PAWEŁ GOŁĄB

Zarządzanie ryzykiem ciągłości działania w firmach ubezpieczeniowych

Instytucje finansowe, w tym zakłady ubezpieczeń, odgrywają bardzo istotną rolę w gospodarce światowej. Następująca duża koncentracja działalności i współzależność podmiotów rynków finansowych, wzrost zagrożenia klęskami naturalnymi, terroryzmem jak również uzależnienie od technologii informatycznych, stwarzają duże ryzyko przerwania działalności przedsiębiorstw ubezpieczeniowych. Celem zarządzania ciągłością działania jest zbudowanie mechanizmów zabezpieczających firmy przed negatywnym wpływem zakłóceń, tak aby w przypadku wystąpienia kryzysu, możliwe było kontynuowanie procesów biznesowych. Głównymi etapami są: zrozumienie organizacji w tym analiza wpływu (BIA), określenie strategii przetrwania, opracowanie procedur składających się na Plan Ciągłości Działania oraz testowanie i utrzymanie programu.

W artykule określono miejsce zarządzania ciągłością działania w procesach zarządzania ryzykami organizacji, dokonano przeglądu metod opisujących ten proces, oraz pokazano kolejne etapy praktycznego wdrożenia programu. Zachowanie bezpieczeństwa operacyjnego przedsiębiorstw ubezpieczeniowych jest już zalecane jako „dobre praktyki" a po wdrożeniu Solvency II stanie się obowiązkowe w każdej firmie ubezpieczeniowej.

1. Wprowadzenie

Zapewnienie ciągłości funkcjonowania instytucji finansowych jest jednym z priorytetowych zadań zarówno dla uczestników rynków finansowych jak i dla kontrolujących je organów nadzoru. Staje się to aktualne szczególnie w obecnych okolicznościach. Jak pisał Peter Drucker w swojej książce wydanej w 1980 roku w Londynie – „Management in turbulent timas" – „w czasach niespokojnych najważniejszym zadaniem kierownictwa jest zapewnienie dla organizacji zdolności do przetrwania, upewnienie się co do jej strukturalnej siły i odporności, zdolności do przeżycia ciosu". Szczególna rola zapewnienia ciągłości działania przypada na instytucje będące uczestnikami systemów finansowych nazywanych „krwiobiegiem gospodarki". Firmy ubezpieczeniowe, będące istotnym uczestnikiem rynków finansowych, zostały powołane aby likwidować lub łagodzić skutki wystąpienia nieprzewidzianych zdarzeń zagrażających ubezpieczonym podmiotom. Aby temu podołać muszą być same zabezpieczone przed ryzykiem przerwania działalności. Tak więc, zabezpieczenie ubezpieczycieli przed skutkami przerw w działalności ma wymiar nie tylko wewnętrzny, ale również społeczny. Od przedsiębiorstw

ubezpieczeniowych wymaga się zapewnienia odpowiedniego poziomu zarządzania ryzykiem w tym ryzykiem ciągłości działania, szczególnie w sytuacjach wystąpienia klęsk żywiołowych. Przerwanie ciągłości działania powoduje spiralę następstw, skutkującą negatywną reakcją interesariuszy i mającą niekorzystny wpływ na społeczeństwo. Konsekwencją jest zmniejszenie wartości i marki firmy. Zostaje to odzwierciedlone w pogorszeniu wyceny firmy przez rynek i agencje ratingowe, co z kolei wpływa na trudności w pozyskiwaniu kapitału. Negatywne reakcje rynku powodują rozszerzenie ryzyka reputacji, co przekłada się na zmniejszenie sprzedaży a co za tym idzie zysku. Przerwanie tej spirali może nastąpić dzięki zastosowaniu zarządzania ciągłością działania (*business continuity management*).

W sytuacji, gdy znakomita większość firm ubezpieczeniowych działa w grupach, silnie powiązanych kapitałowo i zarządczo, przerwanie działania wpływa negatywnie na inne podmioty grup (ryzyko zarażenia). Procesy globalizacji znacząco zintegrowały instytucje finansowe w wymiarze europejskim i światowym, co przełożyło się na zwiększenie ekspozycji na ryzyko operacyjne, w tym ryzyko przerwania ciągłości działania.

2. Przesłanki zarządzania ryzykiem ciągłości działania

Wspólny interes w promowaniu odporności systemu finansowego na poważne zakłócenia wynika z następujących przesłanek[1].

- Podmioty działające na rynkach finansowych odgrywają kluczową rolę w gospodarkach krajowych i światowej dostarczając środków finansowych do systemów płatności, umożliwiają kredytowanie transakcji, dostarczają kapitału inwestycyjnego, ubezpieczają prowadzoną działalność gospodarczą itp.
- Procesy rozrachunkowe i rozliczeniowe są silnie skoncentrowane w większości systemów finansowych. Zakłócenia w tych procesach mogą mieć bardzo niekorzystne konsekwencje, uniemożliwiając uczestnikom rynku dokonanie transakcji i rozliczenie zobowiązań.
- Systemy finansowe stają się technicznie coraz bardziej złożone. Automatyzacja procesów i wykorzystywanie technologii informatycznej znacząco uzależnia je od elementów infrastruktury technicznej takiej jak energia elektryczna, telekomunikacja, Internet. Powoduje to zwiększenie rozmiaru ryzyka operacyjnego.
- Pogłębia się współzależność pomiędzy uczestnikami branży finansowej zarówno krajowymi jak i międzynarodowymi. Większość podmiotów funkcjonuje w postaci grup kapitałowych łącząc działalność bankową, ubezpieczeniową i inwestycyjną. Szybkość, z jaką pieniądze i papiery wartościowe codziennie krążą pomiędzy uczestnikami rynków, wzmacnia wzajemne współzależności. Konsekwencją zakłócenia działalności jednego uczestnika branży może być wystąpienie trudności u innych uczestników (ryzyko zarażenia). Ponadto ze względu na postępującą globalizację rynków zakłócenie w jednym kraju może mieć poważne implikacje w innych krajach.

1. The Joint Forum: Basel Committee of Banking Supervision, International Organization of Securities Commissions, International Association of Insurance Supervision, C/O Bank for International Settlements; *High – Level Principles for Business Continuity*; December 2005, zm. August 2007

- Zwiększają się zagrożenia zewnętrzne takie jak ataki terrorystyczne i inne celowe działania przestępcze skierowane bezpośrednio lub pośrednio na infrastrukturę systemu finansowego.
- Istnieje silna potrzeba utrzymania zaufania społecznego do systemów finansowych.

Powtarzające się lub przedłużające zakłócenia funkcjonowania systemu finansowego podkopują zaufanie i mogą powodować wycofywanie kapitału z tego systemu przez inwestorów na poziomie krajowym i światowym[2].

Problematyka ryzyka operacyjnego, a w konsekwencji także bezpieczeństwa operacyjnego i ciągłości działania, jest przedmiotem rekomendacji obowiązujących w sektorze bankowym w Unii Europejskiej oraz na świecie[3]. Komitet Bazylejski wydał rekomendację dotyczącą zarządzania ryzykiem operacyjnym, w której zawarte są wytyczne odnośnie zarządzania ciągłością działania banków[4]. W Polsce dwie rekomendacje wydane przez Główny Inspektorat Nadzoru Bankowego regulują problematykę ciągłości działania w sektorze bankowym. Są to: „Rekomendacja D"[5] odnosząca się do bezpieczeństwa informacji i teleinformatycznego, oraz „Rekomendacja M"[6] określająca zasady zarządzania ryzykiem operacyjnym. Rekomendacje te odnoszą się do działalności operacyjnej banków, ale ze względu na większą dojrzałość sektora bankowego w zarządzaniu ryzykiem, stanowią znakomity *benchmark* dla zakładów i towarzystw ubezpieczeń. Widząc rosnące znaczenie tej problematyki, KNUiFE zapoczątkowała w 2005 badanie podmiotów nadzorowanych, czego efektem były dwa raporty. Pierwszy dotyczył towarzystw emerytalnych[7], drugi zaś zakładów ubezpieczeń[8]. Stanowiły one podstawę do opracowania klasyfikacji ryzyk na rynku ubezpieczeń opracowaną w ramach międzynarodowych badań, zmierzających do sformułowania ogólnoeuropejskich rekomendacji dobrych praktyk w zarządzaniu ryzykiem przez zakłady ubezpieczeń (tzw. Solvency II)[9]. W ślad za tym, w niektórych zakładach ubezpieczeń (m.in. w PZU S.A, PZU Życie S.A., TUiR Warta S.A., TU Alianz S.A., oraz TU Euler Hermes S.A.) powołane zostały komórki zajmujące się zarządzaniem ryzykiem ciągłości działania, w tym budową planów ciągłości działania. Należy oczekiwać, że proces ten przyspieszy wyraźnie w nadchodzących dwóch latach w ramach przygotowań do wdrażania dyrektywy Solvency II.

---

2. Zobacz: Giorgio Capuri *Corporate Social Responsibility Strategy in Practice,* UniCredit, materiały z konferencji: Strategia Odpowiedzialnego Biznesu, Warszawa 2008.
3. Zobacz więcej w Zawiła-Niedźwiecki Janusz, *Ciągłość Działania Organizacji*, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2008
4. Committee on Banking Supervision *Sound Practices for the Management and Supervision of Operational Risk*, Bank for International Settlements, Basel, 2003
5. Główny Inspektorat Nadzoru Bankowego *Rekomendacja D dotycząca zarządzania ryzykami towarzyszącymi systemom informatycznym i telekomunikacyjnym używanym przez banki*, NBP, Warszawa, 2002
6. Główny Inspektorat Nadzoru Bankowego *Rekomendacja M dotycząca zarządzania ryzykiem operacyjnym w bankach*, NBP, Warszawa, 2004
7. Zawiła-Niedźwiecki J., *Analiza aktualnego stanu zarządzania ciągłością działania przez towarzystwa emerytalne w Polsce*, praca badawcza i zarazem raport dla Komisji Nadzoru Finansowego, Warszawa 2006
8. Zawiła-Niedźwiecki J., *Stan zarządzania ciągłością działania przez zakłady ubezpieczeń w Polsce*, praca badawcza i zarazem raport dla Komisji Nadzoru Finansowego, Warszawa 2007
9. Zawiła-Niedźwicki J. *Ciągłość Działania Organizacji* str. 30.

3. Ryzyko operacyjne

Dyrektywa Solvency II dotycząca ubezpieczeń opiera się na już wprowadzonej w bankowości Basel II i przenosi z niej definicje między innymi ryzyka operacyjnego[10]. Ryzyko operacyjne wg Komitetu Bazylejskiego[11] to:

Ryzyko strat w wyniku niewłaściwego lub błędnego działania:

- procesów,
- ludzi
- systemów
- wpływu wydarzeń zewnętrznych.

Tak więc, ryzyko operacyjne jest wymienione jako jedno z trzech głównych kategorii ryzyk, na jakie narażone są zakłady ubezpieczeń, oprócz ryzyka aktuarialnego (ubezpieczeniowego) i finansowego[12]. Ryzyko operacyjne w sektorze ubezpieczeń pojawia się na skutek występowania zagrożeń zewnętrznych w otoczeniu organizacji, jak też w procesach realizowanych w przedsiębiorstwach ubezpieczeniowych. Zagrożeniami zewnętrznymi są; katastrofy naturalne, terroryzm, zewnętrzne zakłócenia fizycznego środowiska pracy (np. przerwy w dopływie energii elektrycznej). Wewnętrzne zagrożenia to: zakłócenia następujących rodzajów środowiska pracy: fizycznego wewnętrznego, funkcjonalnego, technicznego i informatycznego.

