Załącznik nr 1 A - Macierz dyskowa

Parametr	**Szczegółowy opis wymagania**
Obudowa	Obudowa typu Rack 19” – musi być dostarczona wraz z szynami do instalacji w szafie umożliwiającymi jej serwisowanie. Macierz musi być wyposażona w minimum 2 kontrolery Do urządzenia należy dołączyć kable połączeniowe zgodnie z ilością portów i rodzajem zainstalowanych modułów. Oferowane rozwiązanie musi zawierać się w obudowie o maksymalnej wysokości 2U
Skalowalność	Macierz musi umożliwiać skalowalną rozbudowę on-line Scale-out do minimum 8 kontrolerów zarządzanych z jednej konsoli i 372 dysków oraz Scale-in poprzez dodawanie półek dyskowych do par kontrolerów. Pojedyncza para kontrolerów musi umożliwiać obsługę minimum 90 dysków NVMe. Po takiej rozbudowie musi być możliwość zaprezentowania każdego wolumenu logicznego LUN przez dowolny z kontrolerów bez przerywania dostępu do danych. Oferowane rozwiązanie musi mieć możliwość rozbudowy do 360 rdzeni oraz minimum 7TB pamięci RAM. Rozbudowa nie może powodować wymiany zastosowanych dysków twardych ani kontrolerów.
Kontrolery	Procesory w kontrolerach muszą być wykonane w technologii x86 wiodących producentów - Intel lub AMD. Każdy kontroler macierzy musi być wyposażony w co najmniej 96GB przestrzeni cache służącej do buforowania operacji odczytu oraz zapisu. Kontrolery muszą wspierać jednocześnie ruch - blokowy i plikowy (wymagane protokoły: iSCSI, FC oraz plikowy CIFS - minimum SMB w wersjach 3, 3.1 FTP i SFTP oraz NFS 3, 4, 4,1 4,2). Nie dopuszcza się realizacji funkcjonalności ruchu plikowego za pomocą dodatkowych zewnętrznych urządzeń. Oferowane rozwiązanie musi obsługiwać protokół NVMe na całej ścieżce komunikacji (front-end, back-end). Nie dopuszcza się stosowanie rozwiązania, w którym rozbudowa o dodatkowe półki dyskowe odbywała się po protokole innym niż NVMe. Macierz musi natywnie wspierać protokół NVMe-OF w tym NVMe-OF/TCP oraz NVMe-OF/FC. Kontrolery te muszą działać w sposób redundantny – tj. przy uszkodzeniu dowolnego kontrolera, macierz musi nadal działać i utrzymywać dostęp do odczytu i zapisu danych. Praca w trybie active/active w taki sposób, aby oba kontrolery były aktywne i w tym samym czasie udostępniały urządzenia LUN oraz zasoby plikowe. Oba kontrolery muszą brać czynny udział w obsłudze wszystkich operacji (snapshot, clone, replikacja). Nie dopuszcza się rozwiązania, w którym jeden z kontrolerów działa jedynie jako urządzenie

