Řízení rizik

Risk management

Prevence možných škod
způsobených nepříznivými událostmi

Vývoj SW je riskantní činnost

Přínosy nejisté často jinde, než se čekalo

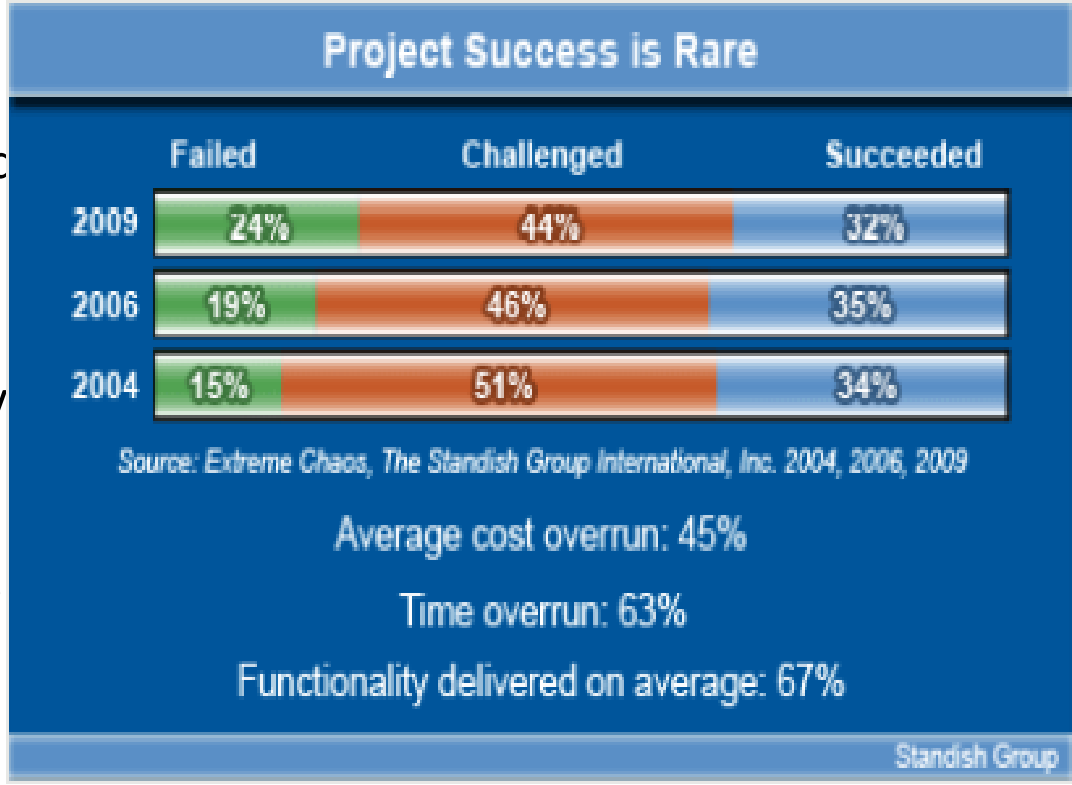
„Je mnoho statistik o efektech IT, chybí ale ty, které hodnotí skutečné přínosy“

Standish CHAOS Report 2009

Vývoj SW je riskantní podnik a moc se to nelepší

Is Project Success Really that Rare?

- Specifically, 32 percent of IT projects were considered successful, having been completed on time, on budget and with the required features and functions.
- Nearly one-in-four (24 percent) IT projects were considered failures, having been cancelled before they were completed, or having been delivered but never used.
- The rest (44 percent) were considered challenged: They were finished late, over budget, or with fewer than the required features and functions.



http://www.cio.com/article/495306/Recession_Causes_Rising_IT_Project_Failure_Rates_

Co je riziko

- **Riziko** je jev nebo událost, která může někdy nastat a pokud nastane způsobí škodu, čili
  - nastává s určitou pravděpodobností *p*,
  - do určité doby *T,*
  - pokud nastane způsobí určitou ztrátu *Z*
  - (srv Hall 1998)
- Riziko se **uskuteční,** dojde-li k rizikové události

Co je riziko

Hall , Managing Risks. Methods for Software Systems Development, SEI Series in Software Engineering, Addison Wesley, 1998).

Mnoho studií o řízení rizik

Odhady atributů rizika

- **Pravděpodobnost** *p* uskutečnění rizika.
- Hodnota pravděpodobnosti *p* se obvykle odvodí ze slovního hodnocení (vyloučeno, velmi nepravděpodobné, dosti nepravděpodobné, nepravděpodobné, spíše nepravděpodobné, tak napůl, spíše pravděpodobné, pravděpodobné, dosti pravděpodobné, velmi pravděpodobné, určitě nastane).
- Jednotlivým hodnocením se přiřadí hodnoty *p* po desetině v rozmezí 0 až 1. Někdy je snazší odhadnout přímo číselnou hodnotu *p*. Např. hodnota pravděpodobnosti havárie lehkovodního atomového reaktoru se dá odhadnout shora z toho kolik reaktorů je v provozu a jak dlouho. Odhad lze dále zpřesnit analýzou přínosů modernizace elektrárny pro bezpečnost provozu.

Atributy rizika (2)

- **Velikost** ztráty *Z* v korunách (velikost rizika) dojde-li k uskutečnění rizika (k rizikové události), lze také použít fuzzy ohodnocení, jako že uskutečnění rizika není přípustné.
- **Moment uskutečnění** rizika, případně etapa prací, kdy může dojít k uskutečnění rizika.
- Události (**triggery**), které způsobí, každý s určitou pravděpodobností, že dojde k uskutečnění rizika. Z pravděpodobností uskutečnění triggerů se určí celková pravděpodobnost (uskutečnění) rizika.

Atributy rizika (3)

- U triggerů sledovat dva atributy
  - Pravděpodobnost
  - Doba kdy je daný trigger aktuální
- Z atributů triggerů se pak určí příslušné atributy rizik.
- Pro dané riziko nemusí být známy všechny triggery. Pak je asi nejlépe, pokud triggery vyhodnocujeme, neznámé trigery specifikovat jako fiktivní trigger s určitou pravděpodobností

Rizika

Rizika nelze vyloučit. Boj s riziky je permanentní činnost

Existenci rizik brát nejen jako hrozbu ale především jako výzvu

- Jak minimalizovat škody,
- jak rozhodnout zda uzavřít smlouvu
- atd

Aparát vyhodnocování rizik lze použít i pro vyhodnocování výhodnosti alternativ řešení

Řízení (správa) rizik

- **Řízení rizik** je soubor činností a opatření umožňující odhadovat a snižovat ztráty případně jiné nepříznivé následky vyvolané rizikovými událostmi
- **Řízení (správa) rizik** je důležitou, často však zanedbávanou, součástí činností při každém projektu.
- Řízení rizik je součástí oboru nazývaného *krizové řízení*
  - patří do teorie organizace a řízení.

Rizika jako výzva

- O *řízení (správě) rizik* se hovoří zpravidla v situaci, kdy jsme již rozhodnuti uskutečnit nějakou činnost a chceme snížit či omezit následky možných rizik spojený s daným rozhodnutím či aktivitou.
- Principy hodnocení rizik používáme i tehdy, když se rozhodujeme, zda nějaký projekt uskutečnit či nikoliv nebo když při rozhodování hodnotíme přínosy a rizika spojená s různými variantami rozhodnutí.

Rizika jako výzvy

- V případě rozhodnutí o stavbě atomové elektrárny musíme do rozhodování zahrnout
  - rizika, která jsou spojena se stavbou a provozem elektrárny, např. terorizmus, přírodní katastrofy
  - ale také rizika a ztráty spojené s rozhodnutím elektrárnu nestavět (závislost na dovozech energií, ekologické zátěže z provozu tepelných elektráren – např. skleníkový efekt (ten může nastat), jiné škody z exhalací (ty jsou prakticky jisté), důsledky dřívějšího vyčerpání fosilních paliv atd.
  - Všimněme si, že bezprostřední rizika jsou velmi významné, dá se ale s nimi něco dělat, to neplatí v případě dlouhodobých efektů jako jsou klimatické změny

Rizika spalování biomasy

- Ztráta hnoje způsobí devastaci půdy
- Rostliny produkující biopalivo nehrání půdu před splachem

Událost, která jistě nastane můžeme hodnotit jako riziko s p=1.

Proč řízení rizik

- **Rizika jsou nedílnou součástí každé činnosti**, včetně těch zdánlivě bezproblémových (k nejvíce úrazům dojde při práci v domácnosti).
- S riziky je nutno počítat a systematicky postupovat tak, aby byla místo hrozby spíše výzvou, jak získat konkurenční výhodu (postupuji promyšleněji, mám menší ztráty).

Proč řízení rizik

- **Řízení rizik by měla koordinovat pověřená skupina pracovníků** (výbor pro řízení rizik RV), který může být identický s řídícím výborem projektu, členy RV mohou být externí experti na rizika.
  - RV se má scházet v termínech stanovených plánem řízení rizik a z každého zasedání má být pořízen zápis
  - U menších organizací se rizikům věnují alespoň některá zasedání řídícího výboru projektu
  - Analýze rizyk by s měla věnovat i jednomužná firma

Rizika u malé firmy

- Ne tak byrokratizované (proorganizované) řízení rizik jako u velké firmy, nejsou na to zdroje a často chybí i informace především při řízení rizik
- Hlavní zásady, které je důležité zachovávat
  - Rizika zjišťovat, detekce rizik je věcí všech, opatření při řízení rizik také,
  - Zjednodušené postupy řízení rizik používat spíše pro malé firmy a malé projekty

Proč a jak řízení rizik

- Základní podmínkou řízení rizik je vytvoření (virtuálního) seznamu rizik, které by mohly nastat. Tato činnost se nazývá **identifikace rizik**.
- Dají se při tom využít **seznamy možných rizik** publikované v různých studiích. Tyto seznamy rychle zastarávají.
- Je třeba používat zdravý rozum a zkušenosti a sledovat co se děje. To by měli dělat všichni

Proč a jak řízení (správa) rizik

- Seznam rizik se vytvoří na základě zkušeností, analýzy situace a aktualizuje se pravidelně na základě skutečného průběhu prací a nově zjištěných skutečností.
- Některá nová rizika mohou být během prací nově identifikována (a doplněna do seznamu), u jiných se může zjistit, že již nejsou aktuální (již se nemohou uskutečnit) nebo že se jejich pravděpodobnost či závažnost změnila.
- Stejně tak se mohou měnit aktuální opatření proti rizikům

Oblasti rizik (návrh SEI pro identifikaci rizik)

Pro každou oblast se stanoví žádoucí vlastnosti a vyhodnotí se jako riziko skutečnost, že daná vlastnost není zajištěna. Nebo se vyhodnotí nežádoucí vlastnost a rizika s ní spojená. To se pak chápe jako ZDROJE RIZIK.

SEI Software Engineering Institute, Carnegie Mellon University

Viz též

ISO 31000:2009, *Risk management – Principles and guidelines*

Oblasti rizik (návrh SEI pro identifikaci rizik)

1 Vlastní proces vývoje. ZDROJE RIZIK:

a) **Požadavky a vize** (stabilita, úplnost, jasnost, platnost, relevance, optimálnost, realizovatelnost, škálovatelnost, novost typu aplikace, ...), **to jsou nejdůležitější rizika** !!!!!

b) Návrh (funkce, obtížnost, rozhraní, testovatelnost, HW omezení, výkonnost)

c) Kódování a testy částí

d) Integrace (prostředí, produkty, systémová podpora)

e) Inženýrské faktory (udržovatelnost,spolehlivost, bezpečnost, zabezpečení, lidské faktory)

Oblasti rizik (SEI)

2. **Vývojové prostředí**
   a) SW procesy (formalizované, vhodné, kontrolovatelné, známé a zvládnuté, souhlas s požadavky)
   b) Systém vývoje (vhodný, s dostatečně službami, snadno použitelný, známý a zvládnutý, spolehlivý, je k dispozici včas)
   c) Procesy řízení (plánování, organizace projektu, zkušenosti a schopnosti manažerů, rozhraní projektu)
   d) Metody řízení (monitorování, personalistika, řízení kvality, řízení konfigurace)
   e) Pracovní prostředí (orientace na kvalitu, spolupráce, komunikace, morálka, týmové schopnosti, odbornost)

Příklady rizik

- **Hardware**: Opožděná instalace, nedostatečný výkon, nevhodné vlastnosti, nefunguje jak bylo slíbeno (stává se často při oživování počítačových sítí), chyby v kabeláži, nedodrženy podmínky instalace, neúplná dodávka, poškození při dopravě, selhání dodavatele, nedodržení
  dohod, slabá podpora ze strany dodavatele, nedodržení záruk.

Příklady rizik (zkušenosti)

3. **Podpůrný (základní) software:**
   - Opožděná instalace, nevhodný pro daný hardware,
   - nesprávná (nevhodná) funkčnost,
   - nedostatečná dokumentace (zvláště záporných vlastností),
   - nedostatečná podpora od dodavatele,
   - chyby v konfiguraci,
   - překročení ceny nebo nedodržení termínu.

