Ciągłość działania IT: od dokumentów w kopalni do zapasowej serwerowni w chmurze

Poziom: podstawy

Dotyczy: planowanie ciągłości działania, ośrodki zapasowe, BS 25999 i ISO 22301, Azure Site Recovery, AWS Elastic Disaster Recovery, NIS2 i ustawa o KSC, RODO, stan na 1 listopada 2026

Czas: ~20 min

Ta strona otwiera książkę o tym, co robimy, gdy nie ma już serwerowni, a nie tylko jednego serwera. Opowiada, jak z dokumentów chowanych w kopalni na wypadek wojny wyrosły zapasowe ośrodki obliczeniowe, normy i wreszcie zapasowa serwerownia wynajmowana w chmurze na godziny. Na końcu jest mapa książki: część stron już jest, reszta powstaje.

Kopie zapasowe odpowiadają na pytanie „czy mamy dane”. Wysoka dostępność odpowiada na pytanie „czy usługa przeżyje awarię jednego serwera”. Ciągłość działania pyta o coś trzeciego: co robi cała firma, gdy pożar, zalanie albo atak zabiera serwerownię, a pani Halina w poniedziałek rano i tak musi wystawić faktury.

Skróty użyte na tej stronie (11)

Skrót	Co znaczy
AWS	Amazon Web Services: chmura Amazonu
BSI	British Standards Institution: brytyjska organizacja normalizacyjna, która wydała BS 7799, a dziś także certyfikuje firmy i prowadzi szkolenia, również w Polsce
ISO	International Organization for Standardization: organizacja, która wydaje normy techniczne używane na całym świecie
IT	Information Technology: dział albo praca związana z komputerami i infrastrukturą firmy
KSC	krajowy system cyberbezpieczeństwa: polska ustawa, od 3 kwietnia 2026 w wersji wdrażającej dyrektywę NIS2, z obowiązkami zgłaszania incydentów

Skrót	Co znaczy
NIS2	Network and Information Security 2: unijna dyrektywa (UE) 2022/2555 o cyberbezpieczeństwie, z terminami zgłaszania poważnych incydentów (24 godziny, 72 godziny, miesiąc)
RODO	Rozporządzenie o Ochronie Danych Osobowych: unijne przepisy o tym, jak firmy mogą przetwarzać dane osobowe
RPO	Recovery Point Objective: ile danych wolno stracić przy awarii
RTO	Recovery Time Objective: jak długo wolno nie działać przy awarii
S3	Simple Storage Service: magazyn plików w chmurze AWS
UE	Unia Europejska

Skąd się wzięło

> **Pojęcie: ciągłość działania.** Zdolność firmy do dalszej pracy w czasie poważnego zdarzenia i do powrotu do normalności w czasie, który firma uznała za znośny. Obejmuje ludzi, procesy, budynki, dostawców i IT, a nie tylko serwery.

> **Pojęcie: odtwarzanie po katastrofie (DR).** Część ciągłości działania, która dotyczy systemów IT: plan, ludzie i środki techniczne, które pozwalają uruchomić usługi gdzie indziej albo od nowa, gdy podstawowe miejsce przestało istnieć.

1951: dokumenty w kopalni

Pierwsze plany ciągłości nie dotyczyły komputerów, tylko papieru. W 1951 roku Herman Knaust zaczął oferować bankom i firmom z Nowego Jorku miejsce w dawnej kopalni rudy żelaza pod Livingston, pod nazwą Iron Mountain Atomic Storage. Nazwa mówi wszystko o epoce: zimna wojna, strach przed atakiem atomowym i przekonanie, że firma bez ksiąg i umów nie podniesie się nawet wtedy, gdy przetrwają ludzie.

1978: pierwszy gorący ośrodek zapasowy

Pod koniec lat 70. firmy przeniosły księgowość i rozliczenia na komputery typu mainframe i zrozumiały, że bez nich nie pracują. W 1978 roku SunGard uruchomił dla jednej z firm w Filadelfii pierwszy gorący ośrodek zapasowy: osobną salę z komputerem, na którym klient mógł wznowić

pracę po awarii własnego. Spółka SunGard powstała formalnie w 1983 roku z działu usług komputerowych koncernu Sun Oil, a jej nazwa była skrótem od „Sun Guaranteed Access to Recovered Data”.

