Zapewnie ciągłości działania – nowe kierunki w zarządzaniu operacyjnym i ochronie reputacji przedsiębiorstw

Tomasz Potocki, dr, Uniwersytet Rzeszowski, Wydział Ekonomii, Katedra Polityki Gospodarczej

Słowa kluczowe: Niepewność, Plany ciągłości działania, Zarządzanie ciągłością działania, reputacja
Klasyfikacja JEL: M21, H12, L14

Wstęp

Zaburzenie ciągłości działania może zakończyć działalność nawet najbardziej innowacyjnej organizacji. Ostatnie coraz częstsze katastrofy naturalne, terroryzm i sabotaż pracowniczy czy zawodność technologii informatycznych wymaga od organizacji lepszego do tego typu zdarzeń w celu utrzymania dostępności swoich usług i produktów. Ich dostępność staje się bowiem kluczowym czynnikiem gwarantującym ciągłość prowadzonej działalności, niezawodną reputację oraz sukces rynkowy. Wzrastająca dominacja usług typu e-commerce wymusza dostępność na poziomie 365×7×24, a przywrócenie dostępności usług w czasie nie dłuższym niż 2 godziny. Wymagania te są podyktowane poprzez:

- klientów oczekujących dostaw i dostępności w trybie ciągłym;
- akcjonariuszy wymagających pełnej kontroli władz spółki i zapewnienia ciągłości działania w sytuacjach kryzysowych;
- pracowników chcących zapewnić ochronę swoich rodzin poprzez ciągłość pracy;
- dostawców dążących do zapewniania terminowego regulowania zobowiązań;
- regulatorów wymagających przestrzegania przepisów prawa niezależnie od sytuacji biznesowej organizacji;
- ubezpieczycieli wymagających należytej staranności organizacji i wypełnienia zapisów umów [Noakes-Fry, Diamond, 2001, s. 2].

Dodatkowo należy zaznaczyć, że prowadzenie działalności biznesowej nie jest wyłącznie domeną sektora prywatnego. Wszystkie organizacje zarówno prywatne, publiczne, jak i non profit dostarczają bowiem usługi bądź produk-

ty swoim klientom. W łańcuchu dostaw pojawiają się incydenty i zdarzenia, które nie tylko mogą zakłócić efektywny proces dostarczania produktów i usług, ale wręcz go zablokować, doprowadzając do przestoju operacyjnego organizacji. Powoduje to najczęściej obniżenie reputacji organizacji, a przy powtarzaniu się takich zdarzeń prowadzi do jej marginalizacji i w końcu do upadku.

Ale jak przygotować się na sytuacje (ataki terrorystyczne, nagłe powodzie czy pożary), których w większości przypadków nie jesteśmy w stanie przewidzieć? Z pomocą przychodzi strategia zapewnienia ciągłości działania obejmująca szerokie spektrum narzędzi technologicznych, elektronicznych, papierowych. Wykorzystująca narzędzia zautomatyzowane i manualne, a także stosująca podejście indywidualne lub globalne. Zyskuje ona coraz większe znaczenie zarówno w procesie zarządzania ryzykiem operacyjnym, jak i ochronie reputacji przedsiębiorstw. Dużą rolę odgrywają działania związanie z zarządzaniem ryzykiem, zarządzaniem kryzysowym czy budowaniem planów ciągłości działania. Należy jednak zaznaczyć, że efektywność tych działań zależy w głównej mierze od ujęcia ich w planach strategii przedsiębiorstwa i pełnej integracji tych działań z działaniami biznesowymi organizacji.

Zarządzanie ciągłością działania początkowo było utożsamiane z działalnością dużych ponadnarodowych korporacji i sektorem publicznym. Jednak, jak wspomnieliśmy powyżej, obecnie jest to wyzwanie dla każdej organizacji, która chce odnosić sukcesy rynkowe związane ze wzrostem sprzedaży, zadowoleniem klientów i rosnącą reputacją wśród akcjonariuszy.

Jak wskazują bowiem badania prowadzone przez The Chartered Management Institute już ponad 52% wśród badanych organizacji stanowią małe i średnie, bądź te reprezentujące specyficzne i niszowe branże [Woodman, Kumar, 2009, s. 4].

Zarządzanie ciągłością działania nie jest jedynie odpowiedzialnością działów IT. Wskazujemy na ten aspekt, gdyż przez wiele lat i w wielu kręgach dominował ten pogląd. Prawdą jest natomiast, że zarządzanie ciągłością działania narodziło się i rozwijało z planów ciągłości systemów IT, ale już dawno przestało być domeną departamentów IT, a stało się częścią strategii przedsiębiorstwa i związane jest bezpośrednio z działaniami pionów biznesowych.

Logika działań w obszarze zarządzania ciągłością działania powinna objąć jako punkt wyjścia prezentację incydentów i zdarzeń, które mogą zachwiać reputacją przedsiębiorstwa, oraz ich wpływu na działalność operacyjną organizacji. Przykłady takich sytuacji prezentowane są w poniższym rozdziale.

Zagrożenia dla ciągłości działania

Organizacje odpowiadające za swoje działania i wyniki przed interesariuszami muszą wziąć pod uwagę zdarzenia „kryzysowe", które wymagają „kryzysowych" działań i nie mogą być nadzorowane w oparciu o typowe procedury działań naprawczych czy narzędzia zarządzania ryzykiem. Jedną z najpoważniejszych konsekwencji wystąpienia sytuacji kryzysowych może być

zniszczenie bądź czasowa niedostępność infrastruktury organizacji, krytycznej z punktu widzenia prowadzenia działalności biznesowej.

W 2007 roku Chartered Management Institute wydał ósmy już raport *Business Continuity Management* poświęcony ciągłości biznesu, w którym zapytał 10 600 członków instytutu w Wielkiej Brytanii o zagadnienia poświęcone zarządzaniu sytuacją kryzysową oraz potrzebą wdrażania systemów zarządzania ciągłością biznesu. Na powyższe ankiety odpowiedziało 1257 respondentów i stanowiło to próbę badawczą dla autorów. Jak wskazują autorzy, gdy w roku 2002 największe zagrożenie dla kontynuowania działalności biznesowej stanowiły krytyczna opinia w mediach (33%), utrata kluczowych umiejętności pracowniczych (24%) i zagrożenia wynikające z infrastruktury IT (18%), to w 2007 roku menedżerowie jako główne zagrożenia identyfikowali wciąż, ale ze znacznie większym wymiarem jako zagrożenia wynikające z infrastruktury IT (39%), utraty pracowników (24%) oraz wcześniej nie wspominane zagrożenia naturalne (28%). Warto na tym etapie przypomnieć czytelnikom kilka zagrożeń naturalnych i wydarzeń, które zachwiały niejednym państwem i globalną korporacją, a wiele z nich wymazały z mapy krajobrazu biznesowego:

Tabela 1.