Příklady rizik (zkušenosti)

5. Management (dnes hlavní riziko, viz Standish group, důvody selhání projektů, 2013)

- Špatně stanovené termíny a cena,
- Nedostatečné zdroje,
- Nezájem manažerů obou stran
- Nezájem uživatelů, nezapojení
- Změna manažera během řešení,
- Organizační neschopnost vést projekt,
- Špatně zvolený partner, chyby v hospodářské smlouvě,
- Nevhodné stanovení cílů, nekvalitní plán realizace, nedostatečná kontrola.
- Restart (selhání projektu a jeho znovuzahájení)

Příklady rizik (zkušenosti)

6. **Lidé**
   - Fluktuace, nemoci,
   - nedostatečné schopnosti,
   - nedostatečné nebo příliš pozdní školení,
   - nedostatečné kvalifikace a zkušenosti,
   - neschopnost týmové práce.
   - Neschopnost ajťáků spolupracovat s uživateli a porozumět znalostnímu oboru uživatel

Příklady rizik (zkušenosti)

7. **Uživatel**
   - **Management nezajišťuje dostatečnou podporu**
   - **slabá podpora spolupráce, nevstřícnost, žádá stále změny**
   - **není zajištěna spolupráce s koncovými uživateli, neúčast na společných pracích, ……**
   - neplatí, odstoupí od smlouvy, nezvládne systém

Příklady rizik (zkušenosti)

- 7. **Uživatel**
  - změny u uživatele (změna cílů, odstoupení od smlouvy atd.), změna majitele (je třeba se před následky bránit ve smlouvě),
  - nebezpečí bankrotu,
  - přechod na IS klade na uživatele příliš velké požadavky,
  - nedodrží se kvalitativní požadavky na IS,
  - Kvalita dat: nepřesnost nedostupnost či nespolehlivost dat.

Z čeho vychází identifikace rizik shrnutí

- Rizika mohou souviset (viz kapitola o specifikacích):
  - *S projektem* (kvalita organizace prací a managementu, zajištění zdrojů, realistické termíny, organizace spolupráce se zákazníkem, monitorování prací, subdodavatelé, týmová spolupráce);
  - Se *SW procesy* (síťové metody, vyladění SW procesů, podpůrné techniky jako správa konfigurace atd.).

Z čeho vychází identifikace rizik, shrnutí

- Rizika mohou souviset (viz kapitola o specifikacích):
  - S *vlastnostmi produktu* (kvalita specifikací, architektura produktu, novost problému, rozsah systému)
  - *S problémy spolupráce se zákazníky* (nezájem, nejasné cíle, změny požadavků, nespolupráce, málo školení, odpor, obavy ze ztráty zaměstnání, nevhodní partneři, restart)
  - *S kvalitou řízení* (chybějící zdroje, nezájem, nezajištění podmínek spolupráce, nereálné termíny , změny manažera, restart)

Rizika často souvisí s uživatelem

- Není schopen zformulovat co potřebuje (to obvykle neznamená co chce), mění zadání, má přehnaná očekávání,
- neposkytne koncové uživatele, neposkytne prostředky, nezajistí manažersky
- nezajistí spolupráci s vhodnými lidmi,
- neplatí, mění majitele (ošetřit ve smlouvě),
- je před bankrotem (ochranou může být rámcová smlouva a postupné platby),
- je jiný než uživatelé našich dřívějších produktů, má jinou velikost, než jsme zvyklí,
- **restart, nebo snaha o velký třesk**

Včasnost identifikace rizik

- Pro úspěch řízení rizik je důležitá *včasná identifikace rizik*. Do seznamu rizik je třeba zahrnout příčiny neúspěchu softwarových projektů, které jsme uvedli v úvodních přednáškách a v oddíle o cílech projektů. Všechna tam uvedená rizika jsou natolik významná, že je třeba je i bez odhadů metrik zahrnout do těch rizik, které je třeba analyzovat. U většiny těchto rizik není obtížné porozumět procesům, které vedou k uskutečnění rizika a včas detekovat problémy. Většinou lze nebezpečí rozpoznat při jednání s uživateli, během interview, a ze způsobu, jak se k věci staví management obou stran.

Indikace rizik

- Důležitým zdrojem indikací rizik je *operativa řízení projektu* jako je pravidelná analýza odchylek od plánu, reakce uživatelů na předvedení (prototypových) řešení a modelů, změny v přístupu k jednání a spoluúčasti na pracích (a intuice čili „čuch“), skluzy …

Udržování seznamu rizik

- Výběr pravděpodobných rizik ze seznamů rizik z literatury nebo vlastní DB rizik a také zkušenost
- Indikace rizik během interview při zjišťování požadavků (názory respondentů)
- Kontrolní dny a oponentury (review, inspekce, standardní oponentury)
- Řízení projektu (odchylky od plánu, nové skutečnosti).
- Iniciativa pracovníků (cítím-li průšvih, hned na to upozorním), zainteresovat všechny
- *Je důležité stále seznam aktualizovat včetně hodnot atributů rizik, K tomu je žádoucí použít vhodné nástroje, např. IS a organizační opatření, např. zainteresovat všechny, aby upozorňovali na rizika*
- *Pozitivně oceňovat spolupracovníky schopné detekovat průšvihy ve fázi zrodu*

Velké a malé projekty a rizika

- U větších projektů je rizikem sama neexistence systému řízení rizik, malá účast řešitelů a koncových uživatelů na identifikaci a analýze rizik (indikuje to špatnou motivaci) případně záporná motivace (strach o místo při detekci rizik, postavení, strach z nového) a chybná výběr klíčových pracovníků uživatele (stakeholders) pro detekci a analýzu rizik.

Velké a malé projekty (2)

- Klíčová rizika
- U menších projektů může být hrozbou malá účast řadových řešitelů a koncových uživatelů na identifikaci a analýze rizik.
  - Snižuje to nejen účinnost řízení rizik, ale je to pravděpodobně příznak dalších skrytých problémů (např. špatných vztahů v týmu).
  - Často k tomu dochází proto, že ten, kdo riziko zjistí, je v jistém smyslu nositelem špatných zpráv a nemusí se proto vždy setkat s uznáním. Je nelehký úkol managementu, aby k takovým jevům nedocházelo. Ostatně ve stejné situaci jsou kvalitní testéři.
  - Boj s těmito riziky třeba chápat všemi členy týmu jako obecně prospěšné opatření.

Pozorování

Každých deset let nové paradigma

Každých deset let se podle Moorova zákona zestonásobí kapacity IT

Riziko: Špatný odhad optimálního postupu (použité technologie, profesní růst) s uvážením Moorova zákona, viz osud Nokie

Změny v informatice

Roky	Typické úlohy	Technologie
-1960	Vědecko technické úlohy	Sálové počítače, děrné štítky, tiskové sestavy, FORTRAN,Algol
1960-1970	Ekonomické výpočty v dávce, postupný nástup terminálů	Sálové počítače, děrné štítky, tiskové sestavy, COBOL, datové systémy
1970-1980	Ekonomické výpočty v dávce, často interaktivní vstup dat, řízení technologií, krize IT 1980	Sálové počítače s terminály, minipočítače děrné štítky, tiskové sestavy, COBOL, C, Pascal, DB ….
1980-1990	Ekonomické výpočty v dávce, interaktivní vstup výstup, úlohy na PC, krize IT 1990 (meze PC)	Sálové počítače s PC místo terminálů, kancelářské úlohy pro PC, datové báze
1990-2009	Interaktivní výpočty na síti, e-komerce, Internet, sociální SW 2002 krize, Internetová bublina 2008 krize, IT nepomohlo	Servery, počítačové sítě, Internet, grafika, vývojová prostředí, databáze, globalizace, webové služby, podpora sociálních sítí

Změny v informatice

Roky	Typické úlohy	Technologie
2000- 2010	IT pro celosvětovou ekonomiku Servisní SW architektury, internet, krize IT 2009	Pokročilé PC, mobily, servery , PC a notebooky
2010	Sociální sítě, SOA řízené dokumenty	Pokročilé sítě, nové paměti, WiFi
2012	Cloudy, Internet pro všechny a na všem, IT ve všem Internet věcí, propojování autonomních systémů na globální úrovni,	Datové a počítačové globální sítě, Chytré mobily chytré spotřebiče
	Digitalizace uživatelských procesů, zapojení uživatelů	

Konkrétní příklady rizik

Registr vozidel a změna paradigmatu

- Registr propojuje nezávislé subsystémy používané jako služby, ty mohou mít různou architekturu
- Výkon závisí na různých skutečnostech
  - Kapacita sítě
  - Databáze
  - Logika řešení
  - Pravidla pro programování klientů a pro rozhraní klientů na systém
- Je třeba orchestrace a hrubozrnné komunikační protokoly komunikace a možná dávkové rozhraní na celoevropské databáze.

Co se relativně málo změnilo

- Lidé
  - Postoje
  - Cíle
  - Předsudky
  - Klínopisná destička z Uru (Sumerové, Abraham, 2000 let před Kr.): „Všude jsou lidé stejní pitomci“
- Potřeba a dovednost a zásady spolupráce a mezilidské komunikace

Jak reagovat na riziko

1. *Přijetí rizika* - žádná opatření (tak to risknem nebo madam Pompadour – po nás potopa).
2. *Vytvoření rezerv* - vytvoření rezerv na krytí případných ztrát. Tím se mohou omezit následné škody (např. v důsledku insolventnosti).
3. *Omezení rizika* – přijetí opatření snižující velikost ztráty *Z*.
4. *Prevence rizika* – přijetí opatření snižující pravděpodobnost *p* uskutečnění rizika; pokud se *p* sníží na nulu hovoříme o *vyloučení* rizika. Při prevenci jsou důležité informace o *triggerech* (bezprostředních příčinách) a procesech, které k riziku vedou.

Jak reagovat na riziko (2)

5. *Odmítnutí rizika* – riziko je natolik závažné, že se projekt se zastaví, nelze-li riziko vyloučit. Riziko tedy není přípustné. Atomky a zelení.
   - Často se zapomíná, že i s odmítnutím rizika mohou být spojeny značné skryté náklady (ztráta výnosů v důsledku zrušení projektu) a další rizika (např. ztráta zastoupení na trhu, ztráta znalostí, u zákazníka náklady na alternativní řešení, jiné škody).

Jak reagovat na riziko (3)

6. *Studium rizika* – hodnocení variant řešení a aspektů rizika nad obvyklý rámec
7. *Přenesení rizika* - ztráta z rizika se (částečně) přenese na jiný subjekt. Typickým příkladem je pojištění, ale také někdy outsourcing (přenos na někoho, kdo to umí lépe, nebo se může snáze vyrovnat s případnými ztrátami).

Jak reagovat na riziko 4

- Minimalizovat maximální riziko
- Místo jedné rizikové události s velmi velkým Z ale malou pravděpodobností *p* zvolím riziko s podstatně větší pravděpodobností ale menší ztrátou, nebo řadu rizik s malou ztrátou tak, aby úhrnná očekávaná ztráta příliš nevzrostla
  - Pět Sullivanů (pět bratrů zahynulo společně na jedné lodi - sourozenci nemají sloužit na jedné válečné lodi)
  - Pojištění je vlastně extrémní případ tohoto přístupu

Samozřejmost, na kterou se zapomíná

- *U každého opatření při řešení rizik je třeba vyhodnotit přínos opatření (měřený hodnotou rizika O = p*Z, tj. očekávané ztráty) proti nákladům a spotřebě jiných zdrojů (např. času špičkových pracovníků) vynaložených na řízení rizika.*

Lidé při řízení rizik

Základní činnosti lidí při řízení rizik

- identifikace rizik,
- změny v hodnocení atributů rizik,
- navrhování a provádění opatření pro snižování následků rizik nebo jejich prevenci,

Těchto činností byse měli účastnit všichni členové vývojového týmu a pracovníci uživatele včetně těch, kteří budou systém používat.

- Pracovníky je nutné motivovat a vyškolit. Pomáhá týmová loajalita a pocit vlastnictví projektu.

Soutěž rizik

- Při identifikaci rizik je obvykle identifikováno mnoho rizik. Osvědčuje se řešit jen několik nejzávažnějších (nejvýše do 12). Jako kriterium závažnosti se obvykle volí očekávaná ztráta (může být fuzzy)

$$O = p * Z.$$

Seznam rizik se uspořádá podle *O* a řeší se většinou nejvýše 10 prvých rizik. Ostatní rizika se tedy přijímají. Hodnocení rizik je třeba pravidelně opakovat a aktualizovat.

Zabezpečení řízení rizik

Pro správu rizik je nutno vytvořit vhodný informačnísystém

1. Připravit prostředí (nástroje, pravidla) – *infrastrukturu*
2. Připravit *procesy* vhodné pro daný účel – kdy, kdo, jaké akce a jejich souběh, podmíněnost a návaznost
3. To vše *implementovat* – plánovat podle vhodné metodologie, stanovit odpovědnosti a pravidla kontroly
4. Připravit *lidi* – kdo, co, jaké akce a role, školení a zainteresovanost

Zabezpečení řízení rizik,větší projekty

1. Definovat procesy jako síť činností pří řízení rizik (identifikace, analýza, hodnocení, stanovení opatření, monitorování rizik i účinků opatření, pravidla dokumentace, zásady plánování včetně požadavků na zdroje, plánování a kontrola, zapojení všech pracovníků).
2. Zabezpečit přípravu pracovníků a jejich účast na řízení rizik (míra a způsob účasti, motivace, školení, vybudování postojů). Jmenovat pracovníka vyčleněného (ne nutně na plný úvazek) pro činnosti spojené s řízením rizik.
3. Zabezpečení infrastruktury a implementace řízení (zabezpečení zdrojů, prostředky spolupráce, např. informační systém rizik, organizační zabezpečení, konkretizace plánu, operativní opatření při provádění plánu).

