Model oceny dojrzałości zarządzania ciągłością działania organizacji

https://doi.org/10.33141/po.2007.04.07
Przegląd Organizacji, Nr 4 (807), 2007, ss. 28-30
www.przegladorganizacji.pl
Towarzystwo Naukowe Organizacji i Kierownictwa (TNOiK)

Janusz Zawiła-Niedźwiecki

Ryzyko operacyjne

Na przestrzeni ostatniego dziesięciolecia w sferze zarządzania gospodarką oraz we wspierającej tę praktykę teorii obserwuje się radykalny wzrost zainteresowania ryzykiem. Stało się tak, bo zdecydowane trendy liberalizacji i globalizacji w gospodarce światowej doprowadziły do niespotykanego dotąd zintensyfikowania konkurencji rynkowej we wszystkich krajach rozwiniętych. Szczególną tego konsekwencją jest poszukiwanie i wdrażanie coraz bardziej wyrafinowanych rozwiązań organizacji pracy, wytwarzania oraz świadczenia usług. To z kolei naraża organizacje na specyficzny rodzaj ryzyka, bezpośrednio związanego z działaniem organizatorskim oraz dyspozycyjnością zasobów wewnętrznych. Ryzyko to nazywane jest ryzykiem operacyjnym.

Od kilku lat problem ryzyka operacyjnego jest przedmiotem badań w sektorze bankowym, prowadzonych na forum Komitetu Bazylejskiego. Zaowocowały one ustaleniem branżowych, o skali międzynarodowej, rekomendacji dobrych praktyk, przy czym wartość ustaleń Komitetu wykracza poza sektor bankowy, odnosi się do dowolnej organizacji, która potrzebuje odpowiedniej sprawności wewnętrznej, zdolnej sprostać wyzwaniom pochodzącym od zagrożeń dla skutecznej działalności. I tak, według Komitetu Bazylejskiego[1)], **ryzyko operacyjne to ryzyko strat w wyniku niewłaściwego lub błędnego działania procesu, ludzi i systemów lub wpływu wydarzeń zewnętrznych.**

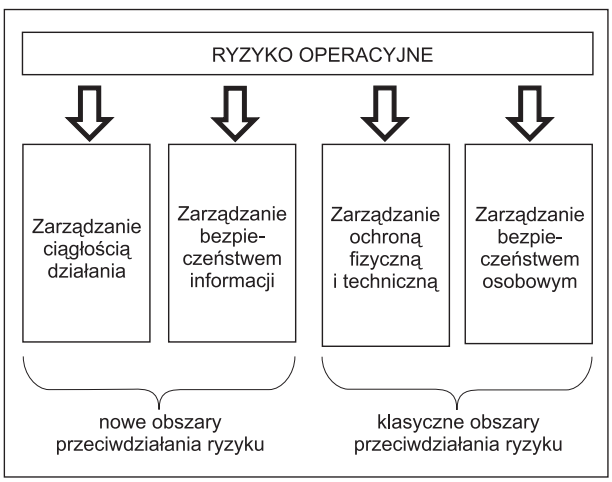
W tym ujęciu ryzyko operacyjne dzieli się na:
- ryzyko oszustwa ze strony pracowników,
- ryzyko oszustwa pochodzące z zewnątrz,
- ryzyko w zakresie zasad zatrudniania i bhp,
- ryzyko w zakresie zasad pracy z klientami, produktami i w biznesie,
- ryzyko szkód zasobów materialnych,
- ryzyko zakłócenia prowadzenia biznesu i niesprawności systemu,
- ryzyko zarządzania wykonywaniem zadań, dostawami i procesami.

W literaturze przedmiotu spotykany jest też inny podział[2)], tj. na: ryzyko oszustwa, ryzyko braku planów szeroko rozumianej odbudowy po katastrofie, ryzyko regulacyjne, ryzyko utraty reputacji, ryzyko administracyjne.

W obu przypadkach jest to charakterystyczne ujęcie przyczynowe. Bezdyskusyjna jest potrzeba takiego podejścia, ale też oczywiste jest, że wymaga ono długiego czasu na badania i następnie praktyczne wdrożenia rozwiązań kompleksowego zarządzania nim. Zanim da to efekty, pragmatyczne jest podejście poprzez skutki (por. rys. 1).

Ten sam pragmatyzm nakazuje w pierwszej kolejności podjąć problem: jak, w sposób przemyślany i zorganizowany, organizacja ma się zachować, gdy ryzyko się spełnia w formie konkretnego zakłócenia. Problem zapewniania niezawodnego działania urządzeń oraz układów technicznych jest znany od zarania dziejów techniki, a kwestia awarii technicznych, ich przyczyn i skutków jest wpisana w praktykę zachowań inżynierskich. Równocześnie widoczny jest brak analogicznie zaawansowanej teorii w odniesieniu do sprawności działania podmiotów o charakterze biznesowym i administracyjnym. Sprawność ta jest naruszana w wyniku oddziaływania czynników ryzyka operacyjnego, tj. zagrożeń, na które podatna jest organizacja, głównie w związku z: niedoskonałością przygotowania procesów wewnętrznych, niedostatkiem umiejętności kadry pracowników lub złym gospodarowaniem zasobami. Rozwiązania zabezpieczające w odniesieniu do ryzyka operacyjnego układają się w cztery obszary przeciwdziałania mu, co ilustruje rys. 1.

Jak dotąd, teoria zarządzania zajmuje się obszarami określonymi na rys. 1 jako klasyczne. Natomiast



Rys. 1. Obszary przeciwdziałania ryzyku operacyjnemu
Źródło: opracowanie własne.

dla obu nowych obszarów konieczne są badania i sformułowanie teorii zarządzania, zarówno bezpieczeństwem, jak i ciągłością działania. Ich zapowiedzią są na przykład coraz powszechniej stosowane „dobre praktyki" zarządzania zasobami i usługami informatycznymi, wynikające ze standardu ITIL[3] oraz normy brytyjskiej BS-15000.

W praktyce zarządzania ciągłością działania powstał wręcz trend, aby za przykładem zarządzania przez jakość podjąć uregulowania normatywne, co jest przedmiotem prac ISO i poszczególnych narodowych komitetów normalizacyjnych.

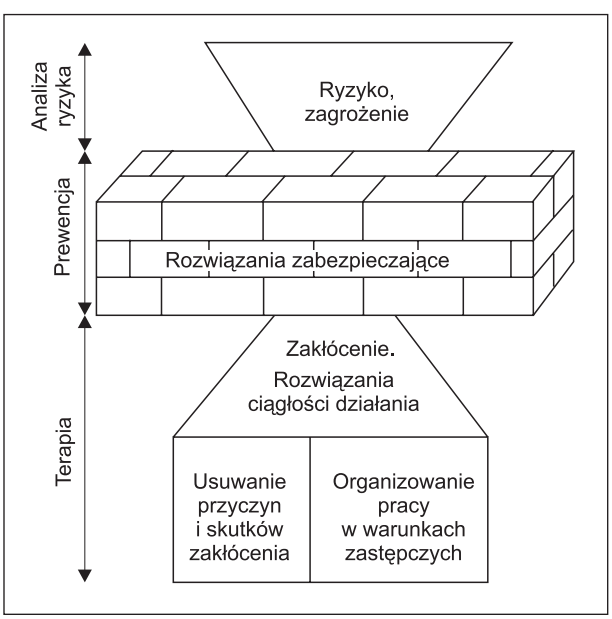
Ponadto wnikliwe spojrzenie na zapewnianie ciągłości działania prowadzi do wniosku, że jako prewencja jest nim także zarządzanie bezpieczeństwem. Co więcej, w większości sytuacji skuteczniejsze i ekonomicznie bardziej uzasadnione jest zapewnianie bezpieczeństwa, a dopiero gdy to nie jest skuteczne, stosowanie rozwiązań zapewniania ciągłości działania.

Rekomendacje dobrych praktyk

Basel II i Solvency II

Są to kompleksy rekomendacji opracowanych pod auspicjami Komitetu Bazylejskiego co do sfery zarządzania działalnością banków (Basel II) oraz przez porozumienie nadzorów ubezpieczeniowych państw członków Unii Europejskiej (CEIOPS)[4], co do sfery zarządzania działalnością zakładów ubezpieczeń. Tylko niewielkie fragmenty odnoszą się do zarządzania ryzykiem operacyjnym i w jego ramach zarządzaniem ciągłością działania.

Koncepcje Basel/Solvency formułowane są zasadniczo z myślą o specyfice banków i zakładów ubezpieczeń, ale w zakresie zarządzania ryzykiem operacyjnym mogą być z równym powodzeniem stosowane przez podmioty o dowolnym charakterze organizacyjnym i działające w bardzo różnych dziedzinach gospodarki i administracji.



Rys. 2. Relacje zadań zapewniania bezpieczeństwa i ciągłości działania
Źródło: opracowanie własne.

