Zavedení systému řízení bezpečnosti informací holdingu Kovárna VIVA a.s.

Bc. Pavel Máčala

Diplomová práce
2016

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2015/2016

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Pavel Máčala**
Osobní číslo:	**A14792**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Informační technologie**
Forma studia:	**kombinovaná**
Téma práce:	**Zavedení systému řízení bezpečnosti informací holdingu Kovárna VIVA a.s.**
Téma anglicky:	**The Implementation of an Information Security Management System in the "Kovárna VIVA a.s." Company**

Zásady pro vypracování:

1. **Vypracujte literární rešerši na téma řízení bezpečnosti informací dle ISO/ČSN 27001.**
2. **Proveďte analýzu současného stavu řízení bezpečnosti ICT ve zvolené firmě.**
3. **Navrhněte způsob řešení ISMS dle vhodné metodiky.**
4. **Posuďte možnost reálné implementace svého řešení a toto dle možností realizujte.**
5. **Proveďte závěrečnou diskusi nad řešením celého projektu.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **MATES, Pavel a Vladimír SMEJKAL. E-government v České republice: právní a technologické aspekty. 2., podstatně přeprac. a rozš. vyd., V nakl. Leges vyd. 1. Praha: Leges, 2012, 464 s. Teoretik. ISBN 978-80-87576-36-6.**
2. **SMEJKAL, Vladimír a Karel RAIS. Řízení rizik ve firmách a jiných organizacích. 4., aktualiz. a rozš. vyd. Praha: Grada, 2013, 483 s. Expert (Grada). ISBN 978-80-247-4644-9.**
3. **BUCKSTEEG, Martin. ITIL 2011. 1. vyd. Brno: Computer Press, 2012, 216 s. ISBN 978-80-251-3732-1.**
4. **LUKÁČ, Ľubomír. IT management: jak na úspěšnou kariéru. Vyd. 1. Brno: Computer Press, 2011, 208 s. ISBN 978-80-251-3378-1.**
5. **SELECKÝ, Matúš. Penetrační testy a exploitace. 1. vyd. Brno: Computer Press, 2012, 303 s. ISBN 978-80-251-3752-9.**
6. **POŽÁR, Josef. Informační bezpečnost. 1.vyd. Plzeň: Aleš Čeněk, 2005. ISBN 978-80-86898-38-5.**

Vedoucí diplomové práce: **doc. Mgr. Roman Jašek, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **5. února 2016**

Termín odevzdání diplomové práce: **20. května 2016**

Ve Zlíně dne 5. února 2016

L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

doc. Mgr. Roman Jašek, Ph.D.
ředitel ústavu

Jméno, příjmení: Pavel Máčala

Název bakalářské/diplomové práce: Zavedení systému bezpečnosti informací holdingu Kovárna VIVA a.s.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové/bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 15. 5. 2016

.....
podpis diplomanta

ABSTRAKT

Téma řeší komplexně procesní zavedení systému řízení bezpečnosti informací s ohledem na procesy a technologie a v souladu s ISO/ČSN normami. Výstupem diplomové práce je návrh zavedení a příprava kompletní dokumentace včetně implementace procesů do firemního prostředí organizace.

Klíčová slova:

Systém řízení bezpečnosti informací, ISMS, analýza rizik, aktiva, normy ISO/ČSN, síťová bezpečnost, bezpečnostní politika firmy.

ABSTRACT

The theme addresses the comprehensive process safety management systém information with regard to processes and technology and in accordance with ISO / ČSN standards. The outcome of this thesis is the design and preparation of full implementation Documentation including the implementation of processes in corporate environments organization.

Keywords:

Information Security Management System , ISMS , risk analysis , asset, standards ISO / ČSN , network security , security policy of the company.

Poděkoval bych rád vyučujícímu panu doc. Mgr. Romanovi Jaškovi, Ph.D, řediteli Ústavu informatiky a umělé inteligence za jeho přednášky v předmětu Bezpečnost informačních systémů, které mi byly velkým přínosem pro zpracování tématu diplomové práce. Určitě bych ještě chtěl poděkovat opět panu doc. Mgr. Romanovi Jaškovi, Ph.D. jako vedoucímu mé diplomové práce za velkou vstřícnost v odborných radách při konzultacích.

Dále bych nechtěl opomenout poděkovat svému zaměstnavateli, firmě Kovárna VIVA a.s., která mi vycházela vstříc, pokud se jednalo o možnost zpracovat firemní téma diplomové práce.

Poděkování, motto a čestné prohlášení, že odevzdaná verze bakalářské/diplomové práce a verze elektronická, nahraná do IS/STAG jsou totožné ve znění:

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

V teoretické části práce bude provedena literární rešerše o problematice ISMS a jeho zavádění dle ISO/ČSN 27001.

Cílem této diplomové práce je provést analýzu současného stavu řízení bezpečnosti ICT v Kovárně VIVA a.s. a na základě této analýzy navrhnout způsob řešení ISMS dle vhodné metodiky.

Dalším krokem je posouzení možnosti reálné implementace mého řešení a jeho samotná realizace.

Vzhledem k tomu, že firma Kovárna VIVA a.s. je plně výrobní společností, je si vedení společnosti a management vědom obrovského konkurenčního boje.

Firma vyrábí zápustkově kované výkovky, které i následně obrábí. Většina těchto výrobků směřuje do automobilového průmyslu.

Aby firma na trhu s těmito komoditami byla úspěšná, musí být schopna vyrábět složitější tvary výkovků, aby tak předběhla konkurenci tureckých, indických a španělských kováren.

A tady nastává pro firmu jedna s priorit. Jak si uchránit své "know how" (vědět jak na to), aby se nedostaly tyto informace ke konkurenci, která by je zneužila ve svůj prospěch a firma Kovárna VIVA a.s. by mohla být vytlačena z konkurenčního boje.

Informace, které kolují v různých podobách firmou, se stávají velmi důležitým prvkem firmy, a proto je firma musí chránit proti zneužití v konkurenčním boji.

Je pravdou, že neexistuje super dokonalý systém ochrany informací, protože hlavní slabinou je selhání lidského faktoru. Tady musí nastoupit management firmy a snažit se svým přístupem k zaměstnancům zajistit v největší míře loajalitu zaměstnanců k firmě.

Loajalita zaměstnanců k firmě je v dnešní době pro ochranu firemních dat prvořadým úkolem firmy. Firma si musí být vědoma, že neloajální zaměstnanec je potenciálním nebezpečím úniku cenných dat nebo informací z firmy.

Neméně důležitým bodem v ochraně dat a informací je jejich ochrana s využitím bezpečnostních informačních technologiích, které máme k dispozici. Důležité je si uvědomit, že k ideální ochraně informací a dat se můžeme jen přiblížit, ale nemůžeme ji dosáhnout, protože narážíme nekompromisně na lidský faktor, který je pro firmu nepředvídatelný.

Základním prvkem v ochraně firemních dat je zavedení systému ISMS podle norem ISO/ČSN 27001. Samozřejmě, že není možné zavést najednou všechny možné prvky zabezpečení, protože to obnáší pro firmu vyčlenit z rozpočtu firmy nemalou finanční částku a určitě by byl zbytečný takový rozsah zabezpečení jako např. u Ministerstva vnitra ČR.

Výhodou firmy Kovárna VIVA a.s. je, že již několik let obhajuje a je držitelem certifikátů EN ISO 9001: 2008; certifikátu z oblasti ekologie EN ISO 14001 :2004 a certifikátu pro "automotive" (automobilový průmysl) ISO/TS 16949 : 2009. Zkušenosti se zaváděním těchto norem se ve velkém mohou vyžít i pro zavedení ISMS podle normy ČSN ISO/IEC 27001 a dalších norem na tuto normu navazující.

I. TEORETICKÁ ČÁST

1 CO JE TO INFORMACE, DATA A INFORMAČNÍ SYSTÉM

1.1 Pojem informace

Pojem informace patří k nejobecnějším kategoriím současné vědy, řadí se mezi takové pojmy, jako hmota, vědomí, myšlení, poznání, pohyb, čas. Podle toho, ve kterém vědním oboru, nebo ve které oblasti lidské činnosti se používá, jsou aplikovány přístupy k jejímu zkoumání a jsou k dispozici různé způsoby jejího chápání, definování. [6]

Informace jsou takové informace obíhající v organizaci a využívané v ovlivňování technologických, manažerských, informačních a jiných procesech. Týkají se především vztahů lidí k manažerské aktivitě, vztahů mezi sebou, jejich vzájemnému působení, potřeb, zájmů, cílů apod. [6]

Z toho plyne, že informace se stává rovněž zbožím, má jistou cenu, hodnotu, která závisí na mnoha faktorech. Lze ji kupovat a prodávat. Takže potřebujeme posoudit hodnotu informace. Důležitá je vnitřní hodnota zprávy, její novota pro příjemce. Proto je tedy cennější takové sdělení, které přináší manažerovi, spolupracovníkovi něco nového, co dosud nevěděl a co může užít ve své činnosti. [6]

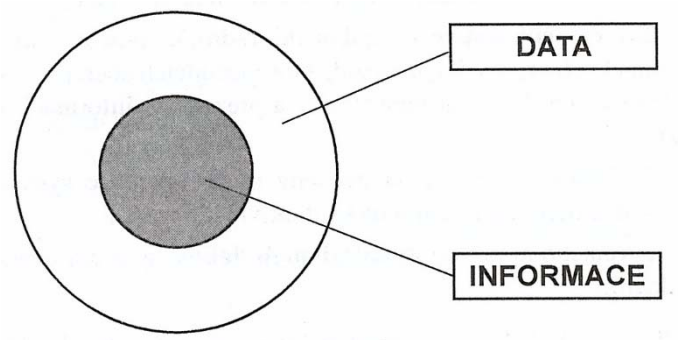
1.2 Pojem data

Data nebo také údaje jsou fakta získaná čtením, pozorováním, výpočtem, měřením, vážením, kreslením atd. Data, údaje chápeme jako:

- Vyjádření faktů a poznatků ve formě, která je vhodná pro další zpracování,
- Vyjádření skutečností a myšlenek v předepsané podobě tak, aby je bylo možné přenášet a zpracovávat,
- Objektivní, sledovatelné vyjádření skutečností nebo znalostí na nějakém médiu tak, že je lze předávat. [6]

Každá informace je tedy údajem, datem, ale jakákoliv uložená dat se nemusejí stát nutně informací. Informací se totiž stanou teprve v okamžiku, kdy příjemci přinesou něco nového. Pojem data chápeme jako zkratkové profesionální značení pro čísla, text, zvuk, obraz, atd.

Tuto skutečnost lze schematicky vyjádřit vztahem množiny a podmnožiny na obrázku 1. [6]



Obrázek 1: Vztah obsahu data a informace [6]

1.3 Informační proces

Informační systém je soubor prvků, které jsou spojeny vzájemnými vztahy, vazbami. Prvky informačního systému tvoří místa transformace dat a informací jako hardware, lidé, programy apod. Vazby jsou tvořeny především spojování kanály, vzájemné působení mezi prvky. [6]

1.4 Informační proces

Pod informačním procesem rozumíme provádění jistých pracovních činností s informacemi. Tím se mění procesy, činnosti a chování organizace. Informační proces je uzavřený cyklus, kterým informace prochází od svého vzniku až ke svému užití. Na jeho začátku i konci je nějaká informační potřeba. Informační proces je zabezpečovaný vhodným informačním systémem jako je sled operací s daty a informacemi, který zejména obsahuje tyto kroky:

- Získávání (sběr) informací,
- přenos informací od zdroje k místu zpracování a jejich soustřeďování,
- registraci (evidování) na místě zpracování,
- ukládání informací pro jejich budoucí využití,
- zpracování informací, zahrnující nejen třídění a posuzování kvality vlastností, ale i vyhledávání doplňkových informací a jejich výběr, analýzu a syntézu, vytváření kvalitativně nových informací,
- využívání informací, což je naplněním vlastního cíle práce s informacemi [6]

1.4.1 Členění druhů informací pro činnost organizace

Jedná se především o tyto druhy informace:

- **Odborné informace**
  Jedná se o informace výrobní, technologické, technické, o politice organizace, výrobních postupech, patentové informace, ovládnutí nové technologie aj.
- **Informace právní**
  Jejím obsahem jsou ustanovení zákonů, vyhlášek, předpisů a jejich výklad s doporučením přístupným všem zaměstnancům.

- **Informace ekonomické**
  Aby bylo účetnictví firmy, vztahy se zákazníky, vztahy k finančním úřadům v pořádku se zákony, využívá většina firem poradenství právníků.
- **Informace o okolním prostředí**
  Důležitými informacemi jsou takové informace, které se týkají okolního prostředí a oblastí, kterou se organizace zabývá. Vlastní rozbor informací z této oblasti je předpokladem úspěšnosti organizace. Jsou to získané informace z veletrhů, konferencí, výstav, porad aj.
- **Informace ze zahraničí**
  Zde jsou to informace z různých stáží manažerů v zahraničí a mezinárodních symposiích.
- **Informace všeobecné**
  Do této části spadají rekvalifikační kurzy, vzdělávání studiem, odbornými kurzy, aj. Je důležité, aby každý zaměstnanec měl rozhled ve svém oboru, ale i o světovém dění.
- **Informace organizačně technické**
  Jsou to informace o organizaci, týkajících se záměrů a koncepcí organizačního rozvoje (strategický plán rozvoje organizace), vztahů mezi organizačními útvary, silných a slabých stránkách organizace, koordinace mezi pracovišti, apod.
- **Informace personální**

Informace z oblasti personální politiky, charakteristik a vlastností manažerů i spolupracovníků, klasifikace potenciálu lidských zdrojů aj., jsou nezbytné pro manažerskou činnost.

- **Informace o informačním systému organizace**
  Většinou se jedná o informace dosti citlivé, např. o závislosti organizace na jejím informačním systému, jeho silných a slabých stránkách apod.
- **Informace specifické**
  Ty je nutno chránit podle zákona, tj. informace tvořící státní tajemství, osobní a zdravotní informace, vojenské, kriminalistické apod. [6]

1.5 vysvětlení základních pojmů informační bezpečnosti

1.5.1 Vybrané pojmy informační bezpečnosti

Informační bezpečnost jako obor zavádí celou řadu nových pojmů a definic. Pro správné pochopení problematiky informační bezpečnosti je nutné vysvětlit alespoň některé základní a nejdůležitější.[6]

ISMS (Information Security Management System) česky Systém řízení bezpečnosti informací je část cekového systému řízení organizace, založená na přístupu (organizace) k rizikům činností, která je zaměřena na ustanovení, zavádění, provoz, monitorování, přezkoumání, údržbu a zlepšování bezpečnosti informací.[7]

Aktivum (Asset). Aktiva jsou všechny hmotné i nehmotné statky, vše, co má pro majitele informačního systému jistou hodnotu. Za nejcennější aktiva se považují peníze, majetek a především dat a informace, jejichž zneužití, ztráta nebo modifikace by organizaci nebo osobě způsobily určitou škodu. [6]

Bezpečnost (Security). Pod pojmem bezpečnost je chápána vlastnost nějakého objektu nebo subjektu (informačního systému či technologie), která určuje stupeň, míru jeho ochrany proti možným škodám a hrozbám**.** [6]

Hrozba (Threat) je skutečnost, událost, síla nebo osoby, jejichž působení (činnost) může způsobit poškození, zničení, ztrátu důvěry nebo hodnoty aktiva. Hrozba může ohrozit bezpečnost (např. přírodní katastrofa, hacker, zaměstnanec aj.). [6]

Ocenění rizik (Risk Assessment) je proces vyhodnocení hrozeb, které působí na informační systém s cílem definovat úroveň rizika, kterému je systém vystaven. Cílem je zjištění, jsou-li bezpečnostní opatření dostatečná, aby snížila pravděpodobnost vzniku škody na přijatelnou úroveň. [6]

Riziko (Risk) je pravděpodobnost, s jakou bude daná hodnota aktiva zničena nebo poškozena působením konkrétní hrozby, která působí na slabou stránku této hodnoty. Je to tedy míra ohrožení konkrétního aktiva. [6]

Útokem, který je nazýván rovněž bezpečnostní incident rozumíme využití zranitelného místa ke způsobení škod/ztrát na aktivech IS. Při analýze možných forem útoků na IT se používají tzv. **penetrační testy**, které otestují připravenost IT odolat těmto útokům nebo odhalí slabinu informačního systému.