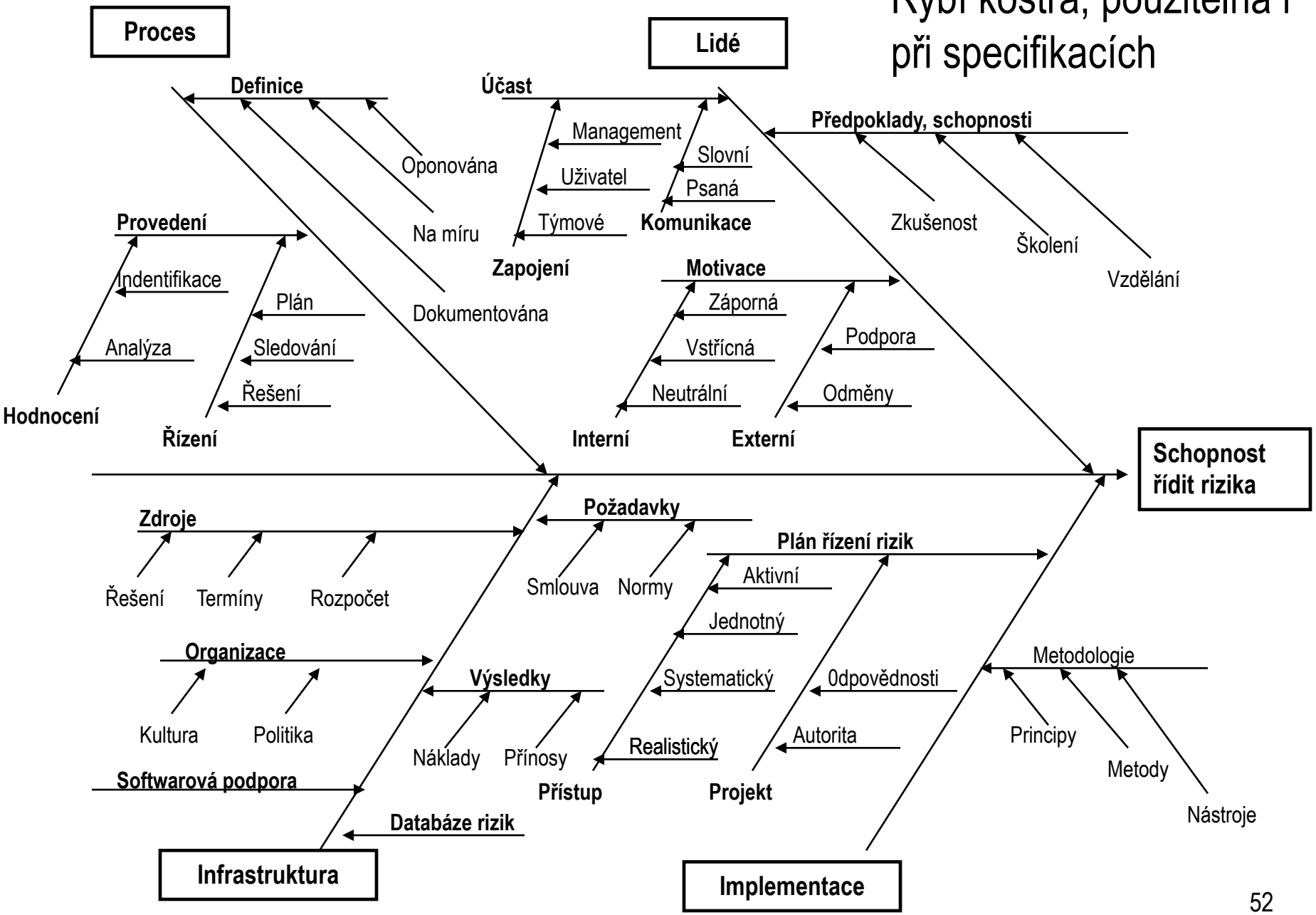
Rozsah činností souvisejících s řízením rizik závisí na velikosti projektu a znalostech lidí. Systém řízení rizik je žádoucí budovat postupně tak, že se zdokonalují potřebné procesy, postupně zapojují pracovníci, buduje infrastruktura (především oběh informaci, které mohou být zprvu pouze na papírových dokumentech) a buduje se organizace řízení rizik.

Naše diskuse má význam i pro specifikaci požadavků pro informační systémy. Dobrý informační systém by měl uživateli poskytovat prostředky pro identifikaci a analýzu rizik.

Je třeba stanovit postupy, vyškolit a zapojit lidi, vytvořit infrastrukturu (často včetně dedikovaného IS) a vše implemetovat

Činnosti při řízení rizik

Rybí kostra, použitelná i při specifikacích



Stupně řízení rizik (Hall, 99)

1. *Řízení na průšvih (přijetí rizika).* Neprovádí se žádné řízení rizik nebo až v případě akutního nebezpečí. Problémy se řeší až když nastanou nebo akutně hrozí.
   - Jsou situace, kdy je takový přístup optimální, např.
     - není-li dostatek zkušeností použitelných při identifikaci, analýze rizik a řízení rizik nebo
     - není dostatek zdrojů či času na jejich řešení.
   - Jinými slovy – všechna rizika se (téměř) přijmou.

Stupně řízení rizik (Hall, 99)

2. *Omezování rizik.* Identifikují se rizika a hledají se cesty, jak omezit jejich následky *Z* a jak snížit pravděpodobnost *p*, že se uskuteční.
   - Nevyžaduje se kvantitativní vyhodnocování atributů (metrik). Hodnocení rizik je spíše subjektivní a slovní (fuzzy).
   - Opatření proti rizikům se často provádějí v podstatě jen v počátečních etapách vývoje a jsou záležitostí spíše manažerů.
   - Sledují se spíše následky než příčiny rizik.

Stupně řízení rizik (Hall, 99)

3. *Prevence.* Činnosti související s omezováním rizik jsou úkolem celého týmu a provádí se ve všech etapách řešení projektu.
   - Identifikace rizik je dobře zvládnuta.
   - Hledají se prapříčiny rizik a detekují se procesy vedoucí k uskutečnění rizik. Mezery bývají v kvantifikaci atributů rizik.

Stupně řízení rizik (Hall, 99)

4. *Analýza a předpověď rizik*. Činnosti z 3. jsou založeny na dobré kvantifikaci (metrikách) atributů.
   - Proto je k činnostem popsaným v předchozím bodě prováděna statistická analýza metrik. To umožňuje předvídat vývoj rizika a lépe odhadnout, kdy se uskuteční. Lze také hodnotit kvalitu práce členů týmu řízení rizik.

Stupně řízení rizik (Hall, 99)

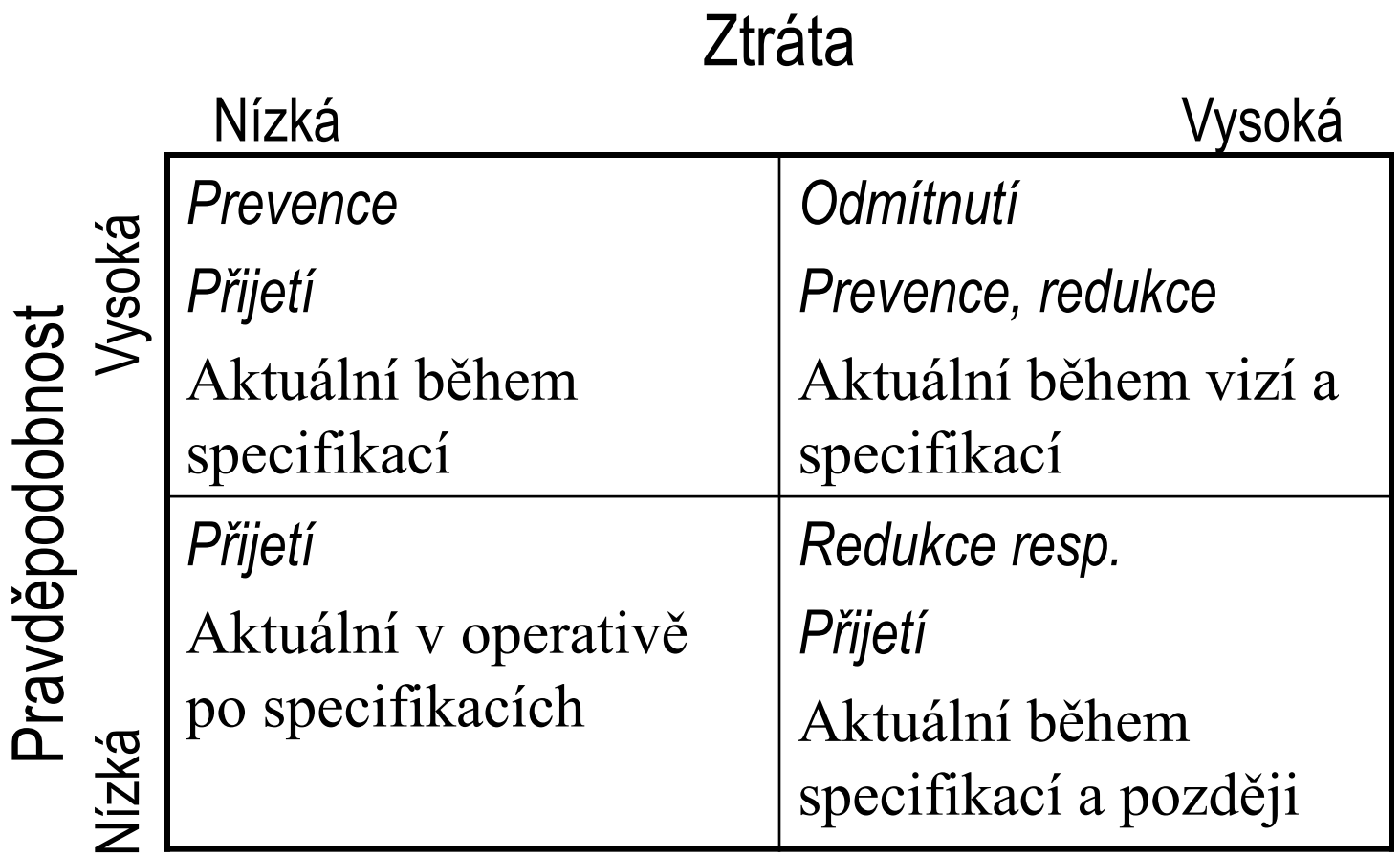
5. *Příležitosti.* Do řízení rizik jsou zapojeni všichni členové týmu, management a do jisté míry i obchodní partneři (např. možnost ohrožení termínů u dodavatelů). Rizika jsou chápána spíše jako výzva a příležitost ke zlepšení práce a nikoliv jako hrozba.

Co dělat, když máme jen hrubé odhady

- V tom případě nedělat složité procesy hodnocení rizik. Důvody:
  - Zbytečná práce, výsledky jsou stejně jen hrubé odhady
  - Odvádění od klíčových problémů
  - Oslabování „zdravého úsudku“
  - Zmenšení ostražitosti (provedl jsem analýzu, jsem za vodou)

Co dělat, když máme jen hrubé odhady jak je v menších podnicích obvyklé

- Odhadneme velikost ztráty a pravděpodobnost rizika dvoustupňovým hodnocením (nízká, vysoká)
- O většinu rizik se staráme až když jejich řešení považujeme za aktuální
- Je ale žádoucí se o rizika starat a sledovat možnost průšvihů a hned reagovat na nově zjištěné skutečnosti



Kurzivou jsou vypsány možné reakce, patkovým písmem – kdy je řešení aktuální

Antipattern

An antipattern is a seemingly good solution that is commonly used but known not to provide any satisfactory results.

