



# **TWORZENIE SYSTEMU ZARZĄDZANIA RYZYKIEM W JEDNOSTKACH SEKTORA FINANSÓW PUBLICZNYCH Z WYKORZYSTANIEM PRAKTYKI ORGANIZACJI NASTAWIONYCH NA ZYSK**

**Zofia Szynkowska**



# TEMATYKA

- Przykład dobrych praktyk w zarządzaniu ryzykiem w Grupie TP
- Założenia systemu zarządzania ryzykiem w Narodowym Centrum Badań i Rozwoju
- Określenie kluczowych wskaźników ryzyka
- Tworzenie planu ciągłości działania w jsfp
- Znaczenie systemu komunikacji w zarządzaniu ryzykiem



# ZALUZENIA SYSTEMU ZARZĄDZANIA RYZYKIEM W NCBIR



- Menedżerskie podejście do jednostki
  1. Usprawnienie zarządzania
  2. Zarządzanie ryzykami finansowanych zadań
  3. Spowodowanie skuteczności i efektywności działania





# ZAŁOŻENIA

- Rezygnacja z kategoryzacji ryzyka
- 1. Kategoria ryzyka nie jest informacją kluczową
- 2. Zasadnym podziałem jest opracowanie strategii i działań operacyjnych
- 3. Istotą zarządzania ryzykiem jest minimalizacja ryzyka zapewniająca skuteczność realizacji celu strategicznego





# ZAŁOŻENIA

- Powiązanie ryzyka z planem działalności i budżetem zadaniowym
  - 1. Ocena na szczeblu strategicznym i operacyjnym zgodności ryzyk z działalnością jednostki
  - 2. Zarządzanie ryzykiem na średnich szczeblach operacyjnego działania



# ZAŁOŻENIA

- Określenie poziomów reakcji na ryzyko
  1. Poziom strategiczny
  2. Poziom operacyjny – wyróżnia 4 główne czynniki ryzyka: procesy, ludzie, systemy i zdarzenia, czynności zlecane na zewnątrz oraz czynniki zewnętrzne.



# ZAŁOŻENIA

- Czynniki ryzyka operacyjnego
  - Komitet Bazylejski w Umowie Kapitałowej określił że ryzyko operacyjne jest to ryzyko straty wynikającej z niedostosowania lub zawodności wewnętrznych procesów, ludzi, systemów technicznych oraz zdarzeń zewnętrznych.





# ZNACZENIE CZYNNIKÓW

- Procesy – obejmują błędy w procedurach lub ich brak.
- Ludzie – straty spowodowane umyślnym działaniem pracowników obecnych lub byłych, czynniki społeczne, stosunki pracownicze, czynniki psychologiczne, odporność na stres, konsekwencje zaburzeń w zarządzaniu kadrami, brak szkoleń, zdolność adaptacji do zmiennych warunków pracy





CD.

- Systemy – straty związane z infrastrukturą organizacji, zawodność techniczna systemów.
- Zdarzenia zewnętrzne – straty będące wynikiem działania czynników naturalnych takich jak powodzie, trzęsienia ziemi, braki w dostawach, działania przestępcze, niepokoje, konflikty społeczne, strajki.





# ZAŁOŻENIA

- Zakres raportowania dotyczy
  1. Natury ryzyk
  2. Wielkości zmian ryzyka
  3. Ograniczenia lub eskalacji ryzyka
  4. Wyników analizy scenariuszy szanse-zagrozenia
  5. Dotkliwości i częstotliwości strat



# ZARZĄDZANIE RYZYKIEM JEST TŁEM SKUTECZNEGO ZARZĄDZANIA ORGANIZACJĄ



- Prostota dokumentacji
- Celowość działań
- Istota odpowiedzialności
- Terminowość raportowania
- Trafność informacji



# OKREŚLENIE KLUCZOWYCH WSKAŹNIKÓW RYZYKA (KRI)



- Key Risk Indicator – Kluczowy Wskaźnik Ryzyka – definiowany jest jako miernik obszaru działalności instytucji, który z dużym prawdopodobieństwem odzwierciedla zmiany poziomu ryzyka tego obszaru. Ryzyko jest utożsamiane z możliwością wystąpienia zagrożenia, które miałyby wpływ na realizację zamierzonych celów organizacji.