V souvislosti s termínem bezpečnost organizace a jejího informačního systému, použití informačních a komunikačních technologií (IS/ICT) je nutné se zmínit ještě o bezpečnosti organizace nebo firmy a informační bezpečnosti.

Jejich vzájemné vztahy nadřízenosti a podřízenosti jsou zobrazeny na obrázku číslo 2. [7]

Obrázek 2: Vztah úrovní bezpečnosti v organizaci [7]

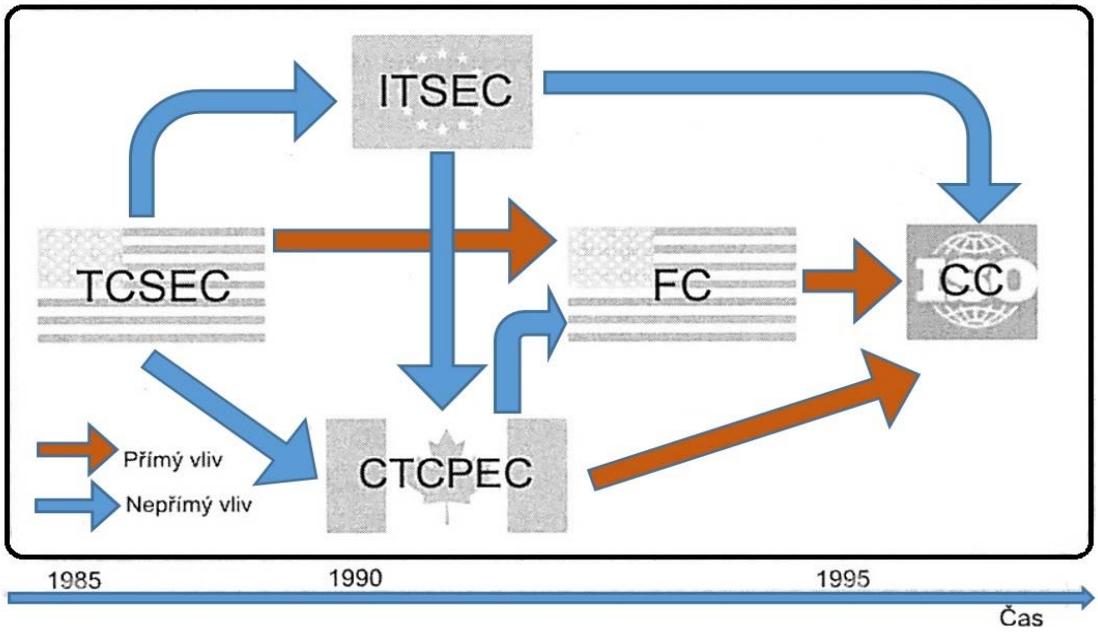
1.6 Historický vývoj hodnocení bezpečnosti

Vývoj bezpečnosti informací a jejího systému řízení nemá příliš dlouhou tradici. Jeho intenzivní potřeba začala vznikat v době, kdy se lokální počítače začaly propojovat do počítačových sítí a významně se rozšířily komunikační kanály mezi počítači různých právních subjektů a organizací. První pohledy na bezpečnost a její řízení se omezovaly jen na bezpečnost informačních systémů a technologií než na nějaké systematické řízení celé bezpečnosti informací. [7]

Prvními kritérii, která v roce 1983 vytvořilo Národní středisko počítačové bezpečnosti USA (National Computer Security Center), je doporučení Kritéria hodnocení důvěryhodných výpočetních systémů Ttrusced Computer Security Evaluation Criteria – TCSEC) (TCS_85), často nazýváno podle barvy obalu Oranžová kniha. V roce 1985 byl tento dokument uznán jako normaMinisterstva obrany USA (department of Defense) a prakticky od té doby tvoří základ pro soubor norem a doporučení, označovaných jako Duhová série (Rainbow Series). Série dnes čítá desítky publikací, mezi nejvýznamnější patří Interpretace bezpečnosti pro počítačové sítě (TG_87) jako Červená kniha a Interpretace bezpečnosti pro systémy řízení báze dat (TG_91) jako Purpurová kniha. [7]

Obdobným směrem se ubíraly i aktivity v Evropě, které byly zpočátku samostatně vyvíjeny jednotlivými státy. Tak vznikla v roce 1990 norma nazývaná Kritéria hodnocení bezpečnosti informačních systémů (Information Technology Security Evaluation Criteria – ITSEC (ITS_91)). Ta pak byla převzata jako norma celou Evropskou unií, kde bylo její správou pověřeno Generální ředitelství (DG) XIII. Přibližně ve stejné době byla rozpracována i Kanadská kritéria hodnocení bezpečnosti počítačových produktů (Canadian Trusted Computer Product Evaluation Criteria – CTCPEC (CTC_93)), ve kterých je sledování bezpečnosti informačních systémů a informačních technologií podstatně rozšířeno a přibližuje se potřebám komerčních organizací. Nedostatky kritérií TCSEC vedly k přepracování americké normy, a tak v prosinci roku 1992 organizace NIST (National Institute of Standards and Technology) a NSA (National Security Agency) vydávají Federální kritéria pro bezpečnost informačních technologií (Federal Criteria – FC). [7]

Od té doby odpovědné orgány jednotlivých zemí společně pracují na vzniku Společných kritérií (Cpmmon Criteria – CC, ISO/IEC 15408 část 1 až 3). Historický vývoj je zachycen na obrázku 3. [7]



Obrázek 3: Vývoj a vztahy kritérií hodnocení bezpečnosti [7]

1.7 Historie normalizace řízení bezpečnosti informací

Dalším vývojovým krokem v řízení bezpečnosti se staly normy, které vznikly ve Velké Británii na základě spolupráce sektoru státní a veřejné správy se sektorem komerčním. Tyto normy, vycházející z předchozích kritérií hodnocení bezpečnosti, si daly za úkol připravit použitelné a používané standardy řízení bezpečnosti informací pro běžné komerční organizace, a proto představují poněkud flexibilnější pohled na řízení bezpečnosti než normy, které vznikly na základě požadavků složek armády a policie. Historický vývoj, spolu s další prognózou vývoje je uveden v tabulce, která je součástí přílohy **P I** – Historický vývoj norem řízení bezpečnosti informací.

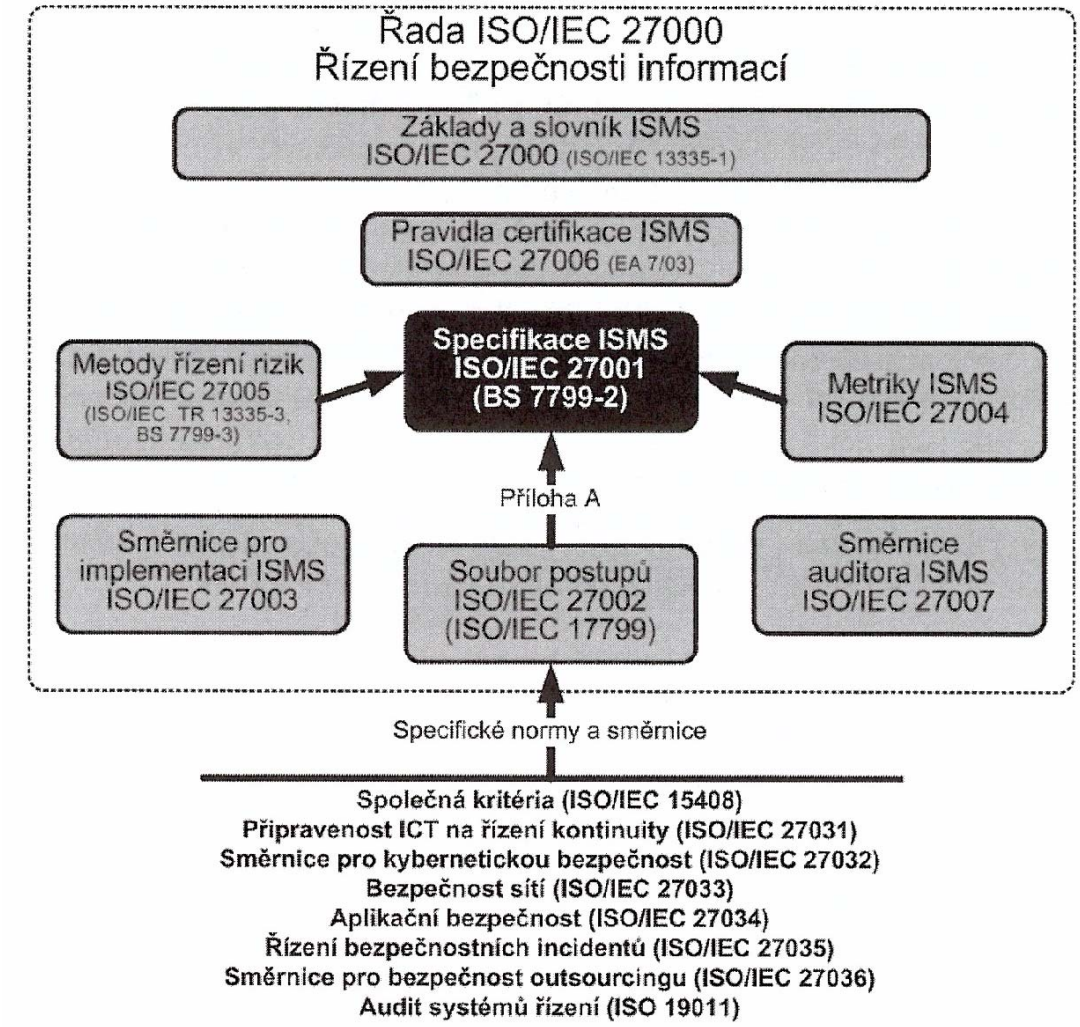
1.8 ISO/IEC 27000 – Řízení bezpečnosti informací

Odpovědnost za normalizaci bezpečnosti informací je v rámci Mezinárodní organizace pro normalizaci ISO zastřešena komisí JTC1/SC27 – Bezpečnostní techniky IT. V poslední době je důležitou snahou této subkomise harmonizovat přístupy a vzájemně provázat vydávané

normy, což ne vždy bývalo v minulosti úplnou samozřejmostí. Teprve nedávno začaly tyto aktivity přinášet hmatatelné výsledky. Nejvíce patrné je to v přístupu k normám, které definují pravidla pro **systém řízení bezpečnosti informací (ISMS)** a které jsou podkomisí vnímány jako jeden z nejdůležitějších prvků normalizace bezpečnosti informací. [7]

Na jaře roku 2005 organizace ISO ohlásila zavedení nové řady norem ISO 27000, která se bude věnovat problematice řízení bezpečnosti informací. [7]

Nová řada norem pro řízení bezpečnosti informací ISO/IEC 27000 a jejím základem jsou normy, jež jsou uvedeny na obrázku 4. [7]



Obrázek 4: Koncept řady ISO/IEC 27000 pro řízení bezpečnosti informací [7]

Stejně jako u jiných systémů řízení (např. jakosti ISO9001, životního prostředí ISO 14001) je za jádro normalizace považována definice systému. V případě ISMS se tak stává klíčovým prvkem mezinárodní norma ISO/EIC 27001:2005 – Systém řízení bezpečnosti informací – Požadavky (Information security management systém – Requirements), která vychází ze známého standardu BS 7799-2 a která byla vydána v říjnu roku 2005. [7]

Nejnovější vydání normy ISO/IEC 27001:2013 je přepracované druhé vydání 2013-10-01.

Druhou nejdůležitější normou této řady je norma ISO/IEC 27002 – Soubor postupů pro řízení bezpečnosti informací (Code of practice for information security management), která obsahuje podrobný výklad vhodných bezpečnostních opatření. Tato norma byla vydána v polovině roku 2005 a to ještě s označením ISO/IEC 1799:2005. Nejnovější vydání normy ISO/IEC 27002:2013 je přepracované vydání z roku 2013.

Na počátku roku 2007 se dalším přírůstkem řady ISO/IEC 27000 stala norma ISO/IEC 27006 – Požadavky na akreditaci orgánů provádějících certifikaci systémů řízení bezpečnosti informací (Requirements for the accreditation of bodies providing certification of information management systems). Tato norma upřesňuje pravidla pro udělování certifikací ISMS a podle ní musí postupovat certifikační orgány, které služby spojené s certifikací IMS poskytují. V roce 2013 byla dokončena revize této normy. Úplný přehled historického vývoje norem je v tabulce přílohy **P I**. [7]

1.9 Systém řízení bezpečnosti informací – ISMS (Information security management system)

V dnešní době vyhroceného konkurenčního boje mezi organizacemi se již žádná z nich neobejde bez řízení bezpečnosti informací. Bezpečnost se tak stala nedílnou součástí každodenního řízení a vnitřní kultury organizace. Aby byly organizace schopny řízení bezpečnosti cíleně, účinně a účelně rozvíjet, je potřebné na tento prvek řízení pohlížet jako na systém řízení bezpečnosti informací. [7]

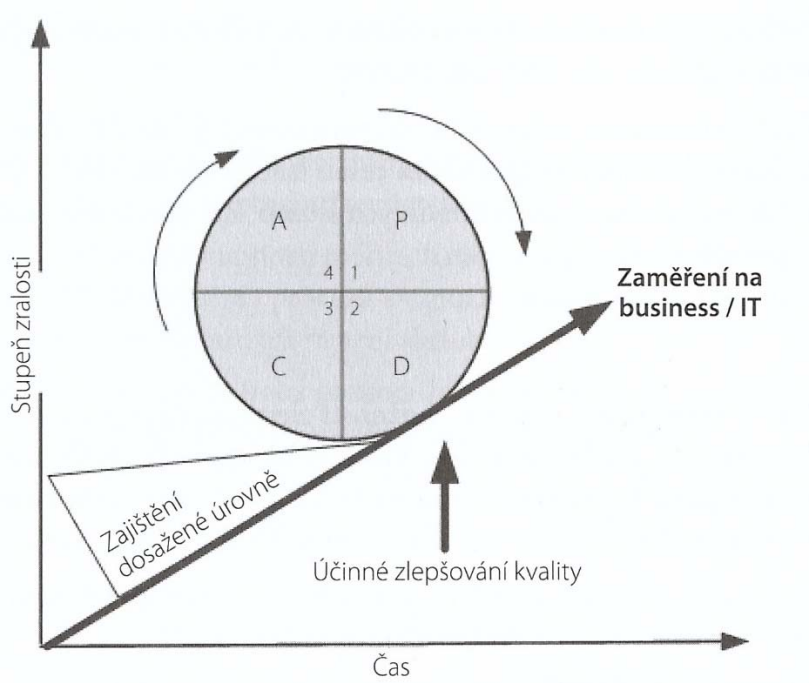
Systém řízení bezpečnosti informací – ISMS je část celkového řízení organizace, založená na přístupu (organizace) k rizikům činností, která je zaměřena na ustanovení, zavádění, provoz, monitorování, přezkoumávání, údržbu a neustálé zlepšování bezpečnosti informací. Systém řízení v sobě zahrnuje organizační strukturu, politiky, plánovací činnosti, odpovědnosti, mechanismy, postupy, procesy a zdroje.[7]

Srdcem tohoto systému řízení je model PDCA. Model vytvořil William Edwards Deming. Narodil se v USA v roce 1900. Získal magisterský titul v oboru matematiky na University of Colorado a doktorát z matematiky a matematické fyziky na Yale University. Nechal se inspirovat myšlenkami Waltera A. Shewharta z oblasti statistických metod aplikovaných při kontrole výroby a v řízení a rozvinul toto téma do oblasti řízení kvality.[3]