Ryzyko można zdefiniować jako kombinację prawdopodobieństwa wystąpienia zdarzenia oraz jego skutków (zalecenie ISO/IEC nr 73).[13] Można to zapisać wzorem $R = P \times S$.

W dziedzinie bezpieczeństwa, przyjmuje się generalnie, że zdarzenia mogą mieć wyłącznie niekorzystne następstwa, a tym samym zarządzanie ryzykiem koncentruje się na zapobieganiu szkodom i ich ograniczaniu. W trakcie prowadzenia każdej działalności gospodarczej w tym także ubezpieczeniowej występują zdarzenia (incydenty) zakłócające normalną działalność grupujące się w 4 głównych obszarach.

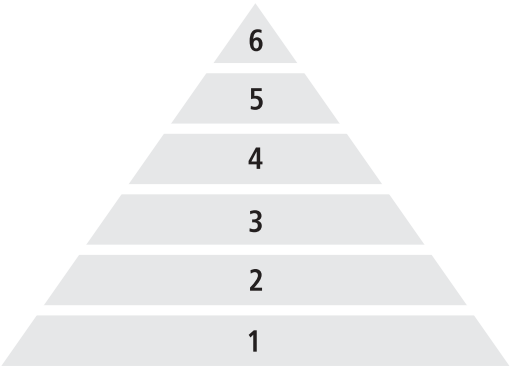
Rys. 1. Charakter występujących zakłóceń

Źródło: Zawiła-Niedźwiecki J.: „Ciągłość działania organizacji" [27]

10. International Association of Actuaries (2002): *Report of Solvency Working Party, of KPMG/European Commission* (2002), *Study into the Methodologies to Assess the Overall Financial Position of an Insurance Undertaking from the Perspective of Prudential Supervision*.
11. Committee on Banking Supervision: *Sound Practices for the Management and Supervision of Operational Risk*
12. Zobacz: *Klasyfikacja ryzyk ponoszonych przez zakłady ubezpieczeń* PIU 2004,
13. Zobacz: Federation of European Risk Management Associations: *Standard Zarządzania Ryzykiem*; www.theirm.org

Zakłady ubezpieczeń są narażone w różnym stopniu na ryzyko operacyjne. Badania szacują wielkość ekspozycji działalności ubezpieczeniowej na ryzyko operacyjne w zależności od rodzaju prowadzonej działalności na 11 proc. w zakładach ubezpieczeń majątkowych (*non life*) i na około 13 proc. w ubezpieczeniach życiowych (*life*)[14]. Aby móc efektywnie realizować wyznaczone cele, wszystkie kategorie ryzyka tj. zagrożenia, że określone zdarzenia, działania lub ich brak, negatywnie wpłyną na przedsiębiorstwo mogą i powinny być kontrolowane. Zarządzanie ryzykiem stanowi centralny element zarządzania strategicznego każdej organizacji i pozwala na metodyczne rozwiązywanie problemów związanych z występowaniem ryzyka tak, aby działalność zarówno w poszczególnych dziedzinach jak i traktowana jako całość – przynosiła trwałe korzyści.[15] Badanie, które zostało przeprowadzone przez KPMG[16] wśród 148 prezesów firm ubezpieczeniowych i reasekuracyjnych określa bardzo wysoką pozycję zarządzania ryzykiem w percepcji zarządzających. 61 proc. ankietowanych menadżerów oceniło, że zarządzanie ryzykiem, w tym ryzykiem operacyjnym, jest ważne i bardzo ważne dla utrzymania przewagi konkurencyjnej firm przez nich zarządzanych. Ryzyka powinny być kontrolowane na poziomie organizacji, w ramach prowadzenia kompleksowej, zintegrowanej polityki zarządzania ryzykiem. Wprowadzenie kompleksowego podejścia do procesu zarządzania ryzykiem pozwala na oszacowanie istotnych ryzyk towarzyszących działalności oraz wypracowanie zintegrowanych strategii zarządzania ryzykiem.[17] Podejście systemowe zakłada wykorzystanie różnych metod do określenia kolejnych aspektów ryzyka operacyjnego[18]. Struktura zarządzania ryzykiem operacyjnym w organizacji składa się z 6 warstw odpowiedzialnych za różne aspekty ryzyka i proponujących określone metodyki zarządzania.

Rys. 2. Struktura zarządzania ryzykiem operacyjnym



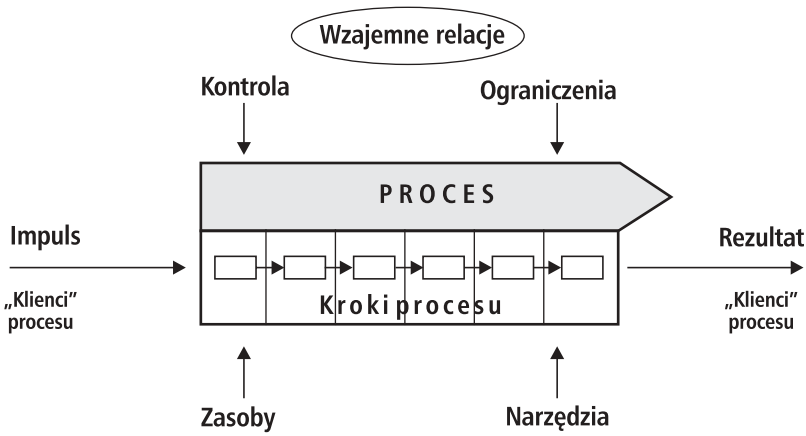
Źródło: Na podstawie Kulik A.; „ABC Zarządzania Ryzykiem" [22]

14. De Nederlandsche Bank: *Risk measurement within financial conglomerates: best practices by risk type*; Research Series Supervision no. 51 February 2003
15. Zobacz: Federation of European Risk Management Associations: *Standard Zarządzania Ryzykiem*; www.theirm.org
16. KPMG: *Globalizing the Risk Business – Surviving and competing in the global insurance industry* www.kpmg.com
17. Ernst & Young Advisory; *Zarządzanie ryzykiem w organizacjach*; www.ey.com
18. Kulik Andrzej CFA: *ABC Zarządzania Ryzykiem – Ryzyko Operacyjne* Prezentacja, Warszawa 2003

4. Identyfikacja procesów jako podstawa zarządzania ryzykiem

Podstawą, na której zbudowana jest infrastruktura zarządzania ryzykiem są procesy realizowane w danej organizacji. Procesem nazywamy logiczny układ powiązanych ze sobą czynności zainicjowanych przez jeden lub więcej czynników (fizycznych lub informacyjnych), powodujących powstanie określonego wyniku, który stanowi wartość dodaną dla klienta. Podstawowe cechy procesu to: występowanie łańcucha kroków procesu, zdefiniowany początek i koniec tzw. *End-to-end*, obecność czynników inicjujących oraz wytworzenie określonego wyniku (produktu lub usługi). Procesy dzielimy na trzy grupy: główne (operacyjne), wsparcia oraz zarządzania. Coraz więcej organizacji dostrzega potrzebę identyfikacji procesów w celu sprawnego zarządzania nimi i ich usprawniania. Mapę procesów tworzymy poprzez zidentyfikowanie wszystkich podmiotów uczestniczących w procesie, zdarzeń inicjujących, spisanie czynności składających się na proces oraz sekwencji i ich wzajemnych relacji.

Rys. 3. Podstawowe charakterystyki procesu



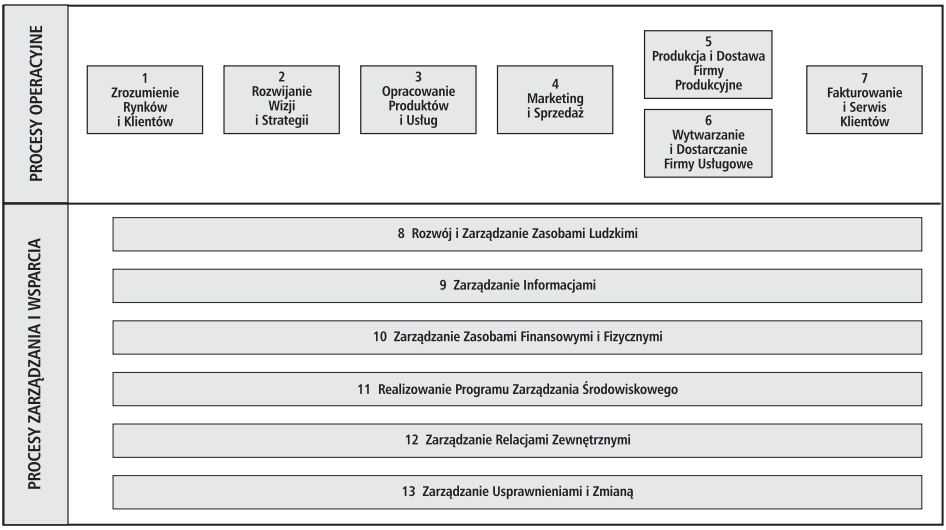
Źródło: opracowanie własne

Wynikiem analizy jest tzw. mapa procesów firmy. Zrozumienie budowy procesu umożliwia przypisanie ryzyk zarówno do procesu jako całości jak i do poszczególnych kroków procesu, co jest najlepszą metodą dokładnej diagnozy ryzyk występujących w organizacji.

Dla potrzeb diagnostycznych dobrze jest się posłużyć dobrymi wzorcami wypracowanymi przez firmy doradcze. Godna polecenia jest klasyfikacja dokonana przez American Productivituy & Quality Center pod tytułem *Process Classification Framework*[19]. Klasyfikacja tam zawarta, opracowana we współpracy z Arthur Andersen, pionierem zarządzania procesowego, umożliwia diagnozę procesów realizowanych w organizacji, które jak już wspomniano, tworzą fundament umożliwiający zbudowanie struktury kompleksowego zarządzania ryzykiem.

19. American Productivity & Quality Center: *Process Classification Framework* www.apqc.org

Rys. 4. Model procesów organizacji



Źródło: APQC: „Process Classification Framework" [1]

5. Metody zarządzania ryzykiem operacyjnym

Kolejną warstwą struktury zarządzania ryzykiem operacyjnym jest Samoocena Ryzyk i Kontroli (*Risk & Control Self Assesment*). Pozwala ona w sposób kompleksowy dokonać analizy i oceny ryzyka i kontroli wewnętrznych w przedsiębiorstwie oraz monitorować ich zmiany. Polega na identyfikacji, ocenie, określeniu reakcji, monitorowaniu i ostatecznie ograniczaniu ryzyka operacyjnego. Na podstawie uzyskanych wyników ustala się sposób zarządzania zidentyfikowanymi ryzykami. Jest to metoda jakościowa wykorzystująca oceny ekspertów, szacujących parametry w oparciu o najlepszą wiedzę i doświadczenie. Wykorzystuje się tutaj techniki heurystyczne i metody opisowe oraz narzędzia i techniki typu: ankiety, formularze, wywiady. Polega najczęściej na przeprowadzaniu warsztatów z kadrą zarządzającą, w rezultacie których, uzyskujemy obraz ryzyka operacyjnego występującego w procesach. Ze względu na stosunkowo dużą możliwość popełnienia dużych błędów, bardziej adekwatne wydaje się używanie wyrażenia „oszacowanie wartości" zamiast „pomiar wartości" ryzyka operacyjnego[20]. Metoda ta jest bardzo przydatna do przeprowadzania części analitycznej (Analiza Wpływu BIA), w procesie zarządzania Ciągłością Działania, ma również zastosowanie do określania Kluczowych Wskaźników Ryzyka (*Key Risk Indicators KRI*) będących kolejnym poziomem struktury zarządzania ryzykiem. Kluczowe Wskaźniki Ryzyka określają parametry procesu biznesowego, odzwierciedlają z dużym prawdopodobieństwem zamiany profilu ryzyka operacyjnego procesu. Wskaźniki KRI są określane na podstawie danych okresowych (miesięcznych, kwartalnych). Ich analiza ma na celu ostrzeganie przedsiębiorstwa przed możliwymi zmianami ryzyka operacyjnego.

