UNIVERZITA JANA AMOSE KOMENSKÉHO PRAHA

BAKALÁŘSKÉ

PREZENČNÍ STUDIUM

2013 - 2016

BAKALÁŘSKÁ PRÁCE

Jiří Čelikovský

Analýza rizik v kontextu norem ČSN ISO/IEC 27005 a ČSN ISO 31000

Praha 2016

Vedoucí bakalářské práce: PaedDr. Ing. Jan Zelinka

JAN AMOS KOMENSKY UNIVERSITY PRAGUE

BACHELOR

FULL-TIME STUDIES

2013 - 2016

BACHELOR THESIS

Jiří Čelikovský

Risk analysis in the context of the ISO/IEC 27005 and ISO 31000 standards

Prague 2016

The Bachelor Thesis Work Supervisor: PaedDr. Ing. Jan Zelinka

Prohlášení

Prohlašuji, že předložená bakalářská práce je mým původním autorským dílem, které jsem vypracoval samostatně. Veškerou literaturu a další zdroje, z nichž jsem při zpracování čerpal, v práci řádně cituji a jsou uvedeny v seznamu použitých zdrojů.

Souhlasím s prezenčním zpřístupněním své práce v univerzitní knihovně.

V Praze dne Jiří Čelikovský

Poděkování

Tímto chci poděkovat vedoucímu své bakalářské práce PaedDr. Ing. Janu Zelinkovi za cenné rady, ochotu a podporu při tvorbě této práce. Dále bych touto cestou rád poděkoval kolektivu vybrané firmy za to, že mi věnoval čas a zpětnou vazbu, kterou mi poskytl při řízeném rozhovoru. V neposlední řadě chci poděkovat Ing. Martině Čelikovské za upřesnění některých skutečností relevantních pro tuto práci.

Anotace

Primárním cílem bakalářské práce je seznámit čtenáře s mezinárodními standardy pro řízení rizik, a to zejména v oblasti bezpečnosti informací. Pro větší názornost je celý proces řízení rizik bezpečnosti informací popsán na vybrané firmě.

V praktické části autor za pomoci dotazníkového šetření zjišťuje úroveň povědomí o analýzách a řízení rizik bezpečnosti informací. Dále za pomoci řízeného rozhovoru se zástupci managementu vybrané firmy a odborníky z oblasti zjišťuje, jak je systém řízení a analýz rizik vnímán na vrcholové úrovni.

V závěru práce se autor věnuje zhodnocení výsledků průzkumů a navržení možných opatření nebo vylepšení v rámci řízení rizik bezpečnosti informací ve vybrané firmě.

Klíčová slova

Analýza rizik, aktivum, bezpečnost informací, ISO, management rizik, mezinárodní standardy řízení, riziko, systém řízení.

Annotation

The primary objective of this bachelor thesis is to present the international standards for risk management, especially in the area of information security to the reader. For better illustration has the entire process of information security risk management been described on a selected company.

The author intends to determine the level of awareness about the analysis of information security risks and their management in the practical part. Furthermore controlled interviews with the selected company´s management representatives and experts in this relevant field are to be used in order to determine the perception of the risk management and risk analysis at the executive level.

The assessment of the surveys´ results together with proposals of potential arrangements or improvements within the information security risk management area in the selected company are presented in the final part of the thesis.

Keywords

Asset, information security, ISO, international management standards, management system, risk, risk analysis, risk management.

ÚVOD

Analýzy rizik jsou každodenní součástí života jedince i firmy. Mnoho lidí si ani neuvědomuje, že analýzu rizika používá. V souladu s cíli práce se autor věnuje analýzám rizik v kontextu mezinárodních norem ČSN ISO/IEC 27005 Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací a ČSN ISO 31000 Management rizik – Principy a směrnice. Vzhledem k obsáhlosti tématu vybral autor firmu, na jejímž příkladu bude demonstrovat a analyzovat průběh procesu řízení rizik.

Primárním cílem bakalářské práce je seznámit čtenáře s mezinárodními standardy pro řízení rizik, a to zejména v oblasti bezpečnosti informací. Celý proces řízení rizik bezpečnosti informací autor popisuje, pro větší názornost, na vybrané firmě.

V praktické části chce autor za pomoci dotazníkového šetření zjistit úroveň povědomí o analýzách a řízení rizik bezpečnosti informací. Dále za pomoci řízeného rozhovoru se zástupci managementu vybrané firmy a odborníky z oblasti zjistit, jak je systém řízení a analýz rizik vnímán na vrcholové úrovni.

Autor stanovil hypotézy pro praktickou část práce. Hypotézy číslo 1 až 4 jsou určeny pro potvrzení nebo vyvrácení pomocí dotazníkového šetření, hypotéza číslo 5 je určena pro potvrzení nebo vyvrácení pomocí řízených pohovorů s pracovníky zařazenými na příslušných pozicích.

1. Autorovo přesvědčení je takové, že obecné povědomí o analýzách rizik je nízké.
2. Laická veřejnost považuje pojem aktivum za účetní položku bez vztahu k rizikům.
3. Velikost firmy ovlivňuje povědomí o problematice a vědomí závažnosti analýz rizik.
4. Audit ve firmě není prováděn jako bezpečnostní prověrka, ale pouze jako ekonomická nebo finanční kontrola.

5. Střední a vyšší management firmy je dostatečně informován o významu analýzy rizik.

Práci autor dělí na teoretickou a praktickou část. V teoretické části objasňuje základní pojmy a uvádí základní definice, dále popisuje způsob řízení rizik bezpečnosti informací v kontextu ČSN ISO/IEC 27005 v obecné rovině, seznamuje čtenáře s vybranou firmou, objasňuje metodiku analýz rizik používaných ve vybrané firmě a popisuje výstupy z analýz rizik vybrané firmy.

Výstupy z průzkumů pomohou vrcholovému vedení vybrané firmy k lepšímu pochopení vnímání řízení rizik a jejich analýz v oblasti bezpečnosti informací. Takové pochopení vrcholovým vedením může směrovat k celkovému zlepšení celého systému řízení bezpečnosti informací, zejména v oblasti lidských zdrojů. Sekundárním přínosem je stručný popis procesu řízení rizik dle mezinárodních norem a objasnění základních pojmů a definic.

Zástupci vedení vybrané firmy si nepřejí, aby v této bakalářské práci byla firma konkretizována. Autor tedy volí označování firmy jako **vybrané firmy.** Veškeré údaje o vybrané firmě, firemních dokumentech a dalších záležitostech týkajících se dotčené firmy jsou uváděny v obecných pojmech. Autor tedy neuvádí čísla a celé názvy dokumentů, na které odkazuje, ale pouze obecné názvy bez interního označení. Stejně jako u dokumentů jsou zobecněny i výstupy z analýzy rizik vybrané firmy. Veškeré informace a data o vybrané firmě jsou podloženy existující a platnou firemní dokumentací.

TEORETICKÁ ČÁST

1 ZÁKLADNÍ POJMY A DEFINICE

Autor v této kapitole popisuje a vysvětluje základní pojmy v oblasti analýzy rizik. Těmito pojmy jsou: Aktivum, hrozba, zranitelnost, protiopatření a vlastní riziko. Každému jednotlivému pojmu je věnována podkapitola, vzhledem k drobným odlišnostem v definicích uvedených v různých zdrojích. Tyto drobnosti se mohou zdát jako malicherné hrátky se slovy, ale mnohdy mohou značně změnit význam pojmu a tím i jeho chápání.

1.1 Aktivum

Značná část populace si pod pojmem aktivum představí účetní položku. Při analýzách rizik bezpečnosti informací je aktivem myšleno cokoliv, co má pro firmu hodnotu. Například i data, zaměstnanci nebo patentová práva.

Smejkal s Raisem doslova uvádějí, že *„Aktivum je všechno, co má pro subjekt hodnotu, která může být zmenšena působením hrozby.“*[1]

1.2 Hrozba

Hrozbou se rozumí jakákoli síla, která je schopná využít zranitelnosti aktiva a tím způsobit riziko. Tuto definici autor vytvořil poté, co nastudoval několik různých definic a vysvětlení, zjistil praxí jak je hrozba (jako pojem) vnímána a sám začal aktivně proces analýzy rizik používat.

Jedna z dalších používaných definic zní: *„Jakýkoli fenomén, který má potenciální schopnost poškodit zájmy a hodnoty chráněné státem. Míra hrozby je dána velikostí*

[1] SMEJKAL, V., K. RAIS. *Řízení rizik ve firmách a jiných organizacích.* Praha : Grada Publishing, a.s., 2006, s. 82. ISBN: 80-247-1667-4.

možné škody a časovou vzdáleností (vyjádřenou pravděpodobností čili rizikem) možného uplatnění této hrozby.“[2]

Tato definice aplikovaná do soukromého sektoru může znít následovně: Jakýkoli fenomén, který má potenciální schopnost poškodit zájmy firmy. Míra hrozby je dána velikostí možné škody a časovou vzdáleností možného uplatnění této hrozby.

Řada norem ISO/IEC 27000 definuje pojem **hrozba** jako: „*Potenciální příčina nechtěného incidentu, jehož výsledkem může být poškození systému nebo organizace“*[3]

1.3 Zranitelnost

„Zranitelnost je nedostatek, slabina nebo stav analyzovaného aktiva (případně subjektu nebo jeho části), který může hrozba využít pro uplatnění svého nežádoucího vlivu.“[4]

Autor v rámci výkonu svého povolání vysvětluje zranitelnost takto: Hrozba využije zranitelnosti a tím vzniká riziko. Zranitelností lze chápat například bezpečnostní nedostatek, narušení fyzického či logického perimetru apod., přičemž tohoto nedostatku může využít hrozba, která vygeneruje riziko.

Smejkal s Raisem ještě zmiňují fakt, že úroveň zranitelnosti aktiva je hodnocena dle dvou faktorů, a to:

1. Citlivostí, kterou vysvětlují jako náchylnost aktiva být poškozeno konkrétní hrozbou.
2. Kritičnost, která je definována jako důležitost aktiva pro analyzovaný objekt.[5]

---

[2] Ministerstvo Vnitra České republiky [online]. 2003 [cit. 2015-12-28]. Dostupné z: http://www.mvcr.cz/clanek/hrozba.aspx

[3] UNMZ. ČSN ISO/IEC *27000 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník.* Praha : Uřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014. s. 17. 95885.

[4] SMEJKAL, V., K. RAIS. *Řízení rizik ve firmách a jiných organizacích.* Praha : Grada Publishing, a.s., 2006, s. 83. ISBN: 80-247-1667-4.

[5] Tamtéž.

1.4 Protiopatření

Protiopatření nebo také pouze opatření má mnoho různých definic a výkladů. Nejvýstižnějším se autorovi jeví definice uvedená ve Slovníku k managementu rizik, která zní: *„Prostředek řízení, který modifikuje riziko.“*[6]

Opatřeními lze chápat jakýkoli proces, pravidlo, zařízení nebo postup, které mohou modifikovat riziko. Opatření nemusejí vždy působit tak, jak byla zamýšlena, to znamená, že nemusejí způsobit zamýšlený modifikující účinek.

Pro názornou představu autor uvádí jako příklad bezpečnostní prvky ve vozidle. Konkrétně bezpečnostní pásy a airbagy. Obě tato opatření, jak pásy, tak airbagy mají za úkol zmírnit dopady na posádku vozu v případě nehody. V případě, že posádka není připoutána bezpečnostním pásem a nehoda se stane, může být usmrcena aktivovaným airbagem. Přitom nehoda nemusela být nijak vážná, ani ve vysoké rychlosti. Zde airbag, jako opatření pro zmírnění dopadu nehody na posádku nezpůsobil zamýšlený modifikující efekt.[7]

1.5 Riziko

Tento pojem je velmi často používán výhradně s negativními konotacemi. Obecně se za riziko dá považovat i potenciální možnost kladného a příznivého výsledku. Konkrétně ve slovníku k managementu rizik je napsáno, že riziko je aplikace nejistoty na konečný plánovaný výsledek s poznámkami, že odchylka **může** být jak kladná, tak záporná.[8]

Riziko v rámci managementu rizik vyjadřuje míru ohrožení aktiva. Velikost rizika je označována jako úroveň nebo míra rizika.

---

[6] UNMZ. TNI 01 0350 *Management rizik - Slovník (Pokyn 73)*. Praha : Úřad pro normalizaci, metrologii a státní zkušebnictví, 2010. s. 14. 86437.

[7] Autor si je vědom nutnosti používání obou zmiňovaných opatření ve vzájemné kooperaci. Příklad uvedl, mimo jiné kvůli tomu, že v poslední době několikrát slyšel věty typu: „Nač se poutat? Máme airbagy.“

[8] UNMZ. TNI 01 0350 *Management rizik - Slovník (Pokyn 73)*. Praha : Úřad pro normalizaci, metrologii a státní zkušebnictví, 2010. s. 8. 86437.

2 ŘÍZENÍ RIZIK BEZPEČNOSTI INFORMACÍ

V této kapitole autor čtenáři přibližuje principy a metody řízení rizik bezpečnosti informací v kontextu mezinárodní normy ČSN ISO/IEC 27005 a ČSN ISO 31000.

ČSN ISO/IEC 27005 je normou z řady standardů zabývajících se informačními technologiemi, konkrétně bezpečnostními technikami. Celá norma je členěna do 12 kapitol, kde první čtyři kapitoly obsahují obecné informace, jako například: předmět normy, citované dokumenty, termíny a definice a strukturu normy. Zajímavou se norma stává od kapitoly páté, která se zabývá podkladovými informacemi, obecný popis procesu řízení rizik je uveden v kapitole šesté, sedmá kapitola se zabývá stanovením kontextu, osmá kapitola řeší posouzení rizik, devátá kapitola popisuje možná ošetření rizik, desátá kapitola hovoří o akceptaci rizik, jedenáctá kapitola je zaměřena na komunikaci rizik a poslední dvanáctá kapitola řeší oblast monitorování a přezkoumání rizik.

ČSN ISO 31000 je výchozí normou v řadě standardů zabývajících se managementem rizik. V tomto případě vysvětluje principy a zásady, které jsou vhodné pro použití při managementu rizik. Norma popisuje vazby mezi Zásadami v kapitole třetí, Rámcem v kapitole čtvrté a Procesem v kapitole páté.

Autor se věnuje především procesu a praktickému používání managementu rizik se zaměřením na specifickou oblast bezpečnosti informací. Proto zde uvádí oba standardy, ve kterých je management rizik řešen. V obecné rovině je možné říci, že standard ČSN ISO 31000 provádí celým systémem managementu rizik v rámci celé organizace a standard ČSN ISO/IEC 27005 konkretizuje poznatky a techniky do oblasti bezpečnosti informací.

2.1 Zásady, rámec a proces managementu rizik

Vazby a interakce mezi zásadami, rámcem a procesem řízení rizik dle normy ČSN ISO 31000 jsou znázorněny graficky v Příloze A.

V části věnované zásadám managementu rizik hovoří standard ČSN ISO 31000 o principech, které je nutné brát v úvahu proto, aby byl systém managementu rizik efektivní. Jedná se především o to, že management rizik:

1. Vytváří a chrání hodnoty.
2. Není izolovanou činností od ostatních procesů firmy.
3. Je důležitou součástí při rozhodování na všech úrovních řízení.
4. Je primárně zaměřen na nejistoty.
5. Je systematický a včasný.
6. Je upravený na míru, pro potřeby firmy.
7. Zohledňuje lidské, kulturní, politické a další faktory.
8. Je dynamický.[9]

Tyto zásady jsou, dle názoru autora, nejdůležitějšími. Pokud vrcholové vedení firmy přijme tyto zásady a bude se jimi řídit, je velmi pravděpodobné, že bude systém řízení rizik funkční a prospěšný firmě. Toto je teoretická část celého systému managementu rizik.

Další, již praktickou částí je rámec managementu rizik. Standard ČSN ISO 31000 hovoří o rámci managementu rizik hlavně kvůli jasnému vymezení oblasti, které se bude systém managementu rizik věnovat. V ideálním světě bude systém managementu rizik přijatý, pochopený a používaný napříč celou firmou. V realitě se většinou jedná o část firmy, její úsek, pobočku nebo jen určitý typ projektu. V této části systému managementu rizik je již uváděn a aplikován Demingův cyklus PDCA.[10]

Nejzajímavější, ale také nejnáročnější je část standardu ČSN ISO 31000 věnující se procesu managementu rizik. Na tuto část se také odkazuje standard ČSN ISO/IEC 27005, který se věnuje již čistě řízení rizik bezpečnosti informací. Jedná se také o část, které se autor věnuje samostatně, v následující části.

[9] UNMZ. *ČSN ISO 31000 Management rizik - Principy a směrnice.* Praha : Uřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2010. s. 18. 86884.
[10] PDCA – z anglického: Plan – Do –Check – Act (Plánuj – dělej – kontroluj – jednej). PDCA je metoda postupného zlepšování, kterou popsal americký statistik William Edwards Deming.

2.2 Proces managementu rizik

Proces managementu rizik je podobně popsán v kapitole 5 standardu ČSN ISO 31000 Management rizik – Principy a směrnice. Autor považuje za nutné upozornit na fakt, že standard ČSN ISO 31000 popisuje obecně management rizik. Standard ČSN ISO/IEC 27005 – Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací již konkretizuje management rizik směrem do oblasti bezpečnosti informací. Autor zde tedy volí, jako referenční standard a rámec pro poskytované informace a popisované skutečnosti kontext standardu ČSN ISO/IEC 27005.

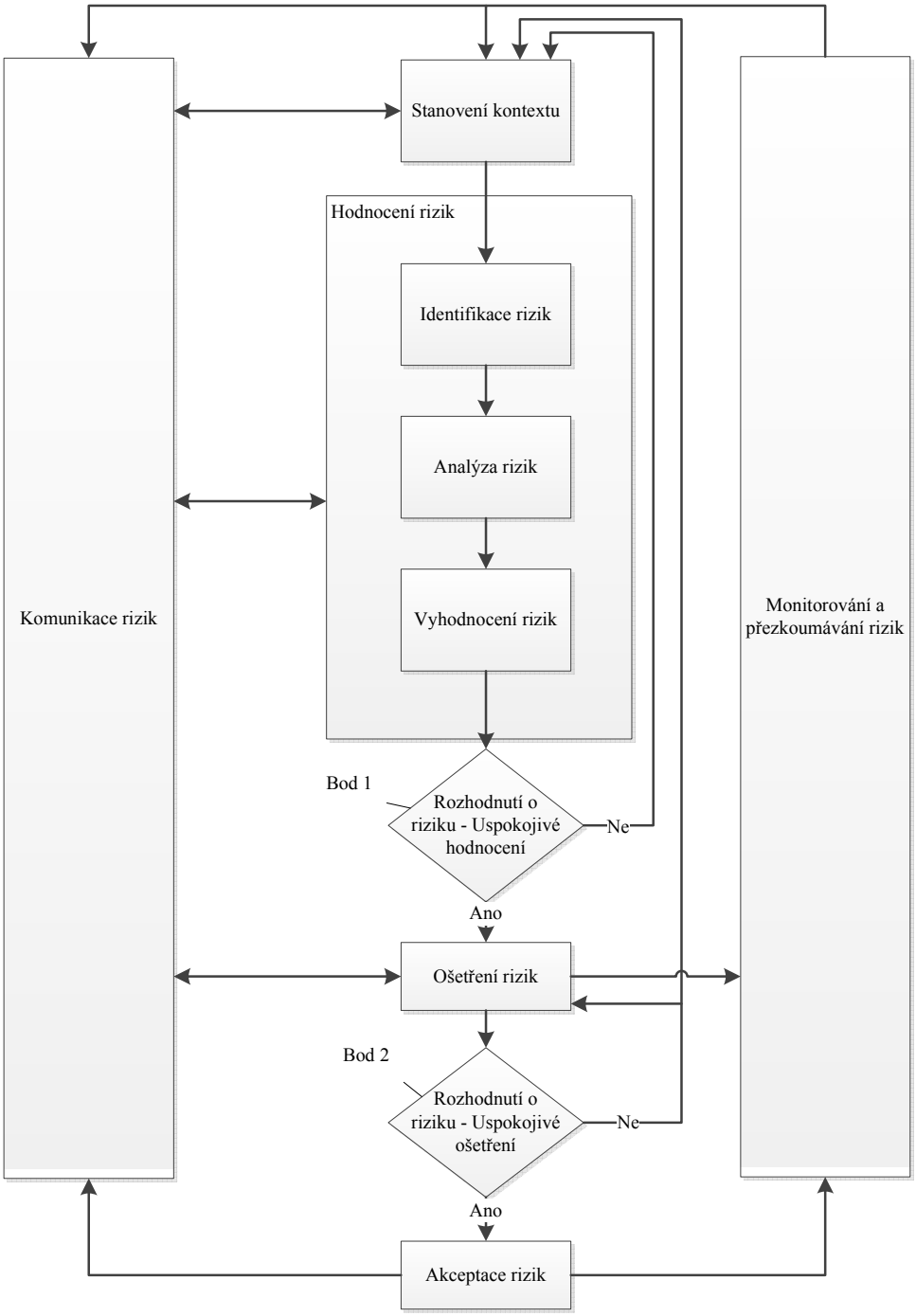
Přehled procesu řízení rizik je znázorněn v Příloze A v části Proces a vychází ze standardu ČSN ISO 31000. Proces řízení rizik bezpečnosti informací je znázorněn na obrázku číslo 1.

