infrastruktury OSE (system powinien zapewniać szeroki wachlarz gotowych rozwiązań monitorowania)
- monitoring parametrów jakościowych łącz a w szczególności monitoring ruchu, poziomu błędów itp. na łączach szkieletowych i dostępowych do jednostek oświatowych:
- monitoring ruchu w szkielecie sieci (ruch do CPE w szkole mierzony na subinterface'ach urządzeń w węzłach OSE)
- pomiary serwisów świadczonych w systemach OSE
- konfiguracja sensorów i próbkowania – możliwość regulacji częstotliwości odpytywania poszczególnych elementów sieciowych, jak również sposobu pobierania danych (np. wybór odpowiedniego protokołu)
- możliwość zapisania konfiguracji monitorów urządzenia do pliku oraz odtworzenia jej na wielu urządzeniach (jeżeli zachodzi potrzeba identycznej konfiguracji dużej liczby urządzeń);
- potencjalnie automatyczne wykrywanie typu urządzeń, systemów, aplikacji i usług na podstawie, którego możliwe będzie automatyczne tworzenie pomiarów:
 - w zakresie wykrywania system powinien wspierać, co najmniej poniższe protokoły: ICMP, skanowanie TCP/UDP, SNMP, SSH, Webservice
 - system powinien udostępniać panel konfiguracyjny wykrywania za pomocą, którego można określić podstawowe parametry procesu, np.: zakresy sieci IP, wykluczenia podsieci, określanie parametrów dostępu (np. community)
 - system powinien umożliwiać przypisanie domyślnych szablonów monitorowania na podstawie danych pozyskanych w wyniku procesu wykrywania infrastruktury
- system musi posiadać funkcjonalność automatycznego tworzenia pomiarów z poziomu zewnętrznych systemów np. z poziomu systemu provisioningu poprzez udostępnienie dedykowanego API

Założenia dotyczące architektury pomiarów

1. W zakresie Performance Management sieć szkieletowa OSE, czyli wszystkie urządzenia w węzłach centralnych i regionalnych OSE (zarówno urządzenia sieciowe jak i urządzenia i systemy

bezpieczeństwa) będą, co najmniej odpytywane o standardowe parametry wydajnościowe (jak w tabeli poniżej). W przypadku serwerów objętych wirtualizacją w węzłach centralnych monitoring będzie wykonywany przez system DCIM (Data Center Infrastructure Monitoring) - zakłada się możliwość przekazywania informacji pomiędzy systemem DCIM a Performance Management. Istotnym pomiarem wykonywanym na urządzeniach w szkieletcie sieci OSE jest pomiar ruchu na interfejsach i subinterfejsach - jest on niezbędny w celu monitoringu wysycenia zamawianych u operatorów łącz oraz monitoringu wykorzystania pasma przez poszczególne szkoły w lokalizacji. W tym kontekście należy założyć, że:

- a. każda szkoła może mieć skonfigurowanych do 5 VLAN'ów (wyniesionych na warstwie II do węzła OSE) i jest konieczny monitoring ruchu per każdy VLAN oddzielnie
 - b. muszą być wykonywane stosowne pomiary, wyliczenia progów wysycenia łącz oraz raportowanie i alarmowanie stanu wysycenia łącz na bazie pomiaru ruchu na portach fizycznych i logicznych
 - c. musi być możliwość wyliczania wykorzystania zamówionej przez szkołę przepływności, jako suma ruchu we wszystkich VLANach danej szkoły
 - d. musi być możliwość wyliczania wykorzystanej przepustowości z danej lokalizacji szkolnej, jako suma ruchu we wszystkich VLANach wszystkich szkół w lokalizacji
 - e. statystyki ruchu z ostatniej doby są przetrzymywane w postaci próbek z dokładnością 5 minutową
 - f. statystyki ruchu z ostatniego tygodnia są przetrzymywane w postaci zagregowanych próbek z dokładnością do 15 minut
 - g. statystyki ruchu z ostatniego miesiąca są przetrzymywane w postaci zagregowanych próbek z dokładnością do 30 minut
 - h. statystyki ruchu z ostatniego roku są przetrzymywane w postaci zagregowanych próbek z dokładnością do 60 minut
 - i. zagregowane statystyki roczne są przechowywane do 5 lat wstecz
2. W przypadku urządzeń CPE zainstalowanych w szkołach pomiary performance'owe jak i potencjalnie pomiary utylizacji portów downstream i upstream będą wykonywane tylko w okresach 3 tygodni po podłączeniu szkoły/lokalizacji szkolnej do sieci OSE oraz w przypadkach niezbędnej diagnostyki zgłoszonych przez szkołę problemów. W przypadku urządzeń SW i AP monitoring taki będzie aktywowany w przypadku zgłoszonych problemów ze szkoły i po decyzji operatora OSE oraz skonfigurowaniu dostępu do tych urządzeń tak by był możliwy. Zakłada się częstotliwość pomiarów performance'owych standardowo na poziomie 300 sekund.
3. Zakłada się również konieczność pomiarów relacji w szkieletcie sieci OSE - FULL MESH między 19-toma węzłami OSE (16 regionalnych i 3 centralne) pomiędzy ruterami shadow w klasach ruchu celem pomiaru opóźnień, strat pakietów i wielkości jittera w tych relacjach i w klasach ruchu. W początkowym okresie sieci OSE będą zaimplementowane 2 klasy ruchu: NC (Network Control) i BE (Best Effort), docelowo w szkieletcie sieci OSE będzie zaimplementowanych do 5 klas ruchu. Zamawiający w sieci szkieletowej będzie stosował klasy ruchu i sposób kolejkowania w oparciu o CBQoS. Pomiary będą wykonywane z częstotliwością 300 sekund. Routery shadow są elementem innego postępowania zakupowego, Zarządzanie pomiarami na routerach shadow pozostaje w obowiązku Wykonawcy, który:

- a. może wykorzystać własne Rozwiązanie OSS w celu komunikacji z ruterami shadow
- b. lub może wykorzystać funkcjonalność Element Managerów (kupowanych w oddzielnym postępowaniu zakupowym) i via API do Element Managera by takie pomiary zakładać i pobierać wyniki pomiarów
- c. ostatecznie musi zapewnić pojawianie się raportów z wynikami tych pomiarów w Centralnym Systemie Raportowym by z niego dalej publikować te raporty na portalu OSE

W tabeli poniżej przedstawiono zestawienie typów pomiarów, jakie powinny być realizowane przez system w ramach poszczególnych obszarów monitorowania. Zakłada się, że Wykonawca przeanalizuje optymalność przedstawionego planu pomiarów i jeśli zaistnieje taka potrzeba to po akceptacji Zamawiającego wprowadzi stosowne modyfikacje.

Obszar monitorowania	Pomiary	Częstotliwość	Uwagi
Sieć szkieletowa	Dostępność urządzenia/interfejsów	1 minuta	opcjonalnie - w razie doraźnej potrzeby - częstotliwość może zostać zwiększona do 1 minuty
	Opóźnienia	5 minut	
	Straty pakietów	5 minut	
	Jitter	5 minut	
	Utylizacja interfejsów	5 minut	
	Błędy na interfejsach	5 minut	
	Utylizacja CPU	5 minut	
	Utylizacja pamięci	5 minut	
	Parametry środowiskowe – voltage, temperatura	5 minut	
	Dedykowane relacje pomiarowe E2E (w klasach ruchu)	5 minut	
	Opóźnienia	5 minut	
	Straty pakietów		
	Jitter		
Urządzenia OSE w jednostkach oświatowych	Dostępność urządzenia CPE, SW, AP	5 minuta	w okresach 3 tygodni po uruchomieniu szkoły oraz w przypadku diagnostyki problemu z usługą/urządzeniem
			j.w.

Obszar monitorowania	Pomiary	Częstotliwość	Uwagi
	Utylizacja interfejsów, błędy na interface (upstream, downstream)	5 minut	j.w.
		5 minut	j.w.
	Utylizacja CPU	5 minut	jw.
	Utylizacja pamięci		
	Opcjonalnie: Opóźnienia sieci Straty pakietów Jitter	5 minut	
Infrastruktura serwerowa i aplikacje	Dostępność serwerów i aplikacji	5 minuta	Dostępność aplikacji może być weryfikowana za pośrednictwem dedykowanych agentów systemowych lub w przypadku ich braku na zasadzie weryfikacji dostępności określonych portów i/lub procesów.
	Statystyki wydajnościowe serwerów i systemów wirtualnych: CPU, RAM, load average, zajętość dysku, service'u itp.	5 minut	
	WebMonitoring – monitorowanie dostępności stron WWW poprzez dedykowane sekwencje testowe	5 minut	
	Monitorowanie specyficznych usług aplikacji (dostępności portów TCP,UDP)		

System Performance Management w warstwie agregacji i przetwarzania będzie realizować zadania związane z procesowaniem kolekcjonowanych danych wydajnościowych, głównie ich agregacją.

Najważniejsze funkcjonalności, które muszą charakteryzować system:

- Agregacja danych: dane z różnych źródeł mogą być kolekcjonowane z różnymi interwałami a system powinien zaprezentować dane dla różnych przedziałów czasowych, zatem zapewniać mechanizmy agregacji i uśredniania danych.
- Korelacja danych wydajnościowych, w tym ewaluacja danych pochodzących z różnych źródeł (np. kalkulacja złożonych metryk)

- Wspomaganie identyfikacji problemu na podstawie analizy krzyżowej danych z różnych urządzeń. (kompleksowa analiza wydajności sieci umożliwiająca porównywanie wskaźników dotyczących różnych elementów może wspomagać znacząco diagnostykę i pozwalać na szybszą identyfikację problemu)
- Możliwość generowania alarmów i/lub notyfikacji dotyczących przekroczenia zadanych progów - także wielopoziomowych - oraz odchyłeń od linii bazowych (monitorowanie wydajności infrastruktury pozwala na proaktywne monitorowanie i reagowanie na problemy zanim faktycznie wystąpią)
- Wyznaczanie trendów i prognoz z uwzględnieniem ich konfigurowalnych okresów (funkcjonalność istotne z perspektywy planowania pojemności sieci)
- Automatyczna predykcja wysycenia zasobów (przede wszystkim pojemności łącz) w oparciu o uśrednione dane historyczne i wyznaczanie trendów
- Posiadanie udokumentowane API, za pośrednictwem, którego będzie możliwa implementacja niestandardowych interfejsów integracji, a także publikacja zgromadzonych i zagregowanych danych w innych systemach OSS/BSS lub/i w portalu OSE

Wymagania funkcjonalne

Podobszar	Nr Wymagania	Treść wymagania
Szczególne wymagania pod kątem monitorowania sieci szkieletowej oraz łącz agregacyjnych i dostępowych	O12.F1	dla łącz szkieletowych system musi przedstawiać wizualizacje zajętości łącz w formie network weathermap
Szczególne wymagania pod kątem monitorowania sieci szkieletowej oraz łącz agregacyjnych i dostępowych	O12.F2	system musi mieć możliwość monitoringu relacji pomiarowych pomiędzy węzłami OSE przy pomocy protokołu typu Two-Way: TWAMP lub/i rozwiązań producenckich (np. Juniper RPM i Cisco IP SLA Monitoring, Huawei NQA, Alcatel SAA) z uwzględnianiem pomiarów w klasach ruchu, w szczególności: <ul style="list-style-type: none"> - opóźnień w warstwie IP (we wszystkich klasach usług i wszystkich relacjach międzywęzłowych) - strat pakietów w warstwie IP (we wszystkich klasach usług i wszystkich relacjach międzywęzłowych) - jittera w warstwie IP (we wszystkich klasach usług i wszystkich relacjach międzywęzłowych) poprzez wykorzystanie własnych mechanizmów lub via API przy wykorzystaniu funkcjonalności Element Managera do urządzeń sieciowych (kupowany w oddzielnym postępowaniu zakupowym)

Podobszar	Nr Wymagania	Treść wymagania
		ostatecznie Rozwiązanie musi zapewnić pojawianie się raportów z wynikami tych pomiarów w Centralnym Systemie Raportowym by z niego dalej publikować te raporty na Portalu Usługowym
Szczególne wymagania pod kątem monitorowania sieci szkieletowej oraz łącz agregacyjnych i dostępowych	O12.F3	system musi mieć możliwość pomiarów kolejek dla poszczególnych klas ruchu na interface'ach i subinterface'ach urządzeń sieciowych w szkielecie OSE
Szczególne wymagania pod kątem monitorowania sieci szkieletowej oraz łącz agregacyjnych i dostępowych	O12.F4	system musi umożliwiać wykonywanie cyklicznych pomiarów typu „Speedtest” dla dowolnej ścieżki sieciowej z możliwością wykonywania pomiaru w klasie ruchu, system musi zapewniać korelację zebranych danych (dla poszczególnych klas ruchu) z m. in. : <ul style="list-style-type: none"> - parametrami jakości sieci - informacjami o wielkości ruchu w sieci - dostępnością poszczególnych węzłów OSE/hostów
Szczególne wymagania pod kątem monitorowania sieci szkieletowej oraz łącz agregacyjnych i dostępowych	O12.F5	system musi zapewniać możliwość konfigurowania specyficznych pomiarów diagnostycznych (np. wykonanie pomiaru w określonej klasie ruchu) i wywoływania ich „na żądanie”
Wymagania całościowe	O12.F6	system musi zbierać informacje co najmniej o : <ul style="list-style-type: none"> - wydajności urządzeń (zajętość CPU, zajętość RAM, zajętość FIB w przypadku urządzeń sieciowych itd.) - zajętości łącz (szkieletowych, agregacyjnych, dostępowych, uplinków na podstawie counterów na interface'ach fizycznych i logicznych oraz alarmować przekroczenia thresholdów - błędach na interface'ach - parametrach środowiskowych (temperatura powietrza chłodzącego, zasilanie itp.)
Szczególne wymagania dotyczące monitorowania urządzeń w sieci LAN w szkołach	O12.F7	system musi zbierać parametry dotyczące parametrów łącz z każdego aktywnego interface'u i subinterface'u
Szczególne wymagania dotyczące monitorowania	O12.F8	system musi mieć możliwość zbierania parametrów z interface'ów fizycznych i logicznych z portów WAN i LAN na CPE

Podobszar	Nr Wymagania	Treść wymagania
urządzeń w sieci LAN w szkołach		
Szczególne wymagania dotyczące monitorowania urządzeń w sieci LAN w szkołach	O12.F9	w przypadku urządzeń CPE zainstalowanych w szkołach system musi wykonywać pomiary performance'owe jak i pomiary utylizacji portów w okresach 3 tygodni po podłączeniu szkoły/lokalizacji szkolnej do sieci OSE oraz w przypadkach niezbędnej diagnostyki (należy założyć średnio do 2 tygodni) zgłoszonych przez szkołę problemów, system musi w tych okresach badać dostępność CPE pod kątem oceny działania łącza od lokalnego dostawcy
Szczególne wymagania dotyczące monitorowania urządzeń w sieci LAN w szkołach	O12.F10	w przypadku urządzeń SW i AP zainstalowanych w szkołach system musi monitorować performance i utylizację portów tych urządzeń w okresach diagnostyki (należy założyć średnio do 2 tygodni) w przypadku zgłoszonych problemów ze szkoły - w celu wykonania tych pomiarów będzie odpowiednio skonfigurowany dostęp do urządzeń należy założyć, że okresy diagnostyczne mogą mieć miejsce w razie potrzeby również w okresach 3 tygodni po podłączeniu szkoły
Szczególne wymagania pod kątem monitorowania urządzeń infrastruktury serwerowej	O12.F11	Rozwiązanie musi umożliwiać integrację pomiędzy CSR (Centralny system Raportowy) a dedykowanym systemem zarządzania infrastrukturą serwerową na poziomie standardowych mechanizmów integracji (co najmniej REST API oraz poprzez wymianę plików w standardowych formatach - CSV, XML, JSON, XLS) w celu prezentowania najważniejszych parametrów wydajnościowych infrastruktury w jednym miejscu, czyli w CSR
Wymagania całościowe	O12.F12	system musi posiadać wsparcie dla architektury rozproszonej – możliwość kolekcji danych poprzez wydzielone dedykowane moduły programowe (kolektory)
Wymagania całościowe	O12.F13	celem mniejszego obciążania łącz pomiędzy węzłami OSE system musi zostać zaimplementowany w architekturze rozproszonej tak by kolekcja danych znajdowała się możliwie jak najbliżej źródła danych; należy uwzględnić architekturę zapewniającą to, że logiczne warstwy systemu wymagające większej wydajności i niezawodności (warstwa prezentacji i przetwarzania danych) były ulokowane w węzłach centralnych
Wymagania całościowe	O12.F14	kolektory muszą zapewniać możliwość konfiguracji częstotliwości pollingu per monitorowany element i/lub typ elementu.
Wymagania całościowe	O12.F15	system musi być tak wyskalowany, aby zapewnić wydajny monitoring wszystkich wymaganych parametrów z minimalną częstotliwością pollingu równą 300 sekund
Wymagania całościowe	O12.F16	kolektory muszą zapewnić buforowanie danych na wypadek braku łączności z jednostką centralną przez okres 36 godzin

Podobszar	Nr Wymagania	Treść wymagania
Wymagania całościowe	O12.F17	<p>systemy standardowo musi przechowywać:</p> <ul style="list-style-type: none"> - surowe dane pomiarowe przez 6 miesięcy - dane zagregowane przez 12 miesięcy <p>jednakże z uwzględnieniem wyjątków:</p> <ol style="list-style-type: none"> 1. statystyki ruchowe (szkielet, agregacja, dostęp - w tym per VLAN szkoły): <ul style="list-style-type: none"> - statystyki ruchu z ostatniej doby mają być przechowywane w postaci próbek z dokładnością 5 minutową - statystyki ruchu z ostatniego tygodnia mają być przechowywane w postaci zagregowanych próbek z dokładnością do 15 minut - statystyki ruchu z ostatniego miesiąca mają być przechowywane w postaci zagregowanych próbek z dokładnością do 30 minut - statystyki ruchu z ostatniego roku mają być przechowywane w postaci zagregowanych próbek z dokładnością do 60 minut- - zagregowane statystyki roczne z ruchu mają być przechowywane do 5 lat wstecz 2. statystyki performance'owe (typu CPE, memory, storage, temp. , itp.): <ul style="list-style-type: none"> - próbki surowe (5 minutowe) mają być przechowywane 3 tygodnie
Wymagania całościowe	O12.F18	system musi dawać możliwość elastycznego konfigurowania parametrów agregacji i przechowywania danych pomiarowych per urządzenie/ grupa urządzeń
Wymagania całościowe	O12.F19	system musi mieć możliwość dostosowywania parametrów poszczególnych kolektorów do specyfiki monitorowanego segmentu sieci
Wymagania całościowe	O12.F20	system musi zapewniać skalowalność horyzontalną i możliwość prostej rozbudowy systemu poprzez dołożenie dodatkowych kolektorów i/lub instancji części centralnej
Wymagania całościowe	O12.F21	system musi posiadać dokumentowane API pozwalające na budowę dodatkowych typów interfejsów północnych i południowych
Wymagania całościowe	O12.F22	system musi prezentować statystyki z pomiarów a także umożliwiać tworzenie widoków w różnych aspektach zainteresowania i dla różnych grup użytkowników
Wymagania całościowe	O12.F23	system musi zapewniać monitoring sieci w warstwie 2 i 3 modelu ISO/OSI
Wymagania całościowe	O12.F24	system musi zapewniać monitoring przy użyciu co najmniej następujących protokołów: RTT ICMP, SNMP, RPING, HTTP, HTTPS (protokół OAM do wykorzystania w dalszych etapach projektu OSE)
Wymagania całościowe	O12.F25	system musi zapewniać monitoring w relacjach pomiarowych E2E przy użyciu protokołów typu Two-Way: TWAMP lub/i rozwiązań producenckich (np. Juniper RPM, Cisco IP SLA Monitoring, Huawei NQA, Alcatel SAA) bezpośrednio z systemu lub poprzez API do Element Managera do urządzeń sieciowych, w związku z tym wymagane jest zarządzanie pomiarami:

Podobszar	Nr Wymagania	Treść wymagania
		<ul style="list-style-type: none"> - poprzez współpracę z ruterami typu shadow bezpośrednio lub/i via API do Element Managera urządzeń sieciowych by pomiary zakładać i pobierać wyniki pomiarów - poprzez zapewnienie wykonywania pomiarów opóźnień, strat pakietów, wielkości jitter pomiędzy węzłami OSE (z uwzględnieniem klas ruchu i vrf) - poprzez zapewnienie cyklicznego pojawiania się raportów z wynikami pomiarów w Centralnym Systemie Raportowym by dalej z niego publikować te raporty na Portalu Usługowym
Wymagania całościowe	O12.F26	system musi zapewniać monitoring parametrów systemów operacyjnych zarówno będących częścią Rozwiązania jak i systemów OSE poza Rozwiązaniem (Element Manager, systemy bezpieczeństwa jak SIEM, SWG, DNS, systemy sieciowe jak Radius, NTP, LDAP, DHCP a także portal OSE) . Ze względu na spodziewaną różnorodność typów elementów infrastruktury OSE system powinien zapewniać szeroki wachlarz gotowych rozwiązań monitorowania (predefiniowane template'y)
Wymagania całościowe	O12.F27	<p>system musi zgłaszać przekroczenia założonych tresholdów/progów na zdefiniowanych pomiarach, w szczególności na pomiarach:</p> <ul style="list-style-type: none"> - wydajności urządzeń i systemów (zajętość CPU, zajętość RAM, zajętość FIB w przypadku urządzeń sieciowych itd.) - zajętości łącz (szkieletowych, agregacyjnych, dostępowych, uplinków) - parametrów środowiskowych (temperatura powietrza chłodzącego, zasilanie itp.)
Wymagania całościowe	O12.F28	przekroczenia progów pomiarowych muszą skutkować wygenerowaniem alarmu przesłanego do systemu Fault Management
Wymagania całościowe	O12.F29	dla przekroczeń progów pomiarowych system musi wspierać generowanie alarmów na podstawie wielopoziomowych progów i linii bazowych
Wymagania całościowe	O12.F30	system musi umożliwiać pomiary jakości ruchu (opóźnienia, straty pakietów, jitter) dla ruchu typu HTTP / HTTPS, RTT ICMP, TCP, UDP
Wymagania całościowe	O12.F31	<p>System musi przedstawiać wykresy zajętości łącz (dla wszystkich łącz na poziomie łącza fizycznego i łącza logicznego / subinterfejsu), w szczególności mają być zbierane cyklicznie, co najmniej :</p> <ul style="list-style-type: none"> - ruch IN i OUT z interfaśów i subinterfaśów (VLAN per szkoła) na urządzeniach w węzłach OSE oraz prezentowane w postaci statystyk graficznych - poziom błędów z interfejsu na urządzeniach w węzłach OSE oraz prezentowane w postaci statystyk graficznych
Wymagania całościowe	O12.F32	system musi prezentować statystyki ruchu per VLAN szkolny (zakłada się, że per szkoła może zostać skonfigurowanych do 5 VLAN) , opis statystyki ma zawierać dane identyfikujące szkołę i jej usługę (np. nazwa, RSPO, VLAN)

Podobszar	Nr Wymagania	Treść wymagania
Wymagania całościowe	O12.F33	system na podstawie pomiarów ruchu musi generować cykliczne raporty na temat co najmniej 95-percentyla i GNR (Godzina Największego Ruch)
Wymagania całościowe	O12.F34	<p>pomiar ruchu generowanego przez szkoły musi polegać na odnotowaniu, co 5 minut liczby przesłanych bajtów w każdym kierunku, na tej podstawie mają być określone różne parametry/charakterystyki ruchu, co najmniej:</p> <ul style="list-style-type: none"> - 95-ty percentyl średnich pięciominutowych określany jako największa średnia 5-cio minutowa spośród próbek średnich 5-cio minutowych pozostałych po odjęciu 5% z próbek z największymi wartościami w zadanym okresie, w kierunku „do” i „od” szkoły – w ujęciu dobowym, tygodniowym i miesięcznym - Godzina Największego Ruchu (GNR) określana, jako początek godziny (z dokładnością do 5-ciu minut) w trakcie której przesłano największą liczbę bajtów – w kierunku „do” i „od” szkoły – w ujęciu dobowym, tygodniowym i miesięcznym (dla doby GNR zawiera się w przedziale od godziny 0:00 do 23:00, dla tygodnia od niedzieli godzina 0:00 do soboty godzina 23:00, dla miesiąca od pierwszego dnia miesiąca, godzina 0:00 do ostatniego dnia miesiąca, godzina 23:00) - średni ruch w GNR w Mb/s określany jako: $[\text{Średni_ruch_w_GNR}] = \frac{([\text{liczba_przesłanych_bajtów}](w_czasie_GNR+60_minut) - [\text{liczba_przesłanych_bajtów}](w_czasie_GNR)) \times 8}{3600 / 1000000}$ w kierunku „do” i „od” szkoły – w ujęciu dobowym, tygodniowym i miesięcznym - średnią prędkość 5-cio minutową przesyłania danych w Mb/s wg formuły: $[\text{Średnia_5-cio_minutowa}](w_czasie_t) = \frac{([\text{liczba_przesłanych_bajtów}](w_czasie_t) - [\text{liczba_przesłanych_bajtów}](w_czasie_t-5_minut)) \times 8}{300 / 1000000}$
Wymagania całościowe	O12.F35	system musi wspierać badanie wysycenia wszystkich łącz a w szczególności łącz dostępowych i eskalować mailowo w oparciu o kilka poziomów wysycień łącz
Wymagania całościowe	O12.F36	system musi monitorować działanie portalu OSE (czasy odpowiedzi, czasy ładowanie stron itp.) oraz wystawianych przez niego API do integracji z Portalem Usługowym
Wymagania całościowe	O12.F37	system musi umożliwiać konfigurację kolektorów i próbkowania – możliwość regulacji częstotliwości odpytywania poszczególnych elementów sieciowych, jak również sposobu pobierania danych (np. wybór odpowiedniego protokołu), próbkowanie ma być wyzwalane systemowo zgodnie ze skonfigurowanym harmonogramem lub przez operatora z konsoli

Podobszar	Nr Wymagania	Treść wymagania
Wymagania całościowe	O12.F38	system musi zapewniać możliwość exportu danych do standardowych formatów plików (co najmniej CSV, XLS, XML, JSON) z pomiarów „real-time” na żądanie użytkownika
Wymagania całościowe	O12.F39	system musi zapewniać możliwość chwilowego wyłączenia monitorowania wybranych urządzeń przez operatora.
Wymagania całościowe	O12.F40	system musi zapewniać możliwość zapisania konfiguracji monitorów urządzenia do pliku oraz odtworzenia jej na wielu urządzeniach (jeżeli zachodzi potrzeba identycznej konfiguracji dużej liczby urządzeń)
Wymagania całościowe	O12.F41	system musi udostępniać panel konfiguracyjny wykrywania monitorowanych urządzeń za pomocą, którego można określić podstawowe parametry procesu wykrywania, np. zakresy sieci IP, wykluczenia podsieci, określanie parametrów dostępu (np. community) itp.
Wymagania całościowe	O12.F42	system musi umożliwiać przypisanie domyślnych szablonów monitorowania na podstawie danych pozyskanych w wyniku procesu wykrywania infrastruktury
Wymagania całościowe	O12.F43	system musi umożliwiać automatyczne tworzenie pomiarów z poziomu zewnętrznych systemów np. z poziomu systemu provisioningu poprzez udostępnienie dedykowanego API
Wymagania całościowe	O12.F44	system musi zapewniać agregację danych, dane z różnych źródeł mogą być kolekcjonowane z różnymi interwałami, jednocześnie system musi prezentować dane dla jeszcze innych przedziałów czasowych, wobec tego system musi zapewniać mechanizmy zarówno agregacji jak i uśredniania danych
Wymagania całościowe	O12.F45	system musi wspierać identyfikację problemu (i przestanie stosowanego alarmu do Fault Management) na podstawie analizy krzyżowej danych z różnych urządzeń (kompleksowa analiza wydajności sieci umożliwiająca porównywanie wskaźników dotyczących różnych elementów może wspomagać znacząco diagnostykę i pozwalać na szybszą identyfikację problemu)
Wymagania całościowe	O12.F46	system musi udostępniać udokumentowane API, za pośrednictwem, którego będzie możliwa implementacja niestandardowych interfejsów integracji, a także publikacja zgromadzonych i zagregowanych danych w innych systemach OSS/BSS
Wymagania całościowe	O12.F47	system musi mieć możliwość integracji z systemami typu Element Managers w celu pobierania danych performance'owych - w sieci OSE będą implementowane Element Manager'y w obszarze sieci, w obszarze bezpieczeństwa, w obszarze zarządzania infrastrukturą serwerową oraz środowiskiem kolokacyjnym
Wymagania całościowe	O12.F48	system musi umożliwiać przygotowywanie danych dla raportów SLA (generowanych w Rozwiązaniu) - zakłada się, że raporty SLA będą

Podobszar	Nr Wymagania	Treść wymagania
		<p>generowane tylko na podstawie zgłoszeń, jednak nie wyklucza się innego podejścia w przyszłości a także potencjalną konieczność pomiarów i wyliczeń pod kątem dodatkowych parametrów SLA (np. dla łącz celem weryfikacji świadczonego SLA na łącza gwarantowane przez operatorów łącz dzierżawionych),</p> <p>zatem Rozwiązanie musi udostępniać mechanizmy pozwalające na przygotowywanie raportów SLA z uwzględnieniem:</p> <ul style="list-style-type: none"> - zakresu/grup elementów, dla których generowany jest raport - definicji parametrów wynikających z umów SLA - zakresów czasowych, np. raport SLA za ostatni miesiąc, raport roczny - prac planowych, np. korekta poziomu SLA ze względu na planowe wyłączenie łącz
Wymagania całościowe	O12.F49	podstawowym interfejsem systemu musi być aplikacja webowa, stanowiąca konsolę operatorsko-administracyjną
Wymagania całościowe	O12.F50	system musi zapewnić możliwość integracji z CSR (Centralny System Raportowy) celem przekazania danych do raportów - między innymi raportów z danymi z ruchu per lokalizacja szkolna/szkoła/VLA szkoły oraz z łącz szkieletowych/agregacyjnych/dostępowych, w szczególności dane dotyczące szkół mają być prezentowane w Portalu Usługowym
Wymagania całościowe	O12.F51	widoki wyświetlane przez użytkowników systemu nie mogą generować się dłużej niż przez 5 sekund, jednak w przypadku widoków statystyk on-line Zamawiający dopuszcza maksymalny czas ich generowania do 8 sekund
Wymagania całościowe	O12.F52	każdy z użytkowników systemu monitorowania powinien posiadać swoje własne imienne konto
Wymagania całościowe	O12.F53	system musi zapewnić możliwość ustanowienia jednego lub więcej użytkowników z uprawnieniami administratora systemu
Wymagania całościowe	O12.F54	system musi umożliwiać tworzenie grup użytkowników, np. w celu kreowania większych pakietów uprawnień dla wielu użytkowników, dla których wymagany jest jednakowy poziom dostępu
Wymagania całościowe	O12.F55	system musi umożliwiać definiowanie ról, które przypisane do użytkowników lub ich grup będą warunkować różne poziomy dostępu (np. dostęp do panelu administracyjnego) i różne uprawnienia (np. wykonywanie operacji zapisu) w ramach systemu
Wymagania całościowe	O12.F56	<p>system musi mieć możliwość restrykcji prezentacji elementów infrastruktury OSE w celu:</p> <ul style="list-style-type: none"> - ograniczenia dostępu użytkownikom tylko do ich infrastruktury (np. dla partnera OSE w danym regionie) - wyświetlania jedynie tych elementów, za które dany użytkownik jest odpowiedzialny

Podobszar	Nr Wymagania	Treść wymagania
Wymagania całościowe	O12.F57	system musi udostępniać informację typu audytowego pozwalającą na weryfikację działań użytkowników, dostarczającą następujące dane: <ul style="list-style-type: none"> - czas logowania użytkownika - adres/hostname źródłowy - niepoprawne próby logowania - błędy wykonywania działań w ramach interfejsu użytkownika, ze wskazaniem danych użytkownika - inne informacje wspomagające diagnostykę i identyfikację naruszeń bezpieczeństwa systemu
Wymagania całościowe	O12.F58	system musi posiadać predefiniowane widoki prezentujące stan monitorowanej infrastruktury - widoki te powinny jednak umożliwiać modyfikację, a także powinna być możliwość kreowania nowych widoków, także w oparciu o te istniejące
Wymagania całościowe	O12.F59	system w ramach interfejsu użytkownika musi pozwalać na przejrzystą wizualizację kolekcjonowanych metryk/statystyk: <ul style="list-style-type: none"> - podstawową formą prezentacji w systemie muszą być różnego rodzaju wykresy m. in. : <ul style="list-style-type: none"> - liniowe - kołowe, tzw. pie-chart's - histogramy - grafy - dane powinny być również prezentowane w formie tabelarycznej - wykresy muszą być dynamicznie odświeżane - wykresy muszą zapewniać dynamiczne skalowanie danych i jednostek
Wymagania całościowe	O12.F60	system musi w zakresie statystyk zapewniać następującą funkcjonalność: <ul style="list-style-type: none"> - wspierać co najmniej następujące parametry w zakresie konfiguracji kolekcji i archiwizacji: <ul style="list-style-type: none"> - częstotliwość pomiarów - parametry agregacji pomiarów i czas archiwizacji - dostosowanie do indywidualnych okresów rozliczeniowych - wspierać możliwość indywidualnego dostosowania prezentacji raportów - sposób prezentacji danych - różnorodność dostępnych widoków - informacje dedykowane dla odbiorcy końcowego
Wymagania całościowe	O12.F61	system musi umożliwiać eksport prezentowanych danych do plików zewnętrznych w standardowych formatach co najmniej CSV, JSON , XML , XLS
Wymagania całościowe	O12.F62	użytkownicy muszą mieć możliwość konfiguracji własnych dashboardów z wykorzystaniem dostępnych elementów wizualizacji
Wymagania całościowe	O12.F63	widoki w systemie muszą umożliwiać dynamiczne zmiany parametrów prezentacji, np. zakresów czasowych czy wybranych monitorowanych elementów

Podobszar	Nr Wymagania	Treść wymagania
Wymagania całościowe	O12.F64	<p>system musi udostępniać predefiniowane zestawy raportów, na przykład grupowane ze względu na typy dostępnych monitorów czy typów raportu. Przykładowe predefiniowane raporty:</p> <ul style="list-style-type: none"> - raporty prezentujące statystyki ruchu sieciowego (m. in. użycie interfejsów, opóźnienia, jitter) - raporty dostępności za określony czas - raporty porównawcze np. tego samego typu raportu dla dwóch różnych elementów, pozwalających na analizę wskaźników wydajnościowych w tym samym okresie pomiaru. - raport wszystkich wskaźników monitorowanych na danym typie elementu - raporty typu Top N według różnych kryteriów - raporty typu inventary korzystające z zasobów określonych w ramach procesu automatycznego wykrywania sieci <p>Wymagany czas przechowywania raportów to 12 miesięcy</p>
Wymagania całościowe	O12.F65	użytkownicy systemu muszą mieć możliwość tworzenia własnych raportów oraz potencjalnie udostępniania ich w postaci szablonów innym użytkownikom
Wymagania całościowe	O12.F66	system musi zapewnić generowanie raportów w standardowych formatach co najmniej PDF, XLS
Wymagania całościowe	O12.F67	szablony raportów udostępniane w ramach systemu (domyślne i utworzone przez użytkowników) powinny zapewniać parametryzację, np. określenie zakresu czasowego, czy listy interfejsów
Wymagania całościowe	O12.F68	<p>system musi zapewniać konfigurowalne mechanizmy logowania umożliwiające :</p> <ul style="list-style-type: none"> - przeprowadzanie diagnostyki funkcjonowania systemu (troubleshooting) - dynamiczne serwisy logowania i śledzenia konfigurowane w trakcie działania systemu - przeprowadzanie weryfikację czynności wykonywanych przez użytkowników systemu <p>system musi posiadać dziennik dla śledzenia zdarzeń systemowych oraz akcji podejmowanych przez użytkownika (np. dodanie bądź usunięcie obiektu), wymagany czas przechowywania danych audytowych to 12 miesięcy</p>
Wymagania całościowe	O12.F69	system musi mieć możliwość uruchomienia odrębnej, niezależnej instancji testowej systemu bez dodatkowych kosztów licencyjnych lub z wykorzystaniem tych samych licencji, co w środowisku produkcyjnym
Wymagania całościowe	O12.F70	system musi posiadać wsparcie producenta lub/i społeczności w zakresie integrowanych typów urządzeń a także rozwoju funkcjonalności pod kątem nowych technologii i nowych typów urządzeń przez cały okres obowiązywania Umowy

Podobszar	Nr Wymagania	Treść wymagania
Wymagania całościowe	O12.F71	system musi mieć możliwość wykonywania kompletnego backupu konfiguracji systemu oraz zbieranych danych wraz z możliwością bezproblemowego odtworzenia
Wymagania całościowe	O12.F72	system musi zapewniać metody powiadomień i eskalacji (po przekroczeniach progów - także wielokrotnych) : - akcje automatyczne, np. uruchomienie zewnętrznego skryptu - wysyłanie wiadomości email - wysyłanie wiadomości SMS
Wymagania całościowe	O12.F73	system musi zapewniać automatyczny provisioning pomiarów w wyniku provisioningu nowej usługi w sieci OSE (w systemie provisioningu będącego integralną częścią Rozwiązania)
Wymagania całościowe	O12.F74	system musi umożliwiać uruchamianie na żądanie pomiarów typu „real-time”, które pozwolą w trybie on-line śledzić zmiany monitorowanego parametru wydajnościowego, bez konieczności automatycznego zapisu pomiaru w systemie
Wymagania całościowe	O12.F75	Rozwiązanie musi wspierać automatyczne wykrywanie typu urządzeń/systemów na podstawie którego możliwe będzie automatyczne tworzenie pomiarów - w zakresie wykrywania system powinien wspierać, co najmniej następujące protokoły: RTT ICMP, skanowanie TCP/UDP, SNMP, SSH
Wymagania całościowe	O12.F76	system musi umożliwiać korelację danych wydajnościowych , w tym ewaluacja danych pochodzących z różnych źródeł - np. kalkulacja złożonych metryk (w niektórych przypadkach odczytanie pojedynczej metryki na danym elemencie nie daje właściwego obrazu wartości wskaźnika i konieczna jest jego kalkulacja na podstawie kilku różnych odczytów), zatem system musi zapewniać możliwość implementacji reguł kalkulacji złożonych metryk
Wymagania całościowe	O12.F77	system musi mieć możliwość wyznaczania trendów i prognoz z uwzględnieniem ich konfigurowalnych okresów
Wymagania całościowe	O12.F78	system musi zapewnić elastyczność w zakresie realizacji pomiarów – wybór pomiędzy predefiniowanymi operacjami pomiarowymi a konfiguracją dowolnych scenariuszy pomiarowych
Wymagania całościowe	O12.F79	Rozwiązanie musi umożliwiać generowanie raportów SLA (monitorowanie kontraktu SLA) bazujący na zebranych danych ticketowych jak i na podstawie danych do pomiarów w systemie Performance Managment. Musi być zapewniona elastyczność w dostosowaniu do specyficznych wymagań rozliczania parametrów SLA oraz możliwość dostosowania raportów do: - umowy SLA z operatorami łącz , podwykonawcami, innymi partnerami OSE - umowy SLA ze szkołami - okresu rozliczeniowego (z uwzględnieniem rozpoczęcia i zakończenia

Podobszar	Nr Wymagania	Treść wymagania
		usługi w trakcie trwania okresu rozliczeniowego) , wymagany czas przechowywania raportów to 12 miesięcy
Wymagania całościowe	O12.F80	system musi mieć możliwość ustalania harmonogramów dla automatycznego generowania i dystrybucji raportów albo w ramach OSS lub/i przy wykorzystaniu Centralnego Systemu Raportowego
Wymagania całościowe	O12.F81	szablony raportów udostępniane w ramach systemu (domyślne i utworzone przez użytkowników) powinny zapewniać parametryzację, np. określenie zakresu czasowego, czy listy interfejsów
Wymagania całościowe	O12.F82	Rozwiązanie musi wspierać funkcjonalność okien serwisowych, które mają wpływ na elementy systemu (np. nie wysyłanie alarmów w trakcie trwania okna), zatem system ma posiadać wsparcie dla funkcjonalności: <ul style="list-style-type: none"> - możliwość definiowania okien serwisowych - definiowanie okien serwisowych w wyniku integracji z procesem biznesowym (np. działu utrzymania) - prezentacja graficzna w raportach i statystykach - dostępność historii - uwzględnienie okien serwisowych w naliczaniu parametrów SLA
Wymagania całościowe	O12.F83	system musi mieć możliwość harmonogramowania zbierania statystyk performance'owych celem optymalizacji obciążenia procesami pomiarowym mierzonych urządzeń jak i samego systemu pomiarowego
Wymagania całościowe	O12.F84	system musi spełniać następujące założenia dotyczące pomiarów ruchu: <ul style="list-style-type: none"> - cykliczny pomiar ruchu (co 300 sekund) per każdy VLAN danej szkoły oddzielnie z interface'ów logicznych na urządzeniach szkieletowych OSE - monitoring wysycenia łącz poprzez cykliczny pomiar portów fizycznych i logicznych (a także wyliczenia i raportowanie stanu wysycenia) - wyliczanie wykorzystania zamówionej przez szkołę przepływności, jako suma ruchu we wszystkich VLANach danej szkoły - wyliczanie wykorzystanej przepustowości z danej lokalizacji szkolnej jako suma ruchu we wszystkich VLANach wszystkich szkół w lokalizacji - statystyki ruchu z ostatniej doby są przechowywane w postaci próbek z dokładnością 5 minutową - statystyki ruchu z ostatniego tygodnia są przechowywane w postaci zagregowanych próbek z dokładnością do 15 minut - statystyki ruchu z ostatniego miesiąca są przechowywane w postaci zagregowanych próbek z dokładnością do 30 minut - statystyki ruchu z ostatniego roku są przechowywane w postaci zagregowanych próbek z dokładnością do 60 minut - zagregowane statystyki roczne są przechowywane do 5 lat wstecz
Wymagania całościowe	O12.F85	oprócz statystyk z interace'ów i subinterface'ów system musi zapewnić wydajność dla monitoringu pozostałych statystyk performance'owych z założeniem : <ul style="list-style-type: none"> - nie mniej niż 10 statystyk per szkieletowe urządzenie sieciowe

Podobszar	Nr Wymagania	Treść wymagania
		<ul style="list-style-type: none"> - nie mniej niż 15 statystyk per szkieletowe urządzenie bezpieczeństwa - nie mniej niż 5 statystyk per urządzenie w lokalizacji szkolnej
Wymagania całościowe	O12.F86	<p>w sieci szkieletowej operatora OSE będą zainstalowane urządzenia wspierające "push model for telemetry", czyli nowy sposób wysyłania danych performance'owych do systemu Performance Management (niebazujący na SNMP) zatem system musi ustawiać n na urządzeniach wysyłanie tych danych (subskrypcja) oraz odbierać i prezentować wspomniane dane telemetryczne na statystykach i w raportach. "Push model for telemetry" jest to nowa technologia i wspólna inicjatywa największych firm telekomunikacyjnych, model ten odchodzi od typowego poolingu danych via SNMP i zakłada odbieranie cyklicznych strumieni danych (wcześniej zasubskrybowanych). Model bazuje na zapisywaniu danych w modelu YANG, kodowaniu ich w postaci GPB (Google Protocol Buffer) messages (w przypadku niektórych producentów również w JSON) a następnie transportowaniu ich przy pomocy gRPC (Google Remote Procedure Calls) dla GPB (w przypadku niektórych producentów również przy pomocy protokołu HTTP dla JSON). Subskrypcja strumienia danych może zostać konfigurowana na różne sposoby w zależności od producenta sprzętu (np. przy pomocy NETCONF, gRPC, CLI)</p>

7.4.2. Zarządzanie konfiguracją (Config Manager)

Skala sieci OSE (ca. 25 tys. jednostek oświatowych) niesie za sobą zarządzanie konfiguracją masowej ilości urządzeń - dodatkowo gro tych urządzeń to heterogeniczny sprzęt instalowany w szkołach o różnorodnych modelach i z różnorodną konfiguracją (zależną od producenta sprzętu). System Config Manager musi objąć swym zasięgiem zarówno sprzęt sieciowy jak i urządzenia/systemy bezpieczeństwa OSE. Należy wziąć pod uwagę to, że część prac konfiguracyjnych (dot. urządzeń w szkołach) będzie wykonywana przez podwykonawców/partnerów serwisowych OSE, którzy muszą mieć możliwość zdalnego korzystania z systemu usprawniającego zarządzanie konfiguracją oczywiście z uwzględnieniem nadanych uprawnień do funkcjonalności i puli urządzeń, za którą odpowiadają. Config Manager musi bardzo ściśle współpracować z systemem Provisioningu gdyż jest dla niego dostawcą szablonów konfiguracji, (podobnie jak Inventory dostawcą puli adresowej oraz puli VLAN'ów) a także z systemem Inventory celem spójnej identyfikacji urządzeń zainstalowanych w OSE oraz ich aktualnej i historycznej konfiguracji a także identyfikacji zainstalowanego oprogramowania na urządzeniach.