> **Pojęcie: ośrodek zapasowy (gorący, ciepły, zimny).** Drugie miejsce, w którym uruchamiamy systemy po utracie pierwszego. Gorący ma sprzęt i dane gotowe do pracy w minuty lub godziny, ciepły ma sprzęt i część danych, zimny ma tylko prąd, chłodzenie i miejsce na sprzęt, który trzeba dopiero przywieźć. Im cieplejszy ośrodek, tym droższy.

2001 i 2005: katastrofy, które zmieniły podejście

Atak 11 września 2001 roku pokazał, że ośrodek zapasowy kilka przecznic od siedziby nie jest zapasowy, gdy zamknięta zostaje cała dzielnica, a ludzie nie mogą dojechać. 8 kwietnia 2003 roku amerykańscy regulatorzy rynku finansowego wydali wspólny dokument o dobrych praktykach odporności systemu finansowego, w którym geograficzne rozproszenie ośrodków zapasowych i zespołów stało się tematem pierwszoplanowym. W sierpniu 2005 roku huragan Katrina zalał Nowy Orlean i przypomniał to samo z innej strony: kopia w szafie obok serwera albo w biurze w tym samym mieście znika razem z oryginałem.

Od BS 25999 do ISO 22301

Brytyjczycy zebrali doświadczenia w normy: najpierw dokument PAS 56 z 2003 roku, potem BS 25999-1 (zbiór praktyk, 2006) i BS 25999-2 (wymagania, 2007), według której firmy mogły się certyfikować. W 2012 roku zastąpiła ją międzynarodowa norma ISO 22301 o systemach zarządzania ciągłością działania, a BS 25999-2 wycofano w listopadzie 2012 roku. Obecne wydanie ISO 22301 pochodzi z 2019 roku, z poprawką klimatyczną z 2024 roku, a ISO pracuje już nad kolejnym (projekt komitetu ISO/CD 22301).

> **Pojęcie: analiza wpływu na działalność (BIA).** Rozmowa z właścicielami usług zapisana w tabeli: co się dzieje, gdy usługa nie działa godzinę, dzień, tydzień, ile kosztuje przestój i ile danych wolno stracić. Z niej biorą się liczby RTO i RPO, a nie z możliwości sprzętu.

