WYDZIAŁ ZARZĄDZANIA
Akademia Górniczo-Hutnicza
im. Stanisława Staszica w Krakowie

Studia Podyplomowe

ZARZĄDZANIE PROJEKTAMI
KWALIFIKACJE PROJECT MANAGERA

edycja 2011/2012

Praca podyplomowa

ZARZĄDZANIE RYZYKIEM ZWIĄZANYM Z TWORZENIEM OPROGRAMOWANIA I ZAPEWNIENIEM JAKOŚCI W PROJEKTACH INFORMATYCZNYCH

Autor: **Paweł Paterek**

Kraków,
Czerwiec 2012

SPIS TREŚCI

WSTĘP

Obecnie obserwuje się wzrost liczby projektów związanych z informatyzacją, tworzeniem oprogramowania w celu osiągnięcia różnych korzyści biznesowych, czy też w celu prowadzenia badań naukowych. Projekty związane z tworzeniem oprogramowania cechują się bardzo wysokim poziomem ryzyka związanym z ich podjęciem i realizacją. Znacznie więcej tego typu projektów kończy się niepowodzeniem w stosunku do projektów o innym charakterze. Oficjalne przyczyny niepowodzenia tych projektów są zazwyczaj bardzo różne, ale większość z nich ma swoje prawdziwe źródło w braku zarządzania ryzykiem lub niewłaściwym zarządzaniu ryzykiem związanym z podjęciem i realizacją tych projektów. Różne względy, takie jak wizerunek organizacji, przewaga rynkowa nad konkurencją, czy potencjalne korzyści biznesowe nie pozwalają wskazywać ryzyka jako przyczyny problemów danej organizacji w podejmowaniu i realizacji projektów. Chcąc jednak zwiększyć szanse oraz ilość projektów zakończonych sukcesem potrzebujemy poznać prawdziwe źródło przyczyn ich niepowodzenia oraz sposoby radzenia sobie z tego typu problemami. W tym kontekście niezmiernie ważne okazuje się zrozumienie tematyki związanej z ryzykiem oraz zarządzaniem ryzykiem w projektach dotyczących tworzenia i zapewnienia jakości oprogramowania.

Tematem niniejszej pracy jest zarządzanie ryzykiem związanym z tworzeniem oprogramowania i zapewnieniem jakości w projektach informatycznych. Celem pracy jest przybliżenie tematyki zarządzania ryzykiem związanym z tworzeniem, testowaniem oprogramowania i zapewnieniem jakości w projektach informatycznych oraz przedstawienie praktycznego sposobu wykorzystania metodyki testowania na podstawie ryzyka (*risk based testing*) w zastosowaniu do projektów informatycznych na bazie teorii oraz doświadczeń z prowadzonych projektów związanych z testowaniem oprogramowania. W pracy przedstawiono teoretyczne aspekty zarządzania ryzykiem na bazie ogólnodostępnej literatury oraz porównano najpopularniejsze metodyki zarządzania projektami w kontekście zarządzania ryzykiem (PRINCE2 oraz PMI). Autor przedstawił wykorzystanie wiedzy związanej z zarządzaniem ryzykiem w projektach dotyczących tworzenia oprogramowania, a w szczególności w testowaniu i zapewnianiu jakości w tego typu projektach na bazie ogólnodostępnej literatury oraz własnych doświadczeń z prowadzonych projektów dotyczących testowania oprogramowania. Zaproponował także na podstawie analizy źródeł internetowych oraz własnych doświadczeń zawodowych wykorzystanie metody testowania z uwzględnieniem ryzyka oraz pokazał praktyczny

sposób wykorzystania tej techniki do zarządzania ryzykiem w projektach związanych z testowaniem oprogramowania. Poruszona w pracy tematyka pozwoliła wyciągnąć wiele istotnych wniosków dotyczących zarządzania ryzykiem w projektach informatycznych. Zostały one przedstawione w treści niniejszej pracy oraz w podsumowaniu na końcu pracy.

Praca została podzielona na cztery rozdziały. Dwa pierwsze rozdziały przedstawiają teoretyczne aspekty zarządzania ryzykiem jako integralną część metodyki zarządzania projektami. Dwa kolejne przedstawiają zarówno teoretyczne, jak i praktyczne aspekty zarządzania ryzykiem w projektach związanych z tworzeniem i testowaniem oprogramowania.

Pierwszy rozdział przedstawia ogólne wprowadzenie do tematyki zarządzania ryzykiem jako integralnej części metodyki zarządzania projektami. W rozdziale tym omówione zostały źródła ryzyka w projektach, cykl zarządzania ryzykiem oraz wymienione zostały techniki i narzędzia stosowane w zarządzaniu ryzykiem.

Drugi rozdział przybliża adaptacje modelu zarządzania ryzykiem oraz porównuje dwie najpopularniejsze metodyki zarządzania projektami PRINCE2 oraz PMI w kontekście zarządzania ryzykiem. W rozdziale tym wymienione zostały pokrótce pozostałe metodyki oraz ich aspekty związane z zarządzaniem ryzykiem.

Trzeci rozdział stanowi omówienie tematyki związanej z zarządzaniem ryzykiem w zastosowaniu do projektów informatycznych związanych z tworzeniem, testowaniem i zapewnieniem jakości oprogramowania. Rozdział przybliża tematyke zarówno na bazie ogólnodostępnej literatury, jak i własnych doświadczeń autora z prowadzonych projektów.

Rozdział czwarty przedstawia przykład zastosowania metodyki testowania uwzględniającej ryzyko (*risk based testing*) w zarządzaniu ryzykiem w projektach związanych z testowaniem oprogramowania w oparciu o materiały dostępne w Internecie oraz własne doświadczenia autora z udziału w tego typu projektach.

Nieniejsza praca nie wyczerpuje tematyki zarządzania ryzykiem w projektach związanych z tworzeniem i testowaniem oprogramowania, a jedynie pokazuje potrzebę dalszego prowadzenia badań w tym obszarze oraz rozwoju i adaptacji tej metodyki w tego typu projektach. Dotyczy to zarówno dalszego rozwoju metodyki testowania w oparciu o ryzyko, jak również poszukiwania innych technik ułatwiających zarządzanie ryzykiem w projektach informatycznych.

ROZDZIAŁ I – ZARZĄDZANIE RYZYKIEM W PROJEKTACH INFORMATYCZNYCH

Projekty informatyczne związane z tworzeniem oprogramowania posiadają wiele specyficznych cech, których nawet niewielkie zmiany mogą zadecydować o sukcesie, bądź niepowodzeniu danego projektu. Przedsięwzięcia te związane są często z szybko zmieniającymi się technologiami oraz cechują się potrzebą szybkiego wdrożenia w celu realizacji bardziej złożonych planów. Mają one bardzo często ograniczony cykl życia, najczęściej spowodowany potrzebą kolejnych zmian wymaganych przez klienta i tym samym potrzebą stworzenia nowszej wersji oprogramowania, która powoduje potrzebę uruchomienia nowego projektu (Szyjewski, 2001, s. 230).

Takie właściwości oraz specyfika projektów obarczone są dużą niepewnością działań, podejmowanych decyzji oraz zdarzeń z nimi związanymi. Pojawia się ryzyko związane z sukcesem lub niepowodzeniem danego projektu, a tym samym niebezpieczeństwem poniesienia straty lub utraty potencjalnych zysków. Ryzyko to inaczej niepewne zdarzenie, które może wystąpić z pewnym prawdopodobieństwem i mieć pozytywny lub negatywny wpływ na projekt. Zazwyczaj ryzyko to jest sumą wielu ryzyk, skorelowanych z danym przedsięwzięciem. Oprogramowanie, jako wynik projektu informatycznego jest bardzo często zaawansowanym technicznie produktem, który dostarcza dla klienta oczekiwanych funkcjonalności w użytecznej postaci. Ryzyko jest związane z niepewnością osiągniętego wyniku co do zgodności dostarczonej funkcjonalności z oczekiwaniami użytkownika (Korczowski, 2009, s. 16-17). Stąd bardzo często z tworzeniem oprogramowania związane jest jego testowanie polegające na weryfikacji, czy dane oprogramowanie jest zgodne z oczekiwaniami i wymaganiami klienta. Zależnie od specyfiki oprogramowania, jego złożoności, strategii firmy oraz innych czynników, testowanie może być częścią tego samego projektu, co tworzenie oprogramowania lub skorelowanym, równoległym projektem (najczęściej w ramach jednego programu).

Możliwość osiągnięcia zysków oraz realizacji celów projektu związana jest nieuchronnie z koniecznością podejmowania różnorakich decyzji, a tym samym z koniecznością podejmowania ryzyka (Szyjewski, 2001, s. 231). Testowanie oprogramowania związane jest z bardzo dużą niepewnością, co do oszacowania ilości koniecznego wysiłku podejmowanego w celu weryfikacji oprogramowania. Ponieważ nie istnieje możliwość przetestowania wszystkiego, od kierownika projektu wymagana jest umiejętność

podejmowania bardzo wielu decyzji odnośnie strategii i wyboru testów pozwalających na zminimalizowanie ryzyka związanego z dostarczeniem wadliwego, bądź niezgodnego z oczekiwaniami klienta oprogramowania w skończonym czasie dla danego projektu.

Tworzenie oprogramowania jest najczęściej niepewną inwestycją, ponieważ bardzo łatwo przekroczyć oczekiwany czas zakończenia, zaplanowany budżet lub nie osiągnąć oczekiwanych zysków z powodu niezgodności z wymaganiami klienta (np. poprzez nieodpowiednie testowanie), stąd zarządzanie takim przedsięwzięciem to przede wszystkim zarządzanie ryzykiem (DeMarco, 2002, s. 82-84). Właściwe zarządzanie ryzykiem to takie podejmowanie decyzji, które pozwoli na uniknięcie zidentyfikowanych zagrożeń oraz potencjalnych szkód, które mogłyby by mieć miejsce w przypadku ich wystąpienia (Chong, Brown, 2001, s. 95). Zarządzanie ryzykiem jest niezbędne w zarządzaniu projektami związanymi z tworzeniem i testowaniem oprogramowania. Umiejętne zarządzanie ryzykiem w każdym projekcie powinno być systematyczne i udokumentowane w odpowiedni sposób przez kierownika projektu (Pritchard, 2002, s. 3).

