Zarządzanie Ciągłością Działania

/ specyfika dla usług Przetwarzania Danych /

Jerzy Kurowski, CISA

Seminarium „MAINFRAME” Zachełmie 30.05 – 2.06.2011

Business Continuity Management /BCM/

- Ciągłość BIZNESU

Plan prezentacji

- Pojęcia i definicje
- Disaster Recovery
- Klasyfikacja SHARE / wg IBM
- Norma BS 25999
- Budowa Planów Ciągłości Działania
- Testy PCD

Zarządzanie Ciągłością Działania - o co chodzi ?

- Zapewnienie ciągłości procesów biznesowych

- Minimalizacja zagrożeń utraty krytycznych aktywów

- Zapewnienie jakości (usług, produktów) i wizerunku

- Zapewnienie przestrzegania przepisów prawa i umów

Definicje i pojęcia

Krytyczny proces biznesowy – proces biznesowy oficjalnie uznany przez ZARZĄD organizacji za krytyczny (którego przerwanie zagraża bardzo poważnymi skutkami finansowymi lub wizerunkowymi). Wybór takich procesów realizowany jest na podstawie analizy BIA (*Business Impact Analysis*).

Krytyczne procesy są obejmowane Planem Ciągłości Działania (BCP – *Business Continuity Plan*).

Analiza BIA (*Business Impact Analysis*) – określenie maksymalnych prawdopodobieństw strat finansowych i czasów krytycznych dla kluczowych procesów biznesowych organizacji.

Analiza ryzyka operacyjnego – proces identyfikacji zagrożeń (zewn. i wewn.) mogących mieć wpływ na kluczowe procesy biznesowe (wraz z istniejącymi środkami kontroli) oraz oszacowanie prawdopodobieństwa wystąpienia zagrożeń.

BCP – *Business Continuity Planning* –

planowanie ciągłości krytycznych procesów biznesowych

BCP – *Business Continuity Plan* – udokumentowany plan postępowania w celu utrzymania ciągłości działania lub odtworzenia krytycznych procesów biznesowych (na minimalnym akceptowalnym poziomie)

DRP - *Disaster Recovery Planning* – plan działań na wypadek „katastrofy" (np. poważnej awarii) – tzw. plany odtworzeniowe

***Disaster Recovery* - odtwarzanie po katastrofie /część BCP/**

Czas krytyczny (CzK) - maksymalny akceptowalny czas przerwy funkcjonowania danego procesu.

Czas odtworzenia (CzO) – czas od wystąpienia zdarzenia (katastrofy) do odtworzenia funkcjonowania procesu na akceptowalnym poziomie. RTO (*Recovery Time Objective*)

$$CzO < CzK$$

RPO (*Recovery Point Objective*) – Poziom aktualności danych odtworzonych po katastrofie (maksymalna dopuszczalna utrata danych).

Disaster Recovery dla procesu Przetwarzania Danych /IT/

DRP - opracowanie kompleksowych i udokumentowanych procedur - planów odtworzenia krytycznych obszarów działalności.

PRZETWARZANIE DANYCH -> BEZPIECZEŃSTWO INFORMACJI

Zabezpieczenia danych – tzw. kopie awaryjne.....

Ośrodek zapasowy – *Disaster Recovery Center*

MAK – minimalna akceptowalna konfiguracja

Umowy z dostawcami, podwykonawcami (dla lokalizacji zapasowej).