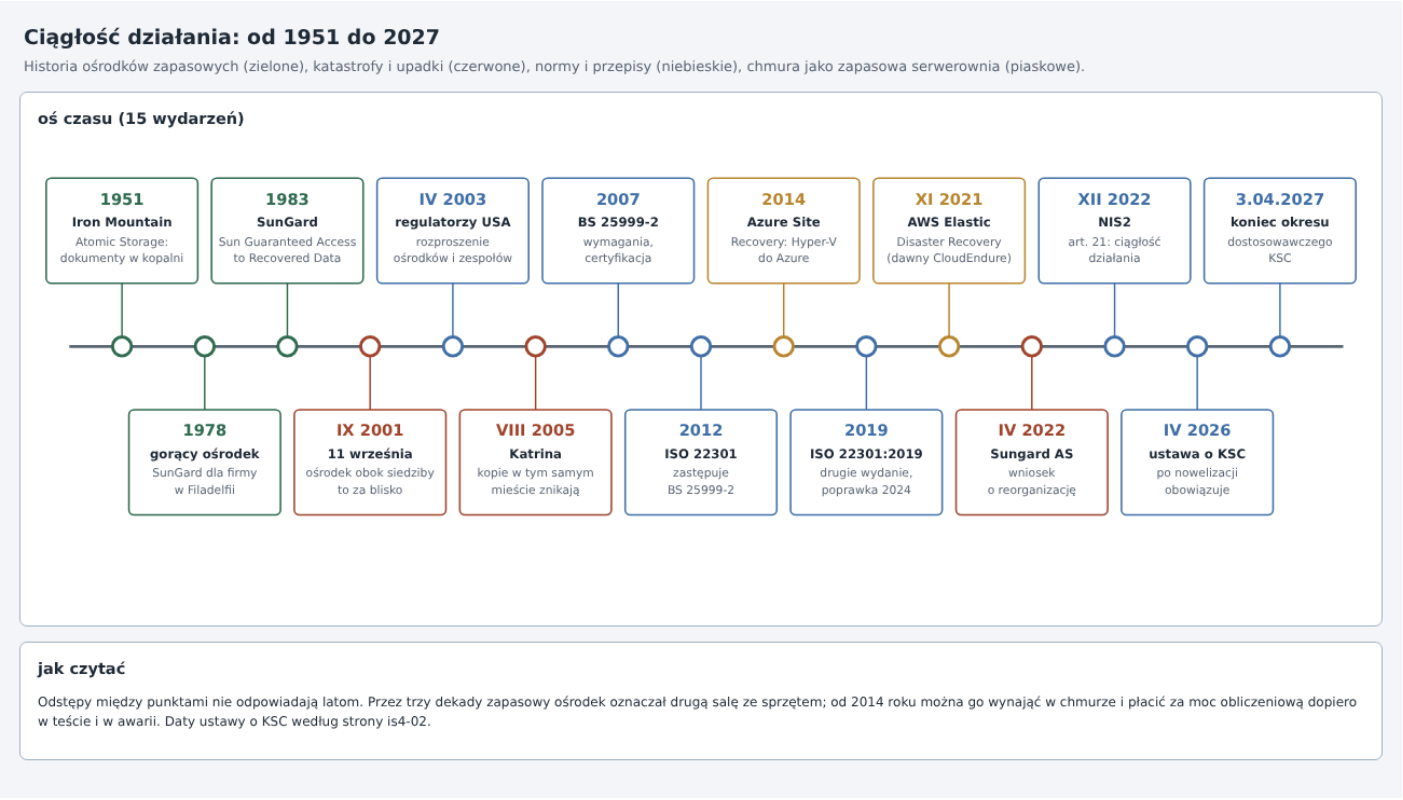
Chmura jako zapasowa serwerownia

Przez trzy dekady zapasowy ośrodek oznaczał drugą salę z drugim kompletem sprzętu, opłacany co miesiąc, nawet gdy stał bezczynnie. Chmura zmieniła rachunek: w 2014 roku usługa Microsoftu Hyper-V Recovery Manager zmieniła nazwę na Azure Site Recovery i zaczęła replikować maszyny z firmowych serwerowni do Azure, a w listopadzie 2021 roku AWS udostępnił Elastic Disaster Recovery, zbudowany na przejętym wcześniej CloudEndure. Maszyny w chmurze czekają wyłączone, płacimy za dyski i licencję usługi, a za moc obliczeniową dopiero wtedy, gdy je uruchomimy w teście albo w awarii. Ciekawostka: w kwietniu 2022 roku spółka Sungard Availability Services, wydzielona z pioniera ośrodków zapasowych, złożyła wniosek o reorganizację, wskazując między innymi przejście firm na pracę zdalną, a jej centra danych przejęli inni operatorzy.

Obowiązki: NIS2, ustawa o KSC i RODO

Dyrektywa NIS2 z grudnia 2022 roku wymienia wśród środków zarządzania ryzykiem ciągłość działania: kopie zapasowe, odtwarzanie po awarii i zarządzanie kryzysowe (art. 21 ust. 2 lit. c). W Polsce przeniosła ją nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa, obowiązująca od 3 kwietnia 2026 roku, z okresem dostosowawczym do 3 kwietnia 2027 roku. Ustawa dotyczy podmiotów kluczowych i ważnych, a czy firma do nich należy, zależy od sektora i wielkości; dla Zielonej rozważa to strona ISO/IEC 27001 a przepisy: NIS2 i ustawa o KSC, RODO, DORA i inne. Niezależnie od KSC, RODO w art. 32 ust. 1 lit. c wymaga zdolności do szybkiego przywrócenia dostępności danych osobowych po incydencie fizycznym lub technicznym.

