

## » Idź do

- Spis treści
- Przykładowy rozdział

## » Katalog książek

- Katalog online
- Zamów drukowany katalog

## » Twój koszyk

- Dodaj do koszyka

## » Cennik i informacje

- Zamów informacje o nowościach
- Zamów cennik

## » Czytelnia

- Fragmenty książek online

## » Kontakt

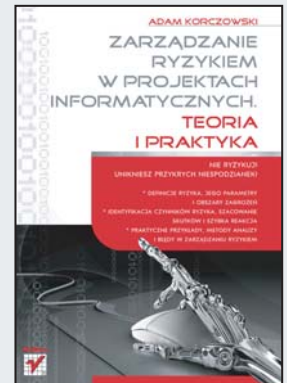
Helion SA  
ul. Kościuszki 1c  
44-100 Gliwice  
tel. 032 230 98 63  
e-mail: helion@helion.pl  
© Helion 1991-2008

## Zarządzanie ryzykiem w projektach informatycznych. Teoria i praktyka

Autor: [Adam Korczowski](#)

ISBN: 978-83-246-1508-7

Format: 158×235, stron: 224



### Nie ryzykuj! Unikniesz przykrych niespodzianek!

- Definicje ryzyka, jego parametry i obszary zagrożeń
- Identyfikacja czynników ryzyka, szacowanie skutków i szybka reakcja
- Praktyczne przykłady, metody analizy i błędy w zarządzaniu ryzykiem

Każdy projekt, program czy dowolne przedsięwzięcie z założenia obarczone są pewnym ryzykiem. Nie da się z góry przewidzieć wszystkich szczegółów i możliwych opóźnień, wymusić od zaangażowanych osób obietnicy dotrzymania terminu ani tak zakląć losu, by nie zrobił jakiegoś złośliwego psikusa. Można jednak ograniczyć ryzyko przez właściwe zaplanowanie całego procesu, wskazanie punktów projektu najbardziej narażonych na błędy i oszacowanie prawdopodobieństwa ich wystąpienia. Takie działanie pozwala wystarczająco szybko zareagować na pojawiające się problemy i wydatnie przyspieszyć tempo prac.

Książka „Zarządzanie ryzykiem w projektach informatycznych. Teoria i praktyka” traktuje właśnie o wszelkich aspektach minimalizowania ryzyka związanego z wdrażaniem projektu informatycznego. Z tego podręcznika dowiesz się, co to jest cykl życia projektu, jak rozpisać jego poszczególne fazy, w jaki sposób oceniać ryzyko i koordynować pracę wielu osób w obszarach objętych kontrolą. Nauczysz się zauważać potencjalne zagrożenia i nie dopuszczać do powstawania wymiernych strat. Ponadto znajdziesz tu życiowe przykłady radzenia sobie w trudnych sytuacjach – do wykorzystania w Twojej własnej praktyce.

- Cykl życia projektu i zarządzania ryzykiem
- Metodyki zarządzania ryzykiem
- Zarządzanie ryzykiem na poziomie strategicznym
- Zarządzanie ryzykiem w programach, projektach, operacyjnym
- Zarządzanie bezpieczeństwem i utrzymaniem ciągłości biznesu
- Definiowanie polityki zarządzania ryzykiem
- Ocena ryzyka
- Planowanie reakcji na ryzyko
- Monitorowanie i sterowanie ryzykiem
- Strategia zarządzania portfelem projektów
- Uzasadnienie biznesowe i analiza ekonomiczna wartości projektu
- Wybrane techniki analizy ryzyka
- Błędy w zarządzaniu ryzykiem
- Podstawy teorii informacji i rachunku prawdopodobieństwa
- Szablony dokumentów wspierających zarządzanie ryzykiem

**Poznaj wszystkie aspekty zarządzania ryzykiem w projektach IT!**

# Spis treści

<b>Od autora .....</b>	<b>7</b>
<b>Rozdział 1. Wprowadzenie .....</b>	<b>9</b>
Podstawowe pojęcia związane z niepewnością .....	9
Zmiana biznesowa w organizacji .....	11
Cykl życia projektu .....	14
Definicje i parametry ryzyka .....	16
Obszary zagrożeń w działalności projektowej .....	19
Metodyki zarządzania ryzykiem .....	32
<b>Rozdział 2. Zasady zarządzania ryzykiem w organizacji .....</b>	<b>37</b>
Zarządzanie ryzykiem na poziomie strategicznym .....	37
Zarządzanie ryzykiem w programach .....	40
Zarządzanie ryzykiem w projektach .....	42
Zarządzanie ryzykiem operacyjnym .....	44
Zarządzanie bezpieczeństwem i utrzymaniem ciągłości biznesu .....	46
<b>Rozdział 3. Proces zarządzania ryzykiem w projektach .....</b>	<b>59</b>
Opis cyklu zarządzania ryzykiem .....	59
Definiowanie polityki zarządzania ryzykiem .....	60
Role i zakresy odpowiedzialności .....	61
Opis procesu i modelu zarządzania ryzykiem .....	64
Poziom akceptacji ryzyka i procedury eskalacji .....	64
Odnośniki do innych poziomów polityki zarządzania ryzykiem .....	65
Identyfikacja czynników ryzyka .....	66
Wejścia procesu identyfikacji .....	68
Wyjścia procesu identyfikacji .....	69
Techniki stosowane do identyfikacji ryzyka .....	69
Czynności procesu identyfikacji .....	70
Ocena ryzyka .....	71
Wejścia procesu oceny ryzyka .....	71
Wyjścia procesu oceny ryzyka .....	72
Techniki stosowane do oceny ryzyka .....	72
Czynności procesu oceny ryzyka .....	73
Określenie i wybór reakcji na ryzyko .....	74
Wejścia procesu określenia i wyboru reakcji na ryzyko .....	74
Wyjścia procesu określenia i wyboru reakcji na ryzyko .....	74
Techniki stosowane do określenia i wyboru reakcji na ryzyko .....	76
Czynności procesu określenia i wyboru reakcji na ryzyko .....	76

Planowanie reakcji na ryzyko .....	77
Wejścia procesu planowania reakcji na ryzyko .....	77
Wyjścia procesu planowania reakcji na ryzyko .....	77
Techniki stosowane do planowania reakcji na ryzyko .....	78
Czynności procesu planowania reakcji na ryzyko .....	78
Monitorowanie i sterowanie ryzykiem .....	78
Wejścia procesu monitorowania i sterowania ryzykiem .....	79
Wyjścia procesu monitorowania i sterowania ryzykiem .....	79
Techniki stosowane do monitorowania i sterowania ryzykiem .....	80
Czynności procesu monitorowania i sterowania ryzykiem .....	80
<b>Rozdział 4. Ryzyko uruchomienia projektu .....</b>	<b>83</b>
Strategia zarządzania portfelem projektów .....	83
Uzasadnienie biznesowe i analiza ekonomiczna wartości projektu .....	86
Niepewność uzasadnienia biznesowego w procesie decyzyjnym uruchamiania projektu .....	91
<b>Rozdział 5. Praktyka zarządzania ryzykiem .....</b>	<b>97</b>
Czynniki krytyczne zarządzania ryzykiem .....	97
Wybrane techniki analizy ryzyka .....	102
Listy kontrolne .....	103
Sesje analityczne, burze mózgów .....	113
Profile ryzyka .....	118
Metody eksperckie .....	123
Analiza założeń .....	127
Drzewa decyzyjne .....	129
Symulacja Monte Carlo .....	134
Analiza wrażliwości .....	139
Techniki sieciowe .....	142
Pozostałe metody diagramowe .....	148
Zarządzanie ryzykiem w przykładowym projekcie .....	152
Opis scenariusza .....	152
Uruchomienie projektu — wstępna analiza ryzyka .....	154
Analiza ryzyka projektu informatycznego .....	161
Ilościowa ocena ryzyka — dobór technik .....	168
Monitorowanie i sterowanie ryzykiem w trakcie realizacji projektu .....	172
Zamykanie projektu — przekazanie wyników do działalności operacyjnej .....	178
Błędy w zarządzaniu ryzykiem .....	179
Błędy przy ustalaniu i egzekwowaniu polityki zarządzania ryzykiem .....	180
Błędy w procesie identyfikacji czynników ryzyka .....	180
Błędy przy szacowaniu ryzyka .....	183
Błędy przy identyfikacji i doborze akcji przeciwdziałających .....	184
Błędy w trakcie monitorowania ryzyka .....	185
Błędy przy zamykaniu projektu .....	186
<b>Dodatek A Podstawy teorii informacji i rachunku prawdopodobieństwa .....</b>	<b>187</b>
<b>Dodatek B Przykładowe szablony dokumentów wspierających zarządzanie ryzykiem .....</b>	<b>195</b>
Uzasadnienie Biznesowe .....	195
Przyczyny uruchomienia projektu .....	195
Spodziewana zmiana biznesowa, którą projekt ma wywołać .....	196
Oczekiwane rezultaty (wyniki) .....	196
Warianty możliwych rozwiązań .....	196
Spodziewane korzyści .....	196

Podstawowe parametry projektu: budżet i ramy czasowe .....	196
Główne czynniki ryzyka biznesowego .....	196
Ogólna ocena wartości projektu .....	196
Rejestr Ryzyka .....	197
Rejestr Zagadnień .....	198
Dokument Otwarcia .....	199
Kontekst projektu .....	199
Definicja projektu .....	199
Formuła realizacji .....	199
Główne parametry projektu .....	199
Pierwotna wersja Uzasadnienia Biznesowego .....	199
Pierwotna wersja Planu Projektu .....	199
Pierwotna wersja Rejestru Ryzyka .....	200
Plan jakości .....	200
Struktura organizacyjna projektu .....	200
Plan komunikacji .....	200
Raport Statusu Projektu .....	201
Data .....	201
Okres sprawozdawczy .....	201
Status budżetu .....	201
Status harmonogramu .....	201
Produkty ukończone w okresie sprawozdawczym .....	201
Bieżące lub potencjalne problemy i aktualizacja ryzyka .....	201
Produkty, które mają zostać ukończone w następnym okresie .....	201
Status zagadnień projektowych .....	202
Wpływ zmian na harmonogram i budżet .....	202
Raport o Sytuacji Nadzwyczajnej .....	203
Opis przyczyn odchyień od planu .....	203
Konsekwencje odchyień .....	203
Dostępne opcje .....	203
Wpływ poszczególnych opcji na: Uzasadnienie Biznesowe, ryzyka, tolerancje projektu i etapu .....	203
Zalecenia kierownika projektu .....	203
Rejestr Doświadczeń .....	204
Zalecenia Działań Poprojektowych .....	205
Generalne zalecenia dotyczące właściwej eksploatacji produktów projektu .....	205
Lista niewytworzonych w projekcie produktów .....	205
Odstępstwa od specyfikacji wymagań dostarczonych produktów .....	205
Żądania zmian niezaimplementowane w ramach projektu .....	205
Zidentyfikowane ryzyka, które mogą mieć wpływ na produkty w trakcie eksploatacji .....	205
Zidentyfikowane akcje dotyczące dodatkowych produktów .....	206
Czynności, które muszą być podjęte przed przekazaniem produktu do programu lub innych projektów .....	206
<b>Bibliografia .....</b>	<b>207</b>
<b>Skorowidz .....</b>	<b>211</b>

## Rozdział 5.

# Praktyka zarządzania ryzykiem

## Czynniki krytyczne zarządzania ryzykiem

Podjęcie projektu, który ma duże znaczenie dla organizacji, jest zazwyczaj poprzedzone analizą strategiczną. Celem takiej analizy jest przede wszystkim stwierdzenie, jaka zmiana biznesowa jest niezbędna i czy dany projekt jest w stanie ją wprowadzić. Wynikiem takiej analizy jest też ustalenie priorytetów względem innych projektów, a także zdefiniowanie odpowiednich relacji do zadań operacyjnych przedsiębiorstwa. Wśród wielu metod stosowanych do celu wyznaczenia strategii jedną z popularniejszych jest analiza pola sił autorstwa Kurta Lewina, służąca do badania uwarunkowań zmian organizacyjnych. Czynniki kształtujące zmianę pochodzą z zewnątrz lub wewnątrz organizacji i mogą jej sprzyjać bądź nie. Uproszczoną wersją tej metody jest analiza **SWOT** (*Strengths — Weaknesses — Opportunities — Threats*), która polega na badaniu silnych i słabych stron organizacji oraz szans i zagrożeń w otoczeniu biznesowym. Porównanie potencjału organizacji ze środowiskiem pozwala na określenie jej pozycji strategicznej i jest podstawą do zdefiniowania nowej lub zmodyfikowania istniejącej strategii. Analiza powinna skupiać się na wyodrębnieniu czynników kluczowych, które mogą mieć decydujący wpływ na przyszłość organizacji. Są to uwarunkowania, fakty, zjawiska, które powinny być w szczególności sposób wyodrębnione, a następnie kontrolowane w trakcie realizacji zmiany. Czynniki te, zwane **krytycznymi czynnikami sukcesu**, możemy odnosić do całej zmiany biznesowej, lecz również do pojedynczych projektów. Czynnikiem tych nie należy mylić z ryzykiem, gdyż nie są one charakteryzowane przez prawdopodobieństwo wystąpienia; z czynnikami krytycznymi sukcesu musimy się z całą pewnością zmierzyć i zapewnić, że nie wpłyną one negatywnie na przedsięwzięcie.

Jakkolwiek rozpatrując czynniki krytyczne, zazwyczaj ma się na myśli sukces zmiany biznesowej, projektu lub programu, to można również zidentyfikować takie, które mają istotne znaczenie dla jednego z obszarów zarządzania — dla zarządzania ryzykiem. Z pewnością większość z tych czynników będzie również istotna dla innych elementów

zarządzania: uzasadnienia biznesowego, sterowania jakością, zmianami. Przed zidentyfikowaniem krytycznych czynników zarządzania ryzykiem należy wytworzyć sobie wizję projektu z wyidealizowanym sposobem zarządzania, a następnie wyodrębnić takie uwarunkowania i fakty, które w rzeczywistych projektach powodują najpoważniejsze odejście od tego ideału. Jest to też pewnego rodzaju „obraz sukcesu” w sferze zarządzania.

Poniższa lista obszarów, w których występują czynniki krytyczne sukcesu zarządzania ryzykiem, dotyczy nie tylko projektów informatycznych, lecz także uwzględnia specyfikę projektów, w których zagadnienia teleinformatyczne mają zasadnicze znaczenie.

### **1. Powiązanie misji, strategii i celów strategicznych organizacji z celami projektu.**

Projekty, zwłaszcza o charakterze informatycznym, traktowane są często w oderwaniu od rzeczywistych celów strategicznych. Ukończenie projektu staje się celem samym w sobie, nie uwzględnia faktu, że projekt jest tylko drogą do wprowadzenia zmiany biznesowej. Szczególne znaczenie ma to dla portfela projektów, gdzie nie są w wyraźny sposób ustanowione zasady przydzielania priorytetów, a każdy projekt traktowany jest przez jego właścicieli jako jedyny, najważniejszy. W tej sytuacji zarządzanie ryzykiem w projektach nie bierze pod uwagę zgodności celów ze strategią, a czynniki ryzyka związane z niewypełnieniem przez projekt misji nie są identyfikowane.

### **2. Jasny obraz sukcesu projektu.**

Zarówno przy rozpatrywaniu zjawisk dla projektu negatywnych, jak i pozytywnych istotne jest określenie, co będzie prawdziwym sukcesem projektu. W przypadku projektów informatycznych często za sukces uważa się wytworzenie sprawnie działającego oprogramowania lub udaną implementację systemu, czasem dodatkowo zweryfikowaną etapem pilotażowego wdrożenia. Tymczasem rzeczywisty sukces projektów, nie tylko informatycznych, polega na uzyskaniu korzyści biznesowych, które mogą nastąpić dopiero wiele miesięcy po zamknięciu projektu. Niemniej jednak zarządzanie ryzykiem należy odnosić do osiągnięcia wszystkich celów pośrednich, z których najważniejsze są właśnie te związane z uzyskaniem produktów o wymaganej jakości. Pozostałe parametry mogą mieć różną wagę: dla niektórych projektów dotrzymanie terminu zakończenia jest absolutnie krytyczne, dla innych ważniejsze jest oszczędne gospodarowanie budżetem albo takie zarządzanie zasobami, które w żaden sposób nie zakłóca działalności operacyjnej organizacji. Celem pośrednim, prowadzącym do sukcesu biznesowego, jest też odpowiednie przygotowanie przyszłej eksploatacji produktów projektu, czyli zapewnienie obsługi serwisowej, przeszkolenie użytkowników systemów, opracowanie dokumentacji. Obraz sukcesu projektu powinien zostać tak zdefiniowany, a następnie rozpowszechniony wśród uczestników projektu, aby nie było żadnych wątpliwości, jakie kryteria odnoszą się do poszczególnych parametrów projektu i jakie są priorytety w osiągnięciu celów pośrednich.

Dla zewnętrznego dostawcy cel biznesowy realizowany jest przez otrzymanie odpowiedniej wartości pieniężnej za wytworzone produkty lub dostarczone usługi. Niemniej obraz sukcesu projektu ze strony dostawcy też musi brać pod uwagę okres eksploatacji produktów, czyli czas po zamknięciu projektu. Wiąże się to nie tylko z ewentualnymi dodatkowymi kosztami obsługi gwarancyjnej, lecz również, a może przede wszystkim, z utrzymaniem prestiżu, który przynosi długofalowe korzyści biznesowe.

### 3. Struktury organizacyjne.

Pierwszym warunkiem sukcesu projektu jest właściwy wybór struktury organizacyjnej projektu oraz mianowanie odpowiednich osób do sprawowania poszczególnych ról w tej strukturze. Szczególnie istotne jest zrozumienie, że struktura ta jest w pewnym sensie autonomiczna i nie podlega rutynowym zasadom działania struktur liniowych (funkcjonalnych). Wprawdzie zagrożenia dla projektów często zazębiają się z problemami występującymi w działalności operacyjnej, niemniej jednak zarządzanie ryzykiem w projektach podlega nieco innym prawom niż zarządzanie ryzykiem operacyjnym. Członkowie komitetów sterujących, zazwyczaj pełniący na co dzień funkcje w zarządzie organizacji, powinni zdawać sobie sprawę, że role pełnione w projektach wiążą się z innymi zakresami obowiązków i odpowiedzialności. Istotne jest więc przygotowanie, niekoniecznie w postaci bardzo sformalizowanych dokumentów, opisu poszczególnych ról w strukturze organizacyjnej projektu.

### 4. Polityka zarządzania ryzykiem.

W większych organizacjach polityka zarządzania ryzykiem stanowi element całej polityki zarządzania i jest odpowiednio udokumentowana. Niemniej nawet wtedy należy upewnić się, czy nie obejmuje ona tylko zagadnień operacyjnych, pomijając specyfikę prowadzenia projektów. Polityka zarządzania ryzykiem w projektach powinna obejmować przede wszystkim zagadnienia związane z zakresem odpowiedzialności za ryzyko, czyli odnosić się do projektowych struktur organizacyjnych, opisanych w punkcie 3. powyżej. Ponadto powinna proponować jednorodne dla danego projektu podejście do ryzyka, rozumiane jako przyjęcie wybranego modelu jego oceny, przebieg procesu, zasady akceptowania ryzyka, sposób podejmowania decyzji. Najwłaściwsze jest przyjęcie dla całej organizacji wspólnej polityki zarządzania ryzykiem z opisem ewentualnych rozbieżności dla projektów o określonej specyfice lub skali.

### 5. Zaangażowanie zarządu projektu w zarządzanie ryzykiem.

Odpowiednio przygotowane opisy ról w projekcie powinny zasadniczo uregulować sprawy związane z odpowiedzialnością za ryzyko i zasadami podejmowania decyzji. Jednak istotne jest osobiste nastawienie zarządu projektu, zwłaszcza członków komitetu sterującego, do zagadnień ryzyka. Pełna świadomość, jakie są korzyści z zarządzania ryzykiem, powinna owocować zaangażowaniem w ten obszar zarządzania, a także przyjęciem do wiadomości implikacji z nim związanych. Zarządzanie ryzykiem kosztuje, ale zwykle się mawiać, że brak zarządzania nim kosztuje jeszcze więcej. Komitet sterujący powinien promować zarządzanie ryzykiem i wspierać — zwłaszcza kierownika — we wszystkich działaniach przeciwdziałających możliwym zagrożeniom. Również istotne jest przyjęcie na siebie przez komitet sterujący odpowiedzialności za monitorowanie pewnych zjawisk, które mogą być trudno dostępne dla innych uczestników projektu; dotyczy to zwłaszcza obszarów polityki, w tym polityki biznesowej, rynku, finansów organizacji i zagadnień prawnych.

### 6. Metodyka zarządzania ryzykiem.

Wybór formalnej metodyki prowadzenia projektu jest równoznaczny z wyborem sposobu zarządzania ryzykiem. Dla projektów prowadzonych mniej formalnie, w oparciu o własne procedury, istotne jest uzgodnienie zasad podejścia do ryzyka

i zdefiniowanie zasad jego obsługi. Nie musi to być szczegółowo opisany proces zarządzania, lecz konieczne jest przede wszystkim określenie zakresu odpowiedzialności za poszczególne czynności objęte cyklem obsługi ryzyka, zwłaszcza w zakresie decyzji o stosowaniu środków zaradczych.

### **7. Wiedza o zarządzaniu ryzykiem wśród udziałowców projektu.**

W projektach informatycznych widać ze szczególną ostrością, jak istotna jest pełna świadomość wszystkich uczestników projektu o zagadnieniach związanych z ryzykiem. Wielkie znaczenia ma udział członków zespołów realizacyjnych w sesjach identyfikowania i oceny ryzyka. Często jedyną osobą, która może właściwie oszacować zagrożenia wynikające z niepewności rezultatów niektórych prac, jest właśnie ich wykonawca. Jeśli nawet te oceny obciążone są dużą dozą subiektywizmu, to zastosowanie odpowiednich technik zwiększa ich wiarygodność i staje się podstawą do stosowania optymalnych akcji przeciwdziałających.

### **8. Przywództwo, osoba kierownika projektu.**

W dużym skrócie odpowiedzialność kierownika polega na tym, aby projekt przez niego prowadzony w określonym czasie wytworzył produkty, które będą w stanie doprowadzić do osiągnięcia korzyści biznesowych, i aby utrzymany został przewidziany na to budżet. Wszystko, co może temu zagrozić, jest przedmiotem działań kierownika projektu, a z tego wynika odpowiedzialność za właściwe zarządzanie ryzykiem. Kierownik musi sobie zdawać sprawę, że dotyczą go też zjawiska niezależne od niego, często trudne do przewidzenia, ale mające wpływ na projekt. Kierownik powinien umotywować zespoły projektowe do aktywnego uczestnictwa w procesach zarządzania, wyznaczyć odpowiednie role (np. właścicieli poszczególnych czynników ryzyka), a przede wszystkim włączyć do planów wszystkie czynności związane z analizą ryzyka, a później jego monitorowaniem i wykonywaniem odpowiednich akcji. Jednym z podstawowych narzędzi, którymi kierownik powinien posługiwać się w trakcie prowadzenia projektu, jest Rejestr Ryzyka.

### **9. Współpraca stron w zarządzaniu ryzykiem.**

Nawet jeśli realizowany jest projekt wewnętrzny, gdzie wszystkie strony należą do jednej organizacji, biorą w nim udział różne strony interesu. Naturalny podział na klientów i dostawców powinien być uzupełniony o przyszłych użytkowników systemów, niekoniecznie należących do organizacji klienta (przykładowo: ministerstwo może zlecić wykonanie systemu informatycznego dla jakiegoś urzędu, który będzie wyłącznym jego użytkownikiem). Każda ze stron oczekuje od projektu nieco innych korzyści, w związku z czym inaczej rozumie zagadnienia ryzyka. Dla klienta istotne jest przede wszystkim ryzyko biznesowe, czyli zagrożenia w osiągnięciu planowanych korzyści. Użytkownik ma na uwadze przede wszystkim jakość produktów projektu, której niedotrzymanie utrudni lub uniemożliwi sensowne ich użytkowanie. Dostawca musi dbać o swoje uzasadnienie biznesowe, które będzie możliwe do wypełnienia, jeśli produkty o wymaganej jakości nie tylko uda się wytworzyć, ale gdy proces wytworzenia nie będzie zbyt kosztowny. Wszystkie możliwe problemy techniczne oraz związane z pozyskaniem odpowiednich zasobów mogą stworzyć takie zagrożenie dla dostawcy. Istotne jest, aby wszystkie strony w projekcie zdały sobie sprawę,



że zarządzanie ryzykiem powinno być sprawą wspólną, do czego pierwszym krokiem jest właściwa wymiana informacji. Przy przyjmowaniu zleceń dostawcy powinni zgłaszać swoje wątpliwości co do terminowego wykonania prac i uzyskania wymaganej jakości. Nie jest to łatwe, zwłaszcza że wątpliwości te mogą rzutować na treść kontraktów. Zalecenie wspólnych działań przy identyfikowaniu i ocenie czynników ryzyka, występujących na styku dostawcy z klientem, powinno zaowocować sprawniejszym prowadzeniem projektu i łatwiej doprowadzić do jego sukcesu.

### **10. Współpraca udziałowców projektu z działami zajmującymi się bezpieczeństwem informatycznym.**

Wdrożenie nowego systemu lub modyfikacja starego wiąże się w organizacji w szczególności z zagadnieniami bezpieczeństwa informacyjnego. Przede wszystkim produkty, powstałe w wyniku projektu, powinny być bezpieczne w eksploatacji, również w sensie bezpieczeństwa danych, na których będą operować. Ponieważ we współczesnych organizacjach większość działalności operacyjnej polega na sprawnym i bezpiecznym działaniu systemów informatycznych, źle wykonany lub niewłaściwie wdrożony system może zagrozić ciągłym procesom gospodarczym, składającym się na operacje biznesowe. Ocena zaimplementowanego systemu przez odpowiednie departamenty prowadzi do zakwalifikowania go jako nadającego się do eksploatacji i warunkuje zakończenie procesu zamykania projektu. W związku z tym nadzwyczaj istotną staje się współpraca tych departamentów z uczestnikami projektu, zwłaszcza ze stroną dostawców.

### **11. Praktyka zarządzania ryzykiem w projektach.**

Nawet w przypadkach, gdy wśród udziałowców projektu istnieje pełna świadomość konieczności zarządzania ryzykiem oraz została przyjęta formalna metoda, brak doświadczenia utrudnia wykorzystanie wiedzy teoretycznej. Rygorystyczne przestrzeganie wszystkich elementów metodyki prowadzi do biurokracji, a w efekcie do wzrostu kosztów zarządzania i trudności w dotrzymaniu terminów prac. W rezultacie prowadzi to do zniechęcenia i utraty zaufania do formalnych metod zarządzania. Utrzymanie formalnych ram zarządzania ryzykiem w rozsądnych granicach, bez przesadnej biurokracji, jest ważnym elementem wpływającym na sprawne i bezpieczne prowadzenie projektu. W przypadkach gdy zarząd projektu i uczestnicy nie mają wystarczającego doświadczenia, porady ekspertów stanowią nieocenioną wartość.

### **12. Procesy identyfikacji i oceny ryzyka.**

Podstawą właściwego zarządzania ryzykiem są pierwsze procesy cyklu: identyfikacja i ocena. Bagatelizowanie zagrożeń, zwłaszcza we wstępnej fazie uruchamiania projektu, prowadzi do podejmowania nieopłacalnych przedsięwzięć, a w trakcie realizacji prac powoduje szereg dodatkowych komplikacji. Wnikliwie przeprowadzona analiza ryzyka umożliwia proaktywne zarządzanie projektem i uniknięcie wielu problemów, które mają miejsce, gdy dany czynnik ryzyka się materializuje.

### 13. Identyfikacja i dobór akcji przeciwdziałających.

W wyniku analizy ryzyka powstaje lista dodatkowych czynności, związanych z zapobieganiem bądź redukcją ryzyka. Generowane są nowe koszty, zwłaszcza w przypadkach konieczności tworzenia planów rezerwowych lub wykupienia ubezpieczeń. Podejmowanie decyzji o wyborze konkretnych przeciwdziałań powinno odbywać się w oparciu o bilans kosztów tych akcji i ich przewidywanej skuteczności. Decyzje te mogą mieć duży wpływ na budżet całego projektu, więc przynajmniej niektóre z nich powinny być podejmowane na wyższym poziomie — przez komitet sterujący.

### 14. Monitorowanie i analizowanie zagadnień projektowych.

Bieżąca obsługa ryzyka również stanowi dodatkowy koszt dla projektu — są to czynności obserwacji zagadnień projektowych i ich analiza pod kątem możliwości pojawienia się nowych czynników ryzyka lub zmiany oceny czynników wcześniej zidentyfikowanych. Metodyki narzucają pewne minima związane z pracochłonnością niezbędną dla sensownej bieżącej obsługi ryzyka, lecz ilość pracy poświęcana na monitorowanie zagadnień będzie różna dla każdego projektu. Kluczem do sprawnego monitorowania ryzyka jest przede wszystkim sensowne przypisanie właścicieli do poszczególnych czynników, a także doświadczenie kierownika projektu.

### 15. Dokumentowanie doświadczeń związanych z ryzykiem.

Jednym z najważniejszych elementów Raportu o Doświadczeniach jest ocena procesów zarządczych, w tym procesu zarządzania ryzykiem, a także ocena dokładności szacunków prawdopodobieństwa i wpływu poszczególnych czynników na projekt. W dokumencie tym, powstającym przy zamykaniu projektu, powinno się też zapisywać wszystkie czynniki, których nie udało się zidentyfikować podczas analizy wstępnej, a które zmaterializowały się w trakcie realizacji projektu. Raporty o Doświadczeniach są nieocenioną pomocą dla kierowników podobnych projektów, mogą się przyczynić do usprawnienia procesów zarządzania i przez to zwiększyć szanse na sukces kolejnych przedsięwzięć.

Przy uruchamianiu projektu warto poświęcić czas na rozpatrzenie wymienionych powyżej obszarów, w których istnieją zagrożenia niewłaściwej obsługi ryzyka. Dla każdego projektu czynniki krytyczne powinny być zidentyfikowane w jak najwcześniejszej jego fazie, gdyż właściwe zarządzanie ryzykiem jest jednym z ważniejszych warunków sprawnego prowadzenia projektu.

## Wybrane techniki analizy ryzyka

Zaproponowane w niniejszym rozdziale techniki analizy ryzyka stanowią całkowicie arbitralny wybór z bardzo szerokiego spektrum metod i technik, stosowanych w zarządzaniu ryzykiem. Przy ich selekcji wzięto pod uwagę nie tylko ich popularność i dostępność, lecz przede wszystkim łatwość stosowania również w niewielkich projektach. Omawianie każdej z technik rozpoczynają uwagi na temat obszaru zastosowań i możliwości implementacji w projektach informatycznych.

## Listy kontrolne

Jedną z najpowszechniej stosowanych, łatwych w użyciu, a zarazem bardzo skutecznych technik, jest metoda list kontrolnych. Wspiera ona głównie proces identyfikacji czynników ryzyka, choć może też być pomocna w trakcie oceny czynników oraz przy identyfikacji i wyborze środków przeciwdziałających. Jakkolwiek stosowana jest przede wszystkim w trakcie wstępnej analizy, powinna być wykorzystywana również w następnych fazach projektu: przy zatwierdzaniu uruchomienia kolejnych etapów, w trakcie okresowych ocen, a nawet przy zamykaniu projektu. Ten ostatni przypadek ma na celu określenie zagrożeń, które mogą nastąpić w trakcie eksploatacji produktów projektu, a także ma stanowić ważny element listy doświadczeń nabytych w czasie całego cyklu projektu.

Technika zakłada, że istnieją gotowe do wykorzystania listy kontrolne, w których zgromadzona jest wiedza o obszarach występowania ryzyka dla danego projektu, o możliwych zdarzeniach i zjawiskach, które mogą mieć wpływ na projekt. Wprawdzie różne instytucje opracowują uniwersalne listy kontrolne lub listy ukierunkowane na dany typ projektu, lecz najwygodniej dla organizacji jest, gdy wypracowała ona sobie własne wykazy typowych czynników uwzględniające nie tylko specyfikę prowadzonych w niej projektów, lecz również uwarunkowania związane ze sposobem działalności przedsiębiorstwa czy instytucji. Wiele czynników ryzyka wynika z otoczenia, w którym funkcjonuje organizacja, a te czynniki z reguły nie są ujmowane w publikowanych i ogólnie dostępnych listach. Istotne jest więc, aby przy planowaniu strategicznym wziąć pod uwagę zbieranie i wymianę informacji o występujących w ramach całej organizacji zagrożeniach dla prowadzonych w niej projektów. Informacja ta staje się podstawą do opracowania firmowych list kontrolnych, które powinny podlegać okresowym przeglądom w szerokim gronie realizatorów projektów oraz ekspertów. Jeśli jednak organizacja nie dysponuje opracowanymi na własne potrzeby listami kontrolnymi lub nie prowadziła dotąd projektów zarządzanych metodycznie, powinna posłużyć się gotowymi listami, najlepiej związanymi z daną branżą.

W projektach informatycznych warto oprzeć się na wiedzy zgromadzonej przez takie organizacje jak wspomniany już Software Engineering Institute (SEI), w którym powstały modele dojrzałości organizacyjnej przedsiębiorstw CMM<sup>®</sup>, a przy wstępnym identyfikowaniu czynników ryzyka wysokiego poziomu — na uniwersalnych listach publikowanych np. przez brytyjską agencję Office of Government Commerce (OGC). Wskazane jest, aby przed rozpoczęciem projektu uzupełnić listy kontrolne poprzez dopisanie dodatkowych elementów wynikających z dokumentów firmowych, zwłaszcza z Raportów o Doświadczeniach z poprzednich projektów.

W poniższych tabelach przedstawione są przykłady list o różnej konstrukcji, które mogą być pomocne w różnych fazach cyklu projektu. Lista umieszczona w tabeli 5.1 jest zbudowana z serii pytań, które nie tylko pomagają zidentyfikować zagrożenia, lecz również, a nawet przede wszystkim, pozwalają na zgrubną ocenę poziomu ryzyka całego projektu. Lista ta nadaje się przede wszystkim do wstępnego porównania projektów przy analizie portfela — może stać się podstawą odrzucenia bądź przyjęcia projektów do realizacji, a następnie do ustalenia ich priorytetów. Jest listą uniwersalną, nadającą się do analizowania projektów różnego typu.

**Tabela 5.1.** Lista kontrolna wspomagająca wstępną ocenę ryzyka projektu

<b>Id.</b>	<b>Obszar zagrożenia, pytanie identyfikujące</b>	<b>Ocena</b>
<b>Strategia, dojrzałość organizacji</b>		
S.1	Czy organizacja posiada jasno sprecyzowaną strategię?	
S.2	Czy planowana zmiana biznesowa jest zgodna z głównymi celami strategicznymi?	
S.3	Czy istnieje powszechne przekonanie, że zmiana jest niezbędna?	
S.4	Czy określony jest poziom oddziaływania zmiany biznesowej na działalność operacyjną?	
S.5	Czy główne krytyczne procesy biznesowe pozostaną nienaruszone przez zmianę?	
S.6	Czy zdefiniowany jest zakres zmiany biznesowej, który ma być zrealizowany przez projekt?	
S.7	Czy organizacja wprowadzała już zmianę biznesową na podobnym poziomie?	
S.8	Czy procesy biznesowe organizacji są przystosowane do wprowadzenia zmiany?	
S.9	Czy osoby, które będą zaangażowane w zarządzanie strategiczne projektu, brały już udział w podobnym przedsięwzięciu?	
<b>Otoczenie biznesowe i polityczne</b>		
B.1	Czy sytuacja polityczna jest stabilna?	
B.2	Czy sytuacja gospodarcza jest stabilna?	
B.3	Czy środki finansowe są łatwe do pozyskania?	
B.4	Czy znany jest wpływ otoczenia biznesowego na zmianę w organizacji?	
B.5	Czy proces wprowadzenia zmiany jest odporny na działania konkurencji?	
B.6	Czy opinia publiczna i media są przychylne?	
B.7	Czy kondycja kluczowych kontrahentów i partnerów jest stabilna?	
B.8	Czy określony jest poziom oddziaływania zmiany biznesowej na działalność operacyjną?	
<b>Sytuacja ekonomiczna/komercyjna organizacji</b>		
E.1	Czy sytuacja rynkowa organizacji jest stabilna?	
E.2	Czy stosunki własnościowe w organizacji są stabilne?	
E.3	Czy organizacja posiada zabezpieczony na okres prowadzenia projektu kapitał obrotowy?	
E.4	Czy stosunki z partnerami są uregulowane?	
E.5	Czy organizacja może w zakresie pozyskania środków inwestycyjnych polegać w dużym stopniu na własnych zasobach finansowych?	
<b>Legislacja, przepisy</b>		
L.1	Czy sytuacja legislacyjna jest stabilna?	
L.2	Czy działalność organizacji jest niewrażliwa na zmiany przepisów?	
L.3	Czy organizacja posiada prawa autorskie do tworzonych przez nią produktów?	
L.4	Czy kontrakty są zgodne z bieżącymi warunkami prawnymi?	
L.5	Czy zawarte umowy są zgodne z prawem międzynarodowym?	

**Tabela 5.1.** Lista kontrolna wspomagająca wstępną ocenę ryzyka projektu — ciąg dalszy

<b>Id.</b>	<b>Obszar zagrożenia, pytanie identyfikujące</b>	<b>Ocena</b>
<b>Dostawcy</b>		
D.1	Czy organizacja polega na sprawdzonych, wiarygodnych dostawcach?	
D.2	Czy podpisane są długoterminowe umowy z kluczowymi dostawcami?	
D.3	Czy projekt jest w małym stopniu uzależniony od pojedynczych dostawców?	
D.4	Czy kluczowi dostawcy posiadają odpowiednie certyfikaty zgodności z normami?	
D.5	Czy u dostawców funkcjonują systemy zarządzania jakością?	
D.6	Czy poziom partnerstwa z dostawcami pozwala na włączenie ich w struktury zarządzania projektem?	
<b>Organizacja</b>		
O.1	Czy polityka korporacyjna uwzględnia funkcjonowanie w jej ramach organizacyjnych struktur projektowych?	
O.2	Czy wdrożona jest i stosowana jako obowiązująca metodyka zarządzania projektem?	
O.3	Czy udziałowcy projektu znają jego cele i produkty?	
O.4	Czy został mianowany przewodniczący komitetu sterującego (sponsor)?	
O.5	Czy przewodniczący komitetu sterującego jest aktywnie zaangażowany w doprowadzenie projektu do sukcesu?	
O.6	Czy do komitetu sterującego zostali włączeni reprezentanci wszystkich stron (klienta, użytkowników, dostawców)?	
O.7	Czy członkowie komitetu sterującego znają swoje zadania i przyjmują odpowiedzialność za ich realizację?	
O.8	Czy proces decyzyjny jest jasno określony i znany udziałowcom projektu?	
O.9	Czy zarząd projektu posiada wystarczające kompetencje do zabezpieczenia zasobów projektu?	
O.10	Czy jest zabezpieczone wsparcie operacyjne projektu?	
O.11	Czy uruchomione są mechanizmy komunikacji wewnątrz projektu oraz projektu z otoczeniem?	
O.12	Czy zarząd projektu dysponuje swoim czasem adekwatnie do skali i potrzeb projektu?	
O.13	Czy istnieje sprawdzony sposób rozwiązywania konfliktów?	
<b>Czynnik ludzki</b>		
C.1	Czy kierownik projektu ma profesjonalne przygotowanie do prowadzenia projektu?	
C.2	Czy kierownik projektu ma cechy charakterologiczne odpowiednie do zarządzania ludźmi?	
C.3	Czy zespół projektowy jest stabilny?	
C.4	Czy uczestnicy mają doświadczenie w pracy w projektach?	
C.5	Czy w zespołach projektowych istnieje świadomość celów projektu i zgoda co do sposobu ich osiągnięcia?	
C.6	Czy ewentualne konflikty wśród członków zespołów są zidentyfikowane i załagodzone?	
C.7	Czy członkowie zespołów są emocjonalnie zaangażowani w osiągnięcie sukcesu projektu?	

**Tabela 5.1.** Lista kontrolna wspomagająca wstępną ocenę ryzyka projektu — ciąg dalszy

<b>Id.</b>	<b>Obszar zagrożenia, pytanie identyfikujące</b>	<b>Ocena</b>
<b>Zarządzanie projektem</b>		
Z.1	Czy do prowadzenia projektu jest stosowana formalna metodyka?	
Z.2	Czy uczestnicy projektu zaznajomieni są z podstawowymi zasadami metodycznego zarządzania projektem?	
Z.3	Czy poziom formalnych procedur został dopasowany do skali i wagi projektu?	
Z.4	Czy został uzgodniony sposób postępowania w sytuacjach nadzwyczajnych?	
Z.5	Czy projekt korzysta z ustandaryzowanych, korporacyjnych metod zarządzania jakością?	
Z.6	Czy są wdrożone i rozpowszechnione wśród uczestników procedury zarządzania konfiguracją produktów i zmianami?	
Z.7	Czy ustanowione są zasady obiegu podstawowych dokumentów projektowych?	
Z.8	Czy cykl życia projektu jest jasno zdefiniowany, a zasady odbioru produktów uzgodnione między stronami?	
<b>Parametry i ograniczenia projektu</b>		
P.1	Czy zakres, budżet i termin zakończenia projektu są zatwierdzone?	
P.2	Czy zatwierdzone parametry czasowe i kosztowe są realistyczne?	
P.3	Czy szacowanie parametrów projektu wsparte jest zastosowaniem sprawdzonych technik i bazuje na dokumentacjach z poprzednich projektów?	
P.4	Czy uzgodnione zostały tolerancje parametrów projektu?	
P.5	Czy zakres (produkty) projektu ma (mają) charakter stabilny?	
P.6	Czy zarząd projektu, a w szczególności jego kierownik, jest świadomy związków pomiędzy definicją parametrów projektu a jego uzasadnieniem biznesowym?	
P.7	Czy ograniczenia zewnętrzne są znane i kontrolowane?	
P.8	Czy ewentualne przekroczenie parametrów projektu ma mały wpływ na działalność całej organizacji?	
<b>Współpraca dostawców z użytkownikami</b>		
W.1	Czy specyfikacja produktów projektu została uzgodniona między stronami?	
W.2	Czy istnieje mniej lub bardziej formalny sposób zarządzania wymaganiami?	
W.3	Czy zostały uzgodnione kryteria akceptacji produktów projektu?	
W.4	Czy zarządzanie zmianami jest formalnie uzgodnione między stronami?	
W.5	Czy użytkownicy uczestniczą (mają uczestniczyć) w przeglądach jakości produktów?	
W.6	Czy zasady przekazywania produktów do eksploatacji są uzgodnione?	
W.7	Czy zostały określone kamienie milowe związane z odbiorami głównych pośrednich produktów?	
<b>Zagadnienia techniczne</b>		
T.1	Czy projekt wykorzystuje znane i sprawdzone technologie?	
T.2	Czy liczba dostawców i poddostawców jest rozsądnie ograniczona i kontrolowana?	
T.3	Czy wykonawcy posiadają odpowiednie kompetencje?	
T.4	Czy istniejąca infrastruktura jest wystarczająca do obsługi nowych produktów?	

**Tabela 5.1.** *Lista kontrolna wspomagająca wstępną ocenę ryzyka projektu — ciąg dalszy*

Id.	Obszar zagrożenia, pytanie identyfikujące	Ocena
<b>Zagadnienia techniczne</b>		
T.5	Czy dostępne techniki kontroli jakości są odpowiednie do rodzaju i poziomu technicznego produktów?	
T.6	Czy złożoność produktów jest na poziomie dostosowanym do możliwości użytkowników?	
T.7	Czy narzędzia przewidziane do wytwarzania produktów są na odpowiednim poziomie technicznym i niezawodnościowym?	
T.8	Czy sposób rozwiązywania problemów technicznych jest ustalony i rozpowszechniony wśród zespołów projektowych?	
T.9	Czy po zamknięciu projektu dostarczone produkty będą mogły być eksploatowane bez udziału wykonawców?	

Oceny ryzyka projektu można dokonać na kilka sposobów; najprostszy polega na udzieleniu na poszczególne pytania odpowiedzi „TAK”/„NIE” i obliczeniu procentowego udziału odpowiedzi „NIE” w całej liście — większy procent świadczy o wyższym poziomie ryzyka. Bardziej wiarygodną ocenę uzyskuje się poprzez stopniowanie odpowiedzi i przypisanie im odpowiednich wartości, np.:

Tak	1
Raczej tak	2
Do pewnego stopnia	3
Raczej nie	4
Nie	5

Większa wartość sumaryczna świadczy o wyższym poziomie ryzyka projektu. Liczby mogą być sumowane według poszczególnych obszarów, co staje się podstawą do takich stwierdzeń jak np.: „Projekt jest niezbyt ryzykowny, lecz w dwóch obszarach: współpracy z dostawcami oraz uwarunkowań prawnych, poziom ryzyka jest ponadprzeciętny”. Nie oznacza to, że wysoka wartość ryzyka w pewnym obszarze dyskwalifikuje projekt. Przykładem może tu być pytanie S.5: „Czy główne krytyczne procesy biznesowe pozostaną nienaruszone przez zmianę?”. Często projekt zostaje uruchomiony właśnie w celu przeprowadzenia rewolucyjnej zmiany biznesowej, polegającej na przeprojektowaniu większości procesów biznesowych. Niemniej fakt, że jest on nadzwyczaj ryzykowny, powinien być uświadomiony wszystkim kluczowym udziałowcom projektu. W takich sytuacjach do sumarycznej oceny ryzyka całego projektu wskazane jest dodatkowe przyjęcie wag dla poszczególnych czynników lub całych obszarów.

Niektóre pytania z listy mają charakter bardzo ogólny i wtedy wskazane jest uszczegółowienie pewnych zagadnień. Przykładowo: pytania B.2 i B.3, częściowo ze sobą powiązane, mogą sprawić kłopot przy wyborze właściwej odpowiedzi. Niestabilna sytuacja gospodarcza (B.2) może być właśnie jednym z impulsów uruchomienia zmiany biznesowej, która to zmiana ma uchronić organizację przed wpływem niestabilności sytuacji krajowej lub globalnej. Z drugiej strony może to utrudnić pozyskanie środków na realizację projektu (B.3).

Ma to też pewien związek z punktem E.5, stawiającym pytanie, w jakim stopniu organizacja może w zakresie pozyskania środków inwestycyjnych polegać na własnych zasobach finansowych.

Przy identyfikowaniu czynników ryzyka należy rozróżnić cztery powiązane ze sobą pojęcia:

- ◆ obszar (kategoria),
- ◆ źródła (przyczyny) ryzyka,
- ◆ niepewne zdarzenia (zjawiska),
- ◆ skutki (tych zdarzeń lub zjawisk).

Pojęcia te często mylone są ze sobą, często źródła ryzyka uznawane są za jego czynniki. Tymczasem czynnikami ryzyka są tylko **niepewne zdarzenia (zjawiska)** i tylko one podlegają zarządzaniu. Określenie obszaru ma pomóc w znalezieniu źródeł ryzyka, które należą do którejś z wymienionych w tabeli 5.1 kategorii lub innej, specyficznej dla danego projektu. Źródła, czyli przyczyny występowania ryzyka — to po prostu fakty lub okoliczności, które istnieją w projekcie. Przyczyny nie są ryzykiem, ponieważ nie wiąże się z nimi żadna niepewność. Natomiast mogą one (choć nie muszą) spowodować wystąpienie ryzyka, które z kolei wywoła odpowiednie skutki. Listy kontrolne mają różne formy: mogą specyfikować tylko obszary, ale zazwyczaj podają również źródła ryzyka. Podczas procesu identyfikacji należy stwierdzić, które przyczyny rzeczywiście występują w projekcie, a następnie powiązać je z możliwymi zdarzeniami, które będą miały wpływ na projekt, jeśli istotnie zajdą.

Na bardzo wysokim poziomie decyzyjnym stosowane są bardziej uproszczone listy kontrolne, pomagające zorientować się w skali zagrożeń dla projektu, będącego we wstępnej fazie definiowania celów, uzasadnienia biznesowego i głównych produktów projektu. Takie podejście zaleca agencja OGC dla rządowych projektów, które mają wprowadzić poważną zmianę biznesową poprzez zastosowanie systemów informatycznych. W listach kontrolnych zamiast obszarów występowania ryzyka podane są kryteria, którym podlega przyszły projekt, a które — odpowiednio ocenione — dają wynik liczbowy odzwierciedlający ogólne zagrożenie, jakiemu będzie on narażony. Takimi kryteriami są m.in.:

- ◆ poziom oczekiwanych korzyści;
- ◆ skala wydatków;
- ◆ liczba użytkowników;
- ◆ wpływ na procesy, struktury organizacyjne oraz legislację (poziom przewidywanych zmian w tych obszarach);
- ◆ wpływ na inne projekty;
- ◆ poziom innowacji;
- ◆ liczba specjalistów z branży IT zaangażowanych w projekt zarówno po stronie dostawców, jak i klienta.

Analiza na podstawie takiej listy pomaga w podjęciu decyzji, czy w obecnej sytuacji warto takie przedsięwzięcie podejmować czy odłożyć je na później lub zrewidować jego definicję.



Na potrzeby projektów systemów informatycznych został opracowany szereg list kontrolnych bardziej szczegółowych, z których na uwagę zasługuje wprawdzie dość „wiekowa”, ale wciąż aktualna lista autorstwa Instytutu SEI. Jest ona próbą ujęcia wszystkich obszarów ryzyka występujących w pełnym cyklu tworzenia oprogramowania i stanowi tzw. taksonomię ryzyka. Zgodnie z teorią taksonomii można zbudować hierarchię klasyfikującą obszary w sposób, który nadaje się do identyfikowania czynników na różnych poziomach szczegółowości. Te poziomy to klasy, elementy i atrybuty. Klasami są: inżynieria produktu, środowisko deweloperskie, ograniczenia programowe. Do każdej z klas można przypisać odpowiednie elementy, np. do klasy inżynierii produktu — wymagania, testy jednostkowe, testy integracyjne itd. Z kolei każdy element posiada swoje atrybuty i przykładowo dla elementu „wymagania” są to m.in. stabilność, kompletność, elastyczność. Pełna taksonomia ryzyka opublikowana jest w dokumencie CMU/SEI-93-TR-6, dostępnym na stronach internetowych Instytutu SEI.

Ważną cechą listy kontrolnej jest łatwość jej stosowania. Obszary powinny być zdefiniowane w sposób, który jest czytelny również dla członków zespołów wykonawczych, czyli w przypadku projektów informatycznych — dla analityków, projektantów, programistów, testerów, wdrożeniowców oraz ich kierowników. Poniżej została przedstawiona przykładowa lista kontrolna ryzyka dla pewnego typu projektów informatycznych. Projekt polega na wdrożeniu oprogramowania, z którego część ma być od podstaw opracowana i wytworzona, a część zakupiona i zintegrowana z nowo opracowanymi modułami; przy wdrożeniu konieczna jest współpraca z dostawcami kupowanego oprogramowania. Lista ta specyfikuje obszary występowania ryzyka i powinna być pomocna przy identyfikowaniu czynników ryzyka zarówno przez twórców oprogramowania, jak i wdrożeniowców.

#### 1. Obszar organizacyjno-zarządczy:

##### a) korporacyjny poziom zarządzania:

- ♦ kultura organizacyjna;
- ♦ stabilność struktur organizacyjnych i własnościowych;
- ♦ stabilność finansowa i rynkowa;
- ♦ procesy zarządcze:
  - Dojrzałość procesów biznesowych.
  - Komunikacja wewnętrzna i zewnętrzna.
  - Planowanie i prognozowanie rozwoju.

##### b) organizacja współpracy z partnerami i dostawcami:

- ♦ zakres i poziom długoterminowych umów partnerskich;
- ♦ kontraktowanie i wsparcie prawne;
- ♦ dostępność zasobów dostawców;
- ♦ polityka zarządzania jakością i wymaganiami;
- ♦ atmosfera współpracy z dostawcami;

- c) zarządzanie projektami:
  - ◆ kultura zarządzania w powiązaniu z działalnością operacyjną;
  - ◆ dojrzałość procesów zarządzania projektami;
  - ◆ doświadczenie;
  - ◆ dostępność kadry zarządzającej;
- 2. Obszar zewnętrzny:
  - a) gospodarka i polityka;
  - b) środowisko, infrastruktura;
  - c) legislacja;
  - d) dojrzałość i kondycja klientów;
  - e) dojrzałość i kondycja dostawców;
  - f) rynek pracy;
- 3. Technika:
  - a) wymagania:
    - ◆ metoda zarządzania wymaganiami;
    - ◆ kryteria akceptacji produktów;
    - ◆ złożoność wymagań;
    - ◆ klarowność wymagań, ich interpretacja przez użytkowników i dostawców;
    - ◆ relacja między oczekiwaniami użytkowników a sformalizowanymi wymaganiami;
    - ◆ proces uzgadniania zmian w wymaganiach;
    - ◆ wymagania dotyczące użytkowników przyszłej eksploatacji systemów;
    - ◆ atmosfera uzgadniania wymagań między stronami;
  - b) moduły zamawiane:
    - ◆ dostępność;
    - ◆ liczba dostawców, możliwość wyboru;
    - ◆ relacje z dostawcami, doświadczenia we współpracy;
    - ◆ sposób uzgadniania specyfikacji;
    - ◆ kontrola jakości produktów finalnych i pośrednich;
    - ◆ kontrola realizacji (terminy, koszty);
    - ◆ zasady odbioru produktów;

- c) wytwórstwo oprogramowania:
- ♦ proces wytwórstwa:
    - Dojrzałość, poziom sformalizowania.
    - Znajomość procesu przez zespoły projektowe.
    - Kontrola procesu.
    - Kontrola produktu, system zarządzania jakością.
  - ♦ zarządzanie:
    - Zarządzanie zespołami, dojrzałość zespołów.
    - Wymiarowanie systemów (szacowanie czasu i kosztów).
    - Zarządzanie jakością.
    - Zarządzanie konfiguracją produktów.
    - Zarządzanie zmianami.
    - Procesy decyzyjne.
  - ♦ przedmiot wytwórstwa:
    - Koncepcja — poziom nowatorstwa.
    - Złożoność.
    - Wieloplatformowość.
    - Wymagania krytyczne (niezawodność, bezpieczeństwo).
    - Wymagania prawne i środowiskowe.
    - Ograniczenia wynikające z infrastruktury.
    - Dostępność komponentów.
    - Wymagania dotyczące kompetencji zespołów.
    - „Testowalność” (możliwość wiarygodnego określenia jakości).
    - Dostępność obsługi.
  - ♦ inżynieria oprogramowania:
    - Specyfikowanie systemów.
    - Projektowanie architektury.
    - Projektowanie systemów bazodanowych.
    - Projektowanie interfejsów użytkownika.
    - Bezpieczeństwo systemów.
    - Zapewnienie niezawodności.
    - Zapewnienie serwisowalności.
    - Testowanie, odbiory.

- ◆ narzędzia:
  - Dostępność, możliwość wyboru.
  - Niezawodność.
  - Złożoność technologiczna, łatwość użycia.
  - Wydajność.
- d) integracja:**
  - ◆ systemy odziedziczone, dokumentacja systemów;
  - ◆ ilość i różnorodność modułów zewnętrznych;
  - ◆ poziom koniecznej modyfikacji systemów dziedziczonych i zakupionych;
  - ◆ jakość danych;
  - ◆ testy integracyjne, narzędzia;
  - ◆ dostępność istniejących systemów w okresie wdrożenia;
  - ◆ zaangażowanie użytkowników systemów w testy akceptacyjne;
- e) infrastruktura techniczna:**
  - ◆ odziedziczona infrastruktura — poziom techniczny, dokumentacja;
  - ◆ specyfikacja wymagań sprzętowych;
  - ◆ wymagane modyfikacje infrastruktury;
  - ◆ dostępność infrastruktury w trakcie projektu;
- 4. Środowisko pracy:**
  - a)** dostępność zasobów;
  - b)** współpraca między zespołami projektowymi a działami operacyjnymi;
  - c)** atmosfera i morale pracowników;
  - d)** komunikacja nieformalna;
  - e)** konflikty, sposoby ich rozwiązywania;
  - f)** współpraca wykonawców z użytkownikami;
  - g)** nastawienie użytkowników do nowych systemów.

Powyższa lista zawiera jedynie obszary, w których występują źródła ryzyka. W trakcie analizy należy bliżej określić te źródła i na ich podstawie zidentyfikować czynniki ryzyka. Przykładowo: w obszarze 3.a.iv (klarowność wymagań, ich interpretacja przez użytkowników i dostawców) źródłem ryzyka są niejasne sformułowania wymagań, które mogą być różnie interpretowane. Rodzi to czynnik ryzyka: „użytkownicy mogą nie uznać pewnej funkcjonalności systemu za zgodną z ich wymaganiami i nie podpisać protokołu odbioru”. Konsekwencją tego może być konieczność negocjacji, a być może dodatkowej pracy polegającej na modyfikacji systemu celem dopasowania go do nowych (?) wymagań. To z kolei skutkuje wydłużeniem projektu, jak również wzrostem kosztów.

Listy kontrolne są nadzwyczaj skuteczną techniką przy wstępnym analizowaniu ryzyka, nie wymagają wielkich nakładów i są łatwe w stosowaniu. Nadają się również do wykorzystania w trakcie realizacji projektu; zakładając, że przynajmniej pod koniec każdego etapu należy przeprowadzić dodatkową analizę ryzyka, identyfikacja nowych czynników jest znacznie łatwiejsza, jeśli mamy do dyspozycji listę, odnoszącą się w szczególności do najbliższej fazy projektu. Zazwyczaj przy uruchamianiu projektu trudno jest skupić się na pozornie mniej ważnych czynnikach związanych np. z fazą testowania systemu. Co najwyżej czynniki związane z tą fazą zostają zidentyfikowane na wysokim poziomie abstrakcji (np. „mogą wystąpić kłopoty przy testowaniu”). Natomiast gdy projekt jest już na etapie integracji systemów, można zauważyć, że np. dane z systemów dziedziczonych mają kiepską jakość, co przy mało wydajnych narzędziach może sprawić bardzo konkretne kłopoty.

Jakość techniki list kontrolnych w dużym stopniu zależy od tego, czy są one uaktualniane i dopasowywane do danego typu projektu. Dlatego nadzwyczaj istotne jest, aby wnioski z zamkniętych projektów, spisane w Raporcie o Doświadczeniach, były wykorzystywane do uzupełniania list kontrolnych.

## Sesje analityczne, burze mózgów

Pod ogólną nazwą sesji analitycznych rozumie się szereg połączonych technik, których używa się w celu pozyskania informacji o ryzyku. W odróżnieniu od metod eksperckich zakłada się, że sporo wiarygodnych danych na temat zagrożeń, a także dodatkowych szans w projekcie można zgromadzić w trakcie spotkań uczestników projektu, w gronie powiększonym o ludzi niezwiązanych z projektem (laików). Oczywiście nie chodzi tu o przypadkową wymianę informacji, ale sterowane sesje, w których uczestnicy, przekazując swoje doświadczenia, posługują się dodatkowo danymi, przede wszystkim pochodzącymi z poprzednich projektów.

Wynikiem sesji analitycznych ma być nie tylko lista zidentyfikowanych czynników ryzyka, lecz również ocena ich parametrów, a w dalszej kolejności dobór środków zaradczych. Wynika z tego, że istotnym elementem tej techniki jest prognozowanie. Powstaje pytanie, jaka może być wiarygodność prognozowania, jeśli w gronie uczestników sesji nie ma prawdziwych, uznanych ekspertów. Michael J. Mauboussin stawia uzasadnioną badaniami tezę („Ile wari są eksperci”, Harvard Business Review Polska, luty 2008), że w przypadku zjawisk probabilistycznych — a z takimi mamy do czynienia przy rozpatrywaniu ryzyka — najbardziej skuteczni okazują się „dobrze poinformowani laicy”. Dotyczy to zarówno okoliczności, w których jest mała swoboda wnioskowania, jak i tych, gdzie ta swoboda jest nieograniczona lub bardzo duża. W związku z tym można uznać, że spotkanie uczestników projektu (część z nich może mieć wiedzę na poziomie eksperckim) z osobami spoza projektu, przy odpowiednim przygotowaniu sesji, może przynieść bardzo dobre wyniki.

Burza mózgów, która może być elementem sesji analitycznej, polega na niczym nieskrępowanej wymianie informacji. Z założenia wszystkie pomysły i opinie nie podlegają krytyce, zatem w wyniku spotkania o takim charakterze pozyskuje się bardzo wiele danych, z których duża część jest albo przynajmniej wydaje się nieprzydatna. Niemniej każdy uczestnik, bez względu na przygotowanie do udziału w projekcie, posiada pewien багаż własnych doświadczeń, który może być przetworzony na informacje istotne przy rozpatrywaniu ryzyka. Odpowiednia atmosfera powinna sprawić, że różne pomysły, pojawiające

się na spotkaniu, mogą zainspirować uczestników do przekazywania swoich ocen, co z kolei generuje wiele nieszablonowych koncepcji. Przydatność tej formy wymiany informacji jest oczywista w kreowaniu koncepcji w pracach badawczych i rozwojowych, natomiast w przypadku analizy ryzyka wskazane jest pewne ukierunkowanie takich sesji, czyli organizowanie „moderowanych burzy mózgów”. Proponowana przez instytut SEI technika oceny ryzyka projektów polegających na tworzeniu oprogramowania (*Software Risk Evaluation* — **SRE**), ma podobny charakter, choć oparta jest na kwestionariuszach taksonomii, czyli listach kontrolnych.

Przeprowadzenie pełnej sesji analitycznej polega na wykonaniu kolejnych kroków:

- 1. Wybór uczestników sesji** — liczba ich powinna oscylować wokół 10. Powinni w niej uczestniczyć:
  - ◆ kierownik projektu;
  - ◆ lider sesji (moderator) — może nim być kierownik projektu lub przedstawiciel biura wsparcia projektu;
  - ◆ przedstawiciel biura wsparcia projektu, spisujący pozyskane informacje, notujący uwagi — funkcję tę może spełniać lider sesji;
  - ◆ członkowie zespołów, których dotyczy rozpatrywana faza projektu; w przypadkach gdy projekt wchodzi w fazę implementacyjną, wskazany jest udział reprezentantów zespołu testerów, kontroli jakości, a także osób odpowiedzialnych za zarządzanie konfiguracją oprogramowania;
  - ◆ kierownicy zespołów — pod warunkiem że potrafią powstrzymać się od okazywania zwierzchnictwa nad członkami swoich zespołów.
- 2. Przygotowanie uczestników**, polegające na wyjaśnieniu procesu analizy ryzyka oraz podstawowych pojęć związanych z identyfikacją i oceną. Najważniejszym elementem tej akcji przygotowawczej jest pełne zrozumienie przez uczestników różnic pomiędzy obszarami i źródłami ryzyka (faktami) a niepewnymi zdarzeniami, czyli czynnikami ryzyka. W drugiej kolejności należy wyjaśnić parametry ryzyka z wyraźnym zaznaczeniem, że prawdopodobieństwo i wpływ na projekt muszą być rozpatrywane oddzielnie, i to dopiero po zidentyfikowaniu czynników. Ważne jest też uświadomienie wszystkim podstawowego założenia, że przy identyfikacji nie bierze się jeszcze pod uwagę zastosowania jakichkolwiek środków zaradczych.

Przygotowanie uczestników może odbyć się w trakcie jednego wspólnego spotkania lub kilku — w grupach o danej specjalności. Można też pogrupować uczestników według poziomu świadomości o zarządzaniu ryzykiem; w takim przypadku w bardziej zaawansowanych grupach przygotowanie będzie polegać głównie na przypomnieniu ogólnych zasad prowadzenia analizy. Na przygotowanie trzeba przeznaczyć — w zależności od doświadczenia uczestników — od jednej godziny do kilku.
- 3. Sesja analityczna cz. I** — jej celem jest sporządzenie listy zidentyfikowanych czynników, ich przynależności do obszarów występowania źródeł ryzyka wraz z propozycją przypisania odpowiednich właścicieli do każdego czynnika. Sesję powinno rozpocząć krótkie wprowadzenie — najodpowiedniejszą osobą

do tego jest kierownik projektu, lecz w przypadku obecności na sesji któregoś z członków komitetu sterującego może być wskazane przekazanie wprowadzenia właśnie jemu. Wprowadzenie powinno zawierać:

- ♦ prezentację obrazu sukcesu projektu; bez względu na to, kto ją przeprowadza, istotne jest zaprezentowanie obu punktów widzenia sukcesu projektu: komitet sterujący koncentruje się na zagadnieniach biznesowych, natomiast kierownik projektu powinien uzupełnić ten obraz wskazaniem priorytetów utrzymania poszczególnych parametrów projektu: harmonogramu, budżetu, jakości produktów;
- ♦ opis podstawowych produktów projektu oraz oczekiwań co do ich parametrów jakościowych;
- ♦ wyjaśnienie ról w projekcie, w szczególności jawne rozróżnienie klienta (zainteresowanego głównie korzyściami biznesowymi) i użytkownika (skupiającego uwagę na produktach i ich jakości);
- ♦ określenie podstawowych parametrów projektu: ramowego harmonogramu, budżetu oraz ich tolerancji;
- ♦ informacje o sposobie realizacji prac projektowych, komunikacji w projekcie, sposobie przyszłej eksploatacji produktów (np. związanym z ich rozproszeniem geograficznym), ograniczeniach operacyjnych;
- ♦ przedstawienie ram tematycznych sesji, czyli poziomu szczegółowości identyfikowanych czynników ryzyka.

Dla kolejnych sesji analitycznych nie wszystkie elementy wprowadzenia będą potrzebne — zależy to przede wszystkim od udziału w sesji nowych członków zespołów.

Kolejnym krokiem powinno być zgłoszenie przez uczestników uwag dotyczących środowiska projektowego, zagadnień, które pojawiły się od ostatniej sesji, a także wniosków na każdy temat związany z ryzykiem. Kierownik projektu może też rozdać przygotowaną wcześniej listę kontrolną, zawierającą specyfikację głównych obszarów i źródeł ryzyka, ukierunkowaną na daną sesję (listy kontrolne zostały omówione w poprzednim rozdziale). Lista może być rozpowszechniona nieco później, po wstępnej analizie ryzyka — ta opcja sprawia, że uczestnicy mogą poszukiwać czynników ryzyka we wszystkich obszarach, nieograniczonych specyfikacją z listy kontrolnej. Sprzyja to szerszemu spojrzeniu na szanse i zagrożenia.

Właściwa analiza przeprowadzana jest poprzez zgłaszanie przez uczestników sesji czynników ryzyka, próbę znalezienia najlepszego ich określenia oraz zapisanie tego w dokumencie wyjściowym (np. „Lista zidentyfikowanych czynników ryzyka”). Kierownik projektu powinien dbać, aby na liście nie pojawiły się źródła ryzyka (fakty), lecz prawdziwe elementy niepewności. Po pojedynczej sesji lista powinna zawierać co najmniej kilkanaście czynników, nie więcej niż 40. Większa liczba czynników może świadczyć o zbytym „rozdrabnianiu się” w identyfikacji szczegółowych zagadnień, przyczyną tego stanu rzeczy może też być niewłaściwie określony zakres sesji analitycznej. W takich przypadkach wskazane jest ściślejsze ograniczenie poziomu identyfikacji: np. wstępna analiza — koncentrujemy się na zagadnieniach biznesowych, analiza

w gronie analityków — koncentrujemy się na wymaganiach i możliwościach ich realizacji itp. Wskazane jest, aby podczas tej sesji zapisać propozycje przypisania do czynników ryzyka najodpowiedniejszych właścicieli.

4. Sesja analityczna cz. II — celem jej jest ocena zidentyfikowanych czynników ryzyka. Sesja ta może być połączona z poprzednią, jeśli nie zostanie przekroczony sensowny limit czasu trwania obu części sesji — wynosi on 2,5 – 3 godzin. W zależności od przyjętego modelu zarządzania ryzykiem ocena może być dokonana poprzez wyznaczenie jednego parametru, np. waga ryzyka: duże, średnie, małe, jednak zazwyczaj stosowany jest model standardowy, polegający na przypisaniu każdemu czynnikowi dwóch parametrów: prawdopodobieństwa i wpływu.

Kierownik projektu powinien na początku tej części sesji wyjaśnić, jak należy rozumieć wpływ na projekt i przypomnieć elementy obrazu sukcesu, wyznaczające priorytety utrzymania poszczególnych parametrów projektu. Następnie powinien określić skalę ocen, która zazwyczaj pochodzi z przyjętej polityki zarządzania. W gronie mniej doświadczonych uczestników sesji wskazane jest podanie skali opisowej („duże, małe, średnie” prawdopodobieństwo lub wpływ). Skala liczbowa (np. wpływ: 1, 2, 3, 4, 5, prawdopodobieństwo: 0,1, 0,3, 0,5, 0,7, 0,9) jest jednak korzystniejsza, gdyż ułatwia szybkie przypisanie priorytetów na liście czynników ryzyka. Z drugiej strony nazwanie wpływu „katastroficznym” czy „marginalnym” ułatwia formułowanie ocen. Kierownik projektu musi — zgodnie z przyjętą polityką zarządzania oraz specyfiką projektu — określić kryteria przypisywania wartości oceny wpływu na projekt. Może to zrobić w odniesieniu do całego projektu lub do poszczególnych jego parametrów. Przykładowe kryteria wpływu zamieszczone są w tabeli 5.2.

**Tabela 5.2.** Przykładowe poziomy wpływu ryzyka na parametry projektu

Poziom narażenia projektu	Wpływ na:			
	wartość biznesową	harmonogram	budżet	jakość produktów
Katastrofalny	zdecydowanie nieopłacalny	znaczne przekroczenie dopuszczalnego marginesu tolerancji	znaczne przekroczenie dopuszczalnego marginesu tolerancji	nieosiągnięcie wymaganych parametrów
Krytyczny	nieopłacalny	groźba przekroczenia tolerancji	groźba przekroczenia tolerancji	problematiczna akceptacja jakości
Średni	na granicy opłacalności	wykorzystanie rezerw w granicach tolerancji	wykorzystanie rezerw w granicach tolerancji	istotne obniżenie parametrów
Marginalny	pewne obniżenie wskaźników opłacalności	niewielkie opóźnienia zadań krytycznych	niewielkie naruszenie rezerw budżetowych	obniżenie poziomu niektórych parametrów
Żnikomy	nieznaczne obniżenie wskaźników opłacalności	wykorzystanie rezerw czasu trwania zadań poza ścieżką krytyczną	możliwe naruszenie rezerw budżetowych	obniżenie poziomu mniej znaczących parametrów



Poziomy wpływ ryzyka mogą być też określone bezpośrednio, np. za katastroficzne dla projektu uważa się przekroczenie budżetu o 50% lub opóźnienie zakończenia projektu o 2 miesiące. Jak widać, definicja kryteriów wpływu może mieć bardzo duże znaczenie przy ocenie ryzyka, a ponadto musi być ona dopasowana do charakteru projektu i okoliczności, w jakich jest on uruchamiany.

5. Sporządzenie raportu oceny ryzyka. Naturalnym sposobem raportowania sesji analitycznej jest wprowadzenie odpowiednich danych do Rejestru Ryzyka. Niemniej jednak wskazane jest opracowanie krótkiego sprawozdania, w którym powinny znaleźć się:
  - ♦ lista czynników ryzyka uszeregowanych według wagi zwanej też ekspozycją; dla modelu standardowego najprościej jest za wagę poszczególnych czynników uznać iloczyn prawdopodobieństwa i wpływu;
  - ♦ lista tych czynników ryzyka, dla których nie udało się uzgodnić któregoś z parametrów (lub obu);
  - ♦ wzajemne zależności pomiędzy czynnikami ryzyka, jeśli udało się je zidentyfikować;
  - ♦ dodatkowe wnioski i uwagi uczestników sesji dotyczące np. przydatności list kontrolnych do oceny ryzyka;
  - ♦ zalecenia dotyczące środków zaradczych (opcjonalnie).



W trakcie oceny parametrów ryzyka należy powstrzymać się przed natychmiastowym identyfikowaniem akcji przeciwdziałających, gdyż zakłóca to obiektywną analizę czynników: częstym błędem jest tu obniżanie oceny danego czynnika, gdyż „wiadomo, jak sobie z tym poradzić” (czyli przyjmuje się *a priori* zastosowanie jakichś środków zaradczych). Prowadzący sesję powinien przypominać uczestnikom, że oceniane są sytuacje, w których nie są zaimplementowane żadne dodatkowe akcje.

6. Sesja analityczna cz. III — ma na celu zidentyfikowanie akcji przeciwdziałających wystąpieniu poszczególnych czynników ryzyka. W niektórych, prostszych przypadkach, możliwe jest połączenie tej sesji z poprzednią, jednak zalecane jest poświęcenie jej odrębnego spotkania. Dzięki temu rozdzielony jest proces oceny od procesu identyfikacji i wyboru środków zaradczych. W przypadku gdy uczestniczą w niej nowe osoby, niezbędne jest wprowadzenie ich w podstawowe zagadnienia zarządzania ryzykiem oraz przedstawienie obrazu sukcesu projektu. Następnie, poczynając od czynników o największej wadze, prowadzona jest dyskusja o możliwych akcjach, które są w stanie obniżyć poziom zagrożenia (lub podwyższyć poziom szansy dla pozytywnych czynników ryzyka). Ułatwieniem identyfikacji akcji jest zdefiniowanie ich kategorii, zgodnie z przyjętą metodyką zarządzania projektem. Najczęściej dla zagrożeń projektu kategoriami tymi są: unikanie (zapobieganie), redukcja, transfer, akceptacja oraz tworzenie planów rezerwowych. Dyskusja powinna obejmować analizę skuteczności środków oraz określenie, czy dana akcja wpływa na obniżenie wpływu, prawdopodobieństwa czy obu tych parametrów. Istotne jest też oszacowanie kosztu zaimplementowania danej akcji. Informacje te niezbędne są do racjonalnego podjęcia decyzji o wyborze jednej lub kilku akcji. Decyzja ta

— zwłaszcza w przypadku wyboru kosztownych akcji — podejmowana jest przez komitet sterujący i na jej podstawie kierownik projektu odpowiednio modyfikuje plany, dopisuje dodatkowe zadania do harmonogramu oraz przypisuje zasoby.

Powyżej wymienione elementy technik analitycznych mogą być stosowane wybiórczo lub w komplecie. Istotna jest jednak kolejność sesji; należy przede wszystkim zwrócić uwagę, aby środki zaradcze nie były identyfikowane przed oceną parametrów poszczególnych czynników ryzyka.

## Profile ryzyka

Wyniki procesów identyfikacji i oceny ryzyka są dokumentowane w Rejestrze Ryzyka, który zawiera — poza opisem każdego czynnika — co najmniej informacje o ich właścicielu, prawdopodobieństwie wystąpienia i wpływie na projekt. Już po pierwszych sesjach poświęconych jakościowej analizie ryzyka ilość danych w Rejestrze jest na tyle duża, że utrudnia priorytetyzację czynników ryzyka. Nie stanowi też skutecznego wsparcia w podejmowaniu decyzji o wyborze odpowiednich środków zaradczych. Pomocne jest tu zastosowanie techniki profilowania ryzyka, która polega na przedstawieniu w postaci graficznej wyników identyfikacji i oceny parametrów poszczególnych czynników. Profil ryzyka gromadzi w jednej tabeli informację o wszystkich (lub najważniejszych) czynnikach, stanowiąc podstawę do dalszej analizy, zwłaszcza w zakresie wyboru akcji przeciwdziałających. Technika ta proponowana jest przez większość metodyk projektowych; w metodyce PRINCE2™ wynikowa reprezentacja graficzna nosi nazwę *Summary Risk Profile*, a w PMBOK® Guide nazywana jest *Probability-Impact Matrix*. Przykład takiego profilu (macierzy) jest przedstawiony na rysunku 5.1.

**Rysunek 5.1.**  
*Profil ryzyka  
dla przykładowego  
projektu*

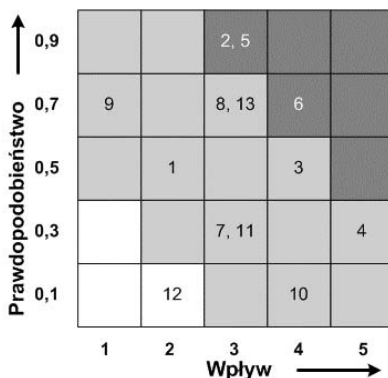
Prawdopodobieństwo ↑	Bardzo duże			2, 5		
	Duże	9		8, 13	6	
	Średnie		1		3	
	Małe			7, 11		4
	Bardzo małe		12		10	
		Bardzo mały	Mały	Średni	Duży	Bardzo duży
		Wpływ →				

W odpowiednich polach macierzy umieszczane są identyfikatory czynników ryzyka, którym wcześniej zostały przypisane oszacowane wartości prawdopodobieństwa i wpływu na projekt. Możliwe jest też przeprowadzanie analizy jakościowej czynników bezpośrednio przy użyciu techniki profilowania — wtedy wyniki oceny czynników zostaną zapisane w Rejestrze Ryzyka na podstawie przydzielonego miejsca w tabeli profilu. Korzystniejsze

jest jednak wcześniejsze przeprowadzenie oceny przy użyciu innych technik (np. w trakcie sesji analitycznych), a następnie zastosowanie profilu do dalszej analizy, przede wszystkim do oceny możliwej skuteczności środków zaradczych. Macierz ryzyka może posługiwać się skalą opisową, jak to przedstawiono na rysunku 5.1, lub odnosić się do liczbowych wartości prawdopodobieństwa i wpływu, jak to jest pokazane na rysunku 5.2. W wielu przypadkach wystarczające jest przyjęcie uproszczonej skali, np.: prawdopodobieństwo — duże, średnie, małe (3, 2, 1); wpływ — duży, średni, mały (3, 2, 1). W tej sytuacji macierz ryzyka będzie miała wymiary 3×3, a nie 5×5.

### Rysunek 5.2.

*Profil ryzyka z liczbowym określeniem wartości parametrów*

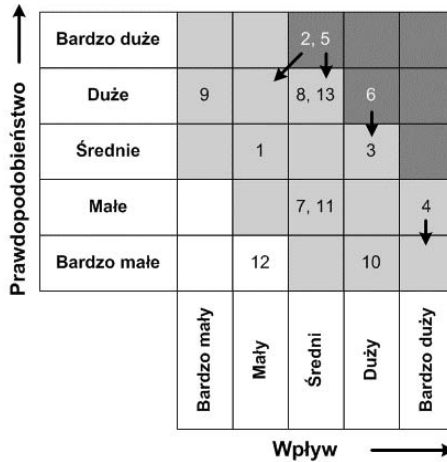


W przypadku liczbowego określenia stopnia wpływu i prawdopodobieństwa wystąpienia czynników można iloczyn wartości tych parametrów potraktować jako miary ryzyka i ewentualnie umieścić je w dodatkowej kolumnie Rejestru Ryzyka.

Jednym z istotniejszych elementów graficznej reprezentacji ryzyka jest ustalenie w profilu strefy zagrożenia, nieakceptowalnej przez komitet sterujący (metodyka PRINCE2™ sugeruje, że strefa ta powinna zostać określona w wyniku uzgodnień komitetu sterującego z kierownikiem projektu). Zaciemniony obszar obejmujący prawe górne pola macierzy na rysunkach 5.1 i 5.2 wyznacza linię graniczną, zwaną linią tolerancji ryzyka lub linią apetytu na ryzyko. Na tych rysunkach zaznaczone zostały również obszary „bezpieczne”, jako przykład możliwego uzgodnienia strefy (pola u dołu z lewej strony), dla której nie podejmuje się żadnych działań zaradczych.

Jeśli jakiś czynnik znajdzie się w strefie poza linią tolerancji, nie zostanie uzyskana zgoda na uruchomienie projektu lub — w przypadkach gdy analiza jest prowadzona w trakcie jego realizacji, np. pod koniec etapu — projekt nie może być kontynuowany. W tej sytuacji rozpatruje się możliwość przesunięcia czynników ryzyka w strefę bezpieczniejszą za pomocą odpowiednich akcji zaradczych. Profil ryzyka jest bardzo wygodnym narzędziem do analizy wpływu danych akcji na poszczególne czynniki. Zazwyczaj działania zaradcze umożliwiają obniżenie wartości prawdopodobieństwa wystąpienia danego zdarzenia, lecz zdarzają się też przypadki, że poprzez odpowiednie działania można zmniejszyć także wpływ danego czynnika na projekt. Przykład wyników takiej analizy przedstawiony jest na rysunku 5.3, gdzie dla czynników o nieakceptowalnym poziomie ryzyka zostały zidentyfikowane i wybrane odpowiednie akcje. Skutkiem tych akcji powinno być przesunięcie identyfikatorów ryzyka w kierunkach zaznaczonych strzałkami — oczywiście ta zmiana parametrów jest również wynikiem szacowania.

**Rysunek 5.3.**  
*Profil ryzyka  
 zmodyfikowany  
 w wyniku wyboru  
 odpowiednich akcji  
 zaradczych*



Podobnie jak dla innych technik szacowania ryzyka, dodatkowym problemem jest konieczność przyjęcia kompromisów dotyczących parametrów projektu; obraz sukcesu projektu powinien m.in. opisywać priorytety, jakie zostają przydzielone budżetowi, terminowi zakończenia i jakości produktów. Priorytety te rzutują na określenie wielkości wpływu czynników na projekt, przykładowo: wpływ ryzyka, które może spowodować wyłącznie opóźnienia prac i odbiorów, nie będzie oceniany jako wysoki, jeśli parametrowi czasu przydzielony zostanie niski priorytet. W bardziej złożonych przypadkach wskazane jest opracowanie profilu ryzyka dla każdego z parametrów: czasu, kosztów, zakresu oraz jakości produktów, a także — a może przede wszystkim — dla uzasadnienia biznesowego projektu. Zakres — w przypadku projektów informatycznych — będzie przede wszystkim rozumiany jako kompletność odwzorowania wymagań klienta i użytkowników przez produkty projektu. Zestaw takich profili, przedstawionych symbolicznie na rysunku 5.4, może też zostać zaprezentowany w postaci skonsolidowanej (np. przy użyciu tabel przedstawianych), po przydzieleniu odpowiednich wag poszczególnym parametrom.

Oczywiście wartość prawdopodobieństwa każdego czynnika pozostaje taka sama dla wszystkich macierzy, zmienna jest tylko wartość wpływu na wybrany parametr projektu. Możliwe jest też ustanowienie różnych granic tolerancji ryzyka dla poszczególnych parametrów projektu, jak to jest pokazane na rysunku 5.4. Jeśli np. czynnik o identyfikatorze nr 11 nie znajduje się w strefie nieakceptowalnego zagrożenia jakości, budżetu i terminu zakończenia projektu, a znalazł się w takiej strefie dla uzasadnienia biznesowego, to projekt nie powinien zostać uruchomiony (lub należy go zatrzymać) z uwagi na duży wpływ tego czynnika na możliwość uzyskania zakładanych korzyści biznesowych.

Profile ryzyka mogą się też posługiwać skalą nieliniową. Przykład profilu, dla którego zdefiniowano w taki sposób wartości wpływu, przedstawiony jest na rysunku 5.5.

Wybór nieliniowej skali wskazuje na awersję do czynników ryzyka mających duży wpływ na projekt. W komórkach macierzy zapisane zostały miary ryzyka, czyli iloczyny wartości prawdopodobieństwa i wpływu przyjętych dla tej nieliniowej skali. W profilu zaznaczone zostały też strefy: nieakceptowalny poziom odpowiada miarom powyżej wartości 1,5, natomiast za strefę bezpieczną uważa się obszar o wartościach poniżej 0,5.



Na podstawie doświadczeń zespołów analityków i programistów, biorąc pod uwagę dodatkowe okoliczności niezbyt formalnego podejścia zarządzania zmianami, określono prawdopodobieństwo takiego zdarzenia jako „duże”. Również duży będzie wpływ tego czynnika na jakość (pewne funkcje mogą zostać przekazane do klienta bez wnikliwego przetestowania), a wpływ na termin oddania gotowych produktów ocenia się na bardzo duży (testy integracyjne prawdopodobnie wykażą konieczność dokonania wielu poprawek w systemie). Wartości wpływu na koszty i uzasadnienie biznesowe przyjęto na poziomie „średnim”, ponieważ zespoły znaczną część poprawek będą musiały poprawiać w ramach już przydzielonego budżetu, a kontrakt z odbiorcą przewiduje tylko ewentualne opóźnienie zapłaty w przypadku konieczności wprowadzania dodatkowych modyfikacji. Gdyby przyjąć miary liczbowe dla prawdopodobieństwa i wpływu tak, jak to pokazano na rysunku 5.2, to otrzymalibyśmy następujące wartości wyników:

$$R_{\text{uzas.bizn.}} = 0,7 \times 3 = 2,1$$

$$R_{\text{koszty}} = 0,7 \times 3 = 2,1$$

$$R_{\text{czas}} = 0,7 \times 5 = 3,5$$

$$R_{\text{jakość}} = 0,7 \times 4 = 2,8$$

Strefy tolerancji ryzyka przedstawione na rysunku 5.4 wskazują na fakt, że najważniejsze dla projektu jest oczywiście uzasadnienie biznesowe, koszty i jakość mają średni priorytet, a dotrzymanie terminowego ukończenia projektu ma wagę najmniejszą. Jeśli przypisać wagi liczbowe do poszczególnych obszarów wpływu na projekt, np. 5, 3, 1, 1, to miarą przedmiotowego czynnika ryzyka byłaby wartość:

$$R = (2,1 \times 5 + 2,1 \times 3 + 3,5 \times 1 + 2,8 \times 3) / 10 = 2,87$$

Jeśli przyjmiemy, że „apetyt” komitetu sterującego na ryzyko nie przekracza wartości 2,5, to bez wykazania, że istnieją środki zaradcze, które mogą zmniejszyć zagrożenie, projekt nie powinien zostać uruchomiony. Nawet gdyby wartość wynikowa była mniejsza od 2,5, to fakt, że wpływ na uzasadnienie biznesowe znalazł się w obszarze poza tolerancją (według rysunku 5.4), nie upoważnia do uruchomienia projektu bez zaplanowania i zaimplementowania odpowiednich akcji.

Dość oczywistym środkiem zaradczym w tej sytuacji wydaje się sformalizowanie systemu zarządzania konfiguracją i zmianami. Drugą akcją przeciwdziałającą mogłoby być zaplanowanie dodatkowych sesji wywiadów analitycznych z przyszłymi użytkownikami systemu, co powinno pomóc w precyzyjniejszym określeniu wymagań funkcjonalnych. Na pewno warto zaimplementować pierwszy środek zaradczy — sprawnie działające procedury zarządzania zmianami są jednym z warunków skutecznego prowadzenia projektów. Można też pomyśleć o zakupie narzędzi informatycznych wspierających zarządzanie konfiguracją oprogramowania; jest to opłacalna inwestycja dla wszystkich firm, które opierają swój biznes na tworzeniu dojrzałych systemów informatycznych. Natomiast nie zawsze udaje się zorganizować dodatkowe wywiady z użytkownikami, którzy zaangażowani są w działania operacyjne i niechętnie godzą się na dodatkowe obciążenia.

Opisane akcje powinny obniżyć prawdopodobieństwo wystąpienia omawianego czynnika ryzyka, natomiast nie zmienią wartości jego wpływu na projekt (jeśli mimo wszystko zajdzie sytuacja, w której scenariusze testowania nie uwzględnią nowej funkcjonalności

