VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

POSOUZENÍ STAVU IMPLEMENTACE ISMS
ISMS IMPLEMENTATION STATUS ASSESSMENT

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — **Robin Černoušek**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Petr Sedlák**
SUPERVISOR

BRNO 2020

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání bakalářské práce

Ústav:	Ústav informatiky
Student:	**Robin Černoušek**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Manažerská informatika
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2019/20

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává bakalářskou práci s názvem:

Posouzení stavu implementace ISMS

Charakteristika problematiky úkolu:

Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Cílem práce je vytvoření nástroje založeného na standardech ISO27k k hodnocení současné úrovně implementace ISMS. Nástroj bude využívat k hodnocení model zralosti (CMM – Capability Maturity Model) pro jednotlivé oblasti. Nástroj umožní stanovení požadované úrovně, které má být dosaženo. Výstupy nástroje budou umožňovat grafické znázornění rozdílu mezi současnou a požadovanou úrovní za jednotlivé oblasti jako podklad k rozhodnutím o prioritách a čerpání zdrojů pro management organizace.

Základní literární prameny:

ČSN ISO/IEC 27001:2013 Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky. Český normalizační institut, 2014.

ČSN ISO/IEC 27002:2013 Informační technologie – Bezpečnostní techniky – Soubor postupů pro řízení bezpečnosti informací. Český normalizační institut, 2014.

DOBDA, L. Ochrana dat v informačních systémech. Praha: Grada Publishing, 1998. ISBN 80-71--9479-7.

DOUCEK, P., L. NOVÁK a V. SVATÁ. Řízení bezpečnosti informací. Praha: Professional Publishing, 2008. ISBN 80-86898-38-5.

POŽÁR, J. Základy teorie informační bezpečnosti. Praha: Vydavatelství PA ČR, 2007. ISBN 978-8--7251-250-8.

POŽÁR, J. Informační bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN 80-86898-38-5.

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2019/20

V Brně dne 29.2.2020

L. S.

doc. RNDr. Bedřich Půža, CSc. ředitel	doc. Ing. et Ing. Stanislav Škapa, Ph.D. děkan

Abstrakt

Bakalářská práce se zabývá problematikou systému řízení bezpečnosti informací a hodnocením současného stavu pomocí vytvořeného nástroje. Teoretická část obsahuje základní východiska a pojmy celé práce. V kapitole analýzy současného stavu je představena organizace a popsán současný stav jejího systému řízení bezpečnosti informací. Vlastním návrhem řešení je potom nástroj formou Excel tabulky, který umožní provést analýzu současného stavu úrovně implementace ISMS ve společnosti.

Klíčová slova

Bezpečnost informací, Systém řízení informační bezpečnosti, ISMS, Ochrana dat, ČSN ISO/IEC 27001, ČSN ISO/IEC 27002, Řízení rizik, Model zralosti

Abstract

Bachelor's thesis deals with the issue of information security management system and evaluation of the current state using a created tool. The theoretical part contains the basic principles and concepts of the whole work. The chapter on the analysis of the current state introduces the organization and describes the current state of its information security management system. The actual design of the solution is a tool in the form of an Excel spreadsheet, which will allow an analysis of the current state of the ISMS implementation level in the company.

Key words

Information Security, Information Security Management System, ISMS, Data protection, ČSN ISO/IEC 27001, ČSN ISO/IEC 27002, Risk Management, Maturity Model

Bibliografická citace

ČERNOUŠEK, Robin. *Posouzení stavu implementace ISMS* [online]. Brno, 2020 [cit. 2020-05-29]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/127731. Bakalářská práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Ing. Petr Sedlák.

Čestné prohlášení

Prohlašuji, že předložená bakalářská práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 29.5. 2020

.....

podpis studenta

Poděkování

Rád bych poděkoval vedoucímu mé bakalářské práce Ing. Petru Sedlákovi za zodpovědný přístup, ochotu a užitečné rady, které mi dopomohly k vytvoření této bakalářské práce. Také děkuji zaměstnancům společnosti za odborné rady a poznatky z praxe.

OBSAH

ÚVOD

V současné době si už jen málokdo dokáže představit své fungování bez moderních technologií jako jsou počítače a mobilní zařízení. Všechny moderní technologie naší společnosti velmi často usnadňují fungování, šetří náš čas i peníze. Všichni neustále generujeme data a jejich objem velice prudce stoupá. Na opačné straně tak vzniká prostor pro ilegální aktivity. Přibývá škodlivých softwarů a kybernetických útoků, které se snaží narušit chod systémů a služeb nebo získat citlivé informace. Z toho důvodu je potřeba data chránit.

Vše se také projevilo ve firemním prostředí a data se tak staly velmi cenným aktivem firem z nejrůznějších odvětví. Většina firem v dnešní době využívá hned několika informačních systémů nebo disponuje dokumenty ve fyzické podobě, které mohou obsahovat citlivé a důležité údaje. S rostoucím objemem dat také přibývá úložišť a informačních systémů, kde se data nacházejí. Může se jednat o data o firemních odběratelích, dodavatelích, zaměstnancích či uživatelích systémů. Všechny data firmě mohou usnadňovat rozhodování, dosahování jejich cílů, případně data také mohou vytvářet konkurenční výhodu.

Stále se více a více mluví o digitalizaci a využívá se cloudových řešení. To ovšem z pohledu bezpečnosti přináší celou řadu rizik a problémů. Pro většinu firem je v současnosti téměř nemožné, aby fungovaly bez odborníků na informační bezpečnost a ochranu dat. Ztráta kontroly nad informačními systémy nebo pouze únik jakýchkoliv citlivých dat by společnosti mohli způsobit nemalé ztráty, pošpinění dobrého jména firmy a v tom nejhorším případě až problémy se samotnou existencí firmy.

Všechny tyto skutečnosti tlačí na vrcholový managment firem napříč všemi odvětvími a nutí je reagovat. Důležité je tedy vybudovat a kontinuálně udržovat a zlepšovat systém bezpečnosti informací. Tento systém může být přínosem pro dosažení firemních cílů, zlepšení důvěryhodnosti a konkurenceschopnosti a také může šetřit firemní zdroje. Systémem informační bezpečnosti a posouzením současného stavu implementace se zabývá tato bakalářská práce.

CÍLE PRÁCE, METODY A POSTUPY ZPRACOVÁNÍ

Tato bakalářská práce se zabývá problematikou systému řízení bezpečnosti informací ve firemním prostředí a také hodnocením současného stavu. K hodnocení výkonnosti ISMS dané firmy využívá vytvořeného nástroje, v podobě Excel souboru, který pomocí jednotlivých ukazatelů hodnotí stav řízení bezpečnosti informací společnosti. Nástroj posuzuje a monitoruje účinnost ISMS pomocí sledování a hodnocení relevantních ukazatelů. Hlavním zdrojem informací pro tuto práci jsou normy řady ISO/IEC 27000.

Hlavním cílem je tedy vytvoření nástroje k posouzení účinnosti a monitorování výkonosti ISMS.

Výstupem bakalářské práce bude nástroj, který umožní systematické a opakovatelné hodnocení úrovně implementace ISMS a může sloužit jako podklad k rozhodování managementu, jelikož zobrazuje rozdíl mezi požadovaným stavem a skutečností.

Teoretická část obsahuje základní východiska a pojmy, na kterých je tato bakalářská práce založena. Vysvětlí tedy všechny pojmy, metody a postupy, kterých práce využívá.

Analýza současného stavu představuje energetickou společnost a odvětví ve kterém podniká. Také analyzuje současný stav informačních, bezpečnostních strategií a analyzuje současný stav systému řízení bezpečnosti informací.

Třetí a poslední část vlastní návrhy řešení obsahuje představení vytvořeného nástroje, včetně jeho funkcionalit a celkového nastavení Excel souboru. Za pomoci nástroje tato kapitola hodnotí současnou úroveň implementace ISMS v jedné ze společností skupiny ES a ukazuje tak využití nástroje.

1 TEORETICKÉ VÝCHODISKA PRÁCE

Teoretická část obsahuje východiska, na kterých jsou založena tvrzení v analýze současného stavu a slouží jako podklad k tvorbě vlastních návrhů řešení. Tato kapitola také vysvětluje základní pojmy z odvětví informační bezpečnosti společně se základními metodami. Kapitola slouží k přiblížení probírané problematiky.

1.1 Základní pojmy

Na úvod bude poskytnut přehled základních pojmů a názvosloví informační bezpečnosti, které usnadní pochopení celé bakalářské práce.

Data

„Soubor hodnot přiřazených základním mírám, odvozeným mírám a/nebo indikátorům“ (1). Pojem data je velmi často zaměňován nebo slučován s pojmem informace. Je ovšem potřeba tyto dva pojmy rozlišit a definovat. Data (někdy také údaj) jsou často chápána jako statická a časově nezávislá fakta (3). Může se jednat o čísla, text, zvuk, obraz nebo jiné smyslové vjemy uložené ve vhodné podobě pro zpracování počítačem (4).

Informace

„Každý znakový projev, který má smysl pro komunikátora i příjemce“ (6). Tento pojem je velmi často skloňován napříč všemi kategoriemi současných věd. Na základě toho, ve kterém oboru se zrovna pohybujeme, je také různě vysvětlován. Pochází z latinského slova „informo – informatio“, což znamená sdělení nebo také poučení a popis něčeho. Je velmi složité jednoznačně vymezit pojem informace, některé zdroje uvádí, že správné vymezení vychází z toho, že ne každé sdělení je pro konkrétního příjemce informací (3). Informace pro společnost představují aktivum, které je pro společnost a její fungování podstatné a je potřeba odpovídající ochrany (1).

Aktivum

Aktivum můžeme definovat jako soubor hmotných i nehmotných věcí, které mají pro určitou osobu, organizaci či stát nějakou hodnotu. Mezi nehmotná aktiva můžeme řadit

například i vlastnosti (dostupný a funkční systém) nebo dobré jméno společnosti. Lidé, jejich znalosti a zkušenosti, jsou také chápáni jako aktivum. Vyhláška o kybernetické bezpečnosti dále rozlišuje na **podpůrná** a **primární aktiva** (5).

Podpůrné aktivum

„Je technické aktivum, zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního a komunikačního systému“ (5).

Primární aktivum

„Je informace nebo služba, kterou zpracovává nebo poskytuje informační a komunikační systém“ (5).

Zranitelnost

„*Slabé místo aktiva nebo opatření, které může být využito jednou nebo více hrozbami“* (1). Obecně zranitelnost tedy označuje nějaké slabé místo aktiva, softwaru nebo zabezpečení, které může být zneužito hrozbami. Zranitelnost i hrozba můžou být způsobeny několika různými faktory. Těmi mohou být například chování lidí nebo technická závada. Může se jednat o úmyslnou chybu nebo neúmyslný nedostatek či závadu. (5,6)

Bezpečnostní zranitelnost

V oboru kybernetické bezpečnosti se zranitelnosti dále dělí na známé a publikované, ovšem ještě neošetřené výrobcem anebo skryté a neobjevené. V případě těch skrytých je důležité, kdo je objeví dříve, jestli útočník nebo uživatelé. Tyto zranitelnosti jsou tak potencionálními bezpečnostními hrozbami a lze je eliminovat důslednými opatřeními (6).

Hrozba

Hrozbou může být skutečnost, událost nebo i lidé, jejichž působení může jakkoliv způsobit poškození, zničení nebo ztrátu důvěrnosti či hodnoty aktiva. Hrozba tedy může ohrozit bezpečnost (3). Ministerstvo vnitra ČR hrozbu definuje následovně: „*Jakýkoli fenomén, který má potenciální schopnost poškodit zájmy a hodnoty chráněné státem.*

Míra hrozby je dána velikostí možné škody a časovou vzdáleností (vyjádřenou obvykle pravděpodobností čili rizikem) možného uplatnění této hrozby“ (7). Obecně můžeme pojem hrozba definovat jako *„Potenciální příčina nechtěného incidentu, jehož výsledkem může být poškození systému nebo organizace“* (1).

Bezpečnostní hrozba

V odvětví informační bezpečnosti stačí definici modifikovat a definovat tak hrozbu bezpečnostní: „*Potenciální příčina nežádoucí události, která může mít za následek poškození systému a jeho aktiv, např. zničení, nežádoucí zpřístupnění (kompromitaci), modifikaci dat nebo nedostupnost služeb“* (6).

Riziko

„Účinek nejistoty na dosažení cílů“ (1). Kromě definice dané samotnou normou lze pojem riziko definovat i následovně: a) Nebezpečí, možnost škody, ztráty, nezdaru. b) Účinek nejistoty na dosažení cílů. c) Možnost, že určitá hrozba využije zranitelnosti aktiva nebo skupiny aktiv a způsobí organizaci škodu (6).

Dopad

a) *„Nepříznivá změna dosaženého stupně cílů.“* b) *„Následky určitého činu nebo události“* (6).

Opatření

Opatření je jedním z prostředků modifikujících riziko. Může zahrnovat jakýkoliv proces, politiku, zařízení, metodu nebo jiné činnosti, které modifikují riziko. Ne vždy však musí opatření vyvolat zamýšlený nebo předpokládaný účinek (1).

Bezpečnostní klasifikace

Bezpečnostní klasifikace slouží k určení stupně ochrany, který data nebo informace vyžadují, spolu s vyznačením tohoto stupně ochrany (6).

Bezpečnostní událost

Jedná se o takovou událost, která může (avšak nemusí) vést nebo způsobit narušení informačních systémů a technologií a definovaných pravidel k jeho ochraně. Událost může vést k celé řadě následků (6).

Následek

Následek můžeme chápat jako výsledek události působící na cíle. V kontextu bezpečnosti informací je následek obvykle negativní a může být vyjádřen kvalitativně nebo kvantitativně (1).

Bezpečnostní incident

Může se jednat o jednotlivé nežádoucí a neočekávané události nebo také o celé série událostí, které mohou s významnou pravděpodobností ohrozit bezpečnost informací (1). Může tedy dojít k porušení nebo bezprostřednímu ohrožení bezpečnostních politik, zásad nebo standartních bezpečnostních pravidel provozu informačních a komunikačních technologií (6).

Bezpečnost informací

Jednoduše řečeno je bezpečnost informací snaha o zachování (ochranu) tří základních aspektů, kterými jsou **důvěrnost**, **integrita** a **dostupnost** (1). Tyto základní vlastnosti jsou vysvětleny dále.

Důvěrnost

Jedná se o základní vlastnost, která zajišťuje, že informace není dostupná nebo odhalena neoprávněným jednotlivcům, entitám nebo procesům (1). Přístup k informacím by měl být tedy omezen tak, aby se k nim dostali pouze tzv. autorizovaní uživatelé (3).

Integrita

Tato vlastnost vyjadřuje přesnost a úplnost informací (1). **Integritu dat** tedy můžeme chápat jako jistotu, že data nebyla změněna. Zároveň by také měla být zajištěna platnost, konzistence a přesnost dat, například v databázích či informačních systémech. Často se využívá kontrolních součtů, hašovacích funkcí nebo redundance.

Integrita systému pak je vlastnost, která nám říká, že systém vykonává svou původní funkci bez narušení a bez záměrné nebo náhodné neautomatizované manipulace se systémem (5).

Dostupnost

Poslední vlastností je dostupnost, která zaručuje přístupnost a použitelnost na žádost oprávněné entity (1).

Entita

Pod tímto pojmem se může skrývat cokoliv, co považujeme ve svém okolí za natolik důležité, abychom tomu věnovali pozornost a přiřadili tomu jméno (8).

1.2 Systém řízení bezpečnosti informací

V současné době již téměř každá organizace shromažďuje, zpracovává a uchovává informace. Tyto informace společně se souvisejícími procesy, systémy, sítěmi i lidmi jsou důležitá aktiva a hrají důležitou roli při dosahování cílů organizace. Bez ohledu na velikost a typ firmy každá firma čelí celé řadě rizik, která mohou narušit bezpečnost a fungování jejich aktiv. Je tedy potřeba zavést, udržovat a neustále zlepšovat systém řízení bezpečnosti informací. To organizace pomůže nejen při snaze dosáhnout jejich cílů, ale také jim zaručí lepší soulad s právními normami a tím zlepší jejich konkurenceschopnost a dobré jméno společnost (1).

Systém řízení bezpečnosti informací nebo také často používané **ISMS** (z anglického Information Security Management System) je soubor politik, směrnic, postupů, zdrojů a činností, které organizace řídí tak, abych zajistily bezpečnosti svých informačních aktiv. ISMS pro společnosti představuje systematický a efektivně dokumentovaný systém řízení a správy informačních aktiv s cílem minimalizovat nebo až naprosto odstranit možnost jejich ztráty nebo poškození. Celý tento systém je založen posuzování rizik a na úrovních přijetí těchto rizik. Jelikož je tento systém navržen univerzálně, je k úspěšné implementaci zapotřebí, aby každá organizace k samotné implementaci přistupovala na základě jejich potřeb (1).

Je tedy vhodné, aby organizace:

- monitorovala a vyhodnocovala efektivnost již zavedených opatření a postupů
- zjišťovala nově vznikající rizika, které je třeba ošetřit
- vybírala, zaváděla a zlepšovala příslušná opatření tam, kde je to potřebné (1)

K úspěšné implementaci dále přispívají následující základní principy (1):

- povědomí o potřebě bezpečnosti informací
- určení odpovědnosti za bezpečnost informací
- začlenění závazku vedení a zájmů zúčastněných stran
- zvýšení společenských hodnot
- posouzení rizika, na základě kterého budou stanovena příslušná opatření, aby bylo dosažení přijatelných úrovní rizika
- bezpečnost začleněná jako základní prvek do informačních sítí a systémů
- aktivní prevence a detekce incidentů bezpečnosti informací
- zajištění komplexního přístupu k řízení bezpečnosti informací
- neustálé opakované posuzování bezpečnosti informací a provádění modifikací dle potřeby (1)

1.2.1 Model PDCA

Pro fungování ISMS je zapotřebí systémový a komplexní přístup, který bude respektovat principy a prvky v rámci celého životního cyklu informační bezpečnosti. Systém ISMS je proto založen na Demingově cyklu neboli PDCA cyklu (**P**lan – **D**o – **C**heck – **A**ct; Plánuj-Dělej-Kontroluj-Jednej). Jedná se o jeden ze základních manažerských principů, který zajišťuje postupné zlepšování procesů, služeb, výrobků aj. díky cyklickému opakování čtyř základních činností Plan-Do-Check-Act. V současné době tento cyklus prošel celou řadou různých modifikací. Jedna z nich připadá v úvahu pro oblast informační bezpečnosti a to varianta OPDCA, která základní model rozšiřuje o fázi Observe – Pozoruj a řadí ji před fázi plánování (5).

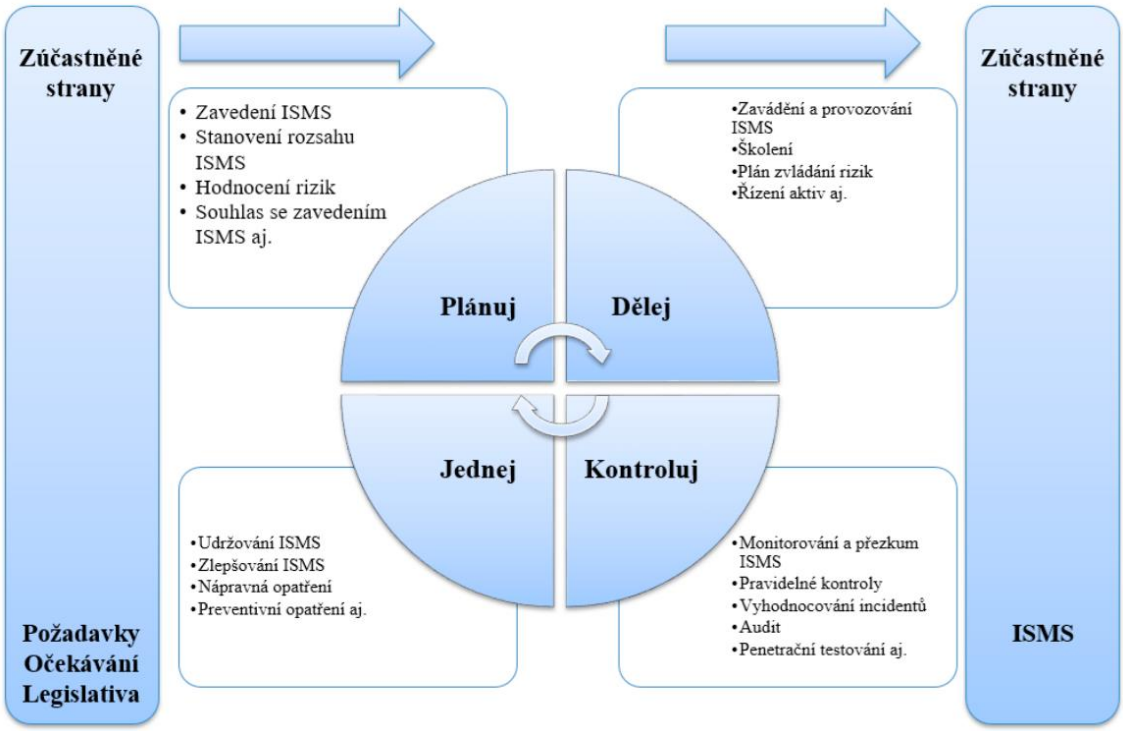
- **Plan** (plánuj) – vymyšlení a naplánovaní změň a zlepšení
- **Do** (dělej) – realizace naplánovaných změn nebo zlepšení
- **Check** (kontroluj) – sledování rozdílu mezi výsledkem a původním záměrem
- **Act** (jednej) – úprava změn, zlepšení a implementace (5)

Na všechny procesy spojené s ISMS lze aplikovat model **PDCA** nebo některé jeho modifikace. Nejlépe tento model znázorňuje nekončící kruh: (5)

Obrázek č. 1: Model PDCA (5)

Systém řízení bezpečnosti informací je tedy založen na principu PDCA cyklu, který zároveň bývá také označován jako životní cyklus ISMS. Ten je složen z následujících částí:

- **Ustavení ISMS** – Ustavení politiky ISMS, cílů, procesů a postupů
- **Zavádění a provoz ISMS** – Zavedení a využívání politiky ISMS, opatření, procesů a postupů
- **Monitorování a přezkoumání ISMS** – Posouzení i měření výkonu procesu vůči nastavené politice ISMS, hlášení výsledků managementu
- **Údržba a zlepšování** – Přijetí opatření k nápravě a přijetí preventivních opatření, snaha o neustálé zlepšování ISMS



Obrázek č. 2: Model PDCA aplikovaný na procesy ISMS (5)

Vztah mezi životním cyklem a PDCA cyklem je tedy následující (5):

- Plánuj = Ustavení
- Dělej = Zavádění a provoz
- Kontroluj = Monitorování a přezkoumání
- Jednej = Údržba a zlepšování (5)

1.2.2 Životní cyklus ISMS

Jak již bylo řečeno, životní cyklus ISMS je založen na principu PDCA cyklu. V průběhu celé cyklu je důležité, aby organizace provedla následující kroky (1):

- identifikace informačních aktiv a jejich bezpečnostních požadavků
- posouzení a ošetření rizik bezpečnosti informací
- výběr a implementace opatření vhodných pro zvládnutí neakceptovatelných rizik
- monitorování, udržování a zvyšování efektivnosti spojených s aktivy (1).

Pro efektivní a trvalou ochranu informačních aktiv organizace je zapotřebí, aby všechny kroky byly neustále opakovány a byly tak schopny se přizpůsobit změnám týkajících se rizik nebo strategií a cílů organizace. Náplň jednotlivých fází životního cyklu ISMS je dána normami ISO/IEC 27001 a ISO/IEC 27002 (1).

Ustavení ISMS

První a také velmi důležitou fází budování ISMS v organizaci je fáze ustavení. V této fázi se začíná formovat řešení včetně vymezení rozsahu a hranic pro realizace následujících fází. Kvalita provedení ustavení má zásadní dopady na fungování ISMS během celého jeho životního cyklu, protože definuje základy celého systému a ovlivňuje tak následující fáze (9,10).

Fázi můžeme dále rozdělit do následujících skupin činností (9,10):

- Definice rozsahu, hranic a vazeb ISMS
- Definice a odsouhlasení prohlášení o aplikovatelnosti
- Analýza a zvládání rizik
- Příprava prohlášení o aplikovatelnosti (9,10)

Zavádění a provoz ISMS

V průběhu této fáze dochází k implementaci bezpečnostních opatření, které byly předtím navrženy ve fázi ustavení ISMS. Tato etapa se neobejde bez následujících aktivit (9,10):

- Formulace plánu zvládání rizik a jeho zavedení
- Zavedení bezpečnostních opatření a formulace příručky bezpečnosti informací, která upřesňuje pravidla a postupy aplikovaných opatření
- Definice programu budování bezpečnostního povědomí a školení uživatelů
- Definice způsobů měření účinnosti opatření a sledování ukazatelů
- Zavedení postupů a dalších opatření pro schopnost rychle reagovat na bezpečnostní incidenty
- Řídit zdroje, dokumentaci a záznamy ISMS (9,10)

Monitorování a přezkoumání ISMS

Primární funkcí této etapy je zajištění zpětné vazby týkající zavádění a dalšího provozu ISMS. Pro vedení organizace je to zdroj informací o tom, zda opatření naplňují potřeby organizace (9,10).

Během této etapy je nutné zajistit následující (9,10):

- Monitoring a ověření účinnosti již aplikovaných opatření
- Interní audit, který pokryje celý rozsah ISMS
- Příprava zprávy o stavu ISMS pro potřeby organizace (9,10)

Udržování a zlepšování ISMS

Poslední a neméně důležitou fází celého cyklu je udržování a zlepšování ISMS. Tato fáze by měla sbírat a poskytovat vedení organizace podněty ke zlepšení ISMS, nápravě nedostatků a nesplněných požadavků (neshod). Činnosti spojené s nápravou a preventivními činnostmi vyžadují řádnou dokumentaci (9,10).

I tato část vyžaduje realizaci určitých činností (10):

- Zavedení zlepšení na základě neshod
- Provádět opatření k nápravě a preventivní opatření pro odstranění nedostatků (9,10)

1.2.3 Řada norem ISMS

Řada norem, která se věnuje problematice ISMS, má za úkol organizacím bez ohledu na velikost a typ usnadnit zavedení ISMS a jeho provoz. Tato řada obsahuje několik norem, které nesou společný název Informační technologie – Bezpečnostní techniky (1).

Ještě před uvedením nejdůležitějších norem, které se zabývají problematikou ISMS, je doplněn slovník základních pojmů o pojem standard a norma. Také jsou představeny některé instituce zabývající se standardizací bezpečnosti informačních technologií.

Standard

Standard představuje dokumentovanou úmluvu obsahující technické specifikace nebo přesně stanovená kritéria, která slouží jako pravidla. Může sloužit také jako definice charakteristických vlastností, které zajistí požadovanou kvalitu procesu, služby, výrobku nebo například materiálu (11).

Norma

Oproti standardu je norma spíše jenom doporučení pro daný standard k realizaci požadovaného řešení (11).

ISO

Zkratka vychází z anglického International Organization for Standardization. Jedná se tedy o mezinárodní organizaci pro standardizaci. Její hlavní činností je podpora rozvoje standardizačních a s tím spojených aktivit, které se zaměřují na usnadnění mezinárodních směn zboží a služeb a na spolupráci ve sféře intelektuální, vědecké, technologické a ekonomické (11).

IEC

Pod touto zkratkou se skrývá International Electrotechnical Commission. V překladu tedy mezinárodní elektrotechnická komise, která připravuje normy z oblasti elektrotechniky a příbuzných oblastí (11).

ČSN

Česká technická norma (ČSN) vzniká nejčastěji dvěma způsoby. Prvním z nich je přejímání evropských a mezinárodních norem do soustavy českých technických norem formou ČSN EN. Druhou možností je potom tvorba původních ČSN, které vyplývají z národních potřeb a z hlediska zachování funkčnosti fondu ČSN (11).

Normy zabývající se problematikou ISMS

Jak již bylo zmíněno, řada norem ISMS má za úkol organizaci usnadnit zavedení a provoz ISMS (1). Celá řada je složena se vzájemně souvisejících norem, které obsahují významné komponenty zaměřující se na technické normy, které popisují požadavky na

ISMS (ISO/IEC 27001) a na organizace, které certifikují shodu s ISO/IEC 270001 (ISO/IEC 27006). Zbylé normy poskytují návod pro různé součásti implementace ISMS a také například obsahují návody pro různá odvětví (1).

V tomto oddíle si tedy představíme nejvýznamnější normy z této řady a stručně vymezíme jejich obsah.

a) **Normy obsahující přehled a terminologii**

ISO/IEC 27000 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník (1)

První norma z této řady poskytuje celkový přehled řady norem ISMS, úvod k systémům řízení bezpečnosti informací (ISMS) a základní termíny a definice použité v řadě norem ISMS (1).

b) **Normy specifikující požadavky**

ISO/IEC 27001 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky (1)

Druhá norma z řady norem ISMS specifikuje požadavky na ustavení, implementování, provozování, monitorování, přezkoumávání, udržování a zlepšování ISMS. Dále také specifikuje požadavky na implementaci opatření bezpečnosti informací upravených podle potřeb organizace. Tato norma je vhodná pro všechny organizace bez ohledu na jejich velikost a odvětví (1).

ISO/IEC 27006 Informační technologie – Bezpečnostní techniky – Požadavky na orgány poskytující audit a certifikaci systémů řízení bezpečnosti informací (1)

Tato norma je stěžejní normou pro orgány, které poskytují audit a certifikaci ISMS v souladu s ISO/IEC 27001. Je určena především k podpoře akreditace certifikačních orgánů (1).

c) Normy popisující obecné směrnice

ISO/IEC 27002 Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací (1)

Předmětem této normy je seznam obecně akceptovaných cílů opatření a opatření pro doporučené postupy. Slouží tak tedy jako návod k implementaci a výběru opatření, jejichž cílem je dosáhnout bezpečnosti informací. Konkrétně kapitola 5 až 18 poskytují konkrétní implementační doporučení a návody na použití doporučených postupů (1).

Tabulka č. 1: Kapitoly bezpečnosti informací dle ISO/IEC 27002 (Upraveno dle: 1)

Označení	Kapitola	Kategorie	Opatření
A.5	Politiky bezpečnosti informací	1	2
A.6	Organizace bezpečnosti zdrojů	2	7
A.7	Bezpečnost lidských zdrojů	3	6
A.8	Řízení aktiv	3	10
A.9	Řízení přístupu	4	14
A.10	Kryptografie	1	2
A.11	Fyzická bezpečnost a bezpečnost prostředí	2	15
A.12	Bezpečnost provozu	7	14
A.13	Bezpečnost komunikací	2	7
A.14	Akvizice, vývoj a bezpečnost systému	3	13
A.15	Vztahy s dodavateli	2	5
A.16	Řízení incidentů bezpečnosti informací	1	7
A.17	Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací	2	4
A.18	Soulad s požadavky	2	8

ISO/IEC 27003 Informační technologie – Bezpečnostní techniky – Směrnice pro implementaci systému řízení bezpečnosti informací (1)

Hned následující norma poskytuje praktický návod pro implementaci a informace důležité pro celý životní cyklus ISMS podle ISO/IEC 27001 (1).

ISO/IEC 27004 Informační technologie – Bezpečnostní techniky – Řízení bezpečnosti informací – Měření (1)

Další v pořadí je norma, která poskytuje návod a doporučení pro vývoj a použití měření. Měření slouží k posouzení efektivnosti ISMS, cílů opatření a opatření použitých k implementaci a řízení ISMS podle specifikace v ISO/IEC 27001 (1).

ISO/IEC 27005 Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací (1)

Jedná se o směrnice pro řízení rizik v bezpečnosti informací. Postupy v této normě podporují obecná pojetí specifikována v ISO/IEC 27001 (1).

ISO/IEC 27007 Informační technologie – Bezpečnostní techniky – Směrnice pro audit systémů řízení bezpečnosti informací (1)

Tato norma poskytuje návod na provádění auditů ISMS a návod popisující kompetence auditorů systémů řízení bezpečnosti informací (1).

ISO/IEC TR 27008 Informační technologie – Bezpečnostní techniky – Směrnice pro audit opatření ISMS

Jedná se o technickou zprávu, která se zaměřuje na přezkoumání opatření bezpečnosti informací, včetně kontroly technické shody s normou na implementaci bezpečnosti informací. Není určena pro audity systému řízení (1).

ISO/IEC 27014 Informační technologie – Bezpečnostní techniky – Správa bezpečnosti informací

Za pomoci této normy organizace může hodnotit, usměrňovat a monitorovat řízení bezpečnosti informací (1).

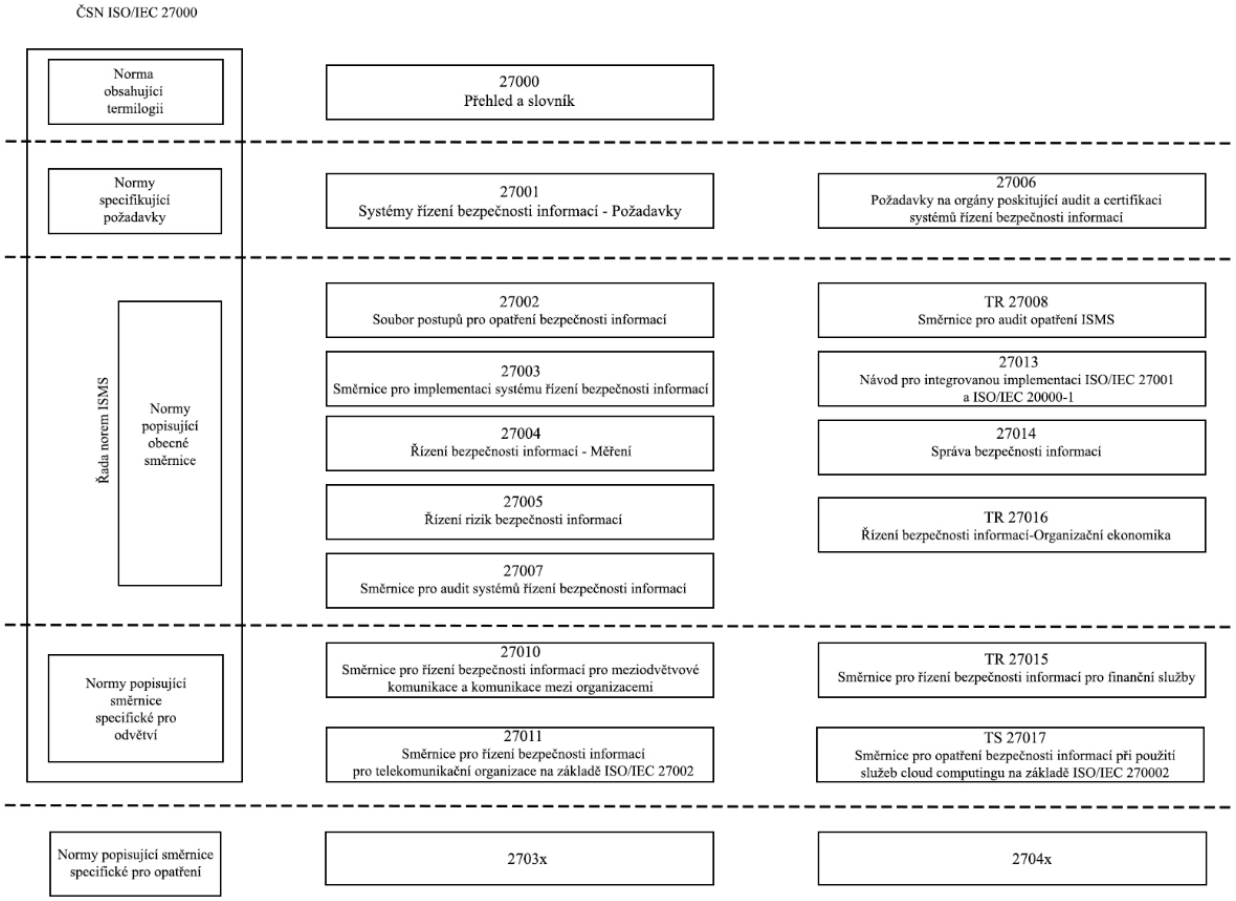
d) Normy popisující směrnice specifické pro jednotlivá odvětví

Do této kategorie spadá velké množství norem a každá z nich podporuje implementaci ISMS v konkrétním odvětví. Mezi ty základní patří následující normy:

Pro implementaci řízení bezpečnosti informací v meziodvětvových komunikacích a komunikacích mezi organizacemi slouží norma **ISO/IEC 27010**. Pro potřeby řízení bezpečnosti informací v oblasti telekomunikačních technologií je k dispozici norma **ISO/IEC 27011**. V případě zdravotnictví se využívá normy s označením **ISO/IEC 27799**, která upravuje ISO/IEC 27002 přímo pro odvětví zdravotnictví. Další normou je **ISO/IEC 27011**, která se zaměřuje na potřeby řízení bezpečnosti informací v telekomunikačních organizacích (1).

Pro potřebu této bakalářské je vhodné zmínit technickou zprávu, která nese označení **ISO/IEC TR 27019**. Tato technická zpráva předkládá směrnice vycházející z normy ISO/IEC 27002 pro použití na systémy řízení procesů v energetickém průmyslu. Cílem tohoto dokumentu je rozšířit původní soubor norem ISO/IEC 27000 na oblast procesních řídících systémů a automatizační techniky, což umožňuje v energetickém rozvodném průmyslu implementovat standardizovaný systém řízení informační bezpečnosti a to podrobně až na úroveň řízení procesů. Svým rozsahem se norma vztahuje na systémy řízení procesů používané v energetice pro řízení a monitorování výroby, přenosu, skladování a distribuci elektrické energie, plynu a tepla v kombinaci s kontrolou podpůrných procesů. Do tohoto rozsahu ovšem nespadají energetické systémy řízení technologických procesů v domácnostech a podobných obytných budovách, konvenční či klasická ovládací zařízení, která jsou postavena na analogovém nebo elektromechanickém principu (12).

Následující obrázek zobrazuje vztahy mezi řadou norem ISMS:



Obrázek č. 3: Vztahy mezi normami řady ISMS (Upraveno dle: 1)

1.3 Rámce využívané pro ISMS

Tato kapitola obsahuje přehled základních rámců a metod využívaných v oblasti managementu informační bezpečnosti. Nejznámějšími jsou rámcová knihovna ITIL nebo metodika COBIT. V obou případech se jedná o univerzální doporučení jak na určité situace reagovat, jde vlastně tedy o jakési soubory nejlepších praktik v oboru. Můžeme zde zařadit také samotnou řadu norem ISO 27000, která byla pospána podrobně už dříve.

1.3.1 ITIL

Zkratka vychází z anglického **IT I**nfrastructure **L**ibrary. V českém prostředí se nijak nepřekládá a běžně se používá přímo zkratka ITIL. Jedná se o mezinárodně uznávaný rámec pro řízení a správu IT služeb. Samotný obsah vychází z nejlepších zkušeností z praxe a nabízí tak podporu pro zvládnutí řízení IT v organizaci. Zaměřuje se na

neustálé měření a zlepšování kvality služeb a to z pohledu organizace i z pohledu zákazníka. V praxi ITIL slouží pro nastavení a řízení IT služeb a procesů. Jeho praktická použitelnost a rozšířenost z nějak v podstatě dělají standard pro řízení IT. Ovšem ITIL není norma, obsahuje pouze doporučení a nejlepší praktiky (best practice) (13).

1.3.2 COBIT

Zkratka opět vychází z anglického **C**ontrol **OB**jectives for **I**nformation and related **T**echnology a v českém prostředí se také nepřekládá. I tomto případě se jedná o soubor nejlepších praktik pro řízení IT v organizaci, které by měly umožnit dosažení cílů organizace díky efektivnímu využívání zdrojů a minimalizaci rizik. První verzi COBIT vydala organizace ISACA v roce 1996. První verze obsahovala pouze rámec, druhé vydání bylo rozšířeno o auditní postupy, sadu implementačních nástrojů a rozpracované procesy kontroly, třetí vydání bylo navíc rozšířeno o manažerské postupy. Třetí a čtvrtá verze byla vydána institutem ITGI (IT Governance Institute). Poslední a nejaktuálnější verzí je COBIT 5 (14).

Tabulka č. 2: Srovnání COBIT, ITIL, ISO 27000 (Vlastní zpracování)

Standard	Vydavatel	Zaměření	Funkce	Oblasti	Certifikace
COBIT	ISACA	IT Governance, audit informačního systému	Mapování IT procesů	4 procesy 34 domén	-
ITIL	OGC	Řízení služeb v IS/ICT	Mapování IT služeb	9 procesů	Certifikace zaměstnanců
ISO 27000	ISO	Shoda s normou	Řízení rizik v oblasti informační bezpečnosti	14 kapitol 35 kategorií 114 opatření	Certifikace organizace

2 ANALÝZA SOUČASNÉHO STAVU

Tato kapitola se zabývá představením energetické společnosti, její ICT infrastruktury, strategie kybernetické bezpečnosti. Dále se také věnuje analýze současného stavu systému řízení bezpečnosti informací v organizaci. Také jsou zde definovány nedostatky současného stavu, které řeší kapitola vlastního návrhu řešení.

2.1 Základní charakteristika společnosti

Energetická společnost (dále jen ES) působící na českém trhu je součástí mezinárodního energetického koncernu působícího především v geografickém regionu Evropy. Všechny společnosti ES skupiny jsou na území České republiky vlastněny a řízeny holdingovou společností se sídlem v Essenu (s obratem 41,48bn EUR, 78 tis. zaměstnanců v roce 2019).

Mezi hlavní činnosti ES na území ČR patří:

- Provozování elektrické distribuční soustavy v jižních Čechách a na jižní Moravě a plynové distribuční soustavy na jihu Čech
- Obchodování s elektrickou energií a plynem na českém trhu. Mezi další činnosti rovněž patří výroba elektrické a tepelné energie v České republice

2.2 ICT infrastruktura společnosti

Infrastruktura ICT v ES je z pohledu bezpečnosti členěna do dvou oblastí, které jsou označovány jako komerční IT (CIT) a procesní IT (OT).

Cílem komerčního IT je podpora skupinových procesů a lokálních obchodních aktivit s využitím standardizace a globálních kontraktů, outsourcingových kontraktů s dodavateli skupinových IT služeb. Jsou zde provozovány služby na podporu především obchodních a administrativních činností jako SAP systémy, kancelářské systémy a aplikace jako je například Microsoft Office 365. Pro oblast komerčního IT je důraz kladen především na bezpečnostní atribut důvěrnosti, oproti OT, kde je důležitý bezpečnostní atribut dostupnosti. V komerčním síťovém prostředí jsou umístěny

počítače a notebooky běžných uživatelů, kteří využívají mimo standardních klientských aplikací Microsoft Office i přístup do Internetu, elektronickou poštu a aplikace na podporu spolupráce jako je Skype pro společnosti, MS Teams, MS SharePoint, MS One Drive pro společnosti. Pro oblast komerčního IT jsou využívány outsourcing služby na provoz pracovních stanic uživatelů, síťových komunikačních služeb (WAN, LAN, Internet), provozování serverů a datových center. Jako součást strategie je pro oblast komerčního IT využíváno i cloud řešení např. Microsoft Azure, AWS, SAP. U všech těchto významných poskytovatelů cloud služeb jsou dohodnuty speciální bezpečnostní opatření pro zajištění vyšší kybernetické bezpečnosti při provozování služeb typu IaaS, PaaS a SaaS. Mimo cloud řešení jsou pro provozování serverů a aplikaci využívány i privátní cloud prostředí a vlastní serverové a komunikační místnosti. Zodpovědnost za ISMS pro oblast IT mají lokální společnosti, které však velkou část formálně přenesenu smluvní formou přes centrální skupinové služby na skupinové poskytovatele (např. lokální poskytovatel IT služeb dodává služby složené z lokálních výkonů IT a SLA dohodnutých skrze centrální IT služby, kde řada těchto služeb je poskytována outsourcingovým partnerem na základě smlouvy pokrývající služby pro celou skupinu).

Procesní IT podporuje ICT infrastruktury sloužící k dispečerskému řízení fyzikálních vlastností přenosové soustavy el. energie a plynu. Zde jsou primárně provozovány řídící systémy SCADA s komunikační sítí přenášející propojující řídící systémy SCADA s ovládacími prvky v rozvodnách elektrické energie a předávacích plynových stanicích. Součástí jsou i prvky KII definované z pohledu Zákona o kybernetické bezpečnosti (ZKB).

Obě výše uvedené IT oblasti jsou vzájemně oddělené formou samostatných síťových prostředí jejichž propojení je z důvodů požadavku na předávání nezbytných informací mezi nimi realizováno prostřednictvím síťového oddělení s využitím firewallů a demilitarizovaných zón na jejich rozhraní.

V rámci holdingové skupiny je definována politika kybernetické společnosti, která tvoří rámec ISMS platný pro všechny společnosti a pro oblast OT jsou navíc kladeny některá specifická opatření nad rámec holdingových pravidel kybernetické bezpečnosti,

vyplývající z legislativních a regulačních požadavků. Jedná se především o ZKB, jehož odlišnosti a v některých případech přísnější požadavky musí být mapovány na skupinová opatření a standardy nebo jejich rozšíření v případě, kdy mapování na skupinová opatření a standardy není možné. V tomto případě můžeme říct, že ISMS pro oblast KII je podmnožinou skupinového ISMS s opatřeními společných stejně jako pro oblast komerčního IT a s doplňujícími pravidly a opatřeními pro oblast regulace v energetice a KII. Primární zodpovědnost za ISMS pro oblast OT má lokální subjekt vlastnící distribuční licenci od Regulačního úřadu a současně jako subjekt odpovědný za dodržování ZKB. Přičemž tento subjekt zajišťuje plnění požadavků vlastními zdroji, službami dohodnutými na lokální úrovni od ostatních servisních společností skupiny v ČR a jejich prostřednictvím i skupinové službu.

Z důvodu požadavků na digitalizaci a poskytování on-line služeb jsou obě síťová prostředí IT a OT propojena prostřednictvím několika DMZ obsahujících infrastrukturní službu a komunikační rozhraní mezi aplikacemi, servery ale i potřebné uživatelské přístupy. Toto rozhraní mezi síťovými prostředími IT a OT je z pohledu kybernetické bezpečnosti velmi významné a je zde snaha minimalizovat přístupy uživatelů na nebezpečných/zranitelných komunikačních protokolech umožňující například přenos škodlivého kódu z prostředí IT do OT, ale i opačně. Proto jsou na rozhraní minimalizovány přímé přístupy na souborové úrovni. Komunikační kanály (protokoly/rozhraní) jsou minimalizována a pokud možno kontrolována a monitorována.

2.3 Strategie kybernetické společnosti

Základní principy strategie kybernetické bezpečnosti jsou zaměřeny obecně na podporu podnikatelských aktivit v ES:

- Zabezpečení spolehlivé dodávky služeb zákazníkům ES
- Vytváření hodnot agilní podporou podnikání ES a jejich zákazníků
- Zjednodušování a zefektivnění pravidel kybernetické bezpečnosti ke zlepšení pracovních činností našich zaměstnanců
- Chránit data zákazníků ES, citlivé informace ES a kritickou infrastrukturu zavedením kybernetické odolnosti ES.

Mezi dlouhodobá nebo aktuální témata s potřebou podpory realizace principů kybernetické bezpečnosti můžeme uvést:

- Řízení správy identit a řízení přístupů (identita jako nový perimetr, 2FA)
- Řízení na základě hodnocení rizik (jednoduchost a transparentnost klasifikace aktiv a posouzení rizik kybernetické bezpečnosti)
- Řízení dodavatelů (definování požadavků a prokazování shody s požadavky ES)
- Outsourcing (hrozby a opatření při přesunu činností na dodavatele)
- Přesun do prostředí cloud (nové hrozby a rizika s provozováním aplikací a služeb u poskytovatelů IaaS, PaaS, SaaS (*aktuálně pro komerční IT*))
- Digitalizace (zvýšení hrozeb/rizik spojených s digitalizací dat)
- Bezpečnost jako součást návrhu (Security by design)
- Robotizace a AI (využití a podpora z pohledu požadavků kybernetické bezpečnosti)
- Shoda s požadavky (definice a zavedení opatření a jejich kontrola k prokázání shody s požadavky ISMS ES a legislativními požadavky (např. ZKB, GDPR))
- Fyzická bezpečnost (především pro oblast KII)
- Zabezpečení komunikačního provozu a IT (požadavky na šifrování a monitoring)
- …

2.4 Současný stav bezpečnosti informací ve společnosti

Popis současného stavu bezpečnosti v ES je primárně zaměřen na oblast komerčního IT. Systém řízení ISMS je tvořen v souladu se skupinovými pravidly kybernetické bezpečnosti založený na systému řízení rizik a prokazování shody se skupinovou politikou kybernetické bezpečnosti. Politika kybernetické bezpečnosti je závazná pro všechny společnosti v rámci skupiny a vymezuje exkluzivní činnosti (Definování kybernetické bezpečnosti skupiny a monitorování její implementace, definování politik a standardů pro oblast kybernetické bezpečnosti skupiny i s monitorováním její implementace, řízení správy rizik kybernetické bezpečnosti a řízení bezpečnostní organizace v rámci skupiny) a definuje cíle jako jsou:

- Ochranu skupiny společností skupiny před interními i externími hrozbami kybernetické bezpečnosti.

- Identifikaci, pochopení a správu rizik souvisejících s kybernetickou bezpečností.
- Identifikaci událostí, které by mohly negativně ovlivnit klíčová informační aktiva či klíčové obchodní procesy.
- Reakce na identifikované události a hrozny, které mají nebo by mohly mít negativní dopad na informační aktiva skupiny.
- Ustavení funkční organizace v rámci skupiny k prosazování těchto cílů na skupinové a regionální úrovni (až do úrovně samostatných legislativních subjektů).

Součástí dokumentu „Politika kybernetické bezpečnosti“ jsou dokumenty označované s označením „Standardy informační bezpečnosti“ kopírující kapitoly standardu ISO 27002.

Jestliže je dokument „Politika kybernetické bezpečnosti“ dokument popisující funkční požadavky a rozsah na obecné úrovni, jsou pak jednotlivé dokumenty nazývané „Standardy informační bezpečnosti“ upřesněním požadavků na minimální bezpečnostní opatření v principu ve dvou úrovních. První úroveň opatření s označením „MUST“ jsou opatření, která musí být splněna vždy a druhou úroveň tvoří opatření s označením „SHOULD“, která jsou také povinná, ale na rozdíl od první úrovně opatření je v tomto případě aplikovat výjimku. Pro představu je zde uveden výčet jednotlivých dokumentů těchto informačních standardů:

- Řízení aktiv
- Řízení přístupů
- Kryptografie
- Fyzická bezpečnost
- Bezpečnost provozu
- Bezpečnost komunikací
- Akvizice, vývoj a údržba systému
- Vztahy s dodavateli
- Řízení incidentů bezpečnosti informací
- Aspekty BCM z hlediska bezpečnosti informací
- Soulad s požadavky
- Bezpečnost lidských zdrojů

Na základě přehledu politik a základních standardů pro oblast kybernetické bezpečnosti je možné popsat obecné hodnocení stavu implementace ISMS v jedné z ES.

Řízení rizik

Pro oblast řízení rizik je důležité zmínit jako základní požadavek klasifikaci CIA bezpečnostních atributů pro informační aktiva, kde pro aplikace je dosažená úroveň dokumentace požadavků ze strany business vlastníků na úrovni 98-100 %. Je stanovena metodika pro posuzování bezpečnostních rizik s využitím nástroje poskytovaného v rámci celé skupiny. Tato metodika podporuje možnost dělání rozhodnutí vedením společnosti v případech, kdy je vyžadováno a vypracováno posouzení bezpečnostních rizik. Identifikovaná rizika mohou být v případě nízkého rizika automaticky přijata, rizika na úrovni vysokého rizika musí být ošetřena a rizika na úrovni střední, která je označována jako ALARP mohou být vlastníkem rizika akceptována nebo ošetřena. Výstupy posouzení rizik jsou přenášeny do katalogu rizik, kde je podpora plánu zvládání rizik. Pro jednotlivé oblasti úrovně implementace ISMS je níže uveden tabulka s popisem silných a slabých stránek dosažených pro jednotlivé oblasti definované Politikou kybernetické bezpečnosti včetně pravidel požadovaných v dokumentech jednotlivých „Standardů informační bezpečnosti“.

2.5 Nedostatky současného stavu

V současné situaci organizace má k dispozici nástroje, které umožňují posouzení současného stavu implementace ISMS. Jedná se ovšem o nástroje, které vyžadují odbornou znalost a zkušenosti z oblasti ISMS. Praxe tedy postrádá jednoduchý nástroj, který by mohl používat i uživatel bez hlubších znalostí a zkušeností z oblasti ISMS. Vlastní návrh řešení se tedy snaží takový nástroj vytvořit a zlepšit tak některé nedostatky současných nástrojů.

Tabulka č. 3: Silné a slabé stránky jednotlivých oblastí (vlastní zpracování)

KAPITOLA ISO 27002	Úspěšně implementováno	Příležitosti ke zlepšení
5 Politika bezpečnosti informací	Politiky bezpečnosti informací jsou definovány, přezkoumávány a aktualizovány	Možnost optimalizovat proces sběru podnětů a požadavků na aktualizaci politik.
6 Organizace bezpečnosti informací	Je definována organizace informační bezpečnosti s přidělenými pravomocemi a zodpovědnostmi. Bezpečnostní role jsou nominovány. Jsou nastaveny komunikační kanály s autoritami. Je zavedena politika ochrany informací při opráci na dálku.	Možnost rozšíření kontaktů na zájmové skupiny v segmentu energetiky za účelem lepší spolupráce. Sjednocení a zpřehlednění pravidel projektové metodiky s ohledm na požadavky informační bezpečnosti.
7 Bezpečnost lidských zdrojů	Je implementován proces náboru novch zaměstnancu, systém školení uživatelů, proces ukončení pracovního poměru a je nastaven proces disciplinárního řízení.	
8 Řízení aktiv	Aktiva jsou dokumentována včetně jejich vlasniku a požadavku zabezpečení informací formou CIA klasifikace aktiv.	Zlepšení dokumentace a zavedení při manipulaci, přepravě a mazání datových médií.
9 Řízení přístupů	Politiky pro řízení přístupů jsou definovány, vynucovány a je nově i zkoumány z pohledu jejich dodržování. Existují procesy pro správu jednoznačných identit uživatelů ve společnosti, jejich aktivace a deaktivace. Dokumentace procesů autentizace a autorizace uživatelů pro přístupy k datům, systémům a aplikacím jsou dokumentovány ve standardních šablonách s poisem prozesu zavedení, aktivace/deaktivace uživatele, přiřazení oprávnění uživateli, správu a modifikaci rolí, pravidelné revize oprávnění, přehled konfliktních rolí a přehled logování těchto činnosti.	Zlepšení kvality dokumentace autorizačních konceptů. Napojování všech nových a pokud je to ekonomicky přínosné i starších aplikací na centralní IAM s cenralní správou přístupů a rolí pro všechny aplikace. Zavedení MFA pro autentizace dle požadavků politik v závislosti na klasifikaci důvěrnosti a integrity informací. Zajištění pravidelných revizí přístupových oprávnění uživatelů k systémům, aplikacím a datům pro decentrálně spravované řízení přístupů (nenavázáno na IDM společnosti).
10 Kryptografie	Politiky s požadavky na využívání a správu kryptografických prostředku jsou dokumentovány. Vlastní PKI společnosti implementováno s možností vydávání klientských a serverových certifikátů veřejne uznávaných jako důvěryhodné. V praxi jsou kryptografické prostředky využívány.	Zlepšení a aktualizace dokumentace systémů využívající kryptografických prostředků s uvedením detailů nastavení z využívání kryptografických prostředků v jejich celém životním cyklu.
11 Fyzická bezpečnost	Politiky a požadavky pro fyzickou bezpečnost definovány a implementovány. Procesy pro řízení fyzických přístupů implementovány.	Potřeba modernizace systému pro řízení fyzických přístupů za účelem zefektivnění procesu jejich řízení a zvýšení bezpečnosti komunikací starších přístupových komunikačních zařízení pro řízení vzdálených fyzických přístupů.
12 Bezpečnost provoru	Je implementována malwerová víceúrovňová malware ochrana klientů, serverů, e-mail komunikací, Internet GW. Je implementován proces řízení změn provozního prostředí s posouzením informační bezpečnosti. Je aplikováno oddělení výnojového, testovacími a produktivního prostředí s ohledem na požadavky kritičnosti pro business, dostupnosti a ochrany informací.	Zlepšení úrovně provozní dokumentace využitím standardizovaných šablon pro aplikace a systémy. Posouzení a realizace plošného logování událostí na centralní Log server, nebo i SIEM s možností on-line vyhdnocování log událostí. Zlepšení úrovně měření a odstraňování závažných technických zranitelností především u starších systémů a aplikací ke zkrácení času implementace kritických záplat. Zlepšení dokumentace zodpovědností za oblast PVM u jednotlivých systémů a aplikací.
13 Bezpečnost komunikací	Jsou definovány polityky a je realizováno jejich vynucování pro oblast NDA, zabezpečení sítí a řízení přístupů k síťovým službám. Sítě jsou dle funkčních nebo bezpečnostních požadavků segmentovány. Nepotřebné síťové služby jsou deaktivovány. Nezabezpečené protokoly jsou v případě přenostu důvěrných informací a hesel v otevřené podobě deaktivovány. Jsou definovány pravidle provozu na sítích. Zapojení monitorování významných síťových segmentů a napojení na SOC/SIEM.	Rozšíření plošného monitoringu síťového provozu a napojení na SOC/SIEM. Optimalizace procesu provozu a patchování síťových prvků.
14 Akvizice, vývoj a údržba systému	Jsou definovány politiky s požadavky na řízení bezpečnosti při vývoji SW aplikací. Jsou definovány pravidla a požadavky na vývoj SW od externích dodavatelů.	Zlepšení procesu a požadavků pravidel při vývoji SW aplikací. Zavedení postupů a pravidel pro testování a akceptaci dodávek SW vývojových produktů od externích dodavatelů.
15 Vztahy s dodavateli	Politiky s požadavky bepečnosti pro dodavatele jsou dokumentovány. Šablony požadavků na bezpečnost pro externí dodavatele jsou dokumentovány a postupně zaváděny při podpisu nových smluv.	Plošné vynucení požadavků na technicko organizační opatření u dodavatelů. Zlepčení procesu pro definování bezpečnostních procesů v procesu nákupu. Zajistit plošné přenesení požadavků na dodavatele i na jejich subdodavatele. Zlepšení postupů při řízení dodavatelů formou kontrol a auditů na dodržování bezpečnostních požadavků kladených zákazníkem jako součást smluvního vztahu.
16 Řízení incidentů bezpečnosti informací	Existuji politiky, procesy a šablony pro hlášení podezření bezpečnostního incidentu, jejich posouzení a případné vyšetřování. Je zavedeno pravidelné reportování stavu bezpečnostních incidentů menežmentu. Je prováděna analýza a poučení z již uzavřených bezpečnostních incidentů.	Zpepčit komunikaci na dodavatelské subjekty s definováním jasných zodpovědností a povinností při identifikaci, hlášení a vyšetřování bezpečnostních incidentů.
17 Aspekty BCM z hlediska bezpečnosti informací	Pravidla pro bezpečnost informací jsou definována.	Podpora inicializace aktualizace a rozšíření BCM aktivity. Podpora projektu BCM při provádění BIA a realizaci DRP.
18 Soulad s požadavky	Jsou definovány politiky s požadavky. Je identifiková a aktualizaován seznam relevantní legislativy. Je navázána úzká spolopráce pro požadavky GDPR s DPO. Existuje a je podporován roční plán auditů kybernetické bezpečnosti.	

3 VLASTNÍ NÁVRHY ŘEŠENÍ

Kapitola vlastního návrhu řešení se zaměřuje na představení samotného nástroje, který má sloužit k hodnocení úrovně implementace ISMS. Tato kapitola poskytne informace o tom, jak nástroj vznikl a vysvětlí také logiku skrytou za jeho fungováním. Jedna část bude věnována funkcionalitě nástroje včetně ukázky použitých funkcí a celého nastavení Excel souboru. V závěru bude práce s nástrojem demonstrováno na modelovém příkladu.

3.1 Obecné informace

Jedná se o komplexní, ale pro uživatele přívětivý a jednoduchý nástroj ve formátu Excel tabulky, který má sloužit jako podpůrný nástroj pro usnadnění procesu hodnocení úrovně implementace ISMS a také jako podklad pro rozhodování managementu. Soubor je složen z několika listů, obsahující přehled všech kapitol ISO 27002, listy jednotlivých kapitol pro samotné hodnocení úrovně implementace ISMS, list pro celkový přehled dosažených výsledků a také list s připravenými grafy pro lepší znázornění výsledků. Nástroj také obsahuje jeden list, který běžnému uživateli není dostupný a slouží pouze jako podpůrný list pro zajištění některých z funkcí nástroje. Jednotlivé listy budou podrobněji vysvětleny v následujícím textu.

Hlavní snahou při vytváření nástroje bylo, aby hodnocení bylo prováděno na základě odpovědí respondentů, kteří nemusí mít v oblasti bezpečnosti informací detailní znalosti a zkušenosti. Celý proces hodnocení je tedy postaven pouze na tom, že uživatel odpovídá na sérii otázek pouze „ANO“, „NE“ anebo „N/R“, což znamená, že tázaná otázka není relevantní a nemá smysl ji brát v úvahu. Nástroj se tedy snaží být pro uživatele co nejpřívětivější a usnadnit mu práci. Primárním zdrojem při tvorbě nástroje byla rodina mezinárodních standardů zaměřená na řízení informační bezpečnosti v organizacích, kterou je **ISO 27000**. Pro tvorbu kontrolních otázek, které slouží k určení úrovně implementace pro každou oblast, bylo využito normy **ISO 27002**. Jak již bylo zmíněno v teoretické části, tato norma organizacím poskytuje soubor nejlepších praktik z oblasti informační bezpečnosti. ISO 27002 může být tedy použito jako

kontrolní seznam praktik, tedy přehled vhodných opatření, které lze praktikovat pro zvýšení bezpečnosti informací v rámci ISMS. Norma ovšem neukládá žádnou povinnost se těchto opatření držet, je na organizaci která opatření pro své podmínky a potřeby využije. Nástroj tedy slouží těm organizacím, které chtějí být v souladu s normami ISO 27000.

3.1.1 Rozložení Excel souboru

Celkově ISO 27002 definuje 114 opatření rozdělených do 14 oblastí pro zvýšení bezpečnosti informací v rámci ISMS. Ve stejném duchu je také rozdělen nástroj na jednotlivé listy.

Obrázek č. 4: Listy kapitol 5-18 (vlastní zpracování)

První list „Přehled kapitol“ obsahuje celkový přehled všech kapitol tak jak je definuje ISO 27002. Každá kapitola obsahuje jednu nebo více hlavních kategorií bezpečnosti. Pořadí kapitol nijak nevyjadřuje jejich význam, protože pro každou organizaci mohou být důležité jiné kategorie a jiná opatření. Každá hlavní kategorie obsahuje cíl opatření, které určují čeho má být dosaženo. Dále je v každé kategorii jedno nebo více opatření, která mohou být použita k dosažení cíle opatření. Všechny předešle zmíněné informace jsou k dispozici na listu „Přehled kapitol“.

Popisy opatření jsou v normě strukturovány následovně:

Opatření

Definuje specifické prohlášení o opatření, které splní cíle opatření.

Pokyny k implementaci

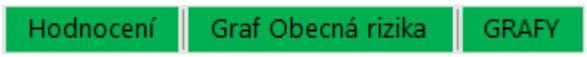
Poskytuje podrobnější informace pro podporu implementace opatření a dosažení cíle opatření. Pokyny nemusí být ve všech situacích zcela vhodné nebo dostačující a nemusí splňovat požadavky organizace na konkrétní opatření.

Další informace

Poskytuje další informace, které může být potřeba vzít v úvahu, například právní aspekty a odkazy na další normy. Pokud nejsou žádné další informace, které mají být poskytnuty, je tato část vynechána.

Na základě všech opatření a informací, které norma ISO 27002 poskytuje, byly vytvořeny kontrolní otázky, které slouží k určení dosažené úrovně v jednotlivých kapitolách a také k určení celkové úrovně implementace ISMS v rámci organizace. V kombinaci s vytvořenými otázkami je ke stanovení výsledné úrovně využito modelu zralosti procesu, který definuje COBIT 5.

Excel soubor dále obsahuje listy, které slouží k vyhodnocování získaných výsledků a jejich grafické interpretaci. List Hodnocení je zdrojem dat pro grafy.



Obrázek č. 5 Hodnocení a grafy (vlastní zpracování)

3.1.2 Model zralosti procesu, COBIT 5

COBIT 5 v tomto modelu pracuje celkem se šesti úrovněmi zralosti, kterých může proces dosáhnout. Úrovně nesou číselné označení 0-5 a tou nejlepší úrovní, které může proces dosáhnout je úroveň 5. Každá úroveň je přesně definována a popsána v COBIT 5:

0 Incomplete process (Neúplný)

Pro tuto úroveň je typické, že proces není kompletní anebo je neúspěšný při snaze dosáhnout definovaného cíle. Na této úrovni většinou neexistuje žádná evidence zamýšleného cíle nebo bývá velmi omezená. Často tato úroveň znamená úplnou neexistenci procesu, případně vysokou nekonzistenci při vykonávání procesu. Neúplnost procesu je také dána absencí definic rolí, odpovědností a celkové dokumentace. Někdy je také tato úroveň označována pojmem absence (chaos).

1 Performed process (Vykonávaný)

Tato úroveň znamená, že proces dosahuje svého zamýšleného cíle. Stále ovšem neexistuje žádná formální definice procesu, rolí a odpovědností. Aktivity jsou vykonávány jen jako reakce na příslušné podněty, není zde žádná proaktivita. Stále také ještě neexistuje dokumentace, proces je tedy minimálně konzistentní a postup při něm se liší na základě toho, kdo ho provádí. Zapojení managementu je minimální a zpětná vazba od zúčastněných stran není sbírána ani vyžadována. Tato úroveň je někdy označována jako počáteční (reaktivní).

2 Managed process (Řízený)

V případě této úrovně již k vykonávanému procesu definován cíl a na aktivity s ním spojené jsou formálně vymezeny zdroje. K tomu už je také potřeba aspoň malého zapojení managementu. Rozsah procesu je definován a odsouhlasen. Lidé provádějí aktivity na základě zkušeností, znalostí a kompetence k jejich roli. Výkonnost procesu se stává více konzistentní, avšak stále existují odchylky. Dochází také k základnímu měření a reportován výkonnosti, alespoň pro interní zúčastněné strany. Tato úroveň bývá označována jako opakovatelná (aktivní).

3 Established process (Zavedený)

Při této úrovni je již viditelné a evidentní zapojení managementu. Všechny aktivity jsou přiměřeně financovány. Začíná být kladen na proaktivní přístup, ale stále spíše převažuje reaktivní. Rozsah procesu je dokumentován. Pracovní postupy a instrukce jsou dokumentovány a udržovány aktuální. Všechny role jsou formálně známy, definovány a přiřazeny. Rozdíly v provedení různými týmy a lidmi jsou minimální. Výkonnost je měřena za pomoci různých metrik a reportována interním i externím zúčastněným stranám. Zpětná vazba od zúčastněných stran je aktivně vyžadována a je na ni brán ohled. Jinak je tato úroveň označována jako definovaná (proaktivní).

4 Predictable process (Předvídatelný)

Na této úrovni je již velmi málo pravděpodobné selhání při snaze dosažení stanového cíle. Organizace tedy musí zvážit, co by mohlo narušit chod procesu a nastavit vhodná opatření k eliminaci nebo alespoň snížení tohoto rizika. Dokumentace procesů je

konzistentní a obsahuje politiky, účel, cíl, postupy, role a metriky. Dokumentace je chráněna před neautorizovanou změnou a také centrálně ukládána a zálohována. Aktivity jsou prováděny vysoce konzistentně a odchylky se vyskytují řídce. Většina procesů, které lze automatizovat, jsou automatizovány. Existuje jasná a dokumentovaná definice úrovní oprávnění pro každou roli. Fondy a zdroje jsou plánovány a přidělovány s předstihem. Výkonnost procesu je průběžně měřena a monitorována. Jsou také nastavený prahové hodnoty pro generování varování v případě, že by měl být narušen chod procesu. Aktivity jsou vykonávány s vysokou konzistencí a generují předvídatelný výstup. Tato úroveň bývá označována za preventivní.

5 Optimising process (Optimalizovaný)
Poslední a zároveň nejvyšší úrovní, které může proces dosáhnout, je úroveň s označením 5. Všechny činnosti pro dosažení této úrovně jsou předmětem managementu a leadershipu. Aktivity jsou vykonávány konzistentně napříč všemi částmi organizace, kde jsou využívány. Zlepšování procesu je aktivně vyžadováno a implementováno v závislosti na hodnotě pro organizaci. Metriky a měření jsou používány k posouzení efektivnosti a kvality výstupů procesu. Procesy, postupy a funkce pravidelně podléhají auditu pro zjištění účinnosti a efektivnosti. Jsou sbírány data a zpětná vazba od zúčastněných stran pro analýzu trendů a možných zlepšení. Dochází k pravidelné komunikaci mezi organizací a poskytovatelem služby k zajištění toho, že je proces aktuální a efektivní.

Důležité je také zmínit, že k dosažení jakékoliv úrovně je potřeba, aby bylo plně dosaženo všech předchozích úrovní. Např. k dosažení úrovně 3 je potřeba, aby proces plně splňoval všechny požadavky úrovně 2 i 1.

Na základě normy ISO 27002 tedy byly formulovány otázky a následně rozděleny do jednotlivých úrovní, které definuje model zralosti procesu v COBIT 5.

Ve výsledku tabulka vypadá následovně:

6 Organizace bezpečnosti informací			
6.1 Interní organizace			
Cíl: Ustanovit řídící rámec pro zahájení a řízení implementace a provozu bezpečnosti informací v rámci organizace.			
6.1.1 Role a odpovědnosti bezpečnosti informací		Jsou všechny odpovědnosti za bezpečnost informací definovány a přiděleny?	**Splněno**
Zralost	**Atributy**	**Indikátory**	-
0: Neúplný	Neexistence	a) Je pravda, že odpovědnosti za bezpečnost informací nejsou definovány a přiděleny?	-
1: Vykonávaný	Výkonnost	a) Jsou známy odpovědnosti za bezpečnost informací?	NE
2: Řízený	Řízení výkonnosti	a) Jsou známy odpovědnosti a pravomoci pro klasifikaci informací a souvisejících aktiv?	NE
		b) Je zajištěna efektivní komunikace pro jasné přiřazení odpovědností?	NE
	Řízení pracovních produktů	a) Jsou odpovědnosti za bezpečnost informací známy všem relevantním uživatelům?	NE
3: Zavedený	Vymezení	a) Jsou identifikována a definována aktiva a procesy bezpečnosti informací?	NE
		b) Je ke každému aktivu přiřazena entita, která je za něj odpovědná a jsou podrobnosti této odpovědnosti dokumentovány?	NE
		c) Jsou stanoveny a dokumentovány úrovně oprávnění?	NE
		d) Jsou určení jednotlivci v dané oblasti kompetentní a je jim dána možnost udržovat krok s vývojem?	NE
		e) Jsou identifikovány a zdokumentovány koordinace a dohled nad bezpečností informací u dodavelských vztahů?	NE
	Zavedení	a) Je definice a přidělování odpovědností prováděno na základě vymezených pravidel?	NE
4: Předvídatelný	Měření	a) Jsou stanoveny kritéria pro měření úplnosti a aktuálnosti odpovědností za bezpečnost informací?	NE
		b) Jsou stanoveny cíle měření pro úplnost a aktuálnost odpovědností za bezpečnost informací?	NE
	Kontrola	a) Je prováděno pravidelné vyhodnocování úplnosti a aktuálnosti odpovědností za bezpečnost informací?	NE
5: Optimalizovaný	Inovace	a) Jsou na základě vyhodnocování vytvářena doporučení, sloužící ke zlepšení definování a určování odpovědností?	NE
	Optimalizace	a) Jsou využívány nástroje a automatizované procesy k efektivnějšímu udržení stanovených cílů?	NE
		Dosažená úroveň:	**0**

Obrázek č. 6: Excel nástroj, kapitola 6 (vlastní zpracování)

Pro všechny ostatní kapitoly a kategorie je vytvořena tabulka ve stejném duchu, liší se pouze otázkami, které jsou závislé na probírané kapitole.

3.2 Funkcionalita a nastavení Excel nástroje

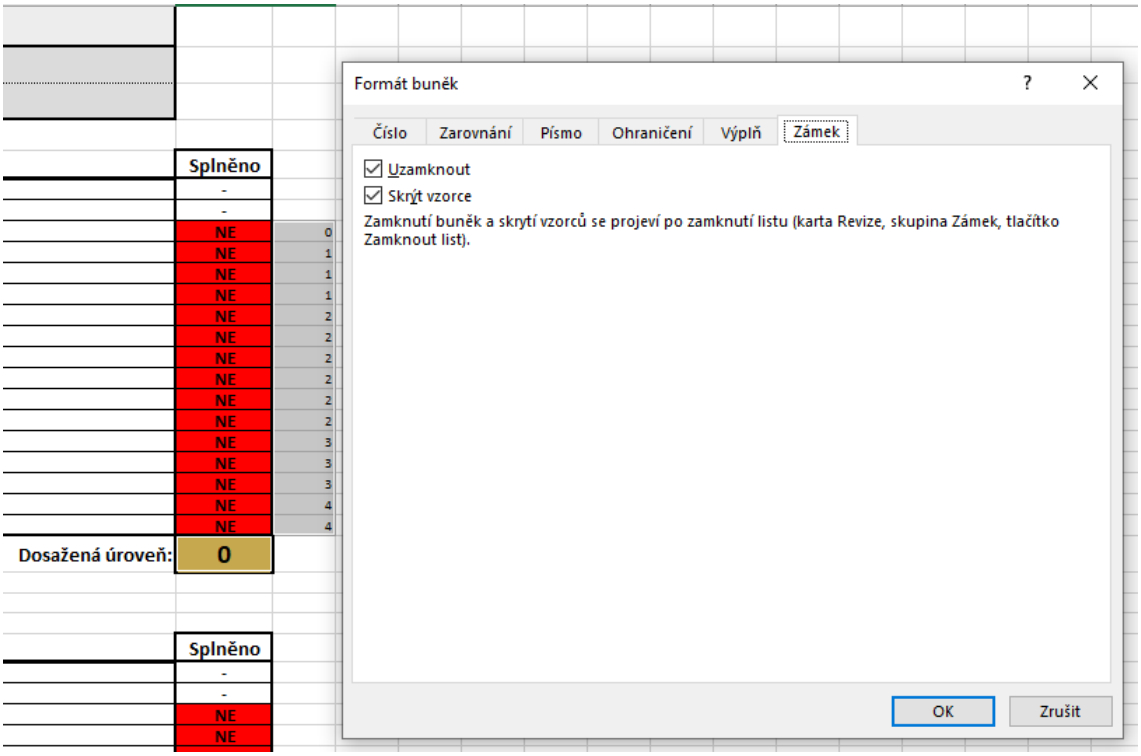
Tato kapitola představí fungování nástroje, použité funkce a nastavení Excel souboru.

3.2.1 Zamknutí listů a buněk

První a také důležitou vlastností soboru, která zajišťuje správné fungování nástroje je nastavení zamknutí listů a buněk. Toto nastavení zajišťuje, že uživatel, který s nástrojem pracuje, nebude schopen jakkoliv pozměnit fungování nástroje a změnit tak výsledek hodnocení.

Listy kapitol 5-18

V každém listu jednotlivých kapitol je nastaveno skrytí vzorců a obsahu buněk, které pro uživatele nejsou důležité a není potřeba, aby k nim měl přístup. Konkrétně se jedná o sloupec E, který skrývá pomocné hodnoty pro výpočet dosažené úrovně. Hodnoty ve sloupci E jsou navíc skryty použitím bílé barvy textu. Pole pod každou kapitolou, které zobrazuje dosaženou úroveň je zamknuto a je skryt vzorec, aby uživatel nemohl změnit hodnotu dosažené úrovně a její určení bylo určeno pouze pomocí vzorce.



Obrázek č. 7: Formát buněk (vlastní zpracování)

List Hodnocení

Tento list není určen primárně uživatelům v roli respondenta jako je tomu u listů 5-18, ale slouží k rychlému nastavení parametrů hodnocení zadaných pro konkrétní společnost uživatelem označovaného jako hodnotitel, který řídí a nakonec vyhodnotí výstupu celého procesu hodnocení dosažené úrovně implementace ISMS včetně prezentování nedostatků a obecných rizik z toho pro společnost vyplývajících.

Na listu hodnocení má uživatel možnost vyplnit pouze buňky, které jsou zvýrazněny světle žlutou barvou. Jedná se o požadovanou úroveň, které chce organizace dosáhnout a procentuální významnost každé podkapitoly přispívající k eliminaci rizika každé jednotlivé kapitoly z pohledu obecného rizika.

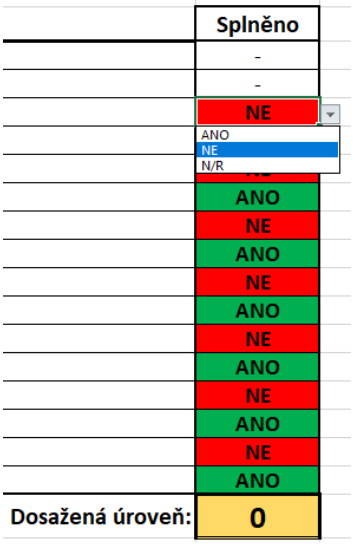
	A	B	C	D	E	F	G
1	Hodnocení oblastí dle normy ISO/IEC 27002						
2							
3	0: Neuplný 1: Vykonávaný 2: Řízený 3: Zavedený 4: Předvídatelný 5: Optimalizovaný						
4	Oblast				Dosažená úroveň	Požadovaná úroveň	Významnost Obecné riziko
5	5 Politiky bezpečnosti informací				0,00	3,00	
6		5.1 Pokyny managementu organizace k bezpečnosti informací			0,00	3,00	
7			5.1.1 Politiky pro bezpečnost informací		0	3	
8			5.1.2 Přezkoumání politik pro bezpečnost informací		0	3	
9	6 Organizace bezpečnosti informací				0,00	3,00	
10		6.1 Interní organizace			0,00	3,00	
11			6.1.1 Role a odpovědnosti bezpečnosti informací		0	3	
12			6.1.2 Princip oddělení povinností		0	3	
13			6.1.3 Kontakt s příslušnými orgány a autoritami		0	3	
14			6.1.4 Kontakt se zájmovými skupinami		0	3	
15			6.1.5 Bezpečnost informací v řízení projektů		0	3	
16		6.2 Mobilní zařízení a práce na dálku			0,00	3,00	
17			6.2.1 Politika mobilních zařízení		0	3	
18			6.2.2 Práce na dálku		0	3	

Obrázek č. 8: List Hodnocení (vlastní zpracování)

3.2.2 Podmíněné formátování a ověření dat

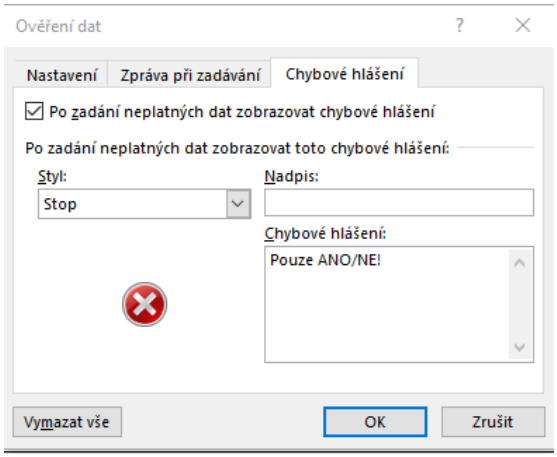
Listy kapitol 5-18

Uživatel tedy na listech jednotlivých kapitol může ve výsledku pouze odpovídat na položené otázky a to buď přímým vepsáním odpovědi do příslušné buňky nebo pomocí rozevíracího seznamu v buňce, který je definován na listu PARAMETRY a je pro běžného uživatele také skryt. Výchozí hodnota odpovědi je nastavena na NE a uživatel může volit z odpovědí ANO, NE a N/R. Pro buňky obsahující odpověď je také nastaveno podmíněné formátování a ověření dat.



Obrázek č. 9: Rozevírací seznam (vlastní zpracování)

Podmíněné formátování je závislé na textovém obsahu buňky a ověření dat umožňuje uživateli použít pouze předdefinované odpovědi.



Obrázek č. 10: Ověření dat (vlastní zpracování)

List Hodnocení

Podmíněné formátování na listě Hodnocení je využito pro znázornění velikosti rizika. Barva, která znázorňuje velikost rizika se řídí podle následující tabulky:

Tabulka č. 4: Barevné rozlišení rizik (vlastní zpracování)

0 = very high
1 = high
2 = medium
3-5 = low

Podmíněné formátování závisí na pomocné hodnotě, která se vypočítává ve sloupci H, vedle každé příslušné buňky:

	A	B	C	D	E	F	G	H
1				**Hodnocení oblastí dle normy ISO/IEC 27002**				
2								
3				0: Neuplný 1: Vykonávaný 2: Řízený 3: Zavedený 4: Předvídatelný 5: Optimalizovaný				
4				**Oblast**	**Dosažená úroveň**	**Požadovaná úroveň**	**Významnost Obecné riziko**	
5		**5**		**Politiky bezpečnosti informací**	**0,00**	**3,00**		1
6			**5.1**	**Pokyny managementu organizace k bezpečnosti informací**	**0,00**	**3,00**		1
7				**5.1.1 Politiky pro bezpečnost informací**	0	3		0
8				**5.1.2 Přezkoumání politik pro bezpečnost informací**	0	3		0
9		**6**		**Organizace bezpečnosti informací**	**0,00**	**3,00**		1
10			**6.1**	**Interní organizace**	**0,00**	**3,00**		1
11				**6.1.1 Role a odpovědnosti bezpečnosti informací**	0	3		0
12				**6.1.2 Princip oddělení povinností**	0	3		0
13				**6.1.3 Kontakt s příslušnými orgány a autoritami**	0	3		0
14				**6.1.4 Kontakt se zájmovými skupinami**	0	3		0
15				**6.1.5 Bezpečnost informací v řízení projektů**	0	3		0

Obrázek č. 11: Pomocné hodnoty ve sloupci H (vlastní zpracování)

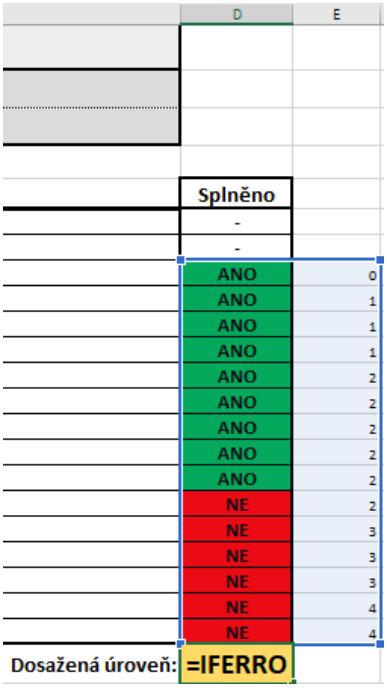
Sloupec H je pro běžného uživatele uzamčen a text má bílou barvu. Fungování výpočtu bude vysvětleno v následujícím textu. Také je nastaveno podmíněné formátování na dosažené úrovně jednotlivých kapitol. V případě, že je dosažená úroveň nižší než požadovaná, hodnota dosažené úrovně zčervená.

3.2.3 Použité vzorce a funkce

K fungování nástroje je využito pouze klasických funkcí, které nabízí Excel. Nástroj tedy neobsahuje žádné makra ani VBA kód.

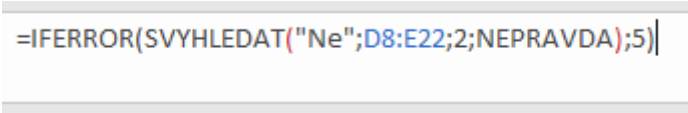
Listy kapitol 5-18, výpočet dosažené úrovně

K určení dosažené úrovně je na každém listu kapitol 5-18 využito funkce, která ve sloupci D vyhledává buňku, která obsahuje „NE“. Po nalezení první buňky splňující podmínku funkce odvodí dosaženou úroveň ze sloupce E, který obsahuje pomocná data pro určení úrovně. Číslo vedle odpovědi je vždy o jedno nižší, než úroveň, ke které je otázka položena. Jak již bylo zmíněno, pro splnění úrovně je potřeba splnění všech požadavků a to i předchozích úrovní. Stačí tedy jednou použít odpověď NE a již není možné dostat se na vyšší úroveň. Uživatel může dále odpovídat, ale výsledek to už nezmění. Přímo v Excel souboru použití funkce vypadá následovně:



Obrázek č. 12: Dosažená úroveň (vlastní zpracování)

Buňka dosažené úrovně obsahuje vzorec:



Obrázek č. 13: Vzorec výpočtu dosažené úrovně (vlastní zpracování)

Výsledná hodnota v tomto případě bude 2. Označení buněk je samozřejmě vždy přizpůsobeno pozici každé tabulky pro hodnocení.

Funkce IFERROR zajišťuje zobrazení úrovně 5 v případě, že uživatel odpoví na všechny otázky ANO. V takovém případě by totiž funkce SVYHLEDAT ve sloupci E nenašla žádnou hodnotu a vrátila by chybu. Parametr NEPRAVDA zajišťuje, že funkce úroveň vyhodnotí po nalezení prvního NE a s dalšími již nepočítá. Jinak by funkce vracela dosaženou úroveň podle poslední buňky, kterou by našla. Výchozí hodnota všech odpovědí je nastavena na NE, aby ve výchozím nastavení byla všude zobrazena dosažená úroveň 0. Sloupec E ani buňka dosažené úrovně nejsou uživateli přístupné.

List Hodnocení

K přenesení výsledných hodnot dosažených úrovní do listu Hodnocení je využito pouze rovnosti buňky z jiného listu kapitol 5-18, která obsahuje příslušnou hodnotu. Ve sloupcích E a F je využito funkce PRŮMĚR k určení dosažených a požadovaných úrovní. Pro výpočet hodnoty za jednu konkrétní kategorii je průměr nastaven na všechny hodnoty jednotlivých opatření:

6.1 Interní organizace	**=PRŮMĚR(E11:E15)**	**3,00**
6.1.1 Role a odpovědnosti bezpečnosti informací	3	3
6.1.2 Princip oddělení povinností	0	3
6.1.3 Kontakt s příslušnými orgány a autoritami	0	3
6.1.4 Kontakt se zájmovými skupinami	0	3
6.1.5 Bezpečnost informací v řízení projektů	0	3

Obrázek č. 14: Výpočet dosažené a požadované úrovně kategorie (vlastní zpracování)

Pro výpočet hodnoty za celou kapitolu je potom průměr nastaven na všechny hodnoty jednotlivých opatření:

6 Organizace bezpečnosti informací	=PRŮMĚR(	3,00
6.1 Interní organizace	E11:E15;E17:	3,00
6.1.1 Role a odpovědnosti bezpečnosti informací	E18)	3
6.1.2 Princip oddělení povinností	0	3
6.1.3 Kontakt s příslušnými orgány a autoritami	0	3
6.1.4 Kontakt se zájmovými skupinami	0	3
6.1.5 Bezpečnost informací v řízení projektů	0	3
6.2 Mobilní zařízení a práce na dálku	0,00	3,00
6.2.1 Politika mobilních zařízení	0	3
6.2.2 Práce na dálku	0	3

Obrázek č. 15: Výpočet dosažené a požadované úrovně kapitoly (vlastní zpracování)

Logika výpočtu je stejná pro dosaženou i požadovanou úroveň, ovšem v případě úrovně požadované (žlutá pole) jsou vstupní hodnoty definovány uživatelem.

Sloupec H na listu Hodnocení obsahuje pomocná data, která slouží k výpočtu obecného rizika pro organizaci. Jak bylo zmíněno dříve, běžný uživatel k těmto hodnotám nemá přístup. Velikost rizika je nejdříve určena pro jednotlivé kategorie a následně je určeno obecné riziko za celou kapitolu.

Velikost za jednotlivá opatření je vypočítána pomocí následující funkce:

6.1.1 Role a odpovědnosti bezpečnosti informací	0	3		=KDYŽ(E11>2;

```
=KDYŽ(E11>2;1;KDYŽ(E11=2;100;KDYŽ(E11=1;1000;10000)))*G11
```

Obrázek č. 16: Velikost rizika pro opatření (vlastní zpracování)

Tato funkce vypočítá pro každé opatření hodnotu, která určuje velikost obecného rizika pro organizaci na základě dosažené úrovně a významnosti opatření. Za celou kategorii je úroveň rizika určena na základě průměrné hodnoty ze všech opatření, které do kategorie spadají:

6.1 Interní organizace	0,00	3,00		=KDYŽ(
6.1.1 Role a odpovědnosti bezpečnosti informací	0	3		0
6.1.2 Princip oddělení povinností	0	3		0
6.1.3 Kontakt s příslušnými orgány a autoritami	0	3		0
6.1.4 Kontakt se zájmovými skupinami	0	3		0
6.1.5 Bezpečnost informací v řízení projektů	0	3		0

```
=KDYŽ(PRŮMĚR(H11:H15)<=1;1;KDYŽ(PRŮMĚR(H11:H15)<=100;2;KDYŽ(PRŮMĚR(H11:H15)<=1000;3;4)))
```

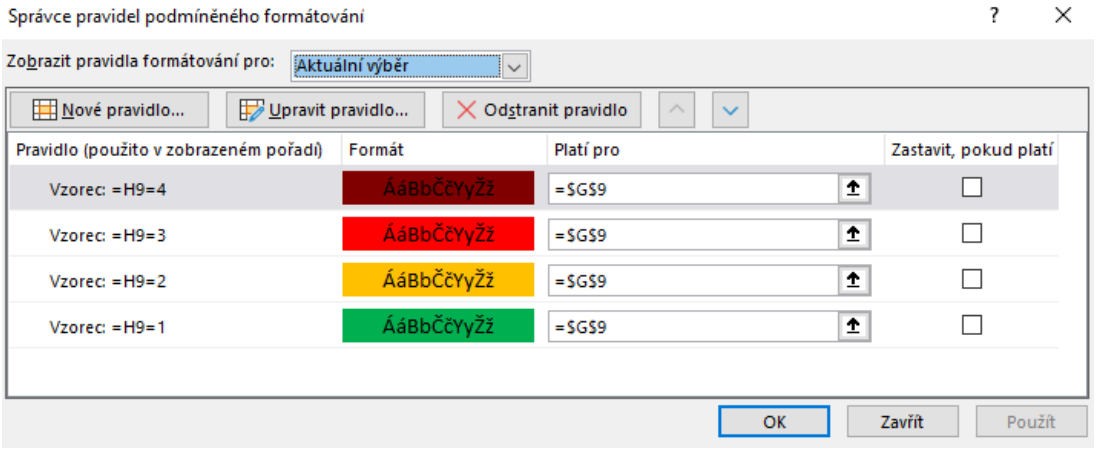
Obrázek č. 17: Velikost rizika celé kategorie (vlastní zpracování)

Hodnoty používané k výpočtům se odvíjí od Tabulky č.4, která byla rozšířena o další hodnoty:

Tabulka č. 5: Pomocné hodnoty (vlastní zpracování)

4	0 = very high	10000
3	1 = high	1000
2	2 = medium	100
1	3-5 = low	1

Hodnoty v levém sloupci slouží k označení úrovně rizika, na kterých závisí podmíněné formátovaní. Pravý sloupec obsahuje prahové hodnoty pro určení výše rizika.



Obrázek č. 18: Pravidla pro barevné označení rizika (vlastní zpracování)

Výše rizika pro celou kategorii je určena pomocí funkce MAX, která vybere nejvyšší riziko, které se v dané kapitole vyskytuje a použije ho také jako riziko pro celou kapitolu.

6 Organizace bezpečnosti informací	**0,00**	**3,00**		=MAX(H10;H16)
6.1 Interní organizace	**0,00**	**3,00**		1
6.1.1 Role a odpovědnosti bezpečnosti informací	0	3		0
6.1.2 Princip oddělení povinností	0	3		0
6.1.3 Kontakt s příslušnými orgány a autoritami	0	3		0
6.1.4 Kontakt se zájmovými skupinami	0	3		0
6.1.5 Bezpečnost informací v řízení projektů	0	3		0
6.2 Mobilní zařízení a práce na dálku	**0,00**	**3,00**		1

Obrázek č. 19: Riziko za celou kapitolu (vlastní zpracování)

List Hodnocení dále slouží jako zdroj dat pro listy Graf Obecná rizika a GRAFY. List GRAFY obsahuje předdefinované paprskové grafy, které zobrazují dosažené výsledky pro jednotlivé kategorie. Graf Obecná rizika souhrnně zobrazuje výši rizika pro

organizaci za všechny kapitoly 5-18. Grafy budou ukázány v rámci příkladu použití nástroje.

3.3 Příklad použití nástroje

Následující kapitola ukáže praktické využití nástroje a jeho výstupy s použitím modelových dat jedné z lokálních společností z oblasti energetiky. Data jsou částečně anonymizována z důvodu zachování anonymity a důvěrnosti informací hodnocené společnosti, z důvodu veřejného publikování této bakalářské práce. Anonymizace nemá praktický dopad na prezentované výstupy nástroje a předvedení funkčnosti nástroje. Pro přehlednost je vždy ukázána pouze část každého listu, celý soubor je k dispozici jako příloha této bakalářské práce. V příloze je soubor vyplněn tak, jak ukazuje tento praktický příklad.

První krokem při procesu posouzení současného stavu implementace ISMS je vyplnění listů 5-18, kde uživatel odpoví na všechny kladené otázky a tím určí hodnoty dosažených úrovní pro všechny kapitoly. Po vyplnění tabulka vypadá následovně:

	A	B	C	D
1	6 Organizace bezpečnosti informací			
2	6.1 Interní organizace			
3	**Cíl:** Ustanovit řídící rámec pro zahájení a řízení implementace a provozu bezpečnosti informací v rámci organizace.			
4				
5	**6.1.1 Role a odpovědnosti bezpečnosti informací**		Jsou všechny odpovědnosti za bezpečnost informací definovány a přiděleny?	**Splněno**
6	**Zralost**	**Atributy**	**Indikátory**	-
7	0: Neúplný	Neexistence	a) Je pravda, že odpovědnosti za bezpečnost informací nejsou definovány a přiděleny?	-
8	1: Vykonávaný	Výkonnost	a) Jsou známy odpovědnosti za bezpečnost informací?	Ano
9	2: Řízený	Řízení výkonnosti	a) Jsou známy odpovědnosti a pravomoci pro klasifikaci informací a souvisejících aktiv?	Ano
10			b) Je zajištěna efektivní komunikace pro jasné přiřazení odpovědností?	Ano
11		Řízení pracovních produktů	a) Jsou odpovědnosti za bezpečnost informací známy všem relevantním uživatelům?	Ano
12	3: Zavedený	Vymezení	a) Jsou identifikována a definována aktiva a procesy bezpečnosti informací?	Ano
13			b) Je ke každému aktivu přiřazena entita, která je za něj odpovědná a jsou podrobnosti této odpovědnosti dokumentovány?	Ano
14			c) Jsou stanoveny a dokumentovány úrovně oprávnění?	Ano
15			d) Jsou určení jednotlivci v dané oblasti kompetentní a je jim dána možnost udržovat krok s vývojem?	Ano
16			e) Jsou identifikovány a zdokumentovány koordinace a dohled nad bezpečností informací u dodavatelských vztahů?	Ano
17		Zavedení	a) Je definice a přidělování odpovědností prováděno na základě vymezených pravidel?	Ano
18	4: Předvídatelný	Měření	a) Jsou stanoveny kritéria pro měření úplnosti a aktuálnosti odpovědností za bezpečnost informací?	Ano
19			b) Jsou stanoveny cíle měření pro úplnost a aktuálnost odpovědnosti za bezpečnost informací?	Ano
20		Kontrola	a) Je prováděno pravidelné vyhodnocování úplnosti a aktuálnosti odpovědností za bezpečnost informací?	Ne
21	5: Optimalizovaný	Inovace	a) Jsou na základě vyhodnocování vytvářena doporučení, sloužící ke zlepšení definování a určování odpovědností?	Ne
22		Optimalizace	a) Jsou využívány nástroje a automatizované procesy k efektivnějšímu udržení stanovených cílů?	Ne
23				**Dosažená úroveň:** 3

Obrázek č. 20: Vyplněná kategorie 6.1.1 (vlastní zpracování)

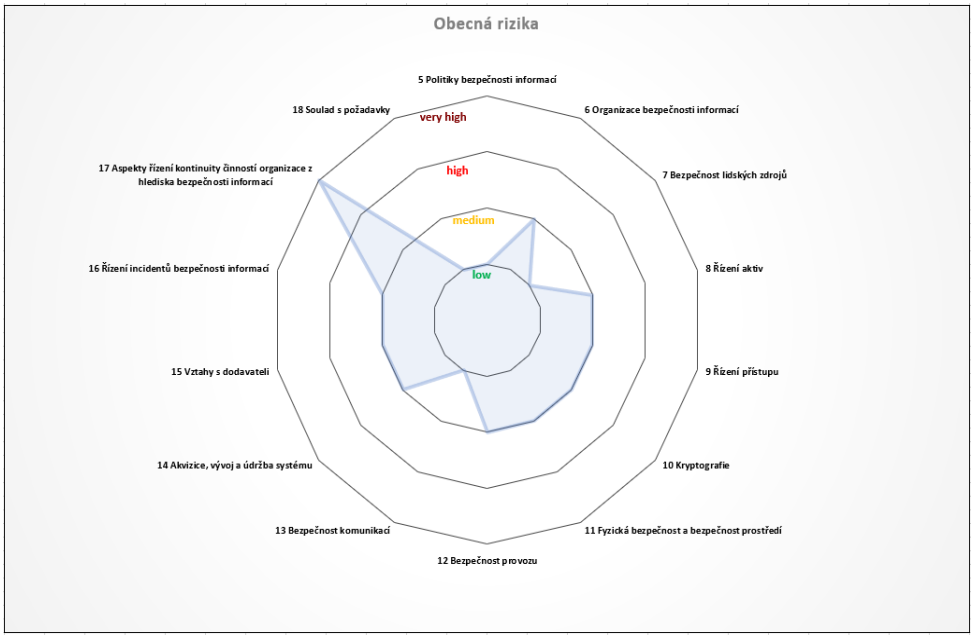
Stejný postup uživatel aplikuje na všechny listy kapitol. Tímto postupem jsou získány hodnoty pro samotné hodnocení, které jsou přeneseny na list Hodnocení. Na tomto listu uživatel dále musí určit požadovanou úroveň pro jednotlivá opatření, kterých chce organizace dosáhnout. V každé kategorii také musí definovat významnost jednotlivých opatření, vždy se dělí 100 % v rámci jedné kategorie mezi všechna opatření.

List Hodnocení po vyplnění vypadá následovně:

	A	B	C	D	E	F	G
1				**Hodnocení oblastí dle normy ISO/IEC 27002**			
2							
3				0: Neuplný 1: Vykonávaný 2: Řízený 3: Zavedený 4: Předvídatelný 5: Optimalizovaný			
4					**Celková úroveň**		
5					**2,9**	**3,0**	
6				**Oblast**	**Dosažená úroveň**	**Požadovaná úroveň**	**Významnost Obecné riziko**
7				**5 Politiky bezpečnosti informací**	**4,00**	**3,00**	
8				**5.1 Pokyny managementu organizace k bezpečnosti informací**	**4,00**	**3,00**	
9				**5.1.1 Politiky pro bezpečnost informací**	4	3	70%
10				**5.1.2 Přezkoumání politik pro bezpečnost informací**	4	3	30%
11				**6 Organizace bezpečnosti informací**	**3,14**	**3,00**	
12				**6.1 Interní organizace**	**3,00**	**3,00**	
13				**6.1.1 Role a odpovědnosti bezpečnosti informací**	3	3	35%
14				**6.1.2 Princip oddělení povinností**	4	3	20%
15				**6.1.3 Kontakt s příslušnými orgány a autoritami**	3	3	10%
16				**6.1.4 Kontakt se zájmovými skupinami**	3	3	5%
17				**6.1.5 Bezpečnost informací v řízení projektů**	2	3	30%
18				**6.2 Mobilní zařízení a práce na dálku**	**3,50**	**3,00**	
19				**6.2.1 Politika mobilních zařízení**	3	3	60%
20				**6.2.2 Práce na dálku**	4	3	40%
21				**7 Bezpečnost lidských zdrojů**	**3,17**	**3,00**	
22				**7.1 Před vznikem pracovního vztahu**	**3,00**	**3,00**	
23				**7.1.1 Prověřování**	3	3	60%
24				**7.1.2 Podmínky pracovního vztahu**	3	3	40%
25				**7.2 Během pracovního poměru**	**3,33**	**3,00**	
26				**7.2.1 Odpovědnosti managementu organizace**	3	3	35%
27				**7.2.2 Povědomí, vzdělávání a školení bězpečnosti informací**	4	3	40%
28				**7.2.3 Disciplinární řízení**	3	3	25%
29				**7.3 Ukončení a změna pracovního vztahu**	**3,00**	**3,00**	
30				**7.3.1 Odpovědnosti při ukončení nebo změně pracovního vztahu**	3	3	100%

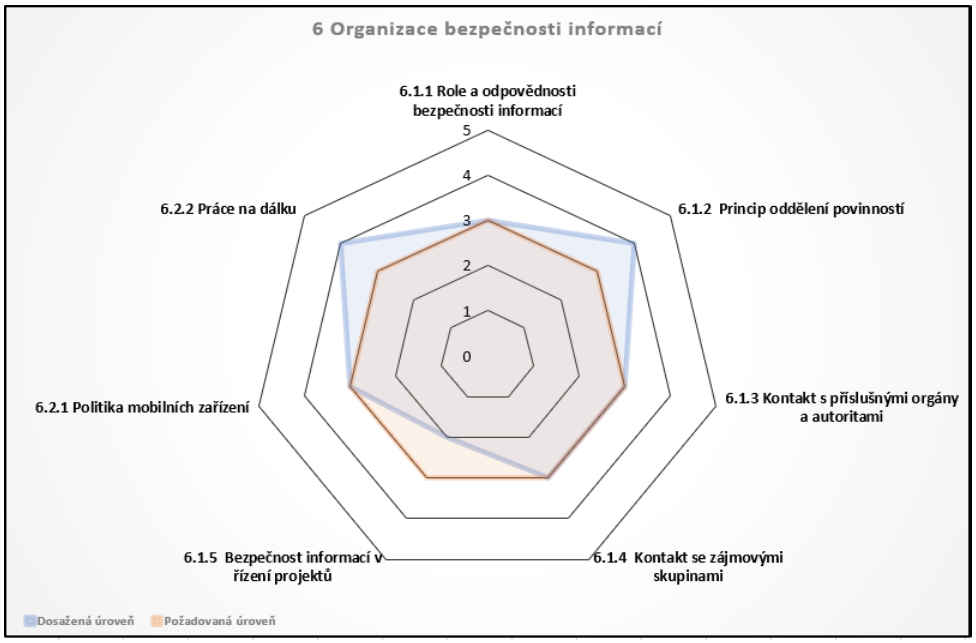
Obrázek č. 21: List Hodnocení obsahující data (vlastní zpracování)

Výsledné data se následně zobrazují v předdefinovaných grafem, které jsou dostupné na listech Graf obecná rizika a GRAFY. V případě této praktické ukázky vypadají grafy následovně:



Graf č. 1: Graf Obecná rizika (vlastní zpracování)

Z grafů pro jednotlivé kapitoly uvedu pouze jeden graf jako příklad, ostatní jsou opět k dispozici v souboru nástroje, který je k dispozici jako příloha této bakalářské práce.



Graf č. 2: Graf kapitoly 6 (vlastní zpracování)

3.4 Ekonomické zhodnocení

Náklady na posouzení současného stavu implementace ISMS zahrnují především využití lidských zdrojů a času, který posouzení věnují. Za předpokladu, že organizace bude chtít určit úroveň implementace ISMS bez využití externích odborníků, můžeme porovnat dvě situace. V jedné nebude mít zaměstnanec společnosti k dispozici nástroj k hodnocení úrovně implementace ISMS a ve druhé ano.

V první případě, bude muset zaměstnanec věnovat svůj čas nastudování požadavků, které organizacím klade norma ISO 27002. Dalším krokem bude manuální porovnávání reálného stavu s požadavky normy. Náročnost tohoto procesu bez využití nástroje můžeme odhadnout na 20 člověkodní s celkovými náklady 150 000Kč. V nákladech je zahrnuto vše, co s výkonem práce zaměstnance souvisí. Jedná se tedy o mzdu, odvody, náklady na cestování, náklady na vybavení zaměstnance (počítač, kancelářské potřeby, …) pronájem kanceláře a zajištění místa k výkonu práce.

V opačném případě, kdy bude mít zaměstnanec k dispozici nástroj k hodnocení úrovně implementace ISMS je situace následující. Zaměstnanec již nebude potřebovat zdlouhavě studovat normy a dále manuálně porovnávat současnou situaci s požadavky. Celkovou náročnost posouzení úrovně implementace ISMS s využitím nástroje můžeme tedy odhadnout na 5 člověkodnů s celkovými náklady 40 000Kč. Důležitým faktem také je, že s opakovaným používání nástroje roste kvalita zpracování a výstupů a zároveň klesá doba, kterou bude zaměstnanec potřebovat k posouzení úrovně implementace ISMS. Užitečné budou pro organizace také data z minulých posouzení, může tak sledovat svůj vývoj v oblasti ISMS.

Tabulka č. 6: Ekonomické zhodnocení (vlastní zpracování)

	bez nástroje	**s nástrojem**
člověkodny	20	5
celkové náklady	150 000Kč	40 000Kč

3.5 Přínos práce pro podnikovou praxi

Za hlavní přínos této bakalářské práce považuji výhody, které přináší vytvořený nástroj. Mezi přednosti práce s tímto nástrojem patří jednoduchost a rychlost provedení posouzení současného stavu ISMS. Tím zároveň dochází k úspoře času a zdrojů na realizaci posouzení. Nástroj zároveň umožňuje opakovatelné posouzení s konzistentními výstupy, které je dále možné porovnávat mezi sebou v různých časových úsecích. Dalším přínosem je také jeho obecnost. Nástroj lze jednoduše využít pro různé společnosti a modifikovat ho jejich potřebám. K dispozici je možnost nastavení požadované úrovně a určení významnosti kategorií/opatření z pohledu rizika pro organizaci.

Předpokládané cíle této práce a výstupy ve formě nástroje na posouzení dosažené úrovně ISMS byly prakticky ověřeny na jedné společnosti ze skupiny ES a výstupy získané z tohoto nástroje poskytovaly srovnatelné výsledky při porovnání s doposud prováděnými aktivitami na posouzení dosažené úrovně implementace ISMS pomocí interních zdrojů a nástrojů podporovaných externími konzultačními firmami. K dosažení výsledků s využitím tohoto nástroje však došlo k podstatnému zrychlení při

získání odpovědí od jednotlivých respondentů díky jednoduchým otázkám s možností odpovědi ANO/NE/NR a s využitím jen interních zdrojů společnosti. Nástroj, který je součástí návrhu vlastního řešení, vykázal výslednou hodnotu 2,86 již po prvním kole hodnocení tímto nástrojem. Hodnoty získané pro stejnou společnosti s podporou externích konzultantů dosahovaly hodnot 2,95.

ZÁVĚR

Bakalářská práce se zabývala tématem posouzení stavu implementace ISMS a hodnocením dosažené úrovně jednotlivých oblastí informační bezpečnosti, které definuje ISO 27002. Využití navrženého nástroje umožňuje sledovat současný stav a postupný vývoj úrovně implementace ISMS v organizaci.

Teoretická část se věnovala základním pojmům, obecným poznatkům souvisejících s oblastí ISMS a byly představeny základní rámce využívané pro ISMS. Tato kapitola tedy poskytla celkový přehled, který přiblíží probíranou problematiku.

Analýza současného stavu se zaměřila na představení energetické společnosti a současný stav bezpečnosti informací. Byla představena infrastruktura ICT ve společnosti a také strategie kybernetické bezpečnosti. Také byly definovány nedostatky, které se snaží zlepšit kapitola návrhu vlastního řešení.

Poslední kapitola představuje vytvořený nástroj, který slouží k posouzení současného stavu implementace ISMS. Nástroj využívá normy ISO 27002 k sestavení otázek, na které je možné odpovídat pouze ANO nebo NE. Otázky jsou dále rozloženy do jednotlivých úrovní dle modelu zralosti procesu, který definuje COBIT 5. Zodpovězením všech kladených otázek je získána dosažená úroveň za jednotlivé kapitoly a následně je určena celková úroveň stavu implementace ISMS. Tato kapitola popisuje také všechny funkčnosti nástroje a nastavení celého Excel souboru.

Na základě podobnosti výsledků vytvořeného nástroje s výsledky již používaných nástrojů v praxi lze usoudit, že bylo dosaženo vymezeného cíle této bakalářské práce, kterým bylo vytvořit nástroj sloužící k posouzení stavu implementace ISMS.

SEZNAM POUŽITÝCH ZDROJŮ

(1) ČSN ISO/IEC 27000. Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Přehled a slovník. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014

(2) ČSN ISO/IEC 27001. Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014

(3) POŽÁR, Josef, 2007. *Základy teorie informační bezpečnosti*. Praha: Vydavatelství PA ČR. ISBN 978-80-7251-250-8

(4) SKLENÁK, Vilém, 2001. *Data, informace, znalosti a Internet*. Praha: C.H. Beck. C.H. Beck pro praxi. ISBN 80-7179-409-0

(5) KOLOUCH, Jan a Pavel BAŠTA, 2019. *CYBERSECURITY*. Praha: CZ.NIC. ISBN 978-80-88168-34-8

(6) JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR, 2015. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze. ISBN 978-80-7251-436-6

(7) Hrozba, 2003. *Ministerstvo vnitra České republiky* [online]. [cit. 2020-04-14]. Dostupné z: https://www.mvcr.cz/clanek/hrozba

(8) DOUCEK, Petr, 2010. *Informační management*. Praha: Professional Publishing. ISBN 978-80-7431-010-2

(9) DOUCEK, Petr; NEDOMOVÁ, Lea; NOVÁK, Luděk; SVATÁ, Vlasta. *Řízení bezpečnosti informací.* Druhé přepracované vydání, Praha: Professional Publishing, 2011, ISBN 978-80-7431-050-8,

(10) POŽÁR, Josef. Systém řízení informační bezpečnosti. In Kný, Milan; Požár, Josef. Aktuální pojetí a tendence bezpečnostního managementu a informační bezpečnosti. Brno: Tribun EU, 2010, ISBN 978-807399-067-1

(11) ONDRÁK, V., P. SEDLÁK a V. MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: CERM, 2013. ISBN 978-80-7204-872-4

(12) ISO/IEC TR 27019:2013. Information technology – Security techniques – Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry. Geneva: International Organization for Standardization, 2013.

(13) ITIL (Information Technology Infrastructure Library). In: ManagementMania.com [online] [cit. 26.04.2020]. Dostupné z: https://managementmania.com/cs/information-technology-infrastructure-library

(14) COBIT 5 (Control Objectives for Information and related Technology). In: ManagementMania.com [online] [cit. 26.04.2020]. Dostupné z: https://managementmania.com/cs/cobit-control-objectives-for-information-and-related-technology

SEZNAM POUŽITÝCH OBRÁZKŮ

SEZNAM POUŽITÝCH TABULEK

SEZNAM POUŽITÝCH GRAFŮ