Po druhé světové válce Deming pomáhal plánovat sčítání lidu v Japonsku. Jeho zkušenosti v oblasti statistické kontroly kvality vedly k pozvání do Japonské unie vědců a inženýrů. Deming postupně proškolil stovky japonských inženýrů a studentů ve statistické kontrole procesů a v oblasti řízení kvality. Demingovo poselství Japoncům bylo stručné: zlepšení kvality sníží na jedné straně náklady, na druhé straně zvýší produktivitu a přinese úspěch na trhu. Vysoká kvalita v kombinaci se snižováním nákladů byla skutečně cestou k úspěchu japonské společnosti. Demingův model pro systém řízení se stal učebnicovým modelem, který lze s úspěchem aplikovat i pro Systém řízení bezpečnosti informací.[3]

1.10 Systém řízení podle modelu PDCA

Model PDCA nazýván taky jako Demingův cyklus „Plánuj-Dělej-Kontroluj-Jednej“ (Plan-Do-Check-Act) se používá k podpoře zlepšovacího přístupu a jeho provádění. Každý úspěšný krok týkající se zlepšení kvality souladu bezpečnosti IT a businessu je důležité následně pevně zakotvit. Je velmi důležité si uvědomit, že Demingův cyklus je iterativní. Neustálým opakováním těchto čtyř činností dochází k vylepšování procesů ISMS a to posouvá organizaci na novou kvalitativní úroveň z hlediska ISMS. Tuto iteraci nejlépe znázorňuje následující obrázek. [3]



Obrázek 5: Demingův cyklus podle ITIL [3]

1.10.1 Jednotlivé činnosti modelu PDCA

Ustanovení ISMS je první etapou jeho budování, při kterém jsou upřesněny formy řešení bezpečnosti informací. Zde je nutné definovat rozsah ISMS a odsouhlasení „Prohlášení o politice ISMS“ (závazek vedení organizace podporovat informační bezpečnost).[7]

Ustanovení ISMS je možné rozdělit na následující činnosti:

- definice rozsahu, hranic a vazeb ISMS,
- definice a odsouhlasení Prohlášení o politice ISMS,
- analýza a zvládání rizik,
- souhlas vedení organizace s navrhovanými zbytkovými riziky a se zavedením ISMS,
- příprava Prohlášení o aplikovatelnosti

Tato etapa budování má zásadní dopady na fungování ISMS během jeho životního cyklu. [7]

Definice rozsahu a hranic ISMS

V rámci této části zavádění ISMS je důležité si připomenout Charakteristické činnosti a cíle organizace, používanou organizační strukturu, umístění lokalit či využívané technologie pro přenos a zpracování informací atd. Na tomto základě je možné stanovit výchozí rozsah a hranice ISMS, který nemusí vždy pokrývat celou organizaci.[7]

Z hlediska praktického prosazení ISMS je možné se ke stanovení rozsahu postavit dvěma způsoby. V prvním případě je rozsah ISMS od počátku identický s rozsahem celé organizace. To vyžaduje poměrně významné investice z hlediska spotřeby zdrojů i financí a ne vždy jsou realizovány všechny plánované a očekávané přínosy řízení bezpečnosti. V mnoha případech velikost projektů bývá pro rozvoj bezpečnosti spíše na škodu. Jinou možností je definovaný rozsah ISMS na počátku omezit a ISMS aplikovat pouze na jasně definovanou část organizace, určený organizační celek či nejčastěji na ucelený informační systém.[7]

Významnou výhodou tohoto řešení, které se soustředí na dílčí celky, je skutečnost, že je možné soustředit vyšší míru úsilí do zvolené oblasti. Rychlejší zavedení ISMS je vhodné realizovat tak, že zkrátíme dobu cyklu PDCA modelu. To jinými slovy znamená, že v daném období např. jednoho roku necháme ISMS projít více cykly např. dvěma nebo třemi. Tímto významným urychlením se stává skutečnost, že do realizace druhého a případně třetího cyklu již promítáme získané skutečnosti. Dochází k lepšímu stanovování priorit dílčích PDCA cyklů.[7]

Prohlášení o politice ISMS

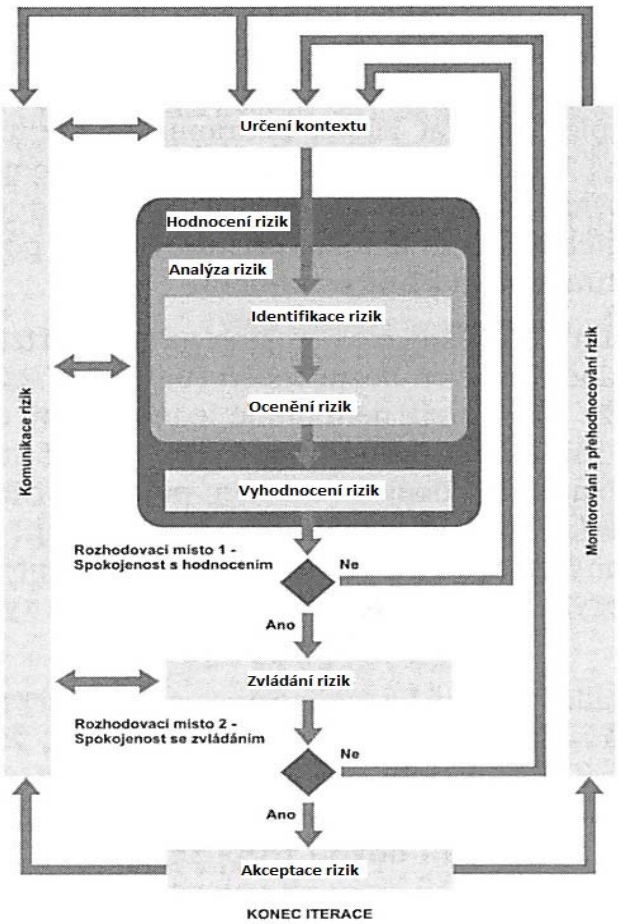
Dalším krokem je definice „Prohlášení o politice“ (zkráceně politika) ISMS, která vzniká na základě specifických potřeb dané organizace. Z praktického hlediska je důležité, aby politika ISMS:

- upřesnila cíle ISMS a definovala základní směr a rámec pro řízení informací,
- zohlednila cíle a požadavky organizace a související zákonné, regulativní a smluvní požadavky,
- vytvořila potřebné vazby pro vybudování a údržbu ISMS v dané organizaci,
- stanovila kritéria, podle kterých jsou popisována a hodnocena rizika,
- byla schválena vedením organizace

Politika ISMS je krátký dokument, ale významný a velmi důležitý, protože prezentuje zájem vedení organizace o řízení bezpečnosti informací a definuje klíčové podmínky pro hodnocení rizik, což je základem pro celý ISMS. Správně definovaná politika ISMS může velmi usnadnit budoucí prosazování pravidel a požadavků na bezpečnost informací v organizaci. [7]

Řízení rizik a teorie analýzy

Řízení rizik je klíčovým nástrojem pro systematické řízení bezpečnosti informací. Přesná znalost skutečných rizik rozhoduje o výběru a prosazení vhodných bezpečnostních opatření schopných snížit negativní dopady těchto rizik. Proto řízení rizik je základem pro každý systém řízení bezpečnosti informací a navíc podstatným způsobem ovlivňuje efektivitu fungování celého ISMS. Terminologie spojená s řízením rizik a vztahy mezi termíny jsou uvedeny na následujícím obrázku 6. [7]



Obrázek 6: Koncept řízení rizik [7]

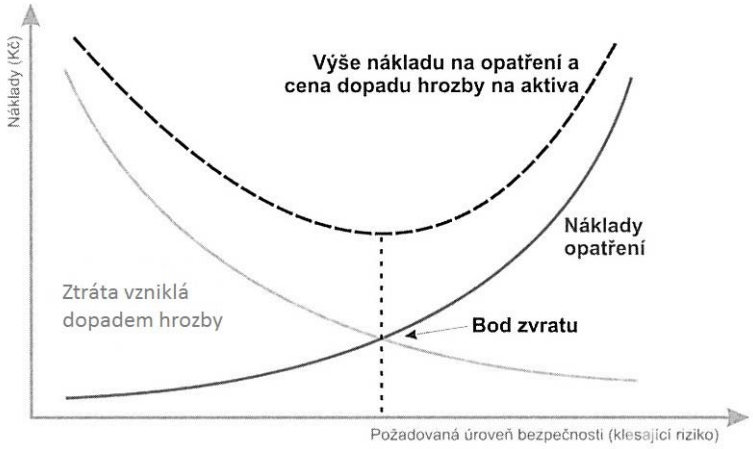
Analýza bezpečnostních rizik a její řízení představuje základní nástroj v rukou vrcholového vedení organizace k ochraně investic, vynaložených do informačních systémů a tím i do podpory hlavních procesů organizace. Vlastní provedení procesu analýzy rizik je možné rozlišit podle podrobnosti a hloubky přístupů k jejímu řešení:

- nedělat nic – akceptovat rizika neznámého rozsahu a síly,
- neformální přístup – analýza rizik se provádí živelně bez dokumentace přesných postupů,
- základní přístup – postupy jsou rámcově zdokumentovány a organizace má celkovou koncepci a vizi řešení bezpečnosti informací,
- detailní přístup – všechna rizika jsou analyzována podrobně podle předem definované a dodržované metodiky,
- přístup kombinovaný – některá rizika jsou analyzována podrobně, některá jsou případně při analýza i záměrně opominuta. [7]

Ve své podstatě je to o tom, že se snažíme nalézat právě nejslabší články a ty posilovat tak, aby míra bezpečnosti byla vyvážená a aby bezpečnost byla ekonomicky zvládnutelná. [7]

Ekonomický aspekt je v praxi realizován oceněním jednotlivých aktiv – jejich hodnotou pro vrcholové vedení organizace. Oceňování aktiv (vlastně se jedná o vyčíslení ztrát, pokud hrozba zničí nebo naruší užitnou hodnotu aktiva – velikost ztráty, jestliže hrozba nastane) není záležitostí nijak jednoduchou, neboť informační systém organizace může ovlivňovat i její nehmotná aktiva typu Know-how organizace, její konkurenční výhodu na trhu, goodwill – její dobrou pověst apod. Oceňování hmotných aktiv není taky jednoduché, protože nějaké aktivum může mít pro různé organizační jednotky různou hodnotu. Proto je dobré, aby se na této práci podílelo více odpovědných manažerů organizace. [7]

Ocenění aktiv bývá v praxi východiskem pro stanovení nákladů na realizaci opatření na jejich ochranu. Vztahy mezi hodnotou aktiva, resp. Mezi ztrátou vzniklou v případě jeho zničení nebo poškození, a náklady na realizaci ochrany aktiva formou opatření jsou uvedeny na obrázku 7. [7]



Obrázek 7: Nákladový model pro realizaci bezpečnostních opatření [7]

Principy řízení rizik

Řízení rizik je komplexním oborem, který se snaží o identifikaci existujících rizik, vyjádření úrovně jejich působení a určení optimálního opatření pro snížení vlivu těchto rizik na přijatelnou úroveň. Pro efektivní řízení rizik je důležité uplatnit následující principy:

- multidisciplinární přístup – vychází od mnoha uživatelů s různými pohledy a názory na význam rizika, jeho identifikaci, zvládání a akceptaci,
- systematické a centralizované řízení – využívá standardizace, soudržnosti, úplnosti přístupů, plánování, využití zkušeností a zlepšování,
- integrovaný proces je potřeba provázat s procesy pro řízení informatiky (IT Governance), řízení bezpečnosti informací, řízení kontinuity organizace apod.,
- odpovědnost za činnosti – musí být zavedena přímá odpovědnost funkčních útvarů a manažerů bezpečnosti/rizik za koordinaci a integraci postupů v celé organizaci; činnosti musí být také prokazatelné,
- dokumentace – musí být úplná, musí splňovat požadavky na konzistenci a musí obsahovat mechanismy, které umožní určit (zjistit) odpovědnosti za provedená rozhodnutí,
- zlepšení znalostí – protože se nejedná o činnost jednorázovou, je nutné ukládat získané znalosti, průběžně je spravovat s cílem sdílet je pro další rozvoj systému řízení rizik; protože řízení rizik je činnost dlouhodobá musí mít proces zlepšování znalostí

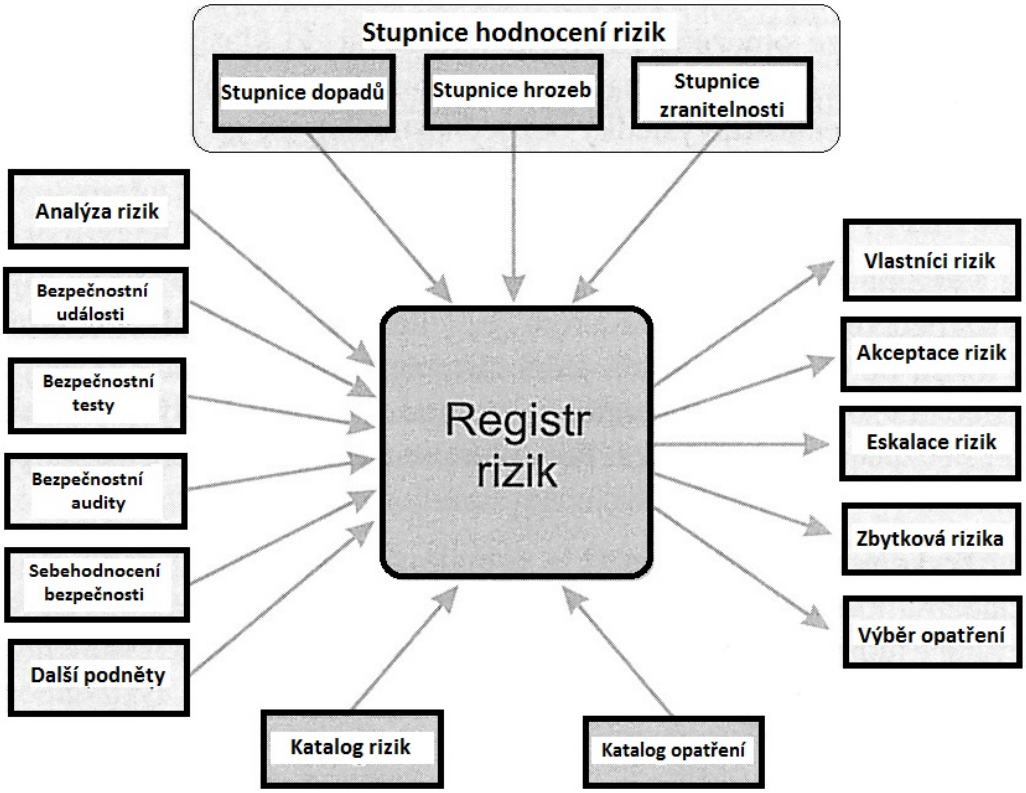
schopnost reagovat na změny jednak v organizaci, jednak v konceptech práce se znalostmi,

- pravidelná aktualizace – je nutné provádět pravidelnou aktualizaci na základě poznatků z monitorování systému řízení bezpečnosti nebo z externích zdrojů, a to nejméně jedenkrát ročně.[7]

Základním prvkem moderního přístupu k řízení rizik je vybudování tzv. registru rizik, do kterého jsou vkládány informace o všech bezpečnostních rizicích. Hlavním důvodem je vybudování a údržba aktuálního přehledu o známých bezpečnostních rizicích. Cílem je všechna zjištěná rizika evidovat, ohodnotit jejich významnost, určit osobu, která je odpovědná za zvládání rizika a sledovat postup zvládání rizika v čase. Tak má bezpečnostní manažer aktuální přehled o odpovědných osobách, o stavu řešení a v případě potřeby je schopen zpracování rizika náležitým správným způsobem interně řešit s ostatními manažery (komunikace rizik).[7]

Při aplikaci moderních metod řízení rizik je potřeba upřesnit následující aspekty:

- Jednoduché hodnocení rizik např. doporučení organizace BITS (Bank Information Technology Secretariat) vydané v roce 2002 v publikaci Technology Risk Transfer Gap Analysis Tool (BIT_02). Riziko se zde počítá jako prostý součin možných dopadů, pravděpodobnosti výskytu dopadu a pravděpodobné účinnosti provedených opatření. [7]
- Definice struktury pro řízení rizik s cílem provázat metodu řízení rizik s konkrétním prostředím informací a komunikačních systémů. Snahou je především jednoznačně určit odpovědnosti související s řízením rizik, definovat pravidla pro rozhodování, způsoby komunikace či vykazování apod.
- Využití různých zdrojů vstupních informací s cílem připravit podmínky pro využití širokého spektra vstupních informačních zdrojů, jak znázorňuje obrázek 8. [7]



Obrázek 8: Postavení registru rizik [7]

Při promítnutí teoretických poznatků o řízení rizik do praxe je potřebné dát pozor na některá doporučení, nebo spíše zásady:

- **Rizikové scénáře by měly být voleny tak, aby byly pro danou organizaci jedinečnými.** Jinými slovy není vhodné pracovat pouze s obecně definovanými hrozbami. Významně lepší srozumitelnost mají rizikové scénáře, které přesně vyjadřují konkrétní situaci organizace (např. obecná rizika typu požár či záplava nahradit rizikovým scénářem „Trvalé poškození aktiv v serverové místnosti, např. v důsledku požáru, povodně, teroristického útoku či jiné neočekávané situace“.
- **Počet rizikových scénářů, se kterými se současně pracuje, by měl být v rozsahu desítek rizik.** Jedním z častých způsobů, jak zabránit možnosti účelného využití výsledků ohodnocení rizik, je překročení limitního počtu rizik. Na základě zkušeností lze konstatovat, že tímto limitem je přibližně 35 – 50 rizik či rizikových scénářů (za ideální lze považovat práci s 20 až 30 riziky). Překročení

limitů vede k neschopnosti promítnout výsledky ohodnocení rizik do účelného rozhodnutí. [7]

- **Všechny hodnoty, které při hodnocení rizik stanovíme, musíme vždy okomentovat.** V případě, že si nezaznamenáme, které prvky ohodnocení jsme již do hodnocení rizika započetli a které jsme byť omylem opomněli, nejsme schopni ohodnocení rozvíjet, ale ve své podstatě pořád hodnotíme od počátku. [7]

Prvním krokem, který je pro řízení rizik důležitý, je identifikace všech aktiv a určení jejich významu pro chod organizace. Aktiva je možné rozdělit do dvou základních skupin:

- **Primární aktiva** – zejména nehmotná aktiva – informace, které jsou organizací využívány, a funkční procesy a aktivity organizace, znalosti a know-how, které mají pro ISMS určitý význam, tj. je potřeba nějakým způsobem zajistit jejich bezpečnost.
- **Sekundární aktiva** – zejména hmotná aktiva – technické vybavení, komunikační infrastruktura, ale i programové vybavení a pracovníci, kteří se podílejí na chodu organizace a jejich organizační uspořádání, prostory, které organizace využívá apod.[7]

Z formálního pohledu je potřebné, aby se systém hodnocení a řízení rizik organizace opíral o jednoznačně stanovená kritéria pro hodnocení a akceptaci rizik. Je především důležité definovat stupnice pro stanovení:

- Míry důvěrnosti aktiv.
- Míry integrity aktiv.
- Míry dopadů a škod.
- Pravděpodobnosti uplatnění hrozby.
- Pravděpodobnosti selhání využívaných bezpečnostních opatření (pravděpodobnost zranitelnosti)
- Stupnice pro vyjádření rizik a hladiny přijatelnosti rizika

Po vytvoření stupnice rizik máme k dispozici nejrizikovější scénáře a ty musíme eliminovat vhodným bezpečnostním opatřením:

- Redukce rizika na nejnižší akceptovatelnou úroveň zavedením bezpečnostních opatření.
- Přenesení rizika – můžeme realizovat pojištěním nebo smlouvou s organizací zajišťující outsourcing, atd.

- Varianta vyhnutí se riziku je sice metodou vysoce defenzivní, nicméně pokud snížíme tím hrozbu nebo dopad hrozby splní i tato varianta svůj úkol v řízení bezpečnosti informací.
- Podstoupení (retence) rizika bez další akce je samozřejmě možné, pokud nám výsledky analýzy rizik dávají naději, že pravděpodobnost naplnění hrozby je malá.

Každé riziko musíme vždy akceptovat (přijmout), což znamená zvládnutí tohoto rizika.

Vždy musíme po akceptaci vyhodnotit, zda riziko bylo eliminováno celé nebo je potřeba ještě zaznamenat nějaká zbytková rizika. [2]

Souhlas vedení se zavedením ISMS a se zbytkovými riziky

Na základě výsledků řízení rizik by měly být připraveny dva formální kroky, ve kterých vedení organizace odsouhlasilo návrh bezpečnostních opatření, která jsou nutná pro snížení bezpečnostních rizik. Současně s tím, by se vedení mělo vyjádřit, zda jsou existující zbytková rizika pro chod organizace přijatelná či nikoli.[7]

Prohlášení o aplikovatelnosti

Prohlášení o aplikovatelnosti (Statement of Applicability) je povinným dokumentem pro organizace, které usilují o shodu svého ISMS s normou ISO/IEC 27001. Tento dokument musí obsahovat cíle opatření a jednotlivá opatření, která byla pro daný ISMS vybrána na pokrytí existujících bezpečnostních rizik. V praxi je prohlášení o aplikovatelnosti nejdůležitějším dokumentem, který postihuje systémové vazby ISMS. Doporučené formáty dokumentu nejčastěji zobrazují matici vztahů mezi zjištěnými riziky a vybranými bezpečnostními opatřeními. [7]

Prohlášení o aplikovatelnosti plní i důležitou zpětnou vazbu, protože jsme pomocí něj schopni jednoduše zkontrolovat, zda došlo k pokrytí všech identifikovatelných rizik příslušnými bezpečnostními opatřeními. V tomto směru by v prohlášení neměla existovat „nepokrytá“ rizika. Poslední zkušenost z tvorby prohlášení o aplikovatelnosti ukazuje možnost využití tohoto dokumentu na systematický popis ISMS, který je jeho základní přehledovou mapou. [7]

Podpora ze strany organizace

Podpora zajištění potřebných zdrojů ze strany organizace ve všech fázích zavádění ISMS musí být vždy zaručena. Organizace musí vyčlenit kompetentní a kvalifikované osoby, které budou tvořit implementační tým společně s vedením podniku. Důležité je seznámení pracovníků s politikou bezpečnosti informací a s důsledky, které pro ně plynou z nedodržování pravidel a požadavků ISMS.

1.10.2 Zavádění a provoz ISMS

Tato etapa životního cyklu ISMS se soustředí na prosazení všech bezpečnostních opatření tak, jak byla navržena při ustanovení ISMS. Důležité je především připravit dílčí plány, kde jsou upřesněny termíny, odpovědné osoby apod. Všechna bezpečnostní opatření by měla být zdokumentována v tzv. Příručce bezpečnosti informací a mělo by dojít k vysvětlení bezpečnostních principů všem uživatelům a manažerům.

Během této etapy zavádění ISMS je nezbytné provést následující činnosti:

- Formulovat dokument Plán zvládání rizika započít s jeho zaváděním.
- Zavést plánovaná bezpečnostní opatření a zformulovat příručku bezpečnosti informací, která upřesní pravidla a postupy aplikovaných opatření v definovaných oblastech bezpečnosti informací.
- Definovat program budování bezpečnostního povědomí a provést přípravu a zaškolení všech uživatelů, manažerů a odborných pracovníků z úseku informatiky a zejména z oblasti řízení bezpečnosti.
- Upřesnit způsoby měření účinnosti bezpečnostních opatření a sledovat stanovené ukazatele.
- Zavést postupy a další opatření pro rychlou detekci a reakci na bezpečnostní incidenty.
- Řídit zdroje, dokumenty a záznamy ISMS. [7]

Plán zvládání rizik

Plán zvládání rizik je důležitý dokument, který popisuje:

- všechny činnosti ISMS, které jsou potřebné pro řízení bezpečnostních rizik

- stanovené cíle a priority těchto činností ISMS
- omezující faktory a potřebné zdroje (personální, finanční, technologické, znalostní apod.
- činnosti, které vedou k potřebnému snižování bezpečnostních rizik
- činnosti, které jsou z pohledu ISMS rutinní a které jsou dány požadavky ISO/IEC 27001, např. naplánování interních auditů, přezkoumání ISMS apod.

Důležité je podotknout, aby při realizaci plánu zvládání rizik byly shromažďovány podklady v podobě záznamů o těchto činnostech. [7]

Příručka bezpečnosti informací

Při tvorbě bezpečnostní dokumentace je potřeba rozlišovat různé úrovně připravovaných dokumentů:

- Na té nejvyšší úrovni jsou to především dokumenty, které si vyžaduje systém řízení a které jsou s ohledem na požadavky ISMS povinné (např. rozsah ISMS, politika ISMS, zpráva o hodnocení rizik, prohlášení o aplikovatelnosti, plán zvládání rizik apod.).
- Ve druhé úrovni je dokumentace, která slouží k podpoře prosazování ISMS a vždy by měla být přizpůsobena konkrétnímu ISMS. Zde souhrnně hovoříme o příručce bezpečnosti informací. Důležitým prvkem při tvorbě této dokumentace je definice dílčích procesů a postupů, které zajišťují efektivní prosazení dílčích bezpečnostních opatření. Proto je důležité definovat kdo, co, kdy, kde a jak má učinit.
- Na nejnižší úrovni bezpečnostní dokumentace se nacházejí tzv. pracovní postupy. Tyto dokumenty by měly podrobně vysvětlovat úkony, které jsou nezbytné pro naplnění dílčích procesů. Ne vždy je tato úroveň nezbytná a často může být řešena odkazem na příslušnou dokumentaci použitých technických systémů. [7]

Při přípravě kvalitní dokumentace je potřeba pamatovat na to, že hlavním cílem tvorby je předání informací určených skupině manažerů, uživatelům, operátorů, správců apod. Této cílové skupině by se měl i podřídit způsob popisu a vyjadřování. Není vhodné do jednoho dokumentu kombinovat více cílových skupin. Mírou kvality dokumentace není počet popsaných stránek, ale srozumitelnost dokumentů pro jejich cílovou skupinu. [7]

Prohlubování bezpečnostního povědomí

Jedním z nejdůležitějších prvků při prosazování ISMS je prohlubování bezpečnostního povědomí, za kterým se skrývá promítnutí všech definovaných pravidel a postupů do skutečného chování všech odpovědných pracovníků a uživatelů. Tento jednoduchý cíl je nicméně složitým úkolem, který vyžaduje vysoké a systematické úsilí. Díky změnám, kterési vyžaduje rozvoj ISMS a pravidelná obměna pracovníků organizace, je to trvalý a nekonečný proces, který často rozhoduje o skutečné efektivitě ISMS. [7]

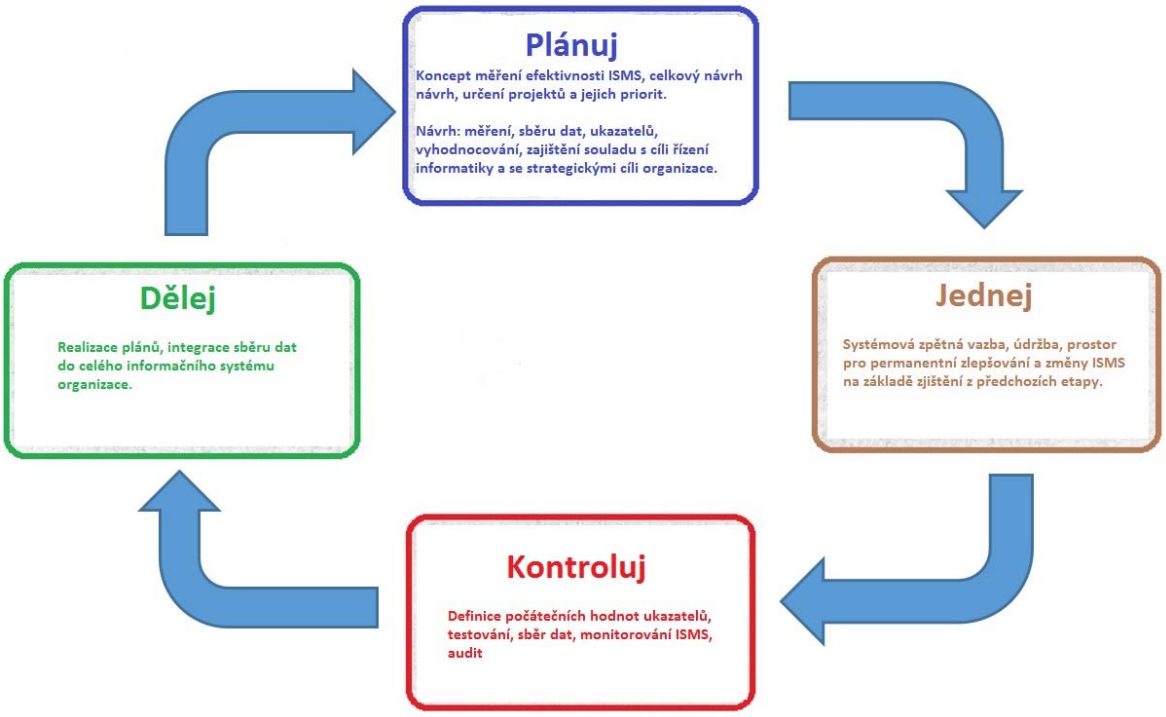
Je nutné všem pracovníkům srozumitelně vysvětlovat bezpečnostní principy a pravidla, seznamovat je s bezpečnostními riziky tak, aby byli schopni správně reagovat na situace, které dokumentace nepostihuje, a projednávat s nimi bezpečnostní incidenty, jejich příčiny a skutečné i potenciální následky. [7]

Jedině touto permanentní a systematickou komunikací s pracovníky bude možné zajistit větší odolnost nejslabšího článku v pomyslném řetězu ISMS. Tím je a vždy bude lidský činitel a jeho nepředvídatelné projevy. [7]

Proces řízení a měření účinnosti ISMS

Dalším důležitým tématem, které je spojeno s prosazováním efektivního řízení bezpečnosti, je měření účinnosti aplikovaných bezpečnostních opatření. Zde je potřeba definovat a pravidelně sledovat objektivní údaje o skutečném fungování systému řízení bezpečnosti, na základě kterých je vhodné provádět všechna důležitá rozhodnutí.[7]

Proces řízení účinnosti systému řízení bezpečnosti informací v organizaci není nikterak jednoduchý a je nutné jej mít na zřeteli již v okamžiku návrhu celého ISMS, protože velmi podstatné kroky pro měření efektivnosti a její vyhodnocování jsou již součástí první etapy životního cyklu, který máme znázorněn na obrázku 9 [7]



Obrázek 9: Schéma PDCA pro zvládání bezpečnostního incidentu [7]

O opravdové účelnosti a účinnosti ISMS se rozhoduje již v etapě plánování. Tehdy probíhá vstupní analýza rizik a na její kvalitě bezprostředně záleží i kvalita navrženého ISMS. Významný vztah k účinnosti celého navrhovaného ISMS má také přístup vrcholového vedení organizace a jeho kompetence. V této etapě je také nutné zohlednit i další zákonné případně jiné úpravy, kterými se organizace musí řídit a které vycházejí z její celkové strategie. [7]

Pro první etapu „Plánuj“ je možné hlavní aktivity sledování účelnosti a účinnosti shrnout do následujících bodů:

- zajistit soulad systému měření účinnost s celkovým systémem řízení v organizaci,
- navrhnout celkový koncept měření účinnost ISMS v organizaci,
- navrhnout metody a způsob vlastního měření účinnost ISMS,
- na základě analýzy rizik určit projekty, které budou sloužit k realizaci bezpečnostní politiky a určit jejich priority pro realizaci,
- navrhnout ukazatele, podle nichž se bude měřit účinnost ISMS, způsoby a periodicitu jejich výpočtu,
- určit způsoby sběru dat k jednotlivým ukazatelům,