Z obrázku číslo 1 vyplývá, že se proces řízení rizik bezpečnosti informací může v několika svých bodech opakovat. Princip tohoto opakování, cyklu, vychází z Demingova cyklu PDCA. Tento cyklus je nejvíce zřetelný na celé činnosti posouzení rizik a zároveň na části ošetření rizik. Tento cyklický postup zajišťuje správnou rovnováhu mezi časovou náročností a vynaloženými zdroji potřebnými k identifikaci opatření. Stále je ovšem stále zajištěno, že rizika s vysokou mírou jsou náležitě posouzena.

V textu standardu ČSN ISO/IEC 27005 je tento obrázek popsán následovně: *„Nejdřív se stanoví kontext. Pak se provádí posouzení rizik. Pokud toto poskytne dostatek informací pro efektivní určení akcí nutných pro modifikaci rizik na přijatelnou úroveň, pak je úkol dokončen a následuje ošetření rizik. Jestliže jsou informace nedostatečné, musí být provedeno další opakování posouzení rizik s revidovaným kontextem (např. kritérii posouzení rizik, kritérii akceptace rizik nebo kritérii dopadu), možná jen na omezených částech celkového rozsahu.“*[11] Viz obrázek číslo 1, Bod 1.

[11] UNMZ. *ČSN ISO/IEC 27005 Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací.* Praha : Uřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013. s. 14. 93071.

Obrázek 1: Znázornění procesu řízení rizik bezpečnosti informací



Zdroj[12]

[12] UNMZ. *ČSN ISO/IEC 27005 Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací.* Praha : Uřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013. s. 14. 93071.

Účinnost ošetření rizik je přímo závislá na kvalitě a výsledcích posouzení rizik. V oblasti ošetření rizik probíhá cyklický proces, který, dle standardu ČSN ISO/IEC 27005, obsahuje následující kroky:

- Posouzení ošetření rizik.
- Rozhodnutí o akceptovatelnosti zbytkového rizika.
- V případě, že úrovně rizika jsou i po ošetření neakceptovatelná, následuje aplikace nového ošetření rizik.
- Posouzení účinnosti ošetření rizik.[13]

V praxi se často stává, že prvotní ošetření rizik nemá ihned zamýšlený účinek. Respektive míra rizika je i přes použité opatření stále nad hranicí akceptovatelnosti. V takovém případě probíhá znovu hodnocení rizika se zohledněním přijatého opatření tedy s úpravou parametrů kontextu pro hodnocení rizika. Po opakovaném hodnocení rizik následuje další ošetření rizik.

Standard ČSN ISO/IEC 27005 uvádí k akceptaci rizik následující: *„Činnosti akceptace rizik musí zajistit, aby vedoucí pracovníci organizace zbytková rizika explicitně přijali. To je důležité zejména v situaci, kdy je zavedení opatření opomenuto nebo odloženo, např. kvůli nákladům.“*[14]

Obecně platí, že opatření použitá k ošetření rizik musejí být úměrná míře rizika. To znamená, že v případě vysoké pravděpodobnosti výskytu nebo vysokému dopadu budou použitá ošetření robustnějšího a z pravidla nákladnějšího typu. U rizik s nízkou mírou rizika budou zákonitě použitá ošetření odpovídajícího rozsahu. Při objasňování tohoto principu v praxi autor používá příklad, ve kterém uvádí, že je zbytečné na komára používat vysoké množství trhaviny.

Použitá opatření mají za úkol omezit riziko. V případě, že by použitá opatření měla destabilizační účinek, je nutné opakovat hodnocení rizik, včetně ošetření rizik tak, aby výsledek neměl dopady na funkčnost, akceschopnost a ekonomickou stabilitu firmy.

[13] UNMZ. *ČSN ISO/IEC 27005 Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací.* Praha : Uřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013. s. 15. 93071.
[14] Tamtéž.

2.2.1 Identifikace rizik

Základní částí celého procesu řízení rizik je identifikace rizik. Identifikace rizik probíhá v několika krocích, které na sebe mohou navazovat v různém pořadí. Pořadí kroků při identifikaci rizik je závislé na zvolené metodice analýzy rizik.

Identifikace rizik obsahuje následující kroky:

Identifikaci aktiv a jejich vlastníků.[15]

V rámci identifikace aktiv se uvádí informace týkající se vlastníka nebo vlastníků aktiva, místa výskytu aktiva, funkce aktiva a další relevantní informace potřebné pro vlastní identifikaci aktiv. Aktiva se identifikují v rámci stanoveného rozsahu.

Identifikace hrozeb.

Pro identifikaci hrozeb jsou vstupem informace získané z přezkoumání případných dřívějších incidentů, od vlastníků aktiv, jejich uživatelů a eventuálně z jiných zdrojů. Jiným zdrojem pro identifikaci hrozeb mohou být vlastní zkušenosti týmu, který provádí celou identifikaci, hrozby identifikované státní správou, katalog hrozeb obsažený v softwarovém nástroji určeném pro analýzy rizik.

Identifikace stávajících opatření.

Při identifikaci aktiv jsou zohledňována stávající a plánovaná opatření. Hlavním účelem tohoto kroku je efektivita celého procesu. Identifikace stávajících opatření má potenciál ušetřit práci nebo případné náklady v případě duplikace ošetření.

V případě identifikace stávajícího opatření se provádí rovnou ověření funkčnosti a účinnosti opatření. Citlivým místem v této fázi je možnost nefunkčního nebo špatně fungujícího opatření, které má potenciál svojí nefunkčností způsobit zranitelnost. Standard ČSN ISO/IEC uvádí, že identifikaci stávajících opatření mohou napomoci činnosti spojené s přezkoumáním dokumentace k opatřením, provedení kontrol

[15] Vlastníkem aktiva není myšlen vlastník po účetní stránce, ale entita, která má aktivum v užívání a má tedy přímý vliv na aktivum.

s pracovníky, kteří mají odpovědnost za bezpečnost informací, přezkoumání fyzických opatření na místě, srovnání použitých a navrhovaných opatření a kontrola z hlediska funkčnosti a účinnosti nebo přezkoumání výsledků interních auditů.[16]

Identifikace zranitelností

Zranitelnosti se identifikují v několika různých oblastech, které jsou však vzájemně provázané. Jedná se o oblasti, které přímo ovlivňují chod společnosti.

„Zranitelnosti lze identifikovat v těchto oblastech:

- *Organizace.*
- *Procesy a postupy.*
- *Běžné praxe řízení.*
- *Pracovníci.*
- *Fyzické prostředí.*
- *Konfigurace informačního systému.*
- *Hardware, software nebo komunikační zařízení.*
- *Závislost na externích stranách.“*[17]

Existence zranitelností nepůsobí škodu, protože zranitelnost musí být využita hrozbou. V takovém případě již škoda vzniká. Zranitelnosti, které nemají potenciál způsobit škodu, tedy nemají hrozbu, nemusejí mít identifikována opatření. Takové zranitelnosti musejí být identifikovány a monitorovány.

Identifikace následků

Identifikace následků je závislá na znalostech a zkušenostech týmu, který provádí celou analýzu aktiv, respektive celou analýzu rizik. V tomto kroku opět vstupují do procesu vlastníci aktiv, kteří spolupracují s realizačním týmem na identifikaci následků, které mohou mít pro aktivum za následek ztrátu důvěrnosti, dostupnosti a integrity.

[16] UNMZ. *ČSN ISO/IEC 27005 Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací.* Praha : Uřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013. s. 20. 93071.
[17] Tamtéž. S. 21.

Následkem se v kontextu analýz rizik rozumí například: ztráta funkce aktiva, nepříznivé podmínky pro provoz aktiva, ztráta obchodu, klíčových pracovníků, dobrého jména, finanční ztráty atd.

Činnosti spojené s identifikací následků sledují možné dopady na organizaci, které by mohly být způsobené incidentem. *„Následek může ovlivnit jedno nebo více aktiv nebo jen část aktiva.“*[18] Následky se dělí do dvou základních kategorií, a to na dočasné[19] a trvalé[20].

2.2.2 Analýza rizik

Metodiky analýzy rizik

Analýzy rizik jsou prováděny v různých úrovních podrobnosti. Tato úroveň je závislá na stavu aktiv, respektive jejich kritičnosti, rozsahu známé zranitelnosti a eventuálních incidentech, které aktiva postihly.

Jsou používány buď kvantitativní, nebo kvalitativní analýzy rizik. *„Kvantitativní analýza rizik používá stupnici s číselnými hodnotami (spíše než popisné stupnice používané při kvalitativní analýze rizik), jak pro následky, tak pro pravděpodobnost, a využívá při tom data z různých zdrojů.“*[21] Kvantitativní způsob analýzy je velmi citlivý na úplnosti číselných hodnot a aktuálnosti používaných modelů. Velmi často jsou využívána historická data incidentů. Značnou nevýhodou je nedostatek takových dat u nově vzniklých rizik nebo slabin společnosti.

Kvalitativní analýza rizik, jak uvádí standard ČSN ISO/IEC 27005, používá k popisu následků a pravděpodobností škálu kvalifikačních atributů. Jak výhodnou vlastnost kvalitativní analýzy je nutné uvést to, že ji všichni příslušní pracovníci mohou

[18] UNMZ. *ČSN ISO/IEC 27005 Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací.* Praha : Uřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013. s. 20. 93071.
[19] Dočasné následky – mohou znamenat například momentální nedostupnost aplikace nebo serveru v případě výpadku napájení.
[20] Trvalé následky – znamenají trvalou nedostupnost například při zničení aktiva. K trvalým následkům je možné zařadit i ztrátu dobrého jména.
[21] UNMZ. *ČSN ISO/IEC 27005 Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací.* Praha : Uřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013. s. 22. 93071.

snadno pochopit. Naopak mezi nevýhody je nutné zařadit závislost na subjektivním výběru škály.[22]

Kvalitativní analýzu rizik je vhodné použít zejména na počátku procesu, při zjišťování a identifikaci rizik, která je nutné zkoumat podrobněji, tam, kde je tento způsob analýzy vhodný k rozhodnutí o riziku a v takových oblastech, kde nejsou vhodné číselné údaje nebo zdroje pro kvantitativní analýzu.

Ve čtvrté kapitole autor popisuje jím použitou konkrétní metodiku na příkladu vybrané firmy.

Posouzení následků

Při posuzování následků je vhodné brát v úvahu hodnotu aktiv dotčených těmito následky. Dopady na organizaci se vyjadřují buď kvalitativně, nebo kvantitativně. Velmi často jsou dopady vyjadřovány ve finančních částkách. Tato skutečnost napomáhá při rozhodování nebo proces rozhodování zefektivňuje.

Na počátku hodnocení následků stojí hodnocení aktiv dle jejich kritičnosti a důležitosti pro obchodní činnost organizace.

„Hodnocení se tedy určuje za použití těchto dvou kritérií:

- *Hodnoty za náhradu aktiva: náklady na obnovení a náhradu informace (je-li to vůbec možné), a*
- *Obchodní následky ztráty nebo kompromitace aktiva…“*[23]

Určení pravděpodobnosti incidentu

V tomto kroku celé analýzy rizik se vychází ze dvou možných zdrojů. Prvním zdrojem jsou záznamy o uskutečněných incidentech daného typu. Druhým zdrojem je

[22] UNMZ. *ČSN ISO/IEC 27005 Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací.* Praha : Uřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013. s. 22. 93071.
[23] Tamtéž.

kvalifikovaný odhad pracovníků provádějících analýzu rizik, popřípadě vlastníka aktiva.

Dle standardu ČSN ISO/IEC 27005 se dále bere zřetel na zranitelnosti a existující opatření spolu s jejich účinností na snížení zranitelnosti. Dalšími možnými podklady pro určování pravděpodobnosti incidentu jsou například: atraktivita a zranitelnost aktiva pro případného útočníka, geografické faktory, selhání a poruchy zařízení apod.[24]

Určení úrovně rizik

Úroveň rizika vychází z hodnoty aktiva, pravděpodobnosti výskytu hrozby a dopadu hrozby na aktivum.

Hodnocení rizik

Hlavním účelem hodnocení rizik je být jedním z podkladů při rozhodování o tom, která rizika mají být ošetřena a pro stanovení priorit pro implementování řešení.[25]

Rozhodnutí o ošetření rizik musejí vzít v úvahu širší kontext rizik a také toleranci rizik třetími stranami mimo organizaci, které mají z rizik benefit. Při takovém rozhodování je nutné brát v potaz požadavky zákonů, předpisů a další požadavky.[26][27]

Jedním z výstupů z hodnocení rizik může být rozhodnutí neošetřovat riziko jinak, než jak je ošetřeno dosavadními opatřeními nebo například rozhodnutí provést další analýzu.

2.2.3 Ošetření rizik

Standard ČSN ISO/IEC 27001, podle kterého se provádějí certifikační audity, uvádí v kapitole týkající se ošetření rizik bezpečnosti informací následující: *„Organizace musí implementovat plán ošetření rizik bezpečnosti informací. Organizace musí*

[24] UNMZ. *ČSN ISO/IEC 27005 Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací.* Praha : Uřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013. s. 23. 93071.
[25] UNMZ. *ČSN ISO 31000 Management rizik - Principy a směrnice.* Praha : Uřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2010. s. 31. 86884.
[26] Tamtéž. S. 32.
[27] Dalšími požadavky mohou být například požadavky zákazníků.

uchovávat dokumentované informace o výsledcích posuzování rizik bezpečnosti informací.“[28]

Cílem celé činnosti ošetřování rizik jsou vybraná opatření směřující k jedné z možností ošetření rizika.

Existují čtyři možnosti jak rizika ošetřit:

- Modifikace rizik.
- Podstoupení rizik.[29]
- Vyhnutí se riziku.
- Sdílení rizik.

Výstupem z celé činnosti by měly být plány ošetření rizik a seznam zbytkových rizik, která je nutné akceptovat vedením společnosti.

Jednotlivé možnosti ošetření rizik jsou popsány v následujících odstavcích.

Modifikace rizik

Cílem této možnosti je upravení úrovně rizika přijetím, odstraněním nebo provedením změny opatření, aby bylo zbytkové riziko hodnotitelné jako přijatelné (akceptovatelné). Podrobné informace o opatřeních jsou uvedeny ve standardu ČSN ISO/IEC 27002.

Podstoupení rizik

V rámci definování kontextu organizace je stanovena úroveň rizika, při které je akceptovatelné. Jestliže úroveň rizika splňuje kritérium akceptace rizik (podstoupení rizik), není nutné přijímat další opatření a riziko je možné podstoupit. Konečné rozhodnutí o akceptaci rizik náleží vrcholovému vedení organizace.

---

[28] *UNMZ. ČSN ISO/IEC 27001 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky*. Praha : Uřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014. s. 12. 95805.

[29] Termín „Podstoupení rizika“ je používán standardem ČSN ISO/IEC 27005. Standard ČSN ISO/IEC 27001 používá výraz „Akceptace rizik“.

Vyhnutí se riziku

Tato možnost klade důraz na odpovědnost organizace. V případě, že zjištěná rizika mají příliš vysokou úroveň nebo náklady na ošetření rizik převyšují přínosy, může se organizace riziku vyhnout tím, že plánovanou nebo existující činnosti nebude dále vykonávat. Další možnou cestou je modifikace podmínek, za nichž je činnost organizace vykonávána.[30]

Sdílení rizik

Sdílením rizik v kontextu mezinárodních standardů pro řízení rizik obecně a řízení rizik bezpečnosti informací je myšleno například pojištění.

Standard ČSN ISO/IEC 27005 explicitně upozorňuje na vnímání sdílení rizik následovně: *„Je však nutné upozornit na to, že je možné sdílet odpovědnost za zvládnutí rizika, ale obvykle není možné sdílet odpovědnost za dopad. Zákazníci obvykle posuzují nepříznivý dopad jako chybu organizace.“*[31]

2.2.4 Akceptace rizik bezpečnosti informací

Akceptaci rizika lze též nazvat přijetí rizika. Je to akt vědomého rozhodnutí převzít určité riziko. Tato rozhodnutí je vhodné zaznamenávat, nejlépe i s kontextem toho, jaké informace akceptaci rizika předcházely a pomocí jaké metody byla stanovena hranice akceptovatelnosti. Jako nejvhodnější formu zaznamenání práce s riziky uvádí standard ČSN ISO/IEC 27005 tvorbu Plánu ošetření (zvládání) rizik[32].

V praxi není vždy snadné určit optimální hranici akceptovatelnosti rizika. Pokud se použije pouze číselná hodnota, může dojít i k přijetí rizika, které by mělo být ošetřeno. V základním principu u akceptovaných rizik dochází ke dvěma stavům:

[30] Modifikace kontextu. Může zahrnovat modernizaci technologie, zpřísnění kontrol, lepší výběr dodavatelů apod.
[31] UNMZ. *ČSN ISO/IEC 27005 Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací.* Praha : Uřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013. s. 27. 93071.
[32] UNMZ. *ČSN ISO/IEC 27005 Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací.* Praha : Uřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013. s. 27. 93071.

- Akceptace bez ošetření a
- akceptace s ošetřením.

Akceptace bez ošetření

Takové riziko je následně sledováno a lze ho prohlásit přímo za riziko zbytkové

Akceptace rizika s ošetřením

Plány ošetření akceptovaných rizik mají za úkol snížit hodnotu rizika, či takové riziko minimalizovat. V plánech se uvádí nejen opatření, která vedou ke snížení rizika, ale i časový rámec, potřebné zdroje a zejména dobu a metodu přehodnocení rizika po jeho ošetření. Riziko, které je přítomno i po ošetření akceptovaného rizika nazýváme rizikem zbytkovým.

Obecně lze akceptaci doporučit v případech nízkých rizik s minimálním dopadem. V takových případech bývá velmi neekonomické a neefektivní vynakládat prostředky a čerpat zdroje.

2.2.5 Monitorování a přezkoumávání rizikových faktorů

Mezi rizikové faktory řadíme hodnotu aktiv a jejich zranitelnost, hrozby, které mohou zranitelnosti aktiva využít, dopady, které hrozba při svém výskytu způsobí. Dále jako faktor zařazuje i velmi komplikovanou oblast pravděpodobnosti výskytu hrozby resp. jejího zapůsobení na zranitelnost posuzovaného aktiva.

Rizika nejsou stálá a stejně tak i rizikové faktory se mohou v čase a prostoru měnit. Ke změnám může docházet i bez varování, náhle bez předchozího varování a proto je nutné sledovat celkový obraz rizik pravidelně a stále. Rizika mohou ovlivňovat i obchodní rozhodnutí firmy.

Standard ČSN ISO/IEC 27005 uvádí jako výstup monitorování a přezkoumání rizikových faktorů: *„Kontinuální soulad řízení rizik s obchodními cíli organizace a s kritérii akceptace rizik*[33]*“*

2.2.6 Monitorování, přezkoumání a zlepšování řízení rizik

Jak autor zmínil výše, celý proces řízení rizik by měl být monitorován. Hlavním účelem monitorování a přezkoumávání rizik je zajištění souladu se stanovenými cíli a v neposlední řadě získáme díky pravidelnému monitoringu i informace o tom, zda proces řízení rizik je neustále přiměřený okolnostem.

Při přezkoumání procesu řízení rizik je nutné přihlédnou k právnímu a environmentálnímu kontextu organizace. Významný vliv na celý proces řízení rizik může mít i konkurenční prostředí dané organizace. Vlivy je proto nutno neustále sledovat a pravidelně posuzovat.

Indikátorem efektivně implementovaného procesu řízení rizik je nepochybně snížený výskyt rizikových situací a událostí. Díky sledování efektivity zavedených opatření se může vedení společnosti rozhodnout k akceptaci dalších rizik, případně ke zmírnění zavedených opatření. Nastavení pravidelného monitorování a přezkoumávání řízení rizik zajišťuje, aby nedošlo ke zhoršení situace.

