Bezpečnostní politika a řízení rizik v organizaci

Security Policy and Risk Management in Organizations

Bc. Martina Stavjaňová

Diplomová práce
2012

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2011/2012

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Martina STAVJAŇOVÁ**
Osobní číslo:	**A10918**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Bezpečnostní politika a řízení rizik v organizaci**

Zásady pro vypracování:

1. **Strategie bezpečnostní úpolitiky a řízení rizik.**
2. **Definice organizačního a odpovědnostního rámce.**
3. **Monitorování, analýza a identifikace rizik.**
4. **Dokumentace výsledků jednotlivých rizik.**
5. **Bezpečnostní incident a návrh na jeho řešení.**
6. **Vyhodnocení rizik a návrhy na opatření k jejich eliminaci.**

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **MLÝNEK, Jaroslav, Zabezpečení obchodních informací. BizBooks, 2007, ISBN 978-80-251-1511-4.**
2. **SMOLÍK, Josef a Tomáš ŠMÍD, Vybrané bezpečnostní hrozby a rizika 21. století, Mezinárodní politologický ústav Masarykovy univerzity, 2010, ISBN 978-80-210-5288-8.**
3. **LIDINSKÝ, V.; I. ŠVARCOVÁ; P. BUDIŠ; Z. LOEBL a B. PROCHÁZKOVÁ, eGovernment bezpečně, Praha: Grada, 2008, ISBN 978-80-247-2462-1.**
4. **SMEJKAL, Vladimír a Karel RAIS, Řízení rizik ve firmách a jiných organizacích, Expert, 2009, ISBN 978-80-247-3051-6.**
5. **MERNA, Tony a Faisal F. AL-THANI, Risk management: řízení rizika ve firmě, Praha: Computer Press, 2007, ISBN 978-80-251-1547-3.**
6. **KRULIŠ, Jiří, Jak vítězit nad riziky: aktivní management rizik. Nástroj úspěšných firem, Praha: Linde, 2011, ISBN 978-80-7201-835-2.**
7. **ČERMÁK, Miroslav, Řízení informačních rizik v praxi, Brno: Tribun EU, 2009, ISBN 978-80-7399-731-1**
8. **VARCHOLOVÁ, Tatiana a Lenka DUBOVICKÁ, Nový manažment rizika, Bratislava: Iura Edition, 2008, ISBN 978-80-8078-191-0**

Vedoucí diplomové práce: **JUDr. Josef Čejka**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **24. února 2012**

Termín odevzdání diplomové práce: **15. května 2012**

Ve Zlíně dne 24. února 2012

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Ve své diplomové práci se budu zabývat bezpečnostní politikou a řízením rizik v praxi. Cílem mé práce má být návrh strategie bezpečnostní politiky a řízení rizik, definování organizačního a odpovědnostního rámce, identifikací, analýzou, vyhodnocením, zvládáním, monitorováním, dokumentací výsledků, vyhodnocením rizik a návrhy opatření k jejich zvládání.

Klíčová slova:

Bezpečnostní riziko, bezpečnost informací, bezpečnostní událost, bezpečnostní incident, důvěrnost, dostupnost, informační a komunikační technologie, mimořádná událost, krizová událost, krizové řízení.

ABSTRACT

In my thesis I will deal with security policy and risk management in practice. The aim of my work to the draft strategy and security policy, risk management, defining the organizational framework and liability, identifying, analyzing, evaluating, managing, monitoring, documentation of results, risk assessments and proposals for measures to deal with it.

Keywords:

Security risk management, information security, security incident, security incident, confidentiality, availability, information and communications technology, emergency, crisis events, crisis management.

Na tomto místě bych ráda poděkovala JUDr. Josefu Čejkovi za vedení diplomové práce za cenné rady, připomínky a metodické vedení práce.

Děkuji také JUDr. Vladislavu Štefkovi za jeho podporu, trpělivost, rady, inspiraci a diskuze nejen při vypracování této diplomové práce.

Rovněž patří můj dík rodině za podporu při studiu a tvorbu potřebného zázemí.

Motto: Štěstí je, když budete chtít to, čeho jste dosáhli! Úspěch je, když dosáhnete toho, co jste chtěli!

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně 7.5.2012

.....
podpis diplomanta

OBSAH

ÚVOD

Každá organizace, bez ohledu na její zaměření, je při výkonu svých činností plně závislá na pracovnících a dostupných - hmotných i nehmotných statků. Nezbytnou součástí základních manažerských plánů jsou proto i úvahy o tom, jak pracovníky a aktiva organizace chránit. Často se objevuje požadavek na vytvoření systému řízení bezpečnosti organizace. Organizace v něm pomocí stanovených cílů, strategií a politik hierarchicky rozvrhuje oblast řešení bezpečnosti od úrovně celé společnosti až po jednotlivé chráněné oblasti - personální, informační a fyzickou. Aktiva organizace mají svoji hodnotu, která je v absolutní většině případů pro organizaci z hlediska jejího fungování kritická. V případě ztráty nebo závažného poškození některých aktiv tak může dojít i k ukončení činnosti organizace, a tím ke značným finančním ztrátám majitele nebo akcionářů, nemluvě o obchodních partnerech, zákaznících i zaměstnancích.

I. TEORETICKÁ ČÁST

1 BEZPEČNOSTNÍ POLITIKA

Úspěch jednotlivce nebo společnosti je věc velmi vrtkavá a nestálá. Často stačí jeden chybný krok a z prosperující organizace se stává černá můra akcionářů. Na pomyslné cestě se před námi objevují různé překážky a nástrahy a my jsme schopni je lépe či hůře zdolávat. Část překážek má společného jmenovatele - data a informace. Nejde jen o to je umět efektivně získávat a využívat, ale musíme je mít k dispozici tehdy, kdy potřebujeme, ve stavu, kdy se na ně můžeme spolehnout, a chráněné tak, aby se nedostaly k někomu, kdo je nemá vidět.

1.1 Teoretické kroky spojené s procesem řešením informační bezpečnosti

1.1.1 Mentální krok

Stále u nás najdeme firmy, pro které jsou jejich informace otázkou existence, ale přesto příslovečně nehnuly v bezpečnosti prstem a patří mezi ty, jež spoléhají na štěstí. Na druhou stranu jsou již firmy, které bezpečnost řeší nebo řešit začaly. Management těchto firem provedl v určitém stádiu důležitý "mentální krok".

Co obnáší "mentální krok"? Management se rozhodl informační bezpečností skutečně zabývat, což obnáší všechny, nebo alespoň některé následující rysy:

- vyčlenění interních lidských zdrojů (zřízení útvaru bezpečnosti, jmenování bezpečnostního managera, alokace pracovníků jiných útvarů),
- vyhrazení finančních prostředků,
- ochota spolupracovat na řešení bezpečnosti s externími dodavateli,
- připravenost vzít na sebe zodpovědnost za bezpečnost na nejvyšší úrovni,
- uvědomění si potřeby spustit systematický proces řešení,
- smíření se s faktem, že řešení bezpečnosti znamená věnovat se této oblasti natrvalo.

Důvodů, proč se management pohnul, může být přitom celá řada - prožité bezpečnostní incidenty, závěry auditu, rozhodnutí majitelů, pozitivní osvětové působení vnitřních sil, snaha získat konkurenční výhodu, srovnání obdobných firem v oboru atd. Podstatné je, že toto rozhodnutí bývá jen výjimečně podloženo tvrdými fakty typu návratnosti investic

(ROI[1]). Proto bývá toto rozhodnutí těžké a "mentální krok" s sebou přináší chápání investic do bezpečnosti analogicky jako nákladů spojených s pojištěním.

1.1.2 Šest kroků správným směrem

Podporu nejvyššího managementu lze považovat za krok nultý. Jaké jsou kroky další? Níže je uvedeno 6 navazujících kroků, které popisují proces řešení bezpečnostní politiky. Lze je bez obav považovat za univerzální vyjádření přístupu k řešení bezpečnosti.

1.1.2.1 Strategie bezpečnosti

tomuto kroku je potřeba udělat dva hlavní krůčky:

- definovat hlavní cíle v oblasti bezpečnosti (co a jak chránit)
- navrhnout a schválit parametry dalších kroků, ideálně ve formě projektu.

První krok vlastně představuje zhmotnění "mentálního kroku". Management stanovuje priority řešení a ty se musí promítnout do cílů a parametrů. Typickými výstupy této části bývá definiční projektová dokumentace a ideálně také Celková bezpečnostní politika - stručný dokument deklarující podporu managementu v oblasti bezpečnosti.

1.1.2.2 Analýza rizik

Riziko je "sexy" pojem a analýza rizik bývá často démonizována. Řada manažerů od týmů provádějících analýzu rizik (např. informací, informačních systémů) očekává zázraky a nečekané odpovědi a je pak zklamána, když dostanou odpovědi, které "… dávno a dobře znají".

Analýza rizik musí poskytnout odpovědi na tři základní otázky:

- Co se stane, když nebude zajištěna bezpečnost (fyzická, IT, krizové řízení,…)?
- Jak může být porušena bezpečnost?
- S jakou pravděpodobností se to stane?

[1] Porovnává čistý účetní zisk vůči velikosti investice, respektive objemu celkových aktiv nebo pasiv (bilanční suma). V českém názvosloví se setkáme častěji s názvem **výnosnost aktiv**, kdežto v prostředí ovlivněném účetními zásadami GAAP (všeobecně uznávané účetní principy) se setkáme častěji s pojmenováním **výnosnost investice**.

Existuje řada specializovaných metodologií na provádění analýzy rizik. Standardním výstupem analýzy rizik je zpráva se sumarizací a prioritizací rizik plus návrh doporučených opatření na jejich eliminaci nebo alespoň snížení.

Bezpečnost je především o prioritách - jde o to netrávit čas chráněním něčeho, co nemá pro společnost cenu. Hlavním cílem analýzy rizik musí být tyto priority co nejdříve a nejpřesněji určit.

1.1.2.3 Bezpečnostní politika

Analýza rizik provedená v předchozím kroku vede k detailnímu poznání organizace, jejích problémů a potřeb. To umožňuje vytvořit klíčový bezpečnostní dokument - bezpečnostní politiku - a zohlednit v něm specifika dané organizace. Jedná se o dokument, který je po přijetí managementem závazný pro celou společnost a který definuje východiska pro všechny další aktivity společnosti v oblasti bezpečnosti. Hlavním cílem bezpečnostní politiky je:

- definovat hlavní cíle,
- stanovit způsob, jak bezpečnost řešit,
- určit pravomoci a zodpovědnosti.

Pokud má organizace vytvořenou a přijatou celkovou bezpečnostní politiku, potom se v tomto kroku jedná o její podrobné rozpracování spolu s politikami pro další oblasti.

1.1.2.4 Bezpečnostní směrnice a standardy

Bezpečnostní politika definuje hlavní pravidla a zásady bezpečnosti. Ty je potřeba ještě dále konkretizovat do podoby detailních pravidel a postupů - bezpečnostních směrnic a standardů. Směrnice a standardy jsou součástí interní legislativy a jako takové se stávají závaznými pro organizaci. Zkušenost ukazuje, že ustanovení politiky by se neměla významně měnit alespoň 2 roky.

1.1.2.5 Implementace bezpečnosti

Zásady a pravidla politiky, resp. standardů a směrnic, se nenaplní automaticky jejich vytvořením a přijetím. Je potřeba nastartovat aktivity (projekty), které bezpečnostní zásady uvedou do života. Z tohoto pohledu se nejedná o uzavřený krok, ale spíše moment, kdy jsou zahajovány jednotlivé bezpečnostní projekty, koordinované ustaveným bezpečnostním managementem.

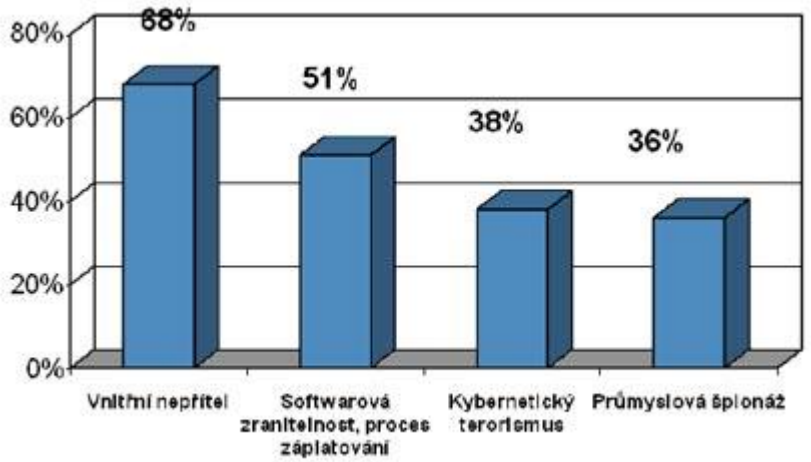
Příklady bezpečnostních projektů mohou zahrnovat:

- bezpečnostní vzdělávání,
- havarijní plánování,
- zabezpečení připojení na internet,
- implementace infrastruktury veřejných klíčů.

1.1.2.6 Monitorování a kontrola

Pokud je ustaven bezpečnostní management a jsou schváleny klíčové bezpečnostní dokumenty, je nutné zajistit dodržování definovaných pravidel a zásad a také zpětnou vazbu, která zajistí, že se významné změny promítnou do příslušné dokumentace a do procesu řízení bezpečnosti.

Reakce na nově se objevující rizika, změny priorit organizace a změny okolního prostředí mohou vyvolat potřebu vrátit se k některému z předchozích kroků řešení bezpečnosti a provést například doplňkovou analýzu rizik, či doplnění chybějících bezpečnostních standardů a směrnic. Neřešit tuto část znamená, že náklady byly vynaloženy jednorázově a že po čase budeme začínat s bezpečností opět prakticky z nuly.



[2]

Obrázek 1 Bezpečnostní rizika

[2] Zdroj: http://www.sntcz.cz/news/pressroom/pressreleases/2009_06_04_DataRobbery.php

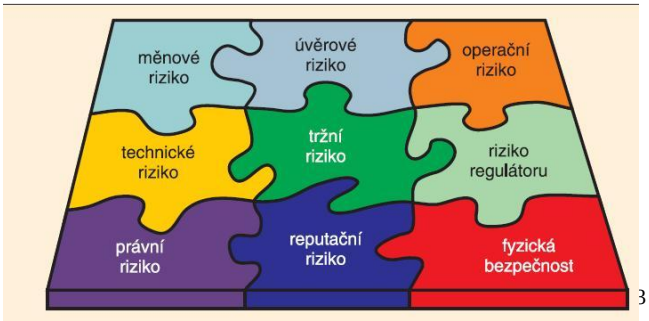
2 ŘÍZENÍ RIZIK

2.1 Komplexní řízení firemních rizik

Autoři různých publikací o řízení rizik vždy správně zdůrazňují, že účinné a efektivní řízení rizik ve firmě nemůže být založeno na řešení izolovaných rizik při náhodných příležitostech! Správným řešením je integrované řízení všech významných rizik ve firmě. Znamená to navrhnout a zavést řízení rizik ve všech důležitých firemních procesech.

Týká se to zejména těchto rizik:

- obchodních (nákup, prodej)
- finančních
- subdodavatelských
- projektových
- výrobních
- bezpečnostních
- informačních
- technických
- personálních
- politických
- vis major (přírodní a jiné katastrofy)



[3]

Obrázek 2 Některé typy rizik a jejich vzájemné vazby

Řada postupů může, ale i nemusí být pokryta explicitními pokyny pro řízení rizik. Záleží to na kvalitě a úrovni znalostí vedoucích pracovníků, zejména vrcholového managementu.

[3] Zdroj: http://www.automatizace.cz/article.php?a=2530

Řada rizik však musí být analyzována a řízena s ohledem na různé legislativní předpisy:

- Řízení rizik podle zákona č. 320/2001 Sb. o finanční kontrole ve veřejné správě.
- Řízení rizik z hlediska bezpečnosti práce podle OHSAS 18001:1999[4] (viz zákon č. 309/2006 Sb.).
- Posouzení rizika podle ČSN EN 1050 z hlediska nebezpečí, která se mohou vyskytovat při používání strojního zařízení, v návaznosti na směrnici Evropského parlamentu a Rady EU 2006/42/ES ze dne 17. května 2006.
- Ve speciálních případech, např. jaderná energetika nebo banky, v rámci pravidel BASEL[5].

Při nesprávném řízení těchto rizik, nebo dokonce při absenci řízení těchto rizik se firma vystavuje možnosti různých sankcí. Přistoupí-li firma ke komplexnímu systému integrovaného řízení rizik, pak se může zvýšit kvalita řízení rizik pro všechny jejich druhy. Například řízení rizik v rámci projektů (viz dále) často naráží na překážku, že firma nemá stanovenu hodnotu akceptovatelného rizika, takže není jasné, jaká výše rizik v projektu je pro firmu přijatelná, a nejsou stanoveny zásady pro vytváření firemních fondů na pokrytí akceptovatelných rizik projektu.

Řízení rizik ve firmách (tzv. Enterprise Risk Management – ERM[6] nebo někdy též Corpotare Risk Management) se stává nedílnou součástí všech firemních procesů úspěšných podniků.

2.1.1 Doporučené metody pro analýzu rizik

Velmi často (viz různé normy a předpisy) bývá přesně stanoveno, jaké druhy nebezpečí je nutno zvažovat a jak při analýze postupovat s využitím různých metod. Pro řadu případů byly v rámci rizikového inženýrství navrženy a využívány různé metody:

- HACCP – analýza rizik chemických a potravinářských výrob

---

[4] OHSAS 18001:2007 je mezinárodně uznávaná norma pro systémy managementu bezpečnosti a ochrany při práci.

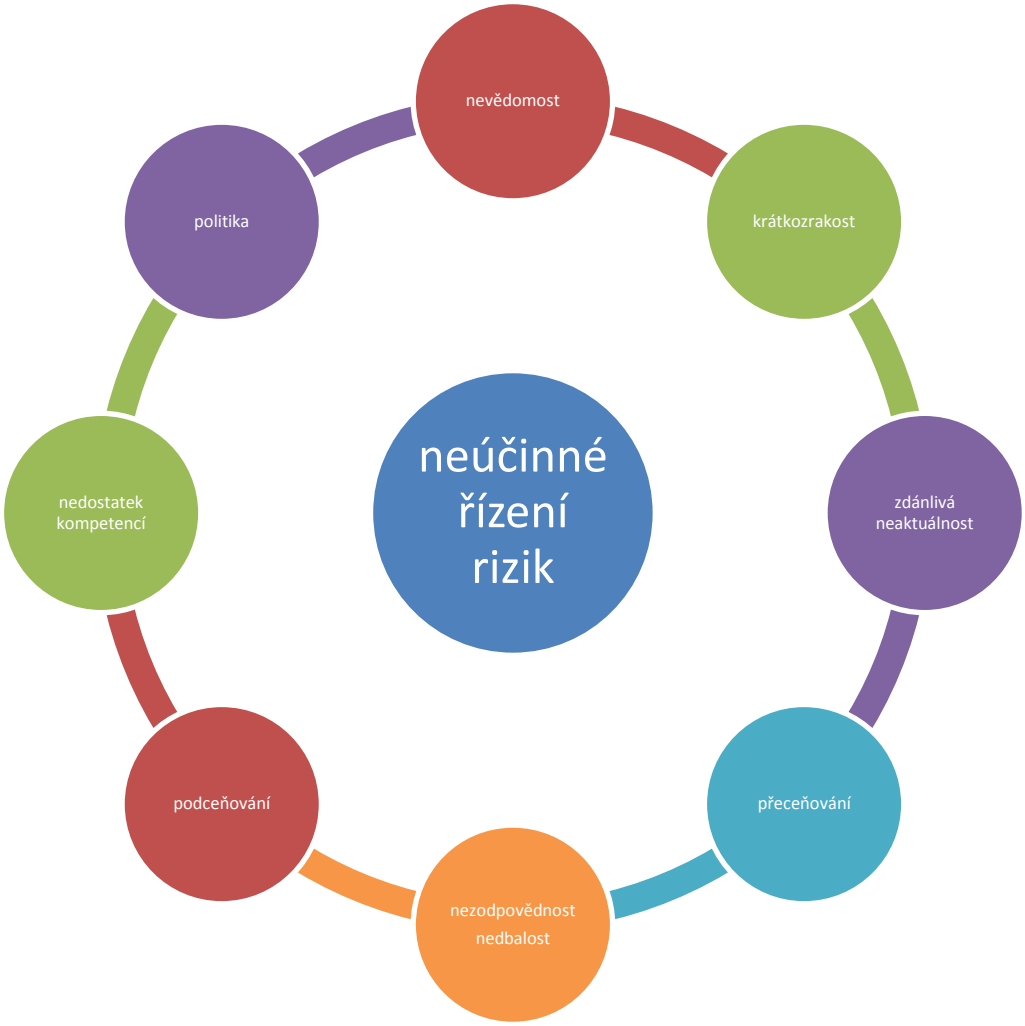
[5] Cílem je podpora bezpečnosti a stability finančního sektoru, zlepšení konkurenceschopnosti, kapitálové požadavky odpovídající rizikům, zohlednění všech rizik, uznání interních bankovních metod hodnocení rizika, aplikace na banky po celém světě, mezinárodně jednotný systém, posílení bankovního dohledu a trhu.