It usually causes loses

It is risky to apply it

The leading antipatterns are difficult to avoid

- It often requires an paradigm change
- Business attitudes
- New ways of requirements specifications
- Marketing issues
- Etc.
- **Is is practically impossible to avoid all antipatterns at once**

Leading antipattern
No legacies, no 3rd party products

- Known also as *All From Scratch*. Implies often the antipattern *Reinvent the wheel* . Can be partly a consequence of the antipattern *Standardization Paralysis*
- A hot candidate on the leading position in the list of antipatterns in many areas
  - *Z* and *p* are especially high in global enterprises, e-government, global information (for example health care) systems

No legacies, no 3rd party products

- *Z* is for great systems usually *very large*
  - Unnecessary redevelopment costs, transfer costs and errors
  - Losses due staff errors, lost staff knowledge
  - Obstacle for a wider use of techniques like Mashup Programming
- *p* is high
  - The use of legacies is in OO world an important antipattern (see e.g. The OO antipatterns Stovepipe Systems, of Islands of Automation)
  - Interests of software vendors are against reuse
  - Bad habits or missing skills of developers
  - Existing software development tools
  - Necessity to change paradigm

No legacies, no 3rd party products

- *In the case of e-government it is always very costly to rewrite existing applications, so we reduce p (prevent the use of the antipattern), it is we should try to use existing applications.*

Scales of *p* and *O* and *p*Z*

p \ *Z*	small	large	very large
low	small	small	large
high	small	large	very large

No legacies, no 3rd party products

- The assessment of the antipattern is the highest possible:

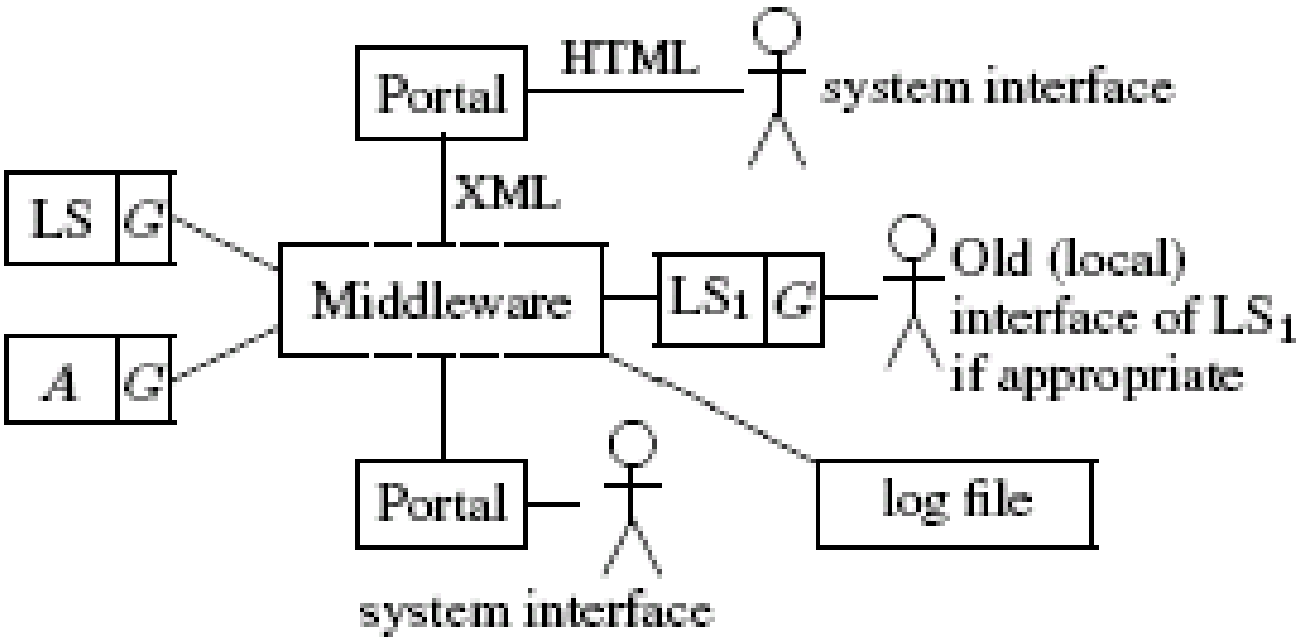
very large

It is the use of existing systems is crucial. We add that it surprisingly requires a specific way of thinking, it is a specific paradigm

No legacies, no 3rd party products

The refactorization of this antipattern can be based on the use of specific *architecture services* serving as front-end gates (or generalized adapters) of legacies as well as third party products or flexible portals of the whole system or a specific services. They the can be used as heads of composite services

SOA with legacies, simplified



Antipattern
No Businessmen Involvement

A wrong practice believing that well designed business processes should not be exceptionally changed by their users (i.e. no agility)

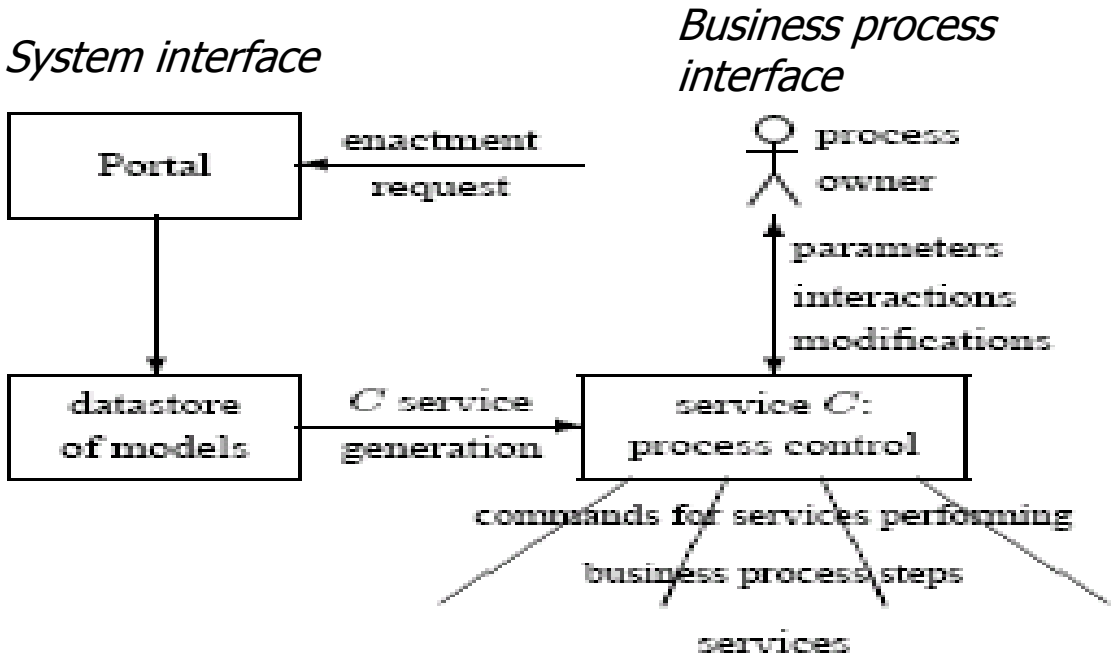
Business antipattern No Businessmen Involvement

- Consequences
  - Losses due necessary deficiencies in process models (data missing, obsolete, expensive ot get, changing business conditions), very important for small enterprises
  - No agile actions based on human experience and intuition
  - Limited business responsibility and agility only possible
  - Difficulties to use old models in “obsolete“ languages

Business antipattern No Businessmen Involvement

- Loss *Z of the antippatern* in business is *large* to *very large, p*
- Probability *p* is rather *high*
  - Agility sometimes desirable
  - Effective implementation not known fully yet
- Level *O= p*Z* is therefore *large* to *very large*

Implemetation of business processes enabling user involvement



Usable in mashup development

No Batch Services

- First systems constructed from autonomous units
  - Stability, reusability, security (Y2K)
  - Lower development effort
  - Used for decades
- Avoidance of batch mode is usually costly, sometimes not needed, *p* is *low, E large to very large , L* is therefore large
  - Batch services can be integrated via services having the capabilities of data stores

Antipattern
Standardization paralysis

- Tendency to use premature and cumbersome standards.
  - Typical for the standardization of user interfaces reflecting user domain knowledge an habits
  - Obstacle for the above implementation of business processes
    - Note the tendency to use SOAP in the massage encoding form
  - Standardization can be used to “implement” Vendor Lock In antipattern known from object oriented world

Antipattern
Standardization paralysis

- *p* is rather *high*
- Z is often *large*
- *O = large*

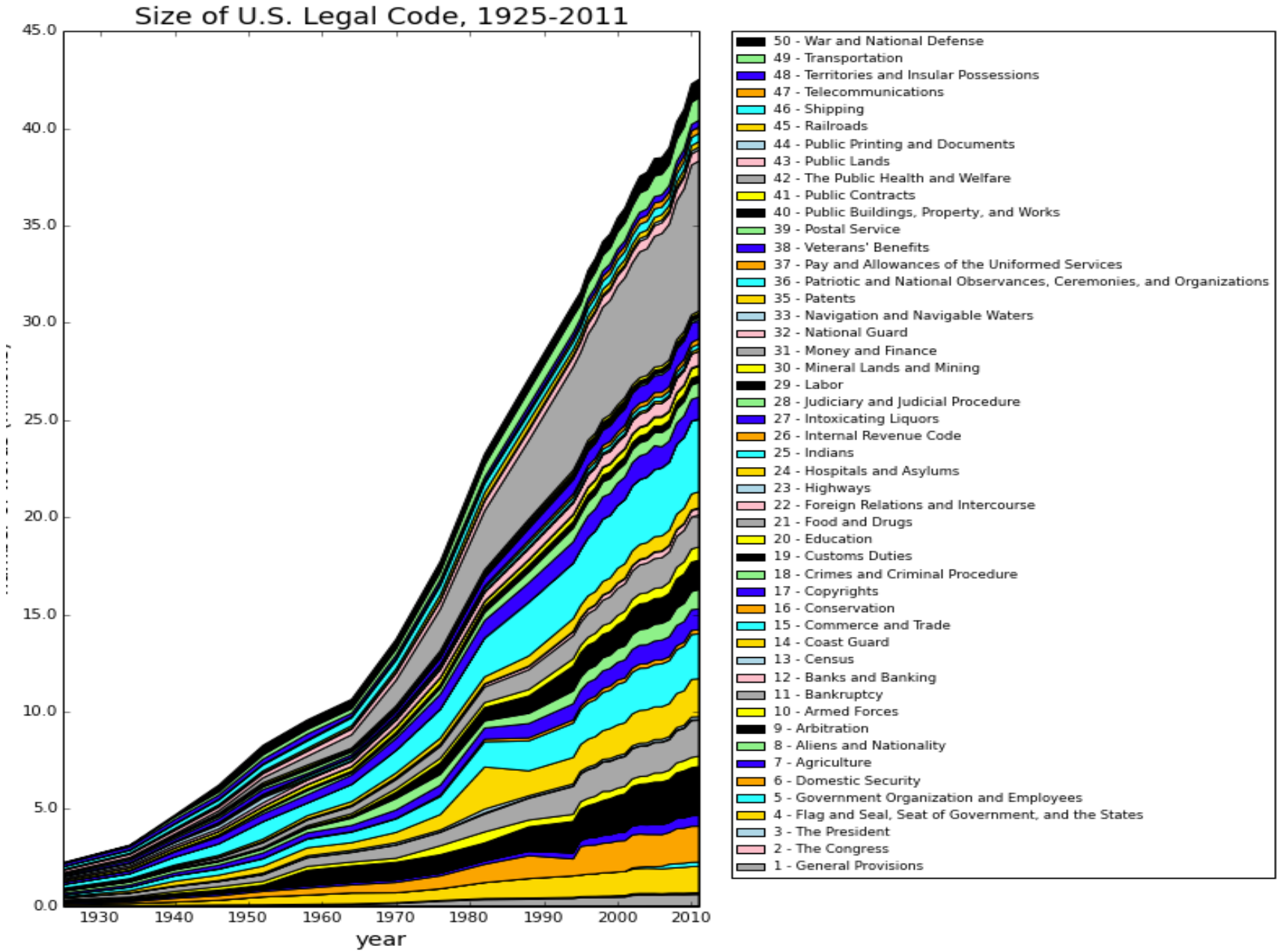
Refactorization

- Use a proper ballance between standards and proprietary solutions to be standardized later using experience anf tool like SOAP – message encoded

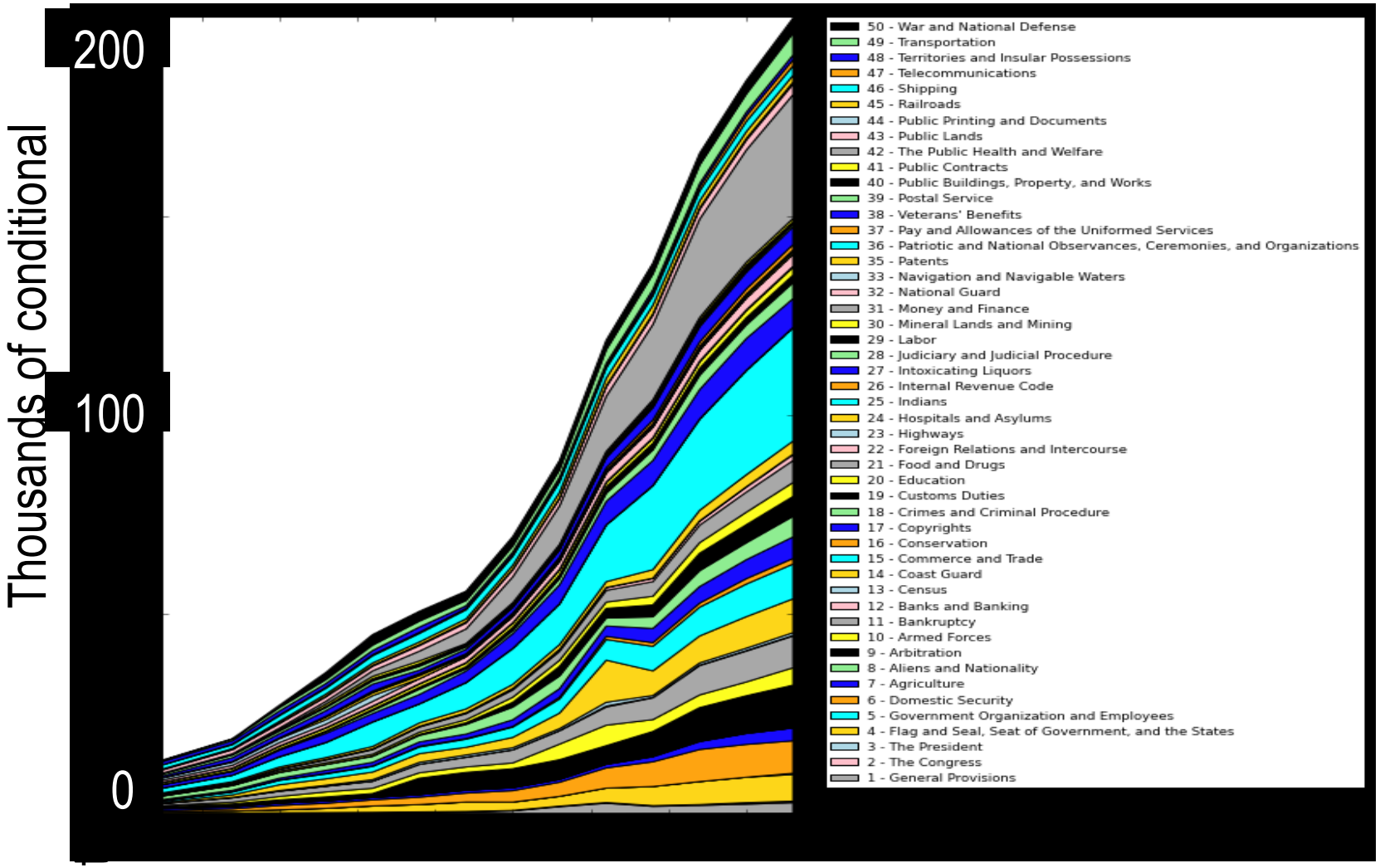
SW metriky pro texty zákonů

- **Délka v počtu slov**
- Roste o cca 4% ročně
  - V období 1925 až 2010 vzrostla 18krát
- **Metrika McCab**e
  - Počet uzlů + počet odkazů
  - Roste o něco pomaleji než délka

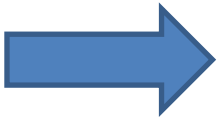
Možný průšvih,viz SSHD projekt



Metrika McCabe pro legislatuivu USA



Něco podobného platí pro SW normy

- SW norem se urodí každý rok spousty
- Jsou zpravidla obrovské (ISO 250xx), desetitisíce stránek nejsou výjimkou
- Každý 5 až deset let se modernizují (často sepisují od začátku
- Velké firmy si je definují k obrazu svému
-  nedají se snadno použít,
- **úniková cesta**“ autonomní komponenty a dokumentově orientovaná SOA

Normy i zákoony musí být zaplevelené

- Jsou důvody se domnívat, že pro normy je problém růstu ostřejší než u zákonů
- Problém nedosažitelné oblasti
  - Veliký text určité kvality nemohu udělat pod jistou dobu
- Doba > c*Delka$^{1/3}$
- V SW není času nikdy dost (dynamika oboru, nadměrná plodnost – antipattern *ještě by se hodilo tohle a tamto“*) nelze tedy udělat normu bez závad

Co s noarmami

- Pro SW normy ještě horší výskyt chyb a nedodělků než pro kód
- Něco se s tím musí udělat, jsou nutné ad hoc dohody nebo použití použitelné implementace podle normy (ne nutně přesná implemetace)
- Inspirací může být SW sám, vývoj využívající a autonomní komponenty

Kauzálni diagramy,

Stát, Podnik

Notace kauzálních diagramů

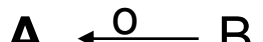
A a B se vyvíjejí synchronně. Roste-li A má B tendenci růst, klesá-li A má B tendenci růst

A a B se vyvíjejí opačně, růst A stimuluje pokles B pokles A stimuluje růst B

Zkratka pro

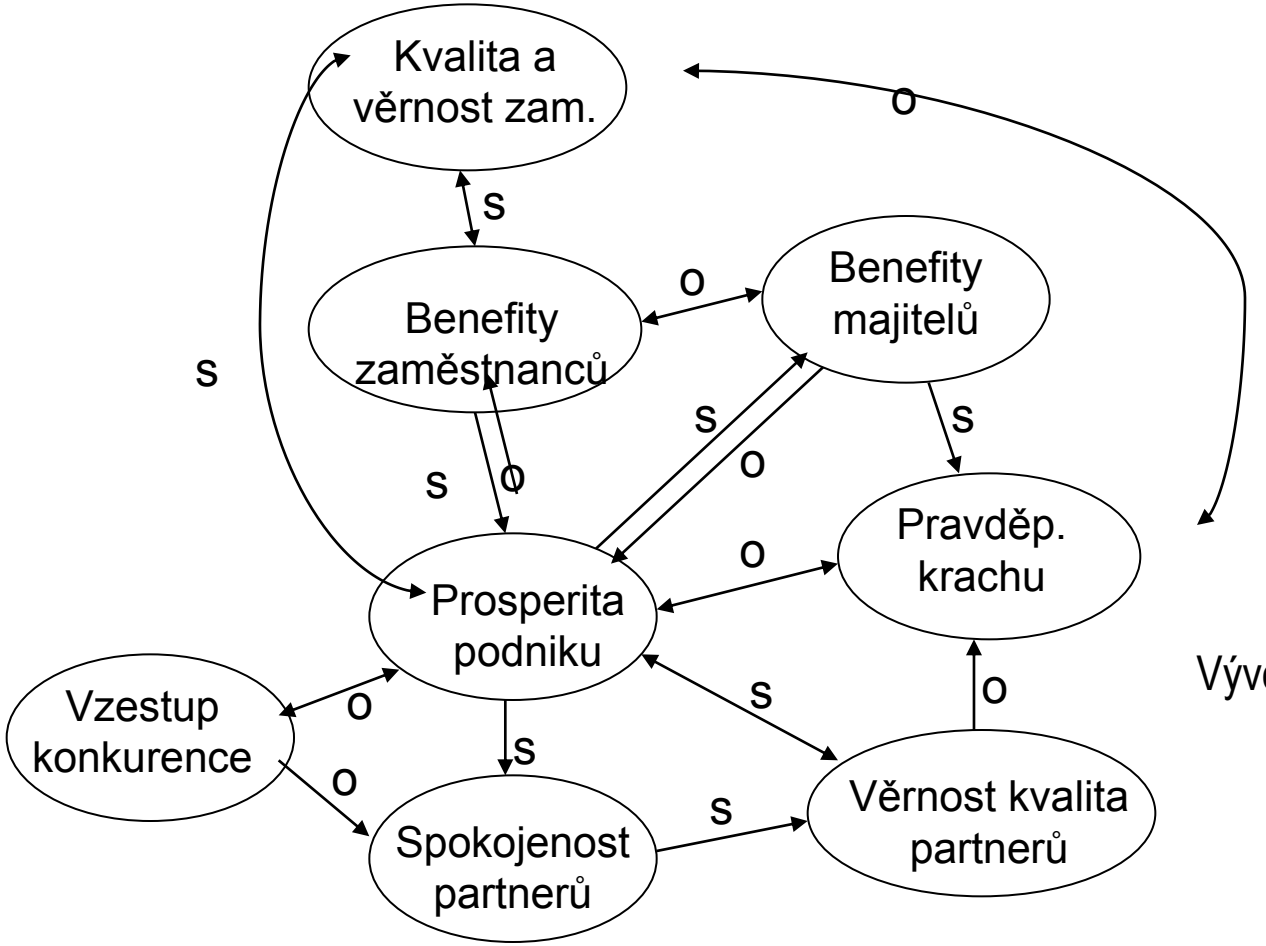
a

Zkratka pro



a

Kauzální závislosti pro podniky



Vývoj a dlouhodobé efekty?

Shrnutí hlavních požadavků

- Hlavní strategické přínosy
  - Pozice na trhu
    - Kvalitní služby a výrobky (montáž aut pro jednotlivé zákazníky na míru)
    - Inovace – tempo, vhodnost
    - Vyhledávání a spolupráce se zákazníky. Znalost jejich požadavků a potřeb
    - Spolupráce a kontrola dodavatelů
  - Podklady pro management, podpora rozhodování
  - Zlepšování kvality zaměstnanců (školení, zajímavá a perspektivní práce), lepší využívání jejich znalostí a schopností
  - Zkvalitňování byznys procesů a byznys inteligence

Shrnutí hlavních požadavků

- Taktické přínosy,
  - důležité, dlouhodobě nestačí
    - Plynulost a včasnost a efektivnost procesů
    - Zlepšování kvality
    - Úspory lidí ??? Ztráta znalostí, stres ve firmě????
    - Efektivnější vnitropodnikové procesy, lepší využití prostředků
    - Úspory zdrojů (zásoby, energie)

Překážky přínosů IS 1

Skrytým zdrojem růstu nákladů na IS bývá

- **nutnost příliš velkých organizačních změn** (prodlužuje to dobu zavádění IS a snižuje po jistou dobu výkon, zvyšuje rizika, zvyšuje náklady),
- snaha o **naprostou úplnost a dokonalost** oproti ***včasnosti***. Specifikace mohou být, jak víme, dokonalé jen postupně při postupném budování systému využíváním zkušeností s dosavadním provozem.
  - Přesné postupy mají smysl jen pro kvalitní data, jinak jsou kontraproduktivní
  - Podnik není počítač, vždy existuje náhodnost a vždy je nutné využívat znalostí a dovedností lidí

Překážky 2

- IS je drahé zboží, které poměrně rychle zastarává.
- Je tedy důležité, aby IS byl uvedeno do provozu včas i za tu cenu, že budou zprvu zprovozněny jen hlavní funkce.
- Cenu IS při metodě velkého třesku (všechno naráz) zvyšují ztráty vzniklé tím, že IS nepracuje během vývoje a uvádění do provozu a že vývoj nelze příliš zkracovat a že se mohu při formulaci požadavků zmýlit

Překážky 3

- Dlouhá doba zavádění IS do provozu zkracuje vlastně i dobu, kdy bude IS v provozu (od optimální doby provozu je nutné odečíst dobu zavádění). Je tedy důležité IS oživit co nejrychleji.
- Jsou známy případy, kdy odkládání uvedení IS do provozu pro nepodstatné maličkosti způsobilo ztráty z přínosů ve výši několikanásobně převyšující cenu IS. Stalo se dokonce, že kvůli odkladům nebyl vcelku vyhovující IS vůbec uveden do provozu.

Ničení dat jako ochrana před Velkým bratrem

Prý nutné pro splnění zásad Deklarace základních lidských práv a svobod, především práva na soukromí

- Data se de facto smí bez explicitního souhlasu dotčených osob používat a shromažďovat pouze k účelům, pro které byla legálně pořízena a to jen pověřenými institucemi
- Každá data nevyhovující této podmínce musí být zničena
- To nazveme **brutální proces ochrany dat (BPOD)**

Špatně nastavená pravidla ochrany osobních dat - úzké místo IS, především veřejných informačních systémů

Brutální metody ochrany (osobních) dat:
nemilosrdně mazat
mají chránit základní lidská práva

Dosahují ale opaku.
Ohrožují budoucnost IT, především ohrožují lidská práva

Riziko chybných mlčky činěných předpokladů, vlastně uplatnění předsudků

1. BPOD jsou v plném souhlasu s Deklarací základních lidských práv a jsou jejím důsledkem
2. BPOD umožňují efektivně chránit osobní data,
   - podstatně omezí počet případů, kdy mohou moje osobní data uniknout
3. BPOD nemají zásadní negativní sociální, celospolečenské a ekonomické efekty a nemají ani podstané negativní dopady na informatiku
   - Předpokládá se tedy, že škody, ke kterým by došlo kompromitováním osobních dat pokud by se BPOD nepoužívala, jsou podstatně závažnější než důsledky nedostupnosti *zveřejnitelných* informací vypočitatelných z osobních dat

Brutální procesy ochrany dat nezlepšují podstatně ochranu dat

- Pro každého je důležité, aby jeho osobní data nepřišla (neunikala) do nežádoucích rukou
  - jako osobě je mi jedno jakým způsobem a za jakým účelem.
- *Existuje ale mnoho kanálů úniku osobních dat a to BPOD nezmění!!*
- Některé existují ze zákona!!!!