Czas krytyczny (czas „podniesienia”):
- max 24 – 48 h ; - banki (do 2 h),

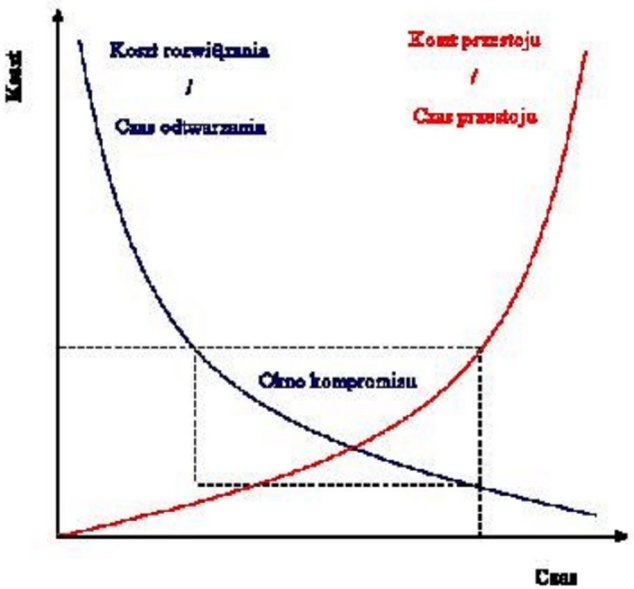
weryfikacja – TESTY !!!

Tradycyjne rozwiązania DR (różny średni *recovery time*):

- **Offsite Data (*Backup Storage*) – tworzenie kopii awaryjnych przechowywanych w zdalnej lokalizacji /RT 18 godz – 7 dni**
- **Cold Standby - dostępny ośrodek z infrastrukturą (HW) /4 g – 2 d**
- **Warm Standby - dane kopiowane do ośrodka zastępczego /10 m – 1 g**
- **Hot Standby – dane kopiowane automatycznie (automatyczne przełączenie na pracę w ośrodku zastępczym) /10 s – 2 min**

KOSZTY !!! - optymalizacja planu DR - podejście biznesowe.....

„okno kompromisu” - pomiędzy dostępnymi środkami na DR , a dopuszczalnymi kosztami przestoju **(w/g IBM)**



Klasyfikacja SHARE dla przetwarzania danych

Organizacja SHARE, zrzeszająca użytkowników środowisk Mainframe zdefiniowała zestaw 7 poziomów rozwiązań typu Disaster Recovery /IBM/.

0 - No off-site data (Kopia lokalna składowana lokalnie)

1 - Pickup Truck Method PTAM (Kopia lokalna składowana zewnętrznie)

2 - PTAM + hot site (Kopia lokalna + Ośrodek Zapasowy)
RPO – częstotliwość kopii lokalnej – 24 godz. RTO > 1 dzień.

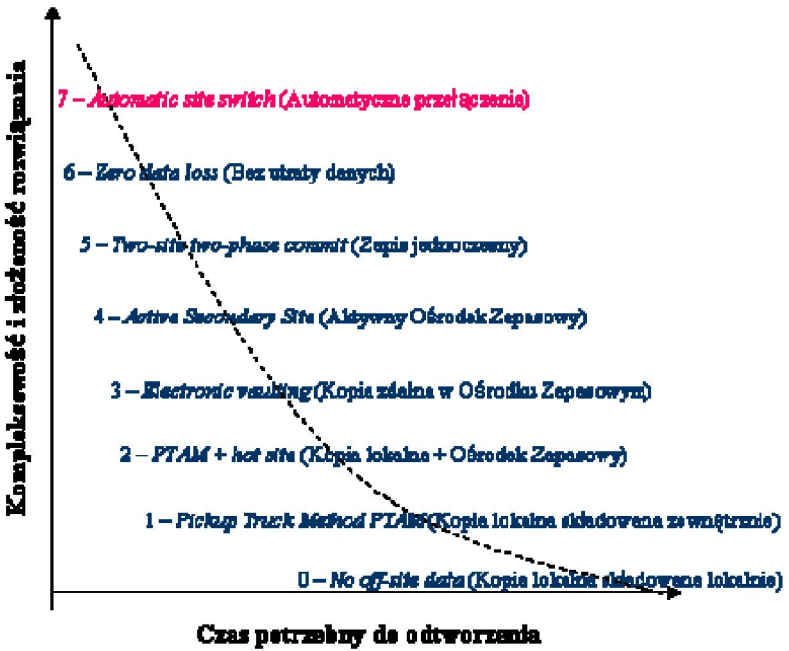
3 - Electronic vaulting (Kopia zdalna w Ośrodku Zapasowym) - ośrodek z minimum zasobami dyskowymi + umowy z dostawcami