[6] Systémy, s jejichž pomocí lze zabezpečit důvěryhodnost informací a kontrolovat jejich koloběh při komunikaci s dalšími stranami – ať už jsou to kolegové z vedlejšího oddělení, nebo externí dodavatelé a partneři.

- HAZOP - analýza rizik technologických provozů
- FMEA – analýza rizik možných vad při konstrukčním návrhu
- CRAMM, IRIS – analýza rizik bezpečnosti automatizovaných informačních systémů
- RIPRAN Branislava Lacka nebo bodovaná metoda s mapou rizik – analýza rizik projektů
- UNRA – univerzální matice pro analýzu rizik budov, tunelů, silnic a jiných fyzických objektů s využitím expertních odhadů Milíka Tichého
- FRAP – proces analýzy rizik s využitím facilitátora
- MQD – proces hodnocení rizik bezpečnosti výrobních strojů
- JBM – hodnocení rizik z hlediska bezpečnosti práce podle Tomáše Neugebauera

Kromě těchto sofistikovaných metod pro analýzu rizik se využívá celá řada dílčích specializovaných technik, jakými jsou např. stromy rizik, příčinkové diagramy, mapy rizik nebo některých obecných technik, např. asociativní mapy, různé techniky expertních odhadů (DELPHI[7]), modelování a simulace (např. program PMF[8] firmy TIMING), technika brainstormingu[9] nebo naopak komplexních metod pro analýzu a řízení firemních rizik (např. metoda IPR[10] od Jiřího Kruliše).

[7] **Delphi metoda** je systematická interaktivní metoda předpovědí, založená na nezávislých vstupech vybraných expertů.
[8] **Project Management Forecast** – program určený pro modelaci a simulování rizik
[9] **Brainstorming** je metoda generování ideí široce používaná týmy, které se zabývají identifikací problémů, alternativním řešením problémů nebo hledáním příležitostí ke zlepšení.
[10] **Identifikace procesů a rizik** - univerzální nástroj pro odhalování rizik a jejich příčin v podnikové praxi



[11]

Obrázek 3 Neúčinné řízení rizik

[11] Zdroj: vlastní

II. PRAKTICKÁ ČÁST

3 STRATEGIE BEZPEČNOSTNÍ POLITIKY

3.1 Základní cíle řízení bezpečnosti

- ochrana života a zdraví zaměstnanců, klientů a dalších osob;
- naplňování požadavků relevantních zákonů a dalších předpisů;
- ochrana informací manipulovaných a ukládaných v organizaci;
- naplňování požadavků vyplývajících ze smluvních vztahů;
- podpora plnění obchodních cílů organizace;
- ochrana svěřených prostředků;
- ochrana majetku organizace;
- ochrana dobrého jména organizace.

Uvedené cíle jsem seřadila podle priorit od nejvyšší po nejnižší. Může se stát, že některé z cílů si v dané situaci můžou navzájem odporovat. V takovém případě se upřednostní dosažení cíle s vyšší prioritou.

Základní cíle řízení bezpečnosti podporují strategické cíle organizace. Důraz jsem proto položila na zajištění ochrany ochrana života a zdraví osob a ochrany informací o klientech organizace.

3.2 Základní principy řízení bezpečnosti

Pro efektivní a hospodárné řízení bezpečnosti musí být uplatňovány následující bezpečnostní principy:

- všichni zaměstnanci organizace jsou odpovědni za zajišťování bezpečnosti aktiv organizace;
- přijímaná bezpečnostní opatření musí být přiměřená riziku, tedy pravděpodobnosti vzniku škody a její velikosti hrozící aktivům organizace;
- činnosti související s řízením bezpečnosti musí být centrálně řízeny a koordinovány;
- pro řízení bezpečnosti musí být vytvořen systém řízení bezpečnostní dokumentace a záznamů na podporu prováděných činností;
- pro provoz a zlepšování systému řízení bezpečnosti musí být zajištěny dostatečné finanční, materiálové a personální zdroje;

- musí být zajištěna dostupnost prostor, majetku a informací organizace, které organizační útvary potřebují k plnění svých povinností, s minimálními narušeními;
- výkon činností související se systémem řízení bezpečnosti musí být pravidelně kontrolován a auditován;
- celý systém řízení bezpečnosti musí být periodicky vyhodnocován a musí být přijímána opatření k jeho zlepšování s důrazem na reakci na nové hrozby, zranitelnosti a aktiva organizace.

3.3 Zásady řízení bezpečnosti

Pro plnění cílů v oblasti bezpečnostní politiky a naplnění bezpečnostních principů, jsem stanovila zásady, které jsou členěny podle jednotlivých oblastí bezpečnostní politiky.

3.3.1 Organizace a řízení bezpečnosti

Základním cílem organizace a řízení bezpečnosti je stanovit rámec pro řízení, prosazování a kontrolu celého systému řízení bezpečnosti.

Opatření organizace a řízení bezpečnosti zejména zahrnují:

- přidělení kompetencí a odpovědností za řízení bezpečnosti;
- stanovení koordinačního rámce;
- definování schvalovacího procesu prostředků pro zpracování informací;
- zajištění ochrany informací ve smlouvách s externími subjekty a zajištění spolupráce s externími subjekty v oblasti ochrany aktiv organizace;
- řízení bezpečnostních rizik s externími subjekty včetně identifikace rizik spojených s jejich přístupem, zajištění bezpečného přístupu klientů a externích subjektů k informacím a ostatním aktivům organizace a zavázání těchto stran k dodržování požadavků organizace na zabezpečení informací a ostatních aktiv organizace.

3.3.2 Řízení aktiv

Cílem řízení aktiv je nastavit a udržovat přiměřenou ochranu aktiv organizace s důrazem na jejich klasifikaci. Cílem klasifikace aktiv je zajištění přiměřenosti ochrany aktiv organizace. Aktiva musí být klasifikovány na základě jejich potřebnosti a důležitosti pro organizaci.

Veškerá aktiva zařazená do systému řízení bezpečnosti musí být ohodnocena a musí být určen jejich vlastník. Za identifikaci a ohodnocení aktiv odpovídá vlastník aktiv. S aktivy

organizace musí být nakládáno způsobem zohledňujícím možná rizika, která s těmito aktivy souvisejí.

Veškerá aktiva, zejména pak informace, se kterými se manipuluje, a které se ukládají v organizaci, musí být klasifikovány a musí být s nimi zacházeno v závislosti na přiděleném klasifikačním stupni. Za obecné stanovení klasifikačního stupně k aktivům odpovídá vlastník aktiva. Za přidělení konkrétního stupně klasifikace k informaci (v elektronické i listinné formě) odpovídá původce (autor, zhotovitel, příjemce[12]) informace.

Pro účely klasifikace informačních aktiv organizace jsem stanovila následující klasifikační schéma:

3.3.2.1 Veřejné údaje

- informace, které mohou být zveřejněny a nevyžadují žádný zvláštní stupeň ochrany ve vztahu k zachování důvěrnosti, dostupnosti a integrity. Tyto informace mohou být volně šířeny i mimo organizaci

3.3.2.2 Interní údaje

- informace související s běžným provozem organizace a jednotlivých organizačních celků (např. vnitřní právní akty, interní komunikace, inventurní záznamy, atd.), které nejsou určeny ke zveřejnění.

3.3.2.3 Chráněné údaje

- údaje a informace, jejichž ochrana vyplývá ze zákona (např. osobní a/nebo citlivé údaje ve smyslu zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů), nebo údaje a informace vyžadující zvýšenou úroveň ochrany na základě obchodních nebo vnitřních požadavků z hlediska dostupnosti, důvěrnosti nebo integrity

Klasifikace hmotných aktiv, které mají charakter nemovitého majetku (objekty a pracoviště) navrhuji upravit zvláštním předpisem[13].

---

[12] Při přijetí informace přicházející do organizace.
[13] Např. Klasifikaci pracovišť organizace a stanovení parametrů pro jejich zabezpečení.

3.3.3 Personální bezpečnost

Cílem personální bezpečnosti je snížit riziko lidské chyby, neetického nebo protiprávního jednání s dopadem na aktiva organizace.

Při prosazování personální bezpečnosti jsem důraz položila na prosazování následujících zásad:

- všechny pracovní pozice musí být zařazeny do rizikových stupňů dle vybraných rizikových kritérií,
- u nově přijímaných zaměstnanců musí být minimalizována rizika, která jsou spojena se zkreslenými, zatajenými, nepravdivými nebo neúplnými údaji, které uchazeč o zaměstnání v organizaci předložil,
- všichni nově přijímaní zaměstnanci musí absolvovat vstupní školení k problematice bezpečnosti a ochraně aktiv,
- všichni zaměstnanci organizace musí absolvovat pravidelně školení k problematice bezpečnosti a ochraně aktiv v minimální periodě 1x za dva roky,
- u vybraných pracovních pozic (v závislosti na rizikovém stupni) musí být zajištěno doplňkové vzdělávání v oblasti bezpečnosti[14],
- všichni vedoucí zaměstnanci organizace musí vyžadovat po svých podřízených a případně po externích smluvních subjektech, dodržování bezpečnostních zásad,
- v případě porušení bezpečnostní politiky organizace a navazující dokumentace bude vůči zaměstnancům vyvozována právní odpovědnost,
- při ukončení zaměstnaneckého poměru, případně smluvního vztahu musí být jasně stanoveny odpovědnosti za úpravu přístupových oprávnění resp. za bezpečné předání svěřených aktiv.

3.3.4 Fyzická bezpečnost

Cílem fyzické bezpečnosti je předcházet neautorizovanému přístupu, poškození a zásahům do objektů, pracovišť a informací organizace. Opatření fyzické bezpečnosti jsou dále využívána pro ochranu hotovosti a majetku před odcizením.

---

[14] např. oblast PO a BOZP, ICT atd.

Fyzická bezpečnost je prosazována zejména prostřednictvím:

3.3.4.1 Klasifikace pracovišť

při které musí být naplňovány zejména následující bezpečnostní zásady:

- Veškeré pracoviště (objekty, kanceláře, technologické prostory atd.), v nichž jsou uchovávány aktiva organizace nebo v nichž se s nimi zachází, musí být zabezpečeny pomocí příslušných fyzických bezpečnostních opatření. Důraz je položen na definování a zajištění ochrany zabezpečených oblastí.
- Zabezpečené oblasti jsou chráněny přiměřenými kontrolami vstupu tak, aby bylo zajištěno, že osoba, která vstupuje do zabezpečených oblastí organizace, má ke vstupu oprávnění.
- V případě změnových řízení[15], která se dotýkají pracovišť organizace, musí být zohledněna bezpečnostní rizika ohrožující aktiva v nich umístěná.

3.3.4.2 Zajištění bezpečnosti

zařízení zpracovávající informace organizace navrhuji prosazovat především prostřednictvím následujících bezpečnostních zásad:

- Zařízení zpracovávající informace organizace musí být umísťována tak, aby se minimalizovalo riziko působení vnějších vlivů a neautorizovaného přístupu.
- Zařízení zpracovávající informace organizace musí být fyzicky chráněna v závislosti na klasifikačním stupni informací jimi zpracovávaných. Zařízení musí být též chráněna před výpadkem elektrického proudu nebo jinými anomáliemi napájení.
- Oprava nebo likvidace zařízení, případně nosiče informací, na nichž byly zpracovávány klasifikované informace organizace, musí být prováděna takovým způsobem, aby zaměstnancem organizace, nebo zaměstnancem externího subjektu

[15] pořízení nového objektu (pořízením nového objektu je myšlena výstavba nového objektu), změna dislokace objektu (změnou dislokace objektu je myšleno přestěhování všech stávajících pracovišť daného objektu do objektu jiného již existujícího), zřízení nové bezpečnostní zóny a změna bezpečnostní zóny (změnou bezpečnostní zóny je myšlena změna charakteru užívání bezpečnostní zóny a změna stavebně-technických parametrů bezpečnostní zóny)

nebylo možné získat z tohoto zařízení informace, které na něm byly zpracovávány, a s nimiž tito zaměstnanci nejsou oprávněni se seznamovat.

3.3.5 Řízení komunikací a řízení provozu

Cílem řízení komunikací a řízení provozu je zajistit správný a bezpečný provoz prostředků pro zpracování informací.

Řízení komunikací a provozu navrhuji realizovat prostřednictvím opatření v následujících oblastech:

- provozní postupy a odpovědnosti;
- řízení dodávek služeb externích subjektů;
- plánování a přejímání IS;
- ochrana proti škodlivým programům a mobilním kódům;
- zálohování;
- správa bezpečnosti;
- bezpečnost při zacházení s médii;
- výměna informací;
- monitorování.

3.3.6 Řízení přístupů

Cílem řízení přístupů je zejména zajistit oprávněný přístup uživatelů, předcházet neoprávněnému uživatelskému přístupu k síťovým službám, operačním systémům a k informacím, uloženým v IS, a zajistit bezpečnost informačních aktiv při použití mobilní výpočetní techniky a zařízení pro práci na dálku.

Řízení přístupu uživatelů organizace k informacím a službám IS organizace musí být prováděno:

- na základě přidělených rolí a přístupových práv do jednotlivých IS;
- v souladu s klasifikací a řízením aktiv;
- v souladu s formálními postupy registrace uživatelů IS organizace a správy přístupu zaměřenými na přidělení, změnu a odebrání přístupu;
- v souladu s postupy správy systému přístupu jednotlivých IS;

Všichni uživatelé musí být seznámeni se svými povinnostmi a s pravidly a postupy užívání přístupu k IS organizace s důrazem na používání uživatelských hesel a jiných

autentizačních prostředků a ochranu neobsluhovaných aplikací, služeb a zařízení při přerušení nebo ukončení práce.

V rámci IS organizace musí být pro jednotlivé části stanoveny a prosazovány způsoby a postupy monitorování včetně stanovení rozsahu, ochrany a vyhodnocování auditních záznamů a časové synchronizace.

Použití mobilních zařízení pro práci s IS organizace na dálku a vzdálený přístup k vnitřním IS organizace musí být řízen.

3.3.7 Akvizice, vývoj a údržba informačních systémů

Cílem zavedení opatření v oblasti akvizice, vývoje a údržby IS je prosadit bezpečnost informačních aktiv do celého životního cyklu užívaných IS, tj. od fáze návrhu, vývoje, testování až po vlastní provoz, údržbu a likvidaci. Implementace součástí IS a návrh jejich změn musí být v organizaci spojen se stanovením vhodných bezpečnostních požadavků.

Akvizice, vývoj a údržba IS budou realizovány prostřednictvím opatření v následujících oblastech:

- bezpečnostní požadavky informačních systémů;
- správné zpracování v aplikacích;
- kryptografická opatření;
- bezpečnost systémových souborů;
- bezpečnost procesů vývoje a údržby;
- řízení technických zranitelností;

3.3.8 Řízení bezpečnostních incidentů

Cílem řízení bezpečnostních incidentů je zajistit, aby incidenty byly řízeny takovým způsobem, který zastaví působení bezpečnostního incidentu a umožní včasnou nápravu s využitím formalizovaného a obecně známého postupu.

Navrhuji, aby řízení bezpečnostních incidentů zahrnovalo:

- hlášení bezpečnostních incidentů,
- stanovení odpovědností a postupů pro zvládání bezpečnostních incidentů,
- informování odpovědných osob o vzniku a řešení bezpečnostních incidentů,
- provádění ponaučení z bezpečnostních incidentů,
- shromažďování důkazů.

Veškeré bezpečnostní incidenty v organizaci musí být centrálně řízeny a spravovány.

3.3.9 Řízení kontinuity činností organizace

Cílem řízení kontinuity činností organizace je zabránit přerušení činností organizace a chránit organizaci před následky závažných chyb, katastrof a nepředvídatelných událostí nebo tyto následky minimalizovat. Důraz je položen na ochranu kritických procesů organizace.

Navrhuji, aby systém zajištění kontinuity činností v organizaci zahrnoval:

- provedení analýzy dopadů k určení rizik pro strategické cíle organizace, včetně identifikace a určení priorit kritických procesů organizace,
- identifikace aktiv, která se účastní kritických procesů,
- vytvoření systému řízení kontinuity činností s důrazem na stanovení strategie, určení a obsazení rolí zajišťující chod tohoto systému,
- návrh postupů pro zachování kontinuity činností a jejich zdokumentování v plánech kontinuity činností,
- provádění testování a aktualizace plánů kontinuity činností.

3.3.10 Soulad s požadavky

Cílem souladu s požadavky je zejména vyvarovat se porušení norem trestního nebo občanského práva, zákonných nebo smluvních povinností.

Navrhuji, aby zajištění souladu s požadavky zahrnovalo:

- Definování a zdokumentování všech relevantních právních a smluvních požadavků, přičemž:
  - Zvláštní pozornost věnují vedoucí pracovníci organizace dodržování ustanovením zákona č.101/2000 Sb. o ochraně osobních údajů a ustanovením zákona o ochraně duševního vlastnictví (především zákon č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským – autorský zákon).
  - Zajištění souladu s legislativou na ochranu osobních údajů dle zákona č.101/2000 Sb. v rámci organizace.
- Provádění pravidelného interního auditu.

3.3.11 Kritéria hodnocení bezpečnostních rizik

Hodnocení úrovně bezpečnostního rizika je určováno na základě ohodnocení aktiva a stanovení úrovně četnosti hrozby a dopadu hrozby. Hodnocení rizik se provádí s využitím analýzy rizik.

Hodnocení úrovně bezpečnostního rizika bude prováděno na základě následujících kritérií:

- stanovení hodnoty jednotlivých aktiv organizace,
- určení požadavků relevantní legislativy a požadavků vyplývajících z uzavřených smluvních vztahů,
- určení možných dopadů identifikovaných hrozeb,
- určení četnosti identifikovaných hrozeb,

Popis způsobu hodnocení bezpečnostních rizik, způsobu výběru opatření a procesů hodnocení účinnosti vybraných navrhuji upravit samostatným předpisem.

3.3.12 Základní právní východiska

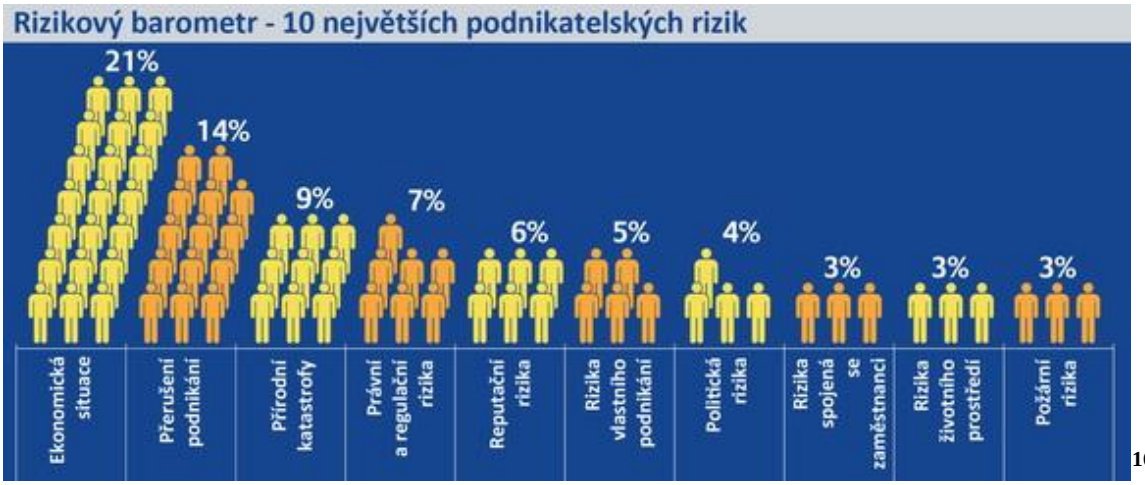
V systému řízení bezpečnosti musí být zohledněny všechny legislativní a regulatorní požadavky pro oblast bezpečnosti, zejména požadavky vyplývající z platného znění:

- zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů;
- zákona č.121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších předpisů;
- zákona č. 133/1985 Sb. o požární ochraně, ve znění pozdějších předpisů,
- zákona č. 309/2006 Sb. kterým se upravují další požadavky bezpečnosti a ochrany zdraví při práci v pracovněprávních vztazích a o zajištění bezpečnosti a ochrany zdraví při činnosti nebo poskytování služeb mimo pracovněprávní vztahy (zákon o zajištění dalších podmínek bezpečnosti a ochrany zdraví při práci), ve znění pozdějších předpisů;
- zákona č. 499/2004 Sb., o archivnictví a spisové službě a změně některých zákonů, ve znění pozdějších předpisů včetně vyhlášek,

3.3.13 Kompetenční a odpovědnostní rámec

Kompetence a odpovědnosti jsou v systému řízení bezpečnostních rizik přiřazeny jednak funkcím v organizační struktuře organizace a dále bezpečnostním rolím.

Nejvyšším orgánem řízení bezpečnosti v organizaci bude Komise pro řízení bezpečnosti organizace (dále je „Komise“). Komise bude poradním orgánem ředitele organizace ve věcech personální, administrativní, fyzické a ICT bezpečnosti a ve věcech řízení bezpečnostních rizik.



16

Obrázek 4 Rizika pro podnikatele

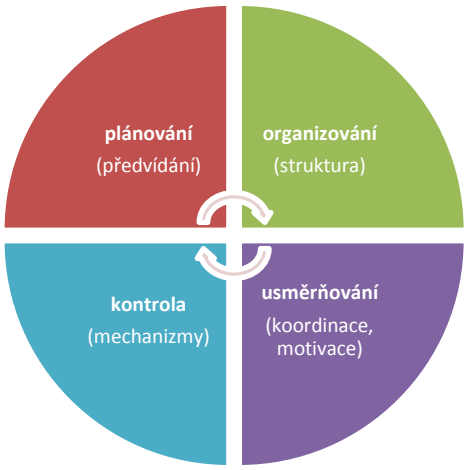
[16] Zdroj: http://www.finparada.cz/clanek.aspx?ID=430

4 SYSTÉM ŘÍZENÍ RIZIK

Řízení rizik je soustavná systematická činnost, která je organizována vedením organizace a ostatními vedoucími zaměstnanci organizace v rámci vnitřního systému řízení a kontroly tak, aby tento systém byl způsobilý včas identifikovat, analyzovat, vyhodnocovat a optimalizovat rizika[17]. Řízení rizik je subsystémem vnitřního systému řízení a kontroly. Tento subsystém je schematicky znázorněn v příloze č. 1. Výstupy systému řízení rizik jsou rovněž jedním ze zdrojů proaktivních podkladových informací pro rozhodování o strategii organizace a pro sestavování plánovacích dokumentů.

Systém řízení rizik bude zahrnovat následující prvky:

- stanovení kontextu řízení rizik,
- strategii řízení rizik,
- identifikaci rizik,
- analýzu rizik,
- vyhodnocení rizik,
- zvládání rizik,
- monitorování a přezkoumávání systému řízení rizik.



[18]

[17] Optimalizace je přesnější pojem, oproti někdy používanému pojmu minimalizace, neboť v sobě zahrnuje mj. nákladovou přiměřenost ve vztahu k očekávanému efektu a zohledňuje i skutečnost, že disponibilní zdroje na zvládání rizik je nutné alokovat dle rizikových priorit.

[18] Zdroj: vlastní

Obrázek 5 Systém řízení rizik

Jedná se o rizika, která jsou spojena především se ztrátou na hmotných aktivech (penězích, movitém a nemovitém majetku) i na nehmotných aktivech (informacích, právech, pověsti) v souvislosti s úmyslnými nebo neúmyslnými vnitřními i vnějšími hrozbami (přírodní katastrofy, požár, terorismus, krádeže, technologické havárie atd.).

Přehled bezpečnostních rizik je uveden v příloze č. 2.

5 STANOVENÍ KONTEXTU ŘÍZENÍ RIZIK

Nezbytnou podmínkou zavedení a účinného fungování systému řízení rizik je stanovení vnějšího a vnitřního kontextu. Stanovení vnějšího kontextu zahrnuje zejména zkoumání a vyhodnocování informací o vnějším prostředí, ve kterém se realizují záměry a cíle organizace, její systémy, procesy a činnosti.

Z tohoto hlediska jsou významné zejména:

- zainteresované strany, z nichž některé se vyznačují značnou mírou subjektivity ve svém vědomém vlivu na organizaci; pokud se týká míry jejich ovlivnitelnosti ze strany organizace, je u jejich jednotlivých skupin rozdílná,
- situace, stavy a trendy včetně potenciálních možností vývoje, které existují a vznikají objektivně (jedná se např. o legislativu ČR i EU, politickou situaci, ekonomické, technologické, demografické trendy vývoje, přírodní katastrofy, hromadná onemocnění a jiná hromadná poškození zdraví apod.).

Stanovení kontextu zahrnuje jak specifikaci zainteresovaných stran, jejich cílů, vzájemných vazeb, míry jejich vlivu na záměry a cíle organizace, tak specifikaci situací, stavů a trendů uvedených výše uvedených.

Zainteresované strany a externí situace, stavy a trendy jsou zdroji vnějších rizik. Stanovení vnějšího kontextu má za cíl vytvořit předpoklady pro chápání a zohlednění externích hrozeb a příležitostí při řízení rizik[19]. Má zajistit, že cíle a míra vlivu zainteresovaných stran, jakož i stavy, trendy a možnosti vývoje, budou vzaty v úvahu při hodnocení rizik, případně při vytváření kritérií pro toto hodnocení. Současně má stanovení vnějšího kontextu význam při formulaci variant zvládání vnějších rizik a výběr optimální varianty z nich tak, aby mj. respektovala oprávněné zájmy zainteresovaných stran.

Vnitřní kontext řízení rizik zahrnuje zejména identifikaci a zhodnocení strategických, procesních, organizačně kompetenčních a řídících vazeb organizace.

Zhodnocení kontextu je základem pro stanovení strategie řízení rizik i jedním z východisek pro další navazující fáze řízení rizik.

---

[19] Např. riziko plynoucí z pandemie chřipky by u značné části institucí spadalo do operačních rizik, s ohledem na nemocností zaměstnanců způsobené poruchy provozních činností.

6 STRATEGIE ŘÍZENÍ RIZIK

Strategie řízení rizik zahrnuje:

- principy řízení rizik,
- způsob stanovení mezních hodnot pro hodnocení rizik,
- členění rizik.

6.1 Princip řízení rizik

Při popisu principu řízení rizik vycházím z následujících principů:

- respektování charakteru organizace;
- vnímání cílů a procesů řízení rizik v propojení se strategickými cíli organizace,
- vnímání rizik a opatření k jejich optimalizaci v propojení s hodnotou[20],
- využívání systému řízení rizik rovněž k identifikaci příležitostí pro organizaci a rizik spojených s jejich realizací,
- zvažování dopadů opatření přijímaných k optimalizaci rizik na zainteresované strany a vztahy s nimi,
- propojení kontinuity řízení rizik a periodického zpracovávání Plánů zvládání rizik (nejméně jednou ročně, soustavné sledování jejich realizace a vyhodnocování jejich plnění; v případě výskytu mimořádných změn externích a interních podmínek a s tím souvisejících nových rizik se provádí úprava Plánů řízení rizik a souvisejících dokumentů),
- provádění periodických revizí systému řízení rizik (nejméně jednou ročně, před zpracováním Plánu zvládání rizik),
- existence průběžného monitoringu vnějšího a vnitřního prostředí, soustavné a účinné předvídání rizik a jejich prevence, včasné varování a reakce v případě identifikace nových významných rizik,
- vytváření historických datových řad informací nezbytných pro řízení rizik a informací o procesu a výsledcích řízení rizik,

[20] Uvedený princip zahrnuje rovněž řešení rizik podle priorit, hodnocení opatření k optimalizaci rizik z hlediska jejich nákladové přiměřenosti ve vztahu k očekávanému efektu.

- znalosti procesu řízení rizik všemi zainteresovanými vedoucími a ostatními zaměstnanci; existence povědomí všech zaměstnanců „napříč“ strukturou organizace o rizicích a jejich významu pro organizaci,
- vnímání rizik v jejich celkovém kontextu a vzájemné provázanosti jako předpoklad správného hodnocení rizik,
- systematičnosti postupu pro všechny fáze řízení rizik, od jejich identifikace až po monitoring přijatých opatření; vytváření, udržování a rozvíjení proaktivní metodologie (včetně používání analytických metod, prognózování, využívání scénářů apod.),
- vzájemné spolupráce všech organizačních složek, útvarů a vedoucích a ostatních zaměstnanců organizace; organizování týmové práce k využití znalostního potenciálu zaměstnanců organizace, chápání řízení rizik jako součásti řízení na všech úrovních, nikoli pouze jako záležitost vedení organizace, případně interního auditu,
- existence těsné vazby finanční a účetní informace, controlling, rozpočtování a plánování při analýze a hodnocení rizik i při navrhování opatření k řízení rizik,
- efektivní komunikaci v procesu řízení rizik; zařazování problematiky řízení rizik jako standardního bodu do programů porad,
- aktivní úloze interního auditu při zkoumání a vyhodnocování systému řízení rizik a formulaci doporučení ke zvyšování přiměřenosti a účinnosti systému řízení rizik.

Periodickou identifikaci, analýzu, hodnocení a optimalizaci rizik prostřednictvím Plánu zvládání rizik, navrhuji provádět v termínech stanovených ředitelem organizace. Uvedené postupy se komplexně vztahují na tento periodický proces. V případech identifikace rizik zjištěných v období po zpracování příslušného Plánu řízení rizik se tyto postupy použijí v přiměřeném rozsahu tak, aby bylo zaručeno přijetí adekvátních opatření k těmto rizikům.

6.2 Způsob stanovení mezních hodnot pro řízení rizik

Analýza rizik vyžaduje zavedení kritérií k hodnocení jejich dvou základních charakteristik, pravděpodobnosti výskytu rizika (P) a intenzity potenciálních následků rizika (D). Pro obě z výše uvedených charakteristik rizik jsem stanovila používání pětistupňové škály hodnocení.

Významnost (hodnota) rizika je dána součinem P x D. Základními mezními hodnotami pro řízení rizik jsou dvě hodnoty významnosti rizika - Risk kapacita a Risk apetit.

6.2.1 Risk kapacita

Risk kapacita je hodnota celkového dopadu všech identifikovaných rizik[21], při jejímž překročení je ohroženo fungování organizace. Tuto hodnota jsem odvodila od hodnoty dopadu rizik, který by způsobil prodlení s plněním splatných závazků vůči smluvním partnerům o 30 dní. S ohledem na zásadu opatrnosti, včetně nezbytnosti přihlížet k politickému a společenskému kontextu organizace, jsem hodnotu Risk kapacity stanovila na 2 mld. Kč.

Tato hodnota byla základem pro vytvoření mezní hodnoty (horní hranice 4. a dolní hranice 5. stupně) dále uvedeného základního pětistupňového hodnocení potenciálního dopadu rizik:

Risk kapacita			
stupeň	**hodnocení dopadu**	**mezní hodnota**	**střed intervalu**
1.	relativně malý	do 100 mil. Kč	50 mil. Kč
2.	citelný	nad 100 do 500 mil. Kč	300 mil. Kč
3.	významný	nad 0,5 do 1 mld. Kč	0,75 mld. Kč
4.	velmi významný	nad 1 do 2 mld. Kč	1,5 mld. Kč
5.	nepřípustný	nad 2 mld. Kč	/fiktivní/ 2 mld. Kč

[22]

6.2.2 Risk apetit

Risk apetit je hodnotou přijatelnosti celkového dopadu rizik pro organizace. Tuto hodnotu jsem odvodila od 3. stupně dopadu a je rovna hodnotě středu příslušného intervalu tj. 0,75 mld. Kč.

6.3 Členění rizik

Rizika v organizaci jsem rozčlenila do následujících skupin:

[21] Dopadem se rozumí jak přímý dopad tak nepřímý, vyvolaný.
[22] Zdroj: vlastní

6.3.1 Rizika finanční

6.3.1.1 Rizika tržní

- úrokové, vztahující se k:
  - úrokům inkasovaným organizací (jedná se zejména o úroky ze zůstatků finančních prostředků organizace na bankovních účtech),
  - k úrokům hrazených organizací (jedná se zejména o úroky hrazené z titulu úvěrů poskytnutých organizaci, případně o úroky z prodlení s plněním smluvních závazků organizace[23]),
- inflační, vztahující se zejména k cenám služeb poskytovaných smluvním partnerům, případně k nákupům nákladných technologií pro zajištění činnosti organizace,
- měnové, vztahující se zejména k mezistátním úhradám[24],
- cenných papírů (investiční), vztahující se zejména k případnému investování prostředků rezervního fondu do cenných papírů, případně riziko vztahující se k dceřiným společnostem.

6.3.1.2 Riziko kreditní

vztahující se k situaci, kdy dlužník organizace nedostojí svým závazkům[25].

6.3.1.3 Riziko solventnosti

vztahující se k situacím ohrožujícím schopnost organizace zabezpečit úhradu svých závazků v čase jejich splatnosti; riziko zahrnuje, kromě splatnostního, objemového a časového nesouladu aktiv a pasiv, rovněž náklady spojené se zajištěním likvidity[26] (obdobně jako rizika legislativní a právní).

---

[23] V případě, že se odvozují od výše repo sazby stanovené Českou národní bankou, zvýšené o sedm procentních bodů viz nařízení vlády ČR č. 142/1994 Sb., ve znění pozdějších předpisů.
[24] Riziko spojené se zavedením jednotné měny EU.
[25] Toto riziko zahrnuje rovněž riziko úpadku dlužníka.
[26] Riziko úpadku.

6.3.1.4 Riziko z budoucích závazků organizace

které jsou pravděpodobné nebo jisté, ale nejistá je jejich výše nebo okamžik, ke kterému vznikne povinnost úhrady.

6.3.1.5 Riziko poklesu tržeb

v důsledku makroekonomických změn.

6.3.1.6 Riziko navýšení nákladů provozních nákladů

v důsledku:

- technologického rozvoje,
- demografického vývoje.

6.3.1.7 Riziko strategického řízení

které je spojeno se správou a řízením organizace zajišťovanou orgány a vedením organizace, zejména se stanovením jejích strategických cílů a systémem jejich projekce do procesních cílů, zajištěním kontinuity její činnosti včetně konkurenceschopnosti vůči ostatním konkurentům, efektivním systémem jejího řízení a kontroly a kompetenčním rámcem.

6.3.1.8 Rizika legislativní a právní

jsou spojena s legislativní úpravou činnosti organizace a jí používanými právními prostředky; do této skupiny náleží rovněž riziko nesouladu činností organizace s právními předpisy a z toho plynoucích následků (obdobně jako riziko solventnosti).

6.3.1.9 Riziko reputační

je spojeno jak s jednáním zainteresovaných stran, tak s postupy organizace a jednáním a postoji jejích zaměstnanců, které jsou způsobilé poškodit pověst organizace.

6.3.1.10 Rizika operační[27]

jsou spojena zejména s:

---

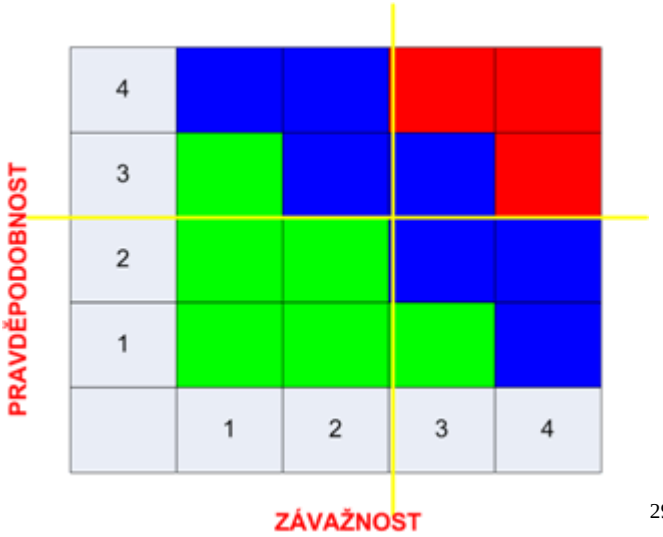
[27] S výjimkou bezpečnostních rizik.

- vnitřním protiprávním jednáním a obcházením právních a vnitřních předpisů zaměstnanci organizace,
- protiprávním jednáním třetích osob,
- jednáním v rozporu s pracovně právními předpisy, předpisy o ochraně zdraví a bezpečnosti při práci; tato rizika zahrnují rovněž diskriminační jednání vůči zaměstnancům organizace,
- hromadnými onemocněními apod.,
- nedostatky, selháním a poruchami systémů, procesů, technických prostředků nebo selháním lidského faktoru (jedná se např. o nedostatečnou funkcionalitu systémů, nedostatky v kontrolní činnosti[28] včetně neautorizovaných transakcí, nejasné kompetence, nedodržování stanovených postupů, chybné transakce, pozdní reakce na změny podmínek a problémy vyžadující řešení, chybná rozhodnutí, chybná data, opomenutí či jiné chyby zaměstnanců, dopady dalších externích faktorů apod.).

Výše uvedené rámcové příklady operačních rizik mohou dle konkrétní situace zahrnovat bezpečnostní rizika. Pro rozhodování v těchto konkrétních situacích jsem v příloze č. 2 vytvořila přehled bezpečnostních rizik.

Výše uvedené členění rizik vychází z obecných podmínek v organizaci s přiměřeným využitím standardů a právních předpisů.

[28] Mezi tato rizika patří rovněž auditorské riziko.



[29]

Obrázek 6 Matice rizik

[29] Zdroj: http://www.riscon.cz/cze/hodnoceni_rizik.html

7 ORGANIZAČNÍ A ODPOVĚDNOSTNÍ RÁMEC ŘÍZNÍ RIZIK

Základním východiskem organizačního a odpovědnostního rámce řízení rizik je zákon o finanční kontrole a Organizační řád organizace. Tento organizační a odpovědnostní rámec zahrnuje např.:

- ředitele organizace,
- Poradu vedení organizace,
- Komisi pro řízení bezpečnosti organizace,
- vedoucí zaměstnance organizace,
- vlastníky rizik,
- ředitele Úseku interního auditu a kontroly (risk managera Oddělení managementu a řízení rizik),
- správní radu organizace a dozorčí radu organizace.

7.1 Ředitel organizace

- schvaluje:
  - Strategii řízení rizik.
  - Katalog rizik a Plán zvládání rizik sestavený na základě ročního periodického vyhodnocení rizik.
  - Opatření ke snížení rizik extrémní významnosti a opatření k rizikům, která si vyhradí.
  - Periodické zprávy o řízení rizik.
- stanoví:
  - vlastníky rizik v případech, kdy rizika náleží do působnosti více jemu přímo podřízených vedoucích zaměstnanců a v případech, které si vyhradí,
  - termíny provedení periodické identifikace, analýzy, hodnocení a optimalizace rizik prostřednictvím Plánu zvládání rizik.

7.2 Porada vedení organizace

- projednává na základě rozhodnutí ředitele organizace:
  - Strategii řízení rizik.
  - Katalog rizik a Plán zvládání rizik sestavené na základě ročního periodického vyhodnocení rizik.
  - Periodické zprávy o řízení rizik.

- Další dokumenty týkající se řízení rizik.

za účelem jejich verifikace a formulace případných doporučení,

- sleduje realizaci opatření ke snížení rizik extrémní a vysoké významnosti.

Jednotliví členové Porady vedení organizace schvalují opatření ke snížení rizik vysoké významnosti spadajících do jejich působnosti.

7.3 Komise pro řízení bezpečnosti organizace

KŘB organizace je poradním orgánem ředitele organizace a napomáhá efektivnímu koordinování bezpečnostních aktivit včetně řízení rizik v celé organizace.

KŘB organizace projednává zejména:

- převoditelnost hodnocení bezpečnostních rizik a rizik do celkového hodnocení rizik organizace,
- členění konkrétních rizik na rizika bezpečnostní a rizika,
- závěrečné zprávy o analýze bezpečnostních rizik včetně variant zvládání rizik.

7.4 Vedoucí zaměstnanci organizace

- odpovídají za:
  - efektivní fungování systému řízení rizik v souladu se zákonem o finanční kontrole, Organizačním řádem organizace,
  - realizaci identifikace, analýzy, hodnocení a zvládaní rizik a příslušné výstupy (zpracování Evidenčních listů rizik, příslušných částí Katalogu rizik, Plánu zvládání rizik, zpráv o vyhodnocení rizik a jejich zvládání apod.),
- monitorují externí prostředí a prostředí organizace s cílem včas identifikovat a ošetřit nová rizika,
- vedou dokumentaci o rizikových událostech včetně těch, které neměly faktický dopad na cíle, procesy apod. organizace, s cílem získávat podklady pro prohlubování objektivity analýzy a vyhodnocování rizik,
- určují vlastníky jednotlivých rizik,
- poskytují potřebnou součinnost risk managerovi.

7.5 Vlastníci rizik

Vlastník rizika odpovídá za optimalizaci[30] rizika prostřednictvím přijímání, resp. navrhování opatření k jejich zvládání, monitorování rizika a přiměřenosti a účinnosti přijatých opatření, případně přijímání či navrhování doplňujících opatření.

Vlastníkem rizika je vedoucí zaměstnanec, do jehož působnosti riziko spadá, nebo jím určený zaměstnanec. Při určování vlastníka rizika je nezbytné zohlednit, zda je z titulu své funkce vybaven kompetencemi potřebnými k realizaci povinností vlastníka. V případě, že riziko náleží do působnosti více vedoucích zaměstnanců přímo podřízených řediteli organizace, určuje jeho vlastníka ředitel organizace na základě žádosti výše uvedených vedoucích zaměstnanců, obsahující jejich stanoviska a doporučení risk managera.

Vlastníci rizik poskytují potřebnou součinnost risk managerovi.

7.6 Ředitel úseku interního auditu a kontroly (risk manager Oddělení risk managementu a analýz)

- odpovídá za:
  - poskytování podpory, zejména formou doporučení, konzultací a koordinace činností, řediteli organizace a vedoucím zaměstnancům organizace při realizaci jednotlivých prvků systému řízení rizik,
  - sumarizaci výsledků procesu řízení rizik do Katalogu rizik, Plánu zvládání rizik a Mapy rizik, včetně výstupů řízení bezpečnostních rizik,
  - zpracování celkových výsledků řízení rizik do zpráv a dalších dokumentů pro poradu vedení organizace, správní radu organizace a dozorčí radu organizace.

  Uvedené úkoly plní rovněž prostřednictvím risk managera začleněného v Oddělení risk managementu a analýz Úseku interního audit a kontroly. K plnění těchto úkolů je, kromě ředitele Úseku interního auditu a kontroly, oprávněn i risk manager vyžadovat součinnost od příslušných vedoucích zaměstnanců organizace a vlastníků rizik.

[30] Optimalizace zahrnuje, kromě snížení rizik, rovněž podstoupení rizika na základě zhodnocení jeho významnosti, nákladové přiměřenosti možných opatření ke snížení rizika ve vztahu k očekávanému efektu těchto opatření i na základě disponibilních prostředků.

7.7 Správní a dozorčí rada organizace

Správní radě organizace a dozorčí radě organizace je pravidelně předkládán reporting řízení rizik, a to v termínech, které stanoví ředitel organizace.

7.7.1 Správní rada

je nejvyšším orgánem organizace a rozhoduje o zásadních otázkách týkajících se její činnosti jako celku. Členové správní rady jsou plně ztotožněni s posláním organizace.

7.7.1.1 Typické činnosti a pracovní náplň členů správní rady

- působení ve správní radě určuje hlavní cíle organizace
- spravuje celou organizaci
- rozhoduje s ohledem na efektivitu

7.7.2 Dozorčí rada

je samostatně definována u společností s ručením omezeným a akciových společností.

7.7.2.1 U společností s ručením omezeným

- dohlíží na činnost jednatelů,
- nahlíží do obchodních a účetních knih a jiných dokladů a kontroluje tam obsažené údaje,
- přezkoumává řádnou, mimořádnou a konsolidovanou, popřípadě i mezitímní účetní závěrku a návrh na rozdělení zisku nebo úhradu ztráty a předkládá své vyjádření valné hromadě,
- podává zprávy valné hromadě ve lhůtě stanovené společenskou smlouvou, jinak jednou ročně,
- svolá valnou hromadu, jestliže to vyžadují zájmy společnosti.

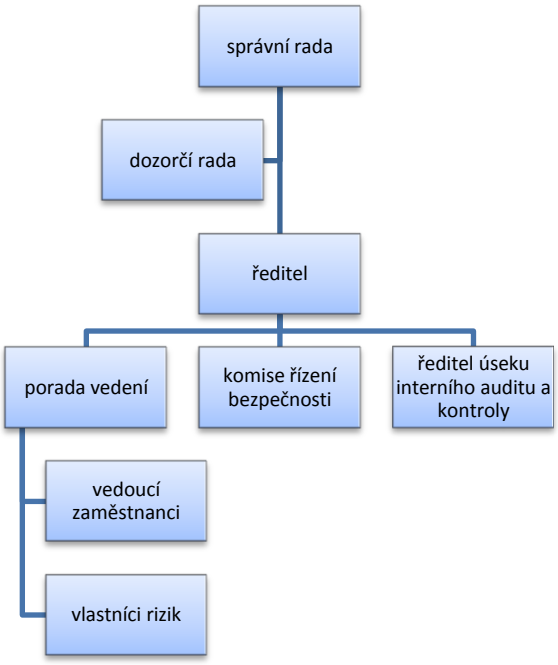
Členové dozorčí rady jsou oprávněni účastnit se valné hromady. Musí jim být uděleno slovo, kdykoli o to požádají.

7.7.2.2 U akciových společností:

- dohlíží na výkon působnosti představenstva a uskutečňování podnikatelské činnosti společnosti,

- přezkoumává řádnou, mimořádnou a konsolidovanou, popřípadě i mezitímní účetní závěrku a návrh na rozdělení zisku nebo úhradu ztráty a předkládá své vyjádření valné hromadě,
- svolává valnou hromadu, jestliže to vyžadují zájmy společnosti, a na valné hromadě navrhuje potřebná opatření.

Členové dozorčí rady jsou oprávněni nahlížet do všech dokladů a zápisů týkajících se činnosti společnosti a kontrolují, zda účetní zápisy jsou řádně vedeny v souladu se skutečností a zda podnikatelská činnost společnosti se uskutečňuje v souladu s právními předpisy, stanovami a pokyny valné hromady[31].



[32]

Obrázek 7 Organizační a odpovědnostní rámec organizace

[31] Zdroj: § 137 a 197 obchodního zákoníku.
[32] Zdroj: vlastní

8 IDENTIFIKACE RIZIK

Identifikace rizik spočívá v identifikaci zdrojů rizik, událostí, stavů a jednání, která by mohla zabránit, ztížit, zpozdit dosažení záměrů a cílů organizace, ohrozit její aktiva, případně ohrozit další subjekty. Cílem je identifikovat rizika, ať je jejich zdrojem prostředí organizace, či vnější prostředí. Identifikace rizik je systematická činnost prováděná jednak v rámci ročního periodického vyhodnocení rizik a tvorby Plánu zvládání rizik a dále kontinuálně, s cílem zachovat aktuálnost řízení rizik.

Identifikace rizik a rizikových faktorů navrhuji provádět pracovními týmy složenými z vedoucích zaměstnanců odpovídajících za řízení příslušných analyzovaných procesů, zaměstnanců tyto procesy zajišťující a případně dalších přizvaných zaměstnanců (zejména těch, kteří odpovídají za realizaci, řízení nebo koordinaci procesů předcházejících či navazujících). Tyto týmy stanoví ředitelé úseků a samostatných odborů organizace. Identifikace probíhá zpravidla formou řízené diskuze (brainstormingu) a vychází z dostupných údajů o procesech a jejich analýzy. Uvedený proces se realizuje postupně na různých úrovních řízení. Nejprve se provede na základě zhodnocení na úrovni odboru, při současném provedení integrace rizik identifikovaných jednotlivými odděleními. V další etapě se provede zhodnocení včetně integrace rizik na úrovni úseků organizace. Podporu tomuto procesu poskytuje risk manager.

Podstata tohoto postupu je obecně platná nejen pro identifikaci rizik, ale rovněž pro další navazující etapy řízení rizik.

Řádná identifikace rizik zahrnuje, resp. vyžaduje:

- existenci strategických cílů organizace,
- vymezení procesů a identifikaci vazeb mezi procesními a strategickými cíli,
- vlastní identifikaci rizik (zahrnující rovněž identifikaci rizikových faktorů),
- popis rizik.

8.1 Strategické cíle

Jedním ze základních cílů řízení rizik je identifikovat rizika ohrožující splnění záměrů a cílů organizace. Z tohoto důvodu je základním předpokladem identifikace rizik (a navazujících procesů řízení rizik) stanovení strategických cílů organizace. Základním dokumentem obsahující tyto cíle bude Strategie a priority organizace.

Na základě tohoto dokumentu a z něj plynoucích požadavků navrhuji formulovat rámec strategických cílů, který zahrnuje např. dosažení:

- optimální sítě odběratelů,
- optimálních smluvních vztahů s dodavateli,
- souladu s legislativou,
- schopnost konkurence na evropském trhu,
- transformace na klientsky orientovanou organizaci,
- účelnosti, hospodárnosti a efektivnosti činností zajišťovaných organizací,
- konsolidace, centralizace informačního systému a jeho podpory strategii organizace.

Složitost a provázanost jednotlivých procesů a cílů organizace v řetězci příčin a následků, často pravděpodobnostního charakteru, může mít za následek, že výše uvedený rámec cílů obsahuje riziko překrývání (stanovit efektivně působící skupinu cílů bez tohoto rizika je však fakticky nemožné).

Tyto skutečnosti mohou klást značné nároky na dále uvedenou identifikaci a hodnocení vazeb procesů na strategické cíle.

8.2 Vymezení procesů a identifikace vazeb mezi procesními a strategickými cíli

Identifikace rizik musí být systematická. V jejím rámci by měly být přezkoumány všechny procesy probíhající v organizaci, neboť nezjištění rizik by mohlo mít významné dopady na fungování organizace.

Z hlediska funkcí obecně existují tři základní skupiny procesů:

8.2.1 Řídící procesy

stanovují jak strategické cíle, tak cíle pro všechny procesy organizace, a které také všechny procesy organizace ovlivňují. Dopady rizik ohrožujících tyto procesy jsou v zásadě dvojího charakteru:

- nesprávné stanovení cílů,
- nesprávný průběh procesů (řídících, podpůrných i výkonných).

Vnitřní rizika těchto procesů a dopady vnějších rizik na ně působících je nezbytné promítnout do hodnocení dopadů na procesy, ke kterým se řízení vztahuje (do cílů těchto procesů).

8.2.2 Podpůrné procesy

vytvářejí podmínky pro realizaci stanovených cílů organizace. Vnitřní rizika těchto procesů a dopady vnějších rizik na ně působících, ohrožují kromě cílů pro ně stanovených i ostatní procesy (výkonné i řídicí) a je rovněž nezbytné je promítnout do jejich cílů (jedná se např. o řízení lidských zdrojů, informační systémy, správu majetku, řízení investiční činnosti apod.).

8.2.3 Výkonné procesy

realizují cíle organizace. Vnitřní rizika těchto procesů a dopady vnějších rizik na ně působících bezprostředně ovlivňují dosažení cílů organizace. Současně je při identifikaci rizik v rámci těchto procesů nutné zohledňovat dopady rizik řídících a podpůrných procesů. Při identifikaci a analýze rizik spočívajících v těchto procesech jsou často identifikovány dopady neidentifikovaných rizik předchozích skupin procesů.

Uvedené procesy je nezbytné analyzovat ve vztahu ke strategickým cílům. Nejprve jsou identifikovány vazby těchto procesů na strategické cíle. V další fázi pak jsou přiřazeny každému strategickému cíli všechny procesy, které jej ovlivňují (viz příloha č. 3), což je základním předpokladem pro vyhodnocení rizik ohrožujících realizaci strategických cílů.

8.3 Vlastník identifikace rizik

V rámci identifikace rizik jsou analyzovány veškeré procesy a aktiva organizace. Identifikace rizik zahrnuje následující činnosti:

- identifikaci potenciálních rizik,
- identifikaci rizikových faktorů,
- identifikaci řídících a kontrolních mechanizmů vztahujících se k identifikovaným rizikům.

Výše uvedené činnosti probíhají ve vzájemné interakci.

8.3.1 Identifikace potenciálních rizik

na základě stanovení kontextu řízení rizik a jeho další analýzy, znalostí systémů, procesů a činností, výsledků jejich monitorování, charakteru aktiv, informací o rizicích, která se vyskytla v minulosti, výsledků kontrol a dalších informací se identifikují potenciální rizika, tzn.:

- jaké události, jednání a stavy představují potenciální hrozby,
- jaké systémy, procesy, činnosti nebo aktiva organizace, případně jaké zainteresované strany mohou být ohroženy,
- jaké procesní a strategické cíle mohou být ohroženy,
- jaké jsou jejich možné příčiny,
- jaký je charakter možných následků.

Takto identifikovaná rizika se začlení do příslušné skupiny rizik, které jsem uvedla v bodě 6.3.

8.3.2 Identifikace rizikových faktorů

Současně se identifikují rizikové faktory tj. podmínky a další faktory umožňující či podporující vznik výše uvedených potenciálních rizik, resp. jejich negativní dopad. Rizikovými faktory souvisejícími s externím prostředím mohou být např. faktory:

8.3.2.1 Legislativní

včetně legislativy EU, např.:

- legislativní omezení rozhodovacího rámce při řízení[33],
- nejasnosti právních předpisů umožňující jejich různý výklad[34],
- časté změny, složitost právních předpisů, absence adekvátních prováděcích předpisů a nedostatek judikatury,
- nesoulad a případné rozporné působení různých právních předpisů,
- neadekvátně krátká doba mezi vydáním a účinností právního předpisu z hlediska jeho implementace do praxe,
- krátká doba pro připomínkové řízení k právním předpisům,

[33] Např. podřízenost režimu zákona č. 137/2006 Sb. o veřejných zakázkách.
[34] Vč. výkladu odlišného od výkladu externích kontrolních orgánů.

- obtížná orientace v předpisech EU (mj. neexistence systémů obdobných ASPI[35]) a rozsudcích Evropského soudního dvora,
- nesoulad se záměry a cíli organizace,
- sankce obsažené v právních předpisech.

8.3.2.2 Právní

- nízká vymahatelnost práva,
- nejednotná aplikace práva na jednotlivých stupních soudní moci,
- nepředvídatelnost rozhodnutí soudu,
- dlouhá doba soudního řízení.

8.3.2.3 Politické

- narušení kontinuity v důsledku změn koncepcí politiky organizace a návazně legislativy (viz. i legislativní faktory),
- lobbing,
- změny cílů a koncepcí územně samosprávných celků,
- změny makroekonomických ukazatelů v důsledku změn dalších politik, např. sociální (viz. i ekonomické rizikové faktory).

8.3.2.4 Ekonomické

- vývoj mezd,
- vývoj zaměstnanosti,
- míra inflace,
- měnové kurzy
- úrokové sazby,
- změny v odvětví[36],
- hospodářský vývoj[37],
- deregulace cen (viz. i legislativní faktory).

---

[35] Komplexní systém pro práci s právními informacemi.
[36] Např. pokles produkce v automobilovém průmyslu až po případný odchod zahraničních firem.
[37] Při hospodářském poklesu lze očekávat potenciální dopady na smluvní dodavatele a plnění jejich závazků.

8.3.2.5 Technologický rozvoj

- nové nákladné výrobní technologie,
- nové nákladné materiály,
- prosazování dražších materiálů na úkor levnějších se stejným efektem,
- nové technologie pro provozní činnosti (např. informační technologie).

8.3.2.6 Postoje, chování a jednání klientů

- ovlivňování klientů ze strany konkurence,
- neadekvátní postupy organizace při komunikaci s klienty a dodavateli (řešení dotazů, stížností apod.),
- kvalita poskytovaných služeb,
- neplnění povinností vůči organizaci ze strany klientů a dodavatelů.

8.3.2.7 Postoje, chování a vyjednávací síla

- smluvní politika,
- neadekvátní postupy organizace při uzavírání smluv a komunikaci s dodavateli,
- prodejní síť.

8.3.2.8 Vztahy s dodavateli

- postupy při výběru dodavatelů,
- obchodní podmínky dodavatelů,
- kvalita smluv s dodavateli,
- neadekvátní kontrola dodávek,
- vstup do likvidace, úpadek dodavatele.

8.3.2.9 Konkurence

- odlišné legislativní podmínky (viz. i legislativní faktory),
- odlišnosti procesů jednotlivých konkurentů

8.3.2.10 Mediální

- postupy při komunikaci se zainteresovanými stranami,
- kvalita podkladů pro komunikaci se zainteresovanými stranami.

8.3.2.11 Demografické

- demografický vývoj ČR (EU),
- vliv migrace[38].

Rizikovými faktory vztahujícími se k vnitřnímu prostředí organizace mohou být např. faktory spadající do oblasti:

- **Řídícího a kontrolního prostředí**, např.:
  - nejasný systém stanovování kompetencí,
  - absence politik (např. „obchodní“),
  - neexistence jednotných postupů[39],
  - tolerance k nedostatkům, nevyvozování důsledků z osobní odpovědnosti,
  - narušení kontinuity ve zpracování procesní analýzy činností.
- **Stanovování cílů**, např.:
  - narušení kontinuity řetězce vize-mise-strategie,
  - nekonkrétnost a neměřitelnost cílů,
  - nereálnost cílů,
  - neadekvátní kontrolní pokrytí stanovování cílů,
  - neadekvátní normativní úprava procesů.
- **Plánování**, např.:
  - nekoordinovanost,
  - nereálné plány,
  - absence plánů včetně plánů pro mimořádné (krizové) situace,
  - neadekvátní kontroly plnění plánů.
- **Organizování**, např.:
  - opožděné či neadekvátní reakce organizační struktury na změny podmínek,
  - neadekvátní koordinace činností mezi útvary.
- **Řídících a kontrolních procesů (činností a aktivit)**, např.:
  - absence kriterií hospodárnosti, účelnosti a efektivnosti,
  - normativně neupravené nebo nedostatečně upravené procesy; kvalita normativní úpravy procesů,

[38] Např.: nižší kupní síla v určitých regionech
[39] Např. v uplatňování sankcí.

  - kvalita personálního zajištění procesů,
  - složitost a kritická místa procesu,
  - významnost řízeného, kontrolovaného (auditovaného) procesu, objem finančních prostředků podléhajících tomuto procesu,
  - kvalita informací pro realizaci procesu a o výsledcích procesu.
- **Výkonných (podpůrných) procesů (činností a aktivit)**, např.:
  - neadekvátní kontrolní pokrytí procesů,
  - normativně neupravené nebo nedostatečně upravené procesy; kvalita normativní úpravy procesů,
  - kvalita personálního zajištění procesů,
  - složitost a kritická místa procesů,
  - významnost procesů, objem finančních prostředků podléhajících procesům,
  - kvalita informací pro realizaci procesů a o výsledcích procesů.
- **Informací a komunikace**, např.:
  - vliv decentralizace IS,
  - čas nezbytný na požadované změny IS,
  - nepřesné interpretace informací,
  - neaktuálnost, nesprávnost apod. informací,
  - hodnota informací pro třetí strany.
- **Personálního zajištění**, např.:
  - adekvátnost kvalifikace zaměstnanců,
  - adekvátnost motivace a hodnocení zaměstnanců,
  - míra chybovosti zaměstnanců,
  - obměna vedoucích zaměstnanců a zaměstnanců včetně míry fluktuace.
- **Technologií**, např.:
  - dostatečnost technologického vybavení,
  - spolehlivost (např. četnost a důsledky poruch) technologického vybavení,
  - kvalita bezpečnostních mechanizmů,
  - nároky na odbornost.
- **Finančních prostředků a hmotného a nehmotného majetku**, např.:
  - kvalita zabezpečení,
  - hodnota hmotného a nehmotného majetku pro třetí strany.

Při identifikaci rizik lze využívat rovněž tzv. indikátorů rizik, kterými jsou např. vývoje určitých ukazatelů vykazující nevysvětlené odchylky od dosavadního nebo předikovaného vývoje, nestandardní a neodůvodněné stavy, situace apod.

8.3.3 Identifikace řídících a kontrolních mechanizmů vztahujících se k identifikovaným rizikům a rizikovým faktorům

V návaznosti na identifikaci potenciálních rizik a rizikových faktorů se identifikují stávající řídící a kontrolní mechanizmy, které působí na snížení významnosti rizika. Současně je účelné již v této fázi zvažovat možná zdokonalení uvedených mechanizmů.

8.4 Popis identifikovaných rizik

bude zahrnovat:

- stručný název rizika postihující jeho charakter včetně uvedení zda se jedná o riziko externí či interní,
- uvedení skupiny rizik podle členění uvedeného v bodu. 6.3,
- označení útvaru, v jehož působnosti bylo riziko identifikováno,
- proces, aktivum, při jehož analýze bylo riziko identifikováno; podstatu rizika (událost, jednání, nebo stav, který představuje hrozbu),
- rizikové faktory a jejich stručnou charakteristiku,
- identifikované příčiny[40]
- mechanizmus působení rizika (např. potenciální finanční újma, přerušení procesu či zpoždění procesu, ohrožení spolehlivosti a integrity informací, potenciální újma na jiných aktivech, narušení vztahů se zainteresovanými stranami),
- ohrožené procesní a strategické cíle,
- označení a stručný popis řídících a kontrolních mechanizmů vztahujících se k identifikovaným rizikům a rizikovým faktorům,
- další zjištěné skutečnosti významné pro další fáze řízení rizika, případně z hlediska potřeb dokumentace procesu[41].

Výše uvedený popis je základem Evidenčního listu rizika (viz příloha č. 8).

[40] V této etapě není identifikace příčin rizika základním cílem. Identifikace příčin je předmětem zejména etapy analýza rizik.
[41] např. poznámky o individuálním či skupinovém vnímání rizika.

8.5 Identifikace příležitostí

Podle principu uvedeného v bodě 6.1 využívám systému řízení rizik rovněž k identifikaci příležitostí pro organizaci.

V případě identifikace příležitostí:

- je nezbytné identifikovat rizika spojená s jejich realizací a v případě rozhodnutí o realizaci příležitosti postupovat dále podle tohoto návrhu,
- rozhodnout o její realizaci, případně ji postoupit k rozhodnutí příslušnému vedoucímu zaměstnanci organizace.

[42]

Obrázek 8 SWOT analýza

[42] Zdroj: http://www.grouputer.com/swot_analysis.html

9 ANALÝZA RIZIK

Cílem analýzy rizik je pochopit rizika ve všech souvislostech, poskytnout objektivní podklady o významnosti rizik a pro rozhodnutí o opatřeních k jejich zvládání.

Analýza se zabývá zkoumáním a vyhodnocováním zdrojů rizik, příčin rizik a rizikových faktorů majících vliv na pravděpodobnost výskytu hrozeb, pravděpodobnost jejich negativního dopadu a na závažnost tohoto dopadu. Dále zahrnuje hodnocení již existujících opatření, která snižují rizika.

V rámci analýzy rizik je rovněž možné provádět slučování obdobných rizik. V průběhu analýzy mohou být také odhaleny další rizikové faktory nebo řídící a kontrolní mechanizmy neidentifikované v předchozí etapě řízení rizik. Jejím výstupem je zejména zhodnocení pravděpodobnosti výskytu a charakteru a závažnosti dopadu[43] a stanovení významnosti rizik.

9.1 Členění rizik na rizika strategická a procesní

Jedním z výstupů analýzy rizik je členění rizik na strategická a procesní rizika. Strategická rizika jsou ta, která ohrožují strategické cíle organizace, které jsem uvedla v bodě 8.1 případně další strategické cíle uvedené v dalších dokumentech organizace. Rizika procesní mají dopad na procesy organizace, avšak neohrožují přímo splnění strategických cílů.

Za strategické riziko však nepovažuji riziko, které sice souvisí s procesy, jejichž cíle jsem identifikovala, podle bodu 8.2, jako cíle s vazbou na strategické cíle, ale jehož charakter a intenzita dopadu nedosáhne alespoň 5. stupně dopadu procesních rizik, který jsem uvedla v bodě. 9.2.2.

9.2 Kritéria pro hodnocení rizik

Hodnocení rizik proběhne nejprve na úrovni jednotlivých procesů. Následně provedu integraci výsledků z hlediska vlivu na strategické cíle (strategická rizika), nebo procesní cíle a dále učiním jejich vyhodnocení.

Zařazení do jednotlivých dále uvedených skupin navrhuji provést s využitím zkušeností, záznamů o výskytu událostí, prognóz apod. Předpokladem adekvátního zařazení

[43] Každá událost může mít více následků a ovlivnit různé cíle.

je soustavné vedení dokumentace o rizikových událostech pro kvalifikované stanovení pravděpodobnosti (četnosti) výskytu a závažnost dopadu. Z tohoto hlediska je důležité, aby o všech rizikových situacích byly vedeny záznamy popisující a pokud možno kvantifikující jejich přímý i související dopad.

9.2.1 Kritéria pro hodnocení pravděpodobnosti výskytu rizik

Jedním z cílů analýzy rizik je stanovit pravděpodobnost výskytu rizika[44]). S ohledem na faktickou nemožnost stanovit tuto pravděpodobnost přesně, jsem pro její vyjádření stanovila následující stupnice pravděpodobnosti:

- **1. stupeň - téměř nemožná** – výskyt rizika je předpokládán maximálně 1x za 20 a více let (pravděpodobnost výskytu za rok ≤5%[45])
- **2. stupeň - výjimečně možná** – výskyt rizika je předpokládán maximálně 1x v intervalu ‹6; 20) let; 5%< pravděpodobnost výskytu za rok ≤ 16,7 %
- **3. stupeň - možná** - výskyt rizika je předpokládán maximálně 1x v intervalu ‹3; 6) let; 16,7%< pravděpodobnost výskytu za rok ≤ 33,3 %
- **4. stupeň - pravděpodobná** - výskyt rizika je předpokládán maximálně 1x v intervalu (1; 3) let; (33,3%< pravděpodobnost výskytu za rok < 100 %)
- **5. stupeň - jistá** – výskyt rizika je předpokládán minimálně 1 x za rok; (pravděpodobnost = 100 %)

9.2.2 Kritéria pro hodnocení dopadu rizik

Dalším cílem analýzy rizik bude stanovit charakter a intenzitu dopadu rizik. S ohledem na nemožnost stanovit dopad přesným finančním vyjádřením jsem použila dále uvedené stupnice tohoto dopadu. Tyto stupnice využívají rovněž pěti stupňů, a to ve dvou variantách. První varianta se bude používat pro vyjádření dopadu strategických rizik. Druhá stupnice se bude používat pro vyjádření dopadu procesních rizik.

---

[44] Souhrnná pravděpodobnost.

[45] Do skupiny téměř nemožného výskytu náleží převážně živelní pohromy, v úvahu připadá pandemie (např. chřipky) apod. V tomto kontextu je nutno zohlednit i dobu, po kterou k události nedošlo. Pokud by například odhadovaná četnost výskytu pandemie chřipky byla 30 let a k události nedošlo 20 let, pak se zařazuje do stupně 2 - maximálně jednou v intervalu ‹6; 20) let. Obdobný postup platí i pro další stupně.

Východiskem pro vyjádření dopadu bude základní stupnice hodnocení dopadu rizik, uvedená v bodě 6.2. S ohledem na skutečnost, že část dopadů rizik nelze vyjádřit ve finančních prostředcích, doplnila jsem tuto stupnici o verbální vyjádření dopadů agregovaných rizik. Agregace bude prováděna do skupin vycházejících z členění uvedeného v bodě. 6.3.

Na úrovni strategických rizik jsem využila výše uvedenou a následně doplněnou základní stupnice dopadu:

- **1. stupeň - relativně malý** - vliv na strategické cíle a funkce organizace je minimální,
- **2. stupeň - citelný** – je způsobilý citelně ovlivnit strategické cíle a funkce organizace, je však bez významných dopadů na vztahy s klienty, dodavateli a dalšími zainteresovanými stranami,
- **3. stupeň - významný** – ovlivní strategické cíle a funkce organizace a je způsobilý narušit vztahy s klienty, dodavateli a dalšími zainteresovanými stranami,
- **4. stupeň - velmi významný** – podstatně ovlivní strategické cíle a funkce organizace, naruší vztahy s klienty, dodavateli a dalšími zainteresovanými stranami,
- **5. stupeň - nepřípustný** – ztráta schopnosti organizace fungovat.

Na úrovni procesních rizik jsem použila následující stupnice dopadu:

- **relativně malý** - vliv na vnitřní procesy organizace je minimální a je zvládán v rámci běžného řízení,
- **citelný** – je způsobilý citelně ovlivnit vnitřní procesy, je však bez významných dopadů na cíle vnitřních procesů organizace,
- **významný** – ovlivní vnitřní procesy organizace a je způsobilý dílčím způsobem narušit realizaci cílů těchto procesů,
- **velmi významný** – podstatně ovlivní cíle vnitřních procesů, avšak jeho dopady jsou řešitelné,
- **nepřípustný** – je na hranici ohrožení strategických cílů a bez včasné a adekvátní reakce je ohrozí a jeho dopady přesáhnou možnosti disponibilních finančních prostředků

Komplexně jsem kritéria pro hodnocení pravděpodobnosti výskytu a závažnosti dopadu rizik uvedla v příloze č. 4.

9.2.3 Určování pravděpodobnosti výskytu, závažnosti dopadu a významnosti rizik

Na základě analýzy jednotlivých rizik navrhuji stanovit hodnoty pravděpodobnosti výskytu rizika a závažnosti dopadu. Hodnota významnosti rizika se pak propočte jako jejich násobek.

Hodnotu významnosti navrhuji stanovit:

- v bodech, jako násobek bodového ohodnocení pravděpodobnosti výskytu a bodového ohodnocení dopadu rizika,
- ve finančních prostředcích, jako násobek středu příslušného intervalu pravděpodobnosti výskytu rizika (v %) a násobku středu příslušného intervalu hodnocení dopadu (v Kč), uvedeného v příloze č. 4.

Předpokladem pro objektivní stanovení uvedených hodnot je zhodnocení a zohlednění již přijatých opatření, která tato rizika snižují.

Grafické znázornění kombinace kritérií pro hodnocení pravděpodobnosti výskytu a závažnosti dopadu rizik a jejich významnosti jsem uvedla v příloze č. 5.

Pokud lze adekvátními prostředky efektivně získat informace umožňující objektivně zhodnotit, podle stupnic uvedených v bodu 9.2.2 brutto hodnoty rizika, je účelné tyto hodnoty určovat. V dokumentech o řízení rizik se pak budou uvádět hodnoty pravděpodobnosti výskytu rizika, závažnosti dopadu a významnosti rizika jak pro brutto riziko, tak pro zbytkové riziko. Dále se zde bude uvedena hodnota vlivu řídících a kontrolních mechanizmů či jiných opatření k optimalizaci rizika (viz příloha č. 6). Rozlišení zbytkového a brutto rizika je významné pro identifikaci nejdůležitějších kontrol v organizaci[46].

Finanční vyjádření dopadu a významnosti rizika je v případech některých rizik, zejména nefinančních (rizika uvedená v čl. 6.3), nezbytné považovat za orientační.

Ke stanovení uvedených hodnot a charakteru rizika doporučuji provádět analýzu zahrnující:

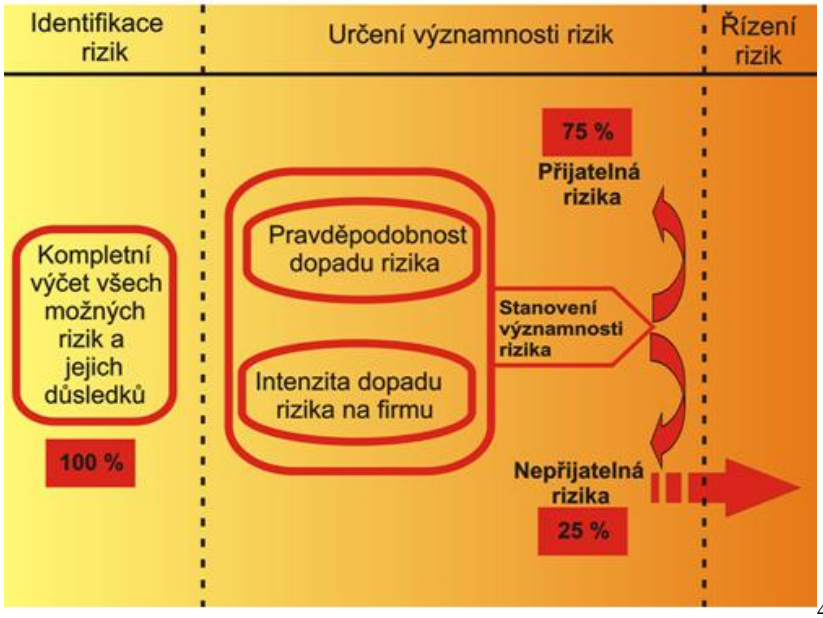
- zdroje rizik (mj. z hlediska míry jejich ovlivnitelnosti ze strany organizace),

[46] Čím je větší rozdíl mezi významností brutto rizika a zbytkového rizika, tím je větší význam řídicích a kontrolních mechanizmů.

- rizikové události[47],
- rizikové faktory,
- příčiny rizik,
- mechanizmy působení rizik,
- řídící a kontrolní mechanizmy a jiná opatření vztahující se k rizikovým událostem a rizikovým faktorům,
- následky,
- ohrožené procesní a strategické cíle.

V rámci výše uvedené analýzy navrhuji posoudit v předchozí etapě identifikovaná rizika (viz čl. 8) z hlediska možného sloučení, resp. přiřazení do podskupin rizik[48].

Součástí analýzy rizik je jejich hodnocení v situacích, kdy dochází k souběhu jednotlivých rizik a kdy může v některých případech dojít k velmi dynamickému nárůstu jejich následků.



[49]

Obrázek 9 Určení významnosti rizika

[47] Události, jednání a stavy, které představují hrozbu.
[48] Podskupin ke skupinám uvedeným v čl. 6.3., např. riziko řízení lidských zdrojů jako podskupina rizik strategického řízení.
[49] Zdroj: http://www.classfin.cz/?pg=ekonomika_detected&Ing=cs&ek1=1

10 VYHODNOCENÍ RIZIK

Cílem vyhodnocení rizik je rozhodnout podle výsledků analýzy rizik o prioritách v řízení rizik, tj. ke kterým rizikům je nezbytné přijmout opatření k jejich snížení a v jakém pořadí mají být tato opatření zpracována a realizována.

Vyhodnocení bude zahrnovat porovnání významnosti jednotlivých rizik se stanovenými kritérii. Navrhuji tyto 4 stupně:

10.1 Nízká významnost

je charakteristická nízkým, nepodstatným vlivem na realizaci cílů organizace; vyžaduje rutinní sledování v rámci provozních postupů.

10.2 Střední významnost

je charakteristická vlivem na dosažení cílů organizace; vyžaduje angažovanost vedoucích zaměstnanců odpovědných za procesy, ve kterých se rizika vyskytují, při jejich zvládání je významným faktorem poměr očekávaného přínosu a nákladů na jejich zvládání.

10.3 Vysoká významnost

je charakteristická podstatným vlivem na dosažení cílů organizace; vyžaduje přímou angažovanost jednotlivých členů vedení organizace při jejich zvládání a monitoring vedení organizace.

10.4 Extrémní významnost

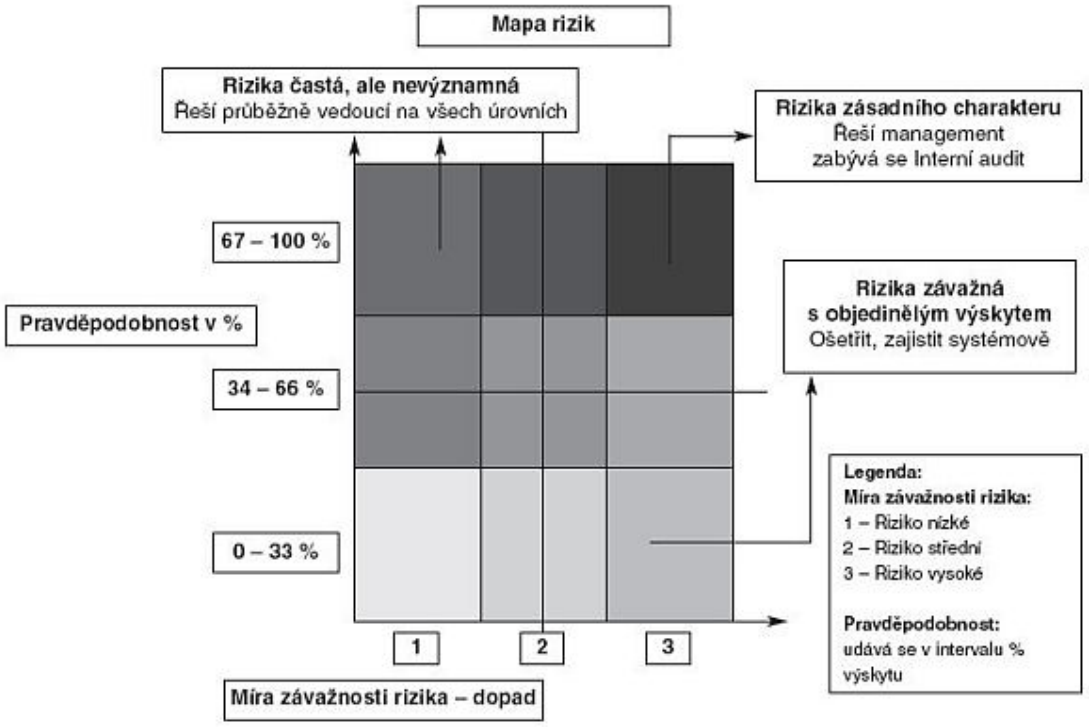
je charakteristická základním vlivem na schopnost dosažení cílů organizace (případně znemožnění jejich dosažení) vyžaduje přímou angažovanost vedení organizace při jejich zvládání a jeho dohled.

Hodnoty pravděpodobnosti výskytu a závažnosti dopadu rizik spadající do jednotlivých výše uvedených stupňů významnosti jsem uvedla v příloze č. 6. Stanovení stupňů významnosti zohledňuje mj. nezbytnost rozlišovat při stejných hodnotách významnosti rizik rozložení pravděpodobnosti výskytu rizika, a věnovat vysokou pozornost rizikům s ojedinělým výskytem, avšak vysoce závažnými dopady viz bod. 11.2.

V rámci stanovení priorit je nezbytné zohlednit kromě významnosti rizik i přínosy, např. varianta činnosti s vyššími možnými ztrátami může být spojena s vyššími možnými přínosy. V takovém případě je třeba vycházet z kontextu s cíli organizace.

Na základě vyhodnocení rizik může být rovněž přijat závěr, že stávající opatření ke snížení některých rizik jsou nákladově nepřiměřená, neboť prostředky, které jsou na ně vynakládány, převyšují skutečný (i potenciální) efekt.

Výsledkem hodnocení rizik je stanovení pořadí jednotlivých rizik podle priorit. Priorita rizik je součástí údajů uváděných v Katalogu rizik (viz příloha č. 9).



[50]

Obrázek 10 Mapa rizik

[50] Zdroj: http://www.ucetnikavarna.cz/archiv/dokument/doc-d8966v11782-analyza-a-rizeni-rizik/?search_query=%24issue%3D34I30

11 ZVLÁDÁNÍ RIZIK

Zvládání rizik zahrnuje zjištění možností pro ošetření rizik, hodnocení těchto možností, přípravu a realizaci Plánu zvládání rizik.

11.1 Identifikace variant zvládání zbytkových rizik

Mezi základní skupiny strategií nakládání se zbytkovými riziky patří:

- vyhnutí se riziku,
- snížení pravděpodobnosti dopadu rizika,
- snížení následků rizika,
- sdílení rizika,
- podstoupení rizika,
- vytváření rezerv.

Níže jsou uvedeny aktivní strategie:

- **Vyhnutí se riziku** se realizuje rozhodnutím, že nebude pokračováno v činnosti (nebude započato s činností), která riziko přináší, např. vyhnutí se riziku ohrožujícímu hotovostní finanční toky se realizuje přechodem na bezhotovostní styk. Vyhýbání se rizikům nesmí však být nepřiměřené, neboť by mohlo vést ke zvýšení významu jiných rizik nebo znemožnit realizaci přínosů (příležitostí) spojených s nerealizovanými činnostmi.
- **Snížení pravděpodobnosti dopadu rizika**, tj. pravděpodobnosti, že určitá událost nastane a/nebo pravděpodobnosti, že bude mít negativní vliv, se realizuje např. režimovými opatřeními vztahujícími se k přístupu do objektů a prostor organizace, k jejím informačním systémům, nastavením a realizací systému předběžné řídící kontroly.
- **Snížení následků rizika** se realizuje např. pravidelnými kontrolami, preventivním snížením hodnot (limitu pokladní hotovosti, skladovaných zásob), adekvátními kompetencemi, bezpečnostními zařízeními a plány pro mimořádné situace.
- **Sdílení rizika** s dalšími organizacemi či osobami realizované např. pojištěním, smluvními ujednáními (inflační doložky, sankční a garanční ujednání), dohody o hmotné odpovědnosti. Tato skupina možností v sobě obsahuje rizika spojená se subjekty, které se podílejí na sdílení (např. že smluvní partneři organizace nebudou s to dostát svým závazkům tj. riziko kreditní). Mezi významné legislativní

možnosti může v některých případech náležet přenos rizika dlouhodobých projektů na podnikatelské subjekty na základě zákona č. 139/2006 Sb., o koncesních smlouvách a koncesním řízení.

Níže jsou uvedeny pasivní strategie:

- **Podstoupení rizik** se realizuje u rizik vyhodnocených jako přijatelná, pokud v rámci disponibilních zdrojů nelze realizovat nákladově přiměřená opatření. Některá rizika nevyhodnocená jako přijatelná jsou vědomě podstupována, pokud se je nepodaří vhodně sdílet nebo jinak zvládat a činnost nelze ukončit. Některá rizika jsou podstupována i nevědomě, pokud se je nepodařilo identifikovat.
- **Vytváření rezerv** slouží k zajištění prostředků na eliminaci následků rizik. Samotné vytváření rezerv je zpravidla ohroženo neexistencí dostatečných zdrojů pro jejich tvorbu, resp. vymezením zdrojů a podmínek pro tvorbu rezerv právními předpisy.

Při volbě výše uvedených strategií je nezbytné z hlediska možnosti a způsobu ovlivnitelnosti přihlížet k tomu, zda se jedná o externí nebo interní rizika, tj. zda zdroje rizik jsou mimo organizaci či spočívají v prostředí organizace (jejích systémech, činnostech, aktivech apod.). Ke každému riziku se, pokud je to možné, identifikují varianty opatření ke zvládání rizik.

11.2 Vyhodnocení variant možností zvládání rizik a výběr optimální z nich

Vyhodnocení variant možností zvládání rizik musí zohlednit:

- zásadu přiměřenosti nákladů na zvládání rizik v porovnání s přínosy; při posuzování nákladů a přínosů je nutno vycházet z celkového kontextu (hodnotit celkové náklady na riziko, přínosy hmotné i nehmotné, dodržovat priority při zvládání rizik[51]),

[51] Zejména při omezeném rozpočtu na řízení rizik, což i logicky i fakticky bývá vždy.

- skutečnost, že zásada přiměřenosti, spolu s přístupem vycházejícím z pořadí rizik dle priorit má za následek, že výsledkem zvládání rizik není jejich minimalizace ale optimalizace[52],
- nutnost věnovat vysokou pozornost zvládání takových závažných rizik, u kterých požadavky kladené na zdravotní, sociální, právní apod. aspekty mohou převážit aspekty ekonomické,
- skutečnost, že přístup ke zvládání rizik musí vycházet ze znalosti hodnot, názorů a oprávněných zájmů zainteresovaných stran,
- nezbytnost rozlišovat při stejných hodnotách významnosti rizik rozložení pravděpodobnosti výskytu rizika, a věnovat vysokou pozornost rizikům s ojedinělým výskytem, avšak s vysoce závažnými dopady, která je nezbytné ošetřit např. prostřednictvím pojištění, plány pro mimořádné situace[53],
- skutečnost, že riziko může být hodnoceno jako „nepřiměřeně kontrolované“, pokud náklady na jeho zvládání jsou neadekvátní přínosu; v tomto případě je na místě zvažovat účelnější a efektivnější využití zdrojů na optimalizaci rizik,
- proveditelnost opatření ke zvládání rizik,
- rizika spojená s realizací opatření ke zvládání rizik.

Na základě výše uvedeného vyhodnocení bude vybrána optimální varianta opatření ke zvládání rizika. Součástí dokumentace této varianty bude zhodnocení předpokládaných nákladů na uvedená opatření, případně v porovnání s celkovými disponibilními zdroji na zvládání příslušné skupiny rizik.

11.3 Plán zvládání rizik

Plán zvládání rizik navrhuji na základě předchozího vyhodnocení, a tento bude obsahovat:

- název rizika,
- opatření k zvládání rizika,
- požadavky na zdroje (finanční, personální apod.),
- vlastníka rizika,

[52] Tento přístup představuje mj. pojetí analogické pojetí správnosti operace dle § 2 písm. l) zákona o finanční kontrole, dle kterého se správností finanční a majetkové operace rozumí její soulad s právními předpisy a dosažení optimálního vztahu mezi její hospodárností, účelností a efektivností.
[53] Tato opatření v případě rizik s vysokou pravděpodobností výskytu ztrácejí své opodstatnění.

- odpovědnost za realizaci jednotlivých opatření,
- kritéria plnění opatření,
- termín realizace opatření, případně termíny a kritéria dílčích plnění,
- požadavky na monitorování realizace opatření a podávání zpráv.

Vzor Plánu zvládání rizik jsem uvedla v příloze č. 7.

12 MONITOROVÁNÍ A PŘEZKOUMÁVÁNÍ SYSTÉMU ŘÍZENÍ RIZIK

Monitorování a přezkoumávání je nedílnou součástí celého procesu řízení rizik. Monitorování by mělo zahrnovat:

- sledování vnějšího a vnitřního prostředí organizace s cílem včas identifikovat nová rizika nebo změny významnosti stávajících rizik,
- sledování poznatků o řízení rizik[54] zahrnující praxi v jiných institucích či principy obsažené ve standardech pro řízení rizik s cílem kontinuálně zdokonalovat řízení rizik,
- sledování realizace Plánu zvládání rizik v rámci programu porad na všech úrovních řízení a realizace či navrhování jeho případných změn,
- zpracovávání periodických zpráv o realizaci Plánu zvládání rizik a jejich projednávání na poradě vedení organizace,
- využívání výsledků monitoringu na průběžné zkvalitňování systému řízení rizik.

Proces řízení rizik by měl být minimálně jednou ročně přezkoumáván z hlediska jeho adekvátnosti potřebám organizace. Toto přezkoumávání bude realizováno před periodickou identifikací, hodnocením a analýzou rizik a stanovením opatření k jejich zvládání v Plánu zvládání rizik.

Přezkoumávání procesu řízení rizik by mělo být rovněž nedílnou součástí jednotlivých interních auditů i konzultačních akcí odboru interního auditu Úseku interního auditu a kontroly.

Nezbytným předpokladem úspěšného řízení rizik ve všech jeho etapách jsou adekvátní informace jak o vnitřním prostředí organizace, tak o jejím vnějším prostředí. Adekvátní informace a jejich včasná a správná komunikace v rámci organizace napomáhá tomu, aby byla včas identifikována rizika a přijímána adekvátní opatření na příslušných úrovních řízení. Současně napomáhá tomu, aby vedoucí zaměstnanci a zaměstnanci odpovědní či participující za řízení rizik na všech úrovních jednotně vnímali podstatu a význam rizik a přijímaných opatření. Komunikace je rovněž předpokladem pro vnímání rizik jako

[54] Předmětem tohoto sledování jsou rovněž rizika identifikovaná jinými subjekty.

faktoru ohrožení nejen pro organizaci jako instituci, ale i pro její zaměstnance, což vytváří základ jejich integrovaného úsilí a podpory řízení rizik a ztotožnění se s přiděleným „vlastnictvím“ rizik.

V řetězci příčin a následků často existují situace, že co je pro jednu stranu příležitostí je pro druhou stranu hrozbou/rizikem. Cílem komunikace je pak dosažení stavu, aby tato rizika, bez jejich dostatečné analýzy, neměla za následek nerealizaci příležitostí pro organizaci jako celek.

Správná komunikace se zainteresovanými stranami je mj. nezbytným předpokladem úspěšné realizace takových opatření ke zvládání rizik, která by tyto strany mohly považovat za ohrožení svých zájmů.

13 DOKUMENTACE VÝSLEDKŮ VYHODNOCENÍ RIZIK A OPATŘENÍ K JEJICH ZVLÁDÁNÍ

Dokumentace výsledků vyhodnocení rizik a opatření k jejich zvládání bude zahrnovat Evidenční list rizika, Katalog rizik a Mapy rizik.

13.1 Evidenční list rizika

Evidenční list rizika bude obsahovat podrobné údaje o riziku, přičemž zahrnuje jak aktuální údaje, tak historické údaje postihující vývoj parametrů rizika; mezi tyto údaje naleží:

- název rizika,
- označení skupiny rizika podle čl. 6.3, a navazujících klasifikací úseků a samostatných odborů vycházejících z jejich podmínek,
- označení útvaru, procesu, činnosti nebo aktiva, při jehož analýze bylo riziko identifikováno,
- popis mechanizmu působení rizika,
- rizikové faktory,
- příčiny rizika,
- vlastník rizika,
- vazby na další útvary, procesy, činnosti nebo aktiva,
- potenciální dopady na procesní cíle a na strategické cíle organizace, potenciální dopady ostatní
- řídící a kontrolní mechanizmy a další opatření již realizovaná k optimalizaci rizika, případně výsledky externích a interních kontrol,
- hodnocení pravděpodobnosti výskytu, závažnosti dopadu a výsledné hodnocení významnosti rizika; pokud je to možné, kromě hodnot zbytkového rizika, i v hodnotách brutto rizika viz čl. 9.2.3, údaje o prioritě rizika,
- opatření přijatá ke zvládání rizika včetně odpovědnosti za jejich plnění, termínů realizace, kritérii plnění,
- předpokládané cílové hodnoty pravděpodobnosti výskytu, závažnosti dopadu a významnosti rizika,
- údaje o monitorování přiměřenosti a účinnosti opatření ke zvládání rizika,
- ostatní relevantní informace, např. o předchozí expozici rizika.

Vzor Evidenčního listu jsem uvedla v příloze č. 8.

13.2 Katalog rizik

Katalog rizik bude obsahovat základní údaje o riziku:

- název rizika,
- označení skupiny rizika podle čl. 6.3, a navazujících klasifikací úseků a samostatných odborů vycházejících z jejich podmínek,
- značení útvaru, procesu, činnosti nebo aktiva, při jehož analýze bylo riziko identifikováno,
- potenciální dopady na procesní cíle a na strategické cíle organizace, potenciální dopady ostatní,
- hodnocení pravděpodobnosti výskytu, závažnosti dopadu a výsledné hodnocení významnosti rizika; pokud je to možné, kromě hodnot zbytkového rizika, i v hodnotách brutto rizika,
- opatření přijatá ke zvládání rizika včetně odpovědnosti za jejich plnění, termínů realizace, kritérii plnění,
- předpokládané cílové hodnoty pravděpodobnosti výskytu, závažnosti dopadu a vyhodnocení významnosti rizika.

Vzor Katalogu rizik jsem uvedla v příloze č. 9.

13.3 Mapy rizik

Mapy rizik budou zobrazovat grafické vyjádření pravděpodobnosti výskytu a závažnosti dopadu rizika, jsou vytvářeny pro strategická rizika, procesní rizika a souhrnné. Mapu rizik lze využít rovněž pro transparentní znázornění brutto rizik, zbytkového rizik a cílového stavu řízení rizik (zbylého rizika po realizaci opatření ke zvládání rizika).

Grafické znázornění Mapy rizik je obsaženo v příloze č. 10.

ZÁVĚR

Na níže uvedeném příběhu si dovolím shrnout všechny informace uvedené v své diplomové práci.

Aničce se narodilo první dítě. V porodnici, hned jakmile je uviděla, si řekla: "Své dítě nikomu nedám ani za nic a nikdy ho neopustím. **(Tím byla stanovena strategie: Bylo rozhodnuto, že se bude ochraňovat, co, jak a za jakou cenu bude chráněno.)**

Po návratu domů se svému děťátku věnovala tak výhradně a usilovně, až únavou usnula na židli vedle postýlky a vzbudil ji až zoufalý dětský pláč. Řekla si, že tak to přece nejde, dítě nesmí zůstávat bez dohledu. Do hlídání bude nutné zapojit taky manžela a tchyni. **(Analýza rizik: Bylo zjištěno, kdy a co může ochranu oslabit a byla přijata opatření pro snížení rizika. Byly určeny priority – nejdřív manžel, přinejhorším tchyně.)**

Ovšem problémy na sebe nadaly dlouho čekat. Tchyně si umínila, že uklízet se bude v celém domě, tak jako dříve a jednou, když ženské odpoledne už padaly únavou, manžel odešel do práce. A tak se dohodli, že manžel bude dočasně chodit jen na ranní směnu, tchyně bude hlídat vždy dopoledne (stejně se brzy ráno budí) a Maruška bude vstávat k dítěti v noci. **(Tak vznikla bezpečnostní politika, tj. základní pravidla a rozdělení odpovědností.)**

Cobydup, dítě se začalo batolit a prozkoumávat všechno, na co dosáhlo. Nezbylo než dbát, aby ubrusy nevisely přes okraj stolu, aby je dítě na sebe nestáhlo, při vaření bylo nutné dítě sledovat nepřetržitě. A taky drobnosti, co vejdou do pusy, nenechávat volně ležet, aby je dítě nepolklo. **(Byly vytvořeny bezpečnostní směrnice a standardy, pro bezpečnostně důležité činnosti byly určeny závazné postupy.)**

Jednoho dne se švagrová rozešla s tím svým, donedávna nadosmrti ideálním partnerem a vrátila se domů. Všechno se zase muselo přeorganizovat. Ze skladiště byl najednou pokoj, krámy se objevily v chodbě a švagrové se nová situace musela vysvětlit z gruntu znova. **(Implementace systému bezpečnosti – vzdělávání, změny, zlepšování.)**

Ale švagrové se nedalo věřit. Neustále aktivně hledala nového partnera. Jednou slíbila hlídání a pak dítě nechala hodinu sedět v zahradní restauraci u limonády. Aničce nezbylo, než všechno občas zkontrolovat a na každou nedbalost vždycky řádně upozornit. Přitom se taky přišlo na to, že zahradní restaurace sice vyhlašuje, že se stará i o děti, ale nikdo tam s malými dětmi raději nechodí. Na základě negativních zkušeností se Anička rozhodla

do této zahradní restaurace již nechodit. **(Monitorování, kontrola a nápravná a preventivní opatření.)**

Tento příběh naznačuje dvě důležité pointy:

- Pochopení toho, co chci chránit, dává smysl pojmu riziko.
- Riziko pak lze korigovat, nikoli však vyloučit.

V bezpečnostní politice a řízení rizik je úspěšný je ten, kdo respektuje skutečnou situaci svého konkrétního případu a účelně využívá teorii a cizí zkušenosti tam, kde jim skutečně rozumí.

ZÁVĚR V ANGLIČTINĚ

The story below, I would like to summarize all the information in my thesis. Annie was born first child. In the hospital, as soon as she saw them, he said, "I will not give your child for anything and never leave him. **(This strategy was established: It was decided that it will protect what, how and at what price will be protected.)**

After returning home with your baby and exclusively devoted so hard that weariness fell asleep on the chair beside her bed and woke up distressed baby's cry. She said that so it does not, the child must not remain unattended. The baby will also need to involve her husband and mother in law. **(Hazard Analysis: It was found, when and what protection may weaken, and measures to reduce risk. Priorities were identified - first husband, mother in law at worst.)**

But the problems on themselves endowed soon. Mother in law was determined that it will clean the whole house, as before, and once, when women fell afternoon fatigue, the husband left for work. So they agreed that the husband will temporarily go up to the morning shift, mother in law will watch every morning (just to wake up early in the morning) and Mary will get up to the child at night. **(This is how the security policy, ie the basic rules and division of responsibilities.)**

Cobydup, the baby began to toddle and explore all that it had reached. Was left to ensure that the tablecloths hang over edge of table so that each child not withdraw, when cooking was necessary to continuously monitor the child. And little things you come in your mouth, do not leave lying around, so that the child swallow. **(They were created safety guidelines and standards for safety-critical activities were determined by binding procedures.)**

One day the sister broke up with her, until recently an ideal partner for life and returned home. Everything had to reorganize again. The warehouse was suddenly room, stuff appeared in the hallway and sister had to explain the new situation from scratch again. **(Implementation of safety - education, change, improvement.)**

But the sister could not believe it. Continuously and actively seek a new partner. One promised to watch the child and then had an hour to sit in the garden restaurant with lemonade. Annie had no choice but to check all times and for every neglect always properly noted. It is also found out that although the garden restaurant announces that takes

care of children, but no one there with young children prefer to not go. Based on negative experiences with Anna decided to have this garden restaurant not to go. **(Monitoring, control and corrective and preventive action.)**

This story suggests two important points:

- Understanding of what I want to protect, it makes sense to the term risk.
- The risk can then be corrected, but not eliminated.

The security policy and risk management is successful is one who respects the real situation of their individual case and effective use of foreign experience and theory, where they actually mean.

POUŽITÉ ZDROJE:

LITERATURA:

[1] ČERMÁK, Miroslav, *Řízení informačních rizik v praxi,* Brno: Tribun EU, 2009, ISBN 978-80-7399-731-1

[2] HAMPTON, John J., *Fundamentals of Enterprise Risk Management,* AMACOM books, 2009, ISBN: 0-8144-1492-3

[3] KRULIŠ, Jiří, *Jak vítězit nad riziky: aktivní management rizik.* Nástroj úspěšných firem, Praha: Linde, 2011, ISBN 978-80-7201-835-2.

[4] LIDINSKÝ, V.; I. ŠVARCOVÁ; P. BUDIŠ; Z. LOEBL a B. PROCHÁZKOVÁ, *eGovernment bezpečně,* Praha: Grada, 2008, ISBN 978-80-247-2462-1.

[5] MERNA, Tony a Faisal F. AL-THANI, *Risk management: řízení rizika ve firmě*, Praha: Computer Press, 2007, ISBN 978-80-251-1547-3.

[6] MLÝNEK, Jaroslav, *Zabezpečení obchodních informací.* BizBooks, 2007, ISBN 978-80-251-1511-4.

[7] REASON, James T., *Managing the Risk sof Organizational Accidents,* Ashgate Publishing, 1998, ISBN: 1840141042.

[8] REASON, James T., *Human Error,* Cambridge University Press, 1990, ISBN: 0-521-31419-4.

[9] SMEJKAL, Vladimír a Karel RAIS, *Řízení rizik ve firmách a jiných organizacích*, Expert, 2009, ISBN 978-80-247-3051-6.

[10] SMOLÍK, Josef a Tomáš ŠMÍD, *Vybrané bezpečnostní hrozby a rizika 21. století*, Mezinárodní politologický ústav Masarykovy univerzity, 2010, ISBN 978-80-210-5288-8.

[11] VARCHOLOVÁ, Tatiana a Lenka DUBOVICKÁ, *Nový manažment rizika,* Bratislava: Iura Edition, 2008, ISBN 978-80-8078-191-0.

LEGISLATIVNÍ DOKUMENTY:

[1] Zákon č. 320/2001 Sb.: o finanční kontrole. In: *Sbírka zákonů České republiky*. 2001. Dostupné z: http://www.mfcr.cz/cps/rde/xchg/mfcr/xsl/zakony_1542.html

[2] Zákon č. 309/2006 Sb.: o zajištění dalších podmínek bezpečnosti a ochrany zdraví při práci. In: *Sbírka zákonů České republiky*. 2006. Dostupné z: http://aplikace.mvcr.cz/archiv2008/sbirka/2006/sb096-06.pdf

[3] ČSN EN 1050. *Bezpečnost strojních zařízení - Zásady pro stanovení rizikovosti*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 1998.

[4] SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY 2006/42/ES: o strojních zařízeních a o změně směrnice 95/16/ES. In: *Úřední věstník Evropské unie*. 2006. Dostupné z: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:157:0024:0086:CS:PF

[5] Zákon č. 101/2000 Sb: o ochraně osobních údajů. In: Sbírka zákonů České republiky. 2000. Dostupné z: http://aplikace.mvcr.cz/archiv2008/sbirka/2000/sb032-00.pdf

[6] Zákon č.121/2000 Sb.: o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon). In: *Sbírka zákonů České republiky*. 2000. Dostupné z: http://aplikace.mvcr.cz/archiv2008/sbirka/2000/sb032-00.pdf

[7] Zákon č.133/1985 Sb.: o požární ochraně. In: *Sbírka zákonů České republiky*. 1985. Dostupné z: http://aplikace.mvcr.cz/archiv2008/sbirka/1985/sb34-85.pdf

[8] Zákon č.309/2006 Sb.: kterým se upravují další požadavky bezpečnosti a ochrany zdraví při práci v pracovněprávních vztazích a o zajištění bezpečnosti a ochrany zdraví při činnosti nebo poskytování služeb mimo pracovněprávní vztahy (zákon o zajištění dalších podmínek bezpečnosti a ochrany zdraví při práci). In: *Sbírka zákonů České republiky*. 2006. Dostupné z: http://aplikace.mvcr.cz/archiv2008/sbirka

[9] Zákon č. 499/2004 Sb.: o archivnictví a spisové službě. In: *Sbírka zákonů České republiky*. 2004. Dostupné z: http://aplikace.mvcr.cz/archiv2008/sbirka/2004/sb173-04.pdf

INTERNETOVÉ ZDROJE:

[1] http://www.systemonline.cz/clanky/informacni-bezpecnost-proc-ne.htm

SEZNAM POUŽITÝCH POJMŮ A ZKRATEK

pojem/zkratka	význam
Administrativní bezpečnost	systém opatření při tvorbě, příjmu, evidenci, zpracování, odesílání, přepravě, přenášení, ukládání, skartačním řízení, archivaci, případně jiném nakládání s dokumenty
Aktiva	účely této práce se rozumí vše, co má pro organizace hodnotu, na co může mít riziko negativní dopad.
Aktivum	(pro účely této práce) – vše, co má pro organizace hodnotu, na co může mít bezpečnostní riziko negativní dopad.
BASEL	Basilejské smluvy, které jsou doporučeními pro bankovní právo a regulace Basilejské komise pro bankovní dohled.
Bezpečnostní incident	jedna nebo více nechtěných nebo neočekávaných bezpečnostních událostí, u kterých existuje vysoká pravděpodobnost dopadu na aktiva organizace a porušení bezpečnostní politiky organizace.
Bezpečnostní riziko	stav, které jsou spojeny především se ztrátou na hmotných aktivech (penězích, movitém a nemovitém majetku), na nehmotných aktivech (informacích,
Bezpečnostní událost	atd., ukazující na možné porušení bezpečnostní
BOZP	bezpečnost a ochrana zdraví při práci
Brutto riziko	riziko, resp. významnost rizika stanovená bez přihlédnutí k působení předchozích opatření realizovaných za účelem jeho zvládání.
CRAM, IRIS	analýza rizik bezpečnosti automatizovaných informačních systémů
ČR	Česká republika
ERM	Řízení rizik společnosti, je to přístup týkající se celé společnosti
EU	Evropská unie
FRAP	proces analýzy rizik s využitím facilitátora
FMEA	analýza rizik možných vad při konstrukčním návrhu
Fyzická bezpečnost	systém opatření, která mají neoprávněné osobě zabránit nebo ztížit přístup k aktivům, popřípadě přístup nebo pokus o něj zaznamenat
HACCP	analýza rizik chemických a potravinářských výrob
HAZOP	analýza rizik technologickcýh procesů

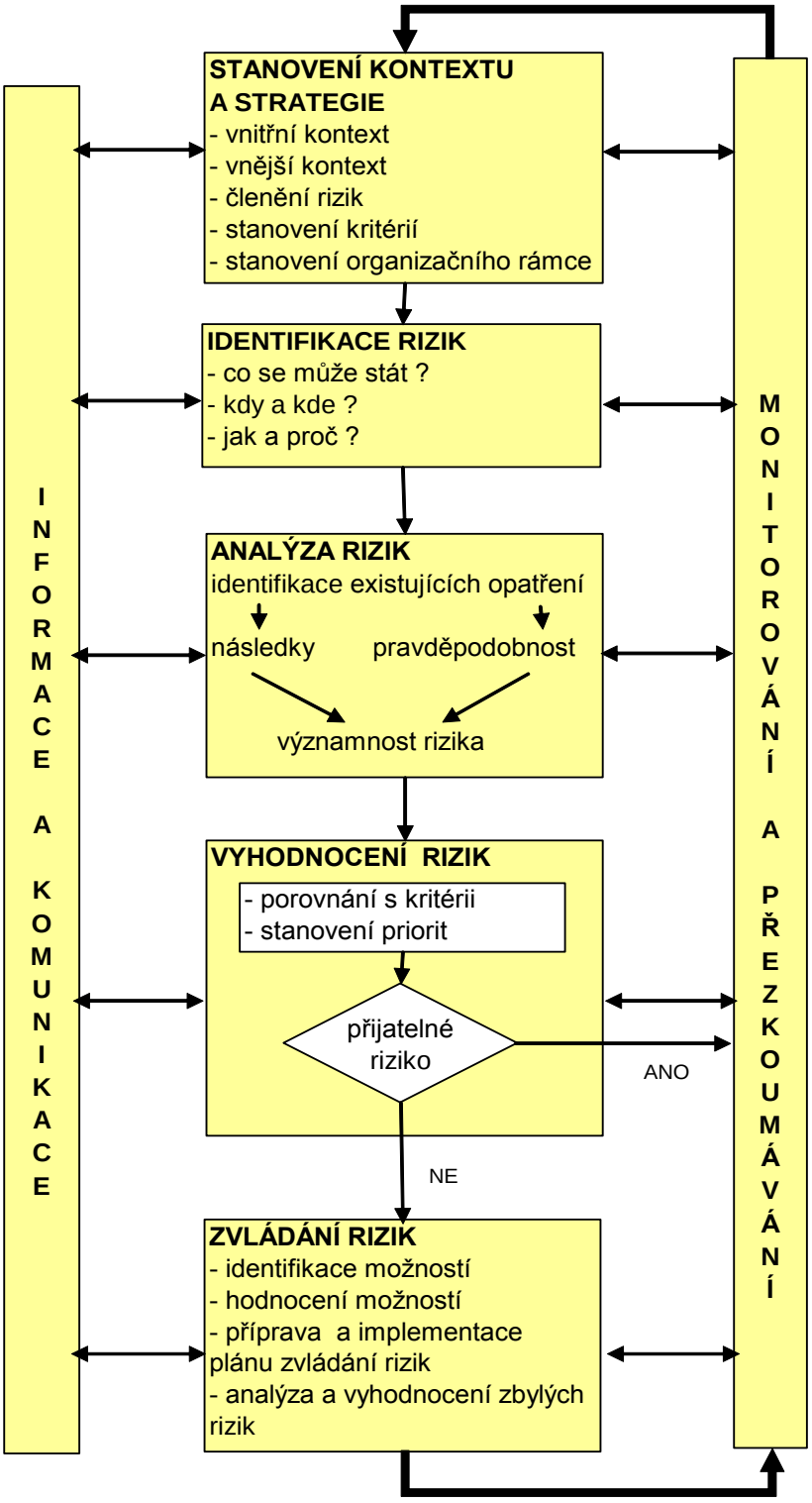
pojem/zkratka	význam
Chráněné údaje	údaje a informace, jejichž ochrana vyplývá ze zákona (např. osobní a/nebo citlivé údaje ve smyslu zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů), nebo údaje a informace vyžadující zvýšenou úroveň ochrany na základě obchodních nebo vnitřních požadavků z hlediska dostupnosti, důvěrnosti nebo integrity
ICT	informační a komunikační technologie
Informace	každý písemný, obrazový, zvukový, elektronický nebo jiný záznam, ať již v podobě analogové či digitální (definice se nevztahuje na nosiče informací)
Informační bezpečnost	systém opatření, jejichž cílem je zajistit důvěrnost, integritu a dostupnost informací, s nimiž tyto systémy nakládají, a odpovědnost správy a uživatele za jejich činnost v informačním nebo komunikačním systému
IS	informační systém
JBM	hodnocení rizik z hlediska bezpečnosti práce podle Tomáše Neugebauera
KŘB organizace	Komise pro řízení bezpečnosti organizace
MQD	proces hodnocení rizik bezpečnosti výrobních strojů
Personální bezpečnost	systém opatření před vznikem zaměstnaneckého poměru, během zaměstnaneckého poměru a při ukončení (změně) zaměstnaneckého poměru
PO	požární ochrana
RIPRAN	bodovaná metoda s mapou rizik - analýza rizik projektů podle Bronislava Lacka
Riziko	hrozba, že může nastat určitá událost, jednání nebo stav, a že bude mít negativní vliv na realizaci záměrů a cílů organizace a její aktiva, případně na další subjekty. Charakter a míra závažnosti /významnost/ rizika jsou dány: 1) pravděpodobností, že určitá událost, jednání nebo stav nastane (P1), a pravděpodobností, že bude mít uvedený negativní vliv (P2), 2) charakterem a intenzitou potenciálních dopadů (následků) uvedeného negativního vlivu (D). Významnost (hodnota) rizika je dána součinem P1 x P2 x D, resp. P x D, kde souhrnná pravděpodobnost (pravděpodobnost výskytu rizika) P = P1 x P2.
Rizikové faktory	podmínky a další faktory umožňující či podporující vznik rizik, resp. jejich negativní vliv.

pojem/zkratka	význam
URNA	univezální matice pro analýzu rizik budov, tunelů, silnic a jiných fyzických objektů s využitím expertních odhadů Milíka Tichého
Zainteresované strany	instituce, organizace a osoby, které mohou ovlivnit cíle a záměry organizace nebo podmínky pro její činnost, nebo být ovlivněny, či se cítit ovlivněny organizace, jejími záměry, cíli, rozhodnutím, činností apod.
Zákon o finanční kontrole	zákon č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů, ve znění pozdějších předpisů
Zbytkové riziko	riziko, resp. významnost rizika stanovená s přihlédnutím k působení předchozích opatření realizovaných za účelem jeho zvládání.

SEZNAM OBRÁZKŮ

SEZNAM PŘÍLOH

PŘÍLOHA Č. 1: SYSTÉM ŘÍZENÍ RIZIK



55

[55] Zdroj: vlastní

PŘÍLOHA Č. 2: BEZPEČNOSTNÍ RIZIKA

Bezpečnostní rizika	
Hrozba	**Popis hrozby**
Loupež	Tato hrozba pokrývá přepadení zaměstnance za účelem získání peněžních nebo jiných aktiv. Může se jednat například o ozbrojené přepadení, pokladny, přepadení zaměstnanců během přepravy peněz do/z banky apod.
Ztráta	Zahrnuje ztrátu (notebooku, média, klíčů, aut. předmětů…) pracovníkem, kterému byl předmět svěřen. Obvykle mimo prostor organizace.
Vloupání/Krádež	Hrozba pokrývá odcizení majetku organizace, případně majetku zaměstnanců z prostor organizace bez pohrůžky násilí (např. z kanceláře, z auta nebo z budovy v mimopracovní době).
Fyzické/slovní napadení zaměstnance	Hrozba pokrývá slovní nebo fyzické napadání zaměstnanců organizace z jakéhokoliv důvodu.
Požár	Hrozba požáru pokrývá incident poškození libovolných fyzických aktiv systému (včetně movitého i nemovitého majetku, dokumentace a magnetických médií) požárem. Míra zranitelnosti budovy a místnosti vůči požáru závisí na rozsahu, na který se požár po vypuknutí může rozšířit a na míře, s jakou naruší fungování organizace.
Poškození vodou	Hrozba poškození vodou pokrývá incident, při němž mohly být části fyzických aktiv systému (včetně dokumentace a magnetických médií) a/nebo části movitého i nemovitého majetku poškozeny vodou. Míra zranitelnosti budovy a místnosti vůči poškození vodou závisí na rozsahu, v jakém může voda zatopit místnost, na rozsahu v jakém může poškodit zařízení a na tom, do jaké míry naruší funkčnost organizace.
Povodeň	Hrozba povodně pokrývá vylití se řeky, vodní nádrže z břehů s následným zaplavením prostor, aktiv organizace, nebo okolní infrastruktury (přilehlé komunikace apod.). Zranitelnost k této hrozbě závisí od toho, zda hodnocená budova je umístěna v zátopové oblasti.
Výbuch	Hrozba výbuchu pokrývá incident exploze technologického zařízení (např. plynová kotelna), který může způsobit zranění lidí, škody na hmotném a nehmotném majetku, nedostupnost systémů. Výbuchy nástražných zařízení jsou zahrnuty v hrozbě „úmyslné poškození.
Přírodní katastrofa	Hrozba přírodní katastrofy pokrývá situaci poškození lokality nebo jejího okolí incidentem způsobeným přírodními poměry (vichřice, sněhová kalamita) nebo lidmi (dopravní nehoda). Míra zranitelnosti prostředí nebo lokality závisí na rozsahu, s jakým katastrofa ovlivní chod organizace.
Úmyslné poškození	Hrozba úmyslného poškození zahrnuje činy vandalismu a další případy, kdy dojde k fyzickému poškození informačního systému, podpůrných zařízení, aut, budov apod., které provedly osoby s nejrůznější motivací.
Prozrazení – neúmyslné, z nedbalosti.	Hrozba zahrnuje neúmyslné prozrazení informací např. při diskusi ve veřejných prostorách, neopatrné konverzaci s "nezaměstnancem, ponecháním dokumentů na veřejně přístupném místě (tiskárny, kopírky atd.) atd.
Vyzrazení certifikátu, hesel, PINů, a jiných autentizačních informací	Tato hrozba pokrývá vyzrazení přístupových hesel, PINů apod. neoprávněným osobám. Oprávněný uživatel tím neztratí přístup.

Provozní chyba	Hrozba provozní chyby pokrývá situace, kdy osoby odpovědné za zajišťování provozu serverového systému, sítí LAN, el. napájení, EZS, EPS apod. mohly udělat chybu při plnění svých pracovních úkolů.
Chyba údržby technického vybavení	Hrozba chyby údržby technického vybavení pokrývá situaci, kdy by osoby odpovědné za údržbu technického vybavení mohly udělat chybu při plnění svých pracovních úkolů.
Chyba úpravy programového vybavení	Hrozba chyby údržby programového vybavení zahrnuje možnost, že by lidé nebo organizace, které jsou odpovědné za údržbu programového vybavení, mohli udělat chybu při své práci.
Chyba uživatele	Hrozba chyby uživatele pokrývá situaci, kdy by uživatelé mohli dělat chyby při používání aplikace.
Pokusy o neoprávněný přístup identifikovatelných osob	Hrozba falšování uživatelské identity identifikovatelnými osobami zahrnuje pokusy neautorizovaných uživatelů získat přístup k informacím, ke kterým nemají oprávnění přistupovat. Tito uživatelé se mohou pokusit získat přístup k těmto informacím tak, že se vydávají za jiného uživatele. Identifikovatelnou osobou je kdokoliv, kdo má legitimní důvod pro přístup k systému (oprávnění uživatelé) nebo práci v budově (uklízečky, pracovníci dodavatelských firem apod.).
Pokusy o neoprávněný přístup cizích osob	Hrozba falšování uživatelské identity cizími osobami zahrnuje pokusy cizích osob získat neautorizovaný přístup k informacím tak, že se vydávají za oprávněného uživatele.
Zavedení destruktivních a škodlivých programů	Destruktivní a škodlivé programy mohou být viry, trojské koně, červi.
Odmítnutí odpovědnosti	Tato hrozba pokrývá: případ, kdy osoba popře, že poslala určitou zprávu (popření původu), případ, kdy osoba popře, že přijala určitou zprávu (popření přijetí)
Neoprávněné nakládání s informacemi	Hrozba "neoprávněné nakládání s informacemi" zahrnuje jakoukoliv záměrnou manipulaci s daty, včetně kopírování, změny, mazání apod.
Zneužití přístupu vývojářů k provozním datům	Hrozba zahrnuje neoprávněné čtení, krádež, modifikaci ostrých dat, která jsou dostupná vývojářům.
Infiltrace komunikace	Infiltrace komunikace pokrývá následující druhy incidentů: Vydávání se za jiný server, Odposlech, Modifikace zpráv, Znepřístupnění služeb (úmyslné), Spamming (rozesílání nevyžádaných emailů)
Zneužití partnerského přístupu	Hrozba zneužití partnerského přístupu zahrnuje případy, kdy je služba zneužita zaměstnancem partnera nebo třetí osobou.
Nedostatek personálu	Hrozba nedostatku personálu pokrývá situaci trvalé nepřítomnosti klíčových osob z jakýchkoli důvodů (výpověď, odchod do důchodu, dlouhodobá práceneschopnost, apod.). Úroveň hrozby pokrývá jednoduchost, s jakou mohou být nahrazeni. Zranitelnost vůči nedostatku personálu závisí na rozsahu, v jakém by nedostatek personálu mohl ovlivnit fungování organizace.
Dočasná nepřítomnost většího počtu zaměstnanců	Hrozba pokrývá dočasnou nepřítomnost desítek procent personálu v důsledku zvýšené nemocnosti, omezení přístupu do budovy (např. v důsledku poruchy komunikací) apod.

Selhání komunikace	Tato hrozba pokrývá: Nedostupnost poskytovatele služeb (ISP), Selhání datového spojení, Nedoručení zprávy, Doručení v chybné posloupnosti (neúmyslné), Pozdní doručení (neúmyslné), Odepření služby (neúmyslné)
Technická závada HW	Hrozba technické závady počítače, paměťového zařízení (externí disk, pásková mechanika), síťového prvku, pokrývá vznik faktorů, které zvyšují pravděpodobnost závady.
Selhání napájení	Hrozba výpadku napájení pokrývá situaci výpadku elektrické sítě.
Selhání klimatizace	Hrozba výpadku klimatizace pokrývá situaci, kdy je nutné přerušit práce z důvodu změny teploty mimo přijatelné meze, způsobené selháním klimatizačního zařízení.
Selhání programového vybavení	Hrozba selhání programového vybavení pokrývá situaci, kdy by systémové, síťové nebo aplikační programové vybavení mohlo selhat a způsobit tak nedostupnost systému nebo oslabit další bezpečnostní mechanismy, nebo kdy by logika aplikačního programového vybavení mohla obsahovat chyby.
Neoprávněná změna zdrojových kódů	Hrozba změny zdrojových kódů zahrnuje jakoukoliv změnu, která nebyla autorizována, ať už zaměstnancem organizace nebo externím útočníkem.
Prozrazení 3. stranou	Prozrazení informace subjektem, který není účastníkem vztahu - například obsahu smlouvy advokátní kanceláří (organizace nebo protistrany), (prozrazení nebo zneužití), přípravy nebo nabídek ve výběrovém řízení poradenskou firmou atd.

PŘÍLOHA Č. 3: TABULKA VAZEB MEZI PROCESNÍMI A STRATEGICKÝMI CÍLY ORGANIUACE

TABULKA VLIVŮ JEDNOTLIVÝCH PROCESŮ NA STRATEGICKÉ cíle									
		optimální sít odběratelů	optimální smluvní vztahy s dodavateli	soulad s legislativou	schopnost konkurence na evropském trhu	transformace na klientsky orientovanou organizaci	účelnosti, hospodárnosti a efektivnosti činností zajišťovaných organizací	konsolidace, centralizace informačního systému a jeho podpory strategii organizace	
číslo	**procesy**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**Poznámka**

[56]

Legenda:

[56] Zdroj: vlastní

přímý vliv – 2
podpůrný vliv – 1
bez vlivu – 0

TABULKA VLIVU PROCESU NA JEDNOTLIVÉ STRATEGICKÉ CÍLE											
Strategické cíle		**Procesy ovlivňující strategické cíle**									
		1.	**2.**	**3.**	**4.**	**5.**	**6.**	**7.**	**8.**	**9.**	**10.**
1.	optimální sít odběratelů										
2.	optimální smluvní vztahy s dodavateli										
3.	soulad s legislativou										
4.	schopnost konkurence na evropském trhu										
5.	transformace na klientsky orientovanou organizaci										
6.	účelnosti, hospodárnosti a efektivnosti činností zajišťovaných organizací										
7.	konsolidace, centralizace informačního systému a jeho podpory strategii organizace										

[57]

Legenda:

Číslo v horním řádku tabulky označuje proces ovlivňující strategické cíle; číselné označení jednotlivých procesů je součástí dokumentace procesu řízení rizik.

[57] Zdroj: vlastní

PŘÍLOHA Č. 4: KRITÉRIA PRO HODNOCENÍ PRAVDĚPODOBNOSTI VÝSKYTUA ZÁVAŽNOSTI DOPADU RIZIK

1. Kritéria pro hodnocení pravděpodobnosti výskytu rizik

Bodová hodnota	Pravděpodobnost výskytu	
1	**téměř nemožná**	**výskyt rizika je předpokládán maximálně 1x za 20 a více let; (pravděpodobnost výskytu za rok je ≤ 5%)**
2	**výjimečně možná**	**výskyt rizika je předpokládán maximálně 1x v intervalu <6; 20) [58]let; (5%< pravděpodobnost výskytu za rok je ≤ 16,7%)**
3	**možná**	**výskyt rizika je předpokládán maximálně 1x v intervalu <3; 6) let; (5%< pravděpodobnost výskytu za rok je ≤ 33,3%)**
4	**pravděpodobná**	**výskyt rizika je předpokládán maximálně 1x v intervalu (1; 3) let; (33,3%< pravděpodobnost výskytu za rok je ≤ 100%)**
5	**jistá**	**výskyt rizika je předpokládán minimálně 1x za rok; (pravděpodobnost výskytu za rok = 100%)**

2. Kritéria pro hodnocení dopadu strategických rizik

Bodová hodnota	Dopad			Hodnota středu intervalu v Kč
1	**relativně malý**	**vliv na strategické cíle a funkce organizace je minimální**	**(0; 100> mil. Kč**	**50 mil. Kč**
2	**citelný**	**je způsobilý citelně ovlivnit strategické cíle a funkce organizace, je však bez významných dopadů na vztahy s klienty, dodavateli a dalšími zainteresovanými stranami**	**(100; 500> mil. Kč**	**300 mil. Kč**
3	**významný**	**ovlivní strategické cíle a funkce organizace a je způsobilý narušit vztahy s klienty, dodavateli a dalšími zainteresovanými stranami**	**(0,5; 1> mld. Kč**	**0,75 mld. Kč**
4	**velmi významný**	**podstatně ovlivní strategické cíle a funkce organizace, naruší vztahy s klienty, dodavateli a dalšími zainteresovanými stranami**	**(1; 2> mld. Kč**	**1,5 mld. Kč**
5	**nepřípustný**	**ztráta schopnosti organizace fungovat, uvalení nucené správy apod.**	**(2; ∞) mld. Kč**	**2 mld. Kč[59]**

[58] Symbol " <; " značí, že hodnota se ještě zahrnuje do intervalu, symbol „)" značí, že hodnota se již nezahrnuje do intervalu.

[59] Jedná se o „fiktivně" stanovený střed intervalu pro výpočet významnosti.

3. Kritéria pro hodnocení dopadu procesních rizik

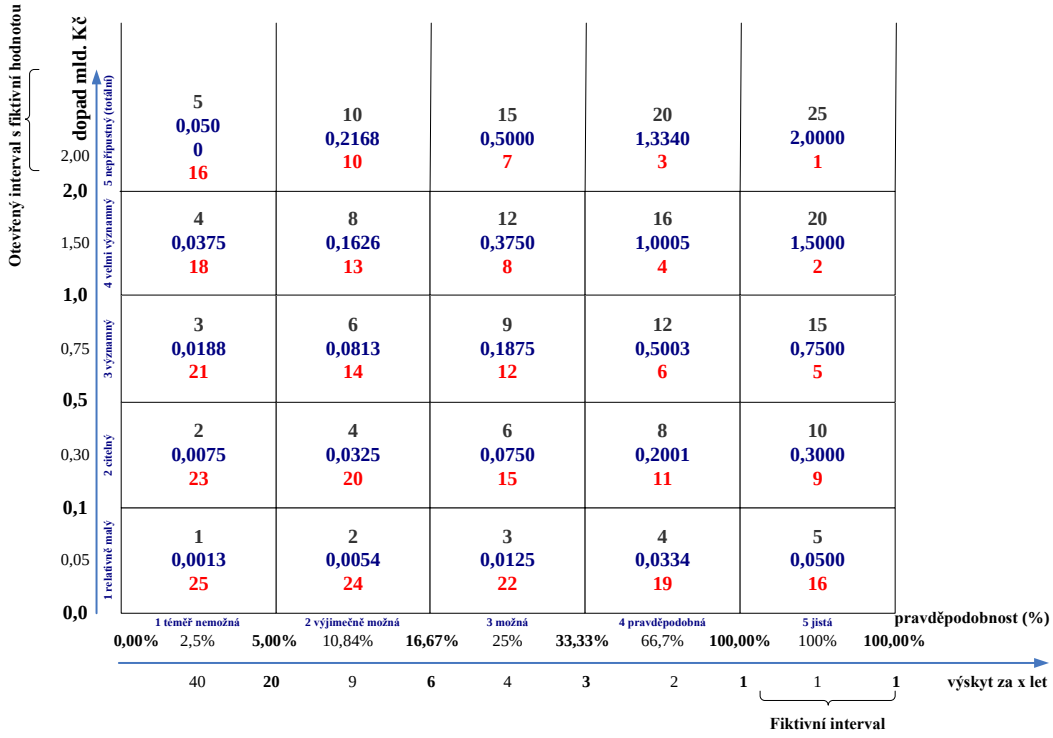
Bodová hodnota	Dopad			Hodnota středu intervalu v Kč
1	**relativně malý**	**vliv na vnitřní procesy je minimální a je zvládán v rámci běžného řízení**	**(0; 3> mil. Kč**	**1,5 mil. Kč**
2	**citelný**	**je způsobilý citelně ovlivnit vnitřní procesy, je však bez významných dopadů na cíle vnitřních procesů**	**(3; 15> mil. Kč**	**9 mil. Kč**
3	**významný**	**ovlivní vnitřní procesy a je způsobilý dílčím způsobem narušit cíle těchto procesů**	**(15; 30> mil. Kč**	**22,5 mil. Kč**
4	**velmi významný**	**podstatně ovlivní cíle vnitřních procesů, avšak jeho dopady jsou řešitelné v rámci prostředků provozního fondu či ostatních fondů organizace**	**(30; 65> mil. Kč**	**47,5 mil. Kč**
5	**nepřípustný**	**je na hranici ohrožení strategických cílů a bez včasné a adekvátní reakce je ohrozí a jeho dopady přesáhnou možnosti disponibilních prostředků provozního fondu či ostatních fondů organizace**	**(65; ∞) mil. Kč**	**65 mil. Kč[60]**

[61]

[60] Jedná se o „fiktivně“ stanovený střed intervalu pro výpočet významnosti.
[61] Zdroj: vlastní

PŘÍLOHA Č. 5: GRAFICKÉ ZNÁZORNĚNÍ KOMBINACEKRITÉRIÍ PRO HODNOCENÍ PRAVDĚPODOBNOSTI VÝSKYTU A ZÁVAŽNOSTI DOPADU RIZIK A JEJICH VÝZNAMNOSTI

Hodnotící matice strategických rizik



Legenda k uvedené matici:

Horní číslo v jednotlivých segmentech vyjadřuje hodnotu agregovaného rizika v daném segmentu v kvalitativních ukazatelích – v bodech, prostřední číslo vyjadřuje hodnotu agregovaného rizika v daném segmentu ve finančním vyjádření (mld. Kč.), dolní číslo vyjadřuje pořadí významnosti jednotlivých segmentů od nejvýznamnějších k nejméně významným ve vazbě na finanční hodnotu významnosti rizika.

Otevřený interval má spodní hranici dopadu 2 mld. Kč, přičemž horní hranice neexistuje. Střední hodnota intervalu je fiktivně oceněna 2 mld. Kč.

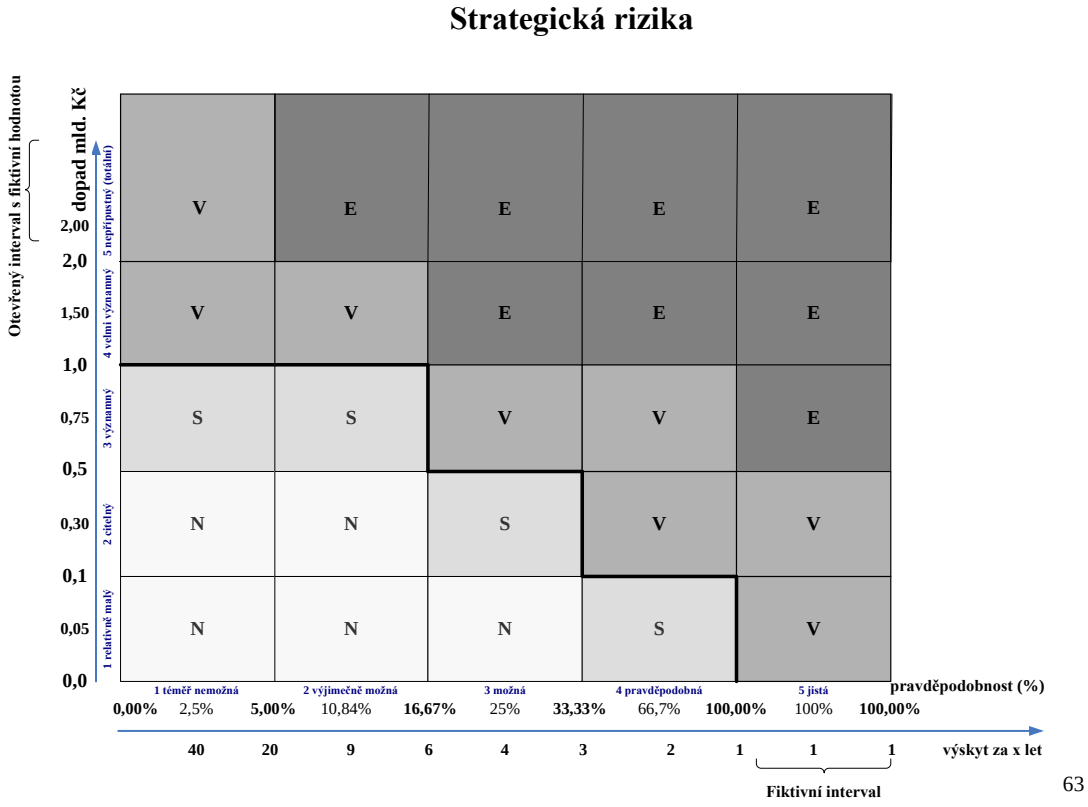
Fiktivní interval má dolní i horní hranici pravděpodobnosti ohodnocenu pravděpodobnost = 1, jedná se o interval s minimálním výskytem rizikové události jednou za rok. Četnost se v tomto intervalu promítá do závažnosti dopadu.

Hodnotící matice procesních rizik

62

[62] Zdroj: vlastní

PŘÍLOHA Č. 6: HODNOTY PRAVDĚPODOBNOSTI VÝSKYTU A ZÁVAŽNOSTI DOPADU RIZIK SPADAJÍCÍCH DI JEDNOTLIVÝCH STUPŇŮ VÝZNAMNOSTI



63

Legenda:

Stupeň významnosti rizika – stupeň významnosti rizika viz čl. 10. (N – nízká; S – střední; V – vysoká; E – extrémní)

[63] Zdroj: vlastní

PŘÍLOHA Č. 7: VZOR PLÁNU ZVLÁDÁNÍ RIZIK

PLÁN ZVLÁDÁNÍ RIZIK									
Název rizik	Skupina rizik	Vlastník rizika	Opatření ke zvládání rizika	Odpovědnost za realizaci jednotlivých opatření	Termín realizace opatření	Kritéria plnění opatření	Požadavky na zdroje	Stupeň významnosti zbytkového rizika	Požadavky na monitoring a reporting

[64]

Legenda:

Skupina rizik *– viz čl. 13. 1. označení skupiny rizik podle členění rizik uvedené v článku 6. 3. a navazujících klasifikací úseků a samostatných odborů organizace vycházejících z jejich podmínek.*
Stupeň významnosti zbytkového rizika - *viz čl. 10. (N – nízká; S – střední; V – vysoká; E – extrémní).*

[64] Zdroj: vlastní

PŘÍLOHA Č. 8: VZOR EVIDENČNÍHO LISTU RIZIKA

EVIDENČNÍ LIST RIZIKA		
Název rizika		
Skupina rizika		
Útvar		
Proces, činnost, aktivum		
Vlastník rizika		
Mechanismus působení rizika		
Rizikové faktory		
Příčiny rizika	hlavní	
	vedlejší	
Potenciální dopady	na strategické cíle	
	na procesní cíle	
	ostatní	
Vazby na další útvary, procesy, činnosti nebo aktiva		
Stávající řídící a kontrolní mechanizmy		

Významnost rizika

brutto riziko				zbytkové riziko					předpokládané cíl. hodnoty rizika				
P	**D**	**V**	**SV**	**P**	**D**	**V**	**SV**	**ZSV[1]**	**P**	**D**	**V**	**SV**	**ZSV[2]**
v bodech				v bodech					v bodech				
%	Kč	Kč		%	Kč	Kč			%	Kč	Kč		

Legenda:
***Skupina rizik** – viz čl. 13. 1 označení skupiny rizik podle členění rizik uvedené v článku 6. 3 a navazujících klasifikací úseků a samostatných odborů organizace vycházejících z jejich podmínek.*
***Proces, činnost, aktivum** – viz čl. 13. 1. označení procesu činnosti nebo aktiva, při jehož analýze bylo riziko identifikováno.*

Významnost rizika *– viz čl. 6. 2. V=P×D (významnost rizika „V“ je dána součinem pravděpodobnosti výskytu rizika „P“ a intenzitou potenciálních následků rizika „D“).*
Brutto riziko *– viz poznámka: v č. 9.2.3. ze které vyplývá, že pokud lze adekvátními prostředky efektivně získat informace umožňující objektivně zhodnotit brutto hodnoty rizika, je účelné tyto hodnoty určovat.*
SV *– stupeň významnosti zbytkového rizika viz čl. 10. (N – nízká; S – střední; V – vysoká; E – extrémní)*
ZSV[1] *– snížení stupně významnosti brutto rizika vlivem působení stávajících řídících a kontrolních mechanismů*
ZSV[2]*očekávané snížení stupně významnosti zbytkového rizika vlivem přijímaných opatření.*

Přijatá opatření[65]				
popis opatření	útvar	odpovědná osoba (funkce)	termín	kritéria plnění
Monitoring rizika				
Ostatní relevantní informace[66]				
Přílohy				

67

[65] V případě, že budou stanoveny, se uvádějí dílčí opatření a dílčí termíny plnění.
[66] Např. o předchozí expozici rizika.
[67] Zdroj: vlastní

PŘÍLOHA Č. 9: VZOR KATALOGU RIZIK

KATALOG RIZIK																					
Skupina rizik	Název rizika	Útvar	Proces, činnost, aktivum	Potenciální dopady			Významnost rizika								Priorita	Přijatá opatření	Významnost rizika			
				na strategické cíle	na procesní cíle	ostatní	brutto riziko				Zbytkové riziko						předpok. cílové hodnoty rizika			
							P	D	V	SV	P	D	V	SV			P	D	V	SV
							v bodech				v bodech						v bodech			
							%	Kč	Kč		%	Kč	Kč				%	Kč	Kč	
							v bodech				v bodech						v bodech			
							%	Kč	Kč		%	Kč	Kč				%	Kč	Kč	

[68]

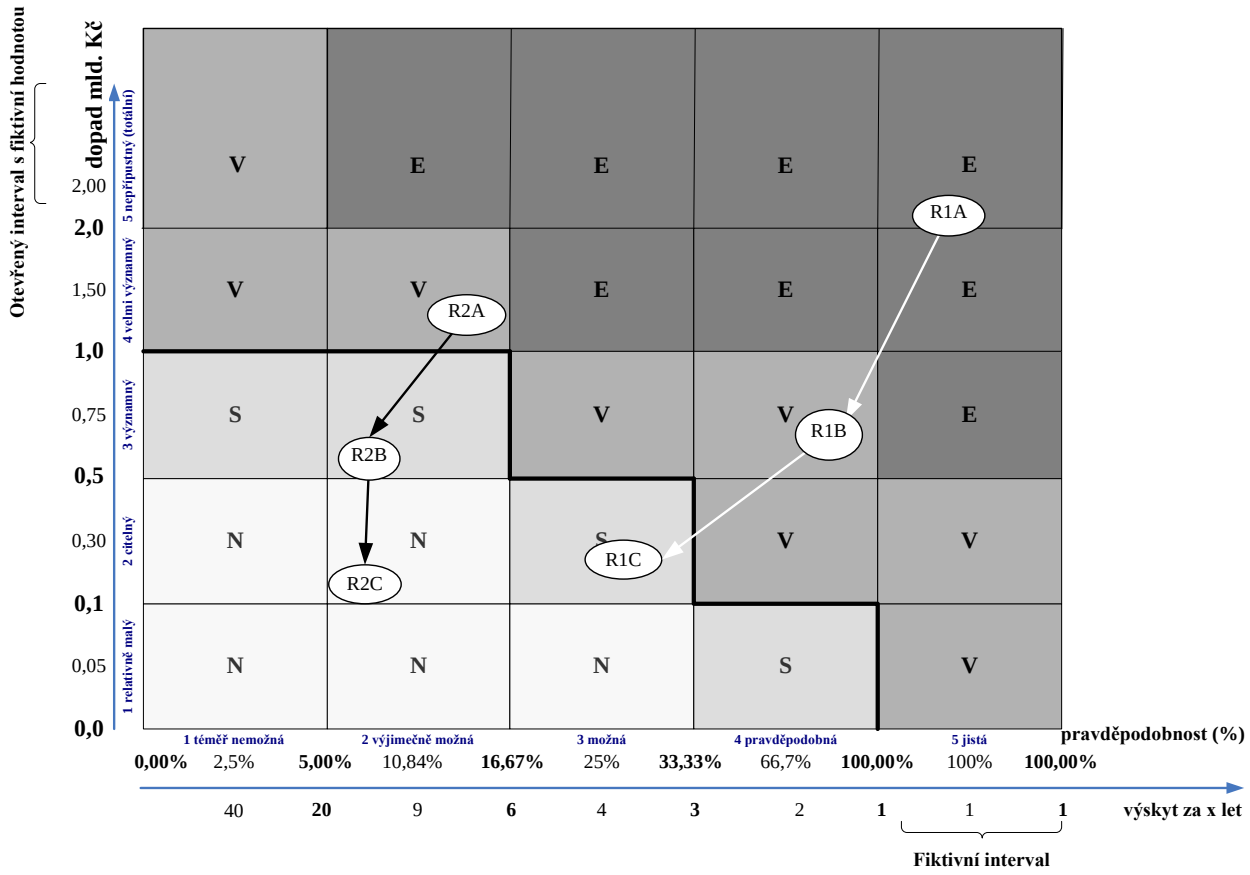
Legenda:

Skupina rizik *– viz čl. 13. 1. označení skupiny rizik podle členění rizik uvedené v článku 6. 3. a navazujících klasifikací úseků a samostatných odborů* organizace *vycházejících z jejich podmínek.*
Proces, činnost, aktivum *– viz čl. 13. 1. označení procesu činnosti nebo aktiva, při jehož analýze bylo riziko identifikováno.*
Významnost rizika *– viz čl. 6. 2. V=P×D (významnost rizika „V" je dána součinem pravděpodobnosti výskytu rizika „P" a intenzitou potenciálních následků rizika „D").*
Brutto riziko *– viz poznámka: v č. 9.2.3.: pokud lze adekvátními prostředky efektivně získat informace umožňující objektivně zhodnotit brutto hodnoty rizika, je účelné tyto hodnoty určovat.*
SV *– stupeň významnosti zbytkového rizika viz. čl. 10. (N – nízká; S – střední; V – vysoká; E – extrémní).*

[68] Zdroj: Vlastní

PŘÍLOHA Č. 10 MAPA RIZIK

69



Legenda:

R1A *- významnost brutto hodnota rizika R1, tj. bez zohlednění působení stávajících řídících a kontrolních mechanizmů.*
R1B *- významnost zbytkového rizika, tj. po zhodnocení stávajících řídících a kontrolních mechanizmů.*
R1C *- předpokládaný cílový stav po realizaci opatření přijatých k optimalizaci rizika - významnost zbylého rizika.*
V daném případě stávající řídící a kontrolní mechanizmy způsobily přesun rizika R1 z pásma extrémní významnosti do pásma vysoké významnosti, což je však stále nedostatečné a byla zvolena opatření, jejichž cílem je snížit významnost rizika na hodnoty pásma střední významnosti.
Význam hodnot u rizika R2 je stejný. V daném případě však stávající řídící a kontrolní mechanizmy zajišťují přesun brutto hodnoty rizika z pásma vysoké významnosti do pásma střední významnosti. Realizace dalších opatření k optimalizaci rizika závisí na zhodnocení nákladů na opatření k přesunu rizika do pásma nízké významnosti, v porovnání s přínosy z toho plynoucími, a na zhodnocení, zda při omezených disponibilních zdrojích na zvládání rizik neexistují rizika s vyšší prioritou.
Pozn.: Pro přehlednost jsou v mapě rizik uvedena pouze dvě rizika.

---

[69] Zdroj: vlastní