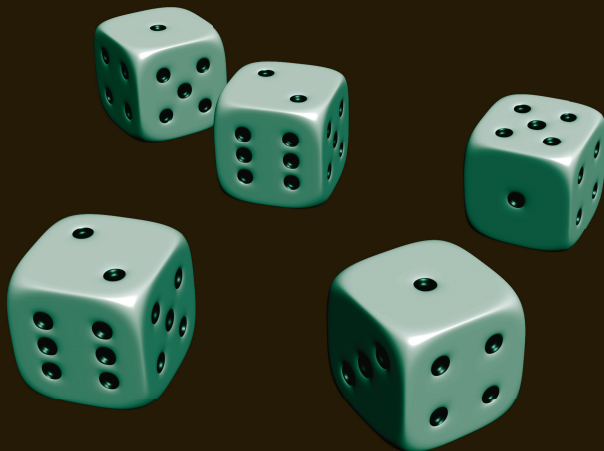




Ryzyko operacyjne w naukach o zarządzaniu

Redakcja naukowa
Iwona Staniec
Janusz Zawiła-Niedźwiecki



Wydawnictwo C.H.Beck

Ryzyko operacyjne w naukach o zarządzaniu

Wydanie zmienione książki
„Zarządzanie ryzykiem operacyjnym”

Autorzy

Marek Blim

Katarzyna Boczkowska

Grzegorz Kierner

Karol Marek Klimczak

Andrzej Marcinkowski

Maciej Owczarek

Paweł Pietras

Iwona Staniec

Maciej Szmit

Agnieszka Zakrzewska-Bielawska

Janusz Zawiła-Niedźwiecki

Ryzyko operacyjne w naukach o zarządzaniu

Redakcja naukowa
Iwona Staniec
Janusz Zawila-Niedźwiecki



Wydawnictwo C.H.Beck

Warszawa 2015

Wydawca: Dorota Ostrowska-Furmanek

Redaktor merytoryczny: Grażyna Nowak

Projekt okładki i stron tytułowych: Ireneusz Gawliński

Ilustracja na okładce: Ireneusz Gawliński

Seria: Zarządzanie

Recenzent pierwszego wydania
Zarządzania ryzykiem operacyjnym:
prof. dr hab. Michał Trocki

Wydanie zmienione książki
„Zarządzanie ryzykiem operacyjnym”



© Wydawnictwo C.H.Beck 2015

Wydawnictwo C.H.Beck Sp. z o.o.
ul. Bonifraterska 17, 00-203 Warszawa
Skład i łamanie: Ireneusz Gawliński
Druk i oprawa: Elpil, Siedlce



ISBN 978-83-255-7316-4
e-book ISBN 978-83-255-7317-1

Spis treści

Wprowadzenie	7
Rozdział 1. Panorama ryzyka (<i>Iwona Staniec, Karol M. Klimczak</i>)	11
1.1. Pochodzenie ryzyka	11
1.2. Ryzyko a bezpieczeństwo.....	13
1.3. Działania obciążone ryzykiem	17
1.4. Przegląd klasyfikacji ryzyka	22
1.5. Matematyczne obrazowanie ryzyka.....	27
1.6. Ryzyko z perspektywy biznesu	29
Pytania kontrolne	34
Rozdział 2. Ryzyko operacyjne (<i>Iwona Staniec, Karol M. Klimczak</i>)	35
2.1. Przegląd definicji i klasyfikacji	35
2.2. Istota oceny ryzyka operacyjnego	42
2.3. Organizacja zarządzania ryzykiem operacyjnym	46
2.4. Zasady zarządzania ryzykiem operacyjnym	50
2.5. Materializowanie się ryzyka operacyjnego.....	58
Pytania kontrolne	64
Rozdział 3. Ryzyko w zarządzaniu projektami (<i>Paweł Pietras</i>)	67
3.1. Charakterystyka zarządzania projektami	67
3.2. Zarządzanie ryzykiem przedsięwzięć.....	72
3.3. Studium przypadku analizy ryzyka	82
3.4. Podsumowanie.....	89
Pytania kontrolne	90
Rozdział 4. Zarządzanie w kryzysie (<i>Agnieszka Zakrzewska-Bielawska</i>)	91
4.1. Kryzys w organizacji.....	91
4.2. Uwarunkowania, przyczyny, objawy i rodzaje kryzysów	95
4.3. Restrukturyzacja jako strategia wyjścia z kryzysu.....	103
4.4. Zarządzanie organizacją w kryzysie	112
Pytania kontrolne	118
Rozdział 5. Bezpieczeństwo środowiskowe i procesowe (<i>Andrzej Marcinkowski, Maciej Owczarek</i>).....	119
5.1. Istota problemu	119
5.2. Zagrożenia	125
5.3. Zarządzanie bezpieczeństwem środowiskowym	127
5.4. Zarządzanie bezpieczeństwem procesowym	132
5.5. Regulacje prawne.....	148
Pytania kontrolne	155