20. Orzeł J.: *Na drodze do zaawansowanych metod ilościowego pomiaru ryzyka operacyjnego – KRI*; Bank i Kredyt, Warszawa 2005

Do modelowania ryzyka z zastosowaniem KRI nadają się zdarzenia występujące często, powodujące umiarkowane straty, dla których posiadamy wystarczającą bazę informacji. Dla zdarzeń występujących rzadko a mających duży wpływ (incydenty przerywające ciągłość działania) KRI nie mogą być zastosowane. Przykładowe Kluczowe Wskaźniki Ryzyka to:

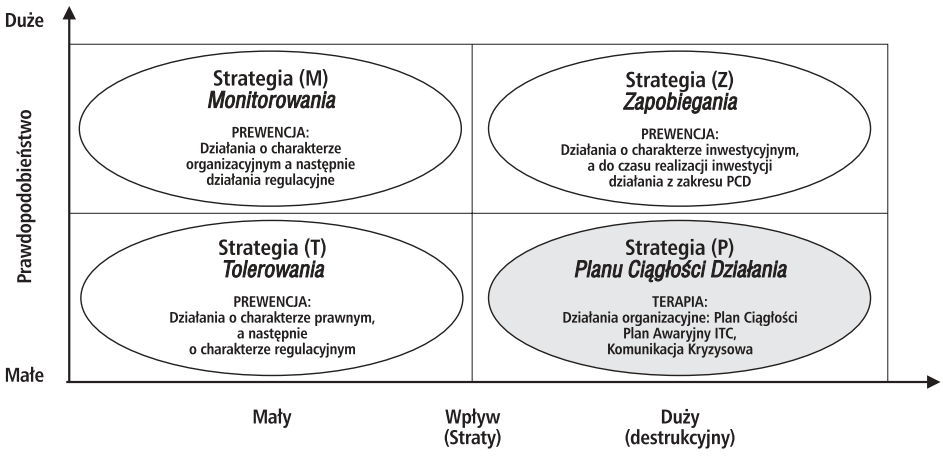
1. Zidentyfikowana liczba słabych punków ochrony informacji
2. Liczba incydentów naruszenia bezpieczeństwa informacji
3. Udział czasu niedostępności systemu informatycznego
4. Liczba i wielkość projektów rozwojowych.

Baza danych strat operacyjnych jest budowana w firmie wykorzystując ustalony system raportowania strat powstałych w wyniku zaistniałych incydentów operacyjnych. Dane te są gromadzone poprzez dedykowany system informatyczny (np. hurtownia danych), bądź też, wykorzystywane są specjalne aplikacje raportujące straty z systemów produkcyjnych. Dotyczy to obszaru strat oczekiwanych, o dużej częstotliwości występowania i nikłej dolegliwości. Na szczycie struktury zarządzania ryzykiem operacyjnym znajduje się obszar analiz. Przetworzenie informacji spływających z poszczególnych poziomów struktury zarządzania ryzykiem operacyjnym, umożliwia skuteczną reakcję na występujące zakłócenia i ograniczenie strat.

6. Strategie reagowania na zakłócenia

W zależności od wielkości wpływu zakłócenia (incydentu) na organizację i prawdopodobieństwa wystąpienia zakłócenia wyróżniamy 4 podstawowe strategie reagowania na zagrożenia[21].

Rys. 5. Strategie reagowania na zakłócenia



Źródło: Opracowanie własne na podstawie ENSI „TISM-BCP" [30]

21. Zawiła-Nadźwiecki J. *Metoda TISM-BCP – Total Security Management, Business Continuity Planning*, European Network Security Institute, Warszawa 2003

- **Strategia tolerowania (T)**: powinna być stosowana w przypadku zakłóceń zewnętrznych nieinwazyjnych i niedestrukcyjnych, rzadko występujących, mających mały wpływ na organizację, przemijających samoistnie i nie powodujących trwałych szkód.
- **Strategia monitorowania (M)**: dotyczy postępowania z zakłóceniami drobnymi, nie destrukcyjnymi, ale często występującymi, o dostatecznej informacji o zakłóceniach do uruchomienia mechanizmów kompensacji.
- **Strategia zapobiegania (Z)**: nazywana strategią prewencji jest stosowana w przypadkach dużego prawdopodobieństwa wystąpienia zakłóceń istotnych elementów działalności, a w szczególności wrażliwych elementów infrastruktury technicznej, których stopień destrukcji jest nieakceptowany.
- **Strategia Planów Ciągłości (P)**: dotyczy postępowania z zakłóceniami istotnymi, destrukcyjnymi o bardzo małym prawdopodobieństwie wystąpienia. Ze względu na niskie potencjalne prawdopodobieństwo wystąpienia katastrof mogących spowodować kryzys, ekonomicznie uzasadniona jest rezygnacja ze Strategii (Z) i uprzednie przygotowanie planu postępowania w sytuacjach kryzysowych.

7. Zarządzanie ryzykiem ciągłości działania

Zarządzanie ciągłością biznesową oparte na Strategii Planów Ciągłości (P), nie powinno być działalnością wyizolowaną w ramach organizacji. Bardzo ważne jest, aby zapewnienie możliwości ciągłego działania w naturalny sposób wynikało z celów firmy i strategii ich osiągnięcia. Brytyjski Instytut Ciągłości Działania (*Business Continuity Institute*) definiuje Zarządzanie Ciągłością Działania jako: „holistyczny proces zarządzania, który ma na celu określenie potencjalnego wpływu zakłóceń na organizację i stworzenie warunków budowania odporności na nie oraz zdolności skutecznej reakcji w zakresie ochrony kluczowych interesów właścicieli, reputacji i marki organizacji, a także wartości osiągniętych w jej dotychczasowej działalności”[22].

Rys. 6. Holistyczny proces zarządzania ciągłością działania

Źródło: BCI „Good Practice Guidelines” [4]

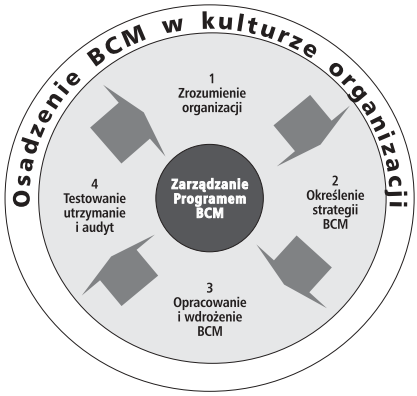
22. Business Continuity Institute: *Business Continuity Management: Good Practice Guidelines* 2002

Zarządzanie Ciągłością Działania (BCM) należy traktować nie jako wąską dyscyplinę uprawianą jedynie przez profesjonalistów, ale jako szerokie spektrum działań zawierających w sobie zarówno zarządzanie ryzykiem, zarządzanie kryzysowe, zarządzanie bezpieczeństwem oraz przywracanie systemów IT po katastrofie i odtwarzania utraconych danych. Jest ono częścią zarządzania korporacyjnego i stanowi zestaw dobrych praktyk dostarczających wytyczne do takiego przeprojektowania procesów wytwarzania produktów i świadczenia usług, aby zwiększyć odporność organizacji na wystąpienie szkodliwych zakłóceń przerwania procesów i poniesienia strat.

Jak już wspomniano zarządzanie ciągłością musi być osadzone w kulturze organizacji, być elementem ładu korporacyjnego (*corporate gevernance*), być wpisanym w procesy realizowane w organizacji i posiadać właścicieli biznesowych. Całościowy Program składa się z pięciu głównych obszarów:

- zarządzanie Programem Ciągłości Działania,
- zrozumienie organizacji,
- określenie Strategii Przetrwania,
- opracowanie i wdrożenie Planów Ciągłości Działania,
- testowanie, utrzymanie i audyt.

Rys. 7. Cykl Życiowy zarządzania ciągłością działania – BCM



Źródło: BS 25999 – 1: „Code of practice" [4]

Opracowana w 2007 norma brytyjska BS 25999[23] dotycząca zarządzania ciągłością działania, traktuje system zarządzania ciągłością w identyczny sposób jak w normach dotyczących systemów zarządzania jakością (ISO 9000-2000). Standard stosuje metodę PDCA: zaplanuj, wykonaj, sprawdź, działaj (*Plan-Do-Check-Act*), jako podstawową do ustanowienia, wdrożenia, monitoringu, testowania, utrzymania i usprawniania systemu zarządzania ciągłością. System ten, otrzymuje jako dane na wejściu oczekiwania i wymagania zainteresowanych stron i poprzez niezbędne działania i procesy tworzy rezultaty ciągłości działania, realizujące wymagania stawiane przez interesariuszy[24].

23. BS 25999 Business Continuity Management: Part 1: *Code of practice*, Part 2: *Specification*
24. Zobacz: BS 25999 - 2 *Specification* str.7

Rekomendowane procesowe podejście, oparte na cyklu PDCA tworzy Cykl Życiowy BCM. Zarządzanie ciągłością działania jest elementem zarządzania ryzykiem organizacji, Jednakże występują między nimi różnice. Możemy je prześledzić na podstawie danych zawartych w tabeli 1.

