Grzegorz Dydkowski, Barbara Kos

Zarządzanie ryzykiem podczas realizacji projektów informatycznych

Ekonomiczne Problemy Usług nr 117, 73-81

2015

ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO
NR 852 EKONOMICZNE PROBLEMY USŁUG NR 117 2015

GRZEGORZ DYDKOWSKI, BARBARA KOS
Uniwersytet Ekonomiczny w Katowicach[1]

ZARZĄDZANIE RYZYKIEM PODCZAS REALIZACJI PROJEKTÓW INFORMATYCZNYCH

Streszczenie

Prowadzenie przedsięwzięć informatycznych wiąże się z ryzykiem. Podczas realizacji przedsięwzięć powstają sytuacje skutkujące wydłużeniem czasu realizacji projektu, nieosiągnięciem zakładanych celów, czy poniesieniem dodatkowych kosztów. Dlatego szczególnie istotne jest właściwe zarządzanie ryzykiem podczas realizacji projektów informatycznych, tak aby minimalizować możliwość wystąpienia niekorzystnych zdarzeń. W artykule skoncentrowano się na rodzajach ryzyka, które mogą wystąpić w trakcie realizacji projektu, oraz zasadach ich podziału pomiędzy strony, tj. zamawiającego oraz realizującego przedsięwzięcie.
Słowa kluczowe: projekt informatyczny, ryzyko, zarządzanie ryzykiem.

Wprowadzenie

Prowadzenie projektów inwestycyjnych, a zwłaszcza przedsięwzięć informatycznych, obarczone jest ryzykiem, ponieważ wpływa na to wiele czynników. Ryzyko utrudnia prowadzenie przedsięwzięć inwestycyjnych. Każde wystąpienie strat powoduje powstanie pytania: czy rzeczywiście te straty musiały wystąpić, czy nie mogły być mniejsze, kto jest odpowiedzialny za ich wystąpienie? Powstałe podczas realizacji przedsięwzięcia straty pogarszają wynik finansowy przedsięwzięcia, a zatem zawsze będzie dążyło się do minimalizacji ryzyka, obniżania prawdopodobieństwa wystąpienia negatywnych zdarzeń oraz – jeśli takie zdarzenia już wystąpią – minimalizacji skutków tych zdarzeń. Ma to szczególne znaczenie podczas realiza-

[1] Katedra Transportu, Wydział Ekonomii.

cji przedsięwzięć informatycznych. Innowacyjny charakter projektów, niepowtarzalność, złożoność, zmienność technologii oraz duże skomplikowanie powodują, że bardzo często występują sytuacje, w których przekracza się planowane koszty przedsięwzięcia, wydłuża czas jego realizacji, czy też nie osiąga zakładanych wcześniej celów wdrożenia danego systemu informatycznego. Dlatego też szczególnie istotne jest właściwe zarządzanie ryzykiem podczas realizacji projektu, tak aby minimalizować prawdopodobieństwo wystąpienia oraz straty, czy też inne negatywne skutki.

1. Otoczenie jako źródło ryzyka podczas realizacji projektu informatycznego

Ryzyko występuje w wielu obszarach życia i działalności człowieka, jest więc przedmiotem badań wielu dyscyplin naukowych. Różnie podchodzi się też do samego pojęcia ryzyka (Szyjewski 2004, s. 217–228; Maciejewski 2010, s. 36–78; Parys 2012, s. 43–45). Najogólniej ryzyko to możliwość, że coś się nie uda, pojawi się niebezpieczeństwo, poniesione zostaną straty. Ryzyko to też jakikolwiek czynnik, zdarzenie lub wpływ zagrażający korzystnemu zakończeniu projektu, w kontekście czasu, kosztu lub jakości (Komisja Europejska 2003, s. 61–63). Można mówić o mniejszym czy też większym ryzyku, a zatem prawdopodobieństwo wystąpienia danego zdarzenia, oznaczającego problemy, czy też sama wielkość strat, nie jest zawsze takie same.

W zależności od przyjmowanych kryteriów można dokonać różnych klasyfikacji ryzyka (Szyjewski 2001, s. 230–258, Dydkowski, Urbanek 2011, s. 91–95, Parys 2012, s. 44–46). Praktycznym jest podział na ryzyko wewnętrzne, związane z błędnymi założeniami dotyczącymi projektu, przyjęciem nierealnego harmonogramu, błędami w doborze kadr, czy też w samej organizacji pracy, oraz ryzyko zewnętrzne, generowane przez otoczenie uczestniczących w projekcie podmiotów. Każda działalność, w tym realizacja projektu informatycznego, wykonywana jest bowiem w określonym otoczeniu, dotyczy to zarówno podmiotu, na rzecz którego realizowane jest przedsięwzięcie (najogólniej zamawiającego), jak i podmiotu bezpośrednio realizującego przedsięwzięcie (wykonawcy). Próbując opisać otoczenie, można wyodrębnić otoczenie dalsze, tj. makroekonomiczne, oraz bliższe mikroekonomiczne (Szewczuk 2001, s. 30–53). W ramach otoczenia makroekonomicznego wymienić można otoczenie polityczne, prawne, międzynarodowe, społeczne i demograficzne, ekonomiczne i technologiczne. Otoczenie mikroekonomiczne to najogólniej dostawcy, w tym dostawca systemu informatycznego, instytucje finansowe, doradcze, konsultingowe, odbiorcy usług realizowanych przez zamawiającego, z ich wymaganiami, oczekiwaniami oraz zmiennością. W obszarze mikroekonomicznym wymienić można też samego zamawiającego ze zdefiniowanym projektem, stawianymi wymaganiami oraz środkami, które może lub zamierza przezna-

czyć na projekt, organizacją podmiotu, ludźmi z ich wiedzą, doświadczeniem, kreatywnością, umiejętnością wzięcia odpowiedzialności oraz motywacją realizacji danego projektu. Te wszystkie elementy w różnym stopniu i w różnych momentach wpływają lub mogą wpływać na realizację przedsięwzięcia, tworząc tym samym burzliwe, zmienne i trudne do przewidzenia otoczenie podmiotów oraz samego przedsięwzięcia.

Współczesną gospodarkę charakteryzuje globalizacja oraz znaczny zakres współpracy i wymiany międzynarodowej, a to oznacza, że wpływ otoczenia zaczyna być coraz bardziej skomplikowany. Podmioty, w tym w szczególności podmioty działające w sektorze informatyki, działają na wielu rynkach, również dostawcy pochodzą z różnych państw czy też kontynentów. W efekcie zmiany, różnego typu lokalne zdarzenia, oddziałują nie tylko lokalnie, ale często również na projekty realizowane w innych krajach czy innych kontynentach. Oczywiście dostawców można zmieniać, jednak wymaga to czasu, a to może oznaczać niedotrzymanie terminu. Projekt informatyczny bowiem to w znacznej mierze integracja w całość komponentów infrastruktury sprzętowej oraz oprogramowania dostarczanych przez różnych dostawców. Z jednej strony ponosi się dodatkowe ryzyko oraz koszty integracji, ale z drugiej uzyskuje korzyści wynikające z możliwości doboru różnych podmiotów (jako poddostawców) oraz korzyści związane z jakością oraz ceną danego komponentu.

2. Alokacja wewnętrznego ryzyka w projekcie informatycznym

Realizacja przedsięwzięcia informatycznego powoduje powstanie ryzyka u obu partnerów – zarówno u zamawiającego, jak również po stronie wykonawcy. Stąd też w interesie obu stron jest odpowiednie zarządzanie ryzykiem. Kluczowa dla minimalizacji ryzyka jest odpowiednia alokacja ryzyka, to jest jednoznaczne przypisanie każdemu z partnerów odpowiedzialności za negatywne skutki wynikające z wystąpienia danego czynnika ryzyka. Właściwą zasadą jest tu przyjęcie założenia, że skutki wystąpienia danego negatywnego zdarzenia powinny obciążać stronę, która ma wpływ na prawdopodobieństwo jego wystąpienia, która może się przed danym zdarzeniem lub jego skutkami w lepszy lub gorszy sposób zabezpieczyć. Reguła ta nie jest zawsze stosowana, czasami niezależnie od tego, czy wykonawca ma wpływ na dane zdarzenie, czy też nie, zamawiający nie chce ponosić określonego ryzyka i przenosi je na wykonawcę lub inny podmiot, ten z kolei wlicza je podczas szacowania ceny oferty. Uzasadnienie postepowania, w którym zamawiający obciąża wykonawcę możliwie jak najszerszym zakresem ryzyka, wynika z faktu, że zamawiający płaci i tym samym oczekuje od wykonawcy kompleksowego zrealizowania przedsięwzięcia. Ponadto wykonawca jest podmiotem posiadającym doświadczenie w realizacji tego typu przedsięwzięć, ich realizacja stanowi

przedmiot jego działalności, a zatem powinien dobrze radzić sobie z zarządzaniem ryzykami i problemami, które mogą wystąpić. Oczywiście możliwe jest rozwiązanie, w którym za określoną płatność podmioty przenoszą określone ryzyka na ubezpieczyciela, a w sytuacji, w której dane ryzyko się zmaterializuje i wystąpi określona strata, ubezpieczyciel powinien wypłacić odszkodowanie rekompensujące tę stratę. Ubezpieczenie może być zatem jednym z instrumentów ograniczania skutków ryzyka.

Podczas przygotowania i samej realizacji przedsięwzięcia można zidentyfikować różne ryzyka. Powinno się to odbyć już na etapie przygotowywania studium wykonalności danego przedsięwzięcia, wówczas, w zależności od ich skali, może to być czynnik decydujący o wstrzymaniu się z realizacją przedsięwzięcia lub też wybraniu innego wariantu.

Wymienić można wiele kategorii ryzyka, różnie też je można hierarchizować, niekoniecznie tylko ze względu na przyczyny powstania lub skutki dla realizowanego projektu. Na ryzyka wewnętrzne, wynikające ze skutków niewłaściwego postępowania, wpływ jest większy niż na ryzyka wynikające z otoczenia. W przypadku zamawiającego istotnym wewnętrznym ryzykiem jest właściwy dobór właściwego partnera – wykonawcy przedsięwzięcia. Najogólniej oczekuje się, aby wykonawca posiadał stosowne kompetencje, doświadczenie, odpowiednie zasoby ludzkie i finansowe, co wydaje się oczywiste, oraz był zainteresowany realizacją danego przedsięwzięcia z sukcesem. W przypadku gdy wybór wykonawcy dokonuje jednostka z sektora finansów publicznych, musi się on odbywać zgodnie z procedurą opisaną w ustawie z dnia 29 stycznia 2004 roku Prawo zamówień publicznych (DzU z 2013 r. poz. 907 z późn. zmianami). Więcej swobody mają tu podmioty sektora prywatnego, niemniej uwzględniając, że większe przedsięwzięcia to najogólniej znaczące wydatki, również stosują otwarte konkurencyjne procedury. Jednak nawet najlepsze procedury nie eliminują ryzyka podpisania umowy z wykonawcą, który z takich czy innych względów nie poradzi sobie z przedsięwzięciem, co dla zamawiającego w najlepszym przypadku oznacza stratę czasu, nieefektywne zaangażowanie własnych zasobów ludzkich i niezrealizowane zupełnie lub w części przedsięwzięcie.

Kolejnym ryzykiem, ściśle wiążącym się z poprzednim, jest ryzyko właściwie sformułowanej umowy, w szczególności konkretnego, kompletnego, jednoznacznego i niebudzącego wątpliwości przypisania obowiązków wykonawcy. Istotne jest, aby realizacja przez wykonawcę zapisów umowy prowadziła do wdrożenia systemu informatycznego odpowiadającego przepisom prawnym, postanowieniom umowy oraz oczekiwaniom zamawiającego. Niestety często występują przypadki, w których strony różnie interpretują zapisy umowy, z reguły w sposób korzystny dla siebie, próbując zwiększyć zakres projektu, czy też w przypadku drugiej strony – ograniczyć funkcje systemu oraz inne parametry jakościowe i w ten sposób ułatwić sobie realizację przedsięwzięcia.

W przypadku gdy wykonawca realizuje przedsięwzięcie na podstawie dokumentacji dostarczonej przez zamawiającego, pojawia się kolejne ryzyko – ryzyko błędów w dokumentacji, jej niekompletności czy niezgodności. Najogólniej to sytuacja, w której realizacja wybranych części przedsięwzięcia zgodnie z projektem nie doprowadza do jego poprawnej działalności, bowiem duże, rozległe systemy informatyczne są projektami nowatorskimi, których działania nie można sprawdzić podczas projektowania. Wykonawca może dowodzić, że realizując przedsięwzięcie zgodnie z zapisami zawartymi w dokumentacji, nie uzyska się poprawnie działającego rozwiązania, a zamawiający ma tu ograniczone możliwości Rozwiązaniem może być realizacja przedsięwzięcia w formule „zaprojektuj i wybuduj", a zatem powierzenie wykonawcy przygotowania stosownych dokumentów, w tym projektów technicznych, oraz później realizacja wdrożenia. Jednak u zamawiającego mogą wówczas pojawić się inne ryzyka związane z przyjętymi przez wykonawcę rozwiązaniami, zmierzającymi najogólniej do obniżenia kosztów samej inwestycji, co często skutkuje wyższymi kosztami eksploatacyjnymi – utrzymania systemu. Pewnym rozwiązaniem może być w tej sytuacji łączne zlecenie części inwestycyjnej wykonawcy oraz utrzymania systemu, np. przez okres pięciu lub więcej lat od momentu zakończenia części inwestycyjnej.

Kolejnym ryzykiem po stronie zamawiającego jest zabezpieczenie odpowiednich środków na terminowe zapłaty dla wykonawcy za wykonywanie poszczególnych etapów czy też całego przedsięwzięcia. Przedsięwzięcia inwestycyjne nie są finansowane wyłącznie środkami własnymi, będącymi w pełnej kwocie w dyspozycji w momencie podpisywania umowy. Często korzysta się z kredytów i innych zwrotnych lub bezzwrotnych zewnętrznych źródeł finansowania, a w przypadku przedsięwzięć, które trwają dłużej, wykorzystuje się także środki pochodzące z bieżącej działalności, które dopiero będą uzyskiwane w trakcie realizacji przedsięwzięcia. Ponadto zamawiający może ponosić ryzyka związane z zastosowaniem formuł określających wysokość płatności od różnych czynników, jeżeli je przewidziano w umowie.

Po stronie wykonawcy występują ryzyka wykonania przedsięwzięcia zgodnie z opisem zawartym w umowie, w ustalonym czasie i kosztach. Oznacza to dla wykonawcy konieczność zmieszczenia się w budżecie przewidzianym dla danego projektu. Przekroczenie budżetu to w pierwszej kolejności zmniejszanie zysku osiąganego z tytułu realizacji danego projektu, później oznacza generowanie straty, na co wykonawca nie może sobie pozwolić. Konieczne jest zatem oszacowanie kosztów realizacji przedsięwzięcia oraz kosztów związanych z czynnikami ryzyka, które może wystąpić i które je obciążą. Jest to dość trudne zwłaszcza w projektach pionierskich, innowacyjnych, dużych i rozległych oraz w niestabilnym i zmiennym otoczeniu. Oznacza to ryzyko wystąpienia kosztów, których wcześniej się nie przewidziało.

Podmiot realizujący przedsięwzięcie informatyczne często jest integratorem, odpowiada za wdrożenie systemu, natomiast nie wytwarza całości sprzętu czy też oprogramowania. Korzysta z wielu dostawców, stąd pojawia się ryzyko właściwego wyboru poddostawców sprzętu i oprogramowania, a szerzej ryzyko odpowiedniego zarządzania projektem.

Podczas realizacji przedsięwzięcia informatycznego występują ryzyka zarówno po stronie zlecającego/zamawiającego, jak i wykonawcy, dotyczą bowiem obowiązków, które z mocy prawa lub też postanowieniami umownymi mają przypisane i za które są odpowiedzialni. Jednak podczas realizacji przedsięwzięcia mogą wystąpić też sytuacje, nieprzewidziane w zawartej umowie, w stosunku do których w umowie odpowiedzialność i zasady postępowania stron nie są opisane. Wynika to po części z dużej różnorodności zdarzeń, które mogą wystąpić podczas realizacji przedsięwzięcia, ale też faktu, że część zdarzeń była uznana za mało prawdopodobne, stąd zostały w umowie pominięte. W przypadku części zdarzeń, np. z działania siły wyższej, trudno określić ich skalę i skutki, przykładowo mogą to być takie zdarzenia jak zniszczenia spowodowane trzęsieniem ziemi, działaniami wojennymi, zamieszkami, zniszczeniem obiektu np. na skutek pożaru wywołanego burzą i wyładowaniami atmosferycznymi. Zdarzenia takie mogą nie wystąpić w miejscu, do którego dostarczany jest system informatyczny, jednak nie są one już takie rzadkie w krajach, w których produkowany jest sprzęt czy też inne komponenty dla danego przedsięwzięcia.

3. Procedura zarządzania ryzykiem i problemami w projekcie

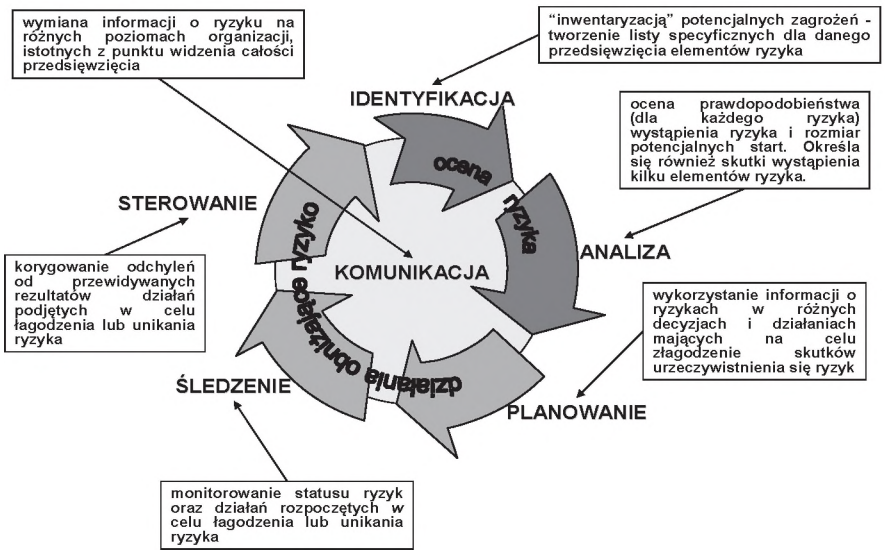
Zarządzanie ryzykiem oraz później już samymi problemami występującymi podczas realizacji projektu jest jednym z istotniejszych obszarów zarządzania projektem. Wynika to z ryzyka, którym obarczone są przedsięwzięcia informatyczne oraz możliwych znaczących negatywnych skutków dla samego projektu w przypadku zaistnienia negatywnych zdarzeń. Ryzykowność projektów informatycznych najlepiej dokumentują dane o projektach, które nie skończyły się powodzeniem (Parys 2012, s. 47–52).

Zasady zarządzania ryzykiem, zwłaszcza w przypadku dużych projektów informatycznych, przyjmują najczęściej charakter opisanych procedur, przyjętych przez strony projektu, w ramach których zobowiązuje się strony do określonych cyklicznych działań. W sposób podobny można też postępować z problemami, tj. negatywnymi zdarzeniami w projekcie. Osoby zajmujące się zarządzaniem ryzykiem powinny posiadać oprócz innych kwalifikacji również takie cechy jak doświadczenie, intuicję, umiejętność trafnej oceny sytuacji oraz wyobraźnię, zwłaszcza co do następstw i skutków zdarzeń. Sam poziom ryzyka, prawdopodobieństwo zaistnienia wybranych zdarzeń, podlega często jedynie subiektywnym ocenom, a skutki tych samych zdarzeń w różnych sytuacjach mogą być diametralnie różne.

Przyjmuje się, że w ramach zarządzania ryzykiem wykonuje się cyklicznie powtarzane działania takie jak (zob. Szyjewski 2004, s. 217–244):

- identyfikowanie – rozpoznawanie ryzyka/problemów,
- analizowanie, kwalifikacja i ocena ryzyka/problemów,
- zapobieganie oraz planowanie reakcji na ryzyko/problemy,
- monitorowanie i kontrola ryzyka/problemów.

Sekwencję czynności zarządzania ryzykiem podczas realizacji projektu zaprezentowano na rysunku 1. W celu identyfikacji ryzyka, które związane jest z realizowanym przedsięwzięciem, można wykorzystać i korzysta się z wielu różnych metod i technik (Radomska-Zalas 2014, s. 9–10). Jednak oprócz samych narzędzi identyfikacji ryzyka, a później też negatywnych zdarzeń – problemów powstałych w wyniku zmaterializowania ryzyka – konieczne są procedury postępowania.



Rys. 1. Model Software Engineering Institute (SEI) zarządzania ryzykiem

Źródło: J. Florek (2012), *Jakość, ryzyko i efektywność przedsięwzięcia informatycznego*, Akademia Podlaska, Prezentacja, www.ap.siedlce.pl, Siedlce 2012. Zob. też: Barczak, Florek, Sydoruk (2006).

Czynności mogą być prowadzone przez strony niezależnie, mogą być też realizowane w trakcie spotkań poświęconych ryzykom w projekcie, z udziałem wybranych ekspertów z zespołów wykonawczych, organizowanych przez kierujących projektem, czy też odpowiedzialnych za ryzyko w projekcie. Można ujednolicić lub też pozostawić do decyzji każdej ze stron zagadnienia samego prowadzenia oraz sposobu ewidencji i opisu ryzyka. Każda ze stron na bieżąco powinna identyfikować ryzyka, przede wszystkim związane z zadaniami, które ma przypisane w pro-

jekcie. Kolejnym krokiem jest przeprowadzenie analizy zmierzającej do oceny danego ryzyka. Powinno się ocenić:

- wagę wpływu (znaczenie dla projektu w przypadku wystąpienia zdarzenia),
- czynniki/przyczyny, które mogą spowodować wystąpienie danego ryzyka, oraz samo prawdopodobieństwo wystąpienia.

Wydaje się że dobrym rozwiązaniem jest informowanie się stron wzajemnie o ryzykach oraz wynikach przeprowadzonych ocen. Tworzy to atmosferę zaufania podczas realizacji przedsięwzięcia. Niestety często tak nie jest – problemy podczas realizacji projektu, opóźnienie, ograniczenie funkcjonalności, większa zawodność systemu mogą skutkować lub skutkują pomniejszeniem wynagrodzenia czy też karami umownymi. Powoduje to, że czasami wykonawca może ukrywać rzeczywiste przyczyny problemów, tak aby poprawić swoją pozycję i w przyszłości pomniejszyć odpowiedzialność za ewentualne niewywiązanie się z umowy.

Zapobieganie i planowanie reakcji na ryzyka powinno być inicjowane i prowadzone przez stronę, która jest zobowiązana na podstawie umowy pomiędzy stronami do wykonania danego zadania, którego ryzyko dotyczy. Strony powinny współdziałać w celu zmniejszania prawdopodobieństwa wystąpienia ryzyka oraz w przypadku jego wystąpienia – skutków.

Partnerzy projektu powinni systematycznie monitorować i kontrolować sam proces podejmowanych reakcji na ryzyka. Jeśli reakcje na ryzyka wymagają skorygowania, powinny podejmować odpowiednie działania w tym zakresie. Wyniki monitorowania, ale też całego zarządzania ryzykiem, powinny być opisywane w odpowiedniej dokumentacji.

Podsumowanie

Zarządzanie projektem informatycznym wymaga zarządzania ryzykami, pozwoli to minimalizować prawdopodobieństwo wystąpienia negatywnych zdarzeń oraz minimalizować ich skutki. Czynności związane z zarządzaniem ryzykiem powinny być wykonywane cyklicznie, wg określonych przez każdą ze stron lub wspólnie procedur. Ich wykonywanie powinno być również monitorowane, tak aby wśród wielu czynności związanych z realizacją projektu nie były pomijane i tym samym aby zarządzanie ryzykiem nie przerodziło się w jedynie zarządzanie negatywnymi zdarzeniami w projekcie.

Literatura

1. Barczak A., Florek J., Sydoruk T. (2006), *Projektowanie zintegrowanych systemów informatycznych zarządzania*, Wydawnictwo Akademii Podlaskiej, Siedlce.

2. Dydkowski G., Urbanek A. (2011), *Partnerstwo publiczno-prywatne*, Prace Naukowe Uniwersytetu Ekonomicznego w Katowicach, Katowice.
3. Florek J. (2012), *Jakość, ryzyko i efektywność przedsięwzięcia informatycznego*, Akademia Podlaska, Prezentacja, www.ap.siedlce.pl, Siedlce.
4. Komisja Europejska (2003), *Wytyczne dotyczące udanego partnerstwa publiczno-prywatnego*, Dyrektoriat Generalny ds. Polityki Regionalnej, Bruksela.
5. Maciejewski G. (2010), *Ryzyko w decyzjach nabywczych konsumentów*, Prace Naukowe Uniwersytetu Ekonomicznego w Katowicach, Katowice.
6. Parys T. (2012), *Ryzyko w projektach wdrożeniowych zintegrowanych systemów informatycznych – próba klasyfikacji pod katem barier i działań nim obarczonych*, Problemy Zarządzania, Vol. 10, nr 3, Uniwersytet Warszawski.
7. Radomska-Zalas A. (2014), *Koncepcja metody identyfikacji i analizy ryzyka w projektach informatycznych*, praca doktorska, Uniwersytet Szczeciński, Szczecin.
8. Szewczuk A. (2001), *Zachowania przedsiębiorstw transportu samochodowego w konkurencyjnym otoczeniu*, Instytut Transportu Samochodowego, Warszawa.
9. Szyjewski Z. (2001), *Zarządzanie projektami informatycznymi*, Placet, Warszawa.
10. Szyjewski Z. (2004), *Metodyki zarządzania projektami informatycznymi*, Placet, Warszawa.
11. Ustawa z dnia 29 stycznia 2004 roku Prawo zamówień publicznych, DzU z 2013 r. poz. 907 z późn. zm.

RISK MANAGEMENT IN INFORMATION TECHNOLOGY PROJECTS

Summary

Investment projects, especially in area of information technology, carry numerous risks. Factors such as innovative nature of the projects, along with their complexity and uniqueness, are commonly reasons for significant cost increases that may lead to over-expenditure, noticeable increases in amount of time required for project completion, or failure to fulfill the planned goals of the implemented information system. Therefore, correct risk management is crucial to success of information technology projects, with the purpose of reducing probability of such factors influencing the projects and lowering potential losses – and other negative factors – connected with their influence. The paper is focused on various types of risk that can occur during the project and rules that govern sharing them between the sides, i.e. both client and the provider.
Keywords: IT project, risk, risk management.

Translated by Barbara Kos