1. Źródła i czynniki związane z ryzykiem

Ryzyko niepowodzenia projektu ma najczęściej wiele różnych przyczyn oraz wiele różnych źródeł ryzyka. Bardzo ważne jest zidentyfikowanie ryzyk o charakterze przyczynowym, a nie tylko tych, które mają wpływ na końcowy wynik całego projektu. Dobrą praktyką jest tworzenie i prowadzenie na bieżąco listy potencjalnych ryzyk w projekcie oraz przypisanych im akcji (DeMarco, 2002, s. 85).

Ryzyka mogą mieć różne źródła, najogólniej sklasyfikowane, jako (Szyjewski, 2001, s. 232-235, Chong, Brown, 2001, s. 63, Pritchard, 2002, s. 9-23):

- **wewnętrzne** – związane ze sposobem planowania projektów w danej firmie, niedostosowanym procesem, długim harmonogramem projektu, wprowadzaniem nowej technologii czy usprawnień,
- **zewnętrzne** (narzucone) – związane z wymaganiami pochodzącymi od klienta, środowiskiem, otoczeniem, miejscem lub czasem, w którym realizowany jest dany projekt, zmianami ekonomicznymi lub prawnymi w trakcie trwania projektu,
- **wprowadzone** – wynikające z zaniedbań, braku wiedzy, doświadczenia, wyboru błędnej strategii działania, bądź podjęcia lub niepodjęcia koniecznych decyzji.

Specyfiką projektów związanych z testowaniem oprogramowania jest bardzo duża dynamika zmian stanu projektu, w zależności od czynników zewnętrznych, obranej strategii i wyników testowania. Powoduje to, że lista aktualnych źródeł ryzyka również dynamicznie i często się zmienia. Wymaga to poświęcenia dużej uwagi przez kierownika projektu na identyfikowanie nowych potencjalnych źródeł ryzyka oraz aktualizacji stanu istniejących ryzyk w celu odpowiedniego dostosowania planu projektu, tak, aby ryzyko terminowego ukończenia projektu było na poziomie akceptowalnym w granicach narzuconych tolerancji. Jeżeli nie jest możliwa modyfikacja planów w granicach założonych tolerancji, jest to sygnał dla komitetu sterującego o tym, że istnieje ryzyko w projekcie, którego nie jesteśmy w stanie zaadresować bez pomocy z zewnątrz.

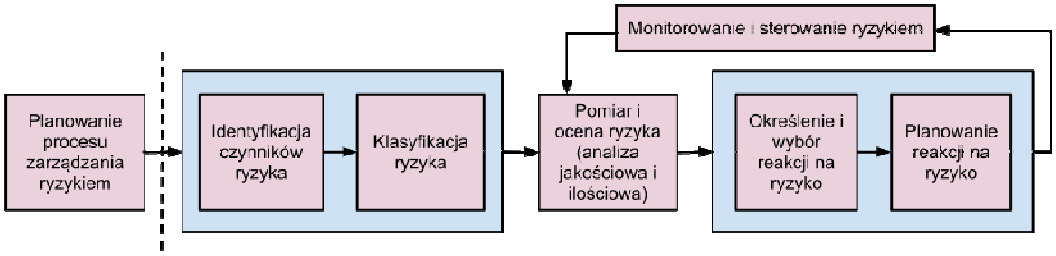
Przykładowe obszary i źródła zagrożeń dla projektów związanych z tworzeniem i testowaniem oprogramowania to (Korczowski, 2009, s. 19-32):

- **niedokładnie sprecyzowane uzasadnienie biznesowe** (nieprecyzyjna estymata zysków z realizacji celów projektu może uniemożliwiać podjęcie właściwej decyzji, czy określony budżet na projekt jest akceptowalny czy nie),
- **nieprecyzyjne wymagania użytkownika** systemu, założenia poczynione przez użytkownika bez specyfikacji w wymaganiach oraz późne zmiany projektowe będące najczęściej wynikiem problemów wykrywanych podczas testowania,
- **zastosowanie przestarzałej technologii** lub niesprawdzonego rozwiązania,
- **zbyt optymistyczne szacowanie prac** związanych z tworzeniem i testowaniem oprogramowania (brak lub niepełna wiedza o możliwym wykorzystaniu oprogramowania) może skutkować przekroczeniem założonego budżetu,
- **współpraca z kontrahentami** (niechęć do udziału w realizacji projektu, znaczne różnice pomiedzy oczekiwaniami klienta, a możliwą realizacją na podstawie zdefiniowanych wymagań mogą wpłynąć na budżet i termin realizacji projektu),
- **współpraca pomiędzy zespołami realizacyjnymi** (konflikt interesów, różnice w profilach psychologicznych, problemy komunikacyjne, zróżnicowanie kulturowe i lokalizacyjne współpracujących ze sobą zespołów w ramach programu),
- **zagadnienia techniczne** (integracja oprogramowania z otoczeniem),
- **bezpieczeństwo informacji** (konieczność modyfikacji istniejącej infrastruktury pod kątem wdrożenia przyszłego oprogramowania).

2. Model zarządzania ryzykiem

Na rysunku 1 przedstawiony został typowy model zarządzania ryzykiem. Na początku (zazwyczaj dla wszystkich projektów prowadzonych w danej firmie) ustala się politykę zarządzania ryzykiem (ustalenia dotyczące funkcjonowania komunikacji, modelu oceny i pomiaru ryzka oraz dopuszczalnych tolerancji poziomu zagrożenia ryzykiem), a następnie zgodnie z tą polityką przygotowuje się plan zarządzania ryzykiem specyficzny dla danego projektu. Składa się on z cyklicznie i systematycznie powtarzanych działań: **identyfikacji ryzyka** (określenia i opisania zdarzeń, które mogą być niepomyślne dla projektu), **klasyfikacji ryzyka** (określenia rodzaju i źródła ryzyka), **pomiaru i oceny ryzyka** (oszacowania prawdopodobieństwa wystąpienia zdarzenia oraz jego negatywnych skutków dla projektu), **planu zapobiegania ryzyku** (określenia możliwych reakcji, wyboru reakcji oraz zaplanowania reakcji na ryzyko w planie projektu) oraz **nadzorowanie i sterowanie** (ocene wdrożonych metod i sposobu zapobiegania ryzyku oraz dalszych możliwości jego wystąpienia). Przygotowanie planu zarządzania ryzykiem, systematyczne zarządzanie i monitorowanie ryzyka w projekcie jest odpowiedzialnością kierownika projektu, ustalenie polityki zarządzania ryzykiem to głównie odpowiedzialność komitetu sterującego, natomiast wszyscy uczestnicy projektu powinni być zaangażowani w działania związane z zarządzaniem ryzykiem (Szyjewski, 2001, s. 236-237, Korczowski, 2009, s. 60-66).

Rysunek 1. Model zarządzania ryzykiem



Źródło: opracowanie własne

W celu prawidłowego pomiaru ryzyka należy wybrać i zastosować odpowiedni model zarządzania ryzykiem najlepiej pasujący do danego typu projektu. Cztery główne kategorie modeli zarządzania ryzykiem to: model uproszczony (jego miarą jest waga ryzyka), model standardowy (gdzie każdy z czynników charakteryzuje prawdopodobieństwo wystąpienia zdarzenia oraz jego wpływ na projekt), modek kaskadowy (uwzględniający dodatkowe

wzajemne interakcje pomiędzy czynnikami) oraz model przyczynowo-skutkowy, który bada efekty mogące wystąpić w reakcji na różne czynniki (Korczowski, 2009, s. 18-19).

Zarządzanie ryzykiem może być przeprowadzone w oparciu o jedną z czterech typowych metod (Chong, Brown, 2001, s. 52):

- **unikanie ryzyka** – poprzez zmiane projektu lub wybór rozwiązania obarczonego mniejszym ryzykiem od innych,
- **łagodzenie ryzyka** – podejmowanie akcji mających na celu obniżenie wpływu ryzyka lub potencjalnej szkody w przypadku materializacji ryzyka,
- **dzielenie ryzyka** – rozłożenie odpowiedzialności i potencjalnych skutków ryzyka na wiekszą liczbę interesariuszy,
- **absorbowanie ryzyka** – akceptacja przyjęcia oraz wzmocnienie własnej pozycji w celu łagodnego odbioru skutków zdarzeń związanych z materializacją ryzyka.

2.1. Planowanie zarządzania ryzykiem

Kierownik projektu związanego z tworzeniem lub testowaniem oprogramownia powinien przygotować plan zarządzania ryzykiem umożliwiający mu prowadzenie działań związanych z: izolowaniem i zmniejszaniem ryzyka, eliminowaniem ryzyka do akceptowalnego poziomu, przygotowaniem sposobów zapobiegania ryzyku oraz przygowaniu odpowiednich rezerw czasowych i budżetowych, dla ryzyk, których nie można złagodzić do bezpiecznego poziomu i których skutki mogłyby wpłynąć niekorzystnie na projekt. Częsta zmiana ryzyka w czasie dla projektów informatycznych oraz brak pełnej informacji o możliwych skutkach ryzyka wymaga od kierownika regularnej aktualizacji planu zarządzania ryzykiem. Przykładowy plan zarządzania ryzykiem może zawierać: opis systemu i podsumowanie projektu, uwarunkowania zarządzania ryzykiem (wybór odpowiedniej strategii i metody), strukturę zarządzania ryzykiem (definicje, rozwiązania, mierniki, sposoby oceny), problemy związane z realizacją (szczegóły związane z adaptacją modelu zarządzania ryzykiem) oraz istotne plany, podsumowanie metodologii, bibliografie i zatwierdzenia (Pritchard, 2002, s. 24-29).

