ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO
NR 690 FINANSE, RYNKI FINANSOWE, UBEZPIECZENIA NR 51 2012

JANUSZ ZAWIŁA-NIEDŹWIECKI

ANALIZA RYZYKA OPERACYJNEGO Z PERSPEKTYWY TEORII ORGANIZACJI

Wprowadzenie

Ryzyko operacyjne polega, poza wpływem czynników zewnętrznych, na możliwości niespełnienia oczekiwań technicznych, efektywności lub kwalifikacji, a także umyślnego popełnienia szkody. Decyduje więc ono o tym, na ile wewnętrzne procesy organizacyjne są wystarczająco skuteczne, w tym odporne na zakłócenia, aby organizacja mogła realizować swe cele gospodarcze. Nie zachodzi przy tym automatyczna synergia obszarów biznesowego i operacyjnego działalności organizacji. Można bowiem wyobrazić sobie sytuację, gdy przedsiębiorstwo, po zaprojektowaniu atrakcyjnego produktu i znalezieniu odpowiedniej kategorii odbiorców, nie jest w stanie sprostać zadaniu wytwarzania lub dostarczania tego produktu klientom w wyniku mało efektywnej organizacji produkcji, sprzedaży, czy szeroko rozumianej logistyki. Może to być problem czysto organizacyjny, ale też braku kwalifikacji personelu, niedostatku funduszy itp. (takiemu, specyficznie organizacyjnemu, spojrzeniu na ryzyko operacyjne poświęcona jest praca I. Staniec, J. Zawiła-Niedźwiecki)[1].

Reagowanie na zidentyfikowane ryzyko operacyjne może polegać na zawiązywaniu rezerw finansowych na wypadek spełnienia się przejawów tego ryzyka lub na prewencji wobec nich. Z uwagi na obszar oddziaływania tych przejawów (organizacyjny lub materialny) prewencja polega na działaniach organizacyjnych i technicznych. Taka ich specyfika wskazuje na potrzebę spojrzenia na ryzyko operacyjne także z perspektywy teorii organizacji, a nie tylko perspektywy adekwatności kapitałowej, która jest preferowana. Spojrzenie organizacyjne jest dotychczas marginalizowane, tymczasem w kontekście czynników procesowych oraz zasobowych prowadzenia działalności jest ono istotniejsze, gdyż prowadzi do zapewnienia zdolności do takiej prewencji.

Celem niniejszego opracowania jest więc pokazanie potrzeby korzystania z ujęcia i klasyfikacji odmiennej niż bazylejska, a odnoszącej się do organizacyjnej charakterystyki działania.

---

[1] *Zarządzanie ryzykiem operacyjnym*, red. I. Staniec, J. Zawiła-Niedźwiecki, C.H. Beck, Warszawa 2008.

Ryzyko operacyjne w ujęciu adekwatności kapitałowej (bazylejskim)

Kwestia ryzyka operacyjnego została w sposób szczególnie intensywny podjęta w latach 90. XX wieku przez Komitet Bazylejski[2], w ramach prac nad kompleksem dobrych praktyk zarządzania ryzykiem w bankowości[3]. Komitet poszedł i w tym przypadku śladem wcześniejszych prac nad finansowymi rodzajami ryzyka.

Komitet Bazylejski podał następującą definicję i klasyfikację ryzyka operacyjnego – „Ryzyko operacyjne to ryzyko strat w wyniku niewłaściwego lub błędnego działania procesu, ludzi i systemów lub wpływu wydarzeń zewnętrznych".

