Západočeská univerzita v Plzni
Fakulta ekonomická

HODNOCENÍ INFORMAČNÍCH RIZIK VYBRANÝCH SUBJEKTŮ PODNIKATELSKÉ SFÉRY

Ing. Marie Černá

disertační práce
k získání akademického titulu doktor
v oboru Podniková ekonomika a management

Školitel: Doc. Ing. Jiří Vacek, Ph.D.

Katedra financí a účetnictví

Plzeň 2016

Čestné prohlášení

Prohlašuji, že jsem disertační práci na téma „Hodnocení informačních rizik vybraných subjektů podnikatelské sféry“ vypracovala samostatně pod odborným dohledem školitele a uvedla jsem veškerou použitou literaturu.

V Plzni dne ....

Ing. Marie Černá

Poděkování

Na tomto místě bych ráda poděkovala za cenné připomínky a poskytnutý čas svému školiteli, Doc. Ing. Jiřímu Vackovi, Ph.D.

V Plzni dne ....

Ing. Marie Černá

Anotace

Disertační práce se zabývá problematikou řízení informačních rizik. Obsahuje teoretické i praktické poznatky z uvedené oblasti. Problematika řízení informačních rizik je aktuálním tématem, ke kterému je přistupováno různými způsoby. Zvolený přístup závisí na oboru, ve kterém se jednotliví autoři prací zabývajících se problematikou informačních rizik a informačního managementu pohybují. S ohledem na odlišné zaměření prací nebo výzkumů různých autorů se liší také terminologie používaná v souvislosti s informačním managementem. V úvodu disertační práce jsou proto vysvětleny pojmy využívané v dalších kapitolách k popisu studované problematiky. Za klíčové jsou považovány pojmy informace, informační společnost, riziko, informační riziko a řízení rizik. V práci je identifikováno začlenění informačního managementu mezi ostatní podnikové aktivity a je precizována definice tohoto pojmu využitelná v oblasti ekonomického řízení studovaných subjektů. Implementace informačního managementu nebo jeho prvků podnikatelskými subjekty by měla být procesem, ve kterém jsou respektovány základní principy, na kterých informační management staví. Jedná se o principy popsané v disertační práci, jako jsou bezpečnost, efektivnost, kvalita, sdílení a shoda. V souladu se snahou Mezinárodní organizace pro standardizaci (ISO) zobecnit pravidla pro implementaci informačního managementu prostřednictvím tvorby norem, které danou problematiku upravují, vychází práce z mezinárodní normy ISO 31000:2009, respektive z normy ČSN ISO 31000, která je jejím překladem. Disertační práce je specificky zaměřena na problematiku využití řízení informačních rizik v ekonomických/účetních odděleních studovaných organizací. V práci je popsána současná situace v oblasti implementace informačního managementu nebo jeho prvků v podnikatelských subjektech definovaných v rámci prováděného výzkumného šetření. U zvolených subjektů byl prováděn empirický výzkum zaměřený na srovnání aktuální situace v analyzované oblasti se standardem, který stanovuje britská norma BS 7799-3:2006, respektive česká technická norma ČSN 36 9790, která je jejím překladem. V souladu s výsledky provedených šetření stanovuje disertační práce návrhy, opatření a doporučení, která mohou napomoci budoucímu zefektivnění práce s informačními riziky v oblasti účetnictví.

Klíčová slova: ČSN 31000 (ISO 31000), ČSN 36 9790 (ISO 36 9790), informace, informační management, informační rizika, informační systémy, řízení rizik, účetnictví

Annotation

The dissertation deals with the issue of information risk management. It contains theoretical and practical findings of this area. Information risk management is currently described by various ways. The selected approach depends on the area of interest, specialization and experience of the individual author dealing with the information risk management issue. Due to the different specialization differs the terminology used in context of information management. At the beginning of the thesis are therefore defined terms used in subsequent chapters to describe the studied issues. The key terms are information, information society, risk, information risk and risk management. The dissertation identifies the inclusion of information management among other business activities. The implementation of information management or its components by business units has to be a process which respects the fundamental principles information management deals with, such as safety, effectiveness, quality, sharing and compliance. In accordance with the effort of the International Organization for Standardization (ISO) to generalize rules for information management implementation through creation of standards governing this issue, the dissertation is based on ISO 31000:2009, respectively on its Czech translation ČSN ISO 31000. The dissertation is specifically focused on the use of information risk management by economical/accounting departments of analyzed organizations. Current situation in the area of information risk management or its components implementation by business entities defined within the conducted research is described. The empirical research is focused on the comparison of the current situation in analyzed companies with the British standard BS 7799-3:2006, respectively its Czech translation ČSN 36 9790. In accordance with the results of conducted research, dissertation is concluded by proposals, measures and recommendations which can make future work with information risks in the area of accounting more effective.

Key words: ČSN 31000 (ISO 31000), ČSN 36 9790 (ISO 36 9790), information, information management, information risk, information systems, risk management, accounting

Annotation

Ce travail s’occupe de la problématique du management de risques informatifs. Il contiens des acquis théoriques et pratiques de domaine nommé. Le management de risques informatives est s’approché de différents façons. L’approche choisi se dépends sur la sphère des auteurs particuliers, qui s’occupent de la problématique. En considération de différent orientation de travails d’origin ou des recherches la terminologie utilisé dans contexte se diffère. Pour cette raison les termes utilisés pour la description de la problématique dans les chapitres suivants sont expliqué dans l’introduction de ce travail. Les termes de la clé sont information, la société d’information, risque, risque informatif et le management de risques. Ce travail identifit l’integration du management informatif dans autres activités de l’entreprise. L’implémentation du management informatif ou ses éléments avec les individus entrepreneurial doit être un procès, qui respects les principes fondamentals, sur qui le management informatif est construit, comme sécurité, efficacité, qualité, partage et conformité. En harmonie d’effort de la International organisation de standardisation (ISO) de généraliser les règles pour l’implémentation du management informatif avec de la création de normes, qui arrangent ce problématique, ce travail prends sa source de la norme international ISO 31000:2009, ou plutôt de la norme ČSN ISO 31000, qui est son traduction. Ce travail est orienté spécifiquement vers la problématique de la utilisation des risques informatifs dans départements économiques/comptables des organisations examinés. Il y a décrit une actuelle situation dans la sphère d’implementation du management informatif ou ses éléments par l'intermédiaire des individus entrepreneurial définis dans le domaine de inquisition de recherche réalisé. Le recherche empirique avec les individus choisis est orienté vers la comparaison de la situation actuelle dans le domaine analysé avec le standard, qui détermine la norme britannique BS 7799-3:2006, ou plutôt la norme technique tchéque ČSN 36 9790, qui est son traduction. En harmonie avec les résults d’inquisition réalisé ce travail détermine des suggestions, mesures et recommendations, qui peuvent aider dans l’avenir avec l’amélioration de travail avec risques de l’information dans le domaine de comptabilité.

Mots clés: ČSN 31000 (ISO 31000), ČSN 36 9790 (ISO 36 9790), information, management informatif, le risque informatif, systèmes d’information, risque management, comptabilité

Obsah

Seznam použitých zkratek

AI	Artificial Intelligence
BI	Business Intelligence
CRM	Customer Relationship Management
CSR	Corporate Social Responsibility
ČR	Česká republika
ČSN	České národní normy
DPPO	Daň z příjmů právnických osob
EDI	elektronická výměna dat
ERP	Enterprise Resource Planning
EUR	Euro
HW	hardware
IPR	Identifikace procesů a rizik
IS	informační systém
IS/ICT	informační systém/informační a komunikační technologie
ISMS	Systém managementu bezpečnosti informací
ISO	International Organization for Standardization
IT	informační technologie
MFČR	Ministerstvo financí České republiky
MIS	Management Information System
MSP	malé a střední podniky
NACE	klasifikace ekonomických činností
PC	osobní počítač
SaaS	Software as a Service
SCM	Supply Chain Management
SW	software
TNI	Technické normalizační informace

Seznam tabulek

Seznam obrázků

Úvod

Podnikatelské subjekty jsou dnes a denně vystaveny obrovskému tlaku okolí, které je nutí zohlednit v rámci aktivit, jimiž se zabývají, stále se vyvíjející a měnící trendy v přání zákazníků, v chování konkurence, nebo v komunikaci. V průběhu zajišťování těchto aktivit se však může kdykoli vyskytnout riziko.

Všechny probíhající podnikové aktivity je proto potřeba neustále kontrolovat. Aby byly společnosti schopny reagovat co nejpružněji na aktuální přání zákazníků nebo na jiné podněty, je nutné procesy, které již v podniku probíhají, nejen podrobovat neustálé kontrole, ale také je obměňovat, rušit, nebo zavádět nové s ohledem na to, jaká varianta je v daném okamžiku pro podnik nejvhodnější. Rozhodovací procesy, týkající se nastavení a změn nastavení podnikových procesů, jsou vnímány jako velice citlivá oblast. Vstupuje do nich velké množství informací získávaných z vnitřních i vnějších zdrojů a výskyt rizik je zde více než pravděpodobný. Proto jsou takováto rozhodnutí, která mohou v důsledku ovlivnit budoucí existenci společnosti, ve většině případů svěřena managementu podniku.

Riziko je dle některých zdrojů (BBA, ISDA, PWC, RMA 1999), (Lam 2003) a (Renn, Aven 2010) definováno jako přímá nebo nepřímá ztráta, která vyplývá z nedostatečnosti nebo selhání vnitřních procesů organizace, ze selhání lidského faktoru nebo ze selhání podnikových systémů, nebo vzniká na základě vnějších událostí. Specifický typ rizika tvoří riziko informační, které je dle (Gantz, Philpott 2012) a (Johnson 2009) popisováno jako možná újma způsobená procesu nebo s ním souvisejícím informacím vyplývající z nějaké plánované nebo náhodné události, která proces nebo s ním související informace negativně ovlivňuje. Negativním ovlivněním informací je myšlen zásah do jejich důvěrnosti, integrity a dostupnosti (ISO/IEC 17799:2005). V praxi může být za informační riziko považováno například neoprávněné, nezákonné, neetické, nesprávné nebo nevhodné zacházení s informacemi. V souvislosti s působením informačního rizika může v podniku docházet k odklonu od stanovených cílů. Může docházet ke změnám v délce trvání podnikových procesů, k navyšování nákladů, k negativnímu působení na vztahy se zákazníky nebo dodavateli, případně k jejich ztrátě.

Společnosti se snaží negativním dopadům rizik zabránit, nebo je alespoň mírnit. Využívají k tomu poznatků řízení rizik. Dle (Kaplan, Mikes 2012) a (McNeil, Rüdiger 2005) se jedná o disciplínu, která společnosti učí pracovat s riziky od jejich identifikace až po návrh opatření na zmírnění jejich dopadů. Na rizika je nahlíženo komplexně, systematicky, zahrnuje se i lidský pohled, který odráží skutečné podmínky dané společnosti. Mezinárodní standard (ISO 31000:2009, s. 11-13) definuje řízení rizik jako: „řízený soubor činností a metod, který se používá k přímé organizaci a kontrole rizik, která mohou mít vliv na dosahování podnikem stanovených cílů.“

Problematika rizik a jejich řízení je velmi obsáhlá a prolíná se řadou dalších oblastí, kterými se zabývají různé vědní disciplíny. Z tohoto důvodu, ačkoli to bude vzhledem k šíři studované problematiky a existujícím intenzivním příčinným vazbám jejích částí obtížné, budou v rámci předkládané disertační práce zohledněny pouze ty typy rizik, které se vztahují k problematice řešené v její praktické části, to je k propojení informací, informačních systémů a účetnictví. Na rizika zde bude nahlíženo zejména jako na potenciální hrozby.

1. Cíle a metodika disertační práce

Současná společnost bývá označována jako informační společnost (Martin 1995) nebo znalostní společnost (Drucker 1993). Informační společností je myšlena „společnost, kde kvalita života i perspektiva sociálních změn a ekonomického rozvoje v rostoucí míře závisí na informacích a jejich využití. V takové společnosti životní úroveň, typické způsoby práce i oddychu, systém výchovy a tržní podmínky jsou výrazně ovlivněny pokrokem v oblasti využívání informací a znalostí“ (Martin 1995, s. 3). Informace a znalosti jsou vnímány jako klíčový zdroj rozvoje společenského života (Vodáček, Rosický 1997). Stávají se, vedle tří „klasických“ ekonomických zdrojů, kterými jsou práce, půda a kapitál, „čtvrtým“ ekonomickým zdrojem (Best 1996).

V souvislosti s tímto pohledem na informace se před zhruba deseti – dvaceti lety vydělil samostatný vědní obor nazývaný „Informační management“ (Information Management) (Vodáček, Rosický 1997). Informační management je dle (Burk, Horton 1991, s. 171) „aplikace tradičních manažerských procesů, zejména zásad managementu pro hospodaření se zdroji, k správě informačních zdrojů a dalších aktiv organizace.“

Informace představují pro podnikatelské subjekty cenné aktivum (Imler 2008), které slouží jako podklad pro veškerá rozhodování a se kterým je proto nutné zacházet velmi opatrně. V rámci práce s informacemi se často setkáváme s riziky (Švarcová, Rain 2012). Zmínku o informačních rizicích nebo o informačním managementu nacházíme obvykle v rámci zpracování širších témat, jako jsou podnikový management, risk management, projektový management, informační systémy a jejich řízení, informace nebo rizika obecně (Cejpek 2005), (Doucek 2004), (Laplante 2009), (Smejkal, Rais 2006), (Sodomka 2006), (Sokolowsky 2002b), (Stonebumer, Goguen a Feringa 2002) a (Svozilová 2007).

Informační rizika jsou popisována také v souvislosti s účetnictvím a auditem (KAČR 2014). Účetnictví je obor, v němž se s riziky setkáváme velmi často. Definice účetnictví dle (Březinová, Munzar 2006, s. 56) vycházející ze Zákona č. 563/1991 Sb. o účetnictví a z teorie procesního řízení říká, že: „Účetnictví je systém soustřeďování, zaznamenávání, ověřování, třídění, dalšího zpracovávání a hodnocení ekonomických informací pro potřeby účetní jednotky, státu, veřejnosti a ostatních subjektů.“

Z tohoto tvrzení je patrná souvislost mezi účetnictvím a informacemi. Lze tedy předpokládat také vztah mezi účetnictvím a informačními riziky.

1.1 Cíle disertační práce

Cílem disertační práce je analyzovat současný stav řízení informačních rizik, která se mohou vyskytnout v rámci podnikových procesů spadajících do kompetence ekonomických/účetních oddělení zvolených podnikatelských subjektů a navrhnout doporučení pro minimalizaci takových rizik.

Dílčí cíle práce jsou následující:

- Zpracovat vybranou část problematiky managementu, rizik a informací.
- Analyzovat a zhodnotit současný stav zahrnutí řízení informačních rizik (s důrazem na propojení informačních rizik a účetnictví) mezi ostatní aktivity vybraných subjektů podnikatelské sféry.

Dále, na základě poznatků z odborné literatury, ostatních dostupných zdrojů a výzkumu autorky:

- Diskutovat souvislosti efektivního řízení informačních rizik a bezproblémového zajištění operací v rámci účetního systému podniku.
- Navrhnout opatření a doporučení, která by pomohla zefektivnit řízení informačních rizik (s důrazem na propojení informačních rizik a účetnictví).

Výstupem práce je vyhodnocení a shrnutí získaných poznatků. Je zde identifikováno začlenění informačního managementu mezi ostatní podnikové aktivity a je precizována definice tohoto pojmu využitelná v oblasti ekonomického řízení studovaných subjektů. Formou závěrečné zprávy je v práci popsána současná situace v oblasti implementace informačního managementu nebo jeho prvků mezi podnikové aktivity podnikatelských subjektů definovaných v rámci prováděného výzkumného šetření zaměřeného na srovnání aktuální situace v analyzované oblasti se standardem, který stanovuje britská norma BS 7799-3:2006, respektive česká technická norma ČSN 36 9790, která je jejím překladem.

Výzkum měl pomoci ověřit následující hypotézy:

- Většina sledovaných společností pod pojmem informačním management vnímá především informační a komunikační technologie a nevěnuje pozornost dalším okruhům, které patří do informačního managementu.
- Více než polovina sledovaných společností se již setkala s pojmem informační management.
- Informačním rizikům spojeným s lidským faktorem věnuje maximální pozornost jen malé množství sledovaných společností.

Získané informace jsou zpracovány pomocí dále popsaných metod, jako jsou deskripce, analýza, syntéza, dedukce, indukce, dotazníkové šetření a expertní rozhovor. Na základě vyhodnocení provedených šetření stanovuje disertační práce návrhy opatření a doporučení, která by napomohla budoucímu zefektivnění práce s informačními riziky v oblasti účetnictví.

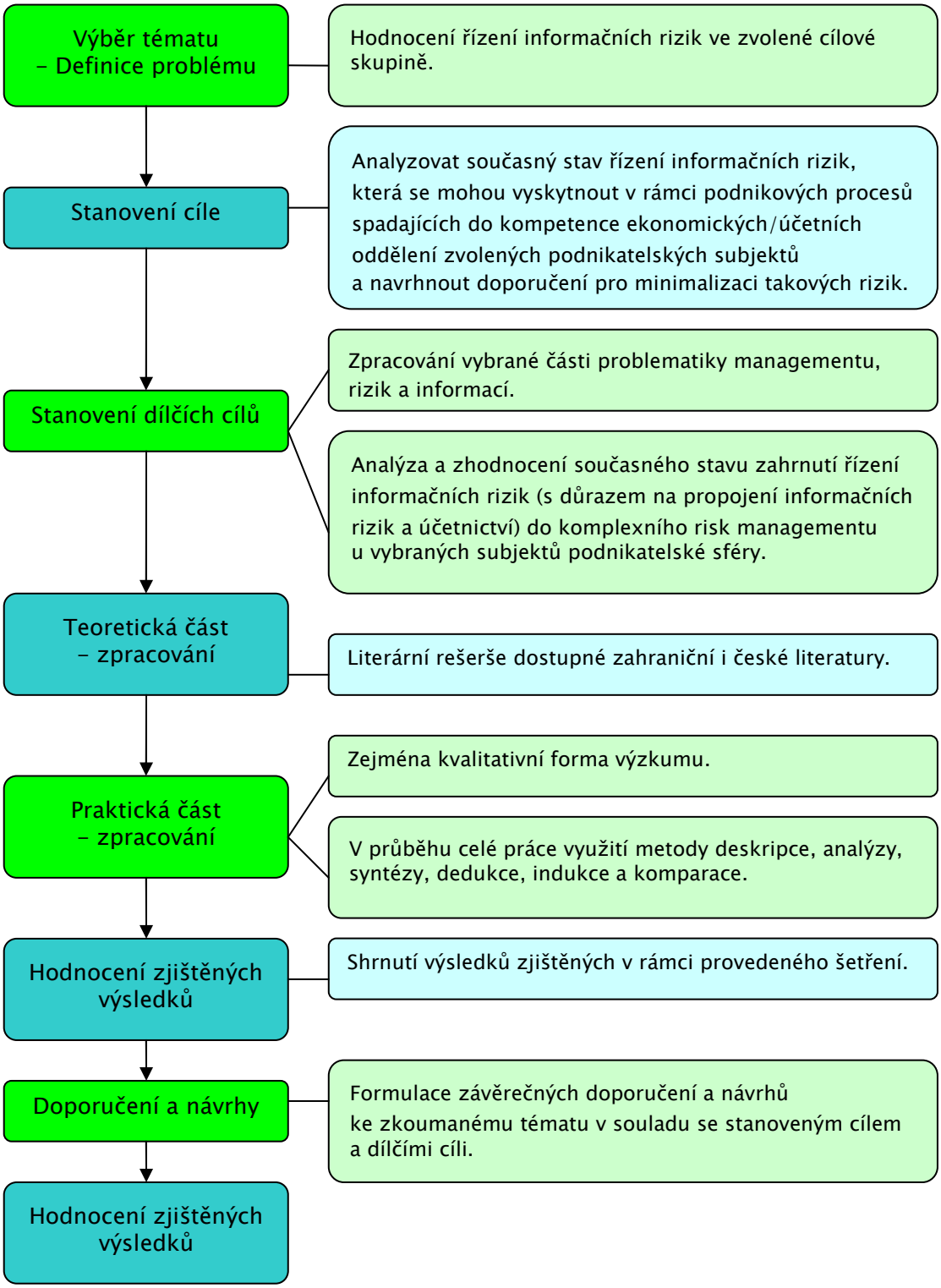
1.2 Metodika disertační práce

V této podkapitole jsou představeny dílčí části procesu zpracování disertační práce a metody použité k tomuto účelu. Je zde charakterizován postup prováděného výzkumu a použité metody zkoumání.

Počáteční krok procesu zpracování disertační práce představuje rešerše zahraniční i české literatury. Primární zdroje týkající se studované problematiky obsahuje zejména literatura zahraniční. V rámci rešeršní činnosti byly využity monografické publikace, publikace v odborných časopisech, konferenční příspěvky, příspěvky ve sbornících, disertační práce věnující se obdobnému tématu, platná česká i zahraniční legislativa a informace poskytnuté respondenty v rámci prováděného empirického šetření. Mezi nejvýznamnější legislativní zdroje patří ISO 31000:2009 Risk management - Principles and guidelines, respektive český překlad této normy ČSN ISO 31000 Management rizik - Principy a směrnice (01 0351) a britská norma BS 7799-3:2006, respektive její český překlad, technická norma ČSN 36 9790 Systém managementu bezpečnosti informací - Směrnice pro management rizik bezpečnosti informací.

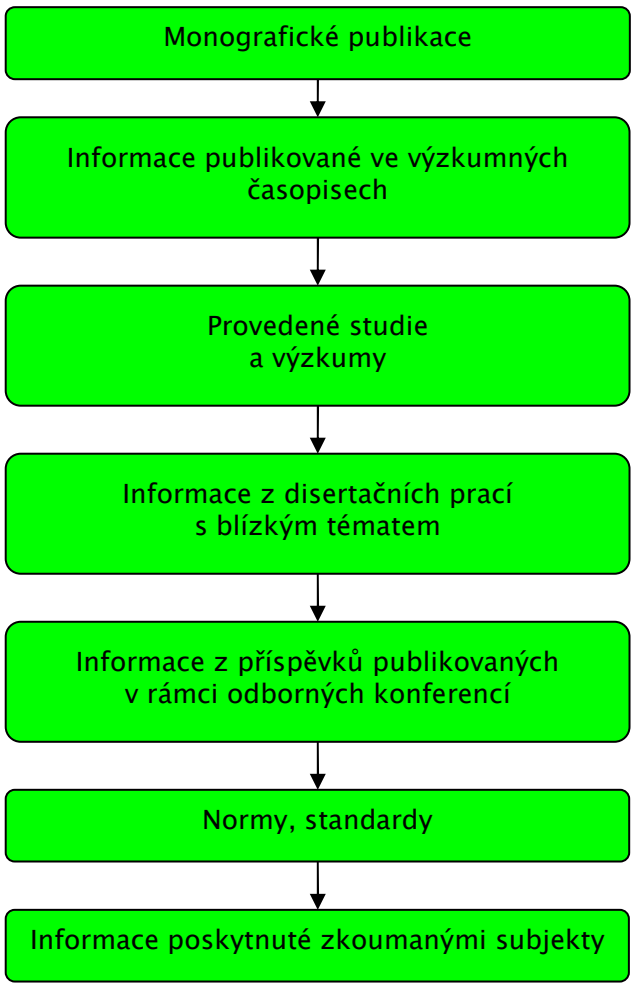
Postup zpracování disertační práce a rešeršní činnost jsou dokumentovány pomocí následujících obrázků.

Obrázek 1: Proces zpracování disertační práce



Zdroj: vlastní zpracování, 2016

Obrázek 2: Rešeršní činnost - zdroje informací relevantních pro zkoumané téma



Zdroj: vlastní zpracování, 2016

Jednotlivé etapy rešeršní činnosti představují sběr, organizování a shrnutí informací získaných z výše uvedených zdrojů společně s vysvětlením studované problematiky, verifikací teorie a jejím dotvářením. V závěru disertační práce je uveden seznam literatury obsahující veškeré zdroje využité při jejím zpracování.

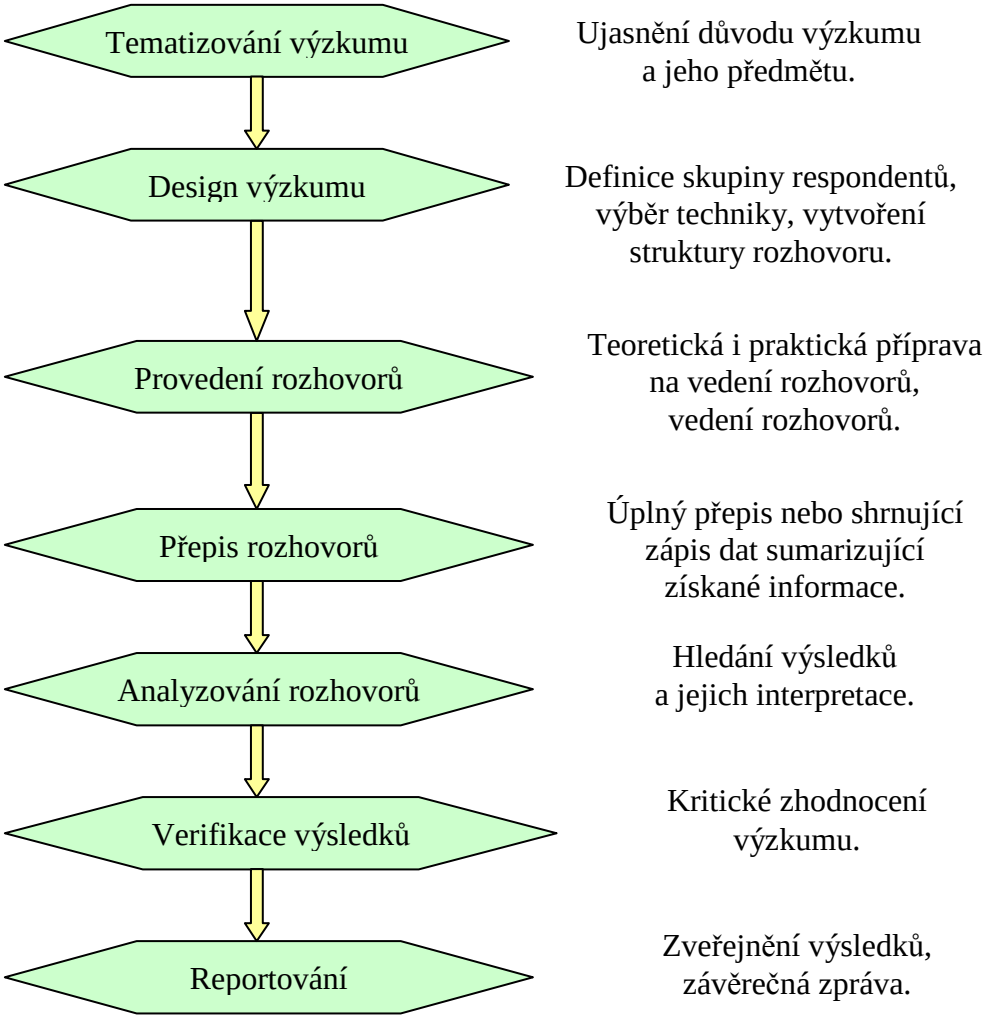
V disertační práci je využíván explorativní výzkum (výzkum sloužící k předběžnému zkoumání výchozí situace) a deskriptivní výzkum (výzkum, který poskytuje základní obraz o vybraných aspektech zkoumaného problému v daném období, popisuje jevy a procesy, které jsou relevantní pro rozhodování) (Stebbins 2001). V rámci výzkumu jsou zpracovávána kvalitativní i kvantitativní data. Stěžejní metodou se stala metoda deskripce, která umožňuje popsat jednotlivé dosud známé skutečnosti o zkoumané

oblasti. V rámci práce je použita také metoda analýzy a rozboru problematiky informačních rizik. Na základě použití těchto metod je na závěr provedena syntéza studované problematiky, která umožňuje navrhnout určitá doporučení, podle kterých by bylo možné postupovat při řešení problematických situací spojených s informačními riziky. V teoretické části práce je postupováno zejména deduktivním způsobem, od obecných poznatků k poznatkům konkrétním, v rámci prováděného výzkumu se nejčastěji uplatnila metoda induktivní.

Data jsou získávána dotazníkovým šetřením, expertními rozhovory a studiem relevantních dokumentů. Je využito zejména kvalitativní zpracování získaných dat. Kvalitativní výzkum označuje dle (Hendl 2006, s. 5) „výzkum zaměřený na interpretace subjektivních významů, popis kontextu jednání a chování, přičemž se zajímá o subjektivní teorie jedinců v daném prostředí.“ Jeho výsledkem je závěrečná zpráva, ve které jsou shrnuty výsledky výzkumu. Subjektivita pohledu dotazovaných subjektů na danou problematiku může být považována jak za negativní vliv, tak za přínos, neboť cílem práce je soustředit se na problémy spojené s praktickým využitím informačních systémů a informací obecně zainteresovaným subjektem. V rámci výzkumu je využito expertních rozhovorů a dotazníkového šetření. Uskutečněné rozhovory lze charakterizovat jako polostrukturované (Doctorandus 2013) v délce trvání cca 45 minut. Metodické postupy expertních rozhovorů a dotazníkového šetření jsou shrnuty v následujících obrázcích 3 a 4.

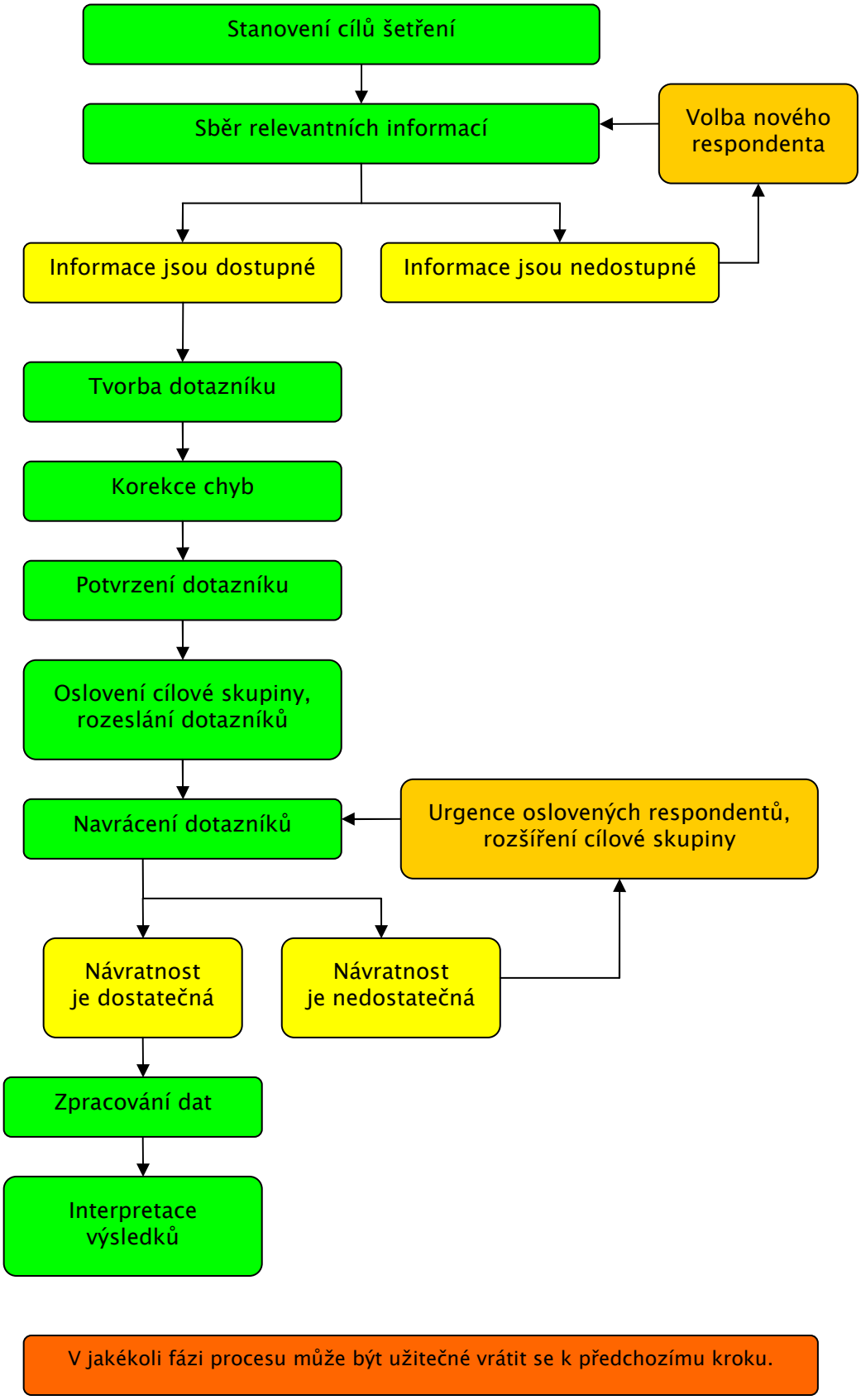
Informace získané výše uvedenými metodami mohou být využity pro doplnění stávajících studijních materiálů, které vysvětlují problematiku informačního managementu. V praxi pak mohou zjištěné informace pomoci zvýšit povědomí o informačních rizicích u pracovníků v dané oblasti nebo v dalších příbuzných oborech a pomoci jim umět se lépe, rychleji a efektivněji vypořádat s řízením informačních rizik.

Obrázek 3: Metodický postup dotazování - expertní rozhovory



Zdroj: vlastní zpracování dle (Hendl 2006) a (Foddy 1995), 2016

Obrázek 4: Metodický postup dotazování - dotazníkové šetření



Zdroj: vlastní zpracování dle (Foddy 1995), 2016

2. Teoretická východiska práce

2.1 Historický rámec

Informace se objevila spolu se vznikem lidské civilizace. Potřeba sdělovat někomu něco, informovat, a umět informace využít provází lidstvo již velmi dlouho. Informace je odedávna využívána k dosahování stanovených cílů s výrazně menším úsilím, než by tomu bylo v případě její neznalosti (Wexelblat, Maes 1999).

V dávné historii byl pojem informace užíván pro předávání smyslového poznání (jak rozdělat oheň, jak si zajistit potravu, jak se ubránit predátorům). Dnes jsou informace chápány jako data, kterým jejich příjemce přisuzuje význam na základě znalostí, kterými disponuje (Vodáček, Rosický 1997). Z pohledu účetnictví představují informace data s ekonomickou hodnotou, s nimiž je spojeno riziko (Day 2008). K novodobému chápání informace přispěly různé přístupy mnoha vědních oborů (například: zemědělství, astronomie). Pro účely této práce bude dále sledován přístup k informacím a k rizikům z práce s nimi plynoucích ve vztahu k účetnictví.

2.1.1 Důležité mezníky ve vývoji účetnictví

Dějiny účetnictví sahají až do pravěku (Brown 2004), (Raulich 1922). Již tehdy se v rámci výměnného obchodu objevovala rizika. Lidé si jejich existenci sice uvědomovali, ale možnosti práce s riziky jim zůstávaly skryty. V období pravěku, starověku a značné části středověku dominovala ústní forma přenosu informací (Fiala 1935), která je spojena s velkým množstvím rizik (například neúmyslná i úmyslná modifikace informace, nedoručení informace, dodatečná ztráta informací).

Psaná forma záznamů snižovala do jisté míry výskyt rizik souvisejících s přenosem informací. Důsledkem potřeby dále zmírňovat a odstraňovat informační rizika spojená se zaznamenáváním informací o obchodních transakcích byl ve 14. století také vznik podvojného účetnictví (Osamu 1955). Za prvního člověka, který zpřístupnil účetnictví široké veřejnosti je považován Luca Pacioli, jehož práce nazvaná Summa de Arithmetica, Geometria, Proportioni et Proportionalita (Souhrn aritmetiky, geometrie, poměrů a proporcí) obsahovala 36 kapitol pojednávajících o podvojném účetnictví. Principy podvojného účetnictví popsané v jeho práci zůstávají dodnes téměř

beze změny (Lauwers & Willekens 1994). Způsoby účetních zápisů doznávaly během let řadu změn (Brown 2004). Společně s účetnictvím se zdokonalovala i metodika a technické možnosti záznamu (mechanická kalkulačka, počítací stroje, počítače nebo vznik nákladového účetnictví) účetních dat (Ceruzzi 2003), (Chatfield, Vangermeersch 2014) a (Childs 1901).

2.1.2 Legislativní rámec současného českého účetnictví - nastavení účetních procesů

Legislativní rámec českého účetnictví dle (MFČR 2015b) a (KAČR 2015) představují níže uvedené dokumenty.

Zákony:

- Zákon č. 563/1991 Sb. o účetnictví,

Vyhlášky provádějící zákon o účetnictví:

- Vyhláška č. 383/2009 Sb.,
- Vyhláška č. 410/2009 Sb.,
- Vyhláška č. 504/2002 Sb.,
- Vyhláška č. 503/2002 Sb.,
- Vyhláška č. 502/2002 Sb.,
- Vyhláška č. 501/2002 Sb.,
- Vyhláška č. 500/2002 Sb.,
- (Vyhláška č. 365/2010 Sb., Vyhláška č. 270/2010 Sb., Vyhláška č. 114/2002 Sb.).

České účetní standardy

Výše uvedené dokumenty ovlivňují nastavení procesů probíhajících v účetním (ekonomickém) oddělení ekonomických subjektů. Mezi tyto procesy se řadí například: financování, rozpočtování, vedení daňové agendy, ekonomika práce a mezd, vedení osobní agendy, vedení právní agendy, využití informační soustavy, rozborová činnost, inventarizace a evidence majetku, ochrana majetku, fungování dodavatelsko-odběratelských vztahů, fakturace (včetně penalizace) a skartace.

Dle (Vodáček, Rosický 1997, s. 38) představují manažerské procesy „účelně uspořádané posloupnosti jednotlivých činností, které transformují vstupní zdroje (údaje, informace, potenciál pracovníků, suroviny, materiály, kapacity strojů a zařízení, kapacity ploch atd.) do požadovaných výstupů (myšlenkových řešení, výrobků, služeb atd).“ Dále je dělíme na předvýrobní, výrobní, povýrobní a další nevýrobní aktivity (Vodáček, Rosický 1997) a (Morton 1991).

Z pohledu Vodáčka a Rosického (1997) patří aktivity účetního oddělení mezi sociálně-ekonomické aktivity spadající dle Mortona (1991) do skupiny povýrobních a nevýrobních činností. Předvýrobní aktivity, mezi které patří například vytváření a analýza finančních plánů, také spadají do kompetence účetního oddělení, nejsou však v Mortonově výkladu zmiňovány. Při provádění podnikových činností může docházet k rizikovým situacím popsaným v následující tabulce, sestavené na základě informací získaných v rámci šetření od zaměstnanců ekonomických oddělení různých typů podnikatelských subjektů.

Tabulka 1: Účetní (ekonomické) oddělení - procesy a rizika

Procesy	Detailní popis procesů	Možná rizika
Financování	- Krátkodobé financování (běžné platby). - Dlouhodobé financování (nákup strojů, technologií).	- Ztráta investovaných prostředků z vnějších příčin (ekonomická krize). - Ztráta investovaných prostředků z vnitřních příčin.
Rozpočtování	- Ekonomické (finanční) vyjádření podnikových úkolů.	- Podhodnocení/nadhodnocení podnikových aktiv.
Vedení daňové agendy	- Zpracování podkladů pro DPPO.	- Selhání lidského faktoru (chybný přepis dat, chybná interpretace předpisů).