Przykłady globalnych katastrof i wydarzeń w okresie 1989–2010, które miały wpływ na ciągłość działania wielu firm

Rok	Wydarzenie
1989	*Trzęsienie ziemi w San Francisco* — 57 ofiar śmiertelnych, prawie 4000 rannych i straty oczasowane na 6 miliardów USD
1992	*Huragan Andrew w Ameryce Środkowej* — 26 ofiar śmiertelnych i straty oczasowane na 26,5 miliardów USD
1993	*Powódź w USA* — 50 ofiar śmiertelnych, 55 tys. osób straciło domy, straty oszacowane na 15 miliardów USD
1995	*Atak terrorystyczny w metrze w Tokio* — 12 osób zginęło, a ponad 1000 zostało zainfekowanych po rozpyleniu sarin.
1995	*Trzęsienie ziemi w prowincji Kobe w Japonii* — 5500 zginęło, straty oszacowano na ponad 200 miliardów USD.
1999	*Strzelanina w szkole w stanie Columbia w USA* — nastolatek zastrzelił 13 osób i ranił ciężko 27.
2001	*Zamach terrorystyczny na WTC* — prawie 3000 osób zginęło w ataku terrorystycznym; bardzo często były to całe firmy ulokowane w budynkach WTC.
2001	*Ustawa Sarbanes-Oxley* — po aferach Enronnu i Tyco powstała nowa ustawa o zobowiązaniach spółek publicznych.
2004	*Tsunami w Azji* — trzęsienie ziemi nad oceanem indyjskim pozbawiło życia prawie 200 tys. osób, a 1,2 mln zostało wysiedlonych z zagrożonych terenów. Straty oszacowano na 10 miliardów USD.
2004	*Huragan Harley i Frances* — huragan na Florydzie zabił 65 osób, a straty oszacowano na prawie 22 miliardy USD.
2004	*Atak terrorystyczny w Madrycie* — w 13 eksplozjach zginęło 191 osób, a ponad 1000 zostało rannych.
2005	*Atak terrorystyczny w Londynie* — w eksplozjach zginęło 52 osób, a ponad 700 zostało rannych

Rok	Wydarzenie
2005	*Huragan Karina, Rita i Whilma* — huragan na Florydzie zabił 2280 osób a straty oszacowano na prawie 128 miliardy USD
2010	*Trzęsienie ziemi w Chile* — ponad 700 ofiar śmiertelnych i straty na poziomie 30 miliardów USD,
2010	*Trzęsienie ziemi na Haiti* — ponad 233 tys. ofiar śmiertelnych i straty przekraczające 8 mld USD,
2010	*Powódź w Polsce* — zginęło 12 osób, a straty szacuje się na 3 miliardy USD.
2010	*Katastrofa lotnicza samolotu prezydenckiego* — zginęło 96 osób, w tym para prezydencka, a także m.in. generałowie Armii Polskiej, wicemarszałkowie Sejmu i Senatu oraz prezes NBP.
2010	*Wybuch islandzkiego wulkanu Eyjafjallajökull* — kilkunastodniowy paraliż lotnisk w całej Europie.
2011	*Trzęsienie ziemi w Japonii*, które pochłonęło 28 tys. ofiar, a skutki są trudne do oszacowania, ale mówi się o ponad 300 miliardach USD.

Źródło: opracowanie własne.

Należy zwrócić uwagę, że większość z prezentowanych tragedii miała swój pozytywny skutek w postaci zmiany podejścia rządu, budowy nowych zabezpieczeń czy tworzenia struktur ochrony państwa. Przykładowo podaję tutaj całkowitą zmianę polityki Japonii po trzęsieniu ziemi z 2005 roku, która zaowocowała stworzeniem nowych technologii budowy autostrad „odpornych" na trzęsienia ziemi, zmianą podejścia do budowy budynków mieszkalnych, a także stworzeniem nowego planu prewencji i zapewnienia ciągłości działania kraju kwitnącej wiśni. Podobnie zawrzało w Stanach Zjednoczonych po tragicznej strzelaninie w 1999 roku. Zaowocowało to zaostrzonymi przepisami bezpieczeństwa na terenie szkół, a także ograniczeniem dostępu do broni dla osób niepełnoletnich. Przykładem całkowitej zmiany polityki państwa do zapewnienia bezpieczeństwa narodowego i ciągłości działania państwa są wydarzenia z 9 września 2001 roku. W 2002 roku stworzono i wcielono w życie *Ustawę o bezpieczeństwie narodowym*, a konsekwencją tej ustawy było stworzenie Departamentu Bezpieczeństwa Narodowego — największej od 50 lat struktury rządowej, która powstała w Stanach Zjednoczonych. Bardzo pechowo wyglądał także rok 2010. Tylko od początku stycznia do końca czerwca doszło aż do 440 katastrof naturalnych. Łączne straty przekroczyły 70 miliardów USD, z czego ponad 22 miliardy USD musiały pokryć firmy ubezpieczeniowe. Niewiele mniej, bo 3,5 miliarda USD., kosztowały powodzie, które zalały Europę (w tym Polskę) na przełomie maja i czerwca. Tylko w naszym kraju straty wyniosły około 3 mld euro [http://www.wyborcza.biz].

Wśród nadchodzących zagrożeń, które mogą zagrozić kontynuacji biznesu należy wymienić wszelkiego rodzaju epidemie, choćby grypy. Niestety, jak wskazano w raporcie *Business Continuity Management*, tylko 13% organizacji posiada plany działania, które pozwalają zabezpieczyć się przed skutkami epidemii i zapewnić kontynuację działalności przedsiębiorstwa.

Pomimo tak drastycznych przykładów ponad połowa z objętych badaniem przeprowadzonym przez Chartered Management Institute menedżerów wskazała na brak jakichkolwiek planów ciągłości działania w reprezentowa-

nych przez nich organizacjach. Jednak autorzy badania widzą wyraźny spadek tej liczby z każdą wersją nowego raportu, co z pewnością może napawać dużym optymizmem.

Innym badaniem, które warto przytoczyć, jest przeprowadzone przez J. Scarborough w 2007 roku. Wskazał on w nich najważniejsze typy zagrożeń, które najbardziej niepokoją menedżerów dużych korporacji biorących udział w badaniu. Wśród nich najważniejszymi są[1]:

- utrata systemów IT (76% respondentów);
- utrata systemów telekomunikacyjnych (67% respondentów);
- szkody w infrastrukturze wywołane pożarem (52% respondentów);
- zniszczenie reputacji marki (47% respondentów);
- utrata kluczowych zasobów osobowych (42% respondentów);
- zapewnienie bezpieczeństwa i higieny pracy (39% respondentów);
- zabezpieczenie dostępu do zasobów (32% respondentów);
- zanieczyszczenie środowiska naturalnego (31% respondentów);
- szkody wywołane katastrofami naturalnymi (27% respondentów);
- bezpieczeństwo oferowanych produktów (16% respondentów);
- ataki terrorystyczne (14% respondentów).

Zgodnie z opracowaniem Chartered Management Institute wśród zagrożeń, które są uwzględniane w standardach i normach do zarządzania ciągłością znajdują się[2]:

- utrata systemów IT;
- utrata systemów telekomunikacyjnych;
- szkody w infrastrukturze wywołane pożarem;
- ataki terrorystyczne;
- szkody wywołane katastrofami naturalnymi;
- zabezpieczenie dostępu do zasobów.

Widać wyraźnie, że skala, różnorodność i częstotliwość dotykających nas zagrożeń jest coraz większa, tym samym potrzebne są szeroko zakrojone działania organizacji zarówno tych prywatnych, jak i publicznych, w celu ochrony bezpieczeństwa obywateli i pracowników z rodzinami. System zarządzania ciągłością działania pozwala na pokrycie dużej części zagrożeń, na które narażona jest organizacja, pozostałe mieszczą się już w innych działaniach z obszaru zarządzania reputacji.

Definicja i zakres ciągłości działania

Gdybyśmy chcieli zdefiniować, czym jest BCM, chyba najlepszym sposobem na udzielenie odpowiedzi byłoby pytanie: Jakie są oczekiwania biznesowe systemu ciągłości działania? W zależności od sektora gospodarki odpowiedzi te mogą się drastycznie różnić, jednak w głównej mierze będą dotyczyły mitygacji obszarów: zaburzeń w działaniu procesów biznesowych, utraty akty-

[1] Na podstawie [Scarborough, 2007].
[2] Na podstawie [*Business Continuity Management*, 2005].

wów, niezgodności z wymaganiami prawnymi, zagrożeń dla reputacji firmy, jej marki i produktów czy niezadowolenia klientów.