Rozdział 6. Bezpieczeństwo pracy a ocena ryzyka zawodowego	
<i>(Katarzyna Boczkowska)</i>	157
6.1. Koncepcje zarządzania bezpieczeństwem pracy	158
6.2. Normalizacja systemów zarządzania bezpieczeństwem pracy	159
6.3. Kultura bezpieczeństwa, klimat bezpieczeństwa i skuteczność zarządzania bezpieczeństwem i higieną pracy	163
6.4. Ryzyko zawodowe i jego ocena	169
6.5. Metody oceny ryzyka zawodowego	176
6.6. Regulacje prawne	185
Pytania kontrolne	189
Rozdział 7. Bezpieczeństwo osobowe <i>(Grzegorz Kierner)</i>	191
7.1. Istota problemu	191
7.2. Zasady zarządzania.....	195
7.3. Projektowanie i utrzymywanie rozwiązań bezpieczeństwa	203
7.4. Regulacje prawne.....	206
Pytania kontrolne	210
Rozdział 8. Bezpieczeństwo informacji <i>(Paweł Pietras)</i>	211
8.1. Istota problemu	211
8.2. Bezpieczeństwo informacji w świetle badań	222
8.3. Pozyskiwanie informacji gospodarczych	223
8.4. Regulacje prawne.....	225
Pytania kontrolne	231
Rozdział 9. Zarządzanie ryzykiem w bezpieczeństwie informacji <i>(Maciej Szmit)</i> ...	233
9.1. Podstawowe pojęcia i definicje.....	236
9.2. Specyfika zarządzania ryzykiem bezpieczeństwa informacji	240
Pytania kontrolne	244
Rozdział 10. Bezpieczeństwo fizyczne. Ochrona obiektu i wartości <i>(Marek Blim)</i> ...	245
10.1. Istota problemu	246
10.2. Przewidywane ryzyka a organizacja i zarządzanie ochroną fizyczną.....	249
10.3. Projektowanie, uzgadnianie i utrzymywanie rozwiązań ochronnych.....	260
10.4. Funkcjonowanie ochrony fizycznej w sytuacjach kryzysowych i nadzwyczajnych	267
10.5. Regulacje prawne.....	269
10.6. Podsumowanie.....	274
Pytania kontrolne	280
Rozdział 11. Ciągłość działania <i>(Janusz Zawila-Niedźwiecki)</i>	281
11.1. Istota problemu	281
11.2. Organizacja zarządzania	285
11.3. Zasady zarządzania.....	289
11.4. Projektowanie i utrzymywanie planów ciągłości działania	293
Pytania kontrolne	306
Podsumowanie	309
Bibliografia	311
Indeks rzeczowy	325

Wprowadzenie

*„Przyszłość ma wiele imion:
Dla słabych jest: nieosiągalna
Dla bojaźliwych jest: nieznaną
Dla odważnych jest: szansą!”*
[Victor Hugo]

Przedsiębiorstwa funkcjonują w szybko zmieniającym się otoczeniu, pod wpływem silnej presji związanej przede wszystkim z koniecznością ciągłej redukcji kosztów funkcjonowania oraz zabezpieczenia się przed ewentualnymi zakłóceniami. Realizowanie tych zadań m.in. poprzez posiadanie nowoczesnej infrastruktury technicznej, podwyższanie kwalifikacji zatrudnionych pracowników, przestrzeganie norm i aktów prawnych oraz stałe konkurowanie z innymi podmiotami stało się przyczyną powstawania wielu zagrożeń funkcjonowania organizacji. Taka sytuacja wymusza na przedsiębiorcach poszukiwanie i stosowanie coraz to nowszych i efektywniejszych metod zarządzania. W związku z tym obecnie bardzo modne staje się zarządzanie ciągłością działania (*Business Continuity Management, BCM*), które ma na celu określenie potencjalnego wpływu zakłóceń na organizację, stworzenie warunków do budowania odporności na nie oraz zdolności do skutecznej reakcji w zakresie ochrony kluczowych interesów właścicieli, reputacji i marki organizacji, a także wartości osiągniętych w jej dotychczasowej działalności. Należy więc się tym zajmować, mając na celu:

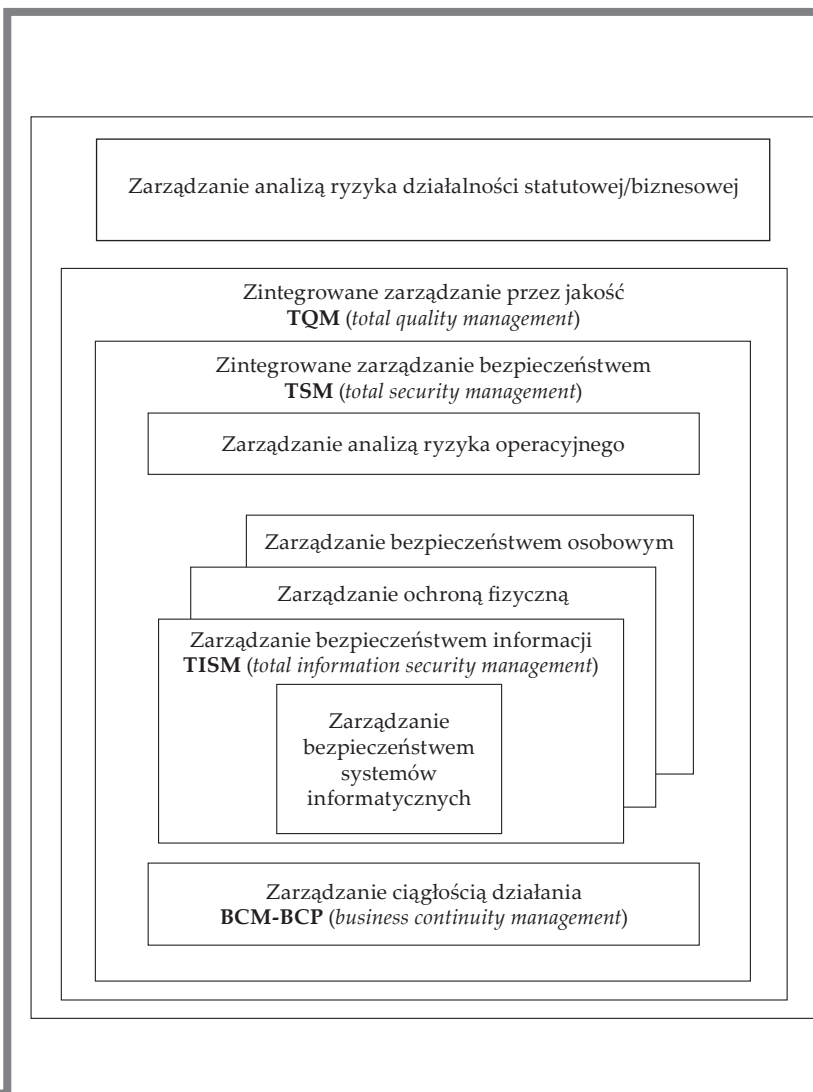
- zagwarantowanie płynności procesów biznesowych,
- zminimalizowanie zagrożenia utraty krytycznych aktywów firmy,
- minimalizację strat czasu i energii na przywrócenie prawidłowych procesów biznesowych bądź odtworzenie utraconych danych,
- zarządzanie jakością i wizerunek firmy,
- uniknięcie konsekwencji prawnych wynikających z niespełnienia obowiązujących przepisów.

Pozyskanie pełnej wiedzy o wszystkich zagrożeniach jest praktycznie niemożliwe głównie dlatego, że różnorodność zjawisk stanowiących zagrożenie osiągnięcia zamierzonych celów przez przedsiębiorstwo jest ogromna. Niebezpieczeństwa te powstają w różnych uwarunkowaniach organizacyjno-prawnych, ekonomiczno-finansowych, techniczno-technologicznych i innych. Oznacza to powstawanie nowych rodzajów ryzyka i metamorfozę już istniejących.