4 - Active Secondary Site (Aktywny Ośrodek Zapasowy) - kompletne wyposażenie (MAK) i obsługa w ośrodku zapasowym

5 - Two-site two-phase commit (Zapis jednoczesny) –
wykorzystanie mechanizmu replikacji danych,
RPO ok. 0 , RTO < 12 godz.

6 - Zero Data Loss (Bez utraty danych) – zdalna kopia lustrzana,
RTO < 1 godz.

7 - Automatic site switch (Automatyczne przełączenie) –
automatyczne zarządzanie DR
RTO max kilka minut


Komplikowość i złożoność rozwiązania
7 – Automatic site switch (Automatyczne przełączenie)
6 – Zero data loss (Bez utraty danych)
5 – Two-site two-phase commit (Zapis jednoczesny)
4 – Active Secondary Site (Aktywny Ośrodek Zapasowy)
3 – Electronic vaulting (Kopia zdalna w Ośrodku Zapasowym)
2 – PTAM + hot site (Kopia lokalna + Ośrodek Zapasowy)
1 – Pickup Truck Method PTAM (Kopia lokalna składowana zewnętrznie)
0 – No off-site data (Kopia lokalnie składowana lokalnie)
Czas potrzebny do odtworzenia

Relacje między normami

ISO 27001 - 145 certyfikatów w Polsce
System Zarządzania Bezpieczeństwem Informacji

ISO 20000 – 1 - 10 certyfikatów
Zarządzanie usługami IT /ITIL/

BS 25999-2:2007 - 6 certyfikatów
System Zarządzania Ciągłością Działania

http://www.iso27000.pl - **rejestr certyfikatów**

3 w/w certyfikaty: Bank Handlowy-W-wa, itelligence Sp. z o.o.

Norma BS 25999 – 2: 2007

Norma definiuje efektywny model zarządzania ciągłością działania organizacji w warunkach kryzysowych /realizacja celów biznesowych/

Cel - zminimalizowania ryzyka związanego z zakłóceniem nieprzerwanego działania organizacji spowodowanego katastrofą lub incydentem

- **utrata zaufania klientów**
- **straty finansowe organizacji**

CIĄGŁOŚĆ => MINIMALIZACJA „PRZESTOJÓW”

Obszary objęte normą BS 25999-1:2006 :

1. **Polityka zarządzania ciągłością działania (cele).**
2. **Proces zarządzania ciągłością (podejście systemowe).**
3. **Analiza działalności (analiza ryzyka).**
4. **Strategia zarządzania ciągłością działania.**
5. **Opracowanie i wdrożenie środków „zapewnienia ciągłości”.**
6. **Monitorowanie, testowanie środków ochrony (plany awaryjne).**
7. **Budowa świadomości pracowników i podmiotów współpracujących.**

BS 25999-2:2007 obejmuje m. in.:

1. Terminologia /definicje/
2. Planowanie Systemu Zarządzania Ciągłością Biznesu
3. Wdrażanie i eksploatowanie SZCB

   (w tym: szacowanie ryzyka, definiowanie planów ciągłości biznesu, planów zarządzania incydentami)
4. Monitorowanie i przegląd SZCB (testy, audyty)
5. Utrzymywanie i doskonalenie SZCB

Norma BS 25999 jest uniwersalna i może być zastosowana przez każdą organizację bez względu na wielkość i branżę (szczególnie polecana dla organizacji, które działają w środowiskach obciążonych dużym ryzykiem, takich jak finanse, telekomunikacja, transport i sektor publiczny, tam gdzie ciągłość operacji ma kluczowe znaczenie).

