



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

ÚSTAV SOUDNÍHO INŽENÝRSTVÍ

INSTITUTE OF FORENSIC ENGINEERING

**RIZIKA SPOJENÁ S ŘÍZENÍM FINANČNÍCH PROCESŮ V
CENTRECH SDÍLENÝCH SLUŽEB V MEZINÁRODNÍ
SPOLEČNOSTI**

RISKS ASSOCIATED WITH MANAGEMENT OF FINANCIAL PROCESSES IN SHARED SERVICES
CENTERS IN INTERNATIONAL COMPANY

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

AUTOR PRÁCE

AUTHOR

Bc. Jan Šimčík

VEDOUCÍ PRÁCE

SUPERVISOR

Ing. Marie Pavláková Dočekalová, Ph.D.

BRNO 2016

Zadání diplomové práce

Ústav: Ústav soudního inženýrství
Student: **Bc. Jan Šimčík**
Studijní program: Rizikové inženýrství
Studijní obor: Řízení rizik firem a institucí
Vedoucí práce: **Ing. Marie Pavláková Dočekalová, Ph.D.**
Akademický rok: 2015/16

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách a se Studijním a zkušebním řádem VUT v Brně určuje následující téma diplomové práce:

Rizika spojená s řízením finančních procesů v centrech sdílených služeb v mezinárodní společnosti

Stručná charakteristika problematiky úkolu:

V závěrečné práci bude zpracována analýza procesů ve finančním centru sdílených služeb v konkrétní mezinárodní společnosti. Vyhodnocena rizika spojená s řízením těchto procesů a navržena opatření minimalizující identifikovaná rizika.

Cíle diplomové práce:

Cílem diplomové práce je analýza procesů ve finančním centru sdílených služeb v konkrétní mezinárodní společnosti. Na základě provedené analýzy a vyhodnocení rizik spojených s řízením těchto procesů budou navržena opatření minimalizující identifikovaná rizika.

Seznam literatury:

SMEJKAL, Vladimír a Karel RAIS. Řízení rizik ve firmách a jiných organizacích. 4., aktualiz. a rozš. vyd. Praha: Grada, 2013, 483 s. Expert (Grada). ISBN 978-80-247-4644-9.

FIŠER, Roman. Procesní řízení pro manažery: jak zařídit, aby lidé věděli, chtěli, uměli i mohli. 1. vyd. Praha: Grada, 2014, 173 s. Manažer. ISBN 978-80-247-5038-5.

VLACHÝ, Jan. Řízení finančních rizik. Praha: Vysoká škola finanční a správní, c2006, 256 s. ISBN 80-86754-56-1.

JÍLEK, Josef. Finanční rizika. 1. vyd. Praha: Grada, 2000, 635 s. Finance (Grada). ISBN 80-7169-5-9-3.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2015/16

V Brně, dne

L. S.

doc. Ing. Aleš Vémola, Ph.D.
ředitel

ABSTRAKT

Práce se zabývá řízením rizik v centru sdílených služeb v mezinárodní společnosti, konkrétně ve společnosti Zebra Technologies CZ s.r.o., a jejím finančním oddělení. V práci se analyzují a vyhodnocují rizika, která se v tomto sektoru vyskytují. V první části práce se řeší pojmy spjaté s procesním managementem, prostředím firmy, riziky, managementem rizik a centry sdílených služeb. V druhé části je provedena analýza procesů, prostředí a následná identifikace, analýza a hodnocení všech rizik. Závěrem je provedeno vyhodnocení rizik a navržena taková opatření, která identifikovaná rizika a jejich dopad minimalizují.

ABSTRACT

The thesis deals with management of risks in finance shared service in international company Zebra Technologies CZ s.r.o. The thesis analyses and evaluates all risks which are common in this finance shared service. In the first part the thesis deals with important concepts which are linked with process management, business environment, risks, risk management and finance shared services. It is followed by analysis of processes then by environment and analysis of all known risks. The last part is made of evaluation of all identified risks and there are suggestions which could eliminate most of them.

KLÍČOVÁ SLOVA

Rizika, risk management, finance, procesy, řízení, analýza, centrum sdílených služeb.

KEYWORDS

Risks, risk management, finance, processes, management, analysis, shared service center.

BIBLIOGRAFICKÁ CITACE

ŠIMČÍK, J. Rizika spojená s řízením finančních procesů v centrech sdílených služeb v mezinárodní společnosti. Brno: Vysoké učení technické v Brně, Ústav soudního inženýrství, 2016. 90 s. Vedoucí diplomové práce Ing. Marie Pavláková Dočekalová, Ph.D..

ČESTNÉ PROHLÁŠENÍ

Prohlašuji, že předložená diplomová práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 27. května 2016

PODĚKOVÁNÍ

Touto cestou bych velmi rád poděkoval mé vedoucí diplomové práce Ing. Marii Pavlákové Dočekalové, Ph.D. za cenné rady a vstřícný a ochotný přístup. Velké díky patří i Ing. Ivovi Knoflíčkovi za poskytnuté informace a čas.

OBSAH

ÚVOD	8
1 CÍLE PRÁCE, METODY A POSTUPY ZPRACOVÁNÍ.....	9
1.1 Cíl práce	9
1.2 Metody a postupy zpracování	9
2 TEORETICKÁ VÝCHODISKA.....	10
2.1 Procesní management.....	10
2.1.1 Proces	10
2.1.2 Procesní řízení	10
2.1.3 Rozdělení procesů	11
2.1.4 Ovlivnitelnost procesního řízení	12
2.2 Prostředí firmy	14
2.2.1 Vnější prostředí	14
2.2.2 Vnitřní prostředí	15
2.2.3 SWOT analýza	16
2.3 Rizika	17
2.3.1 Chápání a přístup k riziku	18
2.3.2 Klasifikace rizik	18
2.3.3 Identifikace rizik.....	21
2.3.4 Metody hodnocení rizik.....	21
2.3.5 Analýza rizik	24
2.3.6 Nástroje pro snižování rizik	25
2.4 Management rizik.....	26
2.5 Centra sdílených služeb (Shared Service Centers).....	28
2.5.1 Rozdíl mezi SSC a outsourcingem.....	28

2.5.2	Outsourcing	29
2.5.3	Insourcing.....	30
3	ANALÝZA SOUČASNÉHO STAVU.....	31
3.1	Společnost Zebra Technologies	31
3.1.1	Historie	32
3.1.2	SSC v Brně	33
3.2	Procesy ve Finance Shared Services (FSS).....	34
3.2.1	Accounts Receivable (AR).....	35
3.2.2	Accounts Payable (AP)	36
3.2.3	General Ledger (GL).....	37
3.2.4	Finance Analysis (FA).....	38
3.2.5	Payroll	38
3.2.6	Treasury.....	39
3.3	Analýza vnějšího prostředí.....	40
3.3.1	PEST analýza	40
3.4	Analýza vnitřního prostředí.....	42
3.4.1	7S faktorů firmy McKinsey.....	42
3.5	SWOT analýza	44
3.6	Identifikace rizik	47
3.6.1	Obecná rizika.....	47
3.6.2	Vnější rizika	48
3.6.3	Vnitřní rizika	48
3.6.4	Procesní rizika	50
3.7	Analýza a hodnocení rizik.....	53
3.7.1	Skórovací metoda s mapou rizik	53

3.7.2	Analýza příčin a důsledků	56
4	VLASTNÍ NÁVRHY	63
4.1	Bezvýznamná rizika	64
4.2	Běžná rizika.....	65
4.3	Významná rizika	65
4.4	Kritická rizika.....	68
4.4.1	Návrh na standardizaci procesů.....	68
4.4.2	Návrh nového informačního systému.....	69
4.4.3	Návrh motivačního programu pro zaměstnance.....	71
4.5	Přínos návrhů	75
	ZÁVĚR	77
	SEZNAM POUŽITÉ LITERATURY	79
	SEZNAM POUŽITÝCH ZKRATEK.....	85
	SEZNAM OBRÁZKŮ	87
	SEZNAM TABULEK.....	88
	SEZNAM GRAFŮ	89
	SEZNAM PŘÍLOH.....	90

ÚVOD

Téma diplomové práce jsem si zvolil záměrně z několika důvodů. Jednak kvůli významu samotných rizik, které v celé dnešní společnosti hrají velice důležitou roli a také kvůli rychlému růstu celého segmentu sdílených služeb v České republice. Dále jsem spojil svůj obor zájmu financí i svou současnou pracovní pozici právě ve středu sdílených finančních služeb v mezinárodní společnosti Zebra Technologies.

V diplomové práci skloubím poznatky jak získané během studia, tak i praktické poznatky získané během svého zaměstnání právě ve společnosti Zebra Technologies.

Zebra Technologies (bývalá Motorola Solutions) je technologická firma, která sídlí v Technologickém parku v Brně a zaměstnává přes 400 lidí, včetně studentů Vysokého Učení Technického. V této práci budu konkrétně rozebírat sdílené centrum finančních služeb, které poskytuje služby pro celou společnost, která působí ve více než 120 zemích světa.

Téma je pro mě aktuální hlavně z toho důvodu, že si mnoho firem neuvědomuje závažnost řízení rizik a jejich dopady, včetně finančního centra sdílených služeb v Brně, a proto bych rád identifikoval, analyzoval a ohodnotil rizika a navrhl všechna možná opatření, která by mohla pro společnost Zebra Technologies ale i jiná střediska finančních služeb znamenat krok vpřed.

1 CÍLE PRÁCE, METODY A POSTUPY ZPRACOVÁNÍ

1.1 Cíl práce

Hlavním cílem práce je identifikovat, analyzovat a ohodnotit rizika, která vyplývají z řízení procesů ve finančním centru sdílených služeb v mezinárodní společnosti Zebra Technologies. Výstupem bude návrh opatření, která budou tato rizika minimalizovat.

1.2 Metody a postupy zpracování

V teoretické části se budu zabývat procesním managementem, prostředím firmy, riziky, managementem rizik a centry sdílených služeb. Poznatky získané z teoretické části a z mé osobní praxe ve firmě Zebra Technologies CZ s.r.o., budou aplikovány do analytické části.

K úspěšnému dosažení výstupu bude zapotřebí provést analýzu společnosti a finančního střediska sdílených služeb. Následovat bude analýza procesů. Procesy vyplývají z jednotlivých oddělení. Analýza vnějšího prostředí bude provedena pomocí PEST analýzy, analýza vnitřního prostředí pomocí rozboru faktorů 7S. K výstupu analýz firemního prostředí poslouží SWOT analýza.

V další části identifikuji rizika a provedu analýzu a hodnocení rizik pomocí skórovací metody s mapou rizik a u vybraných rizik provedu analýzu příčin a důsledků.

V poslední části navrhnu vlastní řešení, která by měla analyzovaná a hodnocená rizika minimalizovat. Budu vycházet z poznatků získaných z teoretické části, firemní praxe, provedených analýz a pravidelných konzultací s ředitelem finančního centra sdílených služeb.

2 TEORETICKÁ VÝCHODISKA

Před samotnou analýzou a následným vyhodnocením rizik je nezbytné podrobně vymezit a interpretovat pojmy, které budou použity v dalších částech této práce.

2.1 Procesní management

2.1.1 Proces

Existuje mnoho interpretací k pojmu proces. Grasseová et al. (2008, s. 7) proces chápe jako „sled navazujících činností popisujících tok práce (postup tvorby přidané hodnoty) postupující od jednoho pracovníka ke druhému (v případě složitých procesů od jednoho útvaru do druhého), poskytující měřitelnou službu nebo výrobek internímu nebo externímu zákazníkovi za předpokladu přeměny vstupů na výstupy a využívání zdrojů.“

Petráčková a Kraus (1995, s. 620) definují proces jako „zákonitý, postupně na sebe navazující a vnitřně spojený. Vzájemné spojení změny jevů, věcí a systémů.“

Řepa (2007, s. 15) říká, že proces je „souhrn činností transformujících souhrn vstupů na souhrn výstupů (zboží nebo služeb) pro jiné lidi nebo procesy, používající k tomu lidi nebo nástroje.“

Z osobního hlediska bych proces interpretoval jako určitou činnost, která vede k určitému výstupu. Tudíž jakákoliv činnost vedoucí k určitému výstupu může být chápána jako proces.

2.1.2 Procesní řízení

V každé organizaci nebo společnosti se na denní bázi setkáváme s procesy a jejich řízením. Každý jednotlivec ve firmě – ať už majitel, manažer či zaměstnanec se buď přímo, nebo nepřímo podílí na určitém procesu (či více procesech), který se v dané firmě odehrává. Dle Fišera (2014, s. 21) by se měl člověk v řízení procesů řídit hlavně zdravým rozumem a měl by si položit tři základní otázky: co by mělo být uděláno, jak se to udělá a kdo to udělá.

Za opravdový rozvoj procesního řízení se dají označit devadesátá léta minulého století, kdy Hammer a Champy (2000, s. 24) definovali organizaci, která je ovlivňována třemi silami: customers (zákazníky), competition (konkurencí) a change (změnou). Dali tedy vzniknout dnes už charakteristickým „3C“, na které by měla každá firma umět reagovat.

V dnešní době jsou známy tři hlavní přístupy k řízení procesů v organizaci:

Funkční přístup – nejstarší, avšak stále nejrozšířenější přístup, který definoval v roce 1776 Adam Smith, se zaměřuje na jednoduchou dělbu práce mezi jednotlivé pracovníky. Firmu to vede k vytvoření organizačních jednotek na základě dovedností a každá má na starosti určitou část procesu. Tento přístup se však jeví jako ne příliš efektivní z důvodu kladení vysokého důrazu na dílčí procesy místo kladení důrazu na celkový proces (ManagementMania.com, 2014). Navíc jak dodává Fišer (2014, s. 38), problémy se obvykle řeší zásahy do funkcí v organizační struktuře organizace a vytvářejí tak nová pracovní místa, místo toho, aby se řešil skutečný zárodek problému.

Procesní přístup – na rozdíl od funkčního přístupu je zaměřen více horizontálně, tedy na samotné procesy. Rozvoj zaznamenal v 90. letech minulého století, které se dají charakterizovat masivním nástupem informačních a komunikačních technologií, díky nimž bylo možno provést rozsáhlé změny dosavadních procesů. (Grasseová et al., 2008, s. 40)

Projektový přístup – je založen na principu jedinečnosti. To znamená, že se využívá u procesů, které se většinou neopakují a své optimální řešení nalézají často až v průběhu realizace projektu. (ManagementMania.com, 2014)

2.1.3 Rozdělení procesů

Samotné procesy jsou a byly nezbytnou součástí fungování každé firmy. Procesy Grasseová (2008) dělí podle důležitosti a účelu, podle struktury a podle doby existence.

Dle důležitosti a účelu jsou procesy děleny na hlavní, řídící a podpůrné.

- Hlavní procesy jsou nejdůležitější a vytváří přidanou hodnotu organizace (výrobek, služba). Dá se tedy konstatovat, že bez hlavního procesu nemůže organizace existovat.

- Řídící procesy mohou být identifikovány jako procesy, které mají za úkol podporovat procesy hlavní a jsou to veškeré manažerské procesy napomáhající chodu organizace.
- Podpůrné procesy zabezpečují samotný chod organizace. V praxi to mohou být personální, účetní a provozní aktivity.

Dle struktury jsou procesy děleny na datové a znalostní.

- Datové procesy mají jasně strukturované pořadí, které se nemění. Typické u výrobního programu, kde se proces na výrobě daného produktu nemění.
- Znalostní procesy jsou opakem k datovým procesům, tudíž struktura pořadí se může měnit a může se jednat např. o tvůrčí postupy.

Dle doby existence jsou procesy děleny na trvalé a dočasné, kde je u dočasných procesů charakteristický vymezený čas trvání procesu. (Grasseová, 2008)

2.1.4 Ovlivnitelnost procesního řízení

Procesní řízení je ovlivnitelné několika faktory. Při změně vstupů se musí změna nutně promítnout i u některého výstupu. Fišer (2014, s. 38–44) uvádí, že úspěšnost procesního řízení závisí na organizační struktuře, kultuře uvnitř organizace a stylu řízení.

Organizační struktura – jak již bylo nastíněno v kapitole 2.1.2, většina organizací je dnes založena na funkčním přístupu řízení. Z toho vyplývá, že vznikají a zanikají pracovní pozice, aby vznikl, resp. zanikl řídicí nebo podpůrný proces místo toho, aby se problém řešil koncepčně skrze hlavní proces. Organizace si tak vytváří trh uvnitř sama sebe a soutěžícími na tomto trhu se stávají manažeři a pracovníci (kteří si vytvářejí vlastní image a uzavírají smlouvy mezi jednotlivými útvary) místo toho, aby organizace konkurovala na trhu vnějším. Hlavní nevýhoda funkčního řízení je tedy shledávána v tom, že jakékoliv zlepšení procesu automaticky neznamena lepší výstup pro organizaci jako celek, nýbrž pro jednotlivce. Naopak procesní řízení je založeno na potřebách organizace jakožto celku, jelikož jsou zdokonalovány a měněny vstupy u samotných procesů a ne pracovní pozice jednotlivců.

Kultura organizace – Armstrong (2007, s. 257) definuje firemní kulturu jako „soustavu sdíleného přesvědčení, postojů, domněnek, norem a hodnot existujících

v organizaci. Podílí se na formování způsobu jednání a vzájemného působení lidí a výrazně ovlivňuje způsoby vykonávání práce, zejména v podmínkách, kde neexistují přímé instrukce.“ Vliv firemní kultury na procesní řízení tak může být považován za zásadní, vzhledem ke všem aspektům, které Armstrong zmiňuje.

Styl řízení – poslední faktor, který uvádí Fišer (2014, s. 42), a který ovlivňuje procesní řízení, je styl, kterým je organizace řízena. Jedná se o manažerský styl řízení vůči podřízeným. Na světě existuje mnoho manažerů, ať už dobrých či špatných, každý má svůj jedinečný styl řízení a osobně jsem toho názoru, že nemůžeme nikdy říct, který styl je nejvhodnější. Každému vyhovuje něco jiného a pro každou organizaci je třeba specifických požadavků. Pro úplnost však uvedu čtyři klasické styly řízení dle Likerta. (Chovani.eu, b.r.)

Autoritativní styl

Nadřízený rozhoduje o všem (co spadá pod jeho pravomoc), komunikace probíhá vertikálně směrem k přímému podřízenému. Názory ostatních jsou většinou autoritativnímu manažerovi lhostejné.

Benevolentní styl

Manažer naslouchá podřízeným, nicméně poslední slovo má vždy on. S podřízenými se snaží jednat jako s partnery a zároveň se je snaží motivovat.

Konzultativní styl

Svá rozhodnutí činí na základě vyslechnutí podřízených. Stále však platí, že má poslední slovo. Motivuje formou odměn, tresty spíše nepoužívá.

Participativní styl

Do řízení se přímo zapojují podřízení a rozhoduje se tak spíše skupinově. U tohoto stylu převládá maximální důvěra ze strany manažera. (Chovani.eu, 2015).

Všechny tři zmíněné veličiny (struktura, kultura a styl) se navzájem ovlivňují. Z hlediska ovlivnitelnosti procesního řízení se tak dá konstatovat, že díky dobrému pochopení těchto veličin může být procesní řízení v organizaci lépe optimalizováno. (Fišer, 2014, s. 45)



Obr. č. 1: Trojúhelník SSK (Zdroj: Fišer, 2014)

Pro lepší představu, Obr. č. 1 znázorňuje propojenost struktury, stylu a kultury v závislosti na ovlivnitelnosti procesního řízení.

2.2 Prostředí firmy

Pro úspěšné řízení firmy a řízení rizik firmy, je zapotřebí znát prostředí, ve kterém se firma nachází.

2.2.1 Vnější prostředí

Mallya (2007, s. 41–48) dělí vnější prostředí na mezinárodní, národní (domácí) a oborové (konkurenční).

K analýze vnějšího prostředí z hlediska *domácího* se nejčastěji používá PEST analýza (někdy také jako PESTLE, PESTE, STEP, STEPE, SLEPTE). Zjednodušeně řečeno se jedná o analýzu politických (právních), ekonomických, sociálních a technologických faktorů, které působí na podnik. (Vochozka, 2012, s. 344)

Z hlediska *konkurenčního* prostředí připadá v úvahu Porterův pětifaktorový model konkurenčního prostředí. Ten určuje konkurenční rivalitu na trhu, která je závislá působením potenciálních konkurentů, dodavatelů odběratelů a možných substitutů, jak znázorňuje Obr. č. 2. (Střelec, 2012)



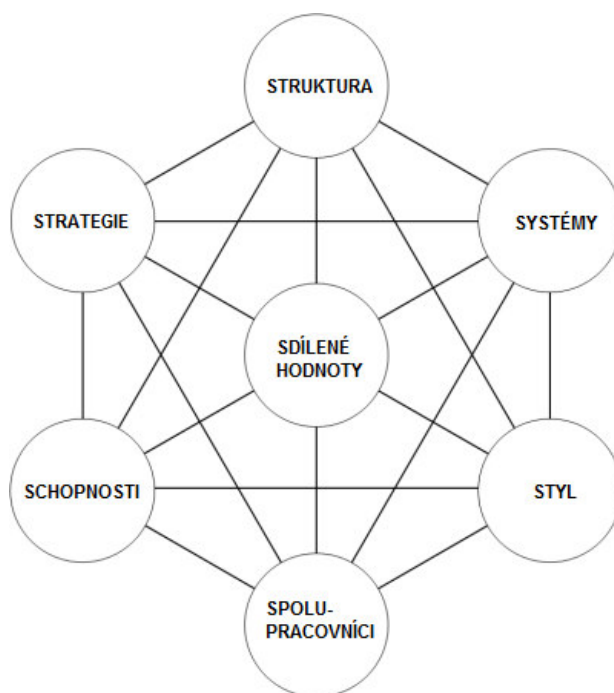
Obr. č. 2: Porterův model pěti sil (Zdroj: Mallya, 2007)

Další užívanou metodou je např. BCG matice, která ilustruje tempo růstu trhu v závislosti na relativním tržním podílu firmy. (Čevelová, 2010, online)

2.2.2 Vnitřní prostředí

Podstatou analýzy vnitřního prostředí je, aby firma poznala své slabé a silné stránky. Jak uvádí Mallya (2007, s. 53), je nezbytné nejprve analyzovat vnitřní faktory firmy. Mezi ně patří faktory finanční, rozpočtové, marketingové, distribuční, výrobní, technické a podnikových a pracovních zdrojů.

Mezi nejznámější model analýzy vnitřních zdrojů patří model faktorů 7S firmy McKinsey, které Smejkal a Rais (2013, s. 39) považují za kritické faktory úspěchu firmy.



Obr. č. 3: Rámec faktorů 7S firmy McKinsey (Zdroj: Smejkal a Rais, 2013)

Jak napovídá Obr. č. 3, za kritické faktory úspěchu firmy jsou považovány sdílené hodnoty firmy, spolupracovníci, schopnosti, strategie firmy, organizační struktura, informační systémy a styl řízení firmy.

Mezi další modely analýzy vnitřního prostředí se dá zahrnout např. kauzální model Burkeho a Litwina, Weisbordův model šesti kategorií, programování vysoké výkonnosti, model souladu/shody, model diagnózy chování jedince a skupiny, model analýzy prostředí, Leavitův model a Tichyův technicko-politicko-kulturní koncept. (Mallya, 2007, s. 73–83)

2.2.3 SWOT analýza

Stojí na pomezí vnitřního a vnějšího prostředí. Podstatou je analyzovat silné a slabé stránky a příležitosti a hrozby podniku. První by se měly analyzovat OT (Opportunities, Threats), které vyplývají z vnějšího prostředí a následně SW (Strenghts, Weaknesses), vyplívající z vnitřního prostředí firmy.

Silné stránky (<i>strengths</i>) zde se zaznamenávají skutečnosti, které přinášejí výhody jak zákazníkům, tak firmě	Slabé stránky (<i>weaknesses</i>) zde se zaznamenávají ty věci, které firma nedělá dobře, nebo ty, ve kterých si ostatní firmy vedou lépe
Příležitosti (<i>opportunities</i>) zde se zaznamenávají ty skutečnosti, které mohou zvýšit poptávku nebo mohou lépe uspokojit zákazníky a přinést firmě úspěch	Hrozby (<i>threats</i>) zde se zaznamenávají ty skutečnosti, trendy, události, které mohou snížit poptávku nebo zapříčinit nespokojenost zákazníků

Obr. č. 4: Tabulka SWOT analýzy (Zdroj: Jakubíková, 2008)

SWOT analýza často identifikuje to, jak se podnik dokáže vyrovnávat se změnami, nastávajícími v prostředí. (Jakubíková, 2008, s. 103)

2.3 Rizika

Jelikož tato práce pojednává o identifikaci, analýze a vyhodnocení rizik, je zapotřebí, aby byly definovány veškeré pojmy spjaté právě s riziky.

Po tom, co byl vymezen proces, je logické, že z každého procesu musí plynout alespoň jedno riziko.

Fotr a Hnilica (2014, s. 17) o riziku tvrdí, že je to možnost vzniku ztráty a výskytu takových událostí, které nepříznivě ovlivní dosažení nastavených cílů.

Smejkal a Rais (2013, s. 90) říkají, že riziko navazuje na filozofické kategorie nutnosti a nahodilosti a s rizikem je spojen pojem neurčitosti výsledku a toho, že aspoň jeden z možných výsledků bude nežádoucí. Následně riziko konkretizují jako „situaci, v níž existuje možnost nepříznivé odchylky od žádoucího výsledku, ve který doufáme nebo ho očekáváme.“

Tichý (2006, s. 16) doplňuje, že je vhodné si povšimnout rozdílů mezi definicemi. Za rizika považuje nebezpečí, zdroje nebezpečí, pravděpodobnost, objekty vystavené nebezpečí a časových změn veličin. Z uvedených kategorií mohu uvést např. rizika: „nebezpečí vzniku nějaké újmy, zdroj takového nebezpečí (přírodní jevy, lidé nebo zvířata a činnosti), pravděpodobnost vzniku příslušné újmy, osoba vystavená újmě a odchylky od očekávaných ztrát.“

2.3.1 Chápání a přístup k riziku

Když se řekne riziko, mnoho lidí si představí pouze skutečnost, kdy se při naplnění skutkových podstat stane něco špatného. To vyplývá i z uvedených definic. Ovšem nemusí tomu tak vždy být. Určitá rizika s sebou můžou přinášet i pozitivní dopad.

Dle Smejkal a Raise (2013) se dá konstatovat, že existují tři přístupy k riziku:

Averze k riziku – manažer nevyhledává a spíše se vyhýbá všem příležitostem, které se pro něj jeví jako rizikové.

Sklon k riziku – manažer se nebojí vstupovat do velkých rizik. Vstupuje do nich za vidinou např. vysokého zisku. Zároveň počítá s tím, že existuje obrovské riziko.

Neutrální postoj k riziku – manažer je spíše realista. Jde do určitého rizika s tím, že ví, co může nastat a hledá kompromis a rovnováhu.

2.3.2 Klasifikace rizik

Rizika jsou často členěna dle mnoha kritérií, a jak říká Tichý (2006, s. 17) zatím neexistuje žádný ucelený systém členění rizik.

Ze základního hlediska jsou rizika dělena na:

Hmotná a nehmotná – hmotná rizika jsou představována těmi, které se dají změřit. Nehmotná rizika souvisejí s duševní činností a někdy jsou označována jako psychologická rizika. (Tichý, 2006, s. 18)

Podnikatelská a čistá – u podnikatelských rizik se dá říci, že mohou být chápány jak pozitivně tak i negativně, tudíž vzniká i šance na úspěch. Naproti tomu rizika čistá jsou spojována jen s negativními vlastnostmi. (Fotr a Hnilica, 2014, s. 20)

Systematická a nesystematická – systematická rizika mohou postihovat např. celé odvětví trhu a jsou vyvolána chováním odvětví jakožto celku, zatímco nesystematická rizika postihují pouze jeden subjekt, např. jednu organizaci a jsou vyvolána chováním dané organizace. (Business.center.cz, 2015)

Pojistitelná a nepojistitelná rizika – rizika se považují za pojistitelná pouze v případě, kdy splňují náležitosti: identifikovatelnost, náhodnost, musí být

kvantifikovatelné a matematicko-statisticky popsatelné a spravedlivé. (Tichý, 2006, s. 306)

Strategická a operační rizika – strategická rizika vyplývají ze strategického rozhodování organizace, kde se řeší otázka: co by mělo být uděláno, zatímco operační rizika vyplývají z operačního rozhodování a řeší otázky typu: jak by to mělo být uděláno. (Tichý, 2006, s. 18)

Vnitřní a vnější rizika – vnitřní rizika se týkají organizace uvnitř. Může jít např. o špatné vztahy na pracovišti či o šíření citlivých dat mezi zaměstnanci. Vnější rizika se mohou naopak týkat vztahů mezi dodavateli, odběrateli, konkurencí a záležitostmi, týkajícími se legality organizace. (Stavný, 2010)

Ovlivnitelná a neovlivnitelná rizika – u ovlivnitelných rizik je možnost působit na jejich příčiny a tak je ovlivňovat a snižovat. U neovlivnitelných rizik nejde nijak působit na jejich příčiny¹, mohou však být nastavena opatření, která budou minimalizovat jejich důsledky. (Fotr a Hnilica, 2014, s. 21)

Primární a sekundární rizika – sekundární rizika vznikají při eliminování primárních rizik. Ta mohou být všechna výše zmíněná. (ManagementMania.com, 2015)

Dle věcné náplně jsou rizika dělena na:

Technicko-technologická rizika – jsou spojená zejména s vývojem nových výrobků. Např. nedodržení technologického procesu.

Výrobní rizika – vzniká nejčastěji z důvodu omezenosti některého vstupu. Může chybět materiál, surovina, energie nebo pracovníci. Mohou být také narušeny dodavatelsko-odběratelské vztahy nebo se mohou porouchat stroje určené k výrobě.

Ekonomická rizika – jsou spjatá především s růstem nákladů, které ovlivňují hospodářský výsledek a z tohoto důvodu patří mezi nejvýznamnější rizika.

Tržní rizika – spolu s ekonomickými riziky se řadí mezi nejvýznamnější rizika, která ovlivňují celý chod organizace. Řadí se mezi ně zejména rizika, která se týkají prodeje a ceny. Dá se konstatovat, že konkurence a spotřebitelé patří mezi subjekty, které nejvíce ovlivňují tato rizika. Je to zejména z důvodu utváření cenové politiky na

¹ Např. živelná pohroma, měnový kurz, atd.

trhu a nutnosti subjektů trhu flexibilní adaptace k stále se měnícím podmínkám na trhu. (Fotr a Hnilica, 2014, s. 22)

Finanční rizika – vztahují se obvykle ke způsobu financování, zdroje financování a řeší otázky týkající se likvidity. Jsou to veškerá rizika, která ovlivňují finanční chod organizace.

Kreditní rizika – u kreditních rizik se řeší spíše otázka solventnosti odběratelů (např. uhradit včas všechny faktury) a dodavatelů (např. dodat včas materiál).

Legislativní rizika – rizika spojená s chováním hospodářské a legislativní politiky vlády. Jsou to nejrozumnější zákony, vyhlášky a opatření, které mají vliv na chod podniku. Může se jednat o daňové zákony, zákon o účetnictví, zákony na ochranu spotřebitelů, ochrana životního prostředí, atd. Mezi legislativní rizika patří i patenty, autorská práva a obchodní známky.

Politická rizika – projevují se jak při nestabilním tak i při stabilním politickém prostředí. Mohou to být rizika spjatá s podnikáním na určitém území, čerpání dotací, cla, znárodnění a další bariéry v podnikání. Spadají mezi ně také teroristické činy, války, stávky, atd.

Environmentální rizika – jsou spjatá s životním prostředím. Mohou to být náklady na zavádění povinných filtračních systémů na snižování emisí, dodržování emisních limitů, poplatky za znečišťování životního prostředí nebo za využívání neobnovitelných zdrojů, apod. (Fotr a Souček, 2011, s. 148)

Informační rizika – jsou spjatá s informačními systémy, kdy při nedostatečném zabezpečení systémů mohou být napadeny a získané informace zneužity neoprávněnou stranou. Nejčastěji se jedná o předstírání identity uživatele, používání dat neoprávněnými uživateli, používání dat neautorizovaným způsobem nebo nedodržení zákona. (Kráľ, 2015)

Lidská rizika – jedná se zejména o rizika lidského chování a jednání všech oprávněných subjektů. Může zde být zařazena i kumulace pracovníků na pozicích a s tím spojená personální politika firmy, nečestné jednání, šikana na pracovišti, stávky, atd.

Zásahy vyšší moci – jsou to zejména rizika, která nemůžou být nikterak ovlivněna. Jedná se o živelné pohromy, havárie nebo i teroristické útoky. (Fotr a Hnilica, 2014, s. 22–23)

Je vhodné podotknout, že výše uvedený výčet rizik není a nikdy nemůže být kompletní z toho důvodu, že ke každé kategorii se dá přiřadit nespočetně mnoho rizik.

2.3.3 Identifikace rizik

Než se rizika začnou analyzovat, je potřeba je nejprve identifikovat a následně ohodnotit z hlediska vzniku. Člověk, který bude identifikovat rizika, by se měl umět vžít do všech subjektů, zúčastněných v daném procesu. Měl by vědět, v jakém prostředí se bude proces nacházet, jaké požadavky na něj budou kladeny a za jakých podmínek budou kladeny. Měl by předpokládat i takové požadavky, které nejsou v souladu se zdravým rozumem a to hlavně z důvodu reálné identifikace všech rizik. S identifikací rizik je spojena budoucnost, ve které mohou být rizika eventuálně realizována. Nesmí se však opomenout i fakt, že je potřeba se ohlédnout i do minulosti a poučit se z předchozích chyb. (Tichý, 2006, s. 127)

2.3.4 Metody hodnocení rizik

Při hodnocení rizik je dobré mít na paměti jak pravděpodobnost vzniku rizika, tak i jeho následek. Metody, které se používají k hodnocení rizik je možno rozdělit do několika skupin² podle:

Schopnosti kvantifikace míry rizika

- kvalitativní metody
- kvantitativní (pravděpodobnostní) metody

Stupně podrobnosti

- metody srovnávací
- analytické metody založené na deterministickém přístupu
- analytické metody založené na pravděpodobnostním přístupu (Fuchs a Vališ, 2004, s. 13)

² Skupiny se navzájem prolínají

Podle schopnosti kvantifikace míry rizika

Metody kvalitativní se liší od kvantitativních tím, že rizika jsou vyjádřena v bodovaném rozsahu (např. 1–10) nebo určena pravděpodobností (např. 1 nebo 0) nebo ohodnocena slovně (např. malé, střední, velké).

Patří mezi ně:

- *Metoda účelových interview* (metoda Delphi) – která je nejužívanější kvalitativní metodou. Je založena na skupinovém vyplňování dotazníků experty na danou problematiku. Ti však nevědí, kdo je členem expertního týmu a vyplňují dotazník zcela subjektivně. Po vyplnění dotazníku se rozesílají zpět, kde je prostor na úpravu svých odpovědí. Postup se opakuje, dokud se nedospěje k vzájemné shodě nebo k předem stanovenému počtu vrácení dotazníku. (Smejkal a Rais, 2013, s. 112–114)
- *Skórovací metoda s mapou rizik* – vychází z metody Delphi pro stanovení expertního odhadu. Každý člen týmu by měl stanovit svůj odhad a výsledek se vypočítá jako aritmetický průměr odhadů všech členů. Výstupem je ocenění rizika, které je vypočítáno jako součin skóre dopadu a skóre pravděpodobnosti v rozmezí 1–100. Poté je sestavena mapa rizik formou dvojrozměrné matice v bodovém grafu. Kvadranty představují významná, kritická, bezvýznamná a běžná rizika. (Doležal et al., 2009, s. 82–83)

Naproti tomu **kvantitativní metody** jsou založeny na matematickém výpočtu rizika, kdy je výsledek interpretován např. v tisících Kč, proto se dá konstatovat, že má tato metoda větší vypovídací hodnotu. Její nevýhodou však může být příliš formalizovaný postup, který se musí dodržovat a časová a finanční náročnost. (Smejkal a Rais, 2013, s. 112–114)

Podle stupně podrobnosti

Metody srovnávací mohou být charakterizovány jako identifikátory zdrojů nebezpečí. Porovnávají a aplikují zkušenosti z provozu a prohlíží zařízení. Odhalují slabiny rizikového zařízení a rizika jsou subjektivně posouzena a řazena v závislosti na podílu na příčinách a samotném průběhu nebezpečné události. Srovnávací metody

dokáží upozornit na nebezpečné části zařízení, nelze však spočítat pravděpodobnost selhání a není tak možné číselně definovat míru rizika. (Fuchs a Vališ, 2004, s. 13)

Patří mezi ně:

- SR Safety Review (bezpečnostní prohlídka)
- CA Checklist Analysis (analýza kontrolním seznamem)
- RR Relative Ranking (relativní klasifikace)

Analytické metody založené na deterministickém přístupu jsou taktéž zaměřeny na identifikaci zdrojů rizika. Na rozdíl od srovnávacích metod již systematicky analyzují příčiny vzniku nebezpečí, proto tak dávají kvalitní představu o chování rizikového zařízení. Nevýhodou, stejně jako u metod srovnávacích, je, že nejsou schopny určit pravděpodobnost výskytu nebezpečí.

Patří mezi ně:

- PHA Preliminary Hazard Analysis (předběžná analýza ohrožení)
- W-I What if? (co se stane, když)
- Ishikawa diagram Diagram rybí kosti (vztahy mezi příčinami a následky)
- Paretův diagram (80 % problémů je způsobeno 20 % příčin)
- HAZOP Hazard and Operability Analysis (analýza zdrojů rizika provozuschopnosti)
- FMEA Failure Mode and Effect Analysis (analýza způsobů a důsledků poruch)
- FTA Failure Tree Analysis (analýza stromu poruch – nekvantitativní)
- ETA Event Tree Analysis (analýza stromu událostí – nekvantitativní)
- CCA Cause-Consequence Analysis (analýza příčin a následků)
- HRA Human Reliability Analysis (analýza lidské spolehlivosti)

Mezi pokročilé metody analýzy systémů patří FTA, ETA, CCA a HRA. (Fuchs a Vališ, 2004, s. 15–16)

Analytické metody založené na pravděpodobnostním přístupu už na rozdíl od předešlých metod, jak sám název napovídá, počítají s pravděpodobností. Za použití matematicko-statistických veličin se vypočítává pravděpodobnost příčiny nebezpečného jevu.

Patří mezi ně:

- FTA Fault Tree Analysis (analýza stromu poruch – kvantitativní)
- ETA Event Tree Analysis (analýza stromu událostí – kvantitativní)
- BD Block Diagram (Blokový diagram)
- MCh Markov Chains (Markovovy řetězce)

Nejpoužívanějšími metodami jsou FTA a ETA. (Fuchs a Vališ, 2004, s. 21–22)

2.3.5 Analýza rizik

Aby bylo možné snižovat rizika, je nutné, aby byly nejprve analyzovány. Předmětem takové analýzy by mělo být definování hrozeb, určení pravděpodobnosti jejich naplnění a konečné stanovení rizik.

Dle Smejkal a Raise (2013, s. 102–105) je obecný postup pro analýzu rizik následující:

- 1. Stanovit hranici analýzy rizik** – stanovit hranici v tom smyslu, že oddělí aktiva, která budou analyzována jakožto riziková, s aktivy, která budou od rizikových oddělena.
- 2. Identifikovat aktiva** – jde o vytvoření seznamu aktiv, která byla oddělena hranicí analýzy rizik a jsou tak identifikována jako riziková.
- 3. Stanovit hodnoty a seskupovat aktiva** – v tomto kroku se jedná o stanovení hodnoty aktiva, které je předmětem škody nebo zničení. Hodnota aktiva bývá často stanovována jak z nákladových, tak i z výnosových položek. Jelikož bývá často více aktiv, provádí se seskupování aktiv se stejnými nebo podobnými vlastnostmi, aby se vytvořily skupiny aktiv, které pak vystupují jako jedno aktivum.
- 4. Identifikace hrozeb** – identifikují se hrozby, které mohou ohrozit vytvořená aktiva a to na základě různých preferencí v závislosti na zkušenostech,

dřívějších analýzách, podle literatury, atd. Pokud se v podniku ještě hrozby neidentifikovaly, je vhodné použít např. metodu Delphi nebo brainstorming.

5. **Analýza hrozeb a zranitelností** – hrozba je hodnocena zvlášť ke každému aktivu nebo skupině aktiv. Zranitelnost aktiva je hodnocena vůči hrozbě. U analýzy se uvažují již nastavená opatření, která pak mohou snižovat úroveň hrozby i zranitelnosti.
6. **Pravděpodobnost jevu** – ne vždy se dá zcela určit, zda zkoumaný jev nastane. Proto se počítá, jaká je pravděpodobnost, zda k jevu dojde nebo ne.
7. **Měření rizika** – riziko může být v některých situacích větší či menší. Jeho výše je dána hodnotou aktiva, úrovní hrozby a zranitelností aktiva. Při měření absolutní výše rizika se obvykle používají základní statistické charakteristiky, jako jsou směrodatná odchylka a rozptyl. (Smejkal a Rais, 2013, s. 102–109)

2.3.6 Nástroje pro snižování rizik

V následující podkapitole budou uvedeny nástroje, které jsou používány pro snižování rizik.

Jak uvádí Rais a Doskočil (2007, s. 87), jedna z nejlepších možností pro ochranu před riziky je **ofenzivní řízení firmy**, které je charakteristické rozvojovou strategií firmy, rozvojem silných stránek firmy a zároveň dostatečnou pružností³ firmy.

Retence rizik je jedna z nejběžnějších metod snižování rizik. Subjekt je sice vystaven mnoha rizikům, nic proti nim však nedělá. Může být vědomá nebo nevědomá a dobrovolná nebo nedobrovolná.

Naproti tomu **redukce rizik** je již metoda, která se snaží proti rizikům preventivně jednat a hrozby tak eliminovat. Může být dělena podle metod odstraňujících příčiny vzniku rizika a metod, které snižují důsledky rizika. Podle příčiny vzniku se sem zahrnuje *transfer rizik*, mezi který patří např. faktoring, forfaiting, akreditiv, akontace, bankovní záruka, inkaso či využití zprostředkovatelů. Metody snižující důsledky rizik mohou být např. *diverzifikace* a *pojištění*. Do samostatné skupiny redukcí rizik by se daly zahrnout *metody operační analýzy*.

³ Reakce na vnější a vnitřní faktory, působící na podnik

Dalšími metodami snižování rizik může být: **sdílení rizik**, kde se riziko rozděluje mezi několik subjektů, **pružnost firmy** – snaží se tak za co nejkratší dobu reagovat na změnu podmínek na trhu, **vyhýbání se rizikům**, což je metoda, která je spíše považována za negativní vůči podnikatelským aktivitám a příležitostem. Celkem běžná je metoda **získávání dodatečných informací**, kdy se zjišťuje co nejvíce informací např. o dodavateli. **Vytváření rezerv** je metoda, kdy si firma vytváří buď materiální nebo finanční rezervy např. pro případy výkyvu dodávek materiálu, nebo např. z důvodu nízkého cashflow. **Prognózování** je založeno na předpovědi, ke které je přiřazena pravděpodobnost jejího uskutečnění a smyslem je především snížení povědomí o neurčitosti v budoucnu.

Dalšími metodami jsou metody **postoptimalizační analýzy**, **síťové analýzy**, **modely hromadné obsluhy** a **metody snižování rizika v rozhodování vrcholového managementu**. (Rais a Doskočil, 2007, s. 87–129)

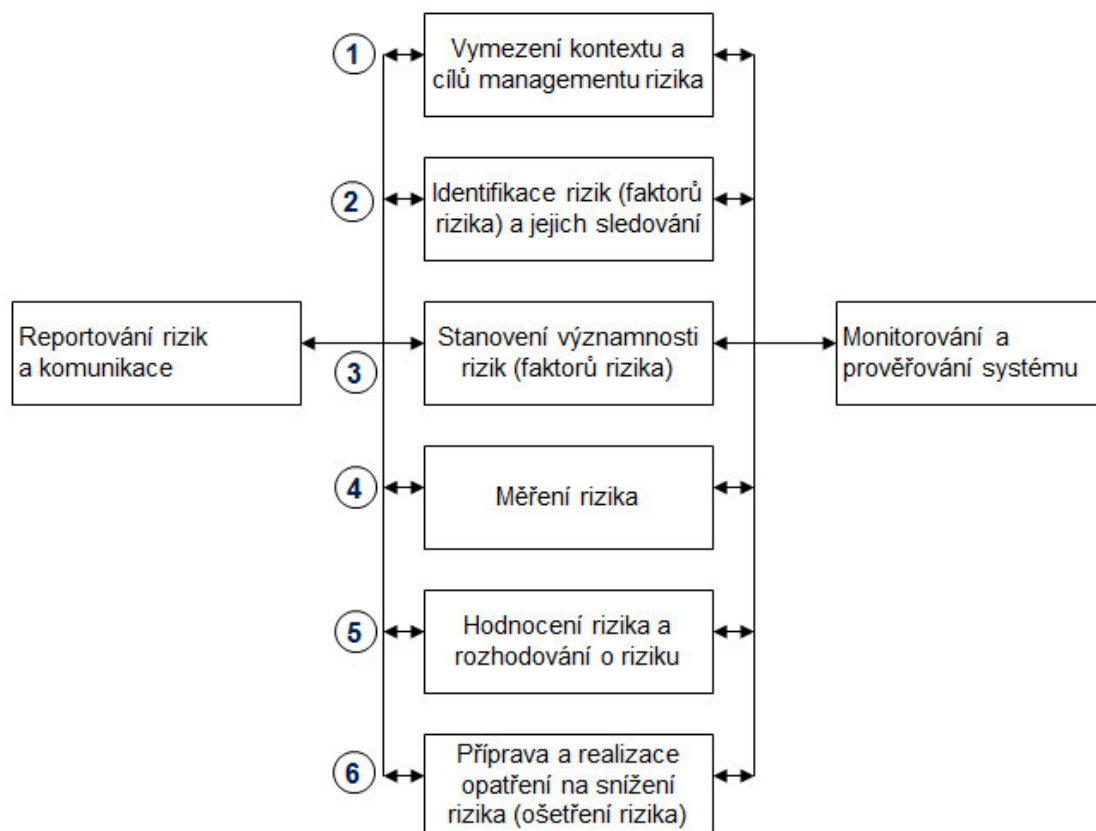
2.4 Management rizik

Management rizik (risk management) bych charakterizoval jako efektivní řízení a práci s riziky, a to tak, aby byla nastavena účinná opatření vedoucí k minimalizaci uskutečnění rizik nebo ke snížení dopadu již uskutečněných rizik.

Naučit se řídit rizika je pro podnik velmi důležité, protože podnik, který tak neučiní, hazarduje sám se sebou, se svojí důvěryhodností a zvyšuje náklady na financování sebe samotného. Je potřeba uvědomit si rozsah a dopad působících rizik a vytvořit si proti nim co nejúčinnější obranný mechanismus. (Rais a Doskočil, 2007, s. 74)

Dle Vochozky a Mulače (2012, s. 438) by se podnik měl zabývat riziky jak z provozního tak i ze strategického hlediska. Uvádí, že důležitost risk managementu v poslední době roste a to zejména v prevenci a s ní spojeným sledováním faktorů, které mohou ohrožovat cíle podniků.

Fotr (2009, s. 1–3) definuje proces managementu rizika jako: „systematický a koordinovaný způsob práce s rizikem a nejistotou uplatňovaný v rámci celé firmy a zahrnující všechny druhy rizik.“



Obr. č. 5: Proces managementu rizika (Zdroj: Fotr, 2009)

Obr. č. 5 znázorňuje proces managementu rizika, kde krok 1, 5 a 6 značí řízení rizika v užším smyslu a krok 2–4 analýzu rizika. Samotný proces je stále se zdokonalujícím, opakujícím a nepřetržitým.

Z celého procesu se dají vyvodit dva výstupy, a to v podobě **reportingu**, kdy se reportuje interním i externím uživatelům a v podobě průběžného **monitoringu**, který má za cíl zdokonalovat systém v závislosti na měnících se podmínkách v podniku.

Rais a Doskočil (2007, s. 75) říkají, že úspěšné řízení rizik může být dosaženo pouze, pokud má podnik:

- jasnou strategii, která je v souladu s cílem podniku,
- kvalitní informační systém, který tak usnadňuje řízení procesů,
- osoby, které dohlížíjí a jsou zodpovědné za řízení rizik,
- jistou flexibilitu a kulturu.

2.5 Centra sdílených služeb (Shared Service Centers)

Se stále rostoucím trhem a stále rostoucí centralizací, kterou můžeme sledovat na mezinárodní úrovni, roste i potřeba centralizace ve společnostech, organizacích a ve firmách. Otázkou zůstává, zda je to potřeba vedoucí k úspěchu či nikoliv.

Centra sdílených služeb (Shared Service Centers, dále jen SSC) se dají charakterizovat jako poskytovatelé interních služeb, kteří zastřešují služby různých druhů napříč organizací na jednom místě. (Pwc.com, 2008)

Ve stále měnícím se prostředí trhu vyvstává potřeba využít všech možných příležitostí, které se naskytnou a vyvarovat se všem hrozbám. Přesně o to se snaží SSC, které si kladou za cíl snižovat náklady, zvyšovat kvalitu poskytovaných služeb, rychlost, pružnost a transparentnost. Zejména kvůli těmto důvodům je zaznamenáván nárůst SSC po celém světě. (Keuper a Lueg, 2013, s. 6)

SSC mohou zastřešovat služby z různých oblastí, jako jsou finance, HR (lidské zdroje), IT, obchod nebo služby z oblasti zadávání zakázek (procurement). (Pwc.com, 2008)

Finance	Procurement	HR	IT	Obchod
přijaté faktury	zakázky spojené s administrativou	databáze uchazečů	vývoj	fakturace
vydané faktury	kontrakty	výplaty	hosting	centrum stížností
kredit/debit	logistika a zboží	administrace osobních dat	softwarová podpora	zákaznické středisko
reporting	objednávky	cestovné	práce s daty	objednávky
vázaná aktiva	vztah s dodavateli			technická podpora
hlavní účetní kniha				
interní reporting				
plánování a předpovídání				

Obr. č. 6: Příklady služeb v SSC (Zdroj: upraveno podle Pwc.com, 2008)

2.5.1 Rozdíl mezi SSC a outsourcingem

Mnoho lidí si představuje SSC jako formu určitého „interního outsourcingu“. Dle Bangemanna (2005, s. 18) zde však existuje rozdíl.

- Shared service center – samostatné interní středisko služeb
- Outsourcing – kompletní alokování služeb k externímu subjektu

Za něco mezi SSC a outsourcingem se dá označit joint venture⁴, což je samostatné interní středisko služeb, spolupracující s partnerem. (Bangemann, 2005, s. 18)

2.5.2 Outsourcing

Outsourcing může být vyložen jako složenina tří slov a to – *outside*, *resource* a *using*. Což v překladu znamená užívání vnějších zdrojů. Nebo jako složeninu dvou slov a to – *out* a *sourcing*. Outsourcing se dá obecně chápat jako převedení aktivit, které si firma dříve zajišťovala sama, na firmu externí, od které jsou tyto výstupy dále nakupovány. Externí subjekty mohou sídlit tam, kde sídlí outsourcovaná firma – mluvíme pak o domácím outsourcingu, nebo může sídlit v zahraničí a jedná se tak o zahraniční, přeshraniční nebo mezinárodní outsourcing. (Dvořáček a Tyll, 2010, s. 2–5)

Greaver (1999, s. 3–5) uvádí až dvacet příčin, proč podnik outsourcuje. Obecně se mluví o organizačních, finančních, výnosových, nákladových a zaměstnaneckých příčinách a příčinách, které souvisí se zdokonalováním aktivit uvnitř podniku.

S outsourcingem souvisí i pojem **offshoring**, což znamená přesunutí aktivity či více aktivit do zemí s velmi nízkými náklady. (Dvořáček a Tyll, 2010, s. 2–5)



Obr. č. 7: Podstata offshoringu (Zdroj: upraveno podle Dvořáček a Tyll, 2010)

⁴ Spojení dvou subjektů za účelem společného podnikání a podílení se tak na společném zisku nebo ztrátě. (Podnikator.cz, 2012)

Výhody outsourcingu

- Orientace podniku na klíčové procesy
- Specializovaný přístup
- Časová úspora
- Efektivnější operativní řízení
- Rozložení rizika i na subjekty, provádějící outsourcing
- Snížení nákladů
- Převedení fixních nákladů na variabilní (Fanta, 2004, s. 12–18)

Nevýhody outsourcingu

- Riziko nedostupnosti v požadovaném termínu
- Závislost na outsourcingové firmě
- Nemožnost kontroly procesu
- Možnost výskytu právních a sociálních problémů (Dvořáček a Tyll, 2010, s. 31)
- Pravděpodobná nesplnění očekávání
- Náklady na samotný outsourcing
- Nejistá kvalita služby
- Riziko změny outsourcingové firmy
- Riziko zneužití či úniku citlivých dat

Z uvedeného výčtu se dá tvrdit, že některé výhody a nevýhody se mohou navzájem vylučovat. (Fanta, 2004, s. 12–18)

2.5.3 Insourcing

Jak uvádí Rydvalová a Rydval (2007, s. 5), jedná se o alokování procesu, který byl původně zajištěn smluvně dodavatelem, mezi činnosti podniku.

Na jednoduchém příkladu SSC může insourcing představovat dříve outsourcované účetnictví, které si dnes podnik zajišťuje sám, například kvůli menším nákladům. Jde o analogický vztah s outsourcingem i s jeho výhodami a nevýhodami.

3 ANALÝZA SOUČASNÉHO STAVU

V analytické části bude představena společnost Zebra Technologies a její finanční středisko služeb (FSS), které sídlí v Brně. Budou shrnuty procesy v jednotlivých odděleních a bude provedena analýza vnitřního a vnějšího prostředí FSS, aby mohla být následně identifikována, zanalyzována a ohodnocena rizika, která na FSS působí.

V celé kapitole bude obsaženo i mnoho anglických pojmů a zkratk, které se obvykle do českého jazyka nepřekládají, proto budu pracovat hlavně s nepřeloženými výrazy.

3.1 Společnost Zebra Technologies

Zebra Technologies je mezinárodní společnost, která vyrábí a prodává zařízení a technologie, které poskytují přesná data a informace koncovým uživatelům. Mezi její portfolio patří: mobilní počítače, tiskárny, snímače dat, bezdrátové LAN technologie, RFID technologie, lokační systémy a další softwary a služby.



Obr. č. 8: Logo Zebra Technologies (Zdroj: Zebra.com, 2015)

Vizi společnosti je: „*Společně s partnery vytvářet chytřejší a více propojený globální byznys.*“ A za poslání si klade uspokojovat zákazníky tak, aby jejich kroky byly co nejlépe promyšlené skrze inovativní produkty a řešení, ze kterých pramení maximální transparentnost. (Zebra.com, 2015).

Zároveň si klade pět interních základních hodnot:

Integrity (integrita) – všichni jsou zavázáni k tomu, že budou jednat čestně, férově a eticky.

Respect (respekt) – vzájemný respekt pro své odlišné dovednosti, zkušenosti a nápady.

Agility (agilnost) – čerpá výhody z kuráže a brání na sebe rizik.

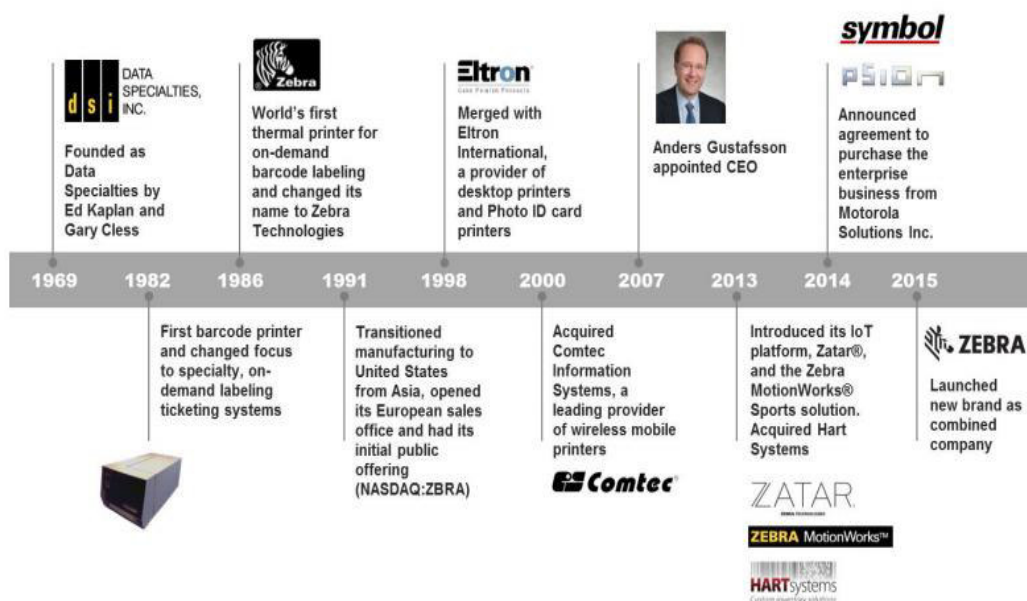
Collaboration (spolupráce) – společnost bere sebe sama jako „jednu Zebra“.

Innovation (inovace) – kreativní tvůrci, kteří se nebojí procesu zdokonalování.

Ve společnosti pracuje zhruba 7000 zaměstnanců ve více než 122 pobočkách, napříč 81 zeměmi s obchodními partnery ve více než 100 zemích z celého světa. (Zebra.com, 2015)

3.1.1 Historie

Společnost byla založena v roce 1969 v USA pod názvem Data Specialties a od té doby vyvinula mnoho revolučních technologií. V roce 1986 se přejmenovala na dnes již užívaný název Zebra Technologies a za celou dobu její existence se buď spojila, nebo přikoupila další technologické společnosti, působící ve stejném nebo příbuzném oboru. V roce 1991 vstoupila na trh s veřejně obchodovatelnými akciemi. V roce 2014 oznámila koupi Motorola Solutions i se všemi jejími dceřinými společnostmi a od minulého roku již vystupuje pod jednotným názvem a značkou Zebra Technologies. (Zebra.com, 2015)



Obr. č. 9: Historie společnosti (Zdroj: Zebra.com, 2015)

3.1.2 SSC v Brně

V České republice působí společnost pod názvem Zebra Technologies CZ s.r.o.⁵, pod kterou spadá celé SSC a sdružuje celkem šest středisek, viz Obr. č. 10.



Obr. č. 10: SSC v Brně (Zdroj: vlastní zpracování)

Provoz výše uvedených středisek se neobejde bez doprovodných oddělení, které zajišťují chod SSC jakožto celku. Patří mezi ně HR oddělení (oddělení lidských zdrojů), payroll (mzdy), IT a facility (zařízení). Dále to je oddělení interního auditu, obchodních operací, forecasting (předpovědi) a oddělení multimédií.

Firma zaměstnává v Brně celkem 446 zaměstnanců⁶, a jelikož jsou služby pro část světa (zejména pro Evropu a část Severní a Jižní Ameriky) insourcovány právě do

⁵ Sídlo: Koleční 2971/1, Královo Pole, 612 00 Brno; IČO: 26780259

⁶ K 1. listopadu 2015

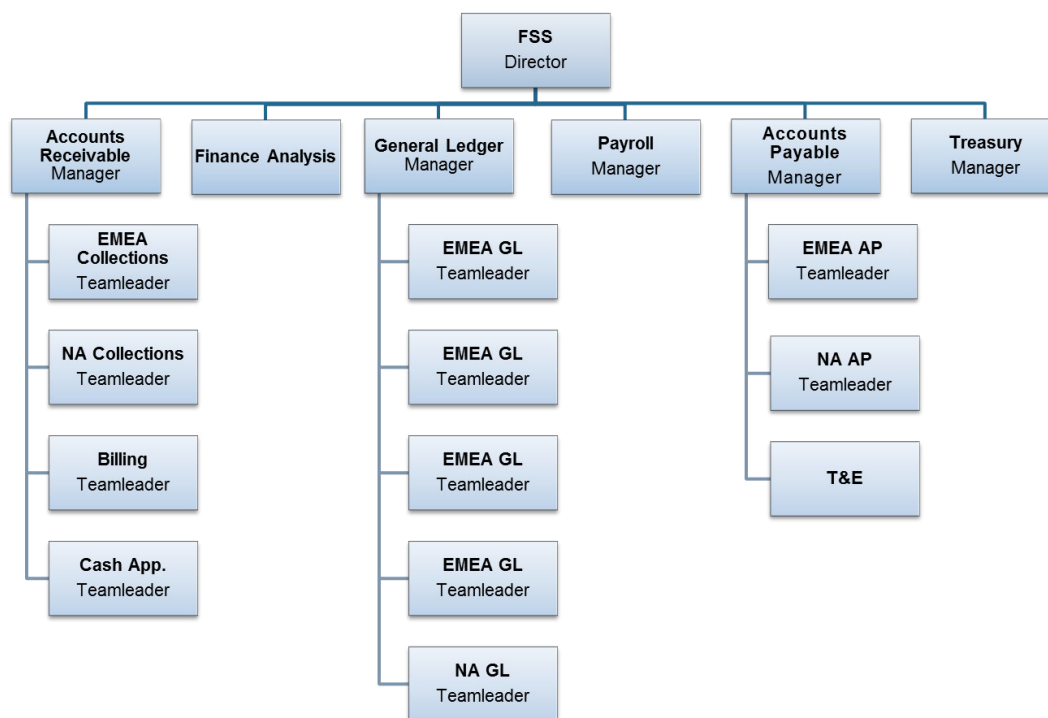
brněnského SSC, 35 % zaměstnanců tvoří cizinci. Ovládání alespoň jednoho cizího jazyka je podmínkou. Pro zajímavost uvedu, že firma zaměstnává 60 % žen a průměrný věk všech zaměstnanců je 32 let.

3.2 Procesy ve Finance Shared Services (FSS)

FSS je jedno ze šesti oddělení celého SSC v Brně. V roce 2004 bylo cílem insourcovat finanční služby⁷ pro region Evropa, Střední východ a Afrika (Europe, Middle East And Africa, dále jen EMEA). Postupem času se do FSS začaly insourcovat i finanční služby pro Severní Ameriku (North America, dále jen NA), Jižní Ameriku (Latin America, dále jen LA) a pro region Asie a Pacifik (Asia and Pacific, dále jen APAC). Nutno podotknout, že se nejedná o všechny finanční činnosti, ale pouze o jejich část. Zbylé činnosti jsou vykonávány ve Spojených státech amerických, Velké Británii a Malajsii. Do roku 2015 byly vykonávány i v Polsku, ty se ovšem přesunuly do Brna a díky tomu se zvětšilo brněnské FSS, kde k 1. 3. 2016 působí 91 zaměstnanců.

Organizační struktura se dá přirovnat k funkční organizační struktuře. V čele stojí ředitel, který vede pět manažerů. Jsou to manažeři oddělení Pohledávek (Accounts Receivable, dále jen AR), Závazků (Accounts Payable, dále jen AP), Hlavní účetní knihy (General Ledger, dále jen GL), Mzdy (Payroll) a Finančních prostředků (Treasury). V oddělení Finančních analýz (Finance Analysis) nepůsobí žádný manažer a všichni zaměstnanci jsou přímí podřízení řediteli FSS.

⁷ Zejména zajišťování kompletního účetnictví



Obr. č. 11: Organizační struktura FSS v Brně (Zdroj: vlastní podle interních zdrojů)

Ve FSS tedy pro účely globálního insourcingu působí celkem šest oddělení, z čehož se AR, AP a GL dají považovat za nejdůležitější. V těchto, co do velikosti, rozsáhlých oddělení jsou nezbytní i teamleadeři, kteří jsou přímí podřízení daných manažerů. Dá se konstatovat, že manažeři jednotlivých oddělení zabezpečují plynulý chod podpurných procesů.

Nutno podotknout, že v následujících podkapitolách, budou všechny procesy popsány velmi zjednodušeně, vzhledem k jejich složitosti.

3.2.1 Accounts Receivable (AR)

Oddělení AR neboli oddělení pohledávek má na starosti tři hlavní procesy a podle nich jsou i koncipovány jednotlivé týmy.

Billing/Invoicing – vydávání faktur a dobropisů za uzavřené kontrakty a opravárenské služby. Ostatní střediska zadávají objednávky do systému Oracle a na základě těchto objednávek jsou vystaveny faktury. Zajímavostí je, že objednávky za

prodaný hardware, jsou plně automatizovány. Vedle faktur vydaných se tým stará i o distribuci jednotlivých faktur⁸.

Cash Applications – přijaté platby se spárují s fakturami a následně se zaúčtují. Účtuje se pro region EMEA a pro region NA.

Collections – týmy mají za úkol vymáhat pohledávky, přičemž strategie je velmi agresivní. Zhruba jen 2 % faktur jsou po splatnosti více jak 60 dnů.

První upomínka se týká faktur, které se blíží splatnosti (tzv. statement), druhá upomínka varuje již na konkrétní faktury a se třetí upomínkou se začíná komunikovat už i s nákupčím na straně Zebry, který vyjednal kontrakt.

Posledním procesem je Credit Risk⁹, ten je však insourcován ve Velké Británii.

3.2.2 Accounts Payable (AP)

Na základě přijatých faktur musí společnost dostávat svým závazkům a tedy platit firmám za poskytnuté produkty či služby. Celé AP oddělení se skládá ze tří týmů. Jeden tým je pro region EMEA, druhý pro region NA/LA, třetí tým (Travel & Expense – T&E) je specifický v tom, že účtuje pouze cestovní náhrady a náklady spojené s ubytováním a reprezentací v rámci společnosti a spadají pod něj oba výše zmíněné regiony.

Hlavní procesy v AP spočívají v účtování faktur na objednávku, účtování faktur bez objednávky a v automatickém účtování faktur nahraných dodavateli.

Zjednodušený proces faktury na objednávku vypadá následovně:

1. Prostřednictvím emailu (v prostředí MS Outlook) nebo pošty AP obdrží fakturu.
2. Je provedena kontrola faktury, zda splňuje všechny náležitosti potřebné k úspěšnému auditu¹⁰, a rozliší se, o jaký typ faktury se jedná, tzn. jakým způsobem, má být zaúčtována.
3. Pokud nesplňuje, je vrácena dodavateli (nejčastěji oddělení AR) nebo nákupčímu, který komunikuje s dodavatelem.

⁸ Faktury se vydávají pro region EMEA a APAC a zhruba jen 20 % faktur je elektronických.

⁹ Nastavování kreditních limitů na základě finančních analýz.

¹⁰ Zákonné náležitosti spadají pod příslušnou právní úpravu země, ze které je faktura vydána.

4. Pokud splňuje, faktura je naskenována do systému a v informačním systému Oracle se zaúčtuje.
5. Validace faktury.
6. Platba faktury.

Denně celé AP obdrží kolem 100 faktur.

Mezi vedlejší činnosti, které mají za cíl podporu hlavního procesu, tedy které vedou ke konečnému zaplacení faktury, patří komunikace s dodavateli, bankami, nákupčími a samotná komunikace napříč týmem a GL (hlavní účetní kniha).

3.2.3 General Ledger (GL)

GL zajišťuje, aby veškeré účetní výkazy na konci každého měsíce během účetní závěrky podávaly věrný a pravdivý obraz. Stará se o to, aby všechny právní entity společnosti splňovaly právní požadavky jednotlivých zemí. GL musí sestavovat finanční výkazy jak podle US GAAP, které se řídí americkou legislativou a podávají přehledný obraz investorům a managementu pro účely obchodu na akciovém trhu, tak podle local GAAP, které se musí sestavovat zvlášť pro každou zemi a řídit se její legislativou. (Pohoda.cz, 2012)

V GL jsou tři hlavní procesy, které mají několik dalších sub-procesů.

US GAAP Compliance – jde o dodržování zmíněných zásad a účtují se zde veškeré operace, které nespadají pod AP nebo AR, nejčastěji majetek.

Fixed Assets – účtování aktiv a majetku společnosti. Řeší se, zda se jedná o náklad (do 5 000 \$ při US GAAP) nebo majetek. Pokud se jedná o majetek, je zaúčtován a následně se promítne v měsíčním reportu, který se dále nahrává do systému a v konečném kroku je promítnut v účetních výkazech.

Statutory Compliance – příprava pro veškerá daňová přiznání – VAT (DPH), CIT (DPPO) a příprava roční účetní závěrky a účetních výkazů pro jednotlivé země.

GL taktéž zajišťuje externí audity a kooperuje s finančními úřady.

3.2.4 Finance Analysis (FA)

Hlavní úloha FA spočívá v podávání reálných dat (reportingu) na základě různých metod, jak přímému nadřízenému, tedy řediteli FSS, tak i jednotlivým oddělením.

Hlavními procesy jsou zde:

SSC Reporting – reportují se výsledky z oddělení AR, AP i GL i celého SSC. Používají se pevně stanovené KPI's¹¹ a kalkulují a predikují se náklady a výkony jednotlivých středisek a oddělení.

Transfer Pricing – analýza ziskovosti napříč entitami (např. náklady brněnského FSS jsou rozloženy na všechny entity, pro které je vedeno účetnictví) pomocí vnitropodnikových faktur.

Procurement¹² – příprava service reportů a reportů pro procurement. Obecně se zde analyzuje proces nákupu, tedy u koho, co a jak nakupovat. Dále se analyzují ceny, dodavatelé, smlouvy a nastavení cen.

Repair Centers – kontrola a analýza nákladů na opravy výrobků firmy v centrech opravy¹³ a předpověď (forecast) nákladů oprav na příští období.

Inventory Audit – kontrola a audit zásob (výrobků) v jednotlivých skladech, *cycle count* (systém vybere několik náhodných položek, které musí být každý měsíc překontrolovány) a *inventory*. Všechny tři činnosti se provádějí každý rok.¹⁴

3.2.5 Payroll

Payroll neboli oddělení mezd má za cíl vyplatit zaměstnancům mzdu včas a správně. Payroll má v Brně na starosti mzdy pro region EMEA, vlastní výpočet mezd a daní je však outsourcována.

Hlavní proces je následující:

¹¹ KPI – Key Performance Indicators, neboli klíčové ukazatele výkonnosti

¹² Přímé nebo nepřímé nakupování služeb (např. energie) od externích dodavatelů.

¹³ Např. společnost Sanmina, která v Brně sdílí jednu budovu se Zebra Technologies, je externí dodavatel opravárenských služeb.

¹⁴ Opravy jsou outsourcovány Sanminou, ovšem zásoby spadají do účetnictví FSS.

1. Na začátku každého měsíce se shromáždí data z IS Oracle. Informace do IS zadává HR (oddělení lidských zdrojů).
2. Shromáždí se pozměňující informace, jako je např. změna mzdy, účtu, absence, atd.
3. Data se nahrají na portál, který je sdílený s outsourcingovou společností.
4. Outsourcingová společnost na základě poskytnutých dat spočítá mzdy a výsledek opět nahrávají na zmíněný portál.
5. Payroll data zkontroluje, jestli souhlasí se vstupy.
6. Manager buď data schválí, nebo zamítne. Pokud je zamítne, vrací se outsourcingové společnosti k opravě.
7. Po schválení se informace přesunují k oddělení Treasury, které vyplácí mzdy zaměstnancům na účty.

Vedle hlavního procesu se každý měsíc připravují tzv. žurnály, které se účtují a GL je finálně zpracovávají.

3.2.6 Treasury

Treasury insourcuje pro účely FSS v Brně pouze část finančních služeb.

Cashflow Forecast – prognózování cashflow na základě dat poskytnutých z AP, AR a GL. Zmíněná oddělení dávají přehled jejich příjmů a výdajů a Treasury má za úkol dělat prognózy a držet stav peněžních prostředků, tak aby byla společnost dostatečně likvidní a zároveň aby nedržela více peněžních prostředků, než je potřeba, z důvodu splácení úvěrů.

Prognózy se vytvářejí na týdenní bázi. Procesní mapa procesu cashflow forecast je součástí Přílohy č. 1.

Bank Statement Management – denně se stahují výpisy z bank a potřebné informace jsou poskytovány ostatním oddělením.

Perform Manual Payments – jedná se o všechny manuální platby, které nemohou být zpracovány automaticky (např. platby nad povolené limity, daně, nájem, atd.). Opět se kooperuje se všemi ostatními odděleními.

Intercompany (netting) – jedná se o platby mezi entitami vlastněné Zebra Technologies. Aby si entity v rámci společnosti neposílaly platby mezi sebou, vypočítává se rozdíl částek, kterou pošle jedna entita druhé.

Funding/Paysource – princip je podobný jako u nettingu, zde se ovšem platby posílají dodavatelům. Cílem je opět omezit počet plateb a snížit tak náklady. Rozdíl spočívá v tom, že peněžní prostředky se posílají na tzv. paysource účet, který třídí peníze dle měn a dle entit.

Ad hoc činnosti – obecně zde platí pravidlo, že čím více procesů je zautomatizovaných, tím více vyvstává problémů a Treasury je musí vyřešit.¹⁵

3.3 Analýza vnějšího prostředí

Z hlediska vnějšího prostředí bude provedena PEST analýza. Ta se bude týkat pouze relevantních faktorů, a proto budou analyzovány pouze ty faktory, které mají vliv na FSS v Brně.

3.3.1 PEST analýza

Politické (právní) faktory

Jelikož firma Zebra Technologies CZ s.r.o., pod kterou spadá celé SSC v Brně, podniká na území České republiky a je tedy zapsaná v obchodním rejstříku, musí se řídit jejími příslušnými právními předpisy. Společnost se v Česku řídí zejména občanským zákoníkem (č. 89/2012 Sb.), zákonem o obchodních korporacích (č. 90/2012 Sb.), zákonem o dani z přidané hodnoty (č. 235/2004 Sb.), zákonem České národní rady o daních z příjmů (č. 586/1992 Sb.), zákonem o účetnictví (č. 563/1991 Sb.) a zákoníkem práce (č. 262/2006 Sb.). Dále se řídí účetními standardy jednotlivých zemí, pro které je vedeno účetnictví. ČR je členem Evropské Unie, tudíž musí plnit směrnice a nařízení EU.

Politická situace v ČR se dá označit za stabilní v porovnání se zbytkem světa. Vláda, v rámci své fiskální politiky, poněkud často mění daňové zatížení, což se za tak stabilní označit už nedá. Zvyšování daní může vést k placení daní v zahraničí a to může

¹⁵ Např. dodavatel tvrdí, že nemá dostatek peněžních prostředků na úhradu faktury. Treasury má právo zkontrolovat toto tvrzení u banky.

mít za důsledek odchod firem do zahraničí. V poslední době navíc ministr financí Andrej Babiš přichází s opatřeními, díky kterým rostou firmám náklady.¹⁶

Stát však podporuje zaměstnanost poskytováním dotací zaměstnavatelům na zaměstnance, a to díky jeho aktivní politice zaměstnanosti. Stát hradí zaměstnavateli buď celou, nebo část mzdy zaměstnance. Taktéž jsou podporováni zaměstnavatelé, kteří zaměstnají absolventy, matky po mateřské dovolené, osoby předdůchodového věku nebo osoby zdravotně postižené, kteří hledají zaměstnání déle než 5 měsíců. (Státní správa, b.r.)

Ekonomické faktory

HDP v ČR meziročně ve třetím čtvrtletí minulého roku vzrostlo o 4,5 %. Inflace v lednu 2016 byla na meziroční úrovni 0,6 % a nezaměstnanost klesla oproti minulému roku ze 7,7 % na 6,4 % (Penize.cz, 2016). V Jihomoravském kraji však nezaměstnanost v lednu letošního roku dosahovala 7,2 %. (Brno.cz, 2016) Oproti minulému roku je to ovšem pokles o 1,2 %. Tato ekonomicky příznivá situace nastala v důsledku expanzivní fiskální politiky a na podnikání v ČR má pozitivní dopad.

Centra sdílených služeb v ČR meziročně rostou o 20 % a s obratem 80 miliard Kč tvoří již 1,5 % HDP. Zaměstnáno je celkem 65 tis. zaměstnanců a do roku 2020 je prognóza 100 tis. zaměstnanců. Vyplyvá to z průzkumu společnosti ABSL, který navíc doplňuje, že 62 % společností plánuje v příštích obdobích rozšířit své kapacity. (ABSL, 2015)

Sociální faktory

Ze sociálních faktorů považují za nejdůležitější vzdělanost obyvatelstva, kdy k 26. 3. 2011 (z posledního sčítání lidu) mělo ukončené vysokoškolské vzdělání 12,5 % obyvatel a střední vzdělání ukončené maturitou 27,1 %. (ČSÚ, 2014, s. 10) Jednotlivá centra sdílených služeb zaměstnávají stovky až tisíce zaměstnanců a více než 70 % z nich má vysokoškolské vzdělání. Kvalitní lidské zdroje jsou hlavní příčinou růstu segmentu sdílených center, a v příštích letech se navíc očekávají další investice v ČR v tomto oboru. Centra sdílených služeb jsou v ČR soustředěny zejména v Praze, Brně a Ostravě a zaujímají zhruba 95 % trhu, z toho 22 % zaměstnanců je soustředěno v Brně.

¹⁶ Např. schválení elektronické evidence tržeb (EET) nebo kontrolního hlášení.

Poskytované služby jsou různé. Finance a účetnictví zaujímají 76 % ze všech podnikových procesů podporovaných SSC v ČR. (ABSL, 2015)

Pracovní síla je v porovnání s průměrem EU podstatně levnější. V roce 2012 byly jednotkové náklady na práci v ČR 10,6 Eura na hodinu. V porovnání s průměrem zbytku EU, které bylo 23,4 eura, to je rozdíl 12,8 eur. (Finance.cz, 2013)

Technologické faktory

EU si uvědomuje důležitost informačních a komunikačních technologií v dnešním světě a aktivně podporuje jejich růst. Operační program Podnikání a inovace pro konkurenceschopnost (OPPIK) nabízí dotace ve výši přes 20 miliard Kč. Ty slouží k vývoji softwaru, zřizování center sdílených služeb a podporu vysokorychlostního internetu. Z těchto dotací je možné financovat jak provozní náklady, tak investice (do hmotného a nehmotného majetku) a dotace mohou být rozděleny mezi podniky všech velikostí, působících v oblastech datových center a outsourcingu pro služby jako jsou účetnictví, finance, administrativa lidských zdrojů, správa IT, grafika, animace nebo projektování. U SSC je podmínkou mezinárodní působnost. (Businessinfo.cz, 2015)

3.4 Analýza vnitřního prostředí

Analýza vnitřního prostředí se bude týkat pouze finančního střediska sdílených služeb, zejména kvůli cílům práce.

3.4.1 7S faktorů firmy McKinsey

Vnitřní prostředí jsem se rozhodl analyzovat metodou 7S faktorů firmy McKinsey, protože ji považuji za nejkomplexnější a vzhledem k cílům práce i za nejefektivnější.

Strategie

FSS v Brně bylo vybudováno především díky dvěma faktorům. Prvním faktorem byl tlak vedení na snižování nákladů globálně se rozrůstající společnosti. Dá se tedy konstatovat, že primární strategií je pozornost na minimalizaci nákladů (cost focus). Druhým faktorem byl do jisté míry skandál dvou amerických společností Enron a

Worldcom¹⁷, díky kterým ve světě narostla snaha o větší transparentnost a zprůhlednění účetnictví velkých společností.

Struktura

Organizační struktura je funkční, jak již bylo zmíněno v kapitole 3.2.

Systémy

Veškerá komunikace, jak interní, tak externí, probíhá pomocí MS Outlook, případně Skype, výjimky se vyskytují v případech nástrojů pro technickou podporu (např. Helpdesk a IT služby). K účetnictví je používán informační systém Oracle, verze Trilogy, a na analýzy a reporty se používá nejčastěji MS Excel. Pro různé služby a potřeby se používají softwary, které jsou vytvořeny speciálně podle požadavků FSS a jsou jich desítky. V současné době je ve FSS snaha o vytvoření jednoho podnikového (ERP) informačního systému.

Styl

Styl řízení bych označil za demokratický. Nadřízený deleguje několik svých pravomocí a podřízený mají vždy možnost vyjádřit se, vznášet požadavky nebo dávat návrhy. Konečné rozhodnutí je však vždy na nadřízeném.

Spolupracovníci

Každý pracovník je přiřazen do určitého týmu a má svou roli. Jeho dovednosti jsou rozvíjeny metodou pravidelných rozhovorů ve vztahu nadřízený – podřízený, kde jsou probírány další možnosti pracovníka a nadřízený sleduje motivaci a chování podřízeného. Bariéry v komunikaci bych označil za minimální hlavně z důvodu nízkého průměrného věku všech spolupracovníků. Stejně tak jsou minimální bariéry i ve vztahu nadřízený – podřízený, troufám si tvrdit, díky demokratickému stylu řízení.

Schopnosti

¹⁷ V roce 2001 zbankrotovala energetická společnost Enron, která v účetnictví zatajovala výdaje, díky kterým rostl zisk firmy (Česká televize, 2011). V roce 2002 se stal podobný případ v telekomunikační společnosti Worldcom, která nadhodnocovala zisk firmy tak, že vykazovala výdaje až v dalších čtvrtletích a to jako investice. Navenek Worldcom vykazoval dobré výsledky pro akcionáře, kteří však mezitím přicházeli o své investice (Měšec.cz, 2005). Na základě těchto kauz byl v USA přijat zákon Sarbanes-Oxley (SOX), který upravuje transparentnost účetnictví. (Finance-management.cz, 2012)

Schopnosti a dovednosti se snaží firma u všech pracovníků rozvíjet. Pravidelně jsou nabízeny jazykové kurzy, školení a tréninky. Jako mistra změn shledávám ředitele FSS. Dokáže komunikovat, dívat se na realitu a nebojí se inovací. Ostatní pracovníci mají možnost, jak už bylo zmíněno, se kdykoliv projevit a navrhnout změnu a musím tvrdit, že se tak často i děje. FSS je velmi flexibilní prostředí a proto musí být všichni pracovníci schopni reagovat na změny v co nejkratší době.

Sdílené hodnoty

Kultura firmy je zde hodně závislá na lidech. Kultura je v celé společnosti hodně silná. Zaměstnanci organizují sportovní, dobrovolnické i zájmové akce pod záštitou společnosti. Z vedení celé společnosti přicházejí poslední dobou tlaky na větší integraci hodnot mezi všechny zaměstnance. Děje se tak formou interních školení, které jsou třikrát do měsíce, a zaměstnanec není nucen se takového školení účastnit.

3.5 SWOT analýza

SWOT analýza umožní identifikovat (z předešlých analýz vnějšího a vnitřního prostředí) silné stránky a příležitosti, které by měly být maximalizovány, a slabé stránky a hrozby, které by měly být minimalizovány.

Tab. č. 1: SWOT matice (Zdroj: vlastní zpracování)

Silné stránky	Slabé stránky
Koncept SSC Demokratický styl Mladý kolektiv Kvalifikovaný personál Stážísté Fluktuace zaměstnanců Kultura společnosti Organizační struktura Životnost managementu Definované cíle Vzdělávání Interní a externí audity	Byrokracie Duplikování práce Informační systémy Zahlcenost managementu Komunikace mimo FSS Jazykové bariéry Nedostatek informací Podřízenost, centralizace
Příležitosti	Hrozby
Ekonomický růst Státní pobídky Vzdělanost	Nedostatek lidských zdrojů Státní regulace Růst daní

Silné stránky

Za nejsilnější stránku považuji ověřenou koncepci SSC. Je to koncept, který je zavedený v mnoha mezinárodních společnostech a pro společnosti s tak velkým rozsahem působnosti a velikostí je úspěšný.

Silnou stránkou FSS je bezpochyby demokratický styl řízení. Atmosféra je přátelská, což má pozitivní dopad na výkon odvedené práce. Jistě tomu napomáhá i mladý a dynamický kolektiv, který musí čelit každý měsíc různým změnám a musí se tak přizpůsobovat. Výhodou je i kvalifikovaný personál. Výběrové řízení se skládá ze tří kol a požadavky na zaměstnance jsou poměrně vysoké, i co se týče odbornosti a vzdělání. FSS dává taktéž prostor i studentům v posledních ročnících i skrze možnost polovičních úvazků. Ti mnohdy přicházejí s inovativními myšlenkami a díky demokratickému stylu řízení dostávají prostor i oni.

Do silných stránek jsem zařadil i fluktuaci zaměstnanců, jelikož je v porovnání s ostatními SSC v regionu velmi nízká. To značí silnou kulturu společnosti a ochotu zaměstnanců setrvat ve společnosti.

Za silnou stránku považuji i organizační strukturu. Každý zaměstnanec je součástí některého z týmů a zodpovídá se svému teamleaderovi. Ten jasně definuje práci svým podřízeným.

Životnost managementu je nad 5 let, což pokládám za silnou stránku z hlediska znalostního managementu a následného předávání informací a znalostí. Management se schází i v rámci jednotlivých týmů a definují společně pomocí metody brainstormingu nové cíle. Průběžně na ně také dohlíží a dbá na jejich plnění.

Vedení usiluje i o vzdělávání svých zaměstnanců a nabízí jim školení a tréninky na různá témata, nejlépe však taková, která budou mít pozitivní dopad na jejich práci. Zaměstnanci mají možnost účastnit se i jazykových kurzů – ty jsou brány jako forma benefitu.

Za velkou výhodu považuji i interní a externí audit, který vede k neustálému zdokonalování.

Příležitosti

Velkou příležitostí je ekonomický růst v ČR. Ekonomice i celému segmentu se daří a společnost si tak může dovolit investovat. V rámci FSS je řeč především o investicích do lidského kapitálu.

Firma může uspořít náklady zapojením se do programu EU – Podnikání a inovace pro konkurenceschopnost (OPPIK), který podporuje i SSC formou dotací.

Příležitostí je i nárůst počtu vzdělaných obyvatel, tím pádem se cílová skupina na trhu práce stává rozšířenější. Přitom náklady na zaměstnance jsou jedny z nejnižších v celé EU.

Slabé stránky

Za velkou slabinu pokládám velkou byrokracii v procesním řízení. Některé procesy vyžadují až tříúrovňové schvalování. Díky tomu se procesy natahují a v některých případech se odvedená práce projeví až při interpretaci reportu, což může trvat i několik týdnů. Při tak vysokém objemu práce si pak zaměstnanci mohou připadat jako strojově nahraditelní. S tím souvisí i duplikování práce v některých odděleních.

Souvislost s byrokratickým zatížením vidím i v informačních systémech. Na příkladu zaúčtování jedné přijaté faktury uvedu, že zaměstnanci musí použít celkem šest softwarů, aby mohla být faktura zaúčtována a zaplacená. K tomuto úkonu je zapotřebí minimálně tři zaměstnanců. Z toho vyplývají neefektivně využitá zdroje. Navíc IS bývají několikrát do měsíce nefunkční. Může to znamenat jak výpadky v komunikaci, tak ztrátu zásadních dat a informací, v nejhorším případě ztrátu a zhoršení vztahů s externími subjekty.

Další slabinu vidím v příliš velkém zatížení přímých nadřízených. Často se stává, že mají den nabytý schůzkami a zbývá jim méně času na své podřízené, nemluvě o nedelegované práci a nutnosti jejich přesčasů, což se může negativně promítat na efektivitě některých nadřízených.

Slabou stránkou je i interní komunikace mimo FSS, kdy se může stát, že komunikace je duplicitní a prodleva je logicky delší, než při osobním styku. Souvisí s tím i bariéry v komunikaci. Ve FSS je drtivá většina česky hovořících zaměstnanců a používaný jazyk, minimálně navenek, je angličtina. Podmínkou pro přijetí zaměstnance

do pracovního poměru je sice ovládání anglického jazyka, i přesto se občas vyskytují bariéry v komunikaci.

Slabinu vidím i v informačním riziku, kdy může v tak byrokraticky zatížené společnosti často docházet ke komunikačnímu šumu, pokud nejsou jasně definována pravidla komunikace.

FSS je podřízeno své mateřské společnosti v USA. Ta může kdykoliv rozhodnout a přesunout celé FSS nebo SSC např. do levnější Asie, pokud by chtěla centralizovat SSC a redukovat náklady na provoz.

Hrozby

Za největší hrozbu pokládám nedostatek kvalifikovaných lidských zdrojů. V praxi se může stát, že člověk s požadovanými dovednostmi a charakteristikami není na trhu práce dostupný. Týmy jsou sice koncipovány tak, aby byly schopny se při výpadku jednoho člena podělit o práci, tento stav je však dlouhodobě neudržitelný.

Velká hrozba spočívá i v regulaci ze strany státu a nárůstu daní v posledních letech. To může mít za důsledek neochotu společnosti platit daně v ČR a trh může v nejhorším případě opustit. Dle mého názoru by měl stát zasahovat do tržního mechanismu co nejméně.

3.6 Identifikace rizik

Na základě provedených analýz jsem identifikoval rizika, která jsem rozdělil na obecná rizika, vnější rizika, vnitřní rizika (uvnitř FSS) a rizika procesní (rizika, vyplývající z procesů jednotlivých oddělení).

3.6.1 Obecná rizika

Jedná se o rizika, kterým nemůže FSS nijak předcházet, může se na ně však připravit.

Živelné pohromy – povodně v této oblasti nehrozí, ale může nastat požár, zemětřesení nebo extrémní výkyvy počasí.

Terorismus – v Evropě v posledních letech a měsících roste počet teroristických činů. Proto se toto riziko stává stále víc aktuálním.

Havárie – může dojít např. k prasknutí potrubí a úniku vody nebo plynu, nebo k letecké havárii. Dále může dojít k výpadku elektrické energie nebo internetu, na kterých je středisko závislé.

3.6.2 Vnější rizika

Ekonomická situace v ČR – nyní se sice ČR nachází z pohledu ekonomického cyklu v růstu, jednoho dne ale nastane stagnace a následná recese. Může to znamenat zpomalení nebo dokonce pokles hospodářského růstu společnosti.

Legislativní změny – může dojít k legislativním změnám, na které bude společnost muset reagovat a aplikovat je. Tato implementace je ze zákona povinná a nezávisí na vůli společnosti.

Nedodržování právních předpisů – jsou to rizika, ze kterých mohou plynout různé sankce a penále.

Ekonomická situace společnosti – z pohledu FSS je ovlivnitelná, ale pouze z malé části. Ekonomická situace celé společnosti je nejvíce závislá na top managementu celé společnosti a na jeho rozhodnutích. Špatná rozhodnutí mohou vést i k zániku celé společnosti.

3.6.3 Vnitřní rizika

Tato rizika se týkají již celého FSS a jsou nejvíce ovlivnitelná.

Rizika informačních systémů – jelikož všichni zaměstnanci pracují na počítači s různými softwary a informačními systémy, tak jejich výpadek zapříčiní neschopnost pracovat. Na základě toho rostou náklady společnosti a může tak dojít k celkovému kolapsu FSS.

Riziko výpadku internetového připojení – většina IS není schopna fungovat bez trvalého připojení k internetu. Část práce se však dá vykonávat i bez připojení.

Informační riziko – s šířením informací vyvstávají i problémy spojené např. s neúmyslným zatajením informace. To pak může znamenat jiný výstup než za předpokladu úplné informace. S tím souvisí i to, že většina služeb je prováděna na dálku a od počítače. Provádějící pracovník není fyzicky u procesu a nemůže si tak ověřit některé informace, které by zjistil jen na místě.

Riziko demokratického řízení – demokratické řízení je sice silnou stránkou, nicméně toto řízení se dá identifikovat i jako riziko a to v tom smyslu, že zaměstnanci mají větší prostor v nakládání se svým časem, což může vést k vyšší neefektivitě práce.

Riziko delegování pravomocí – spočívá v tom, že nadřízený může delegovat i pravomoci, které mohou být zneužity v neprospěch firmy, nebo s nimi může být zacházeno jinak, než by mělo býti.

Komunikační riziko – spočívá v tom, že zaměstnanec nemusí předat dostupné informace té správné osobě. To vede k nevyřešení nebo k natáhnutí času k vyřešení problému.

Riziko jazykových bariér – jde o špatné vyložení problémové situace, které vede k řešení s jiným výstupem.

Riziko složitosti procesů – jde o procesy, které nemusí být pochopeny. Zaměstnanec může chybovat, což se projeví ve výsledku odvedené a v tom případě zbytečné práce.

Riziko aktuálnosti – některé procesy se mohou opozdit hlavně díky složitému procesu schvalování či komplikovanosti procesu. Data a informace, které jsou zpracovávány, již po uplynutí určité doby nemusí být aktuální.

Riziko nesplnění termínů – vysoký objem a neefektivní delegování práce může znamenat nesplnění požadovaných termínů.

Riziko duplikování práce – zejména chyby v komunikaci a IS zapříčiňují duplicitní řešení problémů, díky kterým rostou náklady.

Riziko nemoci – zaměstnanec se může zranit nebo může onemocnět a jeho práci musí vykonat někdo jiný. Navíc v otevřené kanceláři (tzv. „open-office“) riziko přenosu nemoci narůstá.

Riziko odchodu zaměstnanců – nízký věk a cílevědomost přináší riziko odchodu zaměstnanců do jiných firem. Riziko je větší, když je ve firmě mnoho bezdětných mladých žen, které plánují mít děti.

Riziko zneužití dat – jelikož je práce vykonávána od počítače a navíc v online prostředí s nástroji pro online komunikaci, je pravděpodobné, že se zaměstnanec stane obětí phishingu¹⁸ nebo malwaru¹⁹. Tyto útoky mají za cíl zneužití dat.

Riziko ztráty dat – buď náhodným, nebo účelným nedopatřením může dojít ke ztrátě dat, z čehož můžou plynout další problémy.

3.6.4 Procesní rizika

Procesní rizika vyplývají z řízení procesů v jednotlivých odděleních. Nutno podotknout, že mnoho rizik vychází z již identifikovaných vnitřních rizik. V největší míře jsou rizika v přímé korespondenci s riziky plynoucí z informačních systémů.

Accounts Payable

Riziko nezaplacení faktury – plyne z mnoha faktorů, nejčastěji z nedodržení formálních požadavků přijaté faktury.

Riziko opoždění platby – nejčastěji z důvodu chybějící informace nebo z pozdního přijetí od dodavatele.

Riziko penále z prodlení – společnost je s některými dodavateli smluvně zavázána, že pokud nedodrží termín platby, mohou jí být účtovány penále.

Riziko ztráty faktury – při objemu faktur, které AP denně obdrží, se může stát, že se nějaká faktura vynechá nebo omylem ztratí.

Accounts Receivable

Riziko nevystavení faktury – nejčastěji na základě chybějících dat.

Riziko neuhrazení pohledávky – odběratel nemusí uhradit pohledávku z nejrůznějších důvodů. Faktura např. nemusí splňovat potřebné náležitosti nebo se odběratel může potýkat s nízkou likviditou.

General Ledger

Riziko chybného zaúčtování – je tolik právních předpisů jednotlivých zemí, že se zaměstnanec při účtování může jednoduše splést nebo na něco zapomenout. Znamená

¹⁸ Technika k podvodnému získávání dat v elektronické komunikaci.

¹⁹ Počítačový program, který má za cíl vniknout do počítače nebo jej poškodit.

to zkreslené účetní výkazy, z čehož vyplývá nevěrohodný obraz pro akcionáře. Taktéž to značí chybně podané daňové přiznání a z toho plynoucí sankce.

Riziko zkreslení informací – speciálně pro potřeby manažerského účetnictví může mít toto riziko zásadní dopad. Na základě poskytnutých účetních výkazů se rozhoduje management celé společnosti, což má také přímý dopad na celou společnost.

Riziko externího auditu – v tom smyslu, že externí audit může odhalit účetní chyby, které se musí opravit, což zvyšuje náklady firmy.

Finance Analysis

Riziko zkreslení dat – podání nevěrohodného obrazu vedení společnosti na základě špatně zadaných dat.

Payroll

Riziko nevyplacení mzdy – riziko, které se zvyšuje zejména z důvodu nízkého cashflow. Může být zvýšené i v případě nedodržování termínů, či špatné součinnosti s outsourcingovým subjektem. S tím souvisí i pozdní vyplacení mzdy. Může to mít za následek odchod lidských zdrojů, na kterých je společnost závislá.

Riziko neodvedení zákonného pojištění – špatně vypočítaná mzda nebo nevyplacená mzda může znamenat nižší nebo žádný odvod státu. Pro firmu to znamená penále.

Treasury

Riziko nízké likvidity – pokud odběratelé nehradí pohledávky a FSS má naopak povinnost hradit závazky vůči dodavatelům a zaměstnancům.

Riziko zpronevěry peněz – přístup k účtům v bankách může znamenat zneužití těchto přístupů a následné zpronevěry peněz.

Riziko automatizace – čím dál více procesů začíná být zautomatizovaných a čím více procesů je zautomatizovaných, tím více problémů z nich pramení.

Tab. č. 2: Identifikace rizik (Zdroj: vlastní zpracování)

	Riziko
Obecná rizika	
1	Živelné pohromy

2	Terorismus
3	Havárie
Vnější rizika	
4	Ekonomická situace v ČR
5	Legislativní změny
6	Nedodržování právních předpisů
7	Ekonomická situace společnosti
Vnitřní rizika	
8	Informační systémy
9	Výpadky internetového připojení
10	Informační riziko
11	Demokratické řízení
12	Delegování pravomocí
13	Komunikační riziko
14	Jazykové bariéry
15	Složitost procesů
16	Aktuálnost
17	Nesplnění termínů
18	Duplikování práce
19	Nemoc
20	Odchod zaměstnanců
21	Zneužití dat
22	Ztráta dat
Procesní rizika	
23	Nezaplacení faktury
24	Opožděná platba
25	Penále z prodlení
26	Ztráta faktury
27	Nevystavení faktury
28	Neuhrazení pohledávky
29	Chybné zaúčtování
30	Zkreslení informací
31	Externí audit
32	Zkreslení dat
33	Nevyplacení mzdy
34	Neodvedení zák. pojištění
35	Nízká likvidita
36	Zpronevěra peněz
37	Automatizace

3.7 Analýza a hodnocení rizik

3.7.1 Skórovací metoda s mapou rizik

Na základě identifikovaných rizik, kterým bylo přiděleno číselné označení, bude provedena analýza rizik pomocí skórovací metody s mapou rizik. Metoda spočívá v subjektivním ohodnocení rizik experty na základě možnosti výskytu rizika (Tab. č. 3) a jeho dopadu (Tab. č. 4) na stupnici 1–10. Skóre pak tvoří součin možnosti výskytu a dopadu rizika. Rozmezí skóre, tedy ocenění rizika je 1–100. Cílem metody je identifikovat kritická, významná, běžná a bezvýznamná rizika.

Tab. č. 3: Možnost výskytu rizika (Zdroj: vlastní zpracování)

Možnost výskytu	
1–2	Velmi malá
3–4	Malá
5–6	Střední
7–8	Velká
9–10	Obrovská

Tab. č. 4: Dopad rizika (Zdroj: vlastní zpracování)

Dopad	
1–2	Velmi mírný
3–4	Mírný
5–6	Střední
7–8	Velký
9–10	Obrovský

Expertní tým tvoří 8 zaměstnanců firmy. Z toho jsou 3 manažeři a 5 zaměstnanců napříč jednotlivými týmy. Výsledky hodnocení jednotlivých expertů jsou součástí Přílohy č. 2.

Z analyzovaných výsledků byl vypočten aritmetický průměr pro možnost výskytu rizika a jeho dopadu, díky kterému bylo dopočítáno skóre. Skóre s nejvyšší hodnotou představuje největší hrozbu viz Tab. č. 5.

Tab. č. 5: Skóre hodnocení experty (Zdroj: vlastní zpracování)

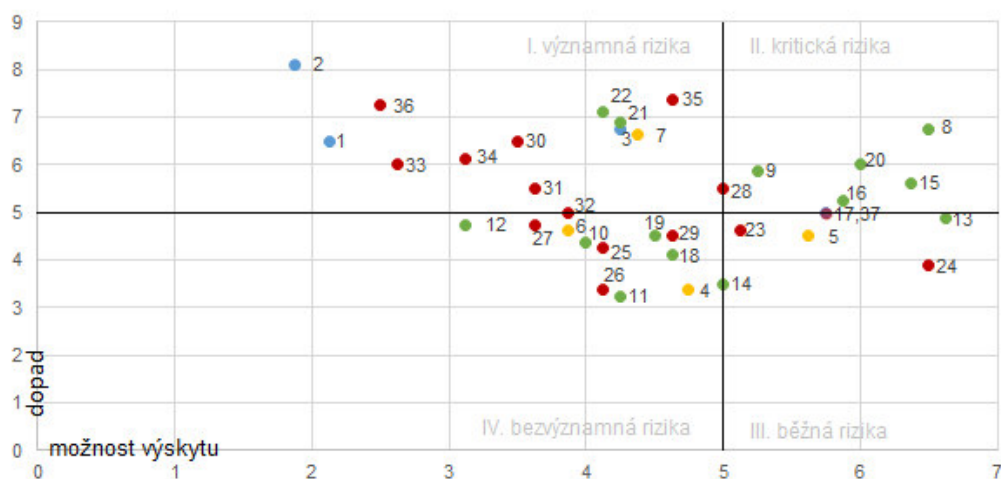
Hodnocení experty			
Riziko	Možnost výskytu	Dopad	Skóre
Obecná rizika			
1	2,1	6,5	13,8
2	1,9	8,1	15,2
3	4,3	6,8	28,7
Vnější rizika			
4	4,8	3,4	16,0
5	5,6	4,5	25,3
6	3,9	4,6	17,9
7	4,4	6,6	29,0
Vnitřní rizika			
8	6,5	6,8	43,9
9	5,3	5,9	30,8
10	4,0	4,4	17,5
11	4,3	3,3	13,8
12	3,1	4,8	14,8
13	6,6	4,9	32,3
14	5,0	3,5	17,5
15	6,4	5,6	35,9
16	5,9	5,3	30,8
17	5,8	5,0	28,8
18	4,6	4,1	19,1
19	4,5	4,5	20,3
20	6,0	6,0	36,0
21	4,3	6,9	29,2
22	4,1	7,1	29,4
Procesní rizika			
23	5,1	4,6	23,7
24	6,5	3,9	25,2
25	4,1	4,3	17,5
26	4,1	3,4	13,9
27	3,6	4,8	17,2
28	5,0	5,5	27,5
29	4,6	4,5	20,8
30	3,5	6,5	22,8
31	3,6	5,5	19,9
32	3,9	5,0	19,4
33	2,6	6,0	15,8

34	3,1	6,1	19,1
35	4,6	7,4	34,1
36	2,5	7,3	18,1
37	5,8	5,0	28,8

Na základě skóre je vytvořena mapa rizik (Graf č. 1), která rozděluje rizika do čtyř kvadrantů. Kvadrant kritických rizik obsahuje rizika s nejvyšším skóre, následuje kvadrant významných rizik, kvadrant běžných rizik a kvadrant bezvýznamných rizik, který obsahuje rizika s nejnižším skóre.

Mapa rizik na vertikální ose zohledňuje velikost dopadu rizika a na horizontální ose možnost výskytu daného rizika.

Graf č. 1: Mapa rizik (Zdroj: Vlastní zpracování)



Rizika jsou v grafu číselně i barevně označena. Modrá barva značí *obecná rizika*, žlutá barva *vnější rizika*, zelená barva *vnitřní rizika* a červená barva *rizika procesní*.

Expertní tým ohodnotil 8 kritických (vnitřních a procesních rizik). Mezi významná rizika patří 13 rizik, mezi běžná 5 rizik a jako bezvýznamná rizika expertní tým ohodnotil 11 rizik. Zajímavostí je, že všechna obecná rizika byla ohodnocena jako významná. V závorce za jednotlivými riziky je skóre z Tab. č. 5, tedy ocenění rizika.

Kritická rizika

- Informační systémy (43,9)
- Výpadky internetového připojení (30,8)
- Složitost procesů (35,9)
- Aktuálnost (30,8)
- Nesplnění termínů (28,8)
- Odchod zaměstnanců (36,0)
- Neuhrazení pohledávky (27,5)
- Automatizace (28,8)

Významná rizika

- Živelné pohromy (13,8)
- Terorismus (15,2)
- Havárie (28,7)
- Ekonomická situace společnosti (29,0)
- Zneužití dat (29,2)
- Ztráta dat (29,4)
- Zkreslení informací (22,8)
- Externí audit (19,9)
- Zkreslení dat (19,4)
- Nevyplacení mzdy (15,8)
- Neodvedení zákonného pojištění (19,1)
- Nízká likvidita (34,1)
- Zpronevěra peněz (18,1)

3.7.2 Analýza příčin a důsledků

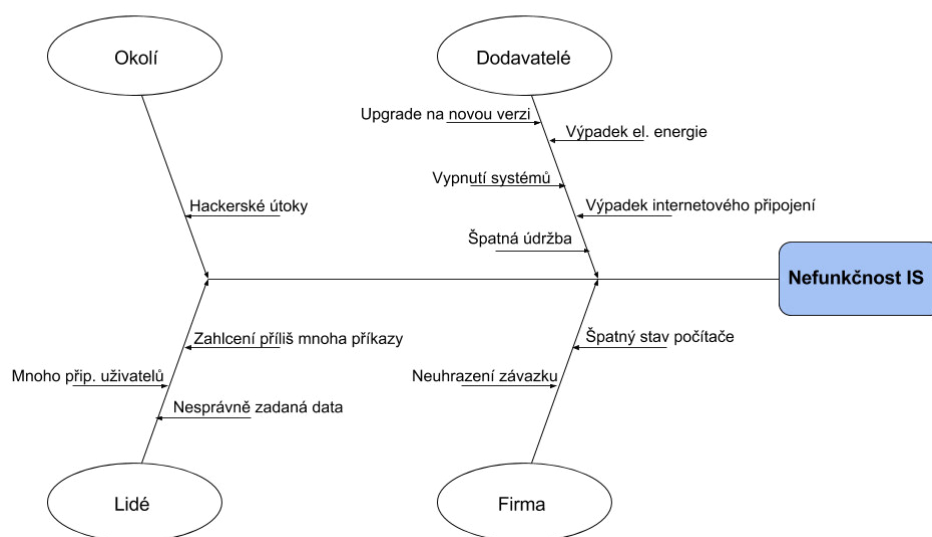
Vybraná kritická a významná rizika, která jsou nejvíce ovlivnitelná, budou dále analyzována pomocí Ishikawa diagramu neboli diagramu rybí kosti. Ten spočívá v analýze příčin a důsledku u jednotlivých rizik.

Kritická rizika

Informační systémy (43,9)

Z pohledu expertů se jedná o největší riziko FSS. Všechny IS jsou propojené a nefunkčnost jednoho může spustit řetězovou reakci a ve finále nemusí fungovat žádný IS. Na informačních systémech stojí celé středisko a jejich kolaps znamená zastavení činnosti. Práce každého zaměstnance je závislá na 100% funkčnosti IS.

Na riziko nefunkčnosti IS (lokálně) působí čtyři hlavní faktory. Dodavatelé, firma, lidé a okolí. Příčiny na straně *dodavatelů* mohou být: výpadek elektrické energie, výpadek internetového připojení, upgrade systémů na novou verzi, vypnutí systémů a špatná údržba systémů. Příčiny na straně *firmy*: neuhrazení faktury za poskytování a údržbu IS a špatný stav počítače, na kterém IS běží. *Lidé* mohou za nesprávně zadaná data, což má ve většině případů za důsledek zamrznutí IS, tudíž nefunkčnost. Mohou za zadání příliš mnoha příkazů, což má stejný důsledek a najednou se může připojit příliš mnoho uživatelů, kteří IS přetíží. Z hlediska *okolí* mohou IS napadnout hackeři. Všechny jmenované příčiny mají za důsledek nefunkčnost IS.



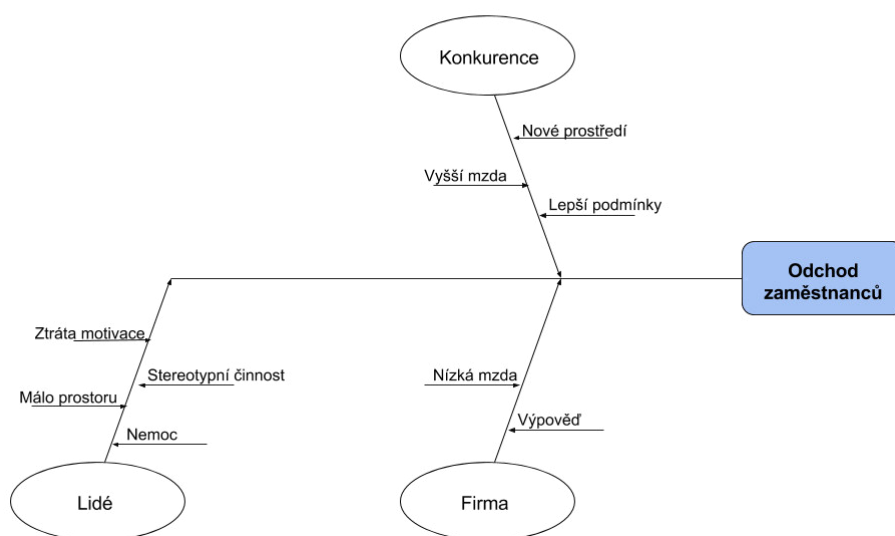
Obr. č. 12: Ishikawa diagram – Riziko informačních systémů (Zdroj: vlastní zpracování)

Informační systémy by se daly bezpochyby zahrnout do příčin některých dalších analyzovaných rizik.

Odchod zaměstnanců (36,0)

Riziko odchodu zaměstnanců bylo ohodnoceno jako druhé nejkritičtější. Vysoké skóre potvrdilo mé úvahy, jelikož FSS je zcela závislé na lidském kapitálu.

Příčiny rizika mohou být velmi subjektivní. Riziko je ovlivněno konkurencí na trhu práce, firmou a samotnými lidmi. Důsledek odchodu zaměstnanců může být buď nedobrovolný, a to výpovědí – zaměstnanec neplní nebo zanedbává své povinnosti nebo mu jeho zdravotní stav nedovoluje práci vykonávat, anebo dobrovolný – zaměstnanec odejde z firmy na základě vlastního rozhodnutí. Může se rozhodnout pro vyšší mzdu, nové prostředí nebo lepší podmínky u jiného zaměstnavatele nebo se může rozhodnout na základě, dle jeho parametrů, nízké mzdy ve FSS. Také může dostávat málo prostoru pro sebeuplatnění, vykonávat stereotypní činnost nebo ztratit celkovou motivaci.



Obr. č. 13: Ishikawa diagram – Riziko odchodu zaměstnanců (Zdroj: vlastní zpracování)

Neuhrazení pohledávky (27,5)

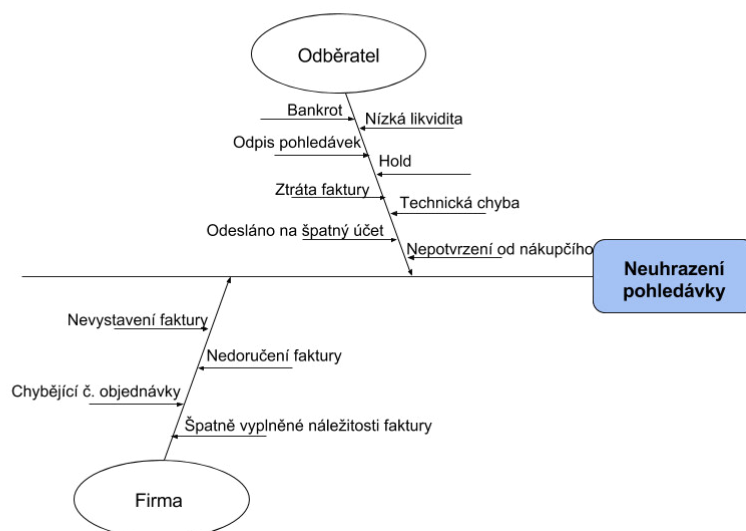
Z rizika neuhrazení pohledávky odběratelem může plynout několik dalších důsledků. Tím nejzávažnějším je bezpochyby nižší likvidita, než s jakou bylo počítáno při řádném uhrazení faktury.

Příčiny neuhrazení pohledávky vidím na straně firmy a odběratele.

Na straně firmy jimi jsou zejména: nevystavení faktury – AR nemá dostatek dat potřebných k vystavení faktury, dále může dojít ke špatnému vyplnění některých z údajů potřebných k zaúčtování a zaplacení faktury (adresa odběratele, datum faktury, číslo faktury, částka, měna a označení, že se jedná o fakturu). FSS nemusí doručit fakturu na správné místo, ať už elektronicky nebo fyzicky a nemusí dodat číslo objednávky, tím pádem odběratel nebude schopen fakturu přiřadit, zaúčtovat a zaplatit.

Na druhé straně odběratel může být v bankrotu a tedy platební neschopnosti, může mít nízkou likviditu, na základě které nebude hradit vybrané faktury, fakturu může odepsat, anebo umístit na tzv. „hold“²⁰. Taktéž nemusí mít potvrzení od nákupčího o proběhlé objednávce. Faktura může být přehlédnuta (ztracena), může se vyskytnout technická chyba na straně odběratele anebo se peníze mohou odeslat, ale na jiný účet.

²⁰ Faktura byla přijata a zaúčtována, avšak nesplňuje některou z povinných náležitostí potřebných k zaplacení faktury.



Obr. č. 14: Ishikawa diagram – Riziko neuhrazení pohledávky (Zdroj: vlastní zpracování)

Automatizace (28,8)

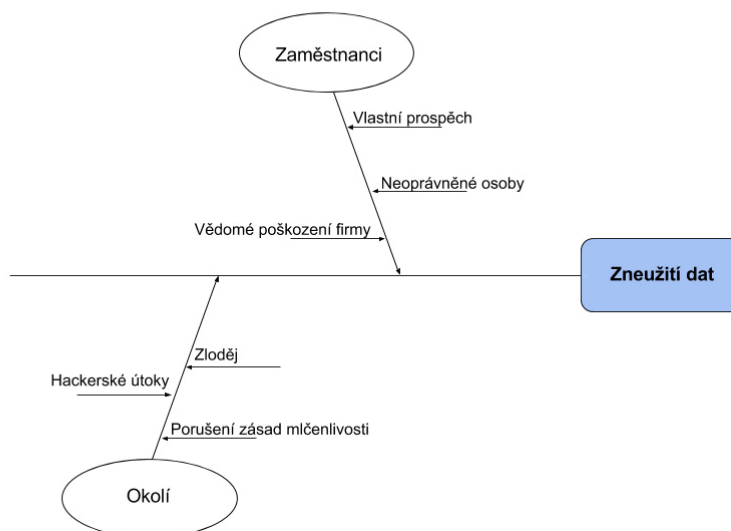
Riziko automatizace je tak široký pojem, který spadá do valné většiny procesů a není jej možné analyzovat pomocí Ishikawa diagramu. Řeč je samozřejmě o negativním dopadu automatizace procesů. Negativní vliv má zejména na lidský kapitál, který postupně nahrazuje a v budoucnu, s nynějším technologickým tempem růstu, bych se nebál užít pojmu, jako je robotika. Negativní dopad má i nyní, kdy jsou zautomatizovány pouze části procesů a implementace v nynější době nevypadá tak, jak by vypadat měla. Z toho důvodu je potřeba vnějšího zásahu při nápravách problémů.

Významná rizika

Zneužití dat (29,2)

Data mohou zneužít buď zaměstnanci, nebo lidé z okolí. Z okolí se může jednat buď o zloděje, kteří se vkradou přímo do FSS a data odcizí, nebo, což je pravděpodobnější varianta, může dojít k hackerskému útoku. V minulosti již opravdu byla zaznamenána snaha o odcizení dat za účelem odcizení peněz. Může také dojít k porušení mlčenlivosti partnerů (dodavatelé, odběratelé, externí subjekty), kteří mají přístupy k citlivým údajům.

Na straně zaměstnanců vidím příčiny ve zneužití přístupů a oprávnění, které vedou k využívání dat ve vlastní prospěch. Další příčinou může být odesílání dat neoprávněným osobám, ať už vědomě či nevědomě, či vědomé poškozování firmy.



Obr. č. 15: Ishikawa diagram – Riziko zneužití dat (Zdroj: vlastní zpracování)

Ztráta dat (29,4)

Ke ztrátě dat může dojít z různých příčin. Většina příčin pramení z informačních systémů nebo ze serverů, kde jsou data uchována. Počítač, který je ve špatném stavu, může zapříčinit výmaz dat na lokálním disku. Slabé zabezpečení dat může znamenat taktéž ztrátu.

Zaměstnanec může být nepozorný a data omylem vymazat nebo neuložit. Taktéž nemusí data evidovat kvůli domněnce nepotřebnosti dat.

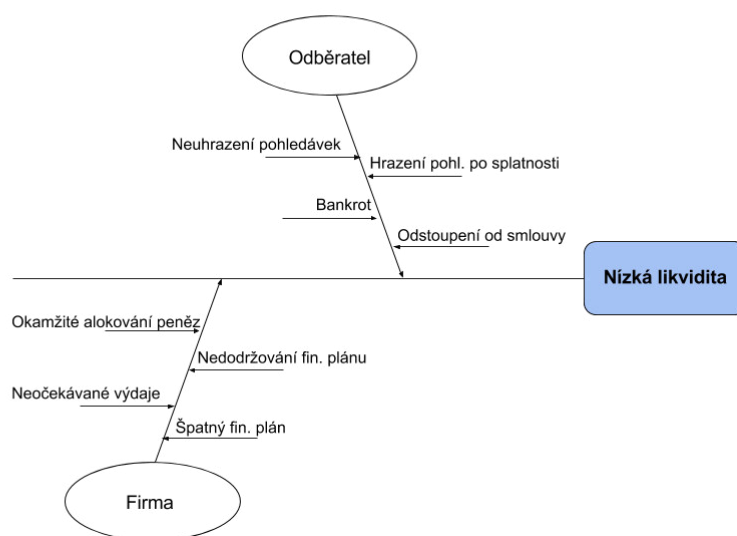
Z okolí mohou přijít hackerské útoky nebo může nastat havárie – výpadek internetového připojení, elektrického proudu, požár, zemětřesení nebo také k výpadku serverů na straně dodavatele.

Nízká likvidita (34,1)

Nízká likvidita byla ohodnocena jako riziko s nejvyšším dopadem v kategorii procesních rizik. Díky nízké likviditě, tedy nízkému cashflow, se může firma dostat do platební neschopnosti. Příčiny vidím zejména ve špatném finančním plánu, který

neodráží realitu, v neočekávaných výdajích (např. penále) a v nedodržování finančního plánu (plán cashflow). Také mohou přijít tlaky z mateřské společnosti o alokování peněz mezi jiné entity.

Další příčiny mohou být na straně odběratelů. Ti mohou přestat hradit faktury nebo mohou hradit faktury po splatnosti. Také může z různých důvodů dojít k úbytku samotných odběratelů.



Obrázek 16: Ishikawa diagram – Riziko nízké likvidity (Zdroj: vlastní zpracování)

4 VLASTNÍ NÁVRHY

V analytické části této diplomové práce byla identifikována a analyzována rizika, která mají na FSS největší dopad. V následující podkapitole navrhnou opatření ke všem rizikům, která jsou ovlivnitelná a povedou k minimalizaci výskytu nebo dopadu těchto rizik. Vycházet budu z výsledků analýz a důraz budu klást na návrhy k rizikům, která mají na FSS největší dopad.

Jelikož FSS nikdy neprovádělo analýzy, monitoring, a tudíž ani vyhodnocování rizik, bylo by v zájmu celé společnosti, aby tak začala konat. Dle mého názoru by společnost měla vytvořit konkrétní pracovní pozici, díky které by byla:

1. identifikována
2. analyzována
3. hodnocena
4. monitorována
5. snižována rizika

Pracovní pozice by měla požadovat takového pracovníka, který strávil v Zebra Technologies alespoň tři roky a pracoval nejméně ve dvou odděleních, aby se vyznal alespoň v části procesů.

Pracovník by měl být komunikativní a proaktivní se zájmem o zdokonalování procesů a měl by to být vyloženě perfekcionista. Měl by mít pravidelné schůzky s teamleadery jednotlivých týmů, na kterých by probírali jednotlivé procesy a z nich plynoucí problémy. Organizačně by mohl být zařazen do oddělení Finance Analysis. Pracovní pozice by byla nazvána Risks Analyst (Analytik rizik) a zodpovědný by byl přímo řediteli.

Náklady na opatření

Při hrubé mzdě 30 000 Kč pro analytika rizik by náklady pro firmu, po zohlednění daně, slevy na poplatníka a zdravotního a sociálního pojištění činily **40 200 Kč** měsíčně.

Druhou variantou je, přiřadit tyto kompetence manažerům a to tím způsobem, že každý manažer by prováděl jmenované úkoly, týkajících se jeho oddělení. Výhodou může být dokonalá znalost procesů, nevýhodou časová vytíženost.

4.1 Bezvýznamná rizika

U většiny bezvýznamných rizik, tedy u rizik, která mají nízkou tvrdost (dopad) a nízkou pravděpodobnost (možnost výskytu) navrhuji **retenci** (podstoupení) rizik. I kdyby se rizika vyskytla, jejich dopad nebude tak závažný a náklady na jejich snížení mohou být vyšší než škoda, kterou by mohla napáchat.

Ekonomická situace v ČR – riziko je neovlivnitelné, nezbyvá nic jiného než retence.

Nedodržování právních předpisů – náklady na outsourcing právních služeb nebo zaměstnání experta nebo expertů v oblasti potřebných zákonů mohou být příliš vysoké, proto vzhledem k bezvýznamnosti rizika navrhuji retenci.

Informační riziko – z části řeší návrh nového informačního systému, viz podkapitola 4.4.2.

Demokratické řízení – navrhuji retenci, jelikož se jedná o riziko s takřka neměřitelným dopadem. Riziko není managementem ani nijak vnímáno.

Delegování pravomocí – i když je riziko bezvýznamné, přinést může pouze pozitiva v efektivnosti zaměstnanců. Proto navrhuji externí školení pro všechny teamleadery, případně i pro manažery, pokud neabsolvovali stejné či obdobné školení. Školení bych zaměřil obecně na téma „Time management“ nebo přímo na téma „Efektivní delegování“. Školení jsou outsourcována společností *TLC Trainings and Languages, s.r.o.*, kde školí čeští i mezinárodní lektori a výhoda spočívá v tom, že všechna školení se mohou přímo adaptovat na poptávku Zebry a zaměstnanec má školení ve formě benefitu.

Náklady na opatření

Cena jednoho celodenního školení je 27 000 Kč. Při úvaze časové vytíženosti teamleaderů a manažerů navrhuji dvě školení, celková cena opatření by tedy byla **54 000 Kč**. Je třeba brát v potaz i náklady ušlé příležitosti, které by vznikly za předpokladu účasti na školeních.

Duplikování práce – z části řeší návrh nového informačního systému, viz podkapitola 4.4.2.

Nemoc – v úvahu přichází investice do podpory sportování a zdravého životního stylu, nicméně navrhuji retenci vzhledem k riziku s bezvýznamným dopadem.

Všechna *procesní rizika* (penále z prodlení, ztráta faktury, nevystavení faktury a chybné zaúčtování) by měl z části řešit návrh nového IS.

4.2 Běžná rizika

Vyznačují se vysokou pravděpodobností výskytu, ovšem nízkou tvrdostí. V úvahu přichází **retence a redukce rizik**.

Legislativní změny – riziko je aktivně redukováno a to formou pravidelných školení, které se týkají nejnovější legislativy. Managementu dále chodí pravidelné newslettery (od školicích agentur), týkající se české legislativy a newslettery, které se týkají legislativy jiných států (od auditorských společností).

Komunikační riziko – v úvahu přichází opět školení či schůzky se zaměstnanci, vzhledem k dopadu však navrhuji retenci rizika.

Jazykové bariéry – v tomto případě firma zabezpečuje pro své zaměstnance jazykové semestrální kurzy, navíc zaměstnanec komunikuje většinu pracovní doby v cizím jazyce. Domnívám se, že v tomto ohledu je uděláno maximum a doporučuji retenci rizika.

Procesní rizika (nezaplacení faktury, opožděná platba) by měl opět z části minimalizovat nový IS.

4.3 Významná rizika

Významná rizika mají sice malou pravděpodobnost výskytu, na druhou stranu, jejich dopad může být velmi tvrdý. Většinou se volí **pojištění** rizik, právě z důvodu tvrdého, v některých případech až katastrofálního dopadu.

Živelné pohromy a havárie – vhodným nástrojem pro snížení těchto rizik je právě pojištění. FSS je pojištěno proti požáru, úderu blesku, výbuchu, nárazu nebo zřícení letadla, zemětřesení, kouři, vodě z vodovodního zařízení a dalším rizikům. Pojištění sice kryje určitá rizika, nicméně nekompenzuje ztráty, které vzejdou z nečinnosti FSS. To musí podávat jasné výstupy. Pro takové potřeby jsou vypracovány

tzv. „Business recovery“ plány, které spočívají v přesném postupu, jak se chovat při zmíněné kritické situaci, aby byly zachovány alespoň hlavní kritické činnosti.

Plány jsou sice vypracovány, ovšem pouze v rámci FSS jakožto celku. Nikdy nebyly zpracovány pro jednotlivé týmy a jejich součinnost.

Z toho důvodu navrhuji vypracování „Team recovery“ plánu, který by zajišťoval hlavní kritické činnosti na úrovni všech týmů, za předpokladu nastání kritické situace. V plánu by měly být zpracovány manuály, které činnosti je třeba zajistit ze všeho nejdříve. Každý teamleader by měl oboznámit svůj tým o tom, že tyto plány existují a jak se k nim dostane. O těchto plánech by zároveň měli vědět i teamleadeři, sídlící ve FSS v Penangu (Malajsie), aby byli schopni pokrýt část procesu. Zároveň každý člen, vlastnící firemní laptop, by si jej měl každý den brát s sebou pro případ výskytu takových rizik.

Náklady na opatření

Jsou **nulové**, jelikož by vypracování takových plánů spadalo do pracovní náplně zaměstnanců.

Terorismus – proti tomuto riziku jsou taktéž nastavena opatření. Součástí budovy, kde FSS sídlí, je i bezpečnostní služba fungující 24 hodin denně a ve všech prostorech kromě toalet jsou bezpečnostní kamery. Pro případ výskytu terorismu je taktéž zpracován „Business recovery“ plán, proto si myslím, že k minimalizaci tohoto rizika je uděláno maximum.

Ekonomická situace společnosti – je ovlivnitelná pouze z části a to formou řízení FSS a odvedených výsledků. Nástroji ke zlepšení ekonomické situace společnosti mohou být všechny ostatní návrhy vedoucí k vyšší efektivitě práce a samozřejmě ke snížení rizik.

Zneužití dat – proti tomuto riziku volím nástroj pojištění rizik a to formou koupě zabezpečovacího systému, který by stál v pozadí nového informačního systému. Jeho hlavním cílem by bylo zabezpečovat data na dvou úrovních. První úroveň by se týkala útokům zvnějšku a druhá interních pracovníků.

V každém počítači sice již je nainstalovaný antivirový program, nicméně ten zabezpečuje data pouze na první úrovni.

Nový software by měl pracovat na pozadí každého počítače a měl by monitorovat zejména externí komunikaci a to tak, aniž by o tom daný uživatel věděl. Nejednalo by se o kontrolu činnosti zaměstnanců ani o špehování. Systém by měl pracovat na bázi algoritmu, který by vyhodnocoval rizikový přenos dat jak směrem ven, tak směrem dovnitř. Rizikové případy by systém měl vyhodnocovat a reporty posílat managementu FSS.

Pro potřeby FSS navrhuji zakoupit software *Kaspersky Total Security for Business*, u kterého jsou hlavní výhody především ve vícevrstvé ochraně, automatické detekci zranitelných míst, ochraně před ztrátou údajů a funkci filtrování obsahu a souborů, která zabezpečuje bezpečnější spolupráci s externími subjekty.

Se správným zabezpečením dat souvisí i další riziko, kterým je ztráta dat. Firma Kaspersky Lab CZ (2015) uvádí, že až čtvrtina internetových útoků končí ztrátou dat.

Náklady na opatření

Pořízení tohoto konkrétního softwaru pro 100 pracovních jednotek (91 zaměstnanců) vychází na 5 819,96 USD/rok, v přepočtu **138 102 Kč/rok**.²¹

Ztráta dat – firma proti riziku ztrátě dat používá software, který automaticky dělá zálohy systémů a souborů. Všechny zálohované soubory se ukládají na servery, které jsou umístěny v Chicagu (USA). Jednou však došlo k výskytu rizika živelné pohromy, hurikánu, v Chicagu a jeho okolí, který zapříčinil výpadky elektrické energie a internetového připojení a zálohy nebyly po několik dnů k dispozici. Naštěstí se podařilo zálohy obnovit.

Zejména z tohoto důvodu navrhuji, aby interní auditoři pravidelně kontrolovali (měsíčně), zda zálohovací systém funguje a s jakou odezvou.

Náklady na opatření

Nulové, jelikož by činnost spadala do pracovní náplně interních auditorů.

Procesní rizika (zkreslení informací, externí audit, zkreslení dat, nevyplacení mzdy, neodvedení zákonného pojištění, nízká likvidita a zpronevěra peněz) budou zahrnuta v návrhu nového IS.

²¹ Při kurzu ČNB, k 12. 5. 2016

4.4 Kritická rizika

Kritická rizika představují pro firmu to největší nebezpečí. Typická je u nich jak vysoká tvrdost dopadu, tak vysoká pravděpodobnost výskytu. Užívanými nástroji k minimalizování těchto rizik je **vyhnoutí se riziku** nebo **redukce rizika**. Vzhledem k analyzovaným rizikům není první nástroj téměř aplikovatelný, proto se budu snažit navrhnout co nejefektivnější řešení, vedoucí k redukci následujících rizik.

Výpadky internetového připojení – jak již bylo řečeno v analytické části, bez internetu není schopen personál fungovat. Proto bylo toto riziko ohodnoceno jako kritické. FSS je napojeno na optický kabel, skrze který je dodáváno připojení k internetové síti. Proto cokoliv, co se stane s optickým kabelem (a riziko je zvýšené, kvůli výstavbovým pracím v Technologickém parku – např. překopnutí kabelu), znamená odstávku internetu. Řešením může být připojení druhého kabelu, to však není příliš reálné vzhledem k pronájmu budovy i služeb od externího subjektu.

Proto navrhuji jednoduché řešení – zřídit internetovou síť do prostor FSS i skrze pevnou linku. Ta by tak byla schopna krýt výpadek optického vlákna.

Náklady na opatření

Zavedení internetového připojení skrz pevnou linku pro potřeby a velikost FSS vychází průměrně na **3 500 Kč/měsíčně**.

Automatizace – toto riziko může přinášet několik problémů, do kterých musí zasáhnout člověk, nicméně se domnívám, že proces automatizace je při dnešních podmínkách vývoje informačních technologií zcela běžný, proto u tohoto rizika navrhuji retenci.

4.4.1 Návrh na standardizaci procesů

Složitost procesů byla hodnocena jako třetí nejrizikovější. Je běžné, že procesy, které by měly být naprosto totožné, se kompletně liší. Konkrétně, avšak velmi zjednodušeně, uvedu na příkladu účtování daní v přijatých fakturách v AP oddělení v týmu EMEA a v týmu NA.

Účtování daní v EMEA týmu je jednodušší v tom, že daň by se měla vypočítat stiskem jednoho tlačítka, případná úprava daně je velmi intuitivní a systém ji víceméně dopočítá automaticky.

Na rozdíl od EMEA týmu, v NA týmu probíhá zaúčtování daně manuálně, kdy v systému není ani vytvořeno tlačítko na výpočet daně. Ta se musí dopočítat skrze několik modulů a díky tomu zabere více času. V NA týmu je typické i rozdílné zaúčtování a dopočítání daní u různých entit. Např. systém není schopen dopočítat daň u americké entity, na rozdíl od kanadské.

Zejména kvůli rozdílným procesům v jinak stejném oddělení navrhuji standardizaci procesů, které by byly schopny minimalizovat několik dalších rizik vyplývajících z procesu. Zejména mluvím o zastupitelnosti zaměstnanců. Na příkladu uvedu, že nemoc jednoho zaměstnance, který účtuje americkou entitu, může znamenat neschopnost účtování jiného zaměstnance na téže entitě kvůli rozdílnému procesu.

Konkrétně navrhuji dokumentaci procesů ve formě manuálu ke každému procesu. Vypracování manuálu by měl na starosti konkrétní zaměstnanec, který proces provádí. Při výpadku jednoho zaměstnance to může znamenat jednoduché pokrytí daného procesu. Dále navrhuji pravidelnou (čtvrtletní) kontrolu těchto manuálů skrze vztah nadřízený – podřízený a pravidelné kontroly procesů skrze interní auditory. Ve firmách s akciemi na americké burze navíc funguje systém dvojích kontrol SOX viz podkapitola 3.4.1, která kontroluje, zda se kontroly ve firmách dějí.

Náklady na opatření

Jsou **nulové**. Zaměstnanci by dokumentaci procesů měli v náplni práce.

Komplexnějším řešením je inovace stávajícího účetního IS Oracle Trilogy a procesy naprogramovat stejně (v součinnosti s IT) nebo procesy standardizovat přímo v novém IS, viz následující podkapitola.

4.4.2 Návrh nového informačního systému

Práce v informačních systémech je naprosto stěžejní pracovní náplní všech zaměstnanců, proto bylo toto riziko, dle mého názoru, ohodnoceno právem jako nejvyšší.

Osobně se domnívám, že většina příčin, které byly analyzovány, by neměly vést k nefunkčnosti IS. Proto navrhuji transfer na nový informační systém.

Ten by měl za cíl být funkční i při mnoha připojených uživateli, při nesprávně zadaných příkazech, datech, při pokusu o vnější útok i při špatném stavu počítače.

Dalším cílem nového IS by mělo být minimalizování většiny procesních rizik, která jsou na IS závislá. Jde o následující analyzovaná rizika: složitost procesů, aktuálnost, nesplnění termínů, neuhrazení pohledávky, zkreslení informací, externí audit, zkreslení dat, nevyplacení mzdy, neodvedení zákonného pojištění, nízká likvidita, zpronevěra peněz, nezaplacení faktury, opožděná platba, penále z prodlení, ztráta faktury, nevystavení faktury a chybné zaúčtování.

Konkrétně navrhuji implementaci systému Oracle, verze Merlin, což je rozšíření stávající verze Trilogy. Hlavní výhodou je, že implementace spočívá v upgradu stávající verze a není potřeba programovat a platit úplně nový IS. Nová verze by měla minimalizovat většinu procesních rizik a bude možno naimplementovat potřebné funkce a moduly, které by měly standardizovat stávající procesy.

Funkce, které by měl nový systém mít:

1. **Helpdesk Tool** – při dotazu od externího subjektu, který pošle dotaz emailem, by měl systém automaticky vygenerovat „ticket“, který by byl přiřazen konkrétnímu zaměstnanci, který má danou problematiku na starosti.
2. **Standardizace procesů** – všechny způsoby účtování by měly být naprogramovány stejně.
3. **Task manager** – součástí IS by měl být modul, do kterého by si každý zaměstnanec psal své úkoly, a systém by dohlížel na jejich plnění. Proces by tak byl tak zautomatizován, že např. při vytvoření ticketu se automaticky vygeneruje a přiřadí i nový úkol.
4. **Vystavování faktur** – systém by měl automaticky na základě vytvořené objednávky vystavit fakturu a poslat ji odběrateli, a zároveň odběratele upomínkovat ke splatnosti.
5. **Automatizace** – na základě zadaných dat, ať už automaticky nebo manuálně, by měl být systém schopen vytvořit např. report podle nastavených kritérií.

6. **Dvojitá kontrola (double check)** – poté, co by byl automaticky vyřešen problém, task manager by vytvořil upomínku, která by přišla odpovědnému zaměstnanci, aby situaci překontroloval, případně schválil nebo zamítnul a zaměstnanec ji dořešil manuálně.
7. **Proces schvalování (workflow)** – u daných procesů je potřeba několika schválení, jelikož sumy u určitých procesů to vyžadují. Z tohoto důvodu by task manager filtroval úkoly dle kategorie a priority nadřazeným, kteří by měli za úkol buď schválit, nebo zamítnout situaci a vrátit ji tak příslušnému zaměstnanci.
8. **Algoritmy k likviditě a plánování (cashflow)** – do samostatného modulu je potřeba naprogramovat i algoritmy, které by pomáhaly finančnímu plánování (vestavěné finanční ukazatele a výpočty) a které by sledovaly likviditu a navrhly další kroky, vyplývající z finančních ukazatelů (na základě výpočtů), vedoucí ke zvýšení likvidity.
9. **Nahrávání faktur** – dodavatelé by měli mít možnost nahrát své faktury do systému sami. Měl by být naprogramován algoritmus, který po nahrání faktury do systému automaticky překontroluje fakturu a pokud všechny potřebné údaje souhlasí, task manager by odeslal upozornění odpovědnému zaměstnanci, který by fakturu zaúčtoval. Pokud by chyběl nějaký potřebný údaj, faktura by byla automaticky navracena dodavateli.

Navržené funkce v novém IS, by měly minimalizovat většinu z analyzovaných procesních rizik.

Náklady na opatření

V současné době se plánuje transformace na jeden informační systém v rámci celé společnosti. Částku nejsem schopen vyčíslit přímo pro FSS, nicméně naplánované náklady samotné společnosti na transformaci celého informačního systému a doprovodných procesů činí 250 mil. USD, což je v přepočtu **5,932 mld. Kč**.

4.4.3 Návrh motivačního programu pro zaměstnance

Riziko **odchodu zaměstnanců** bylo hodnoceno jako druhé největší. Společnost se snaží aktivně vytvářet co nejlepší podmínky pro zaměstnance, protože si uvědomuje, že odliv znalostního kapitálu může být v jistém ohledu problémem.

Jsou rozlišovány pozice „snadno nahraditelné“ a pozice, na kterých je potřeba více znalostí a zkušeností. U těchto pozic je potřeba zvýšené ostražitosti a hlavně individuálního přístupu. V praxi to probíhá tak, že managementem jsou vytipováni konkrétní zaměstnanci a s těmi se pracuje v závislosti, na jakou pozici jsou dále směřováni. Konkrétní zaměstnanci jsou trénováni a školeni, aby byli připraveni na jejich budoucí povýšení a veškeré předání pozice mohlo proběhnout bez větších komplikací. Jde o takovou formu nástupnictví, která zabezpečuje plynulé fungování FSS. S tímto individuálním přístupem nástupnictví souhlasím, protože pro firmu je to promyšlený postup, jak pracovat s rozvojem a udržení lidských zdrojů a hlavně znalostního kapitálu.

Firma se snaží udržet zaměstnance i formou benefitů, kterými jsou:

- jazykové kurzy
- dovolená nad rámec zákona (25 pracovních dní)
- školení
- penzijní fond
- volnočasové aktivity (teambuildingy, firemní večírky)
- příspěvek na sport (fitness program)
- příspěvek na stravné v místní kantýně

Osobně si myslím, že k udržení lidského kapitálu ve firmě může dopomoci několik chybějících benefitů. Proto navrhuji zavedení cafeteria systému. Ten by umožňoval výběr z benefitů, které si zaměstnanec sám vybere. Tento systém využívá dle průzkumu ABSL (2016, s. 32) 49 % center sdílených služeb.

Do balíku dostupných benefitů navrhuji vedle již zavedených benefitů zahrnout:

1. **firemní akcie** – dle mého názoru jsou firemní akcie výborný motivační nástroj. Zaměstnanec při vlastnictví podílu může cítit větší zodpovědnost vůči firmě, což ho může motivovat k lepšímu pracovnímu výkonu.
2. **příspěvek na sport** – poukazy nebo přímo finanční příspěvky na konkrétní sporty. Příspěvek na sport v zavedených benefitech totiž umožňuje využívání pouze jednoho fitness centra v Brně.

3. **postgraduální příspěvky** – zaměstnanci, kteří se chtějí nadále vzdělávat, by měli být podporováni. To znamená příspěvky, které by kryly část nákladů na studium, školení, kurzy, certifikáty nebo odbornou literaturu.
4. **stravenky** – stravenky v současné době ve firmě nejsou, což si myslím, že je velké negativum. Zaměstnanec nemá jinou možnost, než se stravovat v místní zaměstnanecké kantýně, pokud chce na příspěvek dosáhnout.
5. **balíček lékařské péče** – týkal by se příspěvku na lékařskou péči nebo farmaceutika.
6. **pravidelné cvičení** – finance jsou obor, který přináší do života spoustu stresu, výjimkou není ani práce od počítače přímo v kanceláři, proto navrhuji zavedení dobrovolných lekcí jógy (2x týdně, 30 minut), či podobných cvičení na posílení ducha přímo ve vyhrazené místnosti ve FSS. Lekce by mohly v letních měsících probíhat i v příjemném venkovním prostředí okolo sídla FSS.

Navržený motivační program, který by minimalizoval riziko odchodu zaměstnanců, by tedy spočíval v balíčku základních benefitů:

- 25 dní dovolené
- školení
- stravenky
- volnočasové aktivity (teambuildingy, firemní večírky)
- balíček lékařské péče
- pravidelné cvičení

a cafeterie systému (libovolně volitelné benefity)

- firemní akcie
- příspěvek na sport (fitness i další sportovní aktivity)
- penzijní fond
- postgraduální příspěvky

Náklady na opatření

Jelikož navrhuji zavedení systému cafeterie, benefity by měly být ve stejné nebo přibližné hodnotě, aby si zaměstnanci nevybírali ty nejnákladnější benefity. Příspěvek

na sport navrhuji 500 Kč/měsíčně pro každého zaměstnance. Při 91 zaměstnancích to znamená 45 500 Kč/měsíčně. Ve stejné výši by byl příspěvek na postgraduální studium i příspěvek na penzijní fond. U firemních akcií nejsem schopen odhadnout celkové náklady, nicméně měsíční náklady by měly být z hlediska rovnoprávnosti a možnosti svobodné volby výběru ve stejné výši jako ostatní volitelné benefity, tedy **45 500 Kč**.

Příspěvek na stravování navrhuji ve formě stravenek, kdy si firma může uznat daňový náklad v maximálně 70% výši, kterou nová vyhláška MPSV zvýšila na 83 Kč za den. Maximální daňová úleva se projeví při stravence ve výši 105 Kč/den, kdy je zaměstnavatel povinen hradit 55 % z ceny stravenky, což je 57,75 Kč/den. (Hovorková, 2016). Při 252 pracovních dnů a 91 zaměstnanců to je **1 324 323 Kč** za rok.

Balíček lékařské péče, který by byl v základním balíčku benefitů, by činil 300 Kč/měsíc, což je pro všechny zaměstnance celkem **27 300 Kč/měsíčně** s tím, že kdyby jej zaměstnanec nevyužil, měl by nárok využít benefit k nákupu výrobků souvisejících s péčí o zdraví. Např. vitamínů, doplňků stravy nebo jiných zdravotnických pomůcek či farmaceutik.

Pravidelné cvičení by se konalo dvakrát týdně, tedy osmkrát do měsíce. Jedno cvičení vychází zhruba na 600 Kč, což je **4 800 Kč/měsíc**.

Tab. č. 6: Náklady na zavedení nových benefitů (Zdroj: vlastní zpracování)

Benefit	Náklady
sport	45 500 Kč
postgraduální studium	45 500 Kč
penzijní fond	45 500 Kč
firemní akcie	45 500 Kč
stravenky	110 360 Kč
lékařská péče	27 300 Kč
cvičení	4 800 Kč
celkem	187 960 Kč

Měsíční náklady nových opatření, které by snižovaly riziko odchodu zaměstnanců, jsou **187 960 Kč** (v celkové sumě je zahrnut pouze jeden z volitelných benefitů).

4.5 Přínos návrhů

Centra sdílených služeb jsou ověřeným konceptem po celém světě. Důkazem je toho celé rostoucí odvětví v České republice. Při vyhodnocování rizik bylo zjištěno, že minimálně základní opatření na většinu rizik již existuje. Snažil jsem se však navrhnout opatření, která by analyzovaná rizika minimalizovala důsledněji a s větší efektivností.

Nejzásadnějším návrhem vyplývajícím z kritických rizik, by pro firmu byl nový informační systém Oracle Merlin, díky kterému by bylo možno minimalizovat zejména rizika, která vyplývají z jednotlivých procesů.

Ke standardizaci procesů jsem zvolil vypracování manuálů a následné kontroly před implementací nového IS. Po implementaci nového IS by byl problém se standardizací z části vyřešen. Přínosem by byla zejména zastupitelnost chybějících zaměstnanců a proces by mohl být dál vykonáván jiným zaměstnancem.

K riziku odchodu zaměstnanců jsem navrhl motivační program pro zaměstnance, zejména zavedení nových benefitů a systému cafeterie. Jako výstup si představuji méně výpovědí ze strany zaměstnanců a zachování znalostního kapitálu ve firmě.

U rizika výpadku internetového připojení je dle mého názoru řešením zabudování nové sítě formou pevné linky, která by nahrazovala optický kabel v případě přerušení internetového připojení. Znamenalo by to zabezpečení plynulé činnosti i v případě, že dojde k výpadku jednoho zdroje.

K významným rizikům jsem navrhl „Team recovery“ plán, který by popisoval přesný sled událostí při živelné pohromě, havárii nebo teroristickém útoku. Za cíl by měl zachování chodu FSS i po zmíněných událostech.

Proti zneužití dat by byl jistě přínosem nový zabezpečovací software, který by chránil systémy jak z venku, tak zevnitř. U ztráty dat bych zvážil interní audity na měsíční bázi, z důvodu funkčnosti záloh.

U běžných rizik jsou již zavedené mechanismy ke snižování, proto jsem u většiny navrhl retenci rizik.

K bezvýznamným rizikům jsem navrhl školení pro střední, případně i vyšší management na téma „Time management“ nebo „Efektivní delegování“, které by mělo zvýšit efektivitu práce.

Jelikož FSS nikdy neprovádělo analýzy rizik, navrhl jsem vytvořit pracovní pozici „Risks Analyst“, která by měla za úkol rizika zejména analyzovat a vyhodnocovat.

ZÁVĚR

Cílem diplomové práce byla identifikace, analýza a hodnocení rizik, která vyplývají z řízení procesů ve finančním středisku sdílených služeb v mezinárodní společnosti Zebra Technologies a výstupem měly být takové návrhy vlastních řešení, které by minimalizovaly dopady jednotlivých rizik.

Teoretickou část jsem zaměřil na pojmy nezbytné k pochopení dané problematiky. Jednalo se o procesní management, prostředí firmy, rizika, management rizik a na centra sdílených služeb.

V analytické části jsem analyzoval celou společnost, středisko sdílených služeb a jeho finanční středisko sdílených služeb. Následně jsem analyzoval procesy v odděleních Accounts Receivable, Accounts Payable, General Ledger, Finance Analysis, Payroll a Treasury, tudíž ve všech odděleních finančního centra v Brně. Poté jsem za pomoci PEST analýzy analyzoval vnější a pomoci rozboru 7S faktorů firmy McKinsey vnitřní prostředí FSS. Z těchto analýz jsem byl schopen identifikovat silné a slabé stránky a příležitosti a hrozby. Přešel jsem k identifikaci rizik, která jsem rozdělil na obecná, vnější, vnitřní a procesní rizika. Díky identifikaci rizik jsem začal analyzovat a hodnotit jednotlivá rizika pomocí skórovací metody s mapou rizik za přispění osmi expertů. Vybraná kritická a významná rizika jsem podrobil analýze příčin a důsledků.

Veškeré poznatky nabyté z teoretických východisek, analytické části, osobní praxe a osobních konzultací jsem aplikoval do poslední, návrhové části této práce.

Ve vlastních návrzích jsem dospěl k závěru, že mnoho rizik je již z části pokryto, zejména kvůli ověřenému, převzatému konceptu sdílených služeb. I přesto jsem našel nedostatky, díky kterým jsem navrhl vytvoření pozice „Risks analyst“, nový informační systém, standardizaci procesů, motivační program pro zaměstnance, vybudování nové internetové sítě, „team recovery“ plány, nový zabezpečovací software, pravidelné interní audity záloh a nová témata na školení zaměstnanců.

Závěrem bych rád konstatoval, že hlavní přínos této práce shledávám v tom, že dosud neexistuje žádná práce, která by se věnovala přímo rizikům ve finančních centrech sdílených služeb v České republice, natož přímo ve společnosti Zebra Technologies CZ s.r.o. Proto si myslím, že z této práce může čerpat nejenom Zebra

Technologies, ale i ostatní finanční nebo i jiná sdílená centra a to zejména díky metodice použité v analytické a návrhové části. Veškeré poznatky mohou být využity při znalostním a procesním managementu a řízení kvality.

SEZNAM POUŽITÉ LITERATURY

Monografie

ARMSTRONG, M. Řízení lidských zdrojů: nejnovější trendy a postupy. 10. vyd. Praha: Grada, 2007. 800 s. ISBN 978-80-247-1407-3.

BANGEMANN, T. O. Shared services in finance and accounting. Burlington, VT: Gower, 2005, xiv, 246 p. ISBN 0566086077.

DOLEŽAL, J., P. MÁCHAL a B. LACKO. Projektový management podle IPMA. 1. vyd. Praha: Grada, 2009. 507 s. Expert (Grada). ISBN 978-80-247-2848-3.

FÍŠER, Roman. Procesní řízení pro manažery: jak zařídit, aby lidé věděli, chtěli, uměli i mohli. 1. vyd. Praha: Grada, 2014, 173 s. Manažer. ISBN 978-80-247-5038-5.

FOTR, J. a I. SOUČEK. Investiční rozhodování a řízení projektů: jak připravovat, financovat a hodnotit projekty, řídit jejich riziko a vytvářet portfolio projektů. 1. vyd. Praha: Grada, 2011, 408 s. Expert (Grada). ISBN 978-80-247-3293-0.

FOTR, J. a J. HNILICA. Aplikovaná analýza rizika ve finančním managementu a investičním rozhodování. 2., aktualiz. a rozš. vyd. Praha: Grada, 2014, 299 s. Expert (Grada). ISBN 978-80-247-5104-7.

FUCHS, P. a D. VALIŠ. Metody analýzy řízení rizika. Liberec, 2004, 35 s. Skriptum. Technická univerzita v Liberci.

GRASSEOVÁ, M., R. DUBEC a R. HORÁK. Procesní řízení ve veřejném sektoru: teoretická východiska a praktické příklady. 1 vyd. Brno: Computer Press, 2008. 266 s. ISBN 978-80- 251-1987-7.

GREAVES, M. F. Strategic outsourcing: a structured approach to outsourcing decisions and initiatives. New York: AMACOM, 1999, xix, 314 s. ISBN 0-8144-0434-0.

HAMMER, M. a J. CHAMPY. Reengineering - radikální proměna firmy: manifest revoluce v podnikání. 3. vyd. Praha: Management Press, 2000. 212 s. ISBN 80-7261-028-7.

JAKUBÍKOVÁ, D. Strategický marketing. 1. vyd. Praha: Grada, 2008, 269 s. Expert (Grada). ISBN 978-80-247-2690-8

JÍLEK, Josef. Finanční rizika. 1. vyd. Praha: Grada, 2000, 635 s. Finance (Grada). ISBN 80-7169-579-3.

MALLYA, T. Základy strategického řízení a rozhodování. 1. vyd. Praha: Grada, 2007, 246 s. Expert (Grada). ISBN 978-80-247-1911-5.

MARR, B. Key performance indicators: the 75 measures every manager needs to know. 1st ed. New York: Pearson Financial Times Pub., 2012, xxviii, 347 p. ISBN 0273750119.

PETRÁČKOVÁ, V. a J. KRAUS. Akademický slovník cizích slov. 1. vyd. Praha: Academia, 1995, 2 v. ISBN 80200052422.

RAIS, K. a R. DOSKOČIL. Risk management: studijní text pro kombinovanou formu studia. 1. vyd. Brno: Akademické nakladatelství CERM, 2007, 152 s. ISBN 978-80-214-3510-0.

RYDVALOVÁ, P. aj. RYDVAL. Outsourcing ve firmě: průvodce pro manažera s tipy pro české prostředí. 1. vyd. Brno: Computer Press, 2007, vii, 102 s. ISBN 978-80-251-1807-8.

ŘEPA, V. Podnikové procesy: procesní řízení a modelování. 2., aktualiz. a rozš. vyd. Praha: Grada, 2007, 281 s. Management v informační společnosti. ISBN 978-80-247-2252-8.

SMEJKAL, V. a K. RAIS. Řízení rizik ve firmách a jiných organizacích. 4., aktualiz. a rozš. vyd. Praha: Grada, 2013, 488 s. Expert (Grada). ISBN 978-80-247-4644-9.

STAPENHURST, T. The benchmarking book: a how-to-guide to best practice for managers and practitioners. Amsterdam: Elsevier Butterworth-Heinemann, 2009, xli, 454 s. ISBN 978-0-7506-8905-2.

TICHÝ, M. Ovládání rizika: analýza a management. 1. vyd. Praha: C.H. Beck, 2006, xxvi, 396 s. Beckova edice ekonomie. ISBN 80-7179-415-5.

VLACHÝ, Jan. Řízení finančních rizik. 1. vyd. Praha: Vysoká škola finanční a správní, 2006. 256 s. ISBN 80-86754-56-1.

VOCHOZKA, M. a P. MULAČ. Podniková ekonomika. 1. vyd. Praha: Grada, 2012, 570 s. Finanční řízení. ISBN 978-80-247-4372-1.

Internetové zdroje

ABSL. *Sdílené podnikové služby v České republice výrazně rostou*. [online]. 2015 [cit. 2016-04-21]. Dostupné z: http://www.absl.cz/docs/press%20releases/TZ_ABSL_vysledky_151019_FIN.pdf

Brno.cz. *Brno - Ekonomika v číslech*. [online]. 2016 [cit. 2016-04-20]. Dostupné z: <https://www.brno.cz/podnikatel-investor/ekonomika-v-cislech/>

Business.center.cz. *Systematické riziko*. [online]. 2015 [cit. 2015-12-02]. Dostupné z: <http://business.center.cz/business/pojmy/p1960-systematicke-riziko.aspx>

Businessinfo.cz. *Dotace pro ICT: 20 miliard na vývoj software, rychlé sítě a centra sdílených služeb*. [online]. 2015 [cit. 2016-04-21]. Dostupné z: <http://www.businessinfo.cz/cs/clanky/dotace-pro-ict-20-miliard-na-vyvoj-software-rychle-site-a-centra-sdilenych-sluzeb-63612.html>

Česká televize. *Americký sen energetické firmy Enron skončil bankrotem*. [online]. 2011 [cit. 2016-04-23]. Dostupné z: <http://www.ceskatelevize.cz/ct24/ekonomika/1206300-americky-sen-energeticke-firmy-enron-skoncil-bankrotem>

ČEVELOVÁ, M. *Bostonská matice*. Cevelova.cz [online]. 2010 [cit. 2016-03-18]. Dostupné z: <http://www.cevelova.cz/bostonska-matice/>

ČSÚ. *ÚROVEŇ VZDĚLÁNÍ OBYVATELSTVA PODLE VÝSLEDKŮ SČÍTÁNÍ LIDU*. [online]. 2014 [cit. 2016-04-20]. Dostupné z: <https://www.czso.cz/documents/10180/20536250/17023214.pdf/7545a15a-8565-458b-b4e3-e8bf43255b12?version=1.1>

FANTA, P. *Outsourcing*. [online – Autoreferát k doktorské disertační práci]. Praha: VŠE, 2004 [cit. 2016-01-14]. Dostupné z: <https://webhosting.vse.cz/ekisl/prace/Fanta.pdf>

Finance.cz. *Eurostat: Pracovní síla je v ČR podstatně levnější, než průměr EU*. [online]. 2013 [cit. 2016-04-15]. Dostupné z: <http://www.finance.cz/zpravy/finance/385474-eurostat-pracovni-sila-je-v-cr-podstatne-levnejsi-nez-prumer-eu/>

Finance-management.cz. *Sarbanes-Oxley (SOX)*. [online]. 2012 [cit. 2016-04-23]. Dostupné z: <http://www.finance-management.cz/080vypisPojmu.php?IdPojPass=42>

GRASSEOVÁ, M. a kol. Přechteno.com. *Procesní řízení*. [online]. 2015 [cit. 2015-12-02]. Dostupné z: <http://www.precteno.com/grasseova-monika-a-kol-procesni-rizeni-1140>

HOVORKOVÁ, K. IDnes.cz. *Nejvýhodnější stravenka pro firmy i zaměstnance má hodnotu 105 korun*. [online]. [cit. 2016-05-14]. Dostupné z: http://finance.idnes.cz/stravenky-benefit-vyhodna-sazba-day-/podnikani.aspx?c=A160112_125128_podnikani_kho

Chovani.eu. *Styl řízení / styl vedení lidí*. [online]. 2015 [cit. 2015-12-02]. Dostupné z: <http://www.chovani.eu/styl-rizeni-styl-vedeni-lidi/c396>

Justice.cz. *Veřejný rejstřík podle subjektů*. [online]. 2016 [cit. 2016-02-11]. Dostupné z: [https://or.justice.cz/ias/ui/rejstrik-\\$firma?jenPlatne=PLATNE&nazev=zebra+technologies&polozek=50&typHledani=STARTS_WITH](https://or.justice.cz/ias/ui/rejstrik-$firma?jenPlatne=PLATNE&nazev=zebra+technologies&polozek=50&typHledani=STARTS_WITH)

Kaspersky Lab CZ. *Kaspersky Total Security for Business*. [online]. 2015 [cit. 2016-04-30]. Dostupné z: <http://www.kaspersky.com/cz/business-security/total>

Kaspersky Lab CZ. *Čtvrtina DDoS útoků vede ke ztrátě dat*. [online]. 2015 [cit. 2016-04-29]. Dostupné z: <http://www.kaspersky.com/cz/about/news/virus/2015/ctvrtina-DDoS-utoku-vede-ke-ztrate-dat>

ManagementMania.com. *Rizika (Risks)*. [online]. 2013 [cit. 2015-12-20]. Dostupné z: <https://managementmania.com/cs/rizika>

ManagementMania.com. *Řízení procesů*. [online]. 2014. [cit. 2015-12-02]. Dostupné z: <https://managementmania.com/cs/rizeni-procesu>

Měšec.cz. *Odkryté "zázraky" finančních mistrů*. [online]. 2005 [cit. 2016-04-23]. Dostupné z: <http://www.mesec.cz/clanky/odkryte-zazraky-financnich-mistru/>

Penize.cz. *Makroekonomika*. [online]. 2016 [cit. 2016-04-20]. Dostupné z: <http://www.penize.cz/makroekonomika>

Podnikator.cz. *Co je podnikání na bázi tzv. joint ventures*. [online]. 2012 [cit. 2016-01-14]. Dostupné z: <http://www.podnikator.cz/zacatek-podnikani/podnikani-obecne/n:17941/Co-je-podnikani-na-bazi-tzv-joint-ventures>

Pohoda.cz. *US GAAP*. [online]. 2012 [cit. 2016-02-11]. Dostupné z: <http://portal.pohoda.cz/dane-ucetnictvi-mzdy/ucetnictvi/ucetni-standardy/us-gaap/>

Pwc.com. *Point of view: Shared Service Center - the 2nd Generation*. [online prezentace]. 2008 [cit. 2016-01-14]. Dostupné z: https://www.pwc.com/us/en/issues/efficient-shared-services-centers/assets/shared_services_pointofview.pdf

Státní správa. *Dotace na zaměstnance pro rok 2016*. [online]. 2015 [cit. 2016-04-22]. Dostupné z: <http://statnisprava.eu/podnikani/dotace-na-zamestnance-pro-rok-2016/>

STŘELEČ, J. Vlastnicesta.cz. *Porterův model konkurenčních sil*. [online]. 2012 [cit. 2016-02-11]. Dostupné z: <http://www.vlastnicesta.cz/metody/porteruv-model-konkurencnich-sil-1/>

SystemOnLine.cz. *Bezpečnostní rizika IS veřejné správy a zdravotnictví*. [online]. 2015 [cit. 2015-12-20]. Dostupné z: <http://www.systemonline.cz/it-pro-verejny-sektor-a-zdravotnictvi/bezpecnostni-rizika-is-verejne-spravy-a-zdravotnictvi.htm>

VŠE. *Analýza a management rizika*. [online prezentace]. 2009 [cit. 2015-12-20]. Dostupné z: iom.vse.cz/wp-content/uploads/2009/./Analýza-a-management-rizika.ppt

Zebra.com. *ZEBRA CORPORATE FACT SHEET: WINTER 2016*. [online]. 2016 [cit. 2016-02-11]. Dostupné z: https://www.zebra.com/content/dam/zebra_new_ia/en-us/corporate-and-brand/corporate-policies/zebra-corporate-fact-sheet-en.pdf

SEZNAM POUŽITÝCH ZKRATEK

AP	Accounts Payable
APAC	Asia and Pacific
AR	Accounts Receivable
CIT	Corporate Income Tax
ČNB	Česká národní banka
ČR	Česká republika
DPH	Daň z přidané hodnoty
DPPO	Daň z příjmů právnických osob
EMEA	Europe, Middle East and Africa
ERP	Enterprise Resource Planning
EU	Evropská unie
FA	Finance Analysis
FSS	Finance Shared Services
GL	General Ledger
HDP	Hrubý domácí produkt
HR	Human Resources
IS	Informační systém
IT	Informační technologie
KPI	Key Performance Indicators
LA	Latin America
LAN	Local Area Network
mld.	miliard
MPSV	Ministerstvo práce a sociálních věcí

MS	Microsoft
NA	North America
OPPIK	Operační program Podnikání a inovace pro konkurenceschopnost
RFID	Radio Frequency Identification
SOX	Sarbanes-Oxley
SSC	Shared Service Center
T&E	Travel and Expense
tis.	tisíc
US GAAP	United States Generally Accepted Accounting Principles
USA	United States of America
VAT	Value Added Tax

SEZNAM OBRÁZKŮ

Obr. č. 1: Trojúhelník SSK	14
Obr. č. 2: Porterův model pěti sil	15
Obr. č. 3: Rámec faktorů 7S firmy McKinsey	16
Obr. č. 4: Tabulka SWOT analýzy.....	17
Obr. č. 5: Proces managementu rizika	27
Obr. č. 6: Příklady služeb v SSC.....	28
Obr. č. 7: Podstata offshoringu	29
Obr. č. 8: Logo Zebra Technologies	31
Obr. č. 9: Historie společnosti.....	33
Obr. č. 10: SSC v Brně.....	33
Obr. č. 11: Organizační struktura FSS v Brně	35
Obr. č. 12: Ishikawa diagram – Riziko informačních systémů.....	57
Obr. č. 13: Ishikawa diagram – Riziko odchodu zaměstnanců.....	58
Obr. č. 14: Ishikawa diagram – Riziko neuhrazení pohledávky	60
Obr. č. 15: Ishikawa diagram – Riziko zneužití dat.....	61
Obrázek 16: Ishikawa diagram – Riziko nízké likvidity.....	62

SEZNAM TABULEK

Tab. č. 1: SWOT matice.....	44
Tab. č. 2: Identifikace rizik	51
Tab. č. 3: Možnost výskytu rizika.....	53
Tab. č. 4: Dopad rizika.....	53
Tab. č. 5: Skóre hodnocení experty.....	54
Tab. č. 6: Náklady na zavedení nových benefitů	74

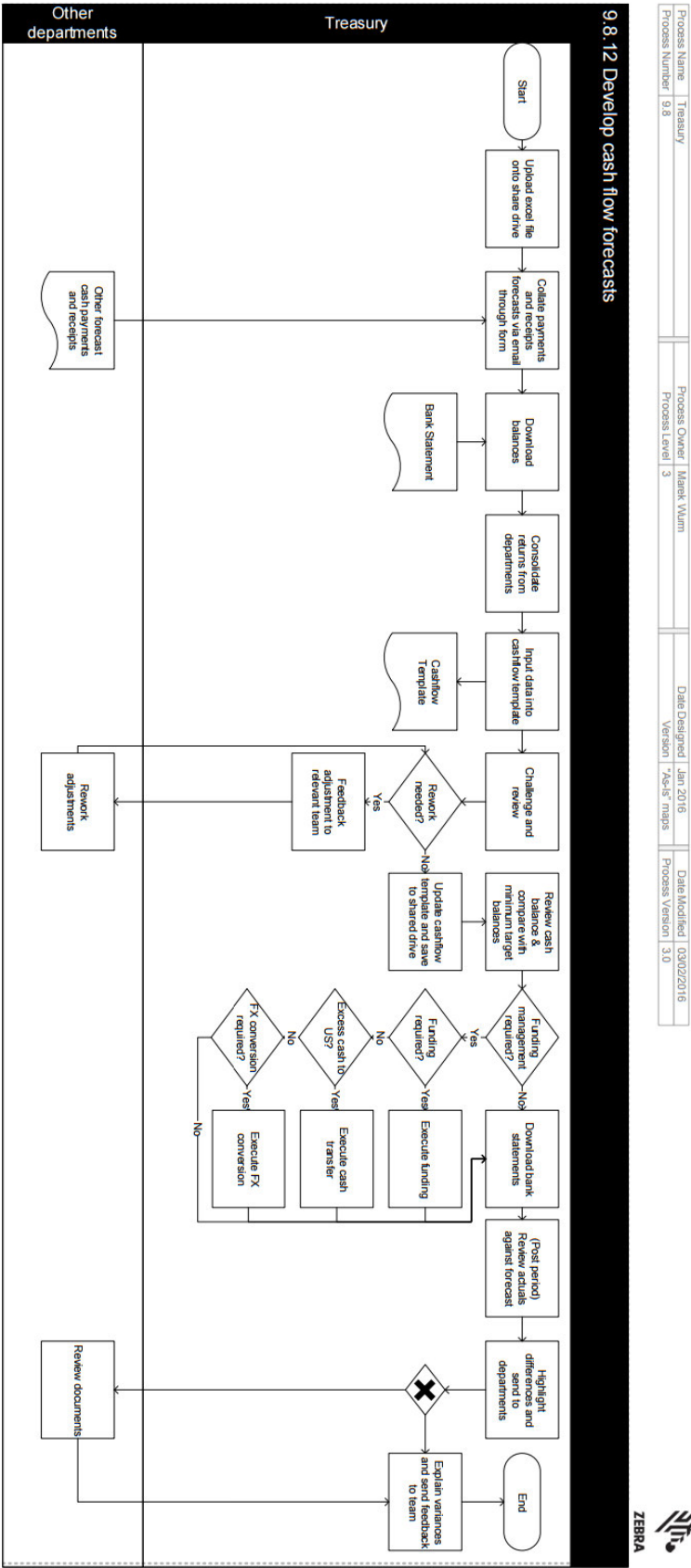
SEZNAM GRAFŮ

Graf č. 1: Mapa rizik	55
-----------------------------	----

SEZNAM PŘÍLOH

Příloha č. 1: Procesní mapa Cashflow forecast	I
Příloha č. 2: Hodnocení experty	II

Příloha č. 1: Procesní mapa Cashflow forecast



Příloha č. 2: Hodnocení experty

Expert 1				Expert 2			
Riziko	Možnost výskytu	Dopad	Skóre	Riziko	Možnost výskytu	Dopad	Skóre
Obecná rizika				Obecná rizika			
1	1	10	10	1	2	4	8
2	2	10	20	2	1	5	5
3	5	8	40	3	4	2	8
Vnější rizika				Vnější rizika			
4	7	2	14	4	5	3	15
5	5	5	25	5	7	1	7
6	3	7	21	6	3	3	9
7	5	9	45	7	2	5	10
Vnitřní rizika				Vnitřní rizika			
8	7	8	56	8	5	5	25
9	6	10	60	9	7	2	14
10	10	8	80	10	2	6	12
11	8	2	16	11	3	1	3
12	3	8	24	12	1	3	3
13	9	7	63	13	5	1	5
14	4	5	20	14	6	2	12
15	8	7	56	15	7	2	14
16	8	6	48	16	1	1	1
17	7	6	42	17	4	2	8
18	7	6	42	18	3	1	3
19	4	3	12	19	2	3	6
20	4	3	12	20	4	7	28
21	6	10	60	21	3	8	24
22	4	10	40	22	1	5	5
Procesní rizika				Procesní rizika			
23	5	8	40	23	5	5	25
24	8	6	48	24	7	1	7
25	2	5	10	25	3	3	9
26	6	4	24	26	2	5	10
27	3	6	18	27	1	6	6
28	3	8	24	28	5	5	25
29	4	7	28	29	5	2	10
30	2	10	20	30	1	9	9
31	3	9	27	31	2	9	18
32	5	6	30	32	3	2	6
33	2	10	20	33	3	8	24
34	4	7	28	34	2	9	18
35	6	8	48	35	3	6	18
36	2	9	18	36	1	10	10
37	7	7	49	37	7	2	14

Expert 3				Expert 4			
Riziko	Možnost výskytu	Dopad	Skóre	Riziko	Možnost výskytu	Dopad	Skóre
Obecná rizika				Obecná rizika			
1	3	7	21	1	2	9	18
2	2	5	10	2	2	9	18
3	5	5	25	3	5	7	35
Vnější rizika				Vnější rizika			
4	4	5	20	4	6	4	24
5	4	6	24	5	4	4	16
6	2	7	14	6	3	4	12
7	5	7	35	7	4	5	20
Vnitřní rizika				Vnitřní rizika			
8	5	5	25	8	5	7	35
9	3	5	15	9	4	6	24
10	4	4	16	10	4	4	16
11	3	4	12	11	6	6	36
12	2	6	12	12	4	6	24
13	5	5	25	13	8	6	48
14	4	3	12	14	5	4	20
15	4	6	24	15	8	8	64
16	5	6	30	16	7	7	49
17	6	6	36	17	6	5	30
18	4	5	20	18	6	4	24
19	5	6	30	19	4	2	8
20	6	8	48	20	8	4	32
21	5	7	35	21	4	7	28
22	5	5	25	22	4	6	24
Procesní rizika				Procesní rizika			
23	5	5	25	23	4	2	8
24	6	4	24	24	7	5	35
25	5	3	15	25	5	6	30
26	4	4	16	26	5	2	10
27	3	4	12	27	4	6	24
28	4	3	12	28	6	6	36
29	4	5	20	29	6	4	24
30	4	5	20	30	3	4	12
31	4	4	16	31	4	6	24
32	4	5	20	32	3	8	24
33	2	7	14	33	4	2	8
34	3	7	21	34	4	6	24
35	4	8	32	35	5	8	40
36	2	8	16	36	3	7	21
37	2	5	10	37	5	3	15

Expert 5				Expert 6			
Riziko	Možnost výskytu	Dopad	Skóre	Riziko	Možnost výskytu	Dopad	Skóre
Obecná rizika				Obecná rizika			
1	4	7	28	1	1	2	2
2	1	10	10	2	1	10	10
3	5	8	40	3	2	10	20
Vnější rizika				Vnější rizika			
4	5	3	15	4	3	4	12
5	8	5	40	5	8	7	56
6	7	5	35	6	6	3	18
7	4	7	28	7	7	9	63
Vnitřní rizika				Vnitřní rizika			
8	7	7	49	8	9	10	90
9	7	4	28	9	4	10	40
10	3	5	15	10	3	2	6
11	7	5	35	11	1	2	2
12	6	3	18	12	4	7	28
13	7	4	28	13	7	6	42
14	6	2	12	14	1	1	1
15	8	4	32	15	7	8	56
16	6	5	30	16	5	3	15
17	7	5	35	17	4	3	12
18	4	5	20	18	3	2	6
19	7	7	49	19	2	3	6
20	9	8	72	20	4	6	24
21	5	7	35	21	2	2	4
22	4	7	28	22	6	8	48
Procesní rizika				Procesní rizika			
23	7	6	42	23	6	2	12
24	8	4	32	24	6	2	12
25	6	5	30	25	4	2	8
26	4	4	16	26	4	1	4
27	4	4	16	27	4	2	8
28	5	5	25	28	6	4	24
29	6	5	30	29	4	2	8
30	6	6	36	30	3	6	18
31	7	6	42	31	2	1	2
32	4	6	24	32	5	6	30
33	1	7	7	33	2	4	8
34	2	5	10	34	2	3	6
35	3	8	24	35	6	9	54
36	2	7	14	36	2	4	8
37	7	3	21	37	7	8	56

Expert 7				Expert 8			
Riziko	Možnost výskytu	Dopad	Skóre	Riziko	Možnost výskytu	Dopad	Skóre
Obecná rizika				Obecná rizika			
1	3	6	18	1	1	7	7
2	5	7	35	2	1	9	9
3	5	5	25	3	3	9	27
Vnější rizika				Vnější rizika			
4	2	4	8	4	6	2	12
5	4	5	20	5	5	3	15
6	3	4	12	6	4	4	16
7	4	5	20	7	4	6	24
Vnitřní rizika				Vnitřní rizika			
8	7	8	56	8	7	4	28
9	5	6	30	9	6	4	24
10	3	4	12	10	3	2	6
11	5	5	25	11	1	1	1
12	4	4	16	12	1	1	1
13	6	6	36	13	6	4	24
14	7	7	49	14	7	4	28
15	6	7	42	15	3	3	9
16	8	8	64	16	7	6	42
17	6	7	42	17	6	6	36
18	5	6	30	18	5	4	20
19	7	8	56	19	5	4	20
20	7	8	56	20	6	4	24
21	5	6	30	21	4	8	32
22	7	8	56	22	2	8	16
Procesní rizika				Procesní rizika			
23	4	4	16	23	5	5	25
24	4	4	16	24	6	5	30
25	4	5	20	25	4	5	20
26	4	4	16	26	4	3	12
27	6	7	42	27	4	3	12
28	6	7	42	28	5	6	30
29	5	6	30	29	3	5	15
30	6	7	42	30	3	5	15
31	4	5	20	31	3	4	12
32	4	5	20	32	3	2	6
33	5	6	30	33	2	4	8
34	6	7	42	34	2	5	10
35	6	7	42	35	4	5	20
36	6	7	42	36	2	6	12
37	6	7	42	37	5	5	25