	przekazujące ruch do hostów. Oba kontrolery dyskowe muszą mieć jednoczesny dostęp do wszystkich dysków w macierzy, które przechowują dane użytkownika. Nie dopuszcza się przypisywania dysków tylko do jednego kontrolera. Macierz musi być odporna na awarię pamięci cache, w szczególności cache przeznaczony do zapisu (ang. write cache) i zapewniać w razie utraty zasilania zabezpieczenie danych niezapisanych na dyski przez nieograniczony czas. Cache do zapisu musi być dostępny w tym samym czasie z obu kontrolerów oraz musi być chroniony przez protekcję RAID1. Każdy kontroler macierzy musi być oparty o jeden wielordzeniowy procesor (minimum 12 rdzeni) i pracować z częstotliwością minimum 2.2 GHz. Macierz musi umożliwiać wykonywanie procesu aktualizacji mikrokodu w trybie online bez przerywania dostępu do zasobów dyskowych macierzy i przerywania pracy aplikacji.
Zasilanie	Urządzenie musi być wyposażone w podwójny, redundantny system zasilania i chłodzenia, gwarantujący nieprzerwany dostęp do wolumenów dyskowych (LUN) oraz działania pamięci cache w przypadku awarii jednego ze źródeł zasilania. Pojedynczy zasilacz nie może przekraczać mocy 1450W.
Przestrzeń dyskowa	Dostarczona Macierz musi zapewnić przestrzeń efektywną (po zastosowaniu mechanizmów kompresji i deduplikacji) minimum 320TiB Osiągnięta przestrzeń 320TiB musi być zapewniona i gwarantowana przez producenta macierzy (Wymagane dostarczenie oświadcznia producenta oferowanej macierzy). Macierz musi posiadać możliwość zapełnienia całej dostarczonej przestrzeni. Jeśli macierz pozwala na zapełnienie tylko części przestrzeni (np. 80%) to pozostająca „pusta- niewykorzystana" przestrzeń nie będzie wliczona w dostarczoną przestrzeń. Oferowana przestrzeń musi składać się minimum 12 dysków SSD NVMe Hot-Swap o pojemności min. 7.68TB. Nie dopuszcza się stosowania dedykowanych modułów zamiast urządzeń dyskowych SSD z komórkami innymi niż TLC oraz NVRAM. Macierz musi umożliwiać instalację minimum 13 dodatkowych dysków NVMe bez dodawania półek, kontrolerów, czy innych elementów. Oferowana macierz musi umożliwiać rozbudowę z granulacją jednego dysku. Macierz w dostarczonej konfiguracji (z włączoną deduplikacją i kompresją) musi umożliwiać osiągnięcie wydajności minimum 99 tysięcy IOPS z przestrzeni dyskowej (przy założeniach: dla bloku danych o wielkości 8k odczyt 70%, zapis 30% oraz wszystkie operacje losowe, 0% trafień w cache) Macierz w dostarczonej konfiguracji (z włączoną deduplikacją i kompresją)

	musi umożliwiać osiągnięcie minimum 770 MiB/s odczytu z przestrzeni dyskowej (nie z cache macierzy) W zaproponowanej konfiguracji macierzy należy także zabezpieczyć przestrzeń hot/spare według zaleceń producenta macierzy. Niedopuszczalne jest zastosowanie dedykowany dysków jako dyski hot-spare. Macierz w żadnej konfiguracji nie może oferować obsługi dysków obrotowych, a co za tym idzie nie może oferować rozbudowy o dyski obrotowe czyli musi być rozwiązaniem zaprojektowanym tylko i wyłącznie do dysków SSD lub modułów flash. Do oferty należy dołączyć wydruk z narzędzia producenta oferowanej macierzy konfiguratora / estymatora – potwierdzony przez producenta, potwierdzający spełnienie powyższych wymagań (zawierający zarówno proponowaną konfigurację sprzętową z dokładnym wskazaniem part number'ów elementów jak i ich ilości, w tym typów i okresów wsparcia licencji i gwarancji) jak i wynikające z niej parametry pojemnościowe i wydajnościowe)
Redukcja danych	Rozwiązanie musi zapewniać mechanizm kompresji i deduplikacji danych w trybie in-line. Kompresja i deduplikacja muszą być integralną częścią systemu macierzowego bez możliwości zatrzymania bądź wyłączenia przez administratora. Mechanizmy kompresji i dedpuplikacji muszą być przezroczyste dla administratora macierzy. Proces deduplikacji musi odbywać się globalnie (minimum w ramach pary kontrolerów). Wobec powyższych wymagań dla każdego wolumenu macierzy musi zachodzić jednocześnie kompresja i deduplikacja danych, która nie wymaga konfiguracji ani żadnej innej interwencji ze strony administratora macierzy. Operacje kompresji i deduplikacji muszą działać na wszystkich rodzajach dostarczanych i opcjonalnych nośników SSD i być dostępne dla wszystkich rodzajów przechowywanych danych (nie jest dozwolone oferowanie rozwiązań, które nie zapewniłyby kompresji i deduplikacji na całej wymaganej pojemności). Redukcja danych musi być wspierana przez dedykowany układ sprzętowy poza procesorem kontrolera macierzy. Mechanizmy redukcji danych muszą być realizowane za pomocą zmiennego bloku, aby zapewnić maksymalną skuteczność tych procesów. Wymagane jest zagwarantowane przez producenta oferowanej macierzy osiągnięcie współczynnika redukcji danych dla całej macierzy na poziomie 5:1 przy spełnieniu wymagań pojemnościowych określonych w punkcie

