



Fundusze Europejskie

K O N F E R E N C J A

Cyberbezpieczeństwo w zamówieniach publicznych

Warszawa, 12 września 2025 r.



Fundusze
Europejskie



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską





Fundusze Europejskie

Chmura w Sektorze Publicznym

Szanse, Ryzyka i Bezpieczeństwo Danych

Aleksander Wojdyła
Securitum



Fundusze
Europejskie



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską





Aleksander Wojdyła

Securitum

- Konsultant ds. cyberbezpieczeństwa
- 5+ lat doświadczenia
- Certyfikaty: CISSP, OSEP, OSCP, ISO27001
- Bezpieczeństwo chmury, infrastruktury, aplikacji internetowych, rozwiązań AI
- Zgodność NIS2, DORA, RODO
- Ponad 15 000 przeszkolonych osób

Agenda

- Wprowadzenie i kontekst zamówień publicznych
 - Modele i rodzaje chmur
- Stan wdrożeń w Polsce i przykłady międzynarodowe
 - Szanse i ryzyka w sektorze publicznym
 - Bezpieczeństwo i regulacje prawne
 - Dobre praktyki i rekomendacje
 - Podsumowanie i dyskusja

Dlaczego chmura w zamówieniach publicznych?

- Przyspieszenie cyfryzacji usług publicznych - krótszy czas wdrażania e-usług dla obywateli i przedsiębiorstw
- Poprawa dostępności - usługi dostępne 24/7, także przy zwiększonym obciążeniu (np. ePUAP, systemy rejestracji)
- Elastyczne skalowanie - możliwość dostosowania zasobów do sezonowych potrzeb administracji
- Efektywność kosztowa - odejście od dużych nakładów inwestycyjnych (CAPEX) na rzecz modelu abonamentowego (OPEX)
- Ciągłość działania - wyższa odporność na awarie dzięki centrom danych i mechanizmom redundancji

Modele usług chmurowych

Model	Co zapewnia dostawca	Co po stronie zamawiającego	Zastosowania i uwagi
IaaS (infrastruktura jako usługa)	Centra danych, wirtualizacja, podstawowe sieci, dostępność	Systemy i sieci (konfiguracja, łatki), kopie zapasowe, tożsamość i uprawnienia, bezpieczeństwo aplikacji	Gdy potrzebna specyficzna konfiguracja korzyść: pełna kontrola nad środowiskiem ryzyko: większy ciężar operacyjny i ryzyko błędów konfiguracji
PaaS (platforma jako usługa)	Środowisko uruchomieniowe, bazy danych, narzędzia wdrożeniowe, automatyczne skalowanie	Kod i dane, polityki dostępu, testy i zgodność	Dla nowych e-usług i szybkich wdrożeń; korzyść: mniej zadań administracyjnych, krótszy czas wdrożenia ryzyko: zależność od platformy, trudniejsze przeniesienie
SaaS (oprogramowanie jako usługa)	Gotowa aplikacja, utrzymanie, aktualizacje, bezpieczeństwo na poziomie usługi	Konfiguracja, role i uprawnienia, integracje, nadzór zgodności	Typowe narzędzia urzędowe (poczta, obieg dokumentów); korzyść: najszybsze wdrożenie, przewidywalne koszty ryzyko: jawność lokalizacja przetwarzania danych, ograniczona kontrola