# KLUCZOWY WSKAŹNIK RYZYKA (KRI)



- Kluczowy Wskaźnik Ryzyka wg R. Rudzki – mówi, iż są to dostępne dla danej organizacji miary ilościowe, których wysokość zgodnie z założeniem pośrednio odzwierciedla poziom ryzyka w tej organizacji (np. odsetek nieobecnych pracowników, odsetek opóźnionych transakcji, liczba awarii sprzętu komputerowego w określonym czasie).

\* ”OpVaR – pomiar ryzyka operacyjnego w oparciu o koncepcję Value at Risk”





# ZASTOSOWANIE METODY KRI

- Wyznaczenie wielkości kapitału na pokrycie ryzyka operacyjnego – modelowanie max wielkość straty dla ryzyk oraz powiązań pomiędzy zarejestrowanymi stratami a poziomami odpowiednich wskaźników
- Badanie trendów i pomiar ryzyka operacyjnego – analiza skuteczności działań kontroli wewnętrznej i analizy jakości procesów biznesowych
- Identyfikacja podatności na zagrożenia



## ZALETY KRI

Metoda KRI jest w głównej mierze wykorzystywana do analizy, monitoringu i kontroli stopnia realizacji celów w odniesieniu do wykonywanych zadań przy użyciu mierzalnych wskaźników.

- utworzenie zestawu wskaźników opisujących poszczególne obszary działalności instytucji
- możliwość monitorowania uzyskanych wartości wskaźników
- badanie trendów ryzyka
- określanie jego profilu
- identyfikowanie i ochronę przed potencjalną podatnością na zagrożenia oraz budowanie systemu wczesnego ostrzegania przed ryzykiem.





## WDROŻENIE KRI OBEJMUJE:

- Identyfikację i opis KRI
- Określenie poziomu oczekiwanego wraz z zakresem tolerancji i poziomu eskalacji/ alarmowania dla wskaźników
- Nadanie priorytetów wskaźnikom
- Pomiar wskaźników
- Wyznaczenie właściwych statystyk dla poszczególnych ryzyk



## WYMOGI DLA KRI

Wskaźniki KRI powinny spełniać podstawowe kryteria w zakresie efektywności, porównywalności i łatwości użycia

- Główne kryteria to;
  - Konieczność odzwierciedlenia obiektywnego pomiaru a nie subiektywnej oceny
  - Mierzalność w zdefiniowanych momentach czasu
  - Przydatność z punktu widzenia procesów zarządzania innych niż ZRO
  - Podatność na audytowanie
  - Łatwość dokonywania pomiaru





# OPIS KLUCZOWEGO WSKAŹNIKA RYZYKA

- powinien zawierać charakterystykę wskaźnika dane kontaktowe i sposób alarmowania w przypadku eskalacji, wielkości progowe/graniczne wraz z zakresem tolerancji
- zbudowanie bazy referencyjnej typowych wskaźników KRI z obszarów: ludzie, procesy, systemy i zdarzenia, czynniki zewnętrzne.



# 1 WYORZENIE PLANU CIĄGŁOŚCI DZIAŁANIA W JSFP



- Uporządkowane, formalne działania o charakterze cyklicznym które zapewnią minimalizację skutków przerwania krytycznych procesów organizacji oraz przygotowanie zaplanowanej, zorganizowanej i skutecznej reakcji.