	Przestrzeń dyskowa. Jeżeli producent nie gwarantuje współczynnika redukcji danych dla całej macierzy na poziomie 5:1, lub gwarantuje je w niższym stopniu, należy dostarczyć taką przestrzeń użyteczną, aby przestrzeń efektywna wynosiła 320TiB W powyższej kalkulacji nie będzie wymagane uwzględnienie danych wcześniej zaszyfrowanych (z pominięciem mechanizmu szyfrowania przez macierz) i wcześniej skompresowanych. Macierz musi mieć funkcjonalność umożliwiającą wyświetlenie informacji na temat danych, które globalnie nie uległy redukcji danych.
Obsługa dysków	Macierz dyskowa musi umożliwiać stosowanie w niej na potrzeby składowania danych minimum dysków, SSD NVMe**.** Oferowana macierz musi obsługiwać dyski TLC lub QLC. W szczególności dyski QLC muszą posiadać dwa interfejsy do jednoczesnego dostępu przez dwa kontrolery. Nie dopuszcza się stosowania dysków lub modułów dyskowych które, rezlizują redukcję danych. Redukcja danych może być tylko globalna. Dopuszcza się tylko operacje szyfrowania (dyski SED) Macierz musi być wyposażona w dyski posiadające podwójne interfejsy. Wymagane jest szyfrowanie danych na dyskach zgodnie z FIPS 140-2 dla wszystkich zainstalowanych nośników. Należy dostarczyć niezbędne licencje na całą pojemność macierzy. Macierz musi mieć funkcjonalność rozszerzania puli dyskowej z granulacją co jeden dysk.
Porty macierzowe	Oferowane urządzenie musi być wyposażone w minimum: 8 portów 25 Gbps, obsadzone modułami Optical 25Gb SR 2 porty 1Gbit przeznaczone do zarządzania macierzą Musi być zapewniona możliwość rozbudowy macierzy o minimum: - 8 portów FC 32Gb lub - 8 portów 25Gb iSCSI jedynie poprzez instalację dodatkowych kart rozszerzeń bez konieczności wymiany kontrolerów.
Poziomy RAID	Macierz musi umożliwiać budowę jednego obszaru danych na wszystkich dyskach wewnątrz macierzy. Dyski muszą być skonfigurowane w taki sposób, aby utrata dwóch dowolnych z nich zapewniła ciągłość dostępu do danych. Macierz musi posiadać skonfigurowaną wydzieloną przestrzeń spare-space zgodnie z zaleceniami producenta.

Kompatybilność	Rozwiązanie musi wspierać następujące środowiska wirtualne oraz aplikace wykorzystywane przez Zamawiającego: VMware, MS Hyper-V, MS Windows, Linux, Oracle, aplikacje: MS Exchange, MS SQL
Integracja z aplikacjami	Oferowana macierz dyskowa musi zostać dostarczona z oprogramowaniem umożliwiającym zarządzanie i automatyzację procesów replikacji oraz ochrony danych z wykorzystaniem mechanizmu migawek (snapshots). Konieczne jest zapewnienie efektywnego tworzenia i przywracania kopii zapasowych, a także szybkiego odzyskiwania danych z uwzględnieniem ich spójności z wykorzystaniem migawek. Oferowane rozwiązanie powinno oferować integrację z istniejącymi aplikacjami zamawiającego (MS Exchange) oraz bazami danych (Oracle RAC, MS SQL), zapewniając możliwość optymalizacji i synchronizacji procesów ochrony danych (migawki i replikacja). Wymagane jest, aby oprogramowanie to wspierało zarówno środowiska wirtualne, jak i fizyczne. Zamawiający wymaga aby dostarczona funkcjonalność była realizowana przez dedykowane oprogramowanie producenta macierzy.
Bezpieczeństwo	Macierz musi mieć wbudowany mechanizm uwierzytelniania dwuskładnikowego możliwy do natychmiastowego uruchomienia, który wykorzystuje tokeny sprzętowe lub programowe do zwiększenia bezpieczeństwa dostępu. Macierz musi umożliwiać pobranie kluczy szyfrujących dla każdego dysku celem przechowywania poza obrębu macierzy, co podnosi bezpieczeństwo. Macierz musi obsługiwać KMIP (Key Management Interoperability Protocol). Macierz musi posiadać funkcjonalność audytu wszystkich czynności wykonanych przez zalogowanych użytkowników. Wszystkie powyższe funkcjonalności muszą być realizowane przez kontrolery macierzy.
Funkcjonalności	System musi obsługiwać natywną integrację z środowiskiem wirtualizacyjnym VMware za pomocą interfejsu VAAI (VMware vStorage API for Array Integration), umożliwiając przypisanie do podsystemu pamięci masowej operacji VMware, takich jak klonowanie/snap, replikacja vVol, monitoring wydajności i mechanizmu vMotion. Rozwiązanie musi integrować się z wirtualnymi środowiskami poprzez dostarczenie przez producenta macierzy narzędzia do zarządzania i monitorowania. Rozwiązanie musi obsługiwać funkcję Local Protection (Snapshot z technologią Redirect-On-Write dla danych blokowych i plikowych i Thin Clones), rozwiązania, które nie obsługują funkcji redirect on write nie są dozwolone. Rozwiązanie musi obsługiwać replikację asynchroniczną na poziomie wirtualnych wolumenów (vVOL). Prezentacja replikowanych wirtualnych