Tabela 1. Porównanie Zarządzania Ryzykiem z Zarządzaniem Ciągłością Działania

	Zarządzanie Ryzykiem	Zarządzanie Ciągłością Działania
Podstawowa metoda	Analiza Ryzyka *Risk Analisis*	Analiza Wpływu na Działalność *Business Impact Analysis*
Kluczowe parametry	Wpływ i Prawdopodobieństwo	Wpływ i Czas
Rodzaj incydentów	Wszystkie typy zdarzeń – często segmentowane	Zdarzenia powodujące znaczące zakłócenie działalności
Rozmiary zdarzeń	Wszystkie rozmiary (koszty) zdarzeń – często segmentowane	Istotne strategicznie: tylko incydenty zagrażające przetrwaniu
Zakres	Zarządzanie ryzykiem w głównych obszarach działalności	Zarządzenie incydentami przeważnie poza głównymi obszarami działalności
Występowanie zdarzeń	Wszystkie rodzaje od stopniowego do nagłego	Nagłe lub gwałtowne zdarzenia (możliwe narastanie incydentu aż do kryzysu)

Źródło: BCI „Good Practice Guidelines" [4]

7.1. ZARZĄDZANIE PROGRAMEM CIĄGŁOŚCI DZIAŁANIA[25]

Skuteczny program zarządzania programem powinien zapewniać, że zdolność organizacji do zarządzania ciągłością jest ustanowiona i utrzymywana na odpowiednim poziomie. Składa się on z trzech kroków[26]:

a. Przydzielenie odpowiedzialności:
   Program musi mieć silne wsparcie wyższego kierownictwa od samej jego inicjacji w organizacji. Jest to konieczne dla podniesienia rangi programu w celu zaangażowania ogółu pracowników. Polega to na wyznaczeniu osoby odpowiedzialnej za wzmiankowany obszar spośród wyższego kierownictwa, najlepiej członka zarządu. Niezbędne też jest wskazanie osoby/osób odpowiedzialnych za jego stworzenie i wdrożenie.
b. Ustanowienie i wdrożenie BCM w organizacji:
   Podstawowym zadaniem w tym etapie jest opracowanie i zakomunikowanie Polityki Ciągłości Działania dla organizacji. Właścicielem Polityki jest najwyższe kierownictwo (zarząd), który jest odpowiedzialny za jej stworzenie, regularne przeglądanie i aktualizację. Polityka jako kluczowy dokument powinna określać zakres i strukturę zarządzania programu BCM., odzwierciedlającego cele, strategie ich realizacji oraz kulturę organizacyjną. Polityka Ciągłości Organizacji jest nazywana w metodologii TISM-BCP

25. Zobacz: Business Continuity Institute: Good Practice Guidelines, Chapter 1: *A Management Guide to Implementing Global Good Practice in Business Continuity Management* 2007
26. HM Government: *How prepared are you?* Business Continuity Management Toolkit, Version 1

jako Strategia Postępowania z Zakłóceniami i Zagrożeniami[27] i składa się z zestawu czterech polityk: Tolerowania, Monitorowania, Zapobiegania i Planu Ciągłości.

c. Ciągłe zarządzanie

Są to działania ciągłe prowadzone w celu zakorzenienia problematyki ciągłości działania i jej powszechnej akceptacji w organizacji. Polega to na ciągłym promowaniu tematyki w firmie, okresowym przeglądzie i aktualizacji planów PCD, testowaniu procedur i sposobów realizacji planów. Efektywny program BCM wymaga stałego koordynowania działań przedstawicieli różnorodnych komórek i jednostek operacyjnych, wsparcia, zarządzania, w trakcie całego cyklu życiowego.

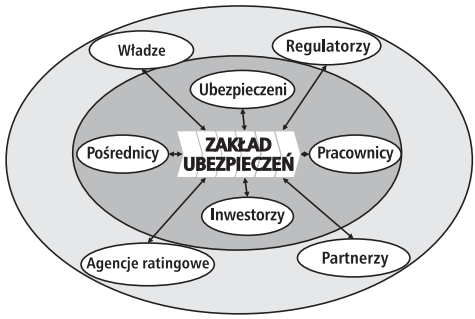
7.2. ZROZUMIENIE ORGANIZACJI

Jest to podstawowy etap cyklu życiowego mający kluczowe znaczenie w zbudowaniu sprawnego Programu Ciągłości Działania, skutecznie zabezpieczającego organizację przed negatywnymi skutkami potencjalnych zakłóceń. Aby dobrze zrozumieć organizację konieczne jest odpowiedzenie na następujące podstawowe pytania:[28]

- Jakie są cele organizacji?
- W jaki sposób są osiągane cele organizacji?
- Jakie produkty/usługi są wytwarzane w organizacji?
- Kto jest zaangażowany (wymagany) (zarówno wewnętrznie i zewnętrznie) w dostarczanie produktów/usług?
- Jaki jest wymagany czas dostarczania produktów/usług?

Jak pamiętamy definicja zarządzania ciągłością działania odwołuje się do zabezpieczenia interesów wszystkich kluczowych interesariuszy, oraz reputacji, marki i działalności kreujących wartość dodaną. Wynika z niej konieczność zidentyfikowania interesariuszy i procesów kluczowych. Dobrze jest sporządzić „mapę interesariuszy" opisującą w sposób graficzny wszystkie zainteresowane strony organizacji. Przykładem takiej mapy jest sporządzona przez K.U. Schanza mapa interesariuszy zakładów ubezpieczeń[29].

Rys. 8. Zarządzanie interesariuszami w ubezpieczeniach

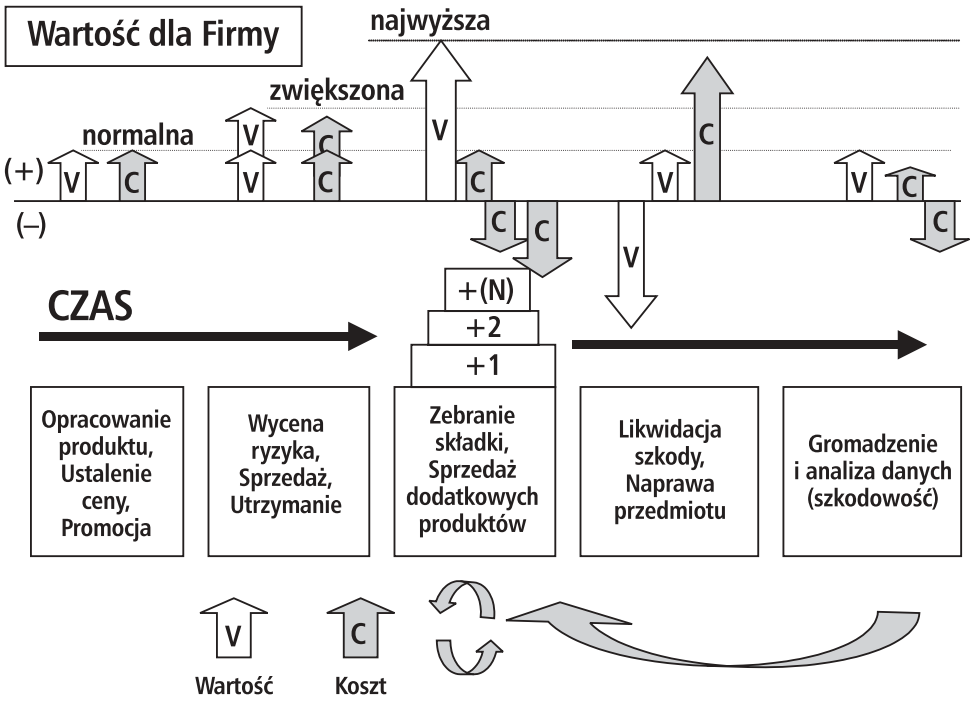


Źródło: K.U. Schanz, „Stakeholder Management in Insurance" [25]

27. Zawiła-Nadźwiecki J. Metoda TISM-BCP – *Total Security Management, Business Continuity Planning*, European Network Security Institute, Warszawa 2003 str. 45
28. Business Continuity Institute: *Good Practice Guidelines* (2007) www.thebci.org
29. Kai Uwe Schanz: Stakeholder *Management in Insurance* www.schanz.com;

Kolejnym krokiem jest sporządzenie mapy procesów na wysokim poziomie ogólności, opisującej główne obszary działalności i powiązania między nimi. Można tu wykorzystać wzmiankowany referencyjny model procesów APQC. Pomocne są też opracowane już, głównie przez firmy doradcze[30] „Łańcuchy wartości"[31] wzorowane na łańcuchu wartości M. Portera.

Rys. 9. Wartość dodana zakładu ubezpieczeń *non life* w łańcuchu wartości



Źródło: Bisker J. „Defining the Insurance Value Chain" [3]

Korzystając z wyznaczonej wiązki celów strategicznych, oraz przyjętych strategii ich realizacji określa się domeny procesów kluczowych, które realizują wyznaczony kierunek rozwoju firmy. Należy również przeprowadzić analizę wolumenu sprzedawanych produktów w poszczególnych grupach, oraz ocenić ich rentowność (wynik techniczny). Konieczne jest również zdiagnozowanie ilości przeprowadzanych operacji w obsłudze posprzedażnej i likwidacyjnej. Wyniki tych analiz umożliwiają skupienie się na najistotniejszych procesach spółki, dostarczających najwięcej wartości.

Etap „Zrozumienia organizacji" składa się z dwóch głównych elementów:

- Analizy wpływu na biznes (*Business Impact Analysis: BIA*)
- Analizy Ryzyka (*Risk Analysis: RA*)

30. KPMG: *Insurance – Globalizing the Risk Business*; www.kpmg.com
31. Zobacz: Bisker J. *Defining the Chain Insurance Value* 2003 www.ibm.com

7.2.1. Analiza Wpływu na Biznes

Analiza ta jest podstawą, z której wynikają wszystkie dalsze etapy cyklu życia zarządzania ciągłością. W jej trakcie identyfikuje się oraz ocenia ilościowy i jakościowy wpływ strat powstałych w wyniku przerwania lub zakłócenia procesów biznesowych. Pierwszym krokiem w tej analizie jest sporządzenie listy kluczowych produktów i usług prowadzonych w organizacji, których zakłócenie z jakiegoś powodu, będzie miało największy wpływ na firmę. Dla każdego zidentyfikowanego produktu i usługi należy rozpatrzyć wpływ zakłócenia w dwóch rodzajach: zdolności organizacji do realizacji celów i zadań (finansowy) i wpływ pozafinansowy (utrata reputacji, wizerunku, wpływ na interesariuszy). Wpływ finansowy to np.:

- utrata możliwości uzyskania przychodów,
- zwiększony koszt działalności,
- obniżenie dochodów (zysków),
- zmniejszenie wydajności i opłacalności,
- koszt zastąpienia aktywów,
- zmniejszenie wartości kapitału i zdolności finansowej.

Na wpływ pozafinansowy składają się następujące składniki:

- utrata reputacja marki i pogorszenie znajomości marki,
- powstanie zobowiązań prawnych i kontraktowych,
- pogorszenie jakości produktów i usług,
- utrata zaufania i wsparcia interesariuszy,
- pogorszenie morale i samopoczucia załogi,
- zmniejszenie kontroli operacyjnej i zarządczej.

Dodatkowym elementem branym pod uwagę w trakcie analizy jest zagrożenie karami ze strony organów regulacyjnych (np. KNF), finansowych (np. UKS) zarówno firmy jak i osób z najwyższego kierownictwa. Często maksymalny wymiar grożących kar jest bardzo wysoki, odnoszący ich wielkość do przypisu składki (np. 0.5 proc. składki ubezpieczeniowej rocznej).