Poniżej przedstawione zostały szczególnie istotne wymagania dla systemu Config Manager:

- wyszukiwanie urządzeń w sieci i automatyczne ściąganie ich konfiguracji, funkcjonalność ta powinna być dostępna dla każdego urządzenia wprowadzonego do systemu w zakresie, który udostępnia producent urządzenia, system musi umożliwiać również definiowanie przedziałów czasowych, w jakich konfiguracja będzie pobierana z możliwością wyspecyfikowania konkretnych godzin dla danych grup urządzeń

- akwizycja specyficznych informacji z urządzenia, system powinien umożliwić pobranie specyficznych danych z urządzenia i przechowanie ich w stosownych zasobach, umożliwiając ich wykorzystanie podczas kreowania późniejszych schematów konfiguracji
- modyfikacja konfiguracji, system powinien umożliwiać ręczną modyfikację konfiguracji, tworzenie schematów dla grup urządzeń zarówno logicznych jak i lokalizacyjnych, w celu późniejszego zastosowania dla danej partii urządzeń bez potrzeby ręcznego wybierania
- wersjonowanie konfiguracji, system po pobraniu konfiguracji z urządzenia lub utworzeniu nowego schematu powinien tworzyć spójne nazewnictwo dla przechowywanych zasobów, pozwalające w łatwy sposób określić, które z plików są nowsze i z kiedy dokładnie pochodzą
- porównywanie konfiguracji, system powinien posiadać możliwość śledzenia zmian konfiguracji w czasie oraz porównywania wybranych 2 lub więcej zapisów konfiguracji z danego czasu.
- eksportowanie konfiguracji do standardowych formatów plików
- zarządzanie oprogramowaniem zainstalowanym na urządzeniach (mile widziana integracja z systemami pakietowania danego producenta sprzętu)
- zdalne wykonywanie komend na żądanie administratora systemu, w tym również shutdown i reboot urządzenia
- uruchamianie narzędzi diagnostycznych (np. ping, traceroute) z poziomu zarządzanego urządzenia
- możliwość działania bezagentowego z wykorzystaniem jednego z dostępnych protokołów komunikacyjnych, brak konieczności instalowania dedykowanego oprogramowania na zdalnych systemach
- możliwość zlecania zadań czasowych, które będą cyklicznie wykonywane na grupach urządzeń - takie podejście pozwoli na realizowanie cyklicznych zadań automatyzacji zależnych od bieżącej struktury i stanu sieci
- możliwość komunikacji statusów wykonanych zadań poprzez różne media dla administratorów lub grup użytkowników - funkcjonalność ta może być zrealizowana poprzez integrację z systemem FM, który realizuje funkcje eskalacji i powiadomień (funkcjonalność zapewni możliwość szybkiej reakcji służb utrzymaniowych w przypadku problemów technicznych przy realizacji zadań automatyzacji)
- możliwość wykonywania i logowania przez system pełnego audytu wykonywanych zmian w systemach, wraz z logami dotyczącymi danych użytkownika, który zmiany wykonał jak również informacje, czego dotyczyły i jakie były ich wartości.

Założenia dotyczące architektury zarządzania konfiguracjami i oprogramowaniem

1. W przypadku urządzeń szkieletowych (urządzenia sieciowe i urządzenia bezpieczeństwa) system Config Management ma zapewniać funkcjonalność zarządzania konfiguracją i oprogramowaniem przez cały czas trwania umowy, co oznacza pobieranie konfiguracji i oprogramowania z urządzeń, ich wersjonowanie i porównywanie a także wgrywanie ich na urządzenia. System ma zapewnić masowe i harmonogramowane zmiany konfiguracji i oprogramowania na urządzeniach.

2. W przypadku zarządzania konfiguracją urządzeń zainstalowanych w szkołach system Config Management ma zapewniać funkcjonalność zarządzania konfiguracją przez cały czas trwania umowy. Zakłada się jednocześnie, że w przypadku CPE jest to pełne zarządzanie wersjami konfiguracji i oprogramowania a w przypadku SW i AP jest to inwentaryzacja konfiguracji i oprogramowania inicjalnego na urządzeniach gdyż operator OSE nie będzie administrował urządzeniami SW i AP a jedynie zapewniał ich instalację i uruchomienie inicjalne (wraz z konfiguracją) oraz musi posiadać inicjalną konfigurację i oprogramowanie tych urządzeń w przypadku ich awarii i gwarancyjnej wymiany na nowe. Dodatkowo dla urządzeń SW i AP niezbędna jest również baza użytkowników i haseł oraz SSID (dla AP) wykorzystywane w konfiguracjach inicjalnych.

Wymagania funkcjonalne

Nr Wymagania	Treść wymagania
O13.F1	system musi zapewniać repozytorium konfiguracji wszystkich urządzeń OSE (szkieletowych: sieciowych, bezpieczeństwa, serwerów a także urządzeń zainstalowanych w szkołach) wraz z jej wersjonowaniem
O13.F2	repozytorium konfiguracji musi przechowywać zapisane konfiguracje w uwspólnionym formacie (np. TXT, XLM, JSON, inne) - w szczególności dla urządzeń CPE pochodzących od różnych producentów – format ten ma być dopasowany do wymagań systemu provisioningu
O13.F3	system musi zapewniać repozytorium szablonów konfiguracji wraz z wersjonowaniem - do wykorzystania przez system provisioningu (musi być zachowana ścisła integracja pomiędzy tymi systemami)
O13.F4	system musi zapewniać repozytorium oprogramowania instalowanego na urządzeniach OSE wraz z jego wersjonowaniem
O13.F5	system musi umożliwiać dystrybucję oprogramowania na urządzenia: jego walidację i instalację oraz zbieranie informacji o zainstalowanym oprogramowaniu
O13.F6	informacje prezentowane przez system muszą być zintegrowane z Inventory i CRM (tak by w kontekście oglądanej konfiguracji było wiadomo jakiego urządzenia dotyczy , gdzie zainstalowanego i świadczącego usługi, dla jakiej szkoły)
O13.F7	system musi być oparty o powszechnie dostępne standardy i technologie do komunikacji z urządzeniami (np. SNMP, NETCONF, XML, REST API, JSON, JMX, IPMI)
O13.F8	system musi zapewniać wyszukiwanie urządzeń w sieci i ściąganie ich konfiguracji
O13.F9	system musi zapewniać akwizycję specyficznych informacji z urządzenia, przechowanie ich w stosownych zasobach umożliwiając ich wykorzystanie podczas kreowania późniejszych schematów konfiguracji (w systemie provisioningu)

Nr Wymagania	Treść wymagania
O13.F10	system musi zapewniać możliwość modyfikacji konfiguracji (tworzenie szablonów konfiguracji dla modeli urządzeń i grup urządzeń zarówno logicznych jak i lokalizacyjnych, w celu późniejszego zastosowania dla danej partii urządzeń bez potrzeby ręcznego wybierania)
O13.F11	system musi umożliwiać porównywanie konfiguracji w celu wykrywania wprowadzonych zmian
O13.F12	system musi umożliwiać cofnięcie konfiguracji do wcześniejszych wersji, w przypadku urządzeń provision'owanych automatycznie z systemu provisioningu musi to być zsynchronizowane z systemem provisioningu
O13.F13	system musi zapewniać możliwość eksportu konfiguracji do standardowych formatów plików (co najmniej TXT, XML)
O13.F14	system musi posiadać funkcjonalność zarządzania oprogramowaniem zainstalowanym na urządzenia
O13.F15	system musi posiadać wbudowane narzędzia diagnostyczne pozwalające na sprawdzenie komunikacji z urządzeniem
O13.F16	system musi umożliwiać odznaczanie konfiguracji bazowej dla konkretnego urządzenia OSE w szkole (konfiguracja bazowa to pełna konfiguracja urządzenia z konkretnymi wpisanymi parametrami typu adresacja, vlan, hasła)
O13.F17	system musi zapewniać konfigurację procesu archiwizacji, porównywania i wersjonowania konfiguracji urządzeń oraz podgląd statusu tych operacji
O13.F18	system musi pozwalać na zmianę podstawowych parametrów konfiguracyjnych systemu
O13.F19	każdy z użytkowników systemu powinien posiadać swoje własne imienne konto
O13.F20	widoki wyświetlane przez użytkowników systemu nie mogą się generować dłużej niż przez 5 sekund (wyjątek może stanowić widok pobierania konfiguracji z urządzenia - czasochłonność tego procesu może, bowiem zależeć od możliwości urządzenia jak i komunikacji z nim)
O13.F21	system musi zapewnić możliwość ustanowienia jednego lub więcej użytkowników z uprawnieniami administratora systemu
O13.F22	system musi umożliwiać tworzenie grup użytkowników, np. w celu kreowania większych pakietów uprawnień dla wielu użytkowników, dla których wymagany jest jednakowy poziom dostępu
O13.F23	system musi umożliwiać definiowanie ról, które przypisane do użytkowników lub ich grup będą warunkować różne poziomy dostępu (np. dostęp do panelu administracyjnego) i różne uprawnienia (np. wykonywanie operacji zapisu) w ramach systemu
O13.F24	system musi mieć możliwość restrykcji prezentacji poszczególnych konfiguracji w celu: - wyświetlania jedynie tych elementów, do których dany użytkownik jest uprawniony
O13.F25	system musi udostępniać informację typu audytowego pozwalającą na weryfikację działań użytkowników, dostarczającą następujące dane: - czas logowania użytkownika - adres/hostname źródłowy - niepoprawne próby logowania

Nr Wymagania	Treść wymagania
	<ul style="list-style-type: none"> - błędy wykonywania działań w ramach interfejsu użytkownika, ze wskazaniem danych użytkownika - inne informacje wspomagające diagnostykę i identyfikację naruszeń bezpieczeństwa systemu
O13.F26	<p>system musi zapewniać funkcjonalność IPAM (IP Address Management) do zarządzania pulami adresacji IP OSE, muszą być spełnione następujące wymagania:</p> <ul style="list-style-type: none"> - IPAM musi pozwalać na planowanie przydzielania adresacji urządzeniom OSE - IPAM musi pozwalać na śledzenie przydzielonej adresacji - IPAM musi pozwalać na zarządzanie i przydzielanie zarówno pojedynczych adresów IP (IPv4 i IPv6) oraz sieci IPv4 i IPv6 - w szczególności system IPAM musi zapewnić: <ul style="list-style-type: none"> - obszary do wpisania informacji, na podstawie, których system będzie wiedział, jakie adresy IP ma rezerwować i zwracać: Hostname CPE, Nazwa szkoły, adres/id szkoły np. RSPO - przydzielanie adresów, które rezerwuje i zwróci adresy IP wcześniej określony, jako adres pojedynczy/zakres(pierwszy możliwy) - możliwość zwrotu adresów – zwolnienie ich w bazie (pojedynczo lub zakresami [x - y], system sam zidentyfikuje pulę, do której ma zwrócić adres/adresy - możliwość podglądu kompletnej historii aktywności przydzielania/zwalniania adresów ip (z opcją wyszukaj co najmniej z okresów: wczoraj/ostatni tydzień/ostatni miesiąc/całość), podgląd logów aktywności - zwracanie informacji (całe zestawienia): - wpisanie nazwy szkoły zwraca adres szkoły oraz adresy ip jeżeli już zostały przydzielone wcześniej, dodatkowo nazwę CPE. - wpisanie konkretnego adresu ip/zakresu zwraca nazwę, adres szkoły oraz nazwę CPE - wpisanie adresu szkoły zwraca nazwę szkoły i adresy ip przydzielone do niej, jeżeli istnieją. - podgląd wykorzystania puli adresowej
O13.F27	<p>Rozwiązanie musi zapewniać funkcjonalność zarządzania statycznymi hasłami do urządzeń – w szczególności chodzi o bazę hasel do użycia na urządzeniach OSE w szkole, muszą być spełnione wymagania :</p> <ul style="list-style-type: none"> - baza hasel musi prezentować hasła w formie zaszyfrowanej (z możliwością odkrycia dla osób uprzywilejowanych) - baza hasel musi posiadać generator hasel by przydzielać je kolejnym urządzeniom - generator hasel musi umożliwiać tworzenie hasel o założonych parametrach (długość, rodzaje używanych znaków (wielkie/małe litery, cyfry, znaki specjalne, znaki przestankowe) w tym hasła wymawialne - hasła w bazie hasel muszą być skojarzone z konkretnym urządzeniem i w przypadku urządzeń OSE zainstalowanych w szkołach ze szkołą, w której urządzenie jest zainstalowane
O13.F28	<p>system musi posiadać wsparcie producenta lub/i społeczności w zakresie integrowanych typów urządzeń a także rozwoju funkcjonalności pod kątem nowych technologii i nowych typów urządzeń przez cały okres obowiązywania Umowy</p>
O13.F29	<p>system musi zapewniać alarmowanie do systemu FM (Fault Management w ramach Rozwiązania) w przypadku nieudanych wykonań automatycznych zadań z zakresu Config Managment i/lub mailową eskalację do służb utrzymaniowych</p>

Nr Wymagania	Treść wymagania
O13.F30	w przypadku CPE system musi zapewnić pełne zarządzanie konfiguracją i oprogramowaniem, natomiast w przypadku urządzeń szkolnych - SW i AP systemy OSS muszą zapewnić inwentaryzację konfiguracji i oprogramowania inicjalnego na urządzeniach dodatkowo dla urządzeń SW i AP niezbędna jest baza użytkowników i haseł oraz baza SSID (dla AP) wykorzystywane w ww. konfiguracjach inicjalnych

7.4.3. Provisioning

Podstawowym założeniem funkcjonowania operatora OSE jest maksymalna automatyzacja powtarzalnych czynności - zwłaszcza konfiguracyjnych i ściśle ich powiązanie z działaniem procesów operacyjnych i biznesowych OSE. W szczególności procesy pozyskania i podłączania szkół, uruchamiania usług a także modyfikacji usług mają być w jak największym stopniu zautomatyzowane. Koncepcja automatyzacji dla procesów OSE obejmuje szereg działań, które są tożsame z provisioningiem niezbędnych konfiguracji w systemach i na sprzęcie OSE, co oznacza, co najmniej:

- uzupełnienie/implementacja konfiguracji urządzeń OSE instalowanym w szkołach na bazie szablonu konfiguracji dla danego modelu urządzenia
- uzupełnienie/implementacja konfiguracji urządzeń szkieletowych sieciowych i bezpieczeństwa (w szczególności konfiguracji usług dla szkół)
- uzupełnienie konfiguracji urządzeń w Config Manager
- uzupełnienie danych w Inventory
- uzupełnianie danych w Magazynie Telekomunikacyjnym
- uruchomienie odpowiednich pomiarów (np. ruchowych z VLANów szkolnych itp.) i zbierania zdarzeń i alarmów (Fault & Performance Management),
- uruchomienie monitoringu sieci i usług a co za tym idzie zainicjowanie automatycznego procesu generowania statystyk i raportów,
- konfiguracja parametrów związanych z bezpieczeństwem na urządzeniach /systemach bezpieczeństwa (np. uruchamianie polityk bezpieczeństwa, ustawianie poziomów filtracji treści itp.)
- integracja z procesami biznesowymi, w których ma miejsce provisioning, np. podłączanie szkoły, zgłoszenia zmian w usłudze itp.
- pobieranie niezbędnych danych do provisioningu z systemów OSS/BSS (np. z CRM i Inventory)

W szczególności system provisioningu ma być otwartym rozwiązaniem umożliwiającym elastyczne i masowe implementowanie usług telekomunikacyjnych świadczonych szkołom w sieci OSE (procesy masowe i powtarzalne). Implementowanie usług ma przebiegać zgodnie z procesami biznesowymi zachodzącymi w OSE (w szczególności z procesem podłączenia szkoły do OSE). Ze względu na heterogeniczność urządzeń w sieci OSE system realizujący usługę provisioningu musi wspierać wszystkie standardowe mechanizmy komunikacji i integracji z urządzeniami sieciowymi a także z

urządzeniami/systemami bezpieczeństwa oraz z systemami nadzoru OSS/BSS będących częścią Rozwiązania.

System provisioningu ma pozwolić na budowanie dowolnych algorytmów w celu zamodelowania i przeprowadzenia procesu implementacji usług na urządzeniach (ich konfiguracja) jak i w systemach nadzoru (odczyt/zapis/modyfikacja danych dotyczących urządzeń, konfiguracji i usług). Algorytm taki musi pozwalać na dowolność zachowania algorytmu w tym na zagnieżdżanie algorytmu w algorytmie, podejmowanie decyzji na podstawie danych wejściowych (również pochodzących z systemów trzecich), wybór ścieżki algorytmu oraz bezpieczne wycofywanie się z przeprowadzonych kroków. Powinien również zapewniać mechanizm transakcyjności - możliwość odwołania, zatrzymania i wznowienia transakcji provisioningowej.

Największym wyzwaniem dla systemu provisioningu jest heterogeniczny sprzęt OSE stawiany w szkołach - CPE (router z funkcjonalnością firewall), switch LAN i Access Pointy Wi-fi. W szczególności część urządzeń CPE i Access Point Wi-fi będzie dostarczana przez beneficjentów POPC (wszystkie switchy LAN dostarczane przez operatora OSE), zatem modele tych urządzeń mogą być znane ze stosunkowo krótkim wyprzedzeniem przed ich instalacją przy podłączaniu szkoły lub wymianie sprzętu po jego uszkodzeniu. Modele urządzeń (CPE, SW, AP) kupowanych przez operatora OSE w kolejnych postępowaniach zakupowych dla kolejnych podłączanych do OSE rejonów będą znane sukcesywnie w trakcie trwania projektu.

Założenia dotyczące architektury provisionowania usług

1. W przypadku szkieletu sieci OSE uruchamianie i modyfikacja usług dla szkół na urządzeniach i systemach będzie obejmować:
 - a. uruchamianie usług sieciowych na urządzeniach sieciowych OSE zarówno w Fazie 1 wdrożenia w ramach tzw. "Aktywatora usług" jak również w dalszych fazach wdrożenia w ramach docelowego systemu OSS i provisionowania usługi End2End; uruchamianie usług na urządzeniach sieciowych może zostać zaimplementowane poprzez bezpośrednie konfigurowanie urządzeń sieciowych (przy wykorzystaniu wszelkich standardowych mechanizmów udostępnianych na urządzeniach szkieletowych - co najmniej SSH i SNMP) lub/i z wykorzystaniem Element Managera do tych urządzeń (wówczas niezbędna jest integracja via API np. REST API i/lub przy pomocy plików płaskich); provisioning ten będzie aktywowany w procesach biznesowym OSE (np. podłączanie szkoły)
 - b. uruchamianie usług bezpieczeństwa na urządzeniach bezpieczeństwa lub/i na systemach bezpieczeństwa odbywać się ma zarówno w Fazie 1 wdrożenia w ramach tzw. "Aktywatora usług" jak również w dalszych fazach wdrożenia w ramach docelowego systemu OSS i provisionowania usługi End2End; w przypadku usług bezpieczeństwa mechanizm integracji może zostać zaimplementowany poprzez bezpośrednie konfigurowanie urządzeń bezpieczeństwa (przy wykorzystaniu wszelkich standardowych mechanizmów udostępnianych na urządzeniach szkieletowych - co najmniej SSH i SNMP) lub/i z wykorzystaniem Element Managera do urządzeń (wówczas niezbędna jest integracja via API np. REST API i/lub przy pomocy plików płaskich) oraz poprzez integrację z systemami bezpieczeństwa bazując na API np. REST API i/lub plikach płaskich; provisioning ten będzie aktywowany w procesach biznesowych OSE (np. podłączenie szkoły)

- c. modyfikacje usług w trakcie ich trwania (zarówno sieciowych jak i bezpieczeństwa) przy pomocy ww. mechanizmów aktywowane będą procesami biznesowymi OSE; procesy te mogą rozpoczynać się na Portalu Usługowym (self service użytkownika portalu) lub w wyniku ich rozpoczęcia przez uprawnione zespoły OSE
- d. ze względu na to, iż Zamawiający planuje realizować procesy związane z podłączaniem szkół w sposób w pełni zautomatyzowany z wykorzystaniem wszelkich możliwych interfejsów API wystawianych przez systemy/urządzenia w szkieletcie systemy/urządzenia te muszą zostać zintegrowane z Aktywatorem Usług oraz docelowym systemem Provisioningu Wykonawcy; należy założyć, że metody integracji będą następujące:
 - interfejs API, np.REST API
 - modyfikacja plików płaskich (pliki konfiguracyjne zapisane na sieciowym zasobie dyskowym, np. TXT, CSV)
 - wymiana plików o standardowych formatach, np. TXT, CSV, JSON, XML
 - bezpośrednia komunikacja z urządzeniami, co najmniej poprzez protokół SSH i SNMP
- e. należy przyjąć, że będą wymagane, co najmniej następujące integracje związane z provisioningiem:
 - integracji z 18 Element Managerami do ADC (w 16 węzłach regionalnych i w 2 centralnych)
 - integracji z 16 Element Managerami do systemu SWG (w 16 węzłach regionalnych)
 - integracji z 18 Element Managerami do systemów NG Firewall (w 16 węzłach regionalnych i w 2 węzłach centralnych)
 - integracji z 2 instancjami Element Managerów do urządzeń sieciowych (w 2 węzłach centralnych, zakładamy jednego producenta, jedna z instancji zapasowa)
 - integracji z 2 element Managerami do systemu DNS (w 2 węzłach centralnych)
 - integracji z 2 instancjami SIEM (w 2 węzłach centralnych)
- f. W zakresie **aktywacji usług sieciowych** szkoły na urządzeniach w szkieletcie sieci OSE będzie niezbędne wykonanie następujących czynności:
 - konfigurację parametrów L2 interfejsu (pojedynczy VLAN albo podwójne tagowanie - QinQ, do 5 VLAN per szkoła)
 - konfigurację adresacji IPv4 / IPv6 na interfejsie (adresy połączeniowe)
 - konfigurację routingu statycznego w stronę szkoły + community dla tych adresów
 - konfigurację QoS na łączy (policer, shaper, RED)
- g. W zakresie **zmian w usługach sieciowych** należy założyć wykonanie, co najmniej:
 - konfiguracji związanej z przydzielaniem szkołom adresów publicznych
 - konfiguracji parametrów L2 związanych z dodatkowymi VLAN'ami dla szkół
 - konfiguracji związanej ze zmianą przepływności usługi dostępu do Internetu do szkoły

- h. W zakresie **aktywacji usług szkoły na urządzeniach/systemach bezpieczeństwa** będzie wymagane wykonanie, co najmniej czynności
- pobranie z systemu IPAM (będącego częścią Rozwiązania) adresu podsieci IP, wydzielonego z puli 100.64.0.0/10 (Shared Address Space zgodnie z RFC6598 / BCP153) i przydzielonego do danej szkoły
 - dodanie ww. adresu podsieci IP do konfigurowalnych polityk na systemach: ACD, NGFW, SWG, DNS
 - na systemie SIEM:
 - inicjacja generowania raportów bezpieczeństwa dla danej szkoły, na podstawie predefiniowanych przez Zamawiającego szablonów
 - określenie harmonogramu generowania raportów dla danej szkoły
- i. W zakresie **zmian w usłudze bezpieczeństwa** należy założyć modyfikację parametrów polityk zdefiniowanych per szkoła na poszczególnych systemach, w tym w szczególności, choć nie wyłącznie:
- na systemie ADC:
 - wyjątki definiujące, jaki ruch ma nie podlegać dekrypcji SSL, np. na podstawie źródłowych lub docelowych adresów IP, adresów URL zawartych w parametrach certyfikatu (pola: SNI lub CN)
 - na systemie NGFW:
 - tworzenie dedykowanych polityk per szkoła blokujących lub przepuszczających ruch z/do zadanych adresów IP, nawiązywany na określonych portach TCP/UDP
 - włączanie i wyłączanie ruchu mailowego (m. in. protokoły IMAP, POP3) wychodzącego i przychodzącego z/do danej szkoły z analizy antywirusowej
 - na systemie DNS:
 - włączenie / wyłączenie lub zmiana listy kategorii treści przypisanych do polityk określających poziom ochrony użytkowników OSE
 - na systemie SWG:
 - tworzenie dedykowanych polityk per szkoła
 - dodawanie i usuwanie kategorii blokowanych, skonfigurowanych w polityce dla danej szkoły
 - dodawanie i usuwanie zawartości statycznych list, zawierających adresu URL, definiujących wyjątki od polityki blokowania dla danej szkoły
 - włączanie i wyłączanie ruchu mailowego (protokoły HTTP i HTTPS) wychodzącego i przychodzącego z/do danej szkoły z analizy antywirusowej
 - na systemie SIEM
 - zmiany dotyczące raportów i harmonogramu raportów bezpieczeństwa dla danej szkoły

Na etapie Projektu Technicznego Zamawiający doprecyzuje listę i szczegółowy zakres procesów podlegających automatyzacji na dostarczanej przez Wykonawcę Infrastrukturze bezpieczeństwa i sieci

2. W przypadku urządzeń w lokalizacjach szkolnych w Fazie 1 provisioning konfiguracji tych urządzeń będzie pokryty poprzez uruchomienie kopii instancji systemu provisioningu używanego przez Zamawiającego obecnie (przed Fazą 1) , w Fazie 1a przy zastosowaniu wdrożonego przez Wykonawcę "Aktywatora usług", natomiast w Fazie 2 Wykonawca uruchomi docelowy system provisioningu w ramach docelowego stosu systemów OSS (może on być rozwinięciem Aktywatora Usług). Provisioning ten ma zapewnić maksymalną możliwą automatyzację masowej konfiguracji urządzeń CPE w lokalizacjach szkolnych. Automatyzacja ta uzależniona jest od możliwości instalowanego urządzenia w zakresie od maksymalnego, czyli ZTP (Zero Touch Provisioning) do minimalnego, czyli przygotowania jedynie plików konfiguracyjnych - należy założyć, że najczęstszym przypadkiem będzie jednak następujący model
- przygotowanie pliku z konfiguracją inicjalną w celu uruchomienia łączności z urządzeniem (konfiguracja na USB - wkładany do urządzenia przez partnera serwisowego)
 - zdalna konfiguracja urządzenia docelową zawartością

Należy założyć użycie standardowych metod integracji/komunikacji z urządzeniami, np. :

- - SSH (w szczególności wymiana kluczy ssh)
 - Telnet
 - Netconf
 - SNMP ver. 2c-3
 - integracja poprzez pliki konfiguracyjne
- Urządzenia typu SW i AP (wyłączając hasła dostępowe i SSID) mają posiadać identyczną konfigurację, zatem ich provisioning polegać będzie na przygotowaniu konfiguracji inicjalnej z szablonu dla danego modelu/producenta urządzenia danego typu instalowanego w danej szkole.

Wymagania funkcjonalne

Nr Wymagania	Treść wymagania
O14.F1	system musi mieć możliwość tworzenia własnych skryptów modułów i wtyczek pozwalających na obsługę niestandardowych urządzeń i protokołów dowolnego producenta i typu
O14.F2	system musi posiadać wbudowane urządzenia diagnostyczne pozwalające na sprawdzenie komunikacji z urządzeniem
O14.F3	system musi mieć możliwość generowanie skryptu do uruchomienia na urządzeniu
O14.F4	system provisioningu musi być zintegrowany z innymi systemami OSS/BSS Rozwiązania biorącymi udział w procesie aktywacji usługi (np. CRM, BPM, Inventory)
O14.F5	system musi umożliwiać wywoływanie/testowanie pojedynczych komend konfiguracyjnych
O14.F6	system musi zapewniać możliwość zmiany podstawowych parametrów konfiguracyjnych systemu
O14.F7	każdy z użytkowników systemu powinien posiadać swoje własne imienne konto
O14.F8	system musi zapewnić możliwość integracji z usługą katalogową LDAP (będącej częścią Rozwiązania) i AD (system Zamawiającego) celem uwierzytelniania i autoryzacji na urządzeniach i systemach OSE
O14.F9	system musi zapewnić możliwość ustanowienia jednego lub więcej użytkowników z uprawnieniami administratora systemu
O14.F10	system musi umożliwiać tworzenie grup użytkowników, np. w celu kreowania większych pakietów uprawnień dla wielu użytkowników, dla których wymagany jest jednakowy poziom dostępu
O14.F11	system musi umożliwiać definiowanie ról, które przypisane do użytkowników lub ich grup będą warunkować różne poziomy dostępu (np. dostęp do panelu administracyjnego) i różne uprawnienia (np. wykonywanie operacji zapisu, dostęp do urządzeń, do których tylko użytkownik może mieć uprawnienia -- np. podwykonawca tylko do urządzeń szkoły, którą serwisuje) w ramach systemu
O14.F12	system musi mieć możliwość restrykcji uruchomienia provisioninga konfiguracji tylko na urządzenia/grupę urządzeń/typ urządzeń, do których dany użytkownik ma uprawnienia
O14.F13	system musi udostępniać informację typu audytowego pozwalającą na weryfikację działań użytkowników, dostarczającą następujące dane: <ul style="list-style-type: none"> - o czas logowania użytkownika - adres/hostname źródłowy - niepoprawne próby logowania - błędy wykonywania działań w ramach interfejsu użytkownika, ze wskazaniem danych użytkownika - inne informacje wspomagające diagnostykę i identyfikację naruszeń bezpieczeństwa systemu
O14.F14	system musi mieć odpowiednią wydajność by zapewnić provisioning z : <ul style="list-style-type: none"> - 18 Element Managerami do ADC (w 16 węzłach regionalnych i w 2 centralnych) - 16 Element Managerami do systemu SWG (w 16 węzłach regionalnych) - 18 Element Managerami do systemów NG Firewall (w 16 węzłach regionalnych i w 2 węzłach centralnych) - 2 instancjami Element Managerów do urządzeń sieciowych (w 2 węzłach centralnych, zakładamy jednego producenta, jedna z instancji zapasowa)

Nr Wymagania	Treść wymagania
	<ul style="list-style-type: none"> - 2 element Managerami do systemu DNS (w 2 węzłach centralnych) - 2 instancje SIEM w 2 węzłach centralnych
O14.F15	<p>w przypadku provisioningu urządzeń sieciowych w szkieletie sieci OSE system musi zapewniać, co najmniej:</p> <ul style="list-style-type: none"> - możliwość konfiguracji usług wymagających konfiguracji na wielu urządzeniach jednocześnie, wraz z walidacją konfiguracji i założeniem konfiguracji "wszystko albo nic" - możliwość provisioningu usług z uwzględnieniem integracji z systemami BSS (np. CRM , BPM) - możliwość provisioningu niezwiązanego z łączami (np. BGP, ACL) - możliwość provisioningu dowolnej konfiguracji ad hoc. przez upoważnionego użytkownika systemu - integrację systemu z IPAM, Inventory i systemem Config Management (będących częścią Rozwiązania) w celu wygenerowania właściwej docelowej konfiguracji <p>W szczególności system musi wspierać:</p> <ul style="list-style-type: none"> - konfigurację parametrów L2 interfejsu (pojedynczy VLAN albo podwójne tagowanie - QinQ, do 5 VLAN per szkoła) - konfigurację adresacji IPv4 / IPv6 na interfejsie (adresy połączeniowe) - konfigurację routingu statycznego w stronę szkoły + community dla tych adresów - konfigurację QoS na łączu (policer, shaper, RED) - konfigurację związaną z przydzielaniem szkołom adresów publicznych - konfigurację związaną ze zmianą przepływności usługi dostępu do Internetu do szkoły <p>Na etapie Projektu Technicznego Zamawiający doprecyzuje listę i szczegółowy zakres procesów podlegających automatyzacji na dostarczanej przez Wykonawcę Infrastrukturze sieci</p>
O14.F16	<p>w przypadku provisioningu urządzeń/systemów bezpieczeństwa OSE system musi zapewniać:</p> <ul style="list-style-type: none"> - możliwość provisioningu usług bezpieczeństwa świadczonych szkołom przy różnym poziomie filtracji treści, co oznacza ustawianie filtracji w systemie SWG (kupowanym w oddzielnym postępowaniu przetargowym) - provisioningu konfiguracji polityk bezpieczeństwa oraz konfiguracji innych aspektów związanych z firewall'ingiem, load-balancingiem i logowaniem zdarzeń bezpieczeństwa w systemach SIEM, NG Firewall, SWG (systemy kupowane w oddzielnym postępowaniach przetargowych) - możliwość provisioningu dowolnej konfiguracji ad hoc. przez upoważnionego użytkownika systemu - możliwość definiowania nowych polityk bezpieczeństwa na systemach typu firewall, zgodnie z przygotowanymi wcześniej szablonami - możliwość zarządzania (dodawanie, zmienianie, usuwanie) szablonów polityk bezpieczeństwa - możliwość definiowanie nowych poziomów filtracji w systemie SWG, zgodnie z przygotowanymi wcześniej szablonami <p>system musi wspierać wszechstronne metody integracji, np.:</p> <ul style="list-style-type: none"> - poprzez interfejs API, co najmniej REST API - poprzez modyfikację plików płaskich (pliki konfiguracyjne zapisane na sieciowym zasobie dyskowym, co najmniej TXT) - poprzez wymianę plików o standardowych formatach, co najmniej TXT, CSV, JSON, XML - poprzez bezpośrednią komunikacją z urządzeniami co najmniej poprzez protokół SSH i SNMP

Nr Wymagania	Treść wymagania
O14.F17	<p>system ma zapewnić maksymalną możliwą automatyzację masowej konfiguracji urządzeń CPE w lokalizacjach szkolnych, automatyzacja ta uzależniona jest od możliwości instalowanego urządzenia w zakresie od maksymalnego, czyli ZTP (Zero Touch Provisioning) do minimalnego, czyli przygotowania jedynie plików konfiguracyjnych - należy założyć, że najczęstszym przypadkiem będzie jednak następujący model</p> <ul style="list-style-type: none"> - przygotowanie pliku z konfiguracją inicjalną w celu uruchomienia łączności z urządzeniem (konfiguracja na USB - wkładany do urządzenia przez partnera serwisowego) - zdalna konfiguracja urządzenia docelową zawartością <p>urządzenia typu SW i AP (wyłączając hasła dostępowe i SSID) mają posiadać identyczną konfigurację zatem ich provisioning musi polegać na przygotowaniu konfiguracji inicjalnej z szablonu dla danego modelu/producenta urządzenia danego typu instalowanego w danej szkole</p>
O14.F18	<p>system musi umożliwić użycie standardowych metod integracji/komunikacji z urządzeniami OSE, np. :</p> <ul style="list-style-type: none"> - SSH (w szczególności wymiana kluczy ssh) - Telnet - Netconf - SNMP ver. 2c-3 - integracja poprzez pliki konfiguracyjne - użycie skryptów i konfiguracja z poziomu CLI
O14.F19	<p>w przypadku provisioningu urządzeń OSE w szkole:</p> <ul style="list-style-type: none"> - system musi zapewnić provisioning całej konfiguracji a w szczególności usług typu "dostęp do Internetu" na heterogenicznych urządzeniach CPE - system musi zapewnić provisioning konfiguracji inicjalnej (pierwotna w czasie podłączania szkoły do OSE) dla urządzeniach SW i AP - system musi mieć możliwość generowania pliku z konfiguracją inicjalną do uruchomienia na urządzeniu CPE z pen-drive - dla CPE wspierających funkcjonalność ZTP (Zero Touch Provisioning) uruchamianie tego typu provisioningu - system musi mieć możliwość provisioningu dowolnej konfiguracji ad hoc. przez upoważnionego użytkownika systemu - system musi zapewniać integrację systemu z bazą haseł oraz z IPAM (będących częścią Rozwiązania) w celu wygenerowania właściwej docelowej konfiguracji dla urządzeń typu CPE - system musi zapewniać integrację systemu z bazą haseł i bazą SSID (będących częścią Rozwiązania) w celu wygenerowania właściwej docelowej konfiguracji dla urządzeń typu SW i AP WI-fi
O14.F20	<p>W zakresie aktywacji usług bezpieczeństwa dla szkoły system provisioningu musi wspierać :</p> <ul style="list-style-type: none"> - pobieranie z IPAM (będącego częścią Rozwiązania) adresu podsieci IP, wydzielonego z puli 100.64.0.0/10 (Shared Address Space zgodnie z RFC6598 / BCP153) i przydzielonego do danej szkoły - dodawanie ww. adresu podsieci IP do konfigurowalnych polityk na systemach : ACD,NGFW, SWG, DNS - inicjowanie na systemie SIEM generowania raportów dla danej szkoły, na podstawie predefiniowanych przez Zamawiającego szablonów oraz określenie harmonogramu generowania tych raportów dla danej szkoły

Nr Wymagania	Treść wymagania
	<p>Na etapie Projektu Technicznego Zamawiający doprecyzuje listę i szczegółowy zakres procesów podlegających automatyzacji na dostarczanej przez Wykonawcę Infrastrukturze bezpieczeństwa</p>
O14.F21	<p>W zakresie zmian w usłudze bezpieczeństwa system musi wspierać modyfikację parametrów polityk zdefiniowanych per szkoła na poszczególnych systemach, w tym w szczególności, choć nie wyłącznie:</p> <ul style="list-style-type: none"> - Na systemie ADC: Wyjątki definiujące, jaki ruch ma nie podlegać dekrypcji SSL, np. na podstawie źródłowych lub docelowych adresów IP, adresów URL zawartych w parametrach certyfikatu (pola: SNI lub CN) - Na systemie NGFW: Tworzenie dedykowanych polityk per szkoła blokujących lub przepuszczających ruch z/do zadanych adresów IP, nawiązywany na określonych portach TCP/UDP Włączanie i wyłączanie ruchu mailowego (m. in. protokoły IMAP, POP3) wychodzącego i przychodzącego z/do danej szkoły z analizy antywirusowej - Na systemie DNS: Włączenie / wyłączenie lub zmiana listy kategorii treści przypisanych do polityk określających poziom ochrony użytkowników OSE - Na systemie SWG: Tworzenie dedykowanych polityk per szkoła Dodawanie i usuwanie kategorii blokowanych, skonfigurowanych w polityce dla danej szkoły Dodawanie i usuwanie zawartości statycznych list, zawierających adresu URL, definiujących wyjątki od polityki blokowania dla danej szkoły Włączanie i wyłączanie ruchu mailowego (protokoły HTTP i HTTPS) wychodzącego i przychodzącego z/do danej szkoły z analizy antywirusowej - Na systemie SIEM: zmiany w generowaniu raportów bezpieczeństwa dla danej szkoły zmiany w harmonogramie generowania raportów dla danej szkoły <p>Na etapie Projektu Technicznego Zamawiający doprecyzuje listę i szczegółowy zakres procesów podlegających automatyzacji na dostarczanej przez Wykonawcę Infrastrukturze bezpieczeństwa</p>
O14.F22	wszystkie wymagane funkcjonalności muszą być dostępne w interfejsie graficznym systemu
O14.F23	system musi zapewniać provisioning urządzeń, do których autoryzacja przebiega z wykorzystaniem protokołów RADIUS i TACACS+
O14.F24	widoki wyświetlane przez użytkowników systemu nie mogą się generować dłużej niż przez 5 sekund
O14.F25	system musi zapewniać kontrolę użytkowników i grup systemu z możliwością przypisywania im ról pozwalających na definiowanie dostępu do określonych skryptów konfiguracji
O14.F26	system provisioningu musi działać bezagentowo
O14.F27	system musi posiadać możliwość zlecania zadań czasowych; statusy wykonanych zadań muszą być komunikowane różnymi drogami (email, sms, alarm w Fault Management)
O14.F28	system musi posiadać wsparcie producenta lub/i społeczności w zakresie integrowanych typów urządzeń a także rozwoju funkcjonalności pod kątem nowych technologii i nowych typów urządzeń przez cały okres obowiązywania Umowy

Nr Wymagania	Treść wymagania
O14.F29	<p>system provisioningu w celu zapewnienia pełnego provisioningu usługi (nie tylko na urządzeniach i systemach sieciowych i bezpieczeństwa) ale także w systemach BSS musi być zintegrowany z:</p> <ul style="list-style-type: none"> - systemem Inventory w celu uaktualnienia danych w Inventory (np. nowe urządzenie, nowa usługa) - systemem BPM (Business Proces Managemet), procesy biznesowe będą wyzwały zadania w systemu provisioningu (musi być uwzględniona informacja zwrotnej z systemu provisioningu w kierunku BPM o statusie wykonanego zadania) - systemem Performance Management w celu uruchomienia stosownych pomiarów i raportów - systemem Fault & Availability Management w celu uruchomienia stosownych pomiarów dostępności - systemem Config Management w celu uruchomienia automatycznego ściągania konfiguracji z nowego urządzenia (w tym z IPAM)
O14.F30	<p>system musi mieć możliwość powtarzalnego i niezawodnego uruchamiania algorytmów provisioningu:</p> <ul style="list-style-type: none"> - algorytmy muszą być zapisywane w repozytorium algorytmów, celem wersjonowania oraz ponownego ich użycia lub wykorzystania w tworzeniu nowego algorytmu - w przypadku, gdy dany krok algorytmu nie powiedzie się, co w szczególności może spowodować zatrzymanie całego algorytmu provisioningu musi być możliwość wycofania się z przeprowadzonych już kroków - wszystkie uruchomienia provisioningu muszą być logowane na poziomie wykonywania każdego kroku w algorytmie celem sprawdzenia poprawnego wykonania kroków i całego algorytmu (logi powinny być przechowywane, co najmniej z ostatnich 3 miesięcy)
O14.F31	<p>system musi mieć możliwość implementacji dowolnego scenariusza/algorytmu provisioningu (scenariusz jest tworzony w dostępnym narzędziu)</p>
O14.F32	<p>algorytm provisioningu musi pozwalać co najmniej na:</p> <ul style="list-style-type: none"> - bezagentową komunikację ze sprzętem/systemami - sprawdzenie/ściągnięcie aktualnej konfiguracji urządzenia - zmianę konfiguracji urządzenia - wgranie oprogramowania/plików na urządzenie - sprawdzenie oprogramowania i sprzętu oraz stanu urządzenia - wykonanie dowolnej komendy na urządzeniu
O14.F33	<p>komunikacja z urządzeniem/systemem musi przebiegać w sposób bezpieczny (przy pomocy odpowiedniej autoryzacji dostępu) – w szczególności musi być możliwość korzystania z mechanizmu wymiany kluczy ssh</p>
O14.F34	<p>system musi umożliwiać uruchamianie scenariusza provisioningu co najmniej w następujący sposób:</p> <ul style="list-style-type: none"> - ręcznie przez administratora - w wyniku wywołania z zewnętrznego skryptu utrzymaniowego - w wyniku wywołania z nadrzędnego procesu czy systemu nadzoru – np. trigger'owanie mailem, pojawieniem się pliku, zmianą stanu usługi, alarmem - z wsadowego pliku dostarczającego niezbędnych danych do scenariusza - z automatycznym pobieraniem danych z systemów nadzoru (do wykorzystania w scenariuszu) , np. dane usługi, szablon konfiguracji, szczegółowe parametry konfiguracji (IP, VLAN, profil bezpieczeństwa itp.)

