Mendelova univerzita v Brně
Provozně ekonomická fakulta

Management rizika v řízení projektů

Diplomová práce

Vedoucí práce:

doc. Ing. Pavel Žufan, Ph.D.

Bc. Robert Gogela

Brno 2015

Děkuji vedoucímu práce doc. Ing. Pavlu Žufanovi, Ph.D. za metodické vedení, cenné praktické rady a trpělivost při vzniku této práce. Děkuji své manželce, bez jejíhož pochopení a podpory bych nebyl schopen studia úspěšně dokončit.

Čestné prohlášení

Prohlašuji, že jsem tuto práci: **Management rizika v řízení projektů**
vypracoval/a samostatně a veškeré použité prameny a informace jsou uvedeny v seznamu použité literatury. Souhlasím, aby moje práce byla zveřejněna v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů, a v souladu s platnou *Směrnicí o zveřejňování vysokoškolských závěrečných prací.*

Jsem si vědom/a, že se na moji práci vztahuje zákon č. 121/2000 Sb., autorský zákon, a že Mendelova univerzita v Brně má právo na uzavření licenční smlouvy a užití této práce jako školního díla podle § 60 odst. 1 Autorského zákona.

Dále se zavazuji, že před sepsáním licenční smlouvy o využití díla jinou osobou (subjektem) si vyžádám písemné stanovisko univerzity o tom, že předmětná licenční smlouva není v rozporu s oprávněnými zájmy univerzity, a zavazuji se uhradit případný příspěvek na úhradu nákladů spojených se vznikem díla, a to až do jejich skutečné výše.

V Brně dne 1. ledna 2015 _____

Abstract

Gogela, R. Risk Management in Project Management. Diploma thesis. Brno: Mendel University, 2014.
Risk management is an essential part of project management, focusing on effective prevention economic impacts of unexpected events during project implementation. The goal of risk management is to find suitable methods of risk identification and assessment related to a specific project, which will provide accurate information for project leaders to take appropriate measures to minimize potential impacts to an acceptable level. This thesis focuses on practical procedures for risk identification and assessment that can be applied without requiring any special knowledge or time-consuming administrative tasks.

Keywords

Project management, risk management, risk assessment, risk analysis, risk treatment, threat, impact.

Abstrakt

Gogela, R. Management rizika v řízení projektů. Diplomová práce. Brno: Mendelova univerzita v Brně, 2014.
Management rizika je nezbytnou součástí řízení projektů, zaměřenou na účinné předcházení ekonomickým dopadům vzniklým z neočekávaných událostí během realizace projektu. Cílem managementu rizika je ve vazbě na konkrétní projekt nalézt vhodné metody identifikace a vyhodnocení rizik, které poskytnou vedení projektu správné informace k přijetí takových opatření, která minimalizují případné dopady na akceptovatelnou úroveň. Práce se zaměřuje na praktické postupy identifikace a hodnocení rizik, které je možné aplikovat bez větších nároků na specializované znalosti nebo časově náročné administrativní činnosti.

Klíčová slova

Řízení projektů, řízení rizika, hodnocení rizik, analýza rizik, zvládání rizik, hrozba, dopad.

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

Podniky v ekonomicky vyspělých zemích v současnosti čelí při svém rozhodování problému nízké míry návratnosti investic do průmyslových aktivit. Podle zprávy Konference OSN o obchodu a rozvoji (UNCTAD, 2013) je míra návratnosti zahraničních investic ve vyspělých zemích od roku 2008 trvale pod úrovní 5%. Takto nízká míra návratnosti investic do průmyslových aktivit způsobuje, že podniky při rozhodování o realizaci investičních projektů pracují ve svých kalkulacích s údaji „na hraně“ akceptovatelné výnosnosti. Pokud se za takových podmínek přesto podnik rozhodne investici realizovat, může každá nečekaná událost způsobit značné finanční dopady, které mohou vést až k zastavení realizačního projektu. Management rizika realizačních projektů se pak stává klíčovým nástrojem udržení rentability investice.

Téma managementu rizika projektů jsem se pro svou práci rozhodl zvolit rovněž proto, že od roku 1990 pracuji v oboru vývoje, dodávek a podpory provozu rozsáhlých informačních systémů. Za dobu své praxe jsem se podílel na mnoha projektech dodávek informačních systémů, zpravidla v rozsahu desítek až stovek miliónů korun. Většina projektů byla úspěšná, ale měl jsem možnost poznat i projekty, které byly buď během realizace zastaveny, nebo byly dokončeny za zcela jiných realizačních podmínek než při zahájení. V této práci se proto soustředím na management rizika z pohledu projektů vývoje a dodávek rozsáhlých informačních systémů, abych při syntéze teoretických poznatků mohl využít své vlastní praktické zkušenosti.

Informační systémy a technologie dnes zajišťují podporu většiny činností všech typů organizací. Míru závislosti na konkrétních službách informačního systému většina organizací nijak nevyhodnocuje a není vůbec neobvyklé, že její skutečnou míru organizace pozná až v situaci dlouhodobější nedostupnosti. Využívání informačních technologií významně ovlivňuje i rychlost jejich zastarávání, která následně vyvolává i potřebu výměny informačního systému. V České republice jsou informační systémy využívány organizacemi v masovějším měřítku téměř 25 let a dalo by se říci, že to není dlouhá doba. Ve skutečnosti za tuto dobu mnoho organizací již několikrát nahradilo svůj informační systém zcela nově vyvinutým systémem. To je samozřejmě způsobeno více faktory než pouze zastaráváním technologií, mezi významné vlivy patří rozvoj a růst organizací, potřeba sdílení služeb a dat informačních systémů s jinými organizacemi.

Vývoj nových rozsáhlých informačních systémů je spojen s mnoha riziky, kdy mnohá mají původ právě v použití nových technologií, se kterými nemají realizátoři dostatečné zkušenosti. V oboru informatiky totiž dochází k paradoxní situaci, kdy po uplynutí doby, která je potřebná k získání dostatečných zkušeností s používanými technologiemi, jsou tyto technologie nahrazovány novou generací technologií se zcela novými přístupy využívání. Realizátoři projektů vývoje informačních systémů „nových generací“ se pak z důvodu nedostatečných zkušeností musí vyrovnávat s mnoha neočekávanými událostmi, které jsou zdrojem projektových rizik se značnými dopady na průběh a výsledek realizačního projektu.

Projektoví manažeři jsou na jedné straně doslova v „první linii“ komunikace se zákazníkem a realizačním týmem, což jim umožňuje včas identifikovat signály budoucích rizikových událostí. Na druhé straně jsou projektoví manažeři často v situaci, kdy nemají pravomoci ani nástroje identifikovaným rizikům účinně čelit. Takovými pravomocemi zpravidla disponuje projektový výbor či jiný kolektivní orgán, jehož členové nemusí mít osobní kontakt s „první linií“ projektu a mohou se rozhodovat v podmínkách asymetrických informací. Kolektivní rozhodování je spojeno i s dalšími negativními vlivy, jako je potlačení určitosti osobní odpovědnosti za rozhodnutí a zpravidla delší doba pro přijetí rozhodnutí.

Měl jsem možnost poznat projekt zmařené, přestože dokončené, investice v objemu stovek miliónů korun, v důsledku chybného rozhodnutí vedení podniku. Hovořil jsem po zastavení projektu s jeho projektovým manažerem a nikdy nezapomenu na jeho alegorické vyjádření: „*Moje odpovědnost byla postavit dálnici z místa A do místa B podle schváleného zadání, nikoliv řešit, zda po ní bude jezdit dostatečný počet aut.*“. Úkolem managementu rizika je, aby byly v řízení realizačních projektů vytvořeny takové podmínky, které buď omezí pravděpodobnost vzniku nežádoucí události, nebo spustí definovanou proceduru k minimalizaci dopadů. Polovinou úspěchu je pochopení samotného investora, že je nejenom vlastníkem příležitosti, ale rovněž i vlastníkem rizika.

2 Cíl práce a metodika

2.1 Cíl práce

Diplomová práce je zaměřena na návrh praktické metodiky pro řízení rizik vyhovující potřebám soudobého projektového managementu. Významným faktorem současných způsobů řízení realizačních projektů je důraz na jejich ekonomickou efektivitu. Praktickými důsledky jsou minimalizace nezbytných lidských zdrojů, doby trvání dílčích etap projektů a související projektové administrativy. Uvedené důsledky tlaku na ekonomickou efektivitu se odrážejí i v moderních přístupech, jakými jsou metody štíhlého nebo agilního řízení projektů.

Cílem diplomové práce v kontextu soudobých přístupů projektového managementu a praktických zkušeností autora je:

- zmapovat a analyzovat existující metodické nástroje managementu projektových rizik při vývoji a dodávce informačních systémů, k syntéze poznatků využít související mezinárodní normy;
- navrhnout metodické postupy a nástroje řízení projektových rizik, které budou využitelné v projektech vývoje softwarových produktů v rámci dodávek komplexních informačních systémů.

2.2 Metodika

Metodika a struktura diplomové práce odráží analyticko-syntetický přístup, kdy jsou nejprve analyzovány existující teoretické poznatky, které jsou následně metodou syntézy využity k návrhu vlastního praktického řešení. V souladu s tímto přístupem je diplomová práce rozdělena na část teoretickou a část praktickou.

Teoretická část práce je obsahem kapitoly Analýza existujících metod. V teoretické části jsou zkoumány především zahraniční odborné literární zdroje metodik, nástrojů a zkušeností v oblasti řízení rizik projektů se zaměřením na projekty budování informačních systémů. Hlavními metodickými zdroji jsou mezinárodně uznávané modely a rámce managementu rizik:

- klasický přístup (Boehm, 1993);
- metodika ATOM (Hillson et Simon, 2012);
- COBIT 5 for Risk (ISACA, 2013);
- normy AS/NZS 4360:2004 a ISO 31000:2009.

Praktická část práce je obsahem kapitoly Výsledky a návrh praktické metody. V praktické části jsou získané poznatky konsolidovány z hlediska jejich aplikovatelnosti v projektech komplexních dodávek informačních systémů, jichž se autor práce účastnil, do návrhu praktických metodických postupů a nástrojů pro manažery odpovědné za správu projektových rizik.

Návrh metodických postupů a nástrojů v praktické části práce vychází ze struktury všeobecně uznávané mezinárodní normy ISO 31000 a obsahuje:

- *metody identifikace a ohodnocení rizikových událostí*:
  - způsoby identifikace rizikových událostí,
  - možné zdroje a příčiny událostí,
- *metody analýzy a vyhodnocení rizik*:
  - ohodnocení pravděpodobnosti událostí,
  - ohodnocení možných následků událostí,
  - kvalitativní a semikvantitativní metody,
  - vyhodnocení rizik;
- *postupy plánování zvládání rizik*:
  - mapa rizik, registr rizik, způsoby zvládání rizik,
  - plán zvládání rizik;
  - komunikace rizik.

Za teoretickou částí práce následuje kapitola Diskuse. V ní je provedena komparace výsledků praktické části práce s konkrétními zkušenostmi autora z reálných projektů. Součástí kapitoly je i diskuse možných přínosů, nedostatků, nákladovosti a účinnosti aplikace navržených metodických postupů a nástrojů.

V závěrečné kapitole jsou deduktivní metodou na základě získaných teoretických poznatků a výsledků práce formulována praktická doporučení pro aplikaci navržené metodiky v praxi tak, aby přinášela svým uživatelům užitek.

3 Analýza existujících metod

Kapitola tvoří teoretickou část diplomové práce a obsahuje popis zmapování a analýzu existujících metodických nástrojů managementu projektových rizik. Cílem analýzy je získat poznatky o klasických a moderních metodách používaných k řízení rizik při vývoji a dodávkách informačních systémů. Dílčím cílem analýzy je ověřit, které přístupy klasických metod používají a rozvíjejí i metody moderní, a je tak možné je považovat za ověřené a uznávané, a naopak, které přístupy prošly významným přehodnocením nebo byly nahrazeny zcela novými.

3.1 Přehled analyzované literatury

K analýze existujících metod byly využity převážně zahraniční literární zdroje dostupné v anglickém jazyce. Důvodem není nedostatek kvalitní domácí literatury, ale skutečnost, že v praxi jsou zadavateli projektů z řad orgánů veřejné moci i soukromých firem požadovány metodické přístupy založené na mezinárodně uznávaných metodických rámcích a normách.

Následující přehled analyzované literatury obsahuje pouze výčet základní literatury, která byla k provedení analýzy zásadním zdrojem:

- BOEHM, B. W. *Software Risk Management*. 2. vyd. Los Alamitos: IEEE Computer Society Press, 1993. 496 s. ISBN 0-8186-8906-4.
- HALL, E. M. *Managing Risk: Methods for Software Systems Development*. 1. vyd. Reading: Addison-Wesley, 1998. 374 s. ISBN 0-201-25592-8.
- HILLSON, D., SIMON, P. *Practical Project Risk Management: The ATOM Methodology*. 2. vyd. Management Concepts, 2012. 258 s. ISBN 978-1-56726-366-4.
- ISACA *COBIT 5 for Risk*. 1. vyd. Rolling Meadows: ISACA, 2013. 216 s. ISBN 978-1-60420-457-5.
- AS/NZS 4360 *Risk management*. 3. vyd. Sydney: Standards Australia / Wellington: Standards New Zealand, 2004. 38 s. ISBN 0-7337-5904-1
- AS/NZS HB436 *Risk Management Guidelines Companion to AS/NZS 4360:2004*. 3. vyd. Sydney: Standards Australia / Wellington: Standards New Zealand, 2005. 120 s. ISBN 0-7337-5960-6
- ISO 31000 *Risk management – Principles and guideline*. Geneva: ISO, 2009. 24 s.
- ISO/IEC 31010 *Risk management – Risk assessment techniques*. Geneva: ISO, 2009. 176 s.

Přehled veškeré použité literatury je uveden v závěru práce v kapitole Literatura.

3.2 Základní pojmy a principy

Existující mezinárodně uznávané metody managementu rizika nezřídka používají odlišné pojmy pro pojmenování dílčích procesů, jež mají výstižně vyjadřovat jejich obsah. Tento nedostatek se nevyhýbá ani české odborné literatuře či technickým normám.

Pro minimalizaci nejasností spojených s použitím více pojmů z analyzované literatury shrnuji v této úvodní kapitole základní principy managementu rizika. Účelem tohoto úvodního shrnutí je seznámení čtenáře se základními procesy, které jsou společné pro všechny metody managementu rizika. Jejich znalost a pochopení umožní lepší orientaci v analyzovaných metodách i přes určité názvoslovné odlišnosti.

3.2.1 Definice základních pojmů

Následující přehled pojmů obsahuje výčet nejdůležitějších pojmů, který je nezbytný pro uvedení čtenáře do problematiky. Pojmy nejsou uspořádány abecedně, ale jsou členěny logicky podle příslušnosti procesů k základním fázím cyklu managementu rizika. Členění pojmů podle jejich příslušnost k nadřízené fázi je zvýrazněno odsazením a barevným vyznačením.

Tab. 1 Přehled základních pojmů

Pojem	Anglicky	Definice
Riziko	Risk	účinek nejistoty na dosažení cílů; pravděpodobnost události v kombinaci s jejími následky
Management rizik	Risk management	koordinované činnosti pro vedení a řízení organizace s ohledem na rizika
Hodnocení rizik	Risk assessment	celkový proces identifikace rizik, analýzy rizik a vyhodnocení rizik
Identifikace rizik	Risk identification	proces hledání, rozpoznávání a popisování rizik
Analýza rizik	Risk analysis	proces pochopení povahy rizika a stanovení úrovně rizika
Vyhodnocení rizik	Risk evaluation	proces porovnání výsledků analýzy rizik s kritérii rizik k určení významu rizik
Kritéria rizika	Risk criteria	referenční hodnoty parametrů, podle kterých se hodnotí závažnost rizika
Odhad rizika	Risk estimation	proces k určení hodnot pravděpodobnosti a následků rizika

Pojem	Anglicky	Definice
Pravděpodobnost	Likelihood	možnost, že něco nastane; možnost výskytu události
Dopad	Impact	nepříznivá změna dosaženého stupně obchodních cílů
Následek	Consequence	výsledek události působící na cíle (totožný význam jako Dopad)
Zvládání rizik	Risk treatment	proces výběru a přijímání opatření pro modifikaci (změnu) rizika
Redukce rizik	Risk reduction	činnosti ke snížení pravděpodobnosti, negativních následků nebo obou těchto parametrů spojených s rizikem
Vyhnutí se riziku	Risk avoidance	rozhodnutí nedopustit zapojení se do rizikových situací, nebo je vyloučit
Podstoupení rizika	Risk retention	přijetí břemene ztráty nebo prospěchu ze zisku vyplývajícího z určitého rizika
Přenos rizika	Risk transfer	sdílení nákladů ze ztrát s jinou stranou nebo sdílení prospěchu ze zisku vyplývajícího z rizika
Akceptace rizik	Risk acceptance	rozhodnutí přijmout riziko
Komunikace rizik	Risk communication	výměna nebo sdílení informací o riziku mezi tím, kdo rozhoduje a ostatními zúčastněnými stranami

Zdroj: Gogela et al., 2011.

Další související pojmy jsou definovány průběžně v textu u popisované problematiky. V případě, že se jedná o významný pojem, je zvýrazněn kurzívou.

3.2.2 Procesy, metody a rámec managementu rizika

Na management rizika je možné pohlížet ze dvou pohledů:

1. *Procesy* managementu rizika – souhrn dílčích činností v jednotlivých fázích cyklu managementu rizika. Názvy procesů vyjadřují, co se má udělat.
2. *Metody* managementu rizika – souhrn metodických postupů, které jsou zdrojem přístupu k realizaci procesů managementu rizika. Názvy metod vyjadřují, jak se to má udělat.

Z uvedeného je zřejmé, že obsah každého dílčího procesu managementu rizika je determinován použitou metodou. Každý specifický přístup k managementu rizika tak současně obsahuje definici procesů i metod. Souhrnný popis procesů a metod se označuje pojmem *rámec managementu rizika* (z anglického framework).

Příklady typických procesů a metod, které tvoří rámec managementu rizika, a jejich vztah ke dvěma hlavním fázím managementu rizika, tj. hodnocení a zvládání rizik, jsou uvedeny v následující tabulce.

Tab. 2 Příklad typického rámce managementu rizika

RÁMEC MANAGEMENTU RIZIKA		
	PROCESY	**METODY**
HODNOCENÍ RIZIK	• Identifikace hrozeb (zdrojů rizik, událostí) • Ohodnocení pravděpodobností a dopadů hrozeb • Kategorizace závažnosti rizik	• Rozhovory • Skupinové techniky • Dotazníky • Kvalitativní • Kvantitativní • Mapa rizik
ZVLÁDÁNÍ RIZIK	• Plán zvládání rizik • Zavedení opatření • Kontrola a audit	• Definování organizačních procesů a odpovědností • Plánování, sledování a vyhodnocování projektů • Řízení subdodavatelů • Konfigurační řízení • Vzdělávací program

Zdroj: vlastní zkušenosti a práce autora.

3.3 Klasický přístup

Název klasický přístup jsem pro kapitolu zvolil nikoliv proto, že by šlo o zavedený pojem, ale protože v kapitole analyzuji 25 let starý zdroj, který ovšem jako jeden z mála nezastaral. Rozsáhlá sbírka odborných textů o řízení softwarových rizik (Boehm, 1993), kterou shromáždil a publikoval Barry W. Boehm v roce 1989, je dodnes uznávaným a hojně využívaným zdrojem. Proto jsem neváhal nazvat jeho dílo pojmem klasický. Boehm je ve svých 79 letech stále aktivním profesorem a současně i ředitelem centra pro systémové a softwarové inženýrství Univerzity Jižní Kalifornie (blíže viz http://csse.usc.edu/new/barry-w-boehm).

Principy a přístupy publikované ve sbírce profesora Boehma tvoří základ většiny moderních metodik. Důkazem nadčasovosti sbírky budiž např. celosvětově uznávaná metodika řízení projektů PMBOK (PMI, 2013), která fakticky vychází a přebírá mnohé metodické modely profesora Boehma publikované v jeho sbírce. Profesor Boehm, jeho kolegové a žáci publikují značný počet inspirativních textů, které jsou veřejně dostupné (blíže viz http://csse.usc.edu/csse/publication/).

Troufám si tvrdit, že s publikacemi profesora Boehma by se měl seznámit každý projektový manažer působící v oblasti vývoje software.

V předchozí kapitole jsem popsal významový rozdíl mezi procesy a metodami řízení rizik. Pro pochopení klasického přístupu k řízení rizik, který analyzuji v této kapitole, je nezbytné vědět, že profesor Boehm se zabývá oborem systémového inženýrství, jehož je řízení rizik jen jednou ze součástí, která není funkční bez komplexního řízení všech faktorů spojených s vývojem softwarových systémů. Není proto překvapením, že profesor Boehm klade důraz na procesy řízení rizik, tedy aby odpovědné osoby především udělaly vše, co mají udělat.

3.3.1 Zdroje přístupu

Profesor Boehm v úvodu své sbírky (Boehm, 1993) popisuje obecné souvislosti projektových rizik v oblasti vývoje software. Přirovnává oblast vývoje software k jiným oblastem lidských činností. Uvádí, že příčiny projektových katastrof se rodí v raných fázích projektů, a že se jedná o poměrně rozšířený závažný problém. Z průzkumu provedeného časopisem Business Week v roce 1988 mezi 600 firmami vyplynulo, že 35% z nich mělo alespoň jeden softwarový projekt, který skočil nezdarem. Přezkoumání většiny těchto projektů ukázalo, že jejich problémům se dalo předejít, nebo je výrazně snížit, pokud by se firmy začaly včas starat o identifikaci a řešení vysoce rizikových prvků projektu.

Profesor Boehm měl možnost během své kariéry spolupracovat s mnoha manažery softwarových projektů a snažil se identifikovat faktory, kterými se odlišují úspěšnější projektoví manažeři od těch méně úspěšných. Někteří byli schopni úspěšně použít vodopádový model vývoje, jiní zase úspěšně používají evoluční model a mnozí úspěšně použili kombinované modely těchto a dalších přístupů. Jeden faktor, který se projevil velmi silně, ukázal, že *úspěšní projektoví manažeři jsou dobří manažeři rizik*. Ačkoliv většinou nepoužívali takové pojmy jako identifikace rizik, hodnocení rizik, řízení rizik, nebo monitoring rizik, byli úspěšní proto, že to dělali. Jimi řízené projekty měly tendenci se vyhnout nástrahám a vyvinuly dobré produkty.

Jak sám profesor Boehm skromně uvádí, on se pouze pokusil o formalizaci svých poznatků a zkušeností z úspěšných projektů do snadno použitelného souboru zásad a postupů, a přispět do tehdy vznikající disciplíny řízení softwarových rizik.