# FAZY ZARZĄDZANIA CIĄGŁOŚCIĄ DZIAŁANIA (BCM)



1. **Zrozumienie organizacji** w celu identyfikacji kluczowych produktów i usług, identyfikacji krytycznych zadań i wspierających je zasobów
2. **Zdefiniowanie strategii** w celu wdrożenia środków bezpieczeństwa, ograniczenia prawdopodobieństwa wystąpienia zagrożeń, ograniczenia wpływu zagrożenia
3. **Opracowanie i wdrożenie reakcji** BCM w celu zapewnienia ciągłości działań krytycznych zadań i zarządzanie incydentami
4. **Testowanie, aktualizacja i przegląd** w celu tworzenia świadomości pracowników i weryfikacji zdolności odtworzenia poprzez testy i audyt
5. **Wbudowanie BCM w kulturę organizacyjną** włączenie aspektów BCM w strukturę zarządzania



# ZROZUMIENIE ORGANIZACJI – FAZA I



- Analiza wpływu (BIA-Business Impact Analysis)
- Oceny wpływu przerwy w działalności
- Wyznaczenia maksymalnego akceptowalnego czasu trwania przerwy, minimalnego poziomu odtwarzania
- Identyfikacja współzależności pomiędzy zdaniem i zasobami
- Identyfikacja krytycznych procesów
- Określenie wymagań w zakresie ciągłości działania
- Analiza i ocena zagrożeń dla procesów krytycznych
- Akceptacja wyników przez kierownictwo jednostki





# ANALIZA WPŁYWU

- Jaki jest najgorszy scenariusz dla szacowania strat
- Jaka jest maksymalna potencjalna strata policzalna i niepoliczalna w aspekcie czasu
- Jaki jest max akceptowalny czas przerwy
- Jaki jest wpływ akceptowalnego czasu przerwy na odtworzenie



# IDENTYFIKACJA KRYTYCZNYCH ZADAŃ



- Ważność zadań wg priorytetów odtworzenia
- Zadania krytyczne, których przerwanie generuje najważniejsze straty w najkrótszym czasie
- Ograniczenie planu ciągłości działania do zadań krytycznych



# OKREŚLENIE WYMAGAŃ W ZAKRESIE CIĄGŁOŚCI DZIAŁANIA



- Określenie dla każdego zadania krytycznego zasobów do jego wznowienia uwzględniające:
  - ✓ zasoby kadrowe
  - ✓ dostęp do budynków, pomieszczeń
  - ✓ infrastrukturę techniczną
  - ✓ zasoby zewnętrzne





# OCENA ZAGROŻEŃ DLA PROCESÓW KRYTYCZNYCH

- Ocenę ryzyka należy określić pod kątem przerwania realizacji zadań krytycznych
- Organizacja powinna być świadoma
  - zagrożenia dla poszczególnych zasobów,
  - podatności zasobów
  - skutku jaki może się wydarzyć w wyniku wystąpienia zagrożenia i przerwania realizacji krytycznego zadania
  - ryzyk występujących w rejestrze ryzyk organizacji
- Metodyka analiza ryzyka powinna być odpowiednia dla profilu działalności organizacji



# WYBÓR ŚRODKÓW BEZPIECZEŃSTWA I ZAPOBIEGAJĄCYCH



- Organizacja w wyniku analizy ryzyka (co-gdyby) identyfikuje środki bezpieczeństwa które:
  - zmniejszają prawdopodobieństwo wystąpienia przerwy
  - skracają czas przerwy
  - ograniczają wpływ przerwy na kluczowe produkty
- Strategie zarządzania ryzykiem mogą być stosowane łącznie
- Ryzyko wystąpienia zagrożeń nie zawsze może być ograniczone do akceptowalnego poziomu.



# ZDEFINIOWANIE STRATEGII – FAZA II



- Strategię Zarządzania Ciągłością działania (BCM) określamy dla:
  - krytycznych zadań i wspierających je zasobów
  - ludzi (zasoby kadrowe) – zabezpieczenie umiejętności i wiedzy, rozdział umiejętności kluczowych, szkoleń,
  - Informacji – zapewnienie dostępności i możliwości odtworzenia informacji niezbędnych do realizacji zadań krytycznych
  - technologii – dostęp, pewne łącza, czasy odtworzenia dla systemów i aplikacji
  - lokalizacji
- Sposobu zapewnienia zasobów – zdefiniowanie i utrzymanie niezbędnych zasobów
- Postępowanie w kwestiach kulturowych i socjalnych
- Określić działania w sytuacji zagrożenia bezpieczeństwa publicznego