Obszar BCM ma być nie tylko dedykowany tworzeniu planów awaryjnych, kryzysowych czy tzw. obrony cywilnej. Ma to być jeden z obszarów zarządzania składający się na prowadzenie odpowiedzialnego biznesu. BCM obejmuje tym samym [http://www.thebci.org]:

- kształtowanie świadomości potrzeby zapewnienia ciągłości działania organizacji jako elementu kultury organizacji,
- tworzenie dedykowanych struktur organizacyjnych,
- definiowanie procesów rozpoznawania i zapobiegania zagrożeniom,
- projektowanie procesów przywracania stanu sprzed wystąpienia zakłócenia, jeśli jednak do tego doszło,
- obudowywanie tych procesów procedurami i rozwiązaniami organizacyjno-technicznymi,
- doskonalenie rozwiązań poprzez testy, ćwiczenia oraz analizowanie powstałych incydentów.

W literaturze ekonomicznej znajdujemy wiele fachowych definicji odnośnie „ciągłości biznesu". Jak wskazują A. Gospodarowicz, K. Jajuga [2008, s. 8]:

Ciągłość działania, po pierwsze

jest postulatem doskonałości systemu działania, jakim jest każda organizacja, a więc i każdy podmiot gospodarczy czy administracyjny. W tym sensie zapewnienie ciągłości działania jest przedmiotem zarządzania strategicznego, wyrażając cel nadrzędny sprawności organizacji i obejmując prymat w obszarze zarządzania ryzykiem operacyjnym.

Po drugie, ciągłość działania

jest rozumiana jako postępowanie organizatorskie tworzące zdolność organizacji do skutecznego reagowania w sytuacji zaistnienia zakłócenia jako wyniku swoistej interakcji przejawów zagrożenia z podatnością organizacji wewnętrznej, infrastruktury lub zasobów. W tym sensie zapewnienie ciągłości działania jest przedmiotem zarządzania operacyjnego i stanowi ostatnie ogniwo zarządzania ryzykiem operacyjnym.

Ogólnie ciągłość działania

to zdolność organizacji do takiego reagowania na zakłócenia warunków normalnej działalności, aby tam, gdzie to możliwe, szybko przywrócić te normalne warunki, a tam, gdzie to niemożliwe, przejść do zaplanowanego sposobu zastępczego wykonywania zadań. Ciągłość działania postrzega się więc zarówno w kontekście zadań organizacji oraz procesów służących realizacji tych zadań, jak i w kontekście czynników mogący zakłócić te procesy, oraz podatności organizacji, stanowiących o jej wrażliwości na zakłócenia.

Zarządzanie ciągłością biznesu opiera się na założeniu, że podstawową odpowiedzialnością władz (zarówno rady nadzorczej i zarządu) jest zapewnienie kontynuacji działalności biznesowej i operacyjnej firmy w całym jej cyklu życia. Zatem może zostać zdefiniowana jako [Woodman, 2007, s. 6]:

Holistyczne zarządzanie procesowe, którego celem jest identyfikacja potencjalnych zagrożeń dla organizacji i jej działalności operacyjnej, gdy nastąpią. Zarządzanie ciągłością biznesu stanowi zatem ramy, w oparciu o które buduje się odporność organizacji wraz z zdolnością do efektywnego reagowania, które zabezpieczy interesy głównych interesariuszy organizacji, jej reputację, ochronę marki i działań budujących wartość dodana dla organizacji.

Zagrożenia na które są narażone organizacje mogą pochodzić z jej wnętrza (np. zaburzenia działania systemów informatycznych), a także z zewnątrz (np. ataki terrorystyczne czy katastrofy naturalne). Jak wskazują badania Gardnera z 2002 roku tylko 25 z 200 globalnych instytucji zainwestowało w budowę systemu BCM [http://www.gardner.com]. Wydać jednak pozytywne sygnały płynące ze świata, które mogą zmienić ten stan rzeczy.

W Wielkiej Brytanii od 2004 roku, kiedy wprowadzono *The Civil Contingencies Act*, wszystkie władze lokalne są zobowiązane do promowania praktyk Zarządzania Ciągłością Biznesu, a także wskazywania zagrożeń, na jakie narażone są firmy, zarówno tych wewnętrznych, jak i zewnętrznych.

Podobny poziom dojrzałości możemy zaobserwować w Stanach Zjednoczonych. Szczególne znaczenie dla rozwoju BCM był atak na Word Trade Center w 2001 w Stanach Zjednoczonych. Spowodował on powstanie wielu ustaw związanych z bezpieczeństwem narodowym. Wskazano w nich, że prawie 80% krytycznej z punktu widzenia bezpieczeństwa narodowego infrastruktury znajduje się w rękach prywatnych, tym samym należy wspierać rozwój działań w obszarze BCM poza administracją publiczną i uświadomić sektor prywatny, jak ważną rolę odgrywa w procesie budowania narodowej strategii BCM[3]. W celu wspierania tych inicjatyw oraz stworzenia zunifikowanego podejścia do problemu BCM powołano do życia American National Standards Institute (ANSI), który w 2004 roku po szeroko zakrojonych konsultacjach branżowych i społecznych opublikował *NEPA 1600 Standard on Disaster/Emergency Management and Business Continuity Programs*. Od tego czasu niewiele się zmieniło, choć ostatnie katastrofy naturalne z przełomu 2010/2011 mogą tą tendencję odwrócić.

Zarządzanie ciągłością działania jest praktyczną dyscypliną naukową, która swoje początki miała trzydzieści lat temu, a bardzo mocno ewoluowała w okresie ostatnich dwudziestu latach. W początkowym okresie zajmowała

[3] Ustawy, które poruszają te zagadnienia to: *Ustawa o narodowym zarządzaniu incydentami* oraz *Ustawa o narodowych planach naprawczych*, obie wydane w 2004 roku przez Departament Bezpieczeństwa Narodowego Stanów Zjednoczonych.

się ona głównie ochroną i odtwarzaniem danych infrastruktury IT, jednakże w ostatnich dziesięciu latach traktowana jest znacznie szerzej (ze szczególnym uwzględnieniem wspierania realizacji strategii instytucji). Proces ten obejmował w szczególności stworzenie ogólnie akceptowanej terminologii, zakresu BCM, standardów i procesu certyfikacji. Po dynamicznym rozwoju przyszedł moment spadku zainteresowania ze strony odbiorców biznesowych. Wiąże się to z brakiem świadomości po stronie instytucji, czym jest BCM, jaki jest jego zakres, a także jak mierzyć korzyści z wdrażania strategii BCM. Dodatkowo niestety należy zaznaczyć, że znacząca większość organizacji nie ma w ogólne planów, infrastruktury, kompetencji ludzkich i procedur pozwalających na pełne zrozumienie i zarządzanie sytuacjami kryzysowymi.

Problem „nieokreśloności" w mniejszym stopniu dotyczy administracji publicznej, sektora finansowego i branży medycznej, dla których wdrożenie strategii BCM jest naturalnym krokiem po stworzeniu strategii jakości, bezpieczeństwa informacji i zarządzania ryzykiem.

Wiąże to współcześnie ze znaczeniem tych sektorów w gospodarce i dla społeczeństwa, a także z problemem reputacji, która dla tych sektorów gospodarki jest dźwignią do zarabiania pieniędzy, a w przypadku poważnego zaburzenia działania (np. zalanie szpitala, awaria infrastruktury elektrycznej w placówkach medycznych, awaria systemów transakcyjnych w banku, brak natychmiastowej i prawidłowej reakcji na atak terrorystyczny ze strony jednostek kryzysowych administracji publicznej) praktycznie eliminuje tzw. drugą szansę w oczach interesariuszy i skutkuje upadkiem bądź odwołaniem ze stanowisk w administracji publicznej i znaczącym spadkiem popularności partii w oczach wyborców.

Tabela 2.