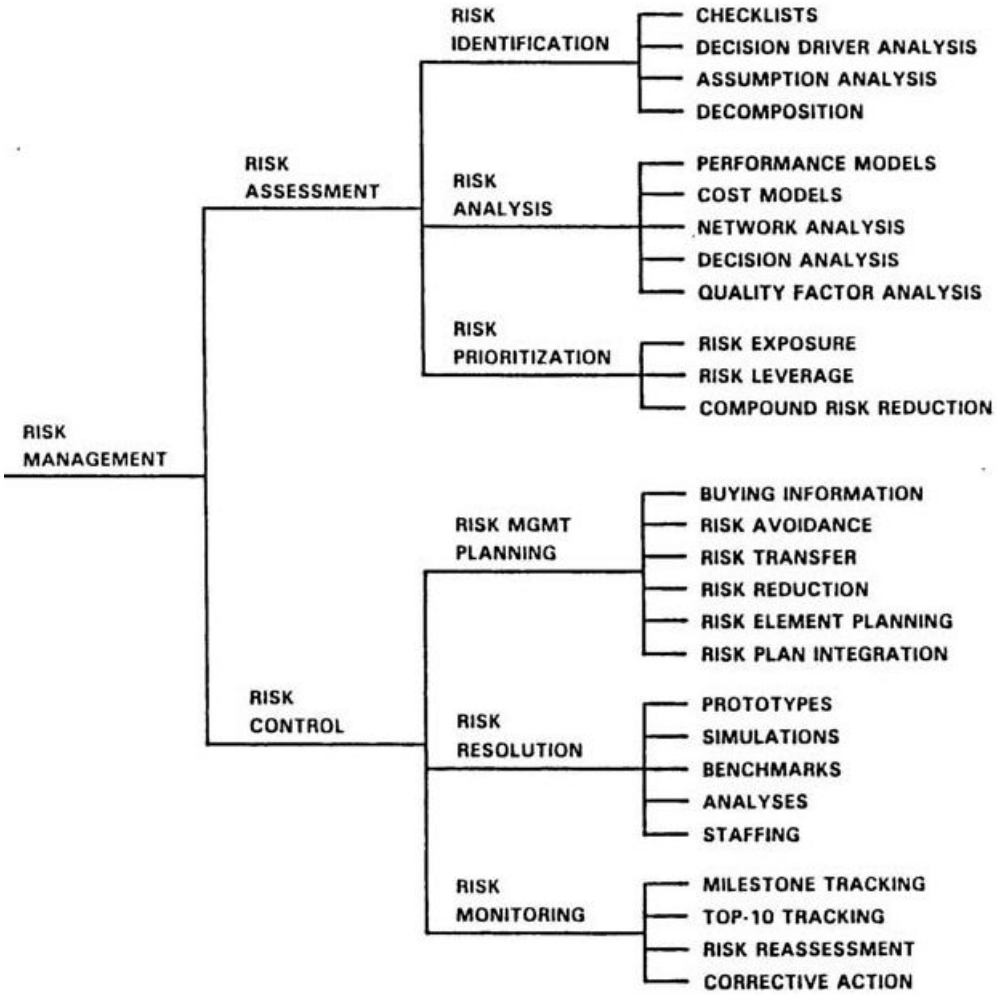
3.3.2 Fáze a kroky managementu rizik

Přístup profesora Boehma k managementu rizik zahrnuje dvě hlavní fáze, posuzování (hodnocení) rizik a řízení (zvládání) rizik, každá se třemi podřízenými kroky:

1. Fáze *posouzení rizik* (hodnocení rizik) zahrnuje kroky:
   1.1. identifikaci rizik;
   1.2. analýzu rizik;
   1.3. kategorizace rizik.

2. Fáze *řízení rizik* (zvládání rizik) zahrnuje kroky:
   2.1. plánování řízení rizik;
   2.2. řešení rizik;
   2.3. monitorování rizik.

Uvedené fáze a kroky managementu rizika znázorňuje následující obrázek.



Obr. 1 Fáze procesu managementu rizik.
Zdroj: Boehm, 1993.

Obsah kroků obou fází managementu rizik stručně uvádím následujícími popisy:

1. **Posouzení rizik** (hodnocení rizik)
   1.1. Identifikace rizik

   Vytváří seznamy rizikových položek specifických pro konkrétní projekt, které mohou s určitou pravděpodobností ohrozit uspokojivý výsledek projektu.

Typické metody identifikace rizik zahrnují seznamy, dekompozice, porovnání se zkušenostmi a dotazování klíčových osob.

1.2. Analýza rizik

Posuzuje míru pravděpodobnosti výskytu a velikosti možné ztráty (následku, dopadu) spojenou s každou z identifikovaných rizikových položek, a posouzení složeného rizika spojeného interakcí více položek.

Typické metody zahrnují síťovou analýzu, rozhodovací stromy, nákladové modely, výkonové modely a statistickou rozhodovací analýzu.

1.3. *Kategorizace rizik* (vyhodnocení rizik)

Seřazuje identifikované rizikové položky do priorit (kategorií) podle závažnosti analyzované míry rizika (funkce pravděpodobnosti a dopadu).

Typické metody zahrnují analýzu vlivu opatření na snížení rizika, zejména analýzu nákladů a přínosů, Delphi a další skupinové techniky.

2. **Řízení rizik** (zvládání rizik)

2.1. Plánování řízení rizik

Vytváří plány, jakým způsobem se bude řešit každá riziková položka (např. vyhnutím se riziku, přenosu rizika, redukcí rizika, nebo získáním informací), včetně koordinace plánů řešení jednotlivých rizikových položek s celkovým plánem projektu.

Typické metody zahrnují kontrolní seznamy rizik se způsoby řešení, analýzu nákladů a přínosů a standardní dokumentovaný plán řízení rizik (obdoba projektového plánu).

2.2. Řešení rizik

Realizuje navržené a schválené způsoby řešení rizikových položek, dokud nejsou rizika eliminována nebo jinak zvládnuta (např. vyhnutím se riziku prostřednictvím zmírnění požadavků).

Typické metody zahrnují prototypy, simulace, referenční měření, rozbor cílů, dohody klíčových osob, vývoj řízený náklady a přírůstkový vývoj.

2.3. Monitorování rizik

Zahrnuje sledování pokroku projektu k řešení rizikových položek a v případě potřeby provedení nápravných opatření.

Typické metody zahrnují sledování milníků plánu řízení rizik a udržování seznamu top 10 rizik, jehož položky jsou revidovány a barevně vyznačeny na týdenní nebo měsíční bázi, nebo při přezkoumání milníku projektu.

Management softwarových rizik je úzce spojen s fázemi životního cyklu vývoje software a ovlivňuje jejich strukturu, obsah a návaznosti. Jak profesor Boehm propojil oba přístupy, popíšu v následujících kapitolách.

3.3.3 Tradiční vodopádový model

Zdrojem přístupu profesora Boehma jsou tradiční modely používané ve vývoji softwarových systémů od 60. let 20. století. V roce 1960 byl poprvé definován souhrnný proces vývoje informačních systémů a pojmenován pojmem *životní cyklus vývoje systémů* (anglicky Systems Development Life Cycle, zkráceně SDLC). Model procesu SDLC specifikoval následující základní fáze vývoje software:

- Plánování (Planning)
- Analýza (Analysis)
- Návrh (Design)
- Implementace (Implementation)
- Údržba (Maintenance)

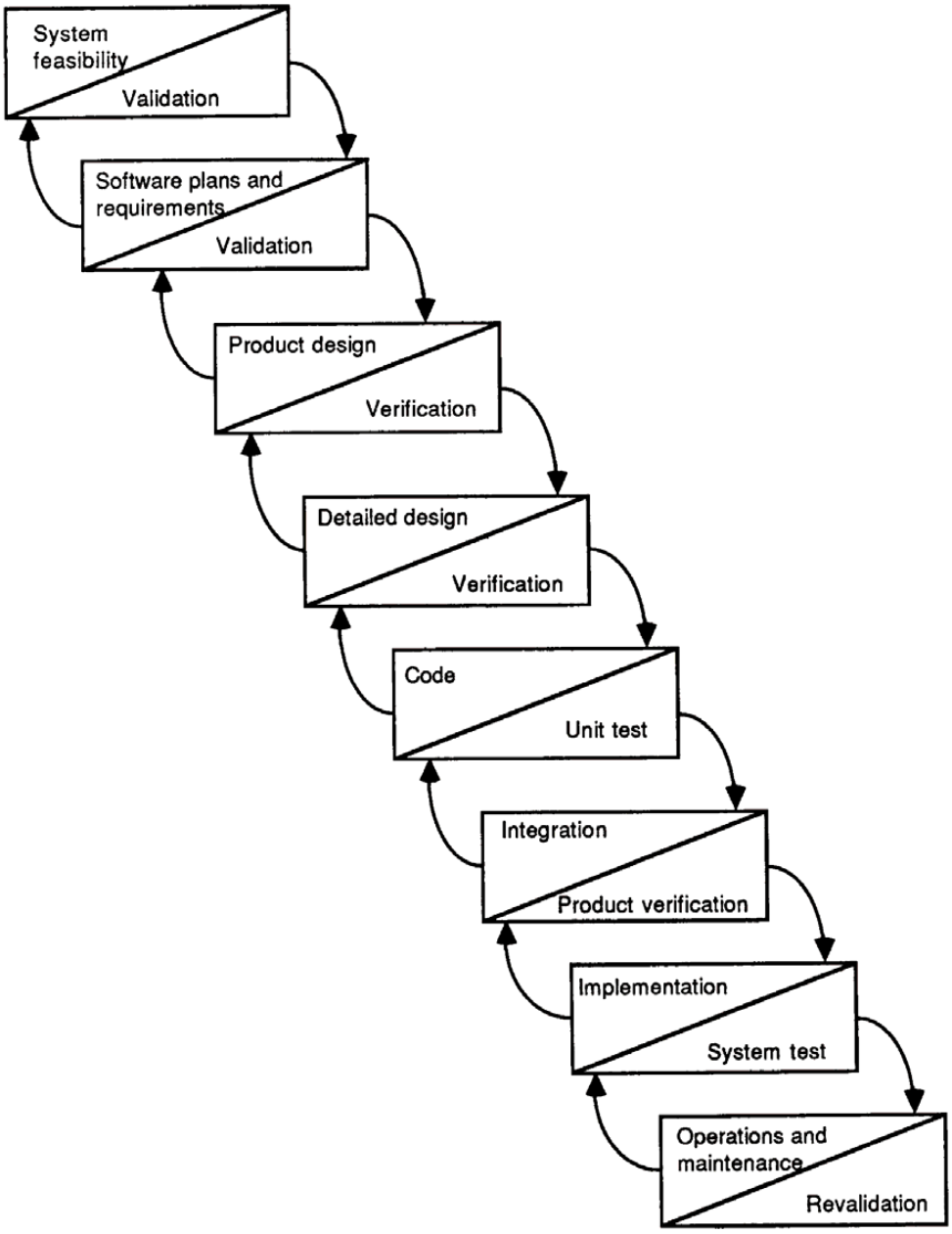
Z modelu procesu SDLC pak byly odvozovány další modely životního cyklu vývoje softwarových systémů, které zpřesňovaly obsah jednotlivých fází procesu vývoje. Nejvíce známým a používaným modelem se stal *vodopádový model*, který v roce 1970 poprvé definoval Winston W. Royce ve svém článku „Managing the Development of Large Software System“ (Royce, 1970). Pojmenování modelu vychází z přirovnání posloupnosti jednotlivých fází k protékání vody vodopádem. Royce se ve svém článku zmiňuje o sedmi základních fázích:

- Systémové požadavky (System requirements)
- Softwarové požadavky (Software requirements)
- Analýza (Analysis)
- Návrh programu (Program design)
- Implementace (Coding)
- Testování (Testing)
- Provoz (Operations)

Princip vodopádového modelu vychází ze sekvenčního přístupu k jednotlivým fázím. Model je charakteristický tím, že jednotlivé etapy životního cyklu se provádějí postupně a vzájemně se neprotínají. Etapy se provádějí podle přesného plánu realizace a zpětně se k nim nevrací, vstoupit do další fáze je možné až tehdy, kdy je předchozí fáze kompletně dokončena a uzavřena.

Vodopádový model lze úspěšně využít v případech, ve kterých je věnován dostatek času počátečním fázím. Jen tak je možné dosáhnout vyšší úspory v pozdějších fázích životního cyklu. Odhalení a odstranění chyby, která je identifikována v počátcích životního cyklu, např. v analýze, je mnohem levnější než kdyby se tatáž chyba opravovala později, např. při testování. V průběhu realizace projektu může nastat situace, kdy návrh softwarového produktu nelze z nějakého důvodu implementovat. Pokud je tato skutečnost zjištěna již ve fázi návrhu, je přepracování návrhu snazší a mnohem méně nákladné, než kdyby byla chyba v návrhu identifikována v dalších fázích.

Existuje mnoho úprav a verzí modelu. Fáze vodopádového modelu ve verzi podle profesora Boehma znázorňuje následující obrázek.



Obr. 2 Vodopádový model životního cyklu vývoje software.
Zdroj: Boehm, 1993.

Jednotlivé fáze životního cyklu vývoje software ve vodopádovém modelu ve verzi podle profesora Boehma obsahují:

- *Studie proveditelnosti* – definuje koncepci softwarového produktu a určuje plán životního cyklu. Ověřujeme: Vytvoříme správný produkt?

- *Analýza a specifikace požadavků* – popisuje, jak problém vyřešit pomocí softwarového systému a specifikuje funkce, provozní schopnosti, očekávané výkonnostní charakteristiky. Ověřujeme: Vytvoříme správný produkt?
- *Celkový návrh* – určuje celkovou softwarovou a hardwarovou architekturu, řídící a datové struktury produktu. Ověřujeme: Vytvoříme produkt podle požadavků?
- *Detailní návrh* – definuje postupy zpracování dat v jednotlivých komponentách produktu, datový model a specifikaci vstupů a výstupů. Ověřujeme: Vytvoříme produkt podle celkového návrhu?
- *Vývoj* – převod postupů zpracování dat definovaných v detailním návrhu do zdrojového kódu a otestování každé vyvinuté komponenty produktu.
- *Integrace* – zprovoznění vyvinutých komponent v testovací hardwarové infrastruktuře a ověření vzájemné funkčnosti všech vyvinutých komponent.
- *Implementace* – nasazení produktu do provozní hardwarové infrastruktury, ověření funkčnosti všech hardwarových a softwarových komponent, ověření funkčnosti rozhraní a ověření výkonnostních charakteristik produktu oproti požadavkům.
- *Provoz a údržba* – specifikace postupů pro instalaci produktu, školení uživatelů, provádění provozní diagnostiky k zajištění dostupnosti systému a rozvoj produktu o další požadovaná funkční vylepšení.

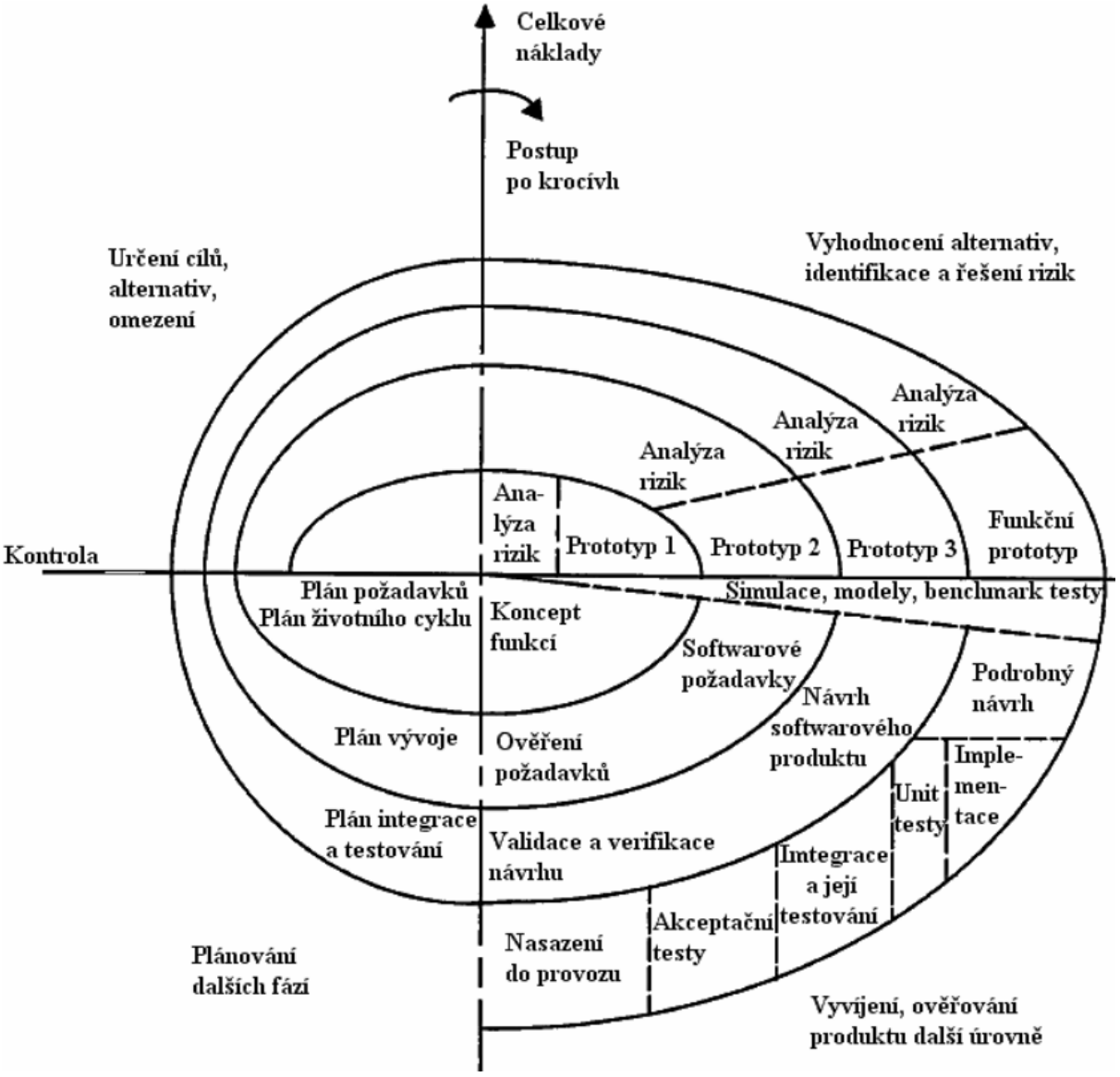
V projektech, které jsou plánovány a řízeny podle vodopádového modelu, musí být každá fáze na svém konci ověřena a musí být potvrzena její kompletnost. Jen tak je možné zahájit následující fázi projektu. Z této skutečnosti vyplývá i hlavní nevýhoda vodopádového modelu. Praxe ukázala, že zejména u rozsáhlejších projektů nelze prakticky dokončit jednu fázi a zahájit další, aniž by se k ní v budoucnu nebylo možné opět vrátit. Požadavky zadavatelů se totiž mohou v průběhu realizace projektu měnit. Zadavatel může vznášet další požadavky, např. po vyzkoušení prototypu produktu. V takovém případě je nutné revidovat výstupy předchozích fází a zapracovat změny do dokumentace.

S jednosměrností modelu, tj. absencí návratu k předchozím fázím, souvisí další problém, že je prakticky nemožné reagovat v průběhu vývojového cyklu na změnové požadavky zadavatele. Finální produkt je zadavateli předán až v době, kdy se nelze vrátit do fází úprav návrhu a vývoje. Tento problém může vést i k neúspěchu celého projektu. Stejná situace může nastat při fázi testování produktu, která následuje samotnou implementaci, tedy v situaci, kdy je produkt téměř připraven k předání zadavateli. Opravy chyb ve fázi testování jsou časově mnohem náročnější, než např. ve fázi návrhu. Pokud se ve fázi testování zjistí zásadní chyba v analýze, může to vést až ke kompletnímu přepracování projektu.

Uvedené nedostatky vodopádového modelu, které měly negativní důsledky především u větších projektů (doba trvání 6 měsíců až 2 roky) vedly k vytvoření mnoha modifikací modelu. Profesor Boehm vytvořil a popsal dodnes aplikovanou modifikaci, spirálový model softwarového procesu.

3.3.4 Spirálový model

Spirálový model vytvořil profesor Boehm v roce 1988. Spirálový model pokrývá hlavní nedostatky vodopádového modelu a je kombinací prototypového přístupu a analýzy rizik. Základním principem modelu je neustálé opakování vývojových kroků, kdy na již ověřenou část systému se v každém dalším kroku přidávají součásti na vyšší úrovni. Postup vývoje v jednotlivých krocích je shodný s původním vodopádovým modelem. Spirálový model, jak jej publikoval profesor Boehm v roce 1988, znázorňuje následující obrázek.



Obr. 3 Spirálový model softwarového procesu.
Zdroj: Boehm, 1993, překlad Tomáš Hlava.

Spirálový model se řadí do skupiny přístupů řízených riziky, ve kterých postup do další fáze závisí na provedení analýzy všech typů rizik a možných problémů. Rizika lze v kontextu spirálového modelu chápat v obecnějším smyslu a mohou například zahrnovat i dopady právních změn nebo marketingu produktu. Model je založen na iterativním přístupu, zavádí opakovanou analýzu všech typů rizik a umožňuje se vyrovnat s pozdější změnou požadavků. Proto je model vhodný pro větší projekty.

Ve spirálovém modelu probíhá vytváření produktu v několika krocích, které se neustále opakují, dokud není produkt hotov. Jádrem modelu je navazování nových částí na již důkladně ověřený základ. Zpočátku se vývoj produktu provádí na základě hrubé specifikace požadavků, v pozdějších fázích je specifikace po konzultacích se zadavatelem postupně zpřesňována.

Životní cyklus softwarového produktu je ve spirálovém modelu rozdělen do čtyř hlavních částí:

- *Určení cílů, alternativ, omezení*
- *Vyhodnocení alternativ, identifikace a řešení rizik*
- *Vyvíjení a ověřování produktu další úrovně*
- *Plánování dalších fází*

Ve spirálovém modelu po každé fázi následuje otestování, vyhodnocení a předání dílčích výsledků. Produkt je tak testován pravidelně již od raných fází vývoje. Tento přístup umožňuje využití automatizovaných testů, testovací případy a scénáře je pak nutné upravit pouze podle aktuální verze produktu. Pravidelné a včasné testování poskytuje příležitosti k včasnému odhalení chyb. Výskyt většího počtu chyb může vyvolat úpravu analýzy, avšak v počátcích vývoje je možné takové úpravy provést mnohem efektivněji než v případě vodopádového modelu.

Přístup profesora Boehma v propojení managementu rizika a životního cyklu vývoje software poskytuje účinný způsob k plánování a řízení větších projektů. Nezbytnou podmínku použití modelu je neustálá spolupráce zadavatele při konzultování požadavků v jednotlivých krocích. Tuto skutečnost lze považovat za výhodu i nevýhodu. Praxe autora diplomové práce ukazuje, že *sdílení odpovědnosti za management rizik mezi zadavatelem a tvůrcem produktu, především společné zvládání a komunikace rizik, je zásadním faktorem úspěchu projektu*.