2.2.7 Zaznamenávání informací v procesu řízení rizik

Doložitelnost a dohledatelnost dokumentovaných informací, které vznikají v průběhu procesu řízení rizik, je jedinou možnou cestou k opravdovému řízení rizik. Při změnách, ke kterým dochází jak v interním, tak v externím kontextu organizace, je nutné znát celou genezi řízení rizik. Toto umožňuje získání zpětné vazby a ověřování si stanovených opatření zejména z pohledu jejich účinnosti a účelnosti.

Podrobné vedení záznamů zejména z analýzy rizik umožňuje v případě potřeby změnu týmu, aniž by hrozilo, že budou všechna aktiva, rizika, hrozby, zranitelnost

[33] UNMZ. *ČSN ISO/IEC 27005 Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací.* Praha : Uřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013. s. 29. 93071.

apod. přeposuzována. Opětovná identifikace aktiv a jejich rizik je velmi neefektivní. V praxi je doložen předpoklad, že dochází při použití různých metod k identifikaci shodných, nebo alespoň podobných hodnot. Střídání různých přístupů a metodik vede k nepřehlednému řízení rizik a je proto nežádoucí.

„Učící se organizace *je koncept, který poprvé zformulovali Chrys Argyris a Donald Schon. Jde o teorii, jak má organizace fungovat, aby dosáhla rovnováhy mezi individuální iniciativou a tvořivostí na jedné straně a pravidly a řádem na druhé straně. Dále se snaží slaďovat individuální i týmovou výkonnost*“.[34] Principy učící se organizace je velmi výhodné aplikovat zejména v oblasti řízení rizik. Dokumentované informace umožní tak získat přehled o přínosech, nákladech a úsilí, které bylo a je věnováno řízení rizik.

Veškeré získané a dohledatelné dokumentované informace dávají základ k možnému zlepšování systému řízení rizik. V rámci zlepšování řízení rizik se nesmí zapomínat na rozvoj znalostí posuzovatelů i managementu.

[34] Učící se organizace. *Management mania* [online]. 2013 [cit. 2016-02-14]. Dostupné z: https://managementmania.com/cs/ucici-se-organizace

3 SEZNÁMENÍ S VYBRANOU FIRMOU

Jak autor uvedl v úvodu, veškeré informace o vybrané firmě budou striktně anonymizovány. Jde o opatření vrcholového vedení, které souhlasilo s použitím firmy jako vzoru, ovšem za podmínky, že v práci nebude uvedeno, o jakou konkrétní firmu se jedná. Vzhledem k tomu, že v této bakalářské práci se vyskytují citlivé údaje o možných zranitelnostech a hrozbách pro firmu, bude autor o této firmě hovořit jako o vybrané firmě.

Vybraná firma působí v České republice a na světovém trhu v odvětví konstrukce, zejména pro automobilový průmysl. Dalšími odvětvími, ve kterých firma působí, jsou letecký průmysl, konstrukce a svařování kolejových vozidel. V období let 2014 a 2015 vybraná firma získala také koncesi na stavbu lodí a konstrukci zbraní. Nejedná se pouze o konstrukci částí celku, ale mnohdy i o velké projekty. V těchto projektech je obsaženo vše od návrhu vzhledu, přes elektrické rozvody až po montáž funkčního prototypu tedy celý výsledný produkt.

Vybraná firma v rámci své působnosti vyniká všestranností, orientací na zákazníka a znalostmi a zkušenostmi svých zaměstnanců. Zaměstnanci tyto zkušenosti získávají z různých částí světa, mnohdy formou výkonu činnosti přímo u zákazníka.

V mnoha různých projektech jsou zaměstnanci vybrané firmy často první na světě, kteří přetvoří jistý nápad či myšlenku do praxe. Nerozhoduje, zda se jedná o drobný díl interiéru, nový typ převodovky, či celé vozidlo.

V prototypové dílně jsou zaměstnanci schopni vytvořit, za pomoci moderních zařízení, modely 1:1, včetně modelů celých vozidel. Jednou z dalších činností vybrané firmy je testování vozidel v reálném provozu. Testování se týká různých typů vozů od různých výrobců. Ve většině případů se jedná o testování dlouhodobé spotřeby s nestandardními typy paliv, při různém zatížení a různých povětrnostních podmínkách.

Firma má implementovány různé mezinárodní normy managementu do celkového systému řízení, který je označován zkratkou ISM, neboli integrovaný systém managementu. Tento systém zahrnuje normy ISO 9001[35], ČSN EN 9100[36], ISO 14001[37], OHSAS 18001[38] a nově ISO/IEC 27001[3940]. Tento výčet autor uvádí pro ilustraci obsáhlosti integrovaného systému managementu ve firmě.

Tento rozsah integrovaného systému managementu je nutný také proto, že vybraná firma v současné době zaměstnává řádově 500 osob na různých pozicích. Integrovaný systém managementu pomáhá ve všech činnostech společnosti, od personalistiky po marketing přes výrobní procesy.

Vzhledem ke společenské a environmentální odpovědnosti vybrané firmy bylo na přelomu roku 2015 a 2016 rozhodnuto o implementaci dalšího mezinárodního standardu a to standardu ČSN EN ISO 50001:2012 – Systémy managementu hospodaření s energií – Požadavky s návodem k použití.[41]

35 ISO 9001, celým názvem českého standardu: ČSN EN ISO 9001:2009 Systémy managementu kvality – Požadavky.
36 ČSN EN 9100, celým názvem českého standardu: ČSN EN 9100:2014 Letectví a kosmonautika – Systémy managementu kvality – Požadavky (podle ISO 9001:2000) a systémy kvality – Model zabezpečování kvality při návrhu, vývoji, výrobě, instalaci a servisu (podle ISO 9001:1994).
37 ISO 14001, celým názvem českého standardu: ČSN EN ISO 14001:2005 Systémy environmentálního managementu – Požadavky s návodem pro použití.
38 OHSAS 18001, celým názvem českého standardu: ČSN OHSAS 18001:2008 Systémy managementu bezpečnosti a ochrany zdraví při práci – Požadavky.
39 ISO/IEC 27001, celým názvem českého standardu: ČSN ISO/IEC 27001:2014 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky.
40 Implementován v průběhu roku 2015 s certifikačním auditem provedeným v prosinci 2015. Součástí procesu byla, mimo jiné, analýza rizik, které týká teoretická část této práce.
41 Implementací a úspěšnou certifikací tohoto standardu bude mimo jiné dosažení shody se zákonnými požadavky zákona číslo 406/2000 Sb. o hospodaření energií.

4 OBJASNĚNÍ METODIKY ANALÝZY RIZIK VE VYBRANÉ FIRMĚ

Jako součást procesu implementace mezinárodního standardu ČSN ISO/IEC 27001:2014 byla provedena analýza rizik. Tato analýza probíhala v několika krocích, které jsou popsané v kapitole 2.2.1 a kapitolách navazujících. V souvislosti s procesem analýzy rizik vznikl dokument, který je pro prokázání shody s ČSN ISO/IEC 27001:2014 povinný. Jedná se o dokument s názvem **Metodika hodnocení rizik**. Autor této práce je autorem firemního dokumentu, který definuje metodiku hodnocení rizik ve vybrané firmě tak, aby byla akceptovatelná z pohledu systému řízení bezpečnosti informací, politik a pravidel integrovaného systému managementu a také zákonných a regulatorních požadavků. Dokument také zajišťuje, aby byly výsledky hodnocení rizik reprodukovatelné a transparentní.

Následující podkapitoly jsou vyjmuty z dokumentu **Metodika hodnocení rizik** a jejich názvy tedy odpovídají zmíněnému dokumentu. Autor znovu upozorňuje, že se jedná o anonymizované údaje, což nic nemění na skutečnosti, že následující informace a postupy jsou využívány prakticky v reálném životě vybrané firmy.

4.1 Postupy

Analýza rizik je základním podkladem pro stanovení cílů řízení bezpečnosti informací a pro výběr opatření, která tyto cíle naplňují. Provádí se periodicky minimálně jednou ročně, v případě změn ve struktuře aktiv (případně hrozeb a zranitelností) je průběžně aktualizována doplňována.

4.1.1 Identifikace aktiv

Identifikace aktiv je prvním krokem hodnocení rizik. Aktivem (z anglického *„asset“*) je z pohledu normy ČSN ISO/IEC 27001 chápáno cokoliv, co má pro organizaci nějakou hodnotu, tedy zjednodušeně:

- Hardware.
- Software.
- Informace (bez ohledu na způsob jejich zaznamenání).

- Zaměstnanci.
- Znalosti.

S identifikací aktiv souvisí nalezení a určení jejich vlastníka, tj. takové osoby, které byla vedením organizace přiřknuta odpovědnost za produkci, vývoj, údržbu, použití a bezpečnost aktiv. Tento pojem neznamená, že by tato osoba byla skutečným vlastníkem konkrétního aktiv a měla k němu vlastnická práva.

Každému aktivu je přidělena jeho hodnota – význam pro činnost organizace. Pro stanovení hodnoty používá organizace následující kritéria:

1. Aktivu je přiděleno bodové hodnocení Důvěrnosti (Du), Integrity (I) a Dostupnosti (Do) dle škály 1 - 5 viz níže.
2. Hodnota aktiva (HA) je určena součtem hodnocení.

HA = Du + I + Do

Společnost (vybraná firma) zavedla následující systém označování důležitých aktiv podle důvěrnosti, společnost považuje za důležité označovat pouze informace, které jsou určené vedení organizace a to symbolem **D4** a důvěrná data zákazníků a to symbolem **D5** (pokud je to možné).

Důvěrnost (Du) – hodnocení dle následků kompromitace informací	**body**	
volně dostupné informace	1	
informace dostupné všem v rámci organizace	2	
informace určené pouze konkrétním oddělením organizace	3	
informace určené pouze vedení organizace	4	**D4**
důvěrné informace zákazníků	5	**D5**

Integrita (I) - hodnocení dle následků změny informací	
volně dostupné informace	1
informace, jejichž změna nebude mít žádný dopad (např. testovací data)	2
informace, jejichž změna bude mít omezený dopad	3
informace (data) zákazníků	4
finance, nabídky, smlouvy	5

Dostupnost (Do) - hodnocení dle následků nedostupnosti informací

volně dostupné informace (lze zjistit jinde bez omezení)	1
informace s omezeným okruhem příjemců, problémy se zjištěním informace jinde	2
informace (data) zákazníků - nekritická; data potřebná pro běh firmy (např. podklady pro mzdy, …)	3
informace (data) zákazníků - kritická; data potřebná pro každodenní běh firmy	4
informace, při jejichž nedostupnosti hrozí ztráta obchodu, zákazníka, kreditu, …	5

4.1.2 Identifikace rizik

Pro každé identifikované aktivum jsou určeny a analyzovány hrozby. Každá tato hrozba využívá jednu nebo několik zranitelností, které jsou také během analýzy identifikovány. Pro každou takto nalezenou zranitelnost a příslušnou hrozbu je určen pravděpodobný dopad na bezpečnost informací organizace pomocí následujících kritérií:

1. Je určena pravděpodobnost zneužití konkrétní zranitelnosti konkrétní hrozbou a ohodnocena na stupnice 1 – 5 (viz níže), dále PV.
2. Je určen předpokládaný dopad na činnosti organizace, tento dopad je také ohodnocen na stupnici 1–5 (viz tabulka), dále DP.

Výsledná míra rizika (MR) je určena takto:

$$\mathbf{MR = HA \times PV \times DP}$$

Míra rizika může nabývat hodnot z intervalu <3;375>.

Jako hraniční míra rizika, kdy je nutné přijímat opatření a míru rizika snižovat, byla vedení vybrané firmy stanovena hodnota **120**[42], která odpovídá mírné pravděpodobnosti výskytu bezpečnostního incidentu (PV 4) se středním dopadem na činnosti organizace (DP 3) u mírně nadprůměrně cenného aktiva společnosti (HA 10).

[42] V případě provádění analýzy rizik nad aktivy, která nejsou ošetřena opatřeními, je stanovována hraniční míra rizika výše. S postupnou implementací opatření může tato hraniční míra rizika klesat. Rizika s mírou vyšší než je stanovený limit je nezbytné ošetřit opatřeními nebo vypracovat **Plán zvládání rizik**.

Pravděpodobnost výskytu		
nepravděpodobné	1	< 1× 10 let
velmi malá	2	1× 10 let
malá	3	< 1× ročně
mírná	4	2-3× ročně
vysoká	5	> 3× ročně

Dopad	
zpoždění prací; zanedbatelné (finanční) ztráty	1
omezení práce; nízké (finanční) ztráty	2
zastavení práce v oddělení; střední (finanční) ztráty	3
nedostupnost pro zákazníka; vysoké (finanční) ztráty	4
zastavení práce v celé firmě; velmi vysoké (finanční) ztráty	5

4.1.3 Vypořádání rizik

Po provedení analýzy rizik je nutné u každého aktiva, kde vypočtená míra rizika překročí akceptační úroveň[43], najít a uvést do praxe opatření, která povedou ke snížení míry rizika. Po jejich aplikaci v praxi je provedena navazující analýza rizik, kdy je k řešeným hrozbám znovu přiřazena pravděpodobnost výskytu (PV) a dopad (DP) a znovu určena míra rizika. Tento proces se periodicky opakuje, dokud není dosaženo míry rizika shodné nebo nižší než je akceptační úroveň.

Opatření, která je možné využít, je vhodné čerpat z Přílohy A[44] normy ČSN ISO/IEC 27001, tato příloha však není vyčerpávající a je vhodné přijmout i jiná opatření vycházející z konkrétní situace organizace.

Pokud již není možné nebo ekonomicky zdůvodnitelné přijímaní dalších opatření snižujících pravděpodobnost nebo dopady bezpečnostního incidentu, je povinností manažera bezpečnosti informací (dále jen MBI) vypracovat o takovýchto rizicích

[43] Akceptační úrovní je hraniční míra rizika.
[44] Příloha A normy ČSN ISO/IEC 27001, tzv. PoA – Prohlášení o aplikovatelnosti. Prohlášení o aplikovatelnosti je mandatorním dokumentem pro případ certifikace systému řízení bezpečnosti informací.

zprávu pro vedení organizace a představitele vedení pro IMS. Vedení organizace tuto zprávu projedná a rozhodne o dalším postupu, který může být následující:

- Akceptace zvýšeného rizika z důvodu ekonomické neúnosnosti protiopatření.
- Rozhodnutí o vyhnutí se rizikům.
- Rozhodnutí o přenesení rizika na třetí stranu (dodavatel, pojišťovna, …).
- Přeskupení aktiv tak, aby se snížila jejich hodnota (např. rozložení informací na více míst apod.).
- Uvolnění dalších zdrojů pro řešení rizik.

4.1.4 Personální odpovědnost

Za vyhotovení a opakované přezkoumání analýzy rizik je zodpovědný MBI. MBI je oprávněn k provedení analýzy sestavit tým vytvořený z odborníků z celé organizace.

Analýza rizik musí být přezkoumána nejméně jednou za rok, nejlépe v rámci přezkoumání IMS.

4.2 Ověřování účinnosti

Účinnost zavedených opatření je ihned ověřena opakovaným provedením analýzy rizik v oblastech, kterých se zavedené opatření dotklo. Z tohoto porovnání je ihned vidět přínos každého zavedeného opatření ke zvýšení bezpečnost informací.

Druhou metodou ověřování účinnosti opatření v praxi je testování správnosti nasazení a skutečného vlivu. Tuto metodu nelze konkretizovat, protože je závislá na konkrétním opatření a konkrétní oblasti, kde bylo opatření zavedeno. Pokud je to možné, stanoví MBI při rozhodnutí o zavedení opatření i vhodnou metodiku pro ověření úspěšnosti jeho nasazení v praxi.[45][46]

[45] ČELIKOVSKÝ, J. *Dokument vybrané firmy: Metodika hodnocení rizik*. Verze 1. 2015.
[46] Autor této práce je autorem firemního dokumentu **Metodika hodnocení rizik.** Ve vybrané firmě působí jako externí spolupracovník v rámci systémů řízení. Vypracování vlastní **Analýzy rizik** prováděli interní zaměstnanci vybrané firmy za metodické podpory autora.

5 POSTUP A VÝSTUPY Z ANALÝZY RIZIK VYBRANÉ FIRMY

V této kapitole autor vysvětluje jednotlivé kroky, které byly nutné k úspěšné realizaci analýzy rizik ve vybrané firmě. Dalším z bodů této kapitoly jsou výstupy z analýzy rizik.

5.1 Postup

V počáteční fázi realizace analýzy rizik ve vybrané firmě bylo určení kontaktních osob v týmech označovaných termínem SPOC[47]. Tato osoba byla zodpovědná za tlumočení požadavků týkajících se analýzy rizik směrem do svého týmu. Zároveň byla zodpovědná za doručení výstupů směrem k týmu provádějícímu vlastní analýzu rizik.

Při této fázi analýzy rizik proběhlo také školení SPOCů a týmu provádějícího analýzu rizik, které bylo zaměřené na metodiku provádění analýzy rizik.

Vlastní analýza rizik postupovala ve dvou hlavních částech, a to v části společné a v části týmové. Ve společné části byla identifikována hlavní aktiva spolu s hrozbami, zranitelnostmi a riziky. Tato identifikace dále obsahovala identifikaci vlastníků aktiv a rizik.

Přes SPOCa byl do týmů distribuován požadavek o provedení vlastních dílčích analýz a vyjádření k proběhlé analýze. To již byla fáze týmová, která obsahovala stejné kroky, jako fáze společná.

Následovala opět společná fáze, ve které byla provedena konsolidace výsledků do přehledné tabulky.

Při výskytu nejasností, nebo žádostech o podporu z jednotlivých týmů, následovaly další schůzky a diskuse na témata týkající se všech dílčích kroků vlastní analýzy.

[47] SPOC – zkratka z anglického Single Point of Contact – jediný kontaktní bod.

V závěru tohoto koloběhu proběhla finalizace a revize vlastní analýzy tak, aby byly závěry přehledné, objektivní a možné prezentovat.

Následné kroky obsahovaly návrhy opatření u rizik, jejichž míra přesáhla stanovenou hranici 120 bodů a referování výsledků na Steering committee[48].

Steering committee, po projednání, schválil akceptovatelná rizika a zbytková rizika. Zároveň byla určena periodicita provedení analýzy rizik. Tato perioda je v současné době nastavena jednou za rok nebo v případě významných změn.

5.2 Výstupy z analýzy rizik

Hlavními výstupy z analýzy rizik jsou zejména:

- Seznam aktiv s jejich vlastníky.
- Seznam hrozeb.
- Seznam zranitelností.
- Seznam rizik s jejich vlastníky a mírou rizika.
- Seznam opatření přiřazených ke konkrétním rizikům.

V rámci zachování bezpečnosti informací a požadavku vedení vybrané firmy není možné tyto seznamy prezentovat.

Dalšími výstupy je vytvoření nebo aktualizace několika dalších dokumentů. V první řadě byl v průběhu implementace Systému řízení bezpečnosti informací ustanoven Krizový štáb, který byl oficiálně jmenován.

Dále vznikl dokument s názvem **Krizový plán**, který obsahuje popis 15 krizových situací. Tabulka obsahuje:

- Číslo a název krizové situace.
- Popis rizik pro fungování vybrané firmy.

[48] Steering committee – Řídící výbor – jedná se o řídící výbor v projektu implementace Systému řízení bezpečnosti informací. Členové Steering committee jsou členy vrcholového vedení rozšíření o manažera bezpečnosti informací.

- Adekvátní reakci na vzniklou situaci.
- Odpovědnou osobu.
- Prevenci vzniku krizové situace.

V návaznosti na Krizový plán vznikl dokument **Plán obnovy**, který obsahuje sadu těchto krizových situací v přehledných tabulkách[49], kde jsou obsaženy instrukce a informace:

- Kam situaci hlásit.
- Kontaktní údaje pro odpovědné osoby.
- Další důležité telefonní kontakty.
- Seznam následných opatření potřebných pro zotavení systému – Plán obnovy.

Spolu se vznikem výše zmiňovaných dokumentů bylo mnoho dalších interních dokumentů aktualizováno. Zmiňované dokumenty jsou zásadní pro fungování firmy v případě krizové situace.

Posledním zásadním výstupem z celého procesu analýzy rizik, respektive implementace Systému řízení bezpečnosti informací je **Zpráva vrcholovému vedení o fungování ISMS[50][51].** Vrcholové vedení vybrané firmy zprávu projednalo, vyžádalo si k některým bodům komentáře či vysvětlení a výsledky schválilo.