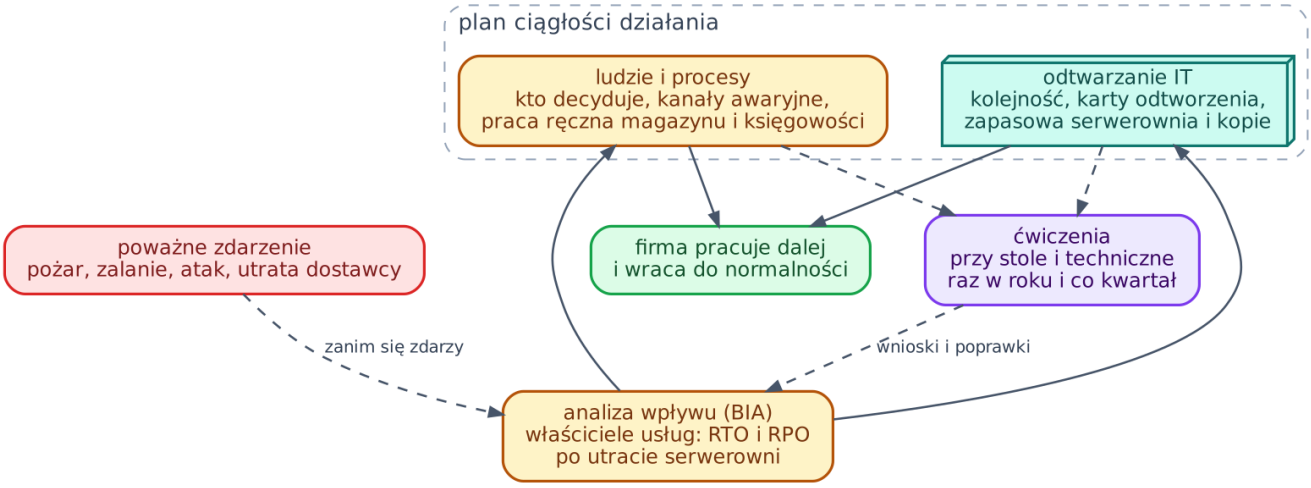
> Ta książka nie jest poradą prawną. Opisujemy, jak zbudować i pokazać środki ciągłości działania, a to, czy i w jakim zakresie przepisy dotyczą konkretnej firmy, ocenia prawnik razem z zarządem.



Rysunek 1. Oś czasu ciągłości działania: od Iron Mountain Atomic Storage w 1951 roku i pierwszego gorącego ośrodka SunGard w 1978 roku, przez 11 września, zalecenia regulatorów USA, Katrinę, BS 25999 i ISO 22301, po Azure Site Recovery, AWS Elastic Disaster Recovery, NIS2 i koniec okresu dostosowawczego ustawy o KSC 3 kwietnia 2027 roku (kliknięcie otwiera pełny rozmiar)

Jak to działa w jednym obrazku

Plan ciągłości działania ma dwie nogi. Pierwsza to ludzie i procesy: kto decyduje, jak się kontaktujemy, gdy nie działa poczta i Teams, jak magazyn wydaje towar na papierze. Druga to odtwarzanie IT: w jakiej kolejności podnosimy usługi, z jakich kopii i w jakim miejscu. Obie nogi spotykają się w liczbach RTO i RPO z analizy wpływu, a po każdym ćwiczeniu wracają do poprawy.



Rysunek 2. Ciągłość działania w jednym obrazku: analiza wpływu daje RTO i RPO, plan ciągłości dzieli się na pracę ludzi bez systemów i odtwarzanie IT w zapasowym miejscu, ćwiczenia sprawdzają oba i wracają poprawkami do analizy (kliknięcie otwiera pełny rozmiar)

Dlaczego Zielona

> **Z ŻYCIA WZIĘTE**
>
> Wtorek, 14:10, ćwiczenie „na papierze” z protokołu testów lokalizacji. Tomek czyta scenariusz: w nocy z niedzieli na poniedziałek woda z pękniętej rury zalała szafy R1 do R3. Marek pyta, czy o 6:00 skanery w Swarzędzu zadziałają, pani Halina pyta o zamknięcie miesiąca, a pan Zbigniew o to, ile dni firma będzie stała. Po godzinie na tablicy wisi odpowiedź, która nikomu się nie podoba: kopie są, ale nie ma gdzie ich odtworzyć, bo zapasowego sprzętu Zielona nie ma, a nowe serwery przyjadą za dwa do trzech tygodni.