Tabela 1

Klasyfikacja rodzajów ryzyka operacyjnego wg Komitetu Bazylejskiego

Kategorie zdarzeń	Rodzaje zdarzeń
1	2
1. Oszustwo wewnętrzne Straty z tytułu działań mających na celu zamierzone oszustwo, sprzeniewierzenie własności lub obejście regulacji, prawa lub polityki spółki, z wyłączeniem zdarzeń z zakresu różnicowania i dyskryminacji, dotyczące co najmniej jednej osoby wewnętrznej	1.1. Działania nieuprawnione
	1.2. Kradzież i oszustwo
2. Oszustwo zewnętrzne Straty z tytułu działań mających na celu zamierzone oszustwo, sprzeniewierzenie własności lub obejście regulacji, prawa przez osobę trzecią	2.1. Kradzież i oszustwo
	2.2. Bezpieczeństwo systemów
3. Praktyka kadrowa i bezpieczeństwo pracy Straty wynikające z działań Banku niezgodnych z prawem pracy, przepisami BHP, porozumieniami zawartymi z pracownikami lub w konsekwencji wypłat roszczeń z tytułu odszkodowań za wypadki przy pracy oraz zdarzeń z zakresu mobingu i dyskryminacji	3.1. Stosunki pracownicze
	3.2. Bezpieczeństwo środowiska pracy
	3.3. Podziały i dyskryminacja
4. Klienci, produkty i praktyka biznesowa Straty wynikające z niezamierzonego lub będącego konsekwencją zaniedbania niewypełnienia zawodowych zobowiązań w stosunku do poszczególnych klientów (w tym wymagań dotyczących uczciwości i odpowiedzialności) albo też z charakteru lub struktury produktu	4.1. Obsługa klientów, ujawnianie informacji o klientach, zobowiązania względem klientów
	4.2. Niewłaściwe praktyki biznesowe lub rynkowe
	4.3. Wady produktów
	4.4. Klasyfikacja klienta i ekspozycje
	4.5. Usługi doradcze

[2] Basel Committee on Banking Supervision *Sound Practices for the Management and Supervision of Operational Risk*, Bank for International Settlements, Basel 2003.

[3] J. Krasodomska: *Zarządzanie ryzykiem operacyjnym w bankach*, PWE, Warszawa 2008 oraz P. Matkowski, *Zarządzanie ryzykiem operacyjnym*, Wolters Kluwer, Kraków 2006.

1	2
5. Uszkodzenia aktywów Straty wynikające z utraty bądź zniszczenia fizycznych aktywów w wyniku klęsk żywiołowych lub innych zdarzeń	Klęski żywiołowe i inne zdarzenia
6. Zakłócenie działalności i błędy systemów Straty wynikające z zakłóceń w działalności i błędów systemów	Systemy
7. Dokonywanie transakcji, dostawa oraz zarządzanie procesami Straty wynikające z błędów podczas przeprowadzania transakcji lub zarządzania procesami., jak również z relacji z kontrahentami i dostawcami	7.1. Wprowadzanie do systemu, wykonywanie, rozliczanie i obsługa transakcji
	7.2. Monitorowanie i sprawozdawczość
	7.3. Dokumentacja dotycząca klienta
	7.4. Zarządzanie rachunkami klientów
	7.5. Uczestnicy procesów niebędący klientami banku (np. izby rozliczeniowe)
	7.6. Sprzedawcy i dostawcy

Źródło: Rekomendacja M dotycząca zarządzania ryzykiem operacyjnym w bankach[4].

Zaawansowanie wprowadzania tych rekomendacji w podmiotach rynku finansowego[5] spowodowało powszechne przyjęcie podejścia bazylejskiego. Należy jednak krytycznie ocenić, że ta definicja i klasyfikacja mają wady metodologiczne i nie spełniają podstawowych wymagań klasyfikacji naukowej, tj. jasności i spójności kryteriów. Zaproponowane kategorie sprawiają wrażenie jedynie generalnego uporządkowania obszernego katalogu historycznych zdarzeń krytycznych, być może praktyczne dla celów określenia poziomu adekwatności kapitałowej, ale z pewnością nie wyczerpujące w aspekcie czynników organizacyjnych. W konsekwencji także definicja ryzyka operacyjnego ma drobne luki. Te wady ujęcia bazylejskiego mają bardzo praktyczne konsekwencje w zakresie wdrażania organizacyjnej odporności na ryzyko.

Ryzyko operacyjne w ujęciu teorii organizacji

Proponowana dalej zmodyfikowana definicja ryzyka operacyjnego uwzględnia znaczenie wybranych procesów biznesowych oraz ujmuje podatności zasobów potrzebnych do realizacji tych procesów w kontekście zagrożeń zewnętrznych i wewnętrznych. Propozycja ta, utrzymana w konwencji zbliżonej do bazylejskiej, brzmi – „Ryzyko operacyjne to ryzyko strat materialnych i reputacyjnych oraz odpowiedzialności prawnej, wynikających

[4] Por. też Dyrektywa 2006/48/EC (tzw. CRD – capital requirement directive).