Procesy	Detailní popis procesů	Možná rizika
Ekonomika práce a mezd	- Zpracování podkladů pro výplatu mezd (docházka, nemocenská, srážky a odvody, namátková kontrola mezd, výplata mezd, reklamace). - Kontrola chybovosti vstupních dat.	- Selhání lidského faktoru (chyby v podkladech, chybný přepis dat).
Vedení osobní agendy	- Zpracování a vedení karty zaměstnance.	- Selhání lidského faktoru (chybný přepis dat). - Záměrná modifikace údajů zaměstnancem podniku.
Vedení právní agendy	- Zpracování podkladů pro právního zástupce podniku.	- Neúmyslná/úmyslná modifikace předkládaných údajů zaměstnancem ekonomického oddělení.
Využití informační soustavy	- Předávání informací mezi odděleními. - Elektronické zpracování dat využívaných ekonomickým oddělením a ostatními středisky.	- Rizika spojená s vedením účetnictví prostřednictvím IS (selhání hardware/software, selhání lidského faktoru při práci s PC a daty, ztráta dat).
Rozborová činnost	- Příprava podkladů pro hodnocení úspěšnosti ekonomických aktivit podniku jeho zřizovatelem/majitelem.	- Struktura podkladů nekoresponduje s požadavky zřizovatele/majitele. - Nedostatečná odbornost posuzovatele předkládaných informací.
Inventarizace a evidence majetku	- Zpracování dat o majetku podniku (inventární karty, účetní stav majetku oproti skutečnosti).	- Neúmyslná/úmyslná modifikace předkládaných údajů zaměstnancem ekonomického oddělení.
Ochrana majetku	- Dokladová (vícečetné podpisy, evidence majetku na kartách proti podpisu). - Fyzická (zabezpečení uložení majetku, trezor).	- Zneužití podpisu zaměstnancem při výběru finančních prostředků z banky. - Nedostatečné zajištění ochrany pracovníka odpovědného za manipulaci s finančními prostředky. - Nesprávná autorizace přístupu k datům.
Fungování dodavatelsko - odběratelských vztahů	- Zpracování nabídek, faktur. - Opravy dokumentů požadované dodavatelem nebo odběratelem.	- Riziko plynoucí z komunikace s dodavatelem/odběratelem. - Komunikační šumy.
Fakturace	- Vkládání vstupních dat do IS. - Zpracování faktur: účtování, kontrola, opravy (faktury vydané, faktury přijaté).	- Selhání lidského faktoru (chybný přepis dat). - Záměrná modifikace údajů zaměstnancem ekonomického oddělení.

Procesy	Detailní popis procesů	Možná rizika
Uchovávání účetních dokladů	- Archivace dokladů dle Zákona č. 563/1991 Sb., o účetnictví.	- Chybné označení dokladů. - Ztráta, zničení nebo poškození dokladů.
Skartace - dokumenty v tištěné podobě	- Skartace (objednání skartace u dodavatele, likvidace chybně vystavených dokladů a dokladů, které již není nutné archivovat).	- Záměna dokladů. - Skartace dokladů, které ještě mají být archivovány. - Únik citlivých informací.

Zdroj: vlastní zpracování dle interních informací analyzovaných společností, 2016

Řízení rizik v podniku by mělo být nastaveno podle pravidel popsaných v dokumentech, které tvoří normativní rámec managementu rizik. Jedná se zejména o dokumenty uvedené v následující tabulce.

Tabulka 2: Normativní rámec řízení rizik

Mezinárodní normy pro management rizik	**České normy pro management rizik**
ISO 31000:2009 Risk management - Principles and guidelines	**ČSN ISO 31000** Management rizik - Principy a směrnice (01 0351), vydáno v říjnu 2010
ISO Guide 73:2009 Risk management - Vocabulary	**TNI 01 0350** Management rizik - Slovník (Pokyn 73) (01 0350), vydáno v srpnu 2010
IEC/ISO 31010:2009 Risk management - Risk assessment techniques	**ČSN IEC/ISO 31010** Management rizik - Techniky posuzování rizik, vydáno v lednu 2011
ISO/IEC 27005:2011 Information technology - Security techniques - Information security risk management	**ČSN 36 9790** Systém managementu bezpečnosti informací - Směrnice pro management rizik bezpečnosti informací
ISO 9000 Quality management	**ČSN EN ISO 9000** Systém managementu kvality - Základní principy a slovník
ISO 9001:2008 Quality management systems - Requirements - *aktualizován na:* **ISO 9001:2015** Quality management systems - Requirements	**ČSN EN ISO 9001** Systémy managementu kvality - Požadavky - *bude aktualizován na:* **ČSN EN ISO 9001:2015 (2016)** Systémy managementu jakosti - Požadavky

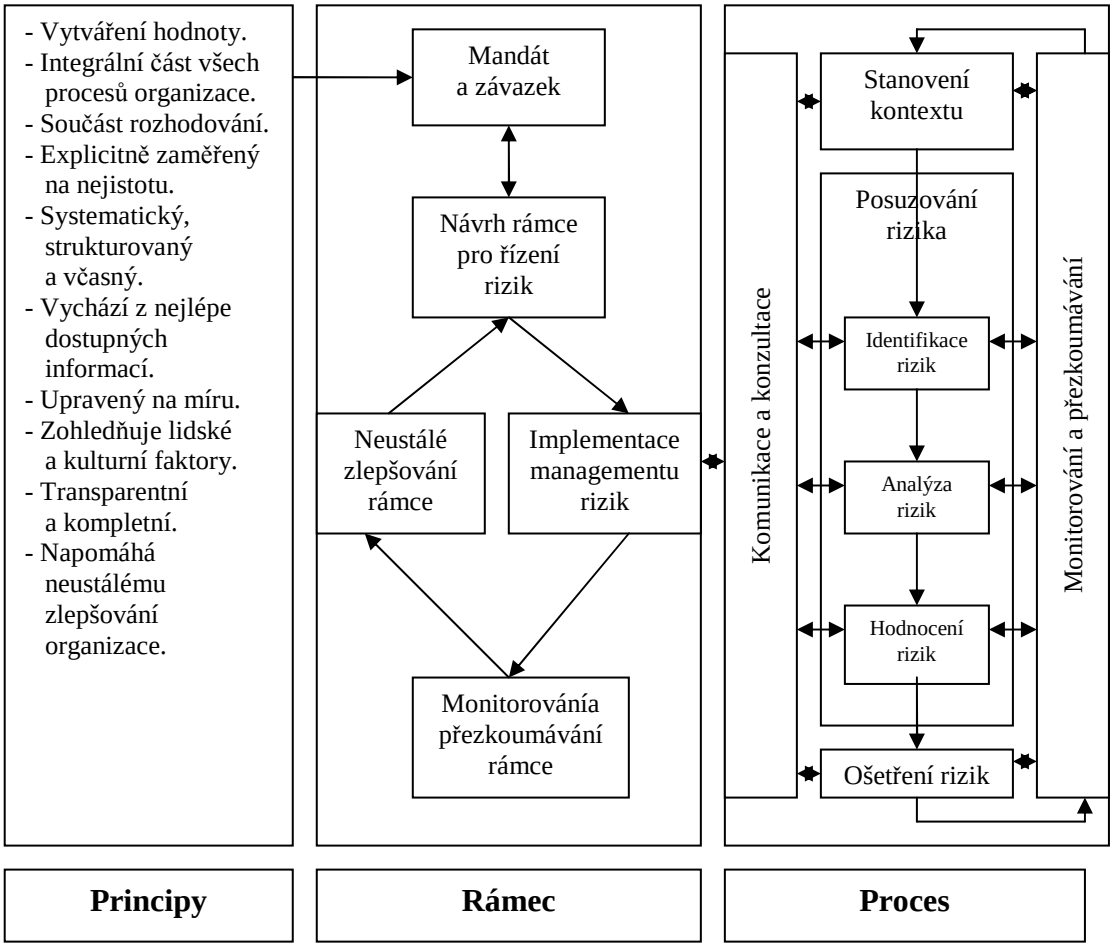
Zdroj: vlastní zpracování dle (ISO 31000:2009), (ISO Guide 73:2009), (IEC/ISO 31010:2009), (ČSN ISO 31000), (ČSN IEC/ISO 31010), (ČSN 36 9790), (TNI 01 350), (ISO 9000), (ČSN EN ISO 9000) a (ISO/IEC 27005:2011), 2016

ISO 31000:2009 definuje metodiku, podle které je možné nastavit řízení rizik podnikatelského subjektu. Pokud organizace zavede risk management v souladu s ISO 31000:2009, umožní tím například:

- zvýšení pravděpodobnosti dosahování cílů organizace,
- podporu proaktivní správy organizace,
- povědomí o nutnosti rozpoznat a řídit rizika v celé organizaci,
- zlepšení identifikace příležitostí a hrozeb,
- dodržování relevantních právních a regulačních požadavků a mezinárodních norem,
- zlepšení systému reportingu,
- zlepšení organizace řízení,
- zvýšení důvěryhodnosti pro zainteresované strany,
- ustavení spolehlivé základny pro rozhodování a plánování,
- zlepšení řízení,
- účinné přidělování a využívání zdrojů pro management rizik,
- zlepšení účelnosti a účinnosti provozních operací,
- zlepšení zdraví, bezpečnosti a ochrany životního prostředí,
- zlepšení prevence ztrát,
- minimalizaci ztrát,
- zlepšení principu učení se v organizaci,
- a zlepšení pružnosti organizace (ISO 31000:2009), (ČSN ISO 31000).

Následující obrázek znázorňuje vztahy mezi principy managementu rizik, jeho rámcem a procesem.

Obrázek 5: Vztah mezi principy managementu rizik, jeho rámcem a procesem



Zdroj: vlastní zpracování dle (ISO 31000:2009) a (ČSN ISO 31000), 2016

Dle principů ISO 31000:2009 je management rizik nedílnou součástí rozhodovacích procesů v podniku. Jím poskytované informace usnadňují rozhodování a umožňují práci s případnými riziky v rámci jednotlivých složek organizace. Naléhavá potřeba řídit informace a rizika, která jsou s nimi spojena, vedla ke vzniku vědní disciplíny označované jako informační management (Day 2008). Účelnost informačního managementu dokazují, mimo jiné, Mortonovy komentáře o inovacích v oblasti manažerské práce.

Informační systémy a technologie podporují dle Mortona (1991):

- provést výrazné (kvalitativně inovativní) změny dosavadní manažerské práce,
- integrovat řízení specializovaných funkčních činností nejen v rámci organizace, ale i v rámci kooperaci s externími partnery,
- měnit podmínky konkurenčního klimatu řady odvětví,
- poskytovat firmám nové strategické příležitosti, které vedou k přehodnocování jejich poslání i způsobů, jak nové formulované cíle realizovat,
- změnit organizační a další podnikové struktury,
- transformovat podniky.

Moderní informační management pracuje s předpokladem transdisciplinárního propojení poznatků managementu, informatiky a systémových přístupů (Morton 1991).

2.1.3 Shrnutí

Informace se objevila spolu se vznikem lidské civilizace. V dávné historii byl však pojem informace užíván v jiném smyslu než v současnosti. K novodobému chápání informace přispěly různé přístupy mnoha vědních oborů včetně účetnictví.

Vznik účetnictví byl důsledkem potřeby zmírňovat a odstraňovat informační rizika spojená se zaznamenáváním informací o obchodních transakcích. Současným trendem účetnictví je úsilí o mezinárodní sjednocení účetních pravidel. Legislativní rámec českého účetnictví představují Zákon č. 563/1991 Sb. o účetnictví, vyhlášky provádějící zákon o účetnictví a české účetní standardy. Uvedené dokumenty ovlivňují nastavení procesů probíhajících v účetním (ekonomickém) oddělení všech ekonomických subjektů. S podnikovými procesy je spojen možný výskyt rizik, jejichž řízení by mělo být nastaveno na základě pravidel popsaných v dokumentech, které tvoří normativní rámec risk managementu. Jedná se o mezinárodní normy ISO 31000:2009, ISO Guide 73:2009, ISO/IEC 31010:2009, české národní normy a technické normalizační informace TNI 01 0350, ČSN ISO 31000, ČSN IEC/ISO 31010 a ČSN 36 9790.

V souvislosti s naléhavou potřebou řídit informace a rizika, která jsou s nimi spojena, vznikla nová vědní disciplína, informační management (Day 2008). Informační

management dnes již předpokládá transdisciplinární propojení poznatků managementu, informatiky a systémových přístupů.

2.2 Informace, informatika a systémové přístupy k podnikovým procesům

2.2.1 Informace

Informace představují pro podniky cenné aktivum, se kterým je potřeba zacházet jako s klíčovým podkladem pro veškerá rozhodování. Oproti jiným aktivům mají některé informace tu vlastnost, že s časem hodnotu neztrácejí, naopak se jejich hodnota vlivem působení faktoru času může zvyšovat (Čermák 2007). Při řízení jsou nepostradatelné takové informace, které napomáhají dosažení stanovených cílů (Hanani, Shapira, Shoval 2001).

Informace je klíčovým výchozím pojmem v informatice (Vodáček, Rosický 1997). „Informace lze chápat jako data, kterým jejich příjemce přisuzuje význam na základě znalostí, kterými disponuje; jsou výsledkem poznání a myšlení, které opětovně iniciuje tvořivé myšlení a následně i jednání. Jsou zdrojem se specifickými vlastnostmi – na rozdíl od ostatních zdrojů, u nichž v procesu použití dochází ke spotřebě, jsou informace zdroj obnovitelný, který se dokonce sám generuje“ (ČSN/ISO IEC 2382-1) a (Vodáček, Rosický 1997, s. 65).

V souvislosti s úlohou informace v procesu řízení je dle (Švarcová, Rain 2012) možné použít následující dělení:

- informace o jednoduchých hospodářských operacích,
- informace pro operativní řízení,
- informace pro taktické řízení,
- informace pro strategické řízení.

Mezi operace, které je možné s informacemi provádět patří dle (Edmunds, Morris 2000):

- zaznamenávání a shromažďování informací na nosiči,
- změna nosiče informace,
- přeprava informace na jiné místo,
- zpracovávání informací,

- organizace a výběr informací,
- transformace informací.

K tomu, aby byly informace pro koncové uživatele užitečné, musí splňovat následující kvalitativní charakteristiky. Musí být dle (Tourish, Robson 2006):

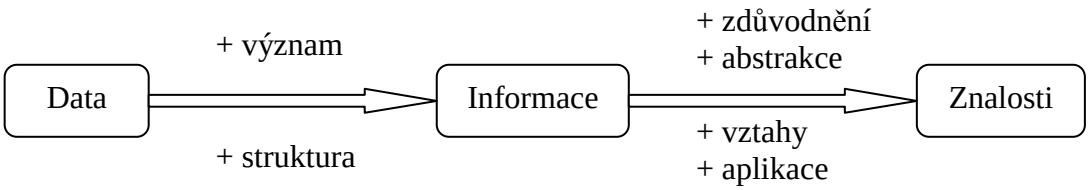
- přesná (bez chyb),
- relevantní (vztahující se k řešené problematice),
- spolehlivé,
- srovnatelné,
- srozumitelné,
- přiměřené (nikoli nedostatečné; s takovou mírou redundance, která umožňuje rekonstrukci informace narušené například šumem při jejím přenosu),
- a včasné.

Koncovým uživatelem informace může být jakýkoli subjekt, například: informatik, účetní, systémový analytik, zákazník, dodavatel, majitel společnosti, státní správa a samospráva nebo obchodník. V souvislosti s rozhodováním na základě všech dostupných informací lze uvést, že nedostatek informací, stejně jako jejich nadbytek, je mimo dalších faktorů (stres, komunikační nesoulad, haló efekt) zdrojem rizika.

Dříve byly činnosti jako shromažďování, třídění či uchovávání dat svěřeny člověku a databáze existovaly ve formě papírových kartoték. Rizika spojená se správou databází je možné identifikovat jak u kartoték používaných v minulosti, tak u dnešních moderních databází. Častá a obtížně identifikovatelná jsou rizika související s možností ztráty nashromážděných dat nebo rizika spojená se selháním lidského faktoru (záměna informací, chybný přenos informace – neúspěšná komunikace, komunikační šumy). Rozvoj informačních technologií mnoho činností, které dříve vykonával člověk, automatizoval, a tím snížil možný výskyt rizik souvisejících s lidským selháním při přenosu dat či vyhledávání informací. Přesto je oblast databází stále oblastí spojenou s možným výskytem informačních rizik. Setkáváme se zde s riziky spojenými s technickým zajištěním funkčnosti databází, s ochranou uchovávaných dat i s riziky souvisejícími se selháním lidského faktoru.

Informace mají pro management organizací velký význam. Současná společnost je známá jako „společnost založená na znalostech“ (znalostní společnost) (Brožová, Houška 2011). V rámci řízení rizik se dnes hovoří spíše o řízení znalostí či požadavků, než o řízení informací (Petříková 2010). Pro takové řízení je potřeba vytvořit v podniku vhodné podmínky. Je nutné mít k dispozici fungující informační systém, který umožní detekovat, sledovat a ošetřit možná rizika (Vrana, Richta 2005).

Obrázek 6: Vztah znalostí, informací a dat



Zdroj: vlastní zpracování dle (Vacek 2010), 2016

Vzhledem k tomu, že znalosti vznikají přetvářením informací (Obr. 6), lze se domnívat, že oblast informací a problematika s nimi spojená zůstává i nadále zajímavou oblastí pro výzkum. V rámci výzkumu je potřeba zaměřovat se nejen na obsah informace, ale také na způsob, jakým je informace sdělována (na formu sdělení), protože smysl a účinek nemá jen obsah informace. Důležitý je také její vliv na příjemce (příjemce na základě obdržené informace formuje své další jednání, myšlení, postoje, emoce).

Přenos představuje jednu z rizikových aktivit spojenou s informacemi. Některá z možných rizik spojených s nevhodně nastaveným způsobem přenosu informací popisuje následující případová studie.

2.2.2 Přenos informací - případová studie (IBM 2013)

Studie popisuje řešení problému přenosu informací (rizika spojená s přenosem informací) ve společnosti, která se pohybuje v oblasti farmaceutického průmyslu. Jedná

se o obchodní skupinu, která se zabývá dodávkami do zhruba 3 000 lékáren. Společnost zaměstnává cca 400 zaměstnanců.

Stávající stav:

- 7 skladů - každý má vlastní zastaralý IT systém a data.
- Není zaveden ERP systém.
- Neexistuje objednávkový systém na web bázi.

Ve společnosti není zaveden ERP systém. Z tohoto důvodu probíhá veškerá komunikace skladů prostřednictvím odesílání textových souborů.

Možná rizika spojená s předáváním informací:

- prozrazení informací,
- ztráta informací,
- nesprávné použití zdrojů nebo aktiv,
- provozní chyba podpůrného personálu,
- selhání software,
- neautorizovaná nebo neúmyslná modifikace informací,
- neúspěšné změny,
- úmyslné poškození zúčastněných stran.

Současné nastavení systému přenosu a sdílení informací znesnadňuje zpracování objednávek (možná rizika se týkají všech oddělení společnosti). Výsledkem je v mnoha případech ztráta zákazníka a objednávky.

Cíl:

Zajištění dodávek do 2 hodin od provedení objednávky zákazníkem.

To není v současné době možné, protože informace, jako stěžejní aktivum, jsou ohroženy mnoha hrozbami, které plynou z neexistence kvalitního vybavení společnosti informačními technologiemi a nedostatku personálu proškoleného v zacházení s informačními systémy. Současný informační systém nedokáže přenést data do skladů tak rychle, aby bylo možné objednávku okamžitě vyřídit.

Řešení:

Zavedení nového systému, který okamžitě zpřístupní data všem skladům (informace v reálném čase).

Společnost se rozhodovala mezi dvěma vytipovanými systémy. Nakonec zvolila IBM Informix, který byl méně náročný na obsluhu a množství zaměstnanců.

Nový stav:

- IBM Informix. (Centrální databáze a 13 databází: 7 skladů a 6 zpracovatelských středisek.)

Informix zajišťuje funkčnost systému pomocí synchronizace systémů vzdálených skladů, přípravy objednávek a správy kmenových dat.

Výsledky:

- Zlepšení práce s informacemi.
- Zvýšení počtu objednávek vyřízených v jednom dni.
- Snížení počtu zaměstnanců - snížení mzdových nákladů.
- Snížení množství faxů, emailů a telefonních hovorů.
- 30% snížení nákladů na hardware.
- 10 - 15% nárůst prodeje.
- 20% snížení chybovosti => 20% nárůst produktivity.

V extrémně konkurenčním prostředí farmaceutického průmyslu umožnilo zavedení nového IS získávat obchody a nepřicházet o ně. Došlo k posílení loajality pracovníků společnosti i k posílení loajality dalších subjektů, které se společností spolupracují.

2.2.3 Informatika a systémové přístupy k podnikovým procesům

Předchozí studie poukazuje na pozitivní dopady zavedení nového informačního systému v podniku, kde této oblasti zatím nebyla věnována dostatečná pozornost. Vhodné a funkční informační systémy usnadňují provádění veškerých podnikových aktivit, čímž do značné míry snižují počet vzniklých rizikových situací. V rámci normy ČSN 36 9790 je doporučováno zaměřit proces managementu rizik na provádění

provozních činností a aplikovat jej na celý systém managementu bezpečnosti informací (ISMS). Nové informační systémy by však měly být do ISMS zahrnuty již ve fázi plánování a návrhu, aby bylo zajištěno, že jakákoliv rizika bezpečnosti informací jsou náležitě řízena.

Rozšíření využití informačních systémů je reakcí podniků na změny a nové přístupy v oblasti řízení podnikových procesů, které je dle (Sodomka 2006) a (Molnár 2000) možné rozčlenit na interní procesy, u nichž je přesně určený vlastník a jejichž řízení má plně pod svou kontrolou management společnosti a na procesy externí, u kterých není vlastník přesně určen a management společnosti je nemá plně pod kontrolou. Dále je možné podnikové procesy rozdělit na:

- Řídící procesy - strategické plánování a řízení společnosti, řízení kvality a inovací.
- Klíčové procesy - výroba, logistika, řízení vztahů se zákazníky.
- Podpůrné procesy - řízení ekonomiky, řízení lidských zdrojů, řízení IS/ICT.

Podpůrným procesem je dle (Pavelka, Klímek 2000) myšlen proces, který nepřidává hodnotu, neprobíhá napříč společností, nemá externí zákazníky a negeneruje tržby.

S ohledem na zaměření disertační práce je blíže specifikována pouze kategorie podpůrných procesů, resp. řízení ekonomiky, do kterého lze dle (Monk, Wagner 2013) zařadit:

- finanční účetnictví,
- řízení a kontrolu nákladů,
- plánování a rozpočtování,
- řízení cash-flow.

Aby mohl systém řízení ekonomických procesů podniku plnit požadavky, kladené na něj v souvislosti s existencí současného turbulentního prostředí, musí být založen na informacích, které pochází ze všech výše uvedených složek řízení ekonomiky (Monk, Wagner 2013).

V souladu s požadavky na řízení podnikových procesů a nabídkou dodavatelů je možné klasifikovat podnikové informační systémy podle jejich praktického uplatnění. Obecně lze podnikové informační systémy rozdělit na:

- ERP (Enterprise Resource Planning) - systém zaměřený na řízení interních podnikových procesů,
- CRM (Customer Relationship Management) - systém řídící procesy směřované k zákazníkům,
- SCM (Supply Chain Management) - systém, který řídí dodavatelský řetězec,
- MIS (Management Information System) - systém určený pro sběr dat ze systémů ERP, CRM, SCM a externích zdrojů, který na jejich základě poskytuje informace pro rozhodovací proces podnikového managementu (Sodomka 2006), (Sodomka, Klčová, Vořechová 2008).

Systémy ERP, CRM a SCM jsou komponentami Business Intelligence (BI). Howard Dresner (Dresner 2015) popisuje BI jako souhrn nástrojů, které umožňují uživatelům ucelený a efektivní přístup k datům v podnikových informačních systémech a jejich analýzu za účelem lepšího porozumění podnikání a zákazníkům.

Dopad uvedeného holisticko-procesního pohledu na podnikový informační systém je patrný v oblasti trhu se softwarovými aplikacemi, pomocí kterých je budován informační systém společností, jejichž cílem je obstát v konkurenčním prostředí globální ekonomiky (Sodomka 2006).

Ve finančním řízení podniku jsou dle Novotného, Poura a Slánského (2005) aplikace BI využívány zejména v oblastech:

- Plánování a prognózování.
- Finanční výkaznictví a konsolidace.
- Analýzy nákladů a ziskovosti.
- **Řízení rizika.**
- Finanční optimalizace.

Obecně je cílem systémové integrace ve smyslu vývoje integrovaného informačního systému nastavení podnikových informačních technologií tak, aby byl s ohledem

na efektivitu a bezpečnost provozu systému vytvořen jednotný informační systém v potřebné kvalitě, a aby byla podpořena podnikatelská strategie podniku (Dresner 2015).

2.2.4 ERP systémy

Pro podnikové informační systémy jsou zásadními aplikace pro řízení interních podnikových procesů: výroby, vnitřní logistiky, personalistiky a ekonomiky. Mezi informační systémy zaměřené na řízení těchto čtyř oblastí patří systémy ERP, které jsou dle (Sodomka 2006) definovány jako účinný nástroj, který je schopen pokrýt plánování a řízení hlavních interních podnikových procesů (zdrojů a jejich transformace na výstupy), a to na všech úrovních řízení, od operativní až po strategickou.

Celosvětový trh ERP rostl dle (Columbus 2014) v roce 2012 o 2,2 % na $24,4B (billion), v roce 2013 o 3,8 % na $ 25,4B (billion). Největší podíl na trhu si dle (Statista 2014) udržela společnost SAP. Mezi deset největších prodejců ERP systémů patří: SAP, Oracle, Sage, Infor, Microsoft, Kronos, Concur, IBM, Totvs a YonYou. V České republice se množství podniků využívajících ERP systémy začalo navyšovat od roku 2009 (Sodomka, Klčová 2010). Největší pozornost ze strany podniků je věnována modulům zaměřeným na účetnictví (ČSÚ 2014). Pevné základy kvalitního ERP řešení tvoří dobře zpracované finanční moduly. Pokud nemáte přehled o vlastních prostředcích a finančních tocích, nemáte přehled o ničem (J.K.R. 2014). Na základě informací získaných prostřednictvím provedených šetření lze uvést, že v současnosti v Čechách využívají ERP systémy velké, střední i malé podniky. Situaci v oblasti ERP systémů v ČR shrnuje následující tabulka.

Tabulka 3: Podniky využívající ERP systémy, Česká republika - leden 2014

Velikost podniku podle počtu zaměstnanců	Podíl podniků využívajících ERP na celkovém počtu podniků v dané velikostní skupině (v %)
10 - 49	19,5
50 - 249	53,3
250 a více	81,1
Celkem	27,7

Zdroj: vlastní zpracování dle (ČSÚ 2014), 2016

S ohledem na zaměření disertační práce jsou dále sledovány zejména ekonomické ERP systémy. Ekonomické ERP systémy využívají společnosti, kterým již nestačí pouze vedení účetní agendy, většinou střední a větší firmy. Záměrem společností, které se rozhodnou implementovat ERP systém, je propojení ekonomických, obchodních, personálních, výrobních a dalších podnikových procesů. Společnosti mohou volit mezi různými systémy. S ohledem na prováděné činnosti, velikost a charakter podniku mohou zvolit libovolnou sestavu modulů ERP (například moduly řízení výroby, řízení vztahů se zákazníky nebo personální informační systém).

Přehled některých ekonomických systémů nabízených v České republice je uveden v následující tabulce.

Tabulka 4: Přehled některých ekonomických ERP systémů nabízených v ČR

Software	Výrobce / Prodejce	Software	Výrobce / Prodejce
ABRA G2, G4, G4	ABRA Software a.s.	K2 Software	K2 atmitec s.r.o.
ALTEC Aplikace	ALTEC a.s.	KARAT	KARAT Software a.s.
Altus VARIO	Altus software s.r.o.	KelWIN, KelEXPRESS, KelSQL	KELOC CS, s.r.o.
ARBES FEIS	ARBES Technologies, s.r.o.	KISS	Sigma Soft, spol. s r.o.
AZ.PRO	PROSPEKS-IT, a.s.	KTKw	KTK SOFTWARE s.r.o.
BENEFIT	Benefit CZ, s.r.o.	MARK	Valet MT, spol. s r.o.
BYZNYS	J.K.R.	MODULSOFT	EN Nástroje, s.r.o.
CUBIQ	HSF spol. s r.o.	MONEY S3, S4, S5	CÍGLER SOFTWARE, a.s.
DataGo4+	INFOSYS spol. s r.o.	MYGEM	Gemco, s.r.o.
DIALOG	Control spol. s r.o.	mywac	myWAC TECHNOLOGIES s.r.o.
DIMENZE++	CENTIS, spol. s r.o.	Notia Business Server	NOTIA Informační systémy
eFiles Enterprise	RKA SW Systems s.r.o.	Orsoft	ORTEX spol. s r.o.
Ekonomika a logistika	Vema, a.s.	PERISKOP	Accord, spol. s r.o.
EPASS	EPASS s.r.o.	PREMIER	PREMIER System, a.s.
ERP IMES	Software OK Příbram, s.r.o.	QAD	QAD Inc./Minerva Česká republika, a.s.
ERP16	CyberSoft, spol. s r.o.	QI	DC Concept a.s.
ESO9	ESO9 intranet a.s.	RIS	Saul IS spol. s r.o.
EXACT	Exact Software CEE s.r.o.	SAP	SAP ČR, spol. s r.o.
flexibee	FlexiBee Systems s.r.o.	SlimOffice	SLIM, s.r.o.

Software	Výrobce / Prodejce	Software	Výrobce / Prodejce
HELIOS RED, ORANGE, GREEN	Asseco Solutions, a.s.	Smart4Web ERP	M2000 spol. s r.o.
IMPULS32	NOVA-SOFT spol. s r.o.	TwistInspire	Beep s.r.o.
INFOS	Infos 2001 spol. s r.o.	Vision32	Vision Praha s.r.o.
IS KOSTKA	APEX Computer, s.r.o.	WAK INTRA	WAK System, spol. s r.o.
JUNO	BETASOFT s.r.o.	WinFas	Organizační kancelář, s.r.o.

Zdroj: vlastní zpracování dle (Účetní software 2015), 2016

Největším dodavatelem ERP systémů je společnost SAP, která má celosvětově největší tržní podíl na trhu ERP systémů. Základním cílem společnosti SAP je maximalizovat spokojenost uživatelů v duchu firemního motta: „Making the world run better & improving people's lives." SAP podporuje množství neziskových organizací a realizuje řadu samostatných CSR projektů (Corporate Social Responsibility = společenská odpovědnost podniku), které vedou k naplnění této vize (SAP 2014).

V podmínkách ČR se se systémem SAP setkáváme často, a to zejména u velkých společností. K implementaci tohoto systému již přistoupilo také množství středních i malých podniků (SAP ČR 2014). MSP však často využívají jiné, pro ně dostupnější, podnikové ERP systémy. V případě účetních společností jsou v rámci výběru ERP zohledňovány kritické oblasti uvedené v následující tabulce.

Tabulka 5: Kritické oblasti ERP sledované v rámci účetních firem

Oblast	Popis
Detailní nastavení účetních předkontací	Využití při automatickém účetním zpracování prvotních dokladů => výrazné urychlení účtování.
Automatizace rutinních a kontrolních procesů	Využití moderních systémů pro sledování průběhu jednotlivých kroků v rámci opakovaných činností s využitím modulu Workflow a autorizace dokladů.
Evidence a archivace dokumentů a záznamů	Využití centra sdílení dokumentů. Je možné uchovávat dokumenty v přehledné struktuře i s nastavením přístupových práv na základě definované organizační struktury společnosti.

Oblast	Popis
Výkaznictví a uživatelské výstupy	Systém uživatelsky definovaných výstupů umožňuje přizpůsobení sestav a formulářů na základě přání jednotlivých zákazníků.

Zdroj: vlastní zpracování dle (J.K.R. 2014), 2016

Některé další faktory ovlivňující volbu informačního systému v MSP jsou uvedeny v následující případové studii.

2.2.5 Výběr a implementace ERP systému pro MSP - případová studie

Studie se zaměřuje na identifikaci rizikových oblastí v procesu výběru a implementace ERP systému podnikem spadajícím dle (European Commission, 2003) do kategorie MSP. Jedná se o společnost zaměřenou dle NACE na výrobu potravinářských výrobků a nápojů (MFČR 2015a). Společnost je rozdělena na pět oddělení, která spolupracují na jednotlivých aktivitách zajišťovaných v rámci nastavení podnikových procesů.

Situace před zavedením ERP:

Management společnosti používá starý informační systém vyvinutý místním dodavatelem softwaru. S rozvojem společnosti se uvedený systém jeví jako nedostačující. Proto se management společnosti rozhodl pro nákup nového IS.

V souladu s požadavky na IS, které se týkaly zejména přenosové rychlosti dat, datové kompatibility se stávajícím systémem (nutnost přenosu velkého množství původních dat), vzhledu a využitelnosti získávaných analýz a možnosti dalšího zpracování získaných výstupů, byl na základě informací získaných od prodejců systémů, stávajících uživatelů systémů, manažerů a zaměstnanců podniku, majitele podniku a informací získaných na internetu (technické parametry systému) volen vhodný informační systém.

V průběhu rozhodovacího procesu bylo nutné brát v úvahu požadavky managementu podniku, kterými byly dlouhodobá dodavatelská podpora, široká kompatibilita systému s garancí další modernizace systému, uspokojení specifických požadavků potravinářského a nápojového průmyslu, modulární materiálové účty, plánování distribučních požadavků a interní pohyb materiálu. Společnost vlastní certifikáty ISO 9001 (Management kvality) a ISO 14001 (Environmentální management). Shoda

s nastavením procesů daných těmito normami požaduje dohledatelnost (traceability) produktů v obou směrech, což zajišťuje program QAD specializovaný na operační management a výrobu.

Provedené referenční návštěvy omezily výběr na dva systémy, QAD a K2. Srovnání některých faktorů ovlivňujících konečné rozhodnutí je uvedeno v následující tabulce.

Tabulka 6: QAD a K2 - porovnání faktorů ovlivňujících výběr ERP

Srovnávané oblasti	K2	QAD
Tvůrce systému	K2 atmitec s.r.o.	QAD Inc.
Prodejce systému v ČR	K2 atmitec s.r.o.	Minerva Česká republika, a.s.
Počet instalací v ČR	550	500
Typ spotřebitele / uživatele IS	výrobní podnik, obchodní společnost, zprostředkovatel služeb	výrobní podnik, distribuční společnost
Doba implementace	3 měsíce	1 - 6 měsíců
Cena pořízení	250 000 Kč	399 000 - 999 000 Kč
Podpora legislativy	česká, slovenská, US GAAP	česká, IAS, slovenská
Dostupné moduly	Marketing, prodej, nákup, sklad, doprava, celnice, výroba, finance, mzdy a personalistika, majetek, účetnictví a analýzy, business intelligence, workflow, média.	QAD EA, EDI, finance, řízení jakosti, prodej a marketing, pohledávky a závazky, plánování, řízení dodavatelských vztahů, technická příprava výroby, výroba, zákaznický servis, zásoby, ostatní.
Uživatelské rozhraní	znakové, grafické, internetové	znakové, grafické, internetové
Kontrolované podnikové procesy	Plánování výroby, koordinace výroby, řízení výroby, management jakosti, finance.	Prodej a marketing, plánování výroby, nákup, řízení výroby, řízení zásob, technická příprava výroby, kontrola kvality, projektový management, CRM, finance.

Zdroj: vlastní zpracování dle (K2 atmitec s.r.o. 2015) a (QAD 2015), 2016

Konečnou volbou managementu podniku byla implementace ERP systému QAD, který využívají i konkurenti společnosti. Tento systém je využíván zejména ve skladech

s velkou pohyblivostí zboží, vysokým počtem skladovaných položek, nebo ve skladech, které jsou ve vlastnictví více obchodních jednotek. Systém QAD je navržen zejména pro komplexní management výrobních podniků v oblasti elektroniky, strojírenství, automobilového průmyslu, potravinářského průmyslu, spotřebního zboží, farmaceutického a chemického průmyslu. Zahrnuje plánování a řízení výroby, prodej, nákup, skladové hospodářství, finanční řízení a řízení servisu. Uživatelé QAD jsou odborníky ve svém oboru a nemusí být specialisté na informační a komunikační technologie. Aplikace QAD jsou proto vyvinuty s intuitivním ovládáním. Uživatelé si mohou zvolit vhodný typ uživatelského rozhraní.

Implementace ERP a situace po jeho zavedení:

Grabot, Mayère a Bazet (2008) popisují implementaci ERP systému v organizaci jako riskantní a složitý projekt. Mnoho implementací ERP ztrácí na úspěšnosti díky časovým prodlevám a dodatečným nákladům, ale také díky omezením ze strany uživatelů, což může v extrémních případech vést k částečné ztrátě kontroly nad společností a jejími aktivitami. Obecně lze implementaci ERP popsat jako proces (Olson 2008), složený z těchto kroků:

- Návrh a plán projektu - obchodní proces a příprava realizace.
- Design - ustavení týmu.
- Implementace systému.
- Rozvoj - dokončení a případné úpravy, uživatelská školení a import dat.
- Testování - kontrola funkčnosti systému s ohledem na stanovené požadavky.
- Spuštění systému - rozhodnutí realizačního týmu o využití systému, stahování a ověřování dat, další uživatelská školení.
- Další podpora - modifikace a změny nastavení systému.

Implementace ERP systému trvá v závislosti na typu systému a velikosti společnosti, která jej bude využívat, od jednoho do šesti měsíců. Ve sledované společnosti trvala implementace systému QAD šest měsíců. V průběhu zavádění nového IS byla do nových databází přesunuta původní data, byly vytvořeny nové číselníky evidovaných položek a proběhla úprava formy finálních výstupů, které systém poskytuje. Dříve chybně nebo nedostatečně nastavené podnikové procesy byly v souladu s možnostmi

nového systému zpracování dat přenastaveny tak, aby zajistily plynulý chod organizace. Nový a původní informační systém byly jednotlivými odděleními používány simultánně více než tři měsíce s cílem identifikovat a eliminovat slabá místa systému. Úspěšnost implementace informačního systému obecně a úspěšnost implementace ve sledované společnosti dokládají následující tabulky.

Tabulka 7: QAD implementace - obecné přínosy

Řízení nákladů	IT management	Ostatní oblasti
Transparentnost nákladů na IT.	Jednodušší organizace fungování IT.	Garance kvality výrobků v souladu s certifikáty ISO.
Časové rozložení počáteční investice.	Dostupnost jednotlivých komponentů je smluvně zaručena.	Snížení zásob.
Prodej nepotřebného hardwaru.	Řešení problémů je smluvně zaručeno.	Využití Just-in-time technologií.
Úspora nákladů v personální oblasti.	Specializace zaměstnanců IT.	Mezinárodní spolupráce.
	Vývoj informačních systémů a vzdělávání uživatelů je smluvně zaručeno.	

Zdroj: vlastní zpracování dle provedených šetření, 2016

Tabulka 8: QAD implementace - dopady do procesů účetního oddělení

Oblast činnosti	Specifikace procesu	Původní informační systém	QAD
Fakturace	Fakturace.	Ruční vkládání dat, chybovost při násobném přenosu dat.	Snížení výskytu chyb vzniklých v rámci přenosu dat. Import dat z jednotlivých komponent systému.
Financování	Provádění běžných plateb, nákup technického vybavení.	Evidence nákupů a běžných plateb, výstupy formou ručně zpracovaných tabulek.	Provázanost modulů jednotlivých oddělení, výstupy zpracované prostřednictvím IS.

Oblast činnosti	Specifikace procesu	Původní informační systém	QAD
Inventarizace	Inventarizace, evidence a ochrana majetku.	Evidence majetku, ruční opravy chyb v dokumentech.	Evidence majetku, přenos úprav mezi dokumenty.
Uchovávání účetních dokladů	Archivace dokladů podle Zákona č. 563/1991 Sb., o účetnictví.	Časté chyby ve značení dokladů, ztráta nebo poškození dokladů.	Snížení výskytu chyb ve značení dokladů.
Skartace - dokumenty v tištěné podobě	Likvidace dokladů.	Předčasná skartace dokladů.	Omezení záměn dokladů, snížení výskytu předčasné skartace.
Ekonomika práce a mezd	Záznamy o zaměstnancích, příprava mezd.	Manuální zpracování, výskyt přepisů.	Snížení výskytu chyb při přenosu dat mezi dokumenty (mezi komponentami IS).
Dodavatelsko odběratelské vztahy	Zpracování nabídek, opravy dokumentů.	Manuální zadávání dat - s každým dokladem nový zápis.	Manuální zadávání dat - přenos dat mezi doklady.
Informační soustava	Předávání informací mezi odděleními.	Informace mezi odděleními předávány ústně (formou porad) nebo písemně (formou mailu).	Sdílení dat jednotlivými odděleními dle odpovědnosti. Omezený přístup k modulům ostatních oddělení - nastavení přístupových práv.
Reporting	Příprava závěrečných zpráv.	Ruční zpracování.	Zpracování prostřednictvím IS.