	wolumenów musi się odbywać za pomocą protokołów SCSI oraz NVMe (rozdzielnie) Należy dostarczyć oprogramowanie do wykonywania spójnych kopii danych aplikacji w minimum wersjach: a) Exchange 2016 i 2019, SQL Server 2017 i 2019, Oracle 18 i 19, VMware dla blokowych i plikowych datastore. b) Spójność kopii rozumieć należy jako funkcjonalność automatycznego przełączenia aplikacji w tryb wykonania spójnej kopii swoich danych. c) Oprogramowanie to musi rozpoznać, na których wolumenach logicznych aplikacja składuje swoje dane i wykonać kopie tylko tych wolumenów. Macierz zarówno na poziomie jednej macierzy, jak i klastra – musi być zarządzana z poziomu jednej aplikacji, dostarczonej przez producenta urządzenia. Nie dopuszcza się dzielenia zarządzania pomiędzy różne aplikacje. Urządzenie powinno na poziomie plikowym umożliwiać zdefiniowanie blokady skasowania danych (funkcjonalność WORM). Blokada skasowania danych musi chronić plik w zdefiniowanym czasie przed usunięciem pliku, modyfikacją pliku. Blokada skasowania danych musi działać w dwóch trybach (do wyboru przez administratora): 1. Możliwość zdjęcia blokady przed upływem ważności danych 2. Brak możliwości zdjęcia blokady przed upływem ważności danych (COMPLIANCE), w tym wypadku wymagane wsparcie norm SEC 17a-4(f) lub ISO Standard 15489-1 w zakresie ochrony danych. Licencje na blokadę usunięcia/zmiany przechowywanych plików muszą być dostarczone wraz z urządzeniem na całą dostarczoną pojemność.
Replikacja	Ofertowana macierz musi wspierać replikację synchroniczną i asynchroniczną na poziomie zasobów blokowych oraz plikowych. Replikowane pary wolumenów blokowych muszą mieć możliwość prezentacji do wybranego hosta lub grupy hostów za pomocą protokołu SCSI oraz NVMe (rozdzielnie). Musi istnieć możliwość zmiany sposobu replikacji dla zasobów blokowych z synchronicznego na asynchroniczny i odwrotnie bez konieczności potrzeby zatrzymywania procesu replikacji. Rozwiązanie musi obsługiwać dwukierunkową asynchroniczną zdalną

	replikację przez IP z opcją ustawienia relacji do: "1:1", "1:n", i "n:1".
Klaster HA zasobów dyskowych	Dostarczone rozwiązanie musi posiadać funkcjonalność replikacji wolumenu w trybie synchronicznym w taki sposób, aby możliwy był jednoczesny zapis i odczyt z obu replikowanych wolumenów na obu macierzach w tym samym momencie. Dodatkowo w razie całkowitej utraty jednej z macierzy, powinny zadziałać mechanizmy wysokiej(HA) dostępności w taki sposób, aby dostęp do wolumenu był nieprzerwany z punktu widzenia serwerów korzystających z zasobów macierzy. Replikacja synchroniczna między macierzami musi odbywać się za pomocą protokołu IP. Funkcjonalność musi być integralną funkcją macierzy. Nie dopuszcza się stosowania urządzeń zewnętrznych.
	Musi istnieć taka możliwość konfiguracji macierzy dyskowych realizujących funkcjonalność klastra HA zasobów dyskowych, aby nie było konieczności używania tzw. świadka (Storage witness, Storage quorum, Storage tiebreaker).
	Funkcjonalność klastra HA zasobów dyskowych musi być realizowana w taki sposób, aby w przypadku całkowitej niedostępności jednej z macierzy dyskowych, ścieżki prezentowane do serwerów i obsługiwane z drugiej macierzy przez multipathing były cały czas dostępne (status ACTIVE/ENABLED)
Quality of Service	Oferowana macierz musi umożliwiać definiowanie polityk Quality of Service na podstawie następujących algorytmów z możliwością przypisania do hosta lub grupy hostów.: 1. Względne polityki wydajnościowe - definicja minimum trzech poziomów profili wydajnościowych 2. Bezwzględne polityki wydajnościowe - definicja na podstawie ilości IOPS oraz MB/s. 3. Bezwzględne polityki wydajnościowe - definicja na podstawie ilości IOPS oraz MB/s w przeliczeniu na wskazaną ilość danych w GB. 4. Bezwzględne polityki wydajnościowe - definicja na podstawie ilości IOPS oraz MB/s z możliwością warunkowego przekroczenia limitu o zadaną wielkość wyrażoną w procentach ustawionego limitu.
Gwarancja	Minimum 3 lata gwarancji wsparcia producenta w miejscu instalacji. Możliwość zgłaszania awarii przez 24 godziny na dobę. Gwarantowany czas reakcji – następny dzień roboczy. Macierz musi umożliwiać pracę oraz wdrożenie w środowisku całkowicie odizolowanym od dostępu do Internetu. Macierz może wysyłać metadane (dane serwisowe) tylko na teren państw Unii Europejskiej lub do państw należących do Paktu Północnoatlantyckiego (NATO).