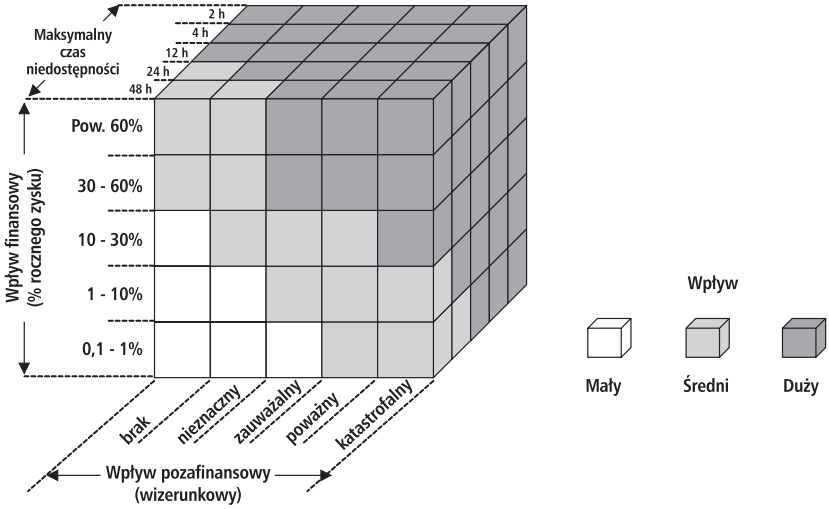
Maksymalne potencjalne straty należy ocenić pod kątem prawdopodobieństwa ich wystąpienia. Na przykład zagrożenie karą w maksymalnej wysokości od regulatora może nie być zrealizowane po wysłaniu informacji o wystąpieniu kryzysu i braku możliwości realizacji określonych wymogów. Wpływ finansowy i reputacyjny powinien być oszacowany i udokumentowany w okresach czasu. Czas niedostępności jest jednym z najważniejszych kryteriów w analizie BIA, przesądzającym o krytyczności procesu. W zależności od rodzaju organizacji ustala się bardziej lub mniej restrykcyjne czasy. Mogą one wynosić od minut (np. operacje na rynku papierów wartościowych, płatność kartami płatniczymi) aż do dni lub tygodni (np. likwidacja szkody). Przykładowe czasy w Analizie BIA mogą wynosić: 2h, 4h, 12h, 24h, 48 h, 7 dni, 30 i więcej dni. Wyłaniając procesy krytyczne w działalności ubezpieczeniowej można się posłużyć dobrymi praktykami opublikowanymi w standardach. Przykładem może być np. Australijski Standard „Zarządzania Ciągłością Działania"[32] określający, jakie czynniki ubezpieczyciele muszą brać pod uwagę w trakcie przeprowadzania analizy BIA. Są to:

32. Australian Prudential Regulation Authority: Prudential Standard GPS 222: *Business Continuity Management*; www.apra.gov.au

- Stopień, w jakim interesy ubezpieczonych mogą być niekorzystnie dotknięte przez zakłócenie normalnych usług i operacji zakładu ubezpieczeń;
- Wpływ finansowy i reputacyjny uszkodzenia możliwości działania ubezpieczyciela ponad określony okres czasu;
- Utrata dochodów jako udział w dochodach całkowitych;
- Stopień trudności, włącznie z potrzebnym do tego czasem, do przywracania działalności lub funkcji wsparcia lub wdrożenia alternatywnych umów (SLA);
- Zdolność ubezpieczyciela do spełniania wymagań regulacyjnych, jeśli były one problemami związanymi z ciągłością działania.

Tak więc, w trakcie BIA są brane pod uwagę 3 czynniki: czas niedostępności procesu, wpływ finansowy i wpływ wizerunkowy. Wpływy są kwantyfikowane w odpowiednich jednostkach: wpływ finansowy najczęściej w procentach zysku netto firmy za dany okres wpływ pozafinansowy jest jakościowo oceniany metodą ekspercką w zależności od liczby niezadowolonych klientów w przedziałach np.: brak, nieznaczny, zauważalny, poważny, katastrofalny. Efektem analizy jest klasyfikacja procesów np. na trzy grupy z wpływem: małym, średnim dużym. Oczywiście każda jednostka ustala indywidualnie rozpiętość i ilość przedziałów wycen w zależności od rodzaju prowadzonej działalności.

Rys. 10. Metoda klasyfikacji wpływu w Analizie BIA



Źródło: opracowanie własne

Przy analizowaniu wpływu przerwania działalności robione jest założenie, że wystąpienie sytuacji kryzysowej może mieć miejsce w najgorszym okresie. Założenie to powoduje przyjęcie **Najgorszych Możliwych Scenariuszy** zdarzeń, co z kolei umożliwia wycenę maksymalnych strat, a w konsekwencji przedsięwzięcie kroków zabezpieczających. W tym celu określamy maksymalny okres czasu, w jakim organizacja może nie dostarczać swoich kluczowych produktów i usług, nie stwarzając istotnego zagrożenia dla swojej egzystencji. Czas ten określany jest mianem: **Maksymalnego Dopuszczalnego Okre-**

su Zakłócenia (*Maximum Tolerable Period of Disruption: **MTPD***). Korzystając z tych wyliczeń możemy wycenić kolejne dwa istotne wskaźniki:

Docelowy Czas Odtworzenia (*Recovery Time Objective: **RTO***) – czas, po którym dane i infrastruktura informatyczna obsługująca procesy biznesowe muszą być odtworzone po awarii lub katastrofie i staną się dostępne dla końcowego użytkownika, na określonym i uzgodnionym poziomie wydajności. W praktyce jest to czas, w którym zostaje uruchomione zapasowe centrum przetwarzania danych.

Docelowy Punkt Odzyskiwania (*Recovery Point Objective: **RPO***) – opisuje, jaka jest maksymalna dozwolona strata danych (np.12 h, 24h). Punkt ten jest uzależniony od częstotliwości tworzenia kopii zapasowych aplikacji informatycznych i określa aktualność (wiek) danych odtworzonych po incydencie.

Dopuszczalny Poziom Wydajności Procesu – uprzednio zdefiniowany poziom realizacji procesów biznesowych w trybie awaryjnym, umożliwiający podtrzymanie działalności w okresie od przekształcenia się incydentu w kryzys do chwili powrotu do normalnej działalności.

Ocena tych parametrów umożliwia wyłonienie **Procesów Krytycznych**, tj. takich procesów, których przerwanie najbardziej zagraża organizacji zarówno pod względem finansowym jak i wizerunkowym.

Identyfikując procesy krytyczne musimy równocześnie diagnozować, jakie systemy i aplikacje informatyczne wspierają proces, z jakimi innymi procesami są powiązane. Konieczność identyfikacji wsparcia informatycznego wynika z faktu, że procesy odtwarzania systemów informatycznych są immanentną częścią zarządzania ciągłością działania. Do opisu procesów krytycznych często wykorzystywane są narzędzia informatyczne zbudowane na relacyjnych bazach danych np. (ARIS, Corporate Modeler, MEGA). Prace analityczne z wykorzystaniem narzędzi IT są znacznie przyspieszone, a dodatkowe funkcje tych aplikacji pozwalają na jednoczesne przypisywanie zasobów wykorzystywanych w realizacji procesu do jego poszczególnych kroków.

Drugim krokiem umożliwiającym poznanie organizacji w kontekście wymagań niezbędnych do pracy w sytuacji kryzysowej jest **Analiza Wymagań Ciągłości Działania** (*Continuity Requirement Analysis **CRA***). Zasoby niezbędne do realizacji procesów krytycznych dzielą się na następujące główne grupy:

- Ludzie:

Oceniamy optymalną liczbę pracowników potrzebnych do prowadzenia krytycznych procesów. Ustalamy minimalny poziom zatrudnienia, przy którym można prowadzić część procesów krytycznych (na uprzednio zdefiniowanym dopuszczalnym poziomie wydajności procesu), oraz niezbędne umiejętności oraz wiedzę, którą muszą się legitymować pracownicy

- Obiekty

Określamy, w jakich aktualnych lokalizacjach są realizowane krytyczne procesy oraz jakie są alternatywne siedziby, w których można prowadzić krytyczną działalność. Opisujemy również uzbrojenie techniczne wykorzystywanych obiektów.

- Technologia informatyczna

Diagnozujemy, jakie systemy/aplikacje są niezbędne do prowadzenia krytycznych procesów. Analizujemy też systemy komunikacyjne i transmisji danych wykorzystywane w trakcie prowadzenia krytycznych procesów.

• Informacja

Ustalamy, jakie informacje są niezbędne w realizacji procesów krytycznych. Analizujemy zarówno informacje przechowywane w sposób tradycyjny (papier) jak i elektroniczny. Niezbędne jest stwierdzenie, w jaki sposób zasoby informatyczne są przechowywane, oraz czy, w jaki sposób i gdzie są wykonywane kopie zapasowe.

• Dostawcy i Partnerzy

Niezbędne jest wylistowanie najważniejszych dostawców i partnerów. Określa się ważność podmiotów, od których zależy realizacja procesów. Konieczne jest rozpoznanie czy, do kogo i jakie istotne procesy zostały przekazane do realizacji poza organizację. (*outsourcing*). W takim przypadku konieczne jest stwierdzenie czy i jaka umowa została zawarta na realizację usług. (tzw. *Service Level Agreement SLA*). Efektem są zestawienia tabelaryczne nazywane niekiedy Minimalną Akceptowalną Konfiguracją (MAK). Informacje tam zawarte umożliwiają wyłonienie zasobów ludzkich, informatycznych i biurowych wymaganych do podtrzymania realizacji procesów krytycznych. Stanowi ona podstawowy element do budowania następnego etapu Strategii Ciągłości Działania.

Ze względu na wagę i podstawowe znaczenie Analizy BIA, najczęściej jest ona prowadzona w formie projektu. Zalecane jest wykorzystywanie metodyk stosowanych w zarządzaniu projektami np. Prince II lub PMI. Struktura zarządzania projektem musi określić organ zatwierdzający produkty projektu (np. komitet sterujący) oraz osobę odpowiedzialną za operacyjne prowadzenie zadań projektowych (kierownik projektu). Sponsorem takiego projektu powinna być osoba posadowiona wysoko w strukturze organizacji najlepiej prezes zarządu lub, co najmniej członek zarządu. Wyniki analizy oraz wnioski z niej płynące muszą być w pełni dokumentowane i zatwierdzane przez właściwe gremia. W zależności od wielkości firmy i struktury zarządzania może to być zarząd, komitet ryzyka operacyjnego lub inne uprawnione ciała. Zalecane są trzy główne metody przeprowadzania analiz. Są to warsztaty, kwestionariusze i wywiady. Dobór optymalnej metody zależy od wielkości firmy, jej kultury organizacyjnej oraz zasobów przeznaczonych do prowadzenia projektu.

7.2.2. Analiza Ryzyka

Ocena Ryzyka,w kontekście zarządzania ciągłością działania, ocenia prawdopodobieństwo i wpływ rozmaitych specyficznych zagrożeń, mogących być przyczyną przerwania działalności. Ocena Ryzyka powinna być skupiona na procesach biznesowych z najkrótszymi czasami odzyskiwania (RTO), zidentyfikowanych w trakcie Analizy Wpływu (BIA).

Pierwszym etapem analizy jest sporządzanie listy zagrożeń. Można się tu posłużyć metodą benchmark porównując ze sporządzonymi listami zagrożeń dostępnymi w istniejących metodykach np. TISM, DRII[33]. Najczęściej zagrożenia dzielą się na: naturalne, ludzkie, technologiczne lub polityczne. W instytucjach finansowych można stosować prostszy, czytelniejszy podział tylko na dwa rodzaje: związane z procesami w tym: związane z ludźmi, budynkami, technologią i informacją oraz z reputacją. Oczywiście ko-

33. DRI International: Professional Practices for Business Continuity Planners: *Risk Evaluation and Control* 2004; www.drii.org

nieczne jest dostosowanie listy zagrożeń do danej organizacji tak, aby występowały tylko najbardziej prawdopodobne i realne. Kolejnym krokiem oceny jest podział na bezpośrednie i pośrednie oraz zewnętrzne i wewnętrzne. Sporządzanie takiej listy musi się odbywać we współpracy z pracownikami bezpośrednio zaangażowanymi w realizacji procesów krytycznych, w trakcie wizji lokalnych. Zweryfikowaną listę zestawiamy z lokalizacjami, w których jest prowadzona działalność. Następnie metodą ekspercką szacujemy prawdopodobieństwo wystąpienia zagrożenia z listy w konkretnej lokalizacji. Po ocenieniu możliwości zrealizowania się zagrożenia analizujemy mechanizmy zabezpieczające w organizacji. Mechanizmy te zmniejszają ryzyka operacyjne w firmie w tym ryzyko przerwania działania. Efektem pracy jest sporządzony raport z analizy zagrożeń, zawierający pełny obraz „apetytu na ryzyko ciągłości działania" będący przedmiotem zatwierdzenia przez właściwe organy firmy.