- určit způsob vyhodnocování včetně určení rolí, které budou s těmito ukazateli pracovat, a určit případné navazující reportovací povinnosti,
- specifikovat případné vazby na systém měření a vyhodnocování informatiky v organizaci.[7]

Etapa „Dělej“ se věnuje z pohledu vedení organizace relativně nejjednodušší činnosti a to je realizaci projektů. Zde padá hlavní odpovědnost za zdar systému řízení účinnosti zejména na bedra projektových manažerů. Hlavním problémem v této etapě je zajistit integraci systému monitorování dat pro vyhodnocování efektivnosti do celého monitorovacího systému organizace. [7]

V etapě „Kontroluj“ jsou hlavními činnostmi týmu připravujícího řízení účinnosti ISMS následující:

- definice počátečních hodnot ukazatelů měření účinnosti ISMS,
- testování systému měření,
- vlastní sběr dat a monitorování ISMS v provozu,
- sběr podkladů pro průběžný audit ISMS [7]

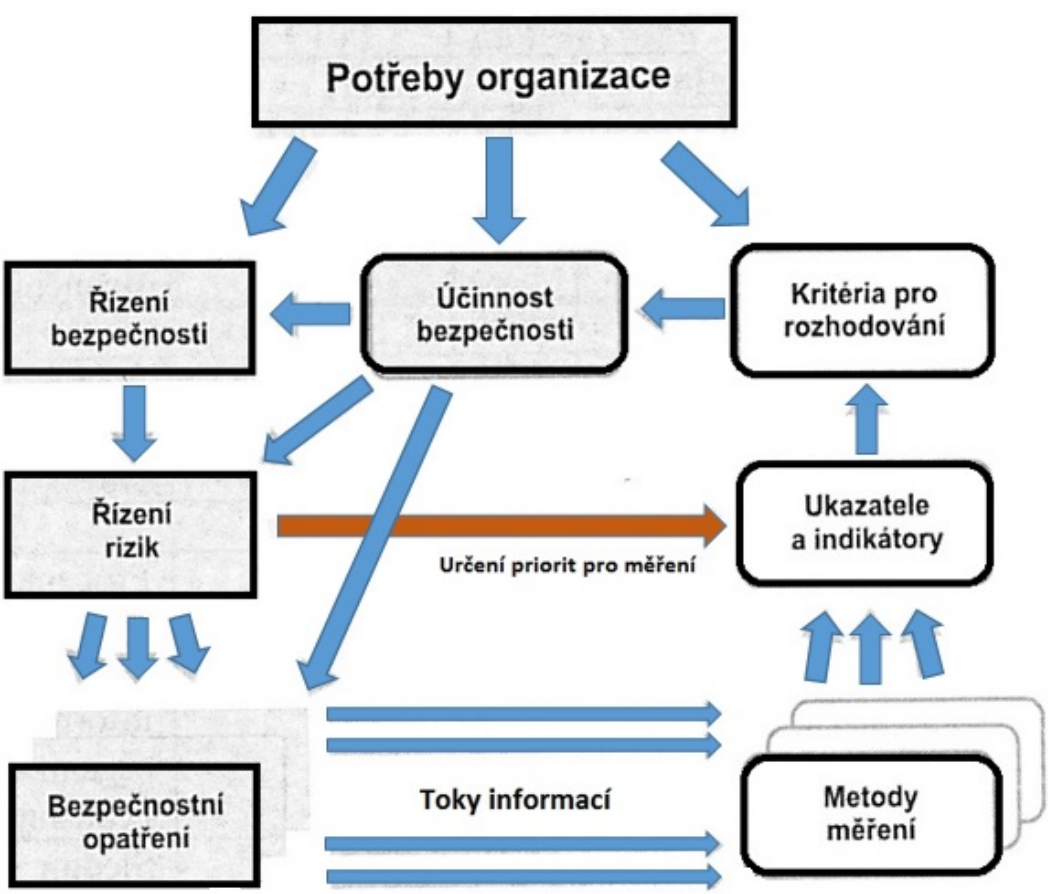
V etapě „Jednej“ je zajištěn permanentní rozvoj ISMS a možnosti jeho pravidelného zlepšování na základě zjištěných výsledků z předchozí etapy. Tato etapa vlastně představuje v praxi realizaci zpětné vazby.[7]

Jinou kapitolou v návrhu ISMS, jeho realizaci a provozu představuje způsob, jak vyhodnocovat jeho jednotlivé složky a jakých využívat pro tato vyhodnocování ukazatelů. V zásadě je možné využívat dvou základních typů ukazatelů:

- poskytující číselné hodnoty,
- sledující průběh procesů. [7]

Ukazatelé poskytující číselné hodnoty, je možné použít na řízení snižování nákladů, zvyšování zisku, růst produktivity, zkracování doby životního cyklu, snižování rizika apod. Procesní ukazatele poskytují data o způsobu, jakým je proces v organizaci implementován a integrován do řídící činnosti. Protože ukazatele obou typů jsou si velmi podobné a v mnoha směrech velmi úzce provázané, stále více manažerů se probírá systémy ukazatelů s cílem eliminovat aktivity a procesy, které nepřinášejí svým průběhem žádnou přidanou hodnotu.[7]

Celé schéma fungování bezpečnostních ukazatelů účinnosti je zachyceno na tomto obrázku.



Obrázek 10: Měření účinnosti ISMS a jeho zpětná vazba [7]

Řízení provozu, zdrojů, dokumentace a záznamů ISMS

Posledním bodem etapy zavedení ISMS je provádění všech činností řízeným způsobem. Tato část není vůbec jednoduchá, protože nestačí „pouze „postupovat podle dohodnutých pravidel, ale je nutné i „shromažďovat podklady“ pro další fázi monitorování. Pro umožnění kontroly správnosti fungování ISMS je podstatné vytvořit definovaná pravidla pro tvorbu, schvalování, distribuci a aktualizaci dokumentace řízení bezpečnosti (včetně odebírání, zneplatnění a skartace již neplatných verzí dokumentů). [7]

Záznam je dokument, ve kterém jsou uvedeny dosažené výsledky nebo ve kterém se poskytují důkazy o provedených činnostech, resp. Jiné informace záznamového charakteru, související se systémem řízení kvality. [7]

Vytváření takovýchto záznamů o dílčích reálných úkonech musí být vytvořeno tak, aby umožňovalo relativně snadné dohledání určitých přesně definovaných skupin aktivit (vyhledávání určitých typů činností, vyhledávání činností realizovaných v daném období či určitou osobou nebo zařízením).[7]

Podstatným provozním požadavkem je též definice postupů a opatření pro řízení incidentů. Zde je nutné využít nástroje, které jsou schopny včas odhalovat bezpečnostní slabiny a incidenty a na tyto události upozornit příslušné odpovědné pracovníky organizace.[7]

Tito pracovníci pak zajistí prošetření podnětů podle definovaných postupů a pravidel včetně zaznamenání průběhu a výsledku šetření. Podněty z řešení bezpečnostních incidentů by měly být taktéž využity pro upřesnění hodnocení rizik a pro optimalizaci pravidel ISMS.[7]

1.10.3 Monitorování a přezkoumání ISMS

Hlavním úkolem této etapy zavádění ISMS je zajistit účinné zpětné vazby. Proto je důležité během této části zavádění ISMS provést následující činnosti:

- monitorovat a ověřit účinnost prosazení bezpečnostních opatření,
- provést interní audity ISMS, jejichž náplň pokryje celý rozsah ISMS,
- připravit zprávu o stavu ISMS a na jejím základě přehodnotit ISMS na úrovni vedení organizace (včetně revize zbytkových a akceptovatelných rizik). [7]

Provádění kontrol ISMS

Základní zpětnou vazbou, která je pro fungování ISMS nezbytná, je provádění kontrol ze strany všech osob, které mají za fungování ISMS nějakou odpovědnost a to na všech manažerských úrovních. [7]

Součástí kontrol ISMS musí být:

- schopnost včasné detekce chyb,
- detekce úspěšných a neúspěšných pokusů o narušení bezpečnosti,
- sledování bezpečnostních událostí a včasná detekce bezpečnostních incidentů,
- vyhodnocení měření účinnosti ISMS a aplikovaných bezpečnostních opatření,

- přehodnocování ohodnocení rizik na základě zkušeností z praktického fungování ISMS a podněty z těchto aktivit promítnout do aktualizace příslušných dokumentů a plánů ISMS. [7]

Interní audity ISMS

Interní audit na rozdíl od kontroly zajišťuje potřebný nezávislý pohled na fungování ISMS. Při plánování auditů je potřeba pamatovat na skutečnost, že by interní audity měly svoje zaměření rovnoměrně rozložit na celý rozsah ISMS samozřejmě při zvážení cílů, priorit a rizikových oblastí ISMS. Audity ISMS by měly prověřovat oba aspekty ISMS. Prvním je dodržování procesních pravidel, kde je dominantním kritériem auditu naplňování požadavků ISO/IEC 27001. Druhým aspektem auditu ISMS je prověření fungování jednotlivých bezpečnostních opatření, která jsou pro potřeby ISMS zavedena. Zde se jako kritérium auditu uplatňuje norma ISO/IEC 27002 a auditoři prověřují způsob, vhodnost a míru prosazení aplikovaných bezpečnostních opatření. [7]

Přezkoumání ISMS vedením organizace

Přezkoumání (Review) – činnost prováděná k určení vhodnosti, přiměřenosti a efektivnosti předmětu přezkoumání k dosažení stanovených cílů. [7]

Podněty a připomínky k ISMS, získané při jeho monitorování, jsou důležitými informacemi, které slouží pro objektivní a účinné přezkoumání ISMS vedením organizace. Přezkoumání by mělo probíhat pravidelně a to nejméně jednou za rok. Není ale výjimkou, že probíhá častěji a to hlavně u nově zavedených ISMS, kde je potřeba přehodnocení častější.[7]

Mezi vstupy pro přezkoumání ISMS patří všechny podstatné informace o fungování ISMS za hodnocené období. Významná pozornost by měla být věnována následujícím skutečnostem:

- výsledkům provedených auditů ISMS,
- zpětné vazbě od zainteresovaných uživatelů a třetích stran,
- existujícím slabinám a hrozbám, které by mohly být při analýze rizik podceněny,
- výsledkům měření účinnosti ISMS,
- změnám, které ovlivňují ISMS,
- získaným doporučením pro další zlepšování ISMS. [7]

Na základě těchto podnětů dochází k posouzení silných a slabých stránek ISMS (SWOT analýza). Mezi důležité výstupy SWOT analýzy patří:

- Zlepšení účinnosti ISMS (zvyšování míry bezpečnosti při snižování náročnosti realizace bezpečnostních opatření),
- Aktualizace ohodnocení rizik a souvisejících plánů pro zvládání rizik,
- Nezbytné úpravy procesů, pravidel a postupů ISMS,
- Plánovaná náročnost ISMS na zdroje (finanční, lidské, technologické apod.) v dalším období. [7]

Častým projevem přehodnocení ISMS je příprava zprávy o stavu ISMS, která shrne, co na ISMS funguje dobře a je možné se otyto vlastnosti v budoucnu opřít a zároveň

rozebere skutečnosti, které zatím optimálně nefungují, a bude nutné je nadále zlepšovat. Pomocí zprávy o stavu ISMS, která by měla být orientována především na budoucnost, je možné s vedením organizace uzavřít „dohodu“ o prohlubování bezpečnosti. [7]

1.10.4 Údržba a zlepšování ISMS

Poslední etapou celého cyklu prosazování ISMS je jeho udržování a zlepšování. Jedná se především o to, že v této fázi by mělo docházet ke sběru podnětů ke zlepšení ISMS a k nápravě všech nedostatků, tzv. neshod, které se v ISMS objevují. [7]

Během této části zavádění je nezbytné provést následující činnosti:

- Zavádět identifikované možnosti zlepšení ISMS (především na základě přehodnocení vedením),
- Provádět odpovídající opatření k nápravě a preventivní opatření pro odstranění nedostatků. [7]

Soustavné zlepšování ISMS

Návrh dokonalých systémů řízení je v praxi velmi náročný. V podstatě takové systémy vůbec neexistují, a proto je velmi důležité do každého systému zapracovat účinnou zpětnou vazbu. Ta by měla fungovat tak, že na jedné straně získává podněty, které mohou vést k efektivnějšímu fungování ISMS, na druhé straně musí tato vazba odhalovat nedostatky a jejich příčiny a vhodným způsobem na tyto podněty reagovat. [7]

Podstatným prvkem zlepšování je především využití pozitivní zpětné vazby. Je žádoucí, aby se zlepšování ISMS opíralo o zkušenosti aktivních účastníků. Ti by měli osoby odpovědné za ISMS informovat o svých podnětech, které mohou fungování ISMS zlepšit. Nápady, pocházející z reálné praxe, jsou vždy nenahraditelné a jejich důslednému zpracování by měla být věnována velká pozornost. [7]

Osoby odpovědné za ISMS by si podnětů, pocházejících od řadových pracovníků měly vážit. U všech podnětů je ale nutné zvážit jejich přímé i nepřímé dopady a důsledky pro organizaci a s tím i související rizika. Pro rozvoj ISMS je důležité i prohlubovat motivaci pracovníků na účasti při všech činnostech spojených s ISMS v tom, aby sdíleli své zkušenosti a aby otevřeně navrhovali, co je vhodné a žádoucí na chodu ISMS zlepšit. Tady by si určitě našla místo japonská metoda postupného zlepšování „Kaizen“. Zlepšování se zaměří na postupnou optimalizaci procesů a pracovních postupů a tím i zvyšování kvality řízení bezpečnosti ISMS. [7]

Odstraňování nedostatků ISMS

Pro odstraňování nedostatků existují dvě formy opatření:

- opatření k nápravě a
- preventivní opatření [7]

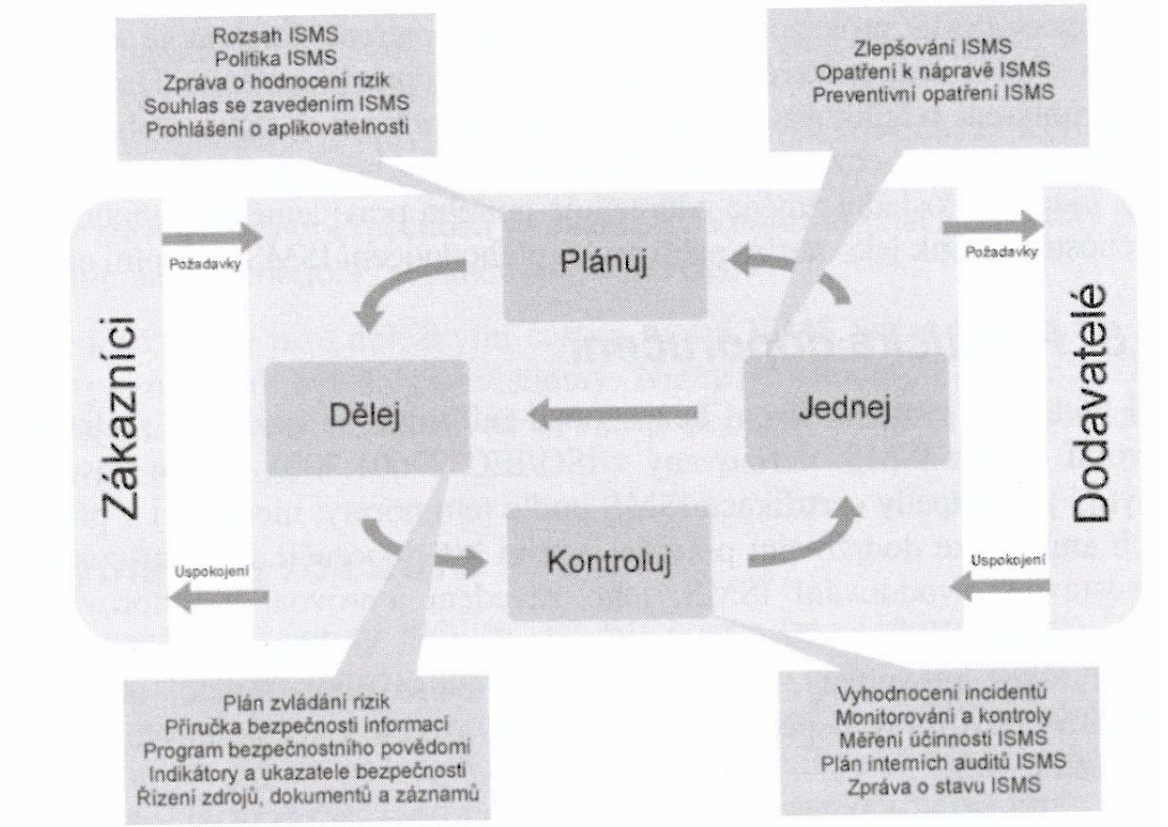
Opatření k nápravě je reaktivní formou řešení nedostatku. V tomto případě se již nedostatek nějakým způsobem projevil (často označujeme tuto skutečnost neshodou) a je potřeba na něj vhodným způsobem reagovat. [7]