Normy ISO 17799 / rodzina ISO 27000

Aktualnie został rozpoczęty proces uzgadniania całej serii nowych norm, kompleksowo podających sugestie dobrych praktyk w tym zakresie. Docelowo mają to być:

- ISO 27000 – słownictwo i terminologia,
- ISO 27001 – specyfikacja systemów zarządzania bezpieczeństwem informacji,
- ISO 27002 – zbiorczy zestaw mechanizmów bezpieczeństwa, cele kontroli i najlepsze praktyki (aktualnie znana jako ISO 17799),
- ISO 27003 – wskazówki dotyczące implementacji serii ISO 27000 w organizacji,
- ISO 27004 – pomiar efektywności systemu zarządzania bezpieczeństwem,
- ISO 27005 – zarządzanie ryzykiem bezpieczeństwa.

Jak z tego wynika, zakłada się ścisłe integrowanie zagadnień zarządzania bezpieczeństwem informacji i zapewnianiem ciągłości działania.

BS 25999 (dawniej jako PAS 56)

Jest to norma brytyjska (a po doświadczeniach z inną normą brytyjską BS 7799, dotyczącą bezpieczeństwa informacji, która stała się normą ISO, a także Polską Normą, można i w tym przypadku oczekiwać podobnego biegu wydarzeń), wokół której koncentruje się obecnie uwaga środowisk z całego świata zaangażowanych w problematykę zapewniania ciągłości działania. Jest ona elementem nowoczesnej koncepcji publicznego nadzoru nad sektorami gospodarki o ważnym znaczeniu społecznym, a polegającego na kompleksowej presji na podmioty gospodarcze, wiążącej ich praktykę biznesową i organizacyjną z zasadami i wymaganiami znanymi m.in. z: MiFID, Basel II, Solvency II, *corporate governance*, w celu powszechnego wprowadzenia planowania ciągłości prowadzonego biznesu i działalności. Wśród intencji wskazuje się zwłaszcza na ochronę interesów publicznych i społecznych oraz długoterminową racjonalizację ogólnych kosztów funkcjonowania.

Dyrektywa UE 2004/39/EC (uzupełnienie przez 2006/73/EC)

Dyrektywa ta (popularnie określana MiFID – *Market in Financial Instruments Directive*) określa następujące obowiązki: „...Państwa członkowskie wymagają, aby przedsiębiorstwa inwestycyjne ustanowiły, wprowadziły i utrzymywały odpowiednią politykę utrzymywania ciągłości działalności gospodarczej, której celem jest zachowanie najważniejszych danych i funkcji oraz utrzymanie usług i działalności inwestycyjnej w razie przerwy w funkcjonowaniu systemów i procedur – a jeśli nie jest to możliwe – możliwie szybkie przywrócenie takich danych i funkcji oraz możliwie szybkie wznowienie usług i działalności inwestycyjnej".

Podejście modelowe

Aspekt jakościowy

Kojarzone przede wszystkim z normami zarządzania przez jakość serii ISO 9000, podejście jakościowe stopniowo tak zdominowało współczesną teorię zarządzania, że ostatnio uznaje się je za podstawę współczesnego paradygmatu zarządzania. Odnośnie do zarządzania ciągłością, podejście procesowe dostarcza podstawowych wskazówek co do utrzymania krytycznych procesów, racjonalizując decyzje, czy w danej sytuacji zapobiegać zakłóceniu, czy też tworzyć plany awaryjne, oraz czemu nadawać priorytet w działaniach naprawczych i zapewniania ciągłości działania.

Drugim fundamentem podejścia jakościowego jest stałe doskonalenie, przedstawiane klasycznie w formie cyklu organizatorskiego.

Aspekt organizacyjny

Sugestie dotyczące organizacji zarządzania ciągłością działania należy przede wszystkim kojarzyć z rekomendacjami zarządzania ryzykiem operacyjnym i ogólnie biznesowym. Wynika z tego, że potrzebne jest wskazanie komórki odpowiedzialnej za bieżące zarządzanie ryzykiem, a ponadto dla sytuacji krytycznych ciała (komitetu, sztabu kryzysowego), które na podstawie zawczasu zdefiniowanych planów i scenariuszy przereorganizuje firmę i pokieruje nią w tym nowym kształcie, do czasu usunięcia przyczyn i skutków zakłócenia, czyli do czasu możliwości powrotu do rutynowych warunków działania.

Wzmocnić to powinny systematyczne audyty/przeglądy. Kwestia ta jest zbieżna z drugim filarem Basel/Solvency oraz z zasadą stałego doskonalenia.

Model dojrzałości

Najbardziej znaną obecnie próbą określenia wzorca w tym zakresie jest metoda BCMM (*Business Continuity Maturity Model*)[5], opracowana przez amerykańską firmę Virtual Corporation Inc. W swej koncepcji przypomina ona opracowany przez BBA[6], ISDA, RMA [5] model oceniania dojrzałości zarządzania ryzykiem.

Skrótowo idea metody jest taka, że przedsiębiorstwo (organizacja) stopniowo osiąga coraz wyższe poziomy dojrzałości, wprowadzając trwale umocowane i systematycznie doskonalone struktury organizacyjne, role uczestniczących oraz zasady i plan działań. Poszczególne poziomy charakteryzują się następującymi cechami.

Poziom 1 – Problematyka BCP nie jest postrzegana przez najwyższe kierownictwo jako znacząca i wymagająca centralnego kierowania. Zajmują się tym poszczególne komórki organizacyjne według własnego rozeznania i w stopniu, które same uznają za słuszny.

Poziom 2 – Strategiczne znaczenie problematyki BCP jest dostrzegane przez jakąś komórkę organizacyjną. W organizacji lub wśród wspierających ją doradców jest jakiś specjalista, który może wspierać prace nad BCP. Najwyższe kierownictwo wie już, że jest to problem poważny, ale jeszcze nie nadaje mu odpowiedniego priorytetu.

Poziom 3 – Najbardziej zainteresowane problematyką komórki organizacyjne prowadzą wspólne działania nad programem BCP. Nie jest to jednak Plan BCP całej firmy. Najwyższe kierownictwo jest świadome poczynań, sprzyja im, ale jeszcze nie jest zdolne do ustanowienia struktur, zadań i Planu BCP.

Poziom 4 – Najwyższe kierownictwo jest świadome strategicznego znaczenia zarządzania BCP. Utworzono stałe biuro zarządzania problematyką BCP. Pracuje się nad zintegrowanymi rozwiązaniami, wspólnymi w całej firmie. Zidentyfikowano krytyczne procesy oraz opracowano plany ich ochrony. Są one testowane i rutynowo aktualizowane.

Poziom 5 – Wszystkie komórki organizacyjne przetestowały pozytywnie plany BCP, w tym zasady dokonywania zmian w planach. Najwyższe kierownictwo też uczestniczyło w testach. Opracowano kilkuletni program rozwoju rozwiązań BCP.

Poziom 6 – Wszystkie komórki organizacyjne uzyskały wysokie oceny przygotowania BCP. Testuje się współdziałanie komórek. Wszelkie zmiany faktyczne w procesach biznesowych oraz także potencjalne w rozwiązaniach samych planów BCP są bieżąco śledzone i uwzględniane w rozwiązaniach BCP.

Zanosi się na to, że powoli rodzi się nowa gałąź teorii zarządzania – *Business Continuity Management* (BCM).

dr inż. Janusz Zawiła-Niedźwiecki
Instytut Organizacji Systemów Produkcyjnych
Politechnika Warszawska

PRZYPISY

1) Committee on Banking Supervision (International Bank for Settlements) „Sound Practices for the Management and Supervision of Operational Risk". Por. także Główny Inspektorat Nadzoru Bankowego „Rekomendacja M".
2) R. KENDALL, *Zarządzanie ryzykiem dla menedżerów*, s. 119–142.
3) ITIL (z ang. – *Information Technology Infrastructure Library*), por. www.ogc.gov.uk
4) CEIOPS – Committee of European Insurance and Occupational Pensions Supervisors, por. www.ceiops.org
5) *The Complete Public Domain Business Continuity Maturity Model*, Virtual Corporation, New Jersey 2005, por. www.virtual-corp.net
6) BBA – British Bankers Association, ISDA – International Swaps and Derivatives Association, RMA – Risk Management Association, por. BBA, ISDA, RMA „Operational Risk: The Next Frontier", British Bankers Association, London 1999.

Summary

Problem of business, it's processes and systems continuity planning (so called BCP), becomes, faced with ever more sophisticated organizational solutions, that are result of increasing competition on the market, more and more visible challenge. In the USA new branch of management science was even established – business continuity management (BCM). In Europe, in the last couple of years in various industries ideas of standards of this sort were suggested. E.g. British Standards Institution created the norm BS 25999, which is to be introduced in whole public administration; Basel Committee proposed certain recommendations of operational risk management to ranking sector (including BCP); European Central Bank had set certain requirements of supervision of important funds transfer systems in the aspect of continuity planning; the European Parliament and The Council of the European Union passed Markets in Financial Instruments Directive.