[49] Ke každé krizové situaci existuje popis, který je podobný Požárním poplachovým směrnicím, které jsou obecně známé. Jediným významným rozdílem mezi popisy krizových situací a Požárními poplachovými směrnicemi je podrobnost informací v dokumentech obsažených.
[50] ISMS – Information security management systém – systém řízení bezpečnosti informací.
[51] Interní dokument určený poradě vedení, který shrnuje celý proces a jeho výstupy do krátké zprávy.

PRAKTICKÁ ČÁST

6 PRACOVNÍ HYPOTÉZY A OTÁZKY

Autor v následujících kapitolách prezentuje své pracovní hypotézy, otázky pro dotazníkový průzkum a pro řízený rozhovor. Na dalších stranách prezentuje výsledky dotazníkového průzkumu a řízeného rozhovoru.

6.1 Pracovní hypotézy

Na základě vlastních zkušeností a podnětů okolí autor stanovil následující soubor hypotéz, které se pomocí **kvantitativních a kvalitativních metod** výzkumu pokusil potvrdit.

1. Autorovo přesvědčení je takové, že obecné povědomí o analýzách rizik je nízké.
2. Laická veřejnost považuje pojem aktivum za účetní položku bez vztahu k rizikům.
3. Velikost firmy ovlivňuje povědomí o problematice a vědomí závažnosti analýz rizik.
4. Panuje obecné přesvědčení, že audit ve firmě není prováděn jako bezpečnostní prověrka, ale pouze jako ekonomická nebo finanční kontrola.
5. Střední a vyšší management firmy je dostatečně informován o významu analýzy rizik.

Hypotézy s pořadovými čísly 1 – 4 byly určeny pro potvrzení pomocí dotazníkového průzkumu. Dotazníkový průzkum se skládal z celkem 22 otázek. Otázky dotazníkového průzkumu jsou prezentovány a vysvětleny v **kapitole 6.2**. Hypotéza s pořadovým číslem 5 byla určena k potvrzení pomocí řízených rozhovorů se zástupci vybrané firmy. Otázky použité při řízeném rozhovoru jsou prezentovány v **kapitole 6.3**.

6.2 Otázky pro dotazníkový průzkum

Autor realizoval dotazníkový průzkum na serveru http://www.survio.cz pod názvem: Řízení rizik v rámci bezpečnosti informací – dotazník k Bakalářské práci. Dotazník obsahoval sadu následující sadu otázek:

1. Jste muž nebo žena?
2. Jaké je Vaše nejvyšší dosažené vzdělání?
3. Jaký je Váš věk?
4. Máte v oblasti systémů řízení bezpečnosti informací nebo v rámci řízení rizik nějaké znalosti/zkušenosti?
5. Jaké je Vaše zaměstnání? V případě více možností zaškrtněte všechny relevantní možnosti.
6. Jaká je velikost firmy, ve které pracuji (ve které jsem byl naposledy zaměstnán)? OSVČ uvedou, pro jak velké firmy nejčastěji pracují.
7. Jakou pozici ve firmě zastávám (zastával/a jsem)?
8. Je Vám znám pojem „AKTIVUM“?
9. Lze považovat software (MS Office, SAP, další programy a aplikace) za aktivum?
10. Co vnímáte jako aktivum? (V kontextu tohoto dotazníku – Výběr z více možností).
11. Lze považovat lidské zdroje (Lidé a jejich Know how[52]) za aktivum?
12. Je vhodné provádět analýzy rizik ve firmách všech velikostí a zaměření?
13. Je vhodné provádět analýzy rizik v týmu?
14. Co z následujících možností považujete za nejcennější aktivum?
15. Je vhodné pro analýzy rizik využívat podpůrných metod? (Brainstorming, audit atd.)
16. Mezi největší rizik lze vždy zařadit personál.
17. Při provádění analýzy rizik je nutné brát v úvahu i právní úpravu týkající se analyzované oblasti.

[52] Anglické sousloví. V překladu znamená „vědět – jak“.

18. Do analýzy rizik bezpečnosti informací není možné zařadit přírodní faktory (oheň, vítr, voda atd.)
19. Při analyzování rizik obchodního případu (zvládneme zakázku, riziko při nesplnění zakázky, zákonné aspekty) bychom měli, za použití různých metod analýz rizik, dospět ke srovnatelným výsledkům.
20. Při analyzování bezpečnostních incidentů bychom měli, za použití různých metod analýz, dospět k podobným příčinám vzniku incidentu.
21. Audit systému řízení (bezpečnosti informací, rizik, kvality apod.) bývá obvykle nepříjemný a náročný pro auditovaného.
22. Výstupem z auditu systému řízení (bezpečnosti informací, rizik, kvality apod.) bývá obvykle postih pro jedince (v konečném důsledku finanční, kariérní atd.)

6.2.1 Vysvětlení otázek dotazníkového průzkumu

Autor považuje za důležité vysvětlit volbu otázek vzhledem ke stanoveným hypotézám, které měly být pomocí dotazníkového průzkumu zjištěny.

Otázky s pořadovým číslem 1 – 3 sloužily ke zjištění složení vzorku respondentů.

Otázky s pořadovým číslem 4 – 7 sloužily ke zjištění zkušeností v oblasti řízení rizik a obecně ke zjištění zkušenosti v rámci systémů řízení jako takových. Dalším sledovaným ukazatelem byla velikost firmy a popřípadě pozice, kterou respondent zastává nebo zastával.

Další otázky, s pořadovým číslem 8 – 20, již cílily na znalosti v oblasti systémů řízení se zaměřením na řízení rizik a bezpečnost informací. Autor zvolil jak konkrétní otázky, tak tvrzení, ke kterým se respondent vyjádřil jedním z definovaných způsobů. Jedním způsobem byl výběr z více možností. Druhým způsobem bylo označení možnosti na pětistupňové škále. Ve většině případů se jednalo o možnosti ANO, Spíše ANO, NEVÍM, Spíše NE a NE.

Poslední dvě otázky, tedy ty s čísly 21 a 22 byly zaměřeny na osobní zkušenost či předpoklad průběhu a dopadu auditu systému řízení.

6.3 Otázky pro řízený rozhovor

Otázky pro řízený rozhovor byly autorem zvoleny ke zjištění úrovně znalosti systému řízení rizik vedoucími pracovníky. Celkem bylo položeno následujících 5 otázek:

1. Vnímáte řízení rizik ve společnosti, kde pracujete?[53]
2. Interní audity bývají náročnější než externí audity. Prosím odůvodněte své tvrzení krátkým komentářem.
3. V rámci auditů systémů řízení rizik je vytvářena dokumentace, která je zbytečnou zátěží pro firmu. Lze s tímto tvrzením souhlasit? Proč?
4. V rámci přípravy systému řízení rizik na audit je vytvářena dokumentace, která je zbytečnou zátěží pro firmu. Lze s tímto tvrzením souhlasit? Proč?
5. Jsou analýzy rizik, respektive systém řízení rizik, ve společnosti kde pracujete vnímány jako represivní nástroj nebo jako účinný nástroj využívaný k rozvoji firmy?

Otázky byly voleny tak, aby mohl autor z odpovědí vyvodit, v jakém stavu se nachází systém řízení rizik ve vybrané firmě. Vzorek pracovníků byl vybrán z projektového týmu, který realizoval implementaci systému řízení bezpečnosti informací a ze zástupců vrcholového managementu vybrané firmy. Rozhovory autor prezentuje a komentuje v **kapitole 8**.

[53] Otázka položena s upřesněním, že autora zajímá úroveň řízení rizik, povědomí o rizicích, soužití se systémem řízení rizik apod.).

7 DOTAZNÍKOVÝ PRŮZKUM

Pro sběr dat v dotazníkovém průzkumu autor zvolil webovou službu **Survio**, kterou využívá i několik velkých českých a nadnárodních společností. Se zmíněnou službou má autor zkušenosti už z minulých let, kdy ji využíval v rámci seminárních prací.

Vzhledem k několika různým metodám šíření dotazníku není možné objektivně určit návratnost dotazníku. Dotazník byl šířen pomocí e-mailu, odkazů na sociálních sítích a za pomoci třetích osob. Dotazníkový průzkum probíhal v období 1.12.2015 – 5.2.2016. Celkem se autorovi navrátilo **82 plně zodpovězených dotazníků**, ze kterých nemusel žádný vyloučit. Složení vzorku respondentů a jejich odpovědí s komentářem autora je uváděno v následujících kapitolách.

7.1 Základní parametry získaného souboru

Tabulka 1: Základní parametry získaného souboru

		Počet respondentů	Podíl v %
Pohlaví	muž	32	39 %
	žena	50	61 %
Vzdělání	základní	1	1,2 %
	střední (výuční list)	0	0 %
	střední (maturita)	38	46,3 %
	vyšší odborné	6	7,3 %
	vysokoškolské	37	45,1 %
Věk	méně než 18 let	1	1,2 %
	18 – 30 let	50	61,0 %
	30 – 50 let	20	24,4 %
	50 a více let	11	13,4

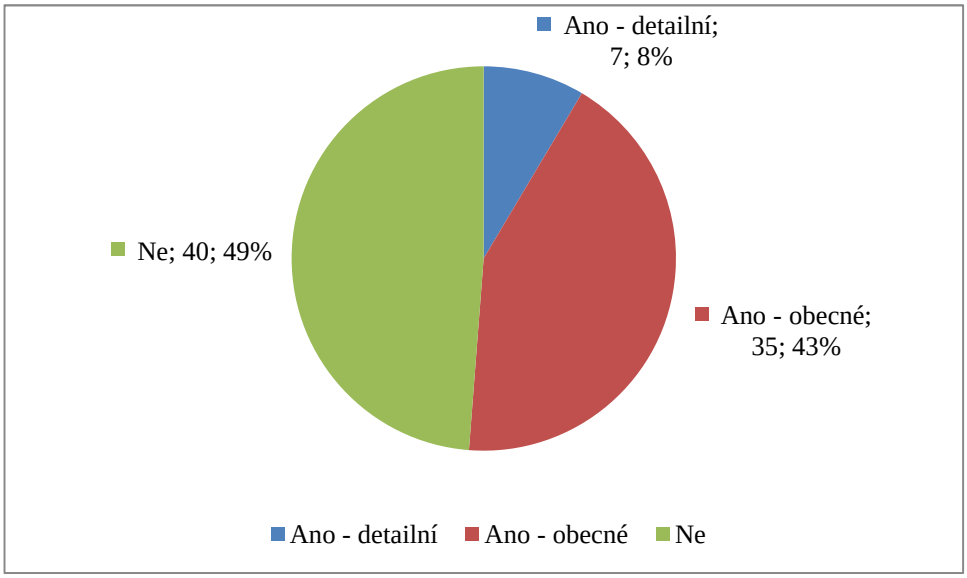
Zdroj[54]

[54] Autor práce, 2016 (vlastní šetření).

7.2 Zkušenosti v oblasti řízení rizik

Jak autor uvedl v kapitole **6.2.1 Vysvětlení otázek dotazníkového průzkumu,** otázky s pořadovým číslem 4 – 7 byly cíleny na zjištění zkušeností v oblasti řízení rizik a pro zjištění obecných zkušeností v rámci systémů řízení.

Graf 1: Znalosti a zkušenosti v oblasti systémů řízení



Zdroj[55]

Otázka položená v dotazníkovém šetření měla konkrétní znění: *Máte v oblasti systémů řízení bezpečnosti informací nebo v rámci řízení rizik nějaké znalosti/zkušenosti?* Výsledné procentuální složení odpovědí znázorňuje **Graf 1**.

Z celkového počtu 82 respondentů pouze 7 (celkem 8% dotázaných) uvedlo, že má detailní znalost v zájmové oblasti. V tomto případě autor předpokládá, že se jedná o konzultanty nebo členy projektových týmů, působících v systémech řízení bezpečnosti informací nebo v rámci řízení rizik.

Naopak velmi zajímavým se autorovi jeví fakt, že 40 respondentů (celkem 49% dotázaných) uvedlo, že nemá žádné znalosti v oblasti řízení rizik nebo v oblasti systémů

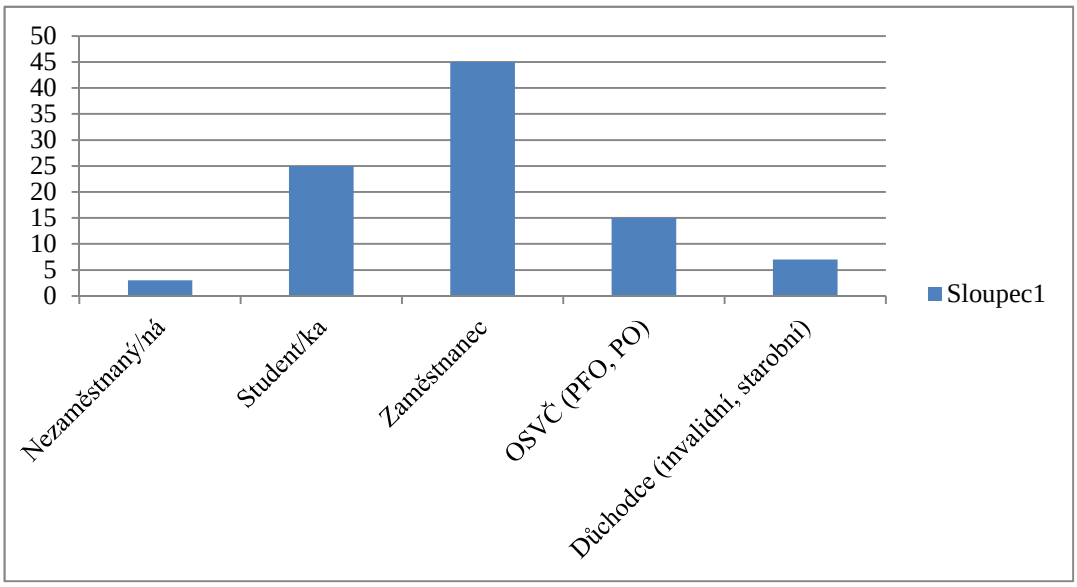
[55] Autor práce, 2016 (vlastní šetření).

řízení bezpečnosti informací. Tento údaj je téměř alarmující. Autor připomíná, že rizikům se nedá žádným způsobem vyhnout, ať jde o rizika v běžném životě či rizika v podnikání. Každá organizace, která má implementován nebo implementuje systém řízení bezpečnosti informací či systém řízení rizik své zaměstnance a dodavatele školí a informuje. To je důvodem, proč je autor práce zaražen četností záporných odpovědí na otázku znalostí a zkušeností.

Možné vysvětlení tak vysokého počtu záporných odpovědí přinesly další údaje získané z dotazníkového šetření, a to údaje o zaměstnání, velikosti firmy a pozici ve firmě, kterou respondent zastává.

V případě zaměstnání se autor zajímal o typ zaměstnání respondenta. V případě více možností, jako například studující zaměstnanec, autor povolil více zaškrtnutých možností. Výsledné rozložení odpovědí prezentuje **Graf 2**.

Graf 2: Zaměstnání



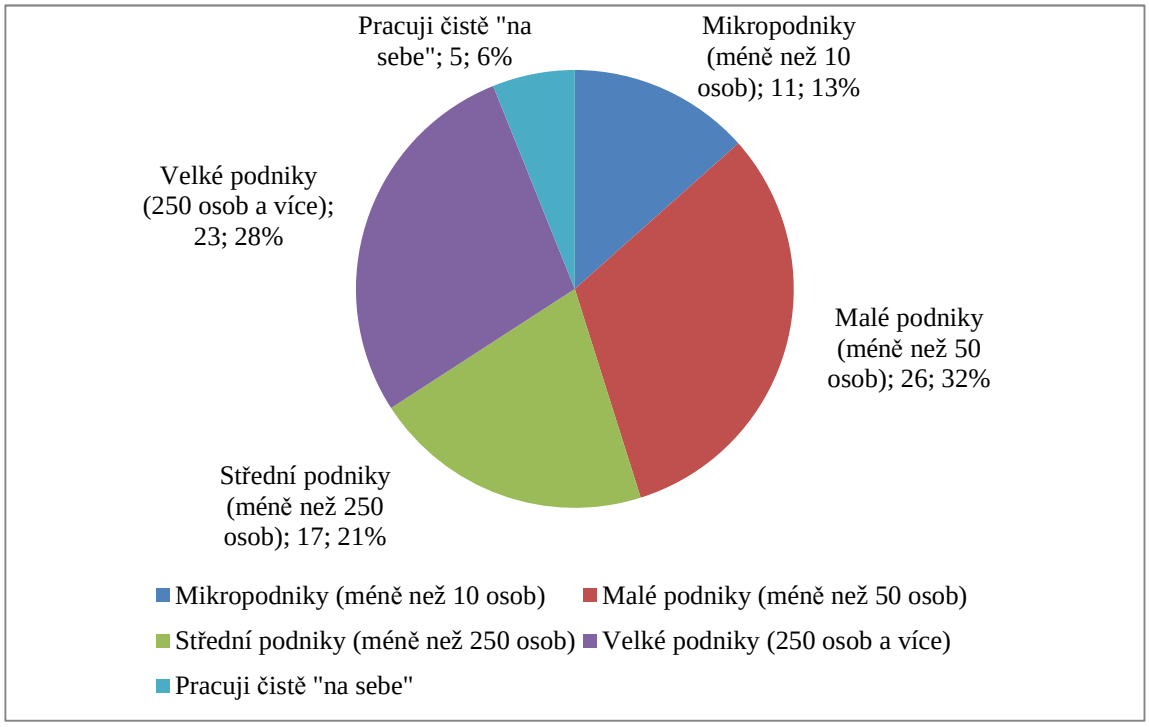
Zdroj[56]

[56] Autor práce, 2016 (vlastní šetření).

I v případě relativně malého vzorku populace je vidět Gaussovské rozložení odpovědí, kdy extrémní případy[57] jsou v nejmenší četnosti a naopak nejvíce standardní možnost je četností zastoupena nejvíce.

Dalším důležitým parametrem pro objasnění neznalosti a nezkušenosti velké části zkoumaného souboru je údaj o velikosti firmy, ve které respondent působí. Rozložení znázorňuje **Graf 3**.

Graf 3: Velikost firmy, kde respondent působí



Zdroj[58]

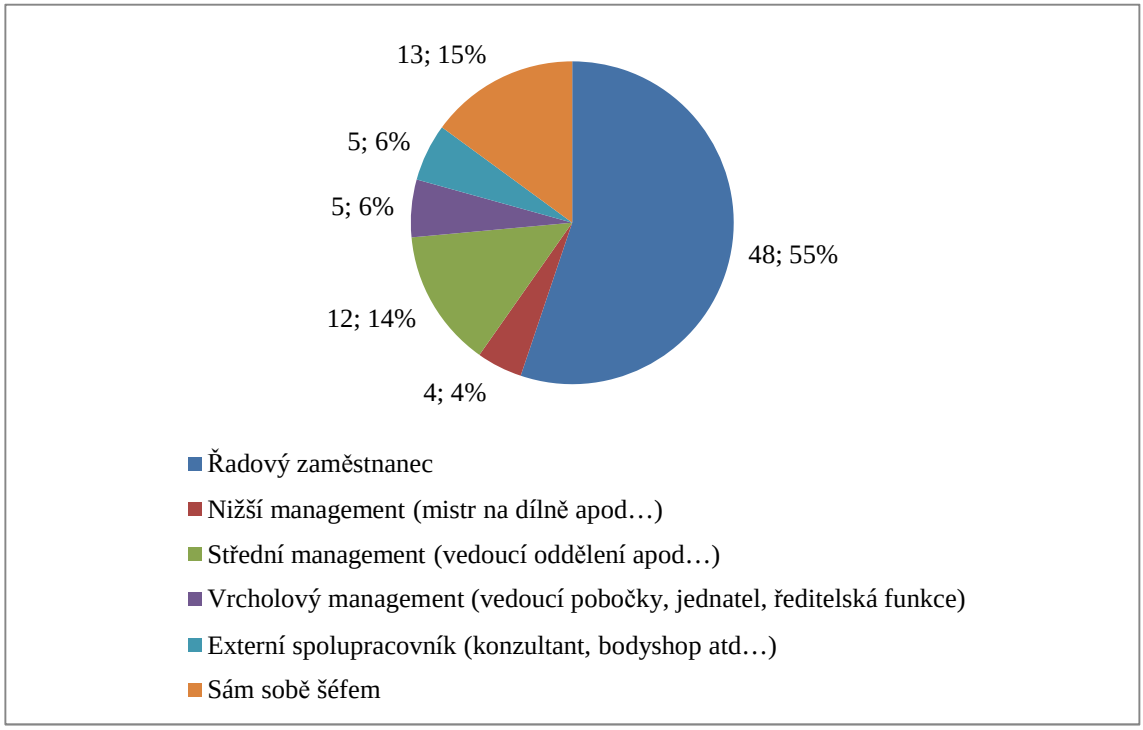
Z průzkumu vyplynulo, že téměř polovina respondentů pracuje v mikropodnicích, malých podnicích nebo sama na sebe. Autor, dle vlastní zkušenosti tvrdí, že právě v menších podnicích bývají znalosti o řízení rizik nebo systému řízení bezpečnosti informací malé, až zanedbatelné. Existují případy, kdy je tomu přesně naopak a veškerý

[57] Autor v kontextu zkoumaných skutečností chápe responze „Nezaměstnaný“ a „Důchodce“ jako extrémní a pro vlastní dotazníkové šetření pouze jako doplňující.
[58] Autor práce, 2016 (vlastní šetření).

personál malého podniku je v problematice zběhlý. V tom případě jde většinou o specializované podniky se zaměřením právě na systémy řízení bezpečnosti informací, rizik nebo přímo na analýzy rizik. Rozdělení podniků na mikropodniky, malé podniky, střední podniky a velké podniky autor čerpal z Úředního věstníku Evropské Komise.[59]

Poslední otázka, která byla zaměřená na oblast znalostí a zkušeností ve zkoumané problematice se týkala pozice, kterou respondent ve firmě zastává nebo zastával. Jak ukazuje **Graf 4**, v drtivé většině se jedná o řadového zaměstnance s 55% zastoupením.