Naproti tomu preventivní opatření je proaktivní formou řešení nedostatků ISMS. V tomto případě se vychází z toho, že se zjištěný nedostatek ještě neprojevil, ale další odklad jeho řešení by mohl vést k tomu, že se v budoucnu nějaká negativní událost objeví a způsobí vážnější problémy. [7]

Důležitým a nenahraditelným prvkem odstraňování nedostatků oběma způsoby je objasnění příčin, které k těmto nedostatkům vedly. V tomto smyslu nestačí pouze zjednat nápravu u konkrétní neshody. Je důležité se podívat na souvislosti a opatření realizovat tak, aby se omezily možnosti opakování tohoto nedostatku. Před prosazením obou typů opatření je též nezbytné posoudit, zda zvolené opatření dostatečně zamezí opakování nedostatku a případně pokryje jeho příčiny. [7]

Postupy pro řešení opatření k nápravě a preventivních opatření musí být zdokumentovány a všechny činnosti s nimi spojené musí být zaznamenány a zahrnuty do dokumentace. Po zavedení opatření je důležité přezkoumat, zda zvolená opatření skutečně zajistila očekávanou změnu účinnosti ISMS. To se provádí přímou kontrolou či v případě vážnějších nedostatků mimořádným auditem ISMS. [7]

Praktické zkušenosti ukazují, že často podceňovanou příčinou nedostatků je nedostatečná znalost požadavků, které ISMS vyžaduje. Je zvláštní, že nedostatečná znalost ISMS je jako příčina uváděna pouze výjimečně. Snad je tomu proto, že si nikdo nechce přiznat svoje chyby. [7]



Obrázek 11: Model PDCA pro řízení bezpečnosti informací [7]

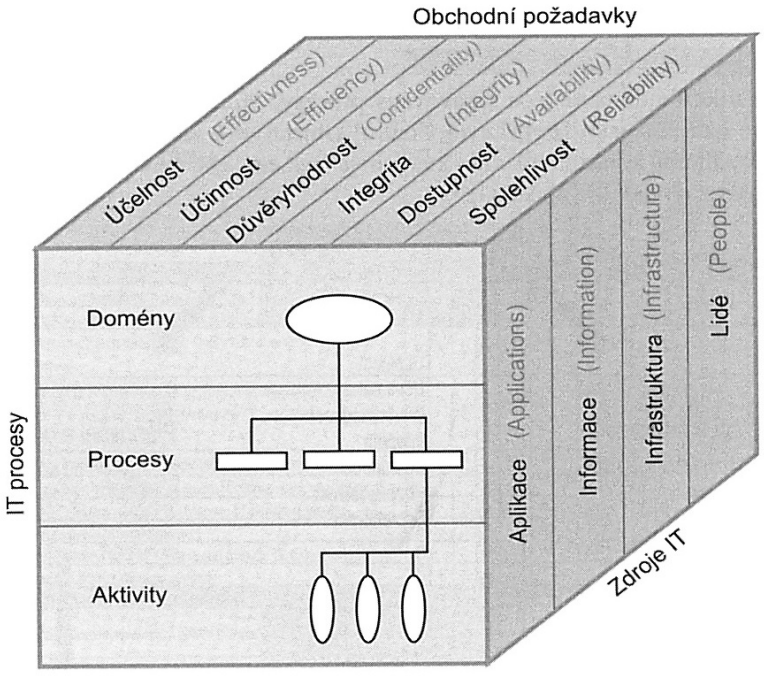
2 METODIKY

Nezbytným předpokladem pro nové koncepce řízení informatiky je jejich podpora ve formě různých standardů, nejlepších zkušeností nebo metodik. Je užitečné se zmínit o dvou metodikách, které jsou obecněji zaměřené a kromě oblasti řízení bezpečnosti se zabývají i dalšími aspekty řízení informatiky organizací. Jedná se o celosvětově rozšířené metodiky COBIT a ITIL. [7]

2.1.1 COBIT

Metodika COBIT (Control Objectives for Information and Related Technology) je pevně spojena s organizací ISACA (information Systems Audit and Control Foundation). Jedná se o sadu všeobecně přijímaných procesů, návodů pro hodnocení, ukazatelů a nejlepších praktických zkušeností, která má za cíl pomoci organizaci maximalizovat užitek plynoucí z informačních technologií. Metodika COBIT je jedním ze základních nástrojů, podporujících IT Governance (řízení) v organizacích. [7]

Základní princip metodiky COBIT je postaven na cílech organizací (strategických požadavcích), zdrojích informačních technologií a procesech. Tyto tři komponenty využívá tzv. Cobit kostka, která je uvedena na obrázku následujícím obrázku.



Obrázek 12: Kostka COBIT [7]

Současně nejlépe ukazuje základní koncepci metodiky: zdroje informatiky, které odpovídají strategickým požadavkům. [7]

COBIT kostka přehledně znázorňuje vzájemné prolínání procesů IT (na úrovni domény, procesů a cílů kontrol/aktivit), zdrojů informatiky (aplikací, informací, infrastruktury, lidí) a požadavků na informační kritéria (efektivnost, výkonnost, důvěrnost, integrita, dostupnost, shoda, hodnověrnost). Procesy IT stojí za bližší pozornost. [7]

Z COBIT kostky je zřetelné, že jsou definovány různé úrovně podrobnosti. Nejobecnější jsou definice domén. Ty COBIT specifikuje čtyři:

- Plánování a organizace.
- Akvizice a implementace.
- Dodávka a podpora.
- Sledování a hodnocení. [7]

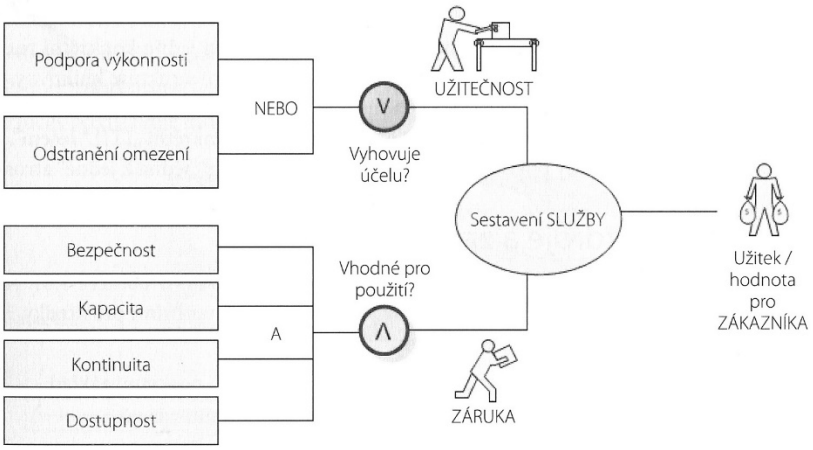
Přehled uvedených domén a jejich vztahy v rámci COBIT kostky je uveden na obrázku

2.1.2 ITIL

ITIL (Information Technology Infrastructure Library) představuje soubor knih, který obsahuje popis způsobů procesního řízení služeb včetně infrastruktury IT, které jsou jejím prostřednictvím poskytovány. Nejnovější verzí ITIL je ITIL Edice 2011, která je dostupná od 29 července 2011. ITIL se koncentruje na plánování, vytváření, modifikaci, dodávku správu, analýzu a použití služeb IT. [7] [4]

Cílem metodiky ITIL je poskytnout ucelený soubor tzv. nejlepších zkušeností pro oblast řízení služeb IT a souvisejících procesů. [7]

ITIL považuje útvar informatiky za poskytovatele služeb a předjímá, že by se měl změnit na „obchodní“ útvar, který poskytuje ostatním útvarům informatické služby. [7]



Obrázek 13: Generování přidané hodnoty pomocí užitečností a záruky[3]

Lidé jako součást organizace služeb nemohou zůstat stranou. Úspěšná realizace strategií závisí do značné míry na každém jednotlivém zaměstnanci. Zaměstnanci představují klíčový faktor pro úspěch organizace. Na základě osobních postojů (attitude) se každá osoba chová (behavior) určitým způsobem. Firemní kultura přitom hraje také důležitou roli (culture). Tyto klíčové faktory úspěchu (známé též jako „ABC informačních technologií“ od Jana Schilta a Paula Wilkinsona) mají zvláštní význam při změnách v organizaci. [3]

Úspěch strategie správy služeb (díky adaptaci ITIL) je možný pouze tehdy, pokud jsou všichni zaměstnanci zapojeni od počátku a je u nich zajištěna orientace na procesy, procesní myšlení a orientace na zákazníka a služby. Zásadní roli hraje otázka komunikace. [3]

V rámci ITIL nejde pouze o čisté IT v podobě hardwarových a softwarových zdrojů. Jde o lidi, kteří (spolu) vytváří organizaci IT, jsou součástí procesů a podporují orientaci služeb. Aby přispěli k úspěchu a uznání organizace IT, a tím i k obchodním úspěchům podniku, musí lidé, procesy a technologie pracovat ruku v ruce [7].

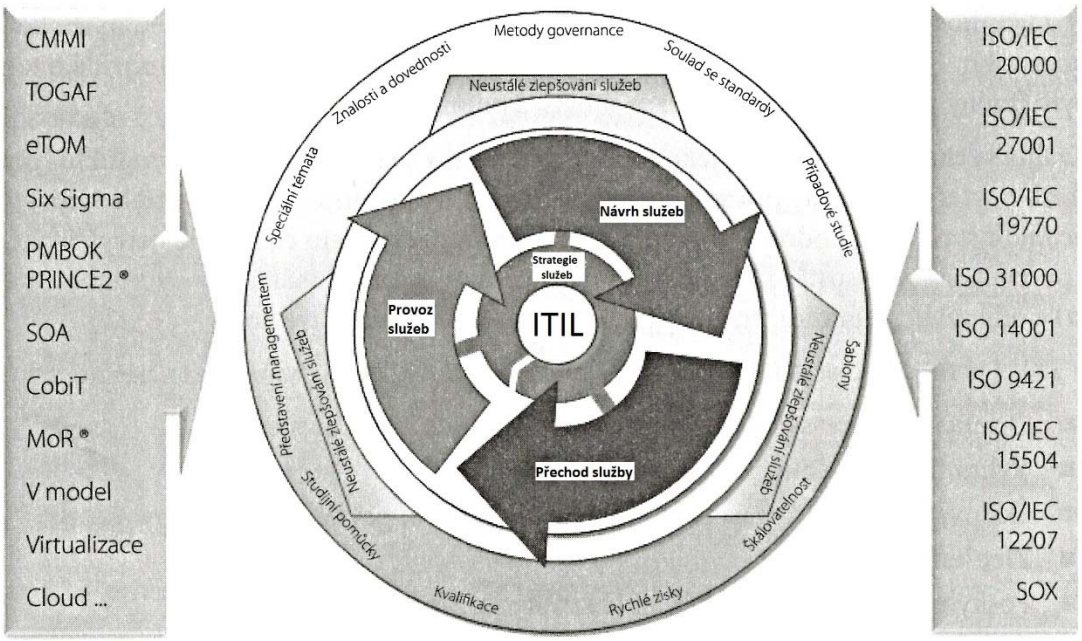
Za klíčové publikace ITIL je označováno pět knih. Každá kniha představuje jednu fázi životního cyklu a popisuje příslušné principy, procesy funkce, organizační a technologické aspekty apod. [3]

Jsou to tyto knihy:

- Strategie služeb (Service Strategy) je základem metodiky. Představuje propojení aktivit organizace se strategií v oblasti informatiky – informační strategií. Obsahuje

definice služeb, strategii ITSM a plánování přidané hodnoty, IT Governance (řízení), definice typů poskytovatelů služeb a strategie návrhu, vývoje a poskytování služeb.

- Návrh služeb (Service Design) obsahuje návrhy služeb IT a architektury informačního systému v organizaci v celém životním cyklu, včetně různých forem sourcingu (insourcingu, outsorcingu) a sdílených služeb.
- Implementace služeb (srvice Transition) zahrnuje návody na implementaci služeb do reálného prostředí. Zahrnuje procesy např. řízení změn, řízení verzí, modely služeb, návrhy kontrol pro uvádění služeb do provozu apod.
- Provoz služeb (Service Operation) podporuje správu služeb v produktivním prostředí, řešení problémů, poruch, stanovení ukazatelů jakosti služeb apod.
- Průběžné zlepšování služeb (Continual Service Improvement) pomáhá zlepšovat zavedené existující služby. [7]



Obrázek 14: Vliv technických témat, norem, standardů na ITIL [3]

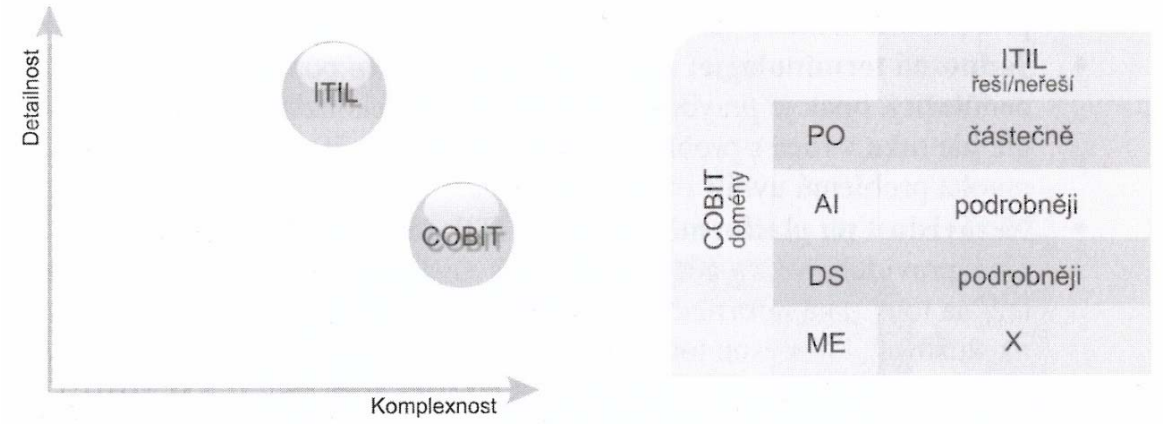
ITIL má dva úhly pohledu k určení hodnoty služby. Zákazníkovi je funkčnost služby přenesena pomocí Utility (užitečnost, fitness for purpose, vhodnost pro daný účel). Jde v tomto ohledu o otázku „co“ bude určeno jako služba. Užitečnost zvedá buď výkonnost zákazníka,

například produktivitu jeho spolupracovníků pomocí nových aplikací a nástrojů, nebo snižuje zákazníkovo omezení, např. při datové komunikaci. Zajištění tohoto pozitivního efektu pokrývá záruka. Existují konkrétní požadavky na požadovanou spolehlivost služby (fitness for use). Ve vztahu ke čtyřem aspektům kvality služby se jedná o otázku „jak“:

- Dostupnost jako schopnost služby IT provést v případě potřeby smluvenou funkci.
- Kapacita jako maximální výkon, který je služba IT schopna poskytnout při dodržení domluvené úrovně služeb.
- Nepřetržitost zajišťuje, že daná služba bude podporovat obchodní procesy i v případě nehody (katastrofy, nepředvídatelné velké incidenty, atd.).
- Bezpečnost k zajištění ochrany firemních hodnot. [3]

2.1.3 Porovnání metodik ITIL a COBIT

Ze studie provedené Information Tchnology Governance Institute plyne, že metodika Cobit je komplexnější, avšak metodika ITIL řeší některé oblasti detailněji. Souhrnně lze konstatovat, že se každou novou verzí metodik dochází k jejich sbližování s tím, že si ponechávají svoje specifika. Jejich současné verze podporují trend vzájemného sbližování, což umožňuje při zavádění ISMS snazší kombinaci a aplikaci v praxi [7].