Zarządzanie cyklem życia ciągłości działania

Krok 1. — Zrozumienie biznesu		
1.1.	**1.2.**	**1.3.**
Cele biznesowe i operacyjne	**Krytyczne punkty działań organizacji**	**Produkty i usługi organizacji**
Krok 2. — Strategia BCM		
2.1.	**2.2.**	**2.3.**
Struktura organizacyjna BCM	**Procesy zdefiniowane dla poszczególnych poziomów organizacji**	**Zasoby potrzebne do realizacji strategii BCM**
Krok 3. — Budowa i wdrożenie systemu BCM		
3.1.	**3.2**	**3.3.**
Plan Ciągłości Działania	**Plan i narzędzia przywrócenia działania**	**Plan Zarządzania Kryzysowego**
Krok 4. — Budowa kultury BCM organizacji		
4.1.	**4.2.**	**4.3.**

Program budowania świadomości BCM	Edukacja i działania wzmacniające świadomość	Przeprowadzanie szkoleń
Krok 5 — Utrzymanie i audytowanie systemu BCM		
5.1.	5.2.	5.3.
Utrzymanie systemu BCM	Audyt systemu BCM	Rozwój BCM

Źródło: opracowanie własne na podstawie *Business Continuity Management: Good Practice Guidelines*, Business Continuity Institute, 2002, s. 84.

Amerykańskie organizacje Disaster Research Institute International (DRII 2004), ASIS International (ASIS 2004), oraz Association of Contingency Planners (ACP 2004) definiują ciągłości działania jako „parasol" aktywności i procesów wspierających proces mitygacji oraz działań w obliczu zaburzeń w działalności biznesowej instytucji, w tym także zarządzania kryzysowego. Z kolei Business Continuity Institute[4] wskazuje, że Zarządzanie Ciągłością Działania jest programem, w którego ramach realizuje się szereg inicjatyw i działań związanych ze strategicznym planowaniem zabezpieczenia organizacji, zarządzania ryzykiem, planami ciągłości działania, zarządzania kryzysowego czy tworzeniem planów ratunkowych. Tabela 2. przedstawia najważniejsze etapy zarządzania cyklem życia ciągłości działania w organizacjach bez podziału na branże.

W ramach pierwszego etapu poprzez wykorzystanie narzędzi do identyfikacji i oceny ryzyk definiuje się zmienne krytyczne z punktu widzenia zaburzenia kontynuacji działalności biznesowej organizacji (zarówno wewnętrzne jak i zewnętrzne), ocenia priorytety w zakresie przywracania głównych procesów biznesowych, a także wskazuje poziom ryzyka (prawdopodobieństwo wystąpienia) dla poszczególnych zmiennych wskazanych powyżej.

Drugi etap to wybór alternatywnych strategii pozwalających na maksymalne ograniczanie strat w przypadku wystąpienia wskazanych w etapie pierwszym zmiennych, ich ocena z punktu widzenia wartości dla środowiska, w którym funkcjonuje organizacja, oraz utrzymania ciągłości krytycznych funkcji, które spełnia organizacja.

Kolejny etap obejmuje działania zmierzające budowy planów ciągłości działania i do włączenia ich w obowiązujące w organizacji procedury, kodeksy i procesy zarządzania jakością i ryzykiem. Dodatkowo określa się narzędzia prewencyjne, które mają wspierać odporność organizacji na wystąpienie działań zaburzających ciągłość działania, np. program ubezpieczeń.

Czwarty etap polega na budowaniu świadomości organizacji na temat znaczenia BCM. Proces ten powinien rozpocząć się od zaangażowania i deklaracji najwyższego kierownictwa oraz właścicieli. W następnym etapie należy

[4] Instytucja, która jako pierwsza użyła i zdefiniowała zwrot BCM.

zdefiniować grupy odbiorców wewnętrznych procesu edukacji i szkolenia, a także najważniejsze grupy interesariuszy zewnętrznych.

Ostatni etap determinujący działania kolejnego cyklu opiera się na ciągłym doskonaleniu systemu poprzez proces testowania, audyty wewnętrzne i zewnętrzne, audyty certyfikacyjne (jeśli system podlega certyfikacji niezależnej jednostki certyfikującej), zarządzanie zmianami systemu i usprawnianiu procesów BCM w organizacji.

W literaturze przedmiotu bardzo często mówi się albo o zarządzaniu kryzysowym, albo o zarządzaniu ciągłością działania, traktując te dwie aktywności jako działania wzajemnie się wykluczające. Jednakże jak wskazuje tabela 2., a także D. Smith te dwie funkcje są w pewnym sensie filarami zarządzania ciągłością działania, na których opiera się cała filozofia BCM, a tym samym jeden z elementów nie może istnieć bez drugiego [Smith, 2002].

Dlatego też wprowadza się do literatury przedmiotu terminologię *Business Continuity and Crisis Management* (BCCM) jako odpowiedź na wskazany powyżej dyskurs naukowy. Najważniejsze jest bowiem, aby działania instytucji zmierzały do podejmowania działań w zakresie przygotowania, reagowania, odtworzenia, działania w okresie przejściowym i przywrócenia ciągłości w obliczu pojawiających się sytuacji kryzysowych. Jeśli dodatkowo proces ten będzie zgodny z strategią organizacji, możemy mówić o efektywnym modelu BCM w organizacji.

Standardy ciągłości działania

Dla wielu osób próba tworzenia standardów do zarządzania ciągłością biznesu wydaje się czymś absurdalnym ze względu na nieprzewidywalność zjawisk, które mogą zaburzyć ciągłość organizacji, będąc jednocześnie podstawą ich tworzenia. Nie ma nic bardziej mylnego. Standardy, dobre praktyki, rekomendacje zapewniają profesjonalnie przygotowane, procesowo ustabilizowane, audytowalne i certyfikowane środowisko instytucji. Tym samym stają się one ramami i szkieletem struktur ciągłości działania umożliwiającymi budowę systemu dostosowanego do specyfiki branży. Standardy nie dają narzędzi do usuwania wszystkich zaistniałych negatywnych sytuacji, jakie mogą wystąpić, ale umożliwiają poszukiwanie optymalnych kosztowo rozwiązań i odpowiednich sposobów zapobiegania tym wydarzeniom.

Jak wskazałem powyżej, instytucja korzystająca ze standardów lub dobrych praktyk w zarządzaniu systemem ciągłości działania powinna uwzględnić specyfikę własnego biznesu i przyjęte zasady szacowania ryzyka. Najlepszym bowiem rozwiązaniem planowania i zarządzania ciągłością biznesu będzie kombinacja narzędzi kontroli wewnętrznej w połączeniu z outsourcingiem usług, która spełnia wymagania biznesowe, prawne, techniczne, ludzkie i operacyjne organizacji. Prawdopodobnie system ciągłości działania będzie ulegał ewolucji i zmianom w kolejnych latach jego funkcjonowania w zależności od zmienności otoczenia, w którym funkcjonuje organizacja, postępowi technicznemu oraz efektywności i zmianom operacyjnym. Poziom audytowal-

ności i certyfikacji systemu ograniczy się wówczas właśnie do oceny ram i struktur, w których ramach dany system funkcjonuje. Dodatkowo zapewni ograniczenia dla jego rozwoju w obszarach niezgodnych ze standardami — tym samy stając się w pewnym stopniu samoregulującym się systemem.

Z drugiej strony bardzo ważne jest, aby proces wyboru standardu lub dobrych praktyk uwzględniał różne aspekty działań branżowych, a w tym w szczególności [Noakes-Fry, Diamond, 2001, s. 1–3]:

- Które informacje, procesy i systemy muszą być dostępne w trybie 24× 7×365?
- Jakie są najbardziej prawdopodobne zagrożenia dla ciągłości działania w obrębie powyższych atrybutów?
- Jakie narzędzia są potrzebne do przywrócenie ciągłości działania w wymienionych powyżej zagrożeniach?
- Jakie są koszty zapewnienia pełnej dostępności w trybie 24×7×365 dla informacji, procesów i systemów?
- Jaki jest stosunek kosztów dostępności/przywrócenia dostępności w stosunku do poziomu zagrożeń i prawdopodobnej wartości straty w przypadku drastycznego wzrostu kosztów obsługi?