Zielona ma kopie z regułą 3-2-1-1-0, drugi serwer kopii w Swarzędzu i archiwum w chmurze, opisane w książce Kopie zapasowe i odtwarzanie. Ma też macierz wysokiej dostępności z RTO i RPO dla każdej usługi. Brakuje trzech rzeczy: miejsca, w którym uruchomimy systemy po utracie serwerowni, dokumentu, który mówi ludziom, co robić, i ćwiczeń, które sprawdzą jedno i drugie. Ta książka zbiera te elementy w całość, a jej pierwsza gotowa część opisuje zapasową serwerownię w Azure z odpowiednikami poza Microsoftem.

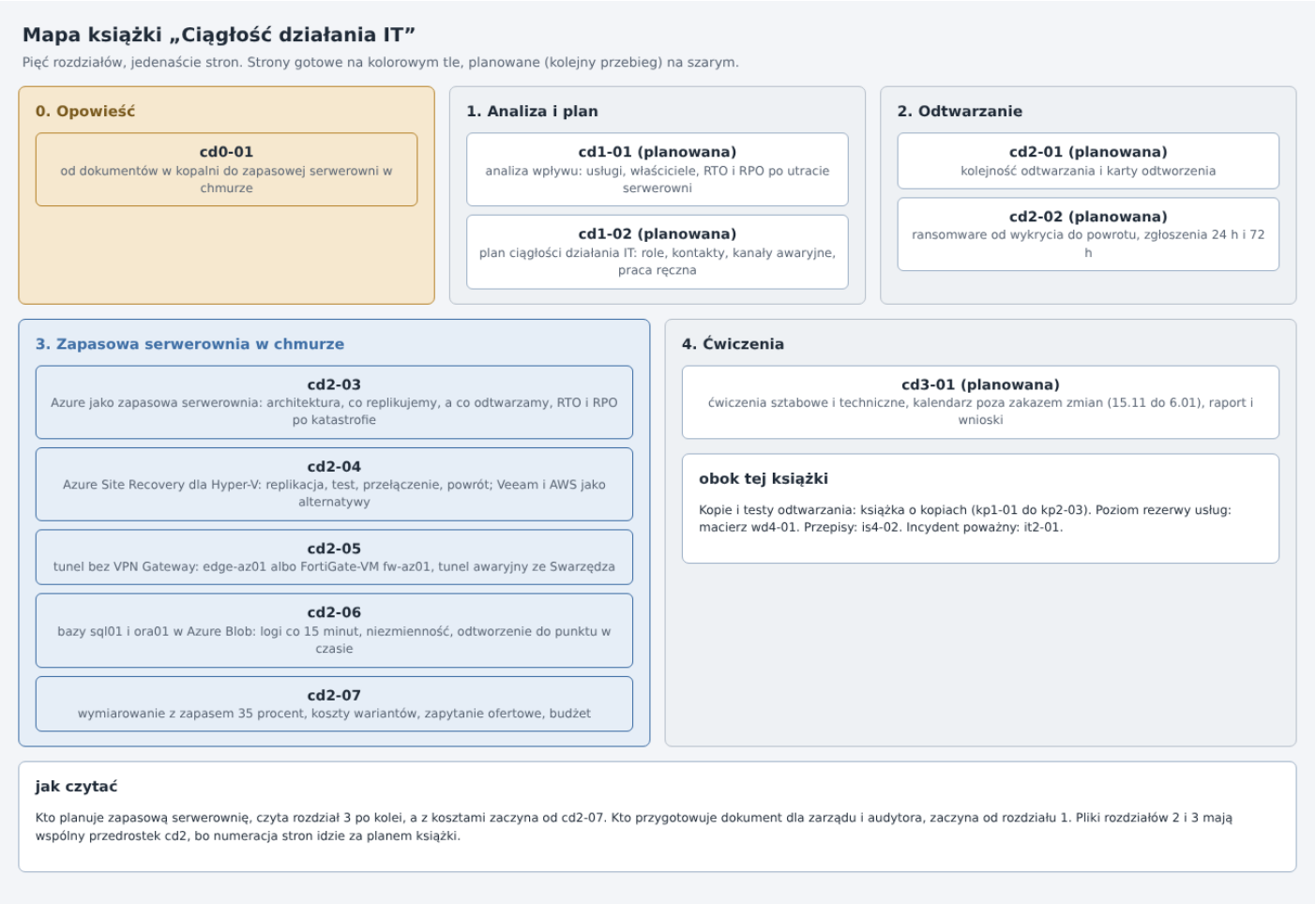
Mity i sprostowania

Obiegowa wersja	Jak jest naprawdę

Mamy kopie, więc mamy plan ciągłości.	Kopia mówi, że dane istnieją. Plan mówi, kto, gdzie, w jakiej kolejności i w jakim czasie je odtworzy oraz jak firma pracuje w tym czasie.
Replikacja do chmury zastępuje kopie.	Replika powtarza także zaszyfrowanie przez napastnika i skasowanie danych, a punkty odtworzenia w usługach replikacji żyją godziny albo dni, a nie miesiące. Kopie z niezmiennością zostają.
Zapasowa serwerownia w chmurze kosztuje tyle co druga serwerownia.	Wyłączone maszyny kosztują dyski i licencję usługi replikacji, a moc obliczeniową płacimy dopiero w teście i w awarii. Najdroższe są zwykle wyjście danych z chmury przy powrocie i godziny ludzi.
Plan ciągłości to dokument dla audytora.	Plan, którego nikt nie przećwiczył, w awarii okazuje się spisem życzeń. Dowodem dla audytora jest protokół z ćwiczenia i lista poprawek.
RTO z macierzy obowiązuje też po pożarze.	RTO w macierzy dotyczy awarii jednej usługi. Po utracie serwerowni obowiązują osobne liczby, uzgodnione z właścicielami, zwykle w godzinach albo dniach.