Graf 4: Pozice respondenta ve firmě



Zdroj[60]

[59] Doporučení Komise ze dne 6. května 2003, týkající se definice mikropodniků, malých a středních podniků (oznámeno pod číslem dokumentu C(2003) 1422) (Úř. věst. L 124, 20.5.2003, s. 36-41). In: *EUR-Lex* [právní informační systém]. Úřad pro publikace Evropské unie [cit. 2016-02-18]. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=URISERV%3An26026

[60] Autor práce, 2016 (vlastní šetření).

Zbylých 45% je rozděleno mezi management od nižšího po vrcholový. Zastoupení externích spolupracovníků je 6% a zastoupení OSVČ (odpověď: „Sám sobě šéfem“) reprezentuje 15% dotazovaných.

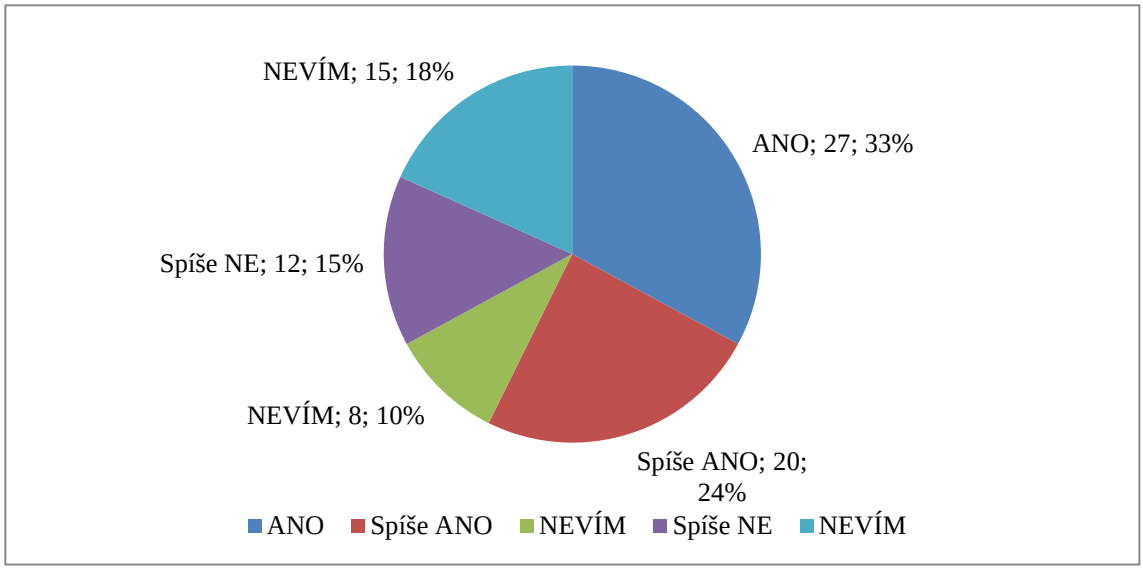
Z těchto dat autor usuzuje, že řadový zaměstnanec s vysokou pravděpodobností nemá znalosti ani zkušenosti z oblasti systémů řízení bezpečnosti informací a řízení rizik. Výše uvedenými daty autor považuje první hypotézu za potvrzenou. Autorovo přesvědčení, že obecné povědomí o analýzách rizik je nízké, se ve výše znázorněných datech potvrzuje. Další data, která jsou prezentována níže, pouze potvrzují autorovo přesvědčení a upřesňují nedostatky ve znalostech pojmů a principů spojených se systémy řízení bezpečnosti informací a analýzami rizik.

7.3 Znalosti v oblasti systémů řízení

V kapitole **6.2.1 Vysvětlení otázek dotazníkového průzkumu** autor objasňuje zaměření otázek s pořadovým číslem 8 – 20. Zaměření těchto otázek bylo na znalosti respondenta v oblasti systémů řízení s orientací na řízení rizik a bezpečnost informací. Otázky se týkaly některých pojmů a jejich chápání respondentem.

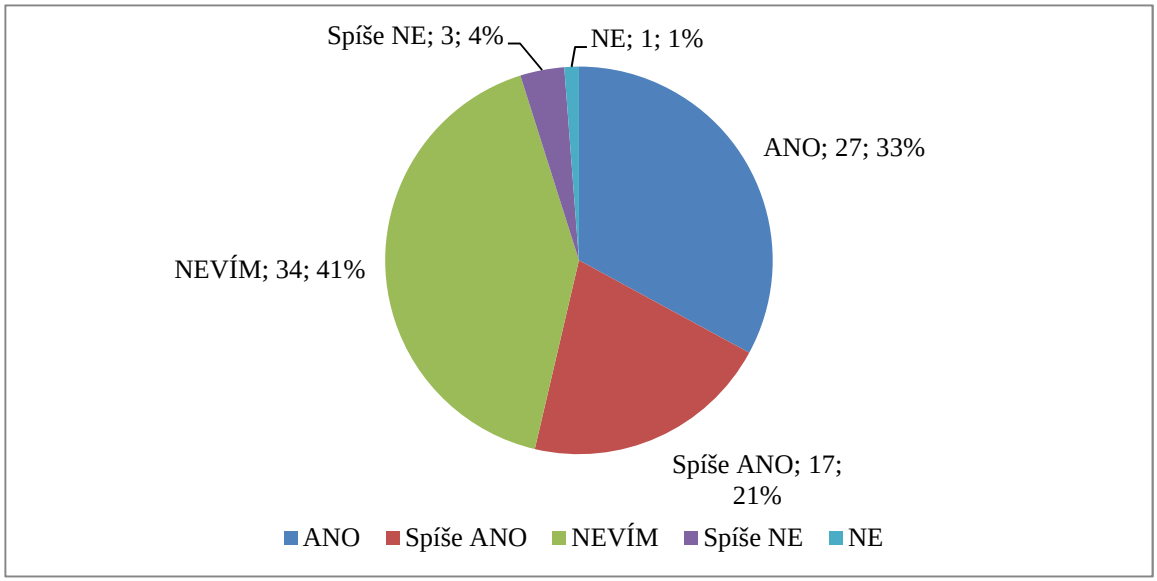
Jako o první se autor zajímal o znalost pojmu **Aktivum**. Tento pojem a jeho chápání je pro systém řízení bezpečnosti informací a analýzy rizik nezbytnou součástí. Čtenář si může udělat obrázek o významu aktiv a správném chápání pojmu aktivum v teoretické části této práce. **Graf 5** znázorňuje odpovědi na otázku, zda je respondentům znám pojem jako takový. V **Grafu 6** je znázorněno vnímání konkrétního typu aktiva respondenty. Autor zvolil otázku, zda lze považovat software (MS Office, SAP a další programy a aplikace) za aktivum. Responze na otázku s pořadovým číslem 10 je znázorněna na **Grafu 7**. Zde mohli respondenti vybírat z 12 typů aktiv, respektive 11 typů aktiv a možnosti, která zahrnuje všechny ostatní. Zamýšleným efektem bylo zjištění, jaká aktiva jsou vnímána dotazovanými jako skutečná aktiva, tedy jako něco co má pro organizaci cenu. Poslední otázkou směřovanou k pojmu aktivum bylo zjištění, zda dotazovaní vnímají lidské zdroje a jejich know-how jako aktivum. Složení odpovědí na otázku týkající se vnímání lidských zdrojů jako aktiva prezentuje **Graf 8**.

Graf 5: Znalost pojmu "AKTIVUM"



Zdroj[61]

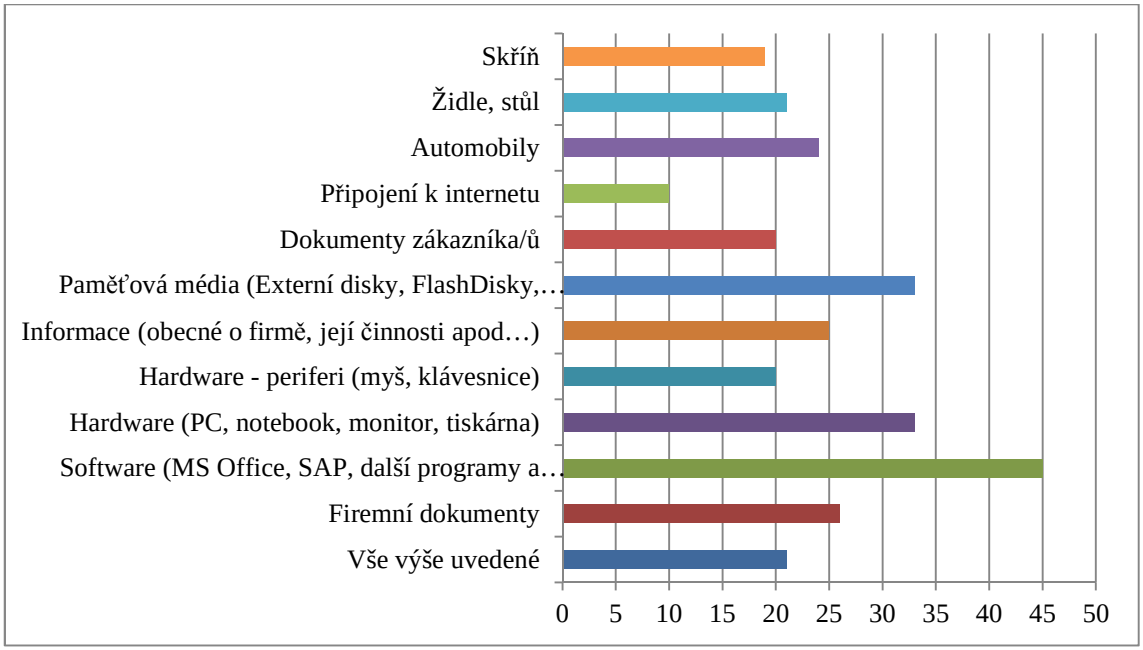
Graf 6: Lze považovat software (MS Office, SAP a další programy a aplikace za aktivum?



Zdroj[62]

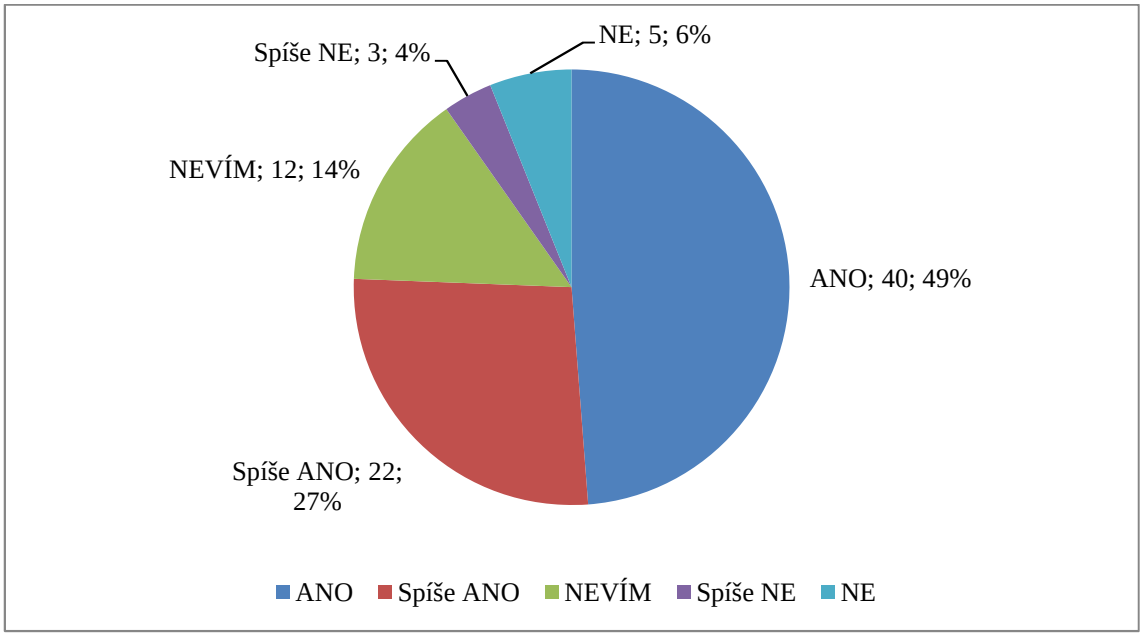
[61] Autor práce, 2016 (vlastní šetření).
[62] Tamtéž.

Graf 7: Co je vnímáno jako aktivum?



Zdroj[63]

Graf 8: Lze považovat lidské zdroje za aktivum?



Zdroj[64]

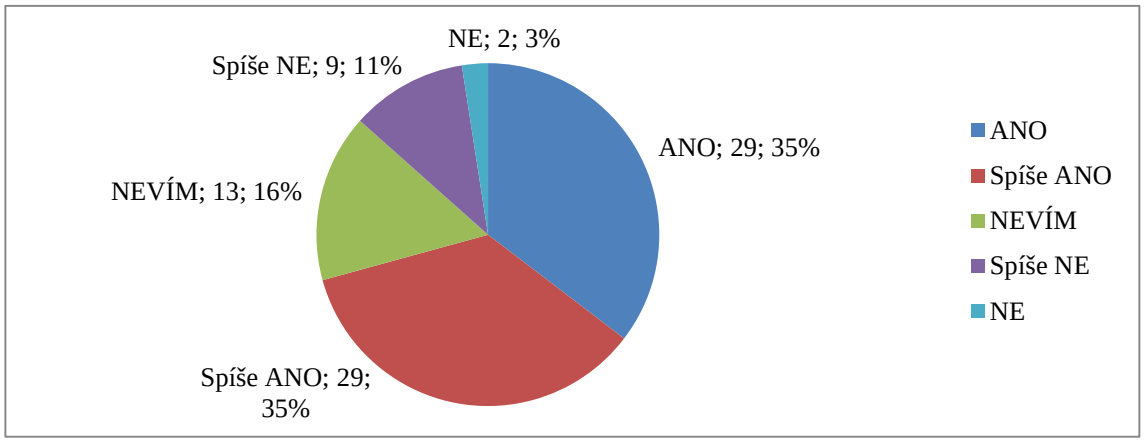
[63] Autor práce, 2016 (vlastní šetření).
[64] Tamtéž.

Jak vyplývá z graficky znázorněných četností odpovědí, 43% dotazovaných **nezná** pojem **Aktivum**. Tomuto údaji odpovídá i počet respondentů, kteří za aktivum nepovažují software nebo nevědí, jestli je vhodné software považovat za aktivum.

Z Grafu 1 je zřejmé, že 7 lidí (8% dotazovaných) odpovědělo, že má detailní znalost v oblasti systémů řízení bezpečnosti informací nebo řízení rizik a dalších 35 lidí (43% dotazovaných) uvedlo, že má obecnou znalost. Graf 7 ukazuje, že všechny nabízené možnosti mezi aktiva řadí 21 lidí (26% dotazovaných.). Zbylých 74% dotazovaných volilo různé kombinace zbylých možností. Autor ze získaných dat usuzuje, že pojem aktivum a jeho význam není veřejnosti moc znám.

Autor hodnotí velmi kladně výsledek u otázky s pořadovým číslem 11, znázorněné Grafem 8. Z tohoto grafu vyplývá, že 76% dotazovaných považuje lidské zdroje za aktivum. V absolutním čísle se jedná o 62 dotazovaných z celkových 82. Kladné hodnocení autor vztahuje hlavně k faktu, že personál bývá v mnoha odvětvích nenahraditelný, popřípadě velmi obtížně nahraditelný. Dalším faktem ověřeným praxí, nejen autorovou, je to, že lidský personál bývá největším zdrojem rizik. Toto tvrzení dokládají i výsledky u otázky s pořadovým číslem 16, kde autor uvedl tvrzení: Mezi největší rizika lze vždy zařadit personál. Výsledek je znázorněn v **Grafu 9**.

Graf 9: Mezi největší rizika lze vždy zařadit personál.

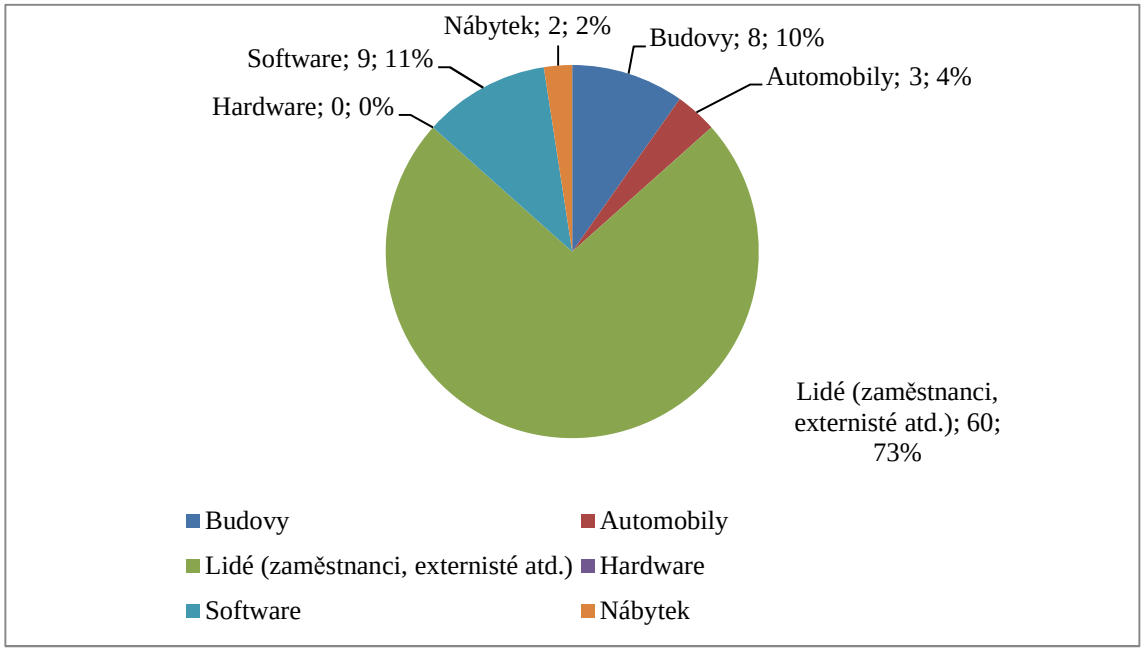


Zdroj[65]

[65] Autor práce, 2016 (vlastní šetření).

Předchozí tvrzení si autor ověřil za pomoci otázky s pořadovým číslem 14. K otázce bylo zařazeno 6 možných odpovědí. Otázka zněla: Co z následujících možností považujete za nejcennější aktivum? Autor prezentuje složení odpovědí v **Grafu 10**.

Graf 10: Nejcennější aktivum.