Niestety standardy/dobre praktyki bardzo często nie dostarczają narzędzi lub procedur działania, a ich wdrożenie oraz późniejsza certyfikacja niekoniecznie musi przynieść wymierne korzyści dla organizacji, jeśli organizacja będzie je traktowała jako kompletny system ciągłości działania. Zwracam jeszcze raz uwagę, że standardy są mapą, która pozwala określić w jaki sposób, w oparciu o jakie założenia, w jakim zakresie i przy wykorzystaniu jakich technik wdrażać, utrzymywać i rozwijać system ciągłości działania. Sama specyfika branżowa może pochodzić z rekomendacji branżowych lub udziału doświadczonych zewnętrznych konsultantów w realizacji projektu.

Kolejnym ważnym aspektem wyboru standardu i przygotowania organizacji do jego adaptacji są więc kwalifikacje zespołu wdrażającego. W przypadku nowatorskich rozwiązań, a do takich możemy z pewnością zaliczyć systemy BCM, należy rozważyć skorzystanie z pomocy zewnętrznej firmy konsultingowej lub niezależnego doradcy, który już na etapie wyboru standardu powinien być włączony w projekt wdrożeniowy. Nie zwalnia to jednak organizacji z budowy własnego zespołu wdrożeniowego, jaki w toku realizacji projektu nabędzie kompetencji pozwalających na przejęcie, utrzymanie i dalszy rozwój systemu ciągłości działania w kolejnych latach jego funkcjonowania w organizacji. Szczególnie istotna pomoc ze strony doradcy może mieć miejsce w przypadku określania, które z elementów należy utrzymywać w ramach organizacji a które outsourcować (np. poprzez ubezpieczenie danego działania, wsparcie firm IT w utrzymaniu środowisk zapasowych, umowy z firmami ochrony mienia czy firmami obsługującymi korespondencję i archiwizację danych wrażliwych).

Liczba i zakres dostępnych standardów w zakresie ciągłości działania są bardzo duże. Z jednej strony dotyczą one tylko administracji publicznej lub

obszaru finansowo-księgowego firm, natomiast z drugiej mają różną kategorię obligatoryjności. Większość z dostępnych standardów jest zaliczana do grupy dobrych praktyk, tzn. ich stosowanie jest zupełnie dobrowolne, inne to zalecenia np. branżowe, które stając się standardem w danej branży (wymajane jest ich wdrażanie w przypadku współpracy międzynarodowej itd.), pomimo że są dobrowolne, to przy pewnej skali biznesu stają się przymusowe, jeszcze inne stają się normami wymaganymi regulacjami danego kraju i ich wdrożenie jest obligatoryjne. Najczęściej właśnie tak wygląda droga tworzenia nowych regulacji prawnych: rozpoczyna się od dobrych praktyk, następnie stają się one zaleceniami, by wejść w ramy regulacji prawnych.

Poniżej przedstawiam kilka najważniejszych standardów (w przypadku chęci pogłębienia przez czytelnika tematyki standardów BCM odsyłam do książki *Ryzyko kryzysu a ciągłość działania* wydanego nakładem wydawnictwa Difin w 2009 roku)[5]:

- Standard NFPA 1600 — amerykański standard opublikowany po raz pierwszy w 1991 roku, natomiast jego ostatnia wersja obowiązuje z roku 2010 roku. Jest on pierwowzorem wszelkich standardów obejmujących swoim zasięgiem zarządzanie kryzysowe i ciągłość działania. Obejmuje swoim zakresem pięć obszarów zarządzania ciągłością działania: zapobieganie kryzysom, minimalizacja skutków, działania naprawcze i odzyskanie zasobów. W początkowych fazach był przeznaczony dla administracji publicznej i organizacji pozarządowych, w późniejszym okresie dostosowywano go także do potrzeb biznesowych zarówno dużych korporacji, jak i małych i średnich przedsiębiorstw. Punktem zwrotnym w jego upowszechnianiu była adaptacja standardu przez Departament Bezpieczeństwa Narodowego Stanów Zjednoczonych na potrzeby budowy planów ciągłości w przypadku ataków terrorystycznych.
- BS 25999 — Norma brytyjska powstała w oparciu o akt PAS 56 stworzona i wydana przez British Standard Institution. Standard obejmuje dwa dokumenty:
- BS 25999–1:2006 — *Code of Practice*, który zawiera ogólne zasady budowy i wdrożenia strategii i systemu ciągłości działania,
- BS 25999–2:2007 *Specification* będący zbiorem szczegółowych wytycznych i zaleceń a także procedury postępowania. Obejmuje on swoim zakresem pełne spektrum działań potrzebnych do planowania, wdrożenia, utrzymania, rozwoju, testowania oraz dokumentowania całego systemu.
  Standard ten jest dedykowany zarówno instytucjom prywatnym, jak i publicznym. Instytucje, które wdrożą system ciągłości działania zgodny z normą BS 25 999, będą miały szanse dokonać jego audytowania i certyfikacji w jednej z jednostek akredytowanych do przeprowadzania certyfikacji z BS 25 999. Jest on przygotowany zgodnie z obowiązującym w ISO podejściem opartym o cykl Deminga, dlatego może stać się wartościowym rozwi-

[5] Na podstawie [Kaczmarek, Ćwiek, 2009, s. 34–47].

nięciem już istniejących systemów zarządzania jakością, ochrony środowiska czy bezpieczeństwa informacji. Bardzo ciekawą propozycją dla instytucji jest narzędzie on line do przeprowadzenia samooceny w zakresie przygotowania do wdrożenia standardu BS 25 999.

- *Civil Contingencies Act 2004* — Jest brytyjską ustawą o zarządzaniu kryzysowym dającą szereg kompetencji organom militarnym i obrony narodowej w przypadku ataku terrorystycznego lub innych zagrożeń dla państwa brytyjskiego. Podstawowym celem jego stworzenia było zapobieganie zagrożeniom militarnym, następnie został rozszerzony o różnego rodzaju zagrożenia dla ludzi i środowiska naturalnego. Dodatkowo ustawa ta ma wspierać branże, które mają kluczowe znaczenia dla zapewnienia ciągłości działania kraju, takie jak telekomunikacja, transport czy finanse i bankowość.
- ISO/PAS 22399:2007 — Międzynarodowa Organizacja Normalizacyjna (ISO) opublikowała w 2007 roku pierwszą formalną normę poświęconą koncepcji BCM, która została zatwierdzona przez 50 krajów. Norma w szczególności stawia nacisk na proces przygotowawczy do zarządzania sytuacją kryzysową zarówno w instytucjach publicznych, jak i przedsiębiorstwach prywatnych. ISO zapowiada wydanie kolejnych norm opartych choćby na standardzie BS 25 999 — jak to miało miejsce w przypadku normy ISO 27 001 — bezpieczeństwo informacji, która najpierw była standardem BS. Data publikacji jest jednak przesuwana przez komitet techniczny powołany przez ISO do jej stworzenia.
- Rekomendacje i zalecenia wydane przez Business Continuity Institute — powstał w 1994 roku i obecnie skupia jedną z największych grup specjalistów zajmujących się tematyką ciągłości działania, a skupia kilka tysięcy członków pochodzących z ponad 100 krajów na świecie. Wydawany przez BCI zestaw przewodników cieszy się ogromnym zainteresowaniem wśród odbiorców. Najczęściej wydawane dokumenty są zgodne z normą BS 25 999.
- BS 22777 — British Standard Institute. *Code of Practise for ICT Continuity* — norma ta dotyczy utrzymania ciągłości działania infrastruktury informacyjnej w organizacji, kładąc jednak największy nacisk na rozwiązania IT. Publikacja standardu BS 25999. zastąpiła i rozszerzyła zakres dotyczący ciągłości działania o inne obszary biznesowe i operacyjne instytucji.