Kanály úniků dat, některé je obtížné jiné nemožné uzavřít

- Mnohé údaje jsou veřejné ze zákona (obchodní rejstříky, registry nemovitostí, ..) a mnohé se z nich dá zjistit, jiné nejsou dostatečně zabezpečeny
- Některá data pacienta jsou např. pro léčbu natolik potřebná, že lékař považuje za správné je i přes zákazy využívat (jinak poruší Hippokratovu přísahu, de facto i zákon)
  - To oslabuje celý systém ochrany dat (legislativní disciplinu)
  - Ukazuje to, že není vše v pořádku

Kanály úniků dat, některé je obtížné jiné nemožné uzavřít

- Registry a rejstříky
  - (katastrální, obchodní, občanů,spolků, …)
- Mobilní telefony
- Webové služby
- Sociální software a sítě
- Serverové stanice, cloudy (DATA JSOU LECKDE)
- Finanční instituce
- Zdravotní instituce
  - (nesmí porušit Hippokratovu přísahu)
- Obchodování na webu
  - (často partneři nejsou dostatečně profesionální a opatrní, někdy ani nemohou být)
- Sledování z družic

BPOD ohrožuje základní lidská práva, např. právo na informace, život a dobrou zdravotní péči

- Příklad zákazu SOA systému na online monitorování výdeje léků jako prevence výroby pervitinu
  - Blokoval se nadměrný výdej léků s pseudoefedrinem jedné osobě za krátkou dobu jako prevence výroby Pervitinu
  - Výroba Pervitinu skutečně významně klesla
  - Systém byl zakázán ÚOOÚ, neboť používal zdravotní data jednotlivých osob (léky, které používají)
- Ponecháváme stranou podezření, že někteří zúčastnění s takovým výsledkem předem počítali

BPOD ohrožuje základní lidská práva, např. právo na život a na dobrou zdravotní péči

Důsledky:

- Výroba Pervitinu se po uplatnění BPOD (skartace a zákaz sběru dat o výdejích léků) zase rozjela
  - Tragédie narkomanů a jejich rodin
  - Posílení podsvětí
  - Znemožnění optimalizace spotřeby léků, kontroly kvality zdravotní péče a podpory zdravotního výzkumu

BPOD ohrožuje základní lidská práva, např. právo na život a na dobrou zdravotní péči

Důsledky 2:

Ztráta budoucích příležitostí:

- Nelze pomýšlet na on-line prevenci chybných medikací (ohrožení životů a zdraví),
  - To způsobuje ztráty životů na úrovni ztrát životů v dopravě (více než tisíc ročně),
    - v USA jsou kvalifikované odhady na úrovní cca 50000 ročně, takže u nás nějaký ten tisíc ročně, jistě existují kvalitnější odhady, základní zjištění platí a dá se použít i ve veřejných debatách.
  - Prevence chybných medikací by to mohla podstatně omezit počet vážných poškození zdraví.
    - V USA se odhaduje na cca 1,2 mil. ročně, takže u nás tak asi 50000 ročně. Počet postižených jde do statisíců

BPOD ohrožuje základní lidská práva, např. právo na život a na dobrou zdravotní péči

Důsledky 3:

Ztráta budoucích příležitostí

- Zhoršení podmínek zdravotnického výzkumu a kvality reakce na epidemie,
- Blokování optimalizace systému zdravotních pojišťoven,
- Kontrola účinků léků, optimalizace léčby.
  - Pár miliard by to hodilo.
- Objev cest šíření cholery analýzou osobních dat provedený londýnským lékařem kolem r. 1850 by dnes byl nezákonný

BPOD ohrožuje základní lidská práva, např. právo na život a na dobrou zdravotní péči

- Zákaz platí i pro využívání dat zdravotních pojišťoven akreditovanými pracovišti
  - To už je naprostá zhovadilost
- Pro státní správu má tedy de facto přednost ochrana dat před ochranou životů a zdraví
  - Pověsti,že některé instituce se k tomu oficiálně hlásí
  - Mělo by být veřejnosti známo, že hlavní efekt často je nemožnost veřejné kontroly!!!

Kde se ÚOOÚ chová nepatřičně

- Většina postupů hodnocení a správy rizik vychází z hodnocení přímých ztrát, nebere dostatečný ohled na skryté ztráty
  - Škody z výroby pervitinu
  - Důsledky ztrát znalostí
  - Sociální nestability

Omezování práva na kvalitní vzdělání

- Chybí nezávislý systém evaluace kvality škol a vzdělávání podle kriterií hodnotitele, např. rodiče
- Proto je obtížné vynucovat kvalitu výuky a správně volit směr studia a školu, není dohled nad efekty didaktických modernizací,
  - Stížnosti u nás i v USA (nedávno Obama)
  - Je dost indikací, že se kvalita vzdělání snižuje (především STEM, nic moc i pro soft obory), ale je obtížné vyvolat změnu k lepšímu
  - STEM cvičí i obecně potřebné pracovní dovednosti (přesné provedení, píle…), právě to není u kavárenských „in“

Rizika restrukturalizace podnikových procesů

- Je velmi žádoucí nemodifikovat radikálně podnikové procesy (business process reingeneering, BPR), pokud to není absolutně nutné. Zanedbání tohoto faktu vede k průšvihům
- V reálných situacích jsou v zemích, jako je ČR, BP skryty v myslích lidí a založeny na zvládnutých dovednostech a mnohé není vůbec explicitně zaznamenáno, vybaví se až při vzniku určité situace
  - Tak zvaná taktilní znalost, tu BBR obvykle zničí
- BPR likviduje znalostní náskok „starých“

Restrukturalizace podnikových procesů

- Obtížnost BPR – případ NDR. Úplná restrukturalizace průmyslu NDR se ukázala jako neobyčejně drahá a velice dlouhodobá záležitost.
  - Ani dnes po více než dvaceti létech není jasné, zda a kdy úspěšně skončí. Jisté náznaky zlepšení existují.
  - Domněka: Struktura průmyslu se zcela rozbila a jeho znovuvybudování je úkol pro více než jednu generaci. Dodnes jsou problémy
    - Cena změny: několik bilionů marek/euro (oficiálně 200 miliard marek (v dnešních cenách cca 300 miliard Euro ročně po mnoho let), fakticky asi mnohem více možná třikrát tolik

Restrukturalizace podnikových procesů

- Ani v USA nejsou s radikální BPR nejlepší zkušenosti i když tam obvykle nepředpokládají iniciativu při jejich provádění, takže se nové procesy snáze naučí a používají.
- Dosti velká kritika výsledků BPR
  - V podstatě se BPR v původním rozsahu neprovádí
  - BPR se zneužívalo pro omezení vlivu starých praktiků

Restrukturalizace podnikových procesů

Studium známých případů BPR naznačuje, že jistější a často i efektivnější cesta než radikální (tvrdé) BPR je angažování kvalitního manažera.

- Příklad IBM v sedmdesátých létech, manažer ji zachránil od krachu, BPR nikoliv
- Revoluční změny podnikových procesů, jako TQM (total quality management), často vedou ke zhoršení výsledků (výsledky průzkumu Gartner Group).
- Nové metody se často přeceňují, neboť je zavádějí nadprůměrní pracovníci a mnoho dobrých výsledků se dosahuje proto, že jsou nadprůměrní,měli by dobré výsledky i při používání jiných metod (viz školské reformy u nás), navíc se používají na to, nač se hodí (srv. hype křivku před líbánky)

Důvody selhání restrukturalizace podnikových procesů

- V déle existujících organizacích v Evropě je mnohé založeno na zkušenostech (vzpomenu si, co mám dělat až když nastane příslušná situace, to je tzv. taktilní dovednost a znalost). V restrukturalizovaných procesech se tato znalost ztratí.
- Změna typu procesů vyžadující změnu kultury (s iniciativou/přesný)
- Nové principy a zásady nemusí být pro danou situaci vhodné. Nové principy mohou být příliš jednostranné a poplatné módám a případně vhodné jen pro některé typy podniků, obvykle velké

Kritické požadavky

- U kritických požadavků se hodnotí rizika nevyhovění požadavku a také
  rizika a problémy spojené s implementací požadavku.
- Pro každý kritický požadavek se hledá odpověď na následující otázky:
  - má požadavek opravdu velký až kritický vliv na užitečnost IS?
  - pokud ano, jaké konkrétní parametry činnosti uživatele ovlivňuje? Tyto parametry by měly být kvantifikovatelné.

    Příklady: vyřizování zakázky se zkrátí z měsíce na čtrnáct dnů, snížení zásob
    o 10%, platby se kontrolují týdně, atd.

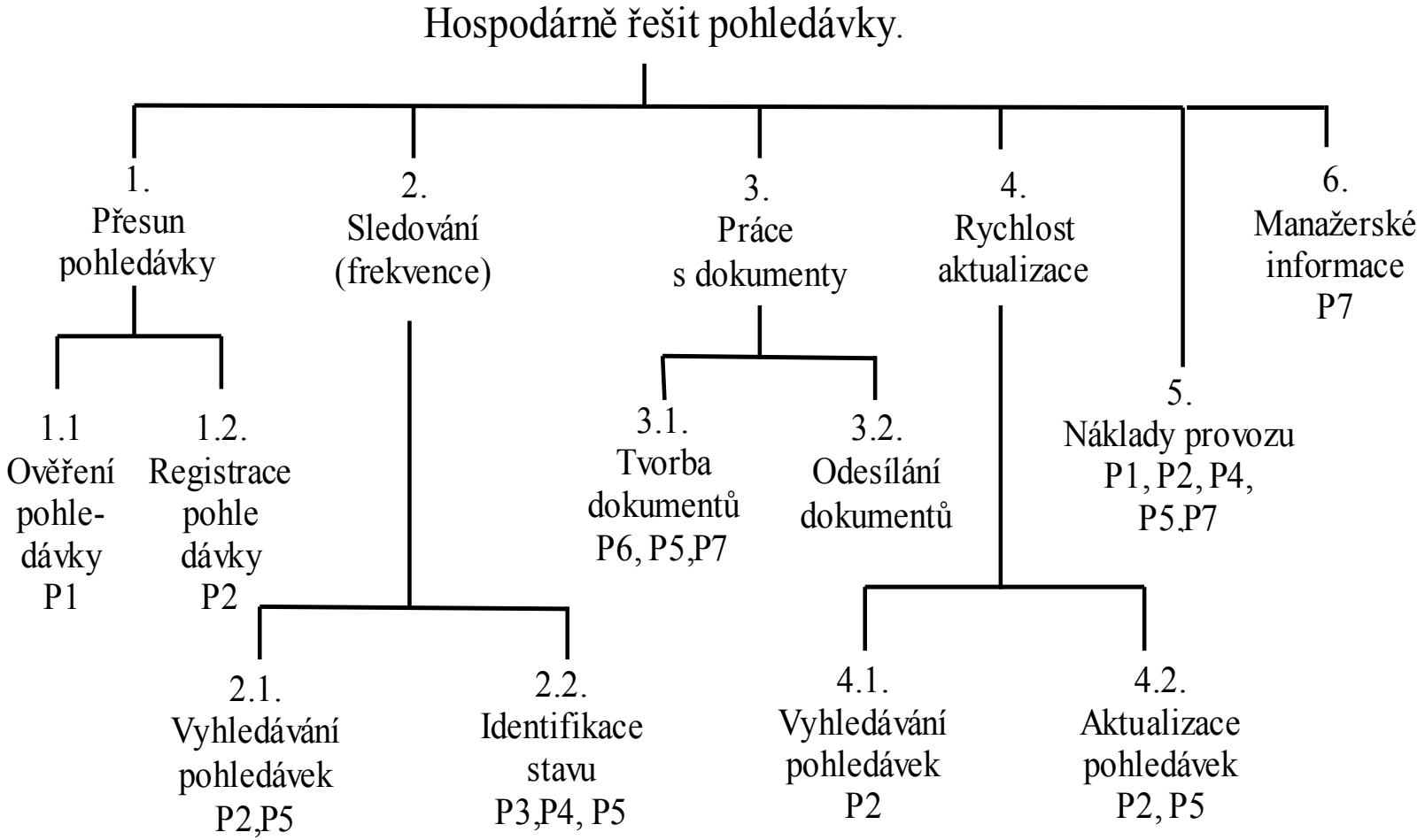
Kritické požadavky

Formálně se při analýze kritických požadavků postupuje následovně:

1. Stanovení podnikových cílů a kritických požadavků na IS. Vymezení priorit cílů. Pokud jsou cíle nezávislé nebo je nelze rozumně integrovat, je vhodné je řešit jako separátní projekty. S návrhem cílů musí souhlasit management.
2. Stanovení kritických oblastí výkonnosti: které důležité činnosti neexistují a které je třeba zlepšit kvantitativně i kvalitativně.

Kritické požadavky

3. Pokrytí jednotlivých kritických oblastí funkcemi: která funkce jak rychle co řeší. Funkce je vhodné analyzovat na základě analýzy **kritických oblastí výkonnosti** (critical performance areas). Při tom se využívá techniky postupné dekompozice. Dekompozice je založena na rozkladu kritického požadavku na požadavky elementárnější. Tak např. požadavek rychlejšího vyřizování pohledávek se rozkládá na požadavek rychlejšího zaznamenávání požadavků do databáze, rychlejší analýzy existujících pohledávek a rychlejší generace urgencí. Rychlejší a úplnější analýza pohledávek může být rozložena do úkolu detekce ekonomicky zajímavých případů a do procesu rozhodování, jak s jednotlivými případy naložit.


Hospodárně řešit pohledávky.
1. Přesun pohledávky
2. Sledování (frekvence)
3. Práce s dokumenty
4. Rychlost aktualizace
5. Náklady provozu P1, P2, P4, P5,P7
6. Manažerské informace P7
1.1 Ověření pohle-dávky P1
1.2. Registrace pohle dávky P2
3.1. Tvorba dokumentů P6, P5,P7
3.2. Odesílání dokumentů
2.1. Vyhledávání pohledávek P2,P5
2.2. Identifikace stavu P3,P4, P5
4.1. Vyhledávání pohledávek P2
4.2. Aktualizace pohledávek P2, P5

Kritické požadavky, příklad

Uveďme postup vyhodnocování rizik v metodologii SSADM na příkladu analýzy systému vyhodnocování pohledávek (viz obr. 1.).

A) Vyhodnocení kritických požadavků (KP).
a) *Stanovení kritických požadavků*.
Zkvalitnit práci při vyřizování pohledávek (včasnost detekce neplatičů) a zmenšit provozní náklady na tuto činnost.
Stručně cíl : Hospodárně řešit pohledávky.
b) *Kritické oblasti výkonnosti .*
Hlavní požadavek : Hospodárně řešit pohledávky.
Činnosti:

B) KP 1. Přesun pohledávky do oddělení fakturace nejpozději do vzniku práva účtovat.
KP 2. Sledování pohledávek ve stanovenou dobu po splatnosti pro provedení nápravných akcí (upomínky, soud).
KP 3. Příprava akcí : Poloautomatická příprava podkladů pro urgence/ soudní řízení .
KP 4. Reakce po pohybech na účtu kam má přijít platba pohledávky (např. zastavení akcí u soudu po obdržení platby).

Kritické požadavky, příklad

Při bližším pohledu se úkol přesunu pohledávky dělí na dvě etapy
- KP 1.1. Ověření pohledávky (relevantnost, splnění formálních náležitostí).
- KP 1.2. Registrace pohledávky.

Podobně sledování pohledávek se člení na:
- KP 2.1. Vyhledání pohledávky.
- KP 2.2. Vyhodnocení stavu pohledávky.

Požadavek KP 3. Příprava akcí - se člení na:
- KP 3.1. Generace dokladů.
- KP 3.2. Odesílání dokladů.

Aktualizace pohledávek má podúkoly:
- KP 4.1. Vyhledávání pohledávek (nemusí mít identický průběh jako KP 2.1).
- KP 4.2. Záznam změn:

Kritické požadavky, příklad

B) Stanovení kvalitativních a kvantitativních požadavků zákazníka *Podnikové cíle*. Na základě analýzy kritických požadavků byly zformulovány následující kvantitativní kritéria.

Cíl 1 : Počet splatných pohledávek (nesplacených více než 10 dnů po splatnosti) k počtu splacených : Dnes 2 :1, požadováno 10:9.

Cíl 2 : Náklady na urgenci jedné pohledávky snížit 3 krát (z 250 Kč na 70 Kč). Důvod cíle: Lze s positivním efektem vymáhat i malé pohledávky počínaje od pohledávek ve výši cca 200 Kč, lze ušetřit pracovníky v oddělení fakturace.

Kritické požadavky, příklad

Konkretizace požadavků do tvaru podcílů:

C1. Snížit průměrnou dobu přesunu pohledávek ze 4 dnů na jeden den.
C2. Sledování pohledávek: Z vyhodnocování a kontroly prováděné dosud jednou za měsíc přejít na provádění jednou za týden.
C3. Doba vyřizování korespondence : Den jako dosud s menší pracností).
C4. Aktualizace pohledávky: Provádět jednou za den místo jednou za týden (optimální by však bylo provádění ihned po změně).

Povinné požadavky:

R1. Pohledávky vymáhat podle zákona.
R2. Přístup k datům podle povinných norem.

Kritické požadavky

- U kritických požadavků se hodnotí rizika nevyhovění požadavku a také
  rizika a problémy spojené s implementací požadavku.
- Pro každý kritický požadavek se hledá odpověď na následující otázky:
  - má požadavek opravdu velký až kritický vliv na užitečnost IS?
  - pokud ano, jaké konkrétní parametry činnosti uživatele ovlivňuje? Tyto parametry by měly být kvantifikovatelné.

    Příklady: vyřizování zakázky se zkrátí z měsíce na čtrnáct dnů, snížení zásob
    o 10%, platby se kontrolují týdně, atd.

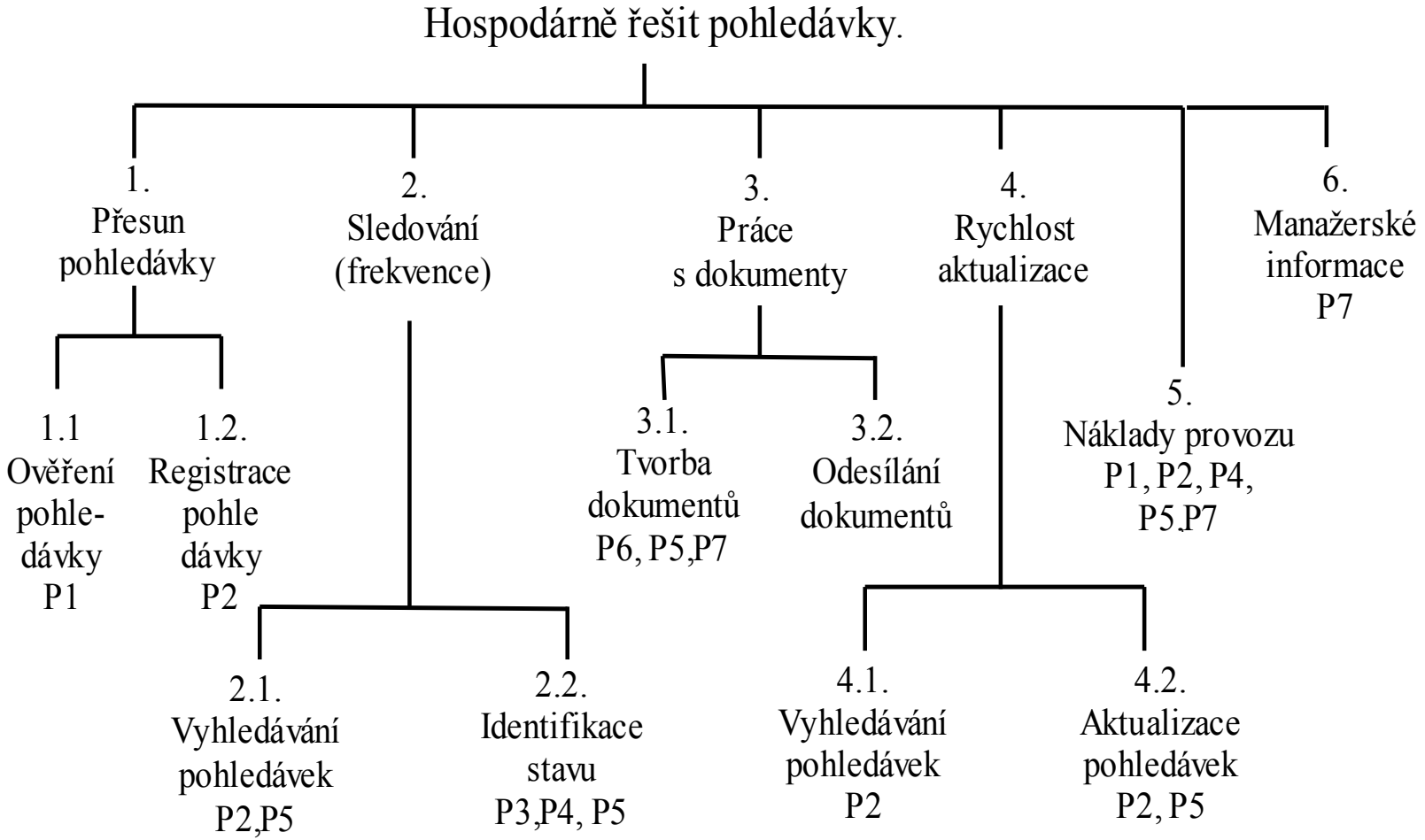
Kritické požadavky

Formálně se při analýze kritických požadavků postupuje následovně:

1. Stanovení podnikových cílů a kritických požadavků na IS. Vymezení priorit cílů. Pokud jsou cíle nezávislé nebo je nelze rozumně integrovat, je vhodné je řešit jako separátní projekty. S návrhem cílů musí souhlasit management.
2. Stanovení kritických oblastí výkonnosti: které důležité činnosti neexistují a které je třeba zlepšit kvantitativně i kvalitativně.

Kritické požadavky

3. Pokrytí jednotlivých kritických oblastí funkcemi: která funkce jak rychle co řeší. Funkce je vhodné analyzovat na základě analýzy **kritických oblastí výkonnosti** (critical performance areas). Při tom se využívá techniky postupné dekompozice. Dekompozice je založena na rozkladu kritického požadavku na požadavky elementárnější. Tak např. požadavek rychlejšího vyřizování pohledávek se rozkládá na požadavek rychlejšího zaznamenávání požadavků do databáze, rychlejší analýzy existujících pohledávek a rychlejší generace urgencí. Rychlejší a úplnější analýza pohledávek může být rozložena do úkolu detekce ekonomicky zajímavých případů a do procesu rozhodování, jak s jednotlivými případy naložit.


Hospodárně řešit pohledávky.
1. Přesun pohledávky
2. Sledování (frekvence)
3. Práce s dokumenty
4. Rychlost aktualizace
5. Náklady provozu P1, P2, P4, P5,P7
6. Manažerské informace P7
1.1 Ověření pohle-dávky P1
1.2. Registrace pohle dávky P2
3.1. Tvorba dokumentů P6, P5,P7
3.2. Odesílání dokumentů
2.1. Vyhledávání pohledávek P2,P5
2.2. Identifikace stavu P3,P4, P5
4.1. Vyhledávání pohledávek P2
4.2. Aktualizace pohledávek P2, P5

Kritické požadavky, příklad

Uveďme postup vyhodnocování rizik v metodologii SSADM na příkladu analýzy systému vyhodnocování pohledávek (viz obr. 1.).

A) Vyhodnocení kritických požadavků (KP).
a) *Stanovení kritických požadavků*.
Zkvalitnit práci při vyřizování pohledávek (včasnost detekce neplatičů) a zmenšit provozní náklady na tuto činnost.
Stručně cíl : Hospodárně řešit pohledávky.
b) *Kritické oblasti výkonnosti .*
Hlavní požadavek : Hospodárně řešit pohledávky.
Činnosti:

B) KP 1. Přesun pohledávky do oddělení fakturace nejpozději do vzniku práva účtovat.
KP 2. Sledování pohledávek ve stanovenou dobu po splatnosti pro provedení nápravných akcí (upomínky, soud).
KP 3. Příprava akcí : Poloautomatická příprava podkladů pro urgence/ soudní řízení .
KP 4. Reakce po pohybech na účtu kam má přijít platba pohledávky (např. zastavení akcí u soudu po obdržení platby).

Kritické požadavky, příklad

Při bližším pohledu se úkol přesunu pohledávky dělí na dvě etapy
- KP 1.1. Ověření pohledávky (relevantnost, splnění formálních náležitostí).
- KP 1.2. Registrace pohledávky.

Podobně sledování pohledávek se člení na:
- KP 2.1. Vyhledání pohledávky.
- KP 2.2. Vyhodnocení stavu pohledávky.

Požadavek KP 3. Příprava akcí - se člení na:
- KP 3.1. Generace dokladů.
- KP 3.2. Odesílání dokladů.

Aktualizace pohledávek má podúkoly:
- KP 4.1. Vyhledávání pohledávek (nemusí mít identický průběh jako KP 2.1).
- KP 4.2. Záznam změn:

Kritické požadavky, příklad

B) Stanovení kvalitativních a kvantitativních požadavků zákazníka *Podnikové cíle*. Na základě analýzy kritických požadavků byly zformulovány následující kvantitativní kritéria.

Cíl 1 : Počet splatných pohledávek (nesplacených více než 10 dnů po splatnosti) k počtu splacených : Dnes 2 :1, požadováno 10:9.

Cíl 2 : Náklady na urgenci jedné pohledávky snížit 3 krát (z 250 Kč na 70 Kč). Důvod cíle: Lze s positivním efektem vymáhat i malé pohledávky počínaje od pohledávek ve výši cca 200 Kč, lze ušetřit pracovníky v oddělení fakturace.

Kritické požadavky, příklad

Konkretizace požadavků do tvaru podcílů:

C1. Snížit průměrnou dobu přesunu pohledávek ze 4 dnů na jeden den.
C2. Sledování pohledávek: Z vyhodnocování a kontroly prováděné dosud jednou za měsíc přejít na provádění jednou za týden.
C3. Doba vyřizování korespondence : Den jako dosud s menší pracností).
C4. Aktualizace pohledávky: Provádět jednou za den místo jednou za týden (optimální by však bylo provádění ihned po změně).

Povinné požadavky:

R1. Pohledávky vymáhat podle zákona.
R2. Přístup k datům podle povinných norem.

Kritické požadavky, příklad

D) Vyhodnocení problémů (formuluje zákazník, někdy dodavatel) je třeba vázat na kritické požadavky např. následujícím způsobem.

P1. *Chybně vedené pohledávky:*

KP 1.1. Ověření přesnosti pohledávek(párování s fakturami).

KP 5. Provozní náklady na evidenci a sledování pohledávky.

P2. *Neefektivní ruční práce, požadavek zahrnout do:*

KP 1.2. Registrace pohledávek.

KP 2.1. KP 4.1. Vyhledávání pohledávek.

KP 5. Pracnost (shrnutí požadavků): Sledovat při všech činnostech.

P 3. *Nedokonalá kontrola pohledávek*:

KP 2. Sledování pohledávek. Pomalé (jednou za měsíc), často nepřesně

Kritické požadavky, příklad

P 4. *Adekvátnost a rychlost rozhodnutí, zda je nutná urgence*. Souvisí s kritickými požadavky
KP 2.2. Identifikace stavu účtu a potřebných opatření.
KP 2. Náklady.
P 5. *Resty* (opožděná evidence plateb a změny adres partnerů).
KP 2.2. Identifikace stavu pohledávky.
KP 3.1. Tvorba dokladů (přesnost, úplnost dokumentů, včasnost).
KP 5. Vyhodnocení nákladů na provedení.
P 6. *Tvorba dokumentů* (musí odpovídat právním požadavkům):
KP 3.1. Generace dokumentů.
P 7. *Tvorba měsíčních statistik* (manažerské informace).
KP 5. Náklady na generaci dokumentů a statistik.

Kritické požadavky, příklad

E) Návrh řešení (stručně) :

Problém P1 (viz. KP 1.1., KP 4.1.) *Nesprávné pohledávky :*
Vyžádání zásahu operátora (který bude mít právo přístupu k fakturám)
Problém P2 (KP 1.2., KP 2.1., KP 4.1, KP 5.) *Neefektivní ruční registrace.* Řešit tím, že se pohledávky zpřístupní uložením do databáze, do které budou mít interaktivní přístup všichni oprávnění pracovníci.
Problém P3 (KP 2.). *Nedokonalá kontrola*. Řešit automatickým vyhledáváním pohledávek podle předem známých i uživatelem zadávaných kritérií.
Problém P4. *Stavy pohledávek* (KP 2.2, KP 5.). Výběr pohledávky se provádí na základě informací, že prošel termín určité činnosti.
Problém P5 *Nedodělky* ("resty", KP 2.2, KP 3.1., KP 3.).
Bude řešeno : Integrací dat (změna adresy se odvodí např. ze změny údajů na dodacím listě), vytvoří se aparát "párování plateb a faktur" a prostředky evidence dat

Kritické požadavky, příklad

F) Úspory

Požadavek managementu byl *uspořit 15 pracovníků*. Při zahrnutí pojištění, daní a režie cca 5 mil Kč /rok

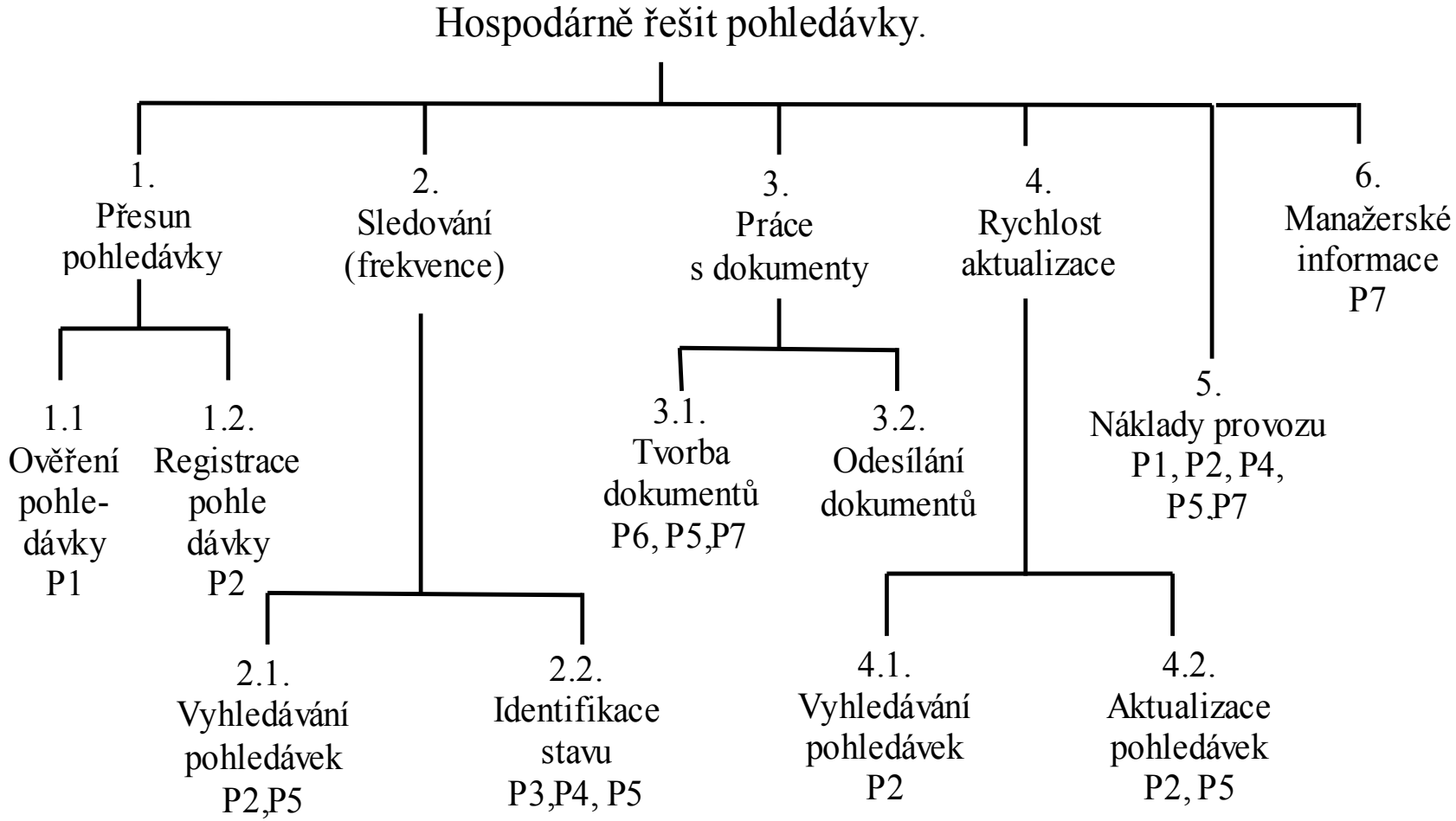
Úspory na prostředcích vázaných na faktury: Zkrácení průměrné doby proplacení o 14 dnů a výnosy z dříve neurgovaných pohledávek přinese cca 5 mil Kč (při několika desítkách pracovníků v oddělení fakturace musí být roční obrat firmy řádově stovky milionů Kč, zlepšení platební kázně zákazníků přinese procenta obratu, tedy miliony).

Snížení skladových zásob: Několik miliónů Kč .

Kritické požadavky, příklad

F) Úspory

Lepší informace pro management a lepší podpora obchodní činnosti (např. snížení počtu reklamací odběratelů, možnost častěji vyhovět přání zákazníků): Více než 10 mil Kč. Tento odhad vyžaduje podrobnější rozbor. Jak je uvedeno výše úspora 15 pracovníků kontrolujících pohledávky naznačuje, že obrat firmy bude řádově ve stamiliónech a tedy rabat v desítkách milionů. Zvětšení obratu o deset procent přinese efekt blízký deseti milionům. Tento přínos je při správném využití dat možný. Vyžaduje však nástroje presentace dat, umožňující rychlou orientaci (vizualizace, těžba dat - data mining) pracovníků managementu. Z uvedeného příkladu je patrné, že i podstatná úspora pracovníků nepředstavuje největší přínos IS.


Hospodárně řešit pohledávky.
1. Přesun pohledávky
2. Sledování (frekvence)
3. Práce s dokumenty
4. Rychlost aktualizace
5. Náklady provozu P1, P2, P4, P5,P7
6. Manažerské informace P7
1.1 Ověření pohle-dávky P1
1.2. Registrace pohle dávky P2
3.1. Tvorba dokumentů P6, P5,P7
3.2. Odesílání dokumentů
2.1. Vyhledávání pohledávek P2,P5
2.2. Identifikace stavu P3,P4, P5
4.1. Vyhledávání pohledávek P2
4.2. Aktualizace pohledávek P2, P5

Příklad analýzy rizik, atomová elekrárna

- Uveďme příklad analýzy rizik obecně známého problému atomových elektráren, na němž lze ukázat řadu aspektů řízení rizik, které se vyskytují u řízení rizik obecně, tedy i u softwarových projektů.
- Na níže uvedeném příkladu analýzy rizik atomové elektrárny lze velmi dobře ukázat problémy, které se nevyhýbají ani softwaru, jsou tam ale méně zjevné a proto se s fatálními důsledky často zanedbávají..

Příklad analýzy rizik, atomová elektrárna

- Výstavba atomových elektráren byla v mnoha zemích zpomalena či zcela zakázána. Česká elektrárna v Temelíně je terčem častých protestů. Jak jsou fundované?

Příklad atomové elektrárny

Za hlavní rizika považují odpůrci i zastánci energie z jádra:

1. Možnost havárie s následným radioaktivním zamořením širokého okolí.
2. Problém odpadů
   - problém bezpečné likvidace nebo uložení radioaktivních odpadů. (tj. realizovatelnost, cena, dlouhodobé ohrožení),
   - problém zneužití (dostupnost pro výrobu jaderných zbraní a možnost vyhrožování radioaktivním zamořením úmyslným rozptylem radioaktivních materiálů).

Příklad analýzy rizik

- Odpůrci elektrárny požadují řešení odmítnutím rizik, tj. původně neuvedením elektrárny do provozu nebo nyní jejím odstavením. Poukazují na kauzu Černobylu. Považují rizika i vzhledem k existenci terorizmu za natolik závažná, že je nechtějí připustit.
- Zastánci elektrárny se domnívají, že se rizika přeceňují a rizika spojená s nedokončením podceňují.
- *Pro přijetí kvalifikovaného rozhodnutí je nutné rizika analyzovat, nějak odhadnout velikosti ztráty Z při uskutečnění rizika a jeho pravděpodobnosti p. Ale také důsledky a rizika rozhodnutí elektrárnu nestavět. A také uvážit, zda nejsou některá rizika překryta jinými (KLDR, Írán, tam se při využíváni atomu neomezuji…)*

Příklad analýzy rizik

- Budeme možné přínosy a rizika hodnotit z hlediska důsledků rozhodnutí elektrárnu odstavit. Níže uvedený rozbor je koncipován jako ilustrační, nikoliv však nereálný příklad. Úplná analýza je záležitostí pro tým odborníků na měsíce až roky práce

Příklad analýzy rizik

- Rozhodnutí elektrárnu odstavit může přinést nějaké úspory a vyloučit výše uvedená rizika. Ohodnocení takových rizik uvádíme s kladným znaménkem.
- Na druhé straně přinese takové rozhodnutí ztráty (např. výpadek výroby elektřiny, nutnost vypouštět exhalace) a může aktualizovat jiná rizika (např. vyšší náklady na řešení skleníkového efektu nebo důsledky ztráty znalostí a možnosti výroby energetických celků). Jednotlivé případy budeme označovat R1, R2, atd.

Příklad analýzy rizik

- R1. Pokud se elektrárna neodstaví bude nutné vybudovat úložiště všeho radioaktivního odpadu a provozovat je dlouhou dobu. Vybudování úložiště bude stát desítky miliard korun, provoz úložiště miliony ročně, skladiště musí být v provozu tisíce let. Je ale dosti pravděpodobné, že se podaří odpad využít znovu jako surovinu a silně snížit množství odpadu a dobu jeho nebezpečnosti. Proto má alternativa R1 pravděpodobnost 0.5.
- Ztrátu ohodnotíme součtem nákladů na vybudování úložiště (50 mld. Kč) a na jeho provoz za 5000 let (5000 *10 mil Kč = 50 mld. Kč). Celkem nejvýše 100 mld. Kč. Ohodnocení přínosu odstavení nejvýše při pravděpodobnosti $p=1/2$ -50 mld. Kč. Tento odhad neuvažuje fakt, že se úložiště musí tak jako tak vybudovat pro již vzniklý odpad. A také to, že existuje možnost využití odpadu a jeho přepracování na odpad s kratším poločasem. Odhad ztráty je tedy spíše nadhodnocen.

Příklad analýzy rizik

- R2. Většina odpadu se zlikviduje v urychlovačích nebo se použije jako palivo. Zbylý odpad pak bude nutné skladovat kratší dobu (bude mít kratší poločas rozpadu). Lze odhadnout, že náklady na úložiště se zkrátí desetkrát a přibude cca jedna miliarda výnosu (to je velmi nízký odhad). Tyto výnosy při nedokončení elektrárny odpadnou. Takže celkový přínos zastavení elektrárny bude s pravděpodobností 0.5 (1-0.5, neboť R1 nastane jen nenastane-li R2) -6 mld Kč . Takže přínos odstavení elektrárny bude asi -3 mld. Kč.

Příklad analýzy rizik

- R3. V případě havárie lze škody počítat v bilionech Kč. Vzhledem k tomu, že se tisíce lehkovodních reaktorů provozují mnoho let a technologie se neustále zlepšuje, lze pravděpodobnost havárie ohodnotit číslem menší než 0.0001. Takže přínos odstranění rizika R3 je v řádu miliard. Hodnota tohoto rizika je 5-10 mld. Kč. Nepříjemná je výška ztráty spojené s uskutečněním rizika. To může být důvodem odmítnutí rizika. Připomeňme ale, že běžně postupujeme velmi vysoké riziko ztráty života, když přecházíme ulici nebo sedáme do automobilu a neděláme optření pro případ pádu asteroidu. Možná i odhad ztráty v bilionech je příliš vysoký
- Bylo by fér prosazovat nové spolehlivé a výkoné technologie výroby elektřiny (tedy spíše jadernou fuzy než větrníky) a ne remcat

Příklad analýzy rizik

- R4 Nedání příležitosti teroristům. Poněvadž jsou útoků jednotky a možných cílů jsou statisíce (nejen atomové elektrárny) a ztráta R4 je tedy srovnatelná se ztrátou R3 ale má nižší pravděpodobnost, je očekávaná ztráta R4 podstatně nižší, než v případě R3. V případě války hrozí pravděpodobně jiná podstatně větší rizika (masové útoky zbraněmi hromadného ničení), než útok na elektrárnu. Takže existence elektrárny situaci a hrozby pravděpodobně významně nezmění. Proto toto riziko hodnotíme na cca 2 mld Kč.