W teorii i praktyce (szczególnie sektora finansowego) znane i wykorzystywane są jednoznacznie określone metody kwantyfikowania ryzyka kredytowego i rynkowego. Niestety, w przypadku wdrażania procesu BCM konieczna jest identyfikacja i zarządzanie ryzykiem operacyjnym. Ryzyko operacyjne wymaga natomiast nowego podejścia ze względu na swoją wieloaspektowość oraz problemy z dostępem do danych umożliwiającymi modelowanie i analizę. W celu identyfikacji i kwantyfikacji ryzyka operacyjnego w przedsiębiorstwie konieczna jest analiza zagrożeń związanych z bezpieczeństwem procesowym i środowiskowym, pracy, fizycznym, osobowym, informacji, w tym funkcjonujących systemów IT

Rysunek 0.1.

Związki *Total Security Management* z *Total Quality Management*



(porównaj rys. 0.1). Uświadomienie i analiza zagrożeń oraz ocena ryzyka (w tym ewaluacja – oszacowanie i wycena) prowadzą do manipulowania ryzykiem, a tym właśnie jest zarządzanie bezpieczeństwem, jeżeli zaś rozwiązania bezpieczeństwa zawodzą lub są nieekonomiczne, wprowadza się rozwiązania ciągłości działania.

Celem pracy jest analiza metod identyfikowania i kwantyfikowania zagrożeń wpływających na powstanie i materializację ryzyka operacyjnego w przedsiębiorstwie oraz zarządzania nimi. W warstwie teoretycznej podjęto zatem próbę przedstawienia ryzyka operacyjnego jako nieodłącznego elementu funkcjonowania przedsiębiorstwa oraz składową poszczególnych zagrożeń. W tym celu zaprezentowano funkcjonujące pojęcia, klasyfikacje, metody kwantyfikacji oraz możliwości materializowania się ryzyka. W warstwie empirycznej zaś zostały przedstawione aspekty ryzyka operacyjnego (zagrożeń), na które narażone jest przedsiębiorstwo funkcjonujące w gospodarce rynkowej. W tym celu dokonano przeglądu organizacji z punktu widzenia stosowania poszczególnych metod identyfikacji, kwantyfikacji, organizacji i zarządzania składowymi ryzyka operacyjnego.

W opracowaniu zawarte są również rozważania dotyczące metody minimalizowania zagrożeń nieosiągnięcia zamierzonych stanów, sprowadzającej się do zarządzania ciągłością działania. W tym celu zaprezentowano planowanie, organizowanie, motywowanie i kontrolowanie jako kolejno następujące i wzajemnie zależne działania, ograniczające ryzyko operacyjne.

W książce wykorzystano metody pozwalające na opisowe prezentowanie badanego problemu, takie jak: indukcyjną, analizy i krytyki, obserwacji i analizy logicznej oraz elementy metod analizy systemowej.

Praca została podzielona na jedenaście rozdziałów. W rozdziale pierwszym przedstawiono panoramę ryzyka. Podjęto próbę zdefiniowania zależności między niepewnością a ryzykiem oraz klasyfikacji ryzyka, a także zwrócono uwagę na działania przedsiębiorstw szczególnie obciążone ryzykiem i ich postrzeganie przez biznes. W rozdziale drugim dokonano przeglądu definicji i klasyfikacji ryzyka operacyjnego, metod jego oceny, propozycji organizacji i zasad zarządzania, wraz z przykładami materializowania się ryzyka operacyjnego. Rozdział trzeci porusza problematykę ryzyka w zarządzaniu projektami. Rozdział czwarty przedstawia zjawiska kryzysowe w przedsiębiorstwach, ujawniając ich przyczyny i skutki oraz możliwe podejścia i rozwiązania. W rozdziałach: piątym, szóstym i siódmym podjęto próbę określenia zasad zarządzania, projektowania i utrzymywania rozwiązań bezpieczeństwa, odpowiednio w aspekcie działalności: procesowej, środowiskowej, stanowiskowej, osobowej. Rozdziały ósmy i dziewiąty dotyczą szeroko pojętego zarządzania bezpieczeństwem informacji, ze szczególnym uwypukleniem roli informacji i jej ochrony w organizacji gospodarczej, jak również zarządzania ryzykiem systemów informatycznych. Rozdział dziesiąty odnosi się do zasad zarządzania bezpieczeństwem fizycznym, którego elementy – występujące w każdej z omawianych działalności – w większości przedsiębiorstw są wciąż traktowane w sposób uproszczony. Ostatni rozdział jest syntezą wcześniejszych rozważań, określając warunki ciągłości działania w przedsiębiorstwie.