ZÁPADOČESKÁ UNIVERZITA V PLZNI
FAKULTA ELEKTROTECHNICKÁ

KATEDRA TECHNOLOGIÍ A MĚŘENÍ

DIPLOMOVÁ PRÁCE

SYSTÉM PRO ŘÍZENÍ RIZIK BEZPEČNOSTI INFORMACÍ

vedoucí: **Doc. Ing. František Steiner, Ph. D.**
autor: **Bc. Miroslav Ipser** **2013/2014**

ZÁPADOČESKÁ UNIVERZITA V PLZNI
Fakulta elektrotechnická
Akademický rok: **2012/2013**

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Miroslav IPSER**
Osobní číslo:	**E11N0017P**
Studijní program:	**N2612 Elektrotechnika a informatika**
Studijní obor:	**Komerční elektrotechnika**
Název tématu:	**Systém pro řízení rizik bezpečnosti informací**
Zadávající katedra:	**Katedra technologií a měření**

Zásady pro vypracování:

1. Seznamte se s problematikou systémů řízení bezpečnosti informací (ISMS) a řízení rizik.
2. Proveďte analýzu požadavků na systém řízení rizik.
3. Navrhněte řešení nástroje pro řízení rizik a hodnocení efektivnosti ISMS.
4. Navržené řešení realizujte.

Rozsah grafických prací: **podle doporučení vedoucího**

Rozsah pracovní zprávy: **30 - 40 stran**

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

Seznam odborné literatury:

1. **ČSN ISO/IEC 27001 Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky**
2. **ČSN ISO/IEC 17799 Informační technologie - Bezpečnostní techniky - Soubor postupů pro management bezpečnosti informací**
3. **ČSN ISO/IEC 27005 Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací**
4. **Berka a spol., Bezpečná počítačová síť**
5. **Internet**

Vedoucí diplomové práce: **Doc. Ing. František Steiner, Ph.D.**
Katedra technologií a měření

Datum zadání diplomové práce: **15. října 2012**

Termín odevzdání diplomové práce: **9. května 2013**

Doc. Ing. Jiří Hammerbauer, Ph.D.
děkan

L.S.

Doc. Ing. Vlastimil Skočil, CSc.
vedoucí katedry

V Plzni dne 15. října 2012

Anotace

Předkládaná diplomová práce je věnována problematice systémů řízení bezpečnosti informací (ISMS) a systému řízení rizik. Úvodní část práce je zaměřena na charakteristiku systémů řízení bezpečnosti informací a popisu jejich základních atributů, následně je komplexně popsán proces řízení rizik. Následně je věnována pozornost požadavkům kladených na systém řízení rizik. V závěru práce je navržen a realizován nástroj pro řízení rizik a měření efektivnosti se záměrem názorné prezentace průběhu procesu řízení rizik a možnosti měření efektivnosti.

Klíčová slova

Systémy řízení bezpečnosti informací, ISMS, řízení rizik, /IEC 27001,ISO/IEC 27005, ČSN ISO/IEC 17799

Abstract

The master thesis is focused on the issue of information security management system (ISMS) and risk management system. The first part is focused on the characteristics of information security management system and also describes their basic attributes. Then there iscomprehensively described the risk management process. Subsequently, attention is paid to the requirements imposed on the risk management system. In conclusion is designed and realized a tool for risk management and measurement of the effectiveness with the intention visual presentation during the risk management process and the possibility of effectiveness measuring.

.
.
.
.
.
.
.
.

Key words

Information security management system, ISMS, risk management, /ISOIEC 27001,ISO/IEC 27005, ČSN ISO/IEC 17799

Prohlášení

Předkládám tímto k posouzení a obhajobě diplomovou práci zpracovanou na závěr studia na Fakultě elektrotechnické Západočeské univerzity v Plzni.

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně, s použitím odborné literatury a pramenů uvedených v seznamu, který je součástí této diplomové práce.

Dále prohlašuji, že veškerý software, použitý při řešení této diplomové práce, je legální.

V Plzni dne 12.5.2014 Jméno příjmení

……..

Poděkování

Tímto bych rád poděkoval vedoucímu diplomové práce Doc. Ing. Františkovi Steinerovi, Ph.D. za cenné profesionální rady, neustálé usměrňování k cíli, připomínky a metodické vedení práce.

Dále bych rád poděkoval svým rodičům, kteří mi byli oporou po celou dobu mého studia.

Obsah

Úvod

Systémy řízení bezpečnosti informací nabývají důsledkem globalizace a vývoje podnikání stále vetší hodnoty. Při respektováni skutečnosti, že moderní podnikání je závislé na informačních technologiích, je nutné si uvědomit, že nepřeberné množství informací je neustále vystavováno působícím hrozbám a daná informace může být znehodnocena, zneužita, či ztracena

Tyto informace, současně nabývají právě vlivem vývoje podnikání a společnosti na své hodnotě. Informace začínají být pro organizace stejně tak cenné jako kapitál, know-how, vybavení, či zaměstnanci. A pokud si společnosti střeží a chrání své zaměstnance, vybavení, know-how a kapitál, je na místě věnovat dostatečnou pozornost také ochraně informací**.** **I**nformace, která má náležité atributy, tedy důvěrnost, integritu a dostupnost a která je využita ve vhodný moment, může totiž společnosti umožnit velký náskok před konkurencí, vyhnout se špatnému rozhodnutí, či uzavření kontraktu a dosažení zisku. Z pohledu informační bezpečnosti jsou informace chráněny bez ohledu na to, zda jsou uloženy v informačním systému, vytištěny na papíře nebo existují pouze v něčí mysli.

Pokrokově uvažující organizace si plně uvědomují nutnost ochrany informací a zvládnutí strategie řízení rizik.

Receptem pro zvládnutí strategie řízení rizik je pro organizaci implementace systémů řízení bezpečnosti informací. Akceptováním všech požadavků uvedených v normě ČSN ISO/IEC 27001 může organizace dosáhnout plné kontroly nad riziky a minimalizovat možnost ztráty kvality informace na minimální hodnotu. Zavádění systémů řízení bezpečnosti je stejně tak jako proces řízení rizik nikdy nekončící proces, který vyžaduje čas a plnou podporu vedení organizace, ale pokud organizace vše zvládne, odměnou jí bude efektivní ochranný systém.

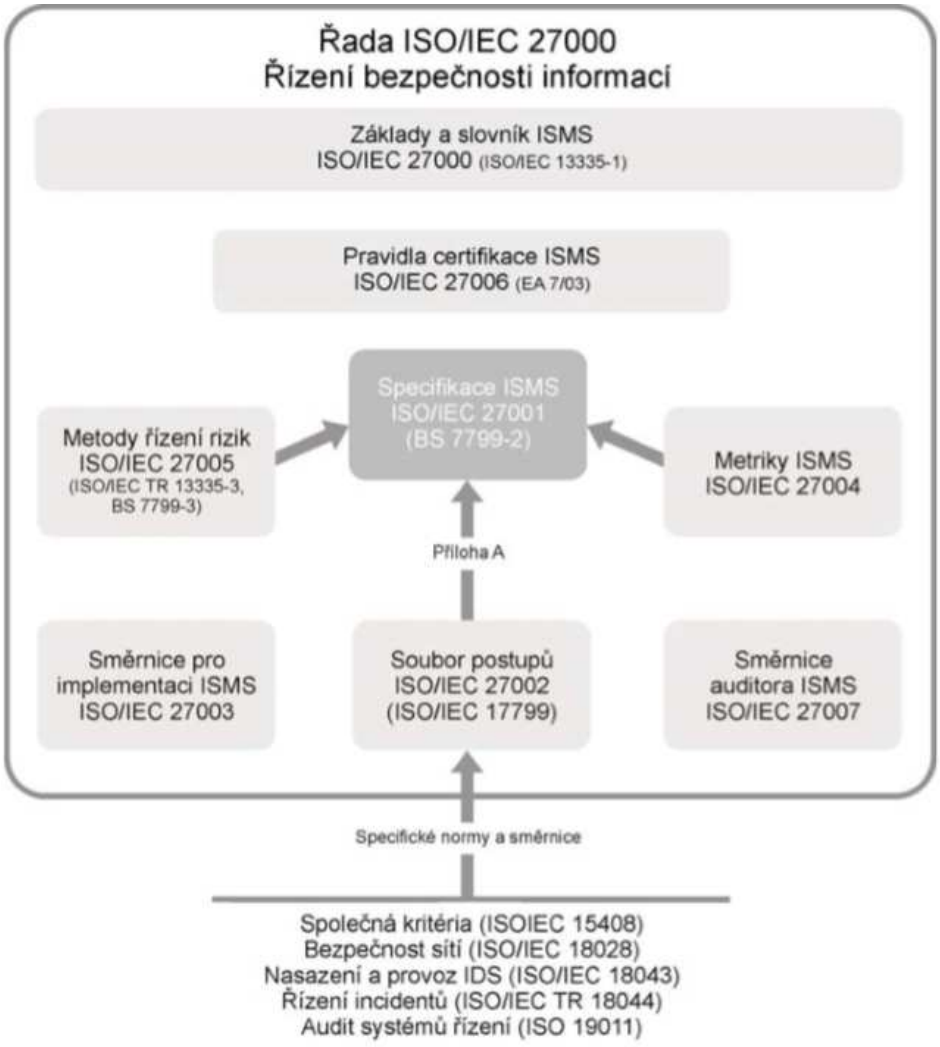
Tato práce je zaměřena na charakterizování systémů bezpečnosti informací a řízení rizik. Jsou zde konzultovány základní stavební pilíře a procesy. Pro efektivnější prezentaci systému je navržen nástroj pro řízení rizik a měření efektivnosti.

Seznam symbolů

zkratka	český název	anglický název
ISMS	Systém řízení bezpečnosti informací	Information Security Management System
IEC	Mezinárodní elektrotechnická komise	International Electrotechnical Commission
ISO	Mezinárodní organizace pro normalizaci	International Organization for Standartization

1 Charakteristika norem

Počátkem roku 2005 organizace ISO (International Organization for Standardization) oznámila uvedení nové řady norem ISO/IEC 27000, které se budou věnovat problematice řízení bezpečnosti informací. Zdrojem pro tvorbu těchto norem byly normy BS 7799 (British Standards). Nosný pilíř, který umožnuje implementovat všechny požadavky v těchto normách je Demingovo kolo (PDCA cyklus) viz obrázek č. 4. Základní hierarchie rodiny těchto norem je zobrazena na obrázku č. 1. Tato kapitola bude věnována základnímu popisu a výčtu norem ze skupiny ISO/IEC (za účelem tohoto výčtu norem a stručné charakteristiky jejich obsahu je zkonstruována tabulka č. 1., uložená v příloze) a podrobnější charakteristice norem ISO/IEC 27001 a ISO/IEC 27005.



Obrázek 1 Koncept řady ISO/IEC 27000 pro řízení bezpečnosti informací [1]

1.1 Norma ČSN ISO/IEC 27001 [2]

(Vlastní název: Informační technologie- Bezpečnostní techniky- Systému managementu bezpečnosti informací- Požadavky)

Tato norma je náhradou za normu ČSN BS 7799-2 (36 9790) z prosince 2004 a vznikla na základě spolupráce ISO (Mezinárodní organizace pro normalizaci) a IEC (Mezinárodní elektrotechnická komise).

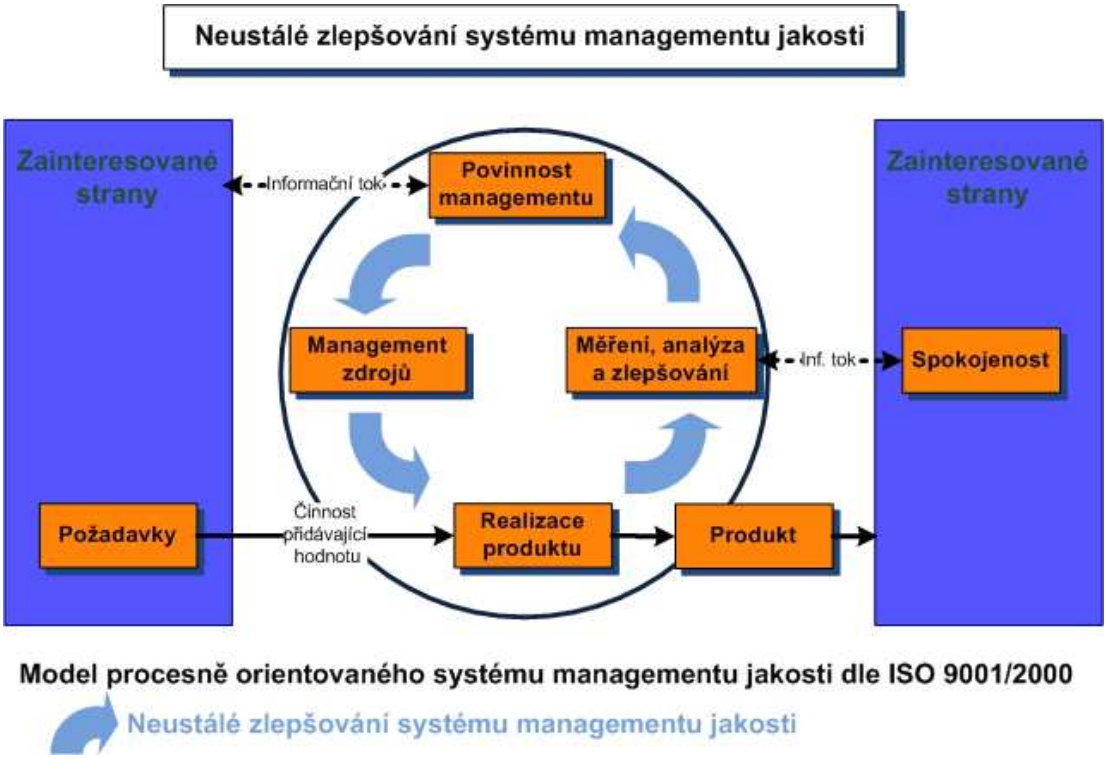
Účel, za kterým byla tato mezinárodní norma sestavena je poskytnout podniku návod a být mu jakousi příručkou a rádcem při ustanovení, zavádění, provozování, monitorování udržování a zlepšování systému ISMS. Obsahuje specifické požadavky pro všechny tyto kroky. Vyloučením některých požadavků v ní uvedené je nepřijatelné. Tedy pokud chce organizace uspět v implementaci ISMS a chce dosáhnout souladu s touto normou, například projít auditem a získat certifikaci.

1.1.1 Přínosy certifikace dle ČSN ISO/IEC 27001 [3]

- Zabezpečení informací
- Organizace je konkurenceschopná
- Spolehlivost systému podporují systémy zálohování
- Odpovědnost je přenesena na zaměstnance
- Je zaručeno kontinuální zlepšování v efektivnosti řízení nákladů
- Je zajištěna péče o kvalitu informací
- Nárůst podnikatelské důvěryhodnosti pro potencionální investory
- Eliminace nákladů za sankce a pokuty, dodržování právních požadavků
- Vybudování firemní kultury
- Motivace zaměstnanců
- Včasné rozpoznání incidentů
- Více záruk o plnění právních a jiných požadavků

Je použitelná a aplikovatelná pro všechny typy organizací (komerční organizaci, vládní agentury a úřady, neziskové organizace) bez ohledu na jejich velikost a povahu činností. Je aplikovatelná na organizace s procesním řízením. Respektive je postavena na faktu, že organizace, která se rozhodla implementovat ISMS a to v jakémkoliv oddělení a rozsahu upustila od funkčního řízení a přešla na procesní řízení.

Norma je plně kompatibilní s dalšími systémy managementu. Jednou z nich je norma ISO 9001:2008 (Quality management system- Systém managementu kvality). Tato norma popisuje požadavky na systém managementu jakosti a podle této normy probíhají také certifikace systému jakosti (systém jakosti je zobrazen na obrázku č. 2) primárním přínosem této normy je procesní přístup.



Obrázek 2 Model systému jakosti dle ISO 9001/2000 [4]

Další normou je ISO 14001:200 (Environmental management systems). Tato norma specifikuje požadavky na systém environmentálního managementu. Umožnuje organizaci vyvinout a zavést politiku a cíle, za účelem řízení rizik (z hlediska životního prostředí) v závislosti na činnostech této organizace. Tato norma je tedy určena pro organizace, které jsou si vědomi své odpovědnosti vůči životnímu prostředí a které chtějí podporovat ochranu životního prostředí a prevenci znečištění. [5]

- Dalšími normami jsou normy ze skupiny ISO/IEC 27000, které jsou pro názornost uvedeny v tabulce číslo 1.

Toto propojení je nastaveno za účelem jednotné implementace a provozu. Tedy, že jeden vhodně navržený systém řízení může splnit požadavky všech těchto výše uvedených norem.

Nástrojem využívaným pro implementaci a aplikaci všech procesů ISMS v této normě je model PDCA. Tento model umožní plné pochopení požadavků na bezpečnost, které jsou chápány jako vstupy do procesu a pomocí nezbytných procesů a činností vytvoří tížené výstupy, které splňují požadavky bezpečnosti a vyhovují představám ustanovených na vstupu. Modelu PDCA je věnována kapitola 2.1, kde je tento model detailně charakterizován.

1.2 Norma ČSN ISO/IEC 27005 (6)

Tato norma nahrazuje normu ČSN ISO/IEC 27005 z července 2009. Norma je strukturována do několika částí a obsahuje ucelený náhled, ve kterém je prezentován přístup k řízení rizik bezpečnosti informací. Forma jejího zpracování je utvořena s přihlédnutím a respektováním požadavků řízení bezpečnosti informací (ISMS), které jsou uvedeny v normě ČSN ISO/IEC 27001. Je tedy flexibilní, jako norma ČSN ISO/IEC 27001 ve vztahu možnosti implementace do rozličných druhů podniků (komerční společnosti, vládní organizace, organizace neziskové), či pouze do jejich jednotlivých oddělení dané organizace (marketingové, finanční), služeb (vztah se zákazníky, či pouze konkrétních fyzických míst (serverovna, archiv) a zároveň s výše uvedenou normou tvoří ucelený systém a nikterak se navzájem neomezují, či nevylučují.

V úvodu je nutno podotknout, že metodiky řízení rizik uvedené v této normě mají pouze ilustrativní charakter a slouží pro nabytí podvědomí o možnostech přístupu k řízení rizik bezpečnosti informací. Norma neposkytuje detailně přesnou příručku, kterou musí všechny organizace do posledního detailu a kroku dodržovat, pokud chtějí úspěšně implementovat tuto součást ISMS. Jinak řečeno, norma poskytuje pouze určitá doporučení a upozornění, jak postupovat a jaké skutečnosti při jednotlivých krocích, či etapách implementace nepřehlížet. (tento fakt je zapříčiněn možností implementace ISMS v široké škále organizací různého typu, jejich rozdílnými strategiemi, vizemi, cíli, dále rozsahem implementace, atd)

V následujících kapitolách jsou konzultovány a prezentovány jednotlivé kroky procesu řízení rizik bezpečnosti informací, které jsou v této normě uvedeny.

2 Systémy řízení bezpečnosti informací

2.1 Charakteristika ISMS

Se současným prudkým rozvojem informačních technologií, které urychlují pokrok a usnadňují práci dílčím uživatelům IS, je spojena i oblast počítačové kriminality, která vykazuje stejný dynamický rozvoj. Pokud se rozvíjí tato oblast je adekvátní a pochopitelná potřeba rozvíjení i oblasti ochrany. Podle statistik dochází k nejvíce útokům na informační systém zevnitř společnosti, kdy dochází ke zneužívání vlastních přístupových prvá ze stran samotných zaměstnanců a to vědomého či nevědomého.

Systém řízení bezpečnosti informací (Information Security Management System - ISMS) je dokumentovaný systém orientovaný na ochranu informačních aktiv. ISMS může být zaveden pro předem určené oddělení společnosti, nebo pro konkrétní informační systém, popřípadě jeho část, či může zcela zahrnovat celou organizaci. Je implementován za účelem, aby byla společnost schopna neustále vyhodnocovat rizika a uplatňovat náležité kontrolní a řídící mechanismy k zachování důvěrnosti, integrity a dostupnosti informací. Záměrem je chránit informační aktiva společnosti, čili nedopustit, aby se informace dostaly do nesprávných rukou, či aby nedošlo k jejich ztrátě. Je mnohem jednodušší případné ohrožení, nebo slabinu odstranit (zredukovat), než následně likvidovat následky škod.

Zavedení systému ISMS je strategickým rozhodnutím vedení organizace, a pro zdařilý a úspěšný průběh zavádění systému řízení bezpečnosti informací je nevyhnutelná spolupráce všech zainteresovaných složek organizace.

Systém je hojně využíván všemi typy podniků bez ohledu na jejich velikost či podnikatelské zaměření (podniky vyrábějící, podniky poskytující služby). Pro tyto podniky jsou informace klíčovou součástí nejen jejich klíčových řídících podnikových procesů, ale i běžných procesů. Či se jedná o podniky, které spravují citlivá data svých klientů a dbají na komplexní zajištění jejich bezpečnosti.

Identifikací a klasifikací aktiv a vyhodnocováním jejich ohrožení a zranitelnosti si může každá organizace vybrat způsoby řízení takovýchto rizik, aby byla zachována důvěrnost, integrita a dostupnost informací. Jedná se o informace příslušných

zainteresovaných stran jako např. informace vlastní klientely, odběratelů, dodavatelů, ale i akcionářů, úředních orgánů, ap..

Dále je možné na základě ISMS získat certifikáty kvality bezpečnosti IS například ISO/IEC 27001 a další podobné, které následně reflektují spolehlivost a důvěryhodnost organizace.

Obrázek 3 Oblasti bezpečnosti informací [7]

Jelikož implementace ISMS je aplikovatelná pouze na procesní přístup, je v této práci pro názornost uvedena kapitola kde je komparativní porovnání funkčního a procesního přístupu.

2.1.1 Funkční přístup vs. procesní přístup

Nutnost přechodu z funkčního řízení na procesní řízení je podnícena vysokou rychlostí vývoje technologií a vývojem tržního prostředí, kterému vévodí přání zákazníka. Došlo tedy k snížení významu vlastní výroby a došlo k navýšení významu činností, podporujících výrobu

(např. logistika, prodej, styk se zákazníkem). Na tento typ činností je kladen velký důraz a velké množství požadavků, jelikož tyto činnosti mají v současných podmínkách silné konkurence nemalý význam. Těmto požadavkům je nutno přizpůsobit uzpůsobit činnosti uvnitř organizace a přetransformovat jejich strukturu. Tradiční hierarchická (útvarová) struktura, kterou prosazuje funkční řízení, se prezentovala jako málo pružná a neefektivní a proto velké množství organizací přešlo na procesní řízení. Definovaly své vnitřní procesy a jim přizpůsobily jejich vnitřní strukturu. Přechod na procesní řízení taktéž umožní organizaci zavádět dílčí systémy a využívání progresivních metod řízení.[8]

Funkční řízení

Funkční řízení bylo tedy předchůdcem procesního řízení. Toto funkční řízení bylo využíváno téměř 200 let. Důsledkem tohoto faktoru, lze tento přístup klasifikovat jako jedno z nejhojněji využívaných manažerských řízení v historii. Jeho otcem byl Adam Smith. Principem a jedinou výhodou, kterou funkční řízení mělo, byla dekompozice výrobních procesů, které byly složité a vysoce sofistikované na jednoduché úkony, které nevyžadovaly kvalifikovaného pracovníka. Ovšem docházelo taktéž ke špatně dokumentovanému chování a nedostatečně popsaným postupům, komunikačním bariérám, nespecifikování zodpovědností a celkový přístup byl tedy vysoce nepružný. Důsledkem těchto faktů klesla efektivnost tohoto přístupu pod únosnou hranici. Bylo tedy nahrazeno procesním řízením.[9]

Procesní řízení

Procesní řízení bylo rozvíjeno ve třech etapách, ve kterých docházelo k utváření samostatných manuálů popisujících výrobní procesy, process managementu a reengineeringu. Tento nový směr vychází ze skutečnosti, že každý produkt, výrobek či služba vzniká konkrétní posloupností specifických činností tedy procesem. Všechny tyto činnosti a vztahy jsou zobrazovány pomocí procesního (postupového) diagramu, který tedy zahrnuje všechny potřebné činnosti, ale také všechny vazby mezi nimi, jejich souslednost a také zodpovědné pracovníky.

Procesní řízení je možné realizovat v několika úrovních. Tyto úrovně jsou vyznačeny dle stupně podrobnosti.

- Úroveň činností (aktivit)

- každý proces je rozvrhnut na dílčí činnosti (aktivity), které lze klasifikovat na: výkonné, kontrolní a rozhodovací. Každá z těchto činností je sledována na vstupu a výstupu. Tato úroveň je postačující pro proces restrukturalizace procesů. Toto modelování se nazývá statické.

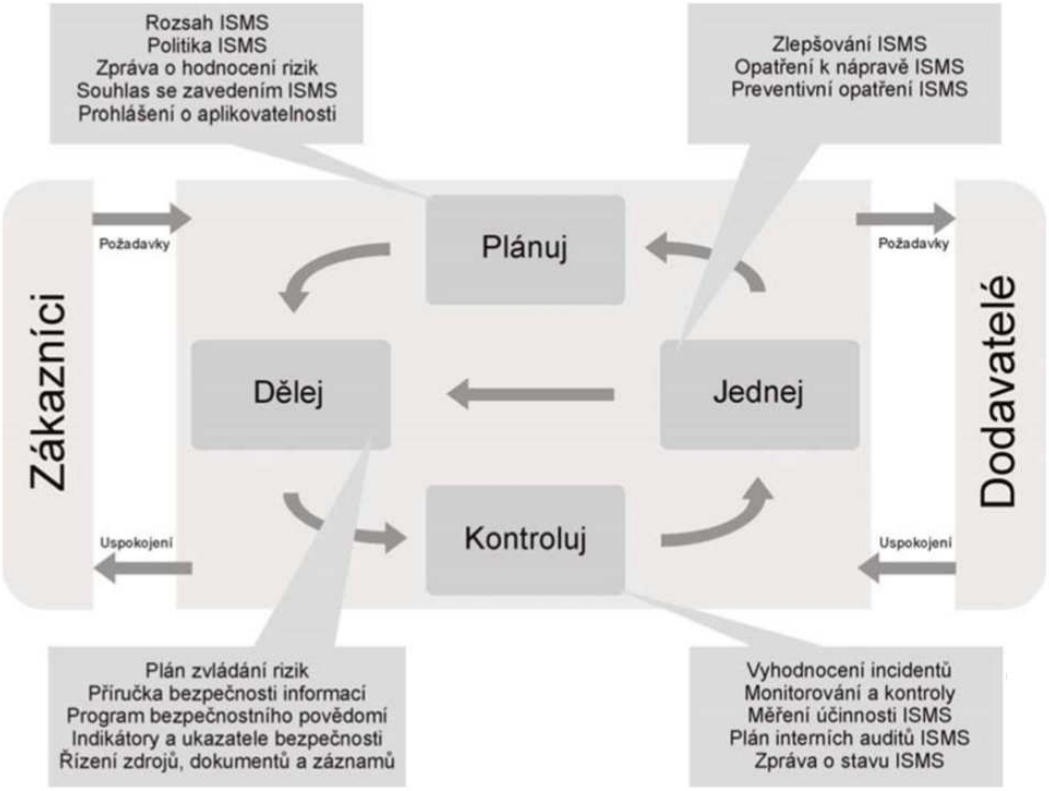
- Úroveň událostí

  - Každá činnost je započata a ukončena konkrétní událostí. To umožnuje sledovat tyto činnosti nejen jako jeden celek, ale také konkrétní výskyty těchto činností a to v reálném čase. Tímto je umožněna realizace řízení procesů (workflow), kde se činnosti střídají s událostmi. Toto modelování se nazývá dynamické.

Při procesním řízení je také využívána procesní mapa. Vzniká propojením procesů v organizaci. Slouží pro znázornění jednotlivých vazeb mezi danými procesy. Proto, aby tato mapa správně pracovala, musí splňovat několik podmínek. Nejdůležitější z nich je, že žádný proces nesmí nikde končit, čili musí na něj navazovat proces další. Z empirických zkušeností vyplývá, že tvorba přechodů mezi jednotlivými procesy a koordinace jejich souběhu je největší m problémem. Procesní mapa dále musí řešit větvení procesů a jejich cyklení.[10]

Realizace a aplikace procesního řízení je spojena nejen s využíváním programových a organizačních nástrojů, ale obnáší také práci s lidmi. Je totiž nutností transformovat jejich myšlení z funkčního řízení na řízení procesní, což bývá někdy velkým problémem, jelikož lidé si neradi zvykají na jiné, nové věci. Ti jsou touto změnou nuceni přejít od stavu, kdy se řídili převážně povely svého nadřízeného do stavu, kdy jejich hlavním smyslem práce je obsloužit proces do kterého jsou zařazeni.

2.2 Charakteristika jednotlivých kroků v cyklu PDCA [2]



Obrázek 4 PDCA model pro řízení bezpečnosti informací [2]

Plánuj:

Organizace jsou povinny v rámci tohoto kroku ustanovit politiku ISMS, stanovit si cíle procesů, kterých chce dosáhnout v rámci managementu rizik. Dále postupy zlepšování bezpečnosti informací a to tak, aby generované výsledky byly v souladu se zvolenou politikou organice a jejími zvolenými cíli. V rámci ustanovení ISMS je organizace povinna provést:

1. určení rozsahu a hranic ISMS na základě posouzení specifických rysů činností organizace, jejího uspořádání, struktury, umístění, aktiv a technologií
2. definici politiky ISMS na základě posouzení výše určených specifických rysů činností organizace. Tato politika určí pravidla činností týkajících se bezpečnosti informací, také stanovuje kritéria, kterými bude hodnoceno riziko. Zvolená politika musí zahrnovat strategii organizace a její organizační strukturu. Pro organizaci je nutné brát v úvahu zákonné nebo regulatorní požadavky. Zvolená politika musí být posléze schválena vedením.

3. stanovit přístup organizace k hodnocení rizik. Identifikovat metodiku hodnocení rizik, která musí vyhovovat politice ISMS (musí splňovat všechny požadavky. A to zákonné a bezpečnostní)Musí také dojít k vytvoření kritérií pro akceptaci rizik a identifikovat jejich akceptační úrovně. Je nutné zvolit takovou metodiku hodnocení rizik, která poskytne výsledky hodnocení rizik v podobě porovnatelné a reprodukovatelné (pro hodnocení rizik existuje řada různých metodik, v normě ISO/IEC TR 13335-3, Informační technologie- Směrnice pro řízení rizik bezpečnosti IT- část 3: Techniky pro řízení bezpečnosti IT
4. identifikovat rizika. Tato identifikace rizik obnáší identifikaci aktiv, která chce organizace chránit. K těmto aktivům přiřadí jejich vlastníky. Dále je nutné identifikovat všechny hrozby pro tyto aktiva a následně identifikovat zranitelnosti, které by mohly být hrozbami využity. Dále je nutné identifikovat, jaké dopady na aktiva by mohla mít ztráta důvěrnosti, integrity a dostupnosti.
5. analyzovat a vyhodnotit rizika. Zde probíhá posuzování dopadů na činnost organizace. Pro organizaci je dobré posoudit tyto dopady, které by potencionálně vznikly za skutečnosti ztráty důvěrnosti, integrity a dostupnosti, jelikož může určit prioritu těm aktivům, kterých se vysoký dopad týká. Posouzena by měla být i reálná pravděpodobnost selhání již zavedených opatření. A to z důvodů nahrazení těchto opatření, či jejich upravení. Posledním krokem je určení, zdali jsou rizika akceptovatelná či ne.
6. identifikovat a vyhodnotit varianty po zvládání rizik. Cílem je aplikovat vhodná opatření, popřípadě modifikovat opatření již zavedená a to za účelem šetření se zdroji. Ke zvládnutí rizik je možno zvolit několik variant přístupů. Při vědomém akceptování rizik (je to v souladu s politikou organizace a jsou splněna kritéria, která byla stanovena pro akceptaci rizik) Další možností je vyhnutí se rizikům, či přenesení rizik spojených s činností organizace na třetí strany, kterými mohou být pojišťovny, či dodavatelé.
7. vybrat cíle opatření a jednotlivá bezpečností opatření pro zvládání rizik. V této normě jsou obsaženy v příloze A.
8. získat souhlas se zbytkovými riziky
9. získat souhlas k zavedení a provozu ISMS
10. připravit prohlášení o aplikovatelnosti obsahující jaké cíle opatření byly zvoleny a proč byly zvoleny a jaká jsou již implementována. Toto prohlášení také obsahuje souhrn, jakým způsobem bude naloženo s identifikovanými riziky.

Dělej:

V tomto kroku dochází k samotnému zavádění a provozování ISMS, respektive k zavedení a využívání politiky ISMS, zvolených opatření, procesů a postupů.
Je nutno formulovat plán zvládání rizik, který vymezí odpovídající činnost vedení, zdroje, odpovědnosti a priority pro ISMS. Tento plán také slouží k dosažení identifikovaných cílů opatření, přičemž dojde k akceptaci zdrojů a k přiřazení rolí a odpovědností.
Dále musí určit způsob měření účinnosti vybraných opatření, je nutné určit, jakým způsobem budou změřené výsledky vyhodnocovány, při důležitém faktu, že vyhodnocování musí být porovnatelné a reprodukovatelné. Dále je nutné školení a zvyšování informovanosti a řídit provoz a zdroje ISMS. Na závěr je nutné zavést postupy a další opatření pro rychlou detekci a reakci na bezpečnostní události a postupy reakce na bezpečnostní incidenty.

Kontroluj:

V tomto kroku probíhá monitorování a přezkoumávání ISMS. Tj. posouzení, kde je to možné i měření výkonu zvolených procesů a to vůči politice ISMS, cílům a praktickým zkušenostem a poskytování výsledků vedení organizace k přezkoumání. Kontinuální monitorování je nutné z důvodů včasné detekce chyb zpracování, včasnou identifikaci úspěšných a neúspěšných pokusů o narušení bezpečnosti a detekci bezpečnostních incidentů. Cílem je detekovat bezpečnostní událost a zabránit tak vzniku bezpečnostnímu incidentu. A pokud dojde k bezpečnostnímu incidentu je cílem učinit vyhodnocení podniknutých činností. Zdali jsou účinné a efektivní. Dochází zde také k pravidelnému přezkoumávání ISMS a to formou interních auditů. Dochází k měření účinnosti zavedených opatření pro ověření dosažení požadované bezpečnosti a v plánovaných intervalech přezkoumání hodnocení rizik, zbytkových rizik a úroveň akceptovatelných rizik, jelikož organizace se vyvíjí (mění se její cíle), společně s ní se mění technologie, účinnost již zavedených opatření, ale také hrozby a zranitelnosti.

Jednej:

Tento poslední krok je zaměřen na udržování a zlepšování efektivnosti ISMS. Za využití výsledků z předchozího kroku Kontroluj, kde probíhalo testování navrhnutých opatření a podrobování systému internímu auditu (Interní audity jsou prováděny v pravidelných intervalech, které jsou určeny plány interních auditů). Náplní tohoto kroku je také navrhnutí nápravných, či preventivních opatření, která je nutno aplikovat na

identifikované neshody, či nedostatky spojené s implementací a udržováním ISMS. Navrhnutá nápravná opatření jsou realizována za účelem zamezení vzniku neshod, nedorozumění, či komplikací při dodržování zvolených postupů, či rolí u určitých činností, či procesů. Tento krok uzavírá PDCA cyklus, ale zároveň ho opět rozbíhá, jelikož je nutné systém ISMS stále analyzovat a zabránit jeho stagnaci ve vývoji.

Všechny výše uvedené kroky, procesy musí být řádně zdokumentované. Dokumenty musí obsahovat záznamy o veškerých rozhodnutích. Tato potřeba je odvozena od potřeby zajistit že veškeré činnosti odsouhlasené vedením je možné zpětně identifikovat a tedy je zajištěna i jejich opakovatelnost. Dokumentace musí dle normy obsahovat prohlášení politiky a cílů ISMS, rozsah ISMS postupy opatření, seznamy aktiv, hrozeb, metodiky hodnocení rizik. Cyklus PDCA umožnuje také vnořování dalších jednotlivých PDCA smyček do jednotlivých kroků a tím umožnuje docílení různých úrovní detailu náhledů. PDCA je tedy nástroj, který umožní popsat celkový proces řízení a to pro každé opatření a každou činnost a umožní tak kontrolovaný a systematický postup při implementaci ISMS.

2.3 Problematika implementace systémů řízení bezpečnosti informací [11]

- **Nedostatečná kompetence odborníků na ISMS**

Jednou z nejvíce problematických oblastí je odborná kompetence pracovníků, kteří jsou zavedením ISMS pověřeni. Důvodem je, že vlastní norma ISO/IEC 27001 obsahuje pouze nejpotřebnější požadavky, které je potřeba splnit. Podrobné vysvětlení, co tyto požadavky v praxi znamenají, však v dané normě nelze nalézt a pro nezkušeného pracovníka, či čtenáře normy jsou informace neefektivní. Je tedy pro úspěšné implementování ISMS ve společnosti nejen dodržování postupů v normě, ale také přítomnost zkušeného odborníka, který danou implementaci dovede do zdárného konce

- **Nedostatky při určení rozsahu ISMS**

Dalším důležitým faktorem je určení oblastí, ve kterých je ISMS implementováno. V praxi se tomuto kroku nevěnuje dostatečné množství pozornosti, což má za následek komplikace při samotné implementaci.

Na první pohled je nejjednodušší zvolit jako oblast implementace celý podnik. Ano, tímto krokem se usnadní vymezení rozsahu systému, ale současně se proces implementace

ISMS velice ztíží. Z praxe je ověřen postup tkvící v zavedení ISMS ve vhodné části společnosti a na základě zkušeností z tohoto zavedení rozšiřovat a zavádět ISMS v dalších částech společnosti

- **Nedostatky při řízení rizik**

Tento nedostatek tkví ve špatné identifikaci míry rizika. Věnování pozornosti malým rizikům je plýtvání časem a zdroji. Pokud společnost, identifikuje svoje rizika správným způsobem, dochází i k jejich účinnému zvládání a tím je zároveň zajištěna účelná a účinná funkčnost ISMS. Pokud avšak společnost, nemá přesnou představu o rizicích, která che pomocí implementace ISMS z minimalizovat, není schopna jejich přesné interpretace, tak tato společnost obvykle ani není schopna ISMS efektivně zavést. Z empirických zkušeností je doporučeno, aby ISMS na počátku pracovalo s desítkami rizik (cca 20 až 30 identifikovaných rizik). Teprve s nabytými zkušenostmi je doporučeno počet rizik navýšit.

Příklady dalších možných nedostatků:

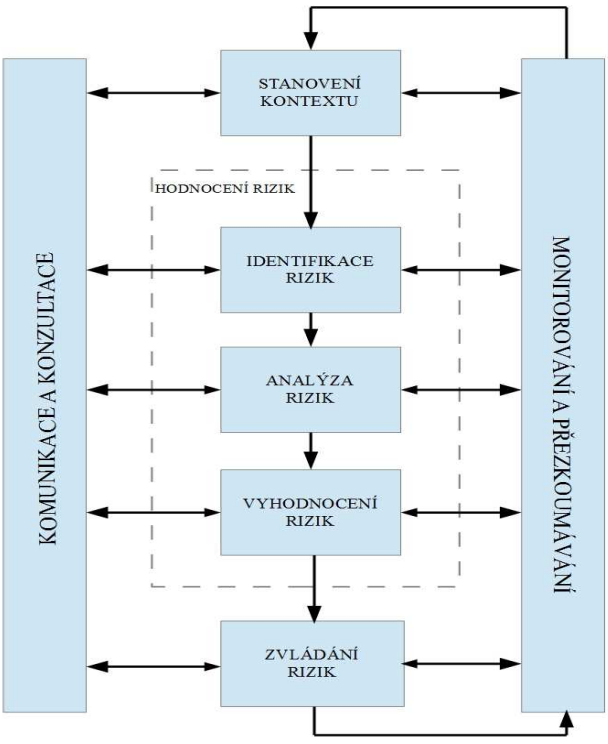
- Nedostatky v dokumentaci ISMS
- Nedostatky při měření účinnosti ISMS
- Nedostatky při řízení záznamů ISMS
- Nedostatky při komunikaci s auditory ISMS

3 Řízení rizik

Řízení rizik je velice důležitý proces. Pro popis je příhodné uvést výraz pana J. Hootena který řekl: „Jestliže nemůžete řídit riziko, nemůžete ho kontrolovat. Pokud ho nemůžete kontrolovat, nemůžete ho šetřit. To znamená, že hrajete hazardní hru a doufáte, že budete mít štěstí.“ Toto naznačuje důležitost uvědomění si faktu, že je v současnosti nezbytnou nutností řídit rizika.

Proces **řízení rizik** požaduje vytvoření příhodné infrastruktury a užití logického a systematického postupu. Řízení rizik je nepřetržitý proces, jednotlivé kroky celého procesu a jejich posloupnost jsou zobrazeny na obrázku č 5. Sestává z těchto základních procesů: stanovení kontextu, vyhodnocení rizik a ošetření rizik. Tyto základní procesy jsou

diverzifikovány do dalších sub procesů a to za účelem efektivnějšího řízení rizik. Těmito sub procesy jsou: pochopení rizik, jejich identifikace, posouzení a to vzhledem k následkům a rozsahu dopadu na činnost organizace, určení jejich pravděpodobnosti výskytu, určení priorit, čili určení plánu ošetření, ochrany aktiv, která jsou identifikovanými riziky ohrožována a která byla politikou organizace určena jako. Tyto jednotlivé procesy a sub procesy budou charakterizovány v následujících kapitolách. Aplikace těchto procesů je opět provedena za pomoci modulu PDCA.[12] Na řízení rizik lze také nahlédnout jako na analýzu důsledků a vytvoření scénářů dopadů incidentů, které nastanou, či mohou nastat při ignoraci nutnosti zavedení určitých protiopatření.



Obrázek 5 Proces řízení rizik [6]

3.1 STANOVENÍ KONTEXTU [6]

Tento proces, činnost je prvotním krokem při zavádění ISMS. Slouží k identifikování potřeb organizace. Sestává se z určení rozsahu a hranic implementace ISMS a určení základních kritérií. Je velice důležité, aby si organizace uvědomila, jak moc je tento krok podstatný a věnovala mu dostatečnou pozornost, jelikož od nastavených metrik, které se

v tomto kroku stanoví, se odvíjí celý proces vyhodnocování rizik a následné zvládání rizik. V tomto kroku tedy probíhá definice rozsahu a hranic procesu řízení rizik bezpečnosti informací. Jsou zde stanovena základní kritéria pro řízení rizik, hodnocení rizik, kritéria dopadu a kritéria akceptace rizik (jednotlivá kritéria jsou popsána v následujících odstavcích).

Důležitým procesem je volba správného přístupu. Tato volba přístupu je komplikována rozmanitostí přístupů v rizikovém inženýrství, jimiž jsou např. přístup analytický, deterministický, fuzzy, heuristický, systémový[13] V normě je uveden přístup systematický a logický, který dokáže plně pokrýt všechny požadavky. Určení hranic a rozsahu je důležitý proces. Určením rozsahu procesu ISMS se zajistí akceptace všech aktiv a eliminace opominutí aktiv, která by mohla být přehlédnuta. Určením hranic dojde ke zjednodušení procesu identifikace rizik. Dojde tedy k vytvoření hranic, které pomohou určit všechna aktivní rizika, která mohou prolomit určené hranice.

3.1.1 KRITÉRIUM HODNOCENÍ RIZIK

Toto kritérium slouží k určení pravidel, které budou sloužit pro klasifikaci rizik získaných analýzou rizik. Tyto kritéria pomohou organizaci určit rizika, která jsou pro ni, vzhledem ke zvoleným prioritám, akceptovatelná, či neakceptovatelná a na základě těchto kritérií budou vyvíjeny aktivity pro eliminaci zvolených rizik (plán ošetření rizik). Při procesu utváření kritérií hodnocení rizik je dobré zohlednit faktory jako je hodnota aktiv, která jsou danými riziky ohrožena, nebo strategický význam jednotlivých procesů v organizaci a výše negativních efektů, právní a legislativní požadavky. Uvědomění si těchto faktorů pomůže ustanovit kritéria hodnocení rizik pro každou organizaci individuálně.

3.1.2 KRITÉRIUM DOPADU

Sestavením kritérií dopadu organizace vytváří seznamy škod, které při nastalých bezpečnostních incidentech mohou nastat. Určení velikosti těchto škod pomáhá při utváření plánu ošetření rizik. Při procesu utváření kritérií dopadu, napomáhá přihlédnout k faktům, jaké aktivum je pro organizaci důležité, respektive zdali poškození daného aktiva může vést k zastavení provozů, či jiných důležitých procesů, nedodržení termínů, či jak je ohrožena důvěrnost, integrita a dostupnost aktiva (informace).

3.1.3 KRITÉRIUM AKCEPTACE RIZIK

Sestavením kritérií akceptace rizik organizace vytváří klasifikační seznam úrovní rizik, která určují, zda jsou jednotlivá identifikovaná rizika akceptovatelná, či nikoliv a je nezbytné učinit další kroky, pro docílení požadované úrovně. Tyto seznamy jsou opět pro každou organizaci individuální, jelikož jsou silně ovlivněny politikami, záměry, nebo cíli dané organizace, či pouze zainteresovaných stran. Při procesu utváření kritérií akceptace rizik, napomáhá přihlédnout k faktům, jaký je poměr obchodního přínosu, ku odhadnutému riziku, či zdali pro určitá rizika existují akceptační limity (smluvní požadavky),či nikoliv (zákony, normy). Při stanovování kritérií akceptace rizik je také nutné přihlédnout na fakt, jak dlouho se očekává, že dané riziko bude existovat (zdali je riziko spojeno s krátkodobou či dlouhodobou činností)

3.2 POSOUZENÍ RIZIK

V tomto kroku dochází k identifikaci všech rizik. Tato identifikována rizika jsou následně ohodnocena dle kritérií stanovených v kroku stanovení kontextu. Posouzení rizik je složeno z těchto dílčích kroků:

3.2.1 IDENTIFIKACE RIZIK

Při procesu identifikace rizik dochází k určování scénářů událostí. K identifikaci rizik dochází na základě určení několika parametrů, s využitím kritérií určených v předešlém procesu.

- **Identifikace aktiv**

Identifikace aktiv je prvním parametrem při identifikaci rizik. Jako aktivum je subjekt, který má určitou hodnotu a vyžaduje ochranu. V tomto procesu dochází k určení aktiv a vlastníků aktiv a to v rámci rozsahu, který byl určen v předešlém procesu (stanovení kontextu).

- **Identifikace hrozeb**

Následujícím krokem je identifikace hrozeb. Hrozba má potenciál poškodit aktivum. Informace o potencionálních hrozbách a pravděpodobnosti jejich výskytu lze získat od vlastníků aktiv, či z předchozích situací. Cílem tohoto procesu je nejen samotná identifikace

hrozeb, ale také identifikace zdrojů těchto hrozeb. Některé hrozby mohou působit i na více aktiv. Existují různé druhy hrozeb. Mohou být charakteru lidského, přírodního, hrozby působící zvenčí, či zevnitř organizace. Pro názornější sestavení a zamezení vynechání potencionálních hrozeb je doporučeno situovat hrozby do skupin, či tříd dle typu (např. neoprávněné akce, přírodní živel) a dále se zaobírat identifikací jednotlivých hrozeb v dílčích skupinách, či třídách.

- **Identifikace stávajících opatření**

Provádí se za účelem vyloučení duplikace opatření, které bylo již zavedeno, dochází tedy k zamezení plýtvání zdroji, které by byly vynaloženy na aplikaci stejných opatření. Paralelně při detekci těchto opatření je zkoumána i jejich funkčnost. Pokud jsou opatření funkční, dostačující (chrání daná aktiva a drží úroveň rizik na akceptovatelné hranici) jsou akceptována a ponechána beze změn. Pokud jsou označena jako nefunkční, vyvstává zde nutnost provést rozhodnutí, zdali zavedené opatření bude upraveno, či zrušeno a nahrazeno opatřením efektivnějším. Výstupem tohoto procesu je soubor již existujících opatření a také opatřeních nových spolu s postupy jejich implementace.

- **Identifikace zranitelností**

V tomto procesu dochází k určení všech potencionálních zranitelností. Vstupními informacemi, které jsou pro tento proces nepostradatelné, je seznam známých hrozeb, aktiv a existujících opatření. Cílem je identifikovat pouze ty zranitelnosti, které mají potenciální hrozby. Zranitelnost bez hrozby není rizikem. Není tedy nutno ji nikterak eliminovat, ale tato zranitelnost by měla být stále monitorována, jelikož může nastat situace, že se v průběhu času nějaká hrozba vyskytne.

- **Identifikace následků**

V tomto procesu probíhá identifikace následků, které mohou nastat v důsledku působení bezpečnostního incidentů. Velikost následků je přímo úměrná velikosti hodnoty aktiva, na které působí, respektive aktiva, které utrpělo vlivem bezpečnostního incidentu ztrátu důvěrnosti, integrity a dostupnosti. Následkem může být například poškození pověsti organizace, snížení efektivnosti výroby, neúspěšné výběrové řízení. Následky lze také klasifikovat jako krátkodobé, či dlouhodobé, to v případě nenávratné ztráty aktiva.

3.3 ANALÝZA RIZIK

Analýza rizik je proces, ve kterém probíhá vyhodnocování rizik. Tento proces lze provádět v rozličných stupních podrobnosti. Tyto stupně jsou závislé na příklad na velikosti ohrožení aktiv, na výši rizika, které ji ohrožuje. Při procesu analýzy rizik lze využít kvantitativní, či kvalitativní metodu (tyto metody jsou charakterizovány v následujících kapitolách). Tato volba je na organizaci. Kvalitativní metoda se oproti kvalitativní metodě vyznačuje nižší náročností a nákladovostí. Empiricky je prokázáno, že pro prvotní analýzu rizik je zvolena metoda kvalitativní, která umožní identifikaci všech rizik a odhalení vysokých rizik. Při následné sekundární analýze je využita metoda kvantitativní (například pro nalezená vysoká rizika).

- kvantitativní metoda [13] [14]

  Tento typ metody využívá matematického aparátu pro výpočet rizika a to z frekvence výskytu hrozby a jejího potenciálního dopadu. Tyto oba dva parametry jsou oceněny ve finančních termínech. Kvantitativní metoda je velice náročná na čas a na množství vynaloženého úsilí. Avšak poskytuje finanční vyjádření, které je pro řízení rizik výhodnější. Kvantitativní přístup k analýze rizik se ujal převážně v oblasti bezpečnosti organizací, konkrétněji v jejich informačních systémech. Nejznámější zástupcem této metodiky je softwarový nástroj CRAMM (CCTA Risk Analysis and Management Method.

- kvalitativní metoda [13]

  Tento typ metody popisuje závažnost dopadu a pravděpodobnost, že určitá událost nastane. Rizika jsou vyjádřena v předem určeném celočíselném rozsahu, či jsou oklasifikována verbálně jako rizika malá, střední a velká. Jsou rychlé a jednoduché na zpracování.

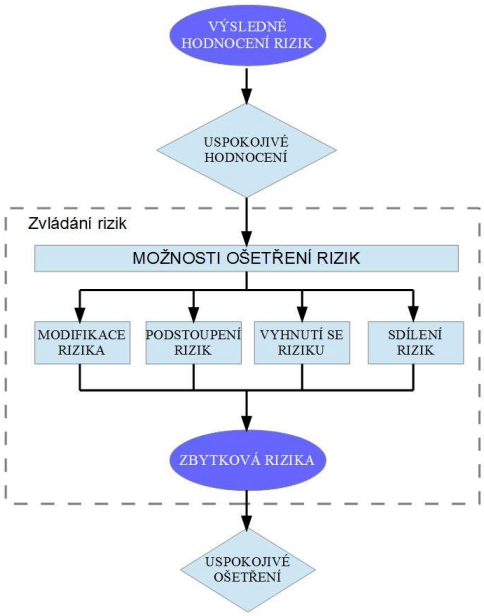
Kvalitativní metoda je v porovnání s kvalitativní metodou mnohem méně exaktní. Je časově méně náročná a není nutné díky její nenáročnosti na zpracování formalizovaného přístupu. Důsledkem toho je kvantitativní metoda vysoce subjektivní a data díky ní získaná mohou činit například při procesu zvládání rizik problémy a to svou nedostatečnou přesností.

3.3.1 VYHODNOCENÍ RIZIK

Vyhodnocení rizik je v analýze rizik závěrečným krokem. Dochází zde ke komparativnímu porovnání výsledků z analýzy rizik, tedy identifikovanými úrovněmi rizik s kritérii rizik, která byla vytvořena a zaznamenána v kroku stanovení kontextu. Výstupem tohoto kroku je rozhodnutí, zdali jsou jednotlivá identifikovaná rizika akceptovatelná, či neakceptovatelná. Pokud jsou rizika označena jako neakceptovatelná, je nutné podrobit je kroku zvládání rizik (viz následující kapitola).

3.4 ZVLÁDÁNÍ RIZIK

Zvládání rizik je proces, pro který tvoří vstupy rizika, která byla shledána v předchozím kroku jako neakceptovatelná (čili vyžadující eliminaci jejich hodnoty) Možností, jak eliminovat tyto hodnoty nabízí tento krok hned několik, přičemž je nutné uvést, že tyto možnosti navzájem nikterak neovlivňují. Jsou jimi možnosti: modifikace rizik, podstoupení rizik, vyhnutí se riziku a sdílení rizika (tyto možnosti jsou individuálně charakterizovány v následujících kapitolách). Celý proces zvládání rizik je vyobrazen na obrázku č.X Při procesu výběru opatření je nutno přihlédnout na faktory, kterými jsou například faktory právní, smluvní požadavky, finanční, technická a časová náročnost, či zdali jsou vybraná opatření omezena například kulturními či etickými kodexy.



Obrázek 6 proces zvládání rizik [6]

Zvládání rizik

- **Modifikace** rizik

K modifikaci rizika je využito procesů zavedení, odstranění, nebo provedením změny. Tyto procesy jsou provedeny tak, aby zbytkové riziko mohlo být překlasifikováno jako akceptovatelné.

- **Podstoupení rizik**

  Jedná se o přijmutí rizika a o jeho vědomé podstoupení a to bez jakéhokoliv následujícího opatření.

- **Vyhnutí se riziku**

  Tato možnost opatření (ošetření rizika) je volena u rizik velmi vysokých, či u rizik pro která jsou nápravná opatření velice finančně náročná. Organizace zvolením této možnosti přímá rozhodnutí o celkovém vyhnutí se danému riziku, tedy že upouští od dané činnosti, která je s daným rizikem spjata, nebo přehodnotí podmínky, při kterých tyto činnosti probíhají.

- **Sdílení rizik**

  Tato možnost opatření využívá možnost sdílení daného rizika se třetí stranou. Toto sdílení má za následek snížení hodnoty rizika. Toto sdílení lze realizovat například uzavřením pojistné smlouvy, či zanesení určitých podmínek do smluv s obchodními partnery.

4 Analýza požadavků na systém řízení rizik [6]

Úkolem systému řízení rizik bezpečnosti informací, je poskytnout organizaci možnost efektivně a systematicky ochránit svá aktiva. Nastolit organizaci systém, který ji umožní zvládat rizika, kterým je vystavena a která mají negativní vliv na širokou škálu parametrů. Jimi může být například konkurenceschopnost organizace na trhu, zvladatelnost vlastních procesů, schopnost dodržování smluvních závazků, právních závazků.

Proto, aby systém řízení rizik bezpečnosti informací byl efektivní, je nutné, aby organizace postupovala dle pokynů a doporučení určených v normě ČSN ISO/IEC 27005.

Tyto požadavky jsou uvedeny v následujících kapitolách

4.1 Nutnost monitorování a přezkoumávání rizik bezpečnosti informací

Při požadavku na efektivní a funkční systém řízení rizik bezpečnosti informací je nutné, aby docházelo k neustálému (a to v ideálním případě) monitorování a přezkoumávání rizikových faktorů.

Důsledkem kontinuálního monitorování a přezkoumávání rizikových faktorů je totiž možnost včasné detekce jakékoliv změny vzhledem ke kontextu organizace a tudíž rychlá reakce na změnu rizik. Rizika nejsou stálá, jsou v čase proměnná a k změně rizik může dojít, bez jakékoliv předešlé indikace.

Požadavkem na systém řízení rizik je tedy vytvoření neustálého monitorování a přezkoumávání již ošetřených rizik, akceptovatelných rizik, tedy jejich dílčích složek, kterými je myšlena hrozba, zranitelnost a pravděpodobnost výskytu. Důsledkem změn těchto parametrů může nastat situace, že vhodnost implementovaných opatření může poklesnout, či že implementovaná opatření budou neefektivní

Dle normy ČSN ISO/IEC 27005 by organizace měla zajistit neustálé monitorování:

- Nových aktiv, která byla identifikována
- Nutných změn hodnot vlivem změny činnosti organizace
- Dalších nových hrozeb, které dosud nebyly ohodnoceny a které mohou působit na organizace zvenčí i zevnitř.
- Možností, kdy nové zranitelnosti, mohou umožnit hrozbám tyto nové zranitelnosti zneužít
- Již identifikovaných zranitelností, které mohou být vystavený působení nových hrozeb
- Zvýšeného dopadu, hrozeb, zranitelností a rizik, která vzájemnou interakcí mohou vytvořit neakceptovatelnou úroveň rizik

Organizace by měla také zajistit potřebné zdroje pro procesy posouzení a ošetření rizik.

4.2 Nutnost komunikace a konzultace rizik bezpečnosti informací

Aby systém řízení rizik, byl efektivní, je nutné, aby probíhala komunikace mezi zainteresovanými stranami a vedoucími, kteří jsou zodpovědní za řízení rizik.
Při procesu řízení rizik je nutné pracovat s velkým množstvím informací. Může zde tedy nastat situace, že některé informace, které obsahují údaje o existenci, charakteru, formě a pravděpodobnosti, závažnosti, ošetření a přijatelnosti, budou přehlédnuty, či mohou být ignorovány a to nesprávně. Vytvořením komunikačních kanálů (obousměrných) mezi zainteresovanými stranami a osobami odpovědnými řízením rizik dojde k eliminaci přehlédnutí, či nesprávnému ignorování konkrétních informací. Komunikace rizik je tedy proces, který umožňuje výměnu informací, které jsou nutné pro objektivní a efektivní řízení rizik. Při tomto procesu dochází k ustanovení dohod, ve kterých je stanoveno jak řídit daná rizika. Tyto dohody jsou přijímány a ustanoveny na základě informací, které poskytly zainteresované strany osobám činící rozhodnutí ve věci řízení rizik.

Vytvoření účinného komunikačního kanálu pomůže také k rychlejšímu a efektivnějšímu přenosu informací od zainteresovaných stran k osobám odpovědných za řízení rizik za situace, že chápání rizika vlivem změny potřeb, či zájmů těchto stran. Důsledkem tohoto bude reakční čas při následném upravování rizik snížen. Zainteresované strany totiž posuzují úroveň přijatelnosti na základě svých potřeb, které se mění a záleží tedy na tom, aby byly jejich potřeby plně uspokojeny. Je doporučeno pro vytvoření tohoto efektivního komunikačního kanálu vytvořit výbor, složený ze zástupců obou stran

Dle normy ČSN ISO/IEC 27005 by komunikace rizik měla být provozována za účelem: [6]

- Efektivnějšímu shromažďování informací o rizicích
- Garance záruky výstupu řízení rizik organizace
- Předávání výsledků získaných z posuzování rizik a informování o plánu ošetření rizik
- Vyhnutí se nedorozumění, mezi zainteresovanými stranami a osobami pověřenými řízením rizik, jehož důsledkem může vzniknout narušení bezpečnosti informací
- Řízení plánování opatření s cílem poklesu následků potenciálního incidentu
- Podpory vykonávat rozhodnutí

- Shromažďování nových informací o řízení rizik bezpečnosti informací
- Zvyšování povědomí

Norma také dále doporučuje vytvoření plánů komunikace rizik pro situace, jak rutinní a známé, tak pro situace nouzové.

Výsledkem vytvoření funkčního komunikačního kanálu bude organizace trvale chápat procesy řízení rizik bezpečnosti informací.

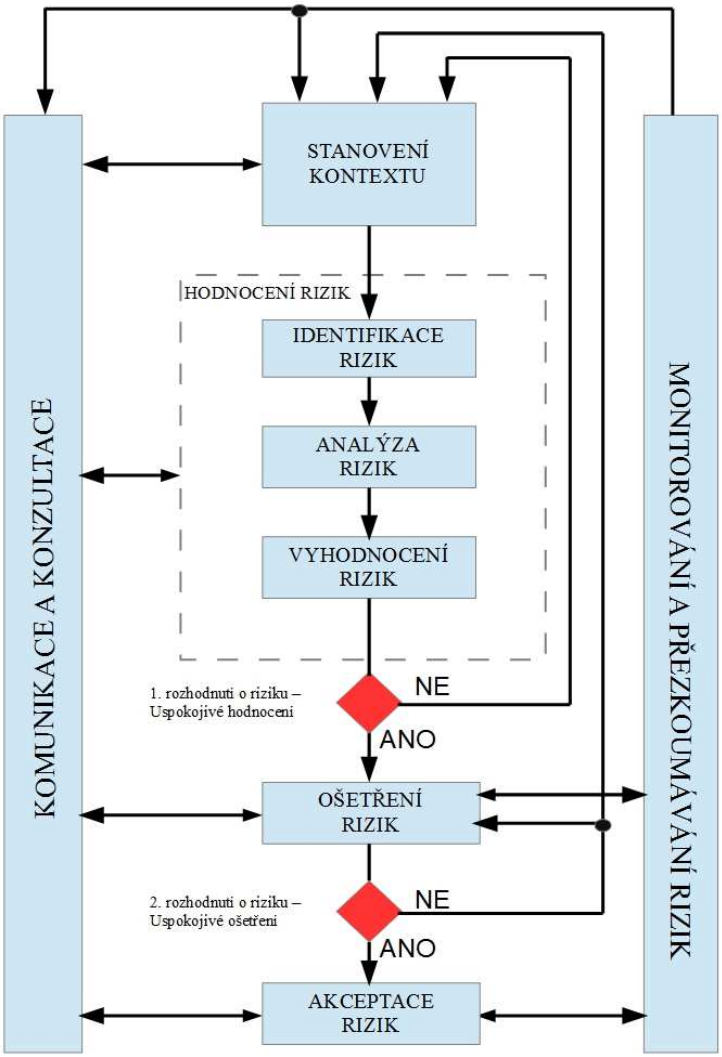
Aplikací všech výše uvedených požadavků na systém řízení rizik bezpečnosti informací bude systém řízení rizik v souladu s politikou organizace.

5 Návrh a realizace nástroje pro řízení rizik a hodnocení efektivnosti

5.1 Nástroj pro řízení rizik

Navržený nástroj je vytvořen v programu Microsoft Office Excel 2010. Tento program byl zvolen na základě jeho masového rozšíření a na jeho dostupnosti. Program poskytuje širokou škálu funkcí, možností importu dat z jiných programů, jako je například Microsoft Office Access, data z webu (například SQL Server), či z jiných externích uložišť. Tento fakt poskytuje široké pole možností jak navržený nástroj provázat s jinými, či připojit k nástroji další moduly a vytvořit tak komplexní a flexibilní systém.

Při tvorbě tohoto nástroje jsem postupoval dle normy ČSN ISO/IEC 27005. Byla dodržována posloupnost kroků uvedených na obrázku číslo 7. Nástroj obsahuje všechny kroky, které jsou uvedeny a popsány v teoretické části této práce. Mnou navržený nástroj je zaměřen na prezentaci procesu řízení rizik a umožní uživateli plné pochopení všech faktorů spojených s tímto procesem.



Obrázek 7 Vývojový diagram procesů řízení rizik [6]

5.1.1 Popis nástroje

Nástroj umožnuje uživateli provést analýzu rizik, identifikaci rizik, ošetření rizik. Pro potřebu výpočtu rizika je využito 3 faktorového vyhodnocení. Tedy dané riziko se počítá z kvantitativní hodnoty aktiva, kvantitativní hodnoty hrozby a z pravděpodobnosti výskytu zranitelnosti. Všechny požadavky přístupy a možnosti jsou popsány v teoretické části této práce a tento navržený nástroj je navržen za účelem prezentování procesu řízení rizik. Nástroj je složen celkem z osmi listů.

Na úvodním listu je stručná charakteristika nástroje a jeho popis. Na následujícím listu: "stanovení kontextu" je uživatel vyzván k zadání vstupních informací. Těmito informacemi jsou: určení rozsahu aktiv a způsob jejich hodnocení, určení rozsahu hrozeb, určení kritérií hodnocení rizik, stanovení dopadu a stanovení kritérií akceptovatelnosti.

Je zde také umístěna nápověda pro názornější ukázku možnosti přístupu k vyhodnocování rozsahu a identifikací úrovní. Na následujícím listu se nachází vstupní tabulky. Jako vstupní data jsem zvolil u aktiv kvalitativní hodnotu a kvantitativní hodnotu. Kvalitativní hodnota je zde uvedena, jelikož je potřebná k výpočtu hodnoty rizika. Hodnota kvantitativní u daného aktiva slouží pro pozdější vyhodnocení efektivnosti a to v případě výskytu bezpečnostního incidentu. V tabulce hrozby je uvedena pouze hodnota kvalitativní.

Tyto dvě vstupní tabulky jsou naformátovány tak, aby uživatel v situaci, kdy nastavená velikost těchto tabulek není dostačující, je nemusel manuálně rozšiřovat. Tabulky jsou uvedeny na obrázku č. 8

AKTIVUM	Hodnota Kvalitativní1	Hodnota Kvantitativní
Databáze	5	500 000 Kč
Datové soubory	3	300 000 Kč
Firemní dokumentace	1	20 000 Kč
Systémová dokumentace	4	450 000 Kč
Smlouvy	4	750 000 Kč
Uživatelské manuály	2	

HROZBY	Hodnota Kvalitativní2
požár	1
poškození vodou	3
znečištění	2
závážná nehoda	4
zničení zařízení nebo médií	5
prach, koroze, zamrznutí	

Obrázek 8 Vstupní tabulky

Pro analýzu rizik byla vytvořena tabulka, viz obrázek číslo 9. V této tabulce je možné po určení aktiv a hrozeb doplnit informace ohledně stávajících opatření, pokud byla nějaká v procesu identifikace stávajících opatření identifikována. Dále je možné vyplnit zranitelnost, která může poskytnout dané hrozbě možnost napadnout aktivum. Tabulka je doplněna také o možnost určení dopadu. Pro ukázku jsem zvolil celočíselné vyjádření dopadu, kdy jednotlivé stupně odpovídají finančním nákladům, které by bylo nutné vynaložit na opravu škod napáchaných konkrétní hrozbou

AKTIVUM	Hodnota Kvalitativní 1	Hodnota Kvantitativní	HROZBY	Hodnota Kvalitativní 2	Stávající opatření	Popis stávajícího opatření	Zranitelnost	ppst výskytu zranitelnosti	Dopad
Databáze	5	500000	selhání zařízení	4	NE		výpadek el energie	2	4
Databáze	5	500000	zneužití oprávnění	5	ANO	přístupová hesla	zneužití	1	4
Databáze	5	500000	vzdálená špionáž	3	ANO	instalace firewall	prolomení	1	4
Smlouvy	4	750000	nezákoné zpracování dat	2	NE		zaměstnanci	4	5
Klimatizace	4	470000	znečištění	2	NE		hlodavci	3	2
Datové soubory	3	300000	chyba v používání	3	NE		absence návodů	5	1
Systémová dokumenta	4	450000	zničení zařízení nebo médií	5			vodovod v archivu	4	4
Firemní dokumentace	1	20000	zneužití oprávnění	5			hacking	4	2

Obrázek 9 Vstupní tabulka pro analýzu rizik

Zadávání dat v případě, kdy na jedno aktivum působí více hrozeb je v tabulce vyřešen možností znázorněné na obrázku číslo 9.

Pro potřebu názorné prezentace identifikovaných rizik při procesu řízení rizik byla vytvořena tabulka, která je zobrazena na následujícím obrázku.

ošetření rizik: NÍZKÉ a výše Hodnota (min) rizika 21 GENEROVAT

Riziko	Klasifikace	AKTIVUM	Hodnota Kvalitativn	Hodnota Kvantitativ	HROZBY	Hodnota Kvalitativní2	Stávající opatření	Popis stávajícího opatření	Zranitelnost	ppst výskytu zranitelnos	Dopad
80	KRITICKÉ	Systémová dokume	4	450000	zničení zařízení nebo m	5	(prázdné)	(prázdné)	vodovod v archiv	4	4
45	VYSOKÉ	Datové soubory	3	300000	chyba v používání	3	NE		absence návodů	5	1
40	STŘEDNÍ	Databáze	5	500000	selhání zařízení	4	NE		výpadek el ener	2	4
32	STŘEDNÍ	Smlouvy	4	750000	nezákoné zpracování d	2	NE	(prázdné)	zaměstnanci	4	5
25	NÍZKÉ	Databáze	5	500000	zneužití oprávnění	5	ANO	přístupová hesla	zneužití	1	4
24	NÍZKÉ	Klimatizace	4	470000	znečištění	2	NE		hlodavci	3	2
20	VELMI_NÍZKÉ	Firemní dokumenta	1	20000	zneužití oprávnění	5	(prázdné)	(prázdné)	hacking	4	2
15	VELMI_NÍZKÉ	Databáze	5	500000	vzdálená špionáž	3	ANO	instalace firewall	prolomení	1	4

Obrázek 10 Kontingenční tabulka pro identifikaci rizik

Tato generovaná kontingenční tabulka je pro intuitivnější použití formátována pomocí filtrů. Nástroj dále umožňuje uživateli v případě velkého množství rizik použít funkci průřezů. Jako kritérium pro volbu jaká rizika budou ošetřena, je zde zvolena úroveň rizika.

Pro prezentování procesu ošetření rizik byla vytvořena tabulka zobrazená na obrázku číslo 11. V procesu ošetření rizik, lze zvolit různé způsoby ošetření. Po zadání všech nových dat týkajících se přijetí různých opatření nástroj určí novou hodnotu rizika a jeho úroveň. Součástí procesu ošetřování rizik je vytváření plánu zvládání rizik.

Tabulka pro ošetření rizik

ošetření	ošetřeno				popis ošetření	náklady	datum zahájení	datum ukončení	nová hodnota rizika	klasifikace
	aktivum	hrozba	zranitelnost	Dopad						
Modifikace	4	5	2	4	vystužení vodovodu	20 000 Kč	1.1.2014	3.1.2014	40	STŘEDNÍ
Modifikace	3	3	2	1	vypracování návodů	15 000 Kč	1.2.2014	2.2.2014	18	VELMI_NÍZKÉ
Sdílení	5	4	2	4	odpovědný poskytovatel	5 000 Kč	3.4.2014	4.5.2014	40	STŘEDNÍ
Modifikace	4	2	3	5	školení	50 000 Kč	1.1.2014	6.7.2014	24	NÍZKÉ
Akceptace	5	5	1	4	Riziko akceptováno				25	NÍZKÉ
Akceptace	4	2	3	2	Riziko akceptováno				24	NÍZKÉ
Modifikace			2	2	instalace firewallu		2.2.2015	2.2.2018		
Akceptace				4	Riziko akceptováno				0	NEPATRNÉ

Obrázek 11 Tabulka pro ošetření rizik

Následujícím krokem je akceptace zbývajících rizik. Pro tuto potřebu byla vytvořena tabulka zobrazená na obrázku číslo 12. V případě, že se nachází nějaké riziko, při stanovených kritérií akceptovatelnosti nad úrovní zvoleného rizika dojde k jeho ohlášení. Poté je tedy nutné, se vrátit zpět do procesu ošetření rizik a zvolit jiné efektivnější opatření.

Tabulka výsledných údajů:

ošetření	ošetřeno				popis ošetření	náklady	datum zahájení	datum ukončení	nová hodnota rizika	klasifikace	Dle kritérií Akceptovatelnosti jsou následná, identifikovaná rizika
	aktivum	hrozba	zranitelnost	dopad							
Modifikace	4	5	2	4	vystužení vodovodu	20 000 Kč	1.1.2014	3.1.2014	40	STŘEDNÍ	NEAKCEPTOVATELNÉ
Modifikace	3	3	2	1	vypracování návodů	15 000 Kč	1.2.2014	2.2.2014	18	VELMI_NÍZKÉ	
Sdílení	5	4	2	4	odpovědný poskytovate	5 000 Kč	3.4.2014	4.5.2014	40	STŘEDNÍ	NEAKCEPTOVATELNÉ
Modifikace	4	2	3	5	školení	50 000 Kč	1.1.2014	6.7.2014	24	NÍZKÉ	
Akceptace	5	5	1	4	Riziko akceptováno				25	NÍZKÉ	RIZIKO SCHVÁLENO
Akceptace	4	2	3	2	Riziko akceptováno				24	NÍZKÉ	RIZIKO SCHVÁLENO
Modifikace		5		2	instalace firewallu		2.2.2015	2.2.2018			
Akceptace	5			4	Riziko akceptováno				0	NEPATRNÉ	RIZIKO SCHVÁLENO

Obrázek 12 Tabulka výsledných údajů

Nástroj umožnuje archivaci všech ošetřených rizik. Toto je nutné pro další monitorování a přezkoumávání kritérií hodnocení těchto rizik, aktiv, hrozeb opatření a zranitelností.

5.2 Měření efektivity

Při určování efektivity je překážkou skutečnost, individuálního přístupu k různým druhům informací, které jsou při procesu řízení rizik bezpečnosti informací generovány. Vlivem individuálního přístupu dochází k individuálnímu vyhodnocení dat a tedy následně i efektivnosti. Toto lze prezentovat na skutečnosti, že pro majitele je mnohem důležitější efektivnost jeho podniku a pro zaměstnance je zase mnohem důležitější, mít informace umožňující řízení svého oddělení a plnění svých povinností.

Pro vyhodnocování efektivnosti je tedy stanovit určité parametry, ukazatele, či metriky, dle kterých bude následné hodnocení vypadat.

Tyto ukazatele lze diverzifikovat na finanční ukazatele, kde parametry může být návratnost investic a na ukazatele nefinančního charakteru.

V navrhnutém nástroji je měřena efektivnost na základě těchto parametrů:

- Procentní vyjádření četnosti jednotlivých úrovní rizik před ošetřením a Procentní vyjádření četnosti jednotlivých úrovní rizik po ošetření viz obrázek č.

Vyjádření efektivity zvhledem k četnosti úrovní rizik před ošetřením a po ošetření

PŘED	ČETNOST RIZIK	% VYJÁDŘENÍ
NEPATRNÉ	0	0,0%
VELMI_NÍZKÉ	2	25,0%
NÍZKÉ	2	25,0%
STŘEDNÍ	2	25,0%
VYSOKÉ	1	12,5%
KRITICKÉ	1	12,5%

PO	ČETNOST RIZIK	% VYJÁDŘENÍ
NEPATRNÉ	1	14,3%
VELMI_NÍZKÉ	1	14,3%
NÍZKÉ	3	42,9%
STŘEDNÍ	2	28,6%
VYSOKÉ	0	0,0%
KRITICKÉ	0	0,0%

vlivem implementace zvolených opatření	
DOŠLO k NÁRŮSTU o	14,3%
DOŠLO k POKLESU o	10,7%
DOŠLO k NÁRŮSTU o	17,9%
DOŠLO k NÁRŮSTU o	3,6%
NEDOŠLO KE ZMĚNĚ	12,5%
NEDOŠLO KE ZMĚNĚ	12,5%

Obrázek 13 Tabulka pro výpočet efektivnosti

- Procentní vyjádření dodržování termínů při implementaci navrhnutých ošetření

Vyjádření efektivity zvhledem k dodržování termínů ukončení procesu implementace přijatých opatření v procesu řízení rizik

ukončení implementace opatření	počet	%
termín ukončení překročen	3	60,00%
termín dodržen	2	40,00%

data jsou čerpána z tabulky ACHRIVACE

Obrázek 14 Tabulka výpočtu efektivnosti

- Procentní vyjádření vynaložených nákladů ošetření na příslušná rizika

Vyjádření efektivnosti vynaložených nákladů na příslušná opatření za skutečnosti vzniku bezpečnostního incidentu

Ošetření	náklady na ošetření	Aktivum	Hodnota Aktiva (kvantitativní)	počet incidentů	Efektivnost opatření
vystužení vodovodu	20 000 Kč	Systémová dokumentace	450 000 Kč	1	96%
vypracování návodů	15 000 Kč	Datové soubory	300 000 Kč		
odpovědný poskytovatel	5 000 Kč	Databáze	500 000 Kč	1	99%
školení	50 000 Kč	Smlouvy	750 000 Kč		
Riziko akceptováno		Databáze	500 000 Kč		
Riziko akceptováno		Klimatizace	470 000 Kč		
instalace firewallu					
Riziko akceptováno					

data jsou čerpána z tabulky ACHRIVACE

pokud nastane incident, je doplněn k příslušnému riziku v této tabulce

za tohoto faktu dojde v této tabulce k výpočtu

Obrázek 15 Tabulka výpočtu efektivnosti

ZÁVĚR

Zadáním této práce bylo seznámení se s problematikou systémů řízení bezpečnosti informací a řízení rizik. Dále bylo nutno vypracovat analýzu požadavků na systém řízení rizik a navrhnout nástroj pro řízení rizik a měření efektivnosti.

Problematice systémů řízení rizik bezpečnosti informací je věnován úvod této práce. Jsou zde prezentovány základní charakteristiky systémů řízení bezpečnosti informací (ISMS) a řízení rizik. Jsou zde popsány základní kroky cyklu PDCA, který je základním nástrojem pro implementaci všech požadavků kladených v normě ČSN ISO/IEC 27001. Dále jsou zde popsány výhody certifikace dle výše zmíněné normy a možné komplikace a nedostatky při procesu jejího zavádění v organizaci. Další část práce je věnována komplexnímu popisu procesu řízení rizik. V úvodu jsou také charakterizovány normy rodiny ČSN IS/IEC 27000.

V závěru je stručně charakterizován nástroj, který byl vytvořen v rámci zadání této práce. K realizaci tohoto nástroje byl využit program Microsoft Office Excel 2010. Nástroj prezentuje systém a následnost všech dílčích kroků při procesu řízení rizik. Nástroj je doplněn o nápovědu, která se nachází na každém listě. Nápověda poskytuje uživateli informace nejen o postupu při ovládání a vyplňování jednotlivých tabulek, ale také informace doplňujícího charakteru, které jsou převzaty z normy ČSN ISO/IEC 27005. Součástí tohoto nástroje já nástroj pro měření efektivnosti. V rámci prezentování principu měření efektivnosti, byly stanoveny vzorová kritéria její hodnocení. Tento nástroj společně s teorií uvedenou v úvodní části této práce tvoří ucelený pohled na systémy řízení bezpečnosti informací, které v dnešní době nabývají stále větší váhy, jelikož hodnota informací stále vzrůstá a nebezpečí jejich zneužití taktéž.

Použitá literatura

[1] DOUCEK, Petr a Luděk NOVÁK. Systém řízení bezpečnosti informací: mezinárodní normy a zkušenosti z praxe. In: [online]. W. Churchilla 4, 130 67 Praha 3. Španělská 2, 120 00 Praha 2 [cit. 2014-01-13]. Dostupné z: „http://si.vse.cz/archive/proceedings/2009/system-rizeni-bezpecnosti-informaci-mezinarodni-normy-a-zkusenosti-z-praxe.pdf“

[2] ČSN ISO/IEC 27001. Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky. Praha : Český normalizační institut, 2006. 35 s.

[3] Nová řada ISO/IEC 27000 [online].Risk Analysis Consultants, 2009 [cit. 2014-03-27]. Dostupné z WWW: <http://www.rac.cz/rac/homepage.nsf/CZ/ISO27000>.

[4] Vlastní cesta [online]. 14.10.2007. [cit. 2014-03-21]. Dostupné z: http://www.vlastnicesta.cz/clanky/system-managementu-jakosti-iso-9001-2000/

[5]]Www.iso.org. [online]. [cit. 2014-03-21]. Dostupné z: http://www.iso.org/iso/catalogue_detail?csnumber=31807)

[6] ČSN ISO 27005. Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací. Praha: Český normalizační institut, 2013.

[7] ČSN ISO/IEC 27002:2006, Informační technologie – Soubor postupů pro management bezpečnosti informací. Praha.

[8] DOMINIK, Vlastimil. Http://www.management-consulting.cz [online]. Neratovice [cit. 2014-03-22]. Dostupné z:http://www.management-consulting.cz/cz/procesni-rizeni

.[9] PROCHÁZKA, Jaroslav. Procesní řízení realizace projektů. Ostrava, 2006. Dostupné z:http://www1.osu.cz/~prochazka/rpri/skripta_ProcesniRizeniProjektu.pdf. Určeno pro další vzdělávání pracovníků výzkumu a vývoje.

[10] ING, JAŠEK, Jiří. Http://www.arisys.cz. [online]. [cit. 2014-03-22].Dostupnéz: http://www.arisys.cz/inpage/isrpro3/

[11] http://si.vse.cz/archive/proceedingsautor Souček Petr [cit. 2014-03-22]. /2009/system-rizeni-bezpecnosti-informaci-mezinarodni-normy-a-zkusenosti-z-praxe.pdf

[12] MERNA, Tony. Risk management: řízení rizika ve firmě. Vyd. 1. Brno: Computer Press, c2007, xii, 194 s. ISBN 978-80-251-1547-3.

[13] PROCHÁZKOVÁ, Dana. *Metody, nástroje a techniky pro rizikové inženýrství: Vydalo České vysoké učení technické v Praze*. 1. vyd. Praha: Karolinum, 2011, s. 248-251.

ISBN 978-80-01-04842-9.

[14]SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích: 3., rozšířené a aktualizované vydání*. 3806. publikace. U Průhonu 22, 170 00 Praha7: Grada Publishing a.s., 2010. ISBN 978-80-247-3051-6.

Seznam obrázků

Seznam příloh

Přílohy

Příloha 1x CD

Příloha 1. Tabulka norem ČSN/IEC 27000

OZNAČENÍ	DATUM VYDANÍ	NÁZEV	CHARAKTERISTIKA
ISO/IEC 27000	2014	*IT - Security techniques - Information security management systems - Overview and vocabulary*	Tato norma obsahuje definici pojmů a terminologický slovník pro další normy z této série.
ISO/IEC 27001 (BS7799-2)	2013	*ITy – Security techniques – Information security management systems – Requirements*	Je hlavní normou pro Systém řízení bezpečnosti informací (ISMS), dříve byla známá jako BS7799 část 2, podle které jsou systémy certifikovány.
ISO/IEC 27002	2013	IT - Security techniques - Code of practice for information security management	Je mezinárodně přijatý standard, respektive sbírka nejlepších praktik z oblasti bezpečnosti informací.
ISO/IEC 27003	2010	*IT - Security techniques - Information security management system implementation guidance*	Norma obsahuje především návod k implementaci ostatních norem série 27000 a je určena k využití ve všech typech organizací, které mají v úmyslu zavést systém řízení bezpečnosti informací (ISMS) dle ISO/IEC 27001.
ISO/IEC 27004	2009	*IT - Security techniques - Information security management - Measurement*	Tato norma je pro organizace pomůckou k měření a prezentaci efektivity jejich systémů řízení bezpečnosti informací (ISMS), zahrnující řídící procesy definované v ISO/IEC 27001 a opatření z ISO/IEC 27002
ISO/IEC 27005	2011 (druhá verze)	*Information technology - Security techniques - Information security risk management*	Norma poskytuje doporučení a techniky pro analýzy informačních rizik. Jejím základem jsou revize dříve vydaných norem ISO/IEC TR 13335-3:1998, ISO/IEC TR 13335-4:2000 a využití některých pasáží BS 7799-3.

ISO/IEC 27006	2011 (druhá verze)	*IT – Security techniques – Requirements for bodies providing audit and certification of information security management systems*	Norma specifikuje požadavky a poskytuje doporučení pro orgány provádějící audit a certifikaci systému řízení bezpečnosti informací (ISMS).
ISO/IEC 27007	2011	*IT - Security techniques - Guidelines for Information security management systems auditing*	Norma obsahuje doporučení k provádění auditů ISMS podle ISO/IEC 27001.
ISO/IEC 27008	2011	*IT - Security techniques - Guidance for auditors on ISMS controls*	Tato norma doplňuje normu ISO/IEC 27007 o "technický audit". Norma dále obsahuje doporučení pro auditory, kteří kontrolují implementovaná ISMS opatření vycházející z ISO/IEC 27002. . Norma je vydána jako spíše jako "technical report" než plnohodnotný mezinárodní standard.
ISO/IEC 27010	2012	*IT— Security techniques — Information security management for inter-sector and inter-organisational communications*	Tato norma poskytuje doporučení ohledně sdílení informací mezi organizacemi a/nebo státy, které spadají do „kritické infrastruktury“. Jedná se například o informace týkající se bezpečnostních rizik, opatření, problémů a/nebo incidentů.
ISO/IEC 27011	2008	*IT - Security techniques - Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*	Je primárně určena pro zavádění ISMS u telekomunikačních operátorů.
ISO/IEC 27013	2012	*IT Security - Security techniques - Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1*	Tato norma poskytuje doporučení pro realizaci jednotné informační bezpečnosti a systému pro řízení IT služeb, založené na standardech ISO/IEC 27001:2005 (ISMS)
ISO/IEC 27014	2013	*Information technology — Security techniques — Governance of information security*	Norma organizacím poskytuje doporučení při návrhu Information Security Governance.

ISO/IEC 27015	2012	*Information technology — Security techniques — Information security management guidelines for financial services*	Obsahuje doporučení a požadavky na řízení bezpečnosti informací v prostředí finančních institucí (banky, pojišťovny apod.).
ISO/IEC 27016	2014	*IT Security — Security techniques — Information security management – Organizational economics*	Tato norma byla publikována jako technická zpráva a obsahuje doporučení pro nastavení bezpečnostního programu s ohledem na předpokládané finanční výsledky.
ISO/IEC 27019	2013	*IT— Security techniques — Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy industry*	Tato norma byla publikována jako technická zpráva a napomáhá organizacím v energetickém průmyslu interpretovat a aplikovat normu ISO/IEC 27002, aby byla zajištěna bezpečnost jejich systémů pro elektronické řízení procesů.
ISO/IEC 27031	2011	*IT — Security techniques — Guidelines for information and communications technology readiness for business continuity*	Obsahuje doporučení pro zajištění kontinuity činností organizace (business continuity)
ISO/IEC 27035	2011	*IT incident management*	Tato norma se věnuje řízení incidentů bezpečnosti informací.
ISO/IEC 27037	2012	*IT — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence*	Norma obsahuje doporučení pro zjišťování, sběr, získávání a uchovávání digitálních důkazů
ISO/IEC 27038	2014	*IT — Security techniques — Specification for digital redaction*	Norma obsahuje doporučení pro publikování digitálních dokumentů.