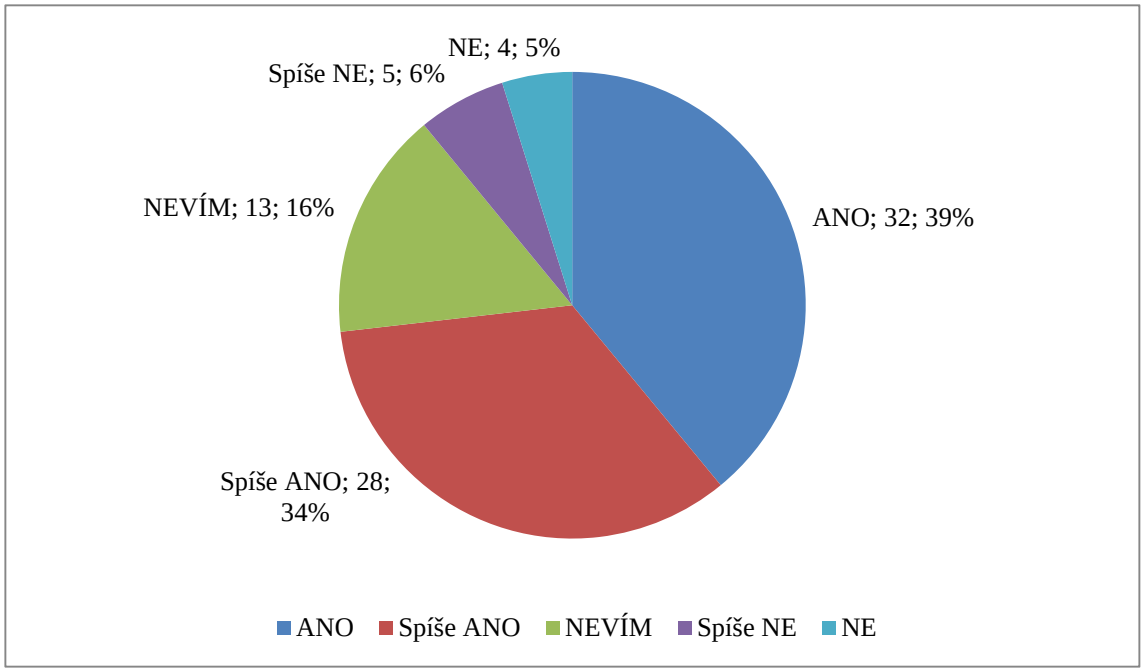
Zdroj[66]

Jednou z často řešených otázek je zda a za jakých podmínek je vhodné analýzy rizik provádět. Velmi frekventovaná je také otázka, zda je vhodné provádět analýzy rizik i v malých firmách, popřípadě mikropodnicích. Tuto oblast autor zkoumá pomocí otázek s pořadovými čísly 12, 13 a 15.

Graf 11 znázorňuje odpovědi respondentů na otázku, zda je vhodné provádět analýzy rizik ve firmách všech velikostí a zaměření. Odpovědi na tuto otázku autora překvapily, vzhledem k již prezentovaným datům, velmi překvapen. Celkem 60 dotazovaných, tedy 73% osob ze zkoumaného vzorku odpovědělo na otázku, že je vhodné provádět analýzy rizik ve firmách všech velikostí a zaměření tedy pozitivně.

[66] Autor práce, 2016 (vlastní šetření).

Graf 11: Je vhodné provádět analýzy rizik ve firmách všech velikostí a zaměření?

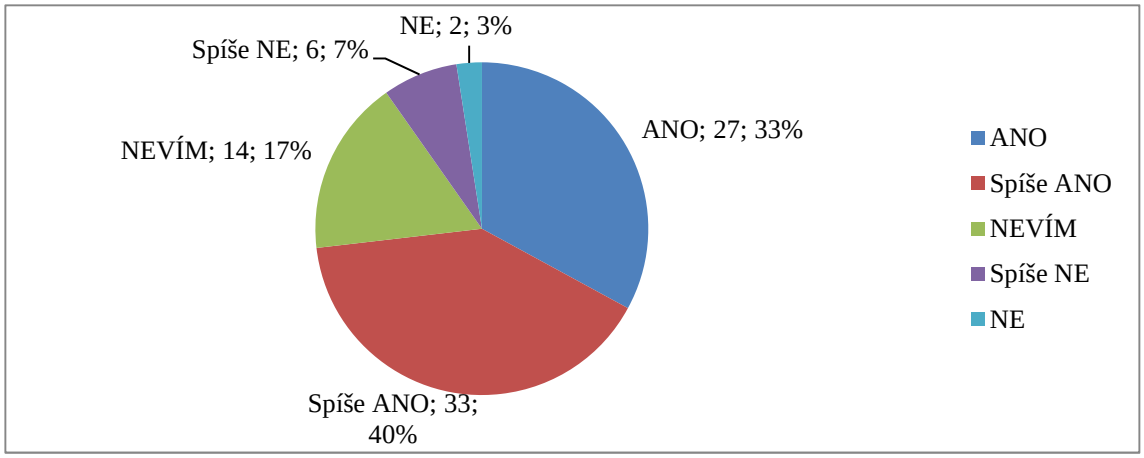


Zdroj[67]

Dalším problémem, se kterým se lidé a často vedení organizací potýká, je zda provádět analýzy rizik v týmu, či nikoli. Autor v rámci výzkumu položil otázku, jestli je vhodné provádět analýzy rizik v týmu. Responze prezentuje **Graf 12**. Za povšimnutí stojí fakt, že souhlasně se vyjádřilo celkem 60 dotazovaných, tedy 73% osob ze zkoumaného vzorku. Druhým zajímavým bodem u této výzkumné otázky je počet negativních responzí. Na zmiňovanou otázku odpovědělo záporně pouze 8 osob, tedy 10% dotazovaných. Zbylých 17%, tedy 14 dotazovaných zvolilo možnost nevím. Tento výsledek poukazuje na to, že není možné provést analýzu rizik v organizaci samostatně. Vylučuje to již jen obsah znalostí jedince. Vhodně složený tým, zodpovědný za provedení analýzy rizik, vydá mnohonásobně lepší výkon a relevantnější výsledky, než pokud by každý prováděl analýzu samostatně.

[67] Autor práce, 2016 (vlastní šetření).

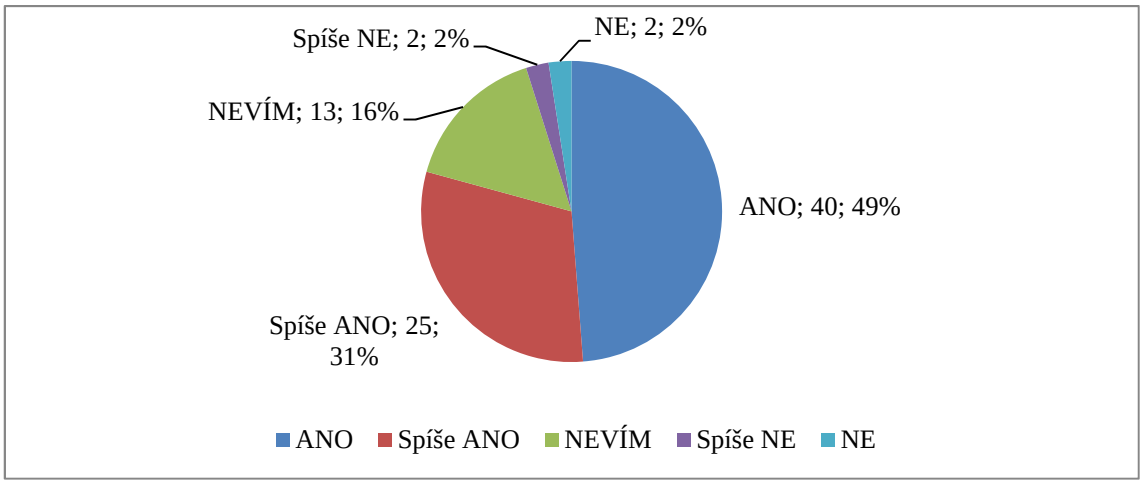
Graf 12: Je vhodné provádět analýzy rizik v týmu?



Zdroj[68]

V souvislosti s prováděním analýz rizik se používají takzvané „**Podpůrné metody**“. Těmito metodami je myšlen například oblíbený brainstorming[69] nebo méně oblíbený audit. Mínění laické veřejnosti o používání těchto metod je takové, jak autor ukazuje na **Grafu 13**. Většina respondentů (80%) uvádí pozitivní odpověď.

Graf 13: Je hodné pro analýzy rizik používat podpůrných metod?



Zdroj[70]

[68] Autor práce, 2016 (vlastní šetření).
[69] Brainstorming – český překlad – bouře mozků, oblíbená metoda pro získávání nových nápadů, prováděná v týmu.
[70] Autor práce, 2016 (vlastní šetření).

Jasnou převahu kladných responzí v grafech 12 a 13 autor chápe tak, že nejlepší možnou cestou pro provedení analýzy rizik, dle laické veřejnosti, je týmová práce s použitím podpůrných metod. Týmová práce je vhodná hlavně kvůli různým znalostem i osobním zkušenostem jednotlivých členů týmu a také kvůli sdílení odpovědnosti za provedenou práci. U podpůrných metod je převaha kladných responzí ještě znatelnější, což je dle autorova názoru důsledkem toho, že český národ rád využije každé příležitosti pro usnadnění práce.

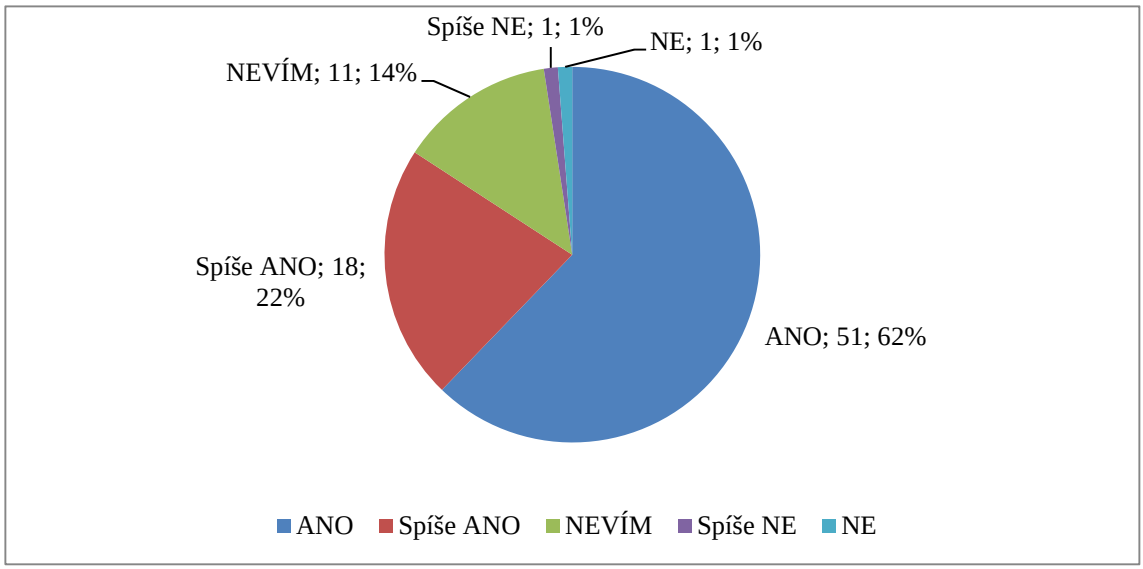
V otázkách s pořadovými čísly 17, 18, 19 a 20 se autor zaměřil na některé aspekty, které je nutné brát v úvahu při provádění analýz rizik. Tématem byla právní úprava týkající se analyzované oblasti[71], přírodních faktorů[72] a možných výstupů z analýz při zkoumání obchodního případu[73] a bezpečnostního incidentu[74]. V této oblasti byl autor příjemně potěšen, protože odpovědi dotazovaných byly v souladu s obecným přesvědčením.

Jak znázorňuje **Graf 14**, 69 respondentů (84% z celkového počtu) vyslovilo souhlas s tvrzením, že je nutné při provádění analýz rizik brát v úvahu právní úpravu týkající se analyzované oblasti. Negativně se vyslovili pouze 2 dotazovaní, tedy 2%. Nevědělo 11 dotazovaných (14%).

U otázky týkající se přírodních faktorů autor očekával vyšší počet odpovědí, které potvrdí, že je nutné zařadit tyto faktory do analýz rizik bezpečnosti informací. Tvrzení bylo položeno negativně takto: *„Do analýz rizik bezpečnosti informací není možné zařadit přírodní faktory (oheň, vítr, voda atd…).“*[75] **Graf 15** znázorňuje rozdělení responzí, kde záporné, tedy odpovědi „NE“ jsou v obecném vnímání správně. Správně se vyjádřilo 53 osob, tedy 64% dotazovaných. Chybné možnosti zvolilo 16 osob, tedy 20% dotazovaných. K otázce se neumělo vyjádřit zbylých 13 osob, což ve výsledku s chybnými odpověďmi znamená 36% dotazovaných.

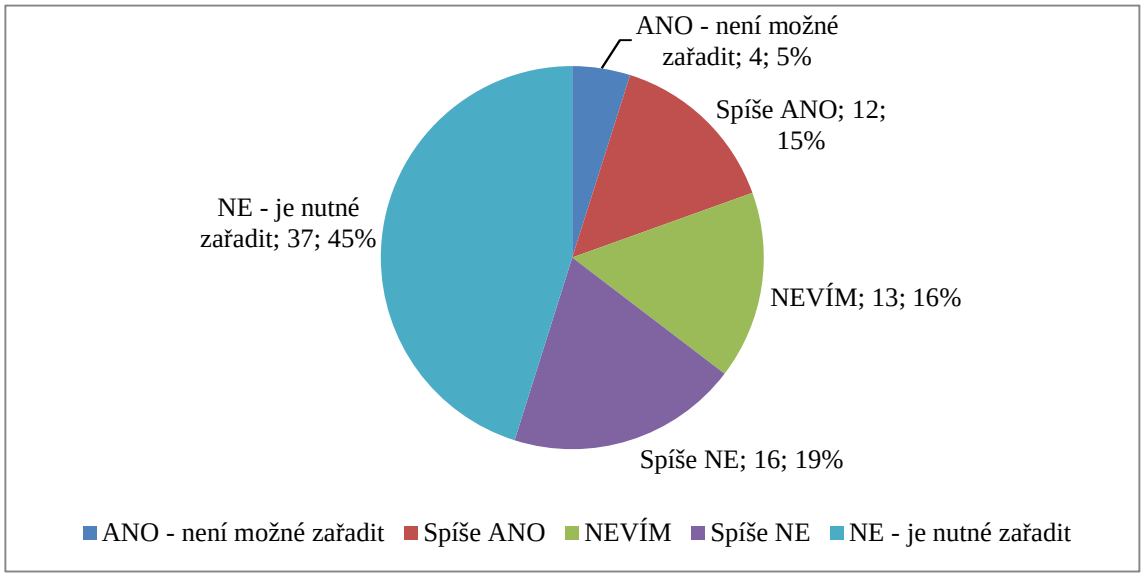
[71] Otázka s pořadovým číslem 17.
[72] Otázka s pořadovým číslem 18.
[73] Otázka s pořadovým číslem 19.
[74] Otázka s pořadovým číslem 20.
[75] Autor práce, 2016 (vlastní šetření).

Graf 14: Při provádění analýzy rizik je nutné brát v úvahu právní úpravu týkající se analyzované oblasti.



Zdroj[76]

Graf 15: Není možné zařadit přírodní faktory.



Zdroj[77]

[76] Autor práce, 2016 (vlastní šetření).
[77] Tamtéž.

Posledními dvěma tvrzeními v této kategorii autor zkoumal, jak laická veřejnost uvažuje v rámci analýz. Tvrzení byla položena podobně tak, aby byl dosažitelný jasný výsledek. Pro ilustraci autor uvádí přesné znění:

1. Při analyzování rizik obchodního případu (zvládneme zakázku, riziko při nesplnění zakázky, zákonné aspekty) bychom měli, za použití různých metod analýz rizik, dospět ke srovnatelným výsledkům.[78]
2. Při analyzování bezpečnostních incidentů bychom měli za použití různých metod analýz, dospět k podobným příčinám vzniku incidentu.[79]

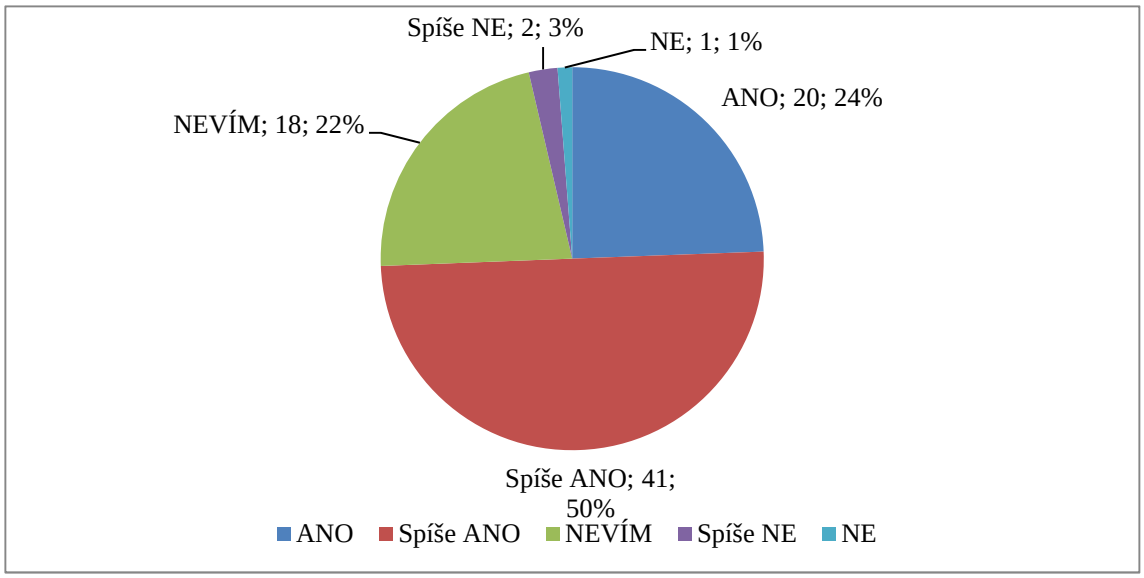
Graf 16 prezentuje mínění laické veřejnosti ohledně srovnatelných výsledků při použití různých metod analýz rizik. Data vyplývající z této otázky jsou uspokojivá. Celkem 61 dotazovaných (74%) se vyjádřilo v kladném smyslu. Zbylých 21 dotazovaných (26%) buď nevědělo, nebo se vyjádřilo negativně. Toto tvrzení autor uvedl také kvůli zájmu na zjištění, zda v závěru vyplňování dotazníkového šetření bude respondent přemýšlet logicky a ne pouze zaškrtávat možnosti, aniž by si přečetl zadání. Výsledná čísla svědčí o poctivém vyplňování a správném odhadu většiny dotazovaných.

Na **Grafu 17** je prezentováno opět mínění laické veřejnosti. Tentokrát v souvislostech bezpečnostních incidentů a jejich příčin a vyšetřování. Rozložení responzí je podobné jako u Grafu 16, ale i přes téměř shodná tvrzení se ve výsledcích drobně liší. Celkový počet kladných odpovědí byl 59 (72%). Zbylých 23 dotazovaných (28%) se vyjádřilo tak, že neví nebo negativně.

Při porovnání dat obsažených v grafech 16 a 17 je pro autora zarážející nárůst negativních odpovědí. U odpovědi „NE“ a „Spíše NE“ se jedná o nárůst o 1 osobu. Tento výsledek je na úkor kladných odpovědí. Odpovědi „NEVÍM“ zůstávají v obou případech na stejném počtu 18 osob.

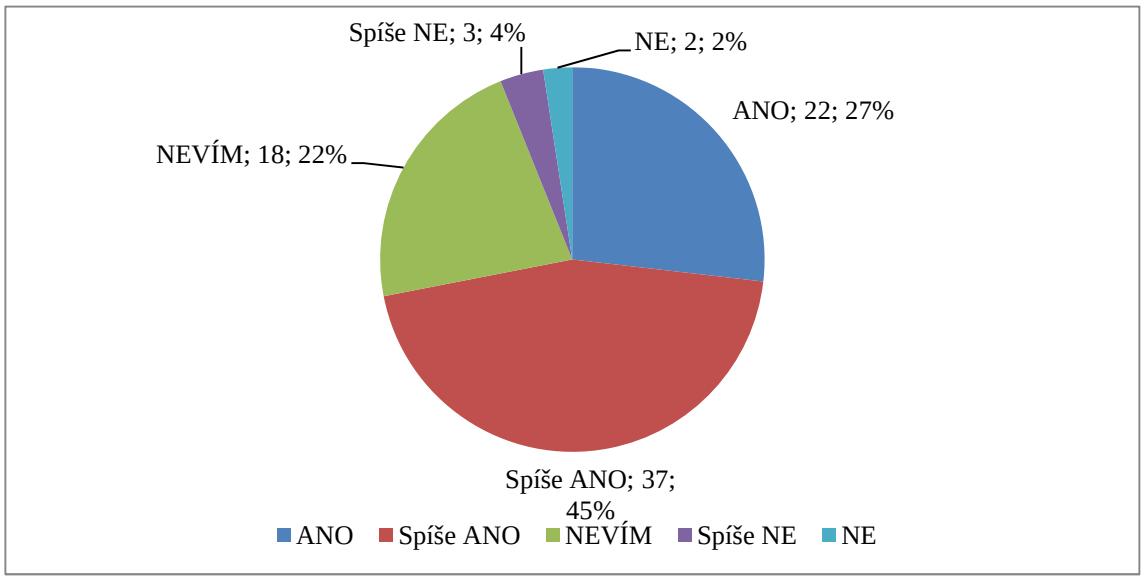
[78] Otázka s pořadovým číslem 19.
[79] Otázka s pořadovým číslem 20.

Graf 16: Analyzování rizik obchodního případu - různé metody - srovnatelné výsledky.



Zdroj[80]

Graf 17:Analyzování bezpečnostního incidentu - různé metody - podobné příčiny.



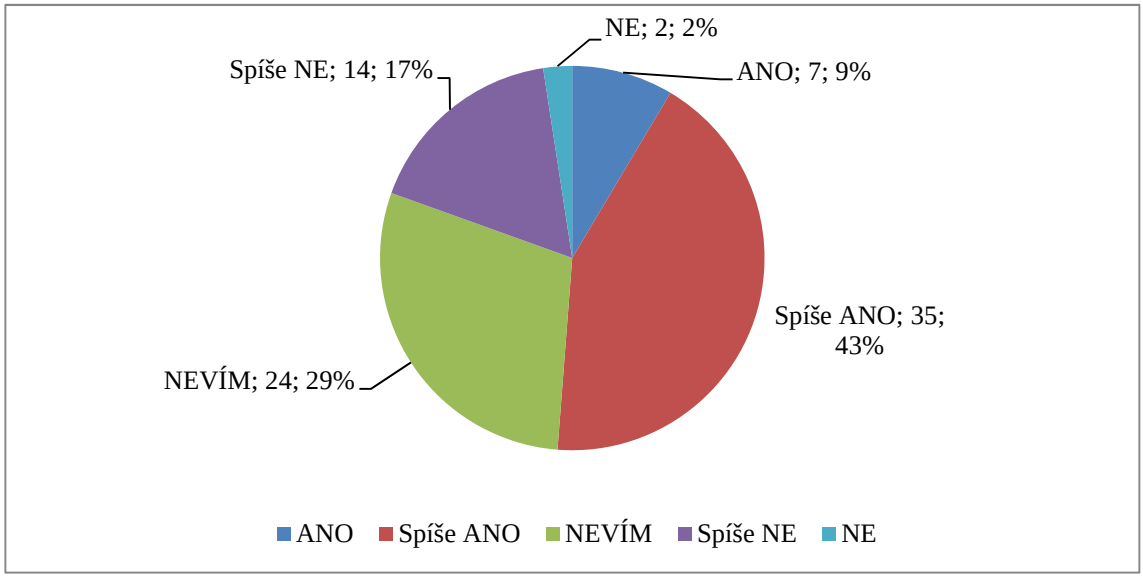
Zdroj[81]

[80] Autor práce, 2016 (vlastní šetření).
[81] Tamtéž.

Poslední dvě tvrzení v dotazníku, tedy otázky s pořadovými čísly 21 a 22, byla zaměřena na osobní zkušenost či předpoklady průběhu a dopadů auditů systémů řízení.

Otázku s pořadovým číslem 21, výsledky prezentuje **Graf 18**, autor položil hlavně z důvodu, že sám ve svém profesním životě realizuje audity systémů řízení. Přesvědčení autora o tom, že audit je laickou veřejností vnímán pouze jako ekonomická nebo finanční kontrola a ne jako jeden z nástrojů ke zlepšování vychází také z osobní zkušenosti.

Graf 18: Audit systému řízení bývá obvykle nepříjemný a náročný pro auditovaného.



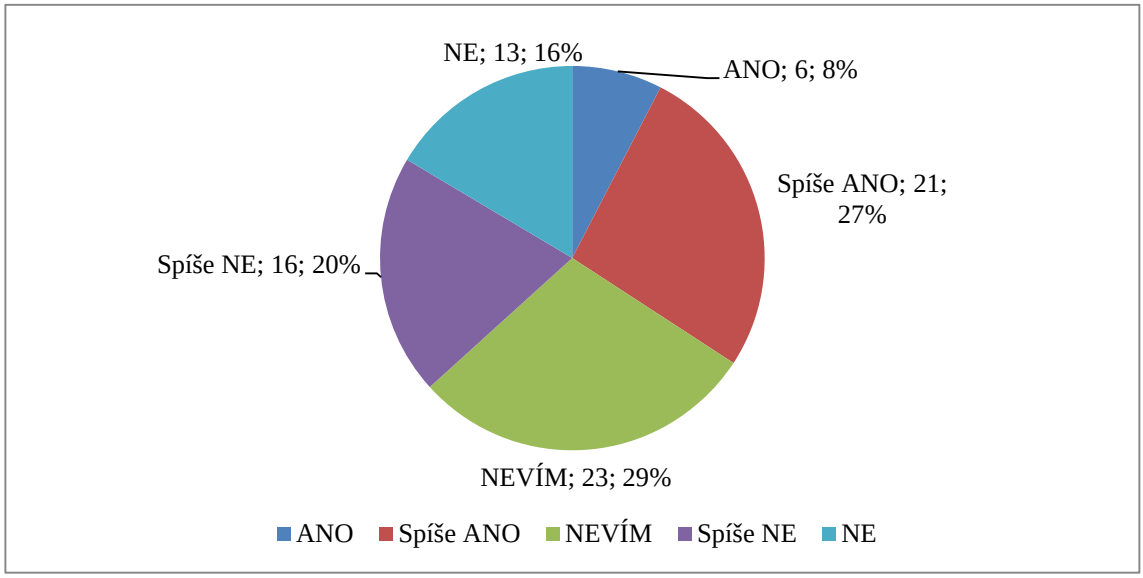
Zdroj[82]

Z dostupných dat vyplynulo, že s tvrzením o nepříjemnosti a náročnosti auditu, souhlasí 42 dotazovaných (52%). Celkem 24 dotazovaných (29%) zvolilo možnost „NEVÍM“. Pouze 16 dotazovaných (19%) odpovědělo negativně. Toto rozložení odpovědí, dle autora svědčí o celkové neznalosti principů auditů systémů řízení. Nejedná se o represivní nástroje, ale o podpůrnou činnost, která ověřuje shodu požadavků s prvky norem, standardů a vnitropodnikových směrnic.

[82] Autor práce, 2016 (vlastní šetření).

Graf 19 prezentuje odpovědi na tvrzení s pořadovým číslem 22. Tvrzení se týká výstupů z auditu systému řízení s dodatkem, že obvykle bývá výstupem postih pro jedince (v konečném důsledku finanční, kariérní atd.).

Graf 19: Výstup z auditu systému řízení = postih pro jedince.



Zdroj

Zde již výsledky svědčily o faktu, že dotazník vyplňovalo i několik respondentů, kteří nejsou v oblasti systémů řízení úplnými laiky. I přes tento fakt je zarážející kolik dotazovaných si myslí, že výstupem z auditu systému řízení bývá postih pro jedince. S tímto tvrzením souhlasilo celkem 27 dotazovaných (35%). Nesouhlasně se k tvrzení vyjádřilo 29 dotazovaných (36%). Nezkušených respondentů, nebo takových, kteří nevědí, co jaké jsou výstupy z auditu systému řízení, bylo 23 (29%).

7.4 Závěry plynoucí z dotazníkového šetření

V této kapitole autor shrnuje výsledky a závěry z dotazníkového průzkumu se vztažením ke stanoveným hypotézám.

Autor se v rámci dotazníkového průzkumu dověděl několik zajímavých skutečnostní. Na základě dat získaných dotazníkovým šetřením zde uvádí, zda byly pracovní hypotézy potvrzeny, či vyvráceny.

1. Autorovo přesvědčení je takové, že obecné povědomí o analýzách rizik je nízké.
    - Tato hypotéza byla za pomoci dat získaných dotazníkovým průzkumem bezezbytku potvrzena. Obecné povědomí laické veřejnosti o analýzách rizik je nízké. Tvrzení podporují data zobrazená v grafech uvedených výše. Autor zde speciálně upozorňuje na data z **grafu 9**, který se zabývá otázkou zařazení personálu mezi rizika. Celkem 24 dotazovaných (**30%**) odpovědělo, že neví nebo negativně (personál nelze zařadit mezi rizika).
2. Laická veřejnost považuje pojem aktivum za účetní položku bez vztahu k rizikům.
    - K autorovu překvapení byla tato hypotéza vyvrácena. V případě této hypotézy se autor odvolává na data uvedená v grafech 5, 6 7, 8 a 10, které se týkají hlavně aktiv.
3. Velikost firmy ovlivňuje povědomí o problematice a vědomí závažnosti analýz rizik.
    - V případě této hypotézy autor nečekal potvrzení nebo vyvrácení, jako spíše určení přímé či nepřímé úměrnosti. Z dat získaných dotazníkovým průzkumem je zřejmé, že nejvyšší povědomí o problematice je v nejmenších organizacích.
4. Audit ve firmě není prováděn jako bezpečnostní prověrka, ale pouze jako ekonomická nebo finanční kontrola.
    - U této hypotézy se autor přesvědčil, že audit systému řízení je vnímán hlavně nepříjemná záležitost s negativními dopady na jedince. V tomto

případě je možné přirovnat, na základě získaných dat, audit ke kontrole.[83]

Autor považuje za důležité uvést fakt, že data jsou mírným způsobem zkreslena, neboť určité procento respondentů v rámci dotazníkového průzkumu je autorovými profesními kolegy. Je tedy jasné, že v případě většího, reprezentativního, vzorku dotazovaných by výsledky byly odlišné.

Výsledky dotazníkového šetření, které zde autor prezentuje jsou k datu 5.2.2016. Dotazníkové šetření je i nadále spuštěno a aktivní. Autor věří, že se mu podaří v průběhu následujících dvou let získat dostatek responzí, aby mohl prohlásit zkoumaný soubor za reprezentativní v kontextu rozložení souboru dle tabulky 1. Záměrem autora je možné rozšíření této bakalářské práce do práce diplomové.

[83] Audit hledá shodu. Kontrola se snaží objevit problém, čili neshodu.

8 ŘÍZENÝ ROZHOVOR

Řízený rozhovor autor realizoval ve vybrané firmě. Respondenti jsou členy vrcholového vedení, týmu odpovědného za implementaci systému řízení bezpečnosti informací a třetí strany, která zajišťuje metodickou podporu v průběhu procesu implementace systému. Hendl ve své knize o kvalitativním výzkumu uvádí: *„Zvláštní pozornost je nutné věnovat začátku a konci rozhovoru. Na začátku dotazování je nutné prolomit případné psychické bariéry a zajistit souhlas se záznamem. Také zakončení rozhovoru je jeho důležitou součástí. Právě na konci rozhovoru nebo při loučení můžeme ještě získat důležité informace.“*[84] Dále Hendl upozorňuje na to, aby tazatel umožnil, eventuálně nabídl dotazovanému možnost dodatečného kontaktu.[85]

Toto doporučení pro fázi řízeného rozhovoru autor nemusel aplikovat. Se všemi dotazovanými má dlouholeté pracovní vztahy, které v některých případech překračují profesní rovinu do roviny přátelské. Autor ještě doplňuje, že důležité informace získával nejen v průběhu jednotlivých rozhovorů, ale i na dalších pracovních schůzkách a tím si utvořil ucelenější obrázek o odpovědích jednotlivých respondentů.

Všichni dotazovaní byli vstřícní a dle názoru autora, maximálně objektivní. Autor si v úvodu rozhorů, které probíhaly samostatně s každým respondentem, vyžádal souhlas s uvedením a zveřejněním odpovědí ve své bakalářské práci. Všichni respondenti souhlasili. V rámci zachování jistého stupně důvěrnosti vedení vybrané firmy autora opět upozornilo, že je vhodné uvést získané údaje anonymně. Autor tedy zvolil do této práce interpretaci odpovědí respondentů bez jmen, ale pouze s iniciálami.

Níže autor uvádí u iniciál jmen stručný popis pozice respondenta, jeho postavení ve vybrané firmě a v systému řízení této firmy. Autor práce připomíná, že popisy pozic a další podrobnosti týkající se vybrané firmy, jsou na výslovné přání vrcholového vedení

[84] HENDL, J. *Kvalitativní výzkum: základní metody a aplikace.* Praha: Portál, 2005. s. 167. ISBN: 80-7367-040-2.
[85] Tamtéž.

zobecněny. V případě popisů postavení jednotlivců ve vybrané firmě sice nejde o citlivé informace, ale kvůli dodržení integrity práce autor volí shodnou metodu popisu jednotlivých skutečností.

- M. Č. – Majitelka a jednatelka externí firmy. M. Č. zajišťuje metodickou podporu IMS[86] ve vybrané firmě. Její hlavní odpovědností je interpretace požadavků mezinárodních standardů a pomoc při jejich implementaci do života vybrané firmy.
- I. N. – Ve vybrané firmě působí na pozici představitele vedení pro IMS, kde je mimo jiné odpovědná za údržbu a rozvoj IMS. Dále zajištění interních auditů, relevantních školení jak pro IMS, tak pro zákonné požadavky[87]. Při implementaci systému řízení bezpečnosti informací měla na starost zejména sběr a kompletaci podkladů, jejich analyzování a prezentování zjištění. Při externích auditech certifikačními orgány a kontrolách ze strany státní správy je zodpovědná za přípravu auditů a kontrol, komunikaci v průběhu auditů a kontrol a prezentování výsledků vrcholovému vedení. Členka Fóra pro bezpečnost informací.
- A. V. – Představitel vedení pro systém řízení bezpečnosti informací. Zástupce IT oddělení v projektovém týmu. Při implementaci systému řízení bezpečnosti informací zodpovědný za kompletaci a doplnění stěžejních dokumentů z hlediska techniky a technologie. Důležitý člen týmu při realizaci analýzy rizik díky znalostem zabezpečení IT ve vybrané firmě.
- M. N. – Jeden z jednatelů vybrané firmy. Vrcholová odpovědnost za IMS. V průběhu implementace systému řízení bezpečnosti informací pouze informován o průběhu procesu. Vzhledem k pozici ve vybrané firmě schvaluje navrhovaná opatření, vyplývající z analýz rizik a auditů celého IMS.

[86] IMS – Integrovaný systém managementu.
[87] Například školení v oblasti bezpečnosti a ochrany zdraví při práci.

- M. U. – Vedoucí IT oddělení v mateřské společnosti vybrané firmy. Dlouhodobě působil jako vedoucí IT oddělení přímo ve vybrané firmě. Má vrcholovou odpovědnost za celé IT ve vybrané firmě, včetně strategií rozvoje IT.

Jak je z popisu pozic respondentů patrné, všichni dotazovaní mají velice úzké propojení s fungováním IMS ve vybrané firmě. Autor celkem prezentuje výsledky řízených rozhovorů se dvěma zástupci vrcholového managementu, dvěma zástupci středního managementu a jednou externí pracovnicí.

8.1 Otázky pro řízený rozhovor a odpovědi respondentů

Otázky autor uvádí v **kapitole 6.3 Otázky pro řízený rozhovor**. V této kapitole jsou autorem uváděny otázky, společně s odpověďmi respondentů.

Otázka 1.: Vnímáte řízení rizik ve společnosti, kde pracujete?

M. Č.: *Samozřejmě, vždyť rizika se skrývají ve všech oblastech řízení firmy. Jako majitel firmy vnímám hlavně podnikatelská rizika a rizika, která souvisí s lidským kapitálem obecně. Zároveň musíme brát v úvahu rizika, která plynou z geopolitické situace.*

I. N.: *Nejen že vnímáme, snažíme se rizika i řídit. Zpočátku to byla pouze rizika BOZP, následně vznikla potřeba řídit rizika obchodních případů a nyní se snažíme řídit veškerá rizika ve všech oblastech nejen řízení firmy, ale i při realizaci zakázek.*

A. V.: *Na mé pozici ve firmě je těžké rizika nevnímat. Do určité doby vnímají pracovníci IT oddělení rizika pouze v souvislosti s hardwarem a softwarem, počítačovými viry a nezkušeností nebo nepozorností uživatelů. Vedení naší firmy se rozhodlo pro zavedení ISMS[88] a mě přidělilo funkci s odpovědností za ISMS. V této době a po několik školeních, jsem začal vnímat rizika v širší souvislosti a ne jen jak jsem uvedl.*

[88] ISMS – systém řízení bezpečnosti informací.

M. N.: *Jako vrcholový manažer považuji řízení rizik za nedílnou součást svých povinností, stejně tak vnímám i zodpovědnost za celý proces řízení rizik.*

M. U.: *Vzhledem k mé korporátní odpovědnosti za ICT si bez řízení rizik vůbec nedovedu výkon své pozice a ani chod firmy představit.*

Otázka 2.: Interní audity bývají náročnější než externí audity. Prosím odůvodněte své tvrzení krátkým komentářem.

M. Č.: *Interní audit je prováděn školeným personálem, který zná podrobně nejen dokumentaci firmy, ale i její kulturu a zvyklosti. Interní audit může mnohem podrobněji zkoumat procesy a jejich vzájemné interakce zejména v oblastech, kde to zejména z kapacitních důvodů není při externím auditu možné. Zároveň má interní audit větší flexibilitu a v případě podpory vedení i mnohem detailnější návrhy a řešení nápravných opatření.*

I. N.: *Vzhledem k tomu, že řídím tým interních auditorů, tak znám všechna úskalí interního auditu. Již od počátku plánování auditů tak, aby interní audit poskytl řádnou a očekávanou zpětnou vazbu a zároveň neparalyzoval firmu je nutné, pracovat jen s perfektně vyškoleným personálem. Náročnost interních auditů indikuje i fakt, že interní auditoři jsou vybráni z řadových zaměstnanců a často se stane, že auditovaný s vyšší pozicí neakceptuje auditora jako autoritu. Důležitost komunikace ve všech vrstvách firmy je proto jednou z nejkomplikovanějších oblastí. Rovněž vhodná prezentace, která popisuje skutečný stav auditovaného procesu, může velice ovlivnit institut interního auditu jako celku. Podpora vedení je proto nutnou podmínkou k řádnému výkonu interního auditu.*

A. V.: *Jsem členem týmu interních auditorů, takže tuto otázku vnímám ze dvou různých úhlů. Bývám přítomen u auditů ze strany certifikačních orgánů i při interních auditech v oddělení IT, jako auditovaný. Na druhou stranu sám audituji v ostatních odděleních. Externí audit nemůže nikdy proniknout skutečnost tak do hloubky, jako interní audit. Z tohoto hlediska usuzuji, že interní audity jsou značně náročnější jak pro auditovaného, tak pro auditora.*

M. N.: *Od interního auditu očekávám „nezávislou“ zpětnou vazbu, to samozřejmě přináší mnohem větší tlak jak na auditory, tak na auditované. Interní audit se týká každého zaměstnance i pracoviště a znalost prostředí je pro auditory důležitou podmínkou pro vynikající výkon.*

M. U.: *Interní auditor zná lépe firmu a její fungování a tudíž se může více zaměřit na detaily.*

Otázka 3.: V rámci auditů systémů řízení rizik je vytvářena dokumentace, která je zbytečnou zátěží pro firmu. Lze s tímto tvrzením souhlasit? Proč?

M. Č.: *Dovolím si nesouhlasit. Samozřejmě přebujelá a nepřehledná dokumentace není k ničemu, ale řádně zpracovaná a jednoduchá dokumentace umožňuje určitou retrospektivu. Vhodně popsaná rizika, či skutečnosti a okolnosti mohou velmi pomoci v případě výměny personálu, při řešení známých situací apod.*

I. N.: *Vrcholový management naší firmy vyžaduje jednoduchou formu záznamu z auditu – výsledný protokol. Každý auditor má podrobnější poznámky zachyceny v auditním dotazníku, a pokud je potřeba tvrzení doložit, jsou ve složce auditu k dispozici i objektivní důkazy, případně odkazy na další dokumenty. Není nic kopírováno, opisováno apod. Veškeré podklady jsou uloženy u mne a jsou vrcholovému managementu a auditorům kdykoliv k dispozici.*

A. V.: *Je těžké říci, jestli je vznikající dokumentace zbytečnou zátěží, či nikoli. Vedení jsou předkládány protokoly z auditů. My, jako interní auditoři, máme zpracován obsáhlý auditní dotazník, jehož součástí je podobný popis zjištěných skutečností.* **Autor: Je tedy možné souhlasit s tvrzením?** A. V.: *S tvrzením spíše nesouhlasím.*

M. N.: *Nesouhlas. Dokumentace auditu je u nás odpovídající potřebám, z vlastního auditu je předkládán protokol, a pokud je to nutné, jsou pozorování doložena jednoduchou formou.*

M. U.: *Nesouhlasím, z auditu je vypracován strukturovaný protokol, více dokumentace není vytvářeno.*

Otázka 4.: V rámci přípravy systému řízení rizik na audit je vytvářena dokumentace, která je zbytečnou zátěží pro firmu. Lze s tímto tvrzením souhlasit? Proč?

M. Č.: *Samozřejmě, pokud je vytvářena dokumentace pouze v rámci přípravy na audit značí to, že systém není řádně prosáklý do firemní kultury. V případě plné implementace vznikají dokumentované informace průběžně a před auditem si maximálně auditovaný prověří, zda jsou například složky obchodních případů kompletní – to v našem případě znamená, že ve složce existuje i záznam o posouzení rizik.*

I. N.: *Vrcholový management naší firmy vyžaduje zdokumentování všech okolností celého průběhu auditu a jedinou možnou formou je právě dokumentace všech kroků, získání relevantních podkladů a jasné stanovení prokazatelného seznámení auditovaných s předmětem auditu. Snažíme se o efektivnost a máme zpracovány Check listy a formuláře, které množství dokumentace redukují.*

A. V.: *V naší firmě je na první pohled dokumentace až příliš. Až při podrobnějším náhledu zaměstnanec zjistí, že se jedná o nezbytné minimum. Díky dlouhodobému fungování různých systémů řízení nevzniká dokumentace pouze pro ISO*[89]*, ale jde o běžný postup podporující firemní procesy.*

M. N.: *Vyžaduji pečlivou přípravu na každý audit a speciálně u auditu řízení rizik je dokonalá příprava jak auditorů, tak auditovaných jediným možným předpokladem kvalitně odvedeného vlastního auditu.*

M. U.: *Nesouhlasím, již princip auditu procesu řízení rizik vyžaduje podrobné zdokumentování všech částí od přípravy, přes realizaci a řádné vyhodnocení.*

[89] Doplňující komentář A. V.: *Jako ISO mám na mysli IMS a jeho audit.*

Otázka 5.: Jsou analýzy rizik, respektive systém řízení rizik, ve společnosti kde pracujete vnímány jako represivní nástroj nebo jako účinný nástroj využívaný k rozvoji firmy?

M. Č.: *Vzhledem k tomu, že firma existuje již 6 let lze říci, že systém řízení rizik u nás prezentuje zejména udržitelný rozvoj, bez řízení rizik bychom již s velkou pravděpodobností neexistovali.*[90]

I. N.: *Od zavedení procesů v oblasti řízení rizik na projektech se ukázalo, že se jedná nejen o účinný nástroj, ale v podstatě o podmínku nezbytnou k dalšímu rozvoji firmy. Řízení rizik nám umožnilo v období recese eliminovat snahy přijímat jakékoliv zakázky a ochránilo firmu proti velmi ztrátovým projektům. Vnímám jako velmi pozitivní vytvoření Plánů kontinuity, které pomohly výrazně k nastavení zrcadla v jednotlivých týmech.*

A. V.: *Vedení vnímá analýzy rizik jako dobrý nástroj k rozvoji. Alespoň takový je můj dojem. Řadový zaměstnanec může analýzu rizik vnímat jako represi pouze okrajově, už jen díky zapojení řadových zaměstnanců do procesu analyzování rizik.*

M. N.: *Jednoznačně vnímám analýzy rizik jako účinný nástroj řízení firmy. Dobře odvedená analýza rizik výrazně zjednodušuje rozhodovací procesy na vrcholové úrovni, zefektivňuje rozhodování o nových projektech. Známá rizika též ovlivňují strategické plánování a udržitelný rozvoj. Rovněž připravenost na identifikované krizové situace zklidňuje prostředí. Zapojení personálu do rozhodovacích procesů formou analýz rizik je též velmi vhodným nástrojem, který pomáhá evangelizaci*[91] *řízení rizik ve firmě jako celku.*

M. U.: *Personál to možná vnímá jako represe, ale pro mne je to takové zrcadlo, které mi pomáhá se stanovení strategického rozvoje do budoucna.*

[90] Poznámka autora: Vzhledem ke znění otázky M. Č. odpovídala za vlastní firmu, nikoli za vybranou firmu.
[91] Evangelizace – hlásání a šíření evangelia – zde vztaženo k hlásání a šíření rizik ve vybrané firmě.

8.2 Závěry plynoucí z řízeného rozhovoru

Autor zde vysvětluje a popisuje závěry, ke kterým došel pomocí řízeného rozhovoru. Pracovní hypotéza pro řízený rozhovor zněla: **Střední a vyšší management firmy je dostatečně informován o významu analýzy rizik.**

Z odpovědí respondentů, hlavně pak zástupců vrcholového vedení autor práce usuzuje, že hypotéza byla bezezbytku potvrzena.

Pánové M. N. a M. U., jako zástupci vrcholového vedení, se shodli, že řízení rizik je nedílnou součástí chodu firmy a výkonu jejich pozic. M. C., která na první otázku odpovídala, jako majitel vlastní firmy se shoduje ve svém tvrzení s M. N. a M. U. Zástupci středního managementu, I. N. a A.V., potvrdili vysoké povědomí o řízení rizik i na nižších stupních řízení vybrané firmy.

Druhou otázku, zabývající se náročností interních auditů odpověděli všichni dotazovaní podobně. Zde autor demonstruje odpovědi na responzi pana M. U.: *Interní auditor zná lépe firmu a její fungování a tudíž se může více zaměřit na detaily.* Z této a z dalších odpovědí vyplývá, že interní audit je vnímán jako náročnější než audit externí.

Otázka číslo 3, která cílila na dokumentaci v rámci systému řízení rizik ve vybrané firmě má také shodné odpovědi. Výsledkem je vyjádření nesouhlasu všech respondentů s tvrzením, že při auditech systému řízení rizik vzniká dokumentace, která je zbytečnou zátěží pro firmu.

I čtvrtá otázka byla zaměřená na tvorbu dokumentace. V tomto případě autor zkoumal, zda dotazovaní souhlasí s tvrzením o vzniku zbytečně zatěžující dokumentace při přípravě systému řízení rizik na audit. I zde se vyskytlo, ve všech případech, negativní hodnocení. Zástupci vrcholového managementu dokonce uvedli, že je vyžadována podrobná dokumentace auditu, což je pro autora jedním z důvodů k tvrzení, že pracovní hypotéza byla potvrzena.

Poslední otázka z řízeného rozhovoru měla za cíl zjistit, zda je systém řízení rizik vnímán jako represivní nástroj, nebo jako nástroj účinný pro potřeby řízení a rozvoje vybrané firmy. Autor z odpovědí vyvozuje, že systém řízení rizik a analýzy rizik mohou

být vnímány, jako represivní nástroj mezi řadovými zaměstnanci, ale střední a vrcholový management vnímá tyto nástroje jako nezbytné pro optimální řízení vybrané firmy. Nejvýstižnější je odpověď I. N., která popisuje průběh zavádění procesů řízení rizik a jejich nezbytnost.

ZÁVĚR

V úvodu práce si autor vytyčil cíle práce, kde deklaruje, že primárním cílem této bakalářské práce je seznámit čtenáře s mezinárodními standardy pro řízení rizik, a to hlavně v oblasti bezpečnosti informací. Autor zvolil, pro větší názornost, vybranou firmu. Tento cíl autor splňuje v teoretické části práce, kde uvádí a vysvětluje základní pojmy, popisuje řízení rizik bezpečnosti informací v kontextu mezinárodních standardů. V dalších kapitolách teoretické části autor seznamuje čtenáře s vybranou firmou, metodikou analýzy rizik, která byla ve vybrané firmě použita a s postupem a výstupy z analýzy rizik ve vybrané firmě.

V praktické části se autor věnoval dotazníkovému průzkumu, kde zjišťoval úroveň povědomí o analýzách rizik a řízení rizik bezpečnosti informací. Autor dotazníkový průzkum celkově zaměřil i na systémy řízení bezpečnosti informací. Čtyři pracovní hypotézy, které byly zaměřené na znalosti a zkušenosti z oblasti systému řízení bezpečnosti informací a řízení rizik autor ověřil. Výsledek je následující:

1. Autorovo přesvědčení je takové, že obecné povědomí o analýzách rizik je nízké.
    - Hypotéza potvrzena.
2. Laická veřejnost považuje aktivum za účetní položku bez vztahu k rizikům.
    - Hypotéza vyvrácena.
3. Velikost firmy ovlivňuje povědomí o problematice a vědomí závažnosti analýz rizik.
    - Hypotéza potvrzena.
4. Audit ve firmě není prováděn jako bezpečnostní prověrka, ale pouze jako ekonomická nebo finanční kontrola.
    - Hypotéza potvrzena.

Autor k potvrzení či vyvrácení hypotéz využil data, která získal dotazníkovým průzkumem, ve kterém nasbíral 82 odpovědí. Parametry získaného souboru autor uvádí v kapitole 7.1 Základní parametry získaného souboru.

Další součástí praktické části byl řízený rozhovor se zástupci vybrané firmy. Autor definoval pracovní hypotézu s číslem 5, která zní takto: Střední a vyšší management firmy je dostatečně informován o významu analýzy rizik. Po vyhodnocení odpovědí respondentů, kteří zastávají ve vybrané firmě pozice na úrovni vrcholového managementu, středního managementu a konzultanta autor dospěl k následujícímu závěru: Střední a vyšší management je ve skutečnosti velmi dobře informován o významu analýzy rizik. Zástupci středního a vyššího managementu explicitně vyžadují provádění analýz rizik a vnímají analýzy rizik jako nedílnou součást vedení firmy.

Autor bakalářské práce seznámí v průběhu prvního čtvrtletí 2016 zástupce vybrané firmy s výsledky svého zkoumání. Tyto výsledky podpoří autorův návrh na zvyšování povědomí o systému řízení bezpečnosti informací a systému řízení rizik ve firmě. Vzhledem k tomu, že firma zaměstnává kolem 500 osob, navrhne autor úpravy v proškolování zaměstnanců se zaměřením na celkové povědomí zaměstnanců o systémech řízení bezpečnosti informací a systémech řízení rizik. Tento krok volí autor z toho důvodu, že z dotazníkového průzkumu vyplývá nepřímá úměrnost mezi velikostí firmy a povědomím zaměstnanců.

V úvodu autor zmiňuje i sekundární přínos práce, kterým má být stručný popis procesu řízení rizik, spolu s objasněním základních pojmů. Dle názoru autora má bakalářská práce potenciál být v dotčené oblasti jedním ze zdrojů použitelných při prvotním seznamování osob se systémy řízení bezpečnosti informací a řízení rizik. Tento potenciál je zvýšen tím, že autor jako podklady pro zpracování bakalářské práce použil mezinárodní standardy zabývající se riziky.

Celá problematika systémů řízení a konkrétně systémů řízení bezpečnosti informací a systémů řízení rizik je velmi obsáhlá a na komplexní pojetí není v bakalářské práci prostor. Autorovým záměrem je rozšíření práce v některé z dalších kvalifikačních prací tak, aby byla problematika systémů řízení bezpečnosti informací a systémů řízení rizik popsána podrobně a kompletně se všemi aspekty. Autor také nechává aktivní dotazníkové šetření. Cílem je získání většího a objektivnějšího vzorku dat. V případě úspěchu chce autor prezentovat výsledky průzkumu v některém z odborných časopisů, eventuálně v krátkém příspěvku na konferenci zaměřené na bezpečnost informací.

SEZNAM POUŽITÝCH ZDROJŮ

Seznam použitých českých zdrojů

Knihy a monografie

HENDL, J. *Kvalitativní výzkum: základní metody a aplikace.* Praha : Portál, 2005. ISBN: 80-7367-040-2.

HNILICA, J., J FOTR. *Aplikovaná analýza rizika ve finančním managementu a investičním rozhodování.* Praha: Grada Publishing, a.s., 2009. ISBN: 978-80-247-2560-4.

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

PAULOVČÁKOVÁ, L, J. HUK, J. KLUGEROVÁ, T. VACÍNOVÁ a D. BENEŠOVÁ. *Jak vypracovat bakalářskou a diplomovou práci.* Praha : Univerzita Jana Amose Komenského, 2015. ISBN: 978-80-7452-106-5.

RAIS, K., R. DOSKOČIL. *Risk management.* Brno : AKADEMICKÉ NAKLADATELSTVÍ CERM, 2007. ISBN: 978-80-214-3510-0.

SMEJKAL, V., K. RAIS. *Řízení rizik ve firmách a jiných organizacích.* Praha : Grada Publishing, a.s., 2006. ISBN: 80-247-1667-4.

VEBER, J. et al. *Management kvality, environmentu a bezpečnosti práce.* Praha : Management Press, s.r.o., 2010. ISBN 978-80-7261-2010-9.

Normy

UNMZ. *ČSN ISO 31000 Management rizik - Principy a směrnice.* Praha : Uřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2010. 86884.

UNMZ. *ČSN ISO/IEC 27000 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník.* Praha : Uřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014. 95885.

UNMZ. *ČSN ISO/IEC 27001 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky.* Praha : Uřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014. 95805.

UNMZ. *ČSN ISO/IEC 27005 Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací.* Praha : Uřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013. 93071.

UNMZ. *TNI 01 0350 Management rizik - Slovník (Pokyn 73).* Praha : Úřad pro normalizaci, metrologii a státní zkušebnictví, 2010. 86437.

Firemní dokumenty

ČELIKOVSKÝ, J. *Dokument vybrané firmy: Metodika hodnocení rizik.* Verze 1. 2015.

VYBRANÁ FIRMA. *Manuál ISMS.* Verze 1. *2015.*

VYBRANÁ FIRMA. *Příručka společnosti.* Verze 12. 2013

VYBRANÁ FIRMA. Příručka IT. Verze 2. 2013

Seznam použitých zahraničních zdrojů

Zahraniční zdroje nebyly použity.

Seznam použitých internetových zdrojů

Doporučení Komise ze dne 6. května 2003, týkající se definice mikropodniků, malých a středních podniků (oznámeno pod číslem dokumentu C(2003) 1422) (Úř. věst. L 124, 20.5.2003, s. 36-41). In: *EUR-Lex* [právní informační systém]. Úřad pro publikace Evropské unie [cit. 2016-02-18]. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=URISERV%3An26026

Učící se organizace. *Management mania* [online]. 2013 [cit. 2016-02-14]. Dostupné z: https://managementmania.com/cs/ucici-se-organizace

ABZ. CZ. Slovník cizích slov [online]. © 2005-2016 [cit. 2016-02-14]. Dostupné z: http://slovnik-cizich-slov.abz.cz/

WWW stránky Vybrané firmy. [online]. 2016 [cit. 2016-02-02]. Dostupné z: http://www.vybrana-firma-web.cz

SEZNAM ZKRATEK

DO - dostupnost

DP - dopad

DU - důvěrnost

I - integrita

IMS – integrovaný systém managementu

ISMS – Information security management systém – systém řízení bezpečnsoti informací

IT – informační technologie

MBI – manager bezpečnosti informací

MR – míra rizika

OSVČ – Osoba samostatně výdělečně činná

PV – pravděpodobnost výskytu

PFO – podnikající fyzická osoba

PO – právnická osoba

SPOC – Single Point of Contact – jediný kontaktní bod

SEZNAM OBRÁZKŮ, TABULEK A GRAFŮ

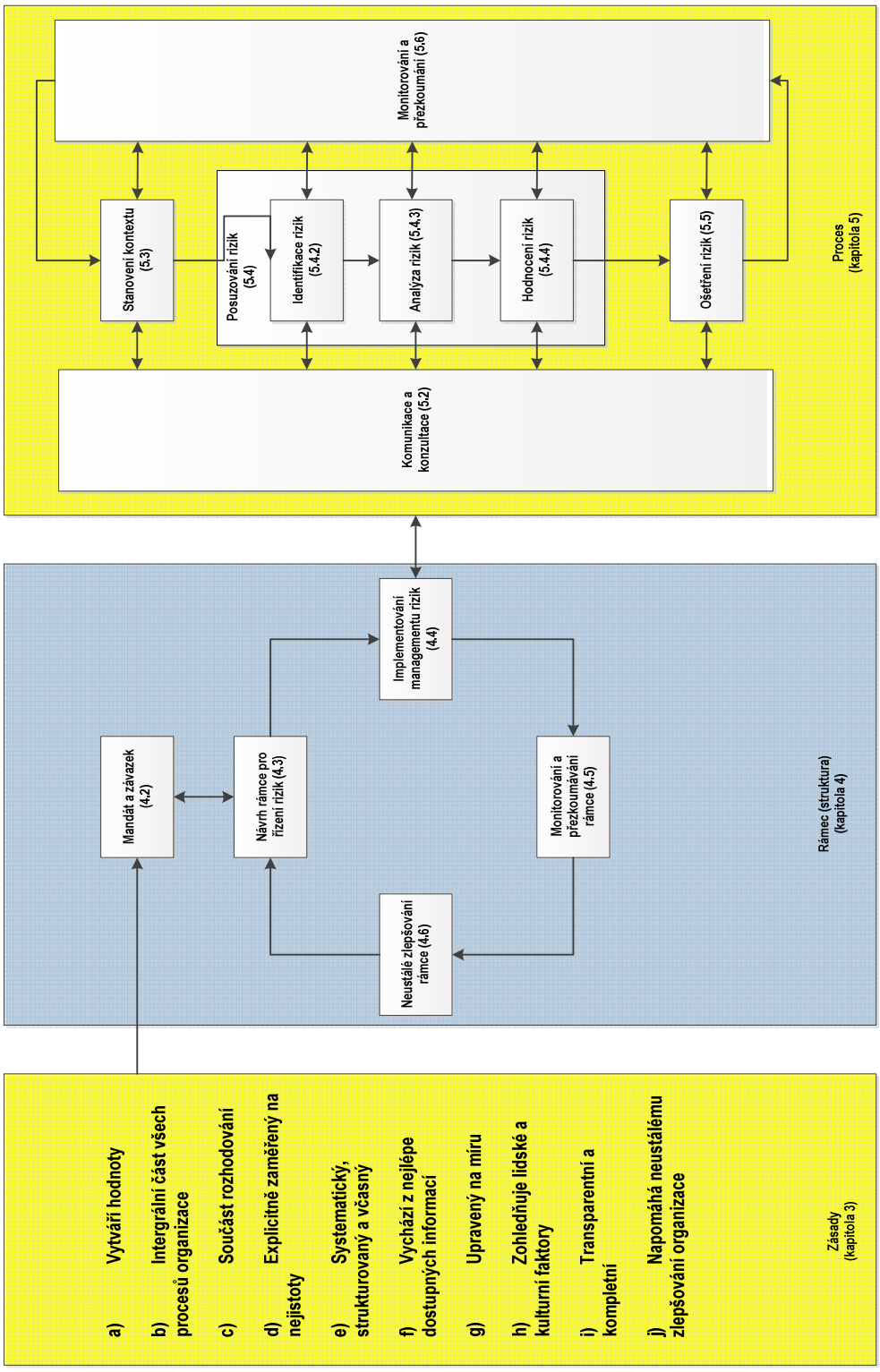
Seznam obrázků

Seznam tabulek

Seznam grafů

SEZNAM PŘÍLOH

Příloha A – Vazby mezi principy, rámcem a procesem managementu rizik



Zdroj[92]

[92] UNMZ. *ČSN ISO 31000 Management rizik - Principy a směrnice.* Praha : Uřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2010. s. 9. 86884.

BIBLIOGRAFICKÉ ÚDAJE

Jméno autora:	**Jiří Čelikovský**
Obor:	**Bc. BS**
Forma studia:	**prezenční studium**
Název práce:	**Analýza rizik v kontextu norem ČSN ISO/IEC 27005 a ČSN ISO 31000**
Rok:	**2016**

Počet stran textu bez příloh: 65

Celkový počet stran příloh: 1

Počet titulů českých použitých zdrojů: 16

Počet titulů zahraničních použitých zdrojů: 0

Počet internetových zdrojů: 4

Vedoucí práce: PaedDr. Ing. Jan Zelinka