

Compliance i ISO/IEC 27001

Zakres, ryzyko, zabezpieczenie i dowód

mgr inż. Jakub Woźniak

Zarządzanie Systemami Rozproszonymi · Semestr zimowy 2026/27

Przykładowy zakres

Rozwój i eksploatacja usługi zamówień: zespół, CI/CD, infrastruktura chmurowa, dane i relacje z dostawcami.

- ISMS: system zarządzania bezpieczeństwem informacji.
- ISO/IEC 27001:2022 określa wymagania dla ISMS.
- Certyfikacja dotyczy określonego zakresu organizacji; nie gwarantuje braku podatności aplikacji.

ISO — ISO/IEC 27001:2022

Własność	Przykład zdarzenia	Skutek
Poufność	Odczyt zamówień przez obcy podmiot	Ujawnienie danych
Integralność	Nieautoryzowana zmiana kwoty	Błędne rozliczenie
Dostępność	Brak odtwarzalnej kopii	Przerwa realizacji

- Sam zasób „baza danych” nie jest jeszcze opisem ryzyka.
- Potrzebne zdarzenie, warunki, skutek i właściciel.

Scenariusz

Wspólny token administratora w CI pozwala po przejęciu potoku odczytać i usunąć produkcyjne zamówienia.

Ocena dydaktyczna	Przed kontrolą	Po ograniczeniu dostępu
Prawdopodobieństwo: skala 1-3	3	1
Skutek: skala 1-3	3	3
Wskaźnik $P \times S$	9	3

Skala porządkowa służy priorytetyzacji; wynik nie jest prawdopodobieństwem ani kwotą straty.

Wariant	Przykład
Ograniczenie	OIDC i rozdzielenie ról potoku
Unikanie	Usunięcie zbędnego dostępu do danych
Dzielenie ryzyka	Uzgodnienia z dostawcą / ubezpieczenie
Akceptacja	Jawna decyzja uprawnionego właściciela

- Po zabezpieczeniach pozostaje ryzyko rezydualne.
- Decyzja i przegląd wymagają właściciela, nie tylko konfiguracji narzędzia.

Pole	Przykładowa treść
Zabezpieczenie	Kontrola dostępu do danych zamówień
Uzasadnienie zastosowania	Ryzyko przejęcia potoku
Stan wdrożenia	Role wdrożone; przegląd cykliczny uruchomiony
Uzasadnienia wyłączeń	Zależne od zakresu i oceny ryzyka

- SoA dokumentuje wybór zabezpieczeń i stan ich zastosowania.
- Plan postępowania opisuje pracę pozostałą do wykonania.

ISO/IEC 27001 Auditing Practices Group — SoA, 2022 (nota edukacyjna).

Twierdzenie	Dokument / konfiguracja	Dowód działania
Worker ma minimalną rolę	Deklaracja IaC	Receive działa; usuwanie kolejki odrzucone
Zmiany są przeglądane	Polityka branch protection	Historia konkretnego wdrożenia
Dane można odtworzyć	Polityka backupu	Raport rzeczywistego restore

- Dokument potwierdza zamiar; dowód operacyjny potwierdza wykonanie.

NIST SP 800-53 — Security and Privacy Controls

Tożsamość	Rola / zakres	Ostatni przegląd
worker-prod	Data Receiver / orders	12.09, właściciel usługi
ci-deploy	Contributor / orders-rg	12.09, platforma
old-migration	Owner / subskrypcja	Brak; konto nieużywane 180 dni

- Sprawdzić uprawnienia efektywne, również dziedziczone i grupowe.
- Priorytet: stare konto z szeroką rolą; samo istnienie poprawnej roli workera nie wystarcza.

Dostawca	Klient
Raport dla wskazanych usług i okresu	Sprawdzenie, czy używana usługa jest w zakresie
Mechanizm szyfrowania	Własna konfiguracja kluczy i dostępu
Mechanizm logowania	Włączenie, retencja i przegląd potrzebnych logów

- Raport dostawcy jest wejściem do oceny; nie zastępuje kontroli konfiguracji klienta.

Microsoft — Shared responsibility

```
package zsr.storage
import rego.v1

default allow := false
allow if {
    input.public_access == false
}
```

- Przykładowe wejście: {"public_access": false} → allow = true.
- Brak pola lub wartość true → brak zgody.
- Integracja musi faktycznie egzekwować wynik; OPA sam nie zmienia zasobu.

Pole	Przykład dydaktyczny
Zakres	Jeden kontener z publicznymi materiałami
Uzasadnienie	Dystrybucja danych jawnych
Właściciel i zatwierdzenie	Właściciel danych + bezpieczeństwo
Termin	30 dni; przegląd przed wygaśnięciem
Warunek	Brak danych zamówień; monitoring zmian

- Wyjątek związany z zasobem i terminem; nie globalne wyłączenie reguły.

Przedstawione materiały

Polityka: test restore co kwartał. Konsola: backupy codziennie zielone. Raport testu: ostatni sprzed 14 miesięcy. Brak właściciela procedury.

- Co potwierdzają dostępne dowody, a czego nie?
- Jaką rozbieżność zapisać i jakie działanie sprawdzi jej usunięcie?
- Czy zakup innego narzędzia backupu rozwiązuje ten problem?

- ISO — ISO/IEC 27001:2022
- Auditing Practices Group — Statement of Applicability, 2022
- NIST SP 800-53 Rev. 5 — Controls
- Microsoft — Shared responsibility
- Open Policy Agent — Policy language

Dokumentacja sprawdzona: 26.09.2026. Dane przypadków: przykłady dydaktyczne.