IT GOVERNANCE

IT PRODUCTION

BUSINESS CONTINUITY PLAN

Wrocław, 8 maja 2017

Bank Zachodni WBK

Grupa Santander

Spis treści

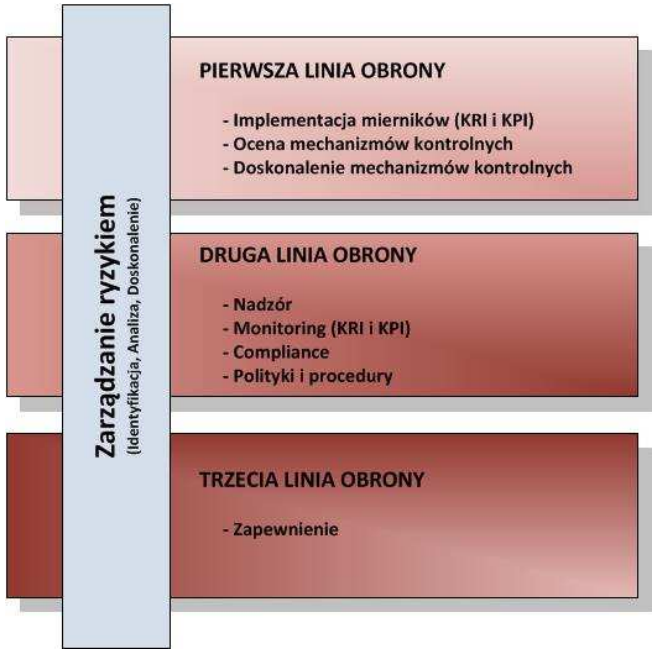
Bank Zachodni WBK
Grupa Santander

IT Governance

Bank Zachodni WBK

Grupa Santander

IT Governance



i. Zarządzanie i nadzór IT

- Sprawdź, czy struktura organizacyjna Technology & Operations zapewnia właściwą segregację funkcjonalną pomiędzy różnymi obszarami kontrolnymi i zapewnia, że działają one zgodnie z ramami regulacyjnymi obejmującymi wewnętrzne i zewnętrzne wymagania dla organizacji.
- Sprawdź, czy istnieje model apetytu na ryzyko, ustalono niektóre powiązane cele i odpowiedni system ich monitorowania.
- Upewnij się, że kierownictwo wyższego szczebla otrzymuje informacje na temat istotnych ryzyk w celu ich monitorowania i podejmowania decyzji

ii. Kontrola ryzyka technologicznego (II linia obrony)

- Sprawdź, czy jednostka zapewniła właściwą kontrolę ryzyka technologicznego polegającą na identyfikacji ryzyka jak również zapewniła właściwe procedury dla tej jednostki, jak również wykorzystanie i raportowanie wyników tych działań.

Przypisy:

IT Governance

Planowanie i zarządzanie

i. Zarządzanie IT - CIO:

- Plany systemowe: wymagania, produkcja, priorytetyzacja, monitorowanie, dostosowanie do biznesu.
- Zarządzanie przestarzałościami.
- Budżet i monitorowanie.
- Stosunki z dostawcami: Wybór i zarządzanie dostawcami, formalizacja umów.
- Nadzór i poziomy usług: SLA (kompletność, adekwatność, formalizacja, metryki itd.) i mechanizmów monitorowania.

ii. Zarządzanie ryzykiem technologicznym:

- Sprawdź, czy w jednostce znajduje się warstwa zarządzania ryzykiem technologicznym, która monitoruje ryzyko technologiczne oraz promuje i monitoruje środki mitygujące. Obejmuje to również wszystko związane z zarządzaniem przez lokalne jednostki ds. zarządzania ryzykiem technologicznymi. Zorientowana na funkcję warstwy ryzyka IT zawartą w obszarach technologii i operacji (T&O).

Przypisy:

IT Production

Bank Zachodni WBK

Grupa Santander

Production

Środowisko produkcyjne

i. Konfiguracja i zarządzanie infrastrukturą.

- Sprawdź istnienie mapy infrastruktury, która umożliwia identyfikację wszystkich zasobów. Informacje te muszą być dynamiczne i aktualizowane, aby umożliwić śledzenie zmian w infrastrukturze IT.
- Upewnij się, że wdrożenia w zakresie infrastruktury technologicznej odbywały się w ramach odpowiednich zasad i procedur.

ii. Obsługa iSeries i systemów Midrange.

- Sprawdź, czy procesy IT zostały skatalogowane zgodnie z ich krytycznością oraz czy istnieją procedury umożliwiające monitorowanie i określenie działań naprawczych w przypadku błędów wykonania, a także zapewnienie możliwości śledzenia wyników ich realizacji, oraz czy określono personel operacyjny odpowiedzialny za podejmowanie tych działań.

iii. Monitoring /iSeries, Systemów Midrange, Sieci, Baz danych.