Nie są to wszystkie standardy i normy, które poruszają problem ciągłości działania. Należałoby także wspomnieć o standardach bezpieczeństwa informacji, standardach finansowych i zarządzania ryzykiem, których integralną częścią jest ciągłość działania. Jednak w przypadku tych norm ciągłość jest tylko jednym z elementów procesu, który opisują, a więc pominąłem je w niniejszej publikacji.

W realiach polskich jednymi z najważniejszych przepisów związanych z ciągłością działania są: ustawa z dnia 28 lutego 2003 roku, polskie *Prawo upadłościowe i naprawcze* oraz akt prawny z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym. Pierwsza z nich dotyczy sytuacji, w której przed-

siębiorstwo nie jest w stanie wypełniać swoich zobowiązań prawnych i finansowych, a przepisy ustawy moją za zadanie w pierwszej kolejności zapewnić kontynuację działalności w procesie naprawczym, natomiast druga określa zasady kierowania i zarządzania przez administrację publiczną sytuacjami kryzysowymi lub związanymi z bezpieczeństwem narodowym. Zagadnienia związane z ciągłością działania można też odnaleźć w ustawach związanych z prawem budowlanym i bankowym, a także kodeksem cywilnym i handlowym. Należy jednak wyraźnie zaznaczyć, że brak jest ustawy, która w sposób kompleksowy przedstawiałaby procedury działania w sytuacji zagrożenia dla ciągłości działania przedsiębiorstw, jak to ma miejsce w przypadku ustaw obowiązujących w Wielkiej Brytanii, Stanach Zjednoczonych czy Niemczech. W obliczu klęsk naturalnych, takich jak powodzie, tornada i klęski naturalne, taka potrzeba jest uzasadniona i powinna stać się przedmiotem prac komisji sejmowych. Mamy bowiem bardzo konkretne i wiarygodne wzorce zarówno ze strony wspomnianych wyżej krajów, jak i instytucji tworzących standardy, jak np. British Standard Institution.

Wdrożenie sytemu ciągłości działania

Gdybyśmy chcieli określić zakres wdrożenia systemu ciągłości działania w jednym z daniu, to należałoby wskazać, że powinien on objąć identyfikację głównych procesów operacyjnych w organizacji, przeanalizowanie konsekwencji z ich niedostępności z różnych powodów oraz przygotowanie planów zapewnienia ciągłości ich działania niezależnie od czynników wewnętrznych i zewnętrznych.

Jednakże przed rozpoczęciem wdrożenia należy rozważyć listę krytycznych zasobów potrzebnych do skutecznego wdrożenia systemu ciągłości działania. Zasoby te zostały zaprezentowane w poniższej tabeli:

Tabela 3.

Kluczowe zasoby do wdrożenia systemu ciągłości działania 6 na 2

Kluczowe zasoby	Opis
Dane	Bezpieczeństwo lokalizacji i ochrony krytycznych informacji i dokumentacji
Infrastruktura	Wyposażenie głównych stanowisk pracy
Komunikacja	Technologie IT i telekomunikacyjne wspierające procesy operacyjne
Ludzie	Kluczowy personel dostarczający odpowiedni poziom usług
Wyposażenie	Wymagania dotyczące wyposażenia z uwzględnieniem dostawców, miejsc przechowywania

Źródło. *Business Continuity Management: Good Practice Guidelines*, Business Continuity Institute, 2002, s. 87.

Widać więc, że sam proces wdrożenia jest związany z intensywnym procesem przygotowawczym określającym cel i strategię wdrożenia, krytyczne zasoby, zakres wdrożenia, oczekiwane rezultaty i harmonogram prac.

Sam proces wdrożenia systemu ciągłości działania jest zbliżony do budowy systemu zarządzania ryzykiem. Tym samym instytucje, które mają wdrożoną metodykę szacowania ryzyka, techniki postępowania z ryzykiem lub inne systemy procesowe choćby system ISO 27 0001 — Bezpieczeństwo informacji, będą miały znacznie łatwiejszą drogę do przejścia na etapie wdrożenia, a w konsekwencji będzie to kosztowało znacznie mniej i zostanie prawdopodobnie zrealizowane w krótszym czasie.

W zależności od opracowań dobrych praktyk i standardów możemy znaleźć różną liczbę kluczowych kroków, które powinny być zrealizowane na etapie wdrożenia. Należy zaznaczyć, że większość z dostępnych podejść znajdujących się w różnych rekomendacjach, dobrych praktykach czy standardach bazuje na metodzie Deminga obejmującej następujące kroki:

- zrozumienie organizacji,
- budowa strategii ciągłości działania,
- wdrożenie strategii ciągłości działania,
- utrzymanie i rozwój systemu.

W moim przekonaniu jest to jednak podejście dość ubogie i nieuwzględniające innych elementów z punktu widzenia systemu zarządzania ciągłości działania. Poniżej zaprezentuję dwa przykładowe scenariusze wdrożenia systemu ciągłości działania obejmujące swoim zakresem od sześciu do dziesięciu kroków. W moim przekonaniu przygotowanie scenariusza czerpiącego inspirację z obu prezentowanych poniżej planów może być bardzo pomocne dla organizacji rozpoczynających proces przygotowawczy do budowy systemu BCM.

Pierwsza z proponowanych metod wdrożenia obejmuje swoim zakresem trzy główne procesy: przygotowawczy (kroki od 1. do 3.), realizacji (kroki 4. i 5.) oraz utrzymania i rozwoju (krok 6.), co pokazuje sześć głównych kroków milowych wdrożenia systemu ciągłości działania[6]:

- Krok 1. — proces inicjacji projektu — obejmuje swoim zakresem rozpoznanie potrzeby w organizacji budowy systemu, znalezienia sponsora projektu, zaangażowanie kierownictwa najwyższego szczebla, aby nadać rangę projektowi, sformułowanie i akceptacja oddelegowania zespołu projektowego, stworzenie struktur nadzorczych nad projektem, zatwierdzenie budżetu projektu oraz uzyskanie akceptacji dla planów projektowych.
- Krok 2. — zdefiniowanie wymagań i stworzenie strategii — obejmuje stworzenie tzw. fundamentów projektowych poprzez sformułowanie krótko- i długoterminowych celów projektu oraz efektów końcowego oddziaływania na organizację. Kluczowym elementem tego kroku jest określenie głównych zagrożeń, na które jest narażona instytucja, szacunkowych strat, jakie mogą wywołać, sposobów radzenia sobie z nimi oraz wymagań dla przywrócenia lub zapewnienia ciągłości działania instytucji.
- Krok 3. — ocena ryzyka — w zależności od poziomu dojrzałości instytucji w zakresie szacowania ryzyka powinna objąć albo przegląd obecnie wystę-

[6] Opracowanie własne na podstawie [Thomas, 2009, s. 3–7].