[5] *Zarządzanie ryzykiem działalności organizacji*, red. J. Monkiewicz, L. Gąsiorkiewicz, C.H. Beck, Warszawa 2010, rozdz. 15.

z niedostosowania lub zawodności procesów i niezbędnych dla nich zasobów (osobowych, materialnych, informacyjnych i finansowych), a powstających w rezultacie zakłóceń będących następstwem oddziaływania zagrożeń wewnętrznych i zewnętrznych".

Wyartykułowane w zaproponowanej definicji czynniki ryzyka odpowiadają w świetle teorii organizacji następującym intencjom:

- możliwe są określone zdarzenia wewnętrzne i zewnętrzne zakłócające działanie organizacji, tzn. naruszające prowadzenie procesów,
- procesy są w określonym stopniu i zakresie podatne na zdarzenia zakłócające,
- określone zasoby są newralgiczne dla utrzymania procesów,
- organizacja może ponosić prawną odpowiedzialność za konsekwencje naruszenia procesów lub zasobów.

Trzeba też podkreślić, że same cechy zasobów mogą lec u podstaw występowania zdarzeń zakłócających. Zwłaszcza dotyczy to specyfiki zasobów ludzkich oraz skomplikowania systemów informatycznych i uzależnienia wielu procesów od tych zasobów i systemów.

Kryteria zaproponowanej w tabeli 2 klasyfikacji odnoszą się do trzech elementów przejawiania się ryzyka:

- charakteru poszczególnych procesów realizowanych w organizacji,
- rodzajów zagrożeń, które mogą oddziaływać zakłócająco na procesy,
- podatności na zagrożenia: organizacji procesów oraz poszczególnych rodzajów zasobów niezbędnych dla prowadzenia tych procesów[6].

Kwestię charakteru procesów ujęto w klasycznym podziale na procesy podstawowe, pomocnicze i zarządzania[7]. Równocześnie ogół procesów potraktowano jako reprezentację czynników wewnętrznego zorganizowania, uzupełniając je o kategorię czynników zewnętrznych związanych z oddziaływaniem otoczenia na organizację.

W tym układzie, zagrożenia – jako przejawy ryzyka – potencjalnie oddziałują na organizację jako całość (a wtedy ujmowane są jako czynniki działające z zewnątrz, tj. z otoczenia) lub na poszczególne kategorie procesów (podstawowych, pomocniczych, zarządzania). W odniesieniu do oddziaływania otoczenia na całość organizacji oraz w odniesieniu do procesów podstawowych wskazano kompleksowe rodzaje ryzyka. Natomiast w odniesieniu do procesów pomocniczych oraz do rodzajów zasobów przyjęto założenie, że procesy te polegają na udostępnianiu zasobów komórkom organizacyjnym prowadzącym procesy podstawowe. Analogicznie przyjęto, że procesy zarządzania bazują na swoistej wartości dodanej do zasobów, jaką jest zorganizowanie wewnętrzne przedsiębiorstwa, a więc na strukturze organizacyjnej i uporządkowanych relacjach między komórkami różnych szczebli.

Kwestię podatności organizacji na zagrożenia w relacji do procesów pomocniczych i zarządzania odniesiono do postulowanych cech systemu idealnego (idea ta po raz pierwszy

---

[6] J. Zawiła-Niedźwiecki: *Ciągłość działania organizacji*, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2008, s. 153.

[7] K. Szczepańska: *Zarządzanie jakością. W dążeniu do doskonałości*, C.H. Beck, Warszawa 2011.

została przedstawiona 1967 r. w pracy G. Nadlera[8]): skuteczności, efektywności, racjonalności, bezpieczeństwa oraz powtarzalności działania i jego rezultatów.