Nr Wymagania	Treść wymagania
O14.F35	system musi umożliwiać masowe uruchamianie algorytmów provisioningu
O14.F36	system musi wspierać komunikację z heterogenicznym sprzętem zainstalowanym w szkołach (w szkołach będą instalowane trzy typy urządzeń: CPE, switch LAN, wi-fi access-point); provisioning będzie dotyczyć konfiguracji urządzeń : - CPE: ruter z funkcją firewall (pełne zarządzanie i administrowanie urządzeniem przez operatora OSE) - switch LAN (operator OSE zapewnia inicjalną konfigurację) - Access Point wi-fi (operator OSE zapewnia inicjalną konfigurację)
O14.F37	system musi posiadać łatwy i intuicyjny interfejs przeznaczony do tworzenia i uruchamiania algorytmów provisioningu
O14.F38	system musi wspierać integrację z systemami OSE i systemami Zamawiającego : - na poziomie API (stosowane wewnętrznie w Rozwiązaniu) lub na poziomie bazodanowym (bazy danych stosowane w Rozwiązaniu) - na poziomie wymiany poczty SMTP
O14.F39	system musi posiadać dostęp do gotowych do wykorzystania bibliotek/funkcji współpracy z istniejącymi na rynku urządzeniami, bazami danych, technologiami integracji (w ramach Rozwiązania)
O14.F40	przed wpisaniem konfiguracji na urządzenie musi być sprawdzane czy jest to konieczne (czy konfiguracja jest już zaimplementowana na urządzeniu)
O14.F41	system musi zapewnić optymalizację ilości sesji nawiązywanych z urządzeniem/systemem (jeżeli algorytm wielokrotnie komunikuje się z tym samym urządzeniem celem wykonania różnych etapów provisioningu konfiguracji, sesja jest zestawiana tylko raz i podtrzymywana na czas wykonania wszystkich operacji na urządzeniu)
O14.F42	w system musi być standardowo wbudowane wysyłanie powiadomień: maile lub/i smsy i/lub alarmy (trapy snmp, syslogi) w wyniku niepoprawnego zakończenia się algorytmu lub w wyniku nieudanego kroku
O14.F43	system musi zapewniać forward'owanie logów i alarmów z działania systemu provisioningu do systemu fault & performance management będącego częścią Rozwiązania
O14.F44	musi istnieć możliwość generowania prostych raportów/statystyk z przeprowadzanych uruchomień algorytmów provisioningu z informacjami, co najmniej, kiedy i przez kogo były uruchamiane oraz jaka była ilość udanych i nieudanych prób włącznie z przyczyną problemu
O14.F45	musi istnieć możliwość eksportowania logów/raportów z przeprowadzanych uruchomień i wycofań scenariuszy provisioningu do plików w standardowym formacie (co najmniej TXT, CSV)
O14.F46	w systemie musi istnieć narzędzie do tworzenia algorytmów/scenariuszy provisioningu usług i konfiguracji przez użytkownika systemu po odpowiednim przeszkoleniu
O14.F47	system musi prezentować listy provision'owanego sprzętu (w ramach Rozwiązania)
O14.F48	system musi prezentować listy provision'owanej konfiguracji (w ramach Rozwiązania)
O14.F49	system musi prezentować listy szablonów konfiguracji (w ramach Rozwiązania)

Nr Wymagania	Treść wymagania
O14.F50	musi istnieć możliwość eksportowania skonfigurowanych algorytmów/scenariuszy provisioningu do standardowych formatów plików celem ich dokumentacji i łatwiejszej potencjalnej migracji tych algorytmów do innego systemu provisioningu
O14.F51	system musi wspierać wersjonowanie konfiguracji po każdej modyfikacji z możliwością podglądu zmian do 5 wersji wstecz

7.4.4 Aktywator Usług (wdrażany w Fazie 1 wdrożenia)

W Fazie 1 wdrożenia OSS/BSS Wykonawca uruchomi systemy Jira Insight, Jira WF, Jira SD, rConfig, skrypty integracyjne a w szczególności system Provisioningu urządzeń instalowanych w szkole przekazany przez Zamawiającego a następnie w celu skutecznego uruchamiania usług sieciowych i bezpieczeństwa na urządzeniach i systemach w szkieletu sieci OSE Wykonawca wdroży tzw. "Aktywator Usług". Zapewni on w okresie do wdrożenia docelowego systemu OSS (z docelowym systemem provisioningu) uruchamianie usług w szkieletu w procesie podłączenia szkół do OSE. Zakłada się, że w tym okresie modyfikacje uruchomionych w docelowej sieci szkieletowej usług OSE zostaną drastycznie zminimalizowane.

W zakresie aktywacji usług szkoły na urządzeniach sieciowych w szkieletu sieci OSE będzie niezbędne wykonanie następujących czynności:

- konfigurację parametrów L2 interfejsu (pojedynczy VLAN albo podwójne tagowanie - QinQ, do 5 VLAN per szkoła)
- konfigurację adresacji IPv4 / IPv6 na interfejsie (adresy połączeniowe)
- konfigurację routingu statycznego w stronę szkoły + community dla tych adresów
- konfigurację QoS na łączu (policer, shaper, RED)

W zakresie aktywacji usług szkoły na urządzeniach/systemach bezpieczeństwa będzie niezbędne spełnienie następujących wymagań i czynności:

- Zamawiający planuje realizować procesy związane z podłączaniem szkół w sposób zautomatyzowany z wykorzystaniem interfejsów API wystawianych przez Element Managery i systemy bezpieczeństwa, zatem systemy te bądź same urządzenia bezpieczeństwa muszą zostać zintegrowane z Aktywatorem Usług Wykonawcy. Należy założyć, że metody integracji będą następujące:
 - interfejs API, np. REST API,
 - modyfikacja plików płaskich (pliki konfiguracyjne zapisane na sieciowym zasobie dyskowym),
 - bezpośrednia komunikacja z urządzeniami, co najmniej poprzez protokół SSH i SNMP
- Proces podłączenia szkoły (czyli aktywacji nowych usług) zakłada:
 - pobranie z IPAM (będącego częścią Rozwiązania) adresu podsieci IP, wydzielonego z puli 100.64.0.0/10 (Shared Address Space zgodnie z RFC6598 / BCP153) i przydzielonego do danej szkoły
 - dodanie ww. adresu podsieci IP do konfigurowalnych polityk na systemach:

- ADC,
- NGFW
- DNS
- SWG
- inicjowanie generowania raportów bezpieczeństwa w SIEM
- Zakłada się, że dostarczona w odrębnym postępowaniu zakupowym infrastruktura bezpieczeństwa musi umożliwiać Zamawiającemu automatyzację wyżej wymienionych procesów.
- Na etapie projektu technicznego Zamawiający doprecyzuje listę i szczegółowy zakres procesów podlegających automatyzacji na dostarczanej infrastrukturze bezpieczeństwa i przy wykorzystaniu dostarczonego przez Wykonawcę Aktywatora Usług

Wymagania funkcjonalne

Nr Wymagania	Treść wymagania
O16.F1	<p>Aktywator Usług musi zostać zintegrowany z urządzeniami sieciowymi / Element Manager'ami do urządzeń sieciowych i bezpieczeństwa oraz systemami bezpieczeństwa sieci OSE celem automatycznego provisioningu konfiguracji tych urządzeń/systemów w procesie podłączania szkół do OSE z użyciem standardowych mechanizmów integracji, w tym stosując :</p> <ul style="list-style-type: none"> - interface API (co najmniej REST API) - modyfikację plików płaskich, co najmniej TXT - wymianę plików w standardowych formatach, co najmniej TXT, XML, JSON, XLS - bezpośrednią komunikację z urządzeniami co najmniej poprzez protokół SSH i SNMP
O16.F2	<p>System w zakresie aktywacji usług bezpieczeństwa w procesie podłączenia szkoły umożliwi:</p> <ul style="list-style-type: none"> - wydzielenie i pobranie z IPAM (będącego częścią Rozwiązania) adresu podsieci IP, wydzielonego z puli 100.64.0.0/10 (Shared Address Space zgodnie z RFC6598 / BCP153) i przydzielonego do danej szkoły - dodanie ww. adresu podsieci do predefiniowanych polityk w systemach bezpieczeństwa: - ADC - NGFW - DNS - SWG - inicjowanie na systemie SIEM generowania raportów dla danej szkoły, na podstawie predefiniowanych przez Zamawiającego szablonów oraz określenie harmonogramu generowania tych raportów dla danej szkoły

Nr Wymagania	Treść wymagania
O16.F3	System w ramach procesu aktywacji konfiguracji usług sieciowych musi na urządzeniach sieciowych w szkieletcie OSE wykonać, co najmniej : - konfigurację parametrów L2 interfejsu (pojedynczy VLAN albo podwójne tagowanie - QinQ, do 5 VLAN per szkoła) - konfigurację adresacji IPv4 / IPv6 na interfejsie (adresy połączeniowe) - konfigurację routingu statycznego w stronę szkoły + community dla tych adresów - konfigurację QoS na łączu (policer, shaper, RED)
O16.F4	Na etapie projektu technicznego dotyczącego Aktywatora Usług Wykonawca doprecyzuje szczegóły integracji na podstawie dostarczonej przez Zamawiającego listy i szczegółowego zakresu procesów podlegających automatyzacji na dostarczanej infrastrukturze sieciowej i bezpieczeństwa
O16.F5	Zastosowana funkcjonalność integracji w ramach Aktywatora Usług wdrażanego na Fazę 1a musi zostać przeniesiona i rozszerzona do systemu Provisioningu uruchamianego przez Wykonawcę w Fazie 2 wdrożenia lub musi zostać uruchomione rozwiązanie równoważne (w zakresie wymaganej funkcjonalności i zgodne z wymaganym harmonogramem)

7.4.5. Inwentaryzacja OSE (Inventory)

System Inwentaryzacji OSE (CMDB) ma szczególną i bardzo ważną rolę w projekcie gdyż jego zadaniem jest zbieranie i udostępnianie wszystkich informacji na temat zasobów OSE - są to, co najmniej:

- informacje techniczne zarówno o zasobach aktywnych jak i pasywnych,
- informacje o zasobach będących własnością Operatora OSE jak i beneficjentów POPC (sprzęt w szkołach),
- informacje na temat zasobów własnych jak i dzierżawionych jak łącza czy miejsca w centrach kolokacyjnych,
- informacje na temat świadczonych usług i ich parametrach,
- typowe informacje inwentarzowe urządzeń zaciągane do systemu w sposób automatyczny (np. numer seryjny, nazwa producenta, model urządzenia, wersje sprzętu i oprogramowania, MAC adres, elementy składowe: chassis, karty, interface'y, dyski itp.)
- typowe informacje inwentarzowe wpisywane do systemu "ręcznie" (np. dane dotyczące gwarancji, SLA, kontakt do wsparcia producenta, numer inwentarzowy itp.)

System Inwentaryzacji OSE musi objąć swym zasięgiem zarówno sprzęt sieciowy i bezpieczeństwa jak również serwery w węzłach regionalnych i centralnych. W związku z powyższym system musi móc komunikować się z dowolnym modelem infrastruktury serwerowej stosowanym w OSE w celu zebrania informacji o sprzęcie fizycznym i serwerach wirtualnych w węzłach centralnych i regionalnych bądź uzyskać te informacje z systemu DCIM (Data Center Infrastructure Monitoring), kupowanego w ramach postępowania.

System musi także posiadać informacje o dodatkowym sprzęcie w centrach kolokacji (np. szafy telekomunikacyjne, UPS'y, klimatyzatory itp.), zatem system Inventory musi być zintegrowane poprzez API z systemem zarządzania centrum kolokacji Zamawiającego (system kupowany w

System Inventory musi także zapewnić identyfikację relacji pomiędzy usługą a infrastrukturą (sprzęt/łącza/serwery), na której ta usługa jest świadczona. W związku z powyższym i w związku z tym, że stanowi on źródło informacji dla pozostałych systemów system Inwentaryzacji OSE musi być idealnie zintegrowany z innymi systemami w ramach Rozwiązania a w szczególności z elementami świadczącymi funkcje CRM i BPM oraz z systemami Config & Provisioning Management. System Inwentory w ramach Rozwiązania ma pełnić rolę lub częściową rolę bazy CMDB. Rozwiązanie, zatem ma dawać pełny widok na wszystkie zasoby sieci OSE.

System Inwentaryzacji ma paszportyzować co najmniej poniższe zasoby:

- serwery i systemy w centrach kolokacyjnych,
- łącza dzierżawione w szkielecie, łącza agregacyjne i dostępne do jednostek oświatowych,
- lokalizacje węzłów szkieletowych (regionalnych i centralnych),
- sprzęt kolokacyjny OSE umiejscowionym w lokalizacjach węzłów,
- sprzęt i systemy sieciowe i bezpieczeństwa zainstalowane w węzłach OSE (dane szczegółowe, np. hardware, software, licencje, serwis itp.),
- lokalizacje jednostek oświatowych (dane teleadresowe, partner serwisowy obsługujący szkołę, operator łącza podłączającego szkołę itp.),
- sprzęt zainstalowany w danej jednostce oświatowej,
- połączenia pomiędzy urządzeniami,
- katalog dostępnych typów urządzeń i producentów,
- katalog dostępnego oprogramowania,
- katalog świadczonych usług (powiązanie z zasobami technicznymi sieci OSE, parametry usług, powiązanie między usługami)

Wszystkie obiekty w bazie Inventory mają być sparametryzowane pod kątem potencjalnych przyszłych analiz i potrzeb, zatem system musi pozwalać na dodawanie dowolnych atrybutów opisujących obiekty w systemie Inventory. System ma umożliwiać generowanie prostych zbiorczych raportów z wykorzystania dowolnych zasobów w Inventory. Musi być również zintegrowany z Centralnym Systemem Raportowym (CSR) w celu generowania cyklicznych raportów.

W szczególności system Inventory musi być zintegrowany z innymi systemami Rozwiązania (CRM, TT & Service Desk, BPM, system Obiegu Dokumentów, Magazyn Telekomunikacyjny, Config Manager) w zakresie, co najmniej poniższych informacji, aby je wygodnie prezentować:

- zawarte umowy kosztowe, zlecenia prac w powiązaniu z lokalizacjami i obiektami (np. umowy serwisowe na łącza lub sprzęt) - pobrane z systemu CRM,
- umowy kosztowe, zamówienia na łącza dostępne w powiązaniu z lokalizacjami szkolnymi i łączami
- zawarte umowy przychodowe w powiązaniu z lokalizacjami i obiektami (np. umowy z jednostkami oświatowymi na usługi świadczone w danej lokalizacji) - pobrane z systemu CRM,

- świadczone usługi na sprzęcie/systemie,
- dane teleadresowe lokalizacji/szkoły/podwykonawcy a przede wszystkim ich osoby kontaktowe - pobrane z systemu CRM
- informacje na temat protokołów odbioru, gwarancji na sprzęt - pobrane z ServiceDesk lub/i systemu Obiegu Dokumentów
- historia zgłoszeń awarii sprzętu/ zadań zleconych (w kontekście wybranego sprzętu) - pobrane z TT
- baza wiedzy na temat problemów i rozwiązań w kontekście usług i/lub urządzenia
- linki do statystyk związanych z danym sprzętem / systemem,
- konfiguracja sprzętowa urządzeń (aktualna i historyczna) - integracja z Config Management
- numery seryjne sprzętu i oprogramowania - pobrane z systemu magazynowego lub wpisane ręcznie
- dostępny sprzęt w magazynie do wykorzystania w ramach projektu OSE - integracja z systemem magazynowym
- inne - lista powiązań z elementami pozostałych systemów Rozwiązania zostanie ustalona na etapie projektu systemu

System Inventory wystawiony w ramach interface'u graficznego Rozwiązania będzie pozwalał uprawnionym użytkownikom na update informacji zawartych w bazie Inventory/CMDB – a zwłaszcza dopisywanie nowego sprzętu i łącz w procesie podłączania jednostki oświatowej do OSE. Partnerzy serwisowi będą mogli wprowadzać zmiany do systemu Inventory (np. dotyczące sieci i urządzeń w obsługiwanych przez nich jednostkach oświatowych) w ramach konkretnych procesów biznesowych i za pomocą specjalizowanych formularzy. Dzięki temu będzie można zachować separację terytorialną oraz wprowadzić mechanizmy kontrolne (np. przeglądanie i zatwierdzanie zmian przez personel OSE).

Wymagania funkcjonalne:

Nr Wymagania	Treść wymagania
O15.F1	system musi zapewniać dostęp do wybranych funkcjonalności po autoryzacji użytkowników – zgodnie z przypisanymi im profilami uprawnień: - zarówno z natywnego systemu autoryzacji - jak i za pośrednictwem mechanizmu Single Sign On dostarczonego przez Wykonawcę - jak również w wyniku integracji z Systemem Zarządzania Tożsamością (kupowanym w oddzielnym postępowaniu zakupowym w dalszych etapach projektu OSE)
O15.F2	system musi pozwalać na batch'owy import danych ze standardowych formatów plików (co najmniej CSV, JSON, XML, XLS) a także na export do ww. formatów plików

Nr Wymagania	Treść wymagania
O15.F3	system musi zapewnić identyfikację relacji pomiędzy usługą a infrastrukturą (sprzęt/łącza/serwery), na której ta usługa jest świadczona
O15.F4	system musi zapewniać funkcjonalność zarówno inwentaryzacji zasobów (fizycznych i logicznych infrastruktury) jak również inwentaryzacji usług/pod usług i ich parametrów
O15.F5	system musi umożliwiać inwentaryzację sieci zbudowanych w wielu technologiach (m.in. DWDM, SDH/PDH, Ethernet, IP/MPLS backbone, ATM, SDN, IP)
O15.F6	<p>system musi zapewniać inwentaryzację infrastruktury sieciowej, bezpieczeństwa a także centrów obliczeniowych (szafy, serwery, zasilanie, klimatyzacja, przełączniki, routery, karty itp.)</p> <p>system musi, zatem umożliwiać następujące sposoby zasilania go danymi:</p> <ul style="list-style-type: none"> - ręczne przez uprawnionego użytkownika systemu - wsadowo ze standardowych formatów plików (co najmniej, CSV, XML, JSON, XLS) - automatycznie bezpośrednio z urządzeń sieciowych, bezpieczeństwa, serwerowych (poprzez co najmniej SNMP, SSH/RCONFIG) - automatycznie via API z systemu DCIM (Data Center Infrastructure Monitoring będącego częścią Rozwiązania) - automatycznie via API z systemu zarządzania kolokacjami OSE (kupowany w oddzielnym postępowaniu) - integracja, co najmniej poprzez REST API, pliki płaskie - CSV, pliki w formacie XML, JSON, XLS
O15.F7	<p>system Inventory (rozumiany tu też, jako CMDB) musi pozwalać na paszportyzację i prezentowanie informacji pochodzących również z systemów trzecich (inne systemy Rozwiązania, systemy OSE, systemy Zamawiającego) w kontekście zasobów w Inventory, są to, co najmniej informacje o:</p> <ul style="list-style-type: none"> - sprzęcie i systemach w sieci OSE - sprzęcie i systemach w centrach obliczeniowych - sprzęcie, serwerach i systemach zainstalowanych w węzłach OSE - sprzęcie w danej jednostce oświatowej - dla ww. punktów hardware, software, licencje, serwis itp. - łączach dzierżawionych i światłowodowych w szkieletcie (dane operatora, gwarantowane parametry SLA itp.) - łączach agregacyjnych i dostępowych do jednostek oświatowych (z zobrazowaniem ich parametrów oraz ich wysycenia) - lokalizacjach węzłów szkieletowych (centralnych i regionalnych) - sprzęcie kolokacyjnym OSE umiejscowionym w lokalizacjach węzłów (np. szafy kolokacyjne, parametry typu ilość U, kWh itp.) - lokalizacjach jednostek oświatowych (partner serwisowy obsługujący lokalizację szkolną, operator łącza podłączającego lokalizację szkolną itp., VLAN zarządzający, CPE) - partnerach serwisowych (powiązanie z obsługiwanyimi szkołami) - operatorach łącz agregacyjnych i ich powiązań z operatorami łącz dostępowych, z PWR, z węzłami OSE - operatorach łącz dostępowych i ich powiązanie z operatorami łącz agregacyjnych, z lokalizacją szkolną, PWR/PPWR/węzłem OSE - PWRach – Punkach Wymiany Ruchu (dane adresowe, szafa, odpowiedzialność, punkt styku) i ich powiązaniach z łączami dostępowym i agregacyjnym - PPWRach - Powiatowy Punkt Wymiany Ruchu (dane adresowe, szafa, odpowiedzialność, punkt styku) i ich powiązaniach z łączami dostępowym do lokalizacji ODN

Nr Wymagania	Treść wymagania
	<ul style="list-style-type: none"> - kontaktach (zarówno w szkołach, w OPSach, u partnerów serwisowych/podwykonawców, u operatorów łącz itp.) - jednostkach oświatowych (dane teleadresowe/oświatowe z bazy MEN, VLANy, sprzęt OSE) i ich powiązanie z lokalizacjami szkolnymi (należy założyć, że w jednej lokalizacji może być więcej niż jedna szkoła jak i to, że jedna szkoła może być w kilku lokalizacjach) - organach prowadzących szkoły (OPS) i ich powiązaniach ze szkołami - połączeniach pomiędzy urządzeniami - katalogu dostępnych typów/modeli urządzeń i producentów (wraz oprogramowaniem) - katalogu dostępnego oprogramowania - katalogu świadczonych usług (powiązanie ze sprzętem i ze szkołą) - cennikach na prace/serwis podwykonawcy - innych potencjalnych elementach niezbędnych dla pozostałych systemów ramach Rozwiązania a w szczególności dla systemu provisioningu <p>Część wyżej wymienionych danych jest zawartością systemów BSS i mają być wyświetlane w wyniku interakcji Inventory z tymi systemami. Sposób implementacji integracji pomiędzy tymi systemami w ramach Rozwiązania pozostaje w gestii Wykonawcy.</p>
O15.F8	system musi pozwalać na identyfikację położenia poszczególnych urządzeń/elementów sieci OSE w pomieszczeniach, w szafach, na półkach
O15.F9	<p>system musi pozwalać na integrację z systemem zarządzania centrum kolokacji kupowanym przez Zamawiającego w odrębnym postępowaniu zakupowym w celu pobierania informacji na temat infrastruktury kolokacyjnej przy wykorzystaniu standardowych mechanizmów integracji - co najmniej:</p> <ul style="list-style-type: none"> - przy pomocy plików płaskich, co najmniej CSV - plików w standardowych formatach, np. XML, JSON, XLS - przy pomocy, co najmniej REST API
O15.F10	system musi umożliwiać generowanie prostych zbiorczych raportów na temat dowolnych zasobów z Inventory oraz przekazywanie/udostępnianie informacji do Centralnego Systemu Raportowego
O15.F11	<p>system musi być zintegrowany z innymi obszarami funkcyjnymi Rozwiązania (CRM, TT & Service Desk, BPM, Fault & Performance Management, Config & Provisioning Managment) aby wygodnie prezentować w GUI użytkownika systemu / całego Rozwiązania a także z workflow procesów biznesowych co najmniej następujące informacje :</p> <ul style="list-style-type: none"> - zawarte umowy kosztowe w powiązaniu z lokalizacjami i obiektami (np. umowy serwisowe na sprzęt), - zawarte umowy kosztowe w powiązaniu z łączami dzierżawionymi i lokalizacjami szkolnymi/szkołami - zawarte umowy kosztowe zawarte z partnerami serwisowymi/podwykonawcami w powiązaniu z lokalizacjami szkolnymi/szkołami - zawarte umowy przychodowe w powiązaniu z szkołami i lokalizacjami szkolnymi (np. umowy z jednostkami oświatowymi na usługi świadczone w danej lokalizacji), - wyliczone parametry SLA w danym okresie rozliczeniowym w powiązaniu z świadczonymi usługami (powiązanie też ze sprzętem/systemem), - dane teleadresowe lokalizacji, osoby kontaktowe (na umowie ze szkołą i versus użytkownicy na portalu OSE) - dane teleadresowe, różne typy kontaktów do partnerów OSE (dostawcy łącz/kolokacji,

Nr Wymagania	Treść wymagania
	<p>podwykonawcy)</p> <ul style="list-style-type: none"> - ceny od dostawców łącz w powiązaniu z łączami dostępowymi - przechowywane dokumentacje / alternatywnie linki do dokumentacji, - przechowywana korespondencja dotycząca lokalizacji i obiektów, - historia zgłoszeń awarii sprzętu/ zadań zleconych (w kontekście wybranego sprzętu), - historia zgłoszeń awarii usługi/reklamacji w kontekście prezentowanych usług, - baza wiedzy na temat problemów i rozwiązań, - linki do statystyk związanych z danym sprzętem / systemem /usługą, - konfiguracja sprzętowa urządzeń (aktualna i historyczna), - numery seryjne sprzętu i oprogramowania, - dostępny sprzęt w magazynie do wykorzystania w ramach projektu OSE - integracja z systemem magazynowym - szablony konfiguracji dla modeli urządzeń, - parametry konfiguracji (IP, VLANy) oraz konfiguracji dla danego urządzenia, - hasła dostępowe do urządzeń (w szczególności zainstalowanych w szkole) dostępne w bezpieczny sposób dla uprawnionych użytkowników
O15.F12	system musi pozwalać uprawnionym użytkownikom na update informacji zawartych w bazie Inventory – w szczególności dopisywanie nowego sprzętu, łącz zamawianych w procesie podłączenia szkoły do OSE
O15.F13	system musi pozwalać partnerom serwisowym na wprowadzanie zmian do Inventory, do których będą uprawnieni (np. dotyczących sieci i urządzeń w obsługiwanych przez nich jednostkach oświatowych) w ramach konkretnych procesów biznesowych i za pomocą specjalizowanych formularzy.
O15.F14	<p>system musi umożliwiać integrację z systemami trzecimi (systemy Zamawiającego) poprzez API np. za pośrednictwem:</p> <ul style="list-style-type: none"> - REST API, SOAP - za pomocą plików płaskich, co najmniej CSV - za pomocą plików w standardowych formatach, np. XML, JSON, XLS
O15.F15	system musi posiadać wsparcie producenta lub/i społeczności w zakresie integrowanych typów urządzeń a także rozwoju funkcjonalności pod kątem nowych technologii i nowych typów urządzeń w trakcie trwania umowy
O15.F16	widoki wyświetlane przez użytkowników systemu nie mogą się generować dłużej niż przez 5 sekund
O15.F17	system musi pozwalać na dowolne dodawanie nowych atrybutów/zmianę obecnych w obiektach w Inventory
O15.F18	systemu musi obrazować niedostępność obiektu typu urządzenie/łącze/system w przypadku wykrycia dla obiektu niedostępności przez system Fault & Availability Management (w ramach Rozwiązania)
O15.F19	funkcjonalność Inventory ma być częścią funkcjonalności bazy CMDB opisanej w wymaganiach dla systemów BSS
O15.F20	<p>w ramach funkcjonalności typu CMDB (baza obiektów/konfiguracji) Rozwiązanie musi :</p> <ul style="list-style-type: none"> - realizować rejestrowanie, przechowywanie, śledzenie oraz prezentowanie informacji o konfiguracji oraz poszczególnych elementach konfiguracji od momentu ich zarejestrowania w

Nr Wymagania	Treść wymagania
	<p>systemie</p> <ul style="list-style-type: none"> - wersjonowanie elementów konfiguracji. - dostarczyć zaimplementowane i uruchomione mechanizmy wykonywania (automatycznie) pobierania konfiguracji oraz elementów konfiguracji. - umożliwiać tworzenie stanów odniesienia konfiguracji, obejmujący zestaw elementów konfiguracji. - realizować funkcje eksportu (co najmniej plik) i udostępniania wybranej konfiguracji lub wybranego stanu odniesienia konfiguracji. - realizować przechowywanie utworzonych stanów odniesienia konfiguracji oraz ich udostępnianie na życzenie. - porównywanie zarejestrowanych stanów odniesienia konfiguracji ze stanami historycznymi. - udostępniać funkcjonalności umożliwiające importowanie elementów konfiguracji wraz z atrybutami z zewnętrznych baz danych. - udostępniać zewnętrznym systemom zgromadzone dane (API, export).

Wymaganie wspólne dla systemów OSS:

Nr Wymagania	Treść wymagania
O17.F1	Rozwiązanie oferowane przez Wykonawcę musi być zgodne z zapisami przedstawionymi w pkt. 7.4 "Opis funkcjonalności dla obszaru OSS"
O17.F2	w ramach wdrożenia OSS Wykonawca jest zobowiązany do przygotowania konfiguracji konsol operatorskich niezbędny do pracy NOC (Network Operation Center), Wykonawca przygotuje te konsole z wydzieleniem, co najmniej 15 widoków dla NOC i 15 dla SOC oraz 10 widoków dla operatorów I linii wsparcia.
O17.F3	system OSS w ramach konfiguracji konsol dla NOC/SOC musi mieć możliwość współdzielenia konsol między użytkownikami w ramach ich uprawnień.
O17.F4	system OSS musi zapewnić możliwość wykrywania urządzeń sieciowych z wykorzystaniem protokołów, co najmniej: ICMP, SSH, TELNET, SNMP (v2c, v3), oraz potencjalnie WMI, JMX, RPC
O17.F5	systemy OSS muszą być zintegrowane z systemem SMTP Zamawiającego w celu wysyłania maili
O17.F6	interfejs webowy systemów OSS musi być wspierany przez popularne przeglądarki internetowe - co najmniej przez Microsoft IE i Mozilla Firefox
O17.F7	interface systemów OSS (co najmniej w zakresie funkcjonalności niezbędnej do wykonywania prac w terenie) musi być dostępny na urządzeniach mobilnych działających na systemach iOS i Android
O17.F8	systemy OSS muszą być dostępne w web'owym interfejsie po zalogowaniu (co najmniej musi być zachowane pojedyncze logowanie dla części OSS i BSS Rozwiązania)

Nr Wymagania	Treść wymagania
O17.F9	system OSS musi pracować w architekturze HA (High Availability) – co najmniej w oparciu o HA infrastruktury serwerowej
O17.F10	Rozwiązanie musi umożliwiać integrację ze storage obiektywnym (protokołem REST API lub S3) w celu przesyłania wybranych danych do archiwum
O17.F11	systemy OSS muszą zapewnić możliwość kreowania nowych użytkowników o różnych poziomach dostępu (np. ReadOnly, ReadWrite, Admin etc.)

7.5. Opis funkcjonalności dla obszaru BSS

7.5.1. Obszar Centrum Kontaktu

Segment	Nr. wymagania	Treść wymagania
Wymagania podstawowe	O21.F1	Wymagane jest, aby automatyczna obsługa klienta była rozwiązaniem sprzętowym i programowym dedykowanym do obsługi połączeń działającym w całości w oparciu o protokół IP.
Wymagania podstawowe	O21.F2	Rozwiązanie musi zapewniać obsługę jednocześnie połączeń przychodzących (inbound) i wychodzących (outbound) z systemu.
Wymagania podstawowe	O21.F3	Rozwiązanie musi umożliwiać obsługę wielu kanałów dostępu (w tym: telefon, chat, e-mail, formularz WWW)
Wymagania podstawowe	O21.F4	Rozwiązanie musi posiadać zintegrowany moduł interaktywnej administrowalnej zapowiedzi głosowej (IVR - Interactive voice response)
Wymagania podstawowe	O21.F5	Rozwiązanie musi posiadać zaimplementowane zaawansowane algorytmy dystrybucji połączeń telefonicznych do kolejek / agentów (ACD – Automatic Call Distribution/ SBR – Skill Based Routing)
Wymagania podstawowe	O21.F6	Rozwiązanie musi zapewniać interakcję modułów IVR i ACD
Wymagania podstawowe	O21.F7	Rozwiązanie musi posiadać funkcję automatycznego oddzwonienia (Call Back), w przypadku nieodebrania połączenia przez konsultanta, realizująca połączenie zwrotne: - automatycznie po ustalonym czasie kierując je do wolnego konsultanta (np. musi się ono odbyć do 10 min.po otrzymaniu zgłoszenia.)

Segment	Nr. wymagania	Treść wymagania
		- na żądanie, z możliwością wybrania, kiedy konsultant ma do niego oddzwonić. Powinna być możliwość skonfigurowania w IVR ram czasowych, w których System wykona połączenie i skieruje je do wolnego konsultanta
Wymagania podstawowe	O21.F8	Rozwiązanie musi umożliwiać obsługę protokołu Voice-over-IP w standardzie SIP (zgodność z RFC3261)
Wymagania podstawowe	O21.F9	Rozwiązanie musi wykorzystywać do przesyłania strumienia głosowego kodek G.711 oraz G.729.
Wymagania podstawowe	O21.F10	Rozwiązanie musi umożliwiać zestawienia bezpiecznej, szyfrowanej komunikacji głosowej w dowolnych relacjach (obsługa protokołu SRTP oraz TLS).
Wymagania podstawowe	O21.F11	Rozwiązanie musi posiadać interfejs graficzny aplikacji użytkownika oraz administratora w języku polskim.
Wymagania podstawowe	O21.F12	Rozwiązanie powinno móc obsługiwać do 150 wydzielonych stanowisk do pracy zmianowej z wykreowanymi kontami dla poszczególnych agentów (nielimitowana liczba kont agentów) oraz w ramach pakietu licencji rozwiązanie powinno dawać możliwość skorzystania z IVR nie mniej jak 300 klientom jednocześnie w kolejce oczekującej.
Wymagania podstawowe	O21.F13	Rozwiązanie stanowiący przedmiot oferty musi być skalowalny, z możliwością obsługi przynajmniej 80 agentów.
Wymagania podstawowe	O21.F14	Rozwiązanie musi umożliwiać wykorzystanie parametrów opisujących specyficzne umiejętności agentów SBR – Skill Based Routing) oraz modyfikowania konfiguracji SBR przez administratorów po stronie NASK.
Wymagania podstawowe	O21.F15	Wszyscy agenci powinni mieć licencje w ramach, których, powinni móc obsługiwać dowolny kanał komunikacyjny.
Wymagania podstawowe	O21.F16	Rozwiązanie musi umożliwiać kontrolę bieżącą pracy agentów przez jednocześnie do 10 nadzorców (supervisors), posiadających licencje z poszerzonym zakresem funkcjonalności w stosunku do agentów o funkcje: raportowania, przeszukiwania biblioteki nagrań.
Wymagania podstawowe	O21.F17	Rozwiązanie musi udostępniać agentom jeden program (w wersji web - ze zintegrowanym klientem WebRTC lub w postaci aplikacji Windows - ze zintegrowanym softfonem) do obsługi wszystkich operacji contact center. Obie wersje powinny również obsługiwać zewnętrzny aparat telefoniczny.
Wymagania podstawowe	O21.F18	Rozwiązanie musi umożliwiać supervisorom dostęp do historii połączeń, nagrań, maili, chatów, raportów statystycznych oraz funkcji zarządzania agentami, listami kontaktów i innymi parametrami.
Wymagania podstawowe	O21.F19	Rozwiązanie musi umożliwiać automatyczne rozpoznawanie dzwoniącego oraz wyświetlanie karty z historią dotychczasowych kontaktów.
Wymagania podstawowe	O21.F20	Rozwiązanie musi umożliwiać wykorzystanie skryptów standaryzujących przebieg rozmów oraz szablonów do obsługi maili / chatów.

Segment	Nr. wymagania	Treść wymagania
Wymagania podstawowe	O21.F21	Rozwiązanie musi mieć możliwość sterowania przebiegiem połączenia przez agenta: <ul style="list-style-type: none"> - transfer połączenia na inny numer - konsultacja - transfer po konsultacji - hold
Wymagania podstawowe	O21.F22	Rozwiązanie musi umożliwiać rejestrację historii kontaktów z agentem contact center (o ile dostępna jest identyfikacja CLIP) oraz rozpoznawanie dzwoniącego na podstawie danych znajdujących się w CRM (numer telefonu) wraz z możliwością importowania kolejnych pozycji
Wymagania podstawowe	O21.F23	Rozwiązanie musi umożliwiać wykorzystanie wielu różnych źródeł danych, jako książek adresowych takich jak przykładowo Active Directory, bazy ODBC, arkusz kalkulacyjny, pliki tekstowe.txt.
Wymagania podstawowe	O21.F24	Tryb ruchu wychodzącego powinien zapewniać funkcjonalności: <ul style="list-style-type: none"> - przekazywanie kontaktu do wydzwonienia na ekran agenta. Agent sam decyduje, kiedy wykonać połączenie do klienta. - tryb automatycznie wykonujący połączenia, w którym System wykonuje tylko tyle połączeń ile jest wolnych agentów, - tryb automatycznie wykonujący połączenia, w którym System wydzwania odpowiednio większą ilość połączeń w stosunku do ilości agentów bazując na danych historycznych, zdefiniowanych parametrach progowych i dedykowanych algorytmach - tryb automatycznie wykonujący połączenia do klientów z Systemu IVR zbierający automatycznie informacje poprzez kody DTMF, opcjonalnie z możliwością detekcji głosu ludzkiego i automatycznych sekretarek.
Wymagania podstawowe	O21.F25	Rozwiązanie musi umożliwiać zarządzanie w oparciu o role, w tym możliwość definiowania własnych ról.
Wymagania podstawowe	O21.F26	Rozwiązanie musi posiadać wspólny interfejs administracyjny dla wszystkich dostarczanych modułów Systemu w języku polskim, łączący funkcje zarządzania, sprawdzania historii pracy i analizy statystycznej przy zastosowaniu raportów oraz monitorowania w czasie rzeczywistym. Raporty i widoki monitoringu mogą być w szerokim zakresie dostosowane do konkretnych potrzeb.
Wymagania podstawowe	O21.F27	Rozwiązanie musi umożliwiać zarządzanie i monitorowanie pracy oraz kolejek i agentów w czasie rzeczywistym. Dostępne raporty bieżące i historyczne z pracy Systemu na poziomie kolejek, agentów, IVR, KPI.
Wymagania podstawowe	O21.F28	Rozwiązanie musi umożliwiać nagrywanie oraz posiadać możliwość eksportowania plików dźwiękowych w formacie WAV lub MP3. (3500 nagrań dziennie, które mają być przechowywane przez okres 3 lat)
Wymagania podstawowe	O21.F29	Funkcjonalność nagrywania rozmów musi zapewniać udokumentowane API umożliwiające integrację z systemami firm trzecich.

Segment	Nr. wymagania	Treść wymagania
Wymagania podstawowe	O21.F30	Musi być możliwa klasyfikacja kontaktów per kanał obsługi (niezbędna do analizy przyczyn kontaktu).
Wymagania podstawowe	O21.F31	Rozwiązanie musi zapewniać funkcjonalność samokontroli działania rozumianej, jako automatyczne testowanie działania serwisów działających na serwerze oraz możliwość wysyłania komunikatów o stanie Systemu protokołem SNMP oraz na definiowane w rozwiązaniu konta poczty internetowej.
Wymagania podstawowe	O21.F32	Rozwiązanie musi umożliwiać konfigurację progów zajętości pamięci i dysków, dla których następuje powiadomienie SMTP.
Wymagania podstawowe	O21.F33	Rozwiązanie musi posiadać mechanizmy służące do wykonywania kopii bezpieczeństwa danych i konfiguracji do wskazanej lokalizacji zdalnej poprzez protokół ssh oraz ftp.
Wymagania podstawowe	O21.F34	Rozwiązanie powinno być wyposażony w mechanizmy łatwego przywracania konfiguracji i danych z kopii bezpieczeństwa. Wykonywanie kopii bezpieczeństwa powinno być możliwe automatycznie z wykorzystaniem definiowanych harmonogramów oraz ręcznie na podstawie odpowiedniej funkcji dostępnej dla użytkowników z odpowiednimi uprawnieniami.
ACD (Automatic Call Distribution)	O21.F35	Rozwiązanie musi umożliwiać kolejkowanie i automatyczną dystrybucję połączeń w zależności od definiowalnych kryteriów – ACD, przy czym algorytmy kolejkowania powinny móc uwzględniać: <ul style="list-style-type: none"> - obciążenie agenta (czas rozmów, ilość odebranych połączeń, czas nieaktywności i inne.) - fakt posiadania przez agenta konkretnych umiejętności (skill) wraz z możliwością określenia ich poziomu (skill level – infolinia, sales, I/II/III linia wsparcia) oraz dawać możliwość modyfikowania SBR (Skills-based routing) dla supervisorów - czas/datę, porę dnia i tygodnia - dodatkowe informacje o dzwoniącym dostępne z zewnętrznych źródeł danych
IVR (Interactive Voice Responder)	O21.F36	Rozwiązanie musi umożliwiać wykorzystanie IVR do interakcja z klientem i przetwarzanie danych wprowadzonych przez klientów.
IVR (Interactive Voice Responder)	O21.F37	Rozwiązanie musi umożliwiać automatyczną obsługę połączeń przez IVR, definiowaną przez skrypty. Skrypty muszą umożliwiać: <ul style="list-style-type: none"> - odgrywanie zapowiedzi głosowych zapisanych w plikach w formacie WAV, MP3 - odczyt i interpretację sygnałów DTMF - możliwość odwoływania się do danych w źródłach HTTP/XML - możliwość sięgania do danych w źródłach SQL, ODBC - możliwość komunikacji z wykorzystaniem Rest API, WebService SOAP API - odczytywanie danych systemowych takich jak liczba połączeń oczekujących w kolejkach, średni czas oczekiwania na połączenie, ilość połączeń obsłużonych, ilość połączeń zaniechanych, ilość połączeń przekierowanych do

Segment	Nr. wymagania	Treść wymagania
		obsługi w kanale IVR, średni czas rozmowy, średni czas oczekiwania w połączeniach zaniechanych - kolejkovanie połączenia do wybranej kolejki z przypisaną do nich grupą agentów
IVR (Interactive Voice Responder)	O21.F38	Rozwiązanie musi umożliwiać wykorzystanie IVR do rozpoznawania klienta na podstawie numeru telefonu (ANI - Automatic Number Identification), numeru wybranej usługi (DNIS - Dialed Number Identification Service).
IVR (Interactive Voice Responder)	O21.F39	Rozwiązanie musi umożliwiać wykorzystanie IVR do automatycznej obsługi dzwoniącego (po jego autoryzacji - ID i PIN) do: - udzielanie informacji personalizowanych - informowania o danych udostępnionych w systemach Zamawiającego (Trouble Ticketing itp.) - sprawdzenia statusów zleceń: - zamknięcie zgłoszenia/potwierdzenie zakończenia braku działania usługi (awarii) - lista incydentów bezpieczeństwa - informowania o aktualnych awariach i problemach - zmiany hasła
IVR (Interactive Voice Responder)	O21.F40	Rozwiązanie musi umożliwiać wykorzystanie IVR do automatycznej obsługi dzwoniącego (bez potrzeby autoryzacji) do: udostępnianie informacji technicznych, handlowych i marketingowych, przechowywanych w postaci nagranych zapowiedzi lub z wykorzystaniem systemu Text To Speech
IVR (Interactive Voice Responder)	O21.F41	Moduł IVR musi umożliwiać przełączanie rozmowy do konsultantów lub do innego serwisu automatycznego
IVR (Interactive Voice Responder)	O21.F42	Moduł IVR musi umożliwiać integracja z zewnętrznymi systemami
Integracja	O21.F43	Funkcjonalność Centrum Kontaktu musi posiadać narzędzia do integracji z innymi systemami Zamawiającego (biznesowymi i back-office), zapewniając dynamiczną wymianę danych poprzez: - ODBC - Pliki płaskie,. txt - Pliki XML - Web Services (preferowany REST API) - HTTP
Portal	O21.F44	Rozwiązanie musi zawierać portal samoobsługowy dla klientów (funkcjonujący pod nazwą - Portal Usługowy), którego zadaniem będzie zapewnienie obsługi klientów usług OSE.
Portal	O21.F45	Portal Usługowy musi zawierać funkcjonalność umożliwiającą rejestrację (zgłoszenie) nowej szkoły do OSE. Dla stanu przejściowego (gdy będą

Segment	Nr. wymagania	Treść wymagania
		funkcjonowały systemy przejściowe i docelowe) rejestracja w sytuacji, gdy w lokalizacji szkolnej już jest podłączone OSE, powinna być kierowana do systemów obsługujących szkoły w danej lokalizacji. W przeciwnym przypadku rejestracja powinna być kierowana do systemów docelowych. Rejestracja jest funkcjonalnością dostępna bez logowania. Weryfikacja uprawnień odbywa się na podstawie kodu autoryzacyjnego przesyłanego do szkół inną drogą
Portal	O21.F46	Portal Usługowy musi zawierać funkcjonalność logowania użytkownika. Musi ona wykorzystywać bazę użytkowników OSE działającą w ramach Portalu OSE. Na podstawie loginu i hasła zwrócone zostaną informacje o szkołach, do jakich dany użytkownik występuje oraz rolach, jakie w tych szkołach pełni - na podstawie tych informacji użytkownik powinien mieć dostępne funkcjonalności na Portalu Usługowym.
Portal	O21.F47	Portal Usługowy musi zawierać funkcjonalność umożliwiającą przeglądanie szkół (np. w formie listy) przypisanych do użytkownika oraz po wybraniu szkoły (lub gdy użytkownik jest przypisany wyłącznie do jednej szkoły) muszą być pokazane usługi dla szkoły wraz z ich parametrami. Dane dotyczące usług w szkołach powinny być pobierane online z właściwych systemów BSS.
Portal	O21.F48	Portal Usługowy musi zawierać funkcjonalność umożliwiającą zgłaszanie problemów przez użytkownika zarówno dotyczących poszczególnych usług jak i niezwiązanych z usługami (np. błędy w danych adresowych, fakturach itp..)
Portal	O21.F49	Portal Usługowy musi zawierać funkcjonalność umożliwiającą modyfikację stanu usług w kontekście szkoły - zamawianie nowych usług, zmiany parametrów aktywnych usług, dezaktywację usług.
Portal	O21.F50	Portal Usługowy musi zawierać funkcjonalność umożliwiającą weryfikację stanu rozliczeń dla szkoły w tym prezentację: faktur, należności, wpłat, salda.
Portal	O21.F51	Portal Usługowy musi zawierać funkcjonalność do prezentacji raportów/statystyk bezpieczeństwa/sieci. Raporty będą wgrywane na zasoby dyskowe przez systemy bezpieczeństwa w postaci plików graficznych, a następnie użytkownik będzie mógł przeglądać te raporty.
Portal	O21.F52	Portal Usługowy musi mieć funkcjonalność do prezentacji alertów. Alerty będą przesyłane przez systemy bezpieczeństwa na zasoby danych (baza danych, pliki) Portalu Usługowego. Użytkownik po zalogowaniu automatycznie powinien mieć zaprezentowane wszystkie nowe alerty (w postaci listy) - od ostatniego zalogowania. Dodatkowo musi być możliwość w ramach opcji przechodzenia do ekranu alertów, na którym będzie można przeglądać alerty oraz je kasować. Operacje powinny być możliwe dla poszczególnych alertów jak i dla grup alertów (grupowanie zarówno poprzez checkboxy jak i filtry)
Portal	O21.F53	Portal Usługowy musi posiadać funkcjonalność umożliwiającą zarządzanie rolami, czyli przypisywanie dostępu do funkcjonalności na podstawie roli użytkownika (np. przeglądanie alertów wyłącznie dla Dyrektora). Musi być możliwe zarządzanie uprawnieniami wynikającymi z poszczególnych roli

Segment	Nr. wymagania	Treść wymagania
		różnorodnie zależnie od typu lokalizacji (np. w lokalizacji OSE użytkownik TRS może zgłaszać problemy, a w lokalizacji MAN już nie).
Portal	O21.F54	Portal Usługowy musi mieć możliwość zarządzania uprawnieniami na poziomie poszczególnych produktów - np. produkty bezpieczeństwa mogą być modyfikowane wyłącznie przez dyrektora, tylko dyrektor może widzieć parametry usług bezpieczeństwa.
Portal	O21.F55	Portal Usługowy musi zapewniać pełne wsparcie dla procesu rejestracji szkoły - musi umożliwiać wgrywanie tzw. harmonogramu, czyli listy szkół, które mogą się zarejestrować, wraz z cennikami dla poszczególnych szkół w regionach za usługi płatne.
Portal	O21.F56	Portal Usługowy musi wysyłać do systemów BSS (lub w etapie przejściowym do systemów BSS-JIRA) zlecenia modyfikacji usług, zgłoszenia rejestracji, zgłoszenia problemów oraz pobierać wszystkie niezbędne dane z systemów BSS.
Portal	O21.F57	Na Portalu Usługowym musi być dostępny Widok Szkoła (otwierany automatycznie po zalogowaniu w przypadku użytkownika przypisanego do jednej szkoły lub po wybraniu szkoły na liście dla użytkowników przypisanych do więcej niż jednej szkoły).
Portal	O21.F58	Widok Szkoła na Portalu Usługowym musi w ramach zakładek (lub podobnej funkcjonalności) prezentować następujące grupy danych: szkoły, lokalizacji, organu prowadzącego, statusu podłączenia do OSE, użytkowników, usług, rozliczeń, zgłoszeń.
Portal	O21.F59	Portal Usługowy musi umożliwiać śledzenie bieżącego statusu zgłoszeń dotyczących zmian na usługach lub zgłoszeń problemów, jakie zostały zarejestrowane na portalu.
Portal	O21.F60	Portal Usługowy musi zawierać funkcjonalność Skrzynki Kontaktowej umożliwiając zalogowanemu użytkownikowi wysyłanie wiadomości do Centrum Kontakt z poziomu Portalu bez konieczności wykorzystywania poczty email. Skrzynka kontaktowa musi umożliwiać zarówno wysyłanie jak i odbieranie wiadomości w ramach funkcjonalności Portalu Usługowego bez konieczności wykorzystania programu pocztowego.
Portal	O21.F61	Portal Usługowy musi zawierać formularz kontaktowy umożliwiający wysłanie przez zalogowanego użytkownika wiadomości email na skonfigurowany adres email. Użytkownik powinien mieć możliwość wpisania, tematu, treści wiadomości oraz adresu email, na jaki ma być dostarczona odpowiedź. Musi być również możliwe dołączenie pliku, jako załącznika do wiadomości.
Portal	O21.F62	Portal Usługowy musi zostać zintegrowany z chat-em umożliwiając kontakt zalogowanego użytkownika z Centrum Kontakt za pośrednictwem kanału chat.
Portal	O21.F63	Portal Usługowy musi zawierać funkcjonalność umożliwiającą aktualizację danych szkoły niezgłoszonej do OSE (funkcjonalność dedykowana dla OPS-

Segment	Nr. wymagania	Treść wymagania
		ów). Aktualizacja danych przez OPS jest funkcjonalnością dostępna bez logowania. Weryfikacja uprawnień odbywa się na podstawie kodu autoryzacyjnego przesyłanego do OPS inną drogą. Funkcjonalność musi umożliwiać poprawienie danych szkolnych wraz z propagacją informacji do wszystkich systemów (zarówno przejściowych jak i docelowych)
Portal	O21.F64	Portal Usługowy musi zawierać funkcjonalność umożliwiającą zarządzanie zgodami użytkowników (RODO, marketingowe, dotyczące usług, itp..).

7.5.2. Obszar Zarządzania Klientami

Nr wymagania	Treść wymagania
O22.F1	Należy stworzyć możliwość wyszukiwania Organu Prowadzącego Szkołę zarówno po danych tego organu (nazwa, adres, NIP) jak i na podstawie danych przypisanych do niego szkół (RSPO, adres, NIP)
O22.F2	Należy stworzyć Widok "Organ Prowadzący Szkołę", na który będą prezentowane dane jednostki organizacyjnej, osób kontaktowych dla OSE oraz lista przypisanych dla danego organu szkół wraz z ich obecnym statusem. Z organu musi być możliwość przejścia do Widoku Szkoły (Widok 360).
O22.F3	Należy stworzyć możliwość wyszukiwania szkoły po danych OPS, osób kontaktowych (numer telefonu, email) oraz danych samej szkoły (RSPO, lokalizacja, dane adresowe, NIP, nazwa)
O22.F4	Należy stworzyć Widok "Szkoła" prezentujący wszystkie dane jednostki oświatowej: <ul style="list-style-type: none"> - dane OPS - dane identyfikacyjne szkoły (RSPO, nazwa, etc.) - dane rozliczeniowe (płatnik, saldo konta) - dane adresowe - osoby kontaktowe - otwarte zamówienia - otwarte sprawy (reklamacje jak również wszelkie inne zgłoszenia)
O22.F5	Należy zapewnić możliwość wyszukania wszystkich szkół dla lokalizacji na podstawie danych jednej ze szkół (RSPO, adres)
O22.F6	Należy stworzyć Widok "Lokalizacja" prezentujący podstawowe dane wszystkich szkół w lokalizacji: <ul style="list-style-type: none"> - dane OPS - podstawowe dane szkół (RSPO, nazwa, NIP) - listę otwartych zamówień (dla lokalizacji jak i szkół w lokalizacji) - listę otwartych zgłoszeń
O22.F7	Wyszukanie OPS, szkoły lub lokalizacji nie może zajmować więcej niż 5 sekund
O22.F8	Otwarcie ekranu OPS, Szkoła, Lokalizacja nie może zajmować więcej niż 5 sekund
O22.F9	Należy stworzyć ekran do przeglądania wszystkich zamówień dla wyszukanej szkoły wraz z możliwością filtrowania po jednym lub wielu filtrach: <ul style="list-style-type: none"> - zakres dat (dla stworzenia, zakończenia zamówienia)

Nr wymagania	Treść wymagania
	<ul style="list-style-type: none"> - statusie - produkcie / ofercie w zamówieniu
O22.F10	<p>Należy stworzyć ekran do przeglądania wszystkich zamówień dla wyszukanej lokalizacji wraz z możliwością filtrowania po jednym lub wielu filtrach:</p> <ul style="list-style-type: none"> - zakres dat (dla stworzenia, zakończenia zamówienia) - statusie - produkcie / ofercie w zamówieniu
O22.F11	Czas wyszukania wszystkich zamówień dla szkoły, lokalizacji lub podwykonawcy nie może przekraczać 7 sekund, zmiana filtrowania nie może trwać dłużej niż 2 sekundy
O22.F12	Rozwiązanie musi posiadać drzewiastą strukturę klienta, gdzie właściciel usługi, może mieć zdefiniowanych różnych płatników za różne usługi (w większości przypadków właściciel usługi = płatnik za usługę), umożliwiając definiowanie wielu kont rozliczeniowych/umów (usługi na oddzielnych fakturach, inne terminy płatności, itd.)
O22.F13	Rozwiązanie musi umożliwiać generowanie unikatowego numeru klienta wg zdefiniowanej przez NASK maski / reguły.
O22.F14	<p>Rozwiązanie w kontekście Klienta musi umożliwiać definiowanie między innymi następujących pól: nazwa, dane adresowe, NIP, adresy do korespondencji, adresy funkcyjne i kontaktowe e-mail, termin płatności, sposób wystawiania faktury, dodatkowe atrybuty etc.</p> <p>Rozwiązanie musi pozwalać na określenie pól i wartości wymaganych/niedozwolonych przy zakładaniu/modyfikacji klienta i innych obiektów oraz umożliwiać elastyczne definiowanie pól identyfikujących Klienta (np. RSPO, zewnętrzny identyfikator)</p>
O22.F15	Rozwiązanie musi pozwalać na elastyczne rozszerzanie modelu informacyjnego
O22.F16	Rozwiązanie musi umożliwiać aktywowanie usług z określeniem czasu/daty ich trwania, po którym powinno nastąpić zaprzestanie rozliczania i deaktywowanie usługi
O22.F17	Rozwiązanie musi umożliwiać ustawienie dezaktywacji usług w dowolnym czasie z dowolną datą w przyszłości
O22.F18	Rozwiązanie musi zawierać Widok 360 dla szkoły prezentujące zamówienia / zgłoszenia zrealizowane, stan obecny usług oraz otwarte / w trakcie zgłoszenia zamówienia.
O22.F19	Rozwiązanie musi zawierać Widok 360 dla lokalizacji prezentujące zamówienia / zgłoszenia zrealizowane, stan obecny usług oraz otwarte / w trakcie zgłoszenia zamówienia.
O22.F20	Rozwiązanie musi być zgodne z modelem danych przedstawionym w rozdziale "3. Architektura Biznesowa Operatora OSE"
O22.F21	Ekran PWR musi wyświetlać wszystkie informacje dla danego PWR-a, operatora odpowiedzialnego za PWR-a, listę łącz doprowadzonych do PWR-a, listę szkół przypisanych dla danego PWR-a.
O22.F22	Ekran: Szkoły musi wyświetlać wszystkie informacje o szkole: podstawowe informacje ewidencyjne (adres, RSPO, nazwa itp.), listę osób kontaktowych, dane OPS, zakładka ze zleceniami (domyślnie zlecenia aktywne/otwarte), dane lokalizacji, w jakiej znajduje się szkoła, usługi aktywne w szkole, zakładkę z danymi rozliczeniowymi (faktury, należności)

Nr wymagania	Treść wymagania
O22.F23	Moduł CRM musi zawierać funkcjonalność umożliwiającą zarządzanie zgodami zarówno na poziomie klienta, użytkownika jak i produktu/usługi

7.5.3. Obszar Zarządzania Partnerami

Nr wymagania	Treść wymagania
O23.F1	Należy stworzyć Widok "Podwykonawca" prezentujący: <ul style="list-style-type: none"> - Podstawowe dane podwykonawcy - Dane kontaktowe podwykonawcy - Dane rozliczeniowe podwykonawcy (w tym bieżące saldo konta) - Listę aktywnych zleceń z podziałem na poszczególne lokalizacje
O23.F2	Należy stworzyć możliwość wyszukania podwykonawcy na podstawie danych podwykonawcy lub szkół lub lokalizacji przypisanych do danego podwykonawcy
O23.F3	Należy stworzyć ekran do przeglądania wszystkich zamówień dla wyszukanego podwykonawcy wraz z możliwością filtrowania po jednym lub wielu filtrach: <ul style="list-style-type: none"> - zakres dat (dla stworzenia, zakończenia zamówienia) - statusie - lokalizacji - szkole
O23.F4	Czas wyszukania podwykonawcy nie może trwać dłużej niż 5 sekund
O23.F5	Rozwiązanie musi umożliwiać konfigurację usług wraz z cenami świadczonych przez partnerów na rzecz Operatora OSE.
O23.F6	Rozwiązanie musi wspierać rozliczenia z partnerami. Umożliwiać przyjmowanie faktur od partnerów, monitorowanie procesu rozliczeń oraz umożliwiać zgłaszanie uwag do faktur.
O23.F7	Rozwiązanie musi umożliwiać edytowanie danych partnerów / dostawców.
O23.F8	Rozwiązanie musi zapewniać wyświetlanie wszystkich obecnych i historycznych zamówień / zleceń wraz z weryfikacją terminowości ich realizacji.
O23.F9	Rozwiązanie musi umożliwiać składowanie / archiwizowanie dokumentów umów z partnerami oraz dostęp do archiwalnych dokumentów. Musi również być możliwe zarządzanie umowami, ich numeracją i czasami obowiązywania.
O23.F10	Rozwiązanie musi umożliwiać zarządzanie cennikami usług dostawców / partnerów: <ul style="list-style-type: none"> - definiowanie usług - wprowadzanie cen ręcznie lub ładowanie ich z pliku - powiązanie cenników z umowami
O23.F11	Rozwiązanie musi umożliwiać funkcjonalność do automatycznej weryfikacji faktur partnerów z cennikami. Taka walidacja powinna być możliwa do włączenia poprzez modyfikacje konfiguracji oddzielnie dla każdego partnera / umowy / regionu.

Nr wymagania	Treść wymagania
O23.F12	Rozwiązanie musi umożliwiać zarządzanie bazą podwykonawców: definiowanie, przypisywanie do lokalizacji, zmiana dostępności, zmiana stanu aktywny / nieaktywny.
O23.F13	Rozwiązanie musi umożliwiać definiowanie wielu rodzaju podwykonawców (partnerzy serwisowi, dostawcy, operatorzy łącz dostępowych, operatorzy sieci regionalnych itp.)

7.5.4. Obszar Rozliczeń

Nr wymagania	Treść wymagania
O24.F1	Rozwiązanie musi umożliwiać rozliczanie produktów zgodnie z ofertą, w jakiej zostały zakupione na podstawie cennika z katalogu produktów.
O24.F2	Faktura powinna być wystawiana wyłącznie dla produktów płatnych i tylko takie produkty powinny się na niej znajdować.
O24.F3	Rozwiązanie musi umożliwiać rozliczanie z klientami w miesięcznych cyklach rozliczeniowych
O24.F4	Musi być możliwe wygenerowanie faktury na żądanie przed upływem cyklu miesięcznego ręcznie, lub w przypadku rozwiązania umowy.
O24.F5	Musi być możliwe skonfigurowanie wielu cykli rozliczeniowych.
O24.F6	Musi być możliwe wybieranie cyklu rozliczeniowego dla każdego konta rozliczeniowego oddzielnie.
O24.F7	Funkcjonalność rozliczeniowa musi uwzględniać zarówno opłaty w modelu abonamentowym jak i jednorazowe (np.. Instalacyjne). Musi być również możliwe rozliczanie produktów jednorazowych np. wizyt serwisowych
O24.F8	Musi być możliwe powiązanie kosztów z produktami (usług partnerów takich jak np.. Instalacja, kosztów zasobów jak np.. koszty łącz). Może to zostać zrealizowane w Centralnym Systemie Raportowym.
O24.F9	Musi być możliwa weryfikacja przychodów z produktów płatnych z kosztami tych produktów w podziale na koszty jednorazowe i cykliczne. Może to zostać zrealizowane w Centralnym Systemie Raportowym.
O24.F10	Rozwiązanie umożliwi konfigurowanie opłat cyklicznych/abonamentowych, opłat jednorazowych/aktywacyjnych, opłat za zdarzenia, (czyli opłat, które będą używane przy rozliczeniach tylko w przypadku zamówienia/zaistnienia, wykonania przez klienta lub przekroczenia poziomu danej usługi)
O24.F11	Rozwiązanie zapewni możliwość określenia terminów płatności od wystawienia, od otrzymania faktury i na dany konkretny dzień miesiąca. Określenie terminu od otrzymania, niezależnie od etykiety na fakturze, powinno odbywać się w rozwiązaniu poprzez dodanie ustalonej liczby dni, z możliwością późniejszej zmiany tej wartości.

Nr wymagania	Treść wymagania
O24.F12	Rozwiązanie musi zapewniać masowe generowanie numerów rachunków, czyli umożliwiać zdefiniowanie dla każdego konta billingowego własnego rachunku, wykorzystując kod klienta i numer konta banku.
O24.F13	Rozwiązanie umożliwi stosowanie tego samego konta bankowego dla wielu umów w obrębie klienta
O24.F14	Rozwiązanie umożliwi zdefiniowanie różnych rachunków bankowych w ramach jednego klienta
O24.F15	Rozwiązanie musi umożliwiać przypisywanie rabatów do każdej kategorii opłat za usługę jak i dla całej faktury, zarówno wyrażonych w % jak i wartości nominalnej. Rabaty będą mogły być stosowane w sposób jednorazowy (na najbliższą fakturę) lub cykliczny (na każdą fakturę). Przypisane rabaty będą wykazywane na fakturze, jako oddzielne pozycje fakturowe z określeniem usługi, jakiej dotyczy rabat.
O24.F16	W ramach funkcjonalności rabatów, rozwiązanie będzie wspierać przydzielanie rekompensat SLA, poprzez wydzielenie dedykowanej kategorii rabatowej z odpowiednią nazwą, umieszczanej na najbliższej fakturze abonamentowej.
O24.F17	Rozwiązanie będzie gotowe na obsłużenie funkcjonalności rozliczania rekompensat SLA, poprzez wyliczanie % niedostępności i rabatu kwotowego na podstawie dostarczanej informacji o czasie awarii i reguł wyliczania rekompensaty.
O24.F18	Aktywacje usług w trakcie okresu rozliczeniowego klienta będą skutkowały naliczaniem opłat proporcjonalnych tylko za dni kalendarzowe, w których usługa była uruchomiona (cena/liczba dni w okresie rozliczeniowym * liczba dni, kiedy usługa była aktywna)
O24.F19	Wszystkie pozycje na fakturze będą zawierały daty od i do jakiego dnia naliczona jest dana opłata, będą posiadały opisy ze zmiennymi atrybutami, zgodnie z konfiguracjami opisów ustalonymi w trakcie wdrożenia.
O24.F20	Rozwiązanie będzie naliczało opłaty stałe z góry za bieżący okres rozliczeniowy z pierwszym dnie danego okresu rozliczeniowego
O24.F21	Rozwiązanie będzie musi umożliwiać stosowanie różnych stawek VAT w zależności od rodzaju usług i typu klienta.
O24.F22	Rozwiązanie będzie dokonywało zaokrągleń naliczonych opłat do dwóch miejsc po przecinku (liczba miejsc po przecinku powinna być konfigurowalna)
O24.F23	Rozwiązanie będzie w przypadku zmiany usługi (typ usługi, parametry usługi) w trakcie trwania okresu rozliczeniowego, tworzyć pozycję korygującą do zera naliczone opłaty za okres od zmiany usługi do końca okresu rozliczeniowego oraz pozycję naliczającą opłaty dla nowej usługi za okres od zmiany usługi do końca okresu rozliczeniowego
O24.F24	Rozwiązanie będzie w przypadku obniżenia/podwyższenia ceny usługi w trakcie trwania okresu rozliczeniowego, tworzyć jedną pozycję fakturową z naliczonym saldem rozliczenia (pozycja zmniejszająca lub zwiększająca) proporcjonalnie dni świadczenia usługi w okresie rozliczeniowym po "starej" cenie i "nowej" cenie
O24.F25	Rozwiązanie będzie w przypadku dezaktywacji usługi w trakcie trwania okresu rozliczeniowego, tworzyć pozycję fakturową zmniejszającą opłatę za usługę proporcjonalnie za dni od daty dezaktywacji do końca okresu rozliczeniowego

Nr wymagania	Treść wymagania
O24.F26	Rozwiązanie musi umożliwiać automatyczne oraz ręczne generowanie dokumentów, e-mail, ponagleń windykacyjnych i innych informacji dla Klienta
O24.F27	Rozwiązanie umożliwi zdefiniowanie dla każdego klienta dnia wystawiania mu faktury/rozliczenia usług
O24.F28	Rozwiązanie musi umożliwiać definiowanie wzorca wyglądu dokumentów (faktury, upomnienia)
O24.F29	Rozwiązanie musi umożliwiać wystawienie Faktury korygującej, Noty odsetkowej (również w procesie automatycznym) oraz innych dokumentów finansowych związanych z rozliczeniami operatora telekomunikacyjnego z klientami.
O24.F30	W Rozwiązaniu zostanie skonfigurowany wygląd, układ i zakres informacji zawartych na dokumentach księgowych, zgodnie z dostarczonym przez NASK wzorem
O24.F31	Dokumenty finansowe w nagłówkach faktur, oprócz wymaganych prawem danych będą zawierały sekcje z numerem klienta, numerem zamówienia/umowy, indywidualnym kontem bankowym, informacjami dodatkowymi.
O24.F32	Dokumenty finansowe będą zawierały odpowiedni układ sekcji nabywców, kody kreskowe oraz znaki sterujące zgodne z przekazaną specyfikacją umożliwiające automatyczną obsługę faktur papierowych
O24.F33	Dokumenty finansowe wystawione z terminem płatności "od otrzymania/dostarczenia" niezależnie od daty bezwzględnej ustalonej w Rozwiązaniu, będą zawierały termin płatności wyrażony słownie, jako "n dni od dostarczenia faktury"
O24.F34	Rozwiązanie będzie posiadać zdefiniowane procesy uruchamiania dziennego / miesięcznego procesu wystawiania faktur możliwe do obsłużenia przez standardowego użytkownika Rozwiązania
O24.F35	Proces miesięcznego wystawiania faktur musi być możliwy do uruchamiania każdego dnia i wystawiania faktur dla klientów z danym dniem rozliczeniowym i/lub dla usług, którym naliczone zostały opłaty do dnia poprzedzającego
O24.F36	Rozwiązanie będzie udostępniać dane wystawionej faktury (pozycje faktury) oraz PDF do zewnętrznych systemów/platform
O24.F37	Rozwiązanie będzie udostępniać interfejs/kreator do wystawienia faktury korygującej do dowolnej faktury klienta
O24.F38	Rozwiązanie musi umożliwiać generowanie duplikatów każdej faktury na dany dzień
O24.F39	Rozwiązanie musi umożliwiać generowanie faktur w trybie "papierowa" i "elektroniczna" w zależności od konfiguracji konta Klienta
O24.F40	Rozwiązanie musi umożliwiać dystrybucję faktur przez różne kanały (e-mail, portal, poczta tradycyjna)
O24.F41	Rozwiązanie musi w ramach wysyłki faktur elektronicznych wykorzystywać certyfikaty poświadczające, iż nadawcą jest NASK.
O24.F42	W rozwiązaniu będzie prowadzona analityka rozliczeń z klientami tj. rozliczanie faktur i innych dokumentów księgowych z dokonywanymi wpłatami. Alokacja wpłat do należności będzie

Nr wymagania	Treść wymagania
	realizowana poza rozwiązanie i będzie przekazywana z systemu TETA. W rozwiązaniu należy zapewnić integrację do pobierania / otrzymywania informacji o wpłatach z systemu TETA.
O24.F43	Rozwiązanie musi umożliwiać tworzenie różnych scenariuszy windykacyjnych, np. ponaglenia e-mail, wezwania do zapłaty do wydruku, żądania zawieszenia usług, żądania rozwiązania umowy, noty odsetkowe itp.
O24.F44	Rozwiązanie powinno zostać zintegrowane z systemem Finansowo-Księgowym NASK (TETA) umożliwiając przesyłanie / eksportowanie wystawionych dokumentów finansowych celem ich obsługi księgowej.
O24.F45	Rozwiązanie powinno zostać zintegrowane z systemem Finansowo-Księgowym NASK (TETA) umożliwiając przyjmowanie / importowanie zarejestrowanych wpłat wraz z informacją o ich alokacji.

7.5.5. Obszar Łańcuch Dostaw

Nr wymagania	Treść wymagania
O25.F1	Rozwiązanie musi umożliwiać zarządzanie stanami magazynowymi w magazynie NASK oraz w magazynach partnerów (np., jako magazyny wirtualne). Muszą być dostępne funkcjonalności do przesuwania stanów / produktów pomiędzy magazynami. Musi być możliwa aktualizacja stanów magazynowych.
O25.F2	Rozwiązanie musi umożliwiać dostęp dla pracowników partnerów do ewidencji magazynów przypisanych dla partnera.
O25.F3	Rozwiązanie musi umożliwiać weryfikację stanów magazynowych w poszczególnych magazynach przypisanych do partnerów względem zamówień, jakie oczekują lub są w realizacji umożliwiając pokazanie braków towarowych w magazynach rzutujących na brak możliwości realizacji zamówień. W ramach funkcjonalności muszą być na ekranie prezentowane magazyny wraz z poziomem braków produktów. Dodatkowo na ekranie musi być wskazana lista / liczba zamówień, które nie będą mogły być zrealizowane.
O25.F4	Rozwiązanie musi umożliwiać modelowanie magazynów w celu odwzorowania cyklu życia urządzeń (np. w sytuacji przekazania CPE do naprawy, CPE nie powinno być kasowane z bazy danych) umożliwiając zachowanie ciągłości wiedzy na temat urządzenia w trakcie całego cyklu jego ewidencji
O25.F5	Rozwiązanie musi umożliwiać śledzenie na podstawie kodów paskowych przemieszczenia urządzeń pomiędzy lokalizacjami sieciowymi oraz magazynami (również wirtualnymi, jak np. „naprawa”).
O25.F6	Wszystkie urządzenia zainstalowane w sieci trafiają do inwentaryzacji przez magazyn w oparciu o zdefiniowaną sekwencję przekazania pomiędzy magazynami, w tym pomiędzy magazynem instalatora a miejscem instalacji. Usunięcie urządzenia z danej lokalizacji wiąże się z jego deinstalacją i przeniesieniem do odpowiedniego magazynu (np. magazynu napraw).
O25.F7	Rozwiązanie musi przechowywać pełną historię każdego urządzenia, głównie historię jego instalacji w poszczególnych lokalizacjach.

Nr wymagania	Treść wymagania
O25.F8	Rozwiązanie musi zapewniać wsparcie procesu zakupowego (generowanie zamówień, importowanie danych o urządzeniach z plików m.in. CSV, Excel, TXT o zdefiniowanej strukturze do umieszczenie na Zamówieniu, PZ)
O25.F9	Rozwiązanie musi umożliwiać ewidencja zarówno urządzeń - elementów policzalnych (sztuk, kompletów, itp.) jak i materiałów - elementów niepoliczalnych (metrów, litrów itp.)
O25.F10	Rozwiązanie musi umożliwiać proste wyszukiwanie oraz rozbudowane mechanizmy wyszukiwania urządzeń po wszystkich zdefiniowanych atrybutach (możliwość zakładania filtrów)
O25.F11	W rozwiązaniu musi być możliwa praca na pojedynczych urządzeniach jak również na grupach urządzeń
O25.F12	Rozwiązanie musi wspierać rejestrację dostaw nowych urządzeń lub zwrotów urządzeń do magazynu, rejestrację wydawania towaru do innych magazynów oraz do eksploatacji.
O25.F13	Rozwiązanie musi zawierać funkcjonalność nadawania kodów kreskowych towarom uczestniczącym w obrocie magazynowym, zapewniając też obsługę drukarek i czytników kodów kreskowych. Wyszukiwanie urządzeń w magazynie lub bazie danych na podstawie kodów kreskowych.
O25.F14	Rozwiązanie musi dostarczyć raporty: - analityczny raport przychodów na dany magazyn bądź grupę magazynów zawierający informację o wszystkich urządzeniach, które we wskazanym przez użytkownika okresie zostały przyjęte na dany magazynu/grupę magazynów - analityczny raport rozchodów z danego magazynu bądź grupy magazynów zawierający informację o wszystkich urządzeniach, które we wskazanym przez użytkownika okresie zostały wydane z danego magazynu/grupy magazynów
O25.F15	Rozwiązanie musi wspierać zarządzanie przekazywaniem towarów pomiędzy magazynem NASK a magazynami partnerów serwisowych. Magazyny zewnętrzne (należące do innych podmiotów) powinny zostać odwzorowane, jako magazyny wirtualne.

7.5.6. Obszar Katalog Produktów

Nr wymagania	Treść wymagania
O26.F1	Rozwiązanie musi umożliwiać definiowanie w ramach katalogu produktów pełnej struktury definicji zawierającej: Produkt, produkty składowe, usługi wykorzystywane w realizacji produktu, usługi powiązane z procesem instalacji i deinstalacji i utrzymania
O26.F2	Rozwiązanie musi umożliwiać definiowanie w ramach katalogu ofert pełne informacji cenowej uwzględniającej: ceny związane z cyklem życia produktu (instalacja, aktywacja, świadczenie, deinstalacja), regionalizację cen (różne oferty cenowe w różnych regionach).
O26.F3	Rozwiązanie musi umożliwiać weryfikację kosztów oferty poprzez powiązanie katalogu ofert z cenami usług poszczególnych partnerów niezbędnych w dostarczaniu i świadczeniu produktu

Nr wymagania	Treść wymagania
O26.F4	Rozwiązanie musi umożliwiać konfigurowanie dowolnych atrybutów dla produktów
O26.F5	Rozwiązanie musi umożliwiać konfigurowanie zależności produktowych: <ul style="list-style-type: none"> - wymaganie - jeden produkt może być oferowany wyłącznie przy zakupie innego - wykluczanie - jeden produkt nie może być oferowany, gdy klient kupuje lub posiada inny produkt - weryfikacja relacji produktowych musi być realizowana zarówno uwzględniając obecnie posiadane przez klienta produktu, obecnie składane zamówienie jak i wszelkie zamówienia w trakcie (niezrealizowane i nieanulowane)
O26.F6	Rozwiązanie musi umożliwiać definiowanie procesów dostarczenia / aktywacji / modyfikacji / dezaktywacji dla poszczególnych produktów.
O26.F7	Rozwiązanie musi umożliwiać definiowanie ofert (warunków cenowych) dla produktów w zależności od regionu / lokalizacji.

7.5.7. Obszar Zarządzania dokumentami

Nr wymagania	Treść wymagania
O27.F1	Rozwiązanie musi umożliwiać generowanie dokumentów na podstawie szablonów - poprzez wypełnienie ich danymi pobranymi z systemów. Generowanie dokumentów z szablonu musi być możliwe zarówno, jako samodzielna funkcjonalność jak również w ramach realizacji procesów.
O27.F2	Rozwiązanie musi umożliwiać masowe generowanie dokumentów dla zadanych warunków zarówno, jako pojedyncza funkcjonalność jak również w kontekście realizacji procesów biznesowych
O27.F3	Rozwiązanie musi zapewniać panel (GUI) umożliwiający zarządzania szablonami dokumentów - dodawanie, usuwanie, modyfikowanie.
O27.F4	Rozwiązanie musi umożliwiać skanowanie, przechowywanie i dostęp do skanów dokumentów.
O27.F5	Funkcjonalność do zarządzania dokumentami musi mieć możliwość wykorzystania / integracji ze storagem obiekowym
O27.F6	Rozwiązanie musi zawierać wydajne repozytorium dokument umożliwiających przechowywanie skanów dokumentów i dostęp do nich z poziomu procesów biznesowych
O27.F7	Repozytorium dokumentów musi zawierać mechanizm indeksowania i GUI do wyszukiwania dokumentów. Musi być możliwe wyszukiwanie dokumentów po danych kluczowych / wyróżniających w modelu danych (np.. RSPO, nr umowy, NIP/REGON itp.)
O27.F8	Rozwiązanie musi zawierać funkcjonalność masowego wydruku dokumentów
O27.F9	Rozwiązanie musi zawierać moduł do zarządzania obiegiem dokumentów.

7.5.8. Obszar Zarządzania przedsiębiorstwem

Nr wymagania	Treść wymagania
O28.F1	Rozwiązanie musi zawierać platformę do komunikacji korporacyjnej w ramach OSE pozwalającą na publikowanie i przekazywanie treści do pracowników OSE (zarówno własnych NASK jak i partnerów).
O28.F2	Rozwiązanie musi zawierać funkcjonalność do rozliczania działalności OSE, jako projektu finansowanego ze środków publicznych. Funkcjonalność może zostać zrealizowana w oparciu o Centralny System Raportowy.
O28.F3	Rozwiązanie musi zostać zintegrowane z systemem TETA celem przekazywania danych z systemów rozliczeniowych
O28.F4	Rozwiązanie musi umożliwiać prowadzenie odrębnej ewidencji przychodów i kosztów związanych: 1) Ze świadczeniem usług bezpiecznego dostępu do internetu 2) z wykonywaniem innych zadań operatora OSE Jak również odpowiedniego rozdzielenia struktury przychodów i kosztów jak to zostało zdefiniowane w ustawie o OSE.
O28.F5	Dezaktywacja usług w trakcie trwania okresu rozliczeniowego powinna skutkować odpowiednim skorygowaniem naliczonych opłat. Dezaktywacja usług z datą w przeszłości powinno skutkować skorygowaniem wszystkich naliczeń od tej daty.
O28.F6	Rozwiązanie musi zawierać funkcjonalności związane z utrzymaniem systemów IT umożliwiające zgłaszanie problemów dotyczących systemów, powiązanie ich z systemami i obsługę w ramach procesów utrzymaniowych.
O28.F7	Rozwiązanie musi zawierać bazę ewidencji konfiguracji - CMDB zintegrowaną z funkcjonalnością zgłaszania incydentów i zgłaszania zmian.
O28.F8	Rozwiązanie SD dla obszaru IT musi umożliwiać zgłaszanie problemów użytkownikom systemów wraz ze wskazaniem, jakiego systemu/ obszaru problem dotyczy
O28.F9	Rozwiązanie musi zawierać funkcjonalność do automatycznego wdrażania zmian kodu na środowisko testowe i produkcyjne
O28.F10	Należy stworzyć bazę wiedzy dotyczącą systemów rozwiązania w ramach Tree (Confluence) zawierająca informacje o problemach, instrukcje stanowiskowe, instrukcje administracyjne, i procesy utrzymaniowe
O28.F11	Baza CMDB musi umożliwiać przechowywanie danych, co najmniej o: - urządzeniach sieciowych - urządzeniach bezpieczeństwa - infrastrukturze serwerowej - oprogramowaniu - aplikacjach - certyfikatach, licencjach, bibliotekach
O28.F12	W bazie CMDB muszą być zebrane informacje pochodzące z Inventory OSS a także informacje związane z zarządzaniem elementami IT jak np. rodzaje i terminy gwarancji i wsparcia. Uzupełnianie/modyfikacja danych w bazie ma być możliwe zarówno:

Nr wymagania	Treść wymagania
	<ul style="list-style-type: none"> - ręcznie - z procesów biznesowych i procesów zachodzących w OSS - zasilaniem batchowym - przy pomocy wystawionego dedykowanego API
O28.F13	Baza CMDB musi umożliwiać rozszerzanie schematu danych o kolejne atrybuty.
O28.F14	Baza CMDB musi posiadać możliwość eksportu i importu danych przy pomocy plików Json i XML
O28.F15	Musi istnieć możliwość raportowania zawartości bazy CMDB w Centralnym Systemie Raportowym
O28.F16	CMDB musi umożliwiać synchronizację/aktualizację obiektów w bazie CMDB z zasobami, którym te obiekty odpowiadają
O28.F17	<p>Należy stworzyć na bazie Sparx Enterprise repozytorium architektoniczne do opisu następujących aspektów architektury operatora OSE:</p> <ul style="list-style-type: none"> - procesów biznesowych - systemów / modułów - integracji pomiędzy systemami / modułami - diagramów sekwencji - modelu danych / diagramu klas

7.6. Środowisko testowe

Systemy w środowisku testowym muszą posiadać identyczną funkcjonalność jak systemy w środowisku produkcyjnym. Środowisko testowe ma służyć do testowania kolejnych wersji developerskich przygotowywanych przez Dostawcę Rozwiązania po to, by po ich zaakceptowaniu móc w sposób sprawny uruchamiać kolejne wersje systemów w środowisku produkcyjnym (wdrożenia kolejnych wersji produkcyjnych leżą w zakresie odpowiedzialności Wykonawcy).

Oprócz identycznych funkcjonalnie systemów jak w środowisku produkcyjnym, należy zapewnić w środowisku testowym emulatory obecnych systemów NASK, z którymi będzie integrowane Rozwiązanie w ramach wdrożenia, czyli emulator systemu Teta i systemu Emid. Portal OSE posiada własne środowisko testowe, zatem Wykonawca jest zobowiązany należy wykonać integrację z nim na poziomie standardowych mechanizmów integracji, takich jak m.in: REST API, pliki płaskie np. JSON, XLS, CSV oraz mechanizmów zasilania Portalu raportami i statystykami.

W celu przygotowania do etapu migracji z przejściowych systemów OSE do docelowego Rozwiązania, systemy w środowisku testowym muszą być gotowe do integracji z systemami sugarCRM i Jira (systemy przejściowe) przy pomocy, co najmniej REST API, plików płaskich (np. JSON, XLS, CSV) oraz przy pomocy protokołu wymiany poczty elektronicznej (SMTP). Systemy sugarCRM i Jira posiadają własne środowiska testowe.

Systemy uruchamiane w środowisku testowym muszą być uruchamiane, jako niezależna instancja od środowiska produkcyjnego i nie mogą powodować dodatkowych kosztów, w tym kosztów licencyjnych po stronie Zamawiającego.

7.7. Infrastruktura dla systemów OSS/BSS

[Opis metryki](#)

Tytuł	Nazwa obszaru	Numer obszaru
Wirtualizacja mocy obliczeniowej	Platforma wirtualizacyjna – wymagania funkcjonalne	31
Moduł wirtualizacji przestrzeni dyskowej	Platforma wirtualizacyjna – wymagania funkcjonalne	31.1
Moduł wirtualizacji funkcji sieciowych	Platforma wirtualizacyjna – wymagania funkcjonalne	31.2
Moduł monitorowania i zarządzania pojemnością i efektywnością platformy	Platforma wirtualizacyjna – wymagania funkcjonalne	31.3
Moduł monitoringu środowiska sieciowego	Platforma wirtualizacyjna – wymagania funkcjonalne	31.4
Moduł zarządzania cyklem życia platformy	Platforma wirtualizacyjna – wymagania funkcjonalne	31.5
Moduł zbierania logów z infrastruktury	Platforma wirtualizacyjna – wymagania funkcjonalne	31.6
Infrastruktura dla środowiska produkcyjnego	Opis infrastruktury wirtualizacyjnej	32
Wymagania ilościowe dla warstwy oprogramowania	Opis infrastruktury wirtualizacyjnej	32.1
Wymagania ogólne dla warstwy sprzętowej dla serwerów w węzłach centralnych	Opis infrastruktury wirtualizacyjnej	32.2
Wymagania ogólne dla warstwy sprzętowej dla serwerów w węzłach regionalnych	Opis infrastruktury wirtualizacyjnej	32.3
Ogólne wymagania techniczne dla obiektowego systemu składowania danych	Obiektowy system składowania danych	33
Wymagania dotyczące skalowalności, budowy i architektury obiektowego systemu składowania dokumentów	Obiektowy system składowania danych	33.1
Szczegółowe wymagania funkcjonalne dla obiektowego systemu składowania danych	Obiektowy system składowania danych	33.2
Deduplikatory	Backup i Archiwizacja	34
Wymagane funkcjonalności oprogramowania do zabezpieczania danych	Backup i Archiwizacja	34.1
Wymagania dotyczące backupu serwerów (Data Center)	Backup i Archiwizacja	34.2
Wymagania funkcjonalności – dotyczących monitorowania, raportowania oraz przeszukiwania backupów	Backup i Archiwizacja	34.3

Wymagania funkcjonalności – dotyczy rozwiązań Continuous Data Protection dla środowisk wirtualnych	Backup i Archiwizacja	34.4
--	-----------------------	------

7.8. Platforma wirtualizacyjna - wymagania funkcjonalne

7.8.1 Wirtualizacja mocy obliczeniowej

Oferowana równoważna warstwa wirtualizacji musi być rozwiązaniem systemowym tzn. musi być zainstalowana bezpośrednio na sprzęcie fizycznym, nie może być częścią innego systemu operacyjnego oraz musi spełniać poniższe warunki:

Identyfikator wymagania	Treść wymagania
O31.F1	Wirtualizator, który wspiera rozwiązanie Microsoft® Clustering Services - Cluster uruchomiony na maszynach wirtualnych z systemem operacyjnym Microsoft® Windows ze wsparciem dla failover clustering, SQL clustering, i AlwaysOn Availability Groups. Wsparcie takie musi być udokumentowane na ogólnodostępnej stronie producenta oprogramowania.
O31.F2	Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z przedziału 1 do 128 procesorowych
O31.F3	Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 6 TB pamięci operacyjnej RAM
O31.F4	Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na zasobach dyskowych
O31.F5	Rozwiązanie musi umożliwiać integrację z rozwiązaniami antywirusowymi firm trzecich w zakresie skanowania maszyn wirtualnych z poziomu warstwy wirtualizacji
O31.F6	Rozwiązanie musi zapewniać zdalny i lokalny dostęp administracyjny do wszystkich serwerów fizycznych poprzez protokół SSH, z możliwością nadawania uprawnień do takiego dostępu nazwanym użytkownikom bez konieczności wykorzystania konta root
O31.F7	Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi
O31.F8	Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii
O31.F9	Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi oraz różnymi konsolami do zarządzania wirtualizacją. Rozwiązanie musi posiadać natywne mechanizmy szyfrowania, podczas przenoszenia maszyn wirtualnych, w czasie ich pracy pomiędzy serwerami fizycznymi
O31.F10	Musi zostać zapewniona odpowiednia redundancja i nadmiarowość zasobów tak by w przypadku awarii np. serwera fizycznego usługi na nim świadczone zostały automatycznie przełączone na inne serwery infrastruktury
O31.F11	Rozwiązanie musi umożliwiać łatwe i szybkie ponowne uruchomienie systemów/usług w przypadku awarii poszczególnych elementów infrastruktury bez utraty danych

O31.F12	System musi umożliwiać uruchamianie kontenerów zbudowanych w topologii Docker Image w wirtualnych maszynach
O31.F13	Rozwiązanie musi zapewniać mechanizm bezpiecznego, bezprzerwowego i automatycznego uaktualniania warstwy wirtualizacyjnej wliczając w to zarówno poprawki bezpieczeństwa, jak i zmianę jej wersji bez potrzeby wyłączania wirtualnych maszyn
O31.F15	Rozwiązanie musi posiadać, co najmniej 2 niezależne mechanizmy wzajemnej komunikacji między serwerami oraz z serwerem zarządzającym, gwarantujące właściwe działanie mechanizmów wysokiej dostępności na wypadek izolacji sieciowej serwerów fizycznych lub partycjonowania sieci
O31.F16	Decyzja o próbie przywrócenia funkcjonalności maszyny wirtualnej w przypadku awarii lub niedostępności serwera fizycznego powinna być podejmowana automatycznie, jednak musi istnieć możliwość określenia przez administratora czasu, po jakim taka decyzja jest wykonywana
O31.F17	Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek
O31.F18	Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do 60 TB
O31.F19	Rozwiązanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej
O31.F20	Rozwiązanie musi umożliwiać konfigurację HA dla każdego swojego komponentu w celu unikania awarii pojedynczego elementu
O31.F21	Oprogramowanie do wirtualizacji musi być wspierane przez producenta oferowanego rozwiązania do automatyzacji procesów (Automatyzacja) oraz wirtualizacji sieci (SDN) na wszystkich poziomach wsparcia (L1-L3). Wsparcie musi odbywać się poprzez jednorodny kanał serwisowy (jeden numer telefonów dla wszystkich zgłoszeń, jeden portal www pozwalający zarządzać licencjami i zgłaszać zlecenia serwisowe)
O31.F22	Wirtualizator musi wspierać TPM 2.0 oznacza to min., że TPM zapewnia mechanizm gwarantujący, że serwer fizyczny uruchomił się z włączoną opcją Secure Boot. Po potwierdzeniu, że Secure Boot jest włączone, system gwarantuje, że wirtualizator uruchomił w prawidłowej, niezmienionej formie poprzez weryfikację podpisu cyfrowego
O31.F23	Wirtualizator musi mieć włączenia funkcji "Microsoft virtualization-based security", tzw. Microsoft VBS dla systemów operacyjnych maszyn wirtualnych opartych o system operacyjny Windows 10 oraz Windows Server 2016.
O31.F24	Wirtualizator musi posiadać funkcjonalność wirtualnego TPM 2.0 dla maszyn wirtualnych Windows 10 oraz Windows 2016. Oznacza to, że punktu widzenia maszyny wirtualnej z systemem operacyjnym Windows 10 lub Windows 2016 wirtualny TPM widziany jest, jako standardowy TPM, gdzie można przechowywać bezpiecznie wrażliwe dane np. certyfikaty. Zawartość wirtualnego TPM przechowywana jest w pliku przynależnym do maszyny wirtualnej oraz musi być szyfrowana. W związku z tym wszystkie standardowe funkcjonalności wirtualizatora tj. wysoka dostępność czy przenoszenie maszyn wirtualnych bez ich wyłączania pomiędzy różnymi serwerami fizycznymi działa prawidłowo. Wirtualizator musi posiadać rolę administratora odpowiedzialnego za zarządzanie kluczami szyfrującymi. Rola ta powinna być odseparowana od roli administratora wirtualizatora. Oznacza, to, że tylko administrator

	odpowiedziany za szyfrowanie ma dostęp do kluczy szyfrujących oraz może zarządzać procesem szyfrowania w obrębie wirtualizatora
O31.F25	UEFI virtual BIOS – wirtualne maszyny uruchomione na systemie do wirtualizacji z wykorzystaniem technologii - Unified Extended Firmware Interface (UEFI)
O31.F26	Dostarczone oprogramowanie musi zapewniać możliwość wirtualizacji dla wszystkich dostarczonych w ramach postępowania serwerów
O31.F27	Rozwiązanie musi posiadać wsparcie dla natywnych dysków 4K
O31.F28	Rozwiązanie wirtualizatora musi posiadać mechanizmy proaktywnej wysokiej dostępności. Oznacza, to, że jeśli serwer fizyczny posiad funkcję przekazania do wirtualizatora informacji o stanie serwera, to wirtualizatora na podstawie tych danych, wirtualizator jest w stanie, proaktywnie przenieść wszystkie maszyny wirtualne na inne prawidłowo działające serwery fizyczne w klastrze, zanim dojdzie do całkowitej awarii serwera fizycznego
O31.F29	Rozwiązanie musi umożliwiać automatyczne równoważenie obciążenia CPU/MEM serwerów fizycznych pracujących, jako platforma dla infrastruktury wirtualnej
O31.F30	Oprogramowanie do wirtualizacji musi zapewniać mechanizm pozwalający tworzyć profil (szablon konfiguracji) wybranego serwera wirtualizującego, a następnie wymuszać ten profil/konfigurację na innych serwerach lub sprawdzać zgodność konfiguracji pomiędzy zdefiniowanym wcześniej profilem a wskazanym serwerem fizycznym
O31.F31	Rozwiązanie musi umożliwiać utworzenie jednorodnego, wirtualnego przełącznika sieciowego, rozproszonego na wszystkie serwery fizyczne platformy wirtualizacyjnej. Przełącznik taki musi zapewniać możliwość konfiguracji parametrów sieciowych maszyny wirtualnej z granulacją na poziomie portu tego przełącznika. Pojedyncza maszyna wirtualna musi mieć możliwość wykorzystania jednego lub wielu portów przełącznika z niezależną od siebie konfiguracją
O31.F32	Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane maksymalnie sprzed roku
O31.F33	Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi
O31.F34	Rozwiązanie, jako funkcja wirtualizatora (jądra) musi umożliwiać szyfrowanie wirtualnych maszyn oraz szyfrowanie maszyny wirtualnej podczas przenoszenia bez przerywania jej pracy na innych host lub zasób dyskowy
O31.F35	System musi zapewniać mechanizm weryfikujący integralność komponentów systemowych i plików hosta wirtualizującego oraz wirtualnej maszyny podczas ich uruchamiania (ochrona systemu hypervisor i OS wirtualnej maszyny na wypadek sfałszowania lub podmiany)

7.8.2 Moduł wirtualizacji przestrzeni dyskowej

Identyfikator wymagania	Treść wymagania
-------------------------	-----------------

O31.1.F1	Oferowane rozwiązanie musi umożliwiać zbudowanie wspólnej przestrzeni dyskowej w oparciu o dyski wewnętrzne serwerów fizycznych. Wymagane wsparcie dla konfiguracji sprzętowej serwera opartej o dyski SSD i HDD oraz dla konfiguracji serwera opartej wyłącznie o dyski SSD
O31.1.F2	Rozwiązanie musi zapewniać możliwość optymalizacji wydajności poprzez wbudowaną funkcjonalność „cache’owania” operacji odczytu / zapisu (Read/Write IO) po stronie serwerów fizycznych
O31.1.F3	Rozwiązanie musi posiadać możliwość budowania własnych schematów konfiguracji dyskowej dla przestrzeni akcelerującej operacje Read/Write (cache) oraz dla przestrzeni budującej pojemność. Wymagana jest możliwość zmiany konfiguracji zarówno pod kątem dostępności, wydajności jak i pojemności "w locie"
O31.1.F4	Rozwiązanie musi być zintegrowane z warstwą wirtualizacji w sposób bezpośredni, niewymagający instalacji/konfiguracji dodatkowych komponentów sprzętowych oraz dodatkowego oprogramowania / dodatkowych maszyn wirtualnych
O31.1.F5	Konfiguracja, zarządzanie i monitoring ww. przestrzeni dyskowej muszą być zintegrowane z konsolą zarządzającą platformą wirtualizacyjną
O31.1.F6	Rozwiązanie musi zapewniać obsługiwane dysków wirtualnych maszyn do rozmiaru min. 60TB,
O31.1.F7	Rozwiązanie musi zapewniać wysoką dostępność oraz odporność na awarie usług uruchomionych na serwerach z zainstalowanym oprogramowaniem do udostępniania przestrzeni dyskowej. Wysoka dostępność musi być realizowana w oparciu o wbudowane mechanizmy oprogramowania i nie dopuszcza się stosowania produktów firm trzecich lub dedykowanych komponentów sprzętowych, aby zapewnić ciągłość działania w przypadku awarii komponentów takich jak: serwer fizyczny i jego komponenty takie jak: dysk cache’ujący, dysk pojemnościowy
O31.1.F8	Rozwiązanie nie może w żaden sposób ograniczać funkcjonalności platformy wirtualizacyjnej zarówno w warstwie mechanizmów niezawodnościowych, wydajnościowo-optymalizacyjnych jak i zarządzania.
O31.1.F9	Rozwiązanie musi posiadać konfigurowalne mechanizmy zabezpieczania danych na wypadek niedostępności danych lub awarii sprzętowej w taki sposób, aby zabezpieczane dane można było rozlokować na min. poniższych poziomach: między różnymi lokalizacjami, między różnymi centrami przetwarzania danych, między różnymi szafami rack/chassis
O31.1.F10	Rozwiązanie musi zapewniać wsparcie dla rozwiązań sprzętowych różnych producentów i posiadać oficjalną stronę producenta, na której znajduje się lista wspieranych lub rekomendowanych konfiguracji. Rozwiązanie nie może wprowadzać ograniczenia, aby na etapie rozbudowy przestrzeni dyskowej wymagana była rozbudowa jedynie o serwery producenta wykorzystane na etapie przed rozbudową. W przypadku rozbudowy o kolejne serwery rozwiązanie nie może wprowadzać wymogu, aby w dostarczanych serwerach wymagana była instalacja komponentów sprzętowych oferowanych tylko przez jednego dostawcę/producenta (np. dyski, adaptory, specjalizowane karty i kontrolery)
O31.1.F11	Rozwiązanie musi zapewniać możliwość rozbudowy i skalowania zarówno mocy obliczeniowej, pojemności przestrzeni cache, jak i pojemności przestrzeni dyskowej
O31.1.F12	Rozwiązanie musi zapewniać możliwość rozbudowy oferowanej przestrzeni dyskowej (dodanie pojedynczego dysku, dodanie serwera/serwerów fizycznych) w sposób niewymagający przestoju i przerwy w dostępie do działających usług wirtualnych

O31.1.F13	Rozwiązanie musi zapewniać możliwość ochrony danych przed utratą ich integralności (np.: sfałszowaniem) za pomocą weryfikacji sum kontrolnych
O31.1.F14	Rozwiązanie musi zapewniać możliwość optymalizacji wydajności poprzez wbudowaną funkcjonalność „cache’owania” operacji odczytu / zapisu (Read/Write IO) po stronie serwerów fizycznych
O31.1.F15	Rozwiązanie musi posiadać na ogólnodostępnej stronie producenta oprogramowania listę wspieranych i certyfikowanych konfiguracji serwerowych. Wymagane jest wsparcie dla min. 3 niezależnych producentów sprzętu serwerowego dostępnego na rynku Unii Europejskiej
O31.1.F16	Oprogramowanie do wirtualizacji podsystemu dyskowego (SDS) musi być wspierane przez producenta oferowanego rozwiązania do automatyzacji procesów (Automatyzacja), wirtualizacji serwerów (Hypervisor) oraz wirtualizacji sieci IP (SDN) na wszystkich poziomach wsparcia (L1-L3). Wsparcie musi odbywać się poprzez jednolity kanał serwisowy (jeden numer telefonów dla wszystkich zgłoszeń, jeden portal www pozwalający zarządzać licencjami i zgłaszać zlecenia serwisowe)
O31.1.F17	Rozwiązanie musi zapewniać możliwość zmniejszanie przestrzeni dyskowej (odjęcie pojedynczego dysku, odjęcie serwera/serwerów fizycznych) w sposób niewymagający przestoju i przerwy w dostępie do działających usług wirtualnych
O31.1.F18	System musi posiadać możliwość udostępniania swojej przestrzeni dyskowej również dla fizycznych systemów operacyjnych w oparciu o technologię iSCSI i umożliwiać zarządzanie dostępnością, pojemnością i wydajnością w locie
O31.1.F19	Rozwiązanie musi posiadać interfejs API umożliwiający automatyzowanie wdrażania/modyfikacji konfiguracji systemu
O31.1.F20	Rozwiązanie musi współdzielić zasób dyskowy dla platformy wirtualizacyjnej oraz musi umożliwiać wykorzystanie ww. przestrzeni dyskowej przez serwery fizyczne nieposiadające dysków wewnętrznych
O31.1.F21	Rozwiązanie musi mieć możliwość skonfigurowania deduplikacji i kompresji przy zapisie danych na dysk grupę pojemnościową (składowanie danych)
O31.1.F22	Rozwiązanie musi mieć możliwość konfiguracji domen niezawodnościowych. Oznacza to możliwość zgrupowania serwerów fizycznych w domenę, a następnie wymuszenie, aby dane po względem niezawodności posiadały swoją kopię na innej domenie, np. serwery znajdują się w kilku szafach rack, na bazie szafy rack tworzona jest domena niezawodnościowa
O31.1.F23	Rozwiązanie musi wspierać, co najmniej 12 węzłów w jednym logicznym klastrze
O31.1.F24	Rozwiązanie powinno wspierać mechanizmy optymalizacji wykorzystania przestrzeni dyskowych. Wymagane wsparcie dla min.: technologii deduplikacji oraz technologii implementującej mechanizmy znane z RAID5 i RAID6 za pomocą oprogramowania
O31.1.F25	Oferowane urządzenia/oprogramowanie ma pochodzić z bieżącej linii produkcyjnej, ma być produktem rozwijanym, w najnowszej stabilnej wersji i nie może być dla niego ogłoszone zakończenie produkcji, koniec sprzedaży, ani koniec wsparcia. Jeżeli oferowane rozwiązania posiadają nowszą wersję, następcę oprogramowania – należy zaoferować rozwiązanie najnowsze

O31.1.F26	Jeżeli do poprawnego działania dostarczanego modułu niezbędne jest wykorzystanie dodatkowych komponentów/licencji, nieujętych w szczegółowym opisie wymagań, to należy je przewidzieć i dodatkowo dostarczyć w ramach proponowanej oferty w ramach danego
-----------	---

7.8.3 Moduł wirtualizacji funkcji sieciowych

Identyfikator wymagania	Treść wymagania
O31.2.F1	Dostarczone oprogramowanie musi oferować możliwość budowy sieci komunikacyjnych (IP) oparcia o środowiska wirtualne.
O31.2.F2	Oferowane oprogramowanie musi zapewniać funkcjonalność tworzenia wirtualnych sieci w sposób niezależny od topologii sieci fizycznej i używanych w obrębie tej sieci w protokołów sieciowych.
O31.2.F3	Rozwiązanie musi posiadać funkcję rozproszonego, wirtualnego przełącznika instalowanego w jądrze wirtualizatora serwerów (Hypervisor), umożliwiającą tworzenie logicznych segmentów sieci L2. Wirtualny przełącznik musi być wspierany bezpośrednio przez producenta wirtualizatora serwerów.
O31.2.F4	Rozwiązanie musi posiadać funkcję rozproszonego, wirtualnego routera instalowanego w jądrze wirtualizatora serwerów (Hypervisor), zapewniającego funkcję bramy domyślnej dla środowiska maszyn wirtualnych. Brama domyślna musi działać w trybie rozproszonym. Przełączanie pakietów L3 musi odbywać się w obrębie fizycznego serwera, bez wynoszenia ruchu do fizycznych przełączników.
O31.2.F5	Rozwiązanie musi posiadać możliwość kreowania segmentów sieci przy użyciu technologii VXLAN.
O31.2.F6	Oferowane oprogramowanie musi zapewnić funkcjonalność łączenia (bridging) środowiska zvirtualizowanego opartego o technologię VXLAN oraz niezvirtualizowanego zdefiniowanego za pomocą technologii VLAN-ów.
O31.2.F7	Oferowane oprogramowanie musi zapewnić funkcjonalność wirtualnego routera wspierającego protokoły BGP.
O31.2.F8	Rozwiązanie musi posiadać funkcję łączenia/bridge segmentów sieci L2 VLAN i VXLAN poprzez zastosowanie wirtualnej bramy/bridge
O31.2.F9	Rozwiązanie musi umożliwiać funkcję translacji adresów IP zarówno dla ruchu wychodzącego ze środowiska wirtualnego (SNAT) jak i przychodzącego (DNAT)
O31.2.F10	Rozwiązanie musi posiadać funkcję serwera DHCP w celu dynamicznego nadawania adresów IP dla środowiska zvirtualizowanego
O31.2.F11	Oferowane oprogramowanie musi udostępniać funkcjonalność zarządzania poprzez ustandaryzowany interfejs tj. API
O31.2.F12	Oprogramowanie do wirtualizacji sieci (SDN) musi być wspierane przez producenta oferowanego rozwiązania do automatyzacji procesów (Automatyzacja) oraz wirtualizacji serwerów (Hypervisor) na wszystkich poziomach wsparcia (L1-L3). Wsparcie musi odbywać się poprzez

	jednorodny kanał serwisowy (jeden numer telefonów dla wszystkich zgłoszeń, jeden portal www pozwalający zarządzać licencjami i zgłaszać zlecenia serwisowe)
O31.2.F13	Aktualizacje oprogramowania powinny odbywać się poprzez zintegrowany portal służący do ich planowania i uruchamiania. Portal musi umożliwiać przegląd wszystkich elementów systemu pod kątem ich aktualnej oraz przygotowanej do aktualizacji wersji. Portal musi oferować wskaźniki postępu aktualizacji, umożliwiać tworzenie planów aktualizacji oraz zapewniać mechanizmy sprawdzenia konsystencji działania systemu przed oraz po aktualizacji
O31.2.F15	Oferowane oprogramowanie musi zapewnić bezpieczeństwo transmisji danych (filtracja pakietów) na poziomie hypervisor/wirtualnego interfejsu sieciowego, dla całości transmisji danych (włączając w to transmisję pomiędzy wirtualnymi maszynami w tym samym wirtualnym segmencie sieci) bez wynoszenia ruchu do fizycznych przełączników lub firewalli
O31.2.F16	Rozwiązania musi posiadać funkcję rozproszonego, stanowego firewall'a instalowanego w/na poziomie jądra wirtualizatora (Hypervisor) serwerów umożliwiający tworzenie polityk bezpieczeństwa w warstwach 2-4 modelu OSI. Nie dopuszcza się stosowania filtracji typu "reflexive".
O31.2.F17	Musi zostać zapewniona możliwość tworzenia reguł firewall'a w trybie stateless dla różnych grup wirtualnych maszyn.
O31.2.F18	Możliwość tworzenia granularnych polityk bezpieczeństwa na poziomie wirtualnego portu maszyny wirtualnej, włączając ruch pomiędzy wirtualnymi maszynami w ramach tego samego segmentu sieci i na tym samym fizycznym serwerze
O31.2.F19	Rozwiązanie musi umożliwiać wykorzystanie dynamicznych obiektów do tworzenia reguł polityk bezpieczeństwa: Wymagane min.: nazwa maszyny wirtualnej, nazwa switcha wirtualnego, nazwa grupy maszyn wirtualnych, system operacyjny wirtualnej maszyny
O31.2.F21	Rozwiązanie powinno oferować w ramach platformy, możliwość terminowania tuneli IPsec site-to-site z metodą autentykacja współdzielonego klucza (pre shared key) lub certyfikatu
O31.2.F22	Rozwiązanie powinno umożliwiać natywną integrację z produktami firm trzecich oferującymi rozwiązania typu antywirus/antymalware w postaci bez agentowej, tj. instalowane na wirtualizatorze serwerów, ale poza wirtualną maszyną
O31.2.F23	Rozwiązanie powinno umożliwiać natywną integrację z produktami firm trzecich oferującymi rozwiązania typu Next Generation Firewall warstwy 7, m.in. Integracja z systemem do zarządzania Next Generation Firewall
O31.2.F24	Rozwiązanie musi umożliwiać przekierowanie wybranego ruchu L2 do rozwiązania firm trzecich z obszaru bezpieczeństwa
O31.2.F25	Oferowane oprogramowanie musi zapewnić funkcjonalność rozkładania/równoważenia ruchu – tj. funkcja wirtualny Load Balancer musi być realizowana i w pełni zintegrowana z platformą do wirtualizacji sieci.

7.8.4 Moduł monitorowania i zarządzania pojemnością i efektywnością platformy

Podobszar / Proces	Identyfikator wymagania	Treść wymagania
-----------------------	----------------------------	-----------------

Wymagania ogólne	O31.3.01	<p>Rozwiązanie musi zapewniać centralną konsolę graficzną za pomocą, której będzie możliwość automatycznej instalacji i konfiguracją następujących modułów:</p> <ul style="list-style-type: none"> • Wirtualizacja mocy obliczeniowej • Wirtualizacji funkcji sieciowych • Wirtualizacji przestrzeni dyskowej • Zbierania zbieranie logów z infrastruktury • Monitorowania i zarządzania pojemnością i efektywnością platformy
	O31.3.02	Rozwiązanie musi zapewniać centralną konsolę graficzną za pomocą, której będzie możliwość automatycznego tworzenia, modyfikowania, usuwania i konfigurowania wirtualnych maszyn
	O31.3.03	Rozwiązanie musi zapewniać centralną konsolę graficzną za pomocą, której będzie możliwość wymiany uszkodzonego serwera fizycznego
	O31.3.04	Rozwiązanie musi zapewniać centralną konsolę graficzną za pomocą, której będzie możliwość dodania dodatkowego serwera fizycznego w celu zwiększenia pojemności
	O31.3.05	Rozwiązanie musi posiadać możliwość definiowania sieci wirtualnych, które łączą maszyny wirtualne w ramach zarządzanej platformy
	O31.3.06	Administrator rozwiązania musi posiadać możliwość definiowania sieci wewnętrznych jak i sieci zewnętrznych połączonych do sieci fizycznej - pozwalającej na komunikację np. do Internetu za pomocą np. NAT
	O31.3.07	Rozwiązanie niezależne od producenta sprzętu, możliwy provisioning wirtualizatora systemów operacyjnych na tzw. bare-metal ze wsparciem dla min. takich producentów jak: Dell, IBM, Huawei, Cisco etc..
	O31.3.08	Posiadanie wsparcia dla platform: KVM, Hyper-V (SCVMM), VMware
	O31.3.10	Rozwiązanie musi umożliwiać rezerwację zasobów fizycznych dla wybranych grup użytkowników oraz pełną kontrolę tych zasobów w obrębie wskazanej grupy użytkowników
	O31.3.11	Rozwiązanie musi mieć możliwość tworzenia wielu logicznych, izolowanych od siebie grup maszyn wirtualnych i określania dla nich zasobów fizycznych
	O31.3.12	Rozwiązanie musi się integrować z innymi systemami zewnętrznymi typu: CMDB, DNS, IPAM, Load Balancer, Service Desk, Monitoring, Web Services, Puppet, Chef, MS SCCM jako plug-iny lub napisanych od początku w języku programowania. Efektem powyższej integracji musi być w pełni automatyczny proces tworzenia i zarządzania usługą niewymagający czynności ręcznych
	O31.3.13	Rozwiązanie musi umożliwiać integrację z Active Directory oraz Open LDAP, i wieloma ich domenami w tym samym czasie

	O31.3.14	Rozwiązanie musi posiadać możliwość granularnego zarządzania uprawnieniami dla poszczególnych użytkowników w zależności od pełnionej roli, opartego na rolach: np.: Tenant Admin, Service Architect, Network Architect
	O31.3.15	Rozwiązanie musi dostarczać mechanizmy monitorowania statusów zdarzeń, notyfikacji o tych zdarzeniach, umożliwiać śledzenie i kontrolę zmian w konfiguracji wszystkich usług, za pomocą min. powiadomień e-mail
	O31.3.16	Oferowane oprogramowanie musi udostępniać funkcjonalność zarządzania poprzez ustandaryzowany interfejs tj. API
	O31.3.17	Rozwiązanie musi umożliwiać zunifikowane mechanizmy uaktualnienia całego stosu oprogramowania wirtualizującego oraz definiowania harmonogramu i zakresu tych aktualizacji
	O31.3.18	Rozwiązanie musi posiadać na oficjalnej stronie producenta listę wspieranych i certyfikowanych konfiguracji serwerowych. Wymagane jest wsparcie dla min. 3 niezależnych producentów sprzętu serwerowego x86 oraz co najmniej 2 różnych producentów przełączników DC dostępnego na rynku Unii Europejskiej
Wymagania szczegółowe	O31.3.F1	Platforma będzie w stanie zbierać informacji na temat wydajności pod kątem zarządzania pojemnością
	O31.3.F2	Platforma musi w sposób inteligentny przewidywać trendy związane z pojemnością środowiska
	O31.3.F3	Platforma musi posiadać moduł odpowiedzialny za analizę środowiska pod kątem optymalizacji wykorzystania zasobów (CPU, RAM, HDD)
	O31.3.F4	Platforma będzie w stanie tworzyć unikalne/dedykowane Data Center, tzw. Będzie możliwe grupowanie obiektów w logiczne zbiory, dla których będzie istniała możliwość informowania o alertach, pojemności, ryzykach zgromadzonych w zbiorze obiektach. Obiekty mogą pochodzić z różnych Data Center objętych tym rozwiązaniem.
	O31.3.F5	Platforma będzie w stanie tworzyć unikalne/dedykowane profile pojemności, tzn. będzie możliwe grupowanie obiektów w logiczne zbiory, dla których będzie istniała możliwość informowania o alertach, pojemności, ryzykach zgromadzonych w zbiorze obiektach
	O31.3.F6	Platforma będzie w stanie tworzyć scenariusze pojemnościowe na zasadzie, "co, jeśli", dla minimum, co, jeśli dodamy kolejne maszyny wirtualne, serwery fizyczne, pamięć masową. Rozwiązanie będzie umożliwiało definiowanie poziomów buforów potrzebnych do zachowania wysokiej dostępności. Analiza pojemności będzie odnosiła się zarówno do średniego obciążenia środowiska, jak również do tzw. skoków obciążenia
	O31.3.F9	Platforma będzie w stanie monitorować infrastrukturę SDS

	O31.3.F10	Platforma w obrębie monitorowania będzie posiadała rozwiązanie generowania alertów na podstawie szeregu anomalii i symptomów, a nie pojedynczych monitorowanych metryk
	O31.3.F11	Platforma będzie dostarczała informacji na temat rekomendowanych działań mających na celu utrzymanie środowiska wirtualnego sprawnego
	O31.3.F12	Platforma będzie w stanie dostarczać analizę głównego problemu (root-cause) oraz rekomendacji z nimi związane
	O31.3.F13	Platforma powinna posiadać wbudowane integracje z zewnętrznym kolektorem logów i zdarzeń
	O31.3.F16	System musi wizualizować online obciążenie środowiska wirtualnego wraz z tzw. funkcjonalnością „drill down”
	O31.3.F17	System musi posiadać funkcjonalność graficznej prezentacji wyników (dashboard)
	O31.3.F18	System musi posiadać funkcjonalność aktywnych map graficznych ukazujących elementy lub całe środowisko wirtualne bez konieczności korzystania z usługi wsparcia technicznego producenta do ich wytworzenia
	O31.3.F19	System powinien automatycznie tworzyć linie bazowe określające typowe zachowanie elementów systemu w danym czasie
	O31.3.F20	System będzie miał dostępne mechanizmy planowania pojemności środowiska, w zakresie nie mniejszym niż dodaniu określonej liczby maszyn wirtualnych
	O31.3.F21	System powinien dokonywać predykcji wykorzystania zasobów maszyn fizycznych na podstawie analiz zebranych danych, informacji pochodzących z modułu zarządzania cyklem życia maszyn wirtualnych oraz planów uruchomienia kolejnych serwerów wirtualnych
	O31.3.F22	System powinien dokonywać predykcji wykorzystania zasobów maszyn wirtualnych na podstawie analiz zebranych danych
	O31.3.F23	System powinien umożliwiać przeglądanie linii trendu monitorowanych parametrów
	O31.3.F24	System musi umożliwiać tworzenie raportów pojemnościowych dla monitorowanego środowiska, zarówno dla urządzeń fizycznych jak i wirtualnych
	O31.3.F25	System musi umożliwiać monitorowanie w czasie rzeczywistym (przeglądane informacje w trybie rzeczywistym - maksymalne dopuszczalne opóźnienie nie większe niż 5 min.)
	O31.3.F26	System musi zbierać oraz prezentować w formie wykresów oraz tabelaryczno-tekstowej zbiorczo oraz osobno dla każdego OS aktualne i historyczne dane dotyczące utylizacji CPU, RAM, HDD oraz interfejsów sieciowych

	O31.3.F27	System musi umożliwiać przeglądanie wszystkich zbieranych statystyk w dowolnie wybranym zakresie czasu w postaci wykresów
	O31.3.F28	System powinien umożliwiać szczegółowe monitorowanie komponentów serwerów fizycznych (CPU, Ethernet, RAM, HDD)
	O31.3.F29	System musi wskazywać „wąskie gardła” a także umożliwiać definiowanie progów wydajności i pojemności w celu identyfikacji przypadków wąskich gardeł
	O31.3.F30	Możliwość uruchamiania ręcznego automatycznych zadań (w tym modyfikujących parametry maszyn wirtualnych) w zależności od aktualnych alarmów, ostrzeżeń, powiadomień, obciążenia
	O31.3.F31	Oprogramowanie musi automatycznie przeszukiwać składy danych w celu wynajdywania: nadmiarowo przyznanego zasobów (CPU, RAM, HDD)
	O31.3.F32	Alarmowanie sytuacji nietypowych (system monitoringu obserwuje i analizuje zachowanie platformy wirtualnej, na tej podstawie podnosi alarmy o np. nie normalnym w tym dniu zwiększonym obciążeniu elementu platformy wirtualnej)
	O31.3.F33	Możliwość dowolnego konfigurowania alertów w środowisku dla różnych grup odbiorców (także z użyciem alertów stworzonych we własnym zakresie),
	O31.3.F34	System powinien pozwalać na odczyt wyświetlanych alarmów w środowisku wirtualnym
	O31.3.F35	System umożliwia definiowanie alertów związanych z: zarządzaniem pojemnością; zarządzaniem wydajnością; anomaliami w środowisku; zarządzanie dostępnością
	O31.3.F36	Narzędzie musi mieć możliwość przypisania alertu do administratora/operatora rozwiązującego problem
	O31.3.F37	Rozwiązanie musi mieć możliwość realizacji funkcji automatycznego lub półautomatycznego równoważenia obciążenia serwerów fizycznych w obrębie klastra logicznego, jak również pomiędzy logicznymi klastrami
	O31.3.F38	Rozwiązanie musi mieć możliwość automatycznego i/lub półautomatycznego z konsoli do zarządzania, zmiany parametrów maszyny wirtualnej w zakresie ilości (vCPU, vRAM, usunięcie snapshota, wyłączenie/włączenie maszyn wirtualnej) na podstawie rekomendacji zmian otrzymywanych przy generowaniu alertu z systemu
	O31.3.F39	Rozwiązanie musi integrować się z częścią wirtualizującą zarówno w warstwie przetwarzania (Hypervisor) jak i sieci (SDN)
	O31.3.F40	Rozwiązanie musi posiadać możliwość zastosowania dodatkowych adapterów umożliwiających integrację w systemami monitorującymi infrastrukturę firm trzecich
	O31.3.F41	Rozwiązanie musi posiadać możliwość zastosowania dodatkowych paczek monitorujących dla rozwiązań firm trzecich

	O31.3.F42	Rozwiązanie musi umożliwiać konfigurację trybu wysokiej dostępności HA dla każdego swojego komponentu w celu unikania awarii pojedynczego elementu
	O31.3.F43	Rozwiązanie musi posiadać możliwość zastosowania dodatkowych adapterów odpowiadających za monitorowanie systemów zewnętrznych takie jak: macierze dyskowe, chmury obliczeniowe, serwery fizyczne, przełączniki LAN/SAN i inne, umożliwiając tym samym wykorzystanie dedykowanych mechanizmów monitorujących określone komponenty
	O31.3.F44	Rozwiązanie musi umożliwiać elastyczne dostosowanie wyglądu interfejsu użytkownika w zależności od indywidualnych potrzeb konkretnego użytkownika
	O31.3.F45	Rozwiązanie musi posiadać funkcję tzw. konfiguratora własnych raportów, który musi umożliwiać tworzenie zaawansowanych raportów dotyczących wszystkich aspektów funkcjonowania platformy sprzętowo-programowej
	O31.3.F46	Rozwiązanie musi posiadać funkcję tzw. konfiguratora własnych widoków zgromadzonych danych, który musi umożliwiać tworzenie zaawansowanych widoków dotyczących wszystkich monitorowanych metryk
	O31.3.F47	Rozwiązanie musi posiadać funkcję tzw. konfiguratora własnych pulpitów kierowniczych (tzw. dashboard) na podstawie zgromadzonych danych w rozwiązaniu. Za pomocą tej funkcjonalności rozwiązanie musi umożliwiać tworzenie zaawansowanych pulpitów kierowniczych (dashborad)
Moduł monitoringu środowiska sieciowego	O31.4.F1	Rozwiązanie musi mieć możliwość analizowania przepływów sieciowych (w tym IPFIX) w warstwie sieciowej wirtualizacji
	O31.4.F2	Rozwiązanie musi mieć możliwość tworzenia raportów przepływów z informacją uwzględniającą adresy IP oraz porty TCP/UDP dla środowiska wirtualnego oraz fizycznego
	O31.4.F3	Rozwiązanie musi mieć możliwość wykorzystania wbudowanego kolektora w celach dalszej analizy ruchu
	O31.4.F4	Rozwiązanie musi mieć możliwość posiadać automatyczne rekomendacje reguł firewalla na bazie zebranych informacji o przepływach
	O31.4.F5	Rozwiązanie musi mieć możliwość wizualizacji ścieżki logicznej i przejść w relacji vm-vm, wskazanie komponentów sieciowych w topologii logicznej i fizycznej - przełączników, routerów, firewalli oraz połączeń między nimi z uwzględnieniem komponentów wirtualnych
	O31.4.F6	Rozwiązanie musi mieć możliwość wizualizacji przepływów pomiędzy maszynami wirtualnymi i/lub środowiskiem fizycznym pogrupowanych ze względu na sieci wirtualne, podsieci, aplikacje, grupy bezpieczeństwa
	O31.4.F7	Rozwiązanie musi mieć możliwość informowania o tym, jakie reguły firewalla wirtualnego są aktualnie zaaplikowane i aktywne

	O31.4.F8	Rozwiązanie musi mieć możliwość informowania o maskowanych regułach firewalla, czyli regułach, które nie są wykorzystywane ze względu na reguły położone wyżej
	O31.4.F9	Rozwiązanie musi mieć możliwość informowania i wizualizacji połączeń maszyn wirtualnych do zasobów dyskowych, połączenia do hosta (wirtualizatora) i wyjścia na zewnątrz do sieci fizycznej
	O31.4.F10	Rozwiązanie musi posiadać funkcjonalność API
	O31.3.F48	Rozwiązanie musi posiadać funkcjonalność monitorowania systemów operacyjnych (np. Windows, Linux) za pomocą zainstalowanego agenta w monitorowanym systemie operacyjnym

7.8.5 Moduł zarządzania cyklem życia platformy

Konsola do automatycznej instalacji i/lub konfiguracji oprogramowania do wirtualizacji serwerów fizycznych, macierzy dyskowej typu SDS na serwerach, wirtualizacji sieci typu SDN wraz z mechanizmami bezpieczeństwa. Dodatkowo rozwiązanie musi być w stanie aktualizować wszystkie powyższe komponenty oprogramowania. Oprogramowanie musi spełniać poniższe warunki:

Identyfikator wymagania	Treść wymagania
O31.5.F1	Rozwiązanie musi posiadać narzędzia skracające proces wdrażania stosu oprogramowania infrastrukturalnego do wirtualizacji serwerów x86, wirtualizacji sieci oraz tworzenia macierzy dyskowej typu SDS poprzez zautomatyzowaną instalację oprogramowania, tworzenie klastrów obliczeniowych (w tym na potrzeby klastrów obliczeniowych pod serwery wirtualne), zarządzania i wdrażanie maszyn wirtualnych infrastruktury
O31.5.F2	Rozwiązanie opcjonalnie musi mieć możliwość automatycznej instalacji, uaktualniania automatycznego platformy do konsolidacji i zaawansowanej diagnostyki logów
O31.5.F3	Rozwiązanie musi posiadać narzędzia automatyzujące konfigurację następujących elementów: serwerów x86, fizycznej sieci w tym VLAN, przestrzeni dyskowej, itp.
O31.5.F4	Rozwiązanie musi umożliwiać zunifikowane mechanizmy uaktualnienia całego stosu oprogramowania wirtualizującego oraz definiowania harmonogramu i zakresu tych aktualizacji
O31.5.F5	Rozwiązanie musi posiadać na oficjalnej stronie producenta listę wspieranych i certyfikowanych konfiguracji serwerowych. Wymagane jest wsparcie dla min. 3 niezależnych producentów sprzętu serwerowego x86 oraz co najmniej 2 różnych producentów przełączników DC dostępnego na rynku Unii Europejskiej

7.8.6 Moduł zbierania zbieranie logów z infrastruktury

Identyfikator wymagania	Treść wymagania
O31.6.F1	Rozwiązanie musi zapewniać możliwość centralnego gromadzenia i analizy wszystkich logów z urządzeń fizycznych wykorzystujących technologię 'Syslog'

O31.6.F2	Rozwiązanie musi integrować się z oprogramowaniem do monitorowania i zarządzania platformą wirtualizacyjną w ten sposób, że z poziomu konsoli użytkownika oprogramowania do monitorowania i zarządzania platformą wirtualizacyjną musi istnieć możliwość uzyskania natychmiastowego dostępu do logów konkretnego urządzenia fizycznego
O31.6.F3	Rozwiązanie musi umożliwiać personalizację i wizualizację logów w postaci wykresów liniowych, kołowych, słupkowych itp.
O31.6.F4	Rozwiązanie musi zapewniać monitorowanie urządzeń typu „Real Time”
O31.6.F5	Rozwiązanie musi posiadać wbudowaną bazę wiedzy dotyczącą logów, zdarzeń itp. platformy wirtualizacyjnej
O31.6.F6	Rozwiązanie musi umożliwiać łatwą korelację wybranych zdarzeń w infrastrukturze fizycznej/wirtualnej oraz ich graficzną prezentację
O31.6.F7	Musi istnieć możliwość personalizacji interfejsu graficznego w zależności od użytkownika/operatora
O31.6.F8	Rozwiązanie musi umożliwiać łatwe i szybkie przeszukiwanie logów w oparciu o zdefiniowane przez użytkownika kryteria
O31.6.F9	Musi istnieć możliwość implementacji dedykowanych modułów do analizy logów innych urządzeń fizycznych np. macierzy dyskowych, przełączników LAN, itp., tak, aby analiza i korelacja wszystkich wiadomości systemowych mogła odbywać się z jednej konsoli zarządzającej
O31.6.F10	Rozwiązanie musi posiadać mechanizmy efektywnej analizy wszystkich rodzajów logów, takich jak np. logi aplikacji, logi sieciowe, pliki konfiguracyjne, informacje, dane wydajnościowe, zrzuty awaryjne itp., a także logów 'nieustrukturyzowanych”
O31.6.F11	Rozwiązanie musi umożliwiać zdefiniowanie struktury dla logów nieustrukturyzowanych
O31.6.F12	Uprawnienia do interfejsu prezentacji i analizy logów muszą dopuszczać rozłączność z uprawnieniami do infrastruktury
O31.6.F13	Rozwiązanie musi umożliwiać generowanie i eksportowanie dowolnych raportów związanych z zarejestrowanymi zdarzeniami i logami

7.9. Opis infrastruktury wirtualizacyjnej

7.9.1 Infrastruktura dla środowiska produkcyjnego

Identyfikator wymagania	Treść wymagania
O32.F1	<p>Środowisko produkcyjne w centralnych ośrodkach przetwarzania danych poza infrastrukturą przeznaczona na systemy OSS/BSS, systemy backup i systemy odtwarzania po awarii (Disaster Recovery) powinno dodatkowo sumarycznie posiadać:</p> <ul style="list-style-type: none"> • min. 1200 vCPU (vCPU = Ilość fizyczna procesorów x Ilość rdzeni fizycznych w procesorze (bez HT)) • min. 7000 GB RAM

	<ul style="list-style-type: none"> • min. 400 TB przestrzeni użytkowej pamięci blokowej (SDS) na platformie All Flash (przed deduplikacją i kompresją). • min. 600 TB przestrzeni użytkowej pamięci obiektowej (po uwzględnieniu Erasure Coding) zainstalowanej w trzech ośrodkach, system odporny na awarie jednego ośrodka.
O32.F2	Cała infrastruktura obliczeniowa w centralnym ośrodku przetwarzania danych nie powinna zajmować więcej przestrzeni w szafach rackowych niż 138 U, jak również nie może zużywać więcej mocy niż 88kW. Wymogi te dotyczą dwóch centralnych ośrodków przetwarzania danych i każdy z nich może pomieścić nie więcej niż 138 U i nie może zużyć mocy większej niż 88kW.
O32.F3	Cała infrastruktura obliczeniowa w trzecim centralnym ośrodku przetwarzania danych nie powinna zajmować więcej przestrzeni w szafach rackowych niż 30 U, jak również nie może zużywać więcej mocy niż 9kW.
O32.F4	<p>Każdy regionalny ośrodek przetwarzania danych powinien składać się z min. dwóch serwerów wraz z dyskami tworząc klastr wysokiej dostępności HA w obszarze przetwarzania (CPU) jak i pamięci masowej (SDS). Środowisko produkcyjne w szesnastu regionalnych ośrodkach przetwarzania danych powinno sumarycznie posiadać:</p> <ul style="list-style-type: none"> • min. 520 vCPU (bez HT) • min. 2200 GB RAM • min. 96 TB przestrzeni użytkowej pamięci blokowej (SDS).
O32.F5	Cała infrastruktura obliczeniowa w każdym z regionalnych ośrodków przetwarzania danych nie powinna zajmować więcej przestrzeni w szafach rackowych niż 6 U, jak również nie może zużywać więcej mocy niż 4,5 kW.

7.9.2 Wymagania ilościowe warstwy oprogramowania

Identyfikator wymagania	Treść wymagania
O32.F6	<p>Licencje dla centralnych ośrodków przetwarzania danych.</p> <p>Wymagane jest dostarczenie licencji zintegrowanej platformy wirtualizacyjnej pozwalającej na jej instalację na wszystkich dostarczonych serwerach i dla wszystkich maszyn wirtualnych działających na platformie dla centralnych ośrodków przetwarzania danych.</p> <p>Moduły, które muszą być dostarczone w ramach zintegrowanej platformy dla centralnych ośrodków przetwarzania danych:</p>

	<ul style="list-style-type: none"> • Moduł wirtualizacji mocy obliczeniowej • Moduł wirtualizacji przestrzeni dyskowej • Moduł wirtualizacji funkcji sieciowych • Moduł zbierania zbieranie logów z infrastruktury IT wraz z jej analizą • Moduł monitorowania i zarządzania pojemnością i efektywnością platformy <p>Moduł zarządzania cyklem życia platformy w warstwie sprzętowej</p>
O32.F7	<p>Licencje dla regionalnych ośrodków przetwarzania danych.</p> <p>Wymagane jest dostarczenie licencji zintegrowanej platformy wirtualizacyjnej pozwalającej na jej instalację na min. 64 CPU lub wszystkich maszyn wirtualnych działających na platformie dla regionalnych ośrodków przetwarzania danych.</p> <p>Wymagane jest dostarczenie oprogramowania tego samego producenta zintegrowanej platformy wirtualizacyjnej dla regionalnych ośrodków przetwarzania danych jak w centralnych ośrodkach przetwarzania danych.</p> <p>Moduły, które muszą być dostarczone w ramach zintegrowanej platformy dla regionalnych ośrodków przetwarzania danych:</p> <ul style="list-style-type: none"> • Moduł wirtualizacji mocy obliczeniowej • Moduł wirtualizacji przestrzeni dyskowej <p>Moduł monitorowania i zarządzania pojemnością i efektywnością platformy</p>

7.9.3 Wymagania ogólne dla warstwy sprzętowej dla serwerów w węzłach centralnych

Dostawca powinien zapewnić serwery spełniające poniższe wymagania. Ilość serwerów powinna składać się z oszacowanych przez dostawcę ilości serwerów potrzebnych do zapewnienia zasobów na systemy OSS i systemy BSS i dodatkowe serwery, których zasoby są określone w p. 7.9.1 (części opisującej centralne ośrodki przetwarzania danych). Wszystkie serwery te muszą być dostarczone w takiej samej konfiguracji. Dodatkowe serwery zapewnią zasoby pod inne systemy instalowane na platformie wirtualizacyjnej wraz z nadmiarowymi serwerami i zasobami pod środowisko testowe. W szczególnych przypadkach dopuszcza się dostarczenie innych serwerów niż wyspecyfikowane poniżej, ale całkowita ilość tych serwerów nie powinna stanowić więcej niż połowa zasobów przeznaczonych na systemy OSS/BSS.

Identyfikator wymagania		Treść wymagania
O32.3.F1	Obudowa	Obudowa Rack o wysokości max 2U z możliwością instalacji do 24 dysków 2.5" Hot-Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.

O32.3.F2	Płyta główna	Płyta główna z możliwością zainstalowania minimum dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
O32.3.F3	Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocessorowych
O32.3.F4	Procesor	Zainstalowane dwa procesory dwudziestordzeniowe klasy x86 umożliwiające przez oferowany model serwera osiągnięcie wyniku min. 105 punktów w teście SPEC CPU2017 Floating Point Speed w układzie dwuprocessorowym. Wynik dla oferowanego modelu serwera musi być dostępny na stronie www.spec.org .
O32.3.F5	RAM	Minimum 384GB min. 2666MT/s RDIMM DDR4 z możliwością rozbudowy do minimum 1024GB. Płyta główna wyposażona w min. 24 sloty na pamięć RAM i co najwyżej połowa slotów może być zajęta.
		Oferowany serwer musi oferować następujące zabezpieczenia pamięci RAM: ECC, Memory Mirroring, Memory demand and patrol scrubbing, Memory Rank Sparing, SDDC (lub Fast Fault Tolerance)
O32.3.F6	Diagnostyka	Panel LCD lub LED umieszczony na froncie serwera, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze lub za pomocą dedykowanego oprogramowania do zarządzania infrastrukturą serwerową.
O32.3.F7	Gniazda PCI	- minimum 8 slotów PCI Express (w tym min. 2 sloty PCI Express x16 generacji 3). Wszystkie sloty muszą być uniwersalne (umożliwiające instalowanie między innymi kart Ethernet).
O32.3.F8	Interfejsy sieciowe/FC/SAS	Wbudowane 2 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 nie zajmujących uniwersalnych slotów PCI.
		Przynajmniej dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT;
		Dodatkowa karta dwuportowa 25Gb Ethernet w standardzie SFP28.
O32.3.F9	Dyski twarde	Możliwość instalacji dysków SATA, SAS, SSD, NVMe.
		Zainstalowane 2 karty SD lub 2 dyski M.2 lub 2 dyski SSD, każdy o pojemności min 16GB, skonfigurowane w RAID 1, przeznaczone do instalacji systemu wirtualizacyjnego.
O32.3.F9a	Dysk SSD pod cache	min. 800GB Hot Swap NVMe Dyski muszą być w stanie zapisać minimalnie 7300 TBW jak również być w stanie dokonać ponad 30000 zapisów na sekundę. Dysk musi być wspierany przez producenta rozwiązania SDS w kategorii dysków przeznaczonych pod zastosowania Cache.
O32.3.F9b	Dysk SSD pod capacity	min. 1.92TB Hot Swap Dyski muszą być w stanie zapisać minimalnie 2000 TBW jak również być w stanie dokonać ponad 15000 zapisów na sekundę. Dysk musi być wspierany

		przez producenta rozwiązania SDS w kategorii dysków przeznaczonych pod zastosowania Capacity.
O32.3.F10	Kontroler RAID	Kontroler RAID obsługujący passthrough lub HBA
O32.3.F11	Ogólne	<p>Oferowane urządzenia/oprogramowanie ma pochodzić z bieżącej linii produkcyjnej, ma być produktem rozwijanym, w najnowszej stabilnej wersji i nie może być dla niego ogłoszone zakończenie produkcji, koniec sprzedaży, ani koniec wsparcia. Jeżeli oferowane rozwiązania posiadają nowszą wersję, następcę oprogramowania – należy zaoferować rozwiązanie najnowsze.</p> <p>Jeżeli do poprawnego działania dostarczanych urządzeń niezbędne jest wykorzystanie dodatkowych komponentów/licencji, nieuwjętych w szczegółowym opisie wymagań, to należy je przewidzieć i dodatkowo dostarczyć w ramach proponowanej oferty w ramach danego</p>
O32.3.F12	Wbudowane porty	min. 3 porty USB z przodu obudowy (w tym jeden umożliwiający bezpośredni dostęp do karty zarządzającej) oraz min. 2 porty USB 3.0 z tyłu obudowy, 2 porty VGA lub 1 port VGA i jeden Display Port, min. 1 port RS232 (DB9), w/w porty nie mogą być uzyskane za pomocą przejściówek
O32.3.F13	Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
O32.3.F14	Wentylatory	Redundantne
O32.3.F15	Zasilacze	Redundantne, Hot-Plug min. 500W każdy o sprawności min. 94%.
O32.3.F16	Karta Zarządzania	<p>Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiające:</p> <ul style="list-style-type: none"> · zdalny dostęp do graficznego interfejsu Web karty zarządzającej · zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera) · szyfrowane połączenie (SSLv3 lub TLS) oraz autentykację i autoryzację użytkownika · możliwość podmontowania zdalnych wirtualnych napędów · wirtualną konsolę z dostępem do myszy, klawiatury · wsparcie dla IPv6 · wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH · integracja z Active Directory · możliwość obsługi przez dwóch administratorów jednocześnie · wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej

		· możliwość podłączenia lokalnego poprzez złącze RS-232 (DB9).
		· możliwość zarządzania bezpośredniego poprzez złącze USB
		· Karta zdalnego zarządzania musi posiadać wbudowaną pamięć flash, min. 8GB lub możliwość dostępu do zewnętrznej pamięci USB/FLASH 8GB
		Dodatkowe oprogramowanie umożliwiające zarządzanie poprzez sieć, spełniające minimalne wymagania:
		· Wsparcie dla serwerów
		· Wsparcie dla protokołów– WMI, SNMP, IPMI, Linux SSH
		· Możliwość eksportu raportu do CSV, HTML
		· Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach
		· Generowanie alertów przy zmianie stanu urządzenia
		· Możliwość przejęcia zdalnego pulpitu
		· Automatyczne zaplanowanie akcji dla poszczególnych alertów w tym automatyczne tworzenie zgłoszeń serwisowych w oparciu o standardy przyjęte przez producentów oferowanego w tym postępowaniu sprzętu
		· Przesyłanie alertów „as-is” do innych konsol firm trzecich
		· Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)
		· Możliwość automatycznego przywracania ustawień serwera, kart sieciowych, BIOS, wersji firmware w przypadku awarii i wymiany któregoś z komponentów (w tym kontrolera RAID, kart sieciowych, płyty głównej).
O32.3.F17	Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001.
		Serwer musi posiadać deklaracja CE.
		Microsoft Windows Server min. w wersji 2016x64 – zgodność potwierdzona dla oferowanego modelu serwera na stronie https://www.windowsservercatalog.com/
		Vmware ESXi 6.7, ESXi 6.5, vSAN – zgodność potwierdzona dla oferowanego modelu serwera na stronie https://www.vmware.com/resources/compatibility/search.php
		Red Hat Enterprise Linux 7.6 (RHEL) – zgodność potwierdzona dla oferowanego modelu serwera na stronie https://access.redhat.com/ecosystem/search/#/ecosystem
O32.3.F18	Warunki gwarancji	Dostarczony sprzęt powinien być nowy, nieużywany dotąd w innych projektach. Zamawiający dopuszcza rozpakowanie sprzętu w celu weryfikacji jego skompletowania i braku usterek.

		Na etapie odbioru sprzętu Zamawiający będzie wymagał dostarczenia dokumentów potwierdzających datę produkcji sprzętu (oświadczenie producenta lub inne dokumenty)
		Czas trwania gwarancji będzie liczony od daty podpisania protokołu odbioru sprzętu i oprogramowania, przy czym odbiór ten nastąpi po uruchomieniu i konfiguracji urządzeń w lokalizacjach wskazanych przez Zamawiającego
		Gwarancja będzie realizowana w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia. Wykonawca zapewni możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta
		W przypadku awarii dysków dyski twarde pozostają własnością Zamawiającego
		Oświadczenie producenta serwera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem
O32.3.F19	Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
		Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

7.9.4 Wymagania ogólne dla warstwy sprzętowej dla serwerów w regionach

Identyfikator wymagania		Treść wymagania
O32.4.F1	Obudowa	Obudowa Rack o wysokości max 2U z możliwością instalacji do 24 dysków 2.5" Hot-Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.
O32.4.F2	Płyta główna	Płyta główna z możliwością zainstalowania minimum dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
O32.4.F3	Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
O32.4.F4	Procesor	Zainstalowane dwa procesory dwudziestordzeniowe klasy x86 umożliwiające przez oferowany model serwera osiągnięcie wyniku min. 75 punktów w teście SPEC CPU2017 Floating Point Speed w układzie dwuprocesorowym. Wynik dla oferowanego modelu serwera musi być dostępny na stronie www.spec.org .
O32.4.F5	RAM	Minimum 256GB min. 2666MT/s RDIMM DDR4 z możliwością rozbudowy do minimum 1024GB. Płyta główna wyposażona w min. 24 sloty na pamięć RAM i co najwyżej połowa slotów może być zajęta.

		Oferowany serwer musi oferować następujące zabezpieczenia pamięci RAM: ECC, Memory Mirroring, Memory demand and patrol scrubbing, Memory Rank Sparing, SDDC (lub Fast Fault Tolerance)
O32.4.F6	Diagnostyka	Panel LCD lub LED umieszczony na froncie serwera, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze lub za pomocą dedykowanego oprogramowania do zarządzania infrastrukturą serwerową.
O32.4.F7	Gniazda PCI	- minimum 8 slotów PCI Express (w tym min. 2 sloty PCI Express x16 generacji 3). Wszystkie sloty muszą być uniwersalne (umożliwiające instalowanie między innymi kart Ethernet).
O32.4.F8	Interfejsy sieciowe/FC/SAS	Wbudowane 2 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 niezajmujących uniwersalnych slotów PCI.
		Przynajmniej dwa interfejsy sieciowe 1Gb Ethernet w standardzie BaseT;
		Dodatkowa karta dwuportowa 25Gb Ethernet w standardzie SFP28.
O32.4.F9	Dyski twarde	Możliwość instalacji dysków SATA, SAS, SSD, NVMe.
		Zainstalowane 2 karty SD lub 2 dyski M.2 lub 2 dyski SSD, każdy o pojemności min 16GB, skonfigurowane w RAID 1, przeznaczone do instalacji sytemu wirtualizacyjnego.
O32.4.F9a	Dysk SSD pod cache	min. 400GB Hot Swap NVMe Dyski muszą być w stanie zapisać minimalnie 4000 TBW jak również być w stanie dokonać ponad 12000 zapisów na sekundę. Dysk musi być wspierany przez producenta rozwiązania SDS w kategorii dysków przeznaczonych pod zastosowania Cache.
O32.4.F9b	Dysk SSD pod capacity	min. 1.92TB Hot Swap Dyski muszą być w stanie zapisać minimalnie 1000 TBW jak również być w stanie dokonać ponad 12000 zapisów na sekundę. Dysk musi być wspierany przez producenta rozwiązania SDS w kategorii dysków przeznaczonych pod zastosowania Capacity.
O32.4.F10	Kontroler RAID	Kontroler RAID obsługujący passthrough lub HBA
O32.4.F11	Ogólne	Oferowane urządzenia/oprogramowanie ma pochodzić z bieżącej linii produkcyjnej, ma być produktem rozwijanym, w najnowszej stabilnej wersji i nie może być dla niego ogłoszone zakończenie produkcji, koniec sprzedaży, ani koniec wsparcia. Jeżeli oferowane rozwiązania posiadają nowszą wersję, następcę oprogramowania – należy zaoferować rozwiązanie najnowsze. Jeżeli do poprawnego działania dostarczanych urządzeń niezbędne jest wykorzystanie dodatkowych komponentów/licencji, nieuwjętych w szczegółowym opisie

		wymagań, to należy je przewidzieć i dodatkowo dostarczyć w ramach proponowanej oferty w ramach danego
O32.4.F12	Wbudowane porty	min. 3 porty USB z przodu obudowy (w tym jeden umożliwiający bezpośredni dostęp do karty zarządzającej) oraz min. 2 porty USB 3.0 z tyłu obudowy, 2 porty VGA lub 1 port VGA i jeden Display Port, min. 1 port RS232 (DB9), w/w porty nie mogą być uzyskane za pomocą przejściówek
O32.4.F13	Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
O32.4.F14	Wentylatory	Redundantne
O32.4.F15	Zasilacze	Redundantne, Hot-Plug min. 500W każdy o sprawności min. 94%.
O32.4.F16	Karta Zarządzania	<p>Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiające:</p> <ul style="list-style-type: none"> · zdalny dostęp do graficznego interfejsu Web karty zarządzającej · zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera) · szyfrowane połączenie (SSLv3 lub TLS) oraz autentykację i autoryzację użytkownika · możliwość podmontowania zdalnych wirtualnych napędów · wirtualną konsolę z dostępem do myszy, klawiatury · wsparcie dla IPv6 · wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH · integracja z Active Directory · możliwość obsługi przez dwóch administratorów jednocześnie · wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej · możliwość podłączenia lokalnego poprzez złącze RS-232 (DB9). · możliwość zarządzania bezpośredniego poprzez złącze USB · Karta zdalnego zarządzania musi posiadać wbudowaną pamięć flash, min. 8GB lub możliwość dostępu do zewnętrznej pamięci USB/FLASH 8GB <p>Dodatkowe oprogramowanie umożliwiające zarządzanie poprzez sieć, spełniające minimalne wymagania:</p> <ul style="list-style-type: none"> · Wsparcie dla serwerów · Wsparcie dla protokołów– WMI, SNMP, IPMI, Linux SSH · Możliwość eksportu raportu do CSV, HTML

		<ul style="list-style-type: none"> · Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach · Generowanie alertów przy zmianie stanu urządzenia · Możliwość przejęcia zdalnego pulpitu · Automatyczne zaplanowanie akcji dla poszczególnych alertów w tym automatyczne tworzenie zgłoszeń serwisowych w oparciu o standardy przyjęte przez producentów oferowanego w tym postępowaniu sprzętu · Przesyłanie alertów „as-is” do innych konsol firm trzecich · Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) · Możliwość automatycznego przywracania ustawień serwera, kart sieciowych, BIOS, wersji firmware w przypadku awarii i wymiany któregoś z komponentów (w tym kontrolera RAID, kart sieciowych, płyty głównej).
O32.4.F17	Certyfikaty	<p>Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001.</p> <p>Serwer musi posiadać deklaracja CE.</p> <p>Microsoft Windows Server min. w wersji 2016x64 – zgodność potwierdzona dla oferowanego modelu serwera na stronie</p> <p>Vmware ESXi 6.7, ESXi 6.5, vSAN – zgodność potwierdzona dla oferowanego modelu serwera na stronie</p> <p>Red Hat Enterprise Linux 7.6 (RHEL) – zgodność potwierdzona dla oferowanego modelu serwera na stronie</p>
O32.4.F18	Warunki gwarancji	<p>Dostarczony sprzęt powinien być nowy, nieużywany dotąd w innych projektach. Zamawiający dopuszcza rozpakowanie sprzętu w celu weryfikacji jego skompletowania i braku usterek.</p> <p>Na etapie odbioru sprzętu Zamawiający będzie wymagał dostarczenia dokumentów potwierdzających datę produkcji sprzętu (oświadczenie producenta lub inne dokumenty)</p> <p>Czas trwania gwarancji będzie liczony od daty podpisania protokołu odbioru sprzętu i oprogramowania, przy czym odbiór ten nastąpi po uruchomieniu i konfiguracji urządzeń w lokalizacjach wskazanych przez Zamawiającego</p> <p>Gwarancja będzie realizowana w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia. Wykonawca zapewni możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta</p> <p>W przypadku awarii dysków dyski twarde pozostają własnością Zamawiającego</p>

		Oświadczenie producenta serwera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem
O32.4.F19	Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
		Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

7.10. Obiektowy system składowania danych

Przedmiotem zamówienia jest rozwiązanie dyskowe składające się z trzech identycznych systemów obiektowych, rozmieszczonych w trzech różnych lokalizacjach połączonych łączami Ethernet. Pojemność, musi zostać uzyskana w oparciu o dyski o pojemności minimum 4TB.

System w warstwie sprzętowej oraz programowej, poza przełącznikami sieciowymi musi pochodzić od jednego producenta (musi być kompletnym produktem opatrzonym numerem seryjnym). Dopuszcza się rozwiązania, w których węzły zarządzające oraz węzły dostępne instalowane są na zewnętrznej platformie wirtualnej VMware, Hyper-V lub KVM.

System musi być odporny na utratę dowolnej macierzy obiektowej (węzła składującego dane) będącej składową systemu, co oznacza, że awaria taka nie może skutkować utratą danych ani niedostępnością systemu. W przypadku utraty jednej macierzy dyskowej wszystkie składowane dotychczas dane muszą być dostępne w takim samym stopniu jak przed utratą macierzy obiektowej.

System musi posiadać centralny interfejs zarządzający całym systemem, lokalnymi użytkownikami i przyznawanie uprawnień dostępu dla różnych ról.

Podobszar / Proces	Identyfikator wymagania	Treść wymagania
Ogólne wymagania techniczne dla obiektowego systemu składowania danych.	O33.1.F1	Przedmiotem zapytania jest dostawa, instalacja i konfiguracja obiektowego systemu składowania danych
	O33.1.F2	Wymagana pojemność nie uwzględnia wykorzystania mechanizmów redukcji danych (przed procesem de-duplikacji i kompresji)
	O33.1.F3	Wymagana pojemność musi być dostarczona i zainstalowana w trzech ośrodkach przetwarzania danych.
	O33.1.F4	Należy zapewnić mechanizm asynchronicznej replikacji obiektów pomiędzy ośrodkami za pomocą istniejących łącz Ethernet.
	O33.1.F5	Dostarczane rozwiązanie musi być produktem rozpoznawalnym na rynku, co oznacza, że powinno być wymieniane w raportach niezależnych organizacji, takich jak Gartner, IDC, Gigaom lub ESG (Enterprise Strategy Group).

	O33.1.F6	Dostarczane rozwiązanie (oprogramowanie zarządzające składowaniem danych) musi być obecne na rynku, od co najmniej 3 lat
	O33.1.F7	Oferowane rozwiązanie musi być produktem gotowym, posiadającym na moment składania oferty wszystkie wymagane przez Zamawiającego funkcjonalności. Do oferty należy załączyć listę wszystkich komponentów urządzenia. Lista ma zawierać, co najmniej nazwy urządzeń, modeli oraz inne informacje pozwalające w sposób jednoznaczny zidentyfikować poszczególne komponenty sprzętowe i programowe.
	O33.1.F8	Oferowane urządzenia i wszystkie jego elementy składowe muszą być fabrycznie nowe i wyprodukowane nie wcześniej niż pół roku przed terminem dostawy do Zamawiającego.
	O33.1.F9	Oferowane urządzenia i wszystkie jego elementy muszą pochodzić od autoryzowanego Dostawcy producenta.
	O33.1.F10	Urządzenia muszą być oznakowane przez producenta w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.
	O33.1.F11	Wraz z rozwiązaniem musi być dostarczony komplet dokumentacji w formie papierowej lub elektronicznej. Dokumentacja papierowa powinna być czytelna. Zamawiający dopuszcza dostawę dokumentacji producenta rozwiązania w językach polskim lub angielskim.
	O33.1.F12	Wraz z rozwiązaniem musi być dostarczony komplet nośników umożliwiający odtworzenie oprogramowania systemowego urządzeń, z których zbudowane jest dostarczone rozwiązanie.
	O33.1.F13	Rozwiązanie musi mieć możliwość podłączenia go do centrum serwisowego producenta, w celu zdalnego monitorowania poprawności funkcjonowania komponentów rozwiązania.
Wymagania dotyczące skalowalności, budowy i architektury obiektowego systemu składowania danych.	O33.1.F14	Wszystkie elementy dostarczonego rozwiązania muszą być redundantne, a jego architektura musi zapewniać odporność na wystąpienie pojedynczego punktu awarii w obrębie poszczególnych grup elementów, to jest, co najmniej: interfejsów dostępowych kontrolerów, serwerów, zasilaczy, wentylatorów, dysków. Odporność na awarię oznacza, że dostęp do urządzenia oraz do składowanych na nim danych musi być realizowany bez przerywania pracy korzystającej z niego aplikacji/systemu, zapewniając możliwość odczytów wszystkich składowanych danych oraz wykonywania zapisów na urządzenie nawet w przypadku awarii lub wymiany pojedynczego elementu urządzenia z ww. grup urządzeń.
	O33.1.F15	Rozwiązanie powinno być odporne na awarię dowolnego z ośrodków tzn. w przypadku całkowitego zniszczenia infrastruktury oferowanego rozwiązania w jednym z ośrodków

		wszystkie dane powinny być dostępne, rozwiązanie powinno umożliwiać kontynuację pracy aplikacji, dostępna przestrzeń podczas awarii jednego z ośrodków powinna cały czas wynosić 100% wymaganej wartości netto, po usunięciu awarii dane powinny zostać automatycznie zsynchronizowane pomiędzy trzema ośrodkami.
	O33.1.F16	Architektura rozwiązania musi zapewniać umieszczenie interfejsów dostępowych i dyskowych wewnątrz wszystkich węzłów klastra, realizujących funkcję obiektowego systemu składowania danych.
	O33.1.F17	Wszystkie elementy opisanej powyżej architektury muszą być ze sobą zintegrowane w taki sposób, aby zapewnić automatyczny przepływ danych pomiędzy różnymi warstwami architektury.
	O33.1.F18	Wydajność osiągnięta w przypadku oferowanej konfiguracji w obrębie węzła, powinna umożliwiać odczyt małych obiektów (16 kB) z prędkością nie mniejszą niż 5000 OBIEKTÓW na sekundę oraz nie mniejszą niż 2GB/s w przypadku dużych obiektów (powyżej 10 MB)
	O33.1.F19	Dostarczone rozwiązanie powinno umożliwiać rozbudowę, do co najmniej 40PB przestrzeni bez konieczności zatrzymywania pracy rozwiązania i bez przerywania dostępu do danych.
	O33.1.F20	Dostarczone rozwiązanie powinno umożliwiać rozbudowę, do co najmniej 20 węzłów.
	O33.1.F21	Komunikacja pomiędzy węzłami oraz na zewnątrz (czyli dostęp do rozwiązania) musi być realizowana za pomocą interfejsów 10GbE lub 25GbE i SFP+.
	O33.1.F22	W przypadku, gdy system wymaga przełączników na potrzeby wewnętrznej komunikacji węzłów dostępowych obiektowego magazynu składowania danych, należy zapewnić redundantne przełączniki LAN 10GbE z odpowiednią ilością portów.
	O33.1.F23	Architektura rozwiązania musi zapewniać możliwość elastycznej rozbudowy, poprzez co najmniej dodawanie niezależnie węzłów dostępowych oraz węzłów przechowywania danych
Szczegółowe wymagania funkcjonalne dla obiektowego systemu składowania danych.	O33.2.F24	Dane w obiektowym magazynie danych muszą być składowane na napędach dyskowych. Nie dopuszcza się rozwiązań zbudowanych w oparciu o napędy taśmowe.
	O33.2.F25	Dostarczone rozwiązanie powinno posiadać wbudowane mechanizmy przechowywania zarówno danych, jak i metadanych (informacji opisujących dane). Nie dopuszcza się wykorzystania rozwiązań plikowych (NAS), jako warstwę przechowywania w systemie składowania danych.

	O33.2.F26	Rozwiązanie powinno posiadać możliwość integracji z aplikacjami za pomocą, co najmniej następujących protokołów i interfejsów: HTTP, S3, REST API, NFS. Jeżeli wykorzystanie któregośkolwiek z wymienionych protokołów i interfejsów wymaga zastosowania dodatkowej licencji lub oprogramowania, to należy je dostarczyć wraz z rozwiązaniem. Musi istnieć możliwość wykorzystania wszystkich protokołów równocześnie.
	O33.2.F27	Rozwiązanie powinno posiadać wbudowane mechanizmy protekcji danych, które gwarantują odczyt wszystkich składowanych danych w przypadku awarii pojedynczego, losowego komponentu architektury (dysku, karty sieciowej, przełącznika LAN, serwera i kontrolera urządzenia).
	O33.2.F28	Zarządzanie wewnętrznymi elementami urządzenia w każdej z lokalizacji powinna być realizowana poza w/w switch'ami dostępowymi, za pomocą dedykowanego do tego switch'a będącego częścią składową oferowanego rozwiązania
	O33.2.F29	W przypadku dysków Zamawiający wymaga, aby dostarczone rozwiązanie wykorzystywało następujące mechanizmy protekcji danych: RAID-6 lub Erasure Coding (EC) dla dysków SAS i SAS-NL
	O33.2.F30	Dostarczone rozwiązanie musi zapewniać i gwarantować niezmiennosc składowanych w nim obiektów, między innymi poprzez wykorzystanie wbudowanej technologii WORM (Write Once Read Many). Zamawiający wymaga, aby funkcjonalność WORM była realizowana wewnątrz dostarczonego gotowego rozwiązania sprzętowego w jego oprogramowaniu systemowym. Zamawiający nie dopuszcza, aby funkcjonalność WORM realizowana była poprzez rozwiązania programowe i rozwiązania uruchamiane w warstwie wirtualizacyjnej (VMware, Hyper-V, KVM i inne).
	O33.2.F31	Rozwiązanie musi posiadać możliwość definiowania różnych poziomów retencji przechowywania danych, gwarantujących brak możliwości skasowania danych przed upływem zdefiniowanego czasu.
	O33.2.F33	Rozwiązanie musi posiadać możliwość wykorzystania, co najmniej 30 atrybutów metadanych dla pojedynczego obiektu.
	O33.2.F34	Zamawiający wymaga, aby dostarczone rozwiązanie posiadało możliwość zdefiniowania, co najmniej 1000 logicznych partycji oraz co najmniej 1000 przestrzeni nazw. Musi istnieć możliwość mapowania i wykorzystania różnych przestrzeni nazw dla różnych aplikacji, w taki sposób, aby dla każdej z tych aplikacji możliwe było definiowanie różnych i niezależnych parametrów i kryteriów składowania danych, w tym, co najmniej: retencji, wersjonowania, indeksowania i replikacji.
	O33.2.F35	Rozwiązanie musi pozwalać na zdefiniowanie partycji, w których istnieje możliwość usuwania danych przed upływem retencji oraz

		partycji, w których usuwanie danych przed upływem retencji jest niemożliwe. Rozwiązanie powinno pozwalać na definiowanie i uruchamianie jednocześnie obydwu typów partycji.
	O33.2.F36	W przypadku partycji, w której istnieje możliwość usuwania danych przed upływem retencji wymagane jest, aby taką operację mógł wykonywać jedynie administrator z odpowiednimi uprawnieniami oraz aby operacja ta była audytowalna, co oznacza, że czynności związane z usuwaniem muszą być rejestrowane w wewnętrznych dziennikach dostarczonego rozwiązania.
	O33.2.F37	Każda ze zdefiniowanych partycji musi mieć możliwość zarządzana przez różnych administratorów.
	O33.2.F38	Rozwiązanie powinno posiadać wbudowany mechanizm wydłużania retencji danych.
	O33.2.F39	Rozwiązanie musi posiadać wbudowany natywny mechanizm automatycznego usuwania danych po upływie czasu retencji.
	O33.2.F40	Rozwiązanie musi posiadać swoje własne wbudowane mechanizmy weryfikacji sum kontrolnych składowanych obiektów.
	O33.2.F41	Rozwiązanie powinno posiadać wbudowane mechanizmy redukcji danych, w tym, co najmniej kompresję danych.
	O33.2.F42	Rozwiązanie musi posiadać wbudowany mechanizm indeksowania i wyszukiwania metadanych. Musi istnieć możliwość wyszukiwania w oparciu o wewnętrzną wyszukiwarke oraz interfejs API pozwalający na integrację silnika wyszukiwania z własną aplikacją.
	O33.2.F43	OBIEKTY (archiwizowane DANE oraz opisujące je METADANE) powinny być przechowywane na dyskach tego samego typu i rozmiarze (nie dopuszcza się stosowania różnych dysków do składowania DANYCH oraz METADANYCH, rozmiar użytych dysków nie powinien być mniejszy niż 4TB oraz nie powinien przekraczać rozmiaru 12TB)
	O33.2.F44	Rozwiązanie powinno posiadać wbudowany mechanizm wersjonowania obiektów.
	O33.2.F45	Rozwiązanie musi posiadać możliwość szyfrowania danych. Szyfrowanie powinno być realizowane: na dyskach obiektowego magazynu składowania danych i na połączeniu do replikacji pomiędzy ośrodkami.
	O33.2.F46	Rozwiązanie musi posiadać natywnie wbudowane mechanizmy umożliwiające replikację składowanych danych pomiędzy różnymi lokalizacjami z wykorzystaniem sieci LAN/WAN i protokołu HTTP. Zastosowanie niniejszego mechanizmu musi również spełniać wymagania replikacji metadanych, uprawnień, polityki retencji

		oraz niezmienności danych tzn. awaria urządzenia w lokalizacji podstawowej nie może eliminować gwarancji niezmienności danych na platformie zdalnej.
	O33.2.F47	Replikacja powinna być możliwa zarówno w trybie Active/Passive, czyli w trybie, w którym do odczytu i zapisu udostępniona jest replikowana przestrzeń nazw tylko w jednym ośrodku, jak i w trybie Active/Active, w którym do odczytu i zapisu udostępnione są replikowane przestrzenie nazw w każdym ośrodku.
	O33.2.F48	Replikacja powinna być możliwa, pomiędzy co najmniej 5 ośrodkami. W każdym z tych ośrodków replikowana przestrzeń nazw musi być jednocześnie dostępna do zapisu i odczytu w przypadku replikacji w trybie Active/Active
	O33.2.F49	Rozwiązanie powinno wspierać różne topologie replikacji danych w tym, co najmniej: 1-do-wielu, 1-do-1, wiele-do-1.
	O33.2.F50	Rozwiązanie powinno posiadać możliwość zarządzania, co najmniej poprzez graficzny interfejs użytkownika oraz poprzez API.
	O33.2.F51	Każda macierz (węzeł) obiektowa musi być wyposażona w minimum 4 porty 10GbE lub 4 porty 25GbE dedykowane do przesyłania danych oraz minimum 1 port 1GbE do zarządzania.
	O33.2.F52	Każda macierz obiektowa musi umożliwiać instalację dysków NL SAS 7,2kRPM o pojemnościach 4TB lub 8TB lub 10TB lub 12TB.
	O33.2.F53	Dostęp do danych SYSTEMU za pośrednictwem S3 API, Swift API oraz NFS v3.
	O33.2.F54	Możliwość szyfrowania składowanych obiektów algorytmem AES-256
	O33.2.F55	Możliwość kompresji składowanych danych.
	O33.2.F56	Możliwość weryfikacji integralności składowanych obiektów.
	O33.2.F57	Wersjonowanie obiektów na poziomie pojedynczych bucket-ów
	O33.2.F58	Tworzenie logicznie odseparowanych obszarów tzw. „MULTI-TENANCY” w obrębie jednej jak i wielu MACIERZY OBIEKTOWYCH (czyli w obrębie całego SYSTEMU w ramach wielu lokalizacji geograficznych); Wymagana jest możliwość rozdzielnego administrowania (np.: przypisywanie użytkowników, tworzenie praw dostępu, monitorowanie wykorzystania) tak tworzonymi obszarami,
	O33.2.F59	Automatyczny monitoring obejmujący m.in.: użycie zasobów on-line (w tym CPU, pamięć, sieć), ilość operacji S3, http
	O33.2.F60	Tworzenie alertów i powiadomień dot. stanu SYSTEMU, automatyczne przesyłanie ich poprzez e-mail

	O33.2.F61	Możliwość autentykacji z użyciem AD/LDAP dla użytkowników SYSTEMU.
	O33.2.F62	<p>Dostarczony sprzęt powinien być nowy, nieużywany dotąd w innych projektach. Zamawiający dopuszcza rozpakowanie sprzętu w celu weryfikacji jego skompletowania i braku usterek.</p> <p>Na etapie odbioru sprzętu Zamawiający będzie wymagał dostarczenia dokumentów potwierdzających datę produkcji sprzętu (oświadczenie producenta lub inne dokumenty)</p> <p>Całość dostarczonego sprzętu objęta będzie 60-miesięczną gwarancją, opartą o gwarancję producenta, umożliwiającą naprawy sprzętu, wymianę wadliwych podzespołów i części. Gwarancja musi umożliwiać dostęp do najnowszych wersji oprogramowania (firmware) oraz poprawek i łatek dla oprogramowania.</p> <p>Możliwość rozszerzenia gwarancji producenta do 7 lat</p> <p>Czas trwania gwarancji będzie liczony od daty podpisania protokołu odbioru sprzętu i oprogramowania, przy czym odbiór ten nastąpi po uruchomieniu i konfiguracji urządzeń w lokalizacjach wskazanych przez Zamawiającego</p> <p>Gwarancja będzie realizowana w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia. Wykonawca zapewni możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta</p> <p>W przypadku awarii dysków dyski twarde pozostają własnością Zamawiającego</p> <p>Oświadczenie producenta serwera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem</p>

7.11 Backup i Archiwizacja

Dostawca musi zapewnić mechanizm backup - restore, który będzie wykorzystywany w środowisku wirtualnym jego zadaniem będzie zapisywanie kopii i przywracanie systemów za pomocą snapshotów. Należy pamiętać, że wirtualizacja serwerowa nie może wnikać w to, co dzieje się w logice aplikacyjnej wewnątrz uruchomionych maszyn wirtualnych. Dopuszcza się zabezpieczanie dodatkowo mechanizmami „tradycyjnych” backupów agentowych, kiedy zajdzie taka konieczność w wyjątkowych przypadkach. Część danych należy archiwizować z o wiele dłuższym czasem retencji, a nie tylko backup'ować, w związku z tym należy zapewnić archiwum obiektowe WORM gdzie mają trafiać zdefiniowane dane. Archiwum

musi posiadać funkcjonalność, która nie pozwoli na zmianę ani wykasowanie danych i będzie równomiernie rozproszone pomiędzy trzema ośrodkami OPD celem zapewnienia bezpieczeństwa danych po awarii OPD (nawet głównego).

Planowane jest, że do celów testowego/cyklicznego sprawdzania możliwości odtworzeniowych z backupów będzie wykorzystywane środowisko testowe. Przyjęto, że wszystkie dane będą przechowywane i archiwizowane w następującym modelu:

1. Codzienna kopia środowiska chmury – 7 dni (7 kopii)
2. Tygodniowa kopia środowiska chmury – 4 tygodni (4 kopie)
3. Miesięczna kopia środowiska chmury – 12 miesięcy (12 kopii)
4. Roczna kopia środowiska chmury – 2 lata (1 kopia)

Wymagana jest możliwość określania RPO i RTO dla zabezpieczanych danych, rozwiązanie ma się cechować szybką implementacją i integracją z środowiskiem chmury OSE, minimalnym ryzykiem oraz relatywnie niskimi nakładami kapitałowymi i kosztami operacyjnymi. Rozwiązanie musi być zoptymalizowane dla infrastruktury wirtualnej i wykorzystywać istniejące w niej mechanizmy związane z wykonywaniem backupów i odtwarzania uwzględniając standardy charakterystyczne dla obszaru wirtualizacji. Od strony licencjonowania rozwiązanie powinno charakteryzować się skalowalnością i łatwością rozbudowy i pozwalać w prosty sposób planować rozbudowę środowiska i związane z tym inwestycje. System do tworzenia kopii zapasowych musi współpracować z architekturą wirtualizacyjną, minimalizować nakłady pracy potrzebnych do konfiguracji i obsługi środowiska. Możliwie uprościć codzienne czynności bez utraty funkcjonalności i przy zwiększeniu elastyczności i szybkości odtwarzania czy automatyzacji.

Założenia przy tworzeniu kopii zapasowych oraz odtwarzania danych:

1. 2 główne OPD są aktywne, gdzie w każdym z nich zaimplementowane jest urządzenie do tworzenia backupu odpowiedzialne za tworzenie kopii zapasowych drugiego ośrodka – w OPD1 tworzone są backupy OPD2 a w OPD2 kopie zapasowe z OPD1,
2. Wszystkie OPD będą połączone pomiędzy sobą logiczną siecią backup,
3. Wszystkie węzły pomiędzy sobą są połączone linkami gwarantującymi możliwość wykonania się kopii zapasowej w założonym oknie backup,
4. Okno potrzebne na wykonywanie kopii zapasowej zawiera się pomiędzy godziną 22 - 6,
5. Wirtualne serwery w regionalnych OPD będą bezstanowymi serwerami i nie wymagają regularnego backup-u.

Dane archiwalne będzie można definiować na żądanie. Wymagane jest, aby infrastruktura przechowywania kopii zapasowych była niezależna fizycznie od zasobów dyskowych chmury OSE (niezależne urządzenie typu appliance, dedykowane serwery itp.). Zakłada się, że ze względu na rozmiar archiwum może być ono współdzielone z urządzeniami oferującymi dostęp do zasobów obiektowych, ale utrzymywane w innej instancji/koszyku/puli zasobów o bardzo ograniczonym dostępie.

7.11.1 Backup i Archiwizacja - Deduplikatory

Identyfikator wymagania	Treść wymagania
O34.F1	Urządzenie musi być przeznaczone do de-duplikacji i przechowywania kopii zapasowych.
O34.F2	Dostarczone urządzenia muszą oferować przestrzeń min. 130TB netto (powierzchni użytkowej) bez uwzględniania redukcji danych (deduplikacji i/lub kompresji). Wymagana skalowalność do minimum 170TB netto.
O34.F3	Oferowane urządzenie musi mieć możliwość sprawdzenia pakietu upgrade'ującego firmware urządzenia (GUI lub CLI), to znaczy sprawdzenia czy nowa wersja systemu nie spowoduje problemów z urządzeniem.
O34.F4	Oferowane urządzenie musi posiadać minimum: - 4 porty Ethernet 10 Gb/s BaseT. Wymagana możliwość obsługi każdym portem protokołów CIFS, NFS, zapewniającymi deduplikację na źródle.
O34.F5	Oferowane urządzenie musi umożliwiać jednoczesny dostęp wszystkimi poniższymi protokołami: CIFS, NFS; zapewniającymi deduplikację na źródle.
O34.F6	Wymagane jest dostarczenie licencji, pozwalającej na jednoczesną obsługę protokołów CIFS, NFS, do oferowanej pojemności urządzenia
O34.F7	Oferowane pojedyncze urządzenie musi osiągać za-agregowaną wydajność (dla maksymalnej konfiguracji) protokołami: NFS co najmniej 3TB/h (dane podawane przez producenta) oraz co najmniej 5 TB/h z wykorzystaniem de-duplikacji na źródle (dane podawane przez producenta).
O34.F8	Urządzenie musi pozwalać na jednoczesną obsługę minimum 150 strumieni w tym jednocześnie: - zapis danych minimum 50 strumieniami; - odczyt danych minimum 50 strumieniami; - replikacja minimum 50 strumieniami. Dane mogą pochodzić z różnych aplikacji oraz dowolnych protokołów (CIFS, NFS) oraz dowolnych interfejsów LAN w tym samym czasie.
O34.F10	Oferowane urządzenie musi de-duplikować dane in-line przed zapisem na nośnik dyskowy. Na wewnętrznych dyskach urządzenia nie mogą być zapisywane dane w oryginalnej postaci (niezdeduplikowanej) z jakiegokolwiek fragmentu strumienia danych przychodzącego do urządzenia.
O34.F11	Technologia de-duplikacji musi wykorzystywać algorytm bazujący na zmiennym, dynamicznym bloku.
O34.F12	Oferowany produkt musi posiadać obsługę mechanizmów globalnej de-duplikacji dla danych otrzymywanych jednocześnie wszystkimi protokołami (CIFS, NFS, deduplikacja na źródle) przechowywanych w obrębie całego urządzenia, co oznacza, że przechowywany na urządzeniu fragment danych nie może być ponownie zapisany bez względu na to, jakim protokołem zostanie ponownie otrzymany. Wszystkie udziały NFS/CIFS również powinny podlegać globalnej deduplikacji – blok danych otrzymany i zapisany nie może zostać ponownie zapisany w obrębie tego samego urządzenia. Przestrzeń składowania zde-duplikowanych danych musi być jedna dla wszystkich protokołów dostępowych, co oznacza zastosowanie pojedynczej bazy deduplikatów bez względu na ilość/rodzaj używanych jednocześnie protokołów dostępowych.
O34.F13	W przypadku niespełnienia opisanego powyżej wymogu globalnej de-duplikacji, przy spełnieniu pozostałych wymaganych funkcjonalności, oferowane urządzenie powinno oferować przestrzeń

	min. 200% netto (powierzchni użytkowej) bez uwzględniania mechanizmów protekcji, wymagana skalowalność urządzenia w takim wypadku do min. 250% netto
O34.F14	Proces de-duplikacji musi odbywać się in-line – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Zapisowi na system dyskowy muszą podlegać tylko unikalne bloki danych niezapisane jeszcze na system dyskowy urządzenia. Dotyczy to każdego fragmentu przychodzących do urządzenia danych.
O34.F15	Proponowane rozwiązanie nie może w żadnej fazie korzystać (w całości lub częściowo) z bufora na składowanie danych w postaci oryginalnej (niezdeduplikowanej) w celu ich późniejszej deduplikacji (wymagana deduplikacja in-line)
O34.F16	Wszystkie unikalne bloki przed zapisaniem na dysk muszą być dodatkowo kompresowane.
O34.F17	Urządzenie musi umożliwiać de-duplikację na źródle i przesłanie nowych, nieznajdujących się jeszcze na urządzeniu bloków poprzez sieć LAN.
O34.F18	De-duplikacja w wyżej wymienionych przypadkach musi zapewniać, aby z zabezpieczanych serwerów do urządzenia były transmitowane poprzez sieć LAN jedynie fragmenty danych nieznajdujące się dotychczas na urządzeniu.
O34.F19	De-duplikacja w wyżej wymienionych przypadkach musi zapewniać, aby z serwerów do urządzenia były transmitowane poprzez sieć tylko fragmenty danych nieznajdujące się dotychczas na urządzeniu.
O34.F20	W przypadku de-duplikacji na źródle poprzez sieć IP (LAN oraz WAN), wymagana możliwość szyfrowania komunikacji kluczem minimum 256 bitów.
O34.F21	Urządzenie powinno umożliwiać zaszyfrowanie przechowywanych danych, wymagane dostarczenie licencji umożliwiających zaszyfrowanie i przechowywanie zaszyfrowanych danych w obrębie maksymalnej pojemności oferowanego urządzenia.
O34.F22	Urządzenie musi wspierać de-duplikację na źródle poprzez sieć minimum dla następujących systemów operacyjnych: - Windows, Linux (RedHat, SuSE)
O34.F23	Oferowane urządzenie musi umożliwiać bezpośrednią replikację danych do drugiego urządzenia takiego samego typu. Konfiguracja replikacji musi być możliwa w każdym z trybów: - jeden do jednego ; - wiele do jednego; - jeden do wielu; - kaskadowej (urządzenie A replikuje dane do urządzenia B, które te same dane replikuje do urządzenia C).
O34.F24	Replikacja musi się odbywać w trybie asynchronicznym. Transmitowane mogą być tylko te fragmenty danych (bloki) które nie znajdują się na docelowym urządzeniu. Ewentualna licencja na replikację musi być dostarczona w ramach postępowania.
O34.F25	Urządzenie musi umożliwiać wydzielenie określonych portów Ethernet dedykowanych do replikacji.
O34.F26	W przypadku wykorzystania portów Ethernet do replikacji urządzenie musi umożliwiać przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami.
O34.F27	Replikacja odbywa się bezpośrednio między dwoma urządzeniami bez udziału serwerów pośredniczących
O34.F28	Replikacji podlegają tylko te fragmenty danych, które nie znajdują się na docelowym urządzeniu

O34.F29	Replikacja zarządzana jest z poziomu wymaganej aplikacji
O34.F30	Aplikacja posiada informację o obydwu kopiach zapasowych znajdujących się w obydwu urządzeniach bez konieczności przeprowadzania procesu inwentaryzacji
O34.F31	Oferowane urządzenie musi działać poprawnie przy wypełnieniu danymi na poziomie, co najmniej 90%. Dokumentacja urządzenia nie może wskazywać na ew. problemy, obostrzenia, które są efektem wypełnienia urządzenia zabezpieczanymi danymi, na poziomie mniejszym niż 90%.
O34.F32	Narzut na wydajność związany z replikacją nie może zmniejszyć wydajności urządzenia o więcej niż 10%.
O34.F33	Wymagana możliwość ograniczenia pasma używanego do replikacji między dwoma urządzeniami – oferowane urządzenie powinno być wyposażone w mechanizm umożliwiający zarządzaniem stopnia wykorzystania pasma na potrzeby replikacji.
O34.F34	Zdeduplikowane i skompresowane dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID 6.
O34.F35	Każda grupa RAID 6 musi mieć przynajmniej 1 dysk hot-spare automatycznie włączany do grupy RAID w przypadku awarii jednego z dysków produkcyjnych. Dyski hot-spare muszą być globalne, możliwe do wykorzystania w innych półkach, w przypadku wyczerpania w nich dysków hot-spare.
O34.F36	Oferowane urządzenie musi umożliwiać wykonywanie SnapShot'ów, czyli umożliwiać zamrożenie obrazu danych (stanu backupów) w urządzeniu na określoną chwilę. Oferowane urządzenie musi również umożliwiać odtworzenie danych ze Snapshot'u.
O34.F37	Odtworzenie danych ze Snapshot'u nie może wymagać konieczności nadpisania danych produkcyjnych jak również nie może oznaczać przerwy w normalnej pracy urządzenia (przyjmowania/odtwarzania backupów). Urządzenie musi pozwalać na przechowywanie minimum 100 Snapshotów jednocześnie w obrębie oferowanej przestrzeni, przy zachowaniu globalnej deduplikacji oraz standardowego trybu pracy urządzenia – umożliwiającego wykorzystanie wszystkich dostępnych funkcjonalności.
O34.F38	Urządzenie musi umożliwiać podział na logiczne części. Dane znajdujące się w każdej logicznej części muszą być między sobą de-duplikowane (globalna de-duplikacja między logicznymi częściami urządzenia).
O34.F39	Urządzenie musi mieć możliwość podziału na logiczne części pracujące równolegle. Producent musi oficjalnie wspierać pracę 10-ciu logicznych części pracujących równolegle z pełną wydajnością urządzenia.
O34.F40	Dla każdej z w/w logicznych części oferowanego urządzenia musi być możliwość zdefiniowania oddzielnego użytkownika zarządzającego daną logiczną częścią de-duplikatora. Użytkownicy zarządzający logiczną częścią A muszą widzieć tylko i wyłącznie zasoby logicznej części A i nie mogą widzieć żadnych innych zasobów oferowanego urządzenia.
O34.F41	Wymagana możliwość zaprezentowania każdej z logicznych części oferowanego urządzenia, jako niezależnego urządzenia dostępnego za pośrednictwem:
	· CIFS
	· NFS

O34.F42	Urządzenie powinno umożliwiać zdefiniowanie blokady skasowania danych (funkcjonalność typu WORM). Blokada skasowania danych musi chronić plik w zdefiniowanym czasie przed usunięciem pliku, modyfikacją pliku.
O34.F43	Blokada skasowania danych musi działać w dwóch trybach (do wyboru przez administratora):
	<ul style="list-style-type: none"> • możliwość zdjęcia blokady przed upływem ważności danych
	<ul style="list-style-type: none"> • brak możliwości zdjęcia blokady przed upływem ważności danych (compliance) <p>Licencje na blokadę usunięcia/zmiany przechowywanych plików muszą być dostarczone wraz z urządzeniem.</p>
O34.F45	Urządzenie musi mieć możliwość przechowywania danych niezmiennych:
	· Video
	· Grafika
	· Pliki pdf
	na udziałach CIFS/NFS.
	Wymagane jest formalne wsparcie producenta dla przechowywania w/w danych na urządzeniu.
O34.F46	Urządzenie musi weryfikować dane po zapisie (nie chodzi o ew. weryfikację danych indeksowych generowanych przez urządzenie, ale o weryfikację wszystkich zabezpieczanych danych backup'owych). Każda zapisana na dyskach porcja danych musi być odczytana i porównana z danymi otrzymanymi przez urządzenie. Powyższa weryfikacja powinna być realizowana w locie, czyli przed usunięciem z pamięci oryginalnych danych (otrzymanych z aplikacji backupowej), musi być realizowana w trybie ciągłym (a nie ad-hoc), wymagane parametry wydajnościowe urządzenia muszą uwzględniać tę funkcjonalność.
O34.F47	Wymagane potwierdzenie opisanej funkcjonalności w oficjalnej dokumentacji producenta oferowanego urządzenia.
O34.F48	Urządzenie musi automatycznie usuwać przeterminowane dane (bloki danych nienależące do backupów o aktualnej retencji) w procesie czyszczenia.
O34.F49	Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać pracy procesów backupu / odtwarzania danych (zapisu / odczytu danych z zewnątrz do systemu).
O34.F50	Wymagana możliwość zdefiniowania maksymalnego obciążenia urządzenia procesem usuwania przeterminowanych danych (poziomu obciążenia procesora).
O34.F51	Wymagana możliwość zdefiniowania harmonogramu wg., którego wykonywany jest proces usuwania przeterminowanych danych (czyszczenia), realizowany równolegle z procesami backup/restore/replication.
O34.F52	Standardowa częstotliwość usuwania przeterminowanych danych (czyszczenie) nie powinna być większa niż 1 raz na tydzień - minimalizując czas, w którym backupy/odtworzenia narażone są na spowolnienie.
O34.F53	Urządzenie musi mieć możliwość zarządzania poprzez
	· Interfejs graficzny dostępny z przeglądarki internetowej

	· Poprzez linię komend (CLI) dostępną z poziomu ssh (secure shell)
034.F54	<p>Dostarczony sprzęt powinien być nowy, nieużywany dotąd w innych projektach. Zamawiający dopuszcza rozpakowanie sprzętu w celu weryfikacji jego skompletowania i braku usterek.</p> <p>Na etapie odbioru sprzętu Zamawiający będzie wymagał dostarczenia dokumentów potwierdzających datę produkcji sprzętu (oświadczenie producenta lub inne dokumenty)</p> <p>Całość dostarczonego sprzętu objęta będzie 60-miesięczną gwarancją, opartą o gwarancję producenta, umożliwiającą naprawy sprzętu, wymianę wadliwych podzespołów i części. Gwarancja musi umożliwiać dostęp do najnowszych wersji oprogramowania (firmware) oraz poprawek i łatek dla oprogramowania.</p> <p>Możliwość rozszerzenia gwarancji producenta do 7 lat</p> <p>Czas trwania gwarancji będzie liczony od daty podpisania protokołu odbioru sprzętu i oprogramowania, przy czym odbiór ten nastąpi po uruchomieniu i konfiguracji urządzeń w lokalizacjach wskazanych przez Zamawiającego</p> <p>Gwarancja będzie realizowana w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia. Wykonawca zapewni możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta</p> <p>W przypadku awarii dysków dyski twarde pozostają własnością Zamawiającego</p> <p>Oświadczenie producenta serwera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem</p>

7.11.2 Backup i Archiwizacja - Wymagane funkcjonalności oprogramowania do zabezpieczania danych

Identyfikator wymagania	Treść wymagania
034.1.F1	Zamawiający wymaga dostarczenia, uruchomienia i wdrożenia systemu do zabezpieczania środowiska Data Center (baz danych, maszyn wirtualnych, serwerów plików, serwerów wolno stojących).
034.1.F2	Wymagane jest dostarczenie wszystkich modułów oprogramowania tak, aby zapewnić backup całości wyspecyfikowanego środowiska oraz spełnić wszystkie wymienione w niniejszej tabeli funkcjonalności. Wymagane wsparcie na oferowane oprogramowanie realizowane przez producenta w okresie min. 5 lat, umożliwiające zgłoszenia w trybie 24x7 NBD, gwarantujące dostęp do najnowszych wersji oprogramowania.

7.11.3 Backup i Archiwizacja - Wymagania dotyczące backupu serwerów (Data Center)

Identyfikator wymagania	Treść wymagania
-------------------------	-----------------

O34.4.F5	Wymagane jest, aby oprogramowanie backupowe zapewniało backup środowiska minimum 10 milionów plików w czasie krótszym niż 1 godzina - jako pełny backup (podany wolumen oraz czas backup'u zostały przytoczone dla zobrazowania wymaganej wydajności)
O34.4.F6	Wymagane jest, aby oprogramowanie backupowe zapewniało szybki backup blokowy wielomilionowych systemów plików na maszynach Windows oraz Linux
O34.4.F7	W trakcie backupu oprogramowanie backupowe musi wykonywać kopie zapasowe fizycznych bloków a nie plików. Wymagana możliwość odtworzenia pojedynczego pliku.
O34.4.F8	W celu minimalizacji czasu backupu oprogramowanie backupowe nie może indeksować plików znajdujących się na zabezpieczanym wolumenie .
O34.4.F9	Wymagane jest, aby oprogramowanie backupowe zapewniało szybki inkrementalny backup blokowy wielomilionowych systemów plików na maszynach Windows oraz Linux.
O34.4.F10	W trakcie backupu inkrementalnego wielomilionowych systemów plików na maszynach Windows oraz Linux oprogramowanie backupowe musi odczytywać tylko te fragmenty dysku, które zmieniły się od ostatniego backupu (wykorzystanie mechanizmu CBT)
O34.4.F11	Oprogramowanie backupowe nie może odczytywać zmienionych plików, jedynie zmienione bloki na dysku.
O34.4.F12	W celu minimalizacji czasu backupu oprogramowanie backupowe nie może indeksować plików backupu inkrementalnego znajdujących się na zabezpieczanym wolumenie.
O34.4.F13	Oprogramowanie backupowe musi mieć możliwość łączenia backupu blokowego pełnego i inkrementalnego w jeden pełen backup.
O34.4.F14	Po połączeniu backupu pełnego i inkrementalnego muszą być dostępne dwa backupy pełne: dotychczas dostępny backup pełny i nowy backup pełny uzyskany w drodze łączenia z backupem inkrementalnym.
O34.4.F16	Oferowane rozwiązanie backupowe musi przechowywać całość własnych informacji (informacje o backupach, mediach) w centralnym pojedynczym katalogu, skopiowanie centralnego katalogu systemu backupu na inną maszynę musi pozwolić na uruchomienie na drugiej maszynie serwera backupu identycznego z oryginalnym. Proces klonowania centralnego katalogu może odbywać się przy wyłączonych procesach backupowych (zapewnienie spójności wewnętrznej bazy danych systemu backupowego).
O34.4.F17	Ze względów bezpieczeństwa rozwiązanie backupowe musi mieć możliwość wykonania kopii wewnętrznej bazy danych w trakcie pracy systemu bez konieczności ograniczania jego funkcjonalności.
O34.4.F18	Oprogramowanie backupowe musi mieć możliwość backupu własnej bazy danych na następujące nośniki: - urządzenie dyskowe; -urządzenie de-duplikacyjne.
O34.4.F20	Oprogramowanie backupowe musi mieć możliwość automatycznego wykonywania backupu własnej bazy danych.
O34.4.F22	Oprogramowanie backupowe po każdorazowym backupie wewnętrznej bazy danych musi raportować poprzez e-mail miejsce, w którym znajduje się ostatni backup wewnętrznej bazy danych oprogramowania backupowego.

O34.4.F23	Backup własnej bazy danych musi pozwalać na odtworzenie wszystkich ustawień systemu backupowego na zupełnie nowej, świeżo zainstalowanej instancji oprogramowania backupowego.
O34.4.F24	Oprogramowanie backupowe musi mieć możliwość (wymagane formalne wsparcie producenta oprogramowania backupowego) działania, jako wirtualna maszyna systemu VMware, Hyper-V, bądź KVM.
O34.4.F27	Oprogramowanie backupowe musi umożliwiać łączenie strumieni backupowych z wielu zabezpieczanych serwerów w sieci LAN.
O34.4.F31	Oprogramowanie backupowe musi mieć możliwość klonowania backupów między dowolnymi mediami: <ul style="list-style-type: none"> • dyskowymi (CIFS, NFS) • (opcjonalnie) de-duplikacyjnymi;
O34.4.F32	Oprogramowanie backupowe musi zapewniać różny czas ważności danych na podstawowym nośniku i nośniku zawierającym kopię (replikę backupu). Definicja czasu przechowywania kopii (repliki) powinna być określona w momencie definiowania zadania duplikacji/klonowania zarówno z interfejsu graficznego jak i z command line.
O34.4.F33	Oprogramowanie backupowe musi mieć możliwość przechowywania informacji o zbackupowanych systemach plików na dwa sposoby: <p>- system backupu przechowuje informację o całym zadaniu backupowym jak również o pojedynczych plikach pozwalając na odtworzenie zarówno całego systemu plików jak również pojedynczego pliku;</p> <p>- system backupu przechowuje jedynie informację o całym zadaniu backupowym systemu plików pozwalając na odtworzenie tylko całego systemu plików jednak minimalizując wewnętrzną bazę danych (nie przechowuje informacji o każdym ze zbackupowanych plików).</p>
O34.4.F34	Oprogramowanie backupowe musi pozwalać na następujące rodzaje backupu systemu plików: <ul style="list-style-type: none"> • Pełny; • Różnicowy; • Inkrementalny
O34.4.F35	Oprogramowanie backupowe musi pozwalać na łączenie backupów pełnych i inkrementalnych w jeden pełen backup. Proces ten musi być niewidoczny dla systemu plików, którego dotyczą backupy pełne i inkrementalne. Proces odtworzenia danych z połączonego backupu pełnego i inkrementalnego musi być identyczny z odtworzeniem danych z normalnie wykonanego backupu pełnego w zakresie zarządzania i wydajności
O34.4.F36	Oprogramowanie backupowe musi pozwalać na łączenie backupów pełnych i inkrementalnych bez odczytu danych z oferowanego urządzenia deduplikacyjnego.
O34.4.F38	Oprogramowanie backupowe musi pozwalać na zatrzymanie procesu backupu oraz jego wznowienie od momentu zatrzymania
O34.4.F39	W przypadku nieudanego backupu dla systemu plików (na przykład zerwanie łączności), oprogramowanie backupowe musi pozwalać na wznowienie backupu od ostatnio poprawnie zbackupowanego katalogu jak również pliku

O34.4.F40	W przypadku konsoli oprogramowania backupowego wymagana możliwość definiowania ważności danych (backupów) na podstawie kryteriów czasowych (dni, miesiące, lata). Po okresie ważności backupy muszą być automatycznie usunięte
O34.4.F41	Oprogramowanie backupowe musi wspierać (wymagane wsparcie producenta) następujące systemy operacyjne: Windows (także Microsoft Cluster) , Linux (Red Hat, SUSE, CentOS), Solaris
O34.4.F42	Oprogramowanie backupowe musi wspierać (wymagane wsparcie producenta) backup online następujących baz danych i aplikacji: MS SQL, Oracle, IBM DB2, MySQL
O34.4.F43	W przypadku baz danych system musi umożliwiać inicjalizację backupu poprzez określone zdarzenie: np. ilość logów, czas, który upłynął od ostatniego zdarzenia lub inne zdarzenie zdefiniowane przez użytkownika
O34.4.F47	Oprogramowanie backupowe musi mieć możliwość odtwarzania pojedynczego serwera Windows bez ponownej instalacji systemu operacyjnego.
O34.4.F48	Rozwiązanie backupowe musi mieć możliwość odtworzenia plików na docelową maszynę w oddziale z poziomu centralnej konsoli systemu backupowego. Nie może być wymagane logowanie się na odtwarzaną maszynę w celu odtworzenia danych z systemu backupowego.
O34.4.F49	Wymagana możliwość odtworzenia danych z zabezpieczonego serwera / komputera jak również z konsoli systemu backupowego. Oprogramowanie backupowe musi umożliwiać zarządzanie bezpośrednią replikacją backupów między urządzeniami przeznaczonymi do duplikacji.

7.11.4 Backup i Archiwizacja - Wymaga funkcjonalności - dotyczących monitorowania, raportowania oraz przeszukiwania backupów

Identyfikator wymagania	Treść wymagania
O34.3.F1	W ramach dostarczonych licencji musi być zapewniona możliwość monitorowania, raportowania, szczegółowego rozliczania z użycia komponentów systemu backupowego oraz analizy błędów dla środowiska kopii zapasowej Zamawiającego.
O34.3.F2	W ramach dostarczonych licencji musi być zapewniona możliwość monitorowania, raportowania, szczegółowego rozliczania z użycia komponentów systemu backupowego oraz analizy błędów dla środowiska kopii zapasowej Zamawiającego. Wymagana dostępność następujących raportów:
	a. Podsumowanie zadań backupowych (liczba backupów udanych, nieudanych, aktywnych, łączny rozmiar zbackupowanych danych)
	b. Podsumowanie zadań odtworzeniowych (liczba odtworzeń udanych, nieudanych, aktywnych, łączny rozmiar odtworzonych danych)
	c. Zbiorcze procentowe zestawienie udanych zadań backupowych z poszczególnych serwerów
	d. Zbiorcze zestawienie zabezpieczanych serwerów, które w sposób ciągły (kilka razy pod rząd) mają problem z backupami

	e. Zestawienie zabezpieczanych systemów plików, które w ogóle nie są backupowane, a co najmniej raz zostały zbackupowane
	f. Spodziewany czas odtwarzania zabezpieczanego serwera oraz potencjalnej utraty danych (czas między ostatnim backupem a chwilą awarii)
	g. Najmniej wiarygodne zabezpieczanych serwery (procent nieudanych backupów)
	h. Lista najwolniejszych/najszybszych zabezpieczanych maszyn
	i. Poziom SLA (procentowa liczba udanych backupów) w odniesieniu do poziomu założonego
	j. Mierzenie poziomu SLA dla poszczególnych zabezpieczanych serwerów przy uwzględnieniu założonego okna backupowego i RPO (punktu, do którego się odtwarzamy)
	k. Liczba danych backupowanych dziennie
	l. Liczba zadań backupowych dziennie
	m. Zużycie zasobów na serwerach backupowych (procesor, pamięć, karty sieciowe LAN, SAN)
	n. Zużycie mediów backupowych
	o. Aktualna konfiguracja systemu backupowego
	p. Historia zmian konfiguracji systemu backupowego
	q. Posiadane licencje systemu backupowego
O34.3.F3	W ramach dostarczonych licencji wymagana możliwość przeszukiwania backupów z poziomu graficznego interface'u (GUI)

7.11.5 Backup i Archiwizacja - Wymaga funkcjonalności – dotyczy rozwiązań Continuous Data Protection dla środowisk wirtualnych

Identyfikator wymagania	Treść wymagania
O34.4.F1	Integracja na poziomie Plug-in z systemami zarządzania wirtualizacją
O34.4.F2	Wsparcie dla funkcjonalności HA wirtualizatora , automatycznego dystrybuowania zasobów warstwy compute i storage.
O34.4.F3	Możliwość integracji z systemami inteligentnego zarządzania infrastrukturą fizyczną, wirtualna i chmurą.
O34.4.F4	Rozwiązanie dostarczane w postaci oprogramowania instalowanego na platformie wirtualizacyjnej.
O34.4.F5	Skalowalność zapewniająca wsparcie dla 500 VM w obrębie pojedynczego systemu do zarządzania centrum danych.

O34.4.F6	Zabezpieczenie dowolnej maszyny wirtualnej wraz z aplikacjami w trybie ciągłym tzn. umożliwiającym odtworzenie do dowolnego punktu w czasie (tzw. PIT – Point In Time), wymagane wsparcie dla najnowszych wersji wirtualizatora.
O34.4.F7	Możliwość tworzenia tzw. CONSISTENCY GROUP zapewniających identyczną konsystencję dla przynależących do danej grupy maszyn wirtualnych (VM), wymagane wsparcie dla min. 50 CONSISTENCY GROUP
O34.4.F8	Możliwość skryptowego tworzenia planów RECOVERY.
O34.4.F9	Zabezpieczenie realizowane za pośrednictwem ciągłej replikacji (a nie za pomocą SNAPSHOT'ów) na poziomie plików maszyny wirtualnej (wirtualnego dysku) oraz RDM, niezależnie od użytego storage'u (tzw. Storage Agnostic -warunkiem jest wsparcie przez producenta wirtualizatora), wymagane wsparcie dla połączeń: iSCSI, NAS oraz DAS
O34.4.F10	Odporność na kilkusekundowe problemy (przeciążenie, zaniki) związane z siecią WAN
O34.4.F11	Wbudowana funkcjonalność deduplikacji oraz kompresji w przypadku transmisji danych poprzez WAN
O34.4.F12	Możliwość przeprowadzania testów DR bez wpływu na zabezpieczane serwery produkcyjne oraz bez konieczności zmian w działaniu replikacji (np.: PAUSE, REVERSE, ...).
O34.4.F13	Proponowane rozwiązanie powinno umożliwiać: - stworzenia DISASTER RECOVERY dla całego zabezpieczanego wirtualnego środowiska; - operacyjne ODTWARZANIE dowolnej maszyny VM wraz z aplikacjami; - MIGRACJI danych w trybie ON-LINE na inne zasoby dyskowe.
O34.4.F14	Możliwość automatycznego zainicjowania procesu REVERSE REPLICATION w przypadku procesów FAILOVER/FAILBACK.
O34.4.F15	Granularność umożliwiająca pominięcie określonych plików maszyny wirtualnej (wirtualnego dysku) związanych z wirtualnymi serwerami VM objętych protekcją
O34.4.F16	Architektura FAULT-TOLERANT, brak pojedynczego punktu awarii.
O34.4.F17	Działanie rozwiązania będącego przedmiotem zapytania nie może mieć żadnego negatywnego wpływu na wydajność zabezpieczanych maszyn i aplikacji.
O34.4.F18	Wyskalowanie systemu powinno gwarantować RPO (Recovery Point Objective) w przypadku codziennej pracy ciągłej na poziomie kilku minut
O34.4.F19	możliwość automatycznego przeprowadzania operacji typu FAILOVER/FAILBACK do dowolnego punktu w czasie określonych testowych maszyn wirtualnych (VM)
O34.4.F20	Możliwość odtworzenia zabezpieczanego środowiska do dowolnego punktu w czasie.
O34.4.F21	Możliwość trybu pracy umożliwiającego objęciem protekcją w sposób automatyczny nowo dodanych maszyn wirtualnych (VM).
O34.4.F22	Rozwiązanie powinno dopuszczać zmiany HW na poziomie infrastruktury zabezpieczanego środowiska bez negatywnego wpływu na działanie systemu.
O34.4.F23	Wsparcie dla VSS, zapewnienie konsystencji aplikacji na poziomie VSS.

O34.4.F24	Możliwość automatycznego przeprowadzania operacji typu FAILOVER/FAILBACK do dowolnego punktu w czasie dla określonych produkcyjnych serwerów wirtualnych (VM), w tym: odtworzenie, uruchomienie (z zachowaniem wymaganej sekwencji), konfigurację.
-----------	--

7.12. Wymagania wdrożeniowe

7.12.1. Zakres prac dla Fazy 0

Faza 0 obejmuje wdrożenie systemu Radius i jego integrację z systemami sieci i bezpieczeństwa dla środowiska produkcyjnego i testowego oraz zapewnienie infrastruktury obliczeniowej dla systemów sieci, systemów bezpieczeństwa zarówno w środowisku produkcyjnym jak i testowym.

Cel realizacji fazy: Zapewnienie środowiska do funkcjonowania sieci docelowej i systemów bezpieczeństwa

Zakres wymagań stawianych Wykonawcy oraz wymaganej funkcjonalności, która musi być wdrożony w Fазie 0 jest przedstawiony w tabeli poniżej.

Identyfikator wymagania	Treść wymagania
O51.F1	Wykonawca zobowiązany jest zapewnić zwirtualizowaną infrastrukturę produkcyjną i testową na potrzeby systemów bezpieczeństwa i systemów sieci szkieletowej. Infrastruktura musi zapewnić wystarczającą wydajność dla systemów. Wykonawca może tę infrastrukturę zapewnić, jako tymczasową w swojej kolokacji (o ile spełnia wymagania Tier-3 zgodnie z normą ANSI/TIA-942 oraz z normę ISO/IEC 27001:2013 - ewentualnie ISO/IEC 27001:2005) lub jako docelową zainstalowaną w węzłach OSE.
O51.F2	Wykonawca jest zobowiązany zainstalować serwer Radius do autoryzacji użytkowników na urządzeniach sieci i urządzeniach bezpieczeństwa. Ten sam Radius ma obsługiwać zarówno urządzenia w środowisku produkcyjnym jak i testowym.
O51.F3	Zwirtualizowana infrastruktura dostarczana w ramach centrum danych Wykonawcy, jako usługa hostingu na potrzeby OSE musi być logicznie wydzielona od pozostałych zasobów w centrum danych Wykonawcy. Centrum danych musi być zlokalizowane na terenie Polski.
O51.F4	W przypadku, gdy infrastruktura jest dostarczana, jako usługa hostingu, wówczas wykonawca zapewni łącze pracujące w warstwie 2, zakończone w węźle centralnym sieci OSE na ul. 11 Listopada w Warszawie, ze stykiem fizycznym 10GBase-LR. Przepustowość łącza musi być dobrana przez Wykonawcę tak, aby zapewnić wystarczającą przepływność zapewniającą pracę systemów OSS/BSS.
O51.F5	Wykonawca zobowiązuje się do wykonania tej fazy i projektu całego Rozwiązania zgodnie z harmonogramem przedstawionym w tabeli Załącznika nr 5 do Umowy

7.12.2. Zakres prac dla Fazy 1

Faza 1 obejmuje wdrożenie systemów BSS - Jira OSE w postaci kopii działających w NASK systemów Jira WF (Workflow) , Jira SD (Service Desk) i Jira Insight (Asset Management), Provisionig, rConfig (wraz ze skryptami integratorskimi), dostarczenia aktywatora dla sieci szkieletowej, rozbudowę infrastruktury obliczeniowej, przeprowadzenie instruktaży i integracje z systemami wskazanymi przez Zamawiającego.

W ramach Fazy 1 wdrożony również musi zostać Portal Usługowy. Zakłada się, że przed produkcyjnym wdrożeniem systemów BSS - Jira OSE w Fазie 1 Wykonawca dostarczy i zainstaluje wymaganą infrastrukturę obliczeniową i systemową (wirtualizacja, systemy operacyjne, środowisko aplikacyjne itp.) pod systemy BSS - Jira OSE i OSE NASK w centrach kolokacji wskazanych przez Zamawiającego. Po wdrożeniu produkcyjnym zakresu z Fazy 1 Wykonawca rozpocznie utrzymanie wdrożonego środowiska. W ramach tej fazy Wykonawca jest zobowiązany do wdrożenia Systemów BSS - Jira OSE w następującym zakresie:

1. systemy BSS - Jira OSE muszą być wdrożone i zintegrowane z pozostałymi systemami OSE NASK i NASK w zakresie funkcjonalności pozwalającym na nieprzerwane działanie wszystkich procesów biznesowych funkcjonujących u operatora OSE
2. systemy BSS - Jira OSE muszą być wdrożone w zakresie spełniającym wymagania przedstawione w tabeli poniżej
3. infrastruktura obliczeniowa gotowa na migrację Portalu OSE z obecnych systemów hostingowych (w momencie tej Fazy Wykonawca rozpoczyna utrzymanie hosting dla Portalu OSE, migrację samego portalu OSE procesują pracownicy Zamawiającego)
4. system BSS - Portal Usługowy musi być wdrożony i zintegrowany z pozostałymi systemami zamawiającego
5. musi zostać wdrożony wspólny widok dla systemów JIRA przejściowych i docelowych
6. musi zostać wdrożone narzędzie agregujące raporty z systemów JIRA przejściowych i docelowych
7. musi zostać zrealizowana migracja zleceń zatrzymanych po procesie pozyskania szkoły do OSE w systemach przejściowych z uwagi na przekroczenie limitu obsługi w obecnym systemie Zamawiającego

Wersja Jira, Insight oraz lista plug-in'ów Jira i ich wersje wykorzystywanych w systemach NASK OSE na dzień ogłoszenia postępowania zakupowego są następujące:

Jira ver. 7.12.1

JIRA Service Desk Application v3.15.1

- AM Utils - 1.3.19
- Actions for JIRA Service Desk - 1.3.29
- Adaptavist ScriptRunner for JIRA - 5.4.34
- Automated Attachments - 1.3.0
- BigGantt - 3.13.4-jira7

- Bob Swift Atlassian Add-ons - Create on Transition - 7.1.0
- Calendar (CoreSoft Labs Commons) - 1.1.1
- Easy Links for JIRA - 1.4.5
- Email This Issue - 7.1.1.9
- EmailTask - 2.4
- Extension for Jira Service Desk - 6.3.1
- HTTP Request Workflow Function Plugin - 1.6.0
- InTENSO Utils - 2.2.3
- Insight - 5.6.2
- Integrity Check for JIRA - 6.2.1
- Quick Subtasks for JIRA - 4.11.0
- SLA PowerBox - 3.2.0
- Unique Regex Custom Field - 1.2.15
- Workflow Powerbox - 1.2.0
- Xporter - 5.7.2
- eazyBI Reports and Charts for Jira - 4.6.2
- Ultimate Theming for JIRA Service Desk.

Cel realizacji fazy: Zapewnienie środowiska o wystarczającej wydajności i odpowiednim utrzymaniu w zakresie realizacji podstawowych procesów OSE, ze szczególnym uwzględnieniem procesu pozyskania i podłączania szkół.

Uwaga: Dopuszczalne jest wdrożenie rozwiązania równoważnego, czyli zamiast użycia kopii systemów JIRA Wykonawca dostarczy rozwiązanie własne - w tym przypadku musi zapewnić tą samą integrację i te same funkcjonalności

Zakres wymagań stawianych Wykonawcy oraz wymaganej funkcjonalności, która musi być wdrożony w Fazie 1 jest przedstawiony w tabeli poniżej.

Identyfikator wymagania	Treść wymagania
O52.F1	Wymagana jest migracja do nowej platformy definicji wszystkich procesów OSE zaimplementowanych w systemach OSE NASK do momentu uruchamiania systemów Jira WF i Jira SD na nowej platformie

Identyfikator wymagania	Treść wymagania
O52.F2	<p>Wymagane jest przeniesienie do nowej platformy wszelkich specyficznych dla systemów Jira ustawień , konfiguracji, plug-in'ów itp. zaimplementowanych w systemach OSE NASK do momentu uruchamiania systemów Jira WF i Jira SD na nowej platformie, w szczególności:</p> <ul style="list-style-type: none"> - dashboardy, - filtry - grupy i profile użytkowników <p>Lub odwzorowanie ich w systemach równoważny, jeżeli dostawca wdroży od razu docelowe systemy</p>
O52.F3	<p>Wymagana jest migracja z obecnych systemów OSE NASK do wdrażanego przez Wykonawcę systemu Jira Insight (lub równoważnego w rozwiązaniu wykonawcy systemu) co najmniej następujących danych ewidencyjnych (mogą dojść nowe elementy nieznane w momencie ogłoszenia niniejszego postępowania zakupowego):</p> <ul style="list-style-type: none"> - bazę typów urządzeń - baza węzłów OSE i PWR - cenniki prac podwykonawców - baza łącz agregacyjnych i szkieletowych - baza urządzeń fizycznych CPE, SW, AP (dostarczana przez dostawcę sprzętu lub beneficjenta POPC) - lista (słownik) statusów szkół - bazę profili monitorowania w Zabbix
O52.F4	<p>Część danych ewidencyjnych - co najmniej te, co podane poniżej są zaciągane on-line'owym mechanizmem z systemu NASK sugarCRM do Jira Insight (lub równoważnego w rozwiązaniu wykonawcy systemu):</p> <ul style="list-style-type: none"> - baza szkół - baza lokalizacji szkolnych - baza kontaktów do szkół i partnerów OSE - szanse i pozycje szansy - umowy przychodowe - umowy z partnerami OSE <p>W związku z powyższym zaimplementowany przez Wykonawcę system Jira Insight musi być zintegrowany z systemem sugarCRM i też pobierać te same dane ewidencyjne</p>
O52.F5	<p>Wymagana jest instalacja JIRA WF, JIRA SD (w tym portal SD) i JIRA Insight w środowisku OSS/BSS na infrastrukturze chmurowej dostarczonej w ramach niniejszego postępowania zakupowego lub systemów równoważnych dostarczanych przez wykonawcę. Dostosowanie systemów równoważnych do pozostałej części architektury jest po stronie wykonawcy (należy zapewnić ten sam zakres funkcjonalności, jaki jest realizowany w systemach przejściowych).</p>
O52.F6	<p>Zapewnienie właściwych wersji i licencji do instalowanych systemów JIRA jest w odpowiedzialności Wykonawcy. Na dzień ogłoszenia zapytania wersje systemów oraz lista plug-in i ich wersji są następujące:</p> <p>Jira ver. 7.12.1</p> <p>JIRA Service Desk Application v3.15.1</p> <p>AM Utils - 1.3.19</p> <p>Actions for JIRA Service Desk - 1.3.29</p> <p>Adaptavist ScriptRunner for JIRA - 5.4.34</p> <p>Automated Attachments - 1.3.0</p>

Identyfikator wymagania	Treść wymagania
	<p>BigGantt - 3.13.4-jira7</p> <p>Bob Swift Atlassian Add-ons - Create on Transition - 7.1.0</p> <p>Calendar (CoreSoft Labs Commons) - 1.1.1</p> <p>Easy Links for JIRA - 1.4.5</p> <p>Email This Issue - 7.1.1.9</p> <p>EmailTask - 2.4</p> <p>Extension for Jira Service Desk - 6.3.1</p> <p>HTTP Request Workflow Function Plugin - 1.6.0</p> <p>InTENSO Utils - 2.2.3</p> <p>Insight - 5.6.2</p> <p>Integrity Check for JIRA - 6.2.1</p> <p>Quick Subtasks for JIRA - 4.11.0</p> <p>SLA PowerBox - 3.2.0</p> <p>Unique Regex Custom Field - 1.2.15</p> <p>Workflow Powerbox - 1.2.0</p> <p>Xporter - 5.7.2</p> <p>eazyBI Reports and Charts for Jira - 4.6.2</p> <p>Ultimate Theming for JIRA Service Desk</p> <p>W przypadku gdy do momentu wdrożenia znajdą zmiany w ww. liście Wykonawca zapewni licencje zgodne z aktualną na dzień wdrożenia listą.</p>
O52.F7	<p>Należy zapewnić takie same integracje dla implementowanych kopii aplikacji JIRA WF, JIRA SD (w tym SD portal) i JIRA Insight do integracji w obecnych systemach JIRA w OSE NASK tak aby realizacja procesów zaimplementowanych w tych systemach przebiegała tak samo jak w środowisku źródłowym. Wszystkie trzy systemy Jira muszą być również ze sobą nawzajem zintegrowane (analogicznie jak w systemach OSE NASK). Wszelkie istniejące skrypty integrujące ww. elementy będą udostępnione przez Zamawiającego celem ich przeniesienia na nowe środowisko. W przypadku wdrożenia rozwiązania równoważnego na systemach wykonawcy, po stronie Wykonawcy znajduje się odpowiedzialność na odzwierciedlenie konfiguracji i integracji w systemach równoważnych.</p>
O52.F8	<p>Systemy Jira WF, Jira SD i Jira Insight (lub systemy równoważne) muszą mieć analogicznie jak tożsame systemy Jira w OSE NASK przygotowany interfejs API do wystawiania danych systemom trzecim, co najmniej:</p> <ul style="list-style-type: none"> - dla Portalu Usługowego / Portalu OSE (baza szkół i ich statusy podłączenia, użytkownicy, usługi, zgłoszenia) - dla raportów excelowych, innych OSE NASK - dla systemu Reporting Services NASK PIB
O52.F9	<p>Zaimplementowana kopia Jira WF (lub systemy równoważne) musi, co najmniej zapewniać integrację z podanymi poniżej systemami NASK (lista tych integracji może ulec zmianie od momentu ogłoszenia niniejszego postępowania:</p> <ul style="list-style-type: none"> - Portal OSE / Portal Usługowy (REST API, generowane raporty JSON) - Provisioning (w tym Rconfig) - systemem poczty elektronicznej NASK - na poziomie procesowej z Arche, SOD, EMID
O52.F10	<p>Zaimplementowana kopia Jira SD (w tym portal Insight) - lub systemy równoważne - musi zapewniać integrację co najmniej z podanymi poniżej systemami NASK (lista tych integracji może</p>

Identyfikator wymagania	Treść wymagania
	ulec zmianie od momentu ogłoszenia niniejszego postępowania: - Provisioning (w tym Rconfig)
O52.F11	Zaimplementowana kopia Jira Insight (lub systemy równoważne) musi zapewniać integrację co najmniej z podanymi poniżej systemami NASK (lista tych integracji może ulec zmianie od momentu ogłoszenia niniejszego postępowania): - sugarCRM - Portal OSE (w szczególności dla synchronizacji danych szkół i kontaktów) - Provisioning (w tym rConfig)
O52.F12	Wykonawca zapewni rozbudowę zasobów infrastrukturalnych dostarczonych w poprzedniej fazie, aby zapewnić wystarczającą wydajność systemów w zakresie realizowanych procesów przy zakładanych parametrach wydajnościowych.
O52.F13	Użytkownicy systemów Jira WF, Jira SD i Jira Insight (lub systemów równoważnych) muszą być identyczni jak w tożsamy systemach w OSE NASK, zatem autoryzacja i uwierzytelnianie użytkowników w tych systemach musi zachodzić w oparciu o NASK AD (Active Directory).
O52.F14	Użytkownicy Jira SD od strony Podwykonawcy lub innych partnerów OSE (niebędący zewidencjonowani w NASK AD) muszą zostać stworzeni również w nowym stosie Jira implementowanym przez Wykonawcę
O52.F15	Wszelkie zmiany funkcjonalne nanoszone w źródłowych systemach Jira WF, Jira SD i Jira Insight w OSE NASK muszą być przez Wykonawcę zaimplementowane w nowym stack'u Jira (po zgłoszeniu przez Zamawiającego) (lub w systemach równoważnych)
O52.F16	Wykonawca zapewni również przeniesienie kopii środowiska testowego systemów Jira WF, Jira SD, Jira Insight (lub systemów równoważnych) na nową infrastrukturę obliczeniową. Systemy z tego środowiska muszą być zintegrowane z testowym środowiskiem Portalu OSE i testowym środowiskiem systemu sugarCRM
O52.F17	Systemy Jira SD, Jira SD i Jira Insight (lub systemy równoważne) muszą zostać zaimplementowane w takiej architekturze, aby zapewnić wysoką dostępność i systemów
O52.F18	Systemy Jira SD, Jira SD i Jira Insight (lub systemy równoważne) muszą zostać zaimplementowane w takiej architekturze, aby zapewnić wysoką wydajność procesów biznesowych - należy założyć, że w okresach szczytu do OSE podłączanych będzie 200 szkół dziennie, czyli należy przewidzieć odpowiednią wielkość obciążenia procesów "pozyskania szkoły", "podłączenia szkoły" i "zamawiania łącz".
O52.F19	Wykonawca zrealizuje migrację wstrzymanych procesów pozyskania (wstrzymanych z uwagi na przekroczenie limitu podłączenia). Migracja będzie dotyczyć wyłącznie procesów, które zostały wstrzymane na ostatnim kroku procesu pozyskania. Jeżeli proces będzie się znajdował w innym kroku to najpierw musi on zostać dokończony w przejściowych systemach, a dopiero wtedy będzie mógł zostać zmigrowany.
O52.F20	Wykonawca wdroży Portal Usługowy realizujący integrację zarówno z systemami przejściowymi jak i docelowymi. W momencie wdrożenia musi on zapewniać następujące funkcjonalności: - rejestracja szkół (na bazie istniejącej w Portalu OSE funkcjonalności) wraz z kierowaniem rejestracji do właściwej grupy systemów; - logowanie użytkowników szkolnych - umożliwiając przejście do części dostępnej dla

Identyfikator wymagania	Treść wymagania
	<p>zalogowanych użytkowników osobom posiadającym uprawnienia;</p> <ul style="list-style-type: none"> - wyświetlanie usług - prezentacja stanu i parametrów usług posiadanych przez szkołę, do której jest przypisany zalogowany użytkownik; - obsługa zgłoszeń - funkcjonalność dostępna dla zalogowanych użytkowników umożliwiającą zarządzanie zgłoszeniami (awarie, incydenty bezpieczeństwa, konsultacje itp.) do operatora OSE; - routing komunikacji do właściwej JIRY (przejściowej lub docelowej);
O52.F21	Wykonawca wdroży wspólny widok na środowiska przejściowe i docelowe umożliwiający użytkownikom biznesowym na operowanie / prezentowanie danych z obu środowisk na jednym ekranie (użytkownikom zarówno z centrum kontaktu, utrzymania, DRP jak również jeden wspólny widok dla parterów serwisowych na JIRA SD). Wspólny widok zapewnia jedno wejście do obu środowisk, chociaż operacje biznesowe będą już realizowane we właściwej grupie systemów. Wspólny widok powinien zapewnić możliwość wyszukiwania szkół i spraw w obu instancjach systemu Jira (przejmowanej w operacje przez Wykonawcę oraz już istniejącej w środowisku Zamawiającego) i prezentowania, jako jednej listy wyszukiwania.
O52.F22	Wykonawca wdroży funkcjonalność do łączenia raportów (lub danych eksportowanych) pochodzących z obu środowisk (przejściowego i docelowego) tak, aby na wyjściu otrzymywać jeden spójny raport łączący dane z obu środowisk. Wymaganie dotyczy również łączenia eksportów danych wykorzystywanych przez systemy spoza rozwiązania (np. Call Center).
O52.F23	Wykonawca wdroży do środowiska docelowego provisioning dla sieci szkolnej wykorzystując kopie systemów przejściowych (provisioning, RConfig)
O52.F24	Wykonawca zapewni wsparcie (merytoryczne i administracyjne) przy przenoszeniu Portalu OSE z infrastruktury NASK na infrastrukturę Wykonawcy.
O52.F25	Wykonawca zainstaluje plugin lub moduł SSO przeznaczony dla utrzymania sesji użytkownika między różnymi instancjami systemu JIRA i wykona prace integracyjne między nową instancją systemu Jira a instancją istniejącą w środowisku Zamawiającego. Moduł powinien zapewniać jednokrotne logowanie użytkownika niezależnie, z której instancji systemu on korzysta i utrzymanie sesji użytkownika bez konieczności ponownego logowania przy przełączaniu widoku lub przełączenia instancji systemu. Nie jest wymagane, aby ten moduł SSO obsługiwał nowy stos BSS i OSS, gdzie powinien zostać zapewniony docelowy moduł SSO.
O52.F26	Wdrożone w fazie 1 rozwiązanie musi zostać zintegrowane z istniejącym systemem Contact Center. Integracja systemów zostanie zrealizowana w taki sam sposób jak systemów przejściowych. W ramach prac należy również zapewnić agregację raportów zasilających usługę Contact Center. Routing komunikacji do właściwych systemów (przejściowych lub docelowych) znajduje się w odpowiedzialności dostawcy usługi Contact Center (poza przetargiem).
O52.F27	Wykonawca zapewni wsparcie (merytoryczne i administracyjne) przy przenoszeniu systemu do zarządzania budżetem (wydatkami) z infrastruktury NASK na infrastrukturę Wykonawcy. System wdrażany w oddzielnym postępowaniu.
O52.F28	Wykonawca wdroży Aktywator - komponent z obszaru OSS umożliwiający provisioning usług na urządzeniach sieci szkieletowej (zarówno w zakresie urządzeń sieciowych jak i urządzeń bezpieczeństwa) umożliwiający pełną aktywację usług. Ostateczny termin wdrożenia funkcjonalności zostanie ustalony przez strony (jednakże nie później niż 1 miesiąc po poprzedniej fazie).

Identyfikator wymagania	Treść wymagania
O52.F29	<p>Wykonawca wdroży obsługę Usług Bezpieczeństwa na Portalu Usługowym (wyświetlanie alertów, raportów), zapewniający następujące funkcjonalności:</p> <p>dla usługi "Ochrona przed szkodliwym oprogramowaniem"</p> <ul style="list-style-type: none"> - Włączanie ochrony dla Poczty elektronicznej - Włączanie ochrony dla Pobierania plików z sieci Internet - Tworzenie białej listy: URLe nieblokowane - Ustalenie poziomu alarmowania <p>dla usługi "Ochrona użytkownika OSE"</p> <ul style="list-style-type: none"> - Wybór listy kategorii blokowanych treści, - Tworzenie białej listy: URLe nieblokowane, - Tworzenie czarnej listy: URLe blokowane, - Tworzenie białej listy dla aplikacji mobilnych (wybór z listy), - Decyzja o analizie ruchu pocztowego (blokada, ochrona, brak kontroli), - Ustalenie poziomu alarmowania. - alarmy (raporty ze zdarzeń wskazujących na niepokojące zjawiska w szkole) - statystyki (statyczne informacje o sposobie wykorzystania Internetu)
O52.F30	Wykonawca wdroży funkcjonalność modyfikacji usług na Portalu Usługowym, czyli możliwość zmiany parametrów i stanu usług posiadanych przez szkołę.
O52.F31	Wykonawca zobowiązuje się do wykonania tej fazy i projektu całego Rozwiązania zgodnie z harmonogramem przedstawionym w tabeli Załącznika nr 5 do Umowy.
O52.F32	Kontent w portalu usługowym musi spełniać kryteria dostępności WCAG 2.0 ("Web Content Accessibility Guidelines", czyli wytyczne dotyczące dostępności treści internetowych) na poziomie AA zgodności z wytycznymi

7.12.3. Zakres prac dla Fazy 2

Faza 2 obejmuje wdrożenie Systemów OSS, rozpoczęcie monitoringu docelowej sieci OSE, integrację ich z systemem BSS - Jira OSE, przejęcie funkcjonalności Inventory (rezygnacja z tej funkcjonalności w BSS Jira OSE) oraz uruchomienie pełnego provisioningu - zarówno szkieletu jak i urządzeń w szkole (rezygnacja z provisioningu systemów przejściowych OSE NASK), przeprowadzenie instruktaży i integracje z kolejnymi systemami wskazanymi przez Zamawiającego. W przypadku, gdy wcześniej rozwiązanie w obszarze infrastruktury bazowało na zasobach własnych wykonawcy wdroży infrastrukturę chmurową zgodnie z docelowymi wymaganiami w ramach kolokacji OSE.

Cel realizacji fazy: Zapewnienie odpowiednio wydajnego środowiska realizującego wszystkie podstawowe funkcjonalności związane z zarządzaniem usługami ściśle zintegrowanego z docelową siecią OSE i w pełni zautomatyzowanego.

Uwaga: Dopuszczalne jest wdrożenie rozwiązania równoważnego, czyli zamiast użycia kopii systemów JIRA Wykonawca dostarczy rozwiązanie własne - w tym przypadku musi zapewnić tą samą integrację i te same funkcjonalności.

Zakres wymagań stawianych Wykonawcy oraz wymaganej funkcjonalności, która musi być wdrożony w Fazy 2 jest przedstawiony w tabeli poniżej.

Identyfikator wymagania	Treść wymagania
O53.F1	Wykonawca zaimplementuje systemy OSS zgodnie z wymaganiami dla obszaru OSS bez rozwiązań dotyczących telemetrii. Telemetria może zostać wdrożona w tej fazie, ale nie jest obowiązkowa. Wykonawca jest zobowiązany do zapewnienia spójności rozwiązania zależnie od przyjętego harmonogramu wdrożenia telemetrii.
O53.F2	Wymagana jest od Wykonawcy realizacja Systemów OSS (w tym funkcjonalności Fault & Perforamce Management, Config Management & Provisioning, Inventory), które będą zintegrowane z Jira WF i Jira SD (lub równoważnym wdrożonym przez wykonawcę rozwiązaniem) w taki sposób by zapewnić realizację wszystkich wymagań zdefiniowanych dla obszaru OSS.
O53.F3	Wymagane jest przełączenie procesu provisioningu dla systemów Jira WF i Jira SD (lub równoważnych wdrożonych przez wykonawcę systemów) na docelowy obszar OSS odłączając go jednocześnie od systemu provisioningu w obszarze Systemów OSE NASK.
O53.F4	Wymagana jest migracja danych z systemu Jira Insight (między innymi niezbędnych do realizacji procesów biznesowych) do komponentów obszaru Inventory Systemów OSS.
O53.F5	Komponent zapewniający funkcjonalność Inventory implementowany w ramach wdrożenia Systemów OSS musi przejąć zadania, jakie pełnił system Jira Insight i musi zostać zintegrowany z systemami Jira WF i Jira SD (lub równoważnych wdrożonych przez wykonawcę systemów)
O53.F6	Komponent zapewniający funkcjonalność Provisioningu implementowany w ramach wdrożenia Systemów OSS musi przejąć zadania, jakie pełnił system Provisioningu obszaru OSE NASK i musi zostać zintegrowany z systemami Jira WF i Jira SD (lub równoważnych wdrożonych przez wykonawcę systemów)
O53.F7	Komponent zapewniający funkcjonalność Config Management implementowany w ramach wdrożenia Systemów OSS musi przejąć zadania, jakie pełnił system rconfig obszaru OSE NASK i musi zostać zintegrowany z systemami Jira WF i Jira SD (lub równoważnych wdrożonych przez wykonawcę systemów)
O53.F8	Wymagana jest z migracja danych z systemu rConfig do komponentu zapewniającego funkcjonalność Config Management w obszarze Systemów OSS celem uzupełnienia informacji historycznych na temat konfiguracji i oprogramowania monitorowanych urządzeń
O53.F9	Komponent zapewniający funkcjonalność Inventory implementowany w ramach wdrożenia Systemów OSS musi mieć przygotowany interface API do wystawiania danych systemom trzecim, co najmniej: - dla Portalu OSE / Portalu Usługowego(baza szkół i ich statusy podłączenia, użytkownicy, usługi, zgłoszenia, inne) - dla raportów excelowych, innych OSE NASK - dla systemu Reporting Services NASK PIB Musi zostać dokonane stosowne dopasowanie sposobu wystawiania danych i ich formatów danych lub przygotowanie nowej integracji tak by proces raportowania nie został zaburzony
O53.F10	Komponent zapewniający funkcjonalność Inventory implementowany w ramach wdrożenia Systemów OSS musi zapewniać integrację co najmniej z podanymi poniżej systemami NASK (lista tych integracji może ulec zmianie od momentu ogłoszenia postępowania zakupowego):

Identyfikator wymagania	Treść wymagania
	<ul style="list-style-type: none"> - sugarCRM - Portal OSE / Portal Usługowy (w szczególności dla synchronizacji danych szkół i kontaktów)
O53.F11	W komponencie zapewniającym funkcjonalność Inwentary w ramach wdrożenia Systemów OSS muszą istnieć analogiczni użytkownicy jak w systemie Jira Insight OSE NASK, z tym, że autoryzacja i uwierzytelnianie użytkowników w docelowym systemie OSS musi zachodzić w oparciu o zaimplementowany w Rozwiązaniu mechanizm SSO (Single Sign On).
O53.F12	Wszelkie zmiany funkcjonalne nanoszone w źródłowych systemach Jira WF, Jira SD w OSE NASK i zgłaszane przez Zamawiającego muszą być przez Wykonawcę implementowane w nowym stack'u Jira na docelowej infrastrukturze OSE.
O53.F13	Wykonawca musi uruchomić środowisko testowe dla systemów z obszaru OSS
O53.F14	Testowe środowisko systemów z obszaru OSS musi zostać uruchomione i zintegrowane z testowym środowiskiem Portalu OSE i testowym środowiskiem systemu sugarCRM
O53.F15	<p>W ramach wdrożenia w Fazie 2 Wykonawca musi przeprowadzić wszystkie niezbędne integracje opisane w wymaganiach dotyczących integracji z systemami zewnętrznymi z obszaru OSS. Są w nich co najmniej integracje z :</p> <ul style="list-style-type: none"> - Element Managerami sieci - Element Managerami systemów bezpieczeństwa - systemem SIEM (zawiera w sobie zbieranie logów bezpieczeństwa, logów do retencji i netflow) - systemem zarządzania środowiskiem kolokacyjnym
O53.F16	Przełączenie architektury - podłączenie nowych komponentów i migracja danych z dotychczasowych do docelowych systemów musi zostać wykonana poza godzinami pracy szkół. Całość prac musi być zrealizowana w ramach jednego przełączenia z oknem serwisowym nie dłuższym niż 8 godzin.
O53.F17	Podłączenie systemów obszaru OSS do JIRA WF i JIRA SD (lub równoważnych wdrożonych przez wykonawcę systemów) nie może pogorszyć wydajności tych systemów. Po stronie wykonawcy jest odpowiednie zabezpieczenie zasobów infrastrukturalnych, aby użytkownicy biznesowi nie odczuli pogorszenia wydajności systemów przetwarzających zlecenia / zamówienia / zgłoszenia.
O53.F18	Wykonawca zobowiązany jest za przygotowanie i zapewnienie planu awaryjnego, dla sytuacji niepoprawnego działania środowiska po włączeniu nowych systemów obszaru OSS i migracji danych. W ramach procedury rollback należy przywrócić środowisko do stanu przed rozpoczęcia wdrożenia.
O53.F19	Wykonawca zaktualizuje w razie potrzeby rozwiązanie do łączenia raportów z obu grup systemów (docelowych i przejściowych)
O53.F20	Wykonawca zaktualizuje w razie potrzeby wspólny widok na środowiska przejściowe i docelowe umożliwiający użytkownikom biznesowym na operowanie danych z obu środowisk na jednym ekranie.
O53.F21	Wykonawca musi uruchomić funkcjonalność SSO w zakresie systemów OSS
O53.F22	Jeżeli wcześniej rozwiązanie było zrealizowane w oparciu o tymczasową infrastrukturę Wykonawcy to musi on wdrożyć infrastrukturę chmurową zgodnie z docelowymi wymaganiami w lokalizacjach Zamawiającego oraz przenieść systemy z rozwiązania tymczasowego na

Identyfikator wymagania	Treść wymagania
	docelową infrastrukturę, co najmniej w zakresie systemów NASK OSE (systemy OSE inne niż OSS/BSS) oraz systemu OSS.
O53.F23	Wykonawca zobowiązuje się do wykonania tej fazy i projektu całego Rozwiązania zgodnie z harmonogramem przedstawionym w tabeli Załącznika nr 5 do Umowy.

7.12.4. Zakres prac dla Fazy 3

Faza 3 obejmuje wdrożenie pełnej funkcjonalności systemów BSS oraz ich integrację z systemami OSS, wdrożenie pełnej funkcjonalności Portalu Usługowego oraz jego przełączenie na systemy BSS, wdrożenie pozostałych wyspecyfikowanych procesów biznesowych. Dodatkowo w ramach w zakresie tej fazy znajduje się przeprowadzenie instruktaży i integracje z systemami wskazanymi przez Zamawiającego. Po wdrożeniu produkcyjnym zakresu z Fazy 3 Wykonawca rozpocznie utrzymanie wdrożonego środowiska. W ramach tej fazy Wykonawca jest zobowiązany do wdrożenia Systemów OSS/BSS zgodnie z wymaganiami przedstawionymi w tabeli poniżej.

Cel realizacji fazy: zapewnienie zautomatyzowane zintegrowanego środowiska (docelowe rozwiązanie) realizującego wszystkie wymagane funkcjonalności.

Zakres wymagań stawianych Wykonawcy oraz wymaganej funkcjonalności, która musi być wdrożony w Fазie 3 jest przedstawiony w tabeli poniżej.

Identyfikator wymagania	Treść wymagania
O54.F1	Wykonawca zaimplementuje docelowe systemy BSS zgodnie z wymaganiami dla obszaru BSS i zintegruje je z systemami OSS tak, aby Rozwiązanie spełniało wymagania dla obszarów OSS, BSS i wspólnych dla całego Rozwiązania.
O54.F2	Wymagana jest migracja danych niezbędnych do obsługi klientów i wszystkich procesów biznesowych z systemów Jira WF i SD (na nowej infrastrukturze OSE) obsługiwanych w tych systemach od Fazy 1 wdrożenia do docelowych systemów BSS.
O54.F3	Wymagana jest migracja danych obszaru zarządzania relacjami z klientem z systemu sugarCRM OSE NASK (obsługiwanych w tym systemie do Fazy 3 wdrożenia) do obszaru CRM docelowych systemów BSS
O54.F4	W ramach wdrożenia Fazy 3 Wykonawca musi przeprowadzić wszystkie niezbędne integracje opisane w wymaganiach dotyczących integracji z systemami zewnętrznymi Zamawiającego z obszaru BSS. Są w nich co najmniej następujące integracje : - integracja z Portalem OSE - integracja z systemem finansowo-księgowym Tetą - integracja z systemem magazynowym Emidem - integracja z systemem sugarCRM - integracja z Reporting Services - integracja z systemem AD - integracja z systemem pocztowym
O54.F5	Wykonawca musi uruchomić środowisko testowe dla systemów z obszaru BSS

Identyfikator wymagania	Treść wymagania
O54.F6	Wykonawca musi uruchomić funkcjonalność SSO w zakresie systemów BSS
O54.F7	Przełączenie architektury - podłączenie nowych komponentów i migracja danych z dotychczasowych do docelowych systemów musi zostać wykonana poza godzinami pracy szkół. Całość prac musi być zrealizowana w ramach jednego przełączenia z oknem serwisowym nie dłuższym niż 8 godzin.
O54.F8	Podłączenie systemów obszaru BSS do pozostałych systemów środowiska nie może pogorszyć wydajności tych systemów. Po stronie wykonawcy jest odpowiednie zabezpieczenie zasobów infrastrukturalnych, aby użytkownicy biznesowi nie odczuli pogorszenia wydajności systemów przetwarzających zlecenia / zamówienia / zgłoszenia.
O54.F9	Wykonawca zobowiązany jest za przygotowanie i zapewnienie planu awaryjnego, dla sytuacji niepoprawnego działania środowiska po włączeniu nowych systemów obszaru BSS i migracji danych. W ramach procedury rollback należy przywrócić środowisko do stanu przed rozpoczęcia wdrożenia.
O54.F10	Migracja dotyczy zarówno przeniesienia danych pomiędzy systemami jak również aktualizacji danych wewnątrz systemów (bez przenoszenia danych), czyli migracji wewnętrznej
O54.F11	W odpowiedzialności dostawcy znajduje się aktualizacja danych w systemach obszaru OSS, jeżeli takie działanie jest niezbędne do poprawnego działania całości architektury po podłączeniu BSS i migracji danych do BSS
O54.F12	W zakresie prac migracyjnych jest również wyłączenie systemów nieistniejących w architekturze docelowej i nierealizujących zadań na inne potrzeby
O54.F13	Wszelkie procesy, sprawy, zamówienia w trakcie (tzw. otwarte procesy) muszą również zostać zmigrowane
O54.F14	Muszą zostać zmigrowane wszelkie dane operacyjne / bieżące. W zakresie danych historycznych niezbędne jest pełne zmigrowanie danych związanych z rozliczeniami z klientami / partnerami oraz spraw / reklamacji.
O54.F15	Wymagana jest pełna migracja historycznych zamówień.
O54.F16	Rozwiązanie migracyjne musi zawierać możliwość wycofania (rollback) migracji bez wpływu na dane klientów niemigrowanych.
O54.F17	Wymagane jest przechowanie historii wszelkich zmian realizowanych w ramach migracji wewnętrznych (w ramach systemu)
O54.F18	Wykonawca w ramach swoich prac przeprowadzi warsztaty analizy biznesowej dla wszystkich zdefiniowanych procesów, jakie nie zostały wdrożone we wcześniejszych fazach. W ramach warsztatów przygotuje definicję / przebieg procesów biznesowych oraz konfigurację dla tych procesów. Na podstawie wyników warsztatów biznesowych wykonawca wdroży procesy do docelowych systemów OSS/BSS.
O54.F19	Wykonawca wdroży na Portalu Usługowym wszystkie brakujące funkcjonalności wyspecyfikowane w Opisie Przedmiotu Zamówienia a niedostarczone wcześniej

Identyfikator wymagania	Treść wymagania
O54.F20	Wykonawca zaktualizuje w razie potrzeby rozwiązanie do łączenia raportów z obu grup systemów (docelowych i przejściowych)
O54.F21	Wykonawca usunie / wyłączy wspólny widok na środowiska przejściowe i docelowe umożliwiające użytkownikom biznesowym na operowanie danych z obu środowisk na jednym ekranie.
O54.F22	Telemetria, jeżeli nie została wdrożona wcześniej może zostać wdrożona w tej fazie, ale nie jest to obowiązkowe. Wykonawca jest zobowiązany do zapewnienia spójności rozwiązania zależnie od przyjętego harmonogramu wdrożenia telemetrii.
O54.F23	Wykonawca wdroży docelowe rozwiązanie w obszarze Contact Center zastępując istniejące obecnie w formie usługi (Alfavox). W ramach wdrożenia dostawca również zapewni obsługę systemów przejściowych przez docelowe rozwiązanie Contact Center (w tym odpowiedni routing komunikacji - zależnie od kontaktującego się klienta musi nastąpić przekierowanie do systemów przejściowych lub docelowych).
O54.F24	Wykonawca musi przeprowadzić migrację danych z obecnego systemu Contact Center (Alfavox) OSE NASK (świadczonego dla OSE w postaci usługi) do obszaru Contact Center w docelowych systemach BSS. W ramach migracji powinny być przeniesione następujące dane: <ul style="list-style-type: none"> - Nagrania razem z metadanymi - Historia kontaktów - Bilingi połączeń - Struktury odpowiedzi - Drzewa IVR - Odpowiedzi skryptów - Dane raportowe - Aktywności agentów - Użytkownicy wraz ze strukturą uprawnień - Zgłoszenia, historia zgłoszeń
O54.F25	Migracja danych Contact Center wykorzystywanych operacyjnie (bieżących) musi zostać zrealizowana w ramach wdrożenia fazy 3. Dane historyczne (nagrania, historia rozmów itp..) mogą zostać zmigrowane w ramach prac okresu stabilizacyjnego, jednakże nie później niż w przeciągu 2 tygodni od zakończenia wdrożenia i musi być realizowane bez wpływu na bieżące działanie systemów
O54.F26	Wdrożenie systemu BSS musi zostać zrealizowane w oparciu docelową infrastrukturę serwerowo-chmurową.
O54.F27	Wykonawca zobowiązuje się do wykonania tej fazy i projektu całego Rozwiązania zgodnie z harmonogramem przedstawionym w tabeli Załącznika nr 5 do Umowy.
O54.F28	Wykonawca w ramach swoich prac przeprowadzi warsztaty analizy biznesowej dla wszystkich procesów wdrożonych we wcześniejszych fazach. W ramach warsztatów przygotuje optymalizację przebiegów procesów biznesowych i konfiguracji oraz zapewni dostosowanie procesów do docelowej architektury OSS/BSS. Na podstawie wyników warsztatów biznesowych wykonawca zaktualizuje wdrożone procesy biznesowe oraz dokona migracji danych w zmigrowanych procesach.

7.12.5. Zakres prac dla Fazy 4

Faza 4 obejmuje migrację klientów z systemów przejściowych OSE NASK do docelowego Rozwiązania. Migracje te mogą dotyczyć zarówno obszaru OSS jak i BSS. Po przeprowadzeniu migracji w środowisku produkcyjnym Wykonawca rozpocznie utrzymanie ostatecznie wdrożonego środowiska. Dopuszczalna jest zarówno migracja online (bez wyłączania systemów) jak i migracja fazowa. Odpowiedzialnością wykonawcy jest zaproponowanie podejścia i uzyskanie akceptacji zamawiającego. W ramach tej fazy Wykonawca jest zobowiązany do migracji do Systemów OSS/BSS zgodnie z wymaganiami przedstawionymi w tabeli poniżej.

Cel realizacji fazy: zapewnienie jednego środowiska do obsługi OSE.

Zakres wymagań stawianych Wykonawcy oraz wymaganej funkcjonalności, która musi być wdrożony w Fазie 4 jest przedstawiony w tabeli poniżej.

Identyfikator wymagania	Treść wymagania
O55.F1	Migracja danych musi być realizowana poza godzinami pracy szkół, w godzinach nocnych z oknem serwisowym nie dłuższym niż 8 godzin (nie dotyczy wariantu migracji online)
O55.F2	Minimalna dopuszczalna granulacja migracji dotyczy jednej lokalizacji - wszystkich szkół w danej lokalizacji.
O55.F3	W wyniku migracji docelowe systemy OSS muszą automatycznie wykryć i zacząć monitorować urządzenia w szkole
O55.F4	W wyniku migracji do docelowych systemy BSS muszą trafić dokumenty dotyczące szkoły (umowy, faktury, protokoły itp.) z systemów przejściowych OSE NASK do systemów docelowych BSS
O55.F5	W zakresie migracji do systemów BSS muszą trafić informacje na temat zgłoszeń w procesach pozyskania i podłączenia szkoły, utrzymaniowych i innych dotyczących migrowanej szkoły (niezbędne do prawidłowego raportowania)
O55.F6	W wyniku migracji komponenty realizujących funkcjonalność Inventory muszą zostać odpowiednio uzupełnione danymi związanymi ze szkołą i jej urządzeniami
O55.F7	Wykonawca zobowiązany jest za przygotowanie i zapewnienie planu awaryjnego, dla sytuacji niepoprawnego działania środowiska po migracji danych. W ramach procedury rollback należy przywrócić dane klientów zmigrowanych do stanu sprzed rozpoczęcia migracji bez jakiegokolwiek wpływu na dane klientów niemigrowanych. Procedura rollback może zostać zastosowana do 12h po zakończeniu migracji i włączeniu systemów (jeżeli były wyłączane)
O55.F8	W zakresie prac migracyjnych jest również wyłączenie systemów nieistniejących w architekturze docelowej i nierealizujących zadań na inne potrzeby
O55.F9	Wszelkie procesy, sprawy, zamówienia w trakcie (tzw. otwarte procesy) muszą również zostać zmigrowane

Identyfikator wymagania	Treść wymagania
O55.F10	Muszą zostać zmigrowane wszelkie dane operacyjne / bieżące. W zakresie danych historycznych niezbędne jest pełne zmigrowanie danych związanych z rozliczeniami z klientami / partnerami oraz spraw / reklamacji.
O55.F11	Wymagana jest pełna migracja historycznych zamówień.
O55.F12	W przypadku migracji online niedostępność danych migrowanych klientów nie może trwać więcej niż 1h
O55.F13	Wymagane jest przechowanie historii wszelkich zmian realizowanych w ramach migracji wewnętrznych (w ramach systemu)
O55.F14	Proces migracji nie może w żaden sposób wpływać na dane klientów niemigrowanych
O55.F15	Migracja dotyczy zarówno przeniesieniem danych pomiędzy systemami (z systemów przejściowych do docelowych) jak również aktualizacji danych w systemach pracujących w obu architekturach (przejściowej i docelowej), czyli migracji wewnętrznej
O55.F16	Migracja dotyczy pełnego zakresu danych znajdujących się w systemach przejściowych JIRA SD, JIRA WF, JIRA Insight, które po migracji nie będą dalej funkcjonować w ramach OSE
O55.F17	Migracja dotyczy również przeniesienia niezbędnych danych z systemów, które dalej częściowo będą wspierać OSE (jak Sugar CRM, EMID, Teta, Portal OSE), jeżeli jest to potrzebne do poprawnego działania systemów środowiska OSS/BSS
O55.F18	Migracja danych nie może w żaden sposób negatywnie wpłynąć na wydajność systemów. Po stronie wykonawcy jest ewentualne zapewnienie rozbudowy infrastruktury
O55.F19	W zakresie migracji znajduje się przeniesienie dokumentów z tymczasowego repozytorium dokumentów, z systemów przejściowych do docelowego repozytorium dokumentów. Wszelkie dane szkół, ich usług, umów oraz zmian, jakie były realizowane na tych obiektach, (jeżeli takie informacje znajdują się w systemach).
O55.F20	W zakresie migracji znajduje się również przeniesienie danych związanych z obszarem OSS (ewidencja sieci, usług, monitorowanie usług i wydajności)
O55.F21	Wymagana jest pełna migracja danych dotyczących ruchu w sieci
O55.F22	Wymagana jest pełna migracja danych dotyczących historii zmian na usługach i urządzeniach w sieci
O55.F23	Wykonawca usunie funkcjonalność do łączenia raportów pochodzących z systemów przejściowych i docelowych.
O55.F24	Telemetria, jeżeli nie została wdrożona wcześniej musi zostać wdrożona w tej fazie. Termin wdrożenia zostanie uzgodniony pomiędzy Wykonawcą a Zamawiającym, ale nie później niż 01.12.2019 i nie później niż zakończy się ta faza wdrożenia.. Zamawiający jest zobowiązany do zapewnienia spójności rozwiązania zależnie od przyjętego harmonogramu wdrożenia telemetrii.
O55.F25	Wykonawca zobowiązuje się do wykonania tej fazy i projektu całego Rozwiązania zgodnie z harmonogramem przedstawionym w tabeli Załącznika nr 5 do Umowy.

Identyfikator wymagania	Treść wymagania
O55.F26	Wykonawca w ramach swoich prac przeprowadzi warsztaty analizy biznesowej dla wszystkich procesów, jakie nie zostały wdrożone we wcześniejszych fazach i nie były zdefiniowane. W ramach warsztatów przygotuje definicję / przebieg procesów biznesowych oraz konfigurację dla tych procesów. Na podstawie wyników warsztatów biznesowych wykonawca wdroży procesy do docelowych systemów OSS/BSS.
O55.F27	Wykonawca musi wdrożyć w docelowych systemach BSS zlecone przez Zamawiającego w ramach utrzymania (opisane w załączniku do Umowy "Zakres usług utrzymania") dodatkowe procesy i raporty.

7.12.6. Zakres prac dla Fazy 5

W ramach Fazy 5 Wykonawca ma za zadanie wdrożenie docelowej infrastruktury obliczeniowej dla produkcyjnych systemów sieci, bezpieczeństwa i części oprogramowania OSS (sondy, kolektory) w Węzłach Regionalnych, które nie zostały wdrożone we wcześniejszych Fazach oraz integrację urządzeń i systemów w tych węzłach z systemami OSS.

Identyfikator wymagania	Treść wymagania
O56.F1	Wykonawca musi dostarczyć zwirtualizowaną infrastrukturę obliczeniową na potrzeby systemów bezpieczeństwa, systemów sieci i części oprogramowania OSS (sondy, kolektory) dla każdego Węzła Regionalnego OSE zgodnie z harmonogramem wdrożenia węzłów OSE Zamawiającego
O56.F2	Infrastruktura instalowana w Węzłach Regionalnych musi spełniać docelowe wymagania zawarte w opisie przedmiotu zamówienia w rozdziale "Wymagania ogólne dla warstwy sprzętowej dla serwerów w regionach"
O56.F3	Wykonawca musi przeprowadzić niezbędne prace konfiguracyjne i integracyjne związane z zarządzaniem z poziomu systemu OSS urządzeniami i systemami OSE zainstalowanymi w każdym z Węzłów Regionalnych z osobna
O56.F4	Wykonawca musi przeprowadzić niezbędne prace konfiguracyjne i integracyjne związane z provisioningiem usług na urządzeniach i systemach OSE zainstalowanych w każdym z Węzłów Regionalnych z osobna
O56.F5	Wykonawca zobowiązuje się do wykonania tej fazy i projektu całego Rozwiązania zgodnie z harmonogramem przedstawionym w tabeli Załącznika nr 5 do Umowy.