Zdroj: vlastní zpracování dle provedených šetření, 2016

Zjištění:

Zavedení nového informačního systému bylo správným rozhodnutím, které v rámci sledovaného oddělení společnosti umožnilo automatizaci některých procesů a snížilo výskyt chyb v rámci práce s doklady.

Problémy spojené se zaváděním IS se vyskytly zejména v oblastech:

- fakturace - obtížná sledovatelnost změn v oblasti reklamací,
- dodavatelsko-odběratelské vztahy - nutná kooperace mezi odděleními k zajištění omezení nadbytečnosti dat plynoucí z vícenásobného pořízení záznamů,
- reporting - identifikace potřeby nové úpravy požadovaného výstupu.

Implementace ERP systému QAD umožnila společnosti lepší přístup k informacím, přinesla zlepšení pracovních postupů a snížení nákladů na interní komunikaci. Současně však užívání nového systému klade vyšší nároky na kvalifikaci zaměstnanců a spolupráci jednotlivých oddělení. V souvislosti s užíváním QAD se postupně objevily požadavky na úpravu finálních výstupů předkládaných jednotlivými odděleními, které bude nutné řešit se zástupci dodavatelské společnosti.

2.2.6 Shrnutí

Informace jsou pro společnosti cenným aktivem. Jejich přenos představuje jednu z rizikových aktivit, které je v rámci získávání, zpracování a uchovávání informací věnována mimořádná pozornost. Jednou z možností, jak nakládat s daty, je jejich zpřístupnění zaměstnancům prostřednictvím informačního systému. Pro podnikové informační systémy jsou zásadními aplikace pro řízení interních podnikových procesů: výroby, vnitřní logistiky, personalistiky a ekonomiky. Mezi informační systémy zaměřené na řízení těchto čtyř oblastí patří systémy ERP, které zefektivňují práci s informacemi a pomáhají řešit problémy spojené s přenosem informací. Podle zjištění prezentovaných společností Panorama Consulting Solutions (Panorama Consulting Solutions 2014) vzrůstá efektivita podniků po instalaci ERP systému až o 37 %.

Aby byl zvolen vhodný ERP systém, je potřeba zvážit aktuální stav technického vybavení (množství serverů a klientů, počet IT zaměstnanců, spolehlivost sítě, aktuálně používaný software). Je nutné zaměřit se také na předpokládaný rozpočet. Nejdůležitějším měřítkem při hodnocení vhodnosti ERP systému je jeho funkce a použitelnost. Nejvhodnějším řešením je provedení analýzy veškerých podnikových procesů a následné přizpůsobení ERP objednateli. Současným trendem v oblasti ERP je zaměření se na zvýšení mobility a lepší využití informací. Dochází k upřednostňování komplexního řešení a prosazování dvouvrstvé strategie nasazování ERP

(jiná konfigurace ERP pro regionální divize a jiná konfigurace ERP pro centrálu). Informační systémy usnadňují provádění veškerých podnikových aktivit, čímž do značné míry snižují počet vzniklých rizikových situací. V rámci normy ČSN 36 9790 je doporučováno zaměřit proces managementu rizik na provádění provozních činností a aplikovat jej na celý systém managementu bezpečnosti informací (ISMS).

2.3 Informační rizika a informační management

Problematika informací, respektive problematika informačních systémů, společně s problematikou informačních rizik a informačního managementu, které jsou vysvětlovány v mnoha titulech, například (Boehm 1998), (Brož 1997), (Jirásek 2008), (Sokolowsky 2002a) a (Spanos, Prastacos, Polymenakou 2002), tvoří základnu, ze které jsou získávány teoretické i praktické informace potřebné pro výzkum popsaný dále v disertační práci.

2.3.1 Rizika obecně - informační rizika

Riziko je pojem, se kterým se lze setkat již v dávné historii. Jeho používání se formalizovalo v 17. století v souvislosti s lodní přepravou. Své kořeny má v italském slově „risico“ a prvotně bylo známo jako úskalí, kterému se při svých cestách museli vyhýbat mořeplavci (Smejkal, Rais 2006). V 17. – 18. století se objevuje v matematice, kde je popisováno v souvislosti s výkladem pravděpodobnosti výher v hazardních hrách a v pojištění lodí (Vacík 2005). Ve smyslu možné ztráty (ekonomický pohled) je riziko chápáno až v posledních desetiletích (Svozilová 2007). Dnes je pojem riziko chápán zejména jako možnost (nebezpečí) vzniku škody, nebo možnost nezdaru při prováděné činnosti.

Obecně ale nelze rizika chápat jen jako negativní dopad na vykonávanou aktivitu. Nejedná se jen o hrozby, i přes to, že takové pojetí obvykle převládá. Rizika můžeme dle (Svozilová 2007) vnímat také jako určitý podnět, motivaci, příležitost k nalezení kvalitnějšího, úplnějšího nebo alternativního řešení daného problému. Literatura (Čermák 2007), (Kruliš 2011) a (Petříková 2010) uvádí různá dělení rizik do skupin podle různých hledisek. I když jsou mnohdy jinak označena, vyskytují se téměř ve všech těchto rozděleních také rizika informační.

Další zdroje, například (Daněk 2007), (Korecký, Trkovský 2011) a (Merna, Faisal 2007) nejčastěji uvádí rizika v rozdělení na rizika finanční, rizika bezpečnostní a ochrany životního prostředí, rizika informačních systémů, projektová rizika, nebo organizační rizika. Toto rozdělení je uváděno zejména v souvislosti se subjekty působícími v podnikatelském sektoru. Odborné publikace (Prokůpková 2007), nebo (Vacek 2006), zabývající se riziky organizací působících v oblasti veřejné sféry, mohou dělit rizika jinak, například na rizika finanční, rizika provozní, rizika spojená

s řízením, rizika spojená s vnitřním a vnějším prostředím, rizika spojená s transakcemi či rizika informační. Rizika můžeme také rozdělovat na rizika představující neustálou hrozbu s případnými obtížně řešitelnými následky a na rizika, která sice vyžadují, aby je měli jednotliví odpovědní pracovníci na zřeteli, ale jejichž řízení či snížení jejich dopadu na činnosti podniku je poměrně snadno řešitelné v rámci relativně krátkého časového úseku. Ve všech uvedených případech je však dle (Blaha 2004), (Čermák 2007) a (Garlick 2007) důležité umět rizika „hlouběji identifikovat“ a určit, která z nich skutečně, ať už podstatnou měrou nebo jen okrajově, ovlivňují činnosti podnikatelských subjektů.

V souvislosti se změnou pohledu na informace se do popředí zájmu dostávají informační rizika a jejich řízení, resp. možnost ovlivnit jejich dopad do podnikových procesů.

- Čermák (2007, s. 17) definuje informační riziko jako: „možnost, že specifická hrozba využije specifickou zranitelnost systému a dojde k ohrožení důvěrnosti, integrity nebo dostupnosti aktiva a tím k nežádoucímu výsledku vedoucímu ke vzniku škody.“
- Česká technická norma (ČSN 36 9790, s. 7), která se zabývá systémem managementu bezpečnosti informací, definuje riziko v obecné rovině, jako: „kombinaci pravděpodobnosti výskytu události a jejích následků,“ přičemž událost v bezpečnosti informací je definována jako: „identifikovaný výskyt stavu systému, služby nebo sítě, který indikuje možné porušení politiky bezpečnosti informací nebo selhání bezpečnostního opatření, nebo předem neznámé situace, která může být významná z hlediska bezpečnosti.“

S ohledem na procesy probíhající v podniku, je možné rozdělit informační rizika na:

- Informační rizika specifická pro určité organizační procesy, směřující vně organizace.
    - Prodej a marketing.
    - Výroba a provoz.
    - Služby zákazníkům.

- Informační rizika specifická pro určité organizační procesy, směřující dovnitř organizace.
    - Lidské zdroje.
    - Výzkum a vývoj.
    - Administrace a IT.
    - Finance a účty.

Dále je možné informační rizika dělit na:

- Rizika spojená s informačními technologiemi.
- Rizika spojená se selháním lidského faktoru.
    - Rizika plynoucí z možnosti, že dojde k ohrožení kvality informací.
    - Rizika plynoucí ze ztráty informací.
    - Rizika plynoucí z úniku a zneužití informací.
    - Selhání při práci s informacemi.

Aby bylo možné informační rizika řídit, je nutné seznámit se s jejich zdroji, příčinami a projevy.

Některé zdroje a příčiny informačních rizik

- Nejasně stanovené, nesprávně pochopené cíle, stanovené jinou osobou než finálním uživatelem produktu.
- Nevnímavost, nespolupráce nebo ztráta zájmu uživatele o nový systém.
- Různá nebo nerealistická očekávání vedoucích pracovníků a uživatelů produktu.
- Nejednoznačné, přísné nebo neúplné požadavky na zadání, mnohdy formulované vedoucím pracovníkem, nikoli uživatelem produktu.
- Špatná interpretace výsledků (z nepochopení, záměrná) (Morozov 2011).
- Nejasná definice projektových rolí a odpovědnosti.
- Nedefinované, nerealistické nebo vnějšími vlivy změnitelné výstupy.
- Velikost týmu pro řízení rizik.

- Různorodost uživatelů produktu.
- Komplexnost systému (produktu).
- Závislost na jiných projektech.
- Použitá technologie.
- Použití IS tam, kde to není vhodné.
- Vyšší moc.

Některé projevy informačních rizik

Mezi projevy (dopady, důsledky) informačních rizik je možné řadit:

- Odklon od stanovených cílů či jejich úplné nedodržení.
- Nevyužití všech možností informačního systému, návrat k původně používanému systému.
- Nesplněné požadavky a „rozčarování“ uživatele informačního systému.
- Časové prodlevy v jednotlivých fázích vývoje informačního systému či nedokončení projektu.
- Nadbytečné nebo nedostatečné informace o možných rizicích v jednotlivých etapách životního cyklu informačního systému.
- Různá míra využití finálního informačního systému uživatelem.
- Nekompatibilita navrženého informačního systému s ostatními částmi informačního systému podniku.

Z výše uvedených informací o zdrojích, příčinách a projevech informačních rizik popsaných v literatuře, která se danou problematikou zabývá, (ČSN 36 9790), (ČSN ISO 31 000) a (Švarcová, Rain 2012), je patrné, že jedním z hlavních zdrojů rizika v rámci informačních systémů může být sám člověk. Odpověď na otázku, jak se s tím vyrovnat, by proto měla být formulována ve spolupráci s odborníky na oblast řízení lidských zdrojů.

2.3.2 Informační rizika v účetnictví

Dle ČSN 36 9790 má posouzení rizika bezpečnosti informací prvořadou důležitost pro finanční a účetní procesy organizace. V oblasti řízení organizace jsou vyžadovány stálé a přesné finanční informace, které je možné sledovat pomocí transparentních kontrol od jejich vzniku až ke chvíli, kdy dochází k jejich využití. Důvěrnost citlivých finančních informací musí být udržována v souladu s předpisy a požadavky podnikání.

Informační systém podniku představuje důležitý nástroj řízení podnikových procesů. Bývá tvořen moduly, které jsou vhodné pro použití v různých odděleních podniku. Jedním z nejdůležitějších modulů podnikového informačního systému je modul účetnictví.

Využívání účetního IS nebo účetního modulu podnikového IS s sebou nese dle (Dolejšová 2006) a (O'Connor, Martinsons 2006) možnost vzniku těchto rizik:

- Pořízení takového HW a SW, který nevyhovuje požadavkům pro vedení účetnictví.
- Nevhodné postupy při vývoji systému ze strany dodavatele účetního IS.
- Neodhalená selhání používaného HW a SW.
- Ztráta nebo poškození dat během jejich zpracování.
- Nespolehlivé zpracování dat.
- Neodhalené chyby ve změnách souborů a databází. Nedostatečné nebo nesprávné přidělení práv k využívání účetního systému.
- Výskyt chyb v účetních programech.
- Nedostatečná dokumentace a nápověda k účetnímu programu.
- Podcenění školení zaměstnanců pracujících s účetním IS.
- Záměrné nebo náhodné chyby způsobené uživateli účetního IS (například: nedodržení podvojnosti účetních záznamů, zaúčtování na nesprávné účty, zaúčtování na nesprávné strany účtů, použití neexistujícího účtu, nesoulad mezi syntetickou a analytickou evidencí, nesoulad mezi částkou uvedenou v IS a na dokladu, nesoulad účetního záznamu a skutečného stavu, nedostatečné opravy účetních zápisů).

- Neprovázanost různých modulů IS (účetnictví - mzdy)
- Nedostatečné omezení přístupu zaměstnanců k modulu.

Riziko plynoucí z chyb způsobených uživateli účetního IS bývá snižováno pomocí nastavení vnitřního kontrolního systému, který v sobě zahrnuje kontrolní prostředí, účetní systém a kontrolní postupy.

Kontrolním prostředím je dle (Dolejšová 2006):

- filosofie a styl řízení podniku,
- organizační struktura podniku,
- metody delegování pravomocí,
- metody sledování kontrol,
- personální politika
- a legislativa.

Účetní systém je dle (O'Connor, Martinsons 2006) spojen s:

- metodami zaznamenávání,
- zpracování,
- a vykazování finančních informací.

Kontrolní postupy jsou dle (Dolejšová 2006) spojeny se:

- správným schvalováním transakcí,
- oddělením funkcí,
- postupy pro zacházení s majetkem,
- práci s podnikovou dokumentací a účetními záznamy,
- prováděním kontrol výkonnosti informačního systému.

S využíváním účetního IS je sice spojena možnost výskytu chyb, jejich množství je však oproti opakovanému manuálnímu zadávání dat nižší. Vzniklé chyby je možné rozdělit na náhodné a záměrné. Vnitřní kontrolní systém podniku je využíván ke snížení výskytu obou uvedených typů chyb. Využití vnitřního kontrolního systému má snížit pravděpodobnost a dopad rizika a správně ho ošetřit. K zajištění snížení výskytu rizik je

nutné využít i dalších možností, jako například důsledné kontroly práce zajišťované přímo účetními. Dle (Dolejšová 2006) jde především o:

- důslednou kontrolu zadávaných dat,
- pravidelnou kontrolu zůstatků jednotlivých účtů,
- důkladnou kontrolu účetních výstupů,
- důkladnou kontrolu výpočtů,
- kontrolu správného a aktuálního nastavení parametrů účetního systému,
- a důkladné přezkoumání věcné a formální správnosti účetních dokladů.

Řízení rizik může účetním usnadnit ČSN 36 9790 - Systém managementu bezpečnosti informací nebo využití mezinárodního auditorského standardu ISA 315 - Identifikace a vyhodnocení rizik významné (materiální) nesprávnosti na základě znalosti účetní jednotky a jejího prostředí, který popisuje práci s riziky uvnitř účetní jednotky. Jsou zde uvedeny informace o postupech vyhodnocování rizik (KAČR 2014).

2.3.3 Proces řízení rizik

Řízení rizik představuje významnou součást strategického řízení každé společnosti, která je definována v různých publikacích. Zabývají se jím například Čermák (2007), Svozilová (2007), britská norma BS 7799-3:2006 a české národní technické normy (ČSN 36 9790 nebo ČSN ISO 31 000).

Proces řízení rizik zahrnuje dle (Čermák 2007) několik kroků:

- Analýza rizik
    - Identifikace aktiv.
    - Stanovení hodnoty aktiv.
    - Identifikace hrozeb a slabin.
    - Stanovení pravděpodobnosti, závažnosti hrozeb a míry zranitelnosti.
- Vyhodnocení rizik
- Zvládání rizik

ČSN 36 9790, která se zaměřuje na efektivní bezpečnost informací pomocí trvalého programu managementu rizik, popisuje proces posouzení rizika jako proces, který zahrnuje:

- Analýzu rizik
  - Identifikace aktiv.
  - Identifikace právních a byznysových požadavků, které jsou významné pro identifikaci aktiv.
  - Ocenění identifikovaných aktiv.
  - Identifikace významných hrozeb a zranitelností u identifikovaných aktiv.
  - Posouzení pravděpodobnosti, že se hrozby a zranitelnosti vyskytnou.
- Hodnocení rizik
  - Kalkulace rizika.
  - Hodnocení rizik podle předdefinované škály rizik.
  - Jedinečnou množinu hrozeb a zranitelností, které mohou vést, jestliže se objeví, k významným ztrátám.
  - Právní, zákonné a smluvní požadavky, které organizace uplatňuje, její obchodní partnery, dodavatele a poskytovatele služeb (ČSN 36 9790).

Detailnější popis jednotlivých kroků řízení rizik je uveden v následujících sub kapitolách.

Analýza rizik

Analýza rizik je tvořena identifikací aktiv, identifikací právních a byznysových požadavků, které jsou významné pro identifikaci aktiv, oceněním identifikovaných aktiv, identifikací významných hrozeb a zranitelností u identifikovaných aktiv a posouzením pravděpodobnosti, že se hrozby a zranitelnosti vyskytnou. Výsledkem analýzy rizik je identifikace a posouzení faktorů, které by mohly ohrozit podnikové procesy. Je založena na identifikaci rizikových faktorů (zdrojů rizika), určování pravděpodobnosti a důsledků působení rizikových faktorů. Mapuje i finanční náklady spojené s případným vznikem nežádoucí události. Tvoří základ managementu rizik

a prevence vzniku krizových situací v podniku (Svozilová 2007). Mezi základní pojmy analýzy rizik patří dle Čermák (2007) a ČSN 36 9790 (2008) pojmy: aktivum, riziko, hrozba a zranitelnost.

- Aktivum je dle ČSN 36 9790 něco, co má hodnotu nebo užitek pro organizaci, její procesy byznysu a jejich kontinuitu. Základní charakteristikou aktiva je hodnota.
- Riziko definuje (ČSN 36 9790, s. 7) jako: „kombinaci pravděpodobnosti výskytu identifikovaného stavu systému, služby nebo sítě, který indikuje možné porušení politiky bezpečnosti informací nebo selhání bezpečnostního opatření, nebo předem neznámé situace, která může být významná z hlediska bezpečnosti, a jejích následků."
- Hrozba je dle ISO/IEC 13335-1:2004 potenciální příčina incidentu, která může mít za následek poškození systému nebo organizace. Hrozbou může být například požár, přírodní katastrofa, krádež zařízení, získání přístupu k informacím neoprávněnou osobou, chyba obsluhy, ale i kontrola finančního úřadu nebo změna kursu české koruny vzhledem k evropské měně, apod. (Smejkal, Rais 2006).
- Zranitelnost je dle ISO/IEC 13335-1:2004 slabá stránka aktiva nebo skupiny aktiv, která může být využita jednou nebo více hrozbami.

Zásadním krokem, který musí společnost provést, pokud chce implementovat systém řízení rizik, je vytvoření registru rizik a stanovení pravděpodobnosti a významnosti rizik pro organizaci. V některých případech ale není možné hrozící rizika identifikovat, popsat a navrhnout postup snížení jejich dopadu na normální chod společnosti. Příčina může být již v počáteční obtížnosti nebo nemožnosti rizika předem identifikovat a v následné neschopnosti ovlivnit je. S tímto typem rizik se setkáváme v oblastech specifické lidské činnosti jako jsou například zdravotnictví nebo sociální služby (Renganathan, Babu, Sarbadhikari 2013).

Příklad analýzy informačních rizik v ekonomickém oddělení potravinářské společnosti

Studie se zaměřuje na analýzu informačních rizik v ekonomickém oddělení společnosti, která se zabývá výrobou potravinářských výrobků a nápojů. Společnost je rozdělena na pět oddělení (ekonomické oddělení (účetní oddělení), obchodní oddělení, výroba, expedice se skladem a laboratoř), která spolupracují na zajištění jednotlivých podnikových procesů. Skladovací prostory společnosti jsou malé, proto je navázána spolupráce s externí společností zajišťující skladování výrobků.

Ekonomické oddělení má čtyři zaměstnance:

- vedoucí ekonomického oddělení - hlavní účetní,
- dvě účetní
- a mzdová účetní.

Zaměstnanci jsou rozděleni do tří kanceláří. První kancelář využívají dvě účetní, druhou hlavní účetní a třetí mzdová účetní. Každá z nich využívá PC s operačním systémem Windows 7. Hlavní účetní využívá také notebook. Hlavní účetní vyřizuje běžnou agendu a koordinuje veškeré aktivity ostatních zaměstnankyň ekonomického oddělení. Zajišťuje řešení komplikací spojených s nejasnostmi v podkladech poskytnutých ekonomickému oddělení ostatními odděleními nebo externími subjekty.

Společnost zavedla v nedávné době nový ERP systém - QAD/MFG Pro, jehož některé moduly využívají všechny zaměstnankyně ekonomického oddělení. Všechny moduly nového systému jsou mezi sebou propojeny. Výpočetní technika je spravována zaměstnancem společnosti speciálně proškoleným pro tuto činnost.

Moduly zpřístupněné zaměstnankyním ekonomického oddělení:

- část pro obchodní oddělení (přehledy - ceny, prodej, reklamace)
- část pro expedici (dodací listy, fakturace)
- část pro ekonomické oddělení (různá přístupová práva - vedoucí ekonomického oddělení má zpřístupněn celý modul)

Veškeré objednávky (i reklamace) zákazníků vyřizuje ekonomické oddělení v součinnosti s obchodním oddělením a s expedicí. Expedice koordinuje činnosti smluvních dopravců a aktivity skladu. Ekonomické oddělení také sleduje platební

morálku zákazníků a povoluje rizikové objednávky (objednávky zákazníků, kteří neuhradili jednu nebo více splatných faktur).

Aktiva je dle ČSN 36 9790 možné dělit do následujících skupin:

- informace (např.: databáze a datové soubory, dokumentace, smlouvy, manuály, směrnice),
- procesy a služby (např.: specifické aplikační činnosti, programování, služby podporující zpracování informací),
- software,
- fyzické položky (počítačové a komunikační vybavení, média, technické vybavení),
- lidé (např.: zaměstnanci, zákazníci).

Tabulka 9: Identifikace a ocenění identifikovaných aktiv

Typ aktiva	Popis aktiva	Hodnota aktiva
Informace	Databáze ekonomického oddělení	4
	Databáze obchodního oddělení	4
	Databáze expedice	4
Procesy a služby	Připojení k serveru	4
SW	Operační systémy	3
	Databázové systémy	3
Fyzické položky (HW)	PC	2
	Notebooky	1

Zdroj: vlastní zpracování dle (ČSN 36 9790) a (Steiner 2007), 2016

Kategorie pro oceňování aktiv - hodnota aktiv pro organizaci:

- 0 - zanedbatelná
- 1 - nízká
- 2 - střední
- 3 - vysoká
- 4 - velmi vysoká

Pro ohodnocení aktiv jsou použity kategorie 0 až 4, přičemž nejdůležitější aktiva jsou označena číslem 4.

Tabulka 10: Identifikace významných hrozeb a zranitelností u identifikovaných aktiv a posouzení pravděpodobnosti, že se hrozby a zranitelnosti vyskytnou

Identifikovaná hrozba	**Pravděpodobnost výskytu hrozby**	**Související zranitelnost**	**Pravděpodobnost výskytu zranitelnosti**
Selhání hardware	Nízká	Mechanické poškození IT.	Střední
Selhání software	Střední	Nejasná specifikace nastavení IS.	Střední
Zcizení aktiv	Nízká	Nedostatečné zabezpečení IT.	Malá
Přírodní katastrofa	Nízká	Požár, povodeň v prostorách s instalovanými IT.	Malá
Nedostatečná aktualizace	Vysoká	Nedostatečná aktualizace software.	Velká
Neúmyslná modifikace	Střední	Neúmyslná úprava informací vedoucí k jejich špatnému použití.	Velká
Nevhodně nastavená komunikace	Vysoká	Nevhodné nastavení komunikačních kanálů vedoucí k nechtěné modifikaci nebo ztrátě informací.	Velká

Zdroj: vlastní zpracování dle (ČSN 36 9790) a (Steiner 2007), 2016

Kategorie oceňování pro hrozby:

- Nízká pravděpodobnost
- Střední pravděpodobnost
- Vysoká pravděpodobnost

Kategorie oceňování pro zranitelnosti:

- Malá pravděpodobnost
- Střední pravděpodobnost
- Velká pravděpodobnost

Hodnocení rizik

Hodnocení rizik představuje zejména kalkulaci rizika a hodnocení rizik podle předdefinované škály rizik. Organizace se soustředí především na kvalitativní vyhodnocení rizik. Výstupem je „seznam rizik“, který předkládá množinu hrozeb a zranitelností, jejichž výskyt by mohl vést ke ztrátám. Vyhodnocení rizik bývá provedeno pomocí matice rizik.

V případě rizika se vždy berou v úvahu dva pojmy, které jsou s ním spojeny, nejistý výsledek a předpoklad, že alespoň jeden z možných výsledků je nežádoucí. Jak jsou hodnota dopadu a hodnota pravděpodobnosti kombinovány při výpočtu rizika záleží dle ČSN 36 9790 na volbě organizace a na vybrané metodě posuzování rizika. Vždy musí být zajištěno zvýšení úrovně rizika v případě zvýšení kteréhokoli ze dvou uvedených faktorů.

Příklad hodnocení rizik v ekonomickém oddělení potravinářské společnosti

Jedním z přístupů při vyhodnocování rizik je dle ČSN 36 9790 sestavení matice s hodnotami rizik, kde první sloupec odpovídá ohodnocení aktiv a ostatní sloupce jsou kombinací hodnoty hrozby a zranitelnosti.

Tabulka 11: Matice s hodnotami rizik

Hodnota aktiva	**Úroveň hrozby**								
	Nízká			**Střední**			**Vysoká**		
	Úroveň zranitelnosti								
	malá	**střední**	**velká**	**malá**	**střední**	**velká**	**malá**	**střední**	**velká**
0	0	1	2	1	2	3	2	3	4
1	1	2	3	2	3	4	3	4	5
2	2	3	4	3	4	5	4	5	6
3	3	4	5	4	5	6	5	6	7
4	4	5	6	5	6	7	6	7	8

Zdroj: vlastní zpracování dle (ČSN 36 9790), 2016

Tabulka 12: Rizika stanovená pro organizací identifikovaná aktiva

Aktivum	Hodnota aktiva	Hrozba	Pravděpodobnost výskytu hrozby	Zranitelnost	Pravděpodobnost výskytu zranitelnosti	Riziko
Databáze ekonomického oddělení	4	Nedostatečná aktualizace	Vysoká	Nedostatečná aktualizace software.	Velká	8
		Neúmyslná modifikace	Střední	Neúmyslná úprava informací vedoucí k jejich špatnému použití.	Velká	7
Databáze obchodního oddělení	4	Nedostatečná aktualizace	Vysoká	Nedostatečná aktualizace software.	Velká	8
		Neúmyslná modifikace	Střední	Neúmyslná úprava informací vedoucí k jejich špatnému použití.	Velká	7
Databáze expedice	4	Nedostatečná aktualizace	Vysoká	Nedostatečná aktualizace software.	Velká	8
		Neúmyslná modifikace	Střední	Neúmyslná úprava informací vedoucí k jejich špatnému použití.	Velká	7
Připojení k serveru	4	Selhání hardware	Nízká	Mechanické poškození IT.	Střední	5
		Nastavení komunikace	Vysoká	Nevhodné nastavení komunikačních kanálů vedoucí k nechtěné modifikaci nebo ztrátě informací.	Velká	8
Operační systémy	3	Selhání software	Střední	Nejasná specifikace nastavení IS.	Střední	5
		Nedostatečná aktualizace	Vysoká	Nedostatečná aktualizace software.	Velká	7
Databázové systémy	3	Selhání software	Střední	Nejasná specifikace nastavení IS.	Střední	5
		Nedostatečná aktualizace	Vysoká	Nedostatečná aktualizace software.	Velká	7
PC	2	Selhání hardware	Nízká	Mechanické poškození IT.	Střední	3
		Zcizení aktiv	Nízká	Nedostatečné zabezpečení IT.	Malá	2
		Přírodní katastrofa	Nízká	Požár, povodeň v prostorách s instalovanými IT.	Malá	2
		Nastavení komunikace	Vysoká	Nevhodné nastavení komunikačních kanálů vedoucí k nechtěné modifikaci nebo ztrátě informací.	Velká	6

Aktivum	Hodnota aktiva	Hrozba	Pravděpodobnost výskytu hrozby	Zranitelnost	Pravděpodobnost výskytu zranitelnosti	Riziko
Notebooky	1	Selhání hardware	Nízká	Mechanické poškození IT.	Střední	2
		Zcizení aktiv	Nízká	Nedostatečné zabezpečení IT.	Malá	1
		Přírodní katastrofa	Nízká	Požár, povodeň v prostorách s instalovanými IT.	Malá	1
		Nastavení komunikace	Vysoká	Nevhodné nastavení komunikačních kanálů vedoucí k nechtěné modifikaci nebo ztrátě informací.	Velká	5

Zdroj: vlastní zpracování dle (ČSN 36 9790) a (Steiner 2007), 2016

V tabulce jsou uvedeny pouze takové kombinace aktiv, hrozeb a zranitelností, které se v dané organizaci mohou vyskytnout. Hodnota rizika pro identifikovaná aktiva je získána přenesením hodnoty rizika uvedené pro konkrétní kombinaci hodnoty aktiva, pravděpodobnosti výskytu hrozby a pravděpodobnosti výskytu zranitelnosti v tabulce číslo 11 (Matice s hodnotami rizik) do tabulky číslo 12 (Rizika stanovená pro organizací identifikovaná aktiva).

V uvedené tabulce je důležitost rizik pro vybranou organizaci rozlišena barevně. Jednotlivé kategorie úrovní rizika dle ČSN 36 9790 jsou:

- Přijatelné riziko 0 - 2 zelená
- Střední úroveň rizika 3 - 5 oranžová
- Vysoká úroveň rizika 6 - 8 červená

Zvládání rizik

Zvládání rizik je nutné stavět na výsledcích provedené analýzy. Je potřeba neustále přehodnocovat úroveň zbytkového rizika (riziko tak malé, že je pro subjekt přijatelné a protiopatření proti němu se nevyžaduje) a akceptovatelného rizika s ohledem na změny:

- organizace,

- technologie,
- cílů činnosti organizace a procesů,
- účinnosti implementace jednotlivých změn,
- vnější události.

Mimo akceptovatelného rizika je v rámci procesu řízení rizik možné identifikovat i riziko neakceptovatelné, které představuje zásadní překážku pro přijetí jakéhokoli projektu.

Vždy je vhodné sestavit zprávu o riziku. Doporučují se dvě varianty, jedna pro management a druhá pro pracovníky, kterým bude svěřena implementace opatření. Úroveň rizika bývá vyjádřena ve stupních (nízká, střední, vysoká).

Zvládání rizik v ekonomickém oddělení potravinářské společnosti - příklad

V následující tabulce jsou shrnuty kombinace aktiv, hrozeb a zranitelností, které se mohou v organizaci vyskytnout. Jsou k nim přiřazeny hodnoty rizika a návrhy opatření, která by vzniku rizika zamezila, nebo alespoň snížila jeho dopady do procesů sledované organizace.

Tabulka 13: Rizika stanovená pro organizací identifikovaná aktiva a opatření vedoucí k jejich zvládnutí

Aktivum	Hrozba	Zranitelnost	Riziko	Opatření
Databáze ekonomického oddělení	Nedostatečná aktualizace	Nedostatečná aktualizace software.	8	Pravidelná aktualizace.
	Neúmyslná modifikace	Neúmyslná úprava informací vedoucí k jejich špatnému použití.	7	Zálohování.
Databáze obchodního oddělení	Nedostatečná aktualizace	Nedostatečná aktualizace software.	8	Pravidelná aktualizace.
	Neúmyslná modifikace	Neúmyslná úprava informací vedoucí k jejich špatnému použití.	7	Zálohování.

Aktivum	Hrozba	Zranitelnost	Riziko	Opatření
Databáze expedice	Nedostatečná aktualizace	Nedostatečná aktualizace software.	8	Pravidelná aktualizace.
	Neúmyslná modifikace	Neúmyslná úprava informací vedoucí k jejich špatnému použití.	7	Zálohování.
Připojení k serveru	Selhání hardware	Mechanické poškození IT.	5	Včasné zajištění servisu.
	Nastavení komunikace	Nevhodné nastavení komunikačních kanálů vedoucí k nechtěné modifikaci nebo ztrátě informací.	8	Nastavení pravidel interní komunikace.
Operační systémy	Selhání software	Nejasná specifikace nastavení IS.	5	Pravidelná kontrola a servis.
	Nedostatečná aktualizace	Nedostatečná aktualizace software.	7	Pravidelná aktualizace.
Databázové systémy	Selhání software	Nejasná specifikace nastavení IS.	5	Pravidelná kontrola a servis.
	Nedostatečná aktualizace	Nedostatečná aktualizace software.	7	Pravidelná aktualizace.
PC	Selhání hardware	Mechanické poškození IT.	3	Včasné zajištění servisu.
	Zcizení aktiv	Nedostatečné zabezpečení IT.	2	Bezpečnostní opatření.
	Přírodní katastrofa	Požár, povodeň v prostorách s instalovanými IT.	2	Bezpečnostní opatření.
	Nastavení komunikace	Nevhodné nastavení komunikačních kanálů vedoucí k nechtěné modifikaci nebo ztrátě informací.	6	Nastavení pravidel interní komunikace.
Notebooky	Selhání hardware	Mechanické poškození IT.	2	Včasné zajištění servisu.
	Zcizení aktiv	Nedostatečné zabezpečení IT.	1	Bezpečnostní opatření.
	Přírodní katastrofa	Požár, povodeň v prostorách s instalovanými IT.	1	Bezpečnostní opatření.
	Nastavení komunikace	Nevhodné nastavení komunikačních kanálů vedoucí k nechtěné modifikaci nebo ztrátě informací.	5	Nastavení pravidel interní komunikace.

Zdroj: vlastní zpracování dle (ČSN 36 9790) a (Steiner 2007), 2016

2.3.4 Informační management

Příklad uvedený v předchozí kapitole dokládá důležitost informací pro společnosti a zdůrazňuje nutnost ochrany těchto aktiv. V souvislosti s novým nazíráním na informace a s přerodem průmyslové společnosti ve společnost informační (Wiegers 2008) se vyčlenil další obor, který se problematikou informací zabývá - informační management.

Jak bylo popsáno v úvodu disertační práce, informační management je dle (Burk, Horton 1991, s. 171) definován jako „aplikace tradičních manažerských procesů, zejména zásad managementu pro hospodaření se zdroji, k správě informačních zdrojů a dalších aktiv organizace."

Informační management vznikl v důsledku potřeby zabývat se detailněji problematikou řízení informací a rizik s jejich řízením souvisejících. Zabývá se navrhováním, implementací a provozem systémů a služeb, které zahrnují procesy získávání, zpracování, ukládání, prezentace a distribuce informací (Doucek 2010).

Teoretické zázemí informačního managementu tvoří informatika, informační věda, systémová analýza, systémové inženýrství a manažerské disciplíny. Technologický základ představují informační a komunikační technologie (Vodáček, Rosický 1997). Literatura (Burk, Horton 1991), (Franks 2013) a (Chessel, Smith 2013) uvádí mnohé definice informačního managementu. Jde o spojení dvou definovaných a běžně užívaných pojmů, informace a management, přesto zde přetrvává nejednoznačnost ve výkladu.

Mezi tři zásadní příčiny nejednoznačnosti výkladu patří dle (Vodáček, Rosický 1997):

- nejednoznačné chápání pojmu management,
- nejednoznačné chápání pojmu informace,
- změna chápání pojmu informační management v průběhu období od jeho vzniku.

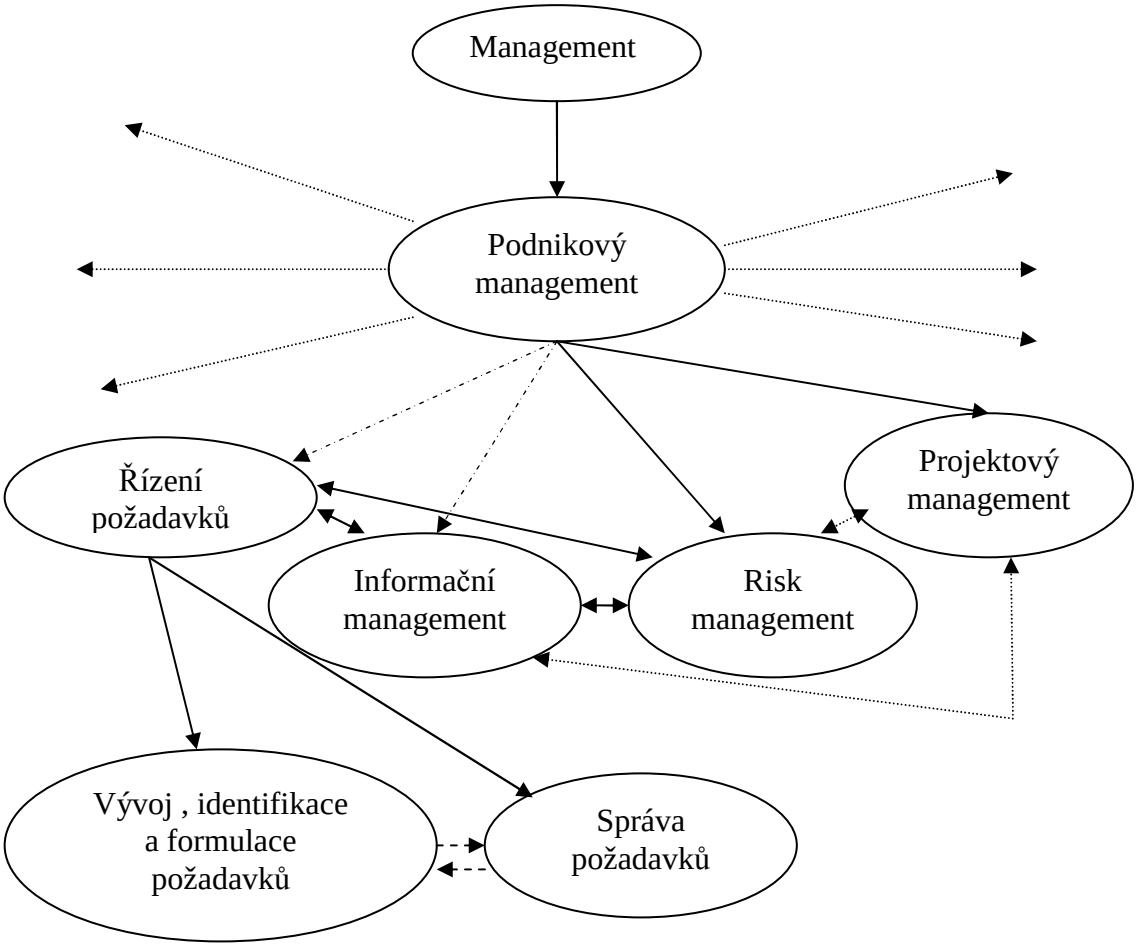
Informačnímu managementu se věnují jak čeští (Vodáček, Rosický 1997), (Švarcová, Rain 2012), tak zahraniční (AIIM 2014), (Knox 2013), (Robertson 2005) a (USC 2003) autoři. Jednotlivé tituly se zabývají buď přímo informačním managementem, nebo se tomuto tématu věnují okrajově v rámci zpracování jiného tématu, jakým je

například znalostní management, vývoj informačních systémů nebo vývoj informačních a komunikačních technologií.