pujących systemów i ich dostosowanie do strategii ciągłości działania, albo przygotowanie nowych narzędzi szacowania ryzyka w oparciu o trzy podkroki:
  — identyfikacja krytycznych dla ciągłości działania organizacji procesów i operacji;
  — analiza wpływu na zyski instytucji, gdy te krytyczne procesy i operacje nie są dostępne wraz z określeniem prawdopodobieństwa ich wystąpienia.
  — stworzenie narzędzi/procedur/rozwiązań do zarządzania tymi krytycznymi procesami i operacjami z uwzględnieniem podejścia akceptacji ryzyka, jego unikania czy też transferu.
- Krok 4. — przygotowanie planów ciągłości działania — w oparciu o proces przygotowawczy w etapie tym należy przygotować plany ciągłości działania obejmujące proces reagowania instytucji w przypadku wystąpienia zdefiniowanych w kroku 3. zagrożeń. Plany ciągłości działania powinny określać. od kiedy zaczynają obowiązywać, jakie są role poszczególnych stanowisk w strukturze organizacyjnej co do poszczególnych zagrożeń dla zarządzania ciągłością działania, jakie są procedury komunikacyjne w przypadku materializacji zagrożeń, a także procedury postępowania w przypadku zagrożenia odnoście bezpieczeństwa IT, osób, infrastruktury, komunikacji i zewnętrznej komunikacji.
- Krok 5. — wdrożenie planów ciągłości działania — po procesie ustanowienia, identyfikacji kluczowych zagrożeń, opracowaniu planów ciągłości działania następuje proces operacyjnego ich wdrożenia w instytucji. Krok ten obejmuje swoim zakresem typowe podkroki związane z zarządzaniem projektami, takie jak: przygotowanie planu projektu i jego akceptacji, ustanowienie metodyki zarządzania projektem ze szczególnym uwzględnieniem metod komunikacji, zarządzania zmianą i ryzykiem projektu, powołaniem zespołów roboczych oraz przeprowadzenie procesu szkoleniowego. Wynikiem końcowym tego kroku jest gotowość organizacji na przedsięwzięcie kroków zarządzania ciągłości działania w przypadku materializacji zagrożeń. Kluczowym etapem tej gotowości są testy planów ciągłości działania, które powinny określić jakie problemy i luki procesowe zaobserwowano w przypadku testowania sytuacji zagrożeń oraz jakie były mierzalne efekty działań naprawczych. Wynikiem tego podkroku powinna być dokumentacja wskazująca na luki w systemie i rekomendacje działań poprawiających system ciągłości działania.
- Krok 6. — ciągły monitoring i rozwój systemu — celem tego kroku jest zapewnienie zgodności rozwoju systemu ciągłości działania z kierunkami rozwoju działalności biznesowej organizacji. Tym samym należy z odpowiednią częstotliwością (przynajmniej raz na pół roku) dokonywać audytu obecnego systemu (wewnętrznego oraz audytu trzeciej strony), cały czas podnosić świadomość wśród pracowników poprzez działalność grup roboczych, edukację i program szkoleniowy oraz efektywnie zarządzać zmianą

systemu. Audyty te stają się szczególnie istotne w przypadku strategicznych z punktu widzenia organizacji wydarzeń, np. przejęcia innej firmy, budowy nowej fabryki, wdrożenia nowej linii produkcyjnej.

Kolejną propozycją wdrożenia systemu ciągłości działania, którą chciałbym przedstawić, jest strategia 10 kroków zaproponowana przez Departament Handlu i Przemysłu Stanów Zjednoczonych w 2006 roku. Obejmuje ona następujące kroki[7]:

- Krok 1. — inicjacja projektu — powołanie kierownika projektu odpowiedzialnego za wdrożenie systemu ciągłości działania, pozyskanie wsparcia i akceptacji projektu ze strony kierownictwa wyższego szczebla i ustanowienie struktur projektowych.
- Krok 2. — ewaluacja ryzyka oraz kontrola — ocena ryzyka i stworzenie procedur jego mitygacji.
- Krok 3. — analiza oddziaływania biznesowego — identyfikacja głównych procesów biznesowych i oszacowanie kosztów wynikających z ich przerwania lub niedostępności. Krok ten zawiera także stworzenie mapy powiązań pomiędzy poszczególnymi krytycznymi procesami oraz możliwości wystąpienia kaskadowego przerwania ciągłości działalności biznesowej.
- Krok 4. — stworzenie strategii ciągłości działania — uwzględnia redukcję ryzyka oraz przywrócenia kluczowych procesów biznesowych. Określenie różnych scenariuszy przywrócenia ciągłości oraz zdefiniowanie ram czasowych.
- Krok 5. — plan reakcji w przypadku sytuacji kryzysowych — ustalenie procesów zarządzania kryzysowego oraz określenie odpowiedzialności w ramach organizacji.
- Krok 6. — stworzenie i wdrożenie planów ciągłości działania — wskazanie właścicieli poszczególnych procesów zapewnienia ciągłości działania oraz synchronizacja BCM z planami strategicznymi organizacji.
- Krok 7. — podnoszenie świadomości i proces szkoleniowy — przeprowadzenie procesu uświadamiania załogi z zakresu BCM, inicjacja działań powinna być przeprowadzona przez kierownictwo najwyższego szczebla, aby proces uświadamiania przebiegał płynnie, przeszkolenie kadr odpowiedzialnych za przywrócenie ciągłości działania oraz zarządzanie kryzysowe.
- Krok 8. — utrzymywanie i testowanie planów ciągłości działania — okresowa kontrola i testowanie systemu zarządzania ciągłością działania, uwzględnianie zmian biznesowych organizacji w systemie BCM oraz ich ciągły monitoring.
- Krok 9. — relacje z otoczeniem i zarządzanie kryzysowe — ciągły proces komunikacji zewnętrznej i wewnętrznej mający na celu informowanie

[7] Opracowanie własne na podstawie [*Information Security: Understanding business continuity management*, 2006].

najważniejszych interesariuszy organizacji o najważniejszych działaniach i zmianach w systemie ciągłości działania.
- Krok 10. — współpraca z regulatorami — informowanie lokalnych regulatorów i organizacji nadzoru o wdrażanych planach ciągłości działania, aby zapewnić pełną ich synchronizację z procesem zarządzania antykryzysowego władz lokalnych oraz w celu zapewnienia zgodności z przepisami legislacyjnymi.

Prezentowany model wdrożenia systemu ciągłości działania jest bardzo podobny do przedstawionego przeze mnie powyżej. Jedną ze znaczących różnic, na którą należy zwrócić uwagę, jest uwzględnienie procesu komunikacji wewnętrznej i zewnętrznej, a także współpracy z lokalnymi organami administracji publicznej przy wdrażaniu i rozwoju systemu ciągłości działania. Powyższe działanie może być zrealizowane przy wysokiej kulturze organizacyjnej instytucji, w której w ramach strategii biznesowej znajdują się elementy związane z *Corporate Governance*, społeczną odpowiedzialnością biznesu i zarządzaniem reputacją. Rekomenduję uwzględnienie kroku 9. i 10. jako tych najważniejszych w procesie wdrożenia systemu ciągłości działania zaprezentowanego w pierwszym przykładzie.

Skuteczne wdrożenie systemu ciągłości działania pozwala na osiąganie przez organizację wielu różnych korzyści. Do podstawowych korzyści płynących z wdrożenia systemu ciągłości działania należy zaliczyć:
- przetrwanie i szybkie przywrócenie działalności biznesowej w sytuacji wystąpienia zjawisk kryzysowych,
- procesowe działanie w sytuacjach kryzysowych i zagrażających ciągłości działania zmniejszające czas reakcji na zagrożenie i większą kontrolę działań,
- spełnianie wymagań nadzorców, regulacji prawnych, organizacji klienckich i partnerów handlowych w zakresie bezpieczeństwa i ochrony ich interesów,
- współpraca z interesariuszami przy budowie i wdrożeniu systemu ciągłości działania wzmacniająca relacje handlowe i długotrwałe bezpieczeństwo współpracy,
- wzrost wskaźnika retencji partnerów handlowych, klientów i dostawców,
- podniesienie poziomu bezpieczeństwa organizacji w oczach otoczenia i interesariuszy (wzrost reputacji instytucji),
- niższe koszty ubezpieczeń w obliczu istnienia procesów i planów ciągłości działania,
- niższe koszty operacyjne zapewnienia kontynuacji działalności w obliczu wystąpienia zjawisk kryzysowych,
- efektywną alokację zasobów osobowych i operacyjnych.

Jednym z trudniejszych wyborów i dylematów, przed którymi stawiana jest organizacja przed wdrożeniem systemu ciągłości działania, jest jego związek z systemem zarządzania ryzykiem. Dzieje się tak dlatego, że obie dyscypliny traktowane są jako zupełnie oddzielne i niezależne. A przecież w obu przy-

padkach mamy do czynienia z określeniem ryzykownych z punktu widzenia zarządzania ryzykiem i ciągłością działania aktywów, procesów i operacji, szacowaniem ryzyka dla instytucji i prawdopodobieństwa ich wystąpienia oraz określenia wpływu na działania biznesowe.

