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: **2013/2014**

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: **6. června 2014**

Termín odevzdání diplomové práce: **25. srpna 2014**

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

L.S.

Doc. Ing. Vlastimil Skočil, CSc.
vedoucí katedry

V Plzni dne 14. října 2013

Anotace

Předkládaná diplomová práce je věnována problematice systémů řízení bezpečnosti informací (ISMS), systému řízení rizik a měření efektivity. Úvodní část práce je zaměřena na charakteristiku systémů řízení bezpečnosti informací a popisu jejich základních atributů, následně je provedena analýza požadavků doplněna o charakteristiku řízení rizik a měření efektivity. Na základě této analýzy je v závěru práce navržen a realizován nástroj pro řízení rizik a měření efektivity.

Klíčová slova

Systémy řízení bezpečnosti informací, ISMS, řízení rizik

Abstract

This master thesis is focused to the issue of information security management systems (ISMS), risk management and measurement of effectiveness. The first part is focused on the characteristics of information security management systems and also describe their basic attributes, then the analysis is supplemented by requirements on the characteristics of risk management and measurement of effectiveness. Based on this analysis, the present work is designed and implemented a risk management tool and measuring effectiveness.

.
.
.
.
.
.
.
.

Key words

Information security management system, ISMS, risk management

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 : 25.8. 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 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.

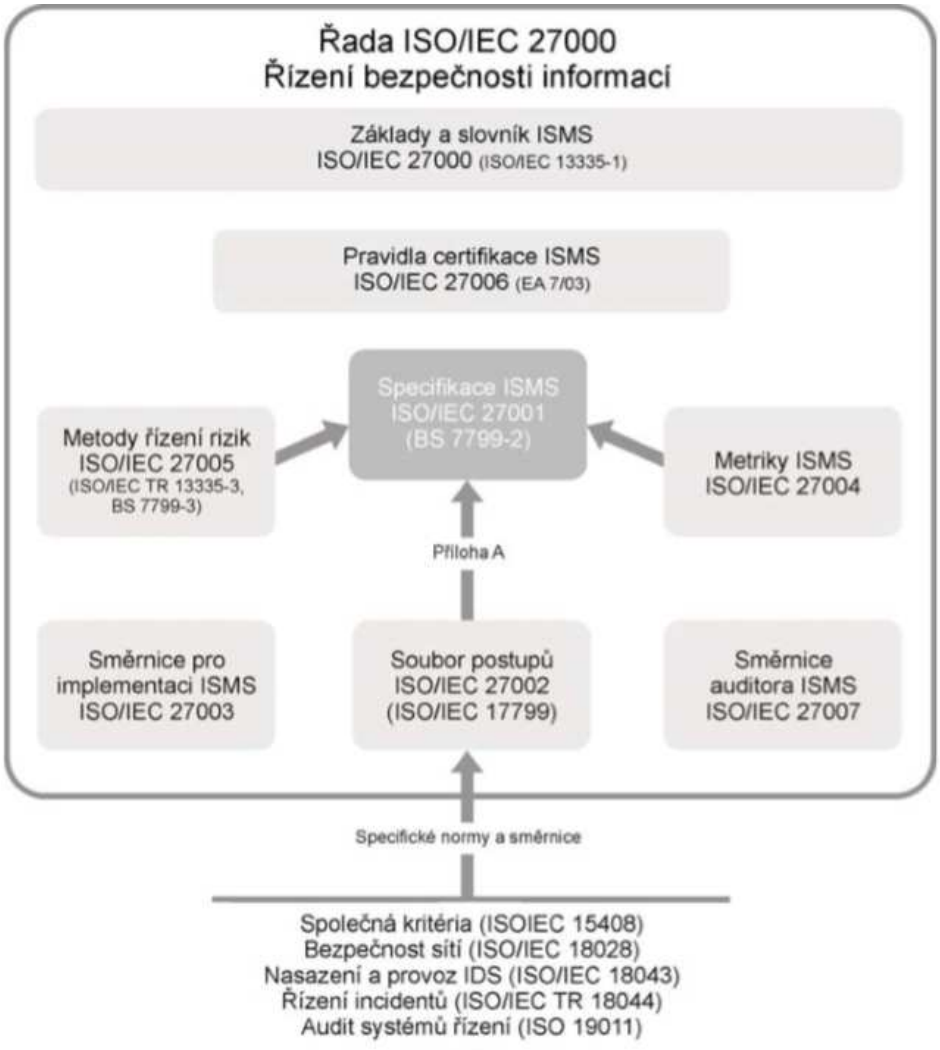
Pokrokově uvažující organizace si plně uvědomují nutnost ochrany informací a zvládnutí strategie řízení rizik.

Receptem pro zvládnutí strategie řízení rizik je pro organizaci implementace systémů řízení bezpečnosti informací. Implementací všech požadavků uvedených v normě ČSN ISO/IEC 27001 může organizace dosáhnout minimalizace možnosti ztráty kvality informace. 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 ISMS a řízení rizik. Jsou zde charakterizovány základní stavební pilíře a procesy. Výstupem této práce je navržený nástroj pro řízení rizik a měření efektivity.

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), jednotlivé kroky PDCA cyklu jsou charakterizovány v kapitole 2. 2. této práce. 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 ČSN ISO/IEC 27001

(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 2006 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. **[2]**

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 kvality a podle této normy probíhají také certifikace systému kvality primárním přínosem této normy je procesní přístup.

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.

Přínosy certifikace dle ČSN ISO/IEC 27001

- 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 **[3]**

1.2 ČSN ISO/IEC 27002

Normu tvoří sbírka nejlepších bezpečnostních praktik, norma byla prvně vydána v červnu roku 2005 pod názvem ISO/IEC 17799. Později došlo ke změně názvu a to na normu ČSN ISO/IEC 27002:2005.

Aktuální verze normy "ISO/IEC 27002:2013 Information technology - Security techniques - Code of practice for information security management"Tato norma obsahuje 14 primárních oddílů kde je definováno 35 cílů opatření. Tyto cíle opatření jsou implementována za účelem ochrany informačních aktiv proti narušení jejich kvality. Je tedy cílem zaručit

jejich důvěrnost, dostupnost a integritu. Tato norma je koncipována tak, aby bylo možné implementovat zde uvedená doporučení, která slouží pouze jako předloha a je možné si je konkrétněji dolaďovat a to v přímé závislosti na požadavcích organizace, do jakékoliv organizace. Respektive do jakéhokoliv typu organizace a do jakkoliv velké organizace.

Obsahem této normy ČSO/IEC 27002 je také soubor nejlepších praktik pro zajištění bezpečnosti informací. Tyto praktiky jsou zde popsány a organizace by je měla vzít v úvahu pro zajištění kontrolních cílů. Nová verze této normy obsahuje 114 "základních" opatření (v předchozí verzi normy z roku 2005 to bylo těchto opatření 133), které se, ale ve skutečnosti dále rozkládají na stovky specifických bezpečnostních opatření, protože je možné pro splnění jednoho bodu navrhnout více opatření.

Norma není rozkazovacího charakteru. Volbu opatření zcela ponechává v kompetenci organizace. Cílem není implementovat vše, co norma uvádí, nýbrž jen ta vhodná opatření, která byla zvolena na základě hodnocení rizik a ta opatření, která je možno v konkrétní situaci implementovat. Tato normou poskytnutá flexibilita při implementaci může mít ale také negativní účinek a to přesně v momentu kdy organizace podstoupí proces certifikace dle normy ČSN ISO/IEC 27001. Může totiž docházet k problémům při vyhodnocování, zdali jsou zvolená bezpečnostní opatření plně v souladu s normou.

1.3 ČSN ISO/IEC 27004

Obsah normy ČSN ISO/IEC 27004 je reakcí na požadavky provádění pravidelných přezkumů účinnosti ISMS a měření účinnosti zavedených opatření za účelem ověření, zda jsou definované bezpečnostní požadavky v organizaci naplněny. Tyto požadavky jsou uvedené v normě ČSN ISO/IEC 27001. Doporučení v normě obsažená jsou zaměřena na úzkou a specifickou oblast vývoje a využívání metrik.

Implementace těchto doporučení je předmětem programu měření bezpečnosti informací. Program měření bezpečnosti informací napomáhá vedení organizace při identifikaci a vyhodnocení nevyhovujících a neúčinných procesů a opatření ISMS a při stanovení priorit činností spojených se zlepšováním nebo změnou těchto procesů anebo opatření.

Tato norma předpokládá, že výchozím bodem je pro rozvoj metrik a měření je dobré porozumění rizikům, kterým organizace čelí a že činnosti hodnocení rizik organizace byly provedeny správně. (tj na základě ISO/IEC 27005, jak to vyžaduje ČSN ISO/IEC 27001)

Měření probíhá za účelem hodnocení účinnosti zavedeného systému řízení bezpečnosti informací (ISMS) a také účinnosti opatření nebo skupin opatření jak je uvedeno v normě ČSN ISO/IEC 27001. Doporučení se týkají politiky, řízení rizik bezpečnosti informací, cílů opatření a procesů.

1.4 ČSN ISO/IEC 27005

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.) [6]

2 Systémy řízení bezpečnosti informací

2.1 Charakteristika ISMS

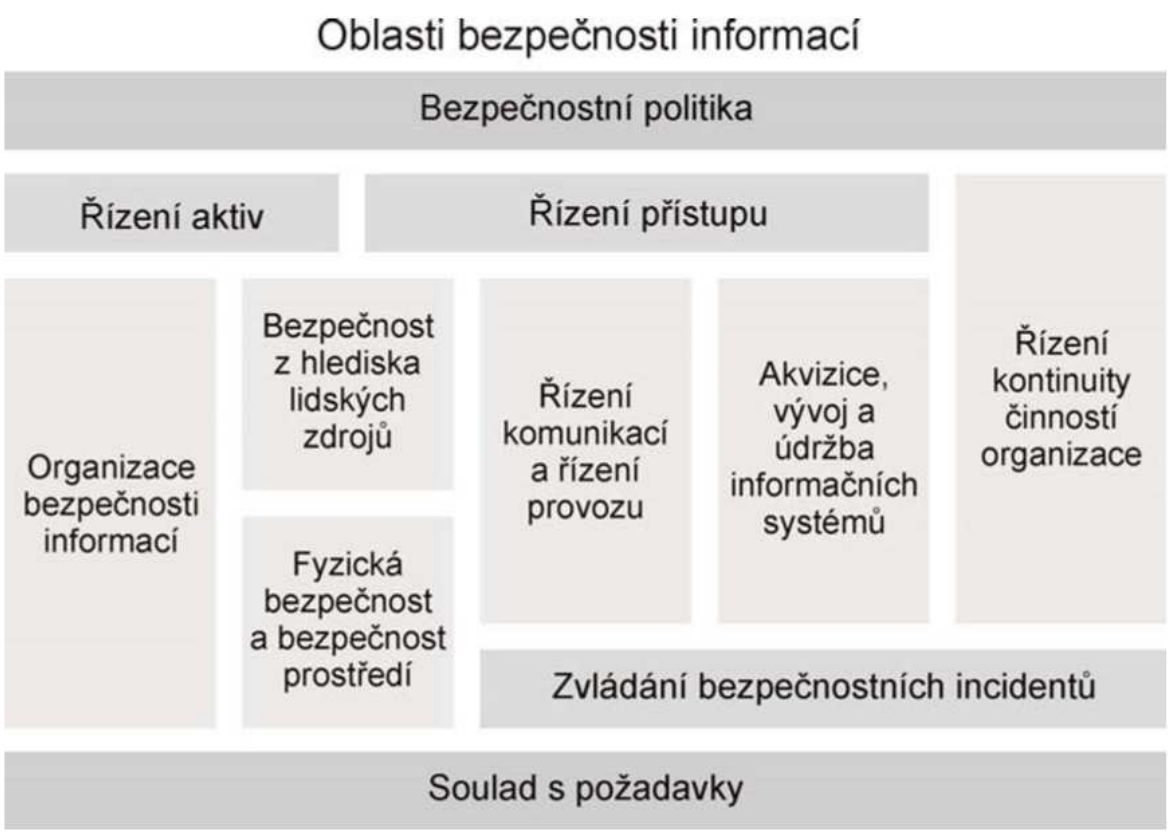
Se současným prudkým rozvojem informačních technologií, které urychlují pokrok a usnadňují práci dílčím uživatelům IS, je spojena i oblast počítačové kriminality, která vykazuje stejný dynamický rozvoj. Pokud se rozvíjí tato oblast je adekvátní a pochopitelná potřeba rozvíjení i oblasti ochrany. Podle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



Obrázek 2. Oblasti bezpečnosti informací dle normy ČSN ISO/IEC 27002 [7]

Jelikož implementace ISMS uplatňuje tzv. procesní přístup řízení, 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, proces 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)
    - o 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

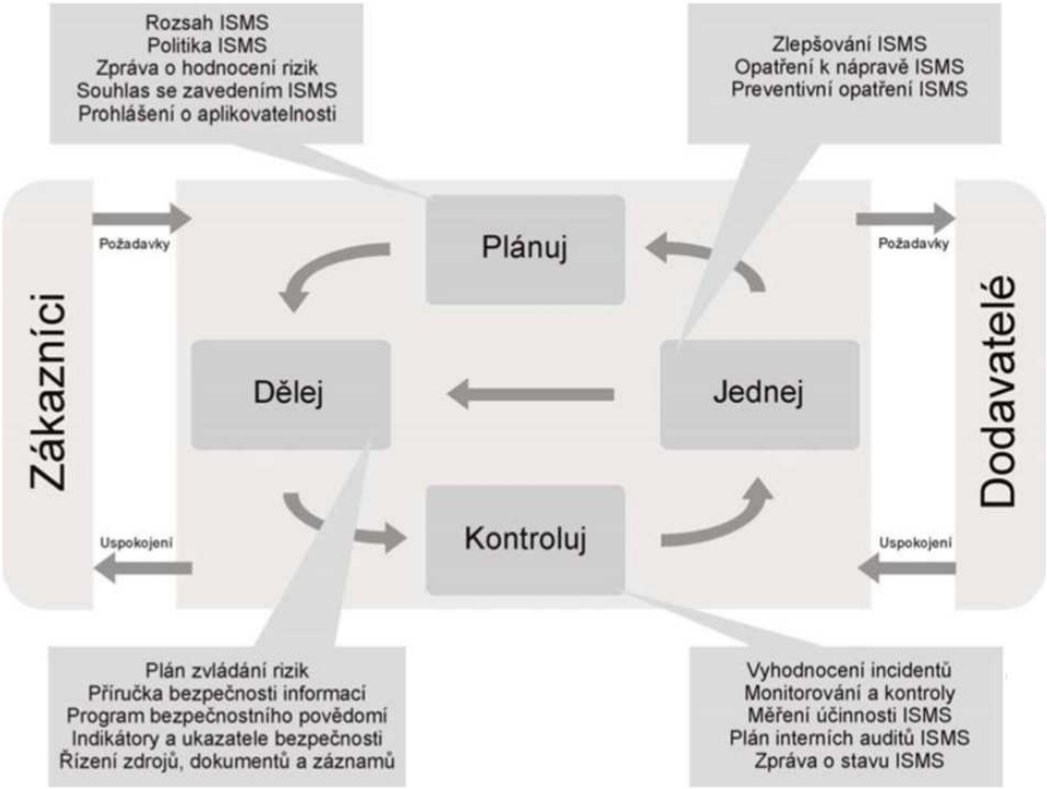
    - o Každá činnost je započata a ukončena konkrétní událostí. To umožnuje sledovat tyto činnosti nejen jako jeden celek, ale také konkrétní výskyty těchto činností a to v reálném čase. Tímto je umožněna realizace řízení

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



Obrázek 3. 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
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 a pro 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 je tedy 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]

2.3 Problematika implementace systémů řízení bezpečnosti informací

Při procesu implementace systémů ISMS dochází k řadě komplikací. Přesto, že organizace postupuje dle požadavků uvedených v normě ČSN ISO/IEC 27001a snaží se pro zjednodušení procesu dodržovat požadavky uvedené v normách: ČSN ISO/IEC 27002, ČSN ISO/IEC 27004, ČSN ISO/IEC 27005 je cesta implementace ISMS spojena s četným množstvím možností jak sejít z cesty úspěšné implementaci ISMS. Zde jsou uvedeny některé možné komplikace, kterých se může organizace dopustit při procesu implementace ISMS.

- **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 chce 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. **[11]**

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 Analýza požadavků na systém řízení rizik

3.1 Požadavky na ISMS dle normy ČSN ISO/IEC 27001

Tyto požadavky jsou rozděleny do následujících subkapitol:

a) Ustavení

1. Určit rozsah a hranice ISMS

   Toto lze učinit na základě posouzení a zvážení činností organizace, upořádáním její struktury, umístění, aktiv a také technologií, které využívá.

2. Definovat politiku ISMS

   Při procesu určování a definování politiky je nutné zahrnout: rámec pro stanovení cílů, nutnost respektovat požadavky a to zákonné, regulatorní a také požadavky (závazky) plynoucí ze smluv týkajících se bezpečnosti. Dále je nutné stanovit kritéria, kterými bude hodnoceno riziko, Tyto všechny výše uvedené části musí zvolená politika akceptovat a obsahovat. J nutné, aby politiku schválilo vedení organizace.

Tyto požadavky je splněny normou ČSN ISO/IEC 27005 a to při procesu Stanovení kontextu (tento proces je charakterizován v kapitole 3.1.1. –A této práce)

3. Stanovit přístup k hodnocení rizik

   Identifikovat metodiku hodnocení rizik (výsledky hodnocení musí být porovnatelné a reprodukovatelné, za tímto účelem je možné využít normu ISO/IEC TR

13335-3, která obsahuje soubor těchto metodik. Je nutné vytvořit kritéria akceptovatelnosti a také kritéria pro identifikaci akceptačních úrovní.

4. Identifikovat rizika
    - Identifikovat aktiva a to v rámci ISMS a také vlastníky aktiv
    - Identifikovat hrozby pro aktiva
    - Zranitelnosti
    - Dopady za ztráty důvěrnosti, integrity a dostupnosti

5. Analyzovat a vyhodnocovat rizika

   Zde je nutné:
    - jaké by to mělo dopady na činnost společnosti, kdyby byla napadena aktiva.
    - Posoudit reálnou pravděpodobnost selhání bezpečnosti při existenci hrozeb, zranitelností a dopadů na konkrétní aktiva za stávajících/zavedených opatření.
    - odhadnout úroveň rizika + určit zda jsou rizika akceptovatelná, nebo vyžadují zvládání podle kritérií o akceptovatelnosti

6. identifikovat a vyhodnotit varianty pro zvládání rizik
    - -aplikace vhodných opatření

Tento požadavky (3,4,5,6) jsou splněny normou ČSN ISO/IEC 27005 při procesu Hodnocení rizik (tento proces je charakterizován v kapitole 3.1.1. –B.1,2,3 této práce)

7. vybrat cíle opatření a jednotlivá bezpečnostní opatření pro zvládání rizik
8. souhlas vedení
9. prohlášení/ protokol o aplikovatelnosti

b) Zavedení

1. Formulovat a zavést plán zvládání rizik
    - Ten vymezí činnosti vedení, určí zdroje, které budou pro dané činnosti vyhrazeny a také rozdělí odpovědnosti

2. Zavést plán zvládání rizik
3. Zavést bezpečnostní opatření

Pro splnění tohoto požadavku lze využít normy ČSN ISO/IEC 27003 nad rámec této práce

Organizace musí přijmout příslušná opatření pro odstranění nedostatků spojených s implementací a provozem ISMS, aby zabránila jejich opětovnému výskytu. Zdokumentované postupy nápravných opatření musí definovat požadavky na identifikaci nesouladu v zavedení, nebo provozu ISMS.

Dle normy ČSN ISO/IEC 27001 je doporučen následující postup:

- Určení příčin nesouladu
- Vyhodnocení potřeby opatření, kterým se zajistí, že se nesoulad znovu nevyskytne
- Určení a zavedení potřebných opatření k nápravě
- Zaznamenání výsledků přijatých opatření
- Přezkoumání přijatých opatření k nápravě
- Určit měřítka efektivnosti zvolených opatření

  Tedy zvolit způsob měření účinnosti vybraných opatření a stanovit jakým způsobem budou tato měření použita k vyhodnocení účinnosti opatření tak, aby závěry byly porovnatelné a reprodukovatelné. Cílem je získat informace říkající, která jednotlivá opatření splňují plánované cíle opatření.
- Zavést programy školení a programy zvyšování bezpečnostního povědomí
- Řídit provoz ISMS a zdroje ISMS

c) Monitorování a přezkoumávání

Vedení organizace musí provádět přezkoumání ISMS organizace v plánovaných intervalech (alespoň jednou za rok), aby zjistilo jeho permanentní přiměřenost, adekvátnost a účinnost. Tato přezkoumání musí také hodnotit možnosti zlepšení a potřebu změn v ISMS, včetně bezpečnostní politiky a cílů bezpečnosti. Výsledky musí být jasně zdokumentovány a musí být o nich udržovány záznamy.

Organizace musí neustále zvyšovat účinnosti ISMS s využitím politiky bezpečnosti informací, cílů bezpečnosti informací, výsledků auditů, analýz, monitorovaných událostí, nápravných a preventivních opatření a přezkoumání prováděných vedením organizace.

V normě ČSN ISO/IEC 27001 jsou uvedeny tyto úkony:

1. Monitorovat a přezkoumávat a zavést další opatření:
    a. Pro včasnou detekci chyb zpracování
    b. Pro včasnou identifikaci úspěšných i neúspěšných pokusů o narušení bezpečnosti a detekci bezpečnostních incidentů
    c. Která umožní vedení organizace určit, zda bezpečnostní aktivity prováděné pověřenými osobami nebo implementace opatření fungují dle očekávání
    d. Umožní detekci bezpečnostní události a zamezí vzniku bezpečnostního incidentu
2. Pravidelně přezkoumávat účinnost ISMS
3. Měřit účinnost zavedených opatření pro ověření toho, že byly naplněny požadavky na bezpečnost

Tento požadavek je splněn normou ČSN ISO/IEC 27004 (kapitola 3.2 této práce)

4. V plánovaných intervalech provádět přezkoumání hodnocení rizik a přezkoumání úrovní zbytkových rizik a úrovní akceptovatelnosti rizik
5. Provádět interní audity ISMS
6. Na úrovni vedení organizace přezkoumávat ISMS (kontrola rozsahu a detekce dalších možných zlepšení)
7. Aktualizovat bezpečnostní plány

d) Udržování a zlepšování

1. Zavádět identifikované možnosti vylepšení ISMS

2. Provádět odpovídající nápravná opatření a preventivní činnosti s využitím svých zkušeností, či zkušeností jiných organizací
3. Projednávat činnosti a návrhy na zlepšení
4. Dosáhnout předpokládaných cílů

V normě ČSN ISO/IEC 27001 je taktéž uveden požadavek na vedení organizace, které by mělo převzít odpovědnost za implementaci systému ISMS a za jeho udržování.
V normě je uvedeno, že vedení organizace musí, poskytnou důkazy o své vůli k ustanovení, zavedení, provozu, monitorování, přezkoumání, udržování a zlepšování ISMS a to tak že:

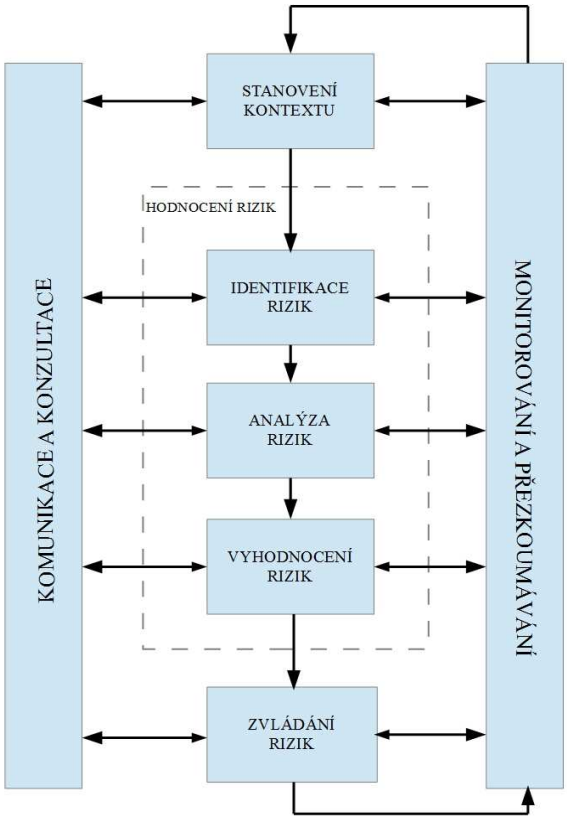
- Ustanoví politiku ISMS
- Zajistí stanovení cílů ISMS a plánu jejich dosažení
- Stanoví role povinnosti a odpovědnosti v oblasti bezpečnosti informací
- Propaguje v rámci organizace význam plnění cílů bezpečnosti informací, jejich souladu s politikou bezpečnosti informací
- Zajistí dostateční zdroje pro ustanovení, zavedení, provozu, monitorování, přezkoumání, udržování a zlepšování ISMS
- Stanoví svým rozhodnutím kritéria pro akceptaci rizik a akceptovatelnou úroveň rizika
- Zajistí provádění interních auditů ISMS
- Provede přezkoumání ISMS

V této kapitole jsou sepsány a popsány jednotlivé požadavky uvedené v normě ČSN ISO/IEC 27001. K těmto jednotlivým požadavkům jsou přiřazeny normy ČSN ISO/IEC 27005 a ČSN ISO/IEC 27004, které umožnují plnění těchto požadavků. Normy ČSN ISO/IEC 27005 a ČSN ISO/IEC 27004 jsou z tohoto důvodu podrobně charakterizovány v následujících kapitolách a je věnována pozornost jejich konceptu a jejich požadavkům, které je nutno splnit v rámci těchto jednotlivých norem.

3.2 Analýza normy ČSN ISO/IEC 27005 (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,



Obrázek 4. Proces řízení rizik [6]

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.

Kroky PDCA cyklu	Jednotlivé procesy obsažené v jednotlivých krocích PDCA cyklu
PLÁNUJ	A. STANOVENÍ KONTEXTU 1. Stanovení kritérií pro hodnocení rizik 2. Stanovení kritérií dopadu 3. Stanovení kritérií pro akceptaci rizik
	B. HODNOCENÍ RIZIK 1. IDENTIFIKACE RIZIK • Identifikace aktiv • Identifikace hrozeb • Identifikace stávajících opatření • Identifikaci zranitelností • Identifikaci následků/dopadů 2. ANALÝZA RIZIK 3. VYHODNOCENÍ
	C. ZVLÁDÁNÍ RIZIK
DĚLEJ	D. Implementace plánu ošetření
KONTROLUJ	E. Kontinuální monitorování přezkoumávání rizik
JEDNEJ	F. Udržování a zlepšování procesu řízení rizik bezpečnosti informací

3.2.1 PLÁNUJ

A. STANOVENÍ KONTEXTU

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 kritérií, 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.

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. **[6]**

1. Stanovení kritérií 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.

2. Stanovení kritérií DOPADU

Sestavením kritérií dopadu organizace vytváří seznamy škod, které při nastalých bezpečnostních incidentech mohou nastat. 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. Stanovení kritérií 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)

B. HODNOCENÍ RIZIK

V tomto kroku dochází k identifikaci všech rizik. Tato identifikována rizika jsou následně ohodnocena dle kritérií stanovených v kroku stanovení kontextu. Aby rizika mohla být hodnocena musí být nejprve identifikována, poté musí být provedena analýza těchto identifikovaných rizik a následně provedeno jejich vyhodnocení.

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 , lze označit cokoliv co má pro organizaci 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.

2. 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

  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.

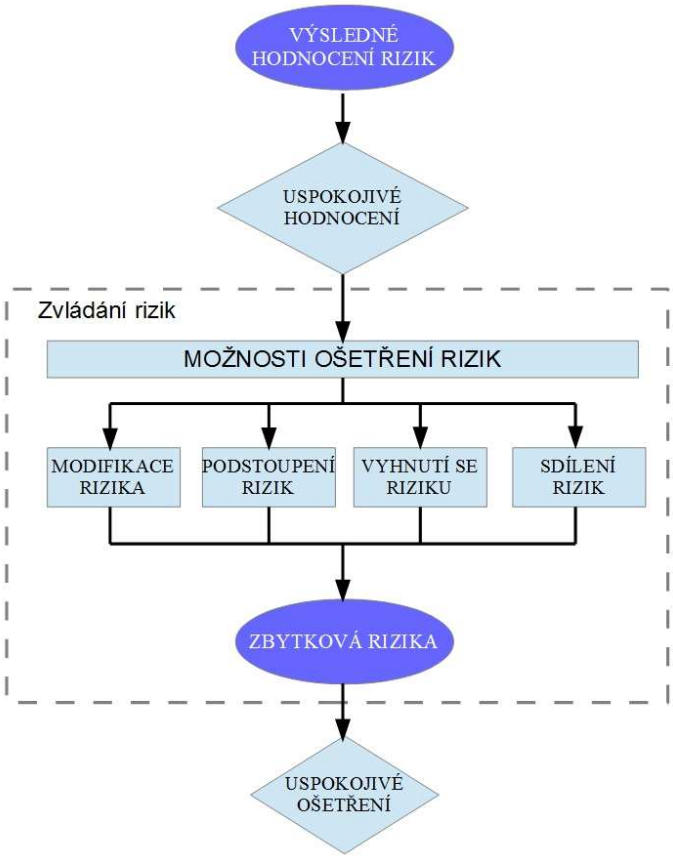
Kvalitativní metoda je v porovnání s kvantitativní metodou mnohem méně exaktní. Je časově méně náročná a není nutné díky její nenáročnosti na zpracování formalizovaného přístupu. Důsledkem toho je kvalitativní metoda vysoce subjektivní a data díky ní získaná mohou činit například při procesu zvládání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

3. VYHODNOCENÍ RIZIK

Při procesu vyhodnocení rizik 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).

C. 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.6. 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 5. Proces zvládání rizik [6]

Možnosti 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.

3.2.2 DĚLEJ

Obsahem tohoto procesu je:

- implementace plánu ošetření rizik. Respektive formulace plánu zvládání rizik, kde se vymezí činnosti vedení, určí se zdroje, které budou využity, Odpovědnosti A cíle kterých chce organizace dosáhnout.
- zavedení plánu zvládání rizik
- zvolit způsob měření účinnosti.

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.

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.

3.2.3 KONTROLUJ

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

3.2.4 JEDNEJ

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

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.

3.3 Analýza normy ČSN ISO/IEC 27004

Program měření bezpečnosti informací napomáhá organizaci poskytovat příslušným zainteresovaným stranám spolehlivé informace týkající se rizik bezpečnosti informací a stavu zavedeného ISMS k řízení těchto rizik. Tento program pokud funguje a je účinný zvyšuje důvěru zainteresovaných stran ve výsledky měření a umožnuje využití těchto metrik k uskutečňování neustálého zlepšování bezpečnosti informací a ISMS.

Norma 27001 vyžaduje, aby organizace prováděla pravidelné přezkoumávání účinnosti ISMS a brala přitom v úvahu výsledky měření účinnosti a měřila účinnost opatření, aby si ověřila, že požadavky na bezpečnost byly splněny. Dále vyžaduje, aby organizace definovala, jakým způsobem bude měřit účinnost vybraných opatření nebo skupin opatření a specifikovala, jak mají být tyto metriky použity pro vyhodnocení účinnosti opatření, aby závěry hodnocení byly porovnatelné a opakovatelné.

Zvolený přístup se bude lišit v závislosti na počtu významných faktorů včetně rizik bezpečnosti informací, kterým organizace čelí. Dále se bude lišit na základě její organizační velikosti, dostupných zdrojích, platných právních, regulačních a smluvních požadavcích. Výběr metody na měření požadavků normou je důležitý. Zamezení věnování nadbytečný

pozornosti činnostem a plýtvání zdroji na úkor jiných.

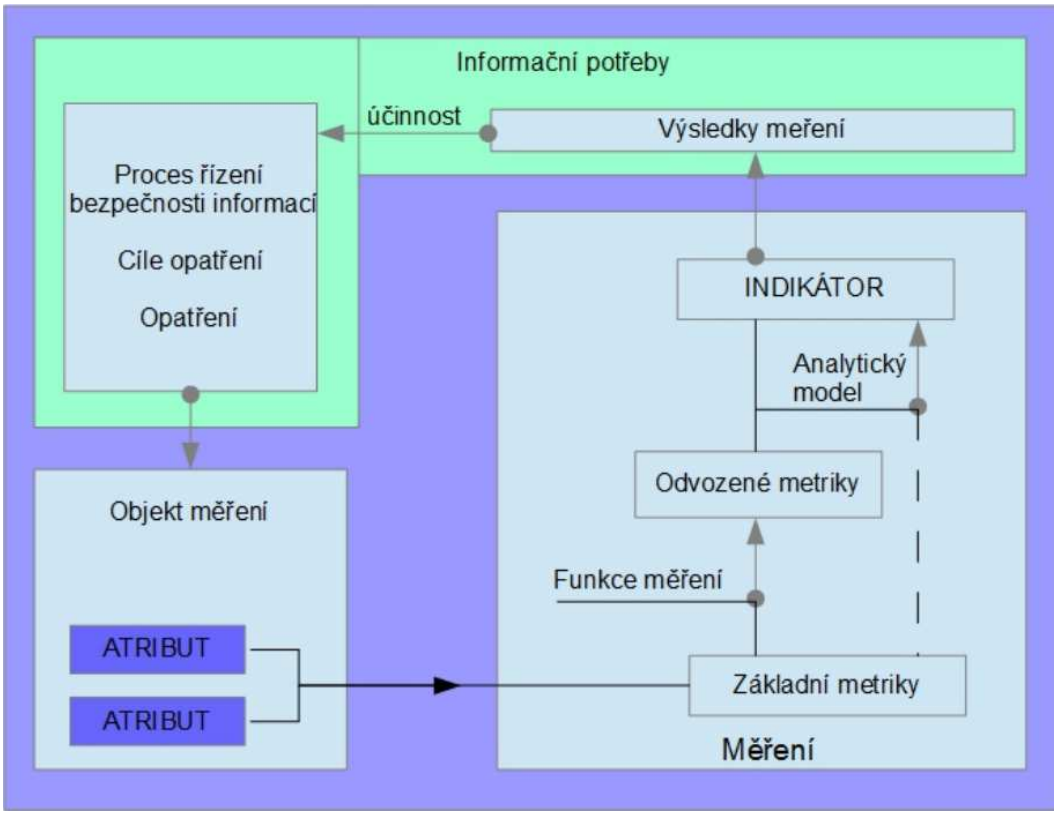
Velký faktor ovlivňující schopnost organizace provádět měření je její velikost. Obecně řečeno velikost a složitost podnikání v kombinaci s důležitostí bezpečnosti informací ovlivňují rozsah potřebného měření, jak z hlediska počtu metrik, které mají být vybrány tak z hlediska četnosti sběru analyzování dat. U malých organizací a středních je dostačující méně komplexní program měření bezpečnosti informací zatím co u velkých budou zavádět a provozovat četné programy pro měření bezpečnosti informací.(Pro malé organizace stačí jeden program měření bezpečnosti informací, velké potřebují několik programů měření.)

Doporučení, která poskytuje tato norma, povedou k vytvoření dokumentace, nastavení procesů měření bezpečnosti informací a jejich následné zlepšování. Vytvořená dokumentace, přispěje k prokázání toho, že účinnost opatření je měřena a hodnocena.

Norma ČSN ISO/IEC 27004 poskytuje základní doporučení pro naplnění požadavků měření, jak je specifikuje ISO/IEC 27001 a týkají se následujících činností:

- Vývoj metrik (základních odvozených, indikátorů)
- Sběru dat a analýzy dat
- Získání výsledků měření
- Sdělení získaných výsledků měření příslušným zainteresovaným stranám
- Použití výsledků měření jako faktorů přispívajících k rozhodnutím souvisejících s ISMS
- Použití výsledků měření k identifikaci pro zlepšování zavedeného ISMS včetně jeho rozsahu, politik cílů opatření procesů a postupů
- Napomáhání neustálému zlepšování programu měření bezpečnosti informací

Pro názornou prezentaci je přiložen (obr. č. 7.) model měření bezpečnosti informací, jehož dílčí části jsou charakterizovány v následujících odstavcích.



Obrázek 6. Model měření bezpečnosti informací [15]

Základní metrika

Základní metrika je nejjednodušší metrika, která může být získána. Základní metrika je vyvozena z využití metody měření, a to na atributy, které jsou u daného objektu měření vybrány. Pro objekt měření je běžné, že má mnoho atributů, ale pouze některé z nich mohou poskytnout užitečné hodnoty, které lze přiřadit k této metrice.

Metoda měření

Logická posloupnost operací použitá ke kvantitativnímu určení atributu s ohledem na stanovené měřítko. typ metody měření V závislosti na povaze operací, použitých ke kvantitativnímu určení atributu, rozlišujeme dva typy metod měření: Subjektivní, nebo kvantitativní určení zahrnuje lidské posouzení, objektivní: kvantitativní určení je založeno na numerických pravidlech např. takových jako sčítání.

Odvozená metrika

Odvozená metrika je soubor několika základních metrik. Tento soubor může obsahovat dvě či více základních metrik, přičemž daná základní metrika může být využita jako vstup právě pro několik odvozených metrik. Odvozená metrika je výsledkem procesu funkce měření.

Funkce měření

Funkce měření je proces, při kterém je za využití celé řady technik kombinováno několik základních metrik. Výsledkem tohoto procesu je právě odvozená metrika. Měřítko a jednotky užité u odvozené metriky je závislé na jednotkách a metrikách, které jsou uvedeny u základní metriky, ale také na způsobu jakou základní metriky kombinovány v procesu funkce měření.

Indikátor

Indikátor je metrika, která poskytuje odhad, či ohodnocení zvolených atributů získaných z analytického modelu s přihlédnutím na definovanou informační potřebu. Indikátory jsou získávány za využití analytického modelu pro určitou základní, či odvozenou metriku a jejich kombinací společně s rozhodovacími kritérii.

Analytický model

Algoritmus nebo výpočet kombinující jednu nebo více metrik a/nebo odvozených metrik s přidruženými rozhodovacími kritérii. Je založen na porozumění nebo na osvojení si očekávaných vztahů mezi základní a/nebo odvozenou metrikou a/nebo jejich chování v čase. Analytický model vytváří odhady a hodnocení, které se týkají definovaných informačních požadavků.

Objekt měření

Objekt (entita) který je charakterizován prostřednictvím měření svých atributů. Objekt může zahrnovat procesy, plány, projekty, zdroje a systémy nebo části systémů.

Atribut

Vlastnost nebo charakteristika objektu, která může být rozlišena lidskými nebo automatizovanými prostředky.

Výsledek měření

Výsledků měření je dosaženo interpretací použitých indikátorů, které jsou založeny na definovaných rozhodovacích kritériích. Tyto rozhodovací kritéria se používají k definování požadavku na samotnou činnost nebo další zkoumání, či k charakteristice úrovně důvěry v dané výsledky měření. Aplikovatelnost rozhodovacích kritérií je široká a lze je aplikovat na celou řadu indikátorů. [16]

3.4 Závěr

V úvodu této kapitoly byla provedena analýza požadavků dle normy ČSN ISO/IEC 27001. Požadavky byly uskupeny do čtyř podkapitol. Toto uskupení bylo provedeno v rámci dodržení rozdělení požadavků/ činností popsaných v kapitole 2.2 této práce, kde byly popsány obsahy jednotlivých kroků PDCA cyklu. V rámci této práce byly k analyzovaným požadavkům normy ČSN ISO/IEC 27001 přiděleny části norem ČSN ISO/IEC 27005 a ČSN ISO/IEC 27004. Které byly posléze charakterizovány v následujících kapitolách této práce.
Norma ČSN ISO/IEC 27001 obsahuje požadavky na činnosti, které musí organizace vykonávat, chce-li získat certifikát na základě této normy. Norma ČSN ISO/IEC 27005 obsahuje informace a podklady potřebné pro splnění požadavků kladených normou ČSN ISO/IEC 27001 v části ustavení u požadavků 1 až 6. Norma ČSN ISO/IEC 27004 obsahuje informace (návody, podklady) pro naplnění požadavků kladených normou ČSN ISO/IEC 27001 a to v části monitorování a přezkoumávání (konkrétněji: Měření účinnosti zavedených opatření pro ověření toho, že byly naplněny požadavky na bezpečnost).

4 Návrh a realizace nástroje pro řízení rizik a hodnocení efektivity

4.1 Základní informace

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 zdroji dat, či připojit k nástroji další moduly a vytvořit tak komplexní a flexibilní systém.

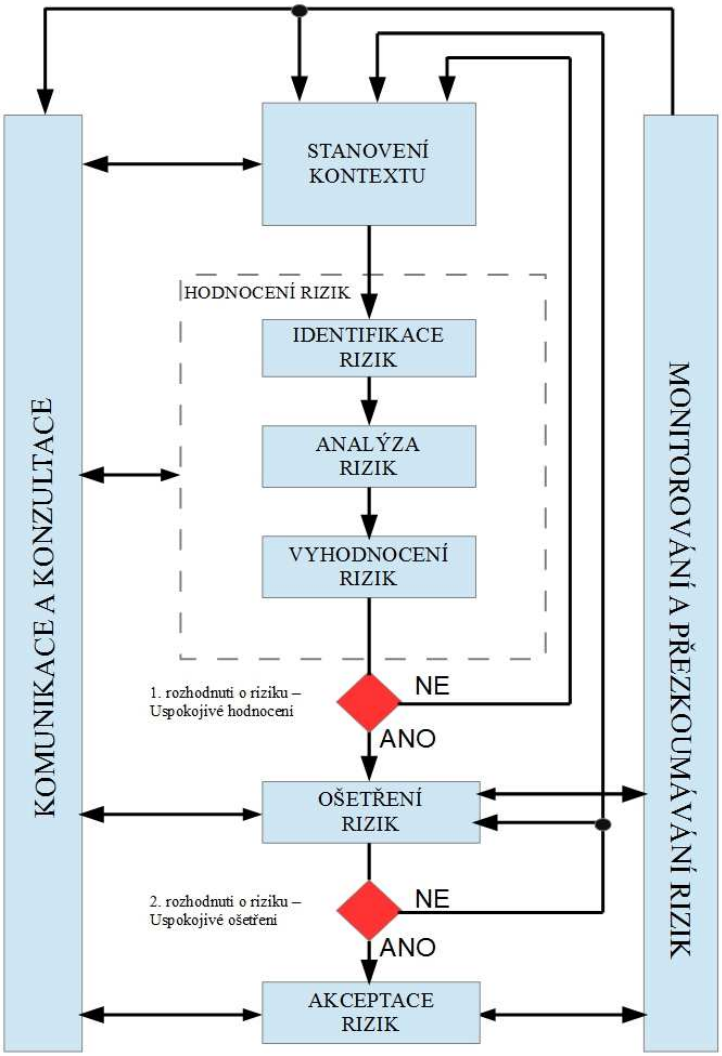
Nástroj se sestává celkem z 15 listů. Z tohoto celkového počtu listů je 6 listů využito k procesu řízení rizik dle normy ČSN ISO/IEC 27005, 1 list je určen pro určování efektivity a to dle normy ČSN ISO/IEC 27004. Pořadí a struktura listů, respektive procesů je koncipováno dle požadavků normy ČSN ISO/IEC 27005 a normy ČSN ISO/IEC 27001. Zbytek listů obsahuje pomocná data a informační data.

V nástroji bylo použito celkem 16 tabulek, které jsou navzájem provázány a to pomocí funkcí, které Excel primárně poskytuje a také pomocí vytvořených 22 modulů obsahujících makra vytvořená v programovacím jazyku VBA. Celkový počet řádků VBA kódu je 460. Tyto vytvořená makra usnadňují ovládání nástroje. Umožňují efektivní a rychlý pohyb mezi jednotlivými listy a spolu se základními funkcemi v Excelu obsaženými kontrolují zadávání dat do tabulek, filtrují a kopírují požadovaná data na žádoucí listy a provádějí požadované aritmetické operace.

Při tvorbě tohoto nástroje jsem postupoval dle požadavků norem ČSN ISO/IEC 27001, ČSN ISO/IEC 27005 a ČSN ISO/IEC 27004. Nástroj zle rozdělit do dvou hlavních částí. V první části je obsažen celý proces řízení rizik bezpečnosti informací a to dle požadavků normy ČSN ISO/IEC 27005 a druhá část nástroje obsahuje měření efektivity zvolených opatření a to dle požadavků normy ČSN ISO/IEC 27004. Nástroj také obsahuje manuál, který jednotlivě popisuje všechny listy (procesy) v nástroji obsažené. Manuál je koncipován tak, aby osvětlil uživateli posloupnost funkcí a kroků při procesu řízení rizik bezpečnosti informací a také při procesu měření efektivity zvolených opatření. Každý list je popsán v konkrétní kapitole, kde je uvedena posloupnost kroků na onom listě a jsou zde také popsány všechny funkce. Tento manuál tedy minimalizuje možnost, že by uživatel při obsluze tohoto nástroje nevěděl, co má dělat.

4.2 Řízení rizik

Při procesu tvorby byla dodržena posloupnost kroků uvedených na obrázku číslo 8., který prezentuje základní princip a následnost kroků při procesu řízení rizik bezpečnosti informací. Tato posloupnost kroků je dána požadavky normy ČSN ISO/IEC 27005. Nástroj obsahuje všechny kroky, které jsou v normě uvedeny a tyto kroku jsou charakterizovány v teoretické části této práce. Pro účely analýzy rizik byla zvolena podrobná analýza rizik. Tato metoda se skládá z identifikace a ohodnocení (v tomto případě kvalitativním) aktiv, odhadu hrozeb pro nalezená aktiva, odhadu zranitelností a identifikace existujících ochranných opatření. Z těchto dat se poté stanoví riziko. Pro výpočet míry rizika byla zvolena kvalitativní metoda,



Obrázek 7 schéma procesu řízení rizik [6]

Popis nástroje

Vstupním listem nástroje pro řízení rizik bezpečnosti informací je Ustavení (stanovení kontextu). Na tomto listu se nachází dle požadavků normy ČSN ISO/IEC 27001 pole určené pro zadávání rozsahu ISMS, respektive rozsahu implementace ISMS, dále se zde nachází pole určené pro zadání zvolené politiky. Uživatel je zde vyzván k vyplnění polí výše uvedených. Pole politika obsahuje dle normy ČSN ISO/IEC 27001 tyto dílčí části: stanovené cíle, metodiku hodnocení rizika. V rámci tohoto kroku je nutné zadat dle požadavků normy ČSN ISO/IEC 27005 způsob ohodnocení aktiv, hrozeb, zranitelností, dále stanovit kritéria hodnocení rizik, kritéria akceptovatelnosti rizik a kritéria hodnocení dopadu.

Před samotným procesem identifikace rizik je nutné dle požadavků normy ČSN ISO/IEC 27005 provést identifikaci aktiv, hrozeb, zranitelností a dopadů. Ta tím to účelem byly vytvořeny 3 tabulky na listu: “zadávací tabulky“. V tabulce aktiva uživatel postupně zadává identifikovaná aktiva, jejich kvalitativní hodnotu a vlastníka aktiva. Uvedený seznam aktiv je pouze pro názornou ukázku a je přebrán z normy ČSN ISO/IEC 17799:2006. Hrozby jsou přebrány z normy ČSN/ISO 27005:2013. V tabulce HROZBY uživatel zadává názvy identifikovaných hrozeb a jejich kvalitativní hodnotu (resp. V tomto případě hodnotu pravděpodobnosti působení hrozby). V tabulce ZRANITELNOSTI zadává uživatel název zranitelnosti a číselné vyjádření její pravděpodobnosti výskytu). Tabulky jsou formátovány, tak že v případě potřeby dalšího místa uživatel může zadávat další nové řádky, které potvrdí enterem a tabulky se automaticky zvětší.

AKTIVUM	Hodnota Kvalitativní 1	Vlastník aktiva	HROZBY	Hodnota Kvalitativní 2	Stávající opatření	Popis stávajícího opatření	Zranitelnost	ppst výskytu zranitelnosti	Dopad
Databáze	5	Novak josef	neodborná manipulace	4	NE		zaměstnanci	4	5
Software	4	Nový Karel	napadeni virem	2	ANO	plán aktualizaci	neaktualizovaný SF	3	3
hardware	2	IT oddělení	selháni funkčnosti	2	NE		stáří zařízení	3	2
Firemni dokumentace	4	Svarný Petr	odcizení	5	NE		absence přístup. Práv	3	4
serverovna	3	IT oddělení	vytopeni	3	NE		vodovod v serverovně	4	3

Databáze
Datové soubory
Firemní dokumentace
Systémová dokumentace
Smlouvy
Uživatelské manuály
Školicí materiály
Provozní a podpůrné postupy

Obrázek 8 Zadávací tabulka

Za účelem identifikace rizik a to dle požadavků normy ČSN ISO/IEC 27005 byla vytvořena zadávací tabulka viz. Obrázek č. 8, kde je současně znázorněno provedení výběru

jednotlivých aktiv, hrozeb a zranitelností z tabulek vyplněných v předchozím kroku.

Následujícím krokem dle normy ČSN ISO/IEC 27005 je analýza rizik. Nástroj využívá podrobnou analýzu rizik a úroveň rizika je vypočtena součinem kvalitativní hodnoty aktiva, hrozby a zranitelnosti. Tabulka vytvořená za účelem analýzy rizik je zobrazena na obrázku číslo 9. (pro přehlednost byla tabulka rozdělena a její části jsou zobrazeny pod sebou).

Riziko	Klasifikace	AKTIVUM	Hodnota Kvalitativní 1	Vlastník aktiva	HROZBY
80	KRITICKÉ	Databáze	5	Novak josef	neodborná manipulace
60	KRITICKÉ	Firemní dokumenta	4	Svarný Petr	odcizení
36	STŘEDNÍ	serverovna	3	IT oddělení	vytopení
24	NÍZKÉ	Software	4	Nový Karel	napadení virem
12	VELMI_NÍZKÉ	hardware	2	IT oddělení	selhání funkčnosti

Hodnota Kvalitativní2	Stávající opatření	Popis stávajícího opatření	Zranitelnost	ppst výskytu zranitelnosti	Dopad
4	NE		zaměstnanci	4	5
5	NE	(prázdné)	absence přístup.	3	4
3	NE		vodovod v serve	4	3
2	ANO	plán aktualizací	neaktualizovaný	3	3
2	NE	(prázdné)	stáří zařízení	3	2

Obrázek 9. Analýza rizik (tabulka)]

Nástroj umožňuje dle kritérií akceptovatelnosti určit rizika, která zvoleným kritériím akceptovatelnosti nevyhovují a vyžadují tedy patřičné ošetření. Nástroj umožňuje pomocí vytvořeného makra převést rizika nevyhovující kritériím akceptovatelnosti do tabulky ošetření rizik (obrázek č. 10), kde dle normy ČSN ISO/IEC 27005 lze analyzovaná rizika ošetřit definovanými způsoby.

Po ošetření všech rizik nástroj v následující tabulce akceptace rizik ověří, zdali jsou všechna rizika, která nevyhovovala kritériím akceptovatelnosti ošetřena natolik, že tato kritéria již splňují. Pokud ano, povolí uživateli přejít na plán akceptovatelnosti, pokud tomu tak není, uživatel musí cyklus ošetření opakovat a zvolit vhodnější opatření,

Tabulka pro ošetření rizik

ošetření	ošetřeno				popis ošetření	náklady	datum zahájení	datum ukončení	Odpovědná osoba	Nová hodnota rizika
	aktivum	hrozba	zranitelnost	Dopad						
Modifikace	5	4	1	5	školení ovládání DT	50 000 Kč	1.1.2014	3.2.2014	Novák Adam	20
Modifikace	3	4	5	1	zavedení hesel	15 000 Kč	1.2.2014	2.2.2014	Sajdl Radek	60
Vyhnutí se	3	3	0	4	přesun serverovny	65 000 Kč	3.4.2014	4.5.2014	Karas J.	0
Akceptace	4	2	3	3	plán aktualizování	50 000 Kč	1.1.2014	6.7.2014	Ježek M.	24
										0

Modifikace
Akceptace
Sdílení
Vyhnutí se

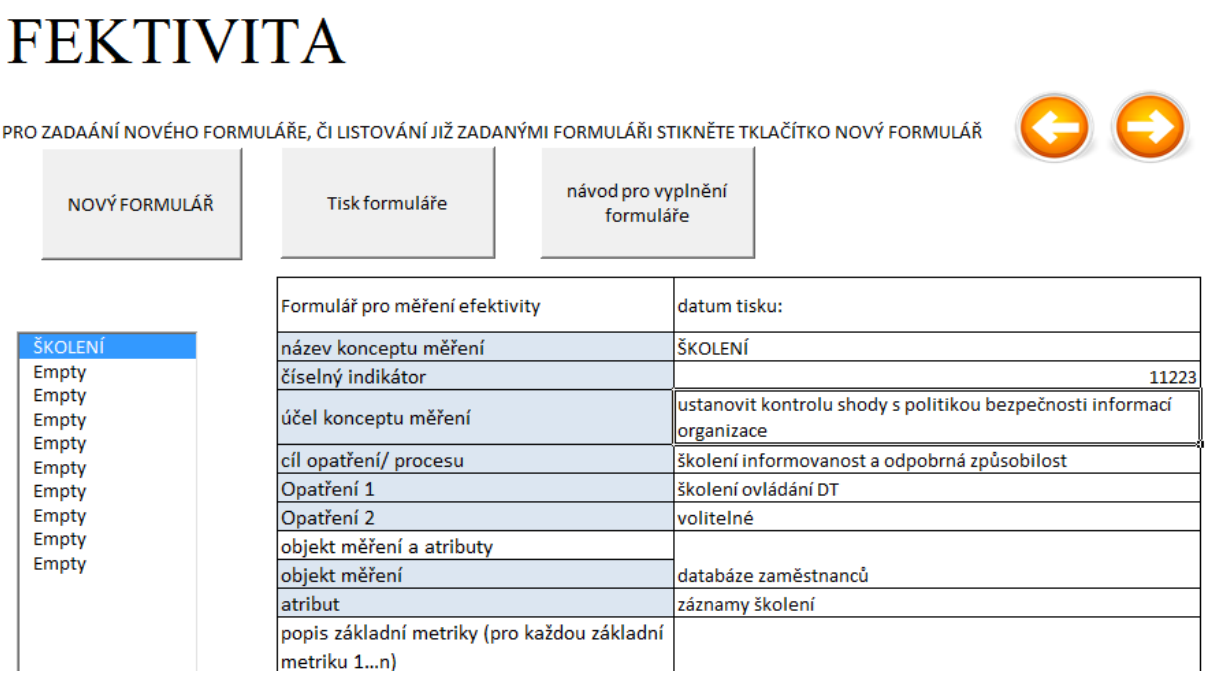
Obrázek 10. Tabulka pro ošetření rizik

Dle požadavků normy ČSN ISO/IEC 27001 je nutné pro proces zavádění zvolených opatření vypracovat plán zvládání rizik. Tento plán je poté vstupem do procesu implementace zvolených opatření a slouží mimo jiné k porovnání dosažených cílů (které jsou v něm uvedeny) s výsledky získanými z procesů měření efektivity. Stanovení plánu zvládání rizik je poslední krok v první části navrženého nástroje.

4.3 Měření efektivity

Z analýzy požadavků uvedených v normě ČSN ISO/IEC 27001 vyplívá nutnost měřit efektivitu zavedených opatření (ošetření). Důsledkem tohoto požadavku je v nástroji navrhnuta funkce měření efektivity. Návodem pro proces měření efektivity byla norma ČSN ISO/IEC 27004. Ta je charakterizována v kapitole 3.3 této práce. Pro měření efektivity byl v nástroji vytvořen list. Na tomto listě se nachází formulář určený pro měření efektivity zvolených ošetření. Tento formulář je plně v souladu s normou ČSN ISO/IEC 27004. Nástroj umožňuje uložení neomezeného počtu formulářů, které lze také vytisknout. Obsahem listu je také odkaz na nápovědu při vyplňování formuláře, která poskytne uživateli informace nutné k úspěšnému zvolení/vyplnění všech potřebných částí, ze kterých se proces měření skládá. Dále se zde nachází tabulka určená pro zaznamenávání všech měření zvolených ošetření (respektive základních informací o těchto opatřeních a o výsledcích měření efektivity těchto ošetření. Na tomto listu je také uveden příklad měření efektivnosti zvoleného opatření (odkazuje na něj tlačítko: Ukázka dat). Ale pro potřeby zaznamenávání všech procesů měření má každý formulář svůj identifikátor a také obsahuje pole pro zadání názvu souboru, kde budou uložena data měření a výsledky měření. Tedy v případě, že bude zapotřebí měřit velké množství opatření, bude tento list obsahovat pouze tabulku obsahující základní informace o

opatření a výsledků měření a seznam všech formulářů, které budou obsahovat názvy externích souborů, ve kterých budou uložena data o měřeních.



Obrázek 9list měření efektivity

Obrázek 10 List měření efektivity

Dle požadavků normy ČSN ISO/IEC 27001 je nutné veškerá rozhodnutí a kroky řádně zdokumentovat, aby bylo možné při zpětné analýze dohledat všechny kroky a operace učiněné při procesu implementace ISMS. Z tohoto důvodu nástroj poskytuje možnost tisku všech důležitých dokumentů jako je prohlášení o aplikovatelnosti (souhlas s akceptováním zbytkových rizik), plán zvládání rizik, formuláře určené pro měření účinnosti zvolených ošetření. Pro splnění požadavků této normy obsahuje nástroj tabulku určenou pro tvorbu plánu interních auditů, které je organizace povinna provádět v rámci požadavku zajištění provádění interních auditů ISMS.

4.4 Závěr

Navržený nástroj prezentuje a dodržuje požadavky kladené normou ČSN ISO/IEC 27005. Umožňuje stanovení kontextu, hodnocení rizik, analýzu rizik, zvládání rizik, Dále navržený nástroj poskytuje měření efektivity u zvolených ošetření a to způsobem definovaným normou ČSN ISO/IEC 27004. Pro dodržení požadavků kladených v normě ČSN ISO/IEC 27001 nástroj umožňuje tisk všech potřebných formulářů a to za účelem dohledání všech rozhodnutí učiněných v rámci implementace ISMS , součástí tohoto nástroje je také plán interních auditů, který musí organizace provádět v rámci zlepšování ISMS.

5 ZÁVĚR

Zadáním této diplomové práce bylo provést seznámení s problematikou systémů řízení bezpečnosti informací, řízení rizik a měření efektivity ISMS. Dále bylo zadáno vypracovat analýzu požadavků na systém řízení rizik a na základě této analýzy navrhnout nástroj pro řízení rizik a měření efektivity.

Problematice systémů řízení rizik bezpečnosti informací je věnován úvod této práce. Zaměřil jsem se na základní charakteristiky systémů řízení bezpečnosti informací (ISMS). Provedl jsem se na popsání základních kroků cyklu PDCA, který je základním nástrojem pro implementaci všech požadavků kladených v normě ČSN ISO/IEC 27001 a také normy ČSN ISO/IEC 27005. Dále jsem zpracoval přehled, ve kterém jsem uvedl výhody certifikace dle normy ČSN ISO/IEC 27001 a také přehled komplikací a možných nedostatků při procesu implementace této normy v organizaci.

Další část práce je věnována analýze požadavků uvedených v normě ČSN ISO/IEC 27001. Ke konkrétním požadavkům jsou přiřazeny části norem ČSN ISO/IEC 27005 a ČSN ISO/IEC 27004, které požadavky splňují. Tyto části norem jsou poté detailně charakterizovány v následujících kapitolách. Na základě této analýzy byl navrhnut a v programu Microsoft Office Excel 2010 sestrojen nástroj umožňující řízení rizik dle normy ČSN ISO/IEC 27005 a měření efektivity dle normy ČSN ISO/IEC 27004.

V závěru práce jsem se věnoval charakteristice mnou navrženého nástroje. V úvodu této části jsem provedl stručnou charakteristiku tohoto nástroje a uvedl důvody volby programu MS Excel, který jsem pro tvorbu nástroje využil. Poté jsem se věnoval přesnějšímu popisu tohoto nástroje a prezentoval jsem všechny jeho funkce a to jak v části řízení rizik, tak v části měření efektivity. Vytvořený nástroj prezentuje systém a následnost všech dílčích kroků při procesu řízení rizik a měření efektivity, nástroj je doplněn o manuál a 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. Nástroj byl vypracován ve dvou verzích. Jedna verze neobsahovala žádná doplněná data, druhá verze obsahovala vzorová data, která slouží jako případová studie a jako ukazatel všech možností a funkcí mnou navrženého nástroje. 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.

[15] BAUEROVÁ, Marie a Petra CÍSAŘOVÁ. MKB Consulting: aktuality. *Http://www.mbk.cz/aktuality-mbk-consulting/csn-en-iso-190112012-smernice-pro-auditovani-systemu-managementu* [online]. Praha, 2013, 5.6.2013 [cit. 2014-07-15]. Dostupné z: http://www.mbk.cz/

[16] ČSN ISO/IEC 27004. *Informační technologie – Bezpečnostní techniky – Řízení bezpečnosti informací: Měření*. inovace. Praha: Český normalizační institut, 2011.

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)	2005	*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	2005	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	2005	*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.