7.3. OKREŚLENIE STRATEGII CIĄGŁOŚCI DZIAŁANIA (PRZETRWANIA)

Ta część cyklu życia BCM dotyczy tworzenia i wyboru Strategii Ciągłości Działania nazywanej również Strategią Przetrwania stosowanej do kontynuowania działalności organizacji pomimo wystąpienia sytuacji kryzysowej. Aby zawęzić obszar analizy, organizacje często definiują zestawy scenariuszy sytuacji kryzysowych, na które firma się przygotowuje. Przykładowymi scenariuszami branymi pod uwagę są:

- Całkowite lub częściowe zniszczenie i/lub niedostępność kluczowych budynków
- Niedostępność krytycznych funkcji biznesowych, systemów i informacji
- Niedostępność istotnych osób z zarządu
- Niedostępność krytycznej wiedzy i kluczowego personelu
- Brak lub uszkodzenie danych
- Uszkodzenie lub strata ważnej infrastruktury (IT, łączność)
- Utrata istotnych partnerów biznesowych lub usługodawców.

Celem etapu jest określenie obszarów organizacji, które powinny zostać objęte szczególną ochroną, wybór odpowiednich metod zabezpieczenia procesów występujących w wyznaczonych obszarach oraz przeprowadzenie analizy alternatywnych rozwiązań umożliwiających ich zabezpieczenie. Prace są prowadzone na procesach krytycznych wyłonionych w Analizie BIA. Budowanie strategii musi być prowadzone w ścisłej współpracy z działami IT ze względu na fakt wykorzystywania technologii informatycznych i telekomunikacyjnych w realizacji procesów. Dotyczy to szczególnie firm ubezpieczeniowych, które wykorzystują w maksymalnym stopniu systemy informatyczne w swej działalności. Tworząc strategie dokonujemy:

- wyboru alternatywnych metod operacyjnych możliwych do zastosowania w celu utrzymania lub wznawiania działalności organizacji po wystąpieniu sytuacji kryzysowej,
- określenia sposobów ochrony podatnych obszarów i wrażliwych punktów krytycznych w procesach biznesowych zidentyfikowanych w trakcie Analizy Ryzyka,
- ustalenia możliwego poziomu realizacji poszczególnych procesów biznesowych w sytuacji kryzysowej bez użycia krytycznych aplikacji i systemów IT,
- zaproponowania rozwiązań zapasowych dla krytycznych systemów informatycznych.

Podczas opracowywania strategii sprawdza się czy firma posiada wystarczające zasoby gwarantujące bezpieczne odtworzenie krytycznych procesów biznesowych w wyma-

ganym czasie. W praktyce polega to na sprawdzeniu czy istnieje, a w przypadku braku zaproponowanie stworzenia, co najmniej:

- Lokalizacji zapasowych dla podtrzymania krytycznych procesów biznesowych
- Zapasowego centrum przetwarzania danych
- Zapasowego call-center

Niezbędna jest również ocena czy proponowane lokalizacje zapasowe są wystarczające pod względem powierzchni, wyposażenia, zabezpieczeń, oddalenia od instalacji podstawowych. Konieczne jest zapewnienie wystarczającej liczby odpowiednich pracowników oraz dostępu do krytycznych danych, dokumentacji i usług zewnętrznych.

Dla każdego z procesów tworzymy Strategię Ciągłości, która może polegać na[34]:

- nie wykonujemy części procesów,
- stosujemy procedury ręczne,
- zawieramy umowy (SLA) na realizację procesu,
- wykorzystujemy zastępczą lokalizację działalności,
- stosujemy alternatywne źródło produktów,
- korzystamy z usługi/ wykonawcy strony trzeciej (*outsourcing*),
- rozdzielamy procesy,
- wykorzystujemy alternatywne kanały łączności.

Wyboru opcji działania można dokonać z wykorzystaniem metod stosowanych w zarządzaniu strategicznym np. analizy SWOT. Bardzo istotnym kryterium przy wyborze strategii są koszty jej wdrożenia. Dla każdego z wariantów niezbędne jest oszacowanie kosztów realizacji w relacji do uzyskanych korzyści. Analiza Koszt – Korzyść jest konieczna w podjęciu decyzji, co do wariantu strategii. Jest również podstawowym dokumentem rozpatrywanym przez zarząd w trakcie podejmowania decyzji inwestycyjnych.

7.4. OPRACOWANIE I WDROŻENIE REAKCJI BCM

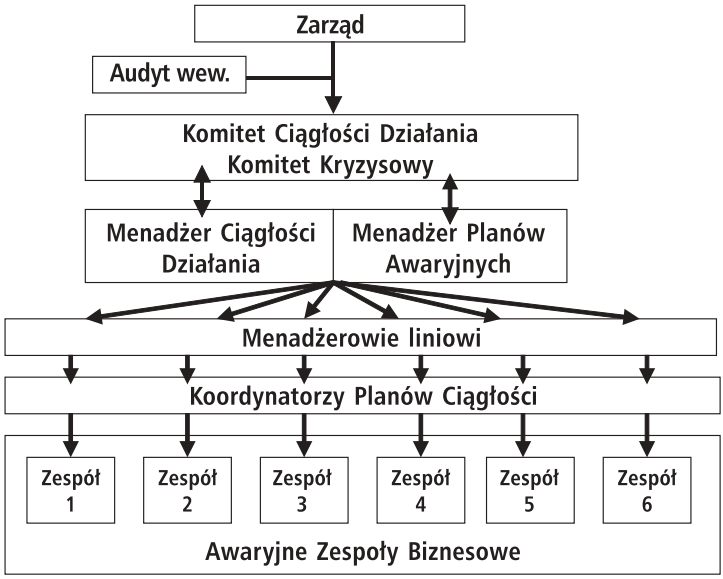
Skuteczna reakcja na występujące incydenty jest możliwa w organizacjach posiadających dedykowaną strukturę zarządzania kryzysowego wyposażoną w uprawnienia do działania. Struktura ta ma dwa różne zadania. W czasie prowadzenia normalnej działalności (czas spokoju) jej główna aktywność skupia się na opracowaniu Planów Ciągłości, i Planów Awaryjnych IT, ich monitorowaniu i zmian w razie konieczności. W przypadku wystąpienia sytuacji kryzysowej przekształca się ona w sztab kryzysowy zarządzający zespołami awaryjnymi.

Najczęściej w organizacjach zostaje wyznaczona osoba odpowiedzialna za całokształt operacyjnego zarządzania ciągłością działania. Jest to stanowisko **Menadżera Ciągłości Działania** (*Business Continuity Manager BCMgr*). Jego zastępcą jest **Menadżer Planów Awaryjnych** (*Disaster Recovery Process Manager DRPMgr*) osoba z pionu informatyki najczęściej odpowiedzialna za eksploatację systemów informatycznych. Obydwaj menadżerowie działają pod nadzorem komitetu składającego się z kluczowych menadżerów w organizacji. Reprezentują oni departamenty: HR, PR, Ryzyka, Administracji, a także, co najmniej jeden z departamentów biznesowych. Audyt wewnętrzny jest w składzie, ale ze

34. DRII: Professional Practices for Business Continuity Planners: Subject Area 4 *Developing Business Continuity Strategies*; 2004; www.drii.org

względu na swoją niezależność występuje w roli obserwatora. Komitet ten funkcjonuje jako samodzielny **Komitet ds. Ciągłości Działania**, lub też jego role może pełnić Komitet Ryzyka Operacyjnego.

Rys.11. Przykładowa struktura zarządzania ciągłością działania



Źródło: opracowanie własne

W chwili zaistnienia kryzysu przekształca się w **Komitet Kryzysowy**. Komitet Kryzysowy jest wspierany przez zespoły wsparcia tworząc sztab kryzysowy. Awaryjne Zespoły Biznesowe, których skład jest ustalony na podstawie wcześniej przeprowadzonej Analizy Wymagań dla procesów krytycznych.

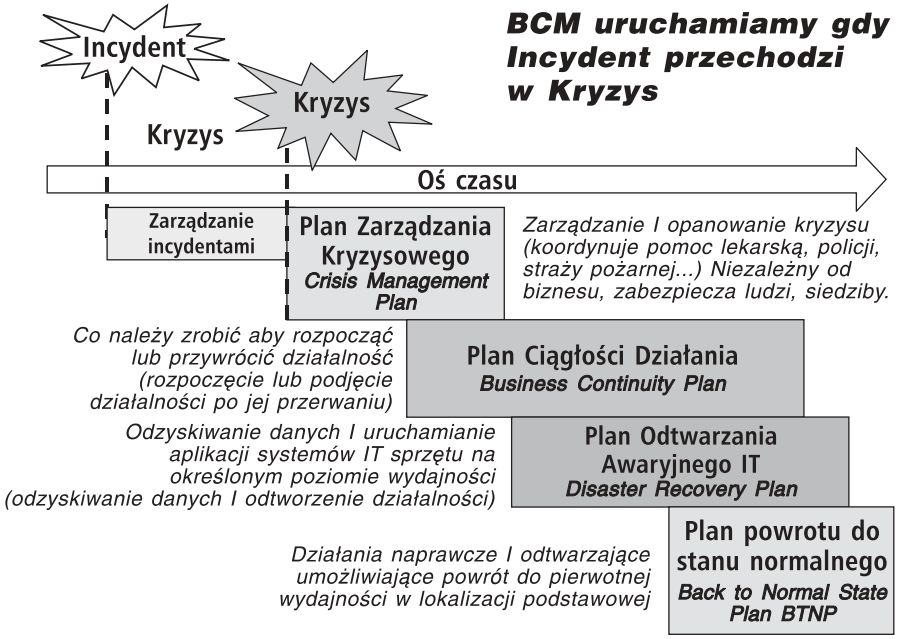
7.5. OPRACOWANIE I WDROŻENIE PROGRAMU ZARZĄDZANIA CIĄGŁOŚCIĄ DZIAŁANIA

Jest to kolejny etap cyklu życiowego dotyczący opracowania i wdrażania odpowiednich planów przygotowań zapewniających zarządzanie incydentem, przywracanie funkcjonowania krytycznych procesów oraz prowadzenie działalności tworzącej kluczowe produkty i usługi.

Plany są to zestawy procedur dla określonych grup pracowników (zespołów awaryjnych), opisujące schematy postępowania w sytuacji kryzysowej. W ramach programu znajdują się cztery główne zestawy planów działania uruchamiane w zależności od interwału czasowego po wystąpienia kryzysu. Są to procedury: zarządzania kryzysowego, plany ciągłości działania, plany awaryjne IT oraz plany powrotu do normalnej działalności. Liczba planów i ich zawartość zależy od organizacji i powinna odzwierciedlać strukturę i kulturę organizacji oraz złożoność jej krytycznych procesów. Dla małych organizacji wystarczy jeden plan zawierający wszystkie wymienione aspekty. Dla firm dużych o rozbudowanej strukturze, działającej w wielu lokalizacjach, tworzy się odrębne zestawy planów dla poszczególnych domen reakcji na kryzys. Najistotniejsze jest, aby plany zawierały wszystkie

informacje, które organizacja potrzebuje do zarządzania w czasie niespodziewanego incydentu i zapewniały ciągłość funkcjonowania krytycznych procesów. Nie mniej istotne jest zapewnienie łatwego dostępu do planów i ich kopii, najczęściej składowanych w lokalizacjach zapasowych.

Rys. 12. Plany w systemie zarządzania ciągłością działania



Źródło: opracowanie własne

7.5.1. Plan Zarządzania Kryzysowego

Doświadczenia wynikające z analizy wystąpienia największych incydentów wykazały, że skuteczne i natychmiastowe zarządzanie sytuacją kryzysową jest znaczącym czynnikiem w zabezpieczeniu organizacji przed szkodami finansowymi i reputacyjnymi. Plan Zarządzania Kryzysowego nazywany niekiedy Planem Zarządzania Incydentami definiuje skład zespołów szybkiego reagowania oraz ich role w pierwszych momentach wystąpienia kryzysu. Powinien zawierać kontakty ze służbami pierwszej pomocy: strażą pożarną, pogotowiem ratunkowym, policją i komórkami zarządzania kryzysowego miast. W przypadku wynajmowania powierzchni biurowych, konieczne jest ustalenie zasad współpracy z administratorem budynków. Częściami takiego planu są zazwyczaj procedury ogłaszania i odwoływania alarmu, ewakuacji z budynków, miejsc alokacji, zachowania pracowników. Kluczowym. elementem takich procedur jest system komunikowania o sytuacji kryzysowej nazywany „drzewem powiadamiania". Umożliwia on na zasadzie kaskady poinformowanie wszystkich pracowników począwszy od najwyższego kierownictwa aż do szeregowego pracownika. W budynkach wielokondygnacyjnych wyznaczani są kierownicy ewakuacji odpowiedzialni za sprawne przeprowadzenie akcji opuszczania budynków przez klientów i załogę. Plany te powinny być systematycznie przeglądane i testowane.

7.5.2. Plany Ciągłości Działania

Stanowią zestawy przetestowanych i udokumentowanych procedur operacyjnego zarządzania ciągłością procesów biznesowych, określających organizację i zasady postępowania w ramach działań stanowiących zaplanowane reagowanie na nieoczekiwane wystąpienie zakłócenia o destrukcyjnym wpływie wywołującym kryzys działalności organizacji. Przyjmuje się, że plany ciągłości powinny zabezpieczać organizacje przed skutkami kryzysu przez około 30 dni. Plany ciągłości tworzy się dla zespołów awaryjnych odpowiedzialnych za zarządzanie procesami krytycznymi. Często tworzy się odrębne procedury dla sztabu kryzysowego i zespołów biznesowych. Ich liczba zależy od zatwierdzonej listy procesów krytycznych. Tworząc plany można korzystać z zaleceń zawartych w dobrych praktykach publikowanych przez DRII[35]; BCI[36]; BS[37]; TISM[38]. Typowy plan powinien zawierać następujące informacje:

1 Cel planu i jego założenia
2 Ogólne informacje dotyczące obszaru objętego planem
3 Akceptacja Planu
4 Dystrybucja Planu
  – Lista dystrybucyjna
  – Metoda dystrybucji
  – Plany informacyjne
  – Metoda komunikacji
  – Procedury eskalacyjne
5 Aktywacja planu
  – Kryteria aktywacji planu
  – Odpowiedzialność za wdrożenie planu
  – Kryteria dla zakończenia planu
  – Odpowiedzialność za zakończenie planu
6. Procedury zespołów sztabowych
7. Procedury zespołów IT
8. Procedury zespołów biznesowych

Przykładowa procedura zespołu awaryjnego składa się z następujących części:

- Schemat struktury organizacyjnej Zespołu Awaryjnego
- Skład Zespołu Awaryjnego
- Zakres odpowiedzialności Zespołu Awaryjnego
- Procedury awaryjne
  – Powiadomienie o zdarzeniu
  – Wdrożenie trybu awaryjnego
  – Praca w trybie awaryjnym

35. DRII: Professional Practices for Business Continuity Planners; Subject Area 6: *Developing and Implementing Business Continuity*; 2004; www.drii.org
36. BCI: Good Practice Guidelines; A Management Guide to Implementing Global Good Practice in Business Continuity Management; Chapter 4: *Developing and Implementing BCM Response* 2007; www.thebci.org
37. BS 25999 - 2 *Specification*
38. Zawiła-Nadźwiecki J. *Metoda TISM-BCP – Total Security Management, Business Continuity Planning*, European Network Security Institute, Warszawa 2003

Bardzo ważnym elementem planu jest Plan Komunikacji Zewnętrznej i Wewnętrznej. Plan ten jest w gestii Zespołu Awaryjnego PR. Doświadczenia firm, które dotknął kryzys mówią o kapitalnym znaczeniu zarządzania informacją z interesariuszami. Szczególna rola przypada komunikacji z mediami. Przekazywanie rzetelnych informacji o stanie firmy dotkniętej kryzysem zmniejsza znacząco straty wynikające z utraty reputacji, co przekłada się na uspokojenie reakcji klientów, a w konsekwencji zmniejszenie strat finansowych.

7.5.3.Plany Awaryjne IT

Funkcjonowanie firm sektora finansowego jest w dużym stopniu zautomatyzowane. Pion Informatyki zajmuje bardzo istotną rolę w planach ciągłości organizacji. Z tego powodu Menadżer Planów Awaryjnych IT jest zobowiązany do szczególnie ścisłej współpracy z Menadżerem Ciągłości Działania. Dla sytuacji awaryjnych opracowuje się procedury umożliwiające uruchomienie krytycznych aplikacji/systemów informatycznych obsługujących wyłonione w Analizie BIA procesy krytyczne. Głównym zadaniem tych planów jest zapewnienie realizacji zdefiniowanych celów odtworzenia w dwóch głównych aspektach: Docelowego Czasu Odtworzenia (RTO) oraz Docelowego Punktu Odzyskania Danych (RPO). Te dwa czynniki determinują zdolność firmy do wyjścia z kryzysu z jak najmniejszymi stratami. Praktycznie polega to na przełączeniu krytycznych systemów informatycznych z lokalizacji głównej na instalacje zapasowe znajdujące się w zapasowym centrum przetwarzania. Po ogłoszeniu uruchomienia planów ciągłości w całości lub części, zostają uruchomione procedury przełączeniowe systemów IT, zaś zespoły awaryjne udają się do wyznaczonych lokalizacji zapasowych. Administratorzy systemów krytycznych do zapasowego centrum przetwarzania, zaś zespoły wsparcia do lokalizacji zapasowej. Plany awaryjne IT uruchamia Menadżer Planów Awaryjnych (*DRP Manager*) na wniosek Menadżera Ciągłości Działania (*BC Managera*). Pozostałe systemy (nie krytyczne) nie podlegają procedurze Planów Awaryjnych i nie są uruchamiane. Wydajność pracy systemów jest ograniczona do poziomu uzgodnionego wcześniej w strategii przetrwania. Moment uruchomienia całkowitego centrum zapasowego powinien być zgodny z ustalonym czasem Docelowego Czasu Odtworzenia (RTO). Po pomyślnym uruchomieniu systemy pracują w trybie awaryjnym do momentu ogłoszenia odwołania Planu Ciągłości Działania.

7.5.4. Plan powrotu do stanu normalnego

Organizacje tworzą plany ciągłości zabezpieczające je na okres około 30 dni. Przez ten czas firma pracuje realizując tylko procesy krytyczne. Oczywiście wydajność jest z tego powodu ograniczona. Głównym celem jest maksymalne skrócenie okresu, w którym obsługiwane są tylko niezbędne aktywności i powrót do sytuacji „normalnej". Aby to mogło nastąpić niezbędne jest przygotowanie zarówno pomieszczeń, wyposażenia jak i skompletowanie załogi. Dotyczy to strony biznesowej jak i informatycznej. Po uzyskaniu informacji o możliwości powrotu do lokalizacji podstawowych następuje przejście z pracy w procedurach awaryjnych do procedur trybu operacyjnego. Procedury przejścia zawierają elementy raportowania (konieczne ze względów dokumentacyjnych); kompletowania dokumentacji wytworzonej podczas pracy w trybie awaryjnym, sprawdzenia poprawności i kompletności wytworzonych danych oraz nadrobienia zaległości. Po wykonaniu powyższych czynności można powrócić do pracy w normalnym trybie operacyjnym

7.6. TESTOWANIE, UTRZYMANIE I AUDYT PROGRAMU ZARZĄDZANIA CIĄGŁOŚCIĄ DZIAŁANIA

Zdolność organizacji do zarządzania ciągłością działania może być uznana za zadawalającą dopiero po jej przetestowaniu, zapewnieniu aktualności i regularnego audytowania tego obszaru.

7.6.1. Testowanie

Opracowanie programu BCM musi się zakończyć sprawdzeniem poprawności i skuteczności rozwiązań. Można tego dokonać za pomocą testów, prób (np. alarmu przeciwpożarowego), ćwiczeń (scenariuszowych). Należy opracować kompleksowy program sprawdzeń od najprostszych po najbardziej angażujące organizację. Należy się zawsze kierować zasadą maksymalnego ograniczania ryzyka utraty zasobów w trakcie testów, przy jednoczesnym zapewnieniu wysokiego poziomu pewności zdolności odtworzenia działalności. Dobrze nakreślone cele,opracowanie realistycznych scenariuszy incydentów oraz ustalenie jednoznacznych kryteriów oceny jest gwarancją powodzenia. Budując harmonogram należy przyjąć założenie progresywnego zwiększania zakresu ćwiczeń. Rodzaje testów znajdują się w tabeli.

Tabela 2. Rodzaje testów

Rodzaj testu	Procesy	Uczestnicy	Częstotliwość	Złożoność
Test notyfikacyjny	Sprawdzenie zawartości planu	Autor planu, inny menadżer (weryfikacja)	Wysoka	Niska
Gra sztabowa	Wykonanie rozszerzonego testu biurowego w celu sprawdzenia interakcji i ról uczestników	Autor planu Główni uczestnicy	średnia	średnia
Ćwiczenia symulacyjne	Włączenie planów powiązanych Plany biznesowe, Komunikacja, Budynki	Główni uczestnicy: obserwatorzy, koordynatorzy	średnia	średnia
Testowanie operacyjne	Przeniesienie pracy do innej lokalizacji. Odtwarzanie istniejącej pracy z lokalizacji przeniesionej	Pracownicy biznesowi, dostawcy centrum zapasowego IT, obserwatorzy, koordynatorzy	średnia	średnia
Pełny Test	Zamknięcie całego budynku i przeniesienie pracy	Wszyscy pracownicy w budynku, pracownicy, dostawcy Zapasowego centrum IT, koordynatorzy obserwatorzy	Niska	Wysoka

Źródło: BCI: Exercising, maintaining & Reviewing BCM Arrangements [7]

Przeprowadzone testy zawsze muszą być zakończone raportem podsumowującym wyniki oraz rekomendującym określone działania usprawniające i naprawcze. Rekomendacje winny być skierowane do konkretnych osób i monitorowane.