Jedynym z powodów może być nieuwzględnianie w systemach zarządzania ryzykiem zdarzeń, których prawdopodobieństwo wystąpienia jest bardzo małe (natomiast konsekwencje materializacji olbrzymie), i zarządzanie tylko incydentami, których prawdopodobieństwo jest wysokie równie jak możliwości jego minimalizacji. Zdarzenia te są natomiast bardzo często przedmiotem analizy w przypadku budowy systemu ciągłości działania. Więc w gruncie rzeczy oba procesy, choć takie same, umożliwiają zarządzanie innymi zdarzeniami. Czy zatem da się je połączyć w wspólny system zarządzania ryzykiem i ciągłością działania? Z punktu widzenia kosztów wdrożenia, szkolenia, utrzymywania systemu i kadr odpowiedzialnych za jego rozwój może to być aspekt godny rozważenia przez najwyższe kierownictwo. To pytanie może nabrać szczególnej istotności w obliczu kryzysu gospodarczego, który — jak wskazuje wielu ekonomistów — wciąż nam zagraża. Wraz z nim wdrażane są plany redukcji kosztów i podnoszenia efektywności biznesowej, a tutaj taki pomysł świetnie by się wpasowywał. Dodatkową korzyścią, którą z całą pewnością uzyskałaby organizacja po budowie zintegrowanego systemu zarządzania ryzykiem i ciągłością działania, jest oszczędność czasu kluczowych zasobów osobowych instytucji, lepsza, bo zunifikowana i ujednolicona kontrola procesów, a także lepszy i dokładniejszy proces raportowania i analizy ryzyka.

Należy wyraźnie zaznaczyć, że proces ten już został rozpoczęty w krajach o wysokiej kulturze zarządzania ryzykiem i ciągłością działania. Najnowsze wymagania w zakresie *Corporate Governance* w Wielkiej Brytanii i Stanach Zjednoczonych narzucają wręcz na instytucję potrzebę synchronizacji i ujednolicenia analiz ryzyka i ciągłości działania, a postępujący proces outsourcingu tylko przyśpieszy ten trend. Proces ten znacznie przyśpieszył w obliczu kryzysu kredytowego 2007–2008, który pokazał nieudolność wielu systemów klasy ERM.

Wymagał on będzie integracji systemów w czterech głównych obszarach[8]:

- Strategia — określenie głównych mierników KPI, celów finansowych oraz innych aspektów strategii biznesowej instytucji, które mierzą apetyt na ryzyko organizacji oraz wzmacniają ustalenie priorytetów strategicznych dla instytucji.
- Analiza porównawcza strategii — identyfikacja i określenie zależności i rozbieżności w strategii biznesowej dla zarządzania ryzykiem i ciągłości działania, kierunków rozwoju systemów, rewizja istniejących procesów i zależności w ich ramach.

[8] W oparciu o podejście proponowane przez firmę Marsh Risk Consulting (http://www.marshriskconsulting.com).

- Budowa strategii dla danych obszarów działania — koncentracja na kluczowych obszarach biznesowych oraz budowa spójnej strategii zarządzania ryzykiem i ciągłością działania.
- Planowanie wdrożenia — rozszerzenie planów ciągłości działania o zagadnienia związane z zarządzaniem ryzykiem.

Należy pamiętać, że proces integracji systemów nie zajmuje tygodnia ani miesiąca, a proces dochodzenia do jego pełnej synchronizacji może trwać kilkanaście miesięcy. W ramach procesu nie należy zapominać o wdrożonych w firmie standardach i kontroli modyfikowanej strategii z jego wymaganiami. Kolejnym elementem, o którym nie można zapomnieć, są przepisy prawne, branżowe, którym podlega organizacja.

Zakończenie

Skutecznie funkcjonujący w instytucji system ciągłości działania pozwala zarządzać zdarzeniami i incydentami, które pomijane są w analizie i zarządzaniu ryzykiem. Prawdopodobieństwo ich wystąpienia jest znacznie niższe, ale konsekwencje mogą zrujnować wieloletni wysiłek organizacji. Czy zatem instytucja może wystawiać się aż na takie ryzyko? Nie powinna, ale niestety tak się obecnie dzieje w większości z firm i organizacji publicznych. A przecież system ciągłości działania to nie tylko niższe koszty operacyjne w długiej perspektywie, bezpieczeństwo i gwarancja wysokiej jakości współpracy z interesariuszami, ale także reputacja i wysoka odpowiedzialność społeczna, której nie można kupić. System ciągłości działania nie zajmuje się szczegółową analizą ryzyk w organizacji, ale z poziomu strategicznego pozwala określić zdarzenia, które zaburzają kontynuację działalności, i w odpowiedni sposób ograniczyć zakres konsekwencji i czas przywrócenia istotnych funkcji operacyjnych. Jest szczególnie istotny, gdyż intuicyjne postępowanie w obliczu chaosu, na który wystawiona jest organizacja, jest praktycznie niemożliwe ze względu na wysoki poziom stresu, zagrożenia i strachu osób zarządzających. W takich właśnie momentach docenia się efektywny system ciągłości działania, racjonalizujący działania i przywracający zdrowy rozsądek.

Tworzenie ustaw poświęconych ciągłości działania w Stanach Zjednoczonych i Wielkiej Brytanii, ich implementacja w organizacjach administracji publicznej, ogólnokrajowe kampanie uświadamiające to bardzo dobry początek dla rozwoju idei BCM na świecie. Jednakże należy pamiętać, że powodzenie i skuteczność systemów BCM będzie zależała od organów inicjujących tego typu działania w instytucjach. Jeśli będzie to biznes, nabędzie on odpowiednią rangę, a odpowiedzialność będzie na najwyższym szczeblu zarządzania, natomiast jeśli będzie to inicjatywa IT, prawdopodobnie będzie to jeden z wielu systemów, którzy nigdy nie znajdzie swojego odzwierciedlenia w strategii całej organizacji.

Bibliografia

Scarborough J., 2007, *Risks during Transportation*, RPW Reports.
Business Continuity Management, 2005, Charted Management Institute.
Business Continuity Management, 2007, Chartered Management Institute.
Business Continuity Management: Good Practice Guidelines, 2002, Business Continuity Institute.
Gospodarowicz A., Jajuga K., 2008, *Ryzyko w działalności gospodarczej*, Wydawnictwo Edukacyjne PWN.
Information Security: Understanding business continuity management, 2006, Department of Trade and Industry.
Kaczmarek T., Ćwiek G., 2009, *Ryzyko kryzysu a ciągłość działania*, Difin.
Noakes-Fry K., Diamond T., 2001, *Business Continuity and Disaster Recovery Planning and Management: Perspective*, „Technology Review".
Smith D., 2002, *Business Continuity Management: Good Practices Guidelines*, The Business Continuity Institute.
Thomas E., 2009, *Business Continuity Management Strategy*, NHS.
Woodman P., 2007, *Business Continuity Management*, The Chartered Management Institute, s. 6.
Woodman P., Kumar V., 2009, *A Decade of Living Dangerously: The Business Continuity Management Report*, The Chartered Management Institute.
www.garder.com.
www.marshriskconsulting.com.
www.wyborcza.biz.

Abstract **Business continuity planning—new directions in operational management and protection of enterprises' reputation**

Today's enterprises are exposed to number of different systematic risks including natural disasters, frauds or information systems defects. These kind of risks may not only disturb company's operational activity but in extreme situations completely destroy reputation or lead to bankruptcy. Business continuity management is a process of uncertainty management, which supports restoring operational continuity and as a consequence protecting reputation. The goal of his paper is to propose BCM as an organizational tool and strategic framework within the context of reputation protection.

Key Words: Uncertainty, Business continuity planning, Business continuity management, reputation

JEL Classification: M21, H12, L14