Na základě studia výše popsaných zdrojů je možné usuzovat, že informační management byl zpočátku zaměřen převážně na technický aspekt řešení. Později se již objevuje „transdisciplinární“ pojetí informačního managementu, propojení informatiky a manažerských pohledů na danou problematiku. Důraz byl nejdřív kladen zejména na hospodárné zajišťování informačních procesů, posléze se důraz přesouvá na efektivitu dosahování cílů organizace za pomoci výpočetní techniky a informačních a komunikačních technologií. V současnosti je informační management chápán jako přístup, který prostupuje celý podnikatelský proces a celou organizaci. V rámci dnešního trans disciplinárního pojetí respektuje informační management stanovení a dosahování cílů řízené organizace a návaznost zajištění informačních procesů. Vytváří manažerské znalostní zázemí a pomáhá zajišťovat strategické i taktické cíle organizace.

Aplikace IS/IT nejsou již pro manažery jen cílem, ale prostředkem, který jim prostřednictvím zabezpečení jejich individuálních informačních potřeb pomáhá zajišťovat kvalitněji manažerské činnosti. Jde tedy o propojení moderního managementu, informatiky, systémových přístupů a pohledů dalších vědních oborů (ekonomie, psychologie, atp.). Místo informačního managementu mezi několika vybranými vědními disciplínami znázorňuje následující obrázek.

Obrázek 7: Místo informačního managementu mezi několika vybranými vědními disciplínami



Zdroj: vlastní zpracování dle (Wiegers 2008), 2016

Mezi další obory spojené s informačním managementem patří dle University of South Carolina (USC 2003) především takzvaná "velká M", což jsou vědní obory, které využívají údaje poskytované informačním managementem. USC označuje tyto disciplíny jako aplikace informačního managementu.

Tabulka 14: "Velká M"

Zkratka	Anglický název	Český název
KM	Knowledge Management	Management znalostí
CM	Content Management	Správa obsahu
PM	Project Management	Projektový management
HRM	Human Resources Management	Řízení lidských zdrojů
ERM	Enterprise Resource Management	Řízení podnikových zdrojů
FM	Financial Management	Finanční management

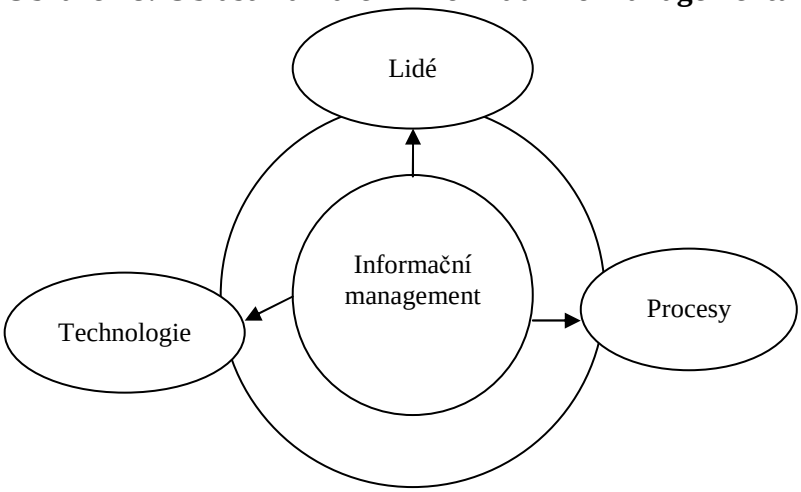
Zdroj: vlastní zpracování dle (USC 2003), 2016

Informační management má široké uplatnění (průmyslová odvětví, školství, zdravotnictví, …). Každá společnost, která nevyužije možností informačního managementu a možností, které jí nabízí technologické zdroje, si dle Hickse (2007) v dnešním konkurenčním prostředí pravděpodobně nedokáže dlouhodobě udržet svou pozici. Přesto se dle zjištěných informací mnohé společnosti informačním managementem nezabývají a výrazné změny v této oblasti nepředpokládají ani v budoucnu.

2.3.5 Přístup k informačnímu managementu v ČR a ve světě

Informační management je zaměřen na tři základní oblasti: procesy, technologie a lidé.

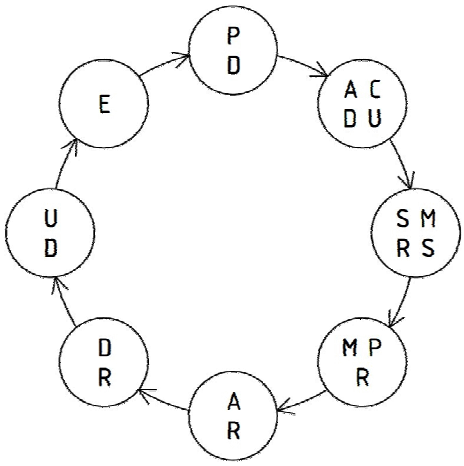
Obrázek 8: Oblasti zaměření informačního managementu



Zdroj: vlastní zpracování dle (InfoReady 2014), 2016

Cílem informačního managementu je automatizace správy a ochrany informací pro účely zachování a využití jejich obchodní hodnoty v rámci podnikatelských aktivit. Jedná se o využívání informačních zdrojů a informačních schopností organizace za účelem tvorby přidané hodnoty pro podnik i pro jeho zákazníky (Dehnashi 2010). U informačního managementu se stejně jako v případě produktu, projektu, nebo informačního systému hovoří o životním cyklu. Životní cyklus informačního managementu je popisován různými způsoby. Na základě informací uvedených v (AIIM 2014) a (Public Works and Government Services Canada 2014) bylo pro tuto disertační práci vytvořeno následující znázornění životního cyklu informačního managementu.

Obrázek 9: Životní cyklus informačního managementu



kde:

PD	=	Plan and Design	=	Plánování a navrhování. (úvodní studie systému)
ACDU	=	Acquire, Create, Derive, Update	=	Získávání, vytváření, odvozování, aktualizace. (příjem informací)
SMRS	=	Store, Manage, Replicate, Share	=	Ukládání, správa, kopírování, sdílení. (utřídění informací)
MPR	=	Maintain, Protect, Recover	=	Udržování, ochrana, obnova. (zachování informací)
AR	=	Archive, Recall	=	Archivace, stažení. (zachování informací)
DR	=	Delete, Remove	=	Odstranění, přemístění.
UD	=	Use, Disseminate	=	Užití, šíření.
E	=	Evaluate	=	Vyhodnocování.

Zdroj: vlastní zpracování dle (AIIM 2014) a (Public Works and Government Services Canada 2014), 2016

Informační management vychází z principů, které využívají i ostatní vědní disciplíny, jejichž zájem se soustředí na oblasti spojené s využitím informací. Souhrn těch nejvýznamnějších principů práce s informacemi, ze kterých vychází informační management, je uveden v následující tabulce.

Tabulka 15: Souhrn nejvýznamnějších principů práce s informacemi, ze kterých vychází informační management

INFORMAČNÍ MANAGEMENT	
Princip	**Vlastnosti informací a pravidla nutná pro naplnění uvedených principů**
Bezpečnost	Utajení
	Integrita
	Dostupnost
Efektivnost (Účinnost)	Vede ke zjištění stavu finančního zdraví podniku
	Vhodné načasování
	Neduplicita
	Práce založená na požadavcích
Kvalita	Platnost
	Konzistentnost
	Komplexnost
Sdílení	Jasnost
	Srozumitelnost
	Přístupnost
	Inter-operabilita
Shoda	Vedení záznamů
	Kontrolovaný přístup k informacím
	Ochrana osobních údajů

Zdroj: vlastní zpracování dle (Government of Western Australia 2012), (McMahon, Lowe, Culley 2004) a (Wilson 1997), 2016

Na základě informací získaných ze zahraniční i české literatury, například (Morabito 2013), (Šidlichovská 2011), je možné definovat následující tři přístupy k informačnímu managementu:

- Přístup zaměřený zejména na informační a komunikační technologie.

(The ICT-Centered Approach)

- Přístup zaměřený zejména na informace.

(The Information-Centered Approach)

- Přístup zaměřený zejména na lidský faktor.

(The People-Centered Approach)

Přístup zaměřený zejména na informační a komunikační technologie. (The ICT-Centered Approach)

Manažeři přijímají tvrzení, že zaměření aktivit informačního managementu pouze do oblasti vylepšování a ochrany ICT vede ke zlepšení výkonnosti podniku. Klíčovými oblastmi, ve kterých se předpokládané zlepšení projeví jsou:

- efektivnost obchodních operací (finance, výroba a distribuce),
- podpora komunikace, která zajistí bezproblémové fungování podnikových procesů,
- podpora manažerského rozhodování, poskytnutí vhodných informací pro prognózy vývoje tržní situace, řízení podnikatelských rizik, sdílení znalostí,
- podpora inovací produktů a podpora rozvoje služeb.

Přístup zaměřený zejména na informace. (The Information-Centered Approach)

Základem tohoto přístupu je přesvědčení, že způsob práce s daty uvnitř společnosti je rozhodující pro přeměnu dat v informace, které pomáhají vylepšit fungování podnikových procesů. Informace pomáhají vylepšit zejména tyto oblasti: vztahy se zákazníkem, produktové a procesní inovace, obchod, marketing a finanční kontrolu. Z tohoto pohledu není pro společnost zabezpečení a funkčnost ICT jedinou nezbytností vedoucí k vylepšení podnikových procesů. Pozornost je nutné věnovat i způsobům sběru, shromažďování, organizaci, zpracování a údržbě informací - způsobům převádění dat v informace.

Přístup zaměřený zejména na lidský faktor. (The People-Centered Approach)

Základní myšlenkou tohoto přístupu je víra, že nenaplnění některých cílů spjatých s ICT a sdílením informací a znalostí souvisí s chováním zaměstnanců a kulturními hodnotami

společnosti. Manažeři by se měli soustředit na kulturní hodnoty a chování spojené s využíváním informací a ICT ve společnosti. V případě informačního managementu se společnosti snaží zvýšit efektivitu práce s informacemi pomocí mechanismů, jako jsou například:

- data mining (Získávání znalostí z databází. Je založeno na metodách AI, strojového učení, statistiky a databázových systémů. Jeho cílem je získat informace z datového souboru a transformovat je do podoby vhodné pro další použití.),
- signaling (Chování, kdy jedna strana o sobě věrohodně předává informace druhé straně. Například zákazník předává prodejci informaci o své ziskovosti, vhodnosti pro uskutečnění nákupu.),
- screening (Chování, kdy jedna strana o sobě věrohodně předává informace druhé straně. V tomto případě provádí výběr prodejce a rozhoduje o vhodnosti zákazníka pro uzavření obchodu.).

V postoji k popsaným přístupům k informačnímu managementu je v současné době patrná změna. Zájem společností se posouvá od zaměření se na ICT směrem k informacím a lidskému kapitálu. Manažeři si již uvědomují nutnost zahrnout do informačního managementu i tzv. měkké faktory. V České republice se tento trend také objevuje, ale přístup zaměřený na ICT v MSP stále převládá.

2.3.6 Důvody aplikace informačního managementu

Společnosti potřebují mít v současném konkurenčním prostředí přehled o veškerých podnikových aktivitách, jejich financování a možnostech budoucího investování. Informační management představuje dle Vodáčka a Rosického (1997) praktickou odbornou činnost provozovanou v kontextu konkrétní organizace zaměřenou na využití informací v rozhodovacích a řídících procesech a na integrování informačních zdrojů a aktivit do podnikových procesů. Může společnostem pomoci vylepšit rozhodovací procesy a efektivně nastavit ostatní podnikové procesy (Edmunds, Morris 2000). Podává manažerům přehledný popis situace, ve které se podnik nachází.

Situace signalizující potřebu aplikace informačního managementu

Společnosti chtějí využívat informace efektivněji. Systém správy informací je však mnohdy nastaven nevhodně. Jednotlivé složky IS mohou být zacíleny pouze na plnění aktivit oddělení, pro která byly vytvořeny, a data jsou izolována. Není tedy jednoduché zprostředkovat informace manažerům nebo zaměstnancům jiných oddělení. Manažerům se tak informace:

- dostanou včas v potřebné kvalitě a kvantitě,
- dostanou v potřebné kvalitě a kvantitě se zpožděním,
- dostanou i redundantní informace,
- nedostanou vůbec.

Hlavní kritická místa:

- Součásti IS (moduly) nabízí rozdílná řešení stejného problému, která vedou k odlišným výsledkům.
- Nedostatečná transparentnost informací.
- Obtížná sumarizace informací z více zdrojů.
- Nedostatečnost poskytovaných informací (kvalita, rozsah).
- Špatná dosažitelnost informací (časové prodlevy).

Přínos aplikace informačního managementu v rámci podnikových procesů

Efektivní informační management vyžaduje zainteresování všech zaměstnanců podniku, kteří se jeho pomocí snaží implementovat podnikovou strategii. Zaměřuje se na důležité oblasti, které mohou podniku pomoci přinést okamžité výhody a podněty pro budoucí plánování.

Řešení, které nabízí informační management:

- Zlepšení spolupráce jednotlivých oddělení podniku.
- Zavedení vhodného IS.
- Nastavení striktních pravidel pro zadávání dat do systému.

- Systém pravidelných reportů.
- Snadná tvorba a dostupnost reportů i v tištěné podobě.
- Vhodné nastavení možností přístupu k jednotlivým složkám (modulům) IS.
- Proškolení odpovědných pracovníků.

2.3.7 Shrnutí

Rizika, kterým jednotlivé společnosti čelí, jsou odlišná. Základem je rozpoznat charakter rizika, popsat jej a redukovat v návaznosti na stanovené podnikové cíle v rámci podnikového procesu řízení rizik. Informační rizika a jejich řízení jsou předmětem české národní technické normy 36 9790. Uvedená norma stanovuje obecné podmínky pro provádění jednotlivých kroků analýzy rizik (identifikace aktiv; identifikace právních a byznysových požadavků, které jsou významné pro identifikaci aktiv; ocenění identifikovaných aktiv; identifikace významných hrozeb a zranitelností u identifikovaných aktiv a posouzení pravděpodobnosti, že se hrozby a zranitelnosti vyskytnou) a hodnocení rizik (kalkulace rizika; hodnocení rizik podle předdefinované škály rizik; jedinečná množina hrozeb a zranitelností, které mohou vést, jestliže se objeví, k významným ztrátám; právní, zákonné a smluvní požadavky, které organizace uplatňuje, její obchodní partnery, dodavatele a poskytovatele služeb).

Kvalitně provedený proces řízení rizik zajistí dle (Doucek 2010) a (Čermák 2007) organizaci:

- Snížení výskytu nepříjemných překvapení.
- Využití příležitosti.
- Zlepšení plánování, výkonu a efektivnosti.
- Zlepšení vztahů se stakeholdery (zúčastněnými subjekty).
- Kvalitní informace pro rozhodovací proces.

Hlavní nedostatky, objevující se v rámci procesu řízení rizik, jsou dle (Čermák 2007) a (Bejček, Čejp, Vystavěl a Katolický 2007):

- Binární chápání nejistoty manažery – předpoklad pouze úplné jistoty nebo nemožnosti.

- Podléhání nezdravému optimismu.
- Vyhýbání se rizikovým rozhodnutím.
- Nevyužívání metod a nástrojů pro podporu strategického rozhodování.
- Absence systému včasného upozornění na hrozící problém.

Dobře zvládnutá problematika řízení rizik je předpokladem správného fungování firmy. Management společnosti musí pracovat s předpokladem, že může dojít k negativním událostem v bezpečnosti informací, které ovlivní podnikové procesy a činit opatření, která budou sloužit jako prostředek pro optimální zvládnutí následků bezpečnostních incidentů.

V souvislosti s novým nazíráním na informace se vyčlenil další obor, který se problematikou informací zabývá - informační management. Informační management vznikl v důsledku potřeby zabývat se detailněji problematikou řízení informací a rizik s jejich řízením souvisejících. Dle Doucka (2010) je možné popsat informační management jako sběr a řízení informací z jednoho či více zdrojů a jejich distribuci jednomu nebo více příjemcům, přičemž management je zde vnímán jako organizace a kontrola, zpracování a doručení informací. Teoretické zázemí informačního managementu tvoří informatika, informační věda, systémová analýza, systémové inženýrství a manažerské disciplíny. Technologický základ představují informační a komunikační technologie.

Informační management byl zpočátku zaměřen převážně na technické řešení úloh. Později se již objevuje „transdisciplinární“ pojetí informačního managementu, propojení informatiky a manažerských pohledů na danou problematiku. V současnosti je informační management chápán jako přístup, který prostupuje celý podnikatelský proces a celou organizaci. V rámci dnešního trans disciplinárního pojetí respektuje informační management stanovení a dosahování cílů řízené organizace a návaznost zajištění informačních procesů. Vytváří manažerské znalostní zázemí a pomáhá zajišťovat strategické i taktické cíle organizace.

Informační management se snaží pracovat s pojmy jako jsou riziko nebo informace, objasnit je a vysvětlit zejména manažerům (vedoucím pracovníkům) podniků, jak s touto problematikou nakládat. Úhel pohledu na oblast řízení rizik se však u informačního managementu a ostatních vědních disciplín, jakými jsou například

podnikový management, projektový management nebo risk management liší (Savolainen 2007) v závislosti na tom, co je hlavním předmětem jejich zkoumání. V rámci předkládané disertační práce je informační management chápán ve smyslu následující specifikace: “Informační management představuje veškeré aktivity spojené s řízením informací v rámci všech standardních i nestandardních procesů, probíhajících v rámci činností zajišťovaných podnikatelskými subjekty nebo subjekty pohybujícími se ve veřejné sféře, za účelem vytváření přidané hodnoty pro danou organizaci, pro společnosti, které s touto organizací spolupracují i pro její zákazníky. Je postaven na třech pilířích, kterými jsou lidé, technologie a procesy.“

Bez informací by pro podniky nebylo možné zajišťovat veškeré podnikové aktivity. Zejména terciární sféra závisí právě na informacích a jejich efektivním řízení. V literatuře (USC 2003), (Weick 2009) je možné najít několik tvrzení, kterými se dá shrnout současný náhled na informace a informační management takto:

- Zpracování informací se stalo jednou z nejdůležitějších podnikových aktivit.
- ICT jsou ve světě obchodu všudypřítomné.
- Informační management se stal nezbytnou součástí podnikání.
- Schopnost pracovat s informacemi (IT skills) je pro současné zaměstnance nezbytností.
- Funkčnost současných aplikací informačního managementu vychází z pokroku ve vývoji informačních technologií a zpracování informací.

3. Výzkum v oblasti informačního managementu a aplikace jeho principů v rámci podnikových procesů

3.1 Expertní rozhovory

V této části disertační práce jsou shrnuty informace získané prostřednictvím expertních rozhovorů. Hlavním cílem bylo zjistit, do jaké míry dochází u jednotlivých vybraných podnikatelských subjektů k začlenění řízení informačních rizik mezi ostatní podnikové procesy. Ověřovanou hypotézou byla, mimo jiné, nízká úroveň zahrnutí řízení informačních rizik do podnikových aktivit vybraných podnikatelských subjektů.

Pro účast na expertních rozhovorech byli kontaktováni odborníci z oblasti účetnictví a informačních technologií, kteří pracují v MSP. MSP jsou dle (European Commission 2003) vymezeny takto:

Za středního podnikatele (MSP) se považuje podnikatel, pokud:

a) zaměstnává méně než 250 zaměstnanců, a

b) jeho aktiva/majetek nepřesahují korunový ekvivalent částky 43 mil. EUR nebo má obrat/příjmy nepřesahující korunový ekvivalent částky 50 mil. EUR,

c) minimálně 75 % základního kapitálu a hlasovacích práv je ve vlastnictví podniku.

Za malého podnikatele se považuje podnikatel, pokud:

a) zaměstnává méně než 50 zaměstnanců, a

b) jeho aktiva/majetek, nebo obrat/příjmy nepřesahují korunový ekvivalent 10 mil. EUR,

c) minimálně 75 % základního kapitálu a hlasovacích práv je ve vlastnictví podniku.

Za drobného podnikatele se považuje podnikatel, pokud:

a) zaměstnává méně než 10 zaměstnanců, a

b) jeho aktiva/majetek, nebo obrat/příjmy nepřesahují korunový ekvivalent 2 mil EUR,

c) minimálně 75 % základního kapitálu a hlasovacích práv je ve vlastnictví podniku.

O účast na expertních rozhovorech byli požádáni pracovníci z podnikatelských subjektů v západních Čechách. Dotazováno bylo 40 zástupců MSP. Mnohé společnosti však vyhodnotily pokládané otázky jako příliš detailní, a proto se z obavy o zneužití citlivých interních informací rozhodly informace neposkytnout.

Informace poskytlo prostřednictvím svých zástupců 15 podnikatelských subjektů. Účastníkům rozhovorů byly kladeny otázky, které se týkají informačního managementu a řízení rizik v rámci IS, který je společnostmi používán. Respondenti byli požádáni o provedení zběžné analýzy situace v oblasti informačních rizik v podniku, kde pracují. Ne všechny oslovené společnosti stručnou analýzu poskytly. Podařilo se však zajistit informace o používaném IS a jeho možných úskalích. Získané informace jsou shrnuty v následující části práce.

3.1.1 Rámec expertních rozhovorů

V rámci expertních rozhovorů byli osloveni zástupci podnikatelských subjektů, jejichž organizační struktura odpovídá požadavkům, které jsou na ně výzkumem kladeny (existence účetního/ekonomického oddělení, předpoklad užívání podnikového informačního systému). Všechny oslovené subjekty zaměstnávají pracovníky, kteří se starají o vedení účetnictví, existují zde účetní/ekonomická oddělení.

V rámci výzkumu byla analyzována rizika, která se v podnicích vyskytují v souvislosti s používáním informačních systémů. Byly zkoumány zejména možné dopady sledovaných rizik na procesy probíhající ve vybraných podnikatelských subjektech včetně uvedení zjištěných možností snížení jejich vlivu na další průběh podnikových činností. Míra zahrnutí řízení informačních rizik do podnikových procesů sledovaných subjektů se liší. Většina respondentů uvedla, že ve společnosti není informační management zaveden. Při detailnějším studiu situace však bylo zjištěno, že společnosti informační rizika v zásadě řídí a mají upraven způsob řízení rizik obecně. Rizika jsou však řízena spíše intuitivně, bez hlubší znalosti teorie informačního managementu a terminologie s ním spojené.

V případě, že byl respondent ochoten poskytnout informace nutné pro sestavení registru rizik, byla na základě získaných dat sestavena tabulka. Hodnocení rizika bylo

provedeno podle metodiky uvedené v ČSN 36 9790 (ohodnocení aktiv, hrozeb, zranitelností a matice s hodnotami rizik) a v odborné práci, která se touto tématikou zabývá (Steiner 2007).

Pro ohodnocení aktiv byly použity následující kategorie:

- 0 - zanedbatelná hodnota
- 1 - nízká hodnota
- 2 - střední hodnota
- 3 - vysoká hodnota
- 4 - velmi vysoká hodnota

Kategorie oceňování hrozeb byly:

- Nízká pravděpodobnost
- Střední pravděpodobnost
- Vysoká pravděpodobnost

Kategorie oceňování zranitelností byly:

- Malá pravděpodobnost
- Střední pravděpodobnost
- Velká pravděpodobnost

Tabulka 16: Hodnocení rizik - matice uvedená v ČSN 36 9790

Hodnota aktiva	**Úroveň hrozby**								
	Nízká			**Střední**			**Vysoká**		
	Úroveň zranitelnosti								
	malá	**střední**	**velká**	**malá**	**střední**	**velká**	**malá**	**střední**	**velká**
0	0	1	2	1	2	3	2	3	4
1	1	2	3	2	3	4	3	4	5
2	2	3	4	3	4	5	4	5	6
3	3	4	5	4	5	6	5	6	7
4	4	5	6	5	6	7	6	7	8

Zdroj: vlastní zpracování dle (ČSN 36 9790), 2016

K jednomu aktivu může existovat více rizik. Stejné riziko se může vyskytovat u různých aktiv. Pojmem „aktivum“ není myšleno pouze aktivum v tom smyslu, v jakém jej používá finanční účetnictví. Aktivem je myšlen i jakýkoli proces, který v účetním oddělení probíhá.

Kategorie úrovní rizika byly nastaveny dle ČSN 36 9790 a odlišeny takto:

Přijatelné riziko (Nízké) 0 - 2 P

Střední úroveň rizika 3 - 5 S

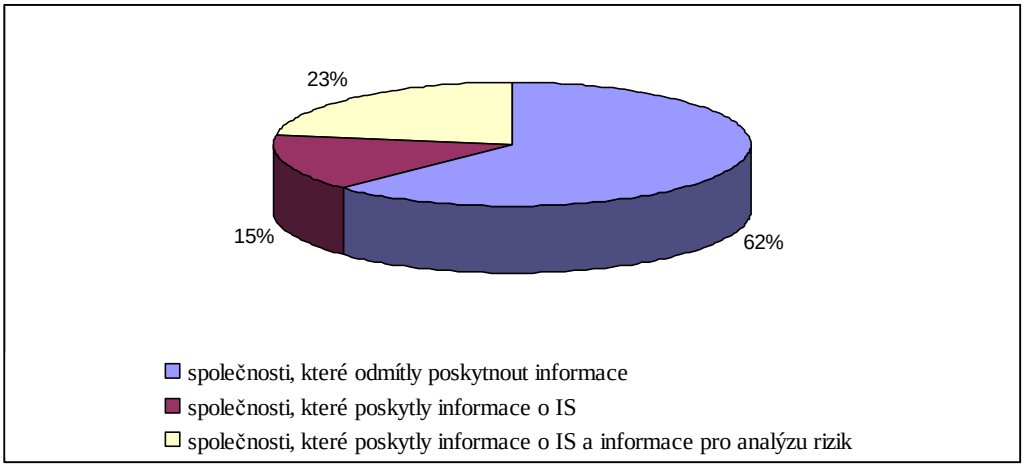
Vysoká úroveň rizika 6 - 8 V

Záznamy pořízené v rámci kvalitativního šetření, expertních rozhovorů, zaměřeného na informační management a aplikaci jeho principů v rámci podnikových procesů oslovených subjektů, jsou zařazeny na konec práce. Jedná se o přílohu C - Výstupy expertních rozhovorů.

3.1.2 Hodnocení expertních rozhovorů - závěrečná zpráva

V rámci expertních rozhovorů bylo osloveno 40 podnikatelských subjektů. Informace z oblasti řízení rizik IS bylo ochotno poskytnout 15 respondentů. Úspěšnost dotazování je 38 %. Z patnácti respondentů jich bylo 9 ochotno provést zběžnou analýzu rizik v rámci ekonomického/účetního oddělení společnosti. V případě shromažďování údajů pro sestavení registru rizik byla úspěšnost dotazování 23 % (ze všech oslovených společností).

Obrázek 10: Úspěšnost získávání informací v rámci expertních rozhovorů



Zdroj: vlastní zpracování, 2016

Odpovědi na pokládané dotazy považovali zástupci oslovených podnikatelských subjektů za citlivé interní informace. Z tohoto důvodu je počet oslovených podniků, jejichž zástupci se rozhodli informace neposkytnout z obavy o jejich zneužití, relativně vysoký.

Jedním z dílčích cílů disertační práce bylo zhodnocení současného stavu zahrnutí řízení informačních rizik do podnikových procesů vybraných subjektů podnikatelské sféry. S ohledem na existenci tří odlišných přístupů k informačnímu managementu popsaným v rešeršní části této práce (přístup zaměřený zejména na informační a komunikační technologie; přístup zaměřený zejména na informace; přístup zaměřený zejména na lidský faktor) a na stanovený cíl disertační práce byly otázky pokládané respondentům v rámci expertních rozhovorů směřovány do tří základních okruhů: informační systém společnosti obecně, informační systém používaný ekonomickým/účetním oddělením specificky a řízení informačních rizik.

Následující tabulky (Tab. 17, 18, 19 a 20) přehledně shrnují informace ze všech tří zkoumaných okruhů. V některých případech byli respondenti ochotni poskytnout i informace potřebné pro sestavení registru rizik. Respondentů, kteří se rozhodli takto detailní informace poskytnout, však byl relativně nízký počet. Informace nutné pro sestavení registru rizik jsou částí respondentů považovány za tak důvěrné, že jejich zveřejnění není možné.

Tabulka 17: Technické vybavení a používaný IS obecně A)

Název společnosti	Technické vybavení (v ks)				Používaný IS	Délka používání IS (v letech)	Nastavení přístupových práv k modulům IS
	PC	Notebook	Server	Externí úložiště			
Respondent číslo 1	31	10	4	0	PREMIER	6	omezena
Respondent číslo 2	100	15	30	0	CSB, NETTO	5 a 2	omezena
Respondent číslo 3	3	1	1	0	POHODA	14	neomezena
Respondent číslo 4	0	1	0	1	ABRA	21	neomezena
Respondent číslo 5	8	3	1	3	Money S3	15	omezena
Respondent číslo 6	---	---	---	0	J.K.R.	17	omezena
Respondent číslo 7	18	6	3	0	HSF Flex	19	omezena
Respondent číslo 8	11	0	1	1	K2	8	omezena
Respondent číslo 9	4	2	1	0	neuvedeno	15	omezena
Respondent číslo 10	2	1	0	0	neuvedeno	9	omezena
Respondent číslo 11	4	3	1	1	ABRA	21	neomezena
Respondent číslo 12	2	1	1	1	PREMIER	4	omezena
Respondent číslo 13	16	5	4	8	Ekonom	5	omezena
Respondent číslo 14	---	---	---	0	J.K.R.	17	omezena
Respondent číslo 15	7	0	1	1	vlastní	18	neomezena

Zdroj: vlastní zpracování, 2016

Tabulka 18: Technické vybavení a používaný IS obecně B)

Název společnosti	Zabezpečení IS			Frekvence zálohování	Zajištění správy IS	Četnost výskytu potíží s IS	IS splňuje požadavky na něj kladené
	Antivirový program	Firewall	Jiné				
Respondent číslo 1	X	X		denně	vlastní zaměstnanci	nejsou	ano
Respondent číslo 2	X	X		denně	vlastní zaměstnanci + dodavatel	občas	ano
Respondent číslo 3	X	X		denně	externí zaměstnanec	nejsou	ano
Respondent číslo 4	X			denně	externí firma	nejsou	ano
Respondent číslo 5	X	X		denně	dodavatel IS	často	ne
Respondent číslo 6	X	X		1xdenně 1xtýdně 1xročně	externí firma	občas	ano
Respondent číslo 7	X	X		denně	dodavatel IS	nejsou	ano
Respondent číslo 8	X			denně	externí firma	nejsou	ano
Respondent číslo 9	X			denně	vlastní zaměstnanci	občas	ano
Respondent číslo 10	X	X		denně	vlastní zaměstnanci + dodavatel	občas	ano
Respondent číslo 11	X			denně	externí firma	občas	ano
Respondent číslo 12	X	X		denně	externí firma	občas	ano
Respondent číslo 13	X	X		denně	vlastní zaměstnanci + dodavatel	občas	ano
Respondent číslo 14	X	X		1xdenně 1xtýdně 1xročně	externí firma	občas	ano
Respondent číslo 15	X			denně	externí firma	nejsou	ano

Zdroj: vlastní zpracování, 2016

Tabulka 19: IS používaný ekonomickým/účetním oddělením společnosti

Název společnosti	Oblast účetnictví je řešena		Frekvence výskytu problémů	Typ problémů	IS splňuje požadavky na něj kladené
	Samostatným úč. programem	Modulem, který je součástí IS			
Respondent číslo 1	X		nejsou	-----	ano
Respondent číslo 2	X		občas	různé (update, upgrade)	ano
Respondent číslo 3	X		nejsou	-----	ano
Respondent číslo 4		X	nejsou	------	ano
Respondent číslo 5		X	často	-----	ne
Respondent číslo 6		X	občas	přenos dat, výpadky internetu	ano
Respondent číslo 7	X		nejsou	-----	ano
Respondent číslo 8		X	nejsou	-----	ano
Respondent číslo 9		X	občas	------	spíše ano
Respondent číslo 10		X	občas	běžné uživatelské a provozní problémy	ano
Respondent číslo 11		X	občas	běžné uživatelské a provozní problémy	ano
Respondent číslo 12		X	občas	mechanické	ano
Respondent číslo 13		X	občas	běžné uživatelské a provozní problémy	ano
Respondent číslo 14		X	občas	přenos dat, výpadky internetu	ano
Respondent číslo 15	X		nejsou	-----	ano

Zdroj: vlastní zpracování, 2016

Tabulka 20: Míra zahrnutí informačního managementu mezi podnikové aktivity

Název společnosti	Respondent zná pojem „informační management“	Společnost informační management využívá	Společnost provádí analýzu rizik	Předpokládá se využití analýzy rizik v budoucnu
Respondent číslo 1	ne	ne	ne	ne
Respondent číslo 2	ano	ne	ne	ne
Respondent číslo 3	ne	ne	ne	neví
Respondent číslo 4	ano	ne	ano	-----
Respondent číslo 5	ne	ne	ano	-----
Respondent číslo 6	ano	ano	v zásadě ano	-----
Respondent číslo 7	ano	ano	ano	-----
Respondent číslo 8	ne	ne	ano	-----
Respondent číslo 9	ano	ne	ne	ne
Respondent číslo 10	ano	ano	ne	-----
Respondent číslo 11	ano	ne	ano	-----
Respondent číslo 12	ano	ano	ano	-----
Respondent číslo 13	ano	ano	ano	-----
Respondent číslo 14	ano	ano	v zásadě ano	-----
Respondent číslo 15	ano	ano	ano	-----

Zdroj: vlastní zpracování, 2016

Technické vybavení a IS obecně

Na základě informací poskytnutých respondenty bylo zjištěno, že je ve sledovaných společnostech věnována dostatečná pozornost technickému vybavení. Většina společností poskytla přesné informace o používaných složkách hardwaru. Informační systém používají již delší dobu všechny sledované společnosti. Ve většině případů se jedná o ERP systém. Typ používaného systému je volen v první řadě na základě vyhodnocení finálních požadavků, které na něj společnost má (nastavení uživatelského prostředí, rychlost práce s daty, kompatibilita s jinými systémy, provázanost modulů a jiné). Dalšími kritérii pro volbu vhodného IS jsou například: cena, dostupnost servisu nebo reference ostatních uživatelů systému. V oblasti MSP stále hraje velmi důležitou roli cena nakupovaného produktu. Přesto je však při výběru vhodného dodavatele kladen důraz nejen na cenu, ale také na hodnocení kvality nakupovaného IS. Společnosti si již uvědomují, že v případě pořízení nebo vylepšení informačního systému se jedná o dlouhodobou investici, která může posunout podnikové procesy vpřed (v případě nákupu vyhovujícího IS), nebo může zaměstnancům společnosti práci znesnadnit (v případě volby nevhodného IS).

Zabezpečení dat (informací) se téměř u všech sledovaných společností omezuje na oblast technického vybavení. Většinou bylo uváděno zabezpečení dat prostřednictvím antivirového programu a síťového firewallu. Dalším uváděným prvkem zabezpečení je denní zálohování dat na záznamová média (CD, DVD, flashdisc), internetová úložiště, server nebo jiné pevné disky. Správu informačního systému si společnosti zajišťují samy prostřednictvím svých vyškolených pracovníků, nebo využívají služeb dodavatele nebo externí společnosti. Výskyt problémů spojených s informačním systémem není podle poskytnutých údajů příliš častý. Pokud se již problémy vyskytnou, jedná se spíše o provozní potíže spojené s nastavením technického vybavení, které lze poměrně snadno a včas odstranit. Většina společností uvedla, že je s používaným IS spokojena.

Trend zahrnutí sledování lidského faktoru byl potvrzen jen v několika společnostech. Zabezpečení sledování rizik spojených s lidským faktorem ve většině sledovaných společností stále není věnována dostatečná pozornost. Společnosti předpokládají, že monitoring informačních rizik souvisejících s lidským faktorem není nutný, neboť možné negativní zásahy ze strany zaměstnanců řeší již nastavení podnikového IS. Všechny společnosti shodně uvádějí, že jedním ze zabezpečovacích prvků je nastavení

omezeného přístupu k informacím, které IS poskytuje (nastavení různých úrovní přístupů k jednotlivým modulům IS). Jako další prvek zabezpečení byla uváděna personální politika společnosti. Záměrem výběrových řízení na různé pozice v rámci společnosti je omezit možné negativní dopady na informační základnu společnosti způsobené selháním lidského faktoru již prostřednictvím hodnocení osobnostních kvalit přijímaného zaměstnance.

V MSP v podmínkách České republiky, resp. západních Čech, v současnosti stále převládá přístup k informačnímu managementu zaměřený zejména na informační a komunikační technologie. Na základě informací poskytnutých v rámci expertních rozhovorů lze dovodit, že si manažeři začínají uvědomovat nutnost zahrnutí lidského faktoru do pohledu na informační management. K řešení, které je podle zahraničních literárních zdrojů (Dias 2001), (Morabito 2013) ideální, k přístupu zaměřenému zejména na lidský faktor, se ale zatím nepropracovali. U některých společností se již objevují náznaky zavádění nových prvků do řízení rizik, výsledkem je však zatím jen jistý posun k přístupu zaměřenému zejména na informace.

IS používaný ekonomickým/účetním oddělením společnosti

Z informací poskytnutých v rámci expertních rozhovorů vyplynulo, že ve většině společností je v rámci ekonomického/účetního oddělení využíván účetní modul ERP systému. Problémy spojené s nastavením a funkcemi účetního IS jsou většinou provozního charakteru. Jedná se zejména o potíže vzniklé v souvislosti se zabezpečením funkčnosti technického vybavení. Servis je zajišťován buď vlastními silami nebo v součinnosti s dodavatelem IS.

Míra zahrnutí informačního managementu mezi podnikové aktivity

S pojmem informační management se již setkalo jedenáct z patnácti respondentů. Sedm z nich informační management aktivně využívá, jedná se však spíše o přístup k informačnímu managementu zaměřený zejména na informační a komunikační technologie. V deseti případech respondenti uvedli, že provádí analýzu rizik. Ne ve všech případech je však pro prováděné aktivity pojem „analýza rizik“ využíván. Společnosti analýzu provádí spíše intuitivním způsobem, bez hlubší znalosti metodik používaných pro řízení rizik. Nejčastěji je intuitivně postupováno v intencích metodiky

IPR (Identifikace procesů a rizik), kterou popisují ČSN 31000 (ISO 31000) a ČSN 36 9790 (ISO 36 9790).

Informace potřebné pro zpracování registru rizik v rámci ekonomického/účetního oddělení společnosti poskytlo (v různé kvalitě) devět respondentů. Kategorie úrovně rizika byly nastaveny dle ČSN 36 9790 a odlišeny takto:

Přijatelné riziko (Nízké)	0 - 2	N
Střední úroveň rizika	3 - 5	S
Vysoká úroveň rizika	6 - 8	V

Ve sledovaných podnicích byla identifikována rizika ve všech třech kategoriích úrovně rizika. Největší počet uvedených rizik spadá do kategorie „vysoká úroveň rizika“, rizika, u kterých je očekáván zásadní dopad do podnikových aktivit. Rizika s malým dopadem do podnikových aktivit, přijatelná rizika, se v ekonomických/účetních odděleních sledovaných společností vyskytují v devíti případech. Ostatní identifikovaná rizika spadají do kategorie označené jako „střední úroveň rizika“. Lze říci, že ve sledovaných společnostech je nutné podniknout opatření, která povedou ke změně stávajících podnikových procesů a jejich nastavení. Rizika, s nimiž přicházejí zaměstnanci ekonomického/účetního oddělení do styku jsou většinou provozního charakteru. Jen v několika málo případech se objevila i neúmyslná úprava informací.