Tabela 2

Autorska propozycja klasyfikacji rodzajów ryzyka operacyjnego

			↑ **PODATNOŚCI** ↑					
			Sprawność operacyjna					
↓ **ZAGROŻENIA** ↓	**Otoczenie**		Ryzyko katastrof naturalnych					
			Ryzyko terroryzmu					
			Ryzyko zewnętrznego zakłócenia funkcjonalnego środowiska pracy					
	Procesy podstawowe		Ryzyko zakłócenia fizycznego środowiska pracy					
			Ryzyko wewnętrznego zakłócenia funkcjonalnego środowiska pracy					
			Ryzyko zakłócenia technicznego (a pozainformatycznego) środowiska pracy					
			Ryzyko zakłócenia informatycznego środowiska pracy					
	Procesy pomocnicze	Obszary materializowania się ryzyka (jako wyraz bezpieczeństwa zasobów i zorganizowania)	Postulaty organizacji idealnej (jako wyraz celu zarządzania)					
				Skuteczny	*Efektywny (optymalny organizacyjnie)*	*Racjonalny (optymalny kosztowo)*	*Bezpieczny*	*Powtarzalny*
			Zasoby osobowe	Ryzyko braku kompetencji	Ryzyko braku rezerw osobowych	Ryzyko fluktuacji kadr	Ryzyko relatywizmu interpretacji Ryzyko złej woli	Ryzyko rutyny (skostnienia)
			Zasoby materialne	Ryzyko braku funkcjonalności	Ryzyko braku rezerw materialnych		Ryzyko ubocznych skutków	Ryzyko zużywania się
			Zasoby finansowe	Ryzyko nietrafności wydatków	Ryzyko nadmiernych wydatków		Ryzyko wyczerpania środków	
			Zasoby informacyjne	Ryzyko braku pełnej treści	Ryzyko nienadążania za rozwojem		Ryzyko niedostępności	Ryzyko zniekształcenia
	Procesy zarządzania		*Zorganizowanie*	Ryzyko incydentu (awarii)	Ryzyko braku potencjału organizacyjnego		Ryzyko prymatu bezpieczeństwa nad skutecznością	Ryzyko braków

Źródło: J. Zawiła-Niedźwiecki: *Pojęcie ryzyka operacyjnego i klasyfikacja jego rodzajów*, „Przegląd Organizacji" 2010, nr 6.

[8] G. Nadler: *Work Systems Design. The ideals Concept*, Irwin, Homewood 1967.

Wskazane w tabeli 2 rodzaje ryzyka mają następujący charakter (opis podano w układzie: P – przyczyna; M – mechanizm realizowania; S – skutki; E – przykłady).

Ryzyko katastrof naturalnych: P – naturalne, przyrodnicze; M – opisany przez nauki przyrodnicze; S – od przyrodniczych (zmiany w środowisku naturalnym), przez społeczne, po dotyczące pojedynczych osób, podmiotów czy lokalizacji; E – trzęsienie ziemi, powódź, huragan, rozległy pożar, nawalne opady deszczu, gradu, śniegu.

Ryzyko terroryzmu: P – społeczne i psychologiczne; M – opisany przez nauki społeczne; S – od społecznych po dotyczące pojedynczych osób, podmiotów czy lokalizacji; E – napad, porwanie, szantaż.

Ryzyko zewnętrznego zakłócenia funkcjonalnego środowiska pracy: P – zewnętrzne wobec funkcjonowania organizacji, często nieznane organizacji; M – bez bezpośredniego związku z normalną działalnością organizacji, odcinający ją jednak od powiązań zewnętrznych; S – niedestrukcyjne ograniczenie możliwości normalnego działania; E – brak dostępu do siedziby spowodowany demonstracja uliczną.

Ryzyko zakłócenia fizycznego środowiska pracy: P – niedostatek zabezpieczeń przed czynnikami oddziaływania na środowisko pracy; M – przekroczenie granic tolerancji; S – ograniczenie możliwości normalnej pracy w odniesieniu do pracowników lub urządzeń o specjalnych wymaganiach; E – za wysoka temperatura z powodów pogodowych lub awarii technicznej.

Ryzyko wewnętrznego zakłócenia funkcjonalnego środowiska pracy: P – zaniedbania w zakresie stosunków i warunków pracy; M – zerwanie relacji wewnętrznych (między komórkami lub stanowiskami) warunkujących przebieg procesów w organizacji; S – niedestrukcyjne ograniczenie możliwości pełnej normalnej realizacji funkcji organizacji; E – strajk, wypadek pracownika.

Ryzyko zakłócenia technicznego środowiska pracy: P – zużycie lub wada ukryta; M – postępujące pogarszanie parametrów jakościowych lub nagłe ich przekroczenie; S – ograniczenie możliwości normalnej pracy; E – awaria urządzenia.

Ryzyko zakłócenia informatycznego środowiska pracy: P + M + S – analogicznie do ryzyka zakłócenia technicznego środowiska pracy, specyficzne przypadki ryzyka technicznego związane z systemami informatycznymi; E – awaria komputera.