Rodzaje chmur i kryteria wyboru

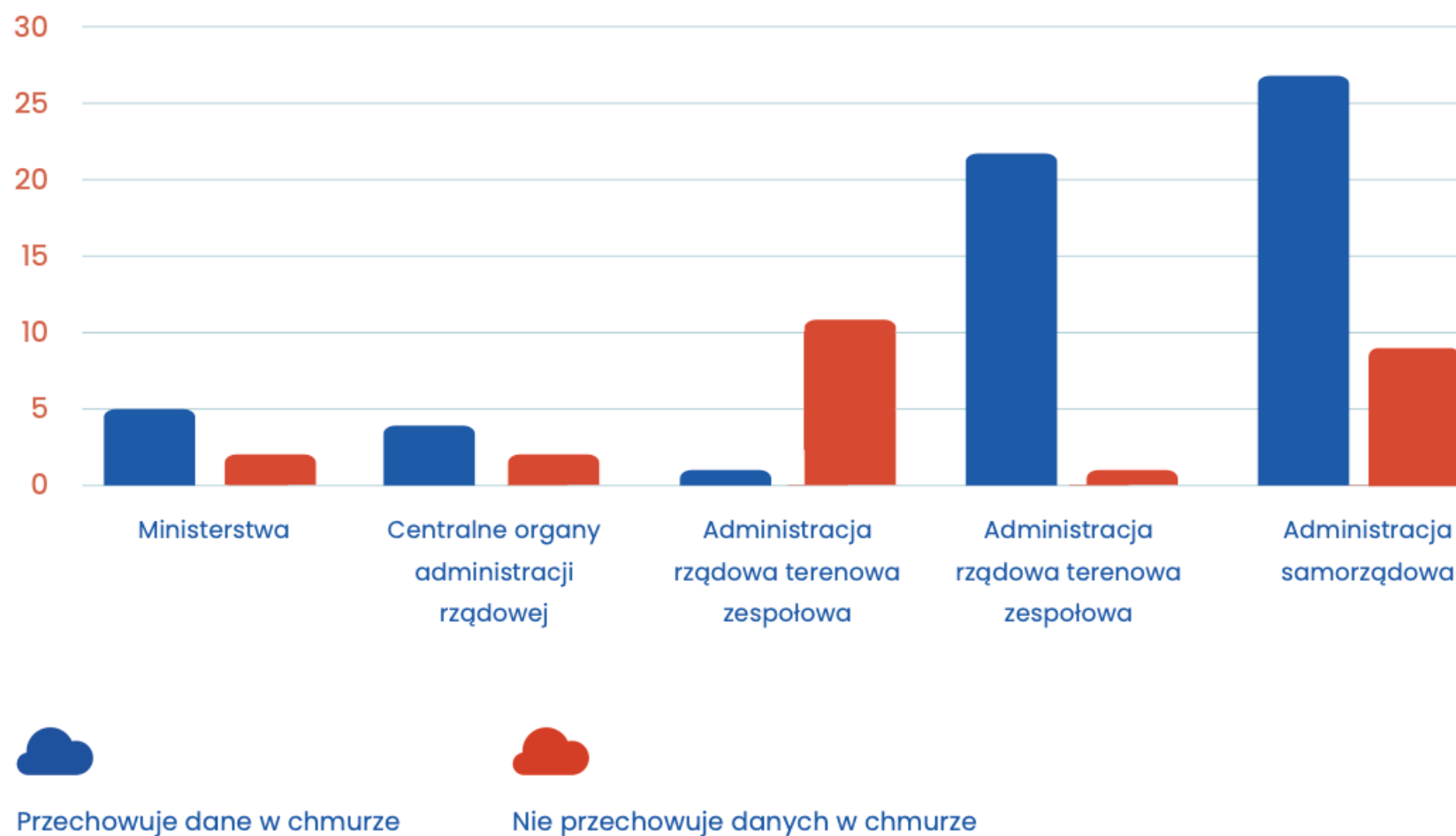
- Publiczna - szybki start, niskie koszty początkowe, szerokie portfolio usług; ryzyko: ograniczona kontrola nad danymi np. GCP, AWS, Azure
- Prywatna - pełna kontrola nad infrastrukturą, możliwość dostosowania; wyższe koszty utrzymania
- Hybrydowa - łączy zalety modeli prywatnego i publicznego; umożliwia etapowe migracje i separację danych wrażliwych
- Wspólnotowa - budowana i współdzielona przez kilka instytucji publicznych; efekt skali, spójne standardy, większa efektywność kosztowa i bezpieczeństwa np. Rządowa Chmura Obliczeniowa (RChO)

Stan wdrożenia chmury w Polsce - Raport Cyfrowa Polska 2025

- Ponad 7/10 jednostek administracji publicznej korzysta z chmury.
- Najchętniej do chmury podchodzą JST.
- Średni roczny koszt brutto korzystania z chmury - 2 799 555,79 zł.
- Kluczowym kryterium wyboru dostawcy były istniejące umowy licencyjne
- Najczęściej wybieranym modelem był SaaS (ponad 50%).
- Większość podmiotów decyduje się na chmurę Microsoft.
- Jedynie 7% badanych jednostek wskazuje bezpieczeństwo jako główne kryterium wyboru dostawcy

Źródło: https://cyfrowapolska.org/wp-content/uploads/2025/06/Raport-Cyfrowa-Polska_chmura-w-administracji.pdf

Przechowywanie danych w chmurze obliczeniowej przez organy administracji publicznej



Obraz rynku i potencjał - raport McKinsey

Wdrożenie chmury na szeroką skalę może wygenerować wartość dodaną odpowiadającą 4% rocznego PKB Polski w 2030 r. (27 mld euro)



Źródło: <https://www.mckinsey.com/pl/our-insights/chmura-2030>

Wyzwania

Firmy wskazują na wyzwania w 5 obszarach – ich przezwyciężenie może pozwolić na przyspieszenie wdrażania chmury

Czynniki ograniczające szeroką adopcję chmury w Polsce, według badań GUS i PMR



**Brak
świadomości**



**Niepewność
regulacyjna**



**Obawy o
bezpieczeństwo**



**Deficyt
kompetencji**



**Obciążenia
finansowe**

McKinsey
& Company

Źródło: <https://www.mckinsey.com/pl/our-insights/chmura-2030>



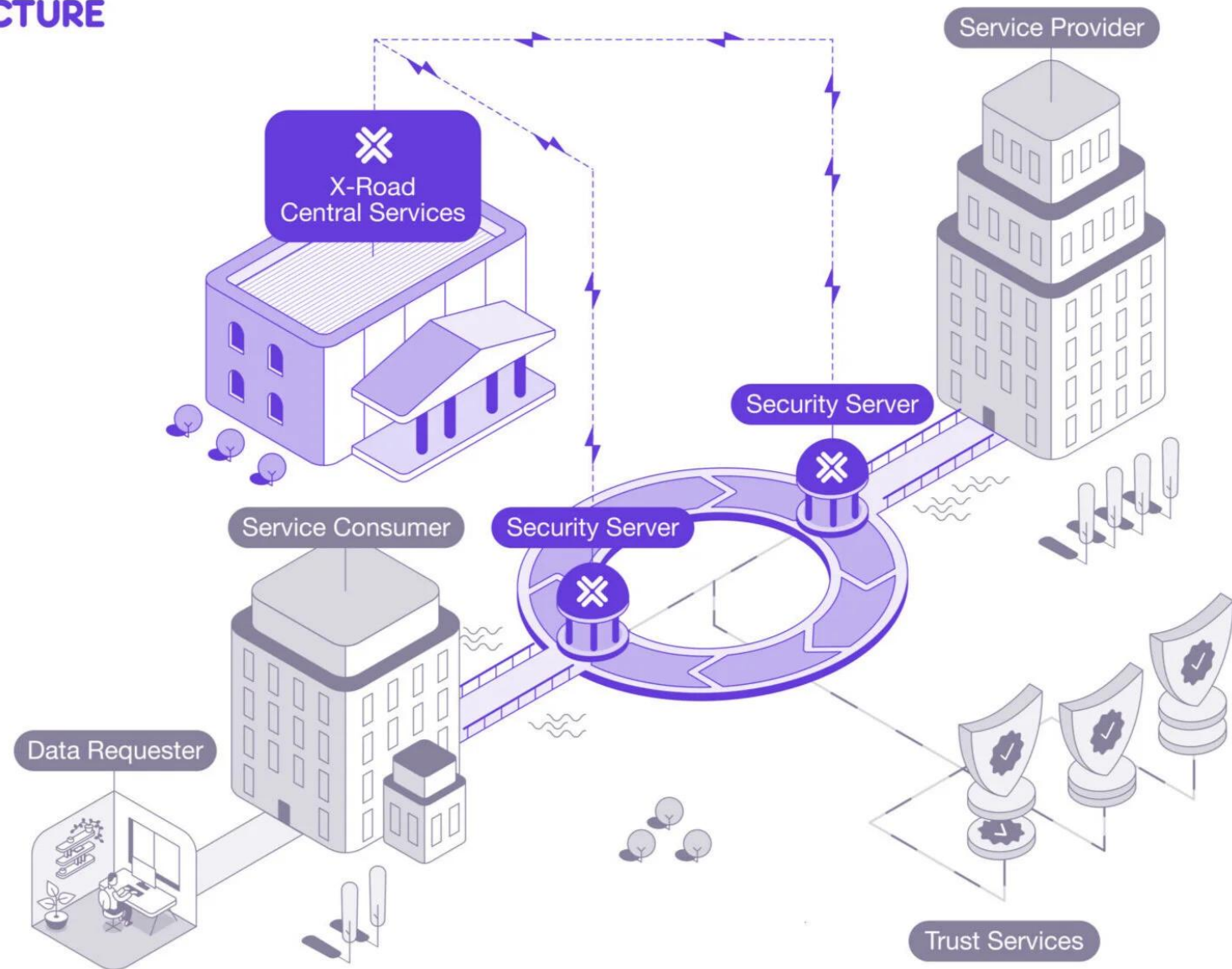
Przykłady międzynarodowe

Estonia - X-Road

- Integracja rejestrów państwowych przez wspólną szynę usług (X-Road)
- 99% usług publicznych online.
- Zasada „raz wprowadzonych danych” - administracja nie żąda ponownie informacji już posiadanych.
- Silna identyfikacja i logowanie dostępu do danych; pełna ścieżka audytu.
- Wniosek: priorytet dla interoperacyjności i standardów wymiany danych.



X-ROAD ARCHITECTURE



Wielka Brytania - G-Cloud

- Zasada „cloud first” dla nowych projektów i odnowień umów.
- G-Cloud: katalog usług i uproszczone zakupy, powtarzalne warunki, krótszy czas postępowań.
- Wspólne szablony wymagań (SLA, bezpieczeństwo).
- Wniosek: centralny katalog zwiększa konkurencję i transparentność.

USA - FedRAMP

- Centralna autoryzacja bezpieczeństwa usług chmurowych dla administracji.
- Wspólne kontrole i oceny - „raz ocenione, wielokrotnie użyte” (oszczędność czasu i kosztów).
- Poziomy zabezpieczeń dopasowane do wrażliwości danych.
- Wniosek: ujednolicone kryteria i audyty przyspieszają adopcję i podnoszą poziom bezpieczeństwa.



Strategia chmurowa w Polsce

Obszar	WIIP - Wspólna Infrastruktura Informatyczna Państwa	ZUCH - katalog usług chmurowych	RChO - Rządowa Chmura Obliczeniowa
Rola	Wspólne komponenty i standardy; spójna architektura dla administracji	Uporządkowany katalog usług i wzorców SWZ	Bezpieczne środowisko chmurowe z lokalizacją danych w Polsce
Zakres	Infrastruktura i usługi wspólne; integracja między urzędami	Opisy usług, SLA, wymagania bezpieczeństwa, przenoszalność, ścieżki audytu	Usługi obliczeniowe i składowania, monitoring, mechanizmy zgodności
Główne korzyści	Mniej duplikacji, efekt skali kosztowej, łatwiejsza integracja	Porównywalność ofert, krótsze postępowania, gotowe wymagania do SWZ	Stała dostępność, elastyczne skalowanie, nadzór i zgodność „wbudowana”
Zastosowanie	Projekty ponadresortowe, integracje między systemami publicznymi	Zakupy powtarzalnych usług chmurowych w jednostkach	Systemy krytyczne, zmienne obciążenia, wymóg lokalizacji danych w kraju
Ryzyka	Adaptacja starszych systemów, zarządzanie zmianą	Aktualność katalogu, dopasowanie do specyfiki jednostki	Zakres dostępnych usług, plan migracji, możliwość przeniesienia danych



Ryzyka

Najczęściej wykrywane błędy

Obszar	Co najczęściej znajdujemy	Skutek w praktyce
Tożsamość i uprawnienia (IAM)	Zbyt szerokie role, konta bez MFA, brak rotacji kluczy	Przejęcie kont, eskalacja uprawnień
Dane i magazyny	Publiczne zasoby, brak szyfrowania, brak klasyfikacji	Ujawnienia danych, naruszenia ochrony danych
Sieć	Usługi admin dostępne z internetu, reguły 0.0.0.0/0, brak segmentacji	Nieautoryzowany dostęp, szybka eskalacja
Usługi zarządzane (np. DB)	Domyślne konfiguracje, opóźnione aktualizacje	Utrata integralności, podatności
CI/CD i sekrety	Klucze oraz tokeny w repozytoriach, brak skanów sekretów	“Włamanie” do chmury przez łańcuch dostaw
Monitorowanie i kopie	Brak pełnych logów i alertów, kopie zapasowe nie testowane	Późne wykrycie incydentu, długie odtworzenie

Co rekomendujemy?

Należy:

- Włączyć logowanie wieloskładnikowe we wszystkich kontach; dla administratorów stosować klucze sprzętowe.
- Ograniczyć uprawnienia do niezbędnych; przeglądać dostępy cyklicznie; uprawnienia administracyjne nadawać tylko na czas zadania (JIT).
- Zredukować ekspozycję na internet: reguły „domyślnie zamknięte”, dostęp wyłącznie z zaufanych adresów, segmentacja środowisk.
- Uruchomić pełne rejestrowanie i monitoring; centralizować dzienniki; ustawić alerty dla działań wrażliwych.
- Chronić klucze i hasła: skanować repozytoria pod wycieki, rotować sekrety, używać menedżera kluczy.
- Zapewnić kopie zapasowe i odtwarzanie: kopie odseparowane, okresowe testy odtworzeniowe.
- Ustandaryzować i automatyzować konfigurację: korzystać z szablonów dobrych praktyk, regularnie skanować ustawienia i egzekwować polityki przed wdrożeniem.



Regulacje i standardy

Standardy Cyberbezpieczeństwa Chmur Obliczeniowych (SCCO)

W jakim celu?

Ujednolica kryteria bezpieczeństwa, ułatwia porównanie ofert i ocenę poziomu ochrony, wspiera wybór dostawcy i modelu przetwarzania.

Adresaci?

Jednostki administracji planujące lub korzystające z chmury oraz dostawcy usług (w tym PChO).

Co zawiera?

Załączniki z listą wymagań i katalogiem zabezpieczeń (w tym rozszerzonych) do wykorzystania przy ocenie i doborze środków ochrony.

Jak używać w postępowaniach?

Wskazać spełnienie wymagań SCCO w opisie przedmiotu i kryteriach oceny, odwoływać się do właściwych załączników na etapie weryfikacji ofert i odbioru.

Standardy Cyberbezpieczeństwa Chmur Obliczeniowych (SCCO)

1. SCCO1: informacje inne niż prawnie chronione.
2. SCCO2: informacje prawnie chronione (np. dane osobowe).
3. SCCO3: informacje niejawnie do „zastrzeżone” (w tym klauzule równoważne międzynarodowe).
4. SCCO4: informacje niejawnie powyżej „zastrzeżone”

Triada bezpieczeństwa informacji

Atrybut (SCCO 3.1)	Na czym polega	Przykładowe kontrolki w chmurze (wg SCCO)	Przykładowe miary/ustalenia
Poufność	Ograniczenie dostępu i ujawniania informacji do uprawnionych	Szyfrowanie transmisji i danych „w spoczynku”, zarządzanie kluczami (KMS), kontrola dostępu i tożsamości	Odsetek zasobów z wymuszonym szyfrowaniem; udział kont z MFA; rejestr dostępu do danych
Integralność	Ochrona przed nieuprawnioną modyfikacją danych	Kontrola zmian, podpisy/sumy kontrolne, niezmiennicze logi; polityki wersjonowania i walidacji	Liczba pozytywnych testów odtworzeniowych; zgodność logów z polityką retencji
Dostępność	Zapewnienie dostępności usług i danych w wymaganym czasie	Redundancja i skalowanie, kopie zapasowe, odtwarzanie po awarii, architektura wielostrefowa	Wymogi RPO/RTO w umowach; rzeczywisty poziom dostępności usług

Macierz wpływu

Atrybut	Niski (L)	Umiarkowany (M)	Wysoki (H)
Poufność	Ujawnienie informacji wywołuje ograniczony niekorzystny wpływ na operacje, zasoby lub osoby.	Ujawnienie informacji wywołuje poważny niekorzystny wpływ na operacje, zasoby lub osoby.	Ujawnienie informacji wywołuje silny lub katastrofalny wpływ na operacje, zasoby lub osoby.
Integralność	Nieautoryzowana modyfikacja/zniszczenie danych ma ograniczony negatywny wpływ.	Nieautoryzowana modyfikacja/zniszczenie danych ma poważny negatywny wpływ.	Nieautoryzowana modyfikacja/zniszczenie danych ma silny lub katastrofalny wpływ.
Dostępność	Zakłócenie dostępu lub użycia systemu ma ograniczony negatywny wpływ.	Zakłócenie dostępu lub użycia systemu ma poważny negatywny wpływ.	Zakłócenie dostępu lub użycia systemu ma silny lub katastrofalny wpływ.

Klasyfikacja danych a wybór chmury

1. **Dane “zwykłe”**: możliwa chmura publiczna, nacisk na dostępność i koszty.
2. **Dane wrażliwe**: chmura prywatna/hybrydowa, rozszerzone środki ochrony i kontrola dostępu.
3. **Informacje niejawne**: poza chmurą publiczną; środowiska o podwyższonym reżimie.
4. Wniosek: rodzaj danych determinuje model i wymagania kontraktowe.

RODO - na co uważać

- Kolokacja, potencjalny dostęp fizyczny do danych —> status podmiotu przetwarzającego; wymagana umowa powierzenia (art. 28).
- Kontrola fizyczna: listy osób uprawnionych, rejestry wejść/wyjść, monitoring, procedury eskorty i audyty.
- Transparentność: dokładne wskazanie lokalizacji ośrodków, wykaz podwykonawców, zasady przenoszenia zasobów między obiektami.
- Ochrona nośników: szyfrowanie dysków/backupów, procedury utylizacji, zakaz wynoszenia bez autoryzacji.



Co jeszcze?

Kontrola kosztów

- Budżet z progami alarmowymi i raportami miesięcznymi.
- Tagi/konta kosztowe na projekty i wydziały.
- Automatyczne wyłączanie środowisk testowych poza godzinami pracy.
- Przegląd rezerwacji/planów oszczędnościowych co kwartał.
- Raport „koszt za usługę chmurową” dla kierownictwa.





Fundusze Europejskie

Dziękuję!
aleksander.wojdyla@securitum.pl



Fundusze
Europejskie



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską