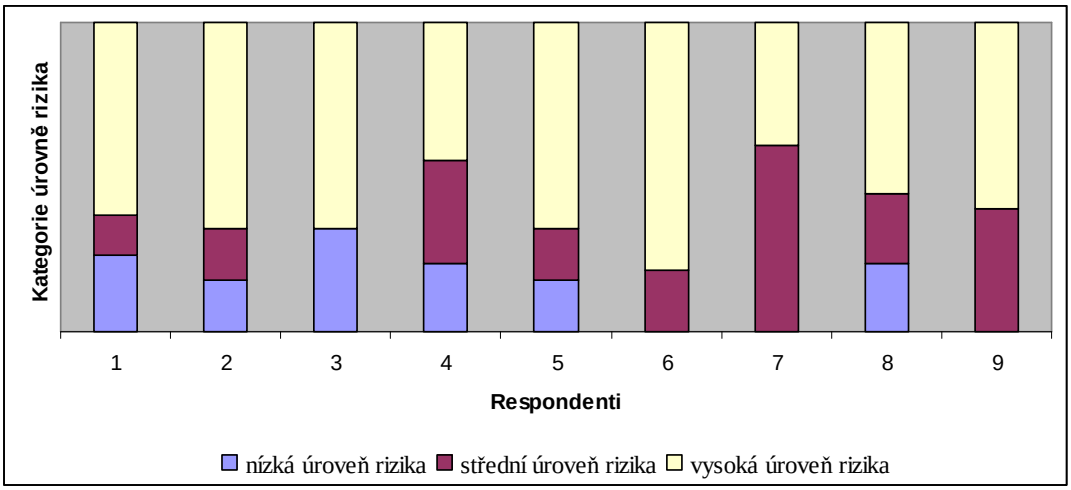
Většinou se v registrech rizik vyskytovala rizika jako nedostatečná aktualizace SW (uváděný stupeň rizika V, S) nebo nevhodné nastavení komunikace. Uvedená rizika většina respondentů považovala za rizika, která je možné řešit, nebo jim lze předcházet. V tomto směru již byly vyvinuty aktivity směřující k nápravě některých podnikových procesů.

Tabulka 21: Kategorie úrovně rizika v jednotlivých sledovaných společnostech

Kategorie úrovně rizika	Sledované společnosti - Množství rizik v jednotlivých kategoriích								
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
N - nízká	2	1	1	2	1	0	0	2	0
S - střední	1	1	0	3	1	1	3	2	2
V - vysoká	5	4	2	4	4	4	2	5	3

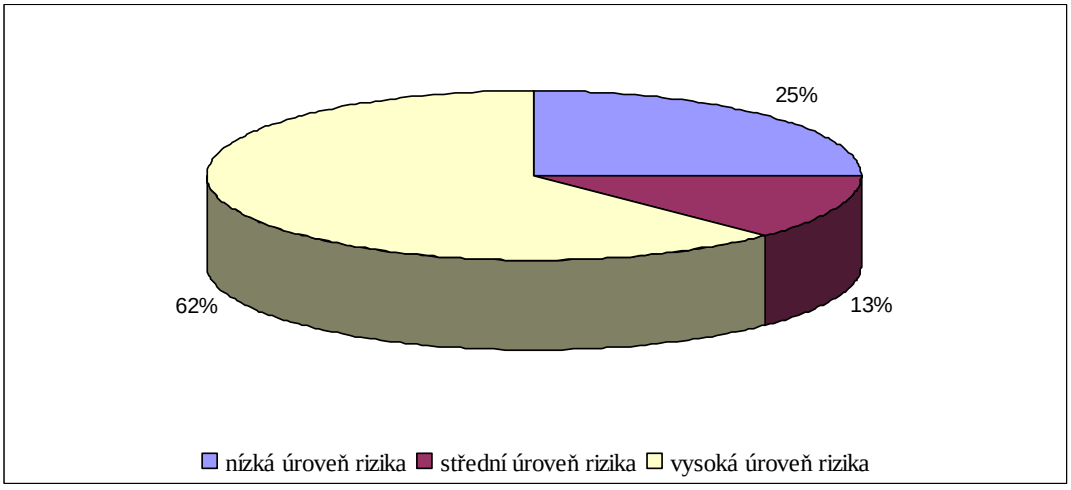
Zdroj: vlastní zpracování, 2016

Obrázek 11: Zastoupení jednotlivých kategorií úrovně rizika v ekonomickém/účetním oddělení sledovaných společností



Zdroj: vlastní zpracování, 2016

Obrázek 12: Kategorie úrovně rizika ve sledovaných společnostech - procentuální vyjádření



Zdroj: vlastní zpracování, 2016

3.1.3 Shrnutí

Tato část práce sumarizuje a hodnotí informace získané prostřednictvím expertních rozhovorů. Osloveno bylo 40 podnikatelských subjektů. Informace z oblasti řízení rizik IS bylo ochotno poskytnout 15 respondentů, z nichž 9 bylo ochotno provést i zběžnou analýzu rizik v rámci ekonomického/účetního oddělení společnosti.

Aby bylo možné zhodnotit současný stav zahrnutí řízení informačních rizik do podnikových procesů u vybraných subjektů podnikatelské sféry, byly otázky pokládané respondentům v rámci expertních rozhovorů rozděleny do tří základních okruhů: informační systém společnosti obecně, informační systém používaný ekonomickým/účetním oddělením specificky a řízení informačních rizik.

Na základě informací poskytnutých respondenty bylo zjištěno, že je ve sledovaných společnostech věnována dostatečná pozornost technickému vybavení, informační rizika spojená se selháním lidského faktoru buď nejsou řešena vůbec, nebo jsou řešena v omezené míře. Společnosti předpokládají, že monitoring informačních rizik souvisejících s lidským faktorem není nutný, neboť možné negativní zásahy ze strany zaměstnanců řeší již nastavení podnikového IS. Informační rizika spojená s lidským faktorem však většinou nevyplývají z aktivních negativních zásahů, ale spíše z nepozornosti, nepořádku a dalších, zdánlivě triviálních faktorů.

V MSP v podmínkách České republiky, resp. západních Čech, v současnosti stále převládá přístup k informačnímu managementu zaměřený zejména na informační a komunikační technologie. Společnosti řídí informační rizika i rizika obecně spíše intuitivním způsobem, bez hlubší znalosti metodik používaných pro řízení rizik.

3.2 Dotazníkové šetření

V této části disertační práce jsou uvedena zjištění z oblasti řízení informačních rizik v ekonomických odděleních vybraných podnikatelských subjektů. Informace byly získány prostřednictvím dotazníkového šetření na téma "Řízeni informačních rizik v organizaci". Hlavním cílem provedeného výzkumu bylo, stejně jako u expertních rozhovorů popsaných v předchozí části práce, zjistit, do jaké míry dochází u oslovených podnikatelských subjektů k začlenění řízení informačních rizik mezi ostatní podnikové procesy. Dotazníkové šetření mělo znovu ověřit autorčinu hypotézu o nízké úrovni zahrnutí řízení informačních rizik v rámci podnikových aktivit vybraných podnikatelských subjektů.

Dotazník, uvedený v příloze disertační práce, byl vytvořen prostřednictvím služeb nabízených společností Survio s.r.o. Tvoří jej 22 otázek z následujících okruhů:

- Okruh 1 - základní údaje o zkoumaném subjektu.
- Okruh 2 - informační systém organizace obecně.
- Okruh 3 - účetní informační systém specificky.
- Okruh 4 - řízení rizik.

Okruhy však nejsou, s ohledem na zkušenosti z předchozího výzkumu, v dotazníku odděleny.

3.2.1 Rámec dotazníkového šetření

Šetření proběhlo od dubna 2015 do ledna 2016. O účast na výzkumu byli požádáni zástupci podnikatelských subjektů vybraných podle následujících kritérií:

- společnost působí v oblasti západních Čech,
- na základě informací o společnosti lze předpokládat existenci jejího ekonomického/účetního oddělení,
- na základě informací o společnosti lze předpokládat využití informačního systému v rámci podnikových procesů.

V souvislosti s nutností identifikovat vhodné respondenty, byla o pomoc požádána i zástupkyně Okresní hospodářské komory Klatovy, která pomoc nejprve přislíbila,

ale posléze spolupráci, s odkazem na přílišnou citlivost požadovaných dat, odmítla. Na základě zvolených kritérií byli autorkou vytipováni a osloveni zástupci 300 podnikatelských subjektů. Vybraným respondentům byl elektronickou formou zaslán dotazník se stručným vysvětlením důvodu a cíle prováděného výzkumu a s žádostí o jeho vyplnění. Dotazník byl dostupný na webových stránkách společnosti Survio s.r.o., prostřednictvím jejichž služeb byl vytvořen. Velké množství společností vyhodnotilo pokládané otázky jako příliš detailní, a proto se z obavy o zneužití citlivých interních informací rozhodly šetření neúčastnit.

S ohledem na uvedenou skutečnost nebyla návratnost dotazníků v prvních měsících prováděného šetření dostatečná, proto bylo nutné oslovit zvolené společnosti znovu. Z důvodu nízké návratnosti dotazníků byla připravena i listinná podoba dotazníku, která byla vybraným respondentům předložena autorkou osobně. V souvislosti s neexistencí oficiálního seznamu podniků, ve kterém by bylo možné hledat vhodné respondenty a s obavami společností o zneužití interních informací, není výzkum v této oblasti jednoduchý. Konečná návratnost činila 63 dotazníků, což představuje 21 %. Autorka se přesto domnívá, že vzorek (63 zpět získaných dotazníků) je dostatečně velký a postačuje k identifikaci a generalizaci některých hledisek implementace a následné aplikace postupů řízení informačních rizik, resp. metody IPR, která je univerzálním nástrojem pro odhalování rizik a jejich příčin, v podnikové praxi.

3.2.2 Informační management a aplikace jeho principů v rámci podnikových procesů jednotlivých respondentů - dotazníkové šetření

V rámci výzkumu byla sledována míra zahrnutí řízení informačních rizik do podnikových procesů a způsob, kterým jsou rizika ve společnosti řízena (používaná metodika řízení rizik). Většina respondentů uvedla, že ve společnosti není informační management zaveden. Přesto bylo při detailnějším rozboru zaslaných odpovědí zjištěno, že se společnosti informačními riziky v zásadě zabývají. Řídí je však většinou intuitivně. Informační management a terminologii s ním spojenou nepoužívají. Odpovědi na jednotlivé otázky dotazníku jsou shrnuty níže.

Otázka č. 1: Do které z níže uvedených skupin patří Vaše společnost?

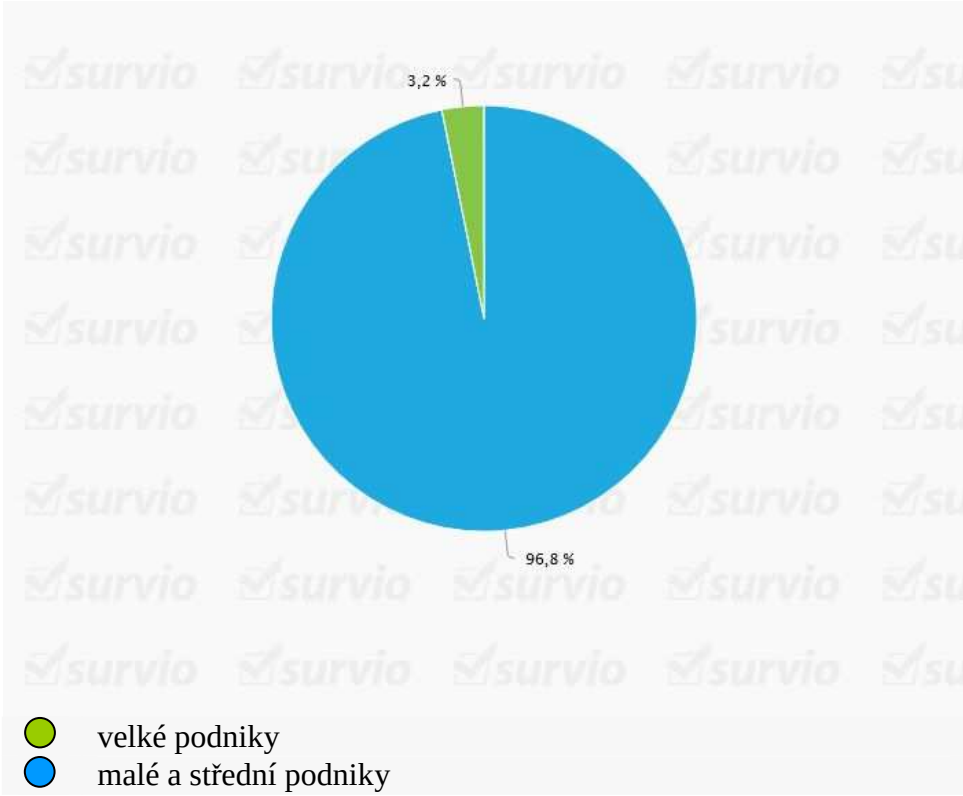
V rámci identifikace vhodných respondentů byly zvažovány společnosti působící v oblasti západních Čech, jejichž součástí je s vysokou pravděpodobností ekonomické/účetní oddělení, a u kterých lze předpokládat využití informačního systému v rámci podnikových procesů. Byli osloveni zástupci tří set podnikatelských subjektů, z nichž většinu tvořily podniky spadající do kategorie MSP.

Tabulka 22: Členění respondentů dotazníkového šetření podle velikosti

Velikost podniku	Počet respondentů	Podíl respondentů
Malé a střední podniky	61	96,8 %
Velké podniky	2	3,2 %
Celkem	**63**	**100 %**

Zdroj: vlastní zpracování, 2016

Obrázek 13: Členění respondentů dotazníkového šetření podle velikosti



Zdroj: vlastní zpracování dle (Survio 2016), 2016

Otázka č. 2: Do jaké oblasti spadá předmět podnikání Vaší společnosti?

Výběr respondentů nebyl omezen předmětem podnikání společnosti. Přesto byla za účelem získání detailnějších údajů o respondentovi pokládána tato otázka.

Tabulka 23: Členění respondentů dotazníkového šetření podle předmětu podnikání

Předmět podnikání - klasifikace dle NACE	**Počet respondentů**
Rostlinná a živočišná výroba	1
Výroba potravinářských výrobků	8
Výroba chemických látek a chemických přípravků	8
Výroba pryžových a plastových výrobků	1
Výroba kovových konstrukcí a kovodělných výrobků, kromě strojů a zařízení	7
Výroba a rozvod elektřiny, plynu, tepla a klimatizovaného vzduchu	2
Shromažďování, sběr a odstraňování odpadů, úprava odpadů k dalšímu využití	1
Výstavba budov	2
Specializované stavební činnosti	8
Maloobchod, kromě motorových vozidel	3
Pozemní doprava	1
Skladování a vedlejší činnosti v dopravě	2
Telekomunikační činnosti	2
Činnosti v oblasti informačních technologií	4
Právní a účetnické činnosti	7
Architektonické a inženýrské činnosti; technické zkoušky a analýzy	5
Sportovní, zábavní a rekreační činnosti	1
Celkem	**63**

Zdroj: vlastní zpracování, 2016

Otázka č. 3: Setkali jste se již s pojmem „informační management“?

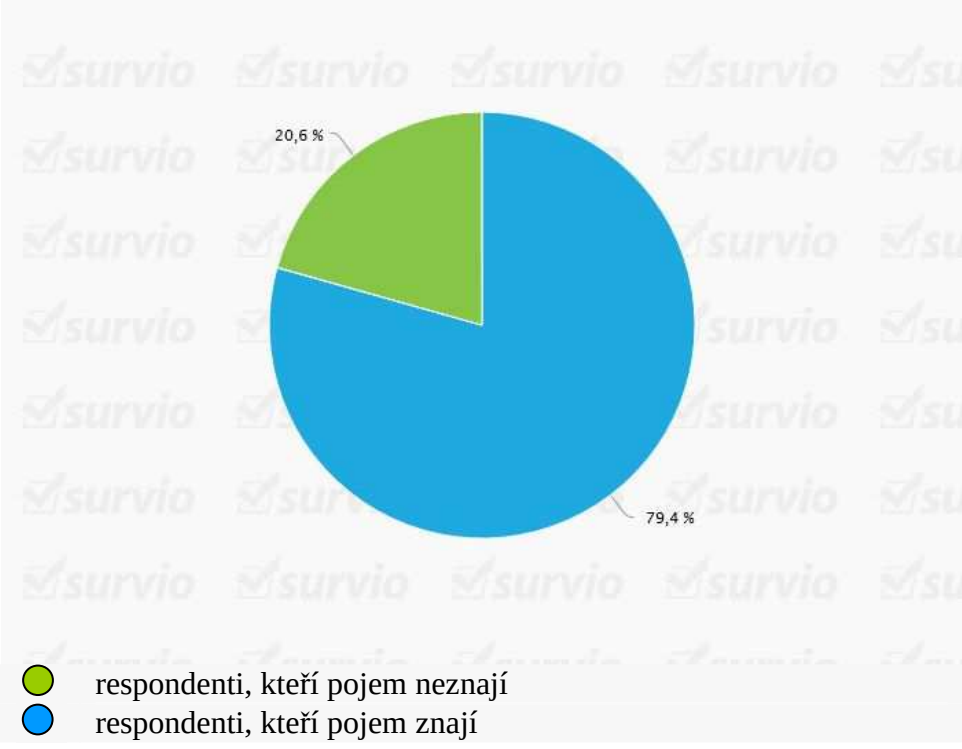
Formulace ověřované hypotézy byla: „Více než polovina sledovaných společností se již setkala s pojmem informační management.“ Výsledky dotazníkového šetření uvedenou hypotézu potvrdily.

Tabulka 24: Povědomí respondentů o informačním managementu

Znalost pojmu informační management	Počet respondentů	Podíl respondentů
Znám pojem informační management	50	79,4 %
Neznám pojem informační management	13	20,6 %
Celkem	**63**	**100 %**

Zdroj: vlastní zpracování, 2016

Obrázek 14: Povědomí respondentů o informačním managementu



Zdroj: vlastní zpracování dle (Survio 2016), 2016

Otázka č. 4: Využívá Vaše společnost informační management?

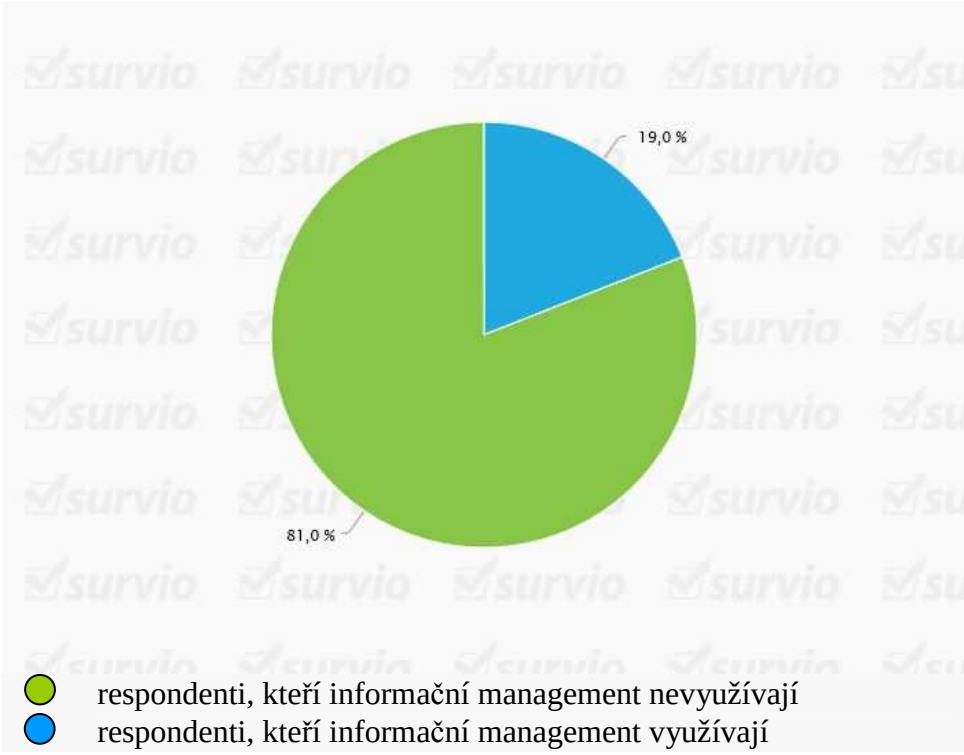
Většina dotazovaných společností se s pojmem informační management již seznámila. Z odpovědí na otázku číslo 4 je však patrné, že tuto disciplínu využívá jen velmi malé množství respondentů.

Tabulka 25: Využití informačního managementu respondenty

Využití informačního managementu	Počet respondentů	Podíl respondentů
Využíváme informační management	12	19 %
Nevyužíváme informační management	51	81 %
Celkem	**63**	**100 %**

Zdroj: vlastní zpracování, 2016

Obrázek 15: Využití informačního managementu respondenty



Zdroj: vlastní zpracování dle (Survio 2016), 2016

Otázka č. 5: Jakou metodiku řízení informačních rizik využíváte?

U otázky číslo 5 bylo možné zaškrtnout současně více odpovědí. Na základě výsledků šetření byla respondenty nejčastěji volena první možnost, řízení informačních rizik intuitivním způsobem. V šesti případech byla označena možnost využití jiné metodiky řízení informačních rizik. Ve specifikaci této možnosti byly uvedeny následující komentáře:

- jsme malá firma, rizika neřídíme,
- vycházíme z vlastních dlouholetých zkušeností a z praxe,
- žádnou metodiku nevyužíváme.

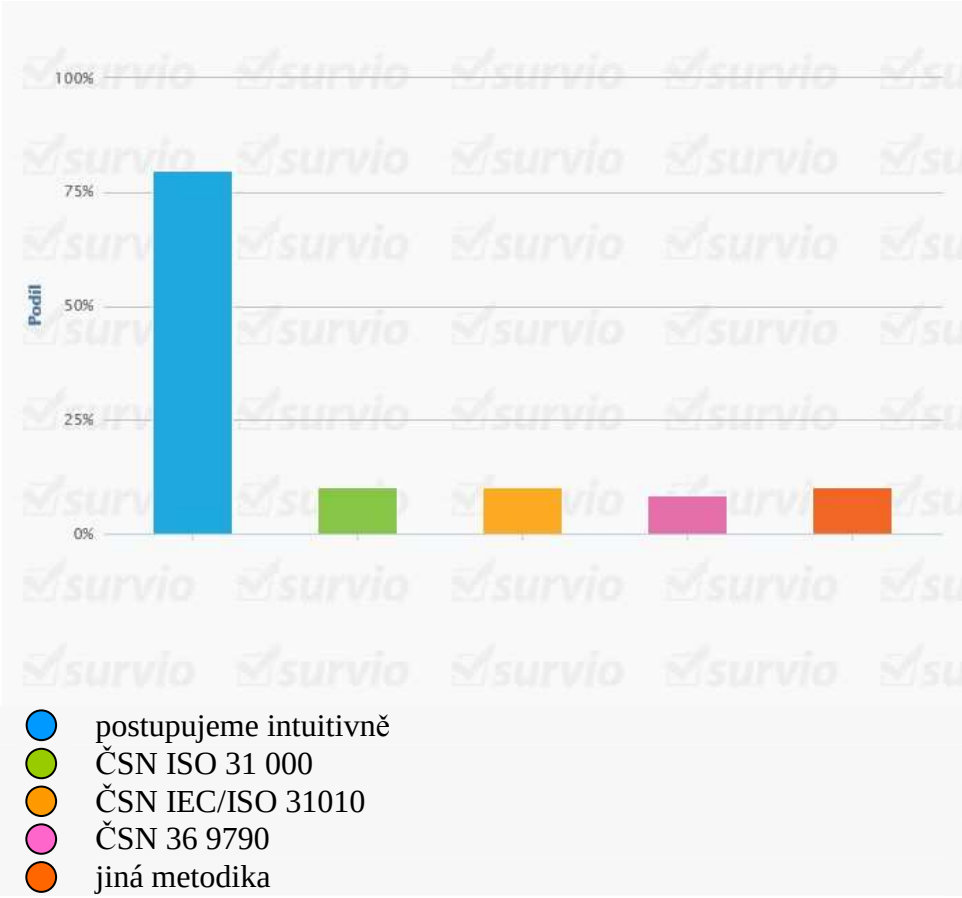
Výsledky shrnuje následující tabulka a obrázek.

Tabulka 26: Členění respondentů podle používané metodiky řízení informačních rizik

Metodika řízení informačních rizik	Počet respondentů	Podíl respondentů
Postupujeme intuitivně	47	79,7 %
ČSN ISO 31000 - Management rizik - Principy a směrnice (01 0351)	6	10,2 %
ČSN IEC/ISO 31010 Management rizik - Techniky posuzování rizik	6	10,2 %
ČSN 36 9790 - Systém managementu bezpečnosti informací	5	8,5 %
Jiná metodika	6	10,2 %

Zdroj: vlastní zpracování, 2016

Obrázek 16: Členění respondentů podle používané metodiky řízení informačních rizik



Zdroj: vlastní zpracování dle (Survio 2016), 2016

Otázka č. 6: Jaké typy rizik Vaše společnost sleduje?

Z odpovědí na tuto otázku vyplývá, že většina společností rizika sleduje. Nejvíce sledovanými oblastmi jsou informační technologie a informace. U rizik spojených s lidským faktorem je nejčastěji volena možnost „rizika jsou sledována“, je zde však současně zaznamenán i nejvyšší počet odpovědí „rizika nesledujeme.“ Získané odpovědi potvrdily hypotézy:

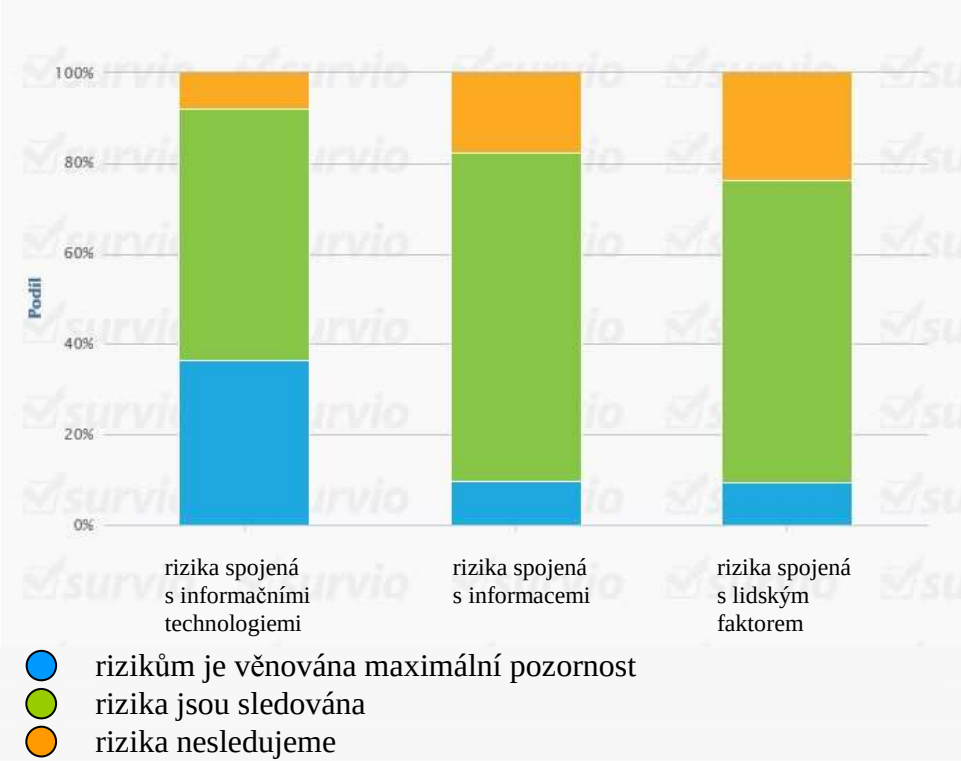
- Většina sledovaných společností pod pojmem informačním management vnímá především informační a komunikační technologie a nevěnuje pozornost dalším okruhům, které patří do informačního managementu.
- Informačním rizikům spojeným s lidským faktorem věnuje maximální pozornost jen malé množství sledovaných společností.

Tabulka 27: Typy rizik sledovaných respondenty

	Míra sledovanosti rizika			
Typ rizika	Rizikům je věnována maximální pozornost	Rizika jsou sledována	**Sloupce 1 a 2 celkem**	Rizika nesledujeme
Rizika spojená s informačními technologiemi	23 respondentů	35 respondentů	**58 respondentů**	5 respondentů
Rizika spojená s informacemi	6 respondentů	45 respondentů	**51 respondentů**	11 respondentů
Rizika spojená s lidským faktorem	6 respondentů	42 respondentů	**48 respondentů**	15 respondentů

Zdroj: vlastní zpracování, 2016

Obrázek 17: Typy rizik sledovaných respondenty



Zdroj: vlastní zpracování dle (Survio 2016), 2016

Otázka č. 7: Pokud nevyužíváte informační management, předpokládáte jeho využití v budoucnu?

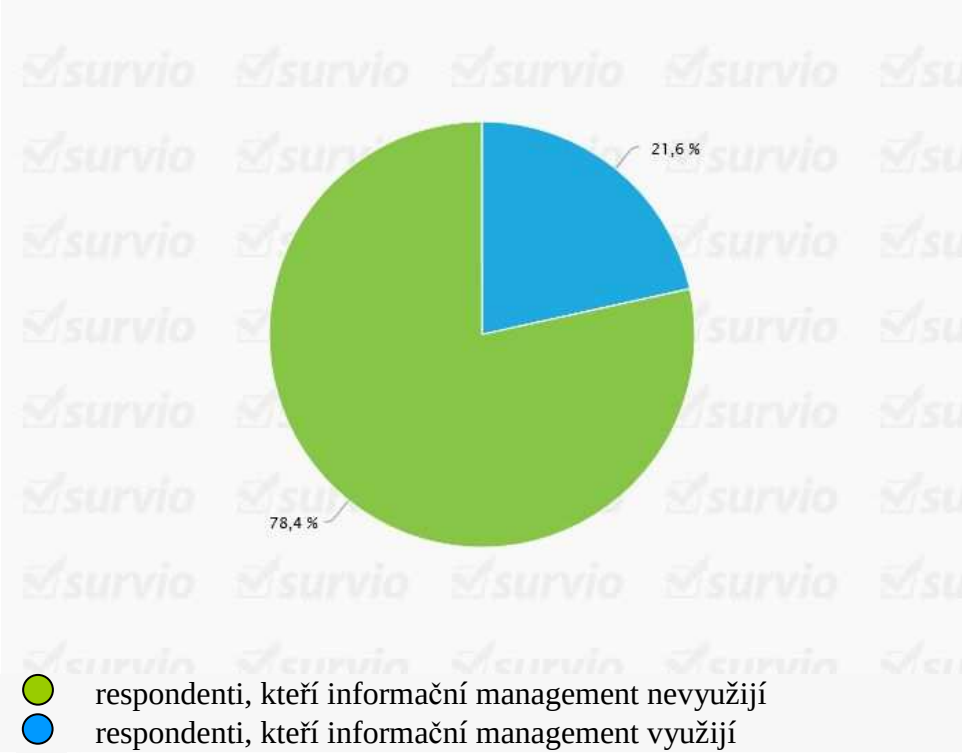
12 respondentů informační management již využívá. Ze zbývajících 51 respondentů se jich pro možnost využití informačního managementu v budoucnu vyslovilo 11, zbylých 40 respondentů s využitím informačního managementu do budoucna nepočítá.

Tabulka 28: Možnost budoucího využití informačního managementu respondenty, kteří jej dosud nevyužívají

Využití informačního managementu	Počet respondentů	Podíl respondentů
Budu využívat informační management	11	21,6 %
Nebudu využívat informační management	40	78,4 %
Celkem	**51**	**100 %**

Zdroj: vlastní zpracování, 2016

Obrázek 18: Možnost budoucího využití informačního managementu respondenty, kteří jej dosud nevyužívají



Zdroj: vlastní zpracování dle (Survio 2016), 2016

Otázka č. 8: Jaký informační systém využívá Vaše společnost?

Typy informačních systémů využívané jednotlivými respondenty shrnuje níže uvedená tabulka. 17 respondentů v odpovědi uvedlo, že využívá vlastní informační systém. Ostatní společnosti uvedly jako nejčastěji využívaný informační systém systémy JKR a různé verze systému Money S. Všechny odpovědi shrnuje následující tabulka.

Tabulka 29: Informační systémy využívané respondenty

Informační systém	Počet výskytů v odpovědích respondentů	Informační systém	Počet výskytů v odpovědích respondentů
ABRA	6	Netto	1
Comstar	1	Pohoda	3
CSB	1	Premier	3
Ekonom	1	QAD	6
EkoSoft	1	SAP	1
HSF Flex	1	Stereo	1
JKR	7	Vision	1
K2	4	Intranetové aplikace	1
Money S	7	Vlastní systém	17

Zdroj: vlastní zpracování, 2016

Otázka č. 9: Jedná se o informační systém „na míru“?

Informační systém vytvořený „na míru“ podnikatelskému subjektu je využíván v sedmnácti společnostech.

Otázka č. 10: Ovlivnily níže uvedené faktory výběr informačního systému ve Vaší společnosti ?

Následující tabulka popisuje vliv faktorů, kterými jsou cena, dostupnost servisu, kompatibilita IS s jinými systémy, nastavení uživatelského prostředí, provázanost modulů, reference ostatních uživatelů systému a rychlost práce s daty, na výběr informačního systému v dotazované společnosti. Podle získaných informací byl výběr IS ovlivněn nejvíce dostupností servisu, kterou označilo celkem 60 respondentů

(52 a 8). Dalšími signifikantními faktory byly rychlost práce s daty (48 a 11 respondentů) a cena (37 a 22 respondentů), následovala provázanost modulů (38 a 16 respondentů) a jako důležité označili respondenti i nastavení uživatelského prostředí (17 a 35 respondentů). Nejméně výběr IS ovlivnily kompatibilita IS s jinými systémy (15 a 29 respondentů) a reference ostatních uživatelů (13 a 31 respondentů).

Tabulka 30: Míra vlivu uvedených faktorů na výběr IS v podniku respondenta

	Míra vlivu faktoru na výběr IS			
Sledovaný faktor	**Faktor ovlivnil výběr IS**	**Faktor výběr IS spíše ovlivnil**	**Faktor výběr IS spíše neovlivnil**	**Faktor výběr IS neovlivnil**
Cena	37 respondentů	22 respondentů	1 respondent	0 respondentů
Dostupnost servisu	52 respondentů	8 respondentů	1 respondent	0 respondentů
Kompatibilita s jinými systémy	15 respondentů	29 respondentů	14 respondentů	2 respondenti
Nastavení uživatelského prostředí	17 respondentů	35 respondentů	8 respondentů	1 respondent
Provázanost modulů	38 respondentů	16 respondentů	5 respondentů	2 respondenti
Reference ostatních uživatelů IS	13 respondentů	31 respondentů	8 respondentů	8 respondentů
Rychlost práce s daty	48 respondentů	11 respondentů	1 respondent	0 respondentů

Zdroj: vlastní zpracování, 2016

Otázka č. 11: Jak je ve společnosti zajištěna bezpečnost dat?

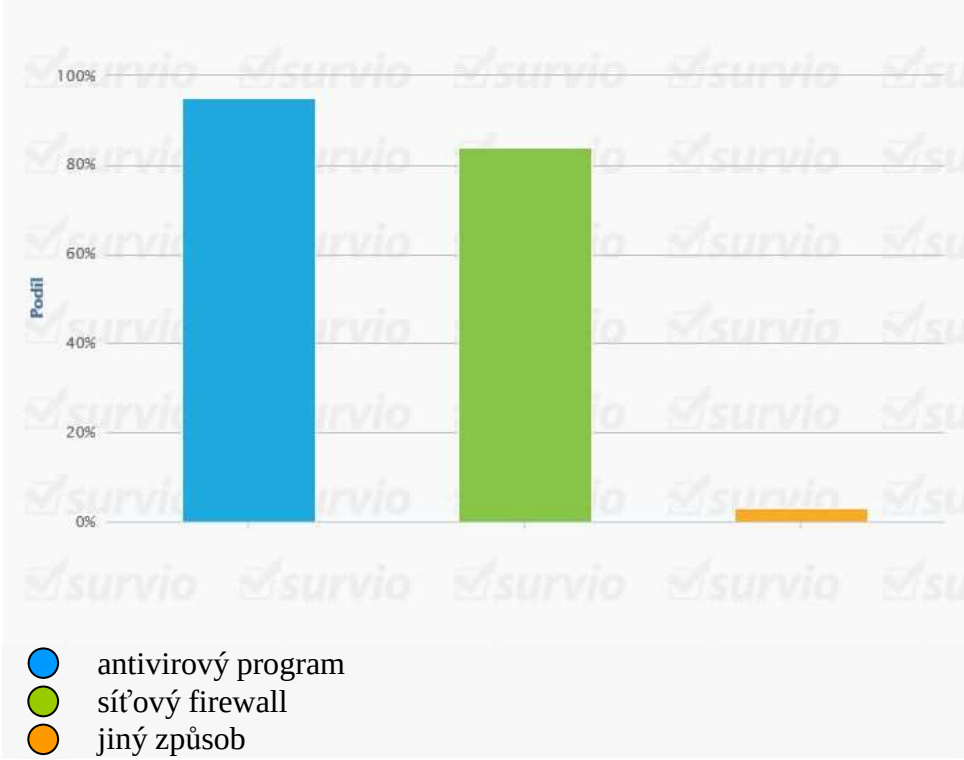
Následující tabulka a obrázek dokládají, že ve většině společností jsou jako standardní zabezpečovací prvky využívány antivirový program a síťový firewall. Dva respondenti uvedli i jiné způsoby zabezpečení, jeden pravidelné kopie dat a druhý datahosting.

Tabulka 31: Způsoby zabezpečení dat využívané jednotlivými respondenty

Způsob zabezpečení dat	Počet respondentů	Podíl respondentů
Antivirový program	59	95,2 %
Síťový firewall	52	83,9 %
Jiný způsob	2	3,2 %

Zdroj: vlastní zpracování, 2016

Obrázek 19: Způsoby zabezpečení dat využívané jednotlivými respondenty



Zdroj: vlastní zpracování dle (Survio 2016), 2016

Otázka č. 12: Data jsou zálohována na:

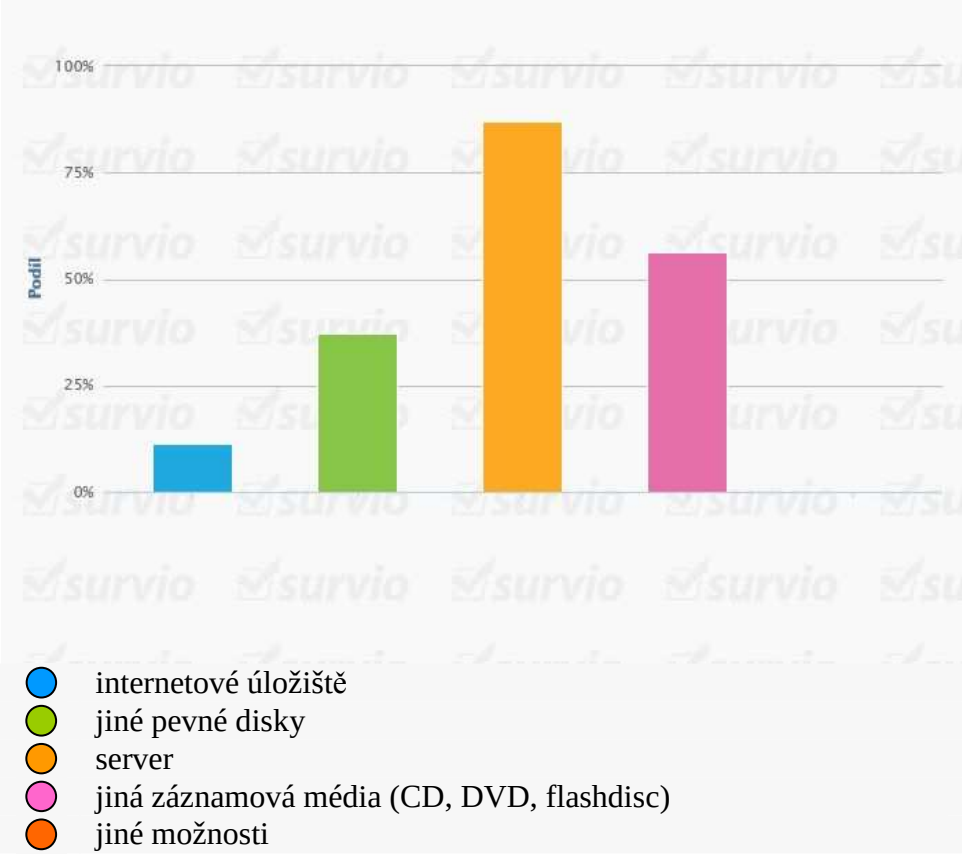
Společnosti byly dotazovány na způsoby zálohování dat. Nejvíce, 54 respondentů, uvedlo, že data zálohuje prostřednictvím serveru, 35 respondentů využívá jiná záznamová média (CD, DVD, flashdisc), 23 jich využívá jiné pevné disky a 7 respondentů uvedlo jako způsob zálohování dat i internetové úložiště. Jiné možnosti nebyly uvedeny.

Tabulka 32: Členění respondentů podle používaného způsobu zálohování

Metodika řízení informačních rizik	Počet respondentů	Podíl respondentů
Internetové úložiště	7	11,3 %
Jiné pevné disky	23	37,1 %
Server	54	87,1 %
Jiná záznamová média (CD, DVD, flashdisc)	35	56,5 %
Jiné možnosti	0	0 %

Zdroj: vlastní zpracování, 2016

Obrázek 20: Členění respondentů podle používaného způsobu zálohování



Zdroj: vlastní zpracování dle (Survio 2016), 2016

Otázka č. 13: Kdo spravuje informační systém společnosti?

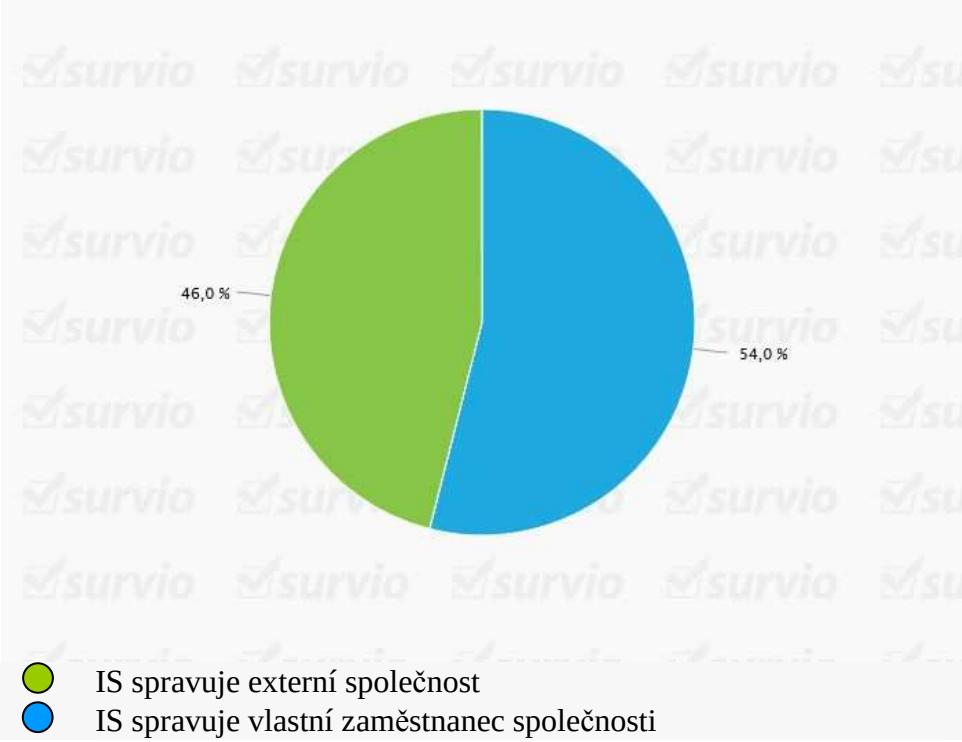
Situace v oblasti správy informačního systému je relativně vyrovnaná. Služby externí společnosti využívá 46 % společností, vlastního zaměstnance má 54 % dotazovaných společností.

Tabulka 33: Správa informačního systému dotazovaných společností

IS společnosti spravuje	Počet respondentů	Podíl respondentů
Zaměstnanec společnosti	34	54 %
Externí společnost	29	46 %
Celkem	**63**	**100 %**

Zdroj: vlastní zpracování, 2016

Obrázek 21: Správa informačního systému dotazovaných společností



Zdroj: vlastní zpracování dle (Survio 2016), 2016

Otázka č. 14: Jakým způsobem je ve společnosti zajištěna oblast účetnictví?

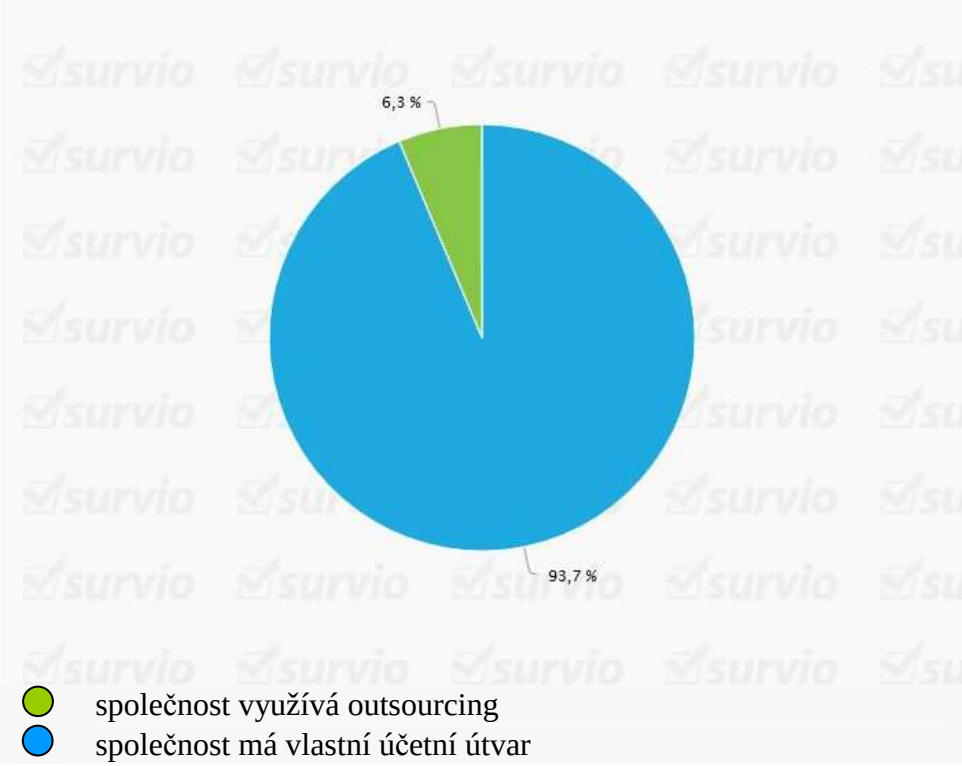
Při identifikaci respondentů bylo postupováno tak, aby byly voleny společnosti s vlastním účetním útvarem. Na základě odpovědí obdržených na otázku číslo 14 je možné konstatovat, že záměr byl z 93,7 % naplněn.

Tabulka 34: Zajištění oblasti účetnictví dotazovaných společností

Způsob zajištění účetnictví	Počet respondentů	Podíl respondentů
Vlastní účetní útvar	59	93,7 %
Využití outsourcingu	4	6,3 %
Celkem	**63**	**100 %**

Zdroj: vlastní zpracování, 2016

Obrázek 22: Zajištění oblasti účetnictví dotazovaných společností



Zdroj: vlastní zpracování dle (Survio 2016), 2016

Otázka č. 15: Jaké jsou důvody pro využití outsourcingu pro oblast účetnictví?

Na tuto otázku odpovídali pouze 4 respondenti. Jako hlavní důvod pro využití outsourcingu byla uváděna skutečnost, že se společnosti nevyplatí mít vlastní účtárnu. Tento důvod uvedly všechny 4 společnosti. Jeden respondent označil jako důvod pro neexistenci vlastního účetního oddělení společnosti také možnost vyhnout se neustálé kontrole upgradů účetního softwaru.

Otázka č. 16: Jaká rizika s sebou, podle Vašeho názoru, přináší outsourcing účetnictví?

45 dotazovaných společností vnímá jako riziko outsourcingu účetnictví ztrátu důvěrnosti dat. 38 respondentů by se v takovém případě obávalo zrušení dodavatelských služeb nebo jejich výpadků a jeden respondent uvedl nižší flexibilitu společnosti v oblasti účetnictví.

Otázka č. 17: Jaká opatření pro minimalizaci rizik plynoucích z outsourcingu účetnictví provádíte?

Mezi opatření směřující k minimalizaci rizik, která plynou z využití outsourcingu účetnictví patří dle respondentů:

- smluvní zajištění,
- časté návštěvy daňových poradců (jednou za 14 dní),
- doklady společnost vystavuje a vkládá do systému sama,
- veškerý účetní software a jeho zálohy jsou umístěny v sídle firmy.

Otázka č. 18: Jaký software je využíván pro oblast účetnictví?

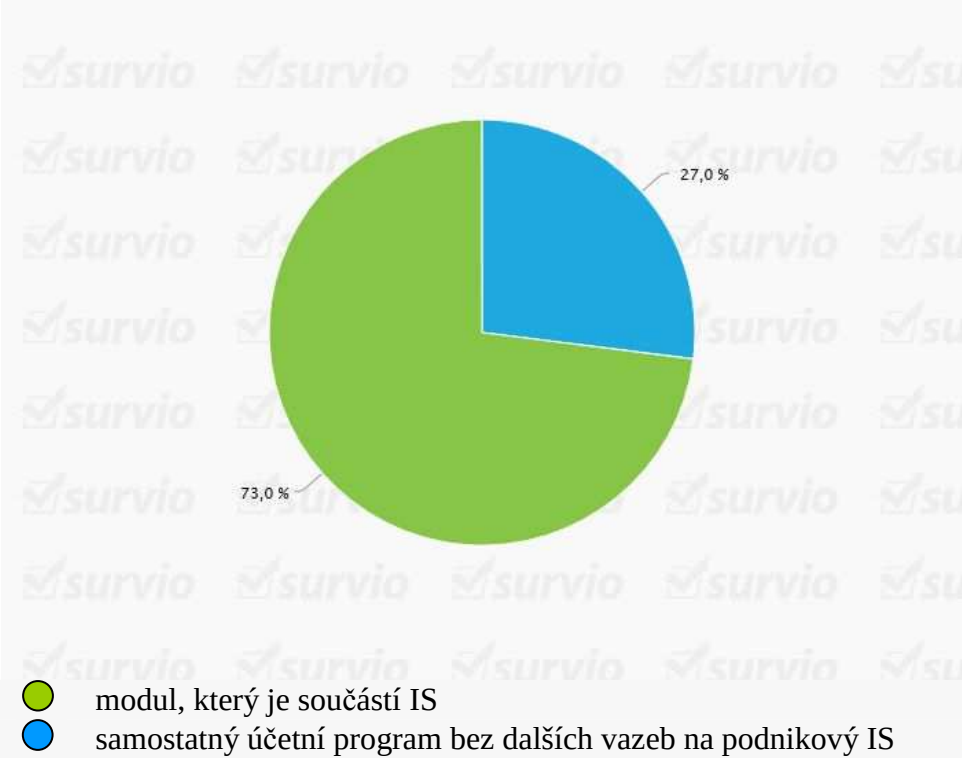
Většina dotazovaných společností využívá na trhu běžně dostupné informační systémy, JKR, Money S, QAD a ABRA. Nejčastěji se jedná o ERP systémy s provázanými moduly, mezi kterými je zahrnut i modul účetnictví.

Tabulka 35: Typ účetního softwaru využívaný respondenty

Způsob zajištění účetnictví	Počet respondentů	Podíl respondentů
Samostatný účetní program bez dalších vazeb na podnikový IS	17	27 %
Modul, který je součástí IS	46	73 %
Celkem	**63**	**100 %**

Zdroj: vlastní zpracování, 2016

Obrázek 23: Typ účetního softwaru využívaný respondenty



Zdroj: vlastní zpracování dle (Survio 2016), 2016

Otázka č. 19: Jsou omezena přístupová práva k informačnímu systému/k modulu účetnictví?

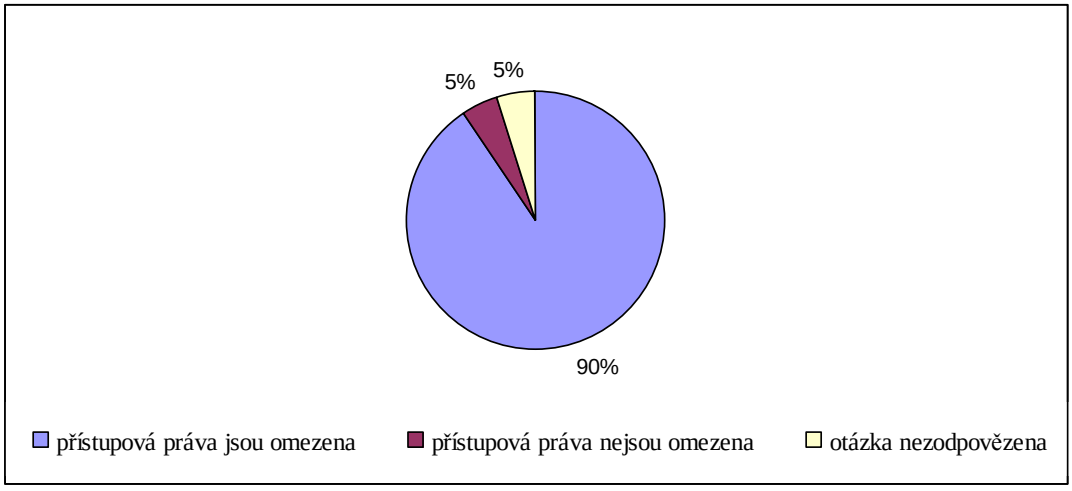
Omezení přístupových práv k účetním informacím je jednou z možností zabezpečení účetních dat. Většina společností, 57 respondentů, tuto možnost využívá, 3 společnosti označily možnost „ne“ a zástupci 3 společností tuto otázku nezodpověděli.

Tabulka 36: Omezení přístupových práv k účetním informacím v dotazovaných společnostech

Přístupová práva	Počet respondentů	Podíl respondentů
Jsou omezena	57	95 %
Nejsou omezena	3	5 %
Respondent odpověď neuvedl	3	5 %
Celkem	**63**	**100 %**

Zdroj: vlastní zpracování, 2016

Obrázek 24: Omezení přístupových práv k účetním informacím v dotazovaných společnostech



Zdroj: vlastní zpracování, 2016

Otázka č. 20: Kdo má přístup k účetním informacím?

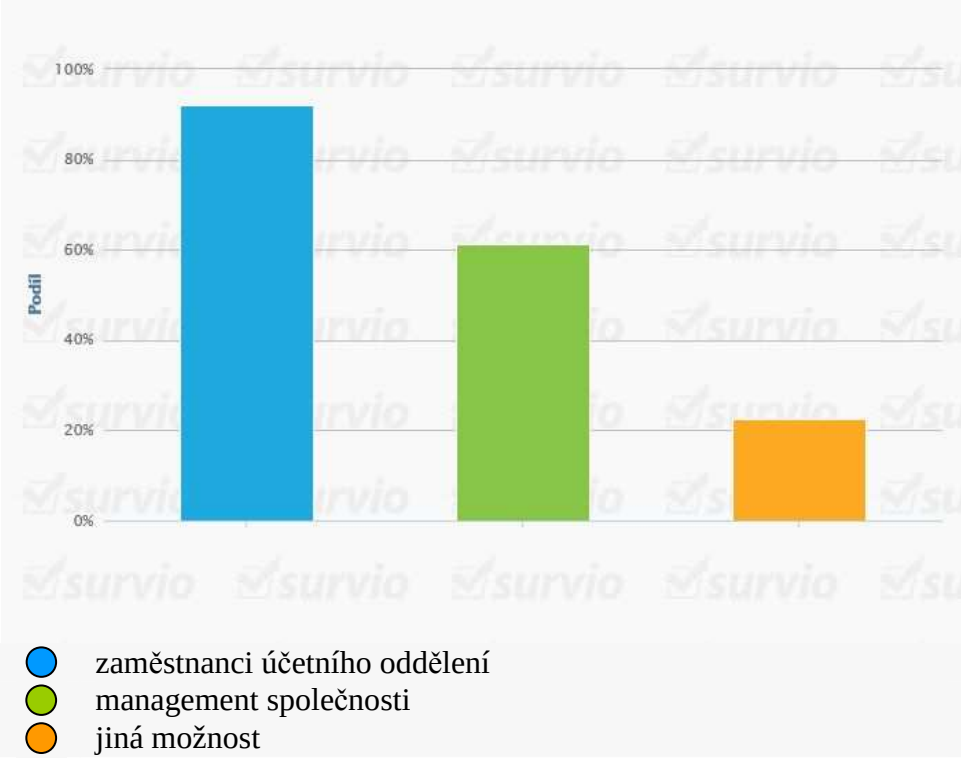
V rámci této otázky bylo možné zaškrtnout více možností. Většina společností zvolila první a druhou možnost. Přístupová práva k účetním informacím ve společnosti mají zaměstnanci účetního oddělení a management společnosti. 14 respondentů zvolilo variantu „jiná možnost.“ V komentáři k této možnosti pak bylo nejčastěji uvedeno, že přístup k účetním informacím má jednatel společnosti.

Tabulka 37: Subjekty s přístupem k účetním informacím společnosti

Přístupová práva	Počet respondentů	Podíl respondentů
Zaměstnanci účetního oddělení	57	91,9 %
Management společnosti	38	61,3 %
Jiná možnost	14	22,6 %

Zdroj: vlastní zpracování, 2016

Obrázek 25: Subjekty s přístupem k účetním informacím společnosti



Zdroj: vlastní zpracování dle (Survio 2016), 2016

Otázka č. 21: Poskytuje účetní informační systém výsledné reporty (přehledy) ve Vámi požadované struktuře a kvalitě?

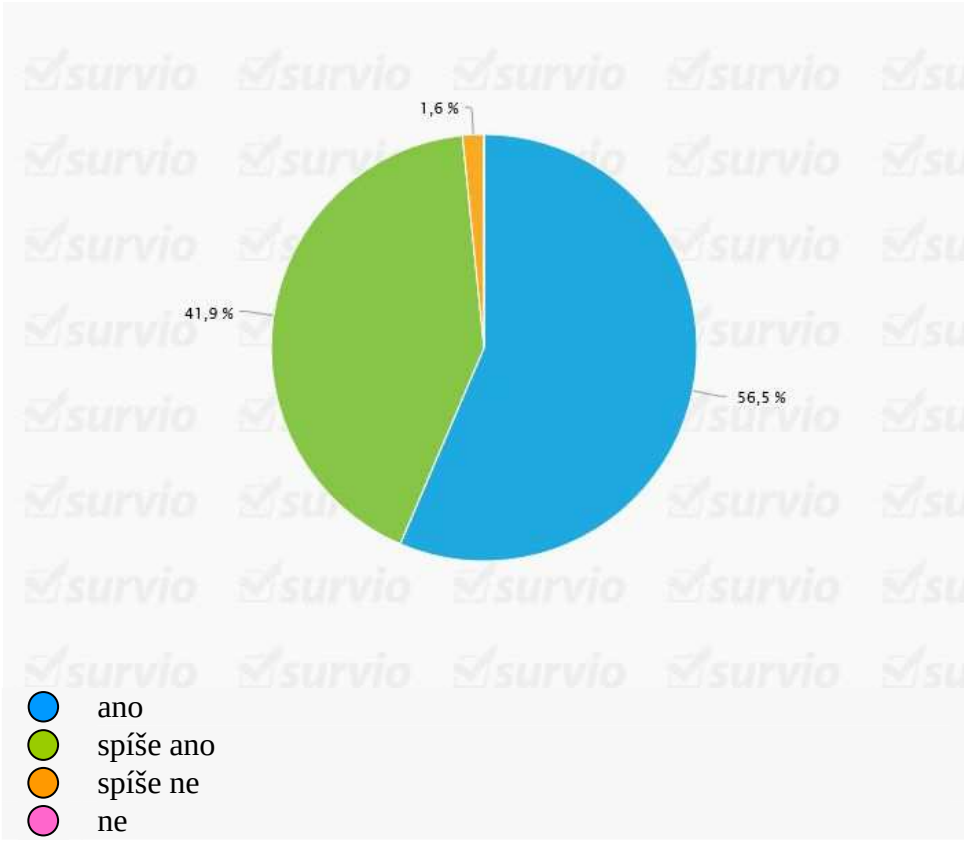
Na otázku, která se týká výsledných reportů sestavovaných prostřednictvím informačního systému, odpovědělo 62 respondentů. Ve většině případů jsou společnosti se strukturou a kvalitou výstupů spokojeni. Nespokojenost projevil jen jeden respondent, který v současné době zvažuje volbu jiného informačního systému.

Tabulka 38: Spokojenost respondentů se strukturou a kvalitou reportů

Informační systém poskytuje reporty v požadované struktuře a kvalitě	Počet respondentů	Podíl respondentů
Ano	35	56,5 %
Spíše ano	26	41,9 %
Spíše ne	1	1,6 %
Ne	0	0 %
Celkem	**62**	**100 %**

Zdroj: vlastní zpracování, 2016

Obrázek 26: Spokojenost respondentů se strukturou a kvalitou reportů



Zdroj: vlastní zpracování dle (Survio 2016), 2016

Otázka č. 22: Splňuje účetní informační systém požadavky na něj kladené?

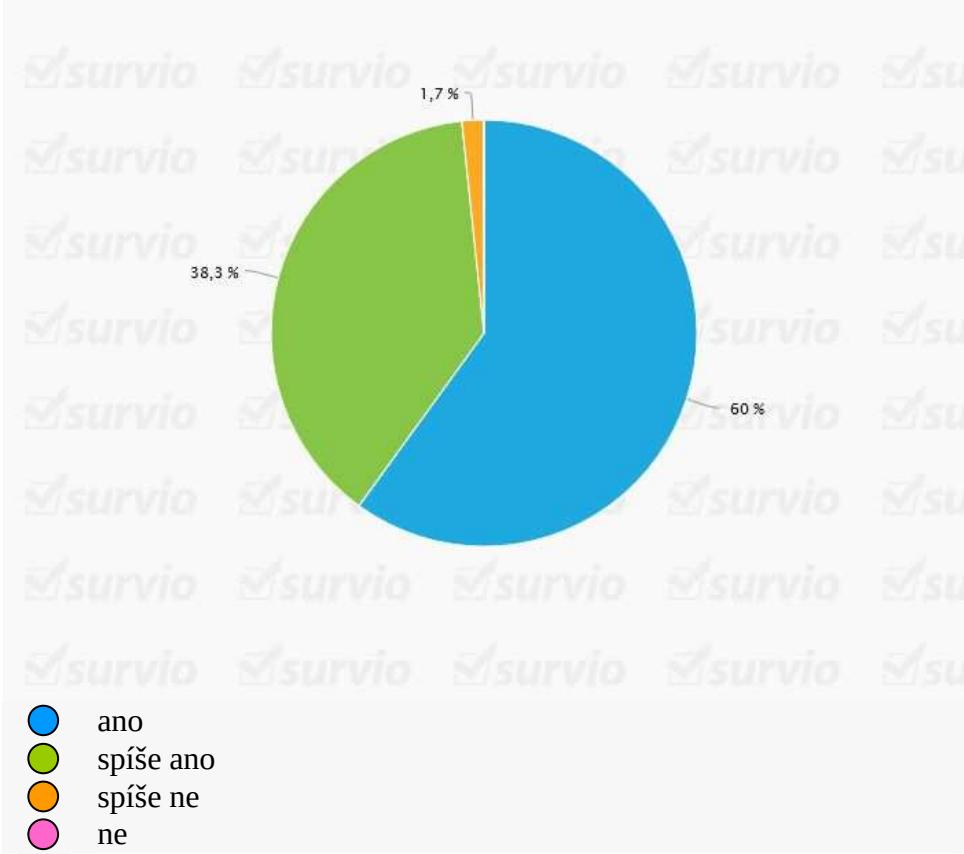
Na výše uvedenou otázku odpovědělo 60 respondentů. Na základě získaných informací lze konstatovat, že většina respondentů je s používaným informačním systémem spokojena. Možnost „spíše ne“ zvolil již zmiňovaný respondent, který do budoucna počítá s výměnou informačního systému.

Tabulka 39: Spokojenost respondentů s informačním systémem

S informačním systémem jsme spokojeni	Počet respondentů	Podíl respondentů
Ano	36	60 %
Spíše ano	23	38,3 %
Spíše ne	1	1,7 %
Ne	0	0%
Celkem	**60**	**100 %**

Zdroj: vlastní zpracování, 2016

Obrázek 27: Spokojenost respondentů s informačním systémem

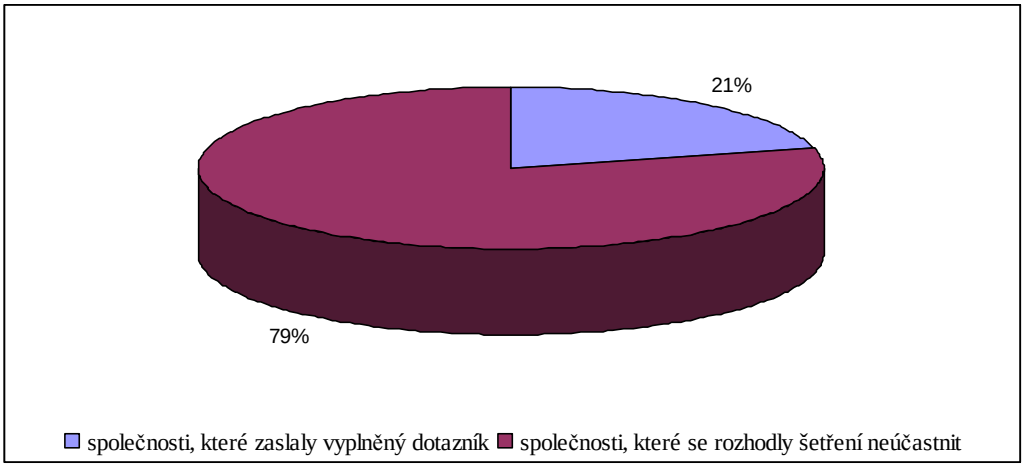


Zdroj: vlastní zpracování dle (Survio 2016), 2016

3.2.3 Hodnocení dotazníkového šetření - závěrečná zpráva

V rámci dotazníkového šetření bylo osloveno 300 podnikatelských subjektů z oblasti západních Čech. Informace spojené s oblastí řízení informačních rizik a informačních systémů poskytlo formou zpět zaslaného dotazníku, vyplněného v různé kvalitě, 63 respondentů. Úspěšnost dotazování je 21 % (všech oslovených společností).

Obrázek 28: Úspěšnost získávání informací v rámci dotazníkového šetření



Zdroj: vlastní zpracování, 2016

Odpovědi na pokládané dotazy považovali zástupci oslovených podnikatelských subjektů za citlivé interní informace. Z tohoto důvodu je počet podniků, jejichž zástupci se rozhodli informace z obavy o jejich zneužití neposkytnout, vysoký.

Prostřednictvím dotazníkového šetření bylo provedeno zhodnocení současného stavu zahrnutí řízení informačních rizik do podnikových procesů vybraných subjektů podnikatelské sféry. S ohledem na existenci tří odlišných přístupů k informačnímu managementu popsaným v rešeršní části této práce (přístup zaměřený zejména na informační a komunikační technologie; přístup zaměřený zejména na informace; přístup zaměřený zejména na lidský faktor) a na stanovený cíl disertační práce, byly otázky uvedené v rozesílaném dotazníku směřovány do čtyř základních okruhů: základní údaje o zkoumaném subjektu, informační systém společnosti obecně, účetní informační systém specificky a řízení informačních rizik. Okruhy však nebyly, s ohledem na zkušenosti z předchozího výzkumu, v dotazníku formálně odděleny.

Základní údaje o zkoumaném subjektu

Na základě odpovědí na otázky z tohoto okruhu bylo možné zjistit, že identifikace skupiny oslovených podnikatelských subjektů proběhla v souladu s nastavenými podmínkami. Oslovené společnosti, které se šetření zúčastnily, působí v oblasti západních Čech, 93,7 % společností má vlastní ekonomické/účetní oddělení a všechny zúčastněné společnosti využívají v rámci podnikových procesů informační systém. Výběr respondentů nebyl omezen předmětem podnikání společnosti. Rozdělíme-li však respondenty podle předmětu podnikání, tvoří nejpočetnější skupinu společnosti, které podnikají v oblastech:

- výroba potravinářských výrobků,
- výroba chemických látek a chemických přípravků,
- specializované stavební činnosti,
- výroba kovových konstrukcí a kovodělných výrobků,
- právní a účetnické činnosti.

Informační systém společnosti obecně

Na základě informací poskytnutých respondenty bylo zjištěno, že je ve sledovaných společnostech věnována dostatečná pozornost technickému vybavení. Informační systém používají všechny sledované společnosti. Ve většině případů se jedná o ERP systém. Mezi informační systémy, které jsou využívány jednotlivými respondenty nejčastěji patří systémy JKR, Money S, QAD a ABRA. 17 respondentů v odpovědi uvedlo, že využívá vlastní informační systém vyvinutý na míru externí softwarovou firmou.

Typ používaného systému je volen s ohledem na tyto faktory (seřazeno sestupně podle uvedené důležitosti):

- dostupnost servisu,
- rychlost práce s daty,
- cena,
- provázanost modulů,

- nastavení uživatelského prostředí,
- kompatibilita IS s jinými systémy,
- reference ostatních uživatelů.

Uvedené řazení jednotlivých faktorů podle významnosti, která je jim přikládána v procesu volby informačního systému, potvrzuje skutečnost, že tento proces stále silně ovlivňuje cena nakupovaného produktu. Přesto je však při výběru vhodného dodavatele kladen důraz nejen na cenu, ale také na služby (zajištění kvalitního a rychlého servisu) dodávané společně s IS. V rámci hodnocení kvality nakupovaného produktu je důraz kladen zejména na rychlost přenosu dat, provázanost modulů IS a nastavení uživatelského prostředí.

Zabezpečení dat, jako jedna z oblastí spojená s řízením informačních rizik, se téměř u všech sledovaných společností omezuje na oblast technického vybavení. Nejčastějším způsobem ochrany dat bylo využití antivirového programu a síťového firewallu. Dalším zabezpečovacím prvkem je zálohování dat. Nejvíce respondentů, uvedlo, že data zálohuje prostřednictvím serveru, následovalo využití jiných záznamových médií (CD, DVD, flashdisc), jiných pevných disků a 7 respondentů uvedlo jako způsob zálohování dat i internetové úložiště. Následuje zabezpečovací prvek, kterým je nastavení omezeného přístupu k informacím poskytovaným informačním systémem. Personální politika společnosti nebyla v rámci šetření jako zabezpečovací prvek uvedena žádnou ze zúčastněných společností.

Správu informačního systému si nadpoloviční většina společností zajišťuje sama prostřednictvím svých vyškolených pracovníků. Zásadní problémy při práci s informačním systémem se u většiny společností nevyskytují, převládá spokojenost s jeho používáním.

Trend zahrnutí sledování lidského faktoru byl potvrzen ve více případech, než tomu bylo u expertních rozhovorů, přesto je tento typ rizik praxí stále nedoceněn. Důvody takového stavu spatřuje autorka v přílišné důvěře respondentů v jimi používaný IS a v lidi, kteří se systémem pracují. Respondenti dotazníkového šetření zřejmě stejně jako společnosti oslovené v rámci expertních rozhovorů mylně předpokládají, že monitoring informačních rizik souvisejících s lidským faktorem není nutný, neboť možné negativní zásahy ze strany zaměstnanců řeší již nastavení podnikového IS.

V podnicích v podmínkách České republiky, resp. západních Čech, v současnosti stále převládá přístup k informačnímu managementu zaměřený zejména na informační a komunikační technologie. Na základě získaných informací však lze usuzovat, že si manažeři začínají uvědomovat nutnost zahrnutí lidského faktoru do pohledu na informační management.

Účetní informační systém specificky

Z informací poskytnutých v rámci dotazníkového šetření vyplynulo, že ve většině společností je v rámci ekonomického/účetního oddělení využíván účetní modul ERP systému. Z důvodu zabezpečení účetních dat mají k modulu přístup jen vybraní zaměstnanci (zaměstnanci účetního oddělení a management společnosti).

Z informací uvedených v dotazníku dále vyplývá, že většina společností je s používaným účetním systémem spokojena. Reporty, které lze prostřednictvím systému vytvářet, splňují bez výhrad předpoklad většiny respondentů (35). 26 respondentů má dle zvoleného typu odpovědi „spíše ano“ drobné výhrady. Nespokojen byl jen jeden respondent, který zvažuje změnu stávajícího informačního systému.

Řízení informačních rizik - Míra zahrnutí informačního managementu mezi podnikové aktivity

S pojmem informační management se již setkala více než polovina respondentů. 12 z nich informační management aktivně využívá. V několika málo případech byla uvedena i využívaná metodika řízení informačních rizik. 79,7 % respondentů uvedlo, že s informačními riziky pracuje intuitivně, bez využití jakékoli standardní metodiky pro jejich řízení. Nejčastěji jsou v zúčastněných společnostech sledována rizika spojená s informačními a komunikačními technologiemi. Společnosti, které informační management nevyužívají ve většině případů neplánují tuto situaci v budoucnu měnit.

Informační rizika identifikovaná v rámci kvantitativního šetření

Rizika, se kterými se sledované společnosti v rámci podnikových procesů setkávají, jsou uvedena v následující tabulce. Rizika byla identifikována v rámci provedeného dotazníkového šetření.

Tabulka 40: Informační rizika identifikovaná v rámci kvantitativního šetření

Typ rizika	Popis rizika	Poznámka
Rizika spojená s ICT - s informačním systémem společnosti	Selhání software.	Riziko identifikováno v rámci otázky č. 22, připadá v úvahu u 40 % respondentů.
	Rizika spojená se zabezpečením dat.	Riziko identifikováno v rámci otázky č. 11, prevenci rizika (zabezpečení dat) uvádí cca 95 % respondentů.
	Neautorizovaný přístup k IS. (omezení přístupových práv)	Riziko identifikováno v rámci otázek č. 19 a 20, omezení přístupových práv k IS podle odpovědnosti uvedlo 95 % respondentů.
	Nesoulad mezi požadavky na poskytované výstupy a reálně poskytovanými výstupy.	Riziko identifikováno v rámci otázky č. 21, připadá v úvahu u 43,5 % respondentů.
	Rizika plynoucí ze správy IS externím subjektem.	Riziko identifikováno v rámci otázky č. 13, připadá v úvahu u 46 % respondentů.
Rizika spojená s informacemi	Ztráta, modifikace nebo poškození dat během jejich zpracování a uchovávání vlastním účetním oddělením.	Riziko identifikováno v rámci otázek č. 12 a 14, prevenci rizika provádí různými způsoby 93,7 % respondentů.
	Ztráta, modifikace nebo poškození dat během jejich zpracování a uchovávání externí společností. (outsourcing)	Riziko identifikováno v rámci otázek č. 12, 14 a 15, prevenci rizika provádí různými způsoby 6,3 % respondentů.
Rizika spojená s lidským faktorem	Neúmyslná a úmyslná modifikace dat. (chybný zápis, záměrná modifikace dat)	Riziko identifikováno v rámci otázky č. 6, počet respondentů, u kterých se může vyskytnout - 48.
	Ztráta důvěrnosti dat, únik informací, krádež dat.	Riziko identifikováno v rámci otázek č. 14, 16 a 19.

Zdroj: vlastní zpracování, 2016

3.2.4 Shrnutí

Tato část práce sumarizuje a hodnotí informace získané prostřednictvím dotazníkového šetření. Osloveno bylo 300 podnikatelských subjektů. Požadované informace bylo ochotno poskytnout 63 respondentů.

Aby bylo možné zhodnotit současný stav zahrnutí řízení informačních rizik do podnikových procesů u vybraných subjektů podnikatelské sféry, byly otázky uvedené v rozesílaném dotazníku směřovány do čtyř základních okruhů: základní údaje o zkoumaném subjektu, informační systém společnosti obecně, účetní informační systém specificky a řízení informačních rizik. Okruhy nebyly, s ohledem na zkušenosti z předchozího výzkumu, v dotazníku formálně odděleny. Na základě informací poskytnutých respondenty bylo zjištěno, že je ve sledovaných společnostech věnována dostatečná pozornost rizikům spojeným s technickým vybavením, informační rizika spojená se selháním lidského faktoru buď nejsou řešena vůbec, nebo jsou řešena v omezené míře. Identifikovaná rizika sumarizuje tabulka číslo 40.

V MSP v podmínkách České republiky, resp. západních Čech, v současnosti stále převládá přístup k informačnímu managementu zaměřený zejména na informační a komunikační technologie. Společnosti řídí informační rizika i rizika obecně spíše intuitivním způsobem, bez hlubší znalosti metodik používaných pro řízení rizik.

4. Návrhy opatření a doporučení, která by napomohla zefektivnění práce s informacemi a informačními riziky

S ohledem na informace získané prostřednictvím šetření popsaných v kapitole 3, je možné tvrdit, že většina sledovaných společností provádí analýzu rizik a do svých podnikových aktivit včleňuje prvky informačního managementu. Jedná se o přístup k informačnímu managementu zaměřený zejména na ICT. Pouze malé množství sledovaných podniků (v rámci expertních rozhovorů jen 2) uvádí informace, z nichž je možné usuzovat na přístup k informačnímu managementu zaměřený zejména na informace s přesahem do přístupu k informačnímu managementu zaměřenému zejména na lidský faktor. Názvosloví informačního managementu není respondenty využíváno, převládá spíše intuitivní charakter prováděných činností spadajících do informačního managementu bez hlubší znalosti teoretických souvislostí.

V rámci expertních rozhovorů byli zástupci sledovaných podnikatelských subjektů seznámeni s legislativním a normativním rámcem pro řízení rizik v oblasti účetnictví, zejména s normami:

- ČSN ISO 31000, která zahrnuje obecný popis metodiky pro řízení rizik,
- ČSN 36 9790, ve které jsou, spolu s popisem metodiky pro hodnocení informačních rizik, uvedeny i příklady rizik, se kterými se lze v podnikové praxi setkat, způsob výpočtu rizika a sestavení matice rizik.

Uvedené normy poskytují návody a rady pro podporu implementace managementu rizik v podnikových procesech. Metoda implementace systému řízení rizik je detailněji popsána ve druhé kapitole disertační práce, v části 2.3.3 Proces řízení rizik.

S ohledem na zjištění plynoucí z obou provedených šetření, byla navržena následující opatření a doporučení, která by napomohla budoucímu zefektivnění práce s informacemi a informačními riziky v rámci procesů (zejména procesů, které jsou v kompetenci účetních/ekonomických oddělení) organizace:

- Seriózně se začít možností řízení informačních rizik zabývat:
    - seznámit se s normativním rámcem pro řízení rizik,
    - seznámit se s metodikami hodnocení informačních rizik,
    - zvolit metodiku nejvhodnější pro danou společnost,

    - postupovat podle zvolené metodiky s ohledem na možné odchylky způsobené zaměřením podnikatelských aktivit společnosti.

- Rozdělit hodnocení informačních rizik do dvou skupin:
    - rizika spojená s ICT,
    - rizika spojená s lidskými zdroji.
- Sestavit a pravidelně aktualizovat seznam rizik pro obě uvedené skupiny rizik.
- Zhodnotit dopady rizik do podnikových aktivit.
- Nastavit podnikové procesy tak, aby se rizika nevyskytovala, nebo aby se alespoň minimalizoval jejich dopad do podnikových aktivit.
- Zbavit se představy, že nastavení IS zabrání vzniku všech rizik spojených s lidským faktorem.
- Uvědomit si, že rizika spojená s lidským faktorem se mohou objevit i přes kvalitně nastavenou personální politiku, protože tento typ rizik nesouvisí pouze s charakterovými vlastnostmi zaměstnanců.
- Nastavit zpracování informací v ekonomickém/účetním oddělení tak, aby se předešlo jejich ztrátě nebo nechtěné modifikaci:
    - proškolení zaměstnanců,
    - nastavení omezeného přístupu k datům dle odpovědnosti zaměstnance,
    - optimální nastavení způsobu zadávání účetních informací do IS (stanovení odpovědných zaměstnanců).
- Sledovat trendy v oblasti řízení podnikových rizik a přizpůsobovat jim systém řízení rizik zavedený v konkrétní organizaci.

5. Dosažení cílů a zhodnocení přínosů disertační práce

Problematika řešená v rámci disertační práce je velmi obsáhlá. Zasahuje do oblastí systémové analýzy, informatiky a informačního managementu a informačních a komunikačních technologií. Cílem disertační práce je analyzovat současný stav řízení informačních rizik, která se mohou vyskytnout v rámci podnikových procesů spadajících do kompetence ekonomických/účetních oddělení zvolených podnikatelských subjektů a navrhnout doporučení pro minimalizaci takových rizik. Za účelem naplnění stanoveného cíle byly využity informace ze dvou po sobě probíhajících šetření, z expertních rozhovorů a dotazníkového šetření.

V rámci obou provedených šetření byl potvrzen předpoklad nízké úrovně zahrnutí řízení informačních rizik do podnikových aktivit sledovaných podnikatelských subjektů. Prostřednictvím šetření byly ověřovány a potvrzeny hypotézy stanovené v úvodu práce:

1) Většina sledovaných společností pod pojmem informačním management vnímá především informační a komunikační technologie a nevěnuje pozornost dalším okruhům, které patří do informačního managementu.
2) Více než polovina sledovaných společností se již setkala s pojmem informační management.
3) Informačním rizikům spojeným s lidským faktorem věnuje maximální pozornost jen malé množství sledovaných společností.

Výsledky šetření vedoucí k potvrzení stanovených hypotéz:

ad1) V rámci expertních rozhovorů uvedli všichni respondenti informace o technickém zabezpečení přenosu a ukládání dat. Popsali používaný HW a SW. Získané informace naznačující orientaci podniků na informační management zaměřený na informace s přesahem k zaměření na lidský faktor poskytli pouze dva zástupci sledovaných subjektů.

V rámci dotazníkového šetření byly společnostmi primárně uváděny informace o technickém zajištění přenosu a ukládání dat. V rámci otázky číslo 5 uvedlo 47 respondentů (79,7 %) využití intuitivního postupu v rámci řízení rizik. Jen 5 respondentů (10,2 %) uvedlo užití normy ČSN 36 9790 - Systém managementu bezpečnosti informací. Otázka číslo 6 poukázala na skutečnost, že nejvíce sledovanými riziky jsou rizika spojená s informačními technologiemi

a informacemi. U rizik spojených s lidským faktorem byla nejčastěji volena možnost „rizika jsou sledována“, současně byl však v tomto případě zaznamenán i nejvyšší počet odpovědí „rizika nesledujeme.“

ad2) V rámci expertních rozhovorů uvedlo znalost informačního managementu jedenáct z patnácti respondentů. V dotazníkovém šetření byla tato hypotéza ověřena zejména otázkou číslo 3, u které 50 respondentů (79,4 %) zvolilo možnost „Znám pojem informační management“.

ad3) V rámci expertních rozhovorů uvedli pouze dva respondenti informace, z nichž lze usuzovat, že je ve společnosti kladen důraz na hodnocení rizik spojených s lidským faktorem. Dotazníkové šetření tuto hypotézu potvrdilo prostřednictvím otázky číslo 6, která prokazuje nejvyšší sledovanost u rizik spojených s informačními technologiemi a nejnižší u rizik spojených s lidským faktorem.

5.1 Přínos práce pro rozvoj vědy a výzkumu

Předkládaná disertační práce přispívá k rozvoji vědy a výzkumu zejména následujícími skutečnostmi.

Práce nabízí ucelený přehled studované problematiky, uvádí detailní charakteristiku:

- nastavení účetních procesů ve společnosti, s ohledem na dodržení normativního rámce pro řízení rizik a platného legislativního rámce současného českého účetnictví,
- systémových přístupů k podnikovým procesům,
- ERP systémů a jejich využití v prostředí českých podniků,
- informací a přístupů k jejich využití,
- informačních rizik a procesu jejich řízení,
- informačního managementu a přístupů k němu.

Podrobně provedená rešerše zahraničních a českých zdrojů umožňuje identifikaci a explikaci pojmů, jako jsou například manažerské procesy, podpůrné procesy, business intelligence (BI), ekonomické ERP systémy, informační rizika a informační management.

Disertační práce popisuje možnost využití metody identifikace procesů a rizik (IPR) s ohledem na přístup k informačnímu managementu vycházející z definice: “Informační management představuje veškeré aktivity spojené s řízením informací v rámci všech standardních i nestandardních procesů, probíhajících v rámci činností zajišťovaných podnikatelskými subjekty nebo subjekty pohybujícími se ve veřejné sféře, za účelem vytváření přidané hodnoty pro danou organizaci, pro společnosti, které s touto organizací spolupracují i pro její zákazníky. Je postaven na třech pilířích, kterými jsou lidé, technologie a procesy.“

Dalším z přínosů práce z hlediska rozvoje vědy a výzkumu jsou výsledky expertních rozhovorů a dotazníkového šetření na téma „Řízení informačních rizik v organizaci“, které poukazují na nedostatky v současném způsobu využívání řízení informačních rizik v rámci podnikových procesů a možnosti zlepšení práce s informacemi a s nimi souvisejícími riziky v případě nastavení podmínek pro zavedení principů daných normativním rámcem pro řízení rizik, resp. normou ČSN 36 9790 a v ní uvedenou metodikou IPR.

Disertační práce a její dílčí části publikované na mezinárodních vědeckých konferencích a v odborných časopisech mohou inspirovat vědecké pracovníky k dalšímu výzkumu v dané oblasti.

5.2 Přínos práce pro praxi

V praxi využitelným výstupem jsou návrhy opatření a doporučení, která by napomohla budoucímu zefektivnění práce s informacemi a informačními riziky v oblasti účetnictví, uvedené v kapitole „Návrhy opatření a doporučení, která by napomohla zefektivnění práce s informacemi a informačními riziky“.

Oba prováděné výzkumy pomohly zvýšit povědomí společností o informačním managementu a možnostech, které nabízí v oblasti řízení rizik podnikatelských subjektů. V rámci expertních rozhovorů byli respondenti obeznámeni s legislativním a normativním rámcem pro řízení rizik a s metodikou IPR. První krok uvedené metodiky, analýzu rizik, měli někteří respondenti možnost zjednodušenou formou vyzkoušet.

Závěr

Předkládaná disertační práce se zabývá problematikou informačních rizik a jejich řízení. Cílem práce je analyzovat současný stav řízení informačních rizik, která se mohou vyskytnout v rámci podnikových procesů spadajících do kompetence ekonomických/účetních oddělení zvolených podnikatelských subjektů a navrhnout doporučení pro minimalizaci takových rizik.

Práce je rozdělena do dvou částí, které jsou propojeny prostřednictvím použitých případových studií. Rešeršní část zpracovává vybranou část studované problematiky. Zahrnuje poznatky z oblastí, jakými jsou například podnikové procesy a jejich nastavení, systémové přístupy k podnikovým procesům, informační systémy v podnikové praxi, využití informací, informační rizika a proces jejich řízení a informační management, získané studiem zahraniční i české literatury. Na základě studia dostupných podkladů, které se zabývají informačním managementem je autorkou specifikován způsob využití definice informačního managementu v oblasti řízení informačních rizik ekonomického/účetního oddělení společnosti. V rámci rešeršní části práce jsou dále diskutovány souvislosti efektivního řízení informačních rizik a bezproblémového zajištění operací v rámci účetního systému podniku. K dokreslení celé problematiky jsou použity případové studie mapující situaci v oblasti řízení rizik v ekonomickém oddělení výrobní společnosti.

Aplikační část se zabývá studiem míry zahrnutí řízení informačních rizik do podnikových procesů spadajících do kompetence ekonomických/účetních oddělení sledovaných podnikatelských subjektů. Hodnocení uvedené problematiky je provedeno v rámci kvalitativního výzkumu zaměřeného na sledování řízení rizik v rámci ekonomických/účetních oddělení malých a středních podniků různého oborového zaměření, které sídlí v oblasti západních Čech a dotazníkového šetření v rámci skupiny respondentů blíže specifikované v kapitole 3.2 Dotazníkové šetření. Výsledky obou šetření jsou popsány prostřednictvím závěrečných zpráv, na jejichž základě jsou navržena opatření a doporučení, která by pomohla zefektivnit řízení informačních rizik v rámci ekonomických/účetních oddělení sledovaných společností.

Vlastní publikace autorky

Příspěvky v odborných časopisech

Černá, M. (2014). Aspects of Information management in context with IS selection by SME. *Procedia Engineering*, 6(69), 745-750.

Černá, M. (2013). Requirements engineering. *Trendy v Podnikání – Business* Trends, 3(1), 42-48.

Statě ve sborníku

Černá, M., & Zborková, J. (2015). Effects of ERP System Implementation to the Soft Drinks Producer´s Sales Department Processes. In K. S. Soliman (Ed.), *Proceedings of the 26th International Business Information Management Association Conference 2015* (s. 1662-1670). Madrid: IBIMA.

Hinke, J., & Černá, M., & Zborková, J. (2015). Social and Economic Aspects of the Limited Availability of Preschool Education in the Czech Republic. In K. S. Soliman (Ed.), *Proceedings of the 25th International Business Information Management Association Conference 2015* (s. 1490-1503). Amsterdam: IBIMA.

Černá, M., & Zborková, J., & Vallišová, L. (2014). Strategic Planning of Klatovy Town in the Area of Education. In L. Čechurová & M. Jiřincová (Eds.), *Sborník příspěvků mezinárodní vědecké konference Trendy v podnikání 2014* (s. 1-7). Plzeň: ZČU v Plzni.

Hinke, J., & Černá, M., & Zborková, J. (2014). The Methodology of Sustainable Business Performance Indicators Determination. In K. S. Soliman (Ed.), *Proceedings of the 23rd International Business Information Management Association Conference 2014* (s. 1033-1047). Valencia: IBIMA.

Hinke, J., & Černá, M., & Zborková, J. (2014). Trends and Management of Private Preschool Education in Conditions of the Czech Republic. In K. S. Soliman (Ed.), *Proceedings of the 23rd International Business Information Management Association Conference 2014* (s.1024-1032). Valencia: IBIMA.

Černá, M. (2013). Aspekty řízení inovací v kontextu ekonomického řízení příspěvkové organizace. In K. Mičudová (Ed.), *Sborník příspěvků mezinárodní vědecké konference Trendy v podnikání 2013* (s. 44-50). Plzeň: ZČU v Plzni.

Černá, M. (2013). Innovation for Competitiveness – Sole Trader in the Construction Sector. In A. Kocourek (Ed.), *Proceedings of the 11th International Conference Liberec Economic Forum 2013 (LEF 2013)* (s. 94-103). Liberec: Technical University of Liberec.

Černá, M. (2012). Information Risks and Their Connection With Accounting. In T. Nagle (Ed.), *Proceedings of the 6th European Conference on Information Management and Evaluation (ECIME 2012)* (s. 375-382). Cork, Ireland: Academic Publishing International Limited.

Černá, M. (2012). Risk, information and their management. In J. Ircingová & J. Tlučhoř (Eds.), *Sborník příspěvků mezinárodní vědecké konference Trendy v podnikání 2012* (s. 1-5). Plzeň: ZČU v Plzni.

Černá, M. (2011). Rizika, informace a úloha komunikace. In M. Horová (Ed.), *Trendy v podnikání 2011. Recenzovaný sborník příspěvků mezinárodní vědecké konference* (s. 1-5). Plzeň: ZČU v Plzni.

Černá, M. (2009). Information Management. In M. Barták (Ed.), *Finance a management v teorii a praxi (sborník příspěvků z konference)* (s. 56-57). Ústí nad Labem: Univerzita J. E. Purkyně.

Černá, M. (2009). Information management. In A. Bodnárová (Ed.), *IMEA 2009* (s. 45-47). Hradec Králové: Univerzita Hradec Králové.

Černá, M. (2009). Informační management – řízení rizik. In K. Křikač & B. Šimek (Eds.), *Vzdělání a ekonomika jako hlavní determinanty hospodářského růstu* (s. 19-22). Plzeň: ZČU v Plzni.

Učební texty, skripta

Kopek, R., & Černá, M., & Plachá, D. (2009). *Účetnictví podnikatelů pro distanční studium I.* Plzeň: ZČU v Plzni.

Kopek, R., & Černá, M. (2008). *Účetnictví podnikatelů pro distanční studium II.* Plzeň: ZČU v Plzni.

Seznam použité literatury

AIIM (2014). *What is information management?* Cit. 07.04.2014, dostupné z: http://www.aiim.org/what-is-information-management

Bejček, M., Čejp, V., & Vystavěl, R., & Katolický, A. (2007). *Inovace a ICT*. Praha: VŠMIE.

Best, D. (1996). *The Fourth Resource. Information and its Management.* UK, Aldershot: Aslib Gover.

Blaha, Z. S. (2004). *Řízení rizika a finanční inženýrství.* Praha: Management Press.

Boehm, V. (1998). Informační zdroje. *Českomoravský profit, 9(4), 5*.

British Bankers' Association, International Swaps and Derivatives Association, & PricewaterhouseCoopers, & RMA. (1999). *Operational Risk: The Next Frontier*. New York: BBA, ISDA, PWC, RMA.

Brown, R. (2004). *History of Accounting and Accountants.* USA, New York: Cosimo Books Inc.

Brož, I. (1997). Management na rozcestí. *Moderní řízení*, 32(2), 4-5.

Brožová, H., & Houška, M. (2011). *Modelování znalostí.* Příbram: Professional Publishing.

Březinová, H., & Munzar, V. (2006). *Účetnictví I.* Praha: Institut Svazu účetních.

Burk, C. F., & Horton, F. W. Jr. (1991). *Infomap: A Complete Guide to Discovering Corporate Information Sources.* Englewood Cliffs, NJ: Information Management Press.

Cejpek, J. (2005). *Informace, komunikace a myšlení.* Praha: Karolinum.

Ceruzzi, P. E. (2003). *A History of Modern Computing (History of Computing).* UK: The MIT Press.

Columbus, L. (2014). *Gartner's ERP Market Share Update Shows The Future of Cloud ERP IS Now.* Cit. 05.09.2014, dostupné z: http://www.forbes.com/sites/louiscolumbus/2014/05/12/gartners-erp-market-share-update-shows-the-future-of-cloud-erp-is-now/

Čermák, M. (2007). *Řízení informačních rizik v praxi.* Praha: DRAFT.

ČSÚ (2014). *Šetření o využívání ICT v podnikatelském sektoru. (ICT 5-01).* Cit. 08.05.2015, dostupné z: http://www.czso.cz

Daněk, R. (2007). Úvod do řízení rizik. *Ekonom*, 11(28), 5.

Day, R. E. (2008). *The Modern Invention of Information. Discourse, History and Power.* USA: Southern Illinois University.

Dehnashi, A. (2010). *Information Management.* Cit. 09.04.2014, dostupné z: http://dehnashi.com/technology.html

Dias, C. (2001). Corporate portals: a literature review of a new concept in Information Management. *International Journal of Information Management*, 21(4), 269-287.

Doctorandus (2013). *Vědecké metody ve společenských vědách.* Cit. 05.09.2013, dostupné z: http://www.doctorandus.info/info/e_kapitoly/vedecke_metody.doc

Dolejšová, M. (2006). *Vnitřní kontrolní systém v účetnictví.* Cit. 09.02.2014, dostupné z: http://www.cvis.cz/hlavni.php?stranka=novinky/clanek.php&id=427

Doucek, P. (2010). *Informační Management.* Příbram: Professional Publishing.

Doucek, P. (2004). *Řízení projektů informačních systémů.* Praha: Mařík.

Dresner, H. (2015). *Business intelligence.* Cit. 09.04.2015, dostupné z: http://www.dresneradvisory.com/

Drucker, P. F. (1993). The Rise of the Knowledge Society. *The Wilson Quarterly*, 17(2), 52-71.

Edmunds, A., & Morris, A. (2000). The problem of information overload in business organisations: a review of the literature. *International Journal of Information Management*, 20(1), 17-28.

European Commission (2003). *Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises. Official Journal of the European Union L124/36.* Cit. 25.01.2015, dostupné z: http://ec.europa.eu/enterprise/policies/sme/files/sme_definition/sme_user_guide_en.pdf

Fiala, J. (1935). *Dějiny účetnictví.* Praha: Pragotisk, Peroutka a spol.

Foddy, W. (1995). *Constructing Questions for Interviews and Questionnaires (Theory and Practice in Social Research).* Cambridge: Cambridge University Press.

Franks, P. C. (2013). *Records and Information Management.* USA: American Library Association.

Gantz, S. D., & Philpott, D. R. (2012). *FISMA and the Risk Management Framework. The New Practice of Federal Cyber Security.* USA: Newnes.

Garlick, A. (2007). *Estimating risk. A management approach.* Hampshire: Gower.

Government of Western Australia (2012). *Information Management Framework.* Cit. 13.04.2014, dostupné z: https://integratedplanning.dlg.wa.gov.au/InfoManagement Framework.aspx

Grabot, B., & Mayère, A., & Bazet, I. (2008). *ERP systems and organizational change.* London: Springer.

Hanani, U., & Shapira, B., & Shoval, P. (2001). Information Filtering: Overview of Issues, Research and systems. *User Modeling and User-adapted Interaction,* 11(3), 203-259.

Hendl, J. (2006). *Kvalitativní výzkum v pedagogice.* Cit. 31.01.2014, dostupné z: http://www.ftvs.cuni.cz/hendl/metodologie/kvalvyzkpedhendl.pdf

Hicks, B. J. (2007). Lean information management: Understanding and eliminating waste. *International Journal of Information Management,* 27(4), 233-249.

Chatfield, M., & Vangermeersch, R. (2014). *History of Accounting: An International Encyclopedia.* USA, New York: Routledge.

Chessel, M., & Smith, H. C. (2013). *Patterns of Information Management.* USA: IBM Press.

Childs, C. W. (1901). *New essentials of book-keeping.* USA, San Francisco: The Whitaker & Ray Co.

IBM Corporation (2013). *Federació Farmacèutica (FedeFarma) - Case Study.* Cit. 16.11.2013, dostupné z: http://www-01.ibm.com/software/success/cssdb.nsf/CS/JHUN-988TGU?OpenDocument&Site=default&cty=en_us

Imler, K. (2008). *Strategické systémy kvality.* Pardubice: Lévay.

InfoReady (2014). *Expert Information Management.* Cit. 09.04.2014, dostupné z: http://www.infoready.com.au/about-us/expert-information-management/

International Organization for Standardization. (2011). *ISO/IEC 27005:2011. Information technology - Security techniques - Information security risk management.* Geneva: International Organization for Standardization.

International Organization for Standardization. (2009). *IEC/ISO 31010:2009. Risk management - Risk assessment techniques.* Geneva: International Organization for Standardization.

International Organization for Standardization. (2009). *ISO 31000:2009. Risk management - Principles and guidelines.* Geneva: International Organization for Standardization.

International Organization for Standardization. (2009). *ISO Guide 73:2009. Risk management - Vocabulary.* Geneva: International Organization for Standardization.

International Organization for Standardization. (2005). *ISO/IEC 17799:2005. Information technology. Security techniques. Code of practice for information security management.* Geneva: International Organization for Standardization.

International Organization for Standardization. (2005). *ISO 9000. Quality management systems.* Geneva: International Organization for Standardization.

International Organization for Standardization. (2004). *ISO/IEC 13335-1:2004. Information technology - Security techniques - Management of information and communications technology security - Part 1: Concepts and models for information and communications technology security management.* Geneva: International Organization for Standardization.

Jirásek, A. J. (2008). *Management budoucnosti.* Praha: Professional Publishing.

JKR (2014). *J.K.R. spol. s r.o.* Cit. 05.01.2014, dostupné z: http://www.jkr.cz/

Johnson, E. M. (2009). *Managing Information Risk and the Economics of Security.* USA: Springer.

Kaplan, R., & Mikes, A. (2012). *Managing Risks: A New Framework.* Cit. 14.01.2015, dostupné z: https://hbr.org/2012/06/managing-risks-a-new-framework

Knox, J. (2013). *A Brief Definition and History of Information Management.* Cit. 08.04.2014, dostupné z: http://speakerknox.wordpress.com/2013/05/21/a-brief-definition-and-history-of-information-management/

Komora auditorů České republiky (KAČR) (2015). *České účetnictví.* Cit. 16.03.2015, dostupné z: http://www.kacr.cz/ceske-ucetnictvi

Komora auditorů České republiky (KAČR) (2014). *ISA 315.* Cit. 05.01.2014, dostupné z: www.kacr.cz/data/pdf/auditorske_standardy/ISA315.pdf

Korecký, M., & Trkovský, V. (2011). *Management rizik projektů se zaměřením na projekty v průmyslových podnicích.* Praha: Grada.

Kruliš, J. (2011). *Jak vítězit nad riziky. Aktivní management rizik – nástroj řízení úspěšných firem.* Praha: Linde.

K2 (2015). *K2 atmitec s.r.o.* Cit. 15.09.2015, Dostupné z: http://www.k2.cz/

Lam, J. (2003). *Enterprise Risk Management. From Incentives to Controls.* USA, Hoboken, New Jersey: John Wiley & Sons Inc.

Laplante, A. P. (2009). *Requirements Engineering for Software and Systems (Applied Software Engineering Series).* USA: Auerbach Publications.

Lauwers, L., & Willekens, M. (1994). Five Hundred Years of Bookkeeping - A portrait of Luca Pacioli. *Tijdschrift voor Ekonomie en Management,* 39(3), 289-304.

Martin, W. J. (1995). *The Global Information Society.* Aldershot: Aslib Gover.

McMahon, Ch., & Lowe, A., & Culley, S. (2004). Knowledge management in engineering design: personalization and codification. *Journal of Engineering design,* 15(4), 307-325.

McNeil, A. J., & Rüdiger, F., & Embrechts, P. (2005). *Quantitative Risk Management. Concepts, Techniques, Tools.* USA: Princeton University Press.

Merna, T., & Faisal, F. A. T. (2007). *Risk Management (Řízení rizika ve firmě.).* Brno: Computer Press.

Ministerstvo financí České republiky (MFČR) (2015a). *Seznam CZ - NACE.* Cit. 16.07.2015, dostupné z: http://wwwinfo.mfcr.cz/ares/nace/ares_nace.html.cz

Ministerstvo financí České republiky (MFČR) (2015b). *Právní rámce.* Cit. 16.03.2015, dostupné z: http://www.mfcr.cz/cs/verejny-sektor/regulace/ucetnictvi/pravni-ramce

Ministerstvo financí České republiky. (1991). *Zákon č. 563/1991 Sb. o účetnictví.* Praha: MFČR.

Molnár, Z. (2000). *Efektivnost informačních systémů.* Praha: Grada.

Monk, E., & Wagner, B. (2013). *Concepts in Enterprise Resource Planning.* Boston: Course Technology.

Morabito, V. (2013). *An Information Management Approach Emphasizing on the "I" in IT.* Berlin: Springer - Verlag.

Morozov, E. (2011). *The Net Delusion: The Dark Side of Internet Freedom.* USA: Public Affairs.

Morton, S. M. S. (1991). *Corporation of the 1990s - Information Technology and Organizational Transformation.* New York: Oxford university Press.

Novotný, O., & Pour, J., & Slánský, D. (2005). *Business Intelligence. Jak využít bohatství ve vašich datech?* Praha: Grada.

O'Connor, N. G., & Martinsons, M. G. (2006). Management of information systems: Insights from accounting research. *Information & Management*, 43(8), 1014-1024.

Olson, A. (2008). *The 6 phases of any business software implementation.* USA: PC Bennett Solutions.

Osamu, K. (1995). *Accounting History.* Japan, Osaka: A. N. Ofset Co. Ltd.

Panorama Consulting Solutions (2014). *Industry Reports.* Cit. 30.10.2014, dostupné z: http://panorama-consulting.com/resource-center/erp-industry-reports/

Pavelka, F., & Klímek, P. (2000). *Aplikovaná statistika.* Zlín: VÚT.

Petříková, R. (2010). *Moderní management znalostí.* Praha: Professional Publishing.

Prokůpková, D. (2007). Řízení rizik v orgánech veřejné správy. *Účetnictví neziskového sektoru (UNES), 4*(2). Dostupné z: http://www.ucetnikavarna.cz/archiv/dokument/doc-d8966v11782-analyza-a-rizeni-rizik/?search_query=$index=194

Public Works and Government Services Canada (2014). *Information Management - Knowledge Area.* Cit. 09.04.2014, dostupné z: http://www.tpsgc-pwgsc.gc.ca/biens-property/sngp-npms/ti-it/conn-know/gi-im-eng.html

QAD (2015). *Minerva Česká republika, a.s.* Cit. 15.09.2015, dostupné z: http://www.minerva-is.eu/

Raulich, H. (1922). *Příspěvek k dějinám účetnictví.* ČR, Uherské Hradiště: Knihtiskárna K. Novotného.

Renganathan, V., & Babu, A. N., & Sarbadhikari, S. N. (2013). A tutorial on Information Filtering Concepts and Methods for Bio-medical Searching. *Health & Medical Informatics,* 4(3), 100131-100136.

Renn, O., & Aven, T. (2010). *Risk Management and Governance. Concepts, Guidelines and Applications.* Germany: Springer-Verlag.

Robertson, J. (2005). *10 principles of effective information management.* Cit. 07.04.2014, dostupné z: http://www.steptwo.com.au/papers/kmc_effectiveim/index.html

SAP (2014). *Enterprise Resource Planning - SAP.* Cit. 01.10.2014, dostupné z: http://www.sap.com/pc/bp/erp.html

SAP ČR (2014). *The Best-Run Businesses Run SAP.* Cit. 01.10.2014, dostupné z: http://www.sap.com/cz/index.html

Savolainen, R. (2007). Filtering and withdrawing: strategies for coping with information overload in everyday contexts. *Journal of Information Science,* 33(5), 611-621.

Smejkal, V., & Rais, K. (2006). *Řízení rizik ve firmách a jiných organizacích.* Praha: Grada.

Sodomka, P. (2006). *Informační systémy v podnikové praxi.* Brno: Computer Press.

Sodomka, P., & Klčová, H. (2010). *Český ERP trh a jeho vývoj v období hospodářské krize.* Cit. 12.09.2014, dostupné z: http://www.cssi.cz/cssi/cesky-erp-trh-jeho-vyvoj-v-obdobi-hospodarske-krize

Sodomka, P., & Klčová, H., & Vořechová, E. (2008). *Aktuální trendy vývoje českého ERP trhu.* Cit. 08.09.2014, dostupné z: http://www.cvis.cz

Sokolowsky, P. (2002a). *Informační požadavky moderního podniku. 1. část.* Praha: Karolinum.

Sokolowsky, P. (2002b). *Organizace a management podnikového zpracování informací. 2. část.* Praha: Karolinum.

Spanos, Y. E., & Prastacos, G. P., & Poulymenakou, A. (2002). The relationship between information and communication technologies adoption and management. *Information & Management,* 39(8), 659-675.

Statista (2014). *Global market share held by the leading enterprise resource planning software companies.* Cit. 12.09.2014, dostupné z: http://www.statista.com/statistics/249637/erp-software-market-share-by-company/

Stebbins, R. A. (2001). *Exploratory Research in the Social Sciences.* USA: SAGE Publications, Inc.

Steiner, F. (2007). *Případová studie analýzy rizik informační bezpečnosti.* Cit. 12.10.2013, dostupné z: http://bpm-tema.blogspot.cz/2007/11/ppadov-studie-analzy-rizik-informan.html

Stonebumer, G., & Goguen, A., & Feringa, A. (2002). *Risk Management Guide for Information Technology Systems.* Gaithersburg: NIST.

STORMWARE s.r.o. (2014). *POHODA.* Cit. 23.04.2014, dostupné z: http://www.stormware.cz/pohoda/pohoda-e1.aspx

Survio (2016). *Dotazníky.* Cit. 03.01.2016, dostupné z: http://www.survio.com/cs/

Svozilová, A. (2007). *Projektový management.* Praha: Grada.

Šidlichovská, Z. (2011). Evaluační přístupy k informačnímu managementu ve státní správě. *ProInflow, 3(1), 50-66.* Dostupné z: http://www.phil.muni.cz/journals/index.php/proinflow/article/view/850

Švarcová, I., & Rain, T. (2012). *Informační management.* Praha: Kernberg Publishing, s.r.o.

Tourish, D., & Robson, P. (2006). Sensemaking and the Distortion of Critical Upward Communication in Organizations. *Journal of Management Studies,* 43(4), 711-730.

USC (2003). *Information Management & Systems. A Brief History of Information Management.* Cit. 08.04.2014, dostupné z: faculty.uscupstate.edu/.../SIMS201_1IMHistory.ppt

Účetní software (2015). *Ekonomické systémy ERP.* Cit. 12.09.2015, dostupné z: http://www.ucetnisoftware.com/ekonomicke_systemy.html

Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. (2011). *ČSN IEC/ISO 31010. Management rizik - Techniky posuzování rizik.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. (2010). *ČSN ISO 31000. Management rizik - Principy a směrnice.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. (2010). *TNI 01 0350. Management rizik - Slovník.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. (2008). *ČSN 36 9790. Systém managementu bezpečnosti informací - Směrnice pro management rizik bezpečnosti informací.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. (2006). *ČSN EN ISO 9000. Systémy managementu kvality - Základní principy a slovník.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. (1998). *ČSN/ISO IEC 2382-1 (36 9001). Informační technologie - Slovník Část 1: Základní termíny.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

Vacek, J. (2010). *Znalostní management. Data, informace, znalosti. Typy znalostí, transformace, techniky a postupy* (Přednáškový materiál). Plzeň: Západočeská univerzita v Plzni.

Vacek, J. (2006). Úvod. In J. Vacek (Ed.), *Moderní management ve veřejné správě* (s. 5-9). Plzeň: Západočeská univerzita v Plzni.

Vacík, E. (2005). *Risk management v podnicích a projektech* (Habilitační práce). Praha: VŠE Praha.

Vodáček, L., & Rosický, A. (1997). *Informační management: Pojetí, poslání a aplikace.* Praha: Management Press.

Vrana, I., & Richta, K. (2005). *Zásady a postupy zavádění podnikových informačních systémů. Praktická příručka pro podnikové manažery.* Praha: Grada.

Weick, K. E. (2009). *Making Sense of the Organization, Volume 2, The Impermanent Organization.* UK, Chichester: John Wiley&Sons Ltd.

Wexelblat, A., & Maes, P. (1999). Footprints: history-rich tools for information foraging. In M. G. Williams & M. W. Altom (Eds.), *Proceedings of the SIGCHI conference on Human Factors in Computing systems* (s. 270-277). USA, New York: SIGCHI.

Wiegers, E. K. (2008). *Požadavky na software. Od zadání k architektuře aplikace.* Brno: Computer Press.

Wilson, T. (1997). Information behaviour: An interdisciplinary perspective. *Information Processing & Management*, 33(4), 551-572.

Seznam příloh

Příloha A: Výzkumná činnost autorky

1) Spoluřešitelka projektu SGS-2012-022 Rozvoj teorie a praxe finančního řízení.
2) Spoluřešitelka projektu SGS-2013-040 Paradigma vývoje v 21. století a jeho vliv na chování ekonomických subjektů.
3) Spoluřešitelka projektu SGS-2015-019 Dopady aktuálních právních, daňových, účetních a sociálních změn na soukromé podniky a veřejný sektor v kontextu rekodifikace soukromého práva.

Příloha B: Struktura expertních rozhovorů

Okruh 1: Základní údaje o zkoumaném subjektu

- Název organizace:
- Právní forma:
- Předmět podnikání:
- Sídlo:
- Počet zaměstnanců:

Okruh 2: Informační systém organizace obecně

- Technické vybavení. Nástroje používané pro správu dat.
- Používaný IS.
- Jedná se o IS „na míru“ nebo ne?
- Jak dlouho je IS společností používán?
- Jak je zajištěna bezpečnost IS (bezpečnost dat)?
- Spravujete IS sami nebo využíváte služeb jiné společnosti (osoby)?
- Kdo řeší případné problémy s IS?
- Jak často se vyskytnou v rámci IS nebo při přenosu dat potíže, které je nutné řešit?
- O jaký typ problémů se jedná?

Okruh 3: Účetní informační systém (IS) specificky

- Počet zaměstnanců účetního oddělení.
- Jakým způsobem je v organizaci řešena oblast účetnictví?
  Typ používaného účetního IS. Je IS součástí podnikového IS, nebo se jedná pouze o modul pro účetnictví bez dalších vazeb na podnikový IS?
- Doba, po kterou je účetní IS používán.
- Kdo ve společnosti má přístup k účetním informacím?
- Jak je zajištěna bezpečnost účetního systému (účetních dat)?
- Kdo řeší případné problémy v této oblasti?
- Jak často se vyskytnou v rámci účetního IS nebo přenosu účetních dat potíže, které je nutné řešit?
- O jaký typ problémů se jedná?

Okruh 4: Řízení rizik

- Znáte pojem informační management?
- Využíváte jej? Jak?
- Provádíte analýzu rizik?
- Pokud ne, předpokládáte její zavedení? V jakém časovém horizontu?
- Jaké plány v oblasti řízení rizik máte do budoucna?
- Došlo ve vašem podniku k nějaké rizikové události?
- Pokud ano, jak jste tuto situaci řešili?
- Vyskytují se v rámci účetního oddělení rizika spojená s osobou účetní?

(Vliv lidského faktoru na zpracovávaná data, na zprostředkovávané informace.)

- Jak je případný vznik takových rizik ošetřen?

Analýza rizik – ekonomické/účetní oddělení - za předpokladu souhlasu organizace

- Identifikace a ocenění aktiv
- Identifikace rizik
- Vyhodnocení rizik
- Zvládání rizik

Příloha C: Výstupy expertních rozhovorů

Respondent číslo 1

Základní údaje o zkoumané společnosti:

- Právní forma: Společnost s ručením omezeným
- Předmět podnikání: výroba, obchod a služby neuvedené v přílohách 1 a 3 živnostenského zákona.
- Počet zaměstnanců: 16
- Počet zaměstnanců účetního/ekonomického oddělení: 1

Informační systém organizace:

Hardwarové vybavení společnosti představuje 31 PC, 10 notebooků a 4 servery, externí úložiště nejsou využívána. Již od roku 2009 využívá společnost IS PREMIER (moduly: evidence zákazníků, evidence hovorů, odběratelé, dodavatelé, evidence majetku, sklad, správce, profibanka). Přístupová práva k jednotlivým modulům nejsou omezena. Bezpečnost dat je zajištěna antivirovým programem a firewallem. Jednou denně probíhá zálohování dat na serveru. Výpočetní technika je spravována zaměstnanci společnosti speciálně proškolenými pro tuto činnost, kteří řeší také veškeré potíže vzniklé v souvislosti se zálohováním dat. Celkově je společnost s používaným IS spokojena. IS splňuje požadavky na něj kladené.

Účetní informační systém:

Oblast účetnictví je ve společnosti řešena samostatným účetním programem bez dalších vazeb na podnikový IS, který je používán již pět let. K účetním informacím mají přístup účetní a jednatelka. Systém splňuje požadavky společnosti, v souvislosti s jeho používáním nevznikají žádné problémy.

Řízení rizik:

V rámci dotazování se na informační management a řízení rizik bylo zjištěno, že zaměstnanci společnosti tento pojem neznají, informační management nevyužívají, neprovádí ani analýzu rizik a do budoucna tyto aktivity neplánují. Přesto byla respondentem poskytnuta data potřebná pro sestavení registru rizik ekonomického oddělení společnosti.

Tabulka C1: Data pro sestavení registru rizik - respondent číslo 1

Aktivum	Hodnota aktiva	Popis rizika	Pravděpodobnost výskytu hrozby	Pravděpodobnost výskytu zranitelnosti	Riziko	Úroveň rizika	Opatření
Databáze ekonomického oddělení	4	Nedostatečná aktualizace SW	V	V	4	S	Častější aktualizace
Databáze zákazníků	4	Selhání SW	N	V	6	V	Zálohování, kontrola
Evidence hovorů	3	Nedostatečná aktualizace SW	V	V	7	V	Zálohování, kontrola
PC	2	Selhání HW	N	M	2	P	Zajištění servisu
Notebooky	2	Selhání HW	N	M	2	P	Zajištění servisu
Operační systémy	3	Nedostatečná aktualizace SW	V	S	6	V	Pravidelná aktualizace
Připojení k serveru	4	Nevhodné nastavení	V	S	7	V	Bezpečnostní opatření
Profibanka	4	Selhání SW	S	V	7	V	Zálohování

Zdroj: vlastní zpracování, 2016

Respondent číslo 2

Základní údaje o zkoumané společnosti:

- Právní forma: Akciová společnost
- Předmět podnikání: řeznictví a uzenářství; hostinská činnost; výroba, obchod a služby neuvedené v přílohách 1 a 3 živnostenského zákona.
- Počet zaměstnanců: cca 250
- Počet zaměstnanců účetního/ekonomického oddělení: 6

Informační systém organizace:

Hardwarové vybavení společnosti představuje cca 100 PC, 15 notebooků a 30 serverů (včetně VHDX - virtuální pevný disk s vyšší úložnou kapacitou než VHD), externí úložiště nejsou využívána. Již pět let využívá společnost IS CSB a dva roky IS NETTO (moduly: MERP, ERP, sklady, výroba). V obou případech se jedná o „IS na míru“. Přístupová práva k jednotlivým modulům jsou omezena. Bezpečnost dat je zajištěna antivirovým programem a síťovým firewallem. Denně probíhá zálohování dat. Výpočetní technika je spravována IT oddělením společnosti, které řeší také veškeré potíže vzniklé v souvislosti se zálohováním dat. Při správě IS je využíváno i služeb externího dodavatele. Celkově je společnost s používaným IS spokojena. Přes drobné problémy splňuje IS požadavky na něj kladené.

Účetní informační systém:

Oblast účetnictví je ve společnosti řešena samostatným účetním programem bez dalších vazeb na podnikový IS, který je používán již tři roky. K účetním informacím mají přístup účetní a část managementu. Účetní systém splňuje požadavky společnosti. V souvislosti s jeho používáním však dochází k různým typům problémů. Většinou se nejedná o problémy závažné. Řešení používaná společností k odstranění problémů jsou update nebo upgrade.

Řízení rizik:

V rámci dotazování se na informační management a řízení rizik bylo zjištěno, že zaměstnanci společnosti tento pojem znají, informační management však nevyužívají, neprovádí ani analýzu rizik a do budoucna tyto aktivity neplánují. Data potřebná pro sestavení registru rizik ekonomického oddělení společnosti nebyla respondentem poskytnuta.

Respondent číslo 3

Základní údaje o zkoumané společnosti:

- Právní forma: Společnost s ručením omezeným
- Předmět podnikání: daňové poradenství; ekonomické a organizační poradenství; koupě zboží za účelem jeho dalšího prodeje a prodej; zprostředkovatelská činnost v oblasti obchodu a služeb; činnost účetních poradců, vedení účetnictví, vedení daňové evidence.
- Počet zaměstnanců: 15
- Počet zaměstnanců účetního/ekonomického oddělení: 2

Informační systém organizace:

Hardwarové vybavení společnosti představují 3 PC, 1 notebook a server, externí úložiště nejsou využívána. Společnost již 14 let využívá účetní software POHODA. Jedná se o systém na pomezí ekonomických IS a ERP systémů, který plně využívá technologie klient-server a databáze SQL. Nabízí nejen větší výkon a bezpečnost systému, zpracování velkého množství dat a souběžnou práci většího počtu uživatelů, ale i rozšiřující funkce z kategorie ERP systémů, jako jsou: pokročilá definice přístupových práv a velká míra přizpůsobení podle potřeb uživatelů (STORMWARE 2014). Společnost používá agendy Účetnictví a Mzdy. Přístupová práva k jednotlivým modulům nejsou omezena. Bezpečnost dat je zajištěna antivirovým programem a firewallem. Jednou denně probíhá zálohování dat na jiné pevné disky. Výpočetní technika je spravována externím zaměstnancem. Celkově je společnost s používaným IS spokojena. IS splňuje požadavky na něj kladené.

Účetní informační systém:

Oblast účetnictví je ve společnosti řešena samostatným účetním programem bez dalších vazeb na podnikový IS, který je používán již 14 let. K účetním informacím mají přístup účetní a jednatelé. Systém splňuje požadavky společnosti, v souvislosti s jeho používáním nevznikají žádné zásadní problémy.

Řízení rizik:

V rámci dotazování se na informační management a řízení rizik bylo zjištěno, že zaměstnanci společnosti tento pojem neznají, informační management nevyužívají, neprovádí ani analýzu rizik a do budoucna si nejsou jisti, jestli budou tyto aktivity provádět. Přesto byla respondentem poskytnuta data potřebná pro sestavení registru rizik ekonomického oddělení společnosti.

Tabulka C2: Data pro sestavení registru rizik - respondent číslo 3

Aktivum	Hodnota aktiva	Popis rizika	Pravděpodobnost výskytu hrozby	Pravděpodobnost výskytu zranitelnosti	Riziko	Úroveň rizika	Opatření
Databáze ekonomického oddělení	4	Nedostatečná aktualizace SW	V	S	7	V	Pravidelná aktualizace
Databáze ekonomického oddělení	4	Neúmyslná úprava informací vedoucí k jejich špatnému použití	V	V	8	V	Zálohování, kontrola
PC	3	Selhání HW - mechanické poškození	N	S	4	S	Včasné zajištění servisu
Notebook	2	Přírodní katastrofa	N	M	2	P	Bezpečnostní opatření
Operační systémy	3	Nedostatečná aktualizace SW	S	V	6	V	Pravidelná aktualizace
Připojení k serveru	4	Nevhodné nastavení komunikace	V	V	8	V	Nastavení pravidel interní komunikace

Zdroj: vlastní zpracování, 2016

Respondent číslo 4

Základní údaje o zkoumané společnosti:

- Právní forma: Společnost s ručením omezeným
- Předmět podnikání: výroba, obchod a služby neuvedené v přílohách 1 a 3 živnostenského zákona.
- Počet zaměstnanců: do 250
- Počet zaměstnanců účetního/ekonomického oddělení: 1

Informační systém organizace:

Hardwarové vybavení společnosti představuje 1 notebook a externí úložiště. Společnost již od roku 1994 využívá ERP systém ABRA (moduly: účetnictví, sklady, fakturace, objednávky). Přístupová práva k jednotlivým modulům nejsou omezena. Bezpečnost dat je zajištěna antivirovým programem. Jednou denně probíhá zálohování dat. Výpočetní technika je spravována externí společností. Celkově je společnost s používaným IS spokojena. IS splňuje požadavky na něj kladené.

Účetní informační systém:

Oblast účetnictví je ve společnosti řešena modulem, který je součástí informačního systému. IS je používán již od roku 1994. K účetním informacím mají přístup zaměstnanci společnosti odpovědní za oblast účetnictví. Systém splňuje požadavky společnosti, v souvislosti s jeho používáním vznikají pouze běžné provozní potíže.

Řízení rizik:

V rámci dotazování se na informační management a řízení rizik bylo zjištěno, že zaměstnanci společnosti tento pojem znají, informační management však nevyužívají. Analýzu rizik provádí pouze zběžně. Data potřebná pro sestavení registru rizik ekonomického oddělení společnosti byla respondentem poskytnuta.

Tabulka C3: Data pro sestavení registru rizik - respondent číslo 4

Aktivum	Hodnota aktiva	Popis rizika	Pravděpodobnost výskytu hrozby	Pravděpodobnost výskytu zranitelnosti	Riziko	Úroveň rizika	Opatření
Notebook	2	Přírodní katastrofa	N	M	2	P	Bezpečnostní opatření
Operační systémy	4	Nedostatečná aktualizace SW	S	V	7	V	Pravidelná aktualizace
Databáze objednávek	4	Selhání HW, SW	V	V	8	V	Zálohy, pravidelný servis

Zdroj: vlastní zpracování, 2016

Respondent číslo 5

Základní údaje o zkoumané společnosti:

- Právní forma: Společnost s ručením omezeným
- Předmět podnikání: výroba nebezpečných chemických látek a nebezpečných chemických směsí a prodej chemických látek a chemických směsí klasifikovaných jako vysoce toxické a toxické; výroba, obchod a služby neuvedené v přílohách 1 a 3 živnostenského zákona.
- Počet zaměstnanců: do 250
- Počet zaměstnanců účetního/ekonomického oddělení: 3

Informační systém organizace:

Hardwarové vybavení společnosti představuje 8 PC, 3 notebooky, server a 3 externí úložiště. Již 15 let využívá společnost IS Money S3 upravený dodavatelem pro potřeby firmy. Přístupová práva k jednotlivým modulům jsou omezena. Bezpečnost dat je zajištěna antivirovým programem a firewallem. Denně probíhá zálohování dat na pevné disky. Výpočetní technika je spravována zaměstnanci dodavatelské společnosti, kteří řeší také veškeré potíže vzniklé v souvislosti s používáním systému. Společnost není se systémem příliš spokojena. Problémem je častá potřeba konzultace vzniklých problémů s dodavatelem IS.

Účetní informační systém:

Oblast účetnictví je ve společnosti řešena modulem, který je součástí informačního systému. K účetním informacím mají přístup účetní a majitel společnosti. Přístupová práva k modulu jsou nastavena v různém rozsahu dle odpovědnosti pracovníků účetního oddělení. Systém nesplňuje požadavky společnosti, v souvislosti s jeho používáním vznikají problémy, které je nutné konzultovat s dodavatelem IS. V budoucnu není vyloučena změna dodavatele IS.

Řízení rizik:

V rámci dotazování se na informační management a řízení rizik bylo zjištěno, že zaměstnanci společnosti tento pojem neznají, informační management nevyužívají, analýzu rizik ale provádí. Data potřebná pro sestavení registru rizik ekonomického oddělení společnosti nebyla respondentem poskytnuta.

Respondent číslo 6

Základní údaje o zkoumané společnosti:

- Právní forma: Akciová společnost
- Předmět podnikání: silniční motorová doprava - nákladní vnitrostátní provozovaná vozidly o největší povolené hmotnosti do 3,5 tuny včetně, - nákladní vnitrostátní provozovaná vozidly o největší povolené hmotnosti nad 3,5 tuny, - nákladní mezinárodní provozovaná vozidly o největší povolené hmotnosti do 3,5 tuny včetně; výroba, obchod a služby neuvedené v přílohách 1 až 3 živnostenského zákona; provádění staveb, jejich změn a odstraňování; projektová činnost ve výstavbě; montáž, opravy, revize a zkoušky elektrických zařízení; montáž, opravy, revize a zkoušky plynových zařízení a plnění nádob plyny; montáž, opravy, revize a zkoušky zdvihacích zařízení; montáž, opravy, revize a zkoušky tlakových zařízení a nádob na plyny; výroba, instalace, opravy elektrických strojů a přístrojů, elektronických a telekomunikačních zařízení; činnost účetních poradců, vedení účetnictví, vedení daňové evidence; poskytování služeb v oblasti bezpečnosti a ochrany zdraví při práci; technicko-organizační činnost v oblasti požární ochrany; opravy silničních vozidel.
- Počet zaměstnanců: do 250
- Počet zaměstnanců účetního/ekonomického oddělení: 5

Informační systém organizace:

Hardwarové vybavení společnosti představují PC pro zaměstnance (centrální počítač se zálohováním dat), notebooky (v rámci ekonomického oddělení notebook vedoucího) a server, externí úložiště nejsou využívána. Již od roku 1997 využívá společnost IS J.K.R. (moduly: finanční účetnictví, fakturace, pokladna, banka, sklady, evidence majetku, mzdy a personalistika, zakázky, doprava, informace (korespondence), manažer). Přístupová práva k jednotlivým modulům jsou omezena podle odpovědnosti jednotlivých zaměstnanců. Existují zde 3 typy nastavení přístupu uživatele k modulům: pasivní, aktivní, správa. Ke všem modulům má přístup ekonomický ředitel společnosti. Bezpečnost dat je zajištěna antivirovým programem a firewallem. Ve společnosti existuje dvojí zálohování dat, centrální počítač a server. Zálohování dat na serveru probíhá jako několikastupňové zálohování: denní zálohování, týdenní zálohování

a roční zálohování (vytváří se také trvalá záloha dat na externím disku). Výpočetní technika je spravována zaměstnanci externí společnosti Airweb spol. s r.o., kteří řeší také případné potíže vzniklé v souvislosti se zálohováním dat nebo jiné technické problémy. Aktualizace IS řeší přímo jeho dodavatel. Celkově je společnost s používaným IS velmi spokojena. IS splňuje požadavky na něj kladené. V zásadě je možné jen občas identifikovat vznik technického problému, jehož řešení zajišťuje externí společnost.

Účetní informační systém:

Oblast účetnictví je ve společnosti řešena modulem, který je součástí informačního systému J.K.R. Ten je společností používán již od roku 1997. K účetním informacím mají přístup čtyři účetní a jejich vedoucí. Přístupová práva k modulu jsou nastavena v různém rozsahu dle odpovědnosti pracovníků ekonomického oddělení. Systém splňuje požadavky společnosti, v souvislosti s jeho používáním nevznikají žádné zásadní problémy. Problémy související s možností selhání lidského faktoru jsou řešeny prostřednictvím nastavení pravidel pro výběr zaměstnanců v rámci personální politiky společnosti.

Řízení rizik:

V rámci dotazování se na informační management a řízení rizik bylo zjištěno, že zaměstnanci společnosti tento pojem znají, informační management využívají, neboť je součástí systému řízení dle ISO. Analýza rizik je zde prováděna intuitivně, nevyužívá se označení „analýza rizik“. Respondentem byla poskytnuta data potřebná pro sestavení registru rizik ekonomického oddělení společnosti.

Tabulka C4: Data pro sestavení registru rizik - respondent číslo 6

Aktivum	Hodnota aktiva	Popis rizika	Pravděpodobnost výskytu hrozby	Pravděpodobnost výskytu zranitelnosti	Riziko	Úroveň rizika	Opatření
Databáze ekonomického oddělení	4	Nedostatečná aktualizace SW	V	V	8	V	Pravidelná aktualizace
Databáze ekonomického oddělení	4	Neúmyslná úprava informací vedoucí k jejich špatnému použití	N	S	5	S	Úprava přístupů k modulům, personální politika společnosti
PC	3	Selhání HW	N	M	3	S	Včasné zajištění servisu
Notebook	2	Selhání HW	N	M	2	P	Včasné zajištění servisu
Notebook	2	Přírodní katastrofa	N	M	2	P	Bezpečnostní opatření
Operační systémy	3	Nedostatečná aktualizace SW	N	V	5	S	Zajištění servisu IT specialistou
Připojení k serveru	4	Nevhodné nastavení komunikace	N	V	6	V	Nastavení pravidel interní komunikace
Server	4	Přírodní katastrofa	N	V	6	V	Bezpečnostní opatření
Zaměstnanci ekonomického oddělení (účetní)	4	Neúmyslná modifikace dat	N	V	6	V	Úprava přístupů k modulům, personální politika společnosti

Zdroj: vlastní zpracování, 2016

Respondent číslo 7

Základní údaje o zkoumané společnosti:

- Právní forma: Akciová společnost
- Předmět podnikání: výroba elektřiny; výroba tepelné energie; rozvod tepelné energie; vodoinstalatérství, topenářství; zámečnictví, nástrojářství; výroba tepelná energie a rozvod tepelné energie, nepodléhající licenci realizovaná ze zdrojů tepelné energie s instalovaným výkonem jednoho zdroje nad 50 kW; výroba, obchod a služby neuvedené v přílohách 1 až 3 živnostenského zákona.
- Počet zaměstnanců: 33
- Počet zaměstnanců účetního/ekonomického oddělení: 4

Informační systém organizace:

Hardwarové vybavení společnosti představuje 18 PC, 6 notebooků a 3 servery, externí úložiště nejsou využívána. Již 19 let využívá společnost IS HSF Flex (moduly: účetnictví, sklady, majetek, mzdy). Jedná se o informační systém „na míru“. Přístupová práva k jednotlivým modulům jsou omezena. Bezpečnost dat je zajištěna antivirovým programem a firewallem. Veškerá data jsou denně zálohována. Potíže vzniklé v souvislosti se zálohováním dat řeší zaměstnanci společnosti speciálně proškolení pro tuto činnost. Informační systém jako takový spravuje externí společnost HSF, problémy se však nevyskytují. Podpora dodavatele je nutná cca jednou za tři roky. Celkově je společnost s používaným informačním systémem spokojena. IS splňuje požadavky na něj kladené.

Účetní informační systém:

Oblast účetnictví je ve společnosti řešena samostatným účetním programem bez dalších vazeb na podnikový IS, který je používán již 19 let. K účetním informacím mají přístup všichni zaměstnanci ekonomického oddělení. Systém splňuje požadavky společnosti, v souvislosti s jeho používáním nevznikají žádné problémy.

Řízení rizik:

V rámci dotazování se na informační management a řízení rizik bylo zjištěno, že zaměstnanci společnosti tento pojem dobře znají, informační management využívají

a samozřejmě také provádí analýzu rizik. Respondentem byla také poskytnuta data potřebná pro sestavení registru rizik ekonomického oddělení společnosti.

Tabulka C5: Data pro sestavení registru rizik - respondent číslo 7

Aktivum	Hodnota aktiva	Popis rizika	Pravděpodobnost výskytu hrozby	Pravděpodobnost výskytu zranitelnosti	Riziko	Úroveň rizika	Opatření
Databáze ekonomického oddělení	4	Nedostatečná aktualizace software	V	S	7	V	Pravidelná aktualizace, zálohování
Databáze ekonomického oddělení	4	Neúmyslná úprava informací vedoucí k jejich špatnému použití	V	V	8	V	Zálohování, kontrola
PC, ostatní hardware	3	Selhání hardware - mechanické poškození	N	M	3	S	Včasné zajištění servisu, zálohování, redundance dat
IT infrastruktura společnosti jako celek	1	Přírodní katastrofa	N	M	1	P	
Operační systémy	3	Nedostatečná aktualizace software	S	V	6	V	Pravidelná aktualizace
Aplikační software	3	Nedostatečná aktualizace	V	V	7	V	Pravidelná aktualizace

Zdroj: vlastní zpracování, 2016

Respondent číslo 8

Základní údaje o zkoumané společnosti:

- Právní forma: Společnost s ručením omezeným
- Předmět podnikání: výroba, obchod a služby neuvedené v přílohách 1 a 3 živnostenského zákona; poskytování nebo zprostředkování spotřebitelského úvěru.
- Počet zaměstnanců: 14
- Počet zaměstnanců účetního/ekonomického oddělení: 2

Hardwarové vybavení společnosti představuje 11 PC, server a externí úložiště. Již osm let využívá společnost informační systém K2 upravený podle potřeb společnosti (např. účetnictví, sklady, prodejna). Přístupová práva k jednotlivým modulům jsou omezena dle odpovědnosti pracovníků. Bezpečnost dat je zajištěna antivirovým programem. Denně probíhá zálohování dat na server. Výpočetní technika je spravována zaměstnanci externí společnosti. Veškeré potíže vzniklé v souvislosti se zálohováním dat jsou řešeny IT pracovníkem analyzované společnosti. Celkově je společnost s používaným IS spokojena. IS splňuje požadavky na něj kladené.

Účetní informační systém:

Oblast účetnictví je ve společnosti řešena modulem, který je součástí informačního systému, který je používán již osm let. K účetním informacím mají přístup účetní, majitel společnosti a správce sítě. Systém splňuje požadavky společnosti.

Řízení rizik:

V rámci dotazování se na informační management a řízení rizik bylo zjištěno, že zaměstnanci společnosti tento pojem neznají, informační management nevyužívají, ale analýzu rizik provádí. Data potřebná pro sestavení registru rizik ekonomického oddělení společnosti byla respondentem poskytnuta.

Tabulka C6: Data pro sestavení registru rizik - respondent číslo 8

Aktivum	Hodnota aktiva	Popis rizika	Pravděpodobnost výskytu hrozby	Pravděpodobnost výskytu zranitelnosti	Riziko	Úroveň rizika	Opatření
Databáze ekonomického oddělení	4	Nedostatečná aktualizace	S	V	7	V	Pravidelná aktualizace, zálohování
PC	3	Selhání hardware	N	V	5	S	Kontrola, servis
Operační systémy	4	Nedostatečná aktualizace	S	V	7	V	Kontrola, servis
Připojení internetu	4	Nedostatečně nastavená komunikace	N	V	6	V	Nastavení a kontrola
Účetní pracovník	4	Selhání lidského faktoru	S	S	6	V	Kontrola a školení

Zdroj: vlastní zpracování, 2016

Respondent číslo 9

Základní údaje o zkoumané společnosti:

- Právní forma: Společnost s ručením omezeným
- Předmět podnikání: velkoobchod; specializovaný maloobchod; zámečnictví.
- Počet zaměstnanců: 8
- Počet zaměstnanců účetního/ekonomického oddělení: 1

Informační systém organizace:

Hardwarové vybavení společnosti představují 4 PC, 2 notebooky a server, externí úložiště nejsou využívána. Již 15 let využívá společnost blíže nespecifikovaný typový IS (např. moduly: účetnictví, sklady). Přístupová práva k jednotlivým modulům jsou omezena dle odpovědnosti pracovníků za jimi spravované oblasti podnikových činností. Bezpečnost dat je zajištěna antivirovým programem. Denně probíhá zálohování dat na server a záznamová média. Výpočetní technika je spravována zaměstnanci společnosti. Veškeré potíže vzniklé v souvislosti se zálohováním dat jsou chápány jako osobní odpovědnost každého zaměstnance.

Celkově je společnost s používaným IS spíše spokojena. IS splňuje požadavky na něj kladené, občas je však potřeba podpory ze strany dodavatele. V souvislosti s IS se vyskytují problémy zejména v souvislosti s jeho aktualizacemi.

Účetní informační systém:

Oblast účetnictví je ve společnosti řešena modulem, který je součástí informačního systému, který je používán již 15 let. K účetním informacím mají přístup účetní a jednatel společnosti. Systém v zásadě splňuje požadavky společnosti, v souvislosti s jeho používáním občas vznikají pouze menší snadno řešitelné problémy. Potíže se vyskytují zejména v souvislosti s nutností aktualizace IS.

Řízení rizik:

V rámci dotazování se na informační management a řízení rizik bylo zjištěno, že zaměstnanci společnosti tento pojem znají, informační management však nevyužívají, neprovádí ani analýzu rizik a do budoucna tyto aktivity neplánují. Data potřebná pro sestavení registru rizik ekonomického oddělení společnosti nebyla respondentem poskytnuta.

Respondent číslo 10

Základní údaje o zkoumané společnosti:

- Právní forma: Společnost s ručením omezeným
- Předmět podnikání: podnikání v oblasti nakládání s nebezpečnými odpady; výroba, obchod a služby neuvedené v přílohách 1 a 3 živnostenského zákona; silniční motorová doprava - nákladní provozovaná vozidly nebo jízdními soupravami o největší povolené hmotnosti přesahující 3,5 tuny, jsou-li určeny k přepravě zvířat nebo věcí, - nákladní provozovaná vozidly nebo jízdními soupravami o největší povolené hmotnosti nepřesahující 3,5 tuny, jsou-li určeny k přepravě zvířat nebo věcí.
- Počet zaměstnanců: 20
- Počet zaměstnanců účetního/ekonomického oddělení: 1

Informační systém organizace:

Hardwarové vybavení společnosti představují 2 PC a 1 notebook. Již devět let využívá společnost blíže nespecifikovaný IS vytvořený dodavatelem „na míru“. Společnost využívá tyto moduly: účetnictví, sklady, doprava, fakturace a mzdy. Přístupová práva k jednotlivým modulům jsou omezena dle odpovědnosti zaměstnanců. Bezpečnost dat je zajištěna antivirovým programem a firewallem. Denně probíhá zálohování dat na záznamová média (CD, DVD, flashdisc). Problémy spojené se zálohováním dat řeší zaměstnanci sami. Výpočetní technika je spravována zaměstnanci společnosti. Je jim poskytnuta součinnost ze strany dodavatele systému (cca jednou ročně je nutná podpora dodavatele systému). Celkově je společnost s používaným IS spokojena, vyskytují-li se problémy, jsou spíše mechanického rázu. IS splňuje požadavky na něj kladené.

Účetní informační systém:

Oblast účetnictví je ve společnosti řešena modulem, který je součástí informačního systému. Ten je společností používán devět let, stejně jako celý IS. K účetním informacím mají přístup dva zaměstnanci. Systém splňuje požadavky společnosti, v souvislosti s jeho používáním nevznikají žádné zásadní problémy. Případný vznik problémů je smluvně ošetřen s dodavatelem systému.

Řízení rizik:

V rámci dotazování se na informační management a řízení rizik bylo zjištěno, že zaměstnanci společnosti tento pojem znají, informační management využívají, analýzu rizik však neprovádí. Přesto byla respondentem poskytnuta data potřebná pro sestavení registru rizik ekonomického oddělení společnosti.

Tabulka C7: Data pro sestavení registru rizik - respondent číslo 10

Aktivum	Hodnota aktiva	Popis rizika	Pravděpodobnost výskytu hrozby	Pravděpodobnost výskytu zranitelnosti	Riziko	Úroveň rizika	Opatření
Databáze ekonomického oddělení	4	Nedostatečná aktualizace SW	N	S	5	S	Pravidelná aktualizace
Databáze evidence odpadů	4	Nedostatečná aktualizace SW	V	V	8	V	Pravidelná aktualizace
PC	3	Selhání hardware	N	S	4	S	Včasný servis
Notebook	3	Selhání hardware	N	S	4	S	Včasný servis
Zabezpečení IS	4	Nabourávání systému	N	V	6	V	Pravidelná aktualizace, proškolení zaměstnanců

Zdroj: vlastní zpracování, 2016

Respondent číslo 11

Základní údaje o zkoumané společnosti:

- Právní forma: Společnost s ručením omezeným
- Předmět podnikání: výroba, obchod a služby neuvedené v přílohách 1 a 3 živnostenského zákona; silniční motorová doprava - nákladní provozovaná vozidly nebo jízdními soupravami o největší povolené hmotnosti nepřesahující 3,5 tuny, jsou-li určeny k přepravě zvířat nebo věcí; činnost účetních poradců, vedení účetnictví, vedení daňové evidence.
- Počet zaměstnanců: 5
- Počet zaměstnanců účetního/ekonomického oddělení: 2

Informační systém organizace:

Hardwarové vybavení společnosti představují 4 PC, 3 notebooky, server a jedno externí úložiště. Společnost již od roku 1994 využívá ERP systém ABRA (moduly: účetnictví, sklady, fakturace, objednávky). Přístupová práva k jednotlivým modulům nejsou omezena. Bezpečnost dat je zajištěna antivirovým programem. Jednou denně probíhá zálohování dat. Výpočetní technika je spravována externí společností.

Celkově je společnost s používaným IS spokojena. IS splňuje požadavky na něj kladené.

Účetní informační systém:

Oblast účetnictví je ve společnosti řešena modulem, který je součástí informačního systému. IS je používán již od roku 1994. K účetním informacím mají přístup všichni zaměstnanci společnosti. Systém splňuje požadavky společnosti, v souvislosti s jeho používáním vznikají pouze běžné provozní potíže.

Řízení rizik:

V rámci dotazování se na informační management a řízení rizik bylo zjištěno, že zaměstnanci společnosti tento pojem znají, informační management však nevyužívají. Analýzu rizik provádí pouze zběžně. Data potřebná pro sestavení registru rizik ekonomického oddělení společnosti nebyla respondentem poskytnuta.

Respondent číslo 12

Základní údaje o zkoumané společnosti:

- Právní forma: Společnost s ručením omezeným
- Předmět podnikání: výroba, obchod a služby neuvedené v přílohách 1 a 3 živnostenského zákona.
- Počet zaměstnanců: 5
- Počet zaměstnanců účetního/ekonomického oddělení: 2

Informační systém organizace:

Hardwarové vybavení společnosti představují 2 PC, 1 notebook, server a externí úložiště. Společnost již čtyři roky využívá IS PREMIER. (moduly: účetnictví, sklady, mzdy, výroba). Přístupová práva k jednotlivým modulům jsou omezena dle odpovědnosti zaměstnance. Bezpečnost dat je zajištěna antivirovým programem a firewallem. Jednou denně probíhá zálohování dat na pevné disky. Výpočetní technika je spravována zaměstnanci externí společnosti. Veškeré potíže vzniklé v souvislosti se zálohováním dat řeší administrátor.

Celkově je společnost s používaným IS spokojena. IS splňuje požadavky na něj kladené, přesto je občas zapotřebí podpora dodavatele (help desk).

Účetní informační systém:

Oblast účetnictví je ve společnosti řešena modulem, který je součástí informačního systému. K účetním informacím mají přístup účetní, obchodníci a vedení společnosti. Přístupová práva k modulu jsou nastavena v různém rozsahu dle odpovědnosti pracovníků. Systém splňuje požadavky společnosti, v souvislosti s jeho používáním nevznikají žádné zásadní problémy.

Řízení rizik:

V rámci dotazování se na informační management a řízení rizik bylo zjištěno, že zaměstnanci společnosti tento pojem znají, informační management využívají a provádí také analýzu rizik. Přesto respondentem nebyla poskytnuta data potřebná pro sestavení registru rizik ekonomického oddělení společnosti.

Respondent číslo 13

Základní údaje o zkoumané společnosti:

- Právní forma: Společnost s ručením omezeným
- Předmět podnikání: zámečnictví; instalace a opravy elektrických strojů a přístrojů; činnost technických poradců v oblasti energetiky; revize a zkoušky vyhrazených tlakových zařízení; revize a zkoušky vyhrazených plynových zařízení; montáž, opravy, revize a zkoušky vyhrazených elektrických zařízení; výroba, obchod a služby neuvedené v přílohách 1 a 3 živnostenského zákona.
- Počet zaměstnanců: 43
- Počet zaměstnanců účetního/ekonomického oddělení: 2

Informační systém organizace:

Hardwarové vybavení společnosti představuje 16 PC, 5 notebooků a 4 servery a 8 externích úložišť. Již pět let využívá společnost IS Ekonom - účetní a evidenční systém (moduly: sklady, účetnictví, majetek, mzdy, fakturace, objednávky, sledování termínů). Přístupová práva k jednotlivým modulům jsou omezena dle okruhu pracovní náplně jednotlivých zaměstnanců. Bezpečnost dat je zajištěna antivirovým programem a firewallem. Jednou denně probíhá zálohování dat. Veškeré problémy spojené se zálohováním řeší IT technik. Výpočetní technika je spravována zaměstnanci společnosti v součinnosti s dodavatelskou firmou, podpora dodavatele je nutná cca dvakrát až třikrát ročně. Celkově je společnost s používaným IS spokojena. IS splňuje požadavky na něj kladené, v souvislosti s jeho používáním se objevují jen běžné uživatelské a provozní problémy.

Účetní informační systém:

Oblast účetnictví je ve společnosti řešena modulem, který je součástí informačního systému. Ten je společností používán pět let, stejně jako celý IS. K účetním informacím mají přístup zaměstnanci účetního oddělení a jednatelé společnosti. Systém splňuje požadavky společnosti, v souvislosti s jeho používáním se vyskytují pouze běžné uživatelské a provozní problémy. Případný vznik problémů je řešen pomocí záložních zdrojů a zálohování dat. Zaměstnanci společnosti jsou proškolováni pro práci s IS.

Řízení rizik:

V rámci dotazování se na informační management a řízení rizik bylo zjištěno, že zaměstnanci společnosti tento pojem znají, informační management využívají a provádí také analýzu rizik. Data potřebná pro sestavení registru rizik ekonomického oddělení společnosti však nebyla respondentem poskytnuta.

Respondent číslo 14

Základní údaje o zkoumané společnosti:

- Právní forma: Akciová společnost
- Předmět podnikání: výroba, obchod a služby neuvedené v přílohách 1 a 3 živnostenského zákona; provádění staveb, jejich změn a odstraňování; projektová činnost ve výstavbě; výroba, instalace, opravy elektrických strojů a přístrojů, elektronických a telekomunikačních zařízení; podnikání v oblasti nakládání s nebezpečnými odpady; vodoinstalatérství, topenářství; výroba elektřiny; silniční motorová doprava - nákladní provozovaná vozidly nebo jízdními soupravami o největší povolené hmotnosti přesahující 3,5 tuny, jsou-li určeny k přepravě zvířat nebo věcí, - nákladní provozovaná vozidly nebo jízdními soupravami o největší povolené hmotnosti nepřesahující 3,5 tuny, jsou-li určeny k přepravě zvířat nebo věcí.
- Počet zaměstnanců: do 250
- Počet zaměstnanců účetního/ekonomického oddělení: 4

Informační systém organizace:

Hardwarové vybavení společnosti představují PC pro zaměstnance (centrální počítač se zálohováním dat), notebooky (v rámci ekonomického oddělení notebook vedoucího) a server, externí úložiště nejsou využívána. Již od roku 1997 využívá společnost IS J.K.R. (moduly: finanční účetnictví, fakturace, pokladna, banka, sklady, evidence majetku, mzdy a personalistika, zakázky, doprava, informace, manažer). Přístupová práva k jednotlivým modulům jsou omezena podle odpovědnosti jednotlivých zaměstnanců. Existují zde 3 typy nastavení přístupu uživatele k modulům: pasivní, aktivní, správa. Ke všem modulům má přístup ekonomický ředitel společnosti. Bezpečnost dat je zajištěna antivirovým programem a firewallem. Ve společnosti existuje dvojí zálohování dat, centrální počítač a server. Zálohování dat na serveru probíhá jako několikastupňové zálohování: denní zálohování, týdenní zálohování a roční zálohování (vytváří se také trvalá záloha dat na externím disku). Výpočetní technika je spravována zaměstnanci externí společnosti Airweb spol. s r. o., kteří řeší také případné potíže vzniklé v souvislosti se zálohováním dat nebo jiné technické problémy. Aktualizace IS řeší přímo jeho dodavatel. Celkově je společnost

s používaným IS velmi spokojena. IS splňuje požadavky na něj kladené. V zásadě je možné jen občas identifikovat vznik technického problému, jehož řešení zajišťuje externí společnost.

Účetní informační systém:

Oblast účetnictví je ve společnosti řešena modulem, který je součástí informačního systému J.K.R. Ten je společností používán již od roku 1997. K účetním informacím mají přístup čtyři účetní a jejich vedoucí. Přístupová práva k modulu jsou nastavena v různém rozsahu dle odpovědnosti pracovníků ekonomického oddělení. Systém splňuje požadavky společnosti, v souvislosti s jeho používáním nevznikají žádné zásadní problémy. Problémy související s možností selhání lidského faktoru jsou řešeny prostřednictvím nastavení pravidel pro výběr zaměstnanců v rámci personální politiky společnosti.

Řízení rizik:

V rámci dotazování se na informační management a řízení rizik bylo zjištěno, že zaměstnanci společnosti tento pojem znají, informační management využívají, neboť je součástí systému řízení dle ISO. Analýza rizik je zde prováděna intuitivně, nevyužívá se označení „analýza rizik“. Respondentem byla poskytnuta data potřebná pro sestavení registru rizik ekonomického oddělení společnosti.

Tabulka C8: Data pro sestavení registru rizik - respondent číslo 14

Aktivum	Hodnota aktiva	Popis rizika	Pravděpodobnost výskytu hrozby	Pravděpodobnost výskytu zranitelnosti	Riziko	Úroveň rizika	Opatření
Databáze ekonomického oddělení	4	Nedostatečná aktualizace SW	V	V	8	V	Pravidelná aktualizace
Databáze ekonomického oddělení	4	Neúmyslná úprava informací vedoucí k jejich špatnému použití	N	S	5	S	Úprava přístupů k modulům, personální politika společnosti
PC	3	Selhání HW	N	M	3	S	Včasné zajištění servisu
Notebook	2	Selhání HW	N	M	2	P	Včasné zajištění servisu
Notebook	2	Přírodní katastrofa	N	M	2	P	Bezpečnostní opatření
Operační systémy	4	Nedostatečná aktualizace SW	N	V	6	V	Zajištění servisu IT specialistou
Připojení k serveru	4	Nevhodné nastavení komunikace	N	V	6	V	Nastavení pravidel interní komunikace
Server	4	Přírodní katastrofa	N	V	6	V	Bezpečnostní opatření
Zaměstnanci ekonomického oddělení (účetní)	4	Neúmyslná modifikace dat	N	V	6	V	Úprava přístupů k modulům, personální politika společnosti

Zdroj: vlastní zpracování, 2016

Respondent číslo 15

Základní údaje o zkoumané společnosti:

- Právní forma: Společnost s ručením omezeným
- Předmět podnikání: výroba, obchod a služby neuvedené v přílohách 1 a 3 živnostenského zákona; malířství, lakýrnictví.
- Počet zaměstnanců: 72
- Počet zaměstnanců účetního/ekonomického oddělení: 1

Informační systém organizace:

Hardwarové vybavení společnosti představuje 7 PC, server a externí úložiště. Společnost již 18 let využívá informační systém na míru, sestavený přímo pro výrobu společnosti. Společnost používá moduly: účetnictví, výrobní sklady a výrobky. Přístupová práva k jednotlivým modulům nejsou omezena. Bezpečnost dat je zajištěna antivirovým programem. Jednou denně probíhá zálohování dat na server a jiné pevné disky. Výpočetní technika je spravována externí společností.

Celkově je společnost s používaným IS spokojena. IS splňuje požadavky na něj kladené, potíže se nevyskytují.

Účetní informační systém:

Oblast účetnictví je ve společnosti řešena samostatným účetním programem bez dalších vazeb na podnikový IS, který je používán již sedm let. K účetním informacím mají přístup účetní a jednatel. Systém splňuje požadavky společnosti, v souvislosti s jeho používáním nevznikají žádné zásadní problémy.

Řízení rizik:

V rámci dotazování se na informační management a řízení rizik bylo zjištěno, že zaměstnanci společnosti tento pojem znají, informační management využívají a provádí také analýzu rizik. Respondentem byla poskytnuta data potřebná pro sestavení registru rizik ekonomického oddělení společnosti.

Tabulka C9: Data pro sestavení registru rizik - respondent číslo 15

Aktivum	Hodnota aktiva	Popis rizika	Pravděpodobnost výskytu hrozby	Pravděpodobnost výskytu zranitelnosti	Riziko	Úroveň rizika	Opatření
Systém ekonomického oddělení	4	Téměř žádná	N	V	6	V	Denní zálohování, externí kontrola
PC	2	Poruchy, mechanické poškození	S	S	4	S	Pravidelné zajištění servisu
Operační systém	3	Nedostatečná aktualizace - nové potřeby zákazníků	S	S	5	S	Nutnost zaktualizování systému
Server	4	Minimální - nové zařízení	N	V	6	V	Bezpečnostní opatření
Zaměstnanci	4	Možná fluktuace	N	V	6	V	Vytvoření lepších pracovních podmínek

Zdroj: vlastní zpracování, 2016

Příloha D: Dotazník

Dotazník

Řízení informačních rizik v organizaci

1) Do které z níže uvedených skupin patří Vaše společnost?

☐ *malé a střední podniky*
(MSP zaměstnává méně než 250 zaměstnanců, aktiva/majetek nepřesahují korunový ekvivalent částky 43 mil. EUR nebo obrat/příjmy nepřesahují korunový ekvivalent částky 50 mil. EUR, minimálně 75% základního kapitálu a hlasovacích práv je ve vlastnictví podniku.)

☐ *velké podniky*

2) Do jaké oblasti spadá předmět podnikání Vaší společnosti?

3) Setkali jste se již s pojmem „informační management“?
(Informační management je definován jako aplikace tradičních manažerských procesů, zejména zásad managementu pro hospodaření se zdroji, k správě informačních zdrojů a dalších aktiv organizace.)

☐ *ano*
☐ *ne*

4) Využívá Vaše společnost informační management (řízení informačních rizik)?

☐ *ano*
☐ *ne*

5) Jakou metodiku řízení informačních rizik využíváte?
(Více možných odpovědí.)

☐ *postupujeme intuitivně*
☐ *ČSN ISO 31000 - Management rizik - Principy a směrnice (01 0351)*
☐ *ČSN IEC/ISO 31010 Management rizik - Techniky posuzování rizik*
☐ *ČSN 36 9790 - Systém managementu bezpečnosti informací*
☐ *jiná metodika*

6) Jaké typy rizik Vaše společnost sleduje?

	rizikům je věnována maximální pozornost	*rizika jsou sledována*	*rizika nesledujeme*
rizika spojená s informačními technologiemi	☐	☐	☐
rizika spojená s informacemi	☐	☐	☐
rizika spojená s lidským faktorem	☐	☐	☐

7) Pokud nevyužíváte informační management, předpokládáte jeho využití v budoucnu?

☐ *ano*
☐ *ne*

8) Jaký informační systém využívá Vaše společnost?
(SAP, QAD, K2, JKR, MS Dynamics, Money S4, jiný)

9) Jedná se o informační systém „na míru“?

☐ *ano*
☐ *ne*

10) Ovlivnily níže uvedené faktory výběr informačního systému ve Vaší společnosti?

	ano	*spíše ano*	*spíše ne*	*ne*
cena	☐	☐	☐	☐
dostupnost servisu	☐	☐	☐	☐
kompatibilita s jinými systémy	☐	☐	☐	☐
nastavení uživatelského prostředí	☐	☐	☐	☐
provázanost modulů	☐	☐	☐	☐
reference ostatních uživatelů informačního systému	☐	☐	☐	☐
rychlost práce s daty	☐	☐	☐	☐

11) Jak je ve společnosti zajištěna bezpečnost dat?
(Více možných odpovědí.)

- ☐ *antivirovým programem*
- ☐ *síťovým firewallem*
- ☐ *jiný způsob*

12) Data jsou zálohována na:
(Více možných odpovědí.)

- ☐ *internetové úložiště*
- ☐ *jiné pevné disky*
- ☐ *server*
- ☐ *záznamová média (CD, DVD, flashdisc)*
- ☐ *jiné možnosti*

13) Kdo spravuje informační systém společnosti?

- ☐ *zaměstnanec/zaměstnanci společnosti*
- ☐ *externí společnost*

14) Jakým způsobem je ve společnosti zajištěna oblast účetnictví?

- ☐ *společnost má vlastní účetní útvar*
- ☐ *účetnictví je zajištěno formou outsourcingu*

15) Jaké jsou důvody pro využití outsourcingu?
(V případě, že společnost využívá outsourcing pro oblast účetnictví.)
(Více možných odpovědí.)

- ☐ *nevyplatí se nám vlastní účtárna*
- ☐ *nemusíme se starat o upgrady softwaru*
- ☐ *jiný důvod*

16) Jaká rizika s sebou, podle Vašeho názoru, přináší outsourcing účetnictví?
(Více možných odpovědí.)

- ☐ *možná ztráta důvěrnosti dat*
- ☐ *výpadek nebo zrušení dodavatele služeb*
- ☐ *jiný typ rizika*

17) Jaká opatření pro minimalizaci rizik plynoucích z outsourcingu účetnictví provádíte?
(V případě, že společnost využívá outsourcing pro oblast účetnictví.)
(např.: smluvní zajištění)

18) Jaký software je používán pro oblast účetnictví?
(V případě, že má společnost vlastní účetní útvar.)

- *samostatný účetní program bez dalších vazeb na podnikový IS*
- *modul, který je součástí IS*

19) Jsou omezena přístupová práva k účetnímu informačnímu sytému/k modulu účetnictví?
(V případě, že má společnost vlastní účetní útvar.)

- *ano*
- *ne*

20) Kdo má přístup k účetním informacím?
(Více možných odpovědí.)

- *zaměstnanci účetního oddělení*
- *management společnosti*
- *jiné možnosti*

21) Poskytuje účetní informační systém výsledné reporty (přehledy) ve Vámi požadované struktuře a kvalitě?
(V případě, že má společnost vlastní účetní útvar.)

- *ano*
- *spíše ano*
- *spíše ne*
- *ne*

22) Splňuje účetní informační systém požadavky na něj kladené?
(V případě, že má společnost vlastní účetní útvar.)

- *ano (v mimořádných případech je nutná podpora dodavatele IS)*
- *spíše ano (občas je nutná podpora dodavatele IS)*
- *spíše ne (je nutná častá podpora dodavatele IS)*
- *ne*