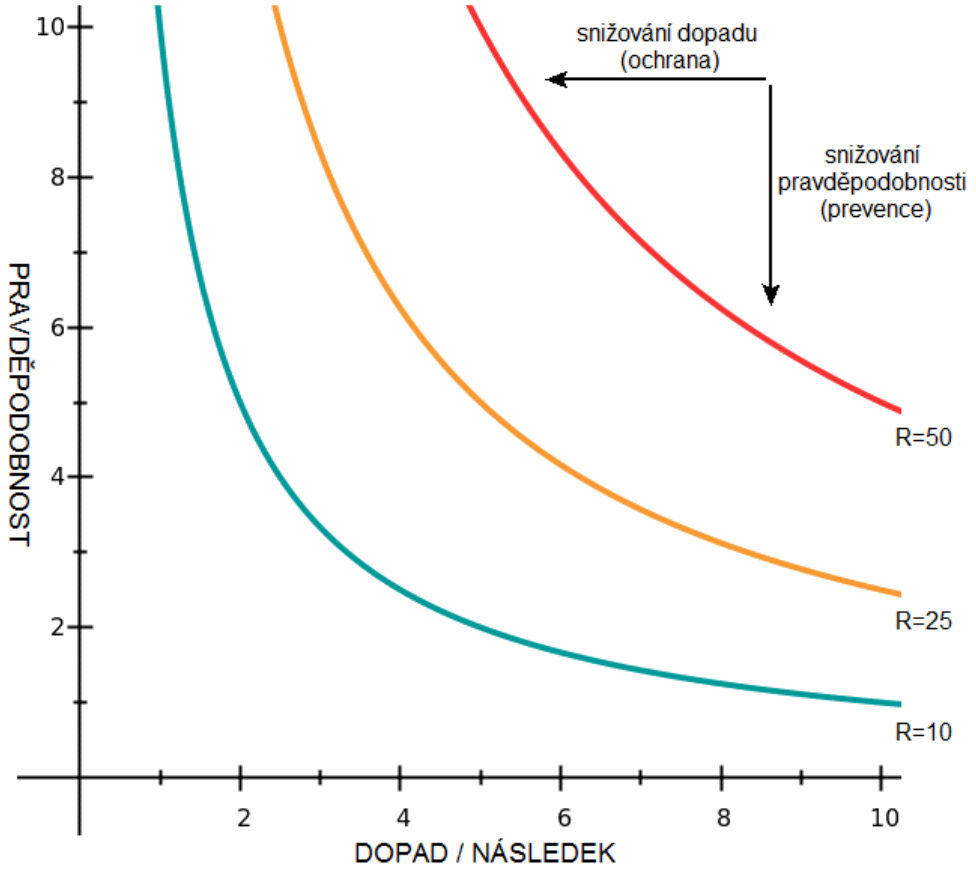
3.3.5 Koncept hodnocení rizik

Charakter rizika nejlépe vystihuje tzv. funkce míry rizika. Funkce míry rizika popisuje funkční závislost mezi proměnnými rizika. Profesor Boehm definuje funkci rizika pojmem *projev rizika* (anglicky Risk Exposure, RE). Projev rizika je funkcí *nevyhovujícího výsledku* (anglicky Unsatisfactory Outcome, UO) a vypočítá se jako součin dvou proměnných, pravděpodobnosti (Prob) a ztráty (Loss[1]):

$$RE = Prob(UO) * Loss(UO)$$

[1] Pojem *ztráta* (Loss) je ekvivalentem pojmů *dopad* (Impact) a *následek* (Consequence)

Míra rizika se ve všech metodikách vždy vyjadřuje jako funkce minimálně dvou proměnných. Dvěma základními proměnnými funkce rizika jsou *pravděpodobnost* výskytu a *dopad* nežádoucí události. Příklady grafického vyjádření funkce rizika znázorňuje následující obrázek.

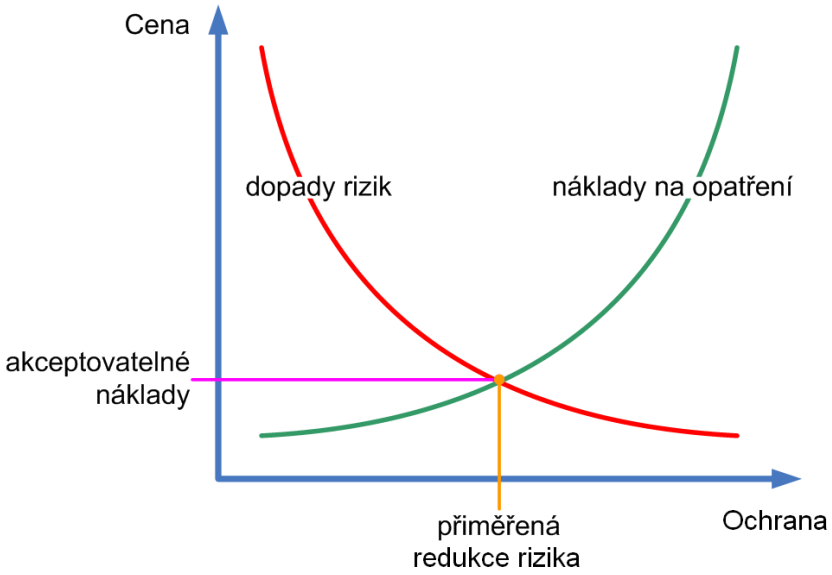


Obr. 4 Příklady tvarů funkcí rizika.
Zdroj: Boehm, 1993, vlastní práce autora.

Z obrázku lze odvodit základní metodu zvládání rizik, a tou je redukce rizika. Riziko lze redukovat buď snižováním pravděpodobnosti výskytu nežádoucí události (prevence), anebo snižováním závažnosti dopadů nežádoucí události (ochrana). Existují ovšem další metody zvládání rizik, jakými jsou vyhnutí se riziku (např. změnou požadavků) nebo přenos rizika (např. outsourcingem nebo pojištěním).

Uvedená dvoufaktorová funkce rizika je nejčastěji používaným způsobem stanovení míry rizika. Existují také analytické a statistické metody stanovení míry rizika, jejichž funkce obsahují další proměnné, např. zranitelnost systému. Funkce rizika s více proměnnými mají složitější matematickou konstrukci a využívají se pouze v kvantitativních metodách při dostupnosti empirických dat. Principy kvantitativních metod hodnocení rizik stručně rozeberu v praktické části práce.

Zvládání rizika jeho redukcí je vždy spojeno s náklady. Proto musíme zvážit, do jaké míry se zvolená opatření k redukci rizik vyplatí. Jde o klasickou analýzu nákladů a přínosu (ceny a užitku). Účinnost opatření, tj. velikost redukce rizika, se na rozdíl od ceny opatření nedá jednoduše kvantifikovat. Všeobecně rozšířená praxe je stanovení velikosti redukce rizika po zavedení opatření expertním odhadem. Vhodné opatření k redukci rizika je takové, které redukuje dopad rizika na dostatečnou (přiměřenou) úroveň za akceptovatelných nákladů. Vztah snižování dopadu rizika opatřením a nákladů na opatření znázorňuje následující obrázek.



Obr. 5 Vztah mezi náklady a redukcí rizika.
Zdroj: Gogela, 2011, upraveno.

Profesor Boehm k výpočtu redukce rizika definuje funkci *účinku redukce rizika* (anglicky Risk Reduction Leverage, RRL) jako poměr snížení projevu rizika (rozdíl RE před a po zavedení opatření) a nákladů na opatření k redukci rizika:

$$RRL = (RE_{before} - RE_{after}) \ / \ \text{Risk Reduction Cost}$$

Z funkce účinku redukce rizika (RRL) profesor Boehm odvozuje důkaz efektivity jeho přístupu v řízení pomocí spirálového modelu. Uvádí jednoduchý příklad výpočtu RRL ve dvou různých fázích projektu řízeného podle vodopádového modelu při opatření ke snížení pravděpodobnosti výskytu rizika:

RRL (Requirements-Design) = (0,3 * $1000K – 0,1 * $1000K) / $20K = 10

RRL (Testing) = (0,3 * $1000K – 0,05 * $1000K) / $150K = 1,67

Zatímco v úvodních fázích projektu (specifikace požadavků – návrh) bude opatření jednoduché a náklady činí 20.000 dolarů, tak v závěrečné fázi projektu (testování) bude opatření podstatně složitější a tomu budou odpovídat i náklady, které činí 150.000 dolarů. Disproporce mezi hodnotami účinku (RRL) je zřejmá.

3.3.6 Doporučení pro praxi

Pro označení projektové role, která odpovídá za řízení rizik, se ustálil pojem *vlastník rizika* (Risk owner). Profesor Boehm se ve svém celoživotním díle snaží poskytovat především praktické rady projektovým manažerům a vlastníkům rizik, než konstruovat složité matematické modely. Jedním z hlavních doporučení je, aby si projektoví manažeři a vlastníci rizik dokumentovali své získané zkušenosti formou vytváření a udržování kontrolních seznamů (tzv. checklist).

Zdrojem schopnosti vlastníka rizik správně identifikovat a ohodnotit rizika je jeho vlastní dlouhodobá zkušenost. Znalost teoretických konceptů je pro vlastníky rizik nikoliv podmínkou, ale výhodou, která jim poskytuje nástroje pro jednodušší správu rizik. Podle profesora Boehma by pro každý projekt měl být identifikován a pravidelně revidován seznam TOP 10 rizik. Sám šel příkladem a ze svých zkušeností takový seznam v roce 1998 vytvořil a není překvapením, že jeho seznam TOP 10 softwarových rizik má dodnes vysoký kredit. Seznam TOP 10 softwarových rizik profesora Boehma shrnuje následující tabulka.

Tab. 3 Seznam TOP 10 softwarových rizik

1.	Nedostatek kvalifikovaného personálu
2.	Nereálné harmonogramy a rozpočty
3.	Vyvíjení špatné programové funkčnosti
4.	Vyvíjení špatného uživatelského rozhraní
5.	Pozlacování (neustálé přidávání funkcí)
6.	Nekončící proud změnových požadavků
7.	Nedostatky v použitých cizích komponentách
8.	Nedostatky v plnění úkolů subdodavateli
9.	Výpadky výkonu v provozním prostředí
10.	Přecenění schopností počítačové techniky

Zdroj: Boehm, 1993.

Existují další zdroje obdobných seznamů TOP 10 kritických softwarových rizik. Na mezinárodní konferenci inženýrů a počítačových vědců, pořádané Mezinárodní asociací inženýrů v roce 2011, vystoupil s příspěvkem Tharwon Arnuphaptrairong, ve kterém prezentoval výsledky svého výzkumu, celkem 12 studií softwarových rizik. Příspěvek (Arnuphaptrairong, 2011) se seznamy TOP 10 rizik je veřejný (viz http://www.iaeng.org/publication/IMECS2011/IMECS2011_pp732-737.pdf).

V návaznosti na doporučení vést projektové seznamy TOP 10 rizik profesor Boehm vytvořil pětibodový plán zvládání softwarových rizik. Konstatuje, že důsledné dodržování těchto pěti bodů je významný počin k vyhnutí se většině příčin kritických projektových selhání. Pětibodový plán shrnuje následující tabulka.

Tab. 4 Plán zvládání softwarových rizik

1. Identifikovat TOP 10 rizik projektu.
2. Vytvořit plán pro řešení každého rizika.
3. Měsíčně revidovat seznam rizik, plán a dosažené výsledky.
4. Prezentovat stav rizik na měsíčních vyhodnoceních projektu.
   - Porovnat se seznamem a stavem rizik předchozího měsíce.
5. Iniciovat vhodná nápravná opatření.

Zdroj: Boehm, 1993.

Zkušenosti autora diplomové práce potvrzují, že složitější proces zvládání rizik už nepřináší podstatná zlepšení. Nezřídka je problémem přesvědčit vlastníky projektu na straně zadavatele i tvůrce produktu, aby takový projektový proces společně zavedli a důsledně prováděli. Neschopnost dohody obou stran o zavedení procesu zvládání rizik je sama osobě významným indikátorem vzniku budoucích problémů a rizik s významnými negativními dopady na úspěch projektu.

3.4 Metodika ATOM

Metodika ATOM (Hillson et Simon, 2012) se od svého uvedení v roce 2007 stala úspěšnou zástupkyní moderních přístupů. Zkratka ATOM se skládá z anglických slov Active Threat and Opportunity Management, česky *Aktivní řízení hrozeb a příležitostí*. Metodika ATOM je příkladem moderních přístupů, pro které jsou typické psychologicko-manažerské techniky, nikoliv matematicko-analytické techniky. V tom autoři metodiky ATOM navazují na doporučení profesora Boehma a shodují se s ním v tom, že největším problémem je přesvědčit management firem a vlastníky projektů o významu řízení projektových rizik a o tom, že i velmi primitivní metody jsou velmi účinné, pokud jsou důsledně používány.

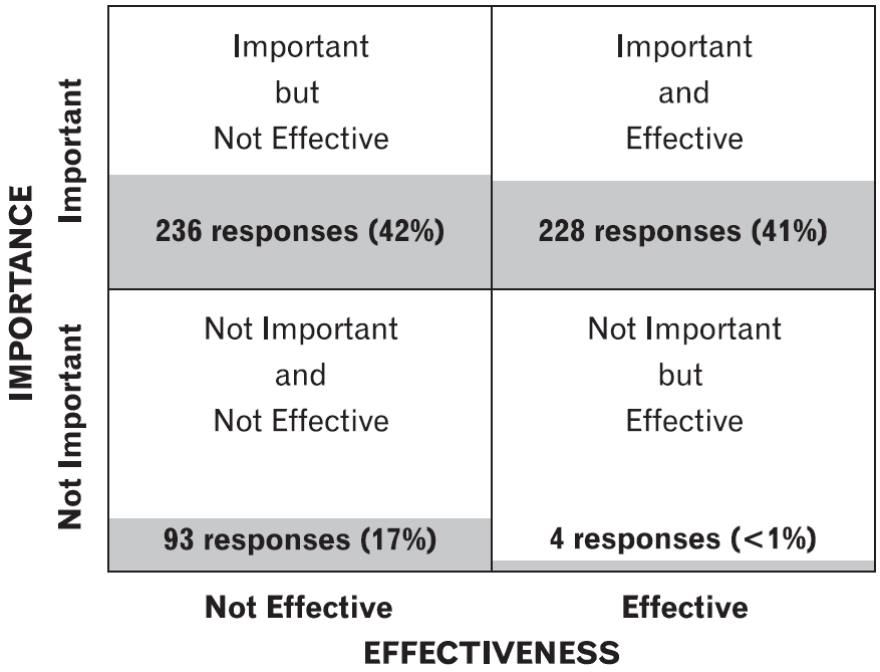
Z uvedeného důvodu obsahuje metodika ATOM velmi jednoduché návody, protože cílem je schopnost jejich osvojení projektovými manažery a vlastníky rizik. Pokud bych měl záměr autorů vyjádřit co nejstručněji, pak bych řekl, že metodika ATOM je popisem důležitého prvku firemní kultury. Publikace (Hillson et Simon, 2012) je napsána srozumitelnou formou a je určena nejen pro manažery, ale pro všechny členy projektových týmu, protože *každý člen týmu je sám příležitostí nebo hrozbou projektu*.

3.4.1 Zdroje přístupu

Autoři metodiky David Hillson a Peter Simon deklarují, že jejich cílem bylo nabídnout jednoduchou příručku, jak provádět management rizika prakticky. Konstatují, že i přes poznání, že řízení rizik je velmi podstatné pro úspěch projektu, tak mnohé výzkumy ukazují, že řízení rizik má nejhorší pověst ze všech technik projektového řízení z pohledu účinnosti jejich používání.

Podle autorů mnohé organizace přiznávají, že hlavní příčinou nízké účinnosti je špatný a neefektivní způsob implementace metod řízení rizik, často jsou příliš složité a jejich používání je časově náročné. Výsledkem je, že mnohé projekty stále selhávají, firmy se stále potýkají s mnoha předvídatelnými problémy a riziky, natož aby zvládaly problémy nepředvídatelné.

Autoři provedli průzkum komplexně posuzující aspekty řízení rizik projektů mezi 561 různými typy organizací. Mezi mnoha aspekty zkoumali i důležitost řízení rizik pro organizace a za jak účinné jej organizace považují. Fascinující pro ně bylo, když provedli korelaci mezi odpověďmi na tyto dvě otázky. Zjednodušení odpovědí na každou otázku do dvou variant (kladná a záporná) dává čtyři možné kombinace, uvedené na následujícím obrázku spolu s procentním podílem respondentů, kteří spadají do každé kategorie.



Obr. 6 Průzkum o důležitosti a účinnosti řízení rizik.
Zdroj: Hillson et Simon, 2012.

Podle autorů je všem jasné, že samotné řízení rizik je v zásadě správné. Koncepty řízení rizik jsou všem jasné, proces je dobře definován na základě osvědčených metod, existují dostupné nástroje na podporu procesu, a existuje mnoho školení k rozvoji znalostí a dovedností v oblasti řízení rizik. Autoři pokládají otázku: Kde je problém? Pokud není v teorii řízení rizik, musí být v praxi. Přesto, že firmy deklarují a zavádějí řízení rizik, aby zvýšily pravděpodobnost projektového a obchodního úspěchu proaktivním řízením účinků nejistoty, realita je jiná.

Autoři dochází k závěru, že problémem není nedostatek pochopení „proč, co, kdo nebo kdy“ na řízení rizik. Nedostatek účinnosti nejčastěji pramení z toho, že se neví „jak na to“. Projektoví manažeři a jejich týmy čelí požadavku dodržování řady

standardů v oblasti řízení rizik, postupů, metod, nástrojů, knih, školení, ve kterých se tvrdí, že řízení rizik funguje. Ale vyvstávají otázky: Jak na to? Jaký způsob zvolit? Jaké metody používat? Jaké podpůrné nástroje?

Metodika ATOM je proto v souladu s výše uvedeným hlavním cílem autorů psána jako příručka, jak řídit rizika v praxi. Pojednává o běžných překážkách pro efektivní řízení rizik a zavádí řadu kritických faktorů úspěchu, jak tyto překážky překonat. Jádro metodiky aktivního řízení hrozeb a příležitostí tvoří obecné metody řízení rizik, které jsou použitelné pro jakýkoliv typ, velikost a obor projektu. K popisovaným metodám autoři vytvořili příklady a nástroje formou šablon, které jsou veřejně dostupné (viz http://www.atom-risk.com/templates.html).

3.4.2 Předpoklady aktivního řízení rizik

Proces řízení rizik, bez ohledu na použitou metodiku, musí splňovat dvě základní podmínky:

1. Rozhodovací pravomoc v řízení projektu je vykonávána osobami s odbornou znalostí specifické náplně projektu, které rozumí i řídícím aktivitám spojených s realizací projektu. Takové porozumění pokrývá všechny aktivity projektového řízení, jako jsou definice rozsahu, principy a financování projektu, finanční řízení, plánování, získávání prostředků, řízení kvality, kontrola změn, přezkoumávání výsledků a další.
2. Proces řízení rizik je integrován s ostatními procesy projektového řízení. To ovlivňuje kromě projektových postupů a nástrojů i celou organizaci projektu. Aktivity řízení projektu musí být plně ovlivněny procesem řízením rizik.

Bez splnění těchto dvou podmínek je málo pravděpodobné, že bude navržen ve všech ohledech realistický plán projektu.

K naplnění uvedených podmínek efektivního řízení rizik je nezbytné správně definovat jednotlivé procesy řízení projektu, vytvořit vhodné nástroje a metody. Definice procesů a vytvoření metod je jen podmínkou nutnou, nikoliv dostačující. Problém spočívá v tom, že většina manažerů, kteří řídí velké projekty, není ochotna anebo schopna metody řízení rizik správně používat. Cílem aktivního řízení rizik projektů je vytvoření jednoduchého, snadno aplikovatelného a dobře zdokumentovaného procesu, který tyto překážky minimalizuje. Autoři metodiky ATOM proto stanovili následující předpoklady efektivního procesu řízení rizik:

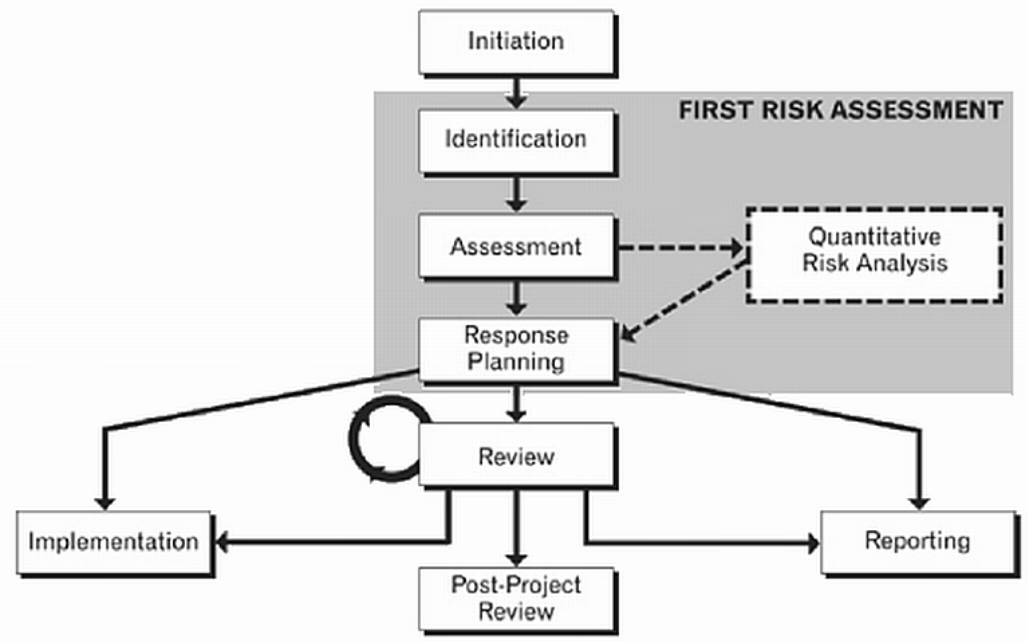
- První krok řízení rizik spočívá v zavedení povinné aktivity, která zajistí, aby byla rizika vůbec identifikována a správně pochopena. Proces efektivního řízení rizik může existovat i vně procesu řízení projektu, ale bez identifikace a vyhodnocení rizik nemůže projekt započít. Pokud proces řízení projektů část řízení rizik neobsahuje, musí být proces řízení projektu doplněn.
- Při definování cílů projektu je nezbytné, aby byly zvažovány všechny možné potenciální události a zdroje nejistot. Potenciálně škodlivé nejistoty (hrozby) musí být identifikovány stejně jako ty, které by pomohly lépe dosáhnout cílů projektu (příležitosti).

- Není nutné řídit všechny nejistoty. Proces řízení rizik musí obsahovat krok výběru, hodnocení a stanovení priorit k rizikům tak, aby byly zdokumentovány největší hrozby a příležitosti. Dále je vhodné zkoumat jednotlivá rizika v interakci s ostatními riziky, zda kumulace jinak nevýznamných rizik není zdrojem rizika s významnými dopady. Užitečné je i stanovit celkový dopad všech identifikovaných rizik na výsledek projektu.
- Po vyhodnocení rizik a stanovení priorit rizik musí následovat rozhodnutí o konkrétních akcích k řešení rizik. Pozornost klíčových osob projektu se musí zaměřit na rozhodování, jak vhodně zareagovat na konkrétní hrozby a příležitosti a jak se vypořádat s celkovým rizikem projektu. Je nezbytné uvažovat o více scénářích, jak rizikům čelit, včetně redefinice cílů projektu.
- Nikdy není možné dosáhnout stavu, ve kterém by řešení rizik byla dostatečné, a které by pokrývalo všechna aktuální rizika. Navíc ani nejlépe definovaný proces řízení rizik nedokáže zajistit okamžitou reakci na identifikovaná rizika. Plánování řešení rizik musí být prováděno ve správném pořadí tak, aby byla zohledněna časová blízkost rizik v průběhu projektu. Podstatné je, aby byly seznamy identifikovaných rizik a plány řešení rizik pravidelně sledovány a revidovány, jedině tak mohou poskytnout požadovaný efekt.
- Uvedené kroky řízení rizik musí být prováděny pouze několika členy projektového týmu odpovědnými za projekt, ale znalost zdrojů rizik a rozhodnutí o zvoleném řešení je důležitá pro všechny členy. Proto je nezbytné o rozhodnutích informovat všechny členy projektového týmu.
- Výsledky analýzy rizik, tj. identifikovaná rizika a jejich hodnocení, se v každém projektu mohou v čase měnit. Proto musí být rizika průběžně znovu posouzena k zajištění vhodného řešení, a toto posuzování musí probíhat během celé doby trvání projektu.
- Efektivní proces řízení rizik v tomto bodě nekončí, protože organizace by se měly z každého realizovaného projektu poučit a získané zkušenosti aplikovat v budoucích projektech. Vyhodnocení po ukončení projektu musí obsahovat i závěry z aplikovaných řešení rizik projektu.

3.4.3 Procesy aktivního řízení rizik

Metodika aktivního řízení rizik ATOM je navržena tak, aby odpovídala požadavku jednoduchého škálovatelného procesu a byla aplikovatelná na všechny typy projektů. Metodika tak přináší spojení osvědčených přístupů, vyzkoušených a osvědčených metod, nástrojů a technik, které jsou kombinovány tak, aby byly snadno použitelné při řízení projektů v praxi.

Každý projekt by měl podle metodiky ATOM zavést proces řízení rizik, který obsahuje osm kroků (fází). Celkový cyklus a souslednost kroků procesu řízení rizik ATOM znázorňuje následující obrázek a jednotlivé kroky popisuje bezprostředně následující tabulka.



Obr. 7 Cyklus kroků procesu řízení rizik ATOM.
Zdroj: Hillson et Simon, 2012.

Tab. 5 Kroky procesu řízení rizik ATOM

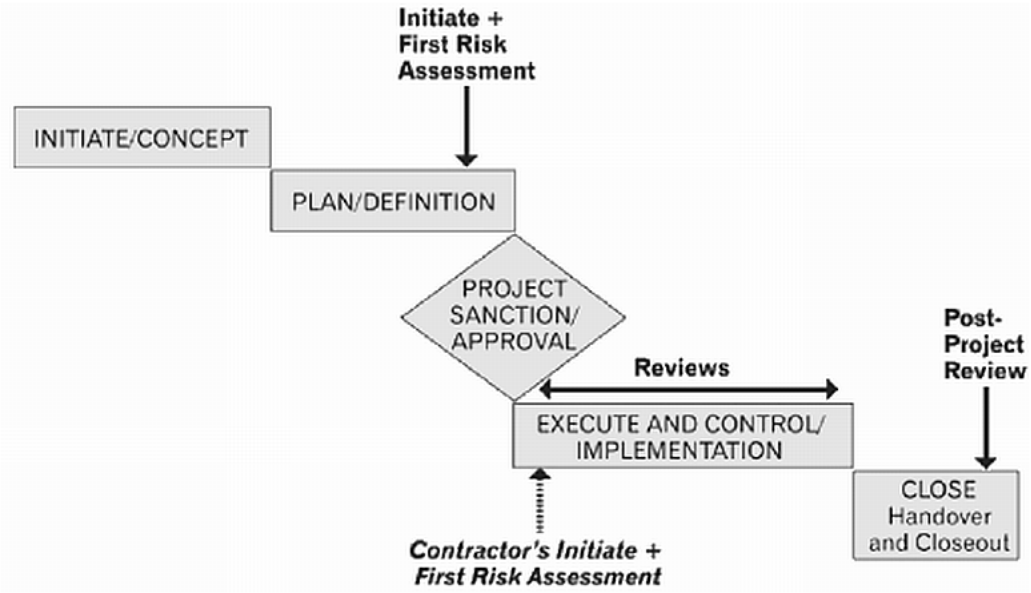
Krok procesu	Činnosti kroku
1. Zahájení	Definice cílů projektu, které byly stanoveny v kontextu zavedeného procesu řízení rizik.
2. Identifikace	Identifikace a zdokumentování pro projekt specifických rizik, která by mohla ovlivnit cíle projektu buď pozitivně (příležitosti), nebo negativně (hrozby).
3. Hodnocení	Stanovení priorit rizik na základě posouzení dopadů jednotlivých hrozeb, ale i závažnosti dopadů působení více hrozeb současně v kombinaci, a určit, které oblasti projektu jsou ohroženy největšími dopady.
4. Plán zvládání	Nalezení alternativních řešení a rozhodnutí o zvolení vhodné strategie a opatření k řešení identifikovaných rizik a určení vlastníka řešení každého rizika.
5. Podávání zpráv	Komunikování aktuálního stavu rizik a výsledků jejich řešení se všemi zainteresovanými stranami projektu.
6. Realizace	Realizace zvolených strategií řešení rizik, zavedení jim odpovídajících opatření a kontrola jejich účinnosti.
7. Přezkoumání	Sledování změn, aktualizace výsledků hodnocení rizik v pravidelných intervalech, zdokumentování revizí.
8. Závěrečné přezkoumání	Získání poučení ze zkušeností po skončení projektu pro zlepšení řízení rizik a řízení projektů v budoucnu.

Zdroj: Hillson et Simon, 2012.

3.4.4 Začlenění procesu do řízení projektu

Úkolem procesu řízení rizik je zkoumání cílů a přínosů projektu, hlavním cílem je snižování dopadů identifikovaných rizik. Cílem zpravidla není rizika eliminovat, ale co nejvíce snížit dopady (např. finanční ztráty) vzniklé při jejich výskytu. Proces řízení rizik je systematický přístup ke snižování dopadů rizik, jehož cílem je zdárný průběh projektu a dosažení očekávaných výsledků.

Začlenění procesu řízení rizik ATOM, jak je znázorněn a popsán na předchozí straně, do fází procesu řízení projektu znázorňuje následující obrázek.



Obr. 8 Začlenění řízení rizika do řízení projektu.
Zdroj: Hillson et Simon, 2012.

Proces řízení projektů má několik charakteristických vlastností, které přímo nebo nepřímo rizika ovlivňují.

Podstatnou vlastností je viditelnost projektu, která je podmíněna prostředky, prostřednictvím nichž může management organizace sledovat, v jaké fázi se jednotlivé projekty nacházejí. Rizika ovlivňují všechny typy projektů, ale projekty vývoje a dodávek software spadají mezi ty nejvíce rizikové. Projekty s abstraktním obsahem, jakým je např. algoritmizace běžných lidských činností, a nehmotnými výsledky jsou vůči rizikům málo odolné. Viditelnost projektů je pro redukci rizik zásadní. Viditelnost projektů je spojena s vyzrálostí všech procesů řízení projektu, jež je současně předpokladem úspěšného zvládání rizik.

Další charakteristickou vlastností řízení projektů je stanovení cíle projektu. Každý cíl je spojen s rizikem. Když stanovujeme cíle, musíme být schopni rizika rozpoznat. Řízení rizik je účinné jen tehdy, pokud projekt má jasně definované cíle. Mezi další charakteristické vlastnosti patří samotný proces vývoje softwarového produktu. Investice do vývoje software jsou veliké a špatně zvládnuté řízení rizik může negativně ovlivnit prodejní výsledky produktu po jeho uvedení na trh.

3.4.5 Metody a nástroje aktivního řízení rizik

Krokem procesu řízení rizik, který je v praxi spojen s největšími překážkami, je hodnocení rizik. Schopnost jeho ovládnutí závisí na použité metodě hodnocení a k ní vytvořených podpůrných nástrojích. Je třeba mít na paměti, že riziko je funkcí pravděpodobnosti a dopadu hrozby (někdy označované zkratkou P-I):

Riziko = pravděpodobnost výskytu hrozby * nežádoucí dopad hrozby

Pro zjednodušení se v praxi nepočítá s přesnými hodnotami pravděpodobnosti a dopadu, protože je téměř vyloučeno je přesně určit. Proto se ke stanovení obou parametrů vytvoří stupnice, která má obvykle alespoň 4 stupně, ne však více jak 7, a jednotlivým stupňům pravděpodobnosti a dopadu se přidělí číselné hodnoty. Někdy se pro oba parametry zvolí lineární stupnice hodnot, tzn. 1, 2, 3, 4…, pak se ovšem výsledná míra rizika vypočítá součtem stupňů pravděpodobnosti a dopadu.

Ke stanovení odpovídajícího stupně pravděpodobnosti a stupně dopadu se v praxi jako pomocné nástroje vytvářejí tzv. vodítka, což jsou příklady událostí s výklady specifickými pro určité prostředí nebo projekt. Tato vodítka pak slouží manažerům projektu a vlastníkům rizik jako nikoliv návod, ale jako pomůcka ke snazšímu stanovení odpovídajícího stupně.

Autoři metodiky ATOM uvádějí příklad vodítek pro stanovení stupně pravděpodobnosti a dopadu hrozby, který je obsažen v následující tabulce.

Tab. 6 Vodítka stanovení stupně pravděpodobnosti a dopadu

STUPEŇ	PRAVDĚPO-DOBNOST	DOPAD NA CÍLE PROJEKTU		
		ČAS	NÁKLADY	KVALITA
Velmi vysoký	71-99%	>20 dnů	>$200K	Zásadní vliv na celkovou funkčnost
Vysoký	51-70%	11-20 dnů	$101K-$200K	Významný vliv na celkovou funkčnost
Střední	31-50%	4-10 dnů	$51K-$100K	Dopad v klíčových funkčních oblastech
Nízký	11-30%	1-3 dny	$10K-$50K	Menší dopad na celkovou funkčnost
Velmi nízký	1-10%	<1 den	<$10K	Menší dopad na sekundární funkce
Žádný	<1%	Bez změny	Bez změny	Žádná změna ve funkčnosti

Zdroj: Hillson et Simon, 2012.

Slabým místem vytváření vodítek je, že mohou být někdy vnímána dogmaticky jako závazný návod, který je důležitější než zdravý rozum hodnotitele. Případná neshoda nad texty vodítek ke zvoleným stupňům má za následek buď degradaci metodiky do příliš triviální podoby, nebo odmítání metodiky některými osobami. V takovém případě je vhodné zamyslet se, zda osoby s takovým přístupem jsou vůbec kompetentní řídit projekty většího rozsahu.

Metodika ATOM doporučuje k identifikaci a hodnocení hrozeb (nehodnotí se riziko, to je funkcí hrozby) použít následující metody a nástroje (techniky):

1. *Identifikace hrozeb*
   - brainstorming se všemi členy projektového týmu spolu se zástupci klíčových dodavatelů;
   - analýza všech předpokladů a omezení projektu, a to jak implicitních, tak explicitních;
   - přezkoumání standardních kontrolních seznamů rizik;
   - ad-hoc identifikace hrozby členy projektového týmu kdykoliv v průběhu projektu;
   - vytvoření výchozího registru rizik se záznamy identifikovaných hrozeb pro další posouzení.
2. *Hodnocení hrozeb*
   - posouzení pravděpodobnosti a dopadu pro každou identifikovanou hrozbu, stanovení odpovídajících hodnot nebo stupňů a výpočet míry rizika;
   - stanovení míry rizika a jí odpovídající závažnosti (prioritě) za použití předem definované tzv. P-I matice pravděpodobností (P) a dopadů (I);
   - vytvoření seznamu TOP rizik a zaměření se na řízení priorit.
   - kategorizace rizik pomocí standardní hierarchické struktury rizik (viz níže) k identifikaci oblastí vystavených rizikům;
   - aktualizace registru rizik (viz identifikace hrozeb) o údaje posouzení.

Pro lepší identifikaci a chápání rizik manažery projektů a vlastníky rizik je vhodné vytvořit tzv. *hierarchickou strukturu rizik* (anglicky Risk Breakdown Structure, RBS). Hierarchická struktura rizik navazuje na koncepci tzv. *hierarchické struktury činností* (anglicky Work Breakdown Structure, WBS), která je nástrojem projektového managementu k rozložení dodávky nebo cíle projektu na jednotlivé dodávané produkty. Technika WBS pomáhá předem stanovit náklady a sledovat postup plnění projektové dodávky. Analogicky je účelem nástroje RBS pomoci předem stanovit rizikové oblasti projektu a strukturovaně sledovat jejich zvládání.

Autoři metodiky ATOM poskytují příklad hierarchické struktury projektových rizik se čtyřmi typickými oblastmi 1. úrovně a 39 oblastmi 2. úrovně. Jejich příklad hierarchické struktury projektových rizik obsahuje následující tabulka.

Tab. 7 Příklad hierarchické struktury rizik

ÚROVEŇ 0	ÚROVEŇ 1	ÚROVEŇ 2
0. RIZIKA PROJEKTU	1. TECHNICKÁ RIZIKA	1.1 Definice rozsahu
		1.2 Definice požadavků
		1.3 Odhady, předpoklady a omezení
		1.4 Technické procesy
		1.5 Technologie
		1.6 Technická rozhraní
		1.7 Návrh
		1.8 Výkon
		1.9 Spolehlivost a udržovatelnost
		1.10 Bezpečí
		1.11 Bezpečnost
		1.12 Testy a akceptace
	2. RIZIKA ŘÍZENÍ	2.1 Řízení projektu
		2.2 Řízení programu
		2.3 Řízení provozu
		2.4 Organizace
		2.5 Plánování zdrojů
		2.6 Komunikace
		2.7 Informovanost
		2.8 Bezpečnost práce
		2.9 Kvalita
		2.10 Pověst
	3. OBCHODNÍ RIZIKA	3.1 Smluvní obchodní podmínky
		3.2 Vnitřní zadávání zakázek
		3.3 Dodavatelé a prodejci
		3.4 Subdodávky
		3.5 Stabilita zákazníka
		3.6 Partnerství a společné podniky
	4. VNĚJŠÍ RIZIKA	4.1 Právní prostředí
		4.2 Směnný kurz
		4.3 Místa, budovy, zařízení
		4.4 Přírodní podmínky, počasí
		4.5 Konkurence
		4.6 Regulační opatření
		4.7 Politická situace
		4.8 Státní zřízení
		4.9 Sociální vrstvy, demografie
		4.10 Nátlakové skupiny
		4.11 Vyšší moc

Zdroj: Hillson et Simon, 2012.

3.5 Metody a nástroje analýzy rizik

Analýza rizik je metodický postup ke kvantifikaci dopadů, které mohou vzniknout jako následek působení nežádoucích událostí na analyzovaný objekt (projekt, systém, atd.). Nežádoucí událost označujeme pojmem *hrozba*. Proces analýzy rizik spočívá v identifikaci a ohodnocení hrozeb, zjištění míry rizika a zařazení rizika do kategorie podle závažnosti. Míra rizika se vypočítá pomocí matematických metod z ohodnocené pravděpodobnosti a dopadu hrozby, případně se bez výpočtu míry rizika přímo stanoví závažnost rizika.

Obsahem analýzy rizik je systematické posuzování, kvantifikace a interpretace možného výskytu nežádoucích událostí a jejich následků.

Cílem analýzy rizik je vyhodnocení závažnosti nežádoucích událostí podle společných kritérií k získání informací k účinnější minimalizaci jejich výskytu anebo následků.

3.5.1 Zdroje metod

K identifikaci, analýze a vyhodnocení závažnosti nežádoucích událostí (hrozeb) se používá logická indukce, vyvozování závěrů z dílčích poznatků. Při analýze rizik se v praxi aplikuje neúplná indukce, protože není možné určit všechny zdroje hrozeb, okolnosti jejich výskytu a ani všechny stavy, které po projevu hrozby mohou nastat.

Pro identifikaci a ohodnocení hrozeb existují dva druhy metod:

1. expertní metody;
2. empirické metody.

Expertní metody jsou založeny na odhadech kvalifikovaných a zkušených osob. Příkladem expertního úsudku je výrok postavy doc. Chocholouška z filmu „Jáchyme, hoď ho do stroje!“, který se omlouval za „politováníhodné nedopatření, k jakému dochází maximálně jednou za 10 let“. Expertní odhad je také svázán s konkrétním časem. Postava doc. Chocholouška se ve filmu jen za několik hodin v ději musela omluvit „za toto politováníhodné nedopatření, ke kterému dochází maximálně… kolikrát, sestro? Třikrát za 10 let.“. Tato zdánlivě ironická scéna ovšem odráží běžnou realitu, a proto je kladen takový důraz na průběžné přezkoumání nebo opakování analýzy rizik.

Empirické metody jsou založeny na vyhodnocení dostupných statistických dat o výskytu, povaze a kvantifikovaných následcích hrozeb. Dostupnost takových dat je v případě hodnocení mnoha typů rizik, včetně projektových, velmi omezená. V případě projektových rizik jen velmi malý zlomek organizací důsledně vede databáze všech možných druhů incidentů včetně údajů o jejich vyhodnocení. Z této skutečnost vyplývá, že použití empirických metod k analýze projektových rizik je stále v rovině teoretického modelování a v praxi je jejich použití ojedinělou výjimkou. Ani autor této práce se během své více jak dvacetileté praxe s reálnou aplikací empirických metod analýzy rizik nesetkal. Přes uvedené skutečnosti však existuje početná odborná literatura na téma empirických metod.

Z uvedeného členění metod pak vycházejí praktické nástroje analýzy rizik, jejichž pojmenování vychází z použité metody:

- kvalitativní analýza rizik – aplikace expertních metod, nestanovuje se míra rizika, ale přímo závažnost rizika;
- semikvantitativní analýza – aplikace expertních metod s využitím matematického aparátu ke stanovení kvantifikované míry rizika;
- kvantitativní analýza – aplikace empirických metod, při kterých se míra rizika zjišťuje výlučně matematickými metodami ze statistických dat.

Následující kapitoly stručně přibližují základní principy používání uvedených nástrojů analýzy rizik, aby bylo v další části práce čtenáři zřejmé, proč a jaký zvolil autor této práce přístup k hodnocení rizik.

3.5.2 Kvalitativní analýza

Kvalitativní analýza rizik je sice nástrojem nejjednodušším, ale nemusí nutně být nástrojem nejméně účinným. Jednoduchost kvalitativní analýzy jednak umožňuje její pochopení širokým spektrem různě zaměřených odborníků, a také zvyšuje pravděpodobnost jejího užití. Jak konstatují i výše analyzované literární zdroje, nejčastějším problémem je, aby organizace vůbec nějakou analýzu rizik prováděly. Proto zavedení i jednoduché kvalitativní analýzy je současně velkou kvalitativní změnou v přístupu organizace k řízení rizik.

Kvalitativní analýza rizik je nástrojem popisným, k vyjádření pravděpodobnosti výskytu hrozby i velikosti jejich následků používá výlučně slovní popis. Z toho důvodu se ani nekvantifikuje míra rizika, ale přímo se určí závažnost rizika, tedy kategorie, která determinuje přístup ke zvládání rizika.

Příklad možného způsobu vyjádření závažnosti rizika pomocí matice ukazuje následující tabulka.

Tab. 8 Příklad kvalitativní analýzy rizik

		Dopad hrozby			
		Malý	Střední	Velký	
Pravděpodobnost hrozby	Malá	**Zanedbatelná**	**Nízká**	**Střední**	**Závažnost rizika**
	Střední	**Nízká**	**Střední**	**Vysoká**	
	Velká	**Střední**	**Vysoká**	**Kritická**	

Zdroj: Hnilica, 2008, upraveno.

Výsledná závažnost rizika se v praxi často vyznačuje barvou, která vizuálně odlišuje přístup k dalšímu postupu řešení rizika. Činnosti spojené s rozhodováním o způsobu řešení rizika patří do následující fáze managementu rizika, označované pojmem zvládání rizik.

3.5.3 Semikvantitativní analýza

Semikvantitativní analýza je kombinací, spíše realistickým kompromisem, analýzy kvalitativní a kvantitativní. Semikvantitativní analýza používá k vyjádření pravděpodobnosti výskytu hrozby a velikosti jejich následků číselné hodnoty, které jsou abstrakcí průběhu funkce rizika (viz kapitola 3.3.5).

Cílem použití škály číselných hodnot je přiblížení se matematickému vyjádření reality, které by mělo poskytovat přesnější výsledky než čistě verbální přístup kvalitativní analýzy. Použití číselných hodnot umožňuje vypočítat výslednou míru rizika součinem hodnot pravděpodobnosti a dopadu. Stejně jako u kvalitativní metody se podle výsledné míry rizika určí závažnost rizika.

Příklad možného způsobu výpočtu míry rizika (výsledek součinu parametrů) a závažnosti rizika (barevně vyznačené kategorie) v maticovém vyjádření ukazuje následující tabulka.

Tab. 9 Příklad semikvantitativní analýzy rizik

		Dopad hrozby (Kč x 1000)			
		10	100	1000	10000
Pravděpodobnost (událostí / rok)	0,0001	**0,001**	**0,01**	**0,1**	**1**
	0,001	**0,01**	**0,1**	**1**	**10**
	0,01	**0,1**	**1**	**10**	**100**
	0,1	**1**	**10**	**100**	**1000**

Zdroj: Hnilica, 2008, upraveno.

Důležité je zdůraznit, že o přiřazení intervalů hodnot mír rizika ke kategoriím závažnosti rizika rozhoduje *vztah k riziku* (anglicky Risk appetite), který je určen individuální charakteristikou tvůrce konkrétního nástroje analýzy rizik nebo jeho uživatelů.

3.5.4 Kvantitativní analýza

Kvantitativní analýza rizik je matematicko-analytický nástroj, který je možné použít v případě dostupnosti dostatečného množství kvalitních statistických dat o nežádoucích událostech a s údaji o rozsahu následků. V takovém případě pak proměnná pravděpodobnost výskytu konkrétního typu události fakticky vypovídá o četnosti, tj. frekvenci výskytu události. Pokud máme k dispozici data o četnosti a rozsahu následků, je možné vypočítat míru rizika s vysokou přesností.

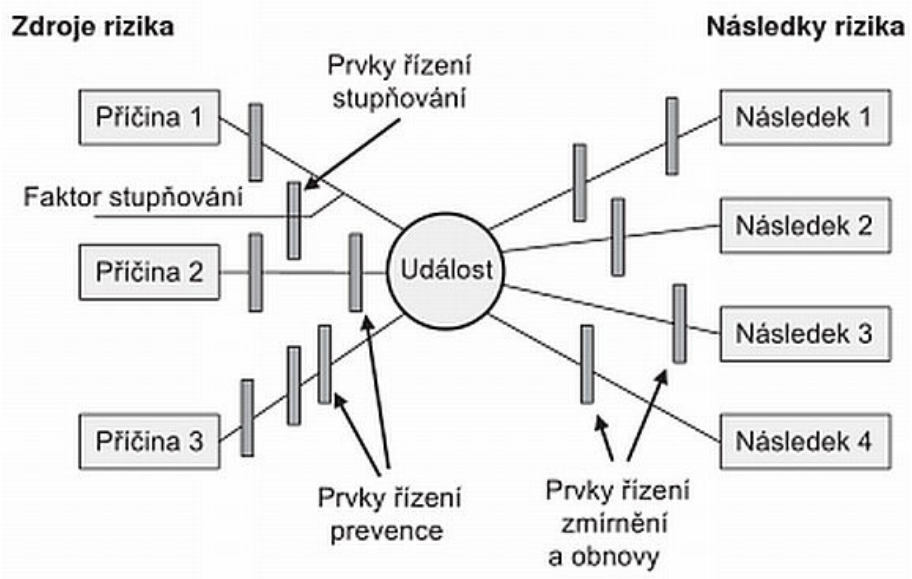
Existují obory podnikání, kde se používá výlučně kvantitativní analýza specifických rizik, jako např. v pojišťovnictví, které disponuje daty o pojistných událostech, nebo v bankovnictví, které disponuje daty o delikvenci úvěrů. Při řízení projektových rizik jsou možnosti vytváření obdobných databází omezené, protože většina projektových selhání se řeší důvěrnou dohodou o vzájemném vypořádání.

3.5.5 Analýza motýlek

Kromě výše popsaných nástrojů analýz rizik, jejichž jádrem je stanovení nebo kvantifikace závažnosti rizika, existují i přístupy řízení rizik, ve kterých je hodnocení a zvládání rizik založeno na metodách logického modelování. Typickým zástupcem logického modelování je metoda analýzy stromu událostí (anglicky Event Tree Analysis, ETA), ve které se používají kauzální analytické nástroje příčin a následků událostí.

Zajímavou zástupkyní logických metod je analýza rizik motýlek (anglicky Bow-tie analysis), která stejně jako analýza stromu událostí analyzuje vztah příčiny a následku. Analýzu rizik motýlek uvádím proto, že její schéma názorně ilustruje význam pojmů *prevence* (snižování pravděpodobnosti hrozby) a *ochrana* (snižování dopadu hrozby), které jsou znázorněny v grafu funkce rizika na obrázku č. 4 v kapitole 3.3.5.

Schéma analýzy rizik motýlek znázorňuje následující obrázek.



Obr. 9 Analýza rizik motýlek.
Zdroj: Korecký et Trkovský, 2011.

Na schématu je zřejmý vztah příčina-událost-následek, jejichž vzájemné vazby je možné ovlivňovat:

1. *Prevencí* – vkládáním prvků řízení prevence příčin, nebo prvků řízení stupňování příčin, ke snížení pravděpodobnosti výskytu události.
2. *Ochranou* – vkládáním prvků řízení zmírnění a obnovy ke snížení následků událostí, tj. ochranou před dopadem událostí, které se uskuteční.

4 Syntéza metod podle normy ISO 31000

Kapitola tvoří přechod mezi teoretickou a praktickou částí diplomové práce. Obsahuje syntézu teoretických poznatků z předchozí části práce a praktických zkušeností autora práce s hodnocením a řízením rizik, které získává od roku 1997 v oblasti řízení rizik bezpečnosti informací. Cílem kapitoly je komplexně popsat důležité prvky zavedení procesu řízení rizik a nástroje, kterými se realizuje provádění jednotlivých fází procesu. Seznámení s obsahem kapitoly poskytne čtenáři dostatečné základy k vytvoření své vlastní metodiky hodnocení a řízení rizik.

4.1 Riziko, jeho řízení a zdroje syntézy

V úvodu kapitoly považuji za užitečné shrnout základní informace, co je riziko a proč má smysl se zabývat jeho řízením. Definice v úvodu práce definuje riziko jako účinek potenciální nejistoty na dosažení cílů. Zásadní je uvědomění, že riziko není nedostatek nebo problém. Riziko je výsledek působení události. Např. pokud se manažer projektu rozhodne realizovat projekt s poddimenzovanými lidskými zdroji, tato skutečnost sama osobě není rizikem, ale problémem. Rizikem v takové situaci může být událost nesplnění termínu odevzdání nebo odmítnutí zadavatele akceptovat výstup z důvodu nízké kvality. Nedostatek personálu je zdrojem uvedených příkladů rizik, nikoliv rizikem samotným.

Rizika jsou spojena se všemi oblastmi podnikových činností, proto rozlišujeme mnoho typů rizik. Nejběžnější typy rizik uvádí následující výčet:

- bezpečí a zdraví osob
- bezpečnosti informací
- bezpečnosti majetku
- finanční
- investiční
- kvality výroby
- obchodní a marketingová
- ochrany životního prostředí
- personální a kompetenční
- podvodů a korupčního chování
- projektová
- provozní
- smluvních vztahů
- strategického směrování

Rizika jsou spojena se soustavnou činností týmu odborníků, ne jednoho člověka.

Efektivní řízení rizik poskytuje organizacím jasné přínosy. Mezi přímé přínosy patří lepší plánování akcí, lepší využití příležitostí, lepší plánování a výkon, zacílení zdrojů, vyvarování se zbytečných výdajů. Řízení rizik má i další neměřitelné přínosy, které spočívají ve zlepšení vztahů mezi spolupracovníky, zkvalitnění informací pro rozhodování, větší důvěryhodnost pro investory, věřitele, pojistitele, zákazníky. Vedení organizace poskytuje řízení rizik zlepšení jejich ochrany, demonstrování úrovně zákony požadované „náležité péče“ a pozitivně může být i dobrý pocit z vlastního příspěvku k ochraně zdraví, životního prostředí a pracovních jistot.

Proces porozumění podstatě rizika a určení jeho úrovně se označuje pojmem *analýza rizik*. Provádí se formou odhadu velikosti rizika (pravděpodobnosti události), se zohledněním dopadu události (následků). Riziko je funkcí pravděpodobnosti události a následků události. Vyjádření rizika se obvykle provádí zařazením do kategorie v relativní verbální stupnici (např. nízká, střední, vysoká) označované pojmem *závažnost rizika*. Absolutní vyjádření rizika se provádí jen výjimečně (např. velikostí ztráty).

Praxe ukazuje, že obor managementu rizika je ve stádiu rychlého rozvoje, trpí roztříštěností terminologie a často nepřesnou až zcela nesprávnou interpretací používaných pojmů. Tato roztříštěnost se nevyhýbá ani českým překladům mezinárodních norem (ČSN) vydávaných Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví. Příkladem je používání pojmů hodnocení a vyhodnocení, které mají v kontextu řízení rizik zcela odlišný význam. Vyhodnocení rizik je závěrečným krokem fáze hodnocení rizik.

Zdrojem syntetické části práce je soubor moderních mezinárodních norem pro management rizik, jejich ekvivalentů v českém jazyce a praktické zkušenosti autora práce s jejich aplikací. Hlavními zdroji zpracování syntézy je řada norem spojených s normou ISO 31000:2009, které vycházejí z dřívější australské normy AS/NZS 4360. Jedná se o následující normy:

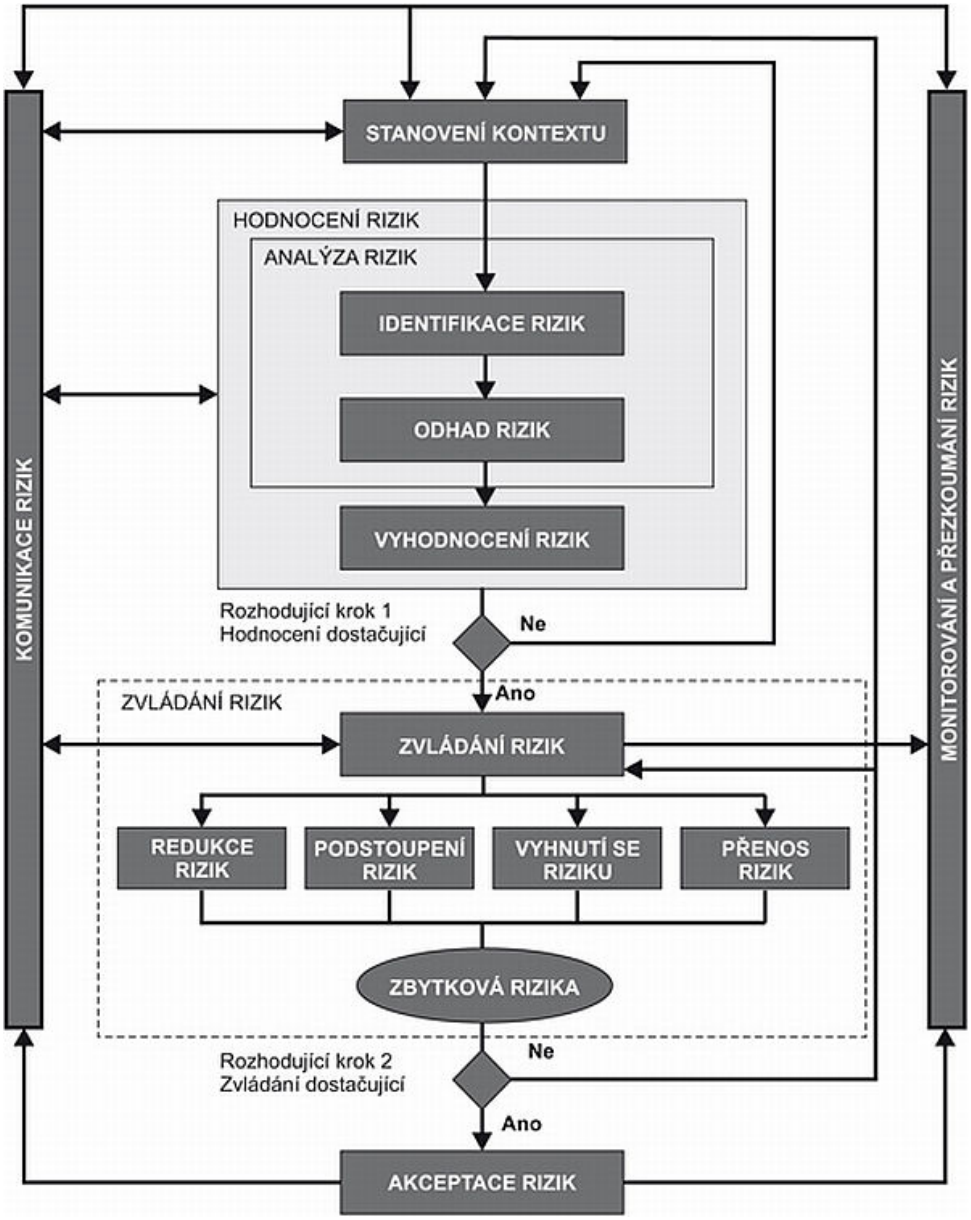
- ISO Guide 73:2009 *Risk management – Vocabulary*
  - TNI 01 0350:2011 *Management rizik – Slovník (Pokyn 73)*
- ISO 31000:2009 *Risk management – Principles and guidelines*
  - ČSN ISO 31000:2010 *Management rizik – Principy a směrnice*
- ISO 31010:2009 *Risk management – Risk assessment techniques*
  - ČSN EN 31010:2011 *Management rizik – Techniky posuzování rizik*
- AS/NZS 4630:2004 a HB 436:2004 (původní australská norma a příručka)

4.2 Zavedení procesu řízení rizik

V první části syntézy se soustředím na klíčové prvky procesu řízení rizik, jež jsou podstatné, aby organizace se záměrem řídit systematickým způsoben jakýkoliv typ rizik zavedla. Pro zavedení procesu řízení rizik v organizaci je nezbytné, aby byly nejprve zdokumentovány jeho postupy (co dělat) a nástroje (jak to dělat). Aby byly popisy správně pochopeny, musí být stručné, srozumitelné a konkrétní.

4.2.1 Fáze řízení rizik podle ISO 31000

Technicky zaměření lidé často požadují schéma, protože „řekne víc než tisíc slov“. Proces řízení rizik podle ISO 31000, jeho fáze, nástroje a vzájemné vazby komplexně znázorňuje následující obrázek.



Obr. 10 Proces řízení rizik.
Zdroj: ČSN ISO/IEC 27005:2009, upraveno.

Obrázek existuje v české verzi ve více variantách, z hlediska struktury i použitých pojmů je nejpřesnější nikoliv ten z normy ČSN ISO 31000, ale z českého překladu starší normy ČSN ISO/IEC 27005:2009 k technikám řízení bezpečnosti informací.

Proces řízení rizik podle ISO 31000 tvoří šest hlavních fází:

1. **Stanovení kontextu** – definice cílů řízení rizik, specifikace klíčových aktivit, stanovení organizační struktury a odpovědností.
2. **Hodnocení rizik** – zdokumentování metodiky hodnocení rizik, analýza rizik, vyhodnocení rizik, výstupem je seznam rizik s přiřazenou závažností.
3. **Zvládání rizik** – rozhodování o způsobu zvládání rizik jejich redukcí, podstoupením, vyhnutím se, nebo přenosem, výstupem je plán zvládání rizik.
4. **Akceptace rizik** – formální akceptace plánu zvládání rizik, kterou vedení organizace nebo projektu stvrzuje svůj závazek přidělení potřebných zdrojů.
5. **Komunikace rizik** – nastavení komunikačních kanálů a způsobu výměny a sdílení informací mezi zainteresovanými stranami.
6. **Monitorování a přezkoumání rizik** – sledování stavu zvládání rizik, vyhodnocování incidentů, pravidelné přezkoumávání, zlepšování.

Praxe ukazuje, že zdar zavedení fungujícího procesu řízení rizik ovlivňují tří základní faktory úspěchu:

- *Úloha vedení organizace a projektu* (fáze stanovení kontextu)
- *Nastavení komunikačních kanálů* (fáze komunikace rizik)
- *Monitorování a zlepšování* (fáze monitorování)

Uvedené faktory reprezentují pojmy často uváděné autory zdrojů teoretické části práce, kterými jsou důslednost a spolupráce. Ovládnutí činností dvou hlavních fází procesu, hodnocení a zvládání rizik, je samozřejmě také důležité, ale pokud nejsou splněny uvedené tři faktory, nepomůže ani použití metod a nástrojů nejlepší praxe. Tři základní faktory úspěchu zavedení procesu si více rozebereme.

4.2.2 Úloha vedení organizace a projektu

Klíčovým problémem systému řízení rizik je dosažení souladu se strategickým směrováním organizace a v případě řízení projektových rizik s cíli projektu. To je důvodem, proč proces řízení rizik začíná fází stanovení kontextu. Bez znalosti cílů organizace nebo projektu není možné formulovat jim odpovídající cíle řízení rizik. Cíle řízení rizik jsou výstupem fáze stanovení kontextu, jejich dokumentovaná podoba se obvykle pojmenuje Politika řízení rizik.

Cíle organizace nebo projektu je nutné si uvědomovat vždy, bez ohledu na způsob řízení rizik. Rizika mají vždy dopad na cíle organizace nebo projektu. Pokud se snažíme rizika řídit systémově, pak bychom vždy měli identifikovaná rizika srovnávat s cíli organizace nebo projektu. Každé identifikované riziko by mělo být spojeno s konkrétním cílem nebo cíli. Pokud cíle nejsou stanoveny, nejsme schopni dostatečně argumentovat, proč je určitá hrozba rizikem. Pokud vedení organizace nebo projektu nekomunikuje své cíle, můžeme považovat za hrozbu něco, co je ve skutečnosti vědomým záměrem vedení.

Podstatné jsou interní cíle organizace a projektu, nikoliv marketingová hesla. Interní cíle organizace a každého projektu musí být proto formulovány explicitně, dokumentovaně a konkrétně. Typickým příkladem špatně formulovaných cílů jsou deklarace typu „cílem je spokojený zákazník“. Příkladem konkrétního strategického cíle organizace je formulace: „minimální průměrná ziskovost projektů je 20%“. Obdobně v případě projektu je příkladem cíle formulace: „vytvořit prototyp aplikace a získat souhlas zákazníka s konceptem do 3 měsíců od zahájení projektu“.

Neméně důležitým výstupem fáze stanovení kontextu je, aby vedení organizace nebo projektu přidělilo pro aktivity řízení rizik dostatečné zdroje a určilo odpovědnosti v procesu řízení rizik. Nezbytnými zdroji jsou jako v případě jiných řídících aktivit zdroje finanční, lidské, materiální a odborné. Prakticky to znamená, aby organizace disponovala lidmi s dostatečnou kvalifikací a zkušenostmi, metodikami a nástroji pro řízení rizik a jeho jednotlivé fáze.

Stanovení odpovědnosti v procesu řízení rizik znamená:

- určit vlastníky rizik, kteří odpovídají za správu oblastí rizik a mají k tomu potřebné pravomoci;
- určit osoby odpovědné za:
  - nastavení, implementaci, údržbu a rozvoj procesu řízení rizik,
  - administraci procesu řízení rizik,
  - realizaci procesu řízení rizik na jednotlivých úrovních organizace,
  - definici měřítek, monitoring, podávání zpráv a eskalační proces,
  - řízení specifických (vybraných) hrozeb a akcí k jejich zvládání.

4.2.3 Nastavení komunikačních kanálů

Nastavení komunikačních kanálů je jedním z nejdůležitějších procesů v řízení rizik. Komunikace otevírá proces řízení rizik všem zainteresovaným osobám, řízení rizik nesmí být něco, čemu málokdo rozumí, nebo se týká jen několika „expertů“.

Nastavení komunikace v řízení rizik není výstupem, ale procesem, jehož cílem je včasné ovlivňování, nikoliv opožděné direktivní vymáhání. Proces komunikace je vstupem pro rozhodování zainteresovaných osob, nikoli prostředkem k přenesení odpovědnosti na jinou skupinu nebo osobu. Rozlišujeme komunikaci jednosměrnou (zprávy, informace, operativní schůzky) a obousměrnou (porady, workshopy, diskusní fóra). Proces komunikace při řízení rizik je významný tím, že:

- posiluje důvěru obchodních partnerů ve vztahu k organizaci (projektu);
- zkvalitňuje posuzování rizik, porozumět rizikům může jen skupina, nikoliv jednotlivec;
- spojuje síly ke zvládání rizik společných více zainteresovaným osobám;
- integruje pohledy na rizika lidí různých profesí a zaměření (provozní pracovníci, techničtí experti, členové projektových týmů, osoby s rozhodovací pravomocí).

4.2.4 Monitorování a zlepšování

Monitorování, přezkoumání a hodnocení musí prostupovat všemi fázemi procesu řízení rizik a pozitivně je motivovat k jejich dalšímu zlepšování. Účinná kontrola je podmínkou dosažení cílů všech lidských činností, nejenom řízení rizik. Proto musí být monitorování a získávání poučení plánovanou součástí procesu řízení rizik.

Prioritou monitorování řízení rizik musí být především sledování všech vysokých rizik od určité úrovně, vyhodnocování nezdarů při zvládání rizik, a to zejména rizik s velkou pravděpodobností výskytu a rizik s vysokými následky, a sledování změn v organizaci nebo projektů souvisejících s riziky.

Monitorování procesu řízení rizik se provádí buď neplánovaně formou kontroly, nebo plánovaně formou pravidelných interních auditů. Hlavním zdrojem pro efektivní monitorování stavu jednotlivých rizik jsou registry rizik. Nezbytnost existence důsledně vedeného registru rizik zdůrazňuje prakticky veškerá odborná literatura. Ze stejného důvodu v závěru analýzy klasického přístupu řízení rizik (viz kapitola 3.3.6) doporučuje profesor Boehm vést seznam TOP 10 rizik projektu, protože i jednoduchý registr rizik je mnohem účinnější než žádný.

4.3 Nástroje a techniky řízení rizik

Ve druhé části syntézy se zabývám praktickými otázkami, způsoby a nástroji práce s riziky, které jsou důležité pro zvládnutí dvou pilířů procesu řízení rizik, fáze hodnocení rizik a fáze zvládání rizik. Pochopení a ovládnutí popisovaných nástrojů činí řízení rizik stejně snadné jako je řízení automobilu. Analogii s ovládnutím řízení automobilu uvádím zcela záměrně, protože ve skutečnosti principy nástrojů řízení rizik jsou velmi jednoduché a důležité je „dostat je do krve“, manažer rizik není odbornost, ale *zkušenost transformovaná do přístupu k dosahování cílů*.

Kapitola popisuje podstatné nástroje a techniky k hodnocení a zvládání rizik, mezi něž autor práce na základě svých zkušeností řadí:

- formulaci rizik;
- identifikaci rizik;
- analýzu rizik;
- vyhodnocení rizik;
- zvládání rizik.

4.3.1 Formulace rizik

Formulací rizika je myšlen popis nežádoucí události – hrozby ve fázi identifikace rizik. Formulace rizika je zcela zásadní problém, protože většina nezdarů řízení rizik má původ ve špatné formulaci rizik.

Hrozbou, která vytváří riziko, je určitá událost, kterou definujeme takto:

Určitá událost = událost, která může, ale nemusí nastat.

Ve fázi identifikace rizik formulujeme možné hrozby třemi možnými způsoby. Příklady možné formulace hrozeb jsou:

1. *Určitá událost vedoucí k dopadu na stanovený cíl*
   - Krupobití poškodí zboží při přepravě, vznikne přímá finanční ztráta.
   - Únik oleje do řeky poškodí pověst společnosti na lokální úrovni.
2. *Určitá událost vlivem zdroje rizika*
   - Finanční ztráta vlivem poškození zboží přepravovaného při krupobití.
   - Poškození pověsti společnosti na lokální úrovni vlivem úniku oleje do řeky.
3. *Určitá událost*
   - Průnik neoprávněné osoby do systému.
   - Neúmyslná chyba administrátora.
   - Požár.

Při identifikaci rizik se zkoumají příčiny (hrozby) a jejich různé následky (dopady), ale pro jejich formulaci a hodnocení hrozby v dalším kroku se uvažuje jen dopad s největšími následky.

4.3.2 Identifikace rizik

Cílem identifikace rizik je sestavit seznam formulovaných hrozeb a dopadů, které budeme dále zkoumat. Seznam zkoumaných rizik může být průřezový pro celou organizaci (projekt), nebo může být specifický pro určitou oblast činnosti organizace (část projektu).

Seznam rizik by měl obsahovat pouze zřetelně významná rizika, jinými slovy s využitím Paretova pravidla by seznam rizik měl obsahovat jen 20% ze všech zkoumaných hrozeb, které mohou způsobit 80% škod ze všech dopadů. Vytvoření seznamu rizik je kritický krok řízení rizik, protože to, co nebude v seznamu obsaženo, nebude následně analyzováno a řízeno.

Identifikace rizik a vytvoření seznamu rizik není úkolem jednotlivce. Naopak je ale nezbytné, aby jednotlivec identifikaci rizik řídil a koordinoval. Osoby, které se účastní identifikace rizik, by měly postupovat podle následujících bodů:

1. identifikovat událost (hrozbu), která ovlivní splnění cílů;
2. pojmenovat možné zdroje a příčiny;
3. zvážit všechny možné dopady na splnění cílů;
4. posoudit i existující opatření, co by se stalo, kdyby neměla účinek;
5. vzít v úvahu místo a čas, kde a kdy jsou rizika možná.

Pro identifikaci rizik je vhodné využít existující katalogy rizik, což jsou seznamy generických rizik specifických pro určitý typ rizik. Katalogy rizik obsahují klíčová rizika pro určitou oblast činnosti nebo aktivitu projektu.

Katalogy projektových rizik jsou většinu dostupné jako hierarchické struktury rizik RBS (viz tabulka č. 7 v kapitole 3.4.5). Katalogy generických rizik jsou nejčastějším nástrojem používaným poradenskými firmami.

Výhodami katalogů rizik jsou zobecněné zkušenosti, zejména ve specializovaných oborech (bezpečnost potravin, bezpečnost informací, jaderná bezpečnost). Slabinou katalogů rizik je jednak velký počet položek, které v konkrétním projektu nemusí být relevantní, a dále, že obsahují pouze názvy oblastí rizik (tzv. generická záhlaví rizik), které samy o sobě nejsou riziky. Jak jsme si řekli výše, je nezbytné rizika přesně formulovat. Katalogy rizik je proto nutné chápat jen jako pomůcku a používat je tvůrčím způsobem.

Dalšími nejpoužívanějšími zdroji a technikami identifikace rizik jsou:

- korporátní metodiky;
- sběr názorů expertů;
- strukturované rozhovory;
- diskuse zainteresovaných osob, brainstorming;
- výsledky kontrol a zprávy z auditů;
- průzkumy a dotazníky;

4.3.3 Analýza rizik

Cílem analýzy rizik je odvození (výpočet) míry rizika, která je dvourozměrnou veličinou pravděpodobnosti události a jejího dopadu. Analýza rizik typicky obsahuje:

- ohodnocení pravděpodobnosti události;
- ohodnocení následků události.

Odvození míry rizika se provádí některým ze způsobů výpočtů podle následující tabulky. Matematické operace (+; *) používají semi- a kvantitativní metody.

Tab. 10 Způsoby výpočtu míry rizika

	Způsob výpočtu	**Použití**
Riziko =	Funkce (pravděpodobnost; dopad)	Obecný tvar
	Verbální stupnice závažnosti rizika	Kvalitativní metody, verbální parametry
	Stupeň pravděpodobnosti + Stupeň dopadu	Lineární stupnice všech parametrů funkce
	Pravděpodobnost * Dopad	Relativní hodnoty pravděpodobnosti, nelineární stupnice
	Pravděpodobnost * Dopad * Váha	Teoretické modely s dalšími parametry

Zdroj: vlastní zkušenosti a práce autora.

Pro řízení zvolené oblasti rizik je volba vhodné metody analýzy rizik a její následné stabilní využívání. Střídání metod způsobuje zbytečnou roztříštěnost, brání nasazení společných softwarových nástrojů a komplikuje provádění monitorování rizik. Metody a nástroje analýzy rizik byly popsány v kapitole 3.5, proto na tomto místě uvedu, jaké podmínky ovlivňují volbu konkrétní metody:

- Kvalitativní analýza rizik
  - vhodná jako úvodní analýza;
  - používá se, když kvantitativní vyjádření není možné nebo není požadováno, nebo když by to bylo neekonomické (čas, náklady).
- Semikvantitativní analýza rizik
  - nejčastěji používaná metoda, stupnice doplněná hodnotami,
  - vyžaduje popisy interpretace číselných hodnot (tzv. vodítka).
- Kvantitativní analýza
  - nejpřesnější metoda,
  - lze použít pouze tehdy, když lze získat dostatek statistických dat.

Nejčastěji používaná metoda semikvantitativní analýzy rizik vyžaduje, aby její uživatelé interpretovali jednotlivé stupně pravděpodobnosti a dopadu obdobným způsobem. K tomuto účelu se vytváří nástroj označovaný pojmem *vodítka*. Vodítka jsou zpravidla formou tabulky, jejíž sloupce obsahují různé pohledy vyjádření pravděpodobnosti a různé pohledy vyjádření velikosti dopadu.

Příklad vodítek pro stanovení pravděpodobnosti výskytu hrozby obsahuje následující tabulka.

Tab. 11 Příklad vodítek stanovení pravděpodobnosti

Hodnota	Pravděpodobnost	Slovní vyjádření	Očekávaná četnost
0,1	Skoro nemožná	Je to možné jen teoreticky	Jednou za 100 let
0,3	Nepravděpodobná	Lze se s tím zřídka setkat	Jednou za 30 let
0,5	Možná	Lze se s tím setkat během vaší praxe	Jednou za 10 let
0,7	Pravděpodobná	Lze se s tím setkat během vaší praxe několikrát	Jednou za 3 roky
0,9	Skoro jistá	Lze to běžně očekávat	Jednou ročně a více

Zdroj: vlastní zkušenosti a práce autora.

Obdobným způsobem se vytvářejí vodítka pro stanovení stupně dopadu. V praxi mají vodítka pro stanovení dopadu větší počet sloupců s různými pohledy na vyjádření následků nežádoucí události.

Příklad vodítek pro stanovení dopadu hrozby obsahuje následující tabulka.

Tab. 12 Příklad vodítek stanovení dopadu hrozby

Hodnota	Dopad	Finanční ztráta (Kč)	Dopad na osoby	Média
5	Minimální	10 000	5	Místní
10	Znatelný	100 000	50	Krajská
20	Významný	1 000 000	500	Celostátní
40	Těžký	10 000 000	5 000	Evropská
80	Kritický	100 000 000	50 000	Celosvětová

Zdroj: vlastní zkušenosti a práce autora.

Výpočet míry rizika a stanovení závažnosti rizika lze v případě semikvantitvních metod vyjádřit maticí. Výpočet míry rizika z hodnot pravděpodobnosti a dopadu hrozeb podle uvedených příkladů vodítek obsahuje následující tabulka.

Tab. 13 Příklad výpočtu míry a závažnosti rizika

		Dopad				
		5	10	20	40	80
Pravděpodobnost	0,1	**0,5**	**1**	**2**	**4**	**8**
	0,3	**1,5**	**3**	**6**	**12**	**24**
	0,5	**2,5**	**5**	**10**	**20**	**40**
	0,7	**3,5**	**7**	**14**	**28**	**56**
	0,9	**4,5**	**9**	**18**	**36**	**72**

Zdroj: vlastní zkušenosti a práce autora.

Barevně vyznačení rizik rozlišuje závažnost rizika a jeho účelem je sdružit větší počet výsledných hodnot míry rizik do několika málo rizikových kategorií. V případě uvedeného příkladu je to 5 úrovní závažnosti rizika (zelená, žlutá, oranžová, červená, hnědá). Nastavení hraničních hodnot mezi jednotlivými úrovněmi závažnosti rizika určuje zvolený vztah k riziku (anglicky Risk appetite). Odlišný vztah k riziku by znamenal jiný způsob barevného vyznačení výsledných hodnot.

4.3.4 Vyhodnocení rizik

Vyhodnocení rizik je důležitý a často opomíjený krok řízení rizik. Cílem vyhodnocení je přenést výsledky analýzy rizik do sféry reálných možností řízení rizik. Účelem vyhodnocení je příprava podkladů pro rozhodnutí, jak s identifikovanými a analyzovanými riziky naložit, kterým rizikům věnovat prvořadou pozornost, a jaké priority přiřadit jednotlivým opatřením.

Prvotní porovnání rizik umožňují zvolené úrovně závažnosti rizika, které se nastavují v nástroji pro výpočet míry rizika (viz barevná vyznačení v tabulce č. 13). Intervaly hodnot úrovní závažnosti rizik jsou stanoveny v první fázi procesu řízení rizik v souvislosti s určením měřítek akceptovatelnosti rizik. Hodnoty intervalů závažnosti rizik nejsou dogma, jsou vždy orientační. Vyhodnocování rizik je tvůrčí činností, není to jen porovnávání čísel.

Mnoho lidí je za určitých okolností ochotno tolerovat některá mnohem větší rizika, než jak jsou nastavena měřítka akceptovatelnosti. Proto se v praxi prosazuje přístup k vyhodnocení rizik, který dělí rizika do tří kategorií závažnosti v analogii k pyramidě, kterou znázorňuje následující obrázek.

Obr. 11 Pyramida akceptace rizika.
Zdroj: vlastní zkušenosti a práce autora.

Pyramida znázorňuje tři odlišné úrovně akceptovatelnosti (tolerance k riziku) a jim odpovídající přístup ke zvládání rizik opatřeními:

- horní skupinu rizik nelze v žádném případě tolerovat a je nutno je ošetřit (jak, popisuje následující kapitola zvládání rizik);
- střední skupinu rizik (šedá zóna) je třeba posuzovat náklady a přínosy opatření a porovnávat je s potenciálními nepříznivými následky;
- spodní skupinou rizik není nutné se dále zabývat, rizika jsou tak malá, že žádná opatření k jejich zvládání nejsou potřeba.

4.3.5 Zvládání rizik

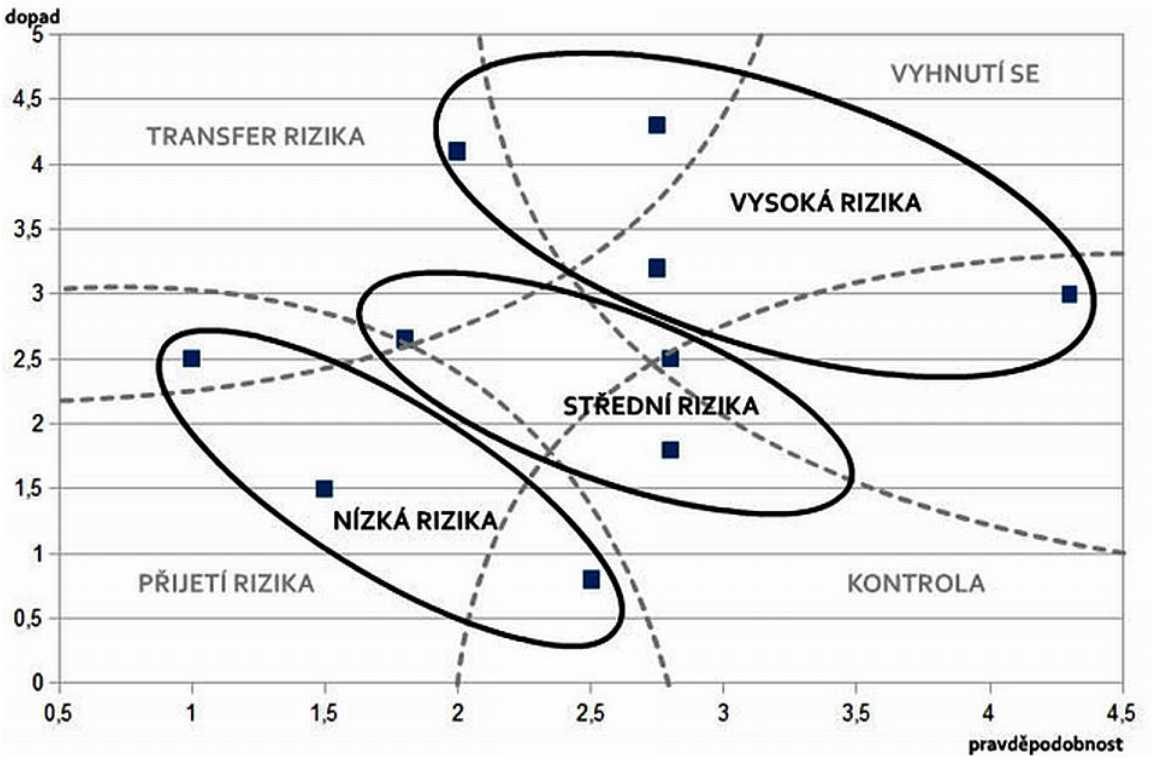
Zvládání rizik je proces, ve kterém se volí způsob řešení rizika a zvolené řešení se realizuje. Obvykle se přijímá alespoň jedno, ale často i více opatření, která realizují zvolený způsob řešení rizika. Standardními možnostmi zvládání rizika jsou:

1. *podstoupení rizika* (přijetí) – nejedná se již o zvládání, ale o jeho ponechání;
2. *redukce rizika* (kontrola) – modifikace (snížení) rizika nasazením opatření;
3. *přenos rizika* (transfer) – sdílení rizika, tj. přenesení na někoho jiného;
4. *vyhnutí se riziku* – zastavení nebo vyhnutí se plánovaným činnostem.

Možnosti zvládání rizika se doporučuje zvažovat v pořadí, v jakém jsou uvedeny ve výčtu. První variantou je nedělat nic (podstoupení), poté zvážit jak by stav zlepšilo zavedení opatření (redukce), nebo zda je možné riziko s někým sdílet (přenos), např. pojištěním, nakonec i zvážit, zda lze rizikovou činnost nedělat (vyhnutí se).

Možnosti zvládání rizik ve vztahu k parametrům rizika, tj. pravděpodobnosti a dopadu nežádoucí události, je užitečné vyjádřit graficky na ploše, která se označuje pojmem *mapa rizik*. Na mapě rizik je zřejmé, která rizika jsou problémem (mají vysokou pravděpodobnost, ale nízký dopad), a která mohou být katastrofou (mají sice nízkou pravděpodobnost, ale vysoký dopad).

Typickou mapu rizik s vyznačením výše uvedených možností zvládání rizik znázorňuje následující obrázek.



Obr. 12 Mapa řízení rizik.
Zdroj: Vose, 2008, překlad Michal Psota.

Zvolený způsob zvládání jednotlivých rizik se následně podrobně zaznamená do Plánu zvládání rizik. Plán zvládání rizik může mít podobu listinného dokumentu, ale vhodnější je vést jej v elektronické podobě dostupné všem zainteresovaným osobám.

Rizika, která zbudou po realizaci procesu zvládání rizik, se nazývají pojmem *zbytková rizika*. Zvládání rizik obvykle přináší rizika nová. Proto je zvládání rizik nekončící cyklický proces (viz obrázek č. 10 v kapitole 4.2.1).

Při zvládání rizika jeho redukcí nasazením opatření volíme zpravidla mezi více alternativami možných opatření. Opatření se v sestupném pořadí účinnosti dělí na následující typy:

- snižující hrozby;
- snižující zranitelnost;
- snižující následky;
- detekující incident;
- umožňující obnovu.

Zvládání rizika jeho přenosem není vždy možná forma, ale je velmi účinná. Nejběžnějšími příklady přenosu rizika jsou:

- subdodávky;
- outsourcing;
- pojištění.

Rizika nejsou přenosem většinou eliminována, jen modifikována, a vznikají rizika nová. Existuje dokonce samostatný typ rizik, rizika outsourcingu a smluvních ujednání. Formulace smluv je klíčový prvek řízení mnoha typů rizik, a je s podivem, jak nedostatečně se tento nástroj v praxi využívá. Sdílení rizika pojištěním umožňuje krýt většinu případných škod působení rizika, ale zdaleka ne všechna rizika jsou pojistitelná. Nelze například pojistit dobré jméno firmy.

4.3.6 Dokumentování

Řízení rizik je řízený proces a musí být dokumentován. Odborné literární zdroje i normy řízení rizik obsahují širokou škálu doporučené dokumentace. Praxe ovšem ukazuje, že podmínkou účinnosti řízení rizik je za žádných okolností nepřipustit formální vytváření dokumentů (anglicky trefně označované Paperwork).

Dokumentace řízených procesů se dělí na řídící dokumenty, označované v normách pojmem *dokumentované postupy*, a záznamy o průběhu procesu a provádění opatření, normami všeobecně označované pojmem *záznamy*. Záznamem je jakýkoliv typ informace, který poskytuje objektivní důkaz o provádění fází a kroků procesu a provádění opatření.

Ve shodě s autory analyzovaných literárních zdrojů považuji za nezbytné vedení tří nejdůležitějších záznamů procesu řízení rizik. Těmito nezbytnými záznamy jsou *Registr rizik*, *Plán řízení rizik* a *Databáze incidentů*.

Registr rizik je jednoduchý seznam nebo databáze s údaji o všech identifikovaných rizicích vedený v elektronické podobě, aby jej bylo možné snadno sdílet. V registru rizik je vhodné ke každému riziku evidovat následující údaje:

- identifikátor rizika;
- vlastník rizika;
- popis rizika, jeho příčin a následků;
- stručný popis stávajících opatření;
- ohodnocení pravděpodobnosti a dopadu;
- výsledná míra rizika;
- rozhodnutí o způsobu zvládání rizika;
- priorita rizika;
- odkaz na příslušný Plán zvládání rizik.

Plán zvládání rizik dokumentuje akce manažerů a přijatá opatření. Je obdobou projektového plánu, obsahuje informace o tom, co, kdo, jak a kdy má udělat. Stejně jako v případě registru rizik je vhodné jej vést v elektronické podobě z důvodu, že stanovuje úkoly pro větší počet osob. Plán zvládání rizik by měl obsahovat:

- úkoly vztahující se ke zvládání jednotlivých rizik;
- odpovědnosti za realizaci stanovených úkolů;
- zdroje pro realizaci jednotlivých úkolů včetně rozpočtu;
- harmonogram realizace;
- způsob a četnost přezkoumání stavu plnění plánu.

Databáze incidentů, v případě důsledného vedení, je významným zdrojem pro identifikaci rizik a přezkoumání ke zlepšování procesu. Nedostatky, incidenty a nezdary, jejichž výskyt je poměrně častý, jsou totiž významnými zdroji rizik. Zaznamenání informací i o zdánlivě drobných problémech může v agregované podobě poskytnout obraz o příčinách mnohem větších problémů. Databáze incidentů by měla o každém incidentu obsahovat následující údaje:

- druh incidentu (rozlišení kategorií podle specifických typů rizik);
- datum a čas zjištění incidentu;
- popis incidentu;
- příčiny a okolnosti incidentu;
- způsob zjištění incidentu;
- zdroje incidentu (např. lidská chyba, selhání technologie, nastavení procesu, úmysl, vyšší moc, …);
- přijatá opatření.

5 Výsledky a návrh praktické metodiky

Kapitola obsahuje výsledky práce ve formě návrhu praktické jednoduché metodiky řízení projektových rizik. Navržená metodika vznikala v letošním roce formou pracovních diskusí s projektovými manažery společnosti Asseco Central Europe, a.s., ve které autor práce působí a která se zaměřuje na vývoj a dodávky softwarových systémů.

Prostředí vzniku ovlivnilo i rozsah metodiky, protože základním požadavkem současného přístupu k řízení projektů je maximální jednoduchost dokumentovaných postupů firemních procesů, přičemž je kladen důraz na způsobilost samotných výkonných pracovníků a projektových manažerů. Požadavek stručnosti a jednoduchosti metodiky vychází z moderních metodických přístupů k vývoji software, jejichž cílem je definovat principy, nikoliv postupy nebo návody.

Význam pojmu *způsobilost* lze definovat jako spojení odborné kvalifikace, zkušeností a odpovědnosti ke specifické oblasti činností. Tento trend je posilován požadavky zadavatelů softwarových systémů, kteří trvají na tom, aby klíčoví členové projektových týmů disponovali mezinárodně uznávanými certifikacemi ze své odborné oblasti. To je i případ autora této práce, držitele titulů CISA (Certified Information Systems Auditor) a CISM (Certified Information Security Manager).

5.1 Kontext agilního vývoj software

Softwarové společnosti v současnosti většinové aplikují přístup tzv. agilního vývoje software. Princip agilního vývoje vychází ze spirálového modelu softwarového procesu, vytvořeného profesorem Boehmem (viz kapitola 3.3.4), ovšem s tím zásadním rozdílem, že průchod jedním cyklem netrvá déle než několik týdnů.

Pochopení kontextu agilního vývoje software je nezbytné pro porozumění reálným podmínkám pro aplikaci metodik řízení rizik ve firmách zabývajících se vývojem software. Tradiční přístup vývoje software spočíval v tom, že funkční požadavky jsou specifikovány na začátku vývoje a jsou neměnné. Proměnnými jsou zdroje a čas. Agilní přístup považuje zdroje a čas za neměnné, předmětem změn je funkcionalita.

V projektech vývoje software agilním přístupem se na počátku stanoví nejdelší možný čas a náklady. Vývojový tým v průběhu projektu pravidelně komunikuje se zadavatelem a průběžně přehodnocuje priority. Metody agilního vývoje nejsou metodikou, ale stručně definované principy. K jejich přiblížení ocituji základní teze Manifestu Agilního vývoje software (Agile Manifesto, 2001):

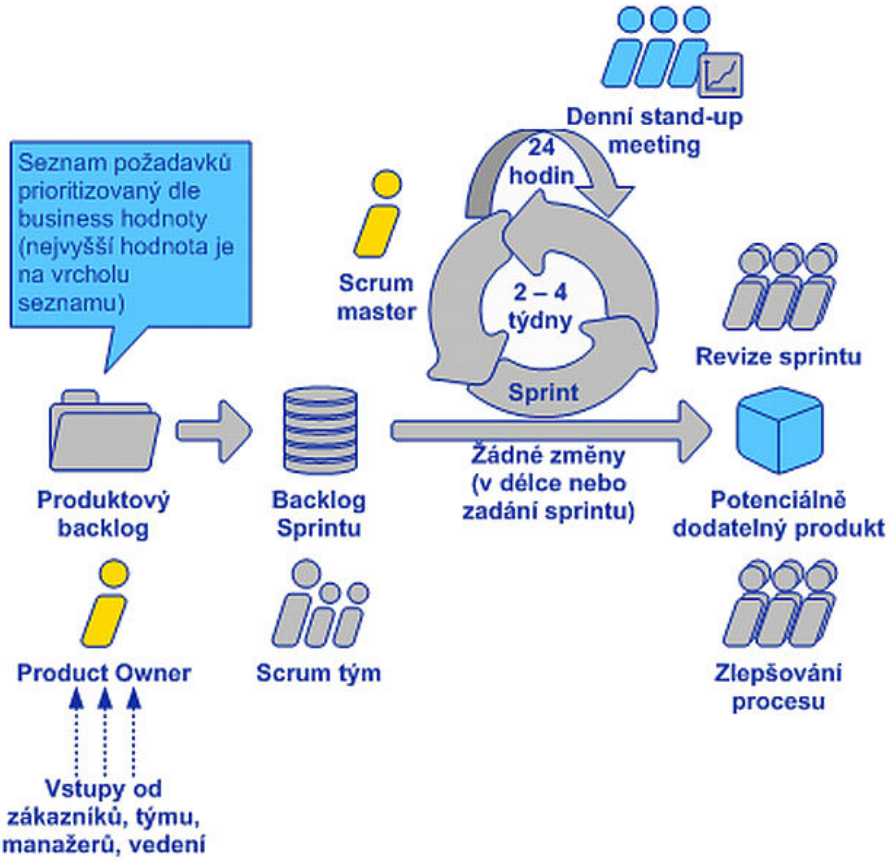
- **Jednotlivci a interakce** před *procesy a nástroji*
- **Fungující software** před *vyčerpávající dokumentací*
- **Spolupráce se zákazníkem** před *vyjednáváním o smlouvě*
- **Reagování na změny** před *dodržováním plánu*
- Jakkoliv jsou body napravo hodnotné, bodů nalevo si ceníme více.

Knesl (2009) definuje fáze softwarového projektu v agilních metodách následovně:

1. Nultá iterace – první krátká analýza a naprogramování základní činnosti. Jde o to, aby na konci byl hotový kousek aplikace, který se dá předvést klientovi.
2. Analýza změny (výběr toho, co se bude implementovat, navrhování změn).
3. Samotná implementace požadované vlastnosti (či vlastností).
4. Předvedení klientovi.
5. Pokud není produkt hotov, zpět na bod 2.
6. Pokud ano, následuje údržba, rozvoj (rovněž v iteracích).

Body 2–4 se označují jako jedna iterace a opakují se tak dlouho, dokud není vývoj úspěšně ukončen, nebo z jiných důvodů pozastaven.

Příkladem metod agilního vývoje je metoda Scrum (Schwaber, 1997). Model agilního vývoje software metodou Scrum znázorňuje následující obrázek.



Obr. 13 Agilní vývoj software metodou Scrum.
Zdroj: UNICORN, 2011.

Celý proces řízení vývoje spočívá v rozdělení prací na jednotlivé iterace (sprinty) se stejnou délkou trvání. V rámci každé iterace jsou pak dílčími týmy realizovány úkoly, které vycházejí ze seznamu požadavků na produkt (produktový backlog).

Z uvedených principů agilního vývoje vyplývá, že se v praxi od projektových týmů požaduje dosahovat hmatatelné výsledky vždy po několika týdnech, kdy končí časově pevně ohraničené iterace. Z toho je zřejmé, že projektové týmy nemají příliš mnoho času zabývat se jakýmikoliv teoretickými modely a metodikami. Nedokumentují rozsáhle ani samotný vývoj, nepoužívají CASE nástroje modelování, tudíž nekreslí složité UML diagramy, nesepisují dokument specifikace požadavků, ani samotný kód nepíší tak, aby vyhovoval všem budoucím představitelným změnám.

Čtenář nechť se sám pokusí poctivě zodpovědět otázku, jak důkladně se projektové týmy mohou při agilním vývoji software zabývat identifikací, hodnocením, zvládáním a monitorováním rizik.

5.2 Metodika řízení rizik

Předkládaná metodika popisuje postupy identifikace, posouzení, plánování odezev a realizaci opatření na rizika na projektu a související nástroje.

Cílem řízení rizik je získání konkurenční výhody v podobě redukce nákladů na odstraňování problémů kvůli neřízeným rizikům a proaktivní přijímání opatření k řízení rizik.

5.2.1 Nejdůležitější pojmy

Riziko projektu je nejistá nebo možná událost v budoucnu s negativním dopadem (škodou) na celkový nebo dílčí úspěch projektu.

Příležitost je nejistá událost, která může mít pozitivní vliv na dosažení cílů projektu.

Znaky rizika: pravděpodobnost, že se událost v budoucnu stane, musí být větší než 0% a menší než 100%. V případě události, která se stane na 100%, nemluvíme o riziku, ale o krizi nebo zásadním problému. Řízení rizik je proaktivní, krizové řízení je reaktivní.

Problém: pokud nastane událost, která spouští riziko, riziko se mění v problém nebo krizi.

Řízení rizik zahrnuje identifikaci rizik, analýzu rizik, plánování odezev na rizika, vyhodnocování rizik a realizaci opatření.

Registr rizik poskytuje nástroj pro průběžné sledování a kontrolu rizik během celého řízení projektu. Registr rizik vyplňuje projektový manažer ve fázi plánování projektu na začátku projektu a aktualizuje jej během celého projektu.

Proces řízení rizik začíná identifikací rizik, pokračuje semikvantitativní analýzou každého identifikovaného rizika a naplánováním opatření na ošetření rizik.

Identifikace a analýza rizik se provádí formou brainstormingu, v ideálním případě na setkání projektového týmu pod vedením manažera projektu. V případě, že týmový přístup není možný, může být posouzení provedeno projektovým manažerem a následně revidováno týmem.

5.2.2 Krok 1: Identifikace

Hlavním cílem kroku identifikace rizik je rozeznat hrozby, které mají vliv na dosažení cílů projektu. Platí následující vztah: zdroj rizika může způsobit/vyvolat rizikovou situaci, která může mít dopad na cíl projektu.

Při identifikaci rizik se do registru rizik zaznamenává:

- Identifikátor rizika
- Datum identifikace
- Kategorie rizika
  - Předmět, smluvní vztahy a ekonomika
  - Řízení a organizace projektu
  - Projektový tým
  - Technologické a kvalita produktu
  - Externality
- Událost – spouštěč rizika, tj. událost, která pokud nastane, vyvolá rizikovou situaci
- Popis dopadu – jaký je dopad na cíl projektu, pokud nastane riziko
- Charakter rizika
  - Interní – nebude se komunikovat zákazníkovi
  - Externí – komunikuje se zákazníkovi

5.2.3 Krok 2: Analýza

Hlavním cílem kroku analýza je posouzení hrozby z pohledu pravděpodobnosti výskytu a ohodnocení dopadu rizika na projekt. Na základě pravděpodobnosti výskytu a ohodnocení dopadu je možné provést klasifikaci závažnosti rizika.

Samotné posouzení rizik je krok, jehož cílem je určení dopadu projektových rizik na cíle projektu a poskytnout řídícímu výboru projektu informace pro rozhodování.

Během analýzy se do registru rizik zaznamenává:

- Pravděpodobnost výskytu hrozby – v procentech. Číslo vyjadřuje předpokládaný podíl počtu výskytů rizika z celkového počtu situací, ve kterých se riziko může vyskytnout.
- Ohodnocení dopadu – dopad hrozby nebo příležitosti v kontextu projektových cílů. Určení dopadu rizika lze vyčíslit následující metodou:
  - Jednotlivec nebo skupina lidí označí svůj subjektivní odhad velikosti dopadu příslušného rizika kvalitativním výrokem z předdefinované stupnice dopadů (nevýznamný, málo významný, významný, velmi významný, kritický).
  - Ke kvalitativně určeným odhadům se přiřadí kvantitativní hodnota, která je předdefinovaná a automaticky vypočítávána v rámci registru rizik.

- Závažnost – hodnocení závažnosti rizika a jeho kategorie se určí vynásobením pravděpodobnosti rizika a kvantitativní hodnoty jeho negativního dopadu. Závažnost rizika je automaticky vypočítána po zadání pravděpodobnosti a dopadu. Závažnosti rizika se následně seřadí podle závažnosti v pořadí od nejvyšší závažnosti (vyznačené automaticky červenou barvou), až po nejnižší závažnost (vyznačené zelenou barvou). Rizika musí být řízena podle priority směrem od rizik s nejvyšší závažností až po rizika s nejnižší závažností.

Výstupem tohoto kroku je klasifikace rizik do 3 kategorií (červená, žlutá, zelená) podle závažnosti. Výpočet závažnosti rizika se provádí pod následující tabulky.

Tab. 14 Určení závažnosti a priority rizika

		DOPAD				
		nevýznamný	málo významný	významný	velmi významný	kritický
		1,15	2,00	2,80	5,00	10,00
PRAVDĚPODOBNOST	10%	0,115	0,200	0,280	0,500	1,000
	20%	0,230	0,400	0,560	1,000	2,000
	30%	0,345	0,600	0,840	1,500	3,000
	40%	0,460	0,800	1,120	2,000	4,000
	50%	0,575	1,000	1,400	2,500	5,000
	60%	0,690	1,200	1,680	3,000	6,000
	70%	0,805	1,400	1,960	3,500	7,000
	80%	0,920	1,600	2,240	4,000	8,000
	90%	1,035	1,800	2,520	4,500	9,000
						ZÁVAŽNOST

Zdroj: výstup práce autora.

Ke kontrole správnosti klasifikace kategorie rizika slouží následující tabulka.

Tab. 15 Popis kategorií závažnosti rizika

ZELENÁ – Nízká závažnost	
V případě výskytu identifikovaného rizika:	
	Nedojde k navýšení rozpočtu.
	Nedojde k navýšení rozsahu.
	Nedojde k takovému posunu termínů, které by ohrozily dílčí milníky.
	Nedojde k takovému navýšení požadavků na kapacity, které by způsobily kolize kapacit.

Žlutá – Střední závažnost	
V případě výskytu identifikovaného rizika:	
	Dojde k navýšení rozpočtu, který však bude řešitelný v rámci přesunu objemu financí mezi rozpočtovými kapitolami.
	Dojde k navýšení rozsahu, které bude možné řešit jinou cestou, než změnovým řízením.
	Dojde k posunu dílčích termínů, avšak fakturační milníky nebudou ohroženy.
	Dojde k navýšení požadavků na kapacity, které bude možné řešit jinou cestou, než změnovým řízením.
Červená – Vysoká závažnost	
V případě výskytu identifikovaného rizika:	
	Dojde k navýšení rozpočtu, nebo rozsahu nebo požadavků na kapacity, nebo k posunu termínů, nebo ke kombinaci výše uvedeného v takové míře, která vyvolá vznik změnového řízení.

Zdroj: výstup práce autora.

5.2.4 Krok 3: Plánování

Hlavním cílem kroku plánování je příprava specifických reakcí na rizika, které by měly odstranit nebo minimalizovat dopad hrozeb na projekt.

Plánování zahrnuje identifikaci a posouzení reakcí na rizika. Reakce musí být přiměřená riziku. Při výběru reakce je důležité vyvážení mezi náklady na implementaci opatření ve srovnání s velikostí dopadu rizika.

Tab. 16 Možnosti reakce na riziko

Reakce	Popis
Podstoupit	Vědomé rozhodnutí ponechat hrozbu bez odpovědi. Ukázalo se ekonomicky nebo jinak výhodnější než použít jinou odpověď. Hrozba bude monitorována a bude posuzováno, zda je i nadále akceptovatelná. Přijatelnost rizika je vhodné určit pro daný projekt stanovením hranice přijetí rizika – tolerance k riziku (např. pro projekt není možná tolerance pro změny oblasti finančního plánu).
Redukovat	Snížit pravděpodobnost výskytu události nebo snížit velikost dopadu události (např. tvorba finančních rezerv, variantní způsob provedení).
Přenést	Přenést dopad na třetí stranu (např. pojištěním) nebo sdílet riziko s třetími stranami (např. subdodavatelem).
Vyhnout se	Změnit některé aspekty projektu (např. rozsah, posloupnosti aktivit) tak, že hrozba buď nebude mít nadále dopad na projekt, nebo nemůže nastat (např. odmítnutí přijmout riskantní podmínku zadavatele projektu, nepřijmout riskantní technické řešení).

Zdroj: výstup práce autora.

Přijatá opatření jsou zapsána do registru rizik. Dopad opatření může mít vliv na jednotlivé úrovně projektu, a proto je třeba je zahrnout do příslušných plánů (časový plán projektu, harmonogram projektu, plán etapy).

Během plánování se do registru rizik zaznamenává:

- Odpověď na riziko
- Opatření k prevenci nebo zmírnění dopadu
- Požadovaný termín realizace opatření
- Náhradní plán – je nutné vypracovat u rizik v kategorii „ČERVENÁ“. Náhradní plán je postup pro výjimečné situace, kdy se podle původního plánu nedá pokračovat. Náhradní plán schvaluje řídící výbor projektu.
- Jméno vlastníka – vlastník rizika je konkrétní člen projektového týmu, který je odpovědný za identifikaci a ohodnocení konkrétního rizika a přijetí opatření ke zmírnění tohoto rizika.

5.2.5 Krok 4: Realizace a monitorování

Cílem kroku realizace je zajistit, aby naplánovaná opatření byla implementována, aby byla monitorována jejich efektivita, a aby byla změněna, pokud provedená opatření nesplnila očekávání.

Na počátku realizace se v registru rizik zaznamená a během monitorování se v registru aktualizuje:

- Stav – riziko může být aktivní nebo uzavřeno. Stav se určuje podle naléhavosti požadované eskalace a výstrahy pro management.
  - Nízká – nízká naléhavost, tj. akceptovatelné riziko, není třeba připravovat žádná opatření ke zmírnění rizika, riziko stačí sledovat.
  - Střední – střední naléhavost výstrahy pro management, tj. opatření ke snížení rizika by měla být přijata v přiměřeném časovém horizontu.
  - Vysoká – vysoká naléhavost výstrahy pro management, tj. okamžitě musí být přijata opatření ke snížení rizika.
  - Uzavřené – riziko nastalo a přesunulo se do registru problémů, nebo riziko již nepředstavuje žádnou hrozbu pro projekt.
- Datum aktualizace stavu – datum aktualizace vyjadřuje datum poslední změny stavu rizik v registru rizik.
- Poznámka – povinná při změně stavu rizika na uzavřené.

5.2.6 Krok 5: Komunikování

Cílem kroku komunikování je průběžně zajišťovat, aby informace o hrozbách, rizicích a problémech byly komunikovány všem relevantním účastníkům projektu.

5.3 Proces řízení rizik

5.3.1 Pravidla a odpovědnosti

Projektoví manažeři, vlastníci rizik jsou povinni dodržovat následující zásady:

- Na všech externích projektech je nutné řídit rizika podle této metodiky řízení rizik přizpůsobené potřebám zákazníka a konkrétního projektu.
- Řízení rizik je kontinuální proces, a proto musí být prováděn v průběhu celého životního cyklu projektu.
- Za identifikaci a řízení rizik na projektu odpovídá projektový manažer.
- Nástrojem pro evidenci a řízení rizik je registr rizik, dostupný v rámci systému věcného plánování příslušného projektu.
- Řízení rizik projektu je jedním z klíčových aspektů pro dosažení očekávaných cílů projektu. Projektová rizika se vztahují na cíle projektu.
- Projektový manažer využívá eskalační mechanismy dostupné v rámci registru rizik pro identifikaci potřeby součinnosti managementu při prevenci jejich výskytu nebo redukci jejich dopadů.
- Projektový manažer eskaluje na úroveň managementu ta rizika, u kterých je nutná součinnost managementu při řešení a realizaci navržených opatření s významným dopadem na cíle projektu.

5.3.2 Hlavní kroky procesu

Při řízení rizik projektu je nutné provést následující kroky:

1. Nastavení aplikační podpory pro vedení registru rizik projektu.
   - Pro nové projekty bude registr rizik nastaven v rámci požadavku na nastavení infrastruktury projektu ve výchozím nastavení podle této metodiky.
   - Pro stávající projekty se dodatečně doplní registr rizik do systému věcného plánování.
2. Úvodní pracovní schůzka projektového týmu za účelem identifikace rizik a naplánování opatření.
   - Identifikace a analýza rizik se realizuje formou brainstormingu na setkání projektového týmu pod vedením manažera projektu.
3. Vyplnění výchozího registru rizik projektovým manažerem v nástroji aplikační podpory.
4. Průběžné sledování, kontrola stavu, komunikace a aktualizace registru rizik projektovým manažerem:
   - min. 1x týdně pro vývojový projekt,
   - min. 1x týdně během realizace změnového řízení,
   - min. 1x měsíčně pro servisní projekt.

5.3.3 Povinné údaje registru rizik

Aplikační podpora registru rizik obsahuje následující položky, přičemž povinné položky jsou zvýrazněny tučně:

- **Identifikátor** (generován automaticky)
- **Datum identifikace**
- **Kategorie rizika**
- **Událost** (spouštěč rizika)
- **Popis dopadu**
- **Charakter rizika**
  - Interní – nebude se komunikovat zákazníkovi
  - Externí – komunikuje se zákazníkovi
- **Pravděpodobnost výskytu v%**
- **Klasifikace dopadu** – navázat na finanční odhad
- Finanční dopad – v Kč
- Počet výskytů
- Celkový finanční dopad – v Kč
- Závažnost rizika – Priorita (vypočtena automaticky)
- **Odpověď na riziko**
- Opatření k prevenci nebo redukci dopadu (není nutné u podstoupených rizik)
- Náhradní plán (pouze u rizik v kategorii červená)
- Požadovaný termín realizace opatření
- **Jméno vlastníka rizika**
- **Jméno realizátora opatření**
- **Stav rizika** (eskalace na řízení rizik v kategorii žlutá a červená)
- Datum aktualizace stavu (automaticky generované)
- **Poznámka** (popis změny atributů rizika)

5.3.4 Vedení registru problémů

Pokud nastane událost, která spouští riziko, riziko se mění v problém nebo krizi. Cílem je monitorovat průběžný stav problémů a přijímat opatření k eliminaci problémů a sankcí v důsledku nedodržení smluvních ujednání. Projektový manažer vede a sleduje registr problémů a přijímá nápravná opatření:

- min. 1x týdně pro vývojový projekt,
- min. 1x týdně během realizace změnového řízení,
- min. 1x měsíčně pro servisní projekt.

Registr problémů obsahuje následující povinné položky:

- Projekt – zkratka projektu podle katalogu projektů
- Identifikátor problému – zadejte např. P-NNNN (P-Problém, NNNN-číslo, které se bude sekvenčně zvyšovat)
- Identifikoval – jméno osoby, která problém identifikovala
- Datum identifikace – datum identifikace problému
- Popis problému – stručný popis problému
- Dopad problému – možné dopady při neřešení daného problému (informace, co se stane, pokud nebude problém včas vyřešen)
- Vlastník – vlastník problému je osoba odpovědná v rámci organizace projektu za hodnocení konkrétního problému a za přijímání opatření k jeho odstranění.
- Závažnost
  - Zelená – nízká závaznost (problém vyžaduje řešení či rozhodnutí, ale není nutné urgentně řešit, problém je třeba monitorovat)
  - Žlutá – střední závaznost (problém vyžaduje zahájení řešení a přijetí tohoto opatření ve stanoveném termínu)
  - Červená – vysoká závaznost (problém je vysoce urgentní a vyžaduje okamžité zahájení řešení a přijetí opatření)
- Návrh řešení – jak problém vyřešit nebo podstatně omezit jeho dopady
- Průběh řešení
- Požadovaný termín řešení
- Datum aktualizace stavu
- Poznámka

5.3.5 Přezkoumání procesu

Proces řízení rizik procesů je kontrolován a přezkoumáván v rámci dalších řídících procesů:

- Interní audity požadavků norem systémů managementu, podle kterých je společnost držitelem certifikátu.
- Hodnocení projektu, kde se hodnotí i schopnost řízení rizik na projektu a aktuální stav rizik.
- Pravidelné porady managementu společnosti nad výstupy z nástroje projektového reportingu.

6 Diskuse

Řídit projektová rizika znamená analyzovat širokou škálu rizikových situací, které mohou s určitou pravděpodobností způsobit projektu vážné problémy, analyzovat jejich pravděpodobnost a velikost možné ztráty, následně je klasifikovat do kategorií určujících jejich zvládání. Výsledek každé analýzy je ovlivněn působením mnoha faktorů. Diskusi o významu a účinnosti řízení rizik na ekonomiku projektů jsem se rozhodl zaměřit na pravděpodobně nejvýznamnější faktor, a tím je individuální nebo skupinové selhání odpovědných osob, tedy lidský faktor.

Obsah kapitoly diskuse vychází ze zkušeností autora, který měl možnost účastnit se mnoha velkých projektů, z nichž některé skončily zcela jiným než žádoucím výsledkem podle stanovených cílů. Ve všech případech byl zdrojem selhání lidský faktor rozhodujících osob, které odkládaly řešení zcela zřejmého problému. Problém vytvářel plynutím času další problémy a stejně jako v případě nabalující se sněhové koule nakonec spustil lavinu, jejímž následkem bývá katastrofa.

Lidský faktor hraje významnou roli ve všech oblastech lidského rozhodování, tím spíše v řízení firem, projektů a rizik. Lidským faktorem se teoreticky zabývali i zakladatelé teorie her, americký ekonom a věhlasný matematik maďarského původu John von Neumann (původním jménem Neumann János Lajos) a rakouský ekonom Oskar Morgenstern. Společně vydali v roce 1944 knihu Theory of Games and Economic Behavior (česky Teorie her a ekonomické chování), ve které tvrdí, že lidský faktor je primárním zdrojem nejistoty.

Zajíček (2011) popisuje lidský faktor na příkladu hry poker a uvádí poznatky dalšího amerického ekonoma, Thomase C. Schellinga, který v roce 2005 obdržel Nobelovu cenu za ekonomii. Shelling pokračoval v rozvoji teorie her a lidského faktoru jako zdroje nejistoty. Než se stal ekonomem, živil se úspěšně jako obchodní vyjednavač, teorii her obohatil o pojem *ohniskový bod*.

Podle Shellinga je nutné lidský faktor brát vždy v úvahu v situacích, jež nelze natrénovat (nelze získat zkušenost prováděním). Lidé se totiž neřídí matematickou analýzou, ale tím, co považují za optimální řešení, a pokud většina lidí uvažuje stejně, pak takové řešení opravdu optimální je. Takovému řešení se v teorii her říká ohniskový bod.

Není překvapením, že to byl Shelling, který v roce 1958 navrhl americké vládě, aby byla zřízena „horká linka“ s Moskvou, právě pro případ, že díky nedostatku komunikace by došlo ke sledování špatného ohniskového bodu, což by vedlo ke vzájemnému nukleárnímu zničení, tedy hře s velmi negativním součtem.

V případě řízení projektů jejich manažeři rovněž čelí situacím, které nelze natrénovat. Většina projektů vývoje a dodávek rozsáhlých informačních systémů je zcela unikátní, nejenom technologicky, ale zejména prostředím a kulturou organizace zadavatele. Zkušenosti projektových manažerů z předchozích projektů jsou podstatné pro formování přístupu k rizikům, ale ve zcela nových situacích nestačí. A takových situací nastává v každém větším projektu vždy více, než jsou všechny zainteresované strany ochotny na začátku projektu připustit.

Osobní poznatek autora práce, jak takovým problémům předcházet, je pěstovat a podporovat otevřenou komunikaci mezi všemi úrovněmi vedení, včetně „horké linky“ k nejvyššímu manažerovi. Nejčastější překážkou otevřené komunikace bývá strach ze sankce, bohužel často oprávněný. V současné době koncentrace organizací do větších celků je čím dál méně představitelné, aby běžný výkonný pracovník zašel bez pozvání do kanceláře generálního ředitele a nebál se mu říci: „Pane řediteli, promiňte, ale to, co požadujete realizovat, je naprostá hloupost.“. Pokud si to laskavý čtenář představit dokáže, doporučuji mu jeho přesvědčení prakticky otestovat. Existence iracionálních záměrů je totiž vlastní každému typu organizace, protože organizaci netvoří budova, ale lidé uvnitř, kteří nejsou neomylní.

6.1 Zdánlivá racionalita rozhodování

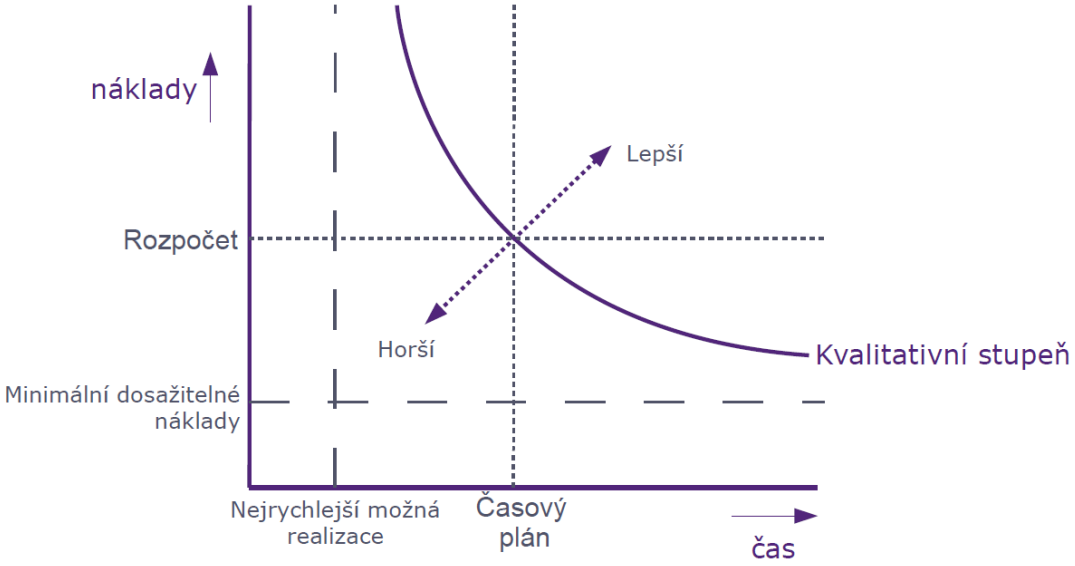
S působením lidského faktoru je často spojen požadavek ekonomické efektivity. Ani velkým projektům se nevyhýbá situace, kdy ekonomická racionalita je jediným zdrojem rozhodování. Nezřídka tak dochází k tomu, že zadavatel se rozhodne vybudovat informační systém, jehož cena by podle nejlepších zkušeností byla např. 300 miliónů Kč. I když má u zadavatele záměr na starosti rozvážný pracovník, který nechá cenu odhadnout znalcem, dojde následně ke schvalování záměru vedením organizace. A podle starého obchodnického pravidla, že každý první návrh ceny je nepřijatelně vysoký, tak ředitel organizace bez jakékoliv znalosti věci rozhodne snížit cenu např. o 30%, tedy na 210 miliónů Kč. Pak zadavatel vypíše výběrové řízení s maximální cenou 210 miliónů Kč. Uchazeči o zakázku mají více zkušeností a rozpoznají, že cena neodpovídá rozsahu požadavků, přesto se rozhodnou podat nabídku, protože je lepší mít zakázku za 200 miliónů, než žádnou. Své rozhodnutí si racionalizují např. ujištěním se, že se následně se zadavatelem nějak dohodnou na rozšíření zakázky nebo další zakázce, která jim pokryje ztráty. A protože je tu i konkurence, tak působením konkurenčních sil dojde k tomu, že většina uchazečů sníží nabídkovou cenu pod 200 miliónů, protože s jedničkou na začátku vypadá cena mnohem lépe. Zakázku získá, jak je obvyklé, nabídka s nejnižší cenou, např. ve výši 168 miliónů Kč. To je skoro polovina ceny, kterou na začátku odhadl zkušený profesionál na základě pečlivé analýzy požadavků zadavatele.

Myslíte, že to, co zde píšu, se nemůže stát? Naopak, trh rozsáhlých informačních systém je posledních několik let v útlumu a je to naprosto běžná situace. Dokážete si představit, že takový projekt bude prost závažných rizik? Nikoliv, protože takový projekt je sám o sobě rizikem. Odborně se takové riziko nazývá pojmem *inherentní riziko*, riziko vnitřně spjaté s obsahem samotného záměru nebo cíle, jenž má být dosažen. Inherentním rizikem je např. podnikatelský záměr vybudování luxusního bytového domu uprostřed průmyslové zóny.

Existence projektů, jejichž cíle jsou spojeny s nereálnými parametry, jako např. ve výše uvedeném příkladu, je způsobena zdánlivou racionalitou rozhodování manažerů. Rozhodnutí ředitele snížit cenu je samo o sobě ekonomicky racionální, ovšem v kontextu věcných a technicky odborných parametrů projektu už takové

rozhodnutí racionální není. To je důvodem, proč odborníci na řízení rizik zdůrazňují, že systematické řízení rizik lze aplikovat pouze na činnosti skupiny osob, nikoliv na činnosti jednotlivce.

Podstatu problému zdánlivé racionality rozhodování spojeného s projekty lze demonstrovat pomocí tzv. trojimperativu projektu, který je modelem vztahu tří faktorů: nákladů, trvání a kvality výstupu projektu. Riziko způsobené zdánlivou racionalitou vzniká v situaci, kdy dojde k rozhodnutí na základě změny jednoho z faktorů, aniž by došlo k reformulaci cílů spojených s ostatními faktory. Grafické vyjádření trojimperativu projektu znázorňuje následující obrázek.



Obr. 14 Trojimperativ projektu.
Zdroj: Duncan, 1996, překlad Karel Hák.

Trojimperativ projektu se také někdy vysvětluje pomocí trojúhelníku LE-R-K. Zkratka LE-R-K znamená: levně, rychle, kvalitně. Pokud si uvedené charakteristiky projektu představíte jako vrcholy trojúhelníku, pak pomocí přímky není možné současně protnout více jak dva vrcholy. Stejně tak v realitě nelze dosáhnout toho, aby realizace výstupu projektu proběhla současně rychle, levně a kvalitně. Může proběhnout jenom levně a rychle, nikoliv kvalitně, nebo levně a kvalitně, ne však rychle, nebo rychle a kvalitně, nikoliv levně.

Pokud budete přizváni k projektu, jehož parametry vyžadují, aby proběhl rychle, levně a současně kvalitně, pak se téměř jistě jedná o projekt s inherentním rizikem a je vhodné zvážit svou účast v projektu. Koncem 90. let 20. století jsem absolvoval školení k plánování projektů u prestižní společnosti LBMS. Nikdy nezapomenu na základní otázku, na kterou by si měl před zapojením do projektu odpovědět každý člen projektového tým: „Co a kde budu dělat po skončení projektu?“

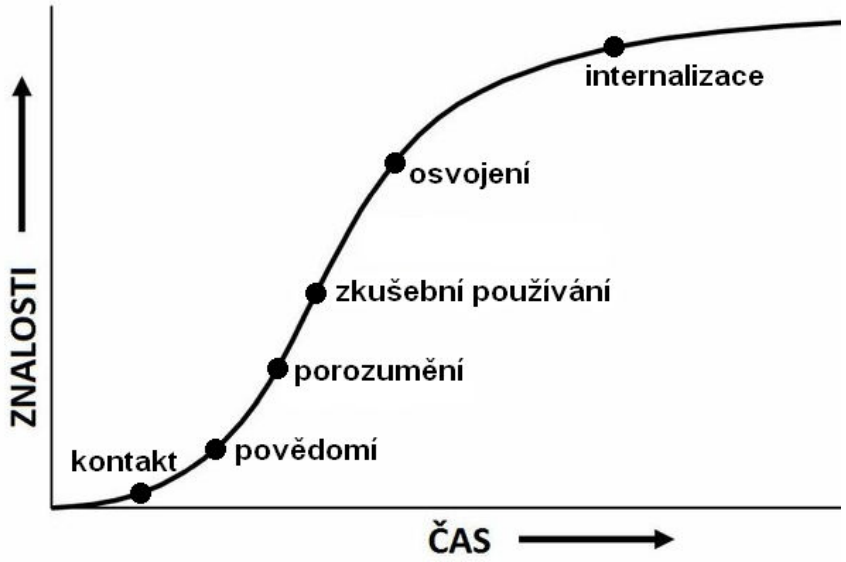
Poslední dva roky jsem působil na obdobném projektu, jaký jsem popsal v úvodu této kapitoly, v roli vedoucího jednoho z realizačních týmů. Projekt byl sjednán za pevnou a zcela nedopovídající nízkou cenu. Všem byla tato skutečnost

zřejmá, zákazník byl spokojen, jak levně dílo pořídí, uchazeč a budoucí realizátor dlouho váhal, zda vůbec podat nabídku. Podal a smlouva byla uzavřena. Projekt skončil úspěšným dodáním díla v požadovaném rozsahu a kvalitě. Ekonomický výsledek projektu byl pro realizátora záporný a z pohledu managementu firmy se po jeho finančním vyhodnocení stal příkladem špatného projektu. Nedošlo ve skutečnosti k záměně příčiny a následku? Nejednalo se zejména o špatné manažerské rozhodnutí managementu, které učinil vědomě před zahájením projektu? Ještě doplním, který člen projektového týmu nakonec sčítal největší individuální ztráty. Byl to sám manažer projektu, se kterým byl po úspěšné akceptaci díla rozvázán pracovní poměr. Poučení z této zkušenosti bylo pro ostatní výkonné členy týmu jednoznačné. Jaké? Zkuste si prosím odpovědět sami.

6.2 Způsobilost osob a vyzrálost procesů

Teorie managementu s faktorem lidských selhání počítá a zavádí pojmy, jakými jsou *způsobilost* a *vyzrálost*. Nejprve se zaměříme na způsobilost osob, již zmíněnou v úvodu kapitoly 5 v souvislosti se skutečností, že moderní přístupy k řízení softwarových projektů upřednostňují způsobilost osob před kvalitou metodik.

Nezbytnost odborné způsobilosti při řízení softwarových projektů a jejich rizik vysvětluje Hall (1998) pomocí křivky procesu získávání znalostí a zkušeností, kterou znázorňuje následující obrázek.



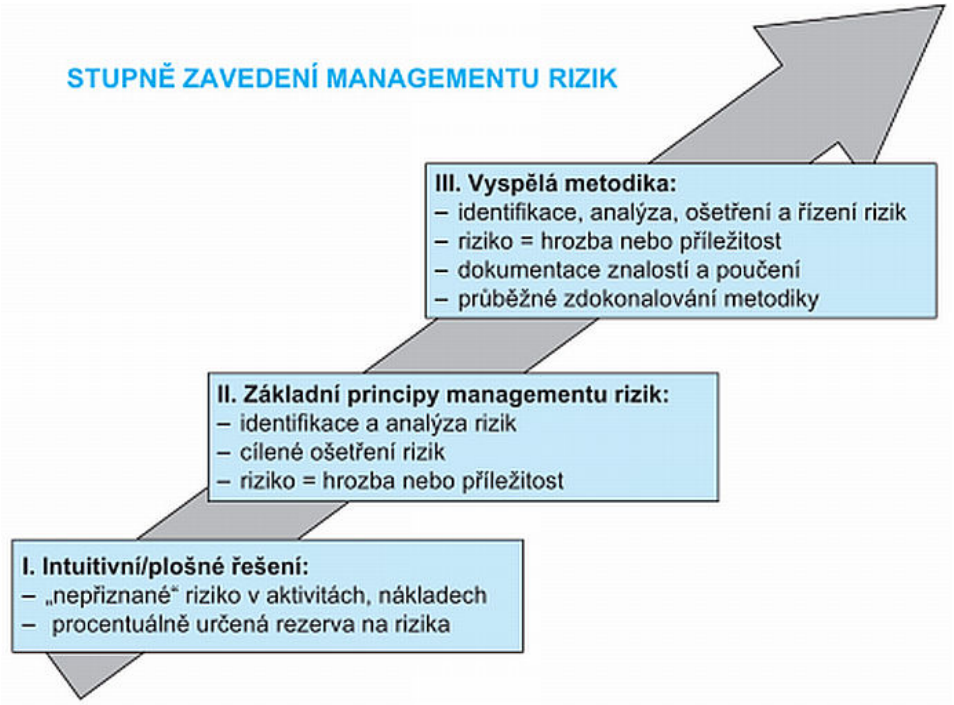
Obr. 15 Proces získávání znalostí a zkušeností.
Zdroj: Hall, 1998, vlastní překlad.

Způsobilost osob se v praxi prokazuje mezinárodně uznávanými a akreditovanými certifikacemi odbornosti osob. Smyslem těchto certifikací je prokázání znalosti daného oboru na úrovni jejich internalizace (viz obrázek) formou komplexní zkoušky a dokladováním vykonávání požadované doby praxe (např. 5 a více let).

Odborné certifikace osob zmiňuji nikoliv proto, že by byly jakousi automatickou zárukou k sestavení kvalitního řídícího týmu projektu, ale z důvodu, že jsou nástrojem ke snižování rizik spojených s lidským faktorem. Existenci této možnosti si začínají uvědomovat i zadavatelé softwarových projektů, kdy požadují po uchazečích záruky na obsazení klíčových pozic týmu projektu konkrétními osobami.

Obdobně jako v případě způsobilosti osob lze principy získávání znalostí a zkušeností aplikovat na organizaci, u kterých lze externě sledovat a vyhodnocovat zlepšování řídících procesů. Stav úrovně kvality a komplexnosti řídícího procesu se označuje pojmem *vyzrálost procesu*. Nástrojem prosazení a ověřování vyzrálosti procesů jsou systémy managementu specifikované mezinárodními normami, podle kterých se mohou organizace certifikovat akreditovaným certifikačním orgánem.

Vysoký stupeň vyzrálosti procesů vyžaduje, aby organizace podporovala neustálý učící se proces sama sebe, který je zdrojem zlepšování, jež vede k vyspělosti. V této souvislosti lze zmínit normu ISO 21827:2008, která zavádí měření vyzrálosti procesů formou modelu vyzrálosti způsobilosti (anglicky Capability Maturity Model, CMM). V případě procesu řízení rizik používají Korecký a Trkovský (2011) analogii stupňů vyzrálosti procesu, kterou znázorňuje následující obrázek.



Obr. 16 Stupně vyzrálosti procesu řízení rizik.
Zdroj: Korecký et Trkovský, 2011.

Nástrojem snižování rizika spojeného s nedostatečnou vyzrálostí procesů je audit smluvního partnera. Zadavatelé softwarových projektů si nejsou této možnosti většinou vědomi nebo není dostatečně využívána. Naopak v mnoha jiných oborech je možnost provedení auditu u dodavatele běžnou součástí smluvních ujednání.

7 Závěr

Management rizika v řízení projektů je významným faktorem při dosahování cílů a ekonomické efektivity projektů. Předkládaná práce se pokouší přiblížit teoretické zdroje, doporučení uznávaných autorů, včetně poznatků z praxe jejího autora, a na těchto východiscích přináší návrh metodiky a nástrojů řízení rizik použitelných v praxi.

Závěrem své práce bych chtěl těm, kterým se tato práce dostane do ruky a budou chtít některé její přístupy aplikovat, poskytnout i několik praktických doporučení. Následující doporučení jsou určena především manažerům softwarových projektů, kteří aplikují metody agilního vývoje.

První doporučení je brát tuto metodiku jako zdroj inspirace, ne jako návod. Řízení rizik je tvůrčí činnost, nikoliv pevně daný výrobní postup, jakým je např. postup výroby cukru, jehož nedodržením není možné dosáhnout výsledku. Každá metodika může být velmi dobrý sluha, ale i špatný pán. Je třeba mít neustále na paměti a řídit se nepsaným pravidlem zkušených praktiků, které zní:

> *Každá metodika slouží jako pomůcka, aby se na nic podstatného nezapomnělo. Její uživatelé nesmí přestat používat svůj vlastní rozum a přenášet svou vlastní osobní odpovědnost na metodiku. Nechat se metodikou „vláčet“ a používat argument „metodika říká“ je nejjistější cesta vedoucí k fatálním chybám.*

Druhým doporučením je vytvořit pro dokumentování rizik a průběhu jejich řešení jednoduchou aplikační podporu. Nejdůležitější záznamy, tj. registr rizik a registr problémů, jsou jednoduché evidence, které je možné vytvořit mnoha softwarovými nástroji. Plán zvládání rizik, který stanovuje úkoly k řešení rizik, je vhodné realizovat nástrojem s podporou tzv. workflow, které umožňuje sledování životního cyklu rizika, případně umí vytvářet přehledy s agregovanými údaji.

Třetím doporučením je nebát se začít s řízením rizik co možná nejjednodušším způsobem. Jedině tak je možné se učit a získávat potřebné zkušenosti. Pokud začnete složitou metodikou, už nikdy nezjistíte, zda podstatně jednodušší metody nepřinášejí obdobné výsledky. Jak ukazuje křivka získávání znalosti na obrázku č. 15 v kapitole 6.2, klíčové je dostat se za její inflexní bod, ve kterém je právě začátek používání získaných znalostí v praxi.

Na úplný závěr mi dovolte upřímně poděkovat všem, kteří věnovali svůj čas a trpělivost k přečtení celého textu práce. Jsem si vědom skutečnosti, že obor řízení rizik je většinově považován za oblast, která vyžaduje úzce specializované znalosti. K tomuto stanovisku přispívá i poměrně složitý jazyk a výskyt mnoha různých pojmů, které často vyjadřují totéž. Ve skutečnosti je řízení rizik všeobecně rozšířená činnost, kterou lidé provádějí podvědomě, např. při předjíždění na silnici. Účinné řízení rizik nevyžaduje ani tolik znalost, jako spíše schopnost realizovat záměry s uvědoměním si všech souvislostí. Nakonec si dovolím citovat jednoho z předních českých odborníků na řízení rizik z jeho přednášky: „*Riziko je to, že rizika, která mohou nastat v budoucnu, neřídíte už dnes.*“.

8 Literatura

AS/NZS 4360 *Risk management*. 3. vyd. Sydney: Standards Australia / Wellington: Standards New Zealand, 2004. 38 s. ISBN 0-7337-5904-1

AS/NZS HB436 *Risk Management Guidelines Companion to AS/NZS 4360:2004*. 3. vyd. Sydney: Standards Australia / Wellington: Standards New Zealand, 2005. 120 s. ISBN 0-7337-5960-6

ARNUPHAPTRAIRONG, T. Top Ten Lists of Software Project Risks: Evidence from the Literature Survey [on-line]. [vid. 2014-12-24]. *Proceedings of The International MultiConference of Engineers and Computer Scientists*, 2011, strany 732-737. Dostupné na http://www.iaeng.org/publication/IMECS2011/IMECS2011_pp732-737.pdf

BOEHM, B. W. *Software Risk Management*. 2. vyd. Los Alamitos: IEEE Computer Society Press, 1993. 496 s. ISBN 0-8186-8906-4.

ČSN ISO/IEC 27005 *Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací*. Úřad pro technickou normalizaci, metrologii a zkušebnictví, 2009. 52 s.

DOLANSKÝ, V., MĚKOTA, V., NĚMEC, V. *Projektový management*. Praha: Grada publishing, 1996. ISBN 80-7169-287-5.

DUNCAN, W. R. *A Guide to the Project Management Body of Knowledge*. Upper Darby: Project Management Institute, 1996. 176 s. ISBN 1-880410-12-5.

COOPER, D., GREY, S., RAYMOND, G., WALKER, P. *Project Risk Management Guidelines: Managing Risk in Large Projects and Complex Procurements*. 1. vyd. Chichester: John Wiley & Sons, 2004. 384 s. ISBN 0-470-02281-7.

GARLICK, A. *Estimating Risk*. Gower Publishing Limited, 2007. 260 s. ISBN 978-0-5660-8776-9.

GOGELA, R., JIRÁSEK, P., NOVÁK, L., POLČÁK, R., POŽÁR, J. *Pracovní příručka bezpečnostního manažera*. 1. vyd. Praha: Policejní akademie ČR v Praze, 2011, 104 s. ISBN 978-80-7251-364-2.

HALL, E. M. *Managing Risk: Methods for Software Systems Development*. 1. vyd. Reading: Addison-Wesley, 1998. 374 s. ISBN 0-201-25592-8.

HILLSON, D., SIMON, P. *Practical Project Risk Management: The ATOM Methodology*. 2. vyd. Management Concepts, 2012. 258 s. ISBN 978-1-56726-366-4.

HNILICA, J. Kvalitativní a semikvalitativní analýza rizika projektu [on-line]. [vid. 2014-12-28]. *Acta Oeconomica Pragennsia*, roč. 16, č. 3, 2008, strany 62-69. Dostupné na http://www.vse.cz/polek/download.php?jnl=aop&pdf=107.pdf

CHAPMAN, CH., WARD, S. *Project Risk Management: Processes, Techniques and Insights*. 2. vyd. Chichester: John Wiley & Sons, 2003. 408 s. ISBN 0-470-85355-7.

ISACA *COBIT 5 for Risk*. 1. vyd. Rolling Meadows: ISACA, 2013. 216 s. ISBN 978-1-60420-457-5.

ISO 10006 *Quality management systems – Guidelines for quality management in projects*. Geneva: ISO, 2003. 32 s.

ISO/IEC 12207 *Systems and software engineering – Software life cycle processes*. Geneva: ISO, 2008. 123 s.

ISO/IEC 15288 *Systems and software engineering – System life cycle processes*. Geneva: ISO, 2008. 70 s.

ISO/IEC 16085 *Systems and software engineering – Life cycle processes – Risk management*. Geneva: ISO, 2006. 34 s.

ISO/IEC/IEEE 16326 *Systems and software engineering – Life cycle processes – Project management*. Geneva: ISO, 2009. 32 s.

ISO 21500 Guidance on project management. Geneva: ISO, 2012. 36 s.

ISO/IEC 21827 *Information technology – Security techniques – Systems Security Engineering – Capability Maturity Model® (SSE-CMM®)*. Geneva: ISO, 2008. 144 s.

ISO 31000 *Risk management – Principles and guideline*. Geneva: ISO, 2009. 24 s.

ISO/IEC 31010 *Risk management – Risk assessment techniques*. Geneva: ISO, 2009. 176 s.

KNESL, J. Agilní vývoj: Úvod [on-line]. 11. 12. 2009 [vid. 2014-12-26]. Dostupné na http://www.zdrojak.cz/clanky/agilni-vyvoj-uvod/

KOLLER, G. *Risk Assessment and Decision Making in Business and Industry*. 2. vyd. Chapman & Hall/CRC, 2005. 352 s. ISBN 978-1-5848-8477-4.

KORECKÝ, M., TRKOVSKÝ, V. *Management rizik projektů: se zaměřením na projekty v průmyslových podnicích*. 1. vyd. Praha: Grada, 2011. 584 s. ISBN 978-80-247-3221-3.

LIENTZ, B., LARSSEN, L. *Risk Management for IT Projects*. 1. vyd. Elsevier Inc., 2006. 352 s. ISBN 978-0-7506-8231-2.

MANNOVÁ, B., VOSÁTKA, K. *Řízení softwarových projektů*. 1. vyd. Praha: ČVUT, Fakulta elektrotechnická, 2005. 187 s. ISBN 80-01-03297-3.

PANDIAN, C. R. *Applied Software Risk Management*. 1. vyd. Auerbach Publications, 2006. 264 s. ISBN 978-0-8493-0524-5.

PMI *A Guide to the Project Management Body of Knowledge (PMBOK Guide)*. 5. vyd. Newton Square: Project Management Institute, 2013. 589 s. ISBN 978-1-935589-67-9.

PRINCE2 *Managing Successful Projects with PRINCE2*. 5. vyd. Norwich: TSO, 2009. 346 s. ISBN 978-0-11-331059-3

ROSENAU, M. D. *Řízení projektů*. 3. vyd. Brno: Computer Press, 2007. 344 s. ISBN 978-80-251-1506-0.

ROYCE, W. Managing the Development of Large Software Systems [on-line]. [vid. 2014-12-22]. *Proceedings of IEEE WESCON*, 1970. Dostupné na http://www.cs.umd.edu/class/spring2003/cmsc838p/Process/waterfall.pdf

SCHUYLER, J. *Risk and Decision Analysis in Projects*. 2. vyd. Project Management Institute, 2002. 259 s. ISBN 978-1-88041-028-8.

SCHWABER, K. SCRUM Development Process. In Sutherland, J., Patel, D., Casanave, C., Hollowell, G., Miller, J. *Business Object Design and Implementation: OOPSLA '95 Workshop Proceedings*, 16 October 1995, Austin, Texas, London: Springer, 1997, pp. 117-134. ISBN 3-540-76096-2.

SCHWALBE, K. *Řízení projektů v IT: kompletní průvodce*. 1. vyd. Brno: Computer Press, 2011. 632 s. ISBN 978-80-251-2882-4.

SMEJKAL, V., RAIS, K. *Řízení rizik ve firmách a jiných organizacích*. 3. vyd. Praha: Grada Publishing, a.s., 2010. 360 s. ISBN 978-80-247-3051-6.

TICHÝ, M. *Ovládání rizika. Analýza a management*. 1. vyd. Praha: C.H.BECK, 2009. 396 s. ISBN 80-7179-415-5.

UNCTAD World Investment Report 2013: Global Value Chains: Investment and Trade for Development [on-line]. [vid. 2014-12-16]. United Nations Conference on Trade and Development, 2013. 264 s. ISBN 978-92-1-056212-6. Dostupné na http://unctad.org/en/publicationslibrary/wir2013_en.pdf

VOSE, D. *Risk Analysis: A Quantitative Guide*. 3. vyd. Chichester: John Wiley & Sons, 2008, 752 s. ISBN 978-0-470-51284-5.

ZAJÍČEK, M. Jak si lidé hrají. Lidové noviny, příloha Orientace [on-line]. 19. 1. 2011 [vid. 2015-1-1]. Dostupné na http://nf.vse.cz/ln-zajicek-jak-si-lide-hraji/