Obrázek 15: Porovnání metodik ITIL a COBIT [7]

2.2 Vybrané zákonné normy České republiky se zásadním vlivem na problematiku bezpečnosti informací

Prvním krokem pro řešení otázek bezpečnosti informací je modifikace stávajícího právního řádu – přijetí nových úprav již existujících zákonů. Tyto zákony pak upravují způsob pořizování dat, jejich uchovávání a zpracování v podmínkách nasazení informačních a komunikačních technologií – vytvářejí transparentní prostředí pro práci daty prakticky v celé ekonomice. Mnohé ze zákonů přímo ukládají povinnosti různým institucím nebo právním subjektům, některé pak jsou základem pro řízení převážně státních institucí, které se profesionálně zabývají kontrolou dodržování zákonných opatření v oblasti bezpečnosti informací. Dalším úkolem nově vznikajících zákonů je harmonizovat právní řád České republiky s právními řády ostatních členských států Evropské unie a s právem unijním jako celkem. [7]

2.2.1 Zákon č. 106/1999 Sb., o svobodném přístupu k informacím

Tento zákon zakládá povinnost pro orgány a organizace poskytovat informace o své činnosti, upravuje jejich poskytování, zejména vyřízení žádosti včetně náležitostí a způsobu podání žádosti, lhůt, opravných prostředků a způsobu poskytnutí informací. Netýká se informací, jejichž nakládání upravují jiné specializované zákony jako např.

- Zákon č. 527/1990 Sb., o vynálezech a zlepšovacích návrzích, ve znění pozdějších předpisů
- Zákon č. 529/1991 Sb., o ochraně polovodičových výrobků, ve znění pozdějších předpisů,
- Zákon č. 478/1992 Sb., o užitných vzorech, ve znění pozdějších předpisů,
- Zákon č. 452/2001 Sb., o ochraně označení původu a zeměpisných označení a o změně zákona o ochraně spotřebitele, ve znění pozdějších předpisů,
- Zákon č. 441/2003 Sb., o ochranných známkách a o změně zákona č. 6/2002 Sb., o soudech, soudcích, přísedících a státní správě soudů a o změně některých dalších zákonů (zákon o soudu a soudcích), ve znění pozdějších předpisů, (zákon o ochranných známkách), ve znění zákona č. 501/2004 Sb. [7]

2.2.2 Zákon č. 227/2000 Sb., o elektronickém podpisu

Zákon byl naposledy upraven zákonem č. 101/2010 Sb. Jeho realizace byla upravena prováděcí vyhláškou č. 304/2001 Sb. Zákon upravuje v souladu s právem Evropských společenství (zejména se Směrnicí Evropského parlamentu a Rady 99/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy) používání elektronického podpisu, elektronické značky, poskytování certifikačních služeb a souvisejících služeb poskytovateli usazenými na území České republiky, kontrolu povinností stanovených tímto zákonem a sankce za porušení povinností stanovených tímto zákonem. Poslední novelizace z roku 2010 ukládá povinnost vést a zveřejňovat i dálkovým přístupem seznam důvěryhodných certifikačních služeb podle „Rozhodnutí Komise Evropských společenství 2009/767/ES ze dne 16. října 2009“. Zákonná aktualizace způsobila, že zaručený elektronický podpis, založený na kvalifikovaném certifikátu, může být vydán i mimo území České republiky certifikační autoritou v kterémkoliv členském státu Unie. [7]

2.2.3 Zákon č. 151/2000 Sb., o telekomunikacích

Poslední novelizace proběhla zákonem č. 153/2010 Sb. Tento zákon se stal základem pro zřízení Českého telekomunikačního úřadu (ČTÚ). Poslední novelizované znění zákona také ukládá povinnost všem poskytovatelům veřejně dostupných telefonních služeb na žádost poskytnout informace z databáze všech svých účastníků veřejně dostupné telefonní služby orgánu oprávněnému k jejich vyžádání podle zvláštního předpisu, a to na jeho náklady. Formu a rozsah poskytovaných informací stanoví prováděcí právní předpis. Nově byla upravena dikce § 99, který se zabývá poskytováním informačních služeb pro případ mimořádných nebo krizových událostí. [7]

2.2.4 Zákon č. 499/2004 Sb., o archivacích a spisové službě

Tento zákon upravuje:

- výběr, evidenci a kategorizaci archiválií,
- ochranu archiválií,
- práva a povinnosti vlastníků archiválií,
- práva a povinnosti držitelů a správců archiválií,
- využití archiválií,
- zpracování osobních údajů pro účely archivnictví

- soustavu archivů
- práva a povinnosti zřizovatelů archivů,
- spisovou službu,
- působnost Ministerstva vnitra a dalších správních úřadů na úseku archivnictví a výkonu spisové služby,
- správní delikty spojené s porušením povinností podle tohoto zákona [7].

Realizace provádějící vyhláškou č. 645/2004 Sb. Vyhláška v § 2 vymezuje pojmy dokument a archiválie [7].

Dokumentem je každý písemný, obrazový, zvukový, elektronický nebo jiný záznam, ať již v podobě analogové či digitální, který vznikl z činnosti původce. Archiválií je takový záznam, který byl vzhledem k době vzniku, obsahu, původu, vnějším znakům a trvalé hodnotě dané politickým, hospodářským, právním, historickým, kulturním, vědeckým nebo informačním významem vybrán ve veřejném zájmu k trvalému uchování a byl vzat do evidence archiválií; archiváliemi jsou i pečetidla, razítka a jiné hmotné předměty související s archivním fondem či s archivní sbírkou, které byly vzhledem k době vzniku, obsahu, původu, vnějším znakům a trvalé hodnotě dané politickým, hospodářským, právním, historickým, vědeckým nebo informačním významem vybrány a vzaty do evidence [7].

2.2.5 Zákon č. 101/2000 Sb., o ochraně osobních údajů

Zákon v souladu s právem Evropských společenství (Směrnice Evropského parlamentu a Rady 95/46ES ze dne 24. října 1995 o ochraně jednotlivců v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů), mezinárodními smlouvami, kterými je Česká republika vázána (Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat č. 108, vyhlášená pod č.115/2001 Sb. M. s.) a naplněním práva každého na ochranu před neoprávněným zasahováním do soukromí upravuje práva a povinnosti při zpracování osobních údajů a stanoví podmínky, za nichž se uskutečňuje předání osobních údajů do jiných států.[7]

Smyslem zákona o ochraně osobních údajů je Listinou základních práv a svobod zaručené právo na ochranu občana před neoprávněným **zasahováním do jeho soukromého a osobního života, neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním osobních údajů.[7]**

2.2.6 Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti

Tento zákon upravuje zásady pro stanovení informací jako informací utajovaných, podmínky pro přístup k nim a další požadavky na jejich ochranu, zásady pro stanovení citlivých činností a podmínky pro jejich výkon a s tím spojený výkon státní správy. Zákon vymezuje působnost a upravuje činnost **Národního bezpečnostního úřadu (NBÚ).**[7]

Prováděcí vyhlášky zákona č. 412/2005 Sb., pak vymezují, v souladu s ustanovení §5 tohoto zákona, druhy zajištění ochrany utajovaných informací, jejichž úroveň je sledována NBÚ:

- Personální bezpečnost
- Průmyslová bezpečnost
- Administrativní bezpečnost
- Fyzická bezpečnost
- Bezpečnost informačních nebo komunikačních systémů
- Kryptografická ochrana [7]

2.2.7 Zákon č. 121/2000 Sb., autorský zákon

Tento zákon zapracovává předpisy Evropských společenství do legislativního řádu České republiky a následně pak upravuje tyto oblasti:

- práva autora k jeho autorskému dílu,
- práva související s právem autorským,
- právo pořizovatele k jím pořízené databázi,
- ochrana práv podle tohoto zákona,
- kolektivní správu práv autorských a práv souvisejících s právem autorským.[7]

2.2.8 Zákon č. 181/2014 Sb., o kybernetické bezpečnosti

Dlouho připravovaný zákon o kybernetické bezpečnosti (ZKB) nabyl platnost vyhlášením ve Sbírce zákonů dne 29. srpna 2014. Zákon nabyl účinnosti dnem 1. ledna 2015. Se zmíněným zákonem úzce souvisejí následující prováděcí předpisy:

- Vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)

- Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích,
- Nařízení vlády č. 315/2014 Sb., kterými se mění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.[10]

Základním cílem Zákona je zvýšit bezpečnost kybernetického prostoru a zejména se snažit ochránit tu část infrastruktury, která je pro fungování státu důležitá a jejíž narušení by vedlo k poškození nebo ohrožení zájmu České republiky.[10]

Cílem Zákona není řešit všechna rizika v kyberprostoru, jako je např. porušování autorských práv, různé podvodné aktivity, úniky dat či šíření závadného elektronického obsahu.[10]

Objekty, které mohou být zařazeny do kritické infrastruktury, mohou být:

- Elektrárny s požadovaným minimálním výkonem 500MW
- Nemocnice s počtem lůžek vyšším než 2500.
- U informačních systémů je to uchovávání dat o více jak 300 000 uživatelích
- U komunikačních systémů je to stanovena rychlost od 1Gbit/s
- Letiště pro zajištění leteckého provozu
- Správa datových schránek, atd.

Zavádění důvěryhodných informačních a komunikačních systémů, jejich bezpečný provoz a správa je povinností České republiky a odpovědností ve všech úrovních veřejné správy, soukromého sektoru a široké veřejnosti s cílem udržení bezpečného, odolného a důvěryhodného prostředí, které využívá příležitostí digitálního věku. Strategie se zaměřuje především na dostupnost, integritu a důvěryhodnost kybernetického prostoru ČR a je koordinována s ostatními souvisejícími strategiemi a koncepty. [10]

2.3 Tuzemské instituce spojené s bezpečností informačních systémů a informačních a komunikačních technologií

Na základě některých z výše uvedených zákonů byly zřízeny instituce, jejichž hlavním úkolem je řešit otázky spojené s bezpečností informačních systémů a informačních a komunikačních technologií převážně řídícího a kontrolního charakteru. Instituce se zaměřují na vy-

brané oblasti bezpečnosti informací, stanovují bezpečnostní požadavky např. formou vydávaných podzákonných dokumentů, nejčastěji vyhlášek, metodik, směrnic, norem, standardů a dalších normativních dokumentů.[7]

Stupeň dodržení podmínek stanovených předpisy (shoda) je zkoumán různými postupy a je prováděn různými subjekty určenými buď přímo podle znění zákona, nebo zprostředkovaně na základě speciálního pověření.[7]

2.3.1 Úřad pro ochranu osobních údajů – ÚOOÚ

Úřad pro ochranu osobních údajů byl založen v souladu s ustanovením zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů a ve své činnosti se jimi řídí. Ochrana soukromí je v ČR zaručena její Ústavou a Listinou základních práv a svobod. Osobní údaje o každé osobě jsou chráněny uvedeným zákonem, který stanovuje pravidla, zásady, práva a povinnosti při nakládání s nimi. ÚOOÚ je nezávislým orgánem, který zejména:

- provádí dozor nad dodržováním zákonem stanovených povinností při zpracování osobních údajů,
- vede registr povolených zpracování osobních údajů,
- přijímá podněty a stížnosti občanů na porušení zákona,
- poskytuje konzultace v oblasti ochrany osobních údajů.[7]

Úlohou ÚOOÚ je tedy chránit soukromí občanů proti zneužití dat uložených v IS/ICT různých organizacích jak soukromých, tak i státních.[7]

2.3.2 Národní bezpečnostní úřad – NBÚ

Národní Bezpečnostní úřad je podle ustanovení § 2 odst. 1 zákona č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy, ve znění pozdějších předpisů, ústředním orgánem státní správy. Podle ustanovení § 136 odst. 1 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů, vykonává NBÚ státní správu v oblasti ochrany utajovaných informací a bezpečnostní způsobilosti a jeho hlavní úkoly jsou vymezeny v ustanovení § 137 tohoto zákona.[7]

Národní bezpečnostní úřad zejména:

- rozhoduje o žádosti fyzické osoby, žádosti podnikatele a žádosti o doklad a o zrušení platnosti osvědčení fyzické osoby, osvědčení podnikatele a dokladu,
- plní úkoly v oblasti utajovaných informací v souladu se závazky vyplývajícími z členství ČR v EU, Organizaci Severoatlantické smlouvy a z mezinárodních smluv, jimiž je ČR vázána,
- vede ústřední registr a schvaluje zřízení registrů v orgánech státu a u podnikatelů,
- ve stanovených případech povoluje poskytování utajovaných informací v mezinárodním styku,
- zajišťuje činnost Národního střediska komunikační bezpečnosti, Národního střediska pro distribuci kryptografického materiálu, Národního střediska pro měření kompromitujícího elektromagnetického vyzařování a Národního střediska pro bezpečnost informačních systémů, které jsou jeho součástí,
- provádí certifikace technických prostředků, informačních systémů, kryptografických prostředků, kryptografických pracovišť a stínících komor,
- Zajišťuje výzkum, vývoj a výrobu národních kryptografických prostředků,
- Vyvíjí a schvaluje národní šifrové algoritmy a vytváří národní politiku kryptografické ochrany.[7]

2.3.3 Ministerstvo vnitra -MV ČR, Odbor koncepce a koordinace ISVS

Útvar je v podřízenosti náměstka ministra vnitra pro veřejnou správu, informatiku, legislativu a archivnictví. Odbor převzal během roku 2007 kompetence bývalého Ministerstva informatiky ČR. Odbor je útvarem zajišťujícím výkon vybraných kompetencí ministerstva podle zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, jak vyplývá ze změn provedených zákonem č. 517/2002 Sb., zákonem č. 413/2005 Sb., zákonem č. 444/2005 Sb., zákonem č. 70/2006 Sb. A zákonem č.81/20006 Sb.[7]

Působnost odboru koncepce a koordinace ISVS je významná zejména v oblasti koncepce, vývoje a provozu informačního systému veřejné správy. V oblasti bezpečnosti informací a bezpečnosti IS/ICT se jedná zejména o:

- **kontrolní činnost** (podle zákona č. 365/2000 Sb.), založenou na atestacích a certifikacích organizací a jejich informačních systémů na standard ISVS, které byly dříve vydány Ministerstvem informatiky ČR, a nyní patří tato činnost pod jurisdikci odboru,

- činnosti spojené s používáním **elektronického podpisu** (podle zákona č. 227/2000 Sb.).[7]

2.3.4 Úřad pro technickou normalizaci, metrologii a státní zkušebnictví – ÚNMZ

Hlavním posláním ÚNMZ je zabezpečovat úkoly vyplývající ze zákonů ČR, upravující technickou normalizaci, metrologii a státní zkušebnictví a úkoly v oblasti technických předpisů a norem uplatňovaných v rámci členství České republiky v Evropské unii. Úřad vykonává působnost státu v následujících oblastech:

- harmonizace technických předpisů,
- technická normalizace,
- metrologie,
- zkušebnictví.[7]

Působnost úřadu je stanovena zákonem č. 20/1993 Sb., o zabezpečení výkonu státní správy v oblasti technické normalizace, metrologie a státního zkušebnictví, dále zákonem č. 22/1997 Sb., o technických požadavcích na výrobky, zákonem č. 505/1990 Sb., o metrologii a dále vyplývá z příslušných usnesení vlády a mezinárodních smluv, jimiž je ČR vázána. Od 1. ledna roku 2009 byla působnost ÚNMZ rozšířena o veškerou činnost, která před tímto datem patřila do kompetence Českého normalizačního institutu.[7]

V České republice jsou normativní práce z oblasti bezpečnosti v oblasti informačních technologií realizovány na půdě ÚNMZ v Technické normalizační komisi 20 (TNK 20 – Informační technologie). Technická normalizační komise jsou odbornými normalizačními orgány s celostátní působností, registrovanými, metodicky řízenými a koordinovanými odborem normalizace ÚNMZ. Normalizace v oblasti informačních technologií, vymezená pro TNK 20, zahrnuje zpracování následujících problémových oblastí:

- kódované grafické soubory znaků,
- telekomunikace a výměna informačních technologií,
- softwarové inženýrství,
- kazety s optickými disky pro výměnu informací,
- kancelářská zařízení na zpracování dat,
- karty a identifikace osob,
- správa dat,

- bezpečnostní techniky, atd.

2.4 Evropské a mezinárodní instituce spojené s bezpečností informačních systémů a informačních a komunikačních technologií

Kromě tuzemských institucí je oblast řízení bezpečnosti informací výrazně ovlivněna činností jak organizací Evropské unie, tak národních institucí jednotlivých evropských zemí. Zde se zejména prosazují instituce Velké Británie a Německa. Významnou úlohu při normalizaci zejména v oblasti IS/ICT a bezpečnosti informací hrají i mezinárodní instituce z mimoevropských zemí. Jedná se především o organizace ze Spojených států amerických. Nejvýznamnější mezinárodní institucí je Mezinárodní organizace pro normalizaci – ISO. V její jurisdikci je přijímání nejvýznamnějších mezinárodních standardů v oblasti řízení IS/ICT a v oblasti bezpečnosti informací. Přijímané standardy mají formu doporučení tzv. nejlepších zkušeností tak, jak se na nich shodli experti mezinárodních pracovních týmů a jak byly schváleny příslušnými normalizačními institucemi.[7]

2.4.1 British Standards Institute – BSI

Organizace BSI byla založena v roce 1901 jako Engineering Standards Committee. Je členskou organizací ISO a za svého působení vydala více než 15 000 průmyslových standardů. V oblasti bezpečnosti informací se jedná o tak zásadní standardy jako jsou **BS 7799, ITIL** a další. V současné době působí na trhu jako společnost BSI Group s pobočkami ve všech světadílech.[7]

2.4.2 Bundesamt für Schicherheit in der Informationstechnik – německý BSI

Organizace se sídlem v Bonnu byla založena dne 1. ledna 1991 jako zvláštní obor Ministerstva vnitra SRN. Představuje nezávislou a neutrální autoritu v oblasti bezpečnosti IS/ICT v podmínkách informační bezpečnosti.[7]

Spektrum jejího zájmu je velmi široké od analýzy rizik nasazení prostředků IS/ICT (upozorňuje na nebezpečí rizik při nasazení prostředků IS/ICT do praxe a navrhuje k nim odpovídající řešení otázek bezpečnosti). BSI se orientuje na různé cílové skupiny klientů – vývojáře

systémů, jejich distributory a koncové uživatele. Z těchto důvodů také BSI pravidelně sleduje a vyhodnocuje trendy v bezpečnosti informací.

2.4.3 European Network and Information Security Agency – ENISA

ENISA je evropskou organizací, která byla ustanovena Evropskou unií, aby uváděla v život rozhodnutí EU v oblasti kybernetické bezpečnosti (cyber security). Představuje také platformu, která sdružuje odborníky v bezpečnosti informací. Hlavními oblastmi její činnosti jsou:

- řízení a zvládání bezpečnostních incidentů,
- zajištění kontinuity procesů organizací (jak hlavních procesů organizací, tak i procesů ICT),
- procesy identifikace a řízení rizik.

Organizace napomáhá Evropské komisi při přípravě, vývoji a změnách legislativy EU v oblasti počítačových sítí a bezpečnosti informací.[7]

2.4.4 Evropská komise pro normalizaci – CEN

Evropská komise pro normalizaci (European Committee for Standardization – CEN) byla založena v roce 1961 národními normalizačními institucemi ze zemí Evropského ekonomického společenství. [7]

Cílem CEN je tvorba technických norem, které podporují volný obchod, bezpečnost pracovníků a zákazníků, interoperabilitu sítí, ochranu životního prostředí a rozšiřování vědeckých a výzkumných programů. CEN je neziskovou technickou organizací, která podléhá belgickým zákonům.[7]

2.4.5 Asociace pro audit a řízení informačních systémů – ISACA

Organizace ISACA se začala formovat v roce 1967. Oficiálně vznikla až v roce 1969 v USA, ve státě Illinois jako Asociace EDP (Electronic Data Processing) auditorů. Během třiceti let svého působení se stala mezinárodní organizací sdružující celosvětově přes 65 000 profesinálů ve více než 170 místních pobočkách (Local Chapters).[7]

ISACA zastřešuje program mezinárodně uznávaných certifikací CISA (Certified Information Systems Auditor), CISM (Certified Information Security Manager), CGEIT (Certified in the Governance of Enterprise IT) a CRISC (Certified in Risk and information Systems Control), organizuje mezinárodní konference a odborné semináře zaměřené na technická i manažerská témata, vytváří celosvětově platné standardy pro audit a řízení informačních technologií, vydává odbornou literaturu a časopis Information Systems Audit Journal.[7]

2.4.6 Institute of Electrical and Electronics Engineers – IEEE

Nezisková organizace IEEE je vedoucí celosvětovou asociací pro rozvoj technologií. Původně bylo označení IEEE zkratkou pro Instituu elektrotechniků a elektroniků (Institute of Electrical and Electrinics Engineers). Dnes je rozsah zájmu organizace IEEE rozšířen do mnoha různých oblastí. Z hlediska tvorby norem IEEE dominuje v oblasti definice protokolů lokálních (LAN a metropolitních (MAN) datových sítí, označovaných identifikátorem 802.[7]

2.4.7 International Electrotechnical Commission – IEC

IEC je vedoucí organizací ve světě, která se zabývá přípravou a vydáváním mezinárodních norem v oblasti elektřiny, elektrotechniky a příbuzných disciplín včetně IS/ICT. Byla založena v roce 1906 a její sídlo je v Ženevě.[7]

2.4.8 Internet Engineering Task Force – IETF

Organizace IETF je otevřenou odbornou komunitou, určující pravidla a protokoly, které jsou využívány v mezinárodní síti Internet. Vzhledem k významu této jedinečné sítě doporučení IETF respektuje většina výrobců informačních a komunikačních technologií a díky tomu jsou de facto standardem pro většinu řešení informačních a komunikačních technologií. Všechna doporučení IETF je možné získat na webových stránkách organizace.[7]

2.4.9 Mezinárodní organizace pro normalizaci – ISO

ISO je Mezinárodní organizace pro normalizaci (Internattional Organization for Standadization) se sídlem v Ženevě, která byla založena v roce 1947. Zabývá se tvorbou, aktualizací a harmonizací mezinárodních norem ISO a jiných druhů dokumentů (technických specifikací – TS, technických zpráv – TR a veřejně dostupných specifikací – PAS, dohod o technických trendech – TTA, dohod z pracovní konference průmyslu – IWA, pokynů ISO apod.).[7]

ISO je světovou federací národních normalizačních organizací (v podmínkách ČR to je ÚNMZ). Mezi základní povinnosti členů patří informovat zainteresované orgány a organizace ve své zemi o nových normalizačních aktivitách, zajišťovat za danou zemi jednotné stanovisko k předkládaným dokumentům a finančně podporovat činnost ISO.[7]

II. PRAKTICKÁ ČÁST

3 ANALÝZA SOUČASNÉHO STAVU

Obsah této kapitoly přináší základní a podrobnější informace o společnosti, jejich zaměstnancích, používaném HW a SW, a to jak ve vlastnictví společnosti tak i formou pronájmu. Celkové shrnutí současného stavu bezpečnosti informací ve společnosti. Důležité informace, které se v průběhu analýzy dále zpracovávaly, byly získány na základě konzultace s vrcholovým managementem společnosti Kovárna VIVA a.s. Pracovní zařazení mé osoby ve firmě je „správce sítě a aplikací“.

3.1 Informace o společnosti Kovárna VIVA a.s.

Kovárna VIVA a.s. je členem skupiny Třineckých železáren – Moravia Steel a je stoprocentním vlastníkem prostějovské firmy Alper a.s., kterou získala s cílem rozšířit své výrobní kapacity.

Kovárna VIVA a.s. je přední českou průmyslovou kovárnou, která se specializuje zejména na výrobu technologicky náročných zápustkových výkovků pro automobilový průmysl, hydrauliku, strojírenství, atd. V současnosti kovárna VIVA má kolem 500 zaměstnanců. Ve zlínském a prostějovském provozu vykazuje celkový obrat přes 1,5 mld. Kč.

Společnost sídlí v místě původních strojíren ZPS Zlín, kde vlastní šest výrobních hal a jednu správní budovu. Jedna výrobní hala je před rekonstrukcí. Všechny haly jsou postaveny mimo záplavovou zónu. Ve správní budově jsou kanceláře ve druhém nadzemním podlaží.

Každá výrobní hala má ve své části vymezen prostor pro kanceláře. Všechny haly jsou propojeny optickým kabelem a v každá hala má vybudovanou strukturovanou kabeláž Cat5. Všechny aktivní síťové prvky jsou od firmy CISCO. Počítače a notebooky jsou z 95% od firmy Fujitsu-Siemens a zbytek tvoří značky, Lenovo a DELL. Serverová infrastruktura je tvořena servery značky Fujitsu-Siemens. Společnost má kolem 180 počítačů a 35 notebooků. Většina počítačů má nainstalovaný operační systém Windows 7 a novější počítače a notebooky mají již operační systém Windows 10. Na všech počítačích se využívají cloudové služby společnosti Microsoft - Office 365. Na všech počítačích, noteboocích, serverech a tabletech je antivirový program od firmy Symantec, centrálně spravovaný ze serveru (automatické aktualizace). Ve dvou výrobních halách jsou přístupové body AP – CISCO pro připojení do Wi-Fi sítě. Dvě internetová připojení jsou do firmy přivedena optickým kabelem. Každé připojení je od jiného poskytovatele Internetu a v případě výpadku primárního připojení je toto připojení ihned nahrazeno sekundárním.

Firma má vybudované dvě serverové místnosti v různých budovách. V případě výpadku primární serverové místnosti je možné použít pro chod firmy druhou serverovou místnost. V serverové infrastruktuře jsou provozovány operační systémy od společnosti Microsoft. Informační systém ABAS od německé společnosti je provozován pod systémem Linux. Virtualizační platforma je Hyper-V od společnosti Microsoft. Webové stránky společnosti jsou provozovány přes webhosting externího poskytovatele.

Zálohování dat v organizaci je zajištěné z hlediska bezpečnosti informací několika způsoby.

- Uchovávají se bitové kopie dat na serveru,
- Data se zálohují po optickém připojení na datové uložiště (ve vlastnictví organizace) mimo firmu v pronajatém místě datového centra,
- Replika dat – geograficky oddělená záloha. Tento způsob zálohy pomocí Hyper-V repliky umožňuje archivovat nastavení, operační systém, aplikace a veškerá data organizace v reálném čase do datového centra NWT. V případě nečekané události na straně organizace je možné na základě vytvořené repliky zprovoznit v datovém centru NWT ve velmi krátkém čase kompletní prostředí organizace s téměř aktuálními daty. Nároky na přenos dat jsou minimální, protože se jedná pouze o takzvaný přírůstkový a změnový přenos.

Jako firewall slouží organizaci dva fyzické firewally od firmy Fortinet (zaručena redundance zařízení). Spojení s firmou Alper a.s. se zajišťuje přes CISCO MERAKI.

Přes antivirový software Symantec jsou ve firmě zakázané všechny USB zařízení. Pokud uživatelé nutně potřebují ke své práci USB zařízení, provede se registrace zařízení a povolí se. Potom se již zařízení sleduje při jakémkoliv připojení do počítačové sítě na PC nebo notebooku. Všechny tisky v organizaci jsou sledovány přes bezpečnostní software SafeQ. Jiná forma tisku v organizaci je zakázána.

Jako problém vidím v tom, že přenosná zařízení, která se připojují do sítě jak přímo, tak přes zabezpečený kanál VPN, nemají šifrovaná data na discích. Jedná se o notebooku, tablety, externí HDD a flesh paměti. I když v organizaci musí být všechny data ukládána na server a na přenosných zařízeních by se neměly žádné data vyskytovat, dochází k tomu, že některé data jsou uživatelé nuceni zpracovávat offline na svém přenosném zařízení. Potom se organizace vystavuje nebezpečí úniku dat, a to se může stát např. krádeží těchto zařízení nebo neúmyslnou ztrátou těchto zařízení. Proto navrhuji využití šifrovacího software PGP Whole Disk Encryption, a to vzhledem k tomu že organizace používá antivirový software od firmy Symantec.

Další zlepšení bezpečnosti informací v organizaci vznikne zavedením politik podle normy ISO/IEC 27001.

Co všichni ve firmě chápou jako nedostatek v řízení IT je dosavadní fungování helpdesku. Zde jsou ty největší problémy:

- uživatelé zasypávají IT požadavky, které někdy hraničí se smysluplností,
- všichni chápou své požadavky, jako požadavky s nejvyšší prioritou a nejsou schopni rozlišovat prioritu mezi nefunkčním PC (které řídí linku na tepelné zpracování) a PC (pro účetní),
- uživatelé vyžadují zásahy ihned a neuvědomují si, že v jednom okamžiku nemůže být servisní technik na dvou místech,
- uživatelé si neuvědomují, že každý zásah servisního technika nebo odborníka na aplikace a databáze má určitou hodnotu, spíše berou IT tak, že jsou jim povinni sloužit za každou cenu,
- Některé požadavky na úpravu informačního systému se udělají úplně zbytečně, protože se po čase nepoužívají, díky špatné analýze záměru.

Díky využití metodiky ITIL je možné v této oblasti zasáhnout a zvrátit její funkčnost k lepšímu.

3.2 Zjištěný stav bezpečnosti

3.2.1 Fyzická bezpečnost společnosti

Všechny výrobní haly a správní budova jsou vybaveny elektronickým zabezpečovacím systémem a požárními hlásiči. Narušení je hlášeno na pult bezpečnostní agentury, která ihned vyjíždí k zásahu. Jakékoliv zahoření v hale nebo v místnostech budovy je hlášeno na pult požární ochrany. Čtyři výrobní haly a správní budova jsou oploceny a hlídány termo-kamerovým systémem ve dne i v noci. Hlavní kamerový pult je u strážní služby, která ihned vyjíždí k zásahu. Ve dne jsou prostory hlídány dalším kamerovým systémem (hlavně pro případ krádeží, identifikace narušitele, atd.). Vstupy do prostoru nádvoří budov a přímo do budov jsou na čipové karty. Každý vstup zaznamenává všechny průchody. Tím se vytváří přehled o pohybu osob v areálu.

Ve všech halách, kancelářích a technických místnostech areálu organizace jsou požární hlásiče, které podléhají pravidelným kontrolám a jsou napojeny na centrální pult požární

ochrany. Serverové místnosti jsou hlídané pomocí teplotních čidel, a pokud teplota překročí stanovenou hranici, ihned se odešle SMS na telefony správy IS/IT. Všechny síťové aktivní prvky jsou v uzamčených rack skříních.

3.2.2 Bezpečnost provozu a komunikací

Společnost má velmi dobře vybudovanou ochranu své sítě a těmito prvky jsou:

- dva redundantní hardware firewally,
- switche CISCO s managementem,
- centrálně ze serveru řízený antivir Symantec na všech PC a serverech,
- uživatelé nemají možnost instalace software na svých PC,
- zablokované USB ve všech PC organizace,
- přes GPO nastavