Bankovní institut vysoká škola Praha

Katedra matematiky, statistiky a informačních technologií

Řízení IT rizik v podnikové praxi

Bakalářská práce

Autor: **Regina Sadrieva**

Informační technologie

Vedoucí práce: **Ing. Lubomír Jankových, CSc.**

Praha **duben, 2013**

Prohlášení:

Prohlašují, že jsem svou bakalářskou práci zpracovala samostatně a v seznamu uvedla veškerou použitou literaturu.

Svým podpisem stvrzuji, že odevzdána elektronická podoba práce je identická s její tištěnou verzí, a jsem seznámena se skutečností, že se práce bude archivovat v knihovně BIVŠ a dále bude zpřístupněna třetím osobám prostřednictvím interní databáze elektronických vysokoškolských prací.

V Praze, dne Regina Sadrieva

Děkuji vedoucímu bakalářské práce, Ing. Lubomírovi Jankových, CSc., za cenné rady, připomínky a neocenitelnou pomoc při zpracování bakalářské práce.

Anotace

V bakalářské práci je objasněna bezpečnost informací. V práci jsou důkladně popsány řešení bezpečností IS/ICT, metodické rámce COBIT a Risk IT, také jsou podrobně popsány bezpečnostní normy ISO/IEC 27xxx. Případová studie je věnovaná průzkumu úrovně ISMS v podnicích.

Klíčová slova: COBIT, Risk IT, ISMS, ISO/IEC 27xxx.

Annotation

The bachelor thesis clarifires concepts of the Information Security. The paper deals with detailed description of Security Management, frameworks as COBIT and Risk IT, also security standards ISO/IEC 27xxx. The case study is dedicated to the paper that is focused on the exploration of the ISMS level in the firm.

Key words: COBIT, Risk IT, ISMS, ISO/IEC 27xxx.

Obsah:

Úvod

Zajišťování bezpečnosti firemního IT je nevděčná práce, která vyžaduje ostražitost, neustálou pohotovost a neustále sledování parametrů výpočetního prostředí. V dnešní době je pro každou organizací nesmírně důležité chránit svá aktiva.

Je spousta metodických rámců, doporučení, zkušeností které popisují jak by se měla chránit aktiva. Ale otázkou je, do jaké míry jsou jednotlivé aspekty bezpečností informací důležité? Bude aplikován celý standard nebo jenom něco? Bude aplikován samostatně, nebo v kombinací s nějakým jiným standardem?

Cílem práce je podat přehled vzorových postupů, zaměřených na řízení IT rizik. V případové studii se pokusit zjistit skutečnou úroveň vnímaní problematiky informační bezpečností v podnikové praxi.

1. Řešení bezpečnosti IS/ICT

Aktiva (assets) představují jednotlivé prvky IS/ICT[1]. Aktivem může být všechno, co má pro organizaci hodnotu, která může být snížená působením hrozby. **Hodnota** je základní charakteristikou aktiva a je relevantní, v závislostí na úhlu pohledu hodnocení. **Zranitelnost** je další charakteristikou aktiva a vyjadřuje citlivost na působení hrozby. Mělo by se počítat s tím, že pro každé aktivum existuje **zranitelné místo**, které může být využito ke způsobení škod nebo ztrát. ([2], s. 331-332) Zranitelné místo je vždy jednou z vlastností IS/ICT. Takové zranitelné místo může být:

- ✓ **Fyzické**, kdy je prvek IS/ICT fyzicky umístěn v prostředí, ve kterém může snadno dojit k jeho poškození, zničení či ztrátě.
- ✓ **Přírodní**, kdy je prvek IS/ICT nemá schopnost se vyrovnat s některými objektivními faktory, jako je záplava, požár, blesk apod.
- ✓ **Technologické**, kdy je prvek IS/ICT svými konstrukčními charakteristikami neumožňuje zajistit například požadovaný plynulý provoz.
- ✓ **Fyzikální**, kdy je prvek IS/ICT pracuje na takových fyzikálních principech, které umožňuji jejich zneužití. Příkladem může být elektromagnetické vyzařování některých komponent, jako jsou monitory, kabeláž komunikační sítě apod.
- ✓ **Lidské**, kdy je prvek IS/ICT ohrožen působením lidí, jejich omylů a neznalostí.

Úroveň zranitelností aktiva se hodnotí podle jeho citlivostí – náchylností aktiva, tj. možností jeho poškození, a kritičností - důležitostí aktiva pro IS/ICT.

Zranitelné místo je pro systém **hrozbou** (threat), což je možnost využit zranitelné místo aktiva k útoku na toto aktivum. Útok se označuje termínem **bezpečnostní incident** (security incident), což je jakákoli událost, která vede k porušení definovaných pravidel a postupu při provozování IS/ICT, včetně pokusů o tato porušení. Zároveň je za bezpečnostní incident označována jakákoli událost, která vede k ohrožení nastavených bezpečnostních vlastností. ([2], s. 332-333)

Hrozby a zranitelná místa využívají tzv. útočnici k uskutečnění svého útoku. Pro označení osob, které realizuji úmyslné útoky, se používá několik termínu:

- ✓ **Hacker** – bere útok jako výzvu a prostředek získání prestiže.

[1] IS/ICT – Information Systém/Information and Communication Technology.

- ✓ **Vyzvědač** (spy) – provádí útoky za účelem zisku informaci, které jsou využívaný pro různé účely.
- ✓ **Terorista** (terrorist) – provádí útoky za účelem vyvolání obavy a strachu.
- ✓ **Vandal** – útočí na systémy s cílem systém zničit či poškodit.
- ✓ **Cracker**, zpravidla programátor – snaží se proniknout do systému jiných vlastníků za účelem jejich krádeže. Typický se orientuje na krádež duševního vlastnictví – těch částí systémů, které jsou chráněný autorským zákonem.
- ✓ **Phracker** – jeho cílem je získání bezplatného přístupu k telefonním službám.
- ✓ **Phreaker** – jeho cílem jsou telekomunikační informace, které mu umožňují získávat přístup k dalším počítačům.

Pravděpodobnost bezpečnostního incidentu zvyšují hrozby a zranitelná místa. Riziko je míra ohrožení aktiva, míra nebezpečí. Hodnota aktiva určuje úroveň rizika.

Protiopatření (countermeasure) snižuje úroveň rizika. Vybíráme taková protiopatření, u nichž náklady na ně vynaložené musí být přiměřené hodnotě chráněných aktiv, nebo hodnotě škod vniklých dopadem hrozby. **Referenční úroveň rizika** je úroveň pod kterou se riziko považuje za zbytkové, přijatelné pro systém, dopad hrozby je tak malý, že jej lze zanedbat. ([2], s. 333)

V rámci IS se definují **bezpečnostní požadavky**:

- ✓ Zachování **důvěrnosti** (confidentiality) – přístup k aktivům mají pouze autorizované subjekty, disponující oprávněním k provádění činnostní v IS/ICT.
- ✓ Zachování **dostupností** (availability) – autorizované subjekty mohou na své vyžádání vykonat činností a není jim odepřen k činnosti přístup.
- ✓ Zachování **integrity** – ke změně aktiva nemůže dojit neautorizovaným subjektem, nepovolenou činností, nekompletním provedením změn. ([2], s. 334)

Další vlastností ovlivňující bezpečnost:

- ✓ Zajištění **prokazatelností** (authentication) – lze vysledovat jakoukoli akci, která v systému proběhla s tím, že lze zjistit původce takové akce.
- ✓ Zajištění **nepopíratelností** (non-repudiation) – subjekt nemůže odmítnout svojí účast na provádění nějaké akce.
- ✓ Zachování **spolehlivostí** (reliability) – reálné chování systému je konzistentní s chováním systému, tak jak je dokumentováno.

Řešení bezpečností IS/ICT se opírá o de jure standardy (ISO řady 27000) a de facto standardy (ITIL - Infirmation Technology Infrastructure Library), ty formulují proces řešení bezpečností IS/ICT, a také obsah jednotlivých aktivit řešení. ([2], s. 334)

Bezpečnostní politikou (BP) se nazývá soubor zásad a pravidel pomoci kterých, organizace chrání svá aktiva, a definuje jaký stupeň zajištění bezpečnostních požadavků má být na konkrétní IS/ICT aplikován. Typy bezpečnostní politiky podle požadovaného stupně zabezpečení jsou:

- ✓ **Promiskuitní** BP, která ve svých pravidlech nikoho neomezuje a povoluje subjektům realizovat vše, včetně toho, co by neměli konat.
- ✓ **Liberální** BP je ve svých pravidlech umožňuje realizovat vše, až na výjimky, které jsou explicitně vyjmenované.
- ✓ **Opatrná** BP je ve svých pravidlech zakazuje vše s výjimkou toho, co je explicitně vyjmenováno.
- ✓ **Paranoidní** BP zakazuje dělat vše, co je potenciálně nebezpečné, tedy i to, co by nemuselo být explicitně zakázáno.

Další neméně důležitou aktivitou je **řízení rizik** (RM – Risk Management) což je proces identifikace, kontroly, eliminace nebo minimalizace bezpečnostních rizik. Cílem je identifikovat specifické oblastí, kde je potřeba zajistit ochranu proti ohrožení a zranitelností, určit jak velká ochrana je nutná, jak velká ochrana existuje a nejekonomičtější cestu, vedoucí k zajištění ochrany. ([2], s. 334-335)

V rámci RM se provádí:

- ✓ **Analýza rizik**, zahrnující definici rozsahu, specifikaci prostředí, identifikaci aktiv, identifikaci protiopatření, identifikaci zranitelnosti a ohrožení, analýzu zranitelností, stanovení rizik a dopadů.
- ✓ **Analýza přínosů a nákladů**, která zahrnuje porovnávání nákladů na protiopatření s odhadovanou výší ztráty, kdyby protiopatření nebyla realizována. Náklady obsahují: investiční náklady, náklady implementace, náklady provozu a údržby, další přímé i nepřímé náklady. ALE (Annual Loss Expectancy) je metoda, která je založena na pravděpodobnosti, že během jednoho roku nastane ohrožení násobeno velikosti ztráty (cenovým vyjádřením), jestliže ohrožení nastane. ([2], s. 334-335)
- ✓ **Výběr a implementace protiopatření** je volba vhodných protiopatření a jejich implementace, včetně sestavení jejich dokumentace.

- ✓ **Testování a hodnocení** je periodické testování a vyhodnocování účinností protiopatření.
- ✓ **Plánování výjimečných situaci** je sestavení plánu možných výjimečných situací a nouzových reakci nebo náhradního provozu, včetně plánování po havarijních činností.

1.1 Hrozby

Hrozba je náhodně nebo úmyslně vyvolána událost, která může mít negativní dopad na důvěrnost, integritu a dostupnost aktiv. Většina hrozeb (více jak 50% všech) patří do kategorie neúmyslných hrozeb. ([2], s. 337) Patří sem náhodné nebo úmyslné:

- ✓ Prozrazení tajných informaci – bezpečný systém nemůže povolit přístup nikomu, aniž by proběhla autentizace.
- ✓ Upravení – bezpečný systém musí zajistit, že nedojde k porušení integrity dat neautorizovaným, náhodným nebo úmyslným způsobem.
- ✓ Zničení – bezpečný systém nesmí dovolit neautorizované zničení IS nebo jeho zdrojů.
- ✓ Bránění v dostupností IS autorizovaným uživatelům – bezpečný systém nesmí odepřít přístup autorizovaným osobám.

Mezí typické útoky související s tím, že jsou v systémech využívaný komunikační prostředky patří: odposlech což je útok v síti směrovaný na zcizení informace, kterou může být číslo kreditní karty, číslo účtu zákazníka apod.; vyhledávání hesel pomocí „trojského koně“, útoků hrubou sílou apod.; modifikace dat což je útok, kdy dochází k modifikaci obsahu určitých transakci nebo změně uložené informaci; odmítnutí/Denial of Service (DoS) je útok, spočívající v tom, že napadený počítač může odmítat poskytovat řádné plnění služeb. ([2], s. 337-338)

1.2 Metodika COBIT

Metodika Cobit je sadou všeobecně přijímaných procesů, návodů pro hodnocení, ukazatelů a nejlepších praktických zkušeností. Hlavní cíl je maximalizace užitku, plynoucího z IT. Metodiku Cobit reprezentuje několik dokumentů, každý ze kterých je určen jiné profesi a úrovní řízení. ([1], s. 78-79) Příklady dokumentu jsou:

- ✓ Pro oblast řízení informační bezpečností: Cobit Security Baseline, Information Security Governance: Guide for Boards of Directors and Executive Management.
- ✓ Pro malé a střední podníky: Cobit Quickstart.
- ✓ Pro organizace spadající pod SOX: IT Cobit Objectives for Sarbanex-Oxley.
- ✓ Pro podporu řízení investic v oblastí IT: Val IT.
- ✓ Pro podporu řízení rizik v oblasti IT: Risk IT.

Principem metodiky Cobit je propojení třech různých aspektů řízení IT v organizacích. Jsou jimi:

- ✓ Cíle organizací ve formě požadavků na vlastností (kritéria) informací. Informační kritéria jsou: efektivnost, výkonnost, integrita, dostupnost, hodnověrnost, shoda.
- ✓ Zdroje IT jsou informace, struktura a lidé.
- ✓ Mapa procesů obsahující čtyři domény, kteří kopíruji životní cyklus řízení IT.

Filosofie metodiky Cobit říká, že business manažeři jsou odpovědni za plnění strategických cílů, které musejí mít vazbu na strategické cíle IT. Pro plnění strategických cílů je zapotřebí informace, na které jsou kladeny různé nároky, týkající se jejich kvality ve formě požadavků (kritérií) informací. Kvalita informací je ovlivněna IT procesy, které jsou uspořádané v uzavřeném životním cyklu (Plan and Organise, Acquire and Implement, Deliver and Support, Monitor and Evatuate). Při realizaci IT procesů jsou využívány IT zdroje: aplikace, informace, infrastruktura, lidé. ([1], s. 79)

Procesy jsou jednoznačně identifikovány zkratkou domény, do které patří a pořadovým číslem procesu v doméně. Procesy se skládají z aktivit. Proces je základní jednotkou Cobitu, protože k němu se vážou všechny informace, potřebné pro efektivní řízení a hodnocení oblasti IT. ([1], s. 80)

Cobit má RACI matici, která informuje manažery o tom, kdo a jakou formou se podílí na realizaci aktivit procesu. Vazba mezi aktivitami a rolemi je popsána čtyřmi formy:

- ✓ „R“ znamená responsible, tj. odpovědný.
- ✓ „A“ znamená accountable, tj. právně odpovědný.
- ✓ „C“ znamená consulted, tj. konzultuje aktivity.
- ✓ „I“ znamená informed, tj. informován o aktivitách.

Cobit rozlišuje 4 úrovně cílů a dva druhy metrik. Úrovně cílů jsou podnikatelské cíle, IT cíle, cíle IT procesů a cíle IT aktivit. ([1], s. 87) Druhy metrik jsou outcome measures, což jsou

výstupní metriky (KGI – Key Goal Indicators), pomáhají hodnotit míru splnění cíle na dané úrovni, a performance indicators, což jsou prováděcí metriky (KPI – Key Performance Indicators), pomáhají hodnotit průběh plnění cílů. Pozitivní vývoj ukazatelů průběhu plnění cílů je předpokladem pro pozitivní plnění výstupních metrik. Výstupní metrika cíle na nižší úrovni je prováděcí metrikou pro cíl nadřízený (tj. cíl procesu). ([1], s. 89)

Nehledě na to že Cobit patří do skupiny standardů „best practice“, neznamená to, že jsou vhodné pro každou organizaci. Proto tím standardem by se mělo inspirovat, a upravit jej tak, aby byl maximálně efektivní v konkrétním prostředí. Všechny procesy a jejích kontroly by se neměly zavádět najednou, je zapotřebí provést zúžení a určit priority jejích zavádění s ohledem na konkrétní podmínky a strategií v dané konkrétní organizací. ([1], s. 91)

1.3 Metodika Risk IT

Cíl Risk IT je definovat komplexní rámec pro řízení rizik, integrující různé úrovně řízení rizik a zároveň aplikovatelný pro oblast řízení rizik IT. Dokument byl zveřejněn v roce 2009 a společně s dokumenty Cobit a Val IT představují provázaný model kontrol, investic a rizika pro oblast řízení a poskytování služeb IT. ([1], s. 103)

Risk IT se skládá ze dvou částí:

- ✓ **The Risk IT Framework** což je rámec pro řízení rizik IT, který vysvětluje základní principy řízení rizik a procesní model.
- ✓ **The Risk IT Practitioner Guide** což je praktický návod pro řízení rizik IT, obsahující praktické návody pro tuto oblast.

Procesy jsou rozděleny do tří domén (číslo označuje počet procesů):

- ✓ RG – Risk Governance, což je správa a řízení rizika 3, zajišťuje, aby proces řízení rizik se stal každodenní součástí rozhodování.
- ✓ RE – Risk Evaluation, což je hodnocení rizik 3, zajišťuje, aby se rizika a příležitostí prezentovaly formou srozumitelnou business manažerům.
- ✓ RR – Risk Response, což je reakce na riziko 3, zajišťuje, aby IT rizika spojená s příležitostmi a událostmi se řídila efektivně a v souladu s prioritami podnikání.

Dokument The Risk IT Practitioner Guide se skládá z osmi kapitol a popisuje oblasti, jako kontext řízení rizik (Risk Universe), postup definování náchylností k riziku, způsob

jak popisovat riziko a vytvářet scénáře rizik, jak Cobit a Val IT mohou pomoci snižovat riziko. Návod také obsahuje seznam obecných scénářů rizik IT. ([1], s. 106)

2. Rodina norem ISO/IEC 27000

Tato mezinárodní norma poskytuje přehled systému řízení bezpečností informaci, které tvoří předmět rodiny norem ISMS[2].([10], s. 7)

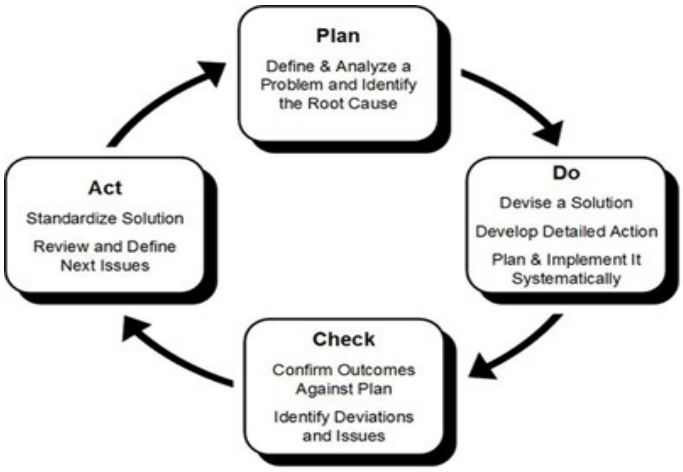
Rodina norem ISMS zahrnuje normy, které:

- ✓ Definuji požadavky na ISMS, a na ty kteří certifikuji takové systémy.
- ✓ Poskytuji přímou podporu, podrobné pokyny a/nebo interpretaci pro všechny procesy Plánuj-Dělej-Kontroluj-Jednej (Plan-Do-Check-Act (PDCA)) a požadavky.
- ✓ Zabývají se směrnicemi ISMS specifickými pro jednotlivá odvětví.
- ✓ Zabývají se posuzováním shody ve vztahu k ISMS.

Tenhle mezinárodní dokument popisuje rodinu norem ISMS včetně úvodu k systémům řízení bezpečností informací a je použitelná pro všechny druhy organizací. ([10], s. 9)

ISMS je systém řízení bezpečností informaci, poskytující model pro ustavení, implementování, zpracovávaní, monitorování, přezkoumávaní, udržování a zlepšování ochrany informačních aktiv, aby byly dosaženy cíle organizace zakládající se na posouzení rizik a úrovni akceptace rizik. K úspěšné implementaci ISMS přispěje analýza požadavku na ochranu informačních aktiv a aplikace kontrolních opatření. ([10], s. 14)

Pro efektivní fungování organizace je zapotřebí identifikovat a řídit činností, využívající zdroje. K tomu se používá tzv. procesní přístup, uvedený v rodině norem ISMS a založený na přístupu PDCA. ([10], s. 15) Na následujícím obrázku je znázorněn přístup PDCA.



Obrázek 1 PDCA. Zdroj: ([10], s. 15)

[2] ISMS – Information Security Management Systém.

Plánuj (Plan) znamená, že je zapotřebí stanovit cíle a vytvořit plány. **Dělej** (Do) znamená, že je zapotřebí stanovené plány implementovat. **Kontroluj** (Check) znamená, že dosažené výsledky by se měly změřit. **Jednej** (Act) znamená opravu a zdokonalování činností. ([10], s. 15)

Cíle, potřeby organizace, požadavky na bezpečnost, obchodní procesy, velikost organizace ovlivňují návrh a implementací ISMS.

ISMS umožňuje podporu e-businessu, je důležitý pro obchodní činností a nezbytný pro řízení rizik. Bezpečnost informaci při návrhu a vývoji informačních systému často podceňována a považována za technické řešení. Ale technické prostředky jsou omezené a můžou být neúčinné, pokud nejsou podporovány řízením a postupy v kontextu ISMS. Začlenit bezpečnost do vytvořeného IS je velice obtížné a nákladné. Identifikace zavedených kontrol a pečlivé plánování je nezbytné. Řízení přístupu by mělo zajišťovat autorizovaný[3] a omezený přístup k informačním aktivům. Výdaje na bezpečnostní kontrolní opatření by měly být přiměřené k předpokládanému obchodnímu dopadu výskytu (uskutečnění) rizika. ([10], s. 18)

[3] Autorizací se rozumí proces ověření přístupových oprávnění uživatele vstupující do informačního systému. Tento proces ve většině případů navazuje na proces autentizace. Autentizace slouží k jednoznačnému určení uživatele, který přistupuje k systému. Cílem autentizace je zajistit, že systém přesně ví, s jakým uživatelem komunikuje, kdo to je. Podstatou autorizace je ověřit, zda daný uživatel má oprávnění provést příslušnou akci, například vložení nového záznamu do seznamu dodavatelů apod.

3. ISO/IEC 27001

Tato norma umožňuje organizaci propojit nebo integrovat ISMS s odpovídajícími požadavky systému managementu. Hlavním cílem ISMS je zajištění odpovídajících a přiměřených bezpečnostních opatření, pro ochranu informačních aktiv. ([11], s. 7-8)

Pro monitorování a přezkoumání ISMS organizace musí provést následující:

- ✓ Monitorovat, přezkoumávat a zavést další opatření:
    1. Včasná detekce chyb zpracování.
    2. Včasná identifikace úspěšných i neúspěšných pokusů o narušení bezpečností a detekce bezpečnostních incidentů.
    3. Možnost vedení organizaci určit, jestli bezpečnostní aktivity prováděné pověřenými osobami, funguji podle očekávání.
    4. Detekce bezpečnostních událostí a zabránění vzniků bezpečnostních incidentu.
    5. Možnost vyhodnocení činností podniknutých při narušení bezpečností.
- ✓ Pravidelně přezkoumávat činnost ISMS (včetně splnění politiky ISMS, cílů a přezkoumání bezpečnostních opatření) s ohledem na výsledky bezpečnostních auditů, incidentů, výsledků měření účinností opatření, návrhu a podnětu všech zainteresovaných stran. ([11], s. 12)
- ✓ Měření účinností zavedených opatření a ověření toho, zda byly naplněny požadavky na bezpečnost.
- ✓ V plánovaných intervalech provádět přezkoumání hodnocení rizik a přezkoumávat zbytková rizika[4] a úroveň akceptovatelného rizika s ohledem na změny:
    1. Organizace.
    2. Technologii.
    3. Cílů činností organizace a procesů.
    4. Identifikovaných hrozeb.
    5. Účinností zavedených opatření.
    6. Regulatorního a právního prostředí, změny vyplívající ze smluvních závazků, změny sociálního klimatu.
- ✓ Provádět interní audity ISMS v plánovaných intervalech.

[4] Zbytkové riziko – riziko zbývající po uplatnění zvládaní rizik. Zvládaní rizik – proces výběru a přijímaní opatření ke změně rizika.

- ✓ Na úrovní vedení organizace pravidelně přezkoumávat ISMS aby se zajistilo, že jeho rozsah je i nadále odpovídající a že se daří nacházet možností zlepšení.
- ✓ Aktualizovat bezpečností plány s ohledem na závěry monitorování a přezkoumání.
- ✓ Zaznamenávat všechny činností a událostí, které by mohly mít dopad na účinnost nebo výkon ISMS. ([11], s. 12-13)

4. ISO/IEC 27002

Tato mezinárodní norma poskytuje doporučení a obecné principy pro vymezení, zavedení, udržování a zlepšování systému managementu bezpečností informací v organizací. ([12], s. 10)

Pro organizaci je důležité určit vlastní bezpečnostní požadavky. K tomu může použit zdroj hodnocení rizik, která organizaci hrozí, s ohledem na strategií a cíle organizace. Identifikují se hrozby, pravděpodobnost a potenciální dopad. Jako další zdroj organizace může použit požadavky zákonů, smluvní ujednání, místní zvyklostí. Třetím zdrojem jsou konkrétní principy, cíle a požadavky, týkající se zpracování informací. ([12], s. 10)

Z pohledů legislativy existují opatření, dodržení kterých je pro organizací důležité. Jde hlavně o ochranu osobních údajů, ochranu důležité dokumentace organizace a ochranu duševního vlastnictví. ([12], s. 11)

Také existují opatření, považována za „best pracices“, jsou to: dokumenty bezpečnostní politiky informací; přidělení odpovědností; bezchybné zpracování v aplikačních systémech; řízení kontinuity činností organizace; řízení technických zranitelností; zvládání bezpečnostních incidentů a kroky k nápravě. ([12], s. 11)

Úspěch implementací bezpečností informací v organizací závisí na kritických faktorech, jako jsou bezpečnostní cíle a činností, monitorování, udržování, podpora ze strany vedení organizace, risk management, realizace školení, zavedení procesů zvládání bezpečnostních incidentů, komplexní vyvážený systém pro ohodnocení míry účinností řízení bezpečností informací a získávání návrhu na zlepšení na základě zpětné vazby. ([12], s. 11-12)

Mohou být nezbytná i další opatření, která nejsou v normě uvedena.

4.1 Hodnocení bezpečnostních rizik

Při procesu hodnocení rizik by měla být identifikována a kvantifikována rizika a také určen jejích význam s ohledem na akceptační kritéria a cíle organizace. Doporučení a priority řízení konkrétních rizik včetně implementací opatření jsou výstupem procesu hodnocení rizik. Celý proces hodnocení rizik může být nutné opakovat pro různé částí organizace nebo jednotlivé informační systémy. ([12], s. 15)

Součástí hodnocení rizik by měla být analýza rizik [5]a vyhodnocení rizik[6]. Pro včasné zjištění změn v bezpečnostních požadavcích by mělo být prováděno hodnocení rizik v pravidelných intervalech a metodický tak, aby výsledky jednotlivých hodnocení byly srovnatelné a reprodukovatelné. ([12], s. 15)

Ještě než se rozhodne o způsobů zvládaní rizika, měla by být stanovená kritéria, pomocí kterých se určí, zda je riziko akceptovatelné. Důvodem k akceptací rizika můžou být neúnosné pro organizací náklady, spojené se zvládáním rizika. O takových rozhodnutích by se měly vytvářet záznamy. ([12], s. 16)

Po hodnocení rizik musí být učiněno rozhodnutí, jakým způsobem bude s identifikovanými riziky naloženo. Možné varianty jsou: aplikace vhodných opatření na snížení velikostí rizika; vědoma a objektivní akceptace rizika, za předpokladů, že je tak učiněno v souladů s politikou organizace a kritérií pro akceptaci rizika; vyhnutí se riziku zamezením činností, které jsou příčinou jeho vzniku; přenos rizika na jiný subjekt. ([12], s. 16)

Pokud bylo rozhodnuto o zvládání rizika pomoci aplikace vhodných opatření, měl by být výběr opatření proveden na základě požadavků identifikovaných v rámci hodnocení rizik. Opatření by měla zaručit snížení rizika na přijatelnou úroveň, s ohledem na: omezení národní a mezinárodní legislativy; cíle organizace; provozní požadavky a omezení; cenu za implementaci včetně provozních nákladu, spojených s přijetím opatření na snížení rizika. ([12], s. 16)

Ve fázi návrhu a specifikací požadavku projektů nového systému by měla být stanovená opatření, v opačném případě to způsobí zvýšení nákladů a neschopnost dosáhnout požadované úrovně bezpečností. ([12], s. 16)

4.2 Bezpečnostní politika

Vydání a aktualizace bezpečnostní politiky je způsobem, jakým vedení organizace podporuje oblast bezpečností informací. Dokument bezpečnostní politiky organizace schvaluje vedení organizace, po publikací je zpřístupněn zaměstnancům a relevantním externím stranám. ([12], s. 16)

[5] Analýza rizik je systematický přístup k odhadu velikostí rizika.
[6] Vyhodnocení rizik je proces porovnání odhadnutých rizik se stanovenými kritérií pro určení jejich důležitostí.

Dokument bezpečnostní politiky by měl obsahovat: ([12], s. 17)

- ✓ Definici bezpečnostní informací, její cíle, rozsah a význam.
- ✓ Prohlášení vedení organizace o záměru podporovat cíle a principy bezpečností informaci.
- ✓ Rámec pro stanovení cílů opatření a opatření včetně jednotného přístupu k hodnocení a řízení rizik.
- ✓ Stručný výklad bezpečnostních zásad (politik), principů, standardů a norem a požadavků na soulad, kterým organizace přikládá zvláštní význam, například:
    1. Dodržování regulatorních, zákonných a smluvních požadavků.
    2. Požadavky na vzdělávání, školení a zvyšování povědomí o bezpečností informací.
    3. Zásady plánování kontinuity činností organizace.
    4. Důsledky porušení bezpečnostních zásad.
- ✓ Stanovení obecných a konkrétních odpovědností pro oblast řízení bezpečností informací včetně hlášení bezpečnostních incidentů.
- ✓ Odkazy na dokumentací, která může bezpečnostní politiku podporovat, například na detailnější bezpečností politiky a postupy zaměřené na konkrétní informační systémy nebo bezpečnostní pravidla, která by měli uživatele dodržovat.

S dokumentem by měli být seznámení uživatele v rámci organizace, a to formou, která je relevantní, přístupná a pochopitelná. ([12], s. 17)

Když nastane změna a také v plánovaných intervalech by se měla bezpečnostní politika informací přezkoumávat. Bezpečnostní politika informací by měla mít vlastníka, kterého schválí vedení organizace, a který pak bude odpovědný za její vytvoření, přezkoumávání a aktualizaci. Nedílnou součástí procesů přezkoumání je posouzení možností zlepšení bezpečností informací. Pro přezkoumání bezpečnostní politiky informací by měly být zohledněný závěry z přezkoumání provedeného vedením organizace. Měl by být vytvořen postup a plán pravidelného přezkoumání vedení organizace. ([12], s. 17)

4.3 Řízení aktiv

Organizace by měla všechna svá aktiva jasně identifikovat, evidovat a udržovat jejích seznám aktuální. Také by měla stanovit relevantní hodnotu a důležitost aktiv. Evidence by měla obsahovat informace potřebné pro případ obnovy po havárií. Měl by být uveden typ aktiva, jeho formát, umístění, informace o záloze, licenční informace a hodnota aktiva pro organizací. Seznam by neměl duplikovat existující seznamy, v případě že se tak stane by měla být zajištěna shoda uváděných informací. ([12], s. 26)

Pro každé aktivum by měl být schválen a zaevidován jeho vlastník a jeho bezpečnostní klasifikace. Úroveň ochrany aktiva se určuje na důležitostí aktiva, jeho hodnoty pro organizací a bezpečnostní klasifikaci. Proces vytvoření seznamu aktiv je nezbytným předpokladem pro řízení rizik. ([12], s. 26)

Informace by měly být klasifikovány tak, aby byla naznačena jejich potřebnost, důležitost a stupeň ochrany. Informace mohou mít různý stupeň citlivostí a mohou být různě kritické, některé mohou vyžadovat vyšší úroveň bezpečností nebo zvláštní způsob zacházení. Měl by existovat systém bezpečnostní klasifikace, který by určoval adekvátní stupeň ochrany a který by dával uživatelům informace o nutností zvláštního zacházení. ([12], s. 28)

Jednou provedená klasifikace není neměnná a může se měnit pode určených pravidel. Vlastník informace zodpovídá za určení klasifikací aktiv a periodické přezkoumávání klasifikace. Počet klasifikačních kategorií by neměl být příliš rozsáhlý to je nepraktické a neekonomické. Úroveň ochrany informací se určuje na základě požadavků na důvěrnost, integritu, dostupnost. S časem informace přestávají být citlivé nebo kritické. S tím by se mělo počítat, protože reklasifikace může být velmi nákladná. Dokumenty se stejnými požadavky na bezpečnost by měly být klasifikovány jako celek. ([12], s. 28)

4.4 Fyzická bezpečnost a bezpečnost prostředí

Prostředky, zpracovávající kritické/citlivé informace, by měly být umístěný v zabezpečených zónách, chráněných vymezeným perimetrem s bezpečnostními barierami a vstupními kontrolami. Jde o fyzickou ochranu zařízení proti neautorizovanému přístupu, poškození a narušení. ([12], s. 34)

Pro zajištění odpovídající úrovně bezpečností by měl být jasně vymezen bezpečnostní perimetr s ohledem na aktiva uvnitř perimetru. Perimetr měl by být v řádném stavu, nesmí existovat snadno proniknutelná místa. Obvodové zdí objektu by měly mít pevnou konstrukci a vstupní dveře by měly být chráněny před neautorizovaným vstupem pomocí kontrolních mechanizmu (mříže, alarmy, zámky). Vstupovat do objektu by měli pouze oprávněné osoby, což zajistí vhodný systém vstupních kontrol. Je zapotřebí monitorovat požární dveře a nepřetržitě chránit opuštěné prostory. ([12], s. 34-35)

4.5 Zálohování informací

Aby obnova všech důležitých informací byla možná v případě katastrofy nebo selhání médií (nosičů dat) by mělo být zajištěno odpovídající zálohovací zařízení. Mělo by být stanoveno minimální nutné množství vytvářených záloh. Také by měly být vytvořeny přesné a úplné záznamy o záložních kopiích s popsanými postupy obnovy. Aby zálohy v případě havárie nebyly poškozeny nebo zničeny, měly být uloženy na bezpečném místě, v dostatečné vzdáleností od sídla organizace. Je nezbytné nutné pravidelně testovat záložní média, aby bylo zajištěno, že se na ně lze spolehnout. Obnovovací postupy museí být pravidelně testovány. Pro zajištění důvěrností zálohovaných informací, by mělo být použito šifrování. ([12], s. 46)

V případě kritických systému by zálohování mělo zahrnovat veškeré systémové informace včetně aplikaci a dat, potřebných pro obnovu systému v případě havárie. Zálohovací proces může být zautomatizován, ale je zapotřebí ho pravidelně testovat. ([12], s. 47)

4.6 Hlášení bezpečnostních událostí

Bezpečnostní událostí by měly být co nejrychleji hlášeny. Pro hlášení bezpečnostních událostí by měl být vytvořen formalizovány postup, definující činností, které by měly být po přijetí hlášení provedeny. K hlášení bezpečnostních incidentu slouží kontaktní místo, které musí být známo všem zaměstnancům a musí být vždy k dispozici. Je zapotřebí seznámit všechny zainteresované s povinností hlásit bezpečnostní incident co nejrychleji. ([12], s. 83)

Postup hlášení bezpečnostního incidentu zahrnuje: vytvoření procesu, který zajistí zpětnou vazbu, tak aby, ten kdo incident nahlásil, byl informován; formuláře pro podporu procesu hlášení bezpečnostní událostí; správné chování, což znamená, že v žádném případě zaměstnanec nesmí prověřovat bezpečnostní událost, ale okamžitě ji nahlásit; odkaz na disciplinární proces. ([12], s. 83)

Bezpečnostní událostí mohou být: ztráta služby, zařízení nebo vybavení; nesprávné fungování nebo přetížení systému; lidský faktor; nesoulad s politikami nebo směrnicemi; nedodržení opatření fyzické bezpečností; nekontrolované změny systému; porušení přístupu atd. ([12], s. 83)

4.7 Řízení kontinuity činností organizace

Cílem je bránit přerušení provozních činností a chránit kritické procesy organizace před následky závažných selhání informačních systému nebo katastrof a zajistit včasnou obnovu činností. ([12], s. 86)

V rámci analýza dopadů musejí být identifikovány důsledky pohrom, bezpečnostních chyb a ztráty dostupností služeb. Pro zajištění obnovy klíčových činností organizace ve stanovených lhůtách, je nutné připravit a implementovat plány kontinuity. Bezpečnost informací je nedílnou součástí procesů řízení kontinuity. Řízení kontinuity činností organizace zahrnuje opatření k identifikací a minimalizací rizik, čímž omezuje důsledky škodlivých incidentů a zajišťuje včasnou dostupnost informací, potřebných pro obnovení nezbytných činností. Rozvoj a údržba kontinuity činností organizace je řízený proces, který by měl existovat v rámci organizace. ([12], s. 86)

Proces rozvoje a údržby kontinuity činností organizace zahrnuje: pochopení rizik, kterým organizace čelí z hlediska pravděpodobností a dopadu; identifikaci všech aktiv; pochopení

dopadů a stanovení cílů pro prostředky zpracovávající informace; zvážení možností uzavření pojistky, tvořící součást procesů zajištění kontinuity činností a řízení rizik; identifikaci a implementaci dodatečných preventivních opatření; zajištění bezpečností zaměstnanců, ochrany majetku organizace a ochrany prostředku pro zpracování informací; formulaci a dokumentaci planu kontinuity činností, pokrývajících požadavky na bezpečnost; pravidelné testování a aktualizace plánů. ([12], s. 86-87)

Vedení organizace by mělo zajistit, aby řízení kontinuity činností organizace bylo součástí procesů a struktury organizace. Plány kontinuity činností organizace kvůli tomu, že pokrývají zjištěné zranitelností, tak mohou obsahovat citlivé informace, které musejí být chráněny. Kopie plánu musejí být ukládány na vzdálených místech (záložní lokalita), aby nedošlo ke zničení v případě havárie v hlavní lokalitě. Každý plán kontinuity musí jasně specifikovat podmínky své aktivace, včetně osob, odpovědných za vykonávání každého bodu plánu. ([12], s. 88)

Každý plán musí mít přiděleného vlastníka. Havarijní postupy, plány manuálního náhradního provozu a plány na znovuobnovení činností musejí být v odpovědností vlastníku daných prostředků nebo vlastníku procesů organizace. Prostředky pro zpracování a výměnu informací, jsou obvykle v odpovědností poskytovatelů servisních služeb. ([12], s. 88)

Systém plánování kontinuity činností organizace musí brát v úvahu: podmínky aktivace plánu; havarijní postupy; částí věnované vztahům s veřejností a efektivní spolupráci s policií, hasiči atd.; postupy obnovy, které popisují činností pro přesun důležitých aktivit na náhradní dočasné místo; dočasné provozní postupy až do doby obnovení činností; postupy, které popisují způsob opětovného uvedení organizace do normálního provozu; harmonogram údržby a testování plánu; individuální odpovědností; kritická aktiva a zdroje potřebné pro zajištění havarijních postupu. ([12], s. 88)

5. ISO/IEC 27005

Tato mezinárodní norma poskytuje doporučení pro řízení rizik bezpečností informací a podporuje obecný koncept specifikovaný v ISO/IEC 27001 a je strukturována tak, aby dostatečně podporovala implementací informační bezpečností založené na přístupu řízení rizik. Znalost modelu, konceptu, terminologie a procesů popsané v ISO/IEC 27001 a ISO/IEC 27002 je nezbytná pro pochopení normy. ([13], s. 7-8)

5.1 Stanovení kontextu

Kontext pro řízení rizik bezpečností informací, zahrnuje základní kritéria pro řízení rizik bezpečností informací, definuje rozsah včetně hranic, a stanoví organizační strukturu pro řízení rizik bezpečností informací. Určit účel řízení rizik bezpečností informací je tím nejdůležitějším, protože to ovlivňuje celý proces stanovení kontextu. Tím účelem mohou být: podpora ISMS, právní shoda, příprava plánu kontinuity činností organizace, příprava plánu reakce na incidenty, popis požadavků na bezpečnost informací. Výstupem mohou být specifikace základních kritérií, rozsahu, hranic a organizační struktury pro proces řízení rizik bezpečností informací. ([13], s. 12)

Přístup k řízení rizik řeší: kritéria vyhodnocení rizik, kritéria dopadu, kritéria akceptace rizik. Kritéria vyhodnocení rizik zohledňují: strategické hodnoty procesu informací o činnostech organizace; kritičnost informačních aktiv; legislativní a regulatorní požadavky; důležitost dostupností, důvěrností a integrity provozu; očekávaní a představy zainteresovaných stran. Kritéria vyhodnocení rizik se používají k určení priorit pro zvládaní rizik. ([13], s. 13)

Kritéria dopadu jsou specifikována na základě škod a ztrát, s ohledem na: úroveň klasifikace ovlivněného informačního aktiva; ztrátu důvěrností, dostupností a integrity; poškozené provozy; ztrátu činností organizace; finanční ztrátu; nedodržení konečných termínu. ([13], s. 13)

Organizace definuje své vlastní škály pro úrovně akceptace rizik s ohledem na to, že pro různé třídy rizik mohou platit různá kritéria akceptace rizik. Kritéria akceptace rizik se lišeji podle toho, jak dlouho se očekává, že riziko bude existovat, tj. jestli je spojeno s dočasnou nebo krátkodobou činností. Kritéria akceptace rizik by měla být stanovena

s ohledem na: obchodní kritéria, právní a regulační aspekty, provoz, technologie, finance, sociální faktory. ([13], s. 13-14)

Organizace musí stanovit rozsah a hranice pro řízení rizik bezpečností informace, aby při hodnocení rizik byla brána v úvahu všechna důležitá aktiva. Také by se měly identifikovat hranice k řešení rizik, která by mohla hranice prolomit. Informace důležité při definování rozsahu a hranic jsou: strategické obchodní cíle, obchodní procesy, funkce organizace, právní požadavky platné pro organizací, bezpečnostní politika organizace, celkový přístup organizace k řízení rizik, informační aktiva atd. Příkladem rozsahu řízení rizik může být aplikace, IT infrastruktura nebo obchodní proces. ([13], s. 14)

Vedení organizace musí stanovit a udržovat organizační strukturu a odpovědností pro proces řízení rizik bezpečností informací. Hlavní role a odpovědnosti jsou: rozvoj procesu řízení rizik bezpečností informací; identifikace a analýza zainteresovaných stran; definování rolí a odpovědností všech částí organizace; stanovení požadovaných vztahu mezi organizací a zainteresovanými stranami; stanovení eskalace rozhodnutí. ([13], s. 14)

5.2 Hodnocení rizik bezpečností informací

Vstupem mohou být základní kritéria, rozsah, hranice a organizační struktura. Rizika musejí být identifikována, kvantifikována nebo kvalitativně popsána. Hodnocení rizik zahrnuje analýzu rizik a vyhodnocení rizik. Hodnocení rizik se provádí ve dvou (nebo více) opakováních. Nejprve se provádí přehledové hodnocení, pro identifikaci potenciálně vysokých rizik. Další opakování zahrnuje důkladné zvážení dalších potenciálně vysokých rizik, odhalených v prvním hodnocení. Cílem identifikace rizik je určit, co může vyvolat ztrátu, jak, kde a proč k tomu může dojit. Pro identifikací hrozeb vstupem mohou být informace o hrozbách, získané z přezkoumání incidentů, od vlastníku aktiv, uživatelů, včetně katalogu vnějších hrozeb. Hrozby se identifikují podle typu (neoprávněné akce, fyzické zničení, technické poruchy) pak v případě potřeby, v rámci obecné třídy se identifikují jednotlivé hrozby. Což zajišťuje, že není žádná hrozba opomenutá, včetně těch neočekávaných. ([13], s. 15-16)

Identifikace stávajících opatření pomůže předejít zbytečným nákladům. Při identifikací stávajících opatření musí být provedena kontrola správné funkčností. V případě že opatření nefunguje tak, jak by fungovat mělo, může to způsobit zranitelnost. Účinnost opatření

se dá odhadnou pomocí údajů o tom, jak snižuje pravděpodobnost hrozby, usnadňuje zneužití zranitelností. ([13], s. 16)

Pro identifikací zranitelností vstupem mohou být seznam známých hrozeb, seznam aktiv a existující opatření. Musejí být identifikovány zranitelností, které jsou náchylné ke zneužití hrozbami, a může tak být způsobena škoda aktivum nebo organizací. Samotný výskyt zranitelností nepůsobí škodu, musí existovat hrozba, která ho využije. Zranitelnost, která nemá odpovídající hrozbu, nemusí vyžadovat přijetí opatření, ale musí být monitorována. Opatření, které se používá nesprávně, samo o sobě představuje zranitelnost. Účinnost opatření závisí na prostředí ve kterém funguje. Naopak, hrozba, která nemá odpovídající zranitelnost, nemusí vyústit v riziko. ([13], s. 17)

Pro identifikací následku vstupem mohou být seznam aktiv, seznam procesu, seznam hrozeb a zranitelností. Je nutné identifikovat následky, které mohou znamenat pro aktivum ztrátu důvěrností, integrity a dostupností. Nutností je určení následku incidentu a posouzení kritérií dopadu, definovaných během činností stanovení kontextu. Může být ovlivněno jedno nebo více aktiv nebo jen část aktiva. Aktiva musejí mít stanovené hodnoty podle svých finančních nákladů nebo podle velikostí následků. Následky mohou být dočasného charakteru nebo mohou být stálé. Organizace by měly identifikovat provozní následky scénářů z hlediska: vyšetřování a doby nápravy; ztráty času; ztráty příležitostí; zdraví a bezpečností; finančních nákladů. ([13], s. 17-18)

5.3 Metodika odhadování rizik

Stupeň podrobností analýzy rizik závisí na kritičností aktiv, rozsahu známe zranitelností a předcházejících incidentech. Metodika odhadu může být kvalitativní nebo kvantitativní nebo kombinací obou. Kvantitativní odhad se používá k získání obecné indikace úrovně rizika a k odhalení větších rizik. Pak je možné provést kvantitativní analýzu větších rizik, protože je méně složité a méně nákladné provést kvalitativní než kvantitativní analýzu. Kvalitativní odhad používá škálu kvalifikačních atributu k popisu velikostí možných následku a pravděpodobností. Výhoda kvalitativního hodnocení je jednoduchost pochopení, nevýhodou je závislost na subjektivním výběru škály. Tyto škály lze upravit tak, aby odpovídaly okolnostem, pro různá rizika lze použit různé popisy. Kvalitativní hodnocení může být

použito: jako počáteční prověřovací činnost k identifikací rizik; v případě, kde jsou číselné údaje nebo zdroje pro kvantitativní hodnocení nevhodné. ([13], s. 18)

Kvalitativní analýza používá skutečné informace a data z různých zdrojů, stupnicí s číselnými hodnotami (pro následky a pravděpodobnost). Kvalita analýzy je závislá na přesností a úplností číselných hodnot. Kvantitativní hodnocení ve většině případu používá historická data incidentů a má přímou souvislost s cíli bezpečností informací a zájmy organizace. Hlavní nevýhodou je nedostatek dat u nových rizik, a kdy nejsou k dispozicí konkrétní, kontrolovatelná data. ([13], s. 18)

5.4 Určení pravděpodobností incidentu

Vstupem mohou být: seznám identifikovaných scénářů incidentu, identifikace hrozeb, ovlivněna aktiva, zranitelností a dopady na aktiva, seznam všech existujících a plánovaných opatření. Po identifikací scénářů incidentu by se mělo za použití technik kvalitativního nebo kvantitativního hodnocení určit pravděpodobnost scénáře a výskytu dopadu. Musí se zohlednit, jak často se hrozby vyskytují a jak snadno lze využit zranitelností. ([13], s. 19)

Určovat pravděpodobnost by se mělo s ohledem na: zkušeností a statistické údaje o pravděpodobností hrozeb; v případě úmyslných hrozeb by se měly zohlednit motivace a schopností, měnicí se v čase; v případě náhodných hrozeb by se měly zohlednit geografické faktory (těsná blízkost chemických nebo naftových závodů, možnost extrémních atmosférických podmínek, lidská selhání, funkční poruchy zařízení). ([13], s. 19)

5.5 Zvládání rizik bezpečností informací

Vstupem je seznam rizik. Čtyři možnosti pro zvládání rizik jsou: redukce rizik, podstoupení rizik, vyhnutí se riziku, přenos rizik. ([13], s. 20)

Při redukcí rizik musejí se vybrat vhodná a odůvodněna opatření. Opatření typ ochrany jako jsou: náprava, vyloučení, prevence, minimalizace dopadu, odstrašování, odhalení, obnovení, monitorování, povědomí. Návratnost investic je důležitá, pokud jde o redukcí rizik a potenciál využívat nové obchodní příležitostí. Při výběru/zavádění opatření by měla být brána v úvahu

omezení: časová, finanční, technická, provozní, etická, kulturní, právní a ekologická. ([13], s. 21-23)

5.6 Metody hodnocení technických zranitelností

K identifikování zranitelností závisejících na kritičností informačních a komunikačních technologií (ICT) lze použit aktivnější metody, jako je testování IS. Každá testovací metoda zahrnuje: automatizovaný nástroj pro scénování zranitelností, testování a vyhodnocení stavu bezpečností, penetrační testování, analýzu zdrojových kódů. ([13], s. 43)

Automatizovaný nástroj pro scénování zranitelností se používá ke skenování skupiny serveru nebo sítě pro známé zranitelné služby, ale je nutné mít na paměti to, že některé potenciální zranitelností, které identifikuje automatizovaný nástroj, nepředstavují v kontextu prostředí systému skutečné zranitelností. Tahle metoda může produkovat falešné pozitivní výsledky. ([13], s. 43)

Testování a vyhodnocení stavu bezpečností obsahuje sestavení a provedení plánu testů (například scénář testu, postup testů, očekáváné výsledky testů). Účelem testování bezpečností systému je testováni účinností bezpečnostních opatření pro ICT, jak byla implementována v provozním prostředí. Cílem je zajistit, aby zavedená opatření splňovala schválenou bezpečnostní specifikací pro SW a HW. ([13], s. 43)

Penetrační testování se používá pro doplnění přezkoumání bezpečnostních opatření a zajištění různých aspektu ICT. V procesu hodnocení rizik lze použit penetrační testování k hodnocení odolností systému vůči úmyslným pokusům obejít ochranu systému. Hlavním cílem je testovat ICT z hlediska zdroje hrozeb a identifikovat potenciální selhání v ochranných schématech systému. ([13], s. 44)

Analýza zdrojových kódů je nejdůkladnějším a nejnákladnějším způsobem hodnocení zranitelností. Metody zahrnují činností jako jsou: rozhovory s lidmi a uživateli, dotazníky, fyzická kontrola, analýza dokumentace. ([13], s. 44)

5.7 Přístupy k hodnocení rizik bezpečností informací

Přehledové hodnocení umožňuje definovat priority a časový sled činností. Pokud to rozpočet nedovoluje, není možné přijmout všechna opatření současně, a proto během procesu zvládání rizik je možné pouze zvládnout nejvíce kritická rizika. Je předčasné zahájit detailní řízení rizik, pokud se o jeho zavedení rok nebo dva stále jen mluví. Dá se přehledové hodnocení zahájit nedetailním hodnocením následků. Další důvod k zahájení přehledového hodnocení je synchronizace s ostatními plány, které se vztahují k řízení změn/kontinuity činností organizace. Je nerozumné kompletně zabezpečovat systém, v případě že je v blízké budoucností plánován outsourcing, ale má smysl provést hodnocení rizik za účelem vymezení outsourcingové smlouvy. ([13], s. 45)

Přehledové hodnocení rizik určuje globální pohled na organizaci, informační systémy, bere v úvahu aspekty technologie. Analýza se soustřeďuje na obchodní a provozní prostředí. Přehledové hodnocení rizik určuje omezený seznam hrozeb a zranitelností, seskupených v definovaných doménách, soustřeďuje se na riziko. Přehledové hodnocení rizik, je vhodnější pro poskytování organizačních a netechnických opatření. ([13], s. 45)

Dosáhnout akceptace programu hodnocení rizik pomůže zahrnutí jednoduchého počátečního přístupu. Jako dobrá pomůcka plánování může posloužit sestavení strategického obrazu organizační struktury pro bezpečnost informací. Systémy, které potřebují ochranu nejvíce, by měly být řešeny prioritně. ([13], s. 45)

Přehledové hodnocení rizik zohledňuje obchodní hodnoty informačních aktiv a rizika z obchodního hlediska organizace. Při rozhodování, zdá je pro zvládání rizik přehledové hodnocení adekvátní, se dají použit různé faktory, které mohou zahrnovat například: cíle organizace, úroveň investic do každého informačního aktiva, informační aktiva. Po zhodnocení těchto faktoru, stává se rozhodnutí snadnějším. ([13], s. 45)

Obecným pravidlem je: pokud nedostatek informační bezpečností může vyústit ve významné nepříznivé následky pro organizací, její obchodní procesy nebo její aktiva, pak je zapotřebí pro identifikací potenciálních rizik provést druhé opakování hodnocení rizik ve více detailní úrovní. ([13], s. 46)

5.8 Detailní hodnocení rizik bezpečností informací

Proces detailního hodnocení rizik bezpečností informací zahrnuje: podrobnou identifikaci a hodnocení aktiv, hodnocení hrozeb pro tato aktiva, hodnocení zranitelností. Jejichž výsledky jsou pak použity k hodnocení rizik a k identifikací zvládání rizik. Detailní hodnocení je nejvhodnější pro informační systémy, na která působí vysoká rizika, protože vyžaduje značnou dobu, úsilí a kvalifikaci. Hodnocení celkových rizik je poslední fázi detailního hodnocení rizik bezpečností informací. ([13], s. 46)

Pro hodnocení pravděpodobností výskytu hrozeb musí být stanoven časový rámec, ve kterém bude mít aktivum hodnotu nebo potřebuje být chráněno. Pravděpodobnost výskytu konkrétní hrozby je ovlivněna: aktivitou aktiva, možným relevantním dopadem, technickými schopnostmi činitele hrozby, náchylností zranitelností ke zneužití. ([13], s. 46)

Je důležité, aby organizace používala metodu, která je pro organizaci vhodná, které organizace důvěřuje a která poskytne opakovatelné výsledky. ([13], s. 46)

5.9 Příklady technik založených na tabulkách

V metodách hodnocení rizik tohoto typu jsou aktuální nebo plánována fyzická aktiva hodnocena ve vztahu k nákladům na jejích výměnu nebo obnovu (Kvantitativní metrika). Náklady se převedou na kvalitativní stupnici jako u informaci. Aktuální nebo plánována softwarová aktiva se hodnotí stejně jako fyzická aktiva, pomoci identifikovaných nákladů na nákup, převedených na stejnou kvalitativní škálu, jako u informaci. ([13], s. 46)

Hodnota informace se zjišťuje pomoci rozhovoru s vlastníky dat, kteří mohou o těchto datech odpovědně hovořit, a tak stanovit hodnotu a citlivost informací ve vztahu ke scénářům nejhoršího případu. Při hodnocení se využívají tzv. vodítka pro hodnocení informací, pokrývající: osobní bezpečí, právní a regulatorní povinností, vymáhání práva, komerční a ekonomické zájmy, finanční ztrátu/narušení činností, veřejný pořádek, obchodní politiku a činností, ztrátu důvěryhodností, smlouvu se zákazníkem. ([13], s. 46)

Vodítka usnadňují identifikací hodnot v číselné škále (příklad viz. stupnici od 0 do 4 uvedenou v matici níže), čímž umožňují určení kvantitativních hodnot tam, kde to je možné a logické, a kvalitativních hodnot tam, kde kvantitativní hodnoty není možné použit. ([13], s. 47)

Pak je nutné vyplnit několik dotazníků pro každý typ hrozby, pro každé seskupení aktiv, které s typem hrozby souvisí. Každá odpověď na otázku získává skore. Body jsou pak sečteny podle vědomostní databáze a porovnány se škálou intervalů. Informace pro vyplnění dotazníku se shromažďuji z rozhovorů s pracovníky z technické, personální a provozní oblastí, fyzických kontrol prostorů atd. ([13], s. 47)

Hodnota aktiv, úrovně hrozeb, zranitelností, které odpovídají každému typů následků jsou proti sobě postaveny v matici, aby bylo možné pro každou kombinaci identifikovat míru rizika na stupnici od 0 do 8. Hodnoty jsou v matici uvedeny strukturovaně. ([13], s. 47)

	Úroveň hrozby	Nízká			Střední			Vysoká		
	Úroveň zranitelností	N	S	V	N	S	V	N	S	V
Hodnota aktiva	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Tabulka 1 Matice 1. Zdroj: ([13], s. 47)

Pro každé aktivum jsou zvažovány zranitelností a relevantní hrozby. V případě že existuje zranitelnost bez odpovídající hrozby nebo hrozba bez relevantní zranitelností, pak žádné riziko nehrozí, avšak je nutné monitorovat situace. Příslušný řádek v matici je identifikován hodnotou aktiva a příslušný sloupec je identifikován pravděpodobností výskytu hrozby a snadností zneužití. Budeme předpokládat že aktivum má hodnotu 3, je hrozba „vysoká“ a zranitelnost „nízká“, míra rizika je 5. Hodnota tohoto přístupu tkví v seřazení rizik, která se mají řešit. ([13], s. 47)

Matice, uvedena níže, vyplývá z úvah o pravděpodobností scénáře incidentu namapovaného proti odhadovanému dopadu. Pravděpodobnost scénáře incidentu závisí na hrozbě, která využívá zranitelnost s určitou pravděpodobností. Tabulka propojuje pravděpodobnost s dopadem, který se vztahuje ke scénáři incidentu. Výsledné riziko se měří na stupnici od 0 do 8 a lze ho vyhodnotit podle kritérií akceptace rizika. ([13], s. 47)

Tato stupnice rizik by mohla být také převedena do jednoduché škály rizik, jako například:

- ✓ Nízké riziko: 0 – 2
- ✓ Střední riziko: 3 - 5
- ✓ Vysoké riziko: 6 – 8

	Pravděpodobnost scénáře incidentu	Velmi nízká	Nízká	Střední	Vysoká	Velmi vysoká
Dopad	Velmi nízká	0	1	2	3	4
	Nízká	1	2	3	4	5
	Střední	2	3	4	5	6
	Vysoká	3	4	5	6	7
	Velmi vysoká	4	5	6	7	8

Tabulka 2 Matice 2. Zdroj: ([13], s. 47)

Tabulku, která je uvedena níže, se dá použit pro uvedení do vzájemného vztahu faktorů následků (hodnota aktiva) a pravděpodobností výskytu hrozeb. Prvním krokem je vyhodnocení následků (hodnota aktiva) na předem definované škále, například 1 až 5, každého ohroženého aktiva (sloupec „b“ v tabulce). V dalším kroku se vyhodnotí pravděpodobností výskytu hrozby, na předem definované škále, například 1 až 5, každé hrozby (sloupec „c“ v tabulce). Ve třetím kroku se vypočtou míry rizika násobením (b x c). Nakonec hrozby budou seřazeny v pořadí podle jim přiřazené míry rizika. U tohoto příkladu 1 označuje nejnižší následky a nejnižší pravděpodobnost výskytu. ([13], s. 47)

Popis hrozby (a)	Hodnota následku (aktiv) (b)	Pravděpodobnost výskytu hrozby (c)	Míra rizika (d)	Seřazení hrozeb (e)
Hrozba A	5	2	10	2
Hrozba B	2	4	8	3
Hrozba C	3	5	15	1
Hrozba D	1	3	3	5
Hrozba E	4	1	4	4
Hrozba F	2	4	8	3

Tabulka 3 Třídění hrozeb pomocí míry rizika. Zdroj: ([13], s. 48)

To je postup, umožňující srovnávat hrozby s pravděpodobností výskytu, pak je seřadit podle priority. V některých případech bude zapotřebí spojit peněžní hodnoty s empirickými stupnicemi. ([13], s. 48)

V dalším příkladu bude kladen důraz na následky incidentů bezpečností informací a na určení priority systému. Tohle se provádí stanovením dvou hodnot pro každé aktivum a riziko, co v kombinací určuje skore pro každé aktivum. Míra rizika systému se určí po sečtení všech skore aktiv. Nejprve se ke každému aktivu přiřadí hodnota, která se vztahuje na potenciální nepříznivé následky, k nimž může dojit, v případě že aktivum bude ohrožen. Hodnota aktiva je přiřazena k aktivu za každou hrozbu aplikovatelnou pro toto aktivum. Pak je stanovena

hodnota pravděpodobnosti, kterou určuje kombinace pravděpodobnosti výskytu hrozby a snadnost zneužití zranitelnosti. ([13], s. 48)

Úroveň hrozby	Nízká			Střední			Vysoká		
Úroveň zranitelností	N	S	V	N	S	V	N	S	V
Hodnota pravděpodobností	0	1	2	1	2	3	2	3	4

Tabulka 4 Stanovení hodnoty pravděpodobností a možných následků rizik. Zdroj: ([13], s. 48)

Následně se přiřadí skore aktivum/hrozba nalezením průsečíku hodnoty aktiva a hodnoty pravděpodobnosti v tabulce níže. Pak se jednotlivá skore aktivum/hrozba sčítají, aby dala celkové skore aktiva. Výsledkem sečtení všech celkových skore aktiv systému je skore systému. ([13], s. 48)

Hodnota aktiva	0	1	2	3	4
	hodnota			pravděpodobností	
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

Tabulka 5 Hodnota Pravděpodobností. Zdroj: ([13], s. 49)

6. Nejznámější analytické metody a metodiky

Metoda **ETA** (Event Tree Analysis) je v překladu z angličtiny Analýza stromu událostí, což je kauzální analytická technika, která se používá pro vyhodnocení průběhu procesu a událostí, vedoucích k možné nehodě. Metoda ETA byla vyvinuta na žádost jaderného průmyslu po havárii v elektrárně Three Mile Island. Princip metody ETA je podobný jako u metody FTA ale liší se tím, že se sledují události vedoucí k poruše, a ne pouze selhání jako je to v případě FTA. Uplatňuje se zejména v oblasti řízení rizik a řízení kvality, či řízení bezpečnosti.[5]

Metoda ETA byla založená na rozboru sekvence činností a událostí v procesu, vedoucích k nehodě, kterou zobrazuje pomocí grafického logického modelu. Metoda ETA zvažuje odezvy bezpečnostního systému a operátorů. Scénář nehod je výsledkem analýzy ETA. V praxi metoda ETA pomáhá systematický popsat série činností bezpečnostního systému a může být požita pro analýzu jakýchkoliv složitých systémů. Používá se pro identifikaci a analýzu systémových slabých míst. Výsledkem jsou doporučení pro snížení pravděpodobnosti nehody a snížení jejich následků. [5]

Metoda **FTA** (Fault Tree Analzsis) byla založená na rozboru vrcholové události nebo problému (například havárie, poruchy, nekvality, vysokých nákladů), systematicky identifikuje faktory, které problém způsobují nebo negativně ovlivňují funkčnost systému. Cíl FTA je detailní analýza, tj. nalezení příčin negativního jevu a snížení pravděpodobností jeho výskytu. Pro jednoduché systémy je vhodnější použít metody FMEA nebo HAZOP. FTA byla poprvé použita v roce 1962 firmou Bell Telephone Laboratories a následně zdokonalená firmou Boeing. Metoda se uplatňuje všude, kde je třeba řešit složité systémy a snižovat poruchovost nebo zvyšovat kvalitu, obzvlášť v odvětvích jako jsou energetika, vesmírný výzkum, letectví, jaderná energetika. [5]

Metoda **FMEA** (Failure Mode and Effect Analysis) je v překladu z angličtiny Analýza možných vad a jejich následků. FMEA je analytická technika, cíl které, je identifikovat místa možného vzniku vad nebo poruch v systémech. Byla vyvinuta v 60-tých letech minulého století v USA v rámci vesmírného programu APOLLO společnosti NASA, jako nástroj pro hledání závažných rizik. V 80-tých letech byla metoda FMEA zpracována do jednotné příručky a následně zahrnuta do normy QS 9000[7]. Během posledních 20-ti let se FMEA

[7] QS9000 je oborová norma automobilového průmyslu. Byla vypracovaná skupinou Chrysler/Ford/General Motors a obsahuje jednak plné znění normy ISO 9001 plus další požadavky zejména z oblasti zavádění nových výrobků, schvalování výrobků zákazníkem, uplatňování vybraných metod, způsobilosti procesů a neustálého

postupně vyvíjela a rozšiřovala, vznikly metody VDA, DRBFM, FMECA aj. které mají základ v této metodě. Vzhledem ke své univerzálnosti se uplatňuje v oblastech jako: řízení rizik, kvality, bezpečnosti. [6]

Podstata metody FMEA tkví v systematické identifikací možných vad výrobku nebo procesu, včetně jejich důsledků, identifikaci kroků omezení příčin těchto vad, včetně dokumentaci celého procesu. Metoda FMEA se nejčastěji používá ve výrobě protože je preventivní metodou, umožňující včasnou identifikaci možných poruch, chyb nebo vad, které mohou ovlivnit funkce systému, výslednou kvalitu, bezpečnost. Metoda vyžaduje zkušený tým, protože správná identifikace možných vad a jejich následků je založena na zkušenostech, doporučuje se složení týmu z více lidí tak, aby se jejich znalosti a zkušenosti vzájemně vykrývaly. [6]

HAZOP (Hazard and Operability Study) je analýza ohrožení a provozuschopnosti, to je jeden z nejjednodušších a nejrozšířenějších přístupů k identifikaci rizik. Metoda HAZOP se zakládá na hodnocení pravděpodobnosti ohrožení a rizik. Její hlavní cíl je identifikace scénářů potencionálního rizika - umožňuje identifikovat nebezpečné stavy, které se mohou na zkoumaném zařízení vyskytnout. Metoda hledá kritická místa a vyhodnocuje potenciální rizika a nebezpečné stavy. To je týmová expertní multioborová metoda, kdy členové týmu hledají scénáře na společném jednání s využitím brainstormingu. Výsledky jsou formulovány v závěrečném doporučení, směřujícím ke zlepšení procesu nebo systému. [7]

Kroky metody HAZOP:

- ✓ Identifikace příčin
- ✓ Odhad možných následků a rizik
- ✓ Návrhy opatření eliminace rizik
- ✓ Ocenění

Metoda byla vyvinuta společností ICI (divizí ICI Petrochemical) pro systematickou podrobnou analýzu bezpečnosti složitého technologického zařízení. Nejčastěji se používá v chemickém průmyslu. HAZOP je velmi flexibilní metodou, která se používá pro velké technologické celky, ale může být použita i pro malá zařízení, je vhodná pro velké i malé organizace. [7]

---

zlepšování. Požadavkům této normy musí vyhovět v různém stupni každý dodavatel do automobilového průmyslu.

Six Sigma je komplexní metoda řízení, označována jako filosofie, kterou musí organizace přijmout, zaměřuje se na neustálé průběžné zlepšování pomocí porozumění potřeb zákazníků, analýzy procesů a standardizace metod měření. To je komplexní pružný systém řízení, založeny na porozumění potřeb a očekávání zákazníků, disciplinovaném používání informací a dat k řízení a rozhodování. V Six Sigma jsou inovace založeny na cyklu zlepšování DMAIC, který zaměřeně vyhledává slabá místa (bottleneck), odstraňuje je. DMAIC je jedním ze stavebních kamenů Six Sigma. [8]

Cíle a charakteristika Six Sigma:

- ✓ Maximalizace zisku
- ✓ Efektivní využívání zdrojů a zvyšování produktivity
- ✓ Redukce podpůrných procesů
- ✓ Minimalizace negativních jevů - defektů, neshod, ztrát, reklamací a nákladů

Spojením Six Sigma a zásad štíhlého přístupu Lean vzniká Lean Sigma. Lean Management je velmi široká metoda řízení, založena na základních principech:

- ✓ Snaha celé organizace se trvale zlepšovat ve všech oblastech a zamezit zbytečnému plýtvání.
- ✓ Co nejlepší uspokojení potřeb zákazníka bez ohledu na to, jakým způsobem.

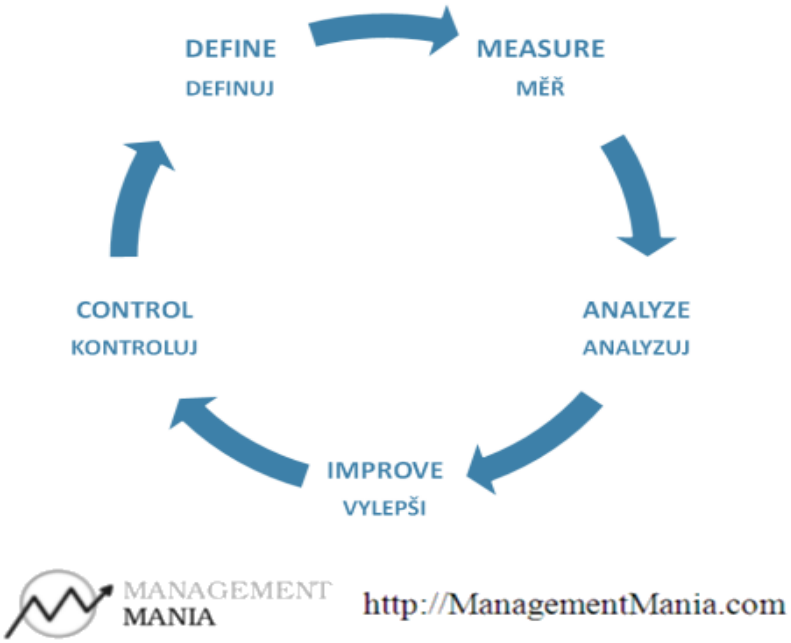
Lean se často používá s různými přívlastky, podle toho na jakou oblast je tato filosofie uplatněna.

DMAIC je cyklus zlepšování a metoda postupného zlepšování, která je integrální součástí metody SixSigma. Lze použit jakékoliv zlepšování, například kvality výrobků, služeb, procesů, aplikací, dat. Jednotlivé fáze celého cyklu pomáhají docílit skutečného zlepšení. To je zdokonalený PDCA cyklus. [9]

Fáze cyklu zlepšení jsou:

- ✓ D (Define) definovat – definují se cíle, popisuje se předmět a cíle zlepšení (výrobek, služba, proces, data, atd.)
- ✓ M (Measure) měřit – měření výchozích podmínek ve smyslu principu “co neměřím, neřídím”
- ✓ A (Analyze) analyzovat – analýza zjištěných skutečností, příčin nedostatků

- ✓ I (Improve) zlepšovat – klíčová fáze celého cyklu, ve které dochází ke zlepšení na základě analyzovaných a změřených skutečností
- ✓ C (Control) řídit – zlepšený nedostatek je třeba zavést - uřídit, udržet zlepšení při životě



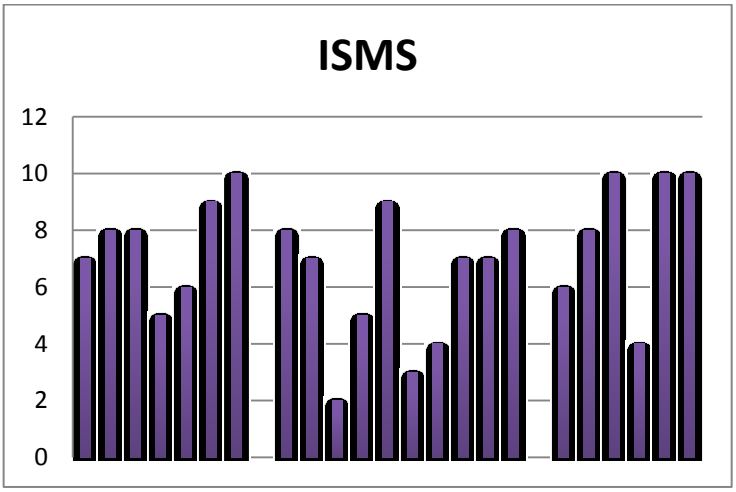
Obrázek 2 DMAIC.

7. Případová Studie

Cílem případové studie bylo zjistit na jaké úrovní jsou jednotlivé aspekty bezpečností v různých podnicích ze subjektivního pohledu představitelů exekutivity. Mým úkolem bylo kontaktovat představitele oddělení IT, pokusit se je vyzvat k tematickému zamýšlení nad úrovní ISMS v jejich konkrétním podniku. Nejdřív jsem se snažila je kontaktovat prostřednictvím e-mailů, ve kterých jsem se reprezentovala jako studentka, která pod vedením společností ANECT a.s. sbírá data pro svou BP. Výsledek byl takový, že nikdo nereagoval. Z mého pohledů možnými příčiny neúspěchu jsou: podezíravost, hodnocení mého e-mailu jako spamu. Po prvním neúspěchu jsem se je snažila kontaktovat telefonický, což skončilo stejným neúspěchem. Z mé zkušeností vyplývá závěr že člověka se statusem „student“ vedeni organizací nebere vážně.

Po mém neúspěchu jsem obdržela data z minulých tematických zamýšlení, kterými se zabývala společnost ANECT a.s., z důvodu ochrany citlivých informací názvy společností nebudou uvedeny.

Průzkumu se zúčastnilo 41 společností, vyhodnocovaly se oblastí důležité pro řízení bezpečností informaci po škále důležitostí od 1 (min) do 10 (max). Na grafech, uvedených níže, škála důležitostí bude označená na svislé ose, společností, které se zúčastnily průzkumu, budou označeny na vodorovné ose. Následující graf znázorňuje úroveň ISMS a její důležitost z pohledu představitelů exekutivity v jednotlivých společnostech. Pouhých 9,7% společností ohodnotilo ISMS na škále důležitostí 10 body. 14,6% společností nemá systém řízení bezpečností informací, tj. přiřadilo ISMS 0 bodů.

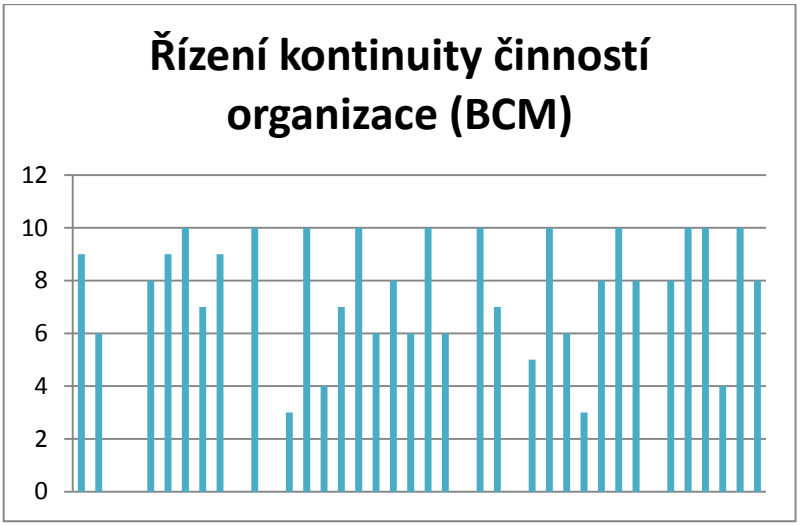


Obrázek 3 Úroveň ISMS. Zdroj: autorka.

Co se týká bezpečností politiky organizace, tak 34% společností ji označily na škále důležitostí 10 body. Bezpečnostní politiku nemá 7,3% společností. Což je znázorněno na obrázku 4.

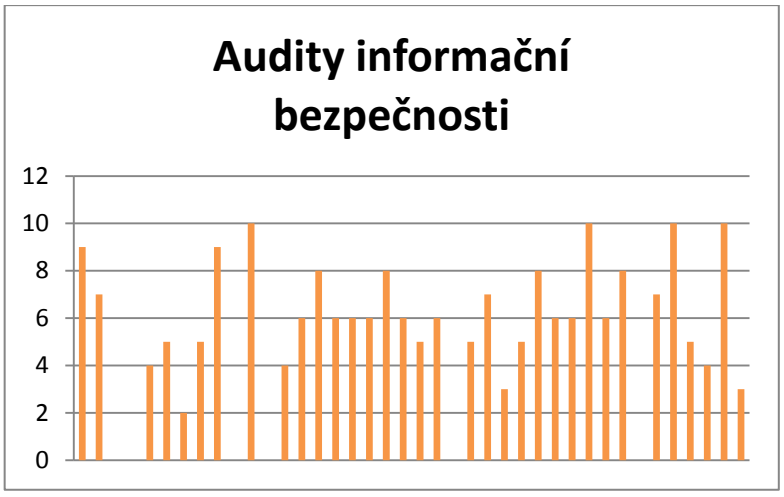
Obrázek 4 Bezpečnostní politika organizace. Zdroj: autorka.

Řízení kontinuity činností na škále důležitostí označilo 10 body 26,8% společností, což je znázorněno na obrázku 5. 19,5% společností ohodnotilo řízení kontinuity činností 0 body.



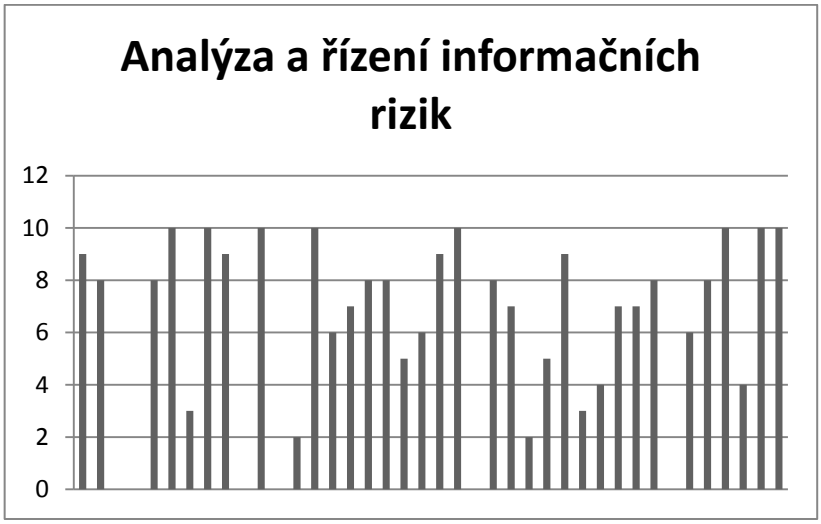
Obrázek 5 Řízení kontinuity činností organizace. Zdroj: autorka.

Auditu informační bezpečností přiřadilo 10 bodů na škále důležitostí 9,7% společností. Což znázorňuje obrázek 6. 14,4% společností neprovádí audity informační bezpečností.



Obrázek 6 Audity informační bezpečností. Zdroj: autorka.

Analýzu a řízení informačních rizik na škále důležitostí označilo 10 body 19,5% společností a 0 body jí označilo 14,6% společností.



Obrázek 7 Analýza a řízení informačních rizik. Zdroj: autorka.

Z výsledku dotazování vyplývá závěr, že praxe se hodně liší od teorie, protože teoretický by každá organizace měla provádět audity, řídit kontinuitu činností organizace, mít bezpečnostní politiku. Že úroveň aplikace ISMS, řízení kontinuity činností, bezpečnostní politiky a auditu je závislá na subjektivním hodnocení důležitostí jednotlivých oblastí vedoucím oddělení IT, CIO, CSO.

CSO[8] by vždy měl přemýšlet nad tím „a co když…?“, měl by vždy mít plán B, měl by vědět co je pro bezpečnost informací v jeho konkrétní společnostní je nezbytné, a do čeho je škoda

[8] CSO – Chief Security Officer.

investovat peníze. Jestli je lepší všechno řešit za použití interních zdrojů nebo outsourcingu. A v případě outsourcingu pečlivě zvážit míru přístupu k citlivým informacím.

Pro společnost je velice důležité mít odborníka v oblastí řízení bezpečností informací, a tým ve kterém budou pracovat jenom ti nejlepší a nespolehlivější lidí. Nikdy se nespokojit s tím že zrovna teď je všechno perfektní, mít na pamětí že situace se může kdykoli zhoršit, a že se taky zhorší.

Závěr

V bakalářské práci jsem se soustředila na řízení IT rizik. Začala jsem teoretickou částí o řešení bezpečností IS/ICT, kde jsem definovala pojem „hrozba“ a podrobně popsala metodické rámce COBIT a Risk IT.

Pak jsem popsala rodinu norem ISO/IEC 27xxx, které jsou klíčové, pro řízení bezpečností. Ve druhé kapitole jsem popsala normu ISO/IEC 27000 která se zabývá ISMS. Ve třetí kapitole jsem věnovala pozornost monitorování a přezkoumání ISMS, což podrobně popisuje norma ISO/IEC 27001. Dále jsem se zaměřila na soubor postupů pro management bezpečnosti informaci (ISO/IEC 27002), který obsahuje hodnocení bezpečnostních rizik, bezpečnostní politiku, řízení aktiv, zálohování informací, hlášení bezpečnostních událostí a řízení kontinuity činností. V páté kapitole jsem se věnovala řízení rizik bezpečností informací (ISO/IEC 27005), konkrétně stanovení kontextu, hodnocení rizik, určení pravděpodobností incidentu, zvládání rizik. Pak jsem uvedla příklady technik založených na tabulkách, které jsem převzala z přílohy normy ISO/IEC 27005.

Šestá kapitola je o nejznámějších analytických metodách, jako jsou metody ETA, FTA, FMEA, HAZOP, Six Sigma. Také jsem popsala cyklus DMAIC, který je integrální součástí metody Six Sigma.

Obsahem sedmé kapitoly je případová studie, ve které je zkoumána úroveň jednotlivých aspektu bezpečností v různých podnicích ze subjektivního pohledu představitelů exekutivity. Věnovala jsem pozornost zejména úrovní zavedení ISMS, bezpečnostní politice organizace, řízení kontinuity činností, auditu informační bezpečností, analýze a řízení informačních rizik. Z materiálů, poskytnutých firmou ANECT a.s. jsem zjistila skutečnou úroveň vnímaní bezpečností jednotlivými firmy, které se zúčastnily průzkumu.

Použitá literatura.

[1] V.SVATÁ, *Audit Informačního systému*. 1 vydání. Praha: Professional Publishing, a.s., 2011, ISBN 978-80-7431-034-8.

[2] L.GÁLA, J.POUR, Z.ŠEDIVÁ, *Podniková informatika*. 2 vydání. Praha: Grada Publishing, a.s., 2009, ISBN 978-80-247-2615-1.

[3] ISACA. Cobit. *Isaca.org* [Online]. [cit. 2012-10-20]. Dostupné z: http://www.isaca.org/COBIT/Pages/default.aspx

[4] ISACA. RiskIT. *Isaca.org* [Online]. [cit.2012-10-20]. Dostupné z: http://www.isaca.org/Knowledge-Center/Risk-IT-IT-Risk-Management/Pages/Risk-IT1.aspx

[5] MANAGEMENTMANIA. ETA. *Managementmania.com* [Online]. [cit.2013-04-02]. Dostupné z: https://managementmania.com/cs/eta-event-tree-analysis-analyza-stromu-udalosti

[6] MANAGEMENTMANIA. FMEA. *Managementmania.com* [Online]. [cit.2013-04-02]. Dostupné z: https://managementmania.com/cs/failure-mode-and-effect-analysis

[7] MANAGEMENTMANIA. HAZOP. *Managementmania.com* [Online]. [cit.2013-04-02]. Dostupné z: https://managementmania.com/cs/hazop-hazard-and-operability-study-analyza-ohrozeni-a-provozuschopnosti

[8] MANAGEMENTMANIA. SIX SIGMA. *Managementmania.com* [Online]. [cit.2013-04-02]. Dostupné z: https://managementmania.com/cs/six-sigma

[9] MANAGEMENTMANIA. DMAIC. *Managementmania.com* [Online]. [cit.2013-04-02]. Dostupné z: https://managementmania.com/cs/cyklus-zlepsovani

[10] ČSN ISO/IEC 27000 – *Informační technologie – bezpečnostní techniky – Systémy řízení bezpečností informací – Přehled a slovník.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

[11] ČSN ISO/IEC 27001 - *Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

[12] ČSN ISO/IEC 27002 - *Informační technologie – Bezpečnostní techniky – Soubor postupů pro management bezpečnosti informací.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

[13] ČSN ISO/IEC 27005 - *Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

Seznam obrázků.

Seznam tabulek.