- Upewnij się, że ma miejsce odpowiednie monitorowanie i śledzenie w systemach i komunikacji, które muszą mieć alarmy i formalne procesy ich obsługi. Narzędzia monitorowania muszą umożliwiać kontrolę alarmów wyłącznie przez osoby wyznaczone do tego zadania.

Production

Środowisko produkcyjne c.d.

iv. Zarządzanie incydentami.

- Zidentyfikuj procedury zarządzania incydentami, narzędzia służące do ich zapisu i zaangażowane obszary . Oceń klasyfikację zdarzeń w oparciu o ich krytyczność, ich obsługę dla pewnej próbki oraz raporty okresowe, które muszą być generowane w celu ich monitorowania.

v. Wdrożenie i zarządzanie zmianami dla systemów iSeries i Midrange.

- Zidentyfikuj i oceń zasoby i procedury określone dla żądania i zarządzania zmianami na platformie w produkcji. Przeprowadź analizę próby przeprowadzonych zmian, sprawdzając czy są one zgodne z metodologią oraz czy użytkownicy działu rozwoju oprogramowania nie mają dostępu do środowiska produkcyjnego.

vi. Kopie zapasowe.

- Uzyskaj zasady i procedury zdefiniowane dla kopii zapasowych i oceń ich adekwatność. Przeanalizuj, czy kopie są zgodne z tymi zasadami oraz czy utrzymanie i przywracanie kopii odbywa się zgodnie z procedurami.

vii. Zarządzanie obiektami.

- Sprawdź, czy obiekty, w których znajdują się systemy posiadające odpowiednią organizację, środki kontroli dostępu i ochrony fizycznej oraz że zapewniona jest ciągłość ich działania wraz z mechanizmami monitorowania tych aspektów (dostawa energii elektrycznej i łączność, kontrola klimatu, wilgotność, ltd.).

Business Continuity Plan

Bank Zachodni WBK

Grupa Santander

Business Continuity Plan

Plan utrzymania ciągłości biznesowej

i. Strategia utrzymania ciągłości

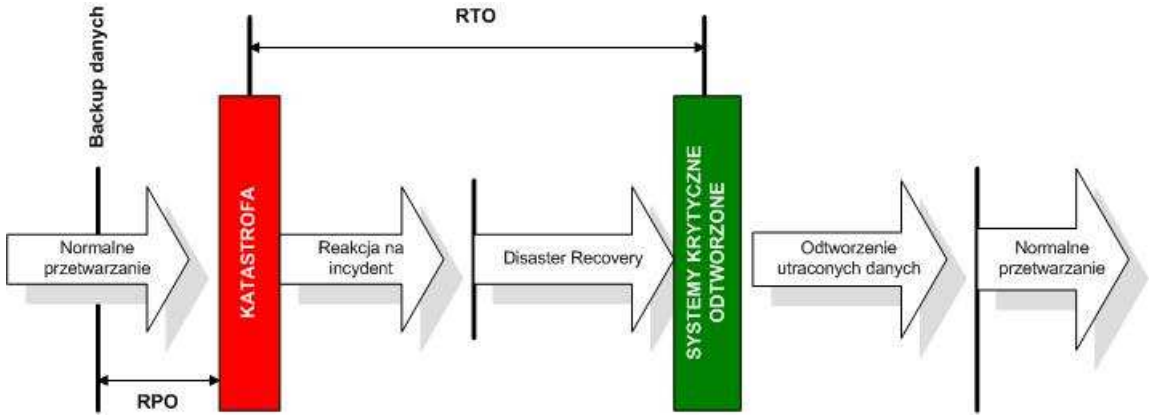
- Oceń plan ciągłości działania i jego dostosowanie do lokalnych rozwiązań. Potwierdź, że istnieje pełna dokumentacja BIA (Business Impact Analysis – Analiza wpływu na biznes) zawierająca procesy biznesowe i zasoby oraz identyfikację kluczowych procedur i procedur działania w przypadku incydentów. Upewnij się, że testy ciągłości są regularnie przeprowadzane i że ich wyniki są wykorzystywane w procesie ciągłego doskonalenia planów.

Business Continuity Plan

Plan utrzymania ciągłości biznesowej c.d.

ii. Technologiczny plan awaryjny

- Sprawdź, czy plan awaryjny uwzględnia zasoby informatyczne zdefiniowane przez analizę BIA jako krytyczne i ich czasy powrotu w planie ciągłości. Sprawdź, czy plan awaryjny jest dostosowany do metodologii korporacyjnej oraz czy są udokumentowane i dostępne procedury odzyskiwania. Plan ten musi zawierać harmonogram testów oraz wnioski z testów, podczas których obecna była kontrola.




Dziękujemy
za poświęcony nam czas
Małgorzata Kałach,
malgorzata.kalach@bzwbk.pl
Bank Zachodni WBK
Grupa Santander