7.6.2. Utrzymanie programu

Utrzymanie planu w pełnej aktualności stanowi gwarancje gotowości spółki na sytuacje kryzysowe. Przesłankami dostosowania planu do nowych warunków są m.in.

- Zmiana lub rozszerzenie działalności
- Zmiana listy procesów krytycznych
- Zmiana przebiegu procesów krytycznych
- Zmiany organizacyjne wpływające na procesy
- Duże zmiany w systemach IT lub wdrożenie nowych
- Zmiany w infrastrukturze telekomunikacyjnej
- Zmiany we współpracy z dostawcami zewnętrznymi
- Zmiany kadrowe w składach zespołów awaryjnych.

Wymienione zmiany należy analizować pod kątem ich wpływu na plany i po zdiagnozowaniu potrzeby należy wprowadzać modyfikacje w istniejących procedurach. W celu sprawnego monitorowania zmian i aktualizacji procedur wprowadza się specjalny System Kontroli Zmiany. Jest to opisana procedura procesu monitorowania zmian w organizacji, oceny ich wpływu (nieistotny, znaczący), rejestracji oraz modyfikacji planów. Ustala też komórki organizacyjne uczestniczące w procesie oraz ich role. Jednostką odpowiedzialną za zarządzanie **Systemem Kontroli Zmiany** jest departament/biuro nadzorujące Plany Ciągłości Działania.

Fundamentalne znaczenie dla ustalenia wysokiej rangi problematyki zarządzania ciągłością biznesową jest trwałe jej osadzenie w kulturze organizacji. Utrzymanie wysokiej świadomości problematyki wśród pracowników utrzymuje ich entuzjazm i gotowość do skutecznej reakcji na incydenty. W tym celu opracowuje się **Program Utrzymania Świadomości Ciągłości Działania**. Polega on na zaprojektowaniu i przeprowadzaniu cyklu szkoleń dla pracowników nowo zatrudnionych wyjaśniających im zadania wynikające z realizacji programu oraz szkoleń uzupełniających dla pozostałej części załogi. Minimalny zakres przekazywanych informacji powinien zawierać:

- Definicje i terminy
- Politykę i standardy
- Role i odpowiedzialności jednostek zaangażowanych
- Procesy krytyczne
- Strategie Ciągłości Działania (Przetrwania)
- Procedury awaryjne i odtworzeniowe.

Program Utrzymania Świadomości ma również za zadanie monitorowanie pojawiających się zmian w kulturze organizacji i dostosowanie się do nich. Kampania świadomościowa musi być prowadzona nieustannie i powinna wykorzystywać wszystkie dostępne środki przekazu w firmie takie jak: tablice ogłoszeń, pisma i biuletyny wewnętrzne, portale intranetowe.

7.6.3. Audyt

Funkcja audytu programu zarządzania ciągłością polega na porównaniu zgodności zdefiniowanej Polityki Ciągłości Działania, standardów i procedur ze stanem faktycznym, wykryciu ewentualnych luk w ich realizacji oraz wydaniu rekomendacji korygujących. Występują trzy podstawowe rodzaje oceny audytowej:

- audyt realizowany przez jednostki zewnętrzne,
- audyt wewnętrzny,
- samoocena.

Dobór właściwej metody jest uzależniony od rangi zadania audytowego, zaawansowania wdrożenia programu zarządzania ciągłością oraz kultury organizacyjnej firmy. Powszechnie uznaje się, że najlepszym i najbardziej dojrzałym sposobem audytowania jest samoocena obszaru wykonywana przez zainteresowane jednostki.

8. Podsumowanie

Realizacja misji zakładów ubezpieczeń, którą jest zapewnienie ciągłej ochrony ubezpieczonych jest możliwa dzięki stworzeniu Programów Zarządzania Ciągłością Działania.

Przełom stuleci zapoczątkował zwiększone zainteresowanie problematyką zarządzania ryzykiem (bomba milenijna), stając się w ostatniej dekadzie jednym z głównych problemów współczesnego zarządzania organizacjami. Nasilone procesy globalizacji i liberalizacji w sektorach finansowych doprowadziły do znacznej koncentracji ryzyka prowadzenia działalności gospodarczej. Postępująca rewolucja informacyjna powoduje, że IT staje się centralnym sposobem komunikacji z klientami, łańcuchem dostawców i partnerów. W tradycyjnych modelach biznesu występował dystans między IT a biznesem. Klient kontaktował się z firmą lub jej przedstawicielami (np. agentami), a dopiero procesy wsparcia obsługiwały informatycznie prowadzoną działalność. W nowym modelu nazywanym czasem *e-business* procesy biznesowe stapiają się z IT w jedną całość. Następuje interakcja klientów z systemami informatycznymi poprzez *interfejsy* oprogramowania lub środki łączności, a nie z pracownikami firmy. Powoduje to zwiększenie wymagań dla IT w zakresie dostępności, szybkości reakcji, oraz zapewnienia bezpieczeństwa. Aby stawić czoła tym wszystkim wyzwaniom firmy budują systemy zarządzania ciągłością działania. Warto zauważyć, że trochę niepostrzeżenie stajemy się świadkami narodzin nowego obszaru zastosowań naukowej organizacji zarządzania, określanego – dziś jeszcze może zbyt pochopnie – mianem teorii *Business Continuity Management* (BCM)[39]. Warto dodać, że Dyrektywa Solvency II, która będzie obowiązywać od 2012 roku nakłada również obowiązek posiadania Planów Ciągłości na zakłady ubezpieczeń.

Mgr. inż. ***PAWEŁ GOŁĄB*** *– jest ekspertem w Departamencie Zarządzania Ryzykiem TUiR Warta S.A./TUnŻ Warta S.A.*

Recenzenci – prof. zw. dr hab. Jan Monkiewicz, prof. zw. dr hab. Wanda Ronka-Chmielowiec.

39. Zawiła-Niedźwiecki Janusz: *Dobre praktyki czy teoria zapewniania ciągłości działania*; Referat

Bibliografia:

1. American Productivity & Quality Center: *Process Classification Framework* www.apqc.org
2. Australian Prudential Regulation Authority: Prudential Standard GPS 222: *Business Continuity Management*; www.apra.gov.au
3. Bisker J. *Defining the Insurance Value Chain* 2003; www.ibm.com.
4. Business Continuity Institute: *Business Continuity Management: Good Practice Guidelines* 2002.
5. Business Continuity Institute: *A Management Guide to Implementing Global Good Practice in Business Continuity Management* (2007) www.thebci.org
6. Business Continuity Institute: *Developing and Implementing BCM Response* 2007; www.thebci.org
7. Business Continuity Institute: *Exercising, maintaining & Reviewing BCM Arrangements* 2007; www.thebci.org
8. BS 25999 Business Continuity Management: Part 1:*Code of practice*, Part 2: *Specification*
9. Capuri G. *Corporate Social Responsibility Strategy in Practice* Uni Credit, materiały z konferencji: *Strategia Odpowiedzialnego Biznesu*, Warszawa 2008.
10. Committee on Banking Supervision *Sound Practices for the Management and Supervision of Operational Risk*, Bank for International Settlements, Basel, 2003.
11. De Nederlandsche Bank: *Risk measurement within financial conglomerates: best practices by risk type*; Research Series Supervision no. 51, February 2003.
12. Disaster Recovery Institute International: *Developing Business Continuity Strategies*; 2004; www.drii.org
13. Disaster Recovery Institute International DRII: *Developing and Implementing Business Continuity*; 2004; www.drii.org
14. Disaster Recovery Institute International: *Risk Evaluation and Control* 2004; www.drii.org
15. Ernst & Young Advisory; *Zarządzanie ryzykiem w organizacjach*; www.ey.com
16. Federation of European Risk Management Associations: *Standard Zarządzania Ryzykiem*; www.theirm.org
17. Główny Inspektorat Nadzoru Bankowego *Rekomendacja D dotycząca zarządzania ryzykami towarzyszącymi systemom informatycznym i telekomunikacyjnym używanych przez banki*, NBP, Warszawa, 2002. www.knf.gov.pl.
18. Główny Inspektorat Nadzoru Bankowego *Rekomendacja M dotycząca zarządzania ryzykiem operacyjnym w bankach*, NBP, Warszawa, 2004. www.knf.gov.pl.
19. HM Government: *How prepared are you?* Business Continuity Management Toolkit, Version 1 www.preparingforemergencies.gov.uk
20. International Association of Actuaries: *Report of Solvency Working Party, of KPMG/European Commission* (2002), *Study into the Methodologies to Assess the Overall Financial Position of an Insurance Undertaking from the Perspective of Prudential Supervision*. www.actuaries.org
21. KPMG: *Globalizing the Risk Business – Surviving and competing in the global insurance industry* www.kpmg.com
22. Kulik A. CFA: *ABC Zarządzania Ryzykiem – Ryzyko Operacyjne* Prezentacja, Warszawa 2003
23. Orzeł J.: *Na drodze do zaawansowanych metod ilościowego pomiaru ryzyka operacyjnego – KRI*; Bank i Kredyt, Warszawa 2005

24. Polska Izba Ubezpieczeń *Klasyfikacja ryzyk ponoszonych przez zakłady ubezpieczeń* Warszawa, 2004; www.piu.org.pl
25. Schanz Kai Uwe: *Stakeholder Management in Insurance* www.schanz.com;
26. The Joint Forum: *High – Level Principles for Business Continuity*; August 2007. www.bis.org
27. Zawiła-Niedźwiecki J.,*Analiza aktualnego stanu zarządzania ciągłością działania przez towarzystwa emerytalne w Polsce*, praca badawcza i zarazem raport dla Komisji Nadzoru Finansowego, Warszawa 2006
28. Zawiła-Niedźwiecki J., *Ciągłość Działania Organizacji*, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2008
29. Zawiła-Niedźwiecki J.: *Dobre praktyki czy teoria zapewniania ciągłości działania*; Referat P.W.
30. Zawiła-Nadźwiecki J. *Metoda TISM-BCP – Total Security Management, Business Continuity Planning*, European Network Security Institute, Warszawa 2003
31. Zawiła-Niedźwiecki J., *Stan zarządzania ciągłością działania przez zakłady ubezpieczeń w Polsce*, praca badawcza i zarazem raport dla Komisji Nadzoru Finansowego, Warszawa 2007

Business Continuity Management in insurance companies – summary

Financial institutions, including insurance companies, play an essential role in the world economy. Increasing concentration of activity and interdependence of financial market institutions, the growth of natural disaster threats, terrorism and dependence on IT technologies create a large risk of discontinuity of activities of insurance companies. The aim of the business continuity management is to build the company's protection mechanisms against negative disruption impact, in such a way that in case of crisis main business processes may be continued. The main stages are the following: understanding of organization, including business impact analysis, creation of business continuity strategy, creation of Business Continuity Plan procedures, testing and program maintenance.

This article describes the place of businesses continuity management in the risk management process, reviews the methodology describing this process as well as identifies major stages of program introduction. Keeping the operational security of the insurance companies is already recommended as "the best practice" of the market and after implementing Solvency II it will be mandatory in every insurance company.