Ryzyko braku kompetencji: P – niewłaściwy dobór pracownika do zadań lub nienadążanie pracownika za dynamiką wyzwań zawodowych; M – nieprofesjonalna ocena przesłanek działania lub podejmowania decyzji; S – błędne działania lub decyzje o skutkach prawnych, materialnych, finansowych, reputacyjnych; E – nieświadomie błędne lub pochopne działanie pracownika.

Ryzyko braku rezerw osobowych: P – niewłaściwe planowanie zadań i zasobów; M – stopniowe lub nagłe wyczerpanie potrzebnej obsady osobowej; S – niemożność pełnego wykonywania zadań; E – nieoczekiwana absencja, niemożność wykonania wszystkich zadań.

Ryzyko fluktuacji kadr: P – niewłaściwe warunki pracy, niewłaściwa ocena sytuacji na rynku pracy; M – poszukiwanie przez pracowników innego miejsca zatrudnienia; S – niemożność zapewnienia odpowiedniej jakości lub rozmiaru lub wydajności wykonywanej pracy; E – nieoczekiwana dymisja, zmiany obsady częstsze niż okres potrzebny na opanowanie zadań na stanowisku pracy.

Ryzyko relatywizmu interpretacji: P – brak jednoznacznej komunikacji lub niedostatek informacji; M – działania rozpoczynane z pozycji obiektywnie właściwych, ale prowadzone w kierunku lub w sposób nieodpowiedni; S – działania nieadekwatne do obiektywnych okoliczności; E – nieświadomie błędne lub pochopne wykonanie polecenia.

Ryzyko złej woli pracownika: P – niewłaściwy pod względem etycznym dobór pracowników do odpowiedzialnych zadań; M – wykorzystanie uprawnień stanowiska pracy lub niedostatecznej ochrony/kontroli do działań sprzecznych z interesem pracodawcy; S – straty materialne lub reputacyjne w działalności pracodawcy; E – rozmyślnie niepoprawne działanie pracownika, sprzeniewierzenie powierzonych środków.

Ryzyko rutyny (skostnienia): P – długotrwałe wykonywanie tych samych zadań lub czynności; M – stopniowe wykształcanie działania odruchowego; S – działanie odruchowe w sytuacji, która wymaga postępowania szczególnego; E – kierowca jadący „na pamięć" mimo zmiany zasad ruchu.

Ryzyko braku funkcjonalności: P – granice funkcjonalności organizacji; M – ujawnienie rzeczywistego charakteru nowego zadania, pozornie podobnego do poprzednich; S – niemożność wywiązania się z zadania; E – przyjęcie zamówienia, które na pewnym etapie realizacji nie może być kontynuowane.

Ryzyko braku rezerw materialnych: P – niewłaściwe planowanie zadań i zasobów; M – brak zasobów stwierdzony już w trakcie wykonywania zadania; S – niemożność wywiązania się z zadania; E – nieoczekiwany brak komponentów w produkcji.

Ryzyko ubocznych skutków: P – niedostateczna znajomość kontekstu zadania; M – działanie powoduje dodatkowe i niekoniecznie od razu jawne efekty o niekorzystnym charakterze; S – straty materialne lub reputacyjne i odpowiedzialność za straty stron trzecich; E – nieoczekiwany szkodliwy efekt planowej działalności.

Ryzyko zużywania się: P – ograniczona trwałość poszczególnych zasobów; M – zużywanie się zasobów prowadzące do przekroczenia granic tolerancji; S – niemożność wywiązania się z zadania; E – utrata parametrów urządzenia wytwórczego.

Ryzyko nietrafności wydatków: P – brak kompetencji lub błędna ocena przesłanek decyzji; M – nieprofesjonalna ocena przesłanek decyzyjnych; S – straty jako wynik błędnych decyzji; E – chybiona inwestycja.

Ryzyko nadmiernych wydatków: P – brak kompetencji lub błędna ocena przesłanek decyzji; M – nieprofesjonalna ocena przesłanek decyzyjnych; S – zawyżony poziom wydatków; E – błąd w negocjacjach handlowych.

Ryzyko wyczerpania środków: P – niewłaściwe planowanie zadań i zasobów finansowych; M – w toku działania zasoby finansowe są wyczerpywane bez możliwości

odpowiednio szybkiego ich uzupełnienia; S – utrata płynności; E – niemożność dokonania zakupu.