Mapa tej książki

Książka ma docelowo jedenaście stron w pięciu rozdziałach. Strony z linkiem są gotowe, pozostałe powstaną w kolejnym przebiegu i do tego czasu podajemy je samym tytułem. Tam, gdzie opisujemy Azure, obok stoi droga bez Microsoftu: AWS Elastic Disaster Recovery, Veeam, restic i S3 Glacier, FreeIPA zamiast kontrolera domeny i Linux z strongSwan zamiast zarządzanej bramy.



Rysunek 3. Mapa książki: opowieść, analiza wpływu i plan ciągłości, kolejność odtwarzania i ransomware, zapasowa serwerownia w Azure w pięciu stronach oraz ćwiczenia; strony gotowe na kolorowym tle, planowane na szarym (kliknięcie otwiera pełny rozmiar)

0. Opowieść

Strona	Na jakie pytanie odpowiada
Ciągłość działania IT: od dokumentów w kopalni do zapasowej serwerowni w chmurze	Skąd się wzięły plany ciągłości i ośrodki zapasowe i czego brakuje Zielonej

1. Analiza i plan

Strona	Na jakie pytanie odpowiada
Analiza wpływu na działalność: usługi, właściciele, uzgodnione RTO i RPO	Ile przestoju i utraty danych zniesie każda usługa po utracie serwerowni i kto to zatwierdza
Plan ciągłości działania IT Zielonej: role, kontakty, kanały awaryjne i praca ręczna	Kto decyduje, jak się kontaktujemy bez poczty i Teams, jak magazyn pracuje na papierze; szablon do wydruku

2. Odtwarzanie

Strona	Na jakie pytanie odpowiada
Kolejność odtwarzania i karty odtworzenia	W jakiej kolejności podnosimy AD i DNS, klaster, `sql01`, `ora01`, `fs01` i `docker01` i co zależy od czego
Ransomware od wykrycia do powrotu	Jak izolujemy, budujemy czyste środowisko, odtwarzamy z kopii niezmiennej i zgłaszamy incydent w 24 i 72 godziny