## OPRACOWANIE I WDROŻENIE REAKCJI BCM – FAZA III

- Zdefiniowanie struktury zarządzania kryzysowego umożliwiającej potwierdzenie charakteru i zakresu działania, przejęcia kontroli nad sytuacją, ograniczenie incydentu, komunikację z kluczowymi uczestnikami krytycznych zadań
- Określenie zawartości planów – cel i zakres, role i odpowiedzialności, wskazanie właściciela i osoby odpowiedzialnej za utrzymanie i aktualizacje planu, dane kontaktowe do wszystkich kluczowych uczestników planu



# OPRACOWANIE I WDROŻENIE REAKCJI BCM – FAZA III



- Opracowanie planu zarządzania incydentami – listę zadań i akcji, kontakty awaryjne, procedury zapewniające bezpieczeństwo, zdrowie i życie pracowników, zdefiniowanie sposobu komunikacji z mediami, lokalizacja centrum kryzysowego, ponadto plany, diagramy, mapy, umowy, listy zasobów, procedury likwidacji szkód i inne
- Opracowanie planu ciągłości działania (BCP) poza wymienionymi wymogi dotyczące zasobów, odpowiedzialnych za przeprowadzone akcje, listy kontaktowe i rejestr przebiegu akcji awaryjnych



# TESTOWANIE PRZEGLĄD I AKTUALIZACJA – FAZA IV

- Zakres obejmuje opracowanie programu testów ich przeprowadzenie, aktualizację i utrzymanie oraz przegląd
- Program testów – musi odpowiadać BCP (plan), ich organizacja w ciągu określonego czasu daje obiektywną pewność że plan będzie działać zgodnie z oczekiwaniami. Określa rodzaj dopuszczonych testów np.: przegląd procedur, gry sztabowe, testy funkcjonalne, pełen test
- Testowanie musi być realistyczne, zaplanowane i uzgodnione, posiadać zdefiniowane cele, złożoność testu powinna odpowiadać Strategii Zarządzania Ciągłością Działania organizacji, uwzględniać pełnione w instytucji role



## TESTOWANIE PRZEGLĄD I AKTUALIZACJA – FAZA IV

- Aktualizacja zapewnia przegląd zmian mających wpływ na BCM a wyniki przeglądu stanowią podstawę do aktywnego zarządzania i nadzoru nad programem BCM, weryfikacji poziomu kompetencji osób odpowiedzialnych oraz monitoringu i kontroli nad ryzykami zagrażającymi ciągłości działania
- Przegląd powinien następować w określonych jednostkach czasu, być udokumentowane, weryfikować zgodność polityki z obowiązującym prawem, standardami, dobrymi praktykami. Przeglądu można dokonać w drodze audytu wewnętrznego i zewnętrznego oraz samooceny



# ZNACZENIE SYSTEMU KOMUNIKACJI W ZARZĄDZANIU RYZYKIEM



Czynniki wpływające na odbiór ryzyka.

- Jakiej sytuacji dotyczy zagrożenie?
- Jaki ryzyko ma charakter dobrowolny (czyli można go w sposób świadomy uniknąć), czy nie?
- Kto przekazuje komunikat, czy jest to osoba której można ufać?





# OTOCZENIE INFORMACJI

- Jakie uwarunkowania są specyficzne dla mojej organizacji?
- Narastanie 'kultury obwiniania'
- Świadomość poufności informacji
- Prawo do decydowania o losach informacji



# PODSTAWOWE ZASADY KOMUNIKACJI RYZYKA



- Pamiętaj do kogo skierowana jest informacja o ryzyku
- Wypracuj stworzenie właściwej wiadomości
- Nie wzmacniaj niepotrzebnie nasilenia ryzyka
- Nie angażuj zbyt wielu argumentów
- Najlepsza jest komunikacja aktywna
- Ujawnienie wszystkich szczegółów nie zawsze jest pomocne
- Unikaj tworzenia próżni komunikacyjnej
- Znaczenie zaufanego źródła informacji





•

Dziękuję za uwagę