2.2. Identyfikacja oraz klasyfikacja ryzyka

Pierwszym procesem w modelu zarządzania ryzykiem jest identyfikacja i rozpoznanie potencjalnych zagrożeń dla sukcesu przedsięwzięcia. Identyfikacja zagrożeń powinna

odbywać się w kontekście możliwych problemów z realizacją celów projektu, w szczególności zagrożenia celów biznesowych (końcowy sukces, spodziewane zyski, satysfakcja klienta). Wynikiem powinna być uporządkowana lista zidentyfikowanych i przeanalizowanych czynników ryzyka. Szczegółowa analiza powinna być przeprowadzona przynajmniej dla ryzyk, których konsekwencje i wpływ na projekt są nieakceptowane dla klienta (Boehm, 1991, s. 32-41, Szyjewski, 2001, s. 237-242).

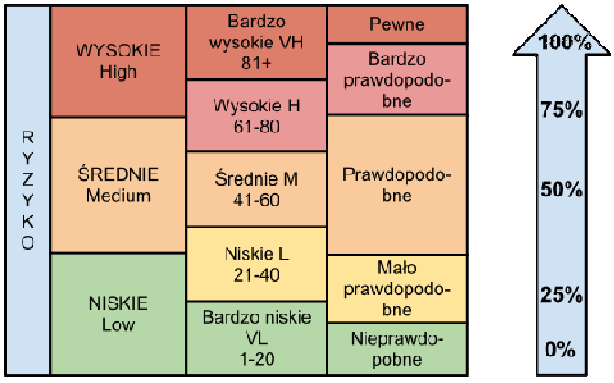
Klasyfikacja ryzyka wymaga zbadania jego źródła, w celu przyporządkowania go do jednej z pięciu płaszczyzn: technicznej, programowej, obsługowej, kosztowej oraz harmonogramowej (Pritchard, 2002, s. 10).

2.3. Pomiar i ocena ryzyka

Proces oceny ryzyka dla projektów informatycznych obejmuje zadania związane z analizą czynników, oszacowaniem prawdopodobieństwa wystąpienia poszczególnych czynników, oszacowaniem skali strat związanych z pojedynczymi czynnikami ryzyka oraz oceną powiązań i wzajemnego wpływu złożonych czynników ryzyka. Dla każdego z czynników powinno się oszacować prawdopodobny termin materializacji ryzyka, ponieważ jest to jedna z kluczowych informacji do podjęcia stosownych akcji (Boehm, 1991, s. 32-41).

Proces oceny ryzyka jest zależny od typu realizowanego przedsięwzięcia, tolerancji klienta, zakładanych celów oraz wyznaczonego wcześniej kryterium sukcesu. Można wyróżnić dwa rodzaje tej oceny: jakościową (pozwala na priorytetyzacje czynników oraz określenie wagi danego zagrożenia) oraz ilościową (pozwala na liczbowe oszacowanie prawdopodobieństwa oraz wymiernych skutków czynników w przypadku ich wystapienia). Miary ryzyka przedstawia rysunek 2.

Rysunek 2. Miary ryzyka



Źródło: (Szyjewski, 2001, s. 244)

Do oceny ilościowej można posłużyć się modelem kosztowym szacowania poziomu ryzyka, gdzie wartość potencjalnych strat jest iloczynem prawdopodobieństwa wystapienia zdarzenia oraz szacowanego kosztu poniesionych strat w przypadku jego wystapienia. Tabela 1 przedstawia macierz poziomu ryzyka w celu ułatwienia oceny ilościowej.

Tabela 1. Macierz poziomu ryzyka

		Straty		
		Wysokie	Średnie	Niskie
Prawdopodobieństwo wystąpienia	Bardzo wysokie	Bardzo wysokie	Wysokie	Średnie
	Wysokie	Wysokie	Wysokie	Średnie
	Średnie	Wysokie	Średnie	Średnie
	Niskie	Średnie	Średnie	Niskie
	Bardzo niskie	Średnie	Średnie	Niskie

Źródło: (Szyjewski, 2001, s. 246)

2.4. Zapobieganie i reakcja na ryzyko

Zapobieganie ryzykom w projektach informatycznych może odbywać się poprzez podjęcie akcji zmniejszających prawdopodobieństwo ich wystapienia lub minimalizacji strat wystapienia tych ryzyk. Podjęcie i wybór akcji zapobiegania ryzyku jest zazwyczaj związane z dodatkowym kosztem planowania akcji zapobiegawczych (ma to najczęściej odzwierciedlenie w budżecie, bądź harmonogramie), stąd bardzo ważna jest właściwa ocena kosztu podejmowanych akcji, które nie powinny przekraczać wartości potencjalnych strat poniesionych w przypadku wystąpienia ryzyka (Korczowski, 2009, s. 74-78).

2.5. Monitorowanie i sterowanie ryzykiem

Monitorowanie ryzyka powinno być systematycznym i ciągłym działaniem podejmowanym przez kierownika projektu. Tworzenie i testowanie oprogramowania wiąże się z dużą dynamiką zmian w projekcie, zarówno zmian wewnętrznych (np. na podstawie wyników testów), jak i zewnętrznych (środowisko oraz infrastruktura, w której powstaje oprogramowanie). Duża liczba nieoczekiwanych sytuacji oraz zmian wymaga uważnego monitorowania w krótkim okresie czasu. Podjęte uprzednio działania dla najbardziej krytycznych ryzyk mogą okazać się zbędne w perspektywie aktualnych wyników testów oraz zmian, które zaszły w trakcie tworzenia i testowania oprogramowania. Monitorowanie w takich projektach powinno być bardziej proaktywne.

3. Techniki zarządzania ryzykiem

Na rynku dostępnych jest bardzo wiele technik zarządzania ryzykiem, które mogą znacząco ułatwić proces zarządzania ryzykiem lub obniżyć jego koszt.

Kryteria doboru technik zarządzania ryzykiem mogą być bardzo różne w zależności od specyfiki projektu. Trzy najważniejsze kryteria względem, których można próbować porównać te techniki to: **wymagane zasoby** (koszt, infrastruktura i wyposażenie projektu, czas wdrożenia, łatwość zastosowania i zaangażowanie czasowe), **możliwości zastosowania** (raportowanie statusu, decyzje planistyczne, strategia wyboru kontraktu, wyznaczanie punktów kontrolnych, wybór źródeł, propozycje budżetu) oraz **otrzymywane wyniki** (dokładność, poziom szczegółowości, użyteczność), (Pritchard, 2002, s. 47-52).

Znane i stosowane techniki w zarządzaniu ryzykiem to: ankiety eksperckie, spotkania planistyczne, metodologie zarządzania ryzykiem, przeglądy dokumentacji, porównania analogii, oceny planu, technika delficka, burza mózgów, metoda Crawforda, analiza SWOT, szablony projektu, listy kontrolne, analiza założeń, analiza decyzji/oczekiwanej wartości pieniężnej, szacowanie zależności, analiza sieciowa, analiza wrażliwości, techniki oceny i przeglądu programu (PERT), inne metody diagramowe, systemy oceny, modelowanie ryzyka, profile ryzyka, drzewa decyzyjne, symulacje Monte Carlo, czynniki ryzyka, macierz reagowania na ryzyko, nadzorowanie wyników czy przeglądy i audyty ryzka (Pritchard, 2002, Korczowski, 2009). Ich opis działania, ocena oraz możliwości zastosowań to temat na osobną i obszerną pracę. Techniki zarządzania ryzykiem mające największe zastosowanie w identyfikacji ryzyka dla projektów informatycznych oraz związanych z testowaniem oprogramowania zostaną przedstawione w rozdziale trzecim.

4. Błędy w zarządzaniu ryzykiem

Ze względu na subiektywny charakter oceny i miar ryzyka w większości przypadków zarządzanie ryzykiem narażone jest znacznie bardziej na błędy i niedokładności, niż pozostałe działania w ramach zarządzania projektem. Błedy te mogą wynikać z: niewłaściwie ustalonej i egzekwowanej polityki zarządzania ryzykiem, niewłaściwego podejścia do identyfikacji czynników ryzyka, przyjęcia nieodpowiednich miar dla szacowania ryzyka, niewłaściwej identyfikacji i niewłaściwym wyborze akcji zapobiegawczych, nieadekwatnego monitorowania oraz błędów popełnianych podczas zamykania projektu (Korczowski, 2009, s. 179-186).

ROZDZIAŁ II – METODYKI ZARZĄDZANIE RYZYKIEM

5. Metodyka PRINCE2

Metodyka PRINCE2 to metodyka zarządzania projektami ukierunkowana na korzyści biznesowe, z jasno określonym i mającym kluczowe znaczenie dla metodyki uzasadnieniem biznesowym. Metodyka nie precyzuje określonej metody do zarządzania ryzykiem, a jedynie podpowiada, jakie kroki należy podjąć, aby dobrze zidentyfikować, ocenić i zarządzać ryzykiem. Ryzyka zidentyfikowane w projekcie powinny być udokumentowane w trakcie planowania, a następnie zaktualizowane na etapie inicjowania projektu przez kierownika projektu. Zarówno lista ryzyk, jak i uzasadnienie biznesowe powinny być aktualizowane i przeglądane wraz z komitetem sterującym podczas każdego przeglądu stanu projektu (Bradley, 2003, s. 211).