3. Zapasowa serwerownia w chmurze

Strona	Na jakie pytanie odpowiada
Azure jako zapasowa serwerownia Zielonej: architektura, co replikujemy, a co odtwarzamy	Jak wygląda sieć DR, gdzie stoi kontroler domeny, które maszyny replikujemy, a które odtwarzamy z kopii, jakie RTO i RPO po katastrofie
Azure Site Recovery dla Hyper-V bez VMM: replikacja, test, przełączenie i powrót	Jak zarejestrować `hv01` i `hv02`, ustawić politykę, przećwiczyć test w izolowanej sieci, przełączyć się i wrócić; Veeam i AWS jako alternatywy
Tunel do Azure bez VPN Gateway: edge-az01 z strongSwan albo FortiGate-VM fw-az01	Czym połączyć Zieloną z siecią DR taniej niż bramą zarządzaną i kto za co odpowiada
Bazy w zimnym archiwum Azure: kopie sql01 i ora01, niezmienność i odtworzenie do punktu w czasie	Jak kopie pełne i logi co 15 minut trafiają do Azure Blob i jak z nich podnosimy bazę w maszynie DR
Wymiarowanie i zakup zapasowej serwerowni w Azure: pojemność, koszty i zapytanie do partnera	Jak policzyć pojemność z zapasem 35 procent, koszt miesięczny wariantów i co wpisać w zapytanie ofertowe

4. Ćwiczenia

Strona	Na jakie pytanie odpowiada
Ćwiczenia ciągłości: sztabowe i techniczne	Jak prowadzić ćwiczenie przy stole i test przełączenia, kiedy (poza zakazem zmian od 15 listopada do 6 stycznia) i jak pisać raport z wnioskami

Kopie i ich testy opisuje książka o kopiach, w tym Testy odtwarzania: plik, maszyna, baza i cała lokalizacja, a poziomy rezerwy każdej usługi Macierz wysokiej dostępności usług Zielonej: poziom rezerwy każdej usługi, zależności i kolejność prac. Zgłaszanie incydentu poważnego jest na stronie Incydent i incydent poważny: od zgłoszenia do zamknięcia.

Nota metodyczna: czego nie wiemy

- Rok 1978 dla pierwszego gorącego ośrodka SunGard podajemy za artykułem z 2015 roku; Wikipedia datuje powstanie spółki na 1983 rok i nie podaje roku startu usługi.
- Dokument regulatorów USA z 2003 roku przytaczamy za komunikatem SEC, bez szczegółowych wymagań z pełnego tekstu.
- Datę pierwszego wydania ISO 22301 (2012) podajemy za informacją BSI o wycofaniu BS 25999-2 w listopadzie 2012 roku.
- Stan usług chmurowych i przepisów odczytaliśmy 1 listopada 2026 roku.

Źródła

Odczyt 1 listopada 2026.

Historia: clui.org, „Iron Mountain, Livingston, New York” (1951, Herman Knaust, Iron Mountain Atomic Storage); engadget.com, „The History of Disaster Recovery” (23 listopada 2015, pierwszy gorący ośrodek SunGard w 1978 roku w Filadelfii); en.wikipedia.org, „SunGard” (1983, wydzielenie z Sun Oil, rozwinięcie nazwy) i „Sungard Availability Services” (wnioski z kwietnia 2019 i 11 kwietnia 2022, sprzedaż aktywów w listopadzie 2022); sec.gov, komunikat 2003-45 z 8 kwietnia 2003 (Interagency Paper on Sound Practices); en.wikipedia.org, „BS 25999” (PAS 56 z 2003, części 1 i 2 z 2006 i 2007, wycofanie w listopadzie 2012); knowledge.bsigroup.com (BS 25999-2 zastąpiona przez ISO 22301); iso.org, ISO 22301:2019/Amd 1:2024 i ISO/CD 22301.

Chmura: itprotoday.com, „Hyper-V Recovery Manager Renamed to Microsoft Azure Site Recovery” (2014); aws.amazon.com, „Announcing general availability of AWS Elastic Disaster Recovery” (listopad 2021).

Przepisy: dyrektywa (UE) 2022/2555 (NIS2), art. 21 ust. 2 lit. c; rozporządzenie (UE) 2016/679 (RODO), art. 32 ust. 1 lit. c; daty ustawy o KSC za stroną ISO/IEC 27001 a przepisy: NIS2 i ustawa o KSC, RODO, DORA i inne.

Ilustracje: wszystkie rysunki na tej stronie są własne, narysowane dla tej bazy.

Revision #2
Created 2026-11-01 18:02:18 UTC by Tomasz Konieczny
Updated 2026-11-01 18:03:42 UTC by Tomasz Konieczny