Ryzyko braku pełnej treści informacji: P – brak kompetencji lub brak dostępu do właściwych źródeł informacji; M – brak informacji w toku podjętego działania wymagającego takiej informacji; S – niemożność wywiązania się z zadania; E – niepełna dokumentacja projektowa.

Ryzyko nienadążania informacji (wiedzy) za rozwojem: P – brak kompetencji lub niedostatki w aktualizacji informacji; M – brak aktualnej informacji w toku podjętego działania wymagającego takiej informacji; S – niemożność wywiązania się z zadania lub wykonanie go w warunkach niepełnej informacji; E – projekt inwestycji na terenie, który właśnie został przeznaczony na inne cele.

Ryzyko niedostępności informacji: P – brak dostępu do właściwych źródeł informacji; M – brak informacji w toku podjętego działania wymagającego takiej informacji; S – niemożność wywiązania się z zadania lub wykonanie go w warunkach niepełnej informacji; E – niedostępność informacji od konkurentów rynkowych.

Ryzyko zniekształcenia informacji: P – brak dostatecznych kompetencji; M – błędne interpretowanie informacji; S – zła lub ograniczona jakość działania; E – prognozy ekonomiczne.

Ryzyko incydentu (awarii): P – podatności w zorganizowaniu działania lub w zasobach organizacji; M – interakcja zagrożeń dla prawidłowego działania z podatnościami; S – niemożność utrzymania dotychczasowej organizacji działania; E – awaria linii produkcyjnej.

Ryzyko braku potencjału organizacyjnego: P – brak dostatecznych kompetencji w zakresie organizacji i zarządzania; M – niewłaściwe planowanie zadań i zasobów; S – niemożność lub ograniczona zdolność do wywiązania się z zadania; E – zakłócenia w złożonym projekcie.

Ryzyko zbytniego prymatu bezpieczeństwa nad skutecznością: P – formalizm w interpretacji przepisów i standardów dobrych praktyk; M – coraz staranniejsze przestrzeganie reguł formalnych ograniczających działanie doprowadza do ograniczania, a nawet sparaliżowania tego działania; S – nieefektywne działanie; E – strajk „włoski".

Ryzyko braków: P – niewłaściwa organizacja działania (obejmująca także nieodpowiednie zasoby); M – działalność jest nieustabilizowana, nieprecyzyjnie zorganizowana, korzysta z niepewnych zasobów; S – wyniki działania nie uzyskują oczekiwanych parametrów jakościowych; E – wadliwy wyrób.

Prewencja wobec ryzyka operacyjnego

Praktyczne organizacyjne podejście do ograniczania ryzyka – tak na poziomie analizy ogólnej (zarządzanie strategiczne)[9], jak i szczegółowej (zarządzanie operacyjne)[10]– oparte na triadzie zakresu analizy (główne procesy biznesowe – krytyczne zagrożenia – kluczowe podatności) prowadzi do identyfikacji zasadniczych potencjalnych zakłóceń i opisu natury zjawiska ich powstawania, przebiegu oraz skutków. Posługiwanie się „organizacyjną" klasyfikacją rodzajów ryzyka operacyjnego pozwala na bieżąco weryfikować, czy analiza obejmuje pełne spektrum wyzwań w odniesieniu do każdego z zagadnień triady procesy – zagrożenia – podatności.

Zidentyfikowanie i opisanie potencjalnych zakłóceń służy poszukiwaniu sposobów: zapobiegania ich wystąpieniom oraz reagowania na nie. Zapobieganie zapewniają rozwiązania zabezpieczające, które powinny spełniać podstawowe 14 zasad kompleksowego zapewniania bezpieczeństwa[11]. Reagowanie zaś zapewniają plany ciągłości działania[12].

Podsumowanie

W cyklu zarządzaniu ryzykiem operacyjnym[13] istotnymi etapami są: identyfikacja ryzyka i jego analiza, dobór rozwiązań wpływających na ograniczanie ryzyka i dobór metod monitorowania ryzyka. W ramach każdego z tych etapów proponowana klasyfikacja zapewnia możliwość wyczerpującej analizy czynników ryzyka oraz doboru sposobów przeciwdziałania mu z perspektywy każdego z cząstkowych rodzajów. Prowadzi to do pełniejszej organizacyjnej prewencji wobec ryzyka. W długoterminowej perspektywie jest to biznesowo atrakcyjniejsze niż tylko zawiązywanie rezerw, co jest główną techniką podejścia bazylejskiego.

Literatura

Basel Committee on Banking Supervision, *Sound Practices for the Management and Supervision of Operational Risk*, Bank for International Settlements, Basel 2003.

Gołąb P., Zawiła-Niedźwiecki J.: *Zapewnianie ciągłości działania jako ograniczanie ryzyka operacyjnego*, [w:] *Zarządzanie ryzykiem działalności organizacji*, red. J. Monkiewicz, L. Gąsiorkiewicz, C.H. Beck, Warszawa 2010.

---

[9] *Zarządzanie ryzykiem działalności organizacji...*

[10] J. Zawiła-Niedźwiecki: *Ryzyko i bezpieczeństwo operacyjne*, [w:] *Zarządzanie ryzykiem działalności organizacji*, red. J. Monkiewicz, L. Gąsiorkiewicz, C.H. Beck, Warszawa 2010.

[11] J. Zawiła-Niedźwiecki: *Ciągłość działania organizacji...*, s. 164.

[12] P. Gołąb, J. Zawiła-Niedźwiecki: *Zapewnianie ciągłości działania jako ograniczanie ryzyka operacyjnego*, [w:] *Zarządzanie ryzykiem działalności organizacji*, red. J. Monkiewicz, L. Gąsiorkiewicz, C.H. Beck, Warszawa 2010.

[13] *Księga dobrych praktyk w zakresie zarządzania ciągłością działania*, red. R. Kaszubski, D. Romańczuk, Związek Banków Polskich, Warszawa 2011, s. 20.

Księga dobrych praktyk w zakresie zarządzania ciągłością działania, red. R. Kaszubski, D. Romańczuk, Związek Banków Polskich, Warszawa 2011.

Krasodomska J.: *Zarządzanie ryzykiem operacyjnym w bankach*, PWE, Warszawa 2008.

Matkowski P.: *Zarządzanie ryzykiem operacyjnym*, Wolters Kluwer, Kraków 2006.

Nadler G.: *Work Systems Design. The ideals Concept*, Irwin, Homewood 1967.

Rekomendacja M dotycząca zarządzania ryzykiem operacyjnym w bankach, Główny Inspektorat Nadzoru Bankowego (obecnie Komisja Nadzoru Finansowego), Warszawa 2004.

Szczepańska K.: *Zarządzanie jakością. W dążeniu do doskonałości*, C.H. Beck, Warszawa 2011.

Zawiła-Niedźwiecki J.: *Ciągłość działania organizacji*, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2008.

Zarządzanie ryzykiem działalności organizacji, red. J. Monkiewicz, L. Gąsiorkiewicz, C.H. Beck, Warszawa 2010.

Zarządzanie ryzykiem operacyjnym, red. I. Staniec, J. Zawiła-Niedźwiecki, C.H. Beck, Warszawa 2008.

Zawiła-Niedźwiecki J.: *Ryzyko i bezpieczeństwo operacyjne*, [w:] *Zarządzanie ryzykiem działalności organizacji*, red. J. Monkiewicz, L. Gąsiorkiewicz, C.H. Beck, Warszawa 2010.

Zawiła-Niedźwiecki J.: *Pojęcie ryzyka operacyjnego i klasyfikacja jego rodzajów* „Przegląd Organizacji" 2010, nr 6.

dr inż. Janusz Zawiła-Niedźwiecki
Politechnika Warszawska
Wydział Zarządzania

Streszczenie

Zarządzanie ryzykiem operacyjnym w ujęciu bazylejskim (adekwatności kapitałowej) nie gwarantuje dostatecznie kompleksowej prewencji wobec przejawów ryzyka. Pod tym względem więcej zapewnia podejście teorii organizacji i klasyfikacja ryzyka operacyjnego w tym ujęciu.

ANALYSIS OF OPERATIONAL RISK FROM THE PERSPECTIVE OF ORGANIZATION THEORY

Summary

Operational risk management in terms of Basel (capital adequacy) does not guarantee a sufficiently comprehensive risk prevention. In this respect the organization theory approach and classification of operational risk in this approach present more value.