Certyfikacja w zakresie normy BS 25999 w Polsce

Przyznano 6 certyfikatów BS 25999

- **PKO BP S.A – VII 2008 (Departament Bezpieczeństwa), DNV**
- **Bank Handowy S.A. – Warszawa - II 2009 (działania operacyjne i struktura technologiczna), BSI**
- **ELKART Sp. z o.o. – VI 2009 (sprzedaż i personalizacja kart), BSI**
- **PCZ S.A. – I 2010 (zarządzanie holdingiem, świadczenie usług medycznych), BSI**
- **Krajowa Izba Rozliczeniowa – VII 2010 (systemy rozliczeniowe ELIXIR i EuroELIXIR), BSI**
- **Itelligence Sp. z o.o. – IX 2010 (outsourcing i konsulting IT), ISOQAR**

ETAPY zapewniania ciągłości:

- **Analiza (BIA, wybór procesów),**
- **Plany awaryjne,**
- **BCP.**

BCP – *Business Continuity Plan* – udokumentowany plan postępowania w celu utrzymania ciągłości działania lub odtworzenia krytycznych procesów biznesowych (na minimalnym akceptowalnym poziomie)

1/ PLANY CIĄGŁOŚCI:

Zakłócenia - Kompensacje

Absencje - zastępstwa 1 + 1 +..., szkolenia

Brak dostaw – zapasy, dodatkowi dostawcy

Awarie sprzętu

- **redundancja,**
- **serwis wewn. (szkolenia),**
- **serwis zewn. (umowy SLA),**
- **ośrodek zapasowy.**

Zagrożenia hali - zabezpieczenia fizyczne, p.poż., ...

2/ Scenariusze zdarzeń / testów

Zewnętrzne – możliwe wersje rozwoju zdarzeń (NAJGORSZE ale PRAWDOPODOBNE)

- obsada wszystkich ról w procesie

Wewnętrzne – modele działania (procesy)

z uwzględnieniem hierarchii celów

3/ Testy planów awaryjnych

Test notyfikacyjny /weryfikacja kompletności planu/

Test papierowy (gra sztabowa)

scenariusze – sprawdzenie roli uczestników

Test operacyjny (pełny)

Przeniesienie procesu (lub wielu procesów) do lokalizacji rezerwowej (odtworzenie biznesu)

Przykłady projektów testów:

A/ CEL- weryfikacja struktur zarządzania kryzysowego
Analiza – kryteria:
a/ Czy prawidłowo rozdzielono zadania ?
b/ Czy liczebność zespołów jest odpowiednia do zadań ?
c/ Czy jest odpowiednie zabezpieczenie zasobów ludzkich (zastępstwa) ?

B/ CEL – Weryfikacja MAK (minim. akceptowalnej konfiguracji)
Kryteria:
a/ Czy MAK jest odpowiednia dla realizacji procesu w zdefiniowanym zakresie ?
b/ Czy uczestnicy testu znają lokalizacje zasobów MAK ?
c/ Czy uczestnicy potrafią korzystać z MAK ?
d/ Czy zdefiniowano wszystkie kontakty zewnętrzne dla realizacji akcji awaryjnej ?

C/ CEL – Weryfikacja procedury awaryjnej
Kryteria:
a/ Czy listy kontaktowe są kompletne i aktualne ?
b/ Czy wszyscy uczestnicy testu znają procedury postępowania ?
c/ Czy w teście dotrzymano czasów krytycznych dla procesu ?
d/ Czy można zrealizować wszystkie zobowiązania procesu ?

Podsumowanie:

BCM - zarządzanie ciągłością biznesu

działania:

- **zrozumieć biznes**
- **określić strategię ciągłości biznesu**
- **opracować rozwiązania oraz plany awaryjne**
- **wdrożyć rozwiązania**
- **testować plany**
- **doskonalić (rozwiązania i plany)**

D Z I Ę K U J Ę