	Macierz musi mieć możliwość ustawienia okna serwisowego o wskazanym czasie trwania. Podczas okna serwisowego pojawiające się zdarzenia na macierzy nie mogą być wysyłane do centrum wsparcia technicznego.

Macierz musi miec mozliwość dodania jej do oprogramowania dostępnego w chmurze, które zapewnia monitorowanie i rozwiązywanie problemów infrastruktury IT (serwerów/macierzy/ rozwiązań hiperkonwergentnych/przełączników sieciowych/deduplikatora). Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności:

Parametr	**Charakterystyka (wymagania minimalne)**
Monitoring	▪ ilość podłączonych oraz rozłączonych systemów ▪ stan podłączonych urządzeń ▪ informacje o potencjalnych zagrożeniach związanych z cyberbezpeczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów ▪ Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia ▪ informacje o statusie gwarancji dla poszczególnych urządzeń ▪ informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń ▪ informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych. ▪ Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych ▪ Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych. ▪ Monitorowanie wydajności, przepustowości oraz opóźnień dla systemów pamięci masowych. ▪ Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC. ▪ Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej. ▪ Monitoring parametrów serwerów z informacją o minimum: ▪ Obciążeniu procesora ▪ Zużyciu pamięci RAM ▪ Temperaturze procesorów ▪ Temperaturze powietrza wlotowego ▪ Zużyciu energii elektrycznej ▪ Zmianach w fizycznej konfiguracji serwera ▪ Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. • Monitoring parametrów pamięci masowych z informacją o minimum: ▪ Opóźnieniach

	▪ IOPS ▪ Przepustowości ▪ Utylizacji kontrolerów ▪ Pojemność całkowita i dostępna ▪ Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów. ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ▪ Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata ▪ Informacje o poziomie redukcji danych ▪ Informacje o statusie replikacji oraz snapshotów • Monitoring parametrów przełączników sieciowych z informacją o minimum: ▪ Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny ▪ Stanie komponentów: zasilacze, wentylatory ▪ Podłączonych hostach ▪ Ilości i statusu portów ▪ Utylizacji procesora ▪ Utylizacji poszczególnych portów ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach.
Aktualizacja firmware	▪ możliwość aktualizcji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania ▪ możliwość aktualizcji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania ▪ możliwość aktualizcji firmware, oprogramowania zarządzającego dla rozwiazań HCI, wraz z informacją o zalecanych wersjach oprogramowania ▪ możliwość aktualizcji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania ▪ możliwość aktualizcji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania
Raporty	▪ Możliwość generowania raportów dla serwerów zawierających informację o: ▪ Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej ▪ Średnim obciążeniu: procesorów, pamięci RAM, IO, ▪ Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o: ▪ Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji

	▪ Generowanie raportów do plików CSV i PDF
Cyberbezpieczeństwo	Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiednią ocenę stanu bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia. Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń. Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych. Możliwość przypisania dedykowanych ról dla poszczególnych administratorów.
Wirtualny asystent	Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy AI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury;
Inne	Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android
Certyfikaty i standardy	Oferowana platforma musi być zaprojektowana zgodnie ze standardami: ▪ ISO 27001 ▪ NIST Security and Privacy Controls for Federal Information Systems and Organization ▪ CSA Cloud Control Matrix