Metodyka PRINCE2 proponuje następujące kroki w cyklu zarządzania ryzykiem (Bradley, 2003, s. 211-216):

- **identyfikacja ryzyka** – wszystkie potencjalne ryzyka są spisywane w formie listy z podziałem na obszary występowania: strategiczne, ekonomiczne, prawne, organizacyjne, zarządzania, związane z czynnikiem ludzkim, polityczne, społeczne, środowiskowe, techniczne i operacyjne,
- **ocena ryzyka** – celem tej oceny jest analiza i oszacowanie zagrożenia zidentyfikowanych ryzyk dla korzyści biznesowych, harmonogramu, jakości oraz wływu na organizacje. PRINCE2 wykorzystuje do tego model standardowy oparty na oszacowaniu prawdopodobieństwa wystąpienia ryzyka oraz skutków jego wystąpienia,
- **reakcja na ryzyko** – możliwe reakcje na wystąpienie ryzyka to: prewencja (zapobieganie wystąpieniu ryzyka lub problemu), redukcja (złagodzenie ryzyka poprzez działania zmniejszające prawdopodobieństwo jego wystapienia lub minimalizujące skutki wystapienia), przeniesienie (eliminowanie ryzyka poprzez oddanie lub współdzielenie odpowiedzialności za ryzko z innymi podmiotami), akceptacja (zgoda na funkcjonowanie w warunkach ryzyka) oraz utworzenie planów rezerwowych (*contingency*) – przewidziane środki w budżecie lub harmonogramie w przypadku materializacji ryzyka,

- **zarządzanie ryzykiem** – według metodyki powinno być proste i skuteczne, oparte na czterech możliwych działaniach: planowaniu akcji zapobiegawczych (analizie i wyborze odpowiednich akcji), przydzielaniu zasobów w planie projektu na cele akcji zapobiegawczych, monitorowanie i raportowanie podjętych działań zaradczych oraz *controlling* (podejmowanie decyzji wynikających z planu).

W odróżnienieniu od metodyki PMBoK, omówionej w nastepnym rozdziale, PRINCE nie włącza planowania w cykl zarządzania ryzykiem, nie rozdziela również oceny ryzyka dla poszczególnych czynników na jakościową oraz ilościową, a jedynie precyzuje te drugą.

Brytyjska agencja rządowa, która posiada prawa autorskie metodyki PRINCE2 jest również w posiadaniu opracowania pod nazwą M_o_R (*Management of Risk*). Opracowanie to ma na celu pomóc organizacjom zdefiniować skuteczny proces dla zarządzania ryzykiem nie tylko dla projektów, ale również na poziomie programów, operacyjnym oraz strategii organizacji. M_o_R stanowi: zbiór zasad, opis możliwych sposobów zaadoptowania tych zasad, opis procesów związanych z zarządzaniem ryzykiem a także sposób, w jaki te trzy elementy powinny być razem połaczone i wykorzystane w celu skutecznego zarządzania ryzykiem w danej organizacji. Na poziomie projektu opracowanie M_o_R jest mocno powiązane z metodyką PRINCE2 i definiuje skuteczne zarządzanie ryzykiem, jako systematyczne i prewencyjne działania polegające na identyfikowaniu ryzyka, analizie i ocenie bezpośredniego wpływu ryzyka, wyborze odpowiednich akcji zaradczych oraz monitorowaniu i ocenie wpływu tych akcji na stan ryzyka (*Management of Risk: Guidance for Practitioners, OGC, 2010*).

Przykładowe czynniki ryzyka podawane w opracowaniu metodyki PRINCE2 (Bradley, 2003, s. 217-220) można podzielić na kilka grup lub elementów i dotyczą one: **zarządzania projektem** (doświadczenia kierownika projektu, udziału klienta), **ludzi zaangażowanych w projekt** (zarówno od strony klienta jak i organizacji, doświadczenia w zespole, zmian personalnych, polityki jakości), **specyfiki projektu** (stopnia złożoności, zastosowania innowacyjnych technologii, dobrze zdefiniowanych wymagań od klienta, relatywnie krótkiego czasu trwania projektu, dobrego oszacowania zadań w ramach projektu, wpływu zmian na istniejące środowisko oraz infrastrukture), **dojrzałości organizacji** (rozumiany i audytowany system zarządzania jakością, wdrażanie usprawnień, korzystanie ze standardów zarządzania), **umowy i współpracy z klientem** (dobrze rozumiane i zdefiniowane wymagania, uzgodniony kontrakt, dobre relacje z klientem) oraz **innych dostawców** (znani i zaufani dostawcy oraz wdrożona polityka jakości u dostawcy).

6. Metodyka PMI

Project Management Body of Knowledge (PMBoK) to zbiór standardów wydany przez amerykański PMI (Project Management Instititue) dotyczący metodyki zarządzania projektami. Celem zarządzania ryzykiem według PMI jest zwiększenie prawdopodobieństwa wystąpienia i wykorzystania pozytywnych skutków ryzyka oraz zmniejszenie prawdopodobieństwa i złagodzenia skutków negatywnych. PMI podobnie jak PRINCE2 definiuje obszary związane z zarządzaniem ryzykiem, które są integralną częścią całej metodyki zarządzania projektami. PMBoK, jako kompendium wiedzy definuje cały cykl zarządzania ryzykiem przedstawiając dokładnie wejścia i wyjścia poszczególnych procesów wchodzących w skład modelu zarządzania ryzykiem, a dodatkowo w porównaniu do PRINCE2 proponuje całą gamę technik i narzędzi, które można wykorzystać w zarządzaniu ryzykiem.

Metodyka PMI definiuje sześć procesów związanych z zarządzaniem ryzykiem w dużej mierze pokrywających się z metodyką PRINCE2 (*A Guide to the Project Management Body of Knowledge*, PMI, 2009, s. 287-328):

- planowanie zarządzania ryzykiem – określa sposób planowania zarządzania ryzykiem w projekcie oraz rodzaje aktywności z tym związane. PMI w odróżnieniu od PRINCE2 jawnie włącza planowanie w cykl zarządzania ryzykiem,
- rozpoznawanie ryzyk – proces polegający na identyfikowaniu ryzyk mających wpływ na projekt oraz dokumentowanie i ich cech, PMI wyraźnie definiuje, że ryzyka mogą mieć charakter zarówno negatywny, jak i pozytywny dla projektu,
- przeprowadzanie jakościowej analizy ryzyk – proces pozwalający na ocene czynników ryzyka oraz na uszeregowanie ich pod kątem prawdopodobieństwa wystąpienia oraz ich potencjalnego wpływu na projekt,
- przeprowadzenie ilościowej analizy ryzyk – proces związany z analizą liczbową i pomiarem wpływu czynników ryzyka na dany projekt, PRINCE2 nie rozdziela tych dwóch procesów analizy ryzyka i traktuje je jako jeden wspólny proces,
- planowanie reakcji na ryzyko – proces definiuje sposoby na zwiększenie szansy i zmniejszenie zagrożeń dla realizacji celów projektu przy wykorzystaniu dostępnych technik i narzędzi,

- monitorowanie i sterowanie ryzykiem – proces wdrażania planów zapobiegania ryzykom, śledzenia i monitorowania wdrożonych akcji zapobiegania negatywnym skutkom ryzyka i wykorzystania pozytywnych ich stron oraz oceny skuteczności całego modelu zarządzania ryzykiem.

W metodyce PMI **planowanie zarządzania ryzykiem** jest przedstawione jako pierwszy proces, ze wskazaniem na jego bardzo ważną role w kontekście interakcji i wpływu na pozostałe procesy zarządzania ryzykiem, jak również na całość metodyki zarządzania PMI. Przygotowanie odpowiedniego planu zarządzania ryzykiem może mieć duży wpływ na zmianę każdego z istotnych elementów zarządzania projektem informatycznym: harmonogramu, budżetu, zakresu czy jakości. Zebrania i analizy planistyczne mogą być wykorzystane w celu skategoryzowania i oszacowania ryzyk (zbudowania macierzy prawdopodobieństwa i skutków) oraz określenia tolerancji interesariuszy wobec zidentyfikowanych ryzyk. W celu ułatwienia **rozpoznawania ryzyk** PMI proponuje takie narzędzia jak: przeglądy dokumentacji, różne techniki gromadzenia informacji (jak burze mózgów, technikę delficką pozwalającą na osiąganie konsensu w zespole ekspertów, ankiety, analizy przyczyn źródłowych), analizę list kontrolnych (bazującą na danych historycznych z podobnych projektów), analizę założeń, techniki oparte na diagramach (jak diagramy przyczynowo-skutkowe, schematy blokowe systemu, czy diagramy wpływów), analize SWOT (badającą projekt z perspektywy atutów, słabości, szans i zagrożeń) oraz opinie ekspertów. W celu **jakościowej analizy ryzyk** PMI proponuje wykorzystać ocenę prawdopodobieństwa i skutków wystapienia ryzyk, wyznaczyć macierz prawdopobieństwa i odpowiadających im skutków, ocenić jakość danych o ryzykach, skategoryzować ryzyka, ocenić pilność ryzyk lub zasięgnąć opinii ekspertów. W celu **ilościowej analizy ryzyk** odpowiednimi narzędziami mogą być: techniki gromadzenia i prezentacji danych (jak ankiety, rozkłady prawdopodobieństwa), techniki jakościowej analizy i modelowania ryzyk (jak analiza wrażliwości, analiza oczekiwanej wartości pieniężnej EMV bazująca na diagramie drzewa decyzyjnego, czy analiza wielokrotnych symulacji za pomocą techniki Monte Carlo) lub też opinie ekspertów. Metodyka proponuje kilka strategii **planowania reakcji na ryzyko** w zależności od jego charakteru: strategie dla zagrożeń (unikania, przeniesienia, łagodzenia, akceptacji), strategie dla szans (podjęcia, udostępnienia, wzmocnienia, akcpetacji), strategie reakcji warunkowych lub opinie ekspertów. Jako przykładowe narzędzia do monitorowania i sterowania ryzykiem metodyka poleca: ponowną ocene ryzyk, audyty ryzyk, analizę odchyleń i trendów, wyniki

pomiaru technicznego, analizę rezerw oraz zebrania poświęcone statusowi wykonania projektu (*A Guide to the Project Management Body of Knowledge*, PMI, 2009, s. 287-328).

7. Inne metodyki

Metodyki PRINCE2 oraz PMI to obecnie dwie najbardziej popularne metodyki, ale nie jedyne, które są wykorzystywane w zarządzaniu projektami oraz w zarządzaniu ryzykiem.

Dwie kolejne metodyki zostały stworzone w Europie: **APM** (*Association for Project Management*) oraz **PCM** (*Project Cycle Management*). Metodyka APM przedstawia model zarządzania ryzykiem oraz model oceny ryzyka, które są bardzo podobne do opisanych w metodyce PRINCE2 oraz PMI. Metodyka PCM jest troche odmienna w swojej postaci od opisanych powyżej i nadal jest w trakcie modyfikacji oraz uzupełniania. Metodyka PCM definiuje pięć faz cyklu życia projektu: programowania, identyfikacji, formułowania, wdrażania oraz ewaluacji i audytu. W fazie identyfikacji, formułowania i wdrażania istotną rolę stanowi analiza czynników ryzyka. Jest ona jednak bardziej integralną częścią metodyki niż osobnym procesem jak ma to miejsce w pozostałych metodykach. Metodyka PCM zajmuje się tylko czynnikami zewnętrznymi ryzyka, co też znacząco odróżnia ją od innych (Korczowski, 2009, s. 34).

Inną metodyką podobną do PRINCE2 i PMI oraz uwzględniającą działania związane z zarządzaniem ryzykiem jest **RAMP** (*Risk Analysis and Management of Projects*). Podstawą tej metodyki jest: klasyfikacja wszystkich rodzajów ryzyka, ocena ryzyka oraz ograniczenie ich wpływu na projekt (Chong, Brown, 2001, s. 258-259).

CMM (*Capability Maturity Model*) to model dojrzałości organizacyjnej stosowany w celu poprawy działań operacyjnych, w tym do zarządzania projektami. Jeden z obszarów dotyczy zarządzania ryzykiem, które jest analizowane w kontekście: definiowania strategii zarządzania ryzykiem, identyfikowania i analizy czynników ryzyka oraz wdrożenia planów łagodzących ryzyko. Model ten udziela praktycznych wskazówek, opisuje możliwe do wykorzystania techniki, w szczególności mające zastosowanie w projektach informatycznych związanych z tworzeniem i testowaniem oprogramowania (Korczowski, 2009, s. 34-35). Ze względu na problematyczne zastosowanie CMM w niektórych aspektach zarządzania projektami informatycznymi powstał model CMMI (Capability Maturity Model Integration), który jest szeroko uznanym modelem poprawy procesów tworzenia oprogramowania w organizacjach.

ROZDZIAŁ III – ZARZĄDZANIE RYZYKIEM W PROJEKTACH ZWIĄZANYCH Z TWORZENIEM I TESTOWANIEM OPROGRAMOWANIA

8. Ryzyko w testowaniu oprogramowania i zapewnianiu jakości

Głównym celem testowania oprogramowania jest zidentyfikowanie wszystkich jego wad, które nie będą akceptowalne z perspektywy klienta i które świadczyłyby o złej jakości tego oprogramowania. Testowanie oprogramowania ma pomóc ocenić jakość oprogramowania na danym etapie projektu i dać możliwość podjęcia decyzji o tym, czy oprogramowanie nadaje się do przekazania do klienta (realizacja celu projektu i uzasadnienia biznesowego). Podjęcie takiej decyzji jest nierozerwalnie związane z ryzykiem, ponieważ nie istnieje taki moment w projekcie, kiedy można stwierdzić, że wszystko zostało już przetestowane i sprawdzone. Tworzenie i testowanie oprogramowania wiąże się z wieloma czynnikami ryzyka i podejmowaniem wielu decyzji obarczonych ryzykiem, stąd niezmiernie ważne jest odpowiednie zarządzanie ryzykiem w tego typu projektach.

Już sama specyfika projektów informatycznych oraz biznesu, który jest z nimi związany jest źródłem bardzo dużego ryzyka, które, jak pokazuje życie, skutkuje duża liczbą projektów informatycznych zakończonych niepowodzeniem. Chcąc uzyskać bezbłędne oprogramowanie i tym samym zapewnić mu odpowiednią jakość możemy spowodować zmiany w budżecie i harmonogramie projektu (dodatkowe koszty lub opóźnienia). Jakość jest tu rozumiana jako zdolność oprogramowania o określonych właściwościach do spełnienia wymagań klienta oraz pozostałych interesariuszy. Dotyczy to również produktu, systemu lub procesu, którego częścią jest to oprogramowanie. Powraca pytanie i konieczność podjęcia decyzji, kiedy zakończyć testowanie. Decyzja ta niezależnie od ilości zaplanowanych i wykonanych testów zawsze będzie związana z ryzykiem. Ryzko to może być dwojakiego rodzaju: **techniczne** – związane z oceną prawdopodobieństwa wystapienia błedu w stworzonym oprogramowaniu oraz szansy na zmniejszenie tego ryzyka poprzez wydłużenie okresu testowania i wykonanie kolejnych testów oraz **rynkowe** – związane z kosztem wydłużenia testowania i tym, co możemy stracić wydłużając projekt (Bereza-Jarociński B., Szomański B. 2009, s. 31).

Sztuką zarządzania ryzkiem w tego typu projektach jest takie planowanie testowania i prowadzenie działań w trakcie trwania projektu, które pozwoli na osiągnięcie akceptowalnego poziomu ryzyka w założonych ramach projektu (budżet, zakres, czas,

jakość), a tym samym na podjęcie decyzji o zakończeniu testowania i osiągnięciu celu projektu (gotowe oprogramowanie odpowiedniej jakości). Testowanie jest niezbędne w celu zapewnienia jakości i powinno być prowadzone w trakcie całego czasu trwania projektu związanego z tworzeniem oprogramowania, kwestią planowania testów pozostaje oszacowanie ilości koniecznych testów do wykonania oraz wykonanie ich w najbardziej optymalny sposób (przede wszystkim pod względem kosztów) (*własne doświadczenia z prowadzonych projektów związanych z testowaniem*).

9. Zarządzanie ryzykiem w tworzeniu i testowaniu oprogramowania

9.1. Podejście do planowania zarządzania ryzykiem

Planowanie testów jest związane z jeszcze większym ryzykiem niż samo tworzenie oprogramowania. Rzadko kiedy przygotowany plan testów ma szanse wydarzyć się dokładnie tak, jak został stworzony na początku przez kierownika projektu. W większości sytuacji wpływ na to ma ryzyko związane z tworzeniem oprogramowania. Dobrze przygotowany plan testów musi uwzględniać ryzyka związane z tworzonym oprogramowaniem, jak na przykład: opóźnienia dostawy oprogramowania do testów systemowych przy jednoczesnym zachowaniu terminu końcowego projektu, słabą jakość oprogramowania dostarczanego w pierwszych etapach powodującą opóźnienia lub przesunięcia w harmonogramie testów, dużą liczbe błedów utrudniającą testowanie w początkowej fazie projektu, czy współdzielenie środowiska testowego z zespołem poprawiającym oprogramowanie (Bereza-Jarociński B., Szomański B. 2009, s. 121).

Planowanie powinno też uwzględniać kryteria podjęcia decyzji o zakończeniu testowania, które jest w zasadzie decyzją biznesową. Ryzyko nieznalezionych błędów w trakcie testowania pozostanie zawsze po zakończeniu projektu. Kryteria decyzji o zakończeniu testowania, określenie poziomu akceptowalnego ryzyka oraz tolerancji dla tego ryzyka powinny być ustalone wspólnie z klientem oraz interesariuszami bazując na ocenie ryzyka technicznego w oparciu o wyniki testów. W oszacowaniu jakości oprogramowania oraz zdefiniowaniu kryteriów pomocne mogą być metryki zbierane w trakcie testowania, takie jak: miary pokrycia wymagań i kodu, wykonany procent testów oraz zadań związanych z testami, liczba nierozwiązanych zgłoszeń błędów, czy liczba nieznanych jeszcze błędów (na podstawie funkcji najlepiej pasującej do krzywej określającej skumulowaną ilość dotychczas znalezionych błędów) (Bereza-Jarociński B., Szomański B. 2009, s. 123).

9.2. Czynniki ryzyka związane z tworzeniem i testowaniem oprogramowania

9.2.1. Narzędzia i techniki do identyfikacji ryzyka

Istnieje wiele narzędzi i technik, którymi kierownik projektu tworzącego lub testującego oprogramowanie może wspomóc się w procesie identyfikacji ryzyk. Wybór odpowiedniej metody powinien być dokonany pod kątem specyfiki danego projektu oraz potencjalnych grup ryzyk z nim związanych. Kierownik projektu może skorzystać z kilku metod, jeśli uzna, że wyniki jednej metody nie dadzą mu wystarczającej informacji o istniejących ryzykach w projekcie. Należy jednak pamiętać, że sam wybór metody, jak i ilość użytych metod wpływa na budżet planowania danego projektu (zarządzanie ryzykiem również jest kosztem w projekcie i należy o tym pamiętać).

W projektach związanych z tworzeniem i testowaniem oprogramowania najczęściej stosowane metody to (Korczowski, 2009, s. 102-152):

- listy kontrolne – jest to skuteczna technika bazująca na przegladaniu listy ryzyk z podobnych projektów realizowanych w przeszłości lub innych źródeł informacji. W literaturze można spotkać dedykowane listy kontrolne dla zespołów tworzących i testujących oprogramowanie. Technika jest prosta i nie wymaga dużych kosztów,
- sesje analityczne i burze mózgów – jest to cała grupa technik polegających na pozyskaniu informacji o potencjalnych źródłach ryzyka (np. poprzez ankiety, analizę przyczyn źródłowych lub analizę założeń). W przypadku burzy mózgów jest to nieograniczona wymiana informacji o możliwych czynnikach ryzyka wśród osób związanych z projektem lub w gronie ekspertów.
- technika delficka – przeprowadzana jest anonimowo w gronie ekspertów. Organizator gromadzi odpowiedzi od poszczególnych specjalistów, zestawia je razem, uzupełniając o swoje kometarze i pytania. Wyniki są wysyłane wszystkim zaangażowanym i na drodze wielokrotnego powtarzania osiągany jest konsensus,
- techniki oparte na diagramach – bardzo popularne w projektach informatycznych ze względu na graficzną prezentacje często skomplikowanych zależności przyczynowo-skutkowych w tworzonych systemach oraz graficzną prezentacje sposobu wyboru i podejmowania decyzji (drzewa decyzyjne),
- metody eksperckie – wyniki bazują na subiektywnych ocenach niezależnych ekspertów, którzy posiadają doświadczenie z podobnych przedsięwzięć.

9.2.2. Przykładowe czynniki ryzyka

Poniżej przedstawiono przykładową listę ryzyk dla projektów związanych z tworzeniem i testowaniem oprogramowania oraz sposób ich pogrupowania – odpowiednio grupa ryzyka, jego źródło i charakter (Schmidt, R.C., Lyytinen, K., Keil, M., and Cule, P. 2001, s. 5-36 oraz *własne doświadczenia z prowadzonych projektów związanych z testowaniem*):

- środowisko organizacji – źródłem jest środowisko, a przyczynami mogą być niewłaściwe zmiany w działalności politycznej lub gospodarczej organizacji, tzn. projekty nie mające właściwego uzsadanienia biznesowego zgodnego ze strategią organizacji (np. powody polityczne) oraz niezgodność wymaganych zmian w procesach biznesowych z kulturą organizacji,
- sponsor i właściciel – źródłem jest decyzyjność, a przyczynami może być brak zgody dla kierownika projektu na realizacje projektu lub brak zaufania oraz słabe relacje z właścicielami lub użytkownikami systemu,
- zarządzanie relacjami – źródłem są relacje z klientami, a przyczynami mogą być brak zaufania lub słabe zaangażowanie ze strony klienta oraz rozbieżności między oczekiwaniami różnych klientów, a tym, co jest dostarczane w ramach projektu,
- zarządzanie projektem – źródłem jest zarządzanie projektem, a przyczyną może być słaba lub niewydajna strategia zarządzania i realizowania planu projektu. Może być to spowodowane brakiem właściwego zarządzania zmianą, brakiem umiejętności, skuteczności i znajomości metodyki zarządzania, niewłaściwym nadzorowaniem realizacji projektu lub niewłaściwym sposobem zarządzaniem ryzykiem,
- zakres – źródłem jest zakres systemu, a przyczyną może być niejasny, ciągle zmieniający się lub tylko częściowo zrozumiały zakres lub cel do realizacji,
- wymagania – źródłem są wymagania, a przyczynami mogą być niezrozumiałe, nieodpowiednie lub nieprecyzyjne wymagania oraz brak lub słaby system do zarządzania wymaganiami oraz walidacji wymagań,
- finansowanie – źródłem jest zarządzanie zasobami, a przyczyną może być nierealistyczny budżet, niedoszacowanie lub błędne oszacowanie wymaganych zasobów do realizacji projektu,

- harmonogramowanie – źródłem jest wykorzystanie zasobów, a przyczynami mogą być słabe zarządzanie wykorzystaniem zasobów i zapotrzebowaniem na zasoby oraz nierealistyczne terminy ukończenia zadań,
- proces tworzenia – źródłem jest proces, a przyczyną może być brak lub niewłaściwy proces prowadzący do problemów z jakością (brak dokumentacji, brak odpowiedniego planowania i wykonania testów),
- pracownicy – źródłem są umiejętności, a przyczynami może być brak odpowiednich umiejętności, wiedzy, doświadczenia zarówno w zespole, jak i u kierownictwa projektu,
- zespół – źródłem jest zespół, a przyczynami może być brak odpowiedniej ilości osób w zespole lub brak kluczowych osób z wymaganymi umiejętnościami oraz ciągłe lub niedopowiednie zmiany personalne w zespole,
- technologia – źródłem jest technologia, a przyczyną może być niewystarczające zrozumienie wybranej technologii, wprowadzenie zupełnie nowej i jeszcze nie sprawdzonej technologii lub brak stabilnej architektury technicznej,
- zależności zewnętrzne – źródłem jest środowisko, w którym realizujemy projekt, a przyczyną jest brak lub słabe zarządzanie lub nadzór nad zewnętrznymi dostawcami,
- planowanie – źródłem jest planowanie, a przyczynami może być brak planowania lub niewłaściwe planowanie.

W badaniach przedstawionych w artykule (Schmidt, R.C., Lyytinen, K., Keil, M., and Cule, P. 2001, s. 5-36) wszystkie ryzyka zostały przeanalizowane, ocenione, uszeregowane i spriorytetyzowane w celu zwrócenia uwagi kierownictwa projektów informatycznych na najważniejsze z nich i są to:

1) brak decyzji i zatwierdzenia projektu przez komitet sterujący,
2) brak zatwierdzenia projektu ze strony użytkownika/klienta,
3) niezrozumiałe wymagania,
4) brak zaangażowania ze strony użytkownika/klienta,
5) brak w zespole osób z wymaganymi umiejętnościami,
6) brak zatwierdzonych wymagań przez klienta oraz interesariuszy,

7) zmiany dotyczące zakresu i celów,
8) wprowadzanie nowych technologii,
9) błędne zarządzanie oczekiwaniami klientów,
10) braki zasobów w zespole lub źle dobrany zespół,
11) konflikty pomiędzy użytkownikami z różnych działów.

9.3. Strategia testowania zmniejszająca poziom ryzyka

Na etapie planowania zarządzania ryzykiem ustalone zostały z komitetem sterującym poziomy akceptacji ryzyka w projekcie oraz tolerancje dla tego ryzyka. Na tym samym etapie kierownik tworzy strategię testowania zatwierdzaną przez komitet sterujący. Strategia powinna uwzględniać potencjalne ryzyko, które może się pojawić w trakcie trwania projektu oraz akcje w ramach zadań testowych mające na celu znaczne ograniczenie możliwości zmaterializowania się ryzyka. Na każdym z etapów projektu, w którym zidentyfikowaliśmy nowe ryzyka musimy oszacować prawdopodobieństwo wystąpienia i potencjalne straty dla wszystkich ryzyk z rejestru ryzyka oraz wybrać te, które nie spełniają kryteriów akceptacji. Dla tych ryzyk konieczne jest zaplanowanie dodatkowych akcji w celu złagodzenia ryzyka lub/oraz przygotowanie planów awaryjnych na wypadek materializacji ryzyka. Działania te najczęściej będą wymagać zmian w planach zarządzania projektem (wymaga to najczęściej aktualizacji budżetu, zakresu, czasu, bądź jakości). Dobrą praktyką jest posiadanie rezerw (tzw. *contingency*) w planach projektu na cele związane z zarządzaniem ryzykiem, które to powinno być częścią strategii testowania. Wybór i zaplanowane akcje nie powinny przekroczyć kosztów potencjalnych strat spowodowanych materializacją danego ryzyka, w przeciwnym wypadku należy jeszcze raz ocenić ryzyko lub dokonać innego wyboru środków zapobiegawczych.

9.4. Monitorowanie ryzyka związanego z jakością oprogramowania

Doświadczenie pokazuje, że testowanie oraz ocena jakości oprogramowania niesie ze sobą dużą ilość trudnych do przewidzenia lub wręcz niemożliwych do przewidzenia sytuacji wymagających systematycznego i ciągłego zarządzania ryzykiem w projekcie. Dużo łatwiej i dużo mniejszym kosztem jesteśmy w stanie zarządzać ryzykiem w projekcie, jeżeli każdego dnia w trakcie trwania projektu będziemy podejmować decyzje, które w pośredni sposób będą uwzględniać ryzyko, które pojawia się na horyzoncie.

ROZDZIAŁ IV – TESTOWANIE OPROGRAMOWANIA UWZGLĘDNIAJĄCE RYZYKO (RISK BASED TESTING)

W projektach związanych z testowaniem oprogramowania jednym z możliwych podejść do zarządzania projektem jest wykorzystanie metodyki testowania uwzględniającego ryzyko (*risk based testing*). Główna idea tej metodyki to koncentracja planowania i wykonania zadań związanych z testowaniem na obszarach o największym ryzyku, bazująca na analizie potencjalnych zagrożeń lub awarii spowodowanych przez tworzone oprogramowanie.

Testowanie na podstawie ryzyka polega na takim prowadzeniu projektu, aby systematycznie i na bieżąco identyfikować oraz przewidywać potencjalne ryzyka w projekcie, oceniać ich prawdopodobieństwo wystapienia i konsekwencje dla użytkownika oraz podejmować działania związane z testowaniem, które pozwolą zmniejszyć to prawdopodobieństwo lub złagodzić negatywne konsekwencje. Cztery podstawowe parametry takiego testowania to: prawdopodobieństwo znalezienia błędu (badanie obszarów, w których spodziewamy się błędów), konsekwencje awarii (ich wpływ na użytkownika), prawdopodobieństwo użycia (ukierunkowanie na funkcjonalności najczęściej wykorzystywane przez użytkownika) oraz łatwość testowania (uwzględniające koszt i czas poświęcony na wykonanie testów w stosunku do możliwego wpływu na użytkownika) (Bereza-Jarociński B., Szomański B. 2009, s. 129, 164-170). Działania podejmowane w projekcie powinny odpowiadać na zidentyfikowane w nim ryzyka w nastepujący sposób:

- wysiłek przeznaczony na testowanie, wybrane techniki testowania, harmonogram zadań oraz rozwiązywane błędy powinny odpowiadać poziomom ryzyk,
- planowanie i zarządzanie testowaniem powinno polegać na łagodzeniu ryzyk w zależności od ich poziomu oraz uruchamianiu niezbędnych planów awaryjnych,
- raportowanie wyników oraz statusu projektu powinno odnosić się do zidentyfikowanych obszarów ryzyka.

Idea metodyki *risk based testing* zakłada, że testowanie będzie realizowane w całym cyklu tworzenia oprogramowania (może to być skorelowany projekt w ramach jednego programu). W szczególności testowanie powinno być częścią planowania projektu informatycznego w celu stworzenia listy ryzyk technicznych i biznesowych wraz z ich priorytetami. Pomijanie testów w fazie planowania jest tu często spotykanym błędem.

10. Przyczyny wyboru metodyki testowania uwzględniającego ryzyko

Specyfiką projektów związanych z tworzeniem i testowaniem oprogramowania jest bardzo duża złożoność technologiczna produktów, często związana z presją czasu ze strony rynku i konkurencji, co sprawia, że ryzko biznesowe dla tych projektów jest na bardzo wysokim poziomie. Z powyższych względów rosną wymagania odnośnie wyboru metodyki testowania oraz sposobu zapewnienia jakości, która z jednej strony musi wystarczająco zminimalizować ryzyko słabej jakości oprogramowania lub braku akceptacji ze strony klienta, a z drugiej zapewnić, że koszty poświęcone na testowanie nie są marnotrawione i są niezbędne dla realizacji celu projektu. Metodyka testowania oparta na ryzyku ma za zadanie pozwolić zrozumieć zarządowi organizacji jakie jest bieżące ryzyko wdrożenia, bądź nie wdrożenia tworzonego oprogramowania, które ma dostarczyć określonych korzyści biznesowych. W projektach związanych z tworzeniem oprogramowania nigdy nie będzie wystarczająco dużo czasu, by przeprowadzić wszystkie testy. Wybór metodyki *risk based testing* ma dać gwarancje wykonania najbardziej krytycznych testów oraz pozwolić kierownikowi projektu podejmować najbardziej optymalne decyzje dotyczące harmonogramu testów minimalizujące ryzko niepowodzenia całego projektu (*Because what you do the rest of the week should hold no surprises*).

11. Potencjalne ryzyka związane z oprogramowaniem

Testowanie uwzględniające ryzyko bazuje na heurystycznej metodzie identyfikowania potencjalnego ryzyka. Do problemu można podejść na dwa różne, wzajemnie uzupełniające się sposoby (*James Bach on Risk-Based Testing*):

- **poprzez analizę wymagań oraz zidentyfikowanie możliwych ryzyk** na podstawie odpowiedzi na pytania dotyczące: luk w oprogramowaniu (jego słabości i potencjalnych awarii), zagrożeń (czynników, które mogą doprowadzić do ich wystapienia) oraz strat (kto lub co jest narażone na straty i jakiego rodzaju),
- **poprzez przegląd potencjalnych obszarów ryzyka z podobnych projektów** i dopasowaniu ich do bieżącej sytuacji. Najczęściej przegląda się różne kategorie kryteriów jakości oprogramowania jak: działanie funkcjonalności, niezawodność, użyteczność, wydajność, łatwość wdrożenia, zgodność ze środowiskiem, koszty wsparcia klienta, testowalność, łatwość utrzymania, przenaszalność do nowej technologii, łatwość dostosowania do potrzeb różnych użytkowników (języki).

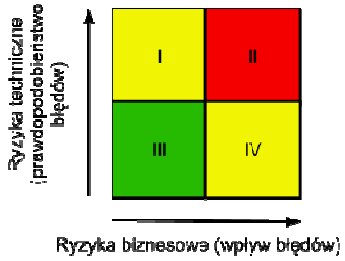
12. Idea działania metodyki testowania uwzględniającego ryzyko

Metodyka testowania uwzględniającego ryzyko opiera się na klasycznym cyklu zarządzaniem ryzykiem omówionym w poprzednich rozdziałach. Działanie metodyki może być opisane w nastepujących krokach (*Because what you do the rest of the week should hold no surprises*):

1) **zebranie wymagań testowych** (określenie zbioru wymagań systemu, które powinny być pokryte testami, uszeregowanie tych wymagań z punktu korzyści biznesowych oraz zatwierdzenie tak określonego zbioru przez interesariuszy),

2) **oszacowanie poziomów ryzyka** (dla powyższego zakresu wymagań należy przeprowadzić ich uszczegółowienie oraz określić poziom ryzyka z nimi związany w gronie interesariuszy projektu oraz biznesu – rysunek 3 przedstawia macierz ryzyka związaną z produktem, w którym pozycja ryzyka w macierzy odpowiada wadze danego ryzyka oszacowanego na podstawie prawdopodobieństwa znalezienia błedów podczas testowania oraz wpływu tych błędów na klienta),

Rysunek 3. Macierz ryzyka produktu



Źródło: (Practical Risk-Based Testing)

3) **planowanie testów** (przygotowanie i uzgodnienie planu oraz harmonogramu testów dla określonych wcześniej wymagań bazując na analizie priorytetów obszarów testowych oraz wagach ryzyka w danym obszarze; w pierwszej kolejności powinny być wykonane testy o najwyższym priorytecie),

4) **zapewnienie zgodności działań z wymaganiami biznesowymi** (analiza planu testów z perspektywy priorytetów biznesowych, uruchomienie procesu testowego zgodnie z ustalonymi prioryetami),

5) **monitorowanie pokrycia testowego** (weryfikacja zgodności pokrycia testowego z ustalonymi wcześniej poziomami ryzyka, weryfikacja pokrycia testowego poprzez analizę kodu źródłowego, oszacowanie poziomów ryzyka dla nowo pojawiających się błędów, modyfikacja priorytetów oraz ponowne uszeregowanie obszarów testowych),
6) **decyzja o przejściu do kolejnego etapu** w odniesieniu do oceny ryzka biznesowego (wykonanie analizy statystycznej związanej z testowaniem, podsumowanie wyników w kontekście poziomów ryzyka pokrytych testami oraz przypisanie komentarzy do poziomów ryzyka nie pokrytych testami),
7) **zakończenie etapu projektu** (lub całości projektu i wdrożenie u klienta).

W metodyce tej najbardziej istotna i wymagająca najwięcej wysiłku od strony zarządzania ryzykiem jest faza planowania (do momentu uruchomienia procesu wykonania testów i jego monitorowania). Bardziej szczegółowo może ona wyglądać następująco (*Practical Risk-Based Testing*):

- **etap planowania** (zebranie dokumentacji z wymaganiami, wybranie techniki oraz przeprowadzenie identyfikacji ryzyk, określenie współczynników prawdopodobieństwa znalezienia błędów w oprogramowaniu oraz wpływu tych błędów na użytkownika, wylicznie wag dla każdego ryzyka i umieszenie ich w macierzy ryzyka dla produktu, określenie listy interesariuszy projektu w celu wspólnej oceny przygotowanego planu i analizy ryzyka),
- **rozpoczęcie, tzw. *kick-off meeting*** (przedstawienie w formie szkolenia wszystkim zainteresowanym jak będzie wyglądał proces testowania, wyjaśnienie wątpliwości związanych z listą ryzyk oraz ich wagami, ustalenie priorytetów dla testowanych obszarów na podstawie wag ryzyka, ustalenie reguł działania, które powinno być zatwierdzone przez wszystkich interesariuszy),
- **indywidualne przygotowanie** (każdy z interesariuszy dokonuje indywidualnej oceny wyników i dokumentuje ją),
- **zebranie indywidualnych wyników** (sprawdzenie ich poprawności, kompletności oraz upewnienie się, że wszyscy niezbędni interesariusze dostarczyli swoje opracowania, następnie przetworzenie i podsumowanie zebranych wyników),

- **spotkanie decyzyjne** (prezentacja wyników wszystkim zainteresowanym, omówienie listy otwartych problemów wraz z próba osiągnięcia konsensusu),
- **zaproponowanie startegii testowej** (na bazie powyższych ustaleń oraz poziomów ryzyka wybierana jest odpowiednia strategia testowa najlepiej dopasowana do otrzymanych wyników).

12.1. Przypadek użycia metodyki

Przedstawiony dalej przypadek użycia metodyki *risk based testing* pochodzi z doświadczeń autora z projektów związanych z testowaniem oprogramowania oraz z *Practical Risk-Based Testing*. Sposób działania metodyki w poszczególnych etapach:

- **faza początkowa** (identyfikacja ryzyk odnoszących się tylko do produktu, gdzie należy zwrócić szczególną uwagę na odfiltrowanie ryzyk dotyczących realizacji projektu, oszacowanie współczynników prawdopodobieństwa wystąpienia oraz wpływu na klienta, przygotowanie planu łagodzenia ryzyka oraz przypisanie konkretnych akcji, które mają to spowodować),
- **faza realizacji projektu** (wykonanie zaplanowanych akcji i monitorowanie postępu w łagodzeniu istniejących ryzyk, identyfikacja nowo pojawiających się ryzyk w trakcie trwania projektu, oszacowanie ich wagi, przygotowanie planu łagodzenia oraz dodanie ich do bieżącej listy ryzyk),
- **koniec każdego etapu/tygodnia** (przygotowanie raportu zawierającego tabele z aktualnym postepem w łagodzeniu ryzyk, tabela powinna zawierać zaktualizowane prawdopodobieństwa dla danego ryzyka oraz przewidywany postęp łagodzenia ryzyka w następnym etapie/tygodniu; przygotowanie obejmuje również macierze ryzyk ze zaktualizowanymi wartościami wag),
- **koniec projektu** (przygotowanie ostatecznej macierzy ryzyka dla produktu z osiągniętymi wagami, omówienie ryzyk o najwyższych poziomach).

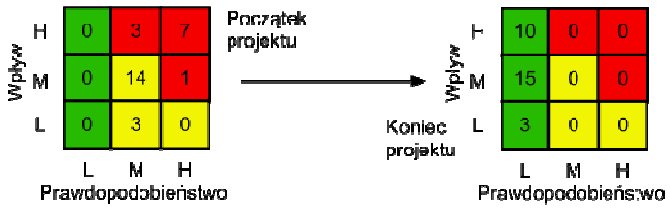
W celu identyfikacji ryzyk zorganizowano burze mózgów z wszystkimi zainteresowanymi (reprezentacja zespołu tworzącego oprogramowanie, doświadczeni testerzy zaznajomieni z wymaganiami, kierownictwo zespołu tworzącego oprogramowanie, kierownik programu w celu identyfikacji ryzyk biznesowych, kierownik zespołu testowego, autorzy wymagań, reprezentacja biznesu oraz pozostali interesariusze projektu). Rezultatem spotkania była tabela ze zdefiniowanymi ryzykami. Każde ryzyko w tabeli zawierało cztery cechy: **opis**

ryzyka (definicja i opis ryzyka w odniesieniu do zmian objętych wymaganiami), **potencjalny wpływ na klienta** (wartości przydzielono do jednej z trzech grup i oznaczono kolorami: wysoki wpływ – czerwony, średni – żółty oraz niski - zielony), **prawdopodobieństwo wystapienia problemu** (wartości przydzielono do jednej z trzech grup i oznaczono kolorami: wysokie prawdopodobieństwo – czerwony, średnie – żółty oraz niskie – zielony) oraz **plan łagodzenia ryzyka** (planowane i przypisane akcje w celu złagodzenia ryzyka).

Proces łagodzenia ryzyka oraz decyzje z nim związane przebiegały następująco:

- **decyzja o zwiększeniu prawdopodobieństwa wystąpienia ryzyka** mogła nastąpić w wyniku znalezienia większej liczby błędów niż przewidywano znaleźć w danym obszarze lub z powodu niezrealizowanych zadań w harmonogramie (zablokowane, opóźnione lub przewidywane opóźnienia zadań z różnych przyczyn),
- **decyzja o zmniejszeniu prawdopodobieństwa wystąpienia ryzyka** mogła nastąpić w wyniku znacznie mniejszej liczby znalezionych błędów niż przewidywano znaleźć w danym obszarze, niskiego współczynnika błędów w stosunku do przewidywanego, znacznego zaawansowania postępu zadań podjętych w wyniku łagodzenia ryzyka bez zwiększonej liczby znalezionych błędów podczas ich realizacji lub też wpływ znajdowanych błędów był oceniany jako niewielki dla klienta/użytkownika. Rysunek 4 przedstawia oczekiwaną zmianę w macierzy ryzyka produktu pomiędzy początkiem i końcem projektu.

Rysunek 4. Zmiany w macierzy ryzyka produktu



Źródło: opracowanie własne

Liczby w macierzy ryzyka odzwierciedlają liczbę ryzyk z listy wszystkich zidentyfikowanych o danej wadze (określonej prawdopodobieństwem i wpływem na klienta za pomocą poziomów i kolorów: H, M, L). Ponieważ wpływ ryzyka na klienta

pozostaje niezmieniony w trakcie trwania projektu, a zmienia się tylko jego prawdopodobieństwo w wyniku łagodzenia ryzyka to w miarę realizacji harmonogramu oczekiwane jest przemieszczanie się ryzyk w macierzy w lewą stronę wraz ze zmianą koloru (jak na rysunku 4 i w tabeli 2). Prawdopodobieństwo ryzyka zawsze pozostanie większe od zera. Celem jest zmniejszenie jego wartości na koniec projektu (TK w tabeli 2) do wartości oczekiwanej i akceptowalnej przez klienta. Decyzja o wdrożeniu u klienta jest rekomendowana, jeśli w projekcie pozostały już tylko ryzyka o poziomie L (lub M, ale zaakceptowane przez interesariuszy projektu).

12.2. Raportowanie stanu projektu z wykorzystaniem metodyki

Przykład raportowania stanu projektu z wykorzystaniem metodyki prezentuje tabela 2. Kolory ryzyk w pierwszej kolumnie są niezmienne i oznaczają wpływ ryzyka na klienta. Na starcie projektu (T1) wszystkie ryzyka są domyślnie niezłagodzone – kolor czerwony (nie wykonaliśmy jeszcze testów). W trakcie trwania projektu zmieniają swoje prawdopodobieństwo i kolor pod wpływem pomyślnego wykonania testów. Ostatnia kolumna oznacza aktualny stan decyzji do rekomendacji wdrożenia u klienta.

Tabela 2. Raportowanie stanu projektu poprzez zmiane poziomu ryzyk

Opis ryzyka	T1	T2	T3	T4	T5	T6	T7	TK
Ryzyko 1	Komentarz	Komentarz						L
Ryzyko 2	Komentarz	Komentarz	Plan	Plan				M
Ryzyko 3	Komentarz	Komentarz	Plan	Plan	Plan	Plan		H
Ryzyko 4	Komentarz	Komentarz	Plan					H
Ryzyko 5	Komentarz	Komentarz	Plan	Plan				H

Źródło: opracowanie własne

13. Najważniejsze zalety metodyki

Cztery najwazniejsze korzyści z zastosowania metodyki testowania opartego na ryzyku:

1) zwiększa prawdopodobieństwo wcześniejszego znalezienia błędów,

2) pozwala wydajniej przydzielić zasoby mając na uwadze ryzyko wdrożenia,

3) ułatwia kierownictwu organizacji podejmowanie decyzji odnośnie wdrożenia,

4) zwiększa wydajność pracy zespołu ukierunkowując go na cel projektu.

PODSUMOWANIE

Obecnie wiele projektów informatycznych, w tym dotyczących tworzenia oprogramowania, kończy się niepowodzeniem z różnych oficjalnie podawanych przyczyn: słabej jakości produktu, rozbieżności produktu z oczekiwaniami klientów, zmian rynkowych zachodzących w trakcie trwania projektu, błędów popełnianych w zarządzaniu takimi projektami oraz wielu innych. W niniejszej pracy przedstawione zostały zarówno teoretyczne, jak i praktyczne aspekty zarządzania ryzykiem związanym z zapewnieniem jakości. Praca przedstawia również praktyczny sposób wykorzystania metody zarządzania ryzykiem w testowaniu oprogramowania (*risk based testing*) na podstawie udziału i doświadczeń autora w projektach związanych z testowaniem oprogramowania. Przegląd literatury, bardziej szczegółowa analiza tych projektów oraz własne doświadczenia zawodowe opisane w tej pracy pokazują, że wiele oficjalnych przyczyn niepowodzenia projektów związanych z tworzeniem oprogramowania ma swoje źródło w ryzyku, które podejmuje się zawsze w tego typu projektach. Ryzyko w projektach dotyczących tworzenia oprogramowania jest o wiele wieksze niż w innego typu projektach, głównie ze względów dużej złożoności technologicznej produktu, presji rynkowej odnośnie czasu wdrożenia, wysokich oczekiwań co do jakości produktu, trudnych do oszacowania korzyści biznesowych, czy problemów z oszacowaniem potrzebnych zasobów i zarządzania tymi zasobami. Brak zarządzania tego typu ryzykiem lub niewłaściwe zarządzanie ryzykiem (w tym niewłaściwy wybór metodyki) od samego początku projektu, a nawet od momentu rozważania decyzji o podjęciu się danego projektu jest przyczyną wielu niepowodzeń tych projektów. Ze względów korzyści biznesowych, przewagi rynkowej nad konkurencją, czy dbania o wizerunek organizacji powody te nie są lub nie mogą być zazwyczaj oficjalnymi przyczynami podawanymi do informacji publicznej. Osobnym polem badań mogłoby być przeprowadzenie odpowiednio sformułowanej ankiety wśród organizacji zajmujących się tworzeniem oprogramowania, która zbadałaby źródła i przyczyny niepowodzenia projektów. Podjęcie ryzyka okazuje się najczęściej konieczne i nieuniknione, jeżeli chcemy uzyskać korzyści biznesowe. Tym samym zarządzanie ryzykiem to jedno z najważniejszych działań, które warto i wręcz powinno się podjąć oraz rozwijać w projektach dotyczących tworzenia i testowania oprogramowania, chcąc zwiększyć szanse oraz ilość projektów zakończonych sukcesem i tym samym osiągnąć cele i korzyści biznesowe z nimi związane.

BIBLIOGRAFIA

Bereza-Jarociński B., Szomański B. 2009, Inżynieria oprogramowania. Jak zapewnić jakość tworzonym aplikacjom, Helion, Gliwice.

Boehm, B. W. 1991, Software Risk Management: Principles and Practices, "IEEE Software", Vol. 8 No. 1.

Bradley K. 2003, Podstawy metodyki PRINCE2, CRM, Warszawa.

Chong Y.Y., Brown E.M. 2001, Zarządzanie Ryzykiem, Oficyna Ekonomiczna, Dom Wydawniczy ABC, Kraków.

DeMarco T. 2002, Zdążyć przed terminem, Studio Emka, Warszawa.

A Guide to the Project Management Body of Knowledge, 2009, Project Management Institute, Inc., Management Training & Development Center.

Korczowski A. 2009, Zarządzanie ryzykiem w projektach informatycznych. Teoria i praktyka, Helion S.A., Gliwice.

Management of Risk: Guidance for Practitioners, 2010, OGC.

Pritchard C. 2002, Zarządzanie ryzykiem w projektach, teoria i praktyka, WIG-PRESS, Warszawa.

Schmidt, R.C., Lyytinen, K., Keil, M., and Cule, P. 2001, Identifying Software Project Risks: An International Delphi Study, "Journal of Management Information Systems", Vol. 17 No. 4.

Szyjewski Z. 2001, Zarządzanie projektami informatycznymi, Placet, Warszawa.

ŹRÓDŁA INTERNETOWE

Because what you do the rest of the week should hold no surprises, http://sjsi.hostdmk.net/wg/pliki/sjsi/doc/7MDrozdz.pdf: 04/05/2012,

Practical Risk-Based Testing, http://www.erikvanveenendaal.nl/NL/files/e-book%20PRISMA.pdf: 04/05/2012,

James Bach on Risk-Based Testing, http://www.eecs.qmul.ac.uk/~norman/SE-pages/Supporting%20documents/James%20Bach%20on%20Risk.doc: 04/05/2012.