
 <div> <div>Centrum</div> <div>Informatyki</div> <div>Resortu</div> <div>Finansów</div> </div>	Nazwa jednostki organizacyjnej:		Centrum Informatyki Resortu Finansów	
	Tytuł dokumentu:		WYMAGANIA OGÓLNE DLA BUDOWANYCH SYSTEMÓW UTRZYMYWANYCH W INFRASTRUKTURZE CIRF	
	Wersja dokumentu:	1.0	Obszar IT	TE
	Data opracowania:	24.10.2023	Kod zakresu dokumentu:	RF / AK

**CENTRUM INFORMATYKI  
RESORTU FINANSÓW**

**WYMAGANIA OGÓLNE DLA BUDOWANYCH  
SYSTEMÓW UTRZYMYWANYCH W  
INFRASTRUKTURZE CIRF**

 <div> <div>Centrum</div> <div>Informatyki</div> <div>Resortu</div> <div>Finansów</div> </div>	Nazwa jednostki organizacyjnej:		Centrum Informatyki Resortu Finansów	
	Tytuł dokumentu:		WYMAGANIA OGÓLNE DLA BUDOWANYCH SYSTEMÓW UTRZYMYWANYCH W INFRASTRUKTURZE CIRF	
	Wersja dokumentu:	1.0	Obszar IT	TE
	Data opracowania:	24.10.2023	Kod zakresu dokumentu:	RF / AK


CENTRUM INFORMATYKI RESORTU FINANSÓW			
Dokument	WYMAGANIA OGÓLNE DLA BUDOWANYCH SYSTEMÓW UTRZYMYWANYCH W INFRASTRUKTURZE CIRF		
Sygnatura dokumentu	CIRF-DIT-2023-26		
Właściciel dokumentu	Centrum Informatyki Resortu Finansów		
Autor/Autorzy	Piotr Celiński, Paweł Ciecierski , Bartłomiej Fila, Daniel Goszewski, Daniel Kujawski, Witold Piasecki, Michał Piotrowski, Mateusz Pyrka, Jan Seliga, Marcin Rutkowski, Edyta Tur, Agnieszka Wasiak		
Komórka organizacyjna odpowiedzialna za opracowanie dokumentu	Departament Infrastruktury	akceptacja EZD	
Weryfikacja formalna	Sylvia Redestowicz, starszy specjalista Wydziału Organizacyjnego	akceptacja EZD	
Akceptacja	Marta Wiśniewska, główny specjalista Departament Zarządzania Informatyzacją	akceptacja email	
	Mariusz Kaszyński, Dyrektor Departamentu Infrastruktury	akceptacja EZD	
	Robert Panek, Dyrektor Departamentu Sieci i Monitorowania	akceptacja EZD	
	Robert Krawczyk, Dyrektor Departamentu Data Center i Bezpieczeństwa	akceptacja EZD	
	Rafał Kasprzak, Zastępca Dyrektora Centrum ds. Infrastruktury IT	akceptacja EZD	
	Marek Balcerczyk, Dyrektor Departamentu Systemów i Usług IT	akceptacja EZD	
	Jakub Dąbrowski, Zastępca Dyrektora Centrum ds. Eksploatacji i Usług IT	akceptacja EZD	
Zatwierdzenie (kwalifikowany podpis elektroniczny)	Hubert Gniadowicz Dyrektor Centrum Informatyki Resortu Finansów	Data zatwierdzenia	13 listopada 2023 r.

## Historia zmian

Nr wersji	Data	Opis	Działanie (*)	Rozdziały (**)	Autorzy
1.0	24.10.2023	Nowy dokument opisujący Wymagania Ogólne Dla Budowanych Systemów Utrzymywanych w Infrastrukturze CIRF	N	W	Wasiak Agnieszka, Celiński Piotr


(\*) Działanie: N-Nowy, Z-Zmiana, W-Weryfikacja

(\*\*) Rozdziały: numery rozdziałów lub W-Wszystkie

 <b>Centrum Informatyki Resortu Finansów</b>	Nazwa jednostki organizacyjnej:		Centrum Informatyki Resortu Finansów	
	Tytuł dokumentu:		WYMAGANIA OGÓLNE DLA BUDOWANYCH SYSTEMÓW UTRZYMYWANYCH W INFRASTRUKTURZE CIRF	
	Wersja dokumentu:	1.0	Obszar IT	TE
	Data opracowania:	24.10.2023	Kod zakresu dokumentu:	RF / AK


## SPIS TREŚCI

<b>1</b>	<b>Definicje .....</b>	<b>4</b>
<b>2</b>	<b>Cel dokumentu .....</b>	<b>5</b>
<b>3</b>	<b>Odpowiedzialność .....</b>	<b>5</b>
<b>4</b>	<b>Zakres, warunki i wyłączenie stosowania .....</b>	<b>5</b>
<b>5</b>	<b>Dokumenty związane .....</b>	<b>5</b>
<b>6</b>	<b>Rola CIRF .....</b>	<b>5</b>
6.1	Ograniczenia w zakresie przydzielanych zasobów .....	6
6.2	Bloki Architektoniczne – wymagania ogólne .....	6
6.3	Systemy składowania danych .....	10
6.4	Definicje środowisk dla systemu .....	11
6.5	Tworzenie i modyfikacja parametrów bloków architektonicznych .....	12
6.6	Ochrona antywirusowa .....	14
6.7	Zarządzanie logami .....	14
6.8	Kopia Zapasowa .....	15
6.9	Zasoby przeznaczone na system – rozliczalność .....	15
6.10	Inne wymagania dla Wykonawców rozwiązań aplikacyjnych na infrastrukturze CIRF .....	16
6.11	Podstawowe standardy sieci .....	16
6.12	Platforma Integracyjna resortu finansów .....	16
6.13	Monitorowanie systemów i usług biznesowych .....	16
<b>7</b>	<b>Wyjątki .....</b>	<b>18</b>
<b>8</b>	<b>Obowiązywanie dokumentu .....</b>	<b>18</b>
8.1.	Wejście w życie dokumentu .....	18
8.2.	Termin obowiązywania .....	18
8.3.	Uregulowania przejściowe .....	18
<b>9</b>	<b>Odwołanie dokumentu .....</b>	<b>18</b>
<b>10</b>	<b>Załączniki .....</b>	<b>18</b>

 <b>Centrum Informatyki Resortu Finansów</b>	Nazwa jednostki organizacyjnej:		Centrum Informatyki Resortu Finansów	
	Tytuł dokumentu:		WYMAGANIA OGÓLNE DLA BUDOWANYCH SYSTEMÓW UTRZYMYWANYCH W INFRASTRUKTURZE CIRF	
	Wersja dokumentu:	1.0	Obszar IT	TE
	Data opracowania:	24.10.2023	Kod zakresu dokumentu:	RF / AK

## 1. Definicje

Pojęcie/skrót	Definicja
<b>ASI</b>	Administrator Systemu Informatycznego – wyznaczony zespół pracowników CIRF posiadający niezbędną wiedzę i uprawnienia do zarządzania Systemem na poziomie aplikacyjnym, funkcjonalnym i biznesowym. Zespół jest odpowiedzialny za koordynację przepływu informacji pomiędzy zespołami technicznymi – infrastrukturalnymi a szeroko rozumianym „Biznesem”
<b>Blok Bazodanowy</b>	Blok architektoniczny dedykowany do udostępniania określonej bazy danych
<b>Blok VA</b>	Blok funkcjonalny składający się z komponentów dostarczonych przez Wykonawcę systemu w postaci Virtual Appliance (maszyna wirtualna z zamkniętą funkcjonalnością)
<b>Bloki Architektoniczne</b>	Grupa maszyn wirtualnych realizująca określoną funkcję w Systemie
<b>CE</b>	Customer Edge – router operatora telekomunikacyjnego znajdujący się w lokalizacji klienta, zarządzany przez operatora
<b>Centralny ServiceDesk (CSD)</b>	Pojedynczy punkt kontaktu między Dostawcą Usług IT a Użytkownikami. Service Desk zarządza Incydentami i Wnioskami oraz obsługuje komunikację z Użytkownikami.
<b>CIRF</b>	Centrum Informatyki Resortu Finansów
<b>CPE</b>	Customer-Provided Equipment – Urządzenie Bezpieczeństwa znajdujące się w lokalizacji klienta i przez niego zarządzane
<b>Dostawca/Wykonawca</b>	Podmiot dostarczający rozwiązanie biznesowe będące kompletnym Systemem. Może to być podmiot AKMF, jak również każdy inny Wykonawca Systemu, który będzie pracował i dostarczał rozwiązanie uruchamiane w infrastrukturze zarządzanej przez CIRF
<b>Farma</b>	Koncepcja architektoniczna umożliwiająca grupowanie serwerów logicznych. Farma składa się z n serwerów logicznych, gdzie n jest zgodne z parametrem Krotność. Bloki architektoniczne, dla których atrybut Grupowanie = Farma muszą zostać objęte mechanizmem farmy zgodnie z przypisaną Krotnością.
<b>Informacja chroniona CIRF</b>	Wszystkie dokumenty zawierające informacje wymagające szczególnej ochrony z punktu widzenia bezpieczeństwa teleinformatycznego infrastruktury CIRF
<b>Karty dopuszczenia systemu do / wycofania systemu z wykorzystania produkcyjnego</b>	To zestaw informacji o systemie, który ma na celu usprawnienie działań związanych z zarządzaniem systemami. Właściciel systemu informatycznego przed jego wdrożeniem, modyfikacją lub całkowitym bądź też częściowym wycofaniem zobowiązany jest do dostarczenia do CIRF wypełnionego dokumentu Karty dopuszczenia systemu do / wycofania systemu z wykorzystania produkcyjnego
<b>Katalog usług</b>	Katalog usług zawiera informacje o dostarczanych produktach, punktach kontaktowych, procedurach składania zamówień i zapotrzebowania
<b>Klaster niezawodnościowy</b>	Oprogramowanie, podnoszące dostępność serwera logicznego, eliminujące pojedynczy punkt awarii. Klaster taki działa w trybie active-passive, tzn. tylko jeden z dwóch serwerów w klastrze jest aktywny w danym momencie. W przypadku awarii jednego węzła inny węzeł w klastrze przejmuje zadania udostępniania usług w ramach procesu zwanego pracą awaryjną (failover). Funkcjonalność klastra niezawodnościowego dla bloków architektonicznych jest realizowana przez mechanizmy wbudowane w systemy operacyjne lub przez komponenty programowe zainstalowane na systemach operacyjnych
<b>Klaster wydajnościowy</b>	Oprogramowanie umożliwiające grupowanie serwerów logicznych w celu zwiększenia mocy obliczeniowej systemu. Klaster wydajnościowy składa się z n serwerów logicznych, gdzie n jest zgodne z parametrem Krotność. Klaster taki działa w trybie active-active, tzn. wszystkie serwery w klastrze są aktywne w danym momencie. Ze względu na brak zewnętrznego fizycznego urządzenia równoważącego ruch oprogramowanie klastra wydajnościowego musi realizować funkcjonalności równoważenia ruchu na wszystkie zgrupowane

 <div> <div>Centrum</div> <div>Informatyki</div> <div>Resortu</div> <div>Finansów</div> </div>	Nazwa jednostki organizacyjnej:		Centrum Informatyki Resortu Finansów	
	Tytuł dokumentu:		WYMAGANIA OGÓLNE DLA BUDOWANYCH SYSTEMÓW UTRZYMYWANYCH W INFRASTRUKTURZE CIRF	
	Wersja dokumentu:	1.0	Obszar IT	TE
	Data opracowania:	24.10.2023	Kod zakresu dokumentu:	RF / AK

	serwery logiczne. Funkcjonalność klastra wydajnościowego dla bloków architektonicznych jest realizowana przez mechanizmy wbudowane w systemy operacyjne lub przez komponenty programowe zainstalowane na systemach operacyjnych
<b>Krotność</b>	Liczba maszyn wirtualnych w bloku architektonicznym
<b>OP</b>	Ośrodek przetwarzania danych, w którym znajdują się serwery z usługami świadczonymi dla pozostałych lokalizacji
<b>OPN</b>	Ośrodek przetwarzania danych w Warszawie (NBP)
<b>OPP</b>	Ośrodek przetwarzania danych w Warszawie (Praga/NASK)
<b>OPR</b>	Ośrodek przetwarzania danych w Radomiu, ul. Samorządowa 1
<b>OPW</b>	Ośrodek przetwarzania danych w Warszawie (MF) – ul. Świętokrzyska 12
<b>PTS/ePTS</b>	Projekt Techniczny Systemu
<b>RF</b>	Resort Finansów
<b>Serwer Aplikacyjny</b>	Blok architektoniczny dedykowany do realizacji określonej funkcjonalności. Zaleca się, by był to komponent bezstanowy
<b>System</b>	Kompletny system realizujący funkcje biznesowe
<b>Środowisko</b>	Zgrupowanie bloków architektonicznych wybranego systemu realizującego określone funkcje biznesowe przeznaczone do działań dla określonej grupy użytkowników, powołany w konkretnych celach
<b>Urządzenia Bezpieczeństwa</b>	Urządzenia sieciowe zapewniające bezpieczną komunikację w sieci WAN RF
<b>WAN</b>	Rozległa sieć komputerowa łącząca lokalizacje RF rozproszone na terenie kraju
<b>WAN RF</b>	Sieć WAN Resortu Finansów
<b>Właściciel Biznesowy</b>	Organ, który jest głównym interesariuszem i inicjatorem dla pracującego Systemu. Właściciel jest odpowiedzialny za zapewnienie finansowania dla wytworzenia i utrzymania Systemu

## 2. Cel dokumentu

Celem standardu jest przedstawienie, w formie uproszczonej informacji dotyczących budowy systemów na podstawie dostarczanych przez CIRF bloków architektonicznych.

## 3. Odpowiedzialność


Za zastosowanie niniejszych wymagań odpowiedzialni są właściciele biznesowi, ASI oraz dostawcy systemów biznesowych pracujących w infrastrukturze utrzymywanej przez CIRF.

## 4. Zakres, warunki i wyłączenie stosowania

Dokument stosuje się w przypadku budowy lub rozbudowy Systemów na infrastrukturze centralnej CIRF. Dokument obowiązuje we wszystkich jednostkach organizacyjnych Resortu Finansów.

## 5. Dokumenty związane

Procedura wytwarzania oprogramowania wersja 1.2

 <div> <div>Centrum</div> <div>Informatyki</div> <div>Resortu</div> <div>Finansów</div> </div>	Nazwa jednostki organizacyjnej:		Centrum Informatyki Resortu Finansów	
	Tytuł dokumentu:		WYMAGANIA OGÓLNE DLA BUDOWANYCH SYSTEMÓW UTRZYMYWANYCH W INFRASTRUKTURZE CIRF	
	Wersja dokumentu:	1.0	Obszar IT	TE
	Data opracowania:	24.10.2023	Kod zakresu dokumentu:	RF / AK

## 6. Rola CIRF

Wszelkie zasoby infrastrukturalne są udostępniane, zarządzane i monitorowane przez jednostkę organizacyjną – Centrum Informatyki Resortu Finansów (CIRF). Zasady udostępniania zasobów zostały opisane w skrócie w niniejszym dokumencie.

CIRF występuje z ramienia szeroko rozumianego resortu finansów jako strona, która weryfikuje zgodność dostarczonych przez dostawców rozwiązań ze standardami obowiązującymi w resorcie finansów. CIRF może odmówić dostarczenia zasobów, jeśli nie są one zgodne ze standardem obowiązującym w CIRF, który jest opisany w tym dokumencie. W przypadku wyższej konieczności udostępnienia zasobów niezgodnych ze standardem obowiązującym w CIRF, pełna odpowiedzialność za działania takich zasobów jest przenoszona na Dostawcę i konsumenta tych zasobów.

CIRF wymaga od Dostawców również:

- dostarczania pełnej dokumentacji systemu obejmującej strukturę systemu, jego powiązania z komponentami zewnętrznymi, procedury administracyjne i operacyjne, które będą wykonywane samodzielnie przez CIRF, wszelkie procedury pozwalające na bezpieczne zatrzymywanie i uruchamianie całego systemu;
- dokumentowania wszystkich wprowadzanych zmian związanych z infrastrukturą i architekturą systemu;
- utrzymywania aktualności dokumentacji, oraz przekazywania jej do CIRF;
- zgłaszania za pomocą posiadanego przez CIRF Centralnego ServiceDesk (jedyne obowiązujące narzędzie do obsługi zgłoszeń) wszelkich potrzeb w zakresie zmian dostarczanej infrastruktury, oraz obejmowania mechanizmem kopii zapasowej obszarów wskazanych przez Wykonawcę, związanych z systemem;
- wykonywania wszelkich działań mających na celu dostosowanie dostarczonych rozwiązań do standardów obowiązujących w resorcie finansów, w szczególności związanych z aspektami bezpieczeństwa teleinformatycznego.

CIRF realizuje procedurę udostępniania zasobów na podstawie wniosków złożonych wraz z zatwierdzonym Projektem Technicznym Systemu.

Standard dokumentowania procesu wytwórczego dla Wykonawcy określa procedura wytwarzania oprogramowania.


### 6.1 Ograniczenia w zakresie przydzielanych zasobów

Na podstawie PTS/ePTS, wycen, zapisów w umowie i innych ustaleń definiowany jest limit wielkości przydzielonych zasobów infrastrukturalnych IT dla systemu, dla wszystkich środowisk razem. Standardem jest, iż Dostawca/Właściciel Biznesowy gwarantuje budżet umożliwiający zapewnienie ich dla danego systemu, w szczególności:

- mocy przetwarzania – serwery;
- przestrzeni na składowanie danych (all-flash, przestrzeń plikowa, przestrzeń obiektowa);
- przestrzeni na składowanie danych kopii zapasowych;
- niezbędnych licencji na elementy infrastrukturalne (wirtualizator, ochrona antywirusowa, licencje pojemnościowe na system backupowy);
- niezbędnych licencji na inne oprogramowanie niezbędne do utworzenia i działania bloków architektonicznych;
- innych niezbędnych komponentów technicznych, sprzętowych i software'owych wymaganych do funkcjonowania infrastruktury związanej z danym Systemem.

CIRF nie gwarantuje zwiększania przydzielonych zasobów do systemu powyżej limitu ustalonego na etapie wycen oraz ustalonego wcześniej finansowania.

Finansowanie przekazane na budowę/rozbudowę systemu jest rozdysponowane przez CIRF na zasoby infrastrukturalne, zgodnie z bieżącymi potrzebami CIRF i nie jest tożsame ze specyfikacją zasobów określonych w wycenie. Finansowanie to stanowi bazę do odtworzenia infrastruktury w CIRF. CIRF zapewnia, iż dysponuje potencjałem umożliwiającym zapewnienie zasobów przeznaczonych na System, który dostarczył finansowanie w stopniu nie mniejszym niż zakres określony w wycenie, będącej podstawą do wyliczenia wartości finansowania dla systemu. Możliwe jest zwiększenie zasobów przydzielonych na system po

	Nazwa jednostki organizacyjnej:		Centrum Informatyki Resortu Finansów	
	Tytuł dokumentu:		WYMAGANIA OGÓLNE DLA BUDOWANYCH SYSTEMÓW UTRZYMYWANYCH W INFRASTRUKTURZE CIRF	
	Wersja dokumentu:	1.0	Obszar IT	TE
	Data opracowania:	24.10.2023	Kod zakresu dokumentu:	RF / AK

wcześniejszej wycenie potrzeb oraz pozyskaniu gwarancji zabezpieczenia środków finansowych pozwalających na uzupełnienie infrastruktury CIRF o niezbędną infrastrukturę.

## 6.2 Bloki Architektoniczne – wymagania ogólne

CIRF wskazuje, iż wszystkie rozwiązania aplikacyjne tworzące system muszą być zbudowane na bazie Bloków Architektonicznych z Katalogu usług CIRF (usługi infrastrukturalne). System wykorzystujący te bloki powinien być tworzony w architekturze Cloud Native, przy wykorzystaniu rozwiązań umożliwiających segmentację usług biznesowych, mikroserwisów, umożliwiając tym samym skalowanie poziome rozwiązania, w celu zwiększenia wydajności i niezawodności systemu.

CIRF wymaga aby system został zbudowany w oparciu o Bloki Architektoniczne, czyli grupy maszyn wirtualnych wykreowanych i następnie funkcjonujących w środowisku zwirtualizowanym CIRF, opartym o technologię Vmware vSphere w wersji 7.x (lub nowszą). Nie dopuszcza się wykorzystywania serwerów fizycznych do bezpośredniego uruchamiania komponentów systemu. CIRF nie posiada infrastruktury pozwalającej na bezpośrednią implementację komponentów na infrastrukturze fizycznej.

Środowisko CIRF zbudowane jest na bazie nowoczesnej platformy sprzętowej (serwerowej) wyposażonej w wysokowydajne procesory wielordzeniowe oparte o architekturę x64 (Intel model XEON GOLD i/lub AMD model EPYC w najnowszych i najbardziej rozbudowanych wersjach jeśli chodzi o liczbę rdzeni) o taktowaniu powyżej 2,5GHz. Analogicznie do procesorów serwery posiadane przez CIRF są wyposażone w odpowiednią ilość pamięci RAM DDR4 o taktowaniu co najmniej 2,5 GHz.

CIRF zakłada, że dla Bloków Architektonicznych (zbioru maszyn wirtualnych) przeznaczonych dla środowisk produkcyjnych zapewni mapowanie 1vCPU na 1 fizyczny rdzeń procesora w przypadku wysokiego obciążenia Systemu. W związku z powyższym Dostawca nie może zakładać zwiększenie udostępnionych zasobów lub zwiększenie wydajności poprzez zastosowania technologii Hypertreading lub analogicznych.

Wszystkie komponenty aplikacyjne instalowane lub wdrażane na udostępnionych Blokach Architektonicznych tworzących system muszą być przystosowane do instalacji i pracy w środowisku izolowanym (tzw. AIR GAP) bez dostępu do Internetu. Wszystkie artefakty, binaria i wymagany kod źródłowy musi być dostarczony w formie umożliwiającej osadzenie w lokalnych repozytoriach posiadanych i utrzymywanych przez CIRF. Dopiero z tych repozytoriów możliwe jest wdrażanie (deployment) aplikacji na zamawianych Blokach Architektonicznych. Dopuszcza się wyjątek, w którym za utrzymanie repozytorium do konkretnego projektu odpowiada jego Dostawca, jednak to repozytorium musi funkcjonować na poziomie infrastruktury zarządzanej przez CIRF, musi być zbudowane ze standardowych bloków architektonicznych udostępnianych przez CIRF i zasadami wykorzystania, administracji (zasoby konsumowane na takie komponenty są wliczane do puli konsumowanej przez cały system i nie powiększają limitu zasobów przydzielonych na ten system). Uprawnienia Wykonawcy są określone dodatkowymi dokumentami precyzującymi powyższe założenia.

Zasoby na potrzeby wykreowania systemu dostarczane są na podstawie zatwierdzonego i zaakceptowanego Projektu Technicznego Systemu – PTS/ePTS.

### 6.2.1 Definicja Bloku Architektonicznego

Bloki Architektoniczne posiadają z góry ustalone funkcjonalności definiowane przez technologie zaimplementowane i działające na tych blokach.

Pojedynczy Blok Architektoniczny składa się z jednego lub więcej serwerów (maszyn wirtualnych), które posiadają takie same parametry ilościowo-jakościowe (atributy bloku), funkcjonalne, oraz mają zainstalowane dokładnie takie same komponenty aplikacyjne oraz systemowe. Idea bloku architektonicznego składającego się z więcej niż jednej maszyny wirtualnej (krotność 2 lub więcej) zakłada, iż w trakcie normalnej eksploatacji systemu wielokrotność maszyn zwiększa wydajność rozwiązania jak i niezawodność. Brak dostępności nawet 50% maszyn wirtualnych składających się na pojedynczy Blok Architektoniczny nie może spowodować niedostępności funkcjonalności udostępnianych przez ten blok, równocześnie dopuszczając jedynie obniżenie jego wydajności na czas wynikający z niedostępności części serwerów (maszyn wirtualnych) składających się na ten blok.

Nie dopuszcza się implementacji, w której pojedynczy Blok Architektoniczny realizuje kilka równoczesnych i różnych ról, np. funkcjonalność aplikacyjną jak też i bazodanową. Jedyny wyjątek dla tej zasady to zamknięty blok typu VA, o którym jest mowa w dalszej części tego dokumentu.

### 6.2.2 Dostęp do funkcjonalności Bloku Architektonicznego

Dostęp do funkcjonalności dostarczanych przez pojedynczy blok architektoniczny jest zależny od



 <b>Centrum Informatyki Resortu Finansów</b>	Nazwa jednostki organizacyjnej:		Centrum Informatyki Resortu Finansów	
	Tytuł dokumentu:		WYMAGANIA OGÓLNE DLA BUDOWANYCH SYSTEMÓW UTRZYMYWANYCH W INFRASTRUKTURZE CIRF	
	Wersja dokumentu:	1.0	Obszar IT	TE
	Data opracowania:	24.10.2023	Kod zakresu dokumentu:	RF / AK

technologii udostępnianej w ramach danego bloku. Mogą to być mechanizmy wynikające wprost z wybranej technologii (np. adres IP/grupa adresów IP dla bazy danych), lub dostęp do adresu IP (VIP) udostępnionego przez posiadany przez CIRF system sprzętowych Load Balancer'ów, który dalej przekierowuje ruch na wszystkie serwery (maszyny wirtualne) składające się na pojedynczy Blok Architektoniczny (np. dla serwerów aplikacyjnych). Dla każdej z wybranych usług i funkcjonalności mogą być zdefiniowane adresy VIP, które będą EndPoint'ami zarówno dla użytkowników końcowych, jak też innych usług.

### 6.2.3 Wyciąg z katalogu dostępnych rodzajów Bloków Architektonicznych

CIRF posiada Katalog usług CIRF (usługi infrastrukturalne) opisujący rodzaj dostarczanych Bloków Architektonicznych i technologie, które wspiera od strony technicznej oraz administruje nimi do poziomu silników wykonawczych technologii aplikacyjnych i bazodanowych zaimplementowanych w ramach tych bloków. Dostawca ma możliwość skorzystania z ich funkcjonalności technologicznej oraz do osadzania na nich i uruchamiania aplikacji w celu dostarczenia funkcjonalności biznesowych.

Katalog ten obejmuje takie technologie jak:

- blok G011.DB.SQL - motor bazy danych MS SQL w wersjach: Standard, Enterprise w konfiguracjach:
  - StandAlone (pojedyncza maszyna wirtualna z bazą danych),
  - AlwaysOn (klaster składający się z kilku maszyn wirtualnych z własnymi bazami i włączonymi mechanizmami synchronizacji);
- blok G011.DB.ORA - motor bazy danych Oracle w wersjach:
  - Enterprise Edition w konfiguracjach StandAlone (pojedyncza maszyna wirtualna z bazą danych),
  - Enterprise Edition w konfiguracji RAC (klaster składający się z kilku maszyn wirtualnych współdzielących ten sam zasób na bazę danych zarządzany technologią ASM);
- blok G011.DB.PGS - motor bazy danych Postgres w konfiguracji:
  - StandAlone (pojedyncza maszyna wirtualna z bazą danych),
  - klastrowej replikacji (z wykorzystaniem PGPool);
- blok G011.DB.MDB - motor bazy danych MongoDB (zestaw kilku maszyn wirtualnych tworzących klaster);
- blok G011.DB.MYS - MySQL - motor bazy danych MySQL;
- blok G012.AP.JBO - serwer aplikacyjny oparty o technologię WildFly;
- blok G012.AP.NET - serwer aplikacyjny oparty o technologię IIS ASP.NET;
- blok G012.AP.AHS - serwer aplikacyjny oparty o technologię Apache HTTP;
- blok G012.AP.WAS - serwer aplikacyjny oparty o technologię IBM Websphere Application Server;
- blok G012.AP.JSP - serwer aplikacyjny oparty o technologię Servlets/JSP Tomcat;
- blok G012.AP.WLS - serwer aplikacyjny oparty o technologię Java EE WebLogic (WLS);
- blok G014.OS.WIN - uniwersalny serwer aplikacyjny oparty na systemie Windows Server 2022 DataCenter;
- blok G014.OS.LNX - uniwersalny serwer aplikacyjny oparty na systemie Linux: SLES, Oracle Linux (OEL), RedHat;
- Szyna ESB - komponent Platformy Integracyjnej Resortu Finansów (pozwala na implementację rozwiązań do wymiany danych pomiędzy Systemami);
- Blok VA - Virtual Appliance (maszyna wirtualna z zamkniętą funkcjonalnością).

Komponenty systemowe oprogramowania Bloków Architektonicznych dostarczanych przez CIRF są objęte odpowiednimi licencjami wynikającymi z ich konstrukcji i realizowanej funkcji. Dostawca zobowiązany jest do dostarczenia licencji w ilości zgodnej z modelem licencjonowania i wymaganiami ilościowymi określonymi w projekcie budowanego systemu. Mechanizm finansowania jest zależny od ustaleń w projekcie, który finansuje konkretne potrzeby systemu.

### 6.2.4 Wielkości zalecane i maksymalne Bloków Architektonicznych

CIRF oczekuje, aby wybrane przez Wykonawcę rozwiązanie realizujące wymagania biznesowe umożliwiło skalowanie poziome poprzez zwiększanie krotności bloków architektonicznych (zwiększenie maszyn wirtualnych). Zalecane parametry wielkościowe maszyn wirtualnych nie powinny być większe niż:

- 8 vCPU;



 <div> <div>Centrum</div> <div>Informatyki</div> <div>Resortu</div> <div>Finansów</div> </div>	Nazwa jednostki organizacyjnej:		Centrum Informatyki Resortu Finansów	
	Tytuł dokumentu:		WYMAGANIA OGÓLNE DLA BUDOWANYCH SYSTEMÓW UTRZYMYWANYCH W INFRASTRUKTURZE CIRF	
	Wersja dokumentu:	1.0	Obszar IT	TE
	Data opracowania:	24.10.2023	Kod zakresu dokumentu:	RF / AK

- 32 GB vRAM;
- 500 GB pojemności na składowanie i przetwarzanie danych operacyjnych – zabezpieczony lokalny dysk wirtualnej maszyny.

W szczególnych i uzasadnionych przypadkach CIRF dopuszcza zwiększenie wielkości zasobów przypisanych do pojedynczej maszyny wirtualnej składającej się na blok architektoniczny, jednakże ogranicza ich maksymalną wielkość do poniższych wielkości jej elementów składowych:

- 24 vCPU;
- 256 GB vRAM;
- 10 TB pojemności na składowanie danych – zabezpieczony lokalny dysk lub grupa dysków.

#### 6.2.5 Rozwiązania kontenerowe implementowane w ramach Bloków Architektonicznych

CIRF dopuszcza wykorzystanie technologii kontenerowych, jednakże rozwiązanie to musi być zaimplementowane zgodnie z ideą Bloków Architektonicznych opisanych powyżej i mieszczących się w opisanych ich parametrach wielkościowych.

Zatem platformą do implementacji rozwiązań wykorzystujących konteneryzację będzie blok architektoniczny o krotności większej niż 1, zbudowany z uniwersalnych serwerów aplikacyjnych opartych na systemie Linux (czyli maszyn wirtualnych) - G014.OS.LNX.

CIRF dopuszcza uruchamianie jako kontenerów komponentów aplikacyjnych/funkcjonalnych jedynie w wersji bezstanowej i pozbawionych elementu „container persistent volumes”, lub posiadających ten element konfiguracji lecz składający dane, które z punktu widzenia niezawodnościowego mogą zostać bezpowrotnie utracone (dane nieistotne z punktu widzenia funkcjonowania systemu).

Zgodnie z powyższym, CIRF nie zaakceptuje rozwiązania, w którym kontenerem będzie na przykład baza danych składająca dane w zasobach lokalnych rozwiązania kontenerowego.

Zgodnie z definicją bloku architektonicznego brak dostępu pojedynczej maszyny wirtualnej składającej się na cały blok (Worker) nie może powodować utraty dostępu do funkcjonalności udostępnianej przez ten blok. Cały blok architektoniczny przeznaczony do obsługi kontenerów, musi być przygotowany i zarządzany w technologii orkiestracji kontenerów – Kubernetes.


W przypadku konieczności składowania danych przez aplikacyjne elementy kontenerowe jedynymi dopuszczalnymi technologiami są posiadane przez CIRF rozwiązania OnPrem (utrzymywane w środowisku CIRF):

- NFS/CIFS: folder udostępniony do wybranych bloków architektonicznych;
- Amazon S3: NameSpace w ramach struktury Tenant przydzielonej dedykowanej dla Zamawiającego dla określonych bloków architektonicznych.

#### 6.2.6 Blok Architektoniczny typu VA

W szczególnych i uzasadnionych przypadkach, gdy nie ma możliwości wykorzystania gotowych technologii z katalogu udostępnionego przez CIRF, dopuszcza się utworzenie, dostarczenie i obsługę bloku architektonicznego typu Virtual Appliance, który musi spełniać następujące kryteria:

- jedna lub więcej maszyn tworzą zamkniętą funkcjonalność (są rozwiązaniem o zamkniętej naturze funkcjonalno-niezawodnościowo-wydajnościowej realizowanej za pomocą wbudowanych mechanizmów);
- budowa i konstrukcja każdej maszyny wirtualnej składającej się na blok ma charakter zamknięty i jest dostarczona jako gotowe rozwiązanie (OVA) kompatybilne w pełni z wersją VMware vSphere 6.7 lub VMware vSphere 7;
- pełną odpowiedzialność za licencjonowanie wszystkich komponentów składających się na taki blok przejmuje Dostawca. Jego obowiązkiem jest przekazać wszystkie zapisy licencyjne umożliwiające potwierdzenie, iż prawo używania rozwiązań wykorzystywanych w takim bloku przez CIRF nie narusza żadnych zapisów licencyjnych jak też regulacji prawnych;
- pełną odpowiedzialność za poprawne, niezawodne i bezpieczne działanie całego bloku przejmuje Dostawca. Nie zwalnia to Dostawcy z obowiązku dostarczenia całej dokumentacji takiego bloku, włącznie z niezbędnymi procedurami administracyjnymi;


 <div> <div>Centrum</div> <div>Informatyki</div> <div>Resortu</div> <div>Finansów</div> </div>	Nazwa jednostki organizacyjnej:		Centrum Informatyki Resortu Finansów	
	Tytuł dokumentu:		WYMAGANIA OGÓLNE DLA BUDOWANYCH SYSTEMÓW UTRZYMYWANYCH W INFRASTRUKTURZE CIRF	
	Wersja dokumentu:	1.0	Obszar IT	TE
	Data opracowania:	24.10.2023	Kod zakresu dokumentu:	RF / AK

- odpowiedzialność CIRF jest ograniczona jedynie do utrzymania dostępnych zasobów w postaci określonej i wymaganej liczby vCPU, vRAM oraz przestrzeni dyskowej, niezbędnych do uruchomienia wszystkich maszyn składających się na taki blok architektoniczny;
- limit wielkości przypisanych zasobów do bloku typu VA jest taki sam jak dla innych Bloków Architektonicznych;
- w przypadku konieczności ochrony backupowej takiego bloku odpowiedzialność CIRF ograniczona jest jedynie do wykonywania tzw. kopii snapshotowej - czyli zabezpieczenie całej wirtualnej maszyny, oraz ewentualnego odzyskania całej wirtualnej maszyny lub maszyn składających się na blok.

### 6.3 Systemy składowania danych

CIRF dysponuje 3 rodzajami technologii do składowania danych stanowiących element Bloku Architektonicznego:

- **Przestrzeń dyskowa „blokowa”** prezentowana bezpośrednio do pojedynczej maszyny wirtualnej jako jej dysk lokalny (dysk VMDK) składowana na posiadanych przez CIRF nowoczesnych macierzach dyskowych klasy Enterprise zbudowanych z dysków NVMe/SSD z zabezpieczeniem RAID i dyskami HotSpare, w których opóźnienia w dostępie do danych nie są dłuższe niż 2ms (zastosowany protokół SAN FC o prędkości co najmniej 16Gbps pomiędzy serwerami fizycznymi a macierzami). Ten rodzaj pamięci jest wykorzystywany przez CIRF jako miejsce składowania całych maszyn wirtualnych, wraz z ich dyskami lokalnymi. W szczególnych przypadkach dopuszcza się utworzenie dedykowanego zasobu blokowego na opisanych powyżej macierzach i zaprezentowanie go bezpośrednio do jednej lub kilku wybranych maszyn wirtualnych tworzących określony Blok Architektoniczny (RDM lub współdzielony RDM). Wynika to z technologii danego Bloku Architektonicznego;
- **Współdzielona sieciowa przestrzeń „plikowa”** publikowana do poziomu systemu operacyjnego Bloku Architektonicznego w technologiach NFS lub CIFS, składowana na nowoczesnych macierzach dyskowych klasy Enterprise posiadanych przez CIRF (funkcjonalność NAS). Komunikacja pomiędzy blokami architektonicznymi a macierzami udostępniającymi dane w tej technologii jest realizowana w warstwie sieciowej o prędkości co najmniej 10GbE. CIRF dysponuje rozwiązaniem, które umożliwia składowanie danych na zasobach wyposażonych w dyski mechaniczne NL SAS i SAS wspomaganych mechanizmami tieringu na bazie dysków SSD lub szybkich z minimalnymi opóźnieniami (NVMe/Flash). Ten rodzaj przestrzeni jest przeznaczony do składowania danych o charakterze statycznym/archiwalnym (NL SAS/SAS) lub dynamicznym (NVMe/SSD), gdzie dane te muszą być dostępne jednocześnie dla wielu serwerów – maszyn wirtualnych;
- **Współdzielona sieciowa przestrzeń „obiektoowa”** – Amazon S3 publikowana do poziomu warstwy aplikacji zainstalowanej na Bloku Architektonicznym i dostępna dla niej za pośrednictwem protokołu http/https „Amazon S3”. Zasoby te są składowane na nowoczesnych rozwiązaniach OnPrem klasy Enterprise posiadanych przez CIRF i pracujących w Ośrodkach Przetwarzania Danych CIRF, wspierających ten protokół komunikacyjny. Ten rodzaj przestrzeni jest przeznaczony do składowania danych, które mają charakter statyczny i archiwalny. Komunikacja pomiędzy blokami architektonicznymi a rozwiązaniami udostępniającymi ten protokół jest realizowana w warstwie lokalnej sieci LAN o prędkości ok. 10Gbps, jednakże ze względu na charakter protokołu komunikacyjnego, jak też mechanizmy składowania danych (dyski NL SAS), dostęp do danych składowanych na zasobach S3 jest wolniejszy niż w przypadku innych, powyżej opisanych technologii. Wynika to z narzutu związanego z protokołem komunikacyjnym (http/https), technologią, wielkością przesyłanych plików, mechanizmem przyjmowania jak też składowania oraz zabezpieczenia danych. Czas dostępu w szczególnych przypadkach może wynieść nawet do kilku sekund w przypadku dużych plików. CIRF zakłada, iż dane zgromadzone w tej technologii nie będą wymagać dodatkowej ochrony w postaci mechanizmu kopii zapasowej, po nałożeniu polityk uniemożliwiających usunięcie/modyfikację danych w ramach indywidualnie udostępnionej przestrzeni NameSpace/Tenant. Możliwe jest zabezpieczenie istotnych danych z punktu widzenia biznesowego poprzez ich synchronizację do analogicznego rozwiązania działającego w innym Ośrodku Przetwarzania Danych CIRF. W takim przypadku ten sam zabezpieczony obiekt jest dostępny jednocześnie z dwóch źródeł poprzez dwa różne

 <b>Centrum Informatyki Resortu Finansów</b>	Nazwa jednostki organizacyjnej:		Centrum Informatyki Resortu Finansów	
	Tytuł dokumentu:		WYMAGANIA OGÓLNE DLA BUDOWANYCH SYSTEMÓW UTRZYMYWANYCH W INFRASTRUKTURZE CIRF	
	Wersja dokumentu:	1.0	Obszar IT	TE
	Data opracowania:	24.10.2023	Kod zakresu dokumentu:	RF / AK

adresy URL do tego obiektu, którego część FQDN wskazuje lokalizację repozytorium z którego zostanie pobrany obiekt.

W przypadku konieczności składowania danych, które mają charakter statyczny i archiwalny (np. nagrania, pliki XML, CSV), CIRF zaleca wykorzystanie opisanych powyżej posiadanych współdzielonych technologii „sieciowych” (S3, NFS/CIFS – NL-SAS/SAS) udostępnionych dla wybranych bloków architektonicznych, zamiast składowania danych na przestrzeni dyskowej lokalnej udostępnionej bezpośrednio w ramach bloku architektonicznego. Wynika to z konieczności optymalizacji kosztów infrastruktury niezbędnej do utrzymania systemu. Zasoby w technologiach S3 i NFS/CIFS NL-SAS/SAS są znacznie tańsze, niż przestrzeń dyskowa prezentowana bezpośrednio do bloku architektonicznego (zabezpieczone lokalne dyski wirtualnych maszyn zbudowane na bazie technologii Flash/NVMe).

## 6.4 Definicje środowisk dla systemu

### 6.4.1 Środowisko produkcyjne (PR/PRD)

Środowisko produkcyjne tworzy zestaw bloków architektonicznych udostępniających funkcjonalności aplikacyjne i biznesowe dla użytkowników i systemów, zgodnie z wymaganiami biznesowymi określonymi dla systemu.

CIRF zakłada, iż system będzie zbudowany z zestawu udokumentowanych bloków architektonicznych bazujących na katalogu CIRF, w których zostaną zaimplementowane wszystkie rozwiązania, funkcjonalności spełniające wszystkie wymagania biznesowe, przeznaczone do eksploatacji systemu.

Z punktu widzenia sieciowego i bezpieczeństwa, środowisko to jest izolowane w ramach dedykowanej podsięci, do której dostęp administracyjny jest ograniczony dla wybranych administratorów, a wszelkie zmiany wymagają zgody CIRF i podlegają ewidencji. Dostęp do takiego środowiska jest rejestrowany i odbywa się wyłącznie za pomocą systemu rejestracji sesji użytkowników oraz tzw. Stacji Pośrednich (przesiadkowych). Takie środowisko może być zabezpieczone mechanizmami Kopii Zapasowej, po zgłoszeniu takiego zapotrzebowania przez Dostawcę lub ASI i wskazaniu zakresu danych, które muszą być zabezpieczone.

### 6.4.2 Środowisko pre-produkcyjne (PP/PRE - Preproduction Test)

Środowisko preprodukcyjne (opcjonalne) powoływane jest na potrzeby testów instalacji paczki z oprogramowaniem. To środowisko stworzone do przeprowadzania testów przedprodukcji. Testy przedprodukcji są często ostatnim etapem testowania przed wdrożeniem oprogramowania lub systemu do produkcji, podobnie jak testy akceptacyjne, jednak mają na celu sprawdzenie, czy wszystkie komponenty systemu lub oprogramowania działają poprawnie w rzeczywistych warunkach produkcyjnych. Analogicznie jak produkcja tworzy je zestaw bloków architektonicznych udostępniających funkcjonalności aplikacyjne i biznesowe dla użytkowników i systemów, zgodnie z wymaganiami biznesowymi określonymi dla systemu. Zakres danych jest ograniczony do minimum niezbędnego do testowania poprawności wgranych pakietów oprogramowania.


CIRF zakłada, iż system będzie zbudowany z zestawu udokumentowanych bloków architektonicznych bazujących na katalogu CIRF, w których zostaną zaimplementowane wszystkie rozwiązania, funkcjonalności spełniające wszystkie wymagania biznesowe, przeznaczone do eksploatacji systemu.

Z punktu widzenia sieciowego i bezpieczeństwa, środowisko to jest izolowane w ramach dedykowanej podsięci, do której dostęp administracyjny jest ograniczony dla wybranych administratorów, a wszelkie zmiany wymagają zgody CIRF i podlegają ewidencji. Dostęp do takiego środowiska jest rejestrowany i odbywa się wyłącznie za pomocą systemu rejestracji sesji użytkowników oraz tzw. Stacji Pośrednich (przesiadkowych). Takie środowisko może być zabezpieczone mechanizmami Kopii Zapasowej, po zgłoszeniu takiego zapotrzebowania przez Dostawcę lub ASI, ale potrzeba ta musi być uzasadniona.

### 6.4.3 Środowiska nieprodukcyjne

CIRF dopuszcza utworzenie oddzielnych środowisk przeznaczonych do celów nieprodukcyjnych (jeśli są wymagane):


Identyfikator środowiska	Opis
TR/TRA	Środowisko szkoleniowe/ Środowisko testowe edukacyjne, które służy do przeprowadzania testów, ćwiczeń i innych działań związanych z edukacją i szkoleniem.

 <div> <div>Centrum</div> <div>Informatyki</div> <div>Resortu</div> <div>Finansów</div> </div>	Nazwa jednostki organizacyjnej:		Centrum Informatyki Resortu Finansów	
	Tytuł dokumentu:		WYMAGANIA OGÓLNE DLA BUDOWANYCH SYSTEMÓW UTRZYMYWANYCH W INFRASTRUKTURZE CIRF	
	Wersja dokumentu:	1.0	Obszar IT	TE
	Data opracowania:	24.10.2023	Kod zakresu dokumentu:	RF / AK

TI/TIN	Środowisko dla testów wewnętrznych, często nazywane też środowiskiem QA (Quality Assurance), jest to kontrolowane, odizolowane środowisko, w którym przeprowadza się testy oprogramowania w celu zapewnienia jego jakości i wydajności przed wypuszczeniem go na rynek lub przed wprowadzeniem zmian do istniejącej aplikacji.
TE/TEX	Środowisko dla testów zewnętrznych jest to środowisko, w którym przeprowadza się testy oprogramowania w celu sprawdzenia jego funkcjonalności, wydajności, jakości i zgodności z wymaganiami przez niezależnych testerów, użytkowników końcowych lub innych zainteresowanych stron spoza zespołu deweloperskiego.
DE/DEV	Środowisko deweloperskie/rozwojowe (Development Test) - środowisko tworzone do przeprowadzania testów w fazie rozwoju aplikacji lub oprogramowania.
SYS	Środowisko testów systemowych, manualnych (System Test) - środowisko tworzone do przeprowadzania testów systemowych w sposób ręczny, tj. bez użycia automatyzacji testów w celu sprawdzenia, czy cały system lub aplikacja działa zgodnie z określonymi wymaganiami i oczekiwaniami.
ATE	Środowisko testów ciągłej integracji lub testów automatycznych (Automated Test) - środowisko, w którym automatyczne testy są wykonywane jako część procesu CI/CD (Continuous Integration/Continuous Delivery). Celem tego środowiska jest zapewnienie, że nowy kod jest testowany automatycznie po każdej zmianie i że aplikacja zachowuje się zgodnie z oczekiwaniami.
UAT	Środowisko testów akceptacyjnych (Acceptance Test) - to środowisko, w którym przeprowadza się testy akceptacyjne oprogramowania lub systemu. Testy akceptacyjne są ostatnim etapem testowania przed wdrożeniem systemu lub oprogramowania do produkcji, i mają na celu potwierdzenie, że system spełnia oczekiwania użytkowników lub klienta oraz działa zgodnie z wymaganiami biznesowymi.
EFF	Środowisko testów wydajnościowych (Efficiency Test) - jest przygotowane w celu oceny wydajności i skalowalności systemu lub aplikacji.
DIS	Środowisko testów wypadkowych (Disaster Recovery & Failover Test) - tworzone w celu przetestowania zdolności systemu lub infrastruktury do przetrwania i odzyskania po wystąpieniu katastrofy lub awarii. Celem jest upewnienie się, że organizacja jest przygotowana do utrzymania ciągłości działania swoich systemów i danych w przypadku nieoczekiwanych zdarzeń.
MIG	Środowisko testów migracji - tworzone w celu oceny procesu przenoszenia danych lub aplikacji z jednego środowiska do innego. Sprawdza czy proces przebiega zgodnie z planem i nie powoduje utraty danych ani awarii aplikacji.
UPG	Środowisko testów podniesienia wersji (Upgrade Test) - budowane w celu oceny procesu aktualizacji oprogramowania, systemu lub infrastruktury. Celem tych testów jest upewnienie się, że proces upgrade przebiega zgodnie z planem i nie powoduje awarii lub utraty danych.

Każde z tych środowisk musi być zbudowane w oparciu o koncepcję bloków architektonicznych (analogicznie jak środowisko produkcyjne). Powinno technicznie odzwierciedlać architekturę środowiska produkcyjnego za wyłączeniem parametrów wydajnościowych i ilościowych. Nie jest dopuszczalne mieszanie w ramach jednego bloku funkcji, blok musi być przypisany tylko do jednego środowiska. CIRF zaleca, by wielkości oraz ilości maszyn składających się na bloki architektoniczne (krotność bloku) były dostosowane do realnych potrzeb, wynikających z potrzeb biznesowych. CIRF rekomenduje aby środowiska nieprodukcyjne były wielokrotnie mniejsze niż środowisko produkcyjne, co bezpośrednio będzie przekładać się na niższe koszty projektu czy też budowanego systemu.

CIRF nie dopuszcza umieszczania i wykorzystywania w środowiskach nieprodukcyjnych jakichkolwiek danych pochodzących ze środowiska produkcyjnego, chronionych prawem powszechnym lub tajemnicą skarbową bez wcześniejszej anonimizacji tych danych. W przypadku zaistnienia takiej potrzeby należy dla tych

 <b>Centrum Informatyki Resortu Finansów</b>	Nazwa jednostki organizacyjnej:		Centrum Informatyki Resortu Finansów	
	Tytuł dokumentu:		WYMAGANIA OGÓLNE DLA BUDOWANYCH SYSTEMÓW UTRZYMYWANYCH W INFRASTRUKTURZE CIRF	
	Wersja dokumentu:	1.0	Obszar IT	TE
	Data opracowania:	24.10.2023	Kod zakresu dokumentu:	RF / AK

środowisk zastosować wszelkie wymagane prawem zabezpieczenia analogiczne jak dla środowiska produkcyjnego.

## 6.5 Tworzenie i modyfikacja parametrów bloków architektonicznych

Podstawą do rozpoczęcia prac związanych z wytworzeniem bloków architektonicznych dla systemu jest uzgodnienie pomiędzy CIRF a Dostawcą/Właścicielem biznesowym systemu/Architektem systemu/ASI dokumentu Projekt Techniczny Systemu (PTS/ePTS).

Dokument ten, dla każdego rodzaju środowiska systemu opisuje:

- architekturę wewnętrzną systemu;
- komponenty biznesowe i funkcjonalne składające się na system;
- wymagania określające ilość bloków, ich rodzaj, krotność każdego bloku, oraz wielkości maszyn składających się na wymagane bloki;
- komunikację pomiędzy blokami, oraz komponentami zewnętrznym;
- dodatkowe wymagane komponenty systemu, między innymi: definicje potrzeb adresów VIP na LoadBalancerach oraz farm serwerów, konieczność utworzenia grup zabezpieczeń na poziomie usługi ActiveDirectory, konieczność dopuszczenia komunikacji mailowej, konieczność definicji rekordów DNS do publikacji usług.

Taki dokument stanowi dla CIRF materiał dla analiz i ewentualnych ustaleń z Właścicielem Systemu/Dostawcą, tak by stał się jednoznaczny dla wszystkich stron. Dopiero po jego zatwierdzeniu Właściciel Systemu/ASI, składa w Centralnym ServiceDesk wniosek o utworzenie bloków, gdzie załącznikiem jest zatwierdzony PTS/ePTS. Ten krok formalnie rozpoczyna proces tworzenia Bloków Architektonicznych, które zostaną udostępnione Dostawcy/Właścicielowi Systemu/ASI.

Po wytworzeniu i przekazaniu Bloków Architektonicznych, CIRF dopuszcza możliwość modyfikacji ich parametrów (wielkości i ilości maszyn wirtualnych składających się na blok architektoniczny), jednak każda taka zmiana jest poprzedzona dostarczeniem zmodyfikowanego PTS/ePTS, który poprzez proces weryfikacji został zatwierdzony. Wszelkie zmiany muszą być zgłoszone przez Dostawcę/Właściciela biznesowego/ASI za pośrednictwem Centralnego ServiceDesk CIRF i zawierać dokładny opis zmian i zatwierdzony PTS/ePTS. Dotyczy to każdego ze środowisk systemu.

Możliwości zmiany poszczególnych elementów składowych bloku są następujące:

- krotność bloku (ilość wirtualnych maszyn składających się na blok) – zmniejszenie i zwiększenie;
- ilość vCPU dla maszyny wirtualnej tworzącej blok – zmniejszenie i zwiększenie (wymagane jest czasowe zatrzymanie maszyny wirtualnej do wykonania tej zmiany);
- ilość pamięci vRAM dla maszyny wirtualnej tworzącej blok – zmniejszenie i zwiększenie (wymagane jest czasowe zatrzymanie maszyny wirtualnej do wykonania tej zmiany);
- wielkość lokalnego dysku podłączonego do maszyny wirtualnej – tylko zwiększenie wielkości, lub usunięcie dysku,
- wielkość zasobu sieciowego opublikowanego do bloku architektonicznego (w technologiach S3/NFS/CIFS) – tylko zwiększenie wielkości lub usunięcie zasobu.

Możliwe jest też usunięcie bloku architektonicznego (wraz z bezpowrotnym usunięciem danych tego bloku) oraz utworzenie nowego bloku, zgodnie z opisanymi powyżej zasadami. Ta zmiana wymaga udokumentowania w PTS/ePTS oraz wysłania przez Dostawcę/Właściciela/ASI zgłoszenia na Centralny ServiceDesk CIRF, zawierającego dokładny opis zmiany oraz zatwierdzony PTS/ePTS.

Zmiana technologii bloku architektonicznego wymaga ponownego dostarczenia oczekiwanej usługi, migracji danych na nowy blok oraz usunięcie nieeksploatowanego.

### 6.5.1 Narzędzie ePTS - <https://epts.mf.gov.pl>

Podstawą udzielenia dostępu do narzędzia jest zawarcie umowy wykonawczej z Zamawiającym oraz założenie konta w Active Directory.

Lista informacji jakie należy przygotować aby uzupełnić projekt ePTS:



 <div> <div>Centrum Informatyki</div> <div>Resortu Finansów</div> </div>	Nazwa jednostki organizacyjnej:	Centrum Informatyki Resortu Finansów	
	Tytuł dokumentu:	WYMAGANIA OGÓLNE DLA BUDOWANYCH SYSTEMÓW UTRZYMYWANYCH W INFRASTRUKTURZE CIRF	
	Wersja dokumentu:	1.0	Obszar IT
	Data opracowania:	24.10.2023	Kod zakresu dokumentu: RF / AK

Informacje podstawowe	
Nazwa projektu	Pełna nazwa systemu
Nazwa skrócona	Skrócona nazwa projektu która posłuży jako podstawa do nazewnictwa przyszłych bloków architektonicznych systemu
Opis projektu	Krótką charakterystyka systemu
Rodzaj środowiska	Minimum jedno środowisko systemu: produkcyjne PR, deweloperskie DE, testowe zewnętrzne TE, testowe wewnętrzne TI, szkoleniowe TR
Dane kontaktowe	Informacja o pełniących rolę: Administratora aplikacji systemu, Wykonawcy, Przedstawiciela AKMF, Menadżera usługi, Właściciela biznesowego
Rysunek logiczny	Rysunek logiczny architektury systemu w formacie PNG lub JPG
Terminy i skróty	Terminy i skróty specyficzne dla systemu jakie będą wykorzystywane w projekcie
Uwierzytelnienie	Uwierzytelnienie użytkowników w środowisko przez podanie: typu ich konta, sposobu uwierzytelniania, mechanizmu uwierzytelniania
Podstawowa architektura	
Ruch sieciowy	Przewidywane maksymalne obciążenie ze źródeł: Internet, Ekstranet, WAN (obciążenie sesji, max liczba użytkowników, liczba jednoczesnych sesji)
Klasa systemu	I (RTO 4h; RPO ≈0h; dostępność 99,4%) II (RTO 12h; RPO 12h; <u>dost.</u> 99%) III (RTO 48h; RPO 24h; <u>dost.</u> 98%) IV (RTO -; RPO -; <u>dost.</u> 96%)
Blok AP	Opis bloków aplikacyjnych technologie: aplikacji i OS; dane o VM: <u>vCPU</u> , <u>vRAM</u> (GB), <u>storage</u> (GB); krotność VM, grupowanie
Blok DB	Opis bloków bazodanowych technologie: baz danych i OS; dane o VM: <u>vCPU</u> , <u>vRAM</u> (GB), <u>storage</u> ; dane (GB), logi (GB); krotność VM, grupowanie
Blok OS	Opis bloków systemowych technologia OS; info o VM: <u>vCPU</u> , <u>vRAM</u> (GB), <u>storage</u> (GB); krotność VM, grupowanie
Backup	Zapoznanie się z polityką backupową CIRF. Opisanie ewentualnego odstępstwa
Dodatkowe oprogramowanie	Dodatkowe oprogramowanie za którego licencje i utrzymanie odpowiada klient
Dodatkowe komponenty	
Platforma	Opis platformy integracyjnej: system źródłowy, docelowy, komponenty (DP, IIB, MQ, IPT), szacowane obciążenie
Usługi HTTPS	Usługi dostępne HTTPS: nazwa bloku, wejście bloku (Internet, WAN), lista przekierowań
Load Balancer	Opis konfiguracji <u>Load Balancera</u> zewnętrznego i wewnętrznego dla poszczególnych usług aplikacyjnych
Certyfikat	Dostarczenie certyfikatu na potrzeby komunikacji HTTPS
Wpisy DNS	Dane do wpisów w DNS dla usług udostępnianych przez środowisko Systemu (ID bloku, nazwa domenowa, typ rekordu DNS, PTR)
Zasób współdzielony	Dodatkowy zasób współdzielony w technologiach: NFS, SMB, S3
Zabezpieczenia	Dostęp do poszczególnych bloków architektonicznych oraz określenie uprawnień (administrator, operator) dla poszczególnych osób
Konto DB	Uprawnienia do baz danych na poziomie ( <u>read only</u> , <u>read write</u> , administrator DB) dla poszczególnych osób
Konta serwisowe	Konto dedykowane do uruchomienia usługi lub dostępu do usługi. Bez możliwości logowania interaktywnego
Czynności serwisowe	Czynności serwisowe wymagające wyższych uprawnień (dane osoby po stronie Klienta, <u>hostname</u> serwerów których dot. konfiguracja, termin)
Przepuszczanie ruchu	Dane do przepuszczenia ruchu: dla administratora, dla komunikacji między systemami i wewnątrz systemu.

## 6.6 Ochrona antywirusowa

Wszystkie serwery - maszyny wirtualne tworzące Bloki Architektoniczne (z wyłączeniem zamkniętych bloków typu Virtual Appliance) są chronione Systemem Antywirusowym posiadanym przez CIRF. Ochrona ta jest realizowana metodą agentową. W każdym przypadku stosowane są standardowe polisy dla poszczególnych rodzajów bloków.

W szczególnych przypadkach jest możliwość zmiany polityk domyślnych (utworzenia nowej dla danego systemu, wykluczenia katalogów, rozszerzeń), po przesłaniu przez Dostawcę/Właściciela biznesowego/ASI zgłoszenia na Centralny ServiceDesk CIRF z dokładnym opisem, uzasadnieniem oraz zaktualizowanym dokumentem PTS, uwzględniającym tę zmianę.

W przypadku zaistnienia incydentu bezpieczeństwa polegającego na wykryciu niepożądanego oprogramowania, jest ono blokowane i powiadamiana jest komórka zajmująca się bezpieczeństwem teleinformatycznym w CIRF.

## 6.7 Zarządzanie logami

CIRF dysponuje centralnym systemem do zbierania i korelacji logów SIEM, który wykorzystuje się do zabezpieczania logów produkcyjnych. Infrastrukturalne logi dla środowisk produkcyjnych są zbierane automatycznie od momentu ich wykreowania. W przypadku logów aplikacyjnych i bazodanowych Dostawca/Właściciela Systemu/ASI planując budowę systemu jest zobowiązany poprzez zgłoszenie w Centralnym ServiceDesk poinformować CIRF o chęci przekazywania logów aplikacyjnych określając ich czas retencji oraz ich ilość w celu określenia kosztów z tym związanych. CIRF zapewnia Właścicielowi Systemu/ASI dostęp do logów systemu.



 <div> <div>Centrum</div> <div>Informatyki</div> <div>Resortu</div> <div>Finansów</div> </div>	Nazwa jednostki organizacyjnej:		Centrum Informatyki Resortu Finansów	
	Tytuł dokumentu:		WYMAGANIA OGÓLNE DLA BUDOWANYCH SYSTEMÓW UTRZYMYWANYCH W INFRASTRUKTURZE CIRF	
	Wersja dokumentu:	1.0	Obszar IT	TE
	Data opracowania:	24.10.2023	Kod zakresu dokumentu:	RF / AK

CIRF na podstawie informacji od ASI przygotowuje odpowiednie korelacje logów, ich wizualizacje oraz zarządza incydentami.

## 6.8 Kopia Zapasowa

CIRF dysponuje Centralnym Systemem Backupowym, który wykorzystuje się do zabezpieczania zasobów pracujących w infrastrukturze zarządzanej przez CIRF. Możliwość wykorzystania tego systemu do objęcia ochroną bloków architektonicznych zależy od wcześniejszych ustaleń z Dostawcą/Właścicielem Systemu/ASI i kwestią sfinansowania niezbędnych jego komponentów wynikających z wielkości środowiska, które ma zostać objęte kopią zapasową.

W ramach procesu tworzenia Bloków Architektonicznych w CIRF kopią zapasową obejmowane są tylko środowiska produkcyjne i wyłącznie zasoby systemowe tych środowisk, które są dostarczone w momencie wykreowania bloku (dyski systemowe, bazy danych systemowe). W ramach tego procesu nie są obejmowane tą ochroną żadne zasoby dostarczone/zbudowane przez Wykonawcę na etapie budowania systemu.

CIRF dokonuje modyfikacji zakresu danych, które mają być chronione mechanizmem kopii zapasowej, po przesłaniu przez Dostawcę/Właściciela Systemu/ASI zgłoszenia na Centralny ServiceDesk CIRF, w którym w sposób jednoznaczny zostanie opisany zakres danych, które muszą być zabezpieczone w ramach środowiska produkcyjnego (nazwy bloków architektonicznych, nazwy maszyn wirtualnych, wskazanie dysków/katalogów/baz danych, które podlegać mają zabezpieczeniu) oraz dołączony jest zatwierdzony i aktualny PTS opisujący te obszary.

W przypadku środowisk nieprodukcyjnych CIRF nie konfiguruje ochrony backupowej dla Bloków Architektonicznych składających się na te środowiska. Istnieje możliwość objęcia taką ochroną innych środowisk, jednak jest to realizowane na podstawie zgłoszenia przesłanego przez Dostawcę/Właściciela Systemu/ASI na Centralny Service Desk CIRF, w którym są wymienione dokładnie obszary, które mają być zabezpieczone (nazwy bloków architektonicznych, nazwy maszyn wirtualnych, wskazanie dysków/katalogów/baz danych, które podlegać mają zabezpieczeniu), oraz dołączony jest zatwierdzony i aktualny PTS/ePTS opisujący te obszary wraz z uzasadnieniem konieczności zabezpieczenia tych obszarów.

Ta dodatkowa ochrona jest realizowana po wcześniejszym ustaleniu pomiędzy CIRF a Właścicielem Systemu, gdyż jest to związane z finansowaniem komponentów infrastrukturalnych wymaganych dla realizacji mechanizmów ochrony kopią zapasową.

Każda zmiana w zakresie zadań i ochrony kopią zapasową wymaga przesłania zgłoszenia przez Dostawcę/Właściciela Systemu/ASI na Centralny Service Desk CIRF, w którym jednoznacznie jest opisany zakres oczekiwanej zmiany.

Ochrona w postaci Kopii Zapasowej umożliwia odzyskanie plików, baz danych, całych serwerów – maszyn wirtualnych, zgodnie ze zdefiniowaną polityką RPO i RTO w zależności od technologii bloku architektonicznego (jeśli wcześniej takie obszary zostały zgłoszone i procedury zostały wdrożone). Odzyskiwanie danych jest realizowane przez CIRF na podstawie zgłoszenia przesłanego przez Dostawcę/Właściciela Systemu/ASI na Centralny Service Desk, w którym jednoznacznie jest wymieniony zakres danych do przywrócenia oraz zakres czasowy, z którego dane mają być przywrócone.

Polityka ochrony danych za pomocą Centralnego Systemu Backupu CIRF umożliwia składowanie danych kopii zapasowych wykonywanych dla bloków architektonicznych o maksymalnym okresie retencji wynoszącym 14 dni. CIRF nie posiada systemu archiwizacji danych, który umożliwia składowanie kopii zapasowych w dłuższym okresie czasu niż 14 dni.


## 6.9 Zasoby przeznaczone na system – rozliczalność

W zależności od ustaleń, określonego finansowania jak też wstępnych wycen będących bazą do pozyskania finansowania, na potrzeby budowy, uruchomienia i eksploatacji systemu przez okres 3 lat CIRF przeznaczy i udostępni Wykonawcy następujące określone zasoby w poniższych kategoriach:

- sumaryczna liczba vCPU;
- sumaryczna liczba GB pamięci vRAM;
- sumaryczna wielkość przestrzeni dyskowej na składowanie danych netto w TB.

Powyższe wskaźniki określają wielkości, w ramach których Dostawca musi się zmieścić sumując parametry jednostkowe wszystkich maszyn wirtualnych, składających się na wszystkie bloki architektoniczne, dla wszystkich środowisk opisanych w dostarczonym dokumencie PTS/ePTS.

Wartości te nie mogą zostać przekroczone – Dostawca ma możliwość manewrowania parametrami

	Nazwa jednostki organizacyjnej:		Centrum Informatyki Resortu Finansów	
	Tytuł dokumentu:		WYMAGANIA OGÓLNE DLA BUDOWANYCH SYSTEMÓW UTRZYMYWANYCH W INFRASTRUKTURZE CIRF	
	Wersja dokumentu:	1.0	Obszar IT	TE
	Data opracowania:	24.10.2023	Kod zakresu dokumentu:	RF / AK

ilościowymi zgodnie z zasadami opisanymi powyżej.

Sumaryczna wielkość przestrzeni dyskowej na składowanie danych netto wyrażona w TB jest traktowana przez CIRF jako wartość netto. Wartość brutto jest większa o ok. 20-25%, gdyż należy zabezpieczyć dodatkowe zasoby wynikające z użytych technologii (przestrzeń na pliki migawkowe – snapshoty, pliki obrazu pamięci RAM – swap, rezerwa miejsca na wolumenach macierzowych itp.)

W celu zbilansowania wielkości skonsumowanej przestrzeni dyskowej netto, CIRF policzy:

- sumaryczną pojemność każdej maszyny wirtualnej wytworzonej na rzecz projektu, gdzie integralnym składnikiem jest dysk lokalny systemowy (ok 100GB), dysk na dane binarne/aplikacje oraz dysk lub dyski dodatkowe zamówione przez Wykonawcę (zgodnie z zatwierdzonym i aktualnym PTS/ePTS), dla wszystkich bloków architektonicznych we wszystkich środowiskach systemu;
- sumaryczną pojemność wszystkich zasobów zamówionych jako: współdzielona sieciowa przestrzeń „plikowa” (na podstawie zatwierzonego i aktualnego PTS/ePTS), dla wszystkich środowisk systemu;
- sumaryczną pojemność wszystkich zasobów zamówionych jako: współdzielona sieciowa przestrzeń „obiektowa” (na podstawie zatwierzonego i aktualnego PTS/ePTS), dla wszystkich środowisk systemu.

Po wyliczeniu w/w elementów dokona ich zsumowania i przeliczenia na jednostkę TB. Wartość będąca wynikiem tej operacji musi być niższa lub równa wartości określonej jako „sumaryczna wielkość przestrzeni dyskowej na składowanie danych netto”.

## 6.10 Inne wymagania dla Wykonawców rozwiązań aplikacyjnych na infrastrukturze CIRF

- Wszystkie wymagane funkcjonalności związane z dostępnością usług biznesowych muszą być skonfigurowane przez Wykonawcę w taki sposób aby uruchamiały się automatycznie. Wznawianie połączeń i usług po restarcie usług na zewnętrznych blokach ma działać w sposób automatyczny.
- Dostawca aplikacji jest zobowiązany do dostarczania aktualizacji zainstalowanych na blokach komponentów (w tym oprogramowania dodatkowego).
- CIRF rekomenduje projektowanie i budowanie komunikacji pomiędzy komponentami systemu w oparciu o FQDN – jednoznaczne nazwy domenowe, zamiast odnoszenia się do IP konkretnych maszyn wirtualnych.

## 6.11 Podstawowe standardy sieci

Informacje dotyczące sieci LAN i WAN CIRF, z uwzględnieniem zasad dostępu do podstawowych usług sieciowych opisano w dokumencie „Standardy sieci CIRF”, traktowanym jako Informacja chroniona CIRF, który stanowi załącznik nr 1 do niniejszego dokumentu.


## 6.12 Platforma Integracyjna resortu finansów

Platforma Integracyjna to rodzaj rozwiązania technologicznego, które umożliwia łączenie różnych systemów, aplikacji i danych w jedną spójną i zintegrowaną infrastrukturę. Głównym celem platformy integracyjnej jest ułatwienie przepływu informacji i zapewnienie interoperacyjności między różnymi technologicznymi elementami organizacji oraz systemami z poza organizacji. Koncepcja architektury Platformy integracyjnej opiera się o wzorzec integracyjny Service Oriented Architecture (SOA). Architektura SOA rozkłada komponenty procesów biznesowych na podstawowe elementy składowe, które mogą być wykorzystane w wielu miejscach przez wiele aplikacji/systemów, świadcząc usługi zgodnie z założonymi procesami biznesowymi. Rozwiązanie to umożliwia wykorzystanie komunikacji asynchronicznej i synchronicznej oraz obsługuje różne protokoły komunikacyjne, takie jak HTTP, SOAP, REST, JMS, MQTT, AMQP, MQ czy inne, co pozwala na integrację z różnymi rodzajami systemów.

„Platforma Integracyjna” została przedstawiona w załączniku nr 2 do niniejszego dokumentu i sklasyfikowana jako Informacja chroniona CIRF.

## 6.13 Monitorowanie systemów i usług biznesowych

Centralnymi narzędziami do monitoringu stanu systemów i usług biznesowych w CIRF są NAGIOS2 oraz CSM2. Narzędzia te mają różne przeznaczenie, natomiast wzajemnie się uzupełniają. Trzecim, opcjonalnym narzędziem jest Dynatrace.

 <div> <div>Centrum</div> <div>Informatyki</div> <div>Resortu</div> <div>Finansów</div> </div>	Nazwa jednostki organizacyjnej:	Centrum Informatyki Resortu Finansów	
	Tytuł dokumentu:	WYMAGANIA OGÓLNE DLA BUDOWANYCH SYSTEMÓW UTRZYMYWANYCH W INFRASTRUKTURZE CIRF	
	Wersja dokumentu:	1.0	Obszar IT
	Data opracowania:	24.10.2023	Kod zakresu dokumentu: RF / AK

### 6.13.1 NAGIOS2 (checkmk)

Nagios, a dokładnie Checkmk w wersji 2.2 odpowiada głównie za monitorowanie warstw infrastrukturalnych, czyli m.in. parametrów systemów operacyjnych serwerów wirtualnych oraz składników na nich zainstalowanych. Monitorowanie odbywa się za pomocą agenta, który zawarty jest w template'ach maszyn wirtualnych przygotowanych przez CIRF i wydawanych Klientowi na podstawie wniosków o blok architektoniczny w CSD. Każdy serwer oddawany do użytku Klientowi, jest z automatu dodawany również do systemu monitorowania NAGIOS2.

Komunikacja między agentem, a serwerami Nagios odbywa się po porcie 6556, a ruch nawiązuje agent. Defaultowe parametry, które są monitorowane dla poszczególnych rodzajów bloków przedstawiono w załączniku nr 3 do niniejszego dokumentu „Wymagania\_Ogólne\_dla\_budowanych\_Systemów\_Nagios”.

System ten pozwala również budować własne czujki i umieszczać je w odpowiednim katalogu na monitorowanych serwerach. Są to skrypty lokalne pisane np. w BASH lub PowerShell, które w odpowiedniej konstrukcji zwracają wyniki i są interpretowane przez system monitorowania. Ponadto, bezpośrednio z serwerów Nagios można sprawdzać i monitorować inne elementy, weryfikujące stan aplikacji, strony http czy bazy danych. To jednak nie jest dodawane w standardzie i każda taka potrzeba musi być zgłoszona do wydziału odpowiedzialnego za systemy monitorowania w CIRF.

Przykładowe sprawdzenie:

- testowanie usługi http/https, wyszukiwanie wyrażeń regularnych na stronie, śledzenie przekierowań, kodów odpowiedzi, sprawdzanie czasów połączeń i raportowanie czasów wygaśnięcia certyfikatów;
- wykonanie selectu na bazie (PostgreSQL, MSSQL, MYSQL) w zdefiniowanym formacie w celu weryfikacji jej działania, bądź też w celu zwrócenia określonego wyniku i alertowania w przypadku przekroczenia progów;
- sprawdzanie czasów odpowiedzi na portach z systemu monitorowania;
- wysyłanie zapytań do elasticsearch o występowanie specyficznych komunikatów, ustawienia progów na liczbę messages;
- monitorowanie stanu usług linuxowych udostępnianych przez polecenie systemctl;
- monitorowanie procesów linux/windows – dostępność procesu/progi wydajnościowe;
- monitorowanie stanu usług windowsowych;
- monitorowanie środowiska Kubernetes;
- monitorowanie maszyny wirtualnej Javy poprzez agenta Jolokia;
- dodatkowe statystyki związane z pracą Apache.

**WAŻNE:** Aby system biznesowy był monitorowany produkcyjnie 24/7 przez zespół monitoringu CIRF, musi być dostarczony podpisany wniosek o dopuszczenie systemu do użytkowania produkcyjnego - KARTA DOPUSZCZENIA/WYCOFANIA SYSTEMU DO WYKORZYSTANIA PRODUKCYJNEGO.


### 6.13.2 CSM2 (inTrack)

Oprogramowanie to skupia się na wysokopoziomowym monitorowaniu usługi biznesowej dostarczanej do Klienta jako całości. Implementowane są tu m.in. scenariusze EUM (end user monitoring) naśladujące ruchy Klienta w udostępnionej usłudze. Badane są czasy i kody odpowiedzi stron www oraz innych endpointów mających wpływ na działanie usługi. System ma również możliwość monitorowania baz danych np. PostgreSQL, Oracle itp. za pomocą selectów oraz budowania własnych skryptów w języku PYTHON. Intrack posiada możliwość wzbogacania metryk w progowanie oraz wysyłkę powiadomień e-mail (notyfikacje), wyliczenie i generowanie raportów SLO dla monitorowanych usług oraz możliwość tworzenia dashboardów. Monitorowanie odbywa się za pomocą wykonywanych scenariuszy zaimplementowanych na próbnikach CSM2.

**WAŻNE:** Wszystkie potrzeby w zakresie CSM2 powinny być zgłaszane przez ASI lub menadżerów usług do wydziału odpowiedzialnego za systemy monitorowania w CIRF, w celu objęcia monitorowaniem usługi tym narzędziem.

### 6.13.3 Dynatrace

Jest to oprogramowanie klasy APM (Application Performance Monitoring), które monitoruje wydajność aplikacji oraz jej komponentów składowych. Jest to zaawansowane narzędzie, które jest stosowane dla wybranych, kluczowych usług biznesowych. Za pomocą modułu DEM możliwe jest badanie odczuć cyfrowych

 <div> <div>Centrum</div> <div>Informatyki</div> <div>Resortu</div> <div>Finansów</div> </div>	Nazwa jednostki organizacyjnej:		Centrum Informatyki Resortu Finansów	
	Tytuł dokumentu:		WYMAGANIA OGÓLNE DLA BUDOWANYCH SYSTEMÓW UTRZYMYWANYCH W INFRASTRUKTURZE CIRF	
	Wersja dokumentu:	1.0	Obszar IT	TE
	Data opracowania:	24.10.2023	Kod zakresu dokumentu:	RF / AK

użytkownika, może to być wykonywane na trzy sposoby – Synthetic Monitoring, Real User Monitoring, Session Replay - możliwość monitorowania 100% transakcji użytkownika. Technologia Smartscape pozwala na budowanie dynamicznych i automatycznych wizualizacji aplikacji, co zapewnia kompleksową możliwość obserwacji wszystkich komponentów aplikacji i zależności w górę, w dół i na wszystkich poziomach stosu technologicznego. Za pomocą wbudowanej AI pozwala na działania proaktywne - wykrywanie root cause. AI automatycznie wykrywa problemy napotykane przez klientów i wykorzystuje informację o topologii, transakcjach, wykonywanym kodzie, aby precyzyjnie określić pierwotną przyczynę problemów. Instrumentacja odbywa się w sposób automatyczny i wymaga zainstalowania Agenta Dynatrace Oneagent (ruch inicjuje agent na porcie 443). Rozszerzenie monitoringu o jeszcze dodatkowe dane możliwe jest poprzez wykorzystanie wtyczek uruchamianych z ActiveGate.

**WAŻNE:** Dynatrace jest narzędziem płatnym, zatem objęcie monitorowaniem tym narzędziem wiąże się z koniecznością dostarczenia do CIRF środków na ten cel.

## 7. Wyjątki

Nie dotyczy.

## 8. Obowiązkiwanie dokumentu

### 8.1. Wejście w życie dokumentu

Dokument wchodzi w życie z dniem jego zatwierdzenia przez Dyrektora Centrum Informatyki Resortu Finansów.

### 8.2. Termin obowiązywania

Dokument obowiązuje do odwołania.

### 8.3. Uregulowania przejściowe

Nie dotyczy.

## 9. Odwołanie dokumentu

Nie dotyczy.

## 10. Załączniki

Wszystkie dokumenty sklasyfikowane w powyższym dokumencie jako Informacja chroniona CIRF zostaną:

- udostępnione podmiotowi spoza resortu finansów, biorącemu udział w postępowaniu zgodnym z ustawą Prawo Zamówień Publicznych, po podpisaniu stosownego oświadczenia o poufności informacji i wykorzystania ich jedynie w celu złożenia oferty lub
- udostępnione Wykonawcy po podpisaniu umowy z Zamawiającym.

Poniższe dokumenty stanowią Informację chronioną CIRF:

1. załącznik nr 1 - Standardy sieci CIRF
2. załącznik nr 2 - Platforma Integracyjna
3. załącznik nr 3 - Wymagania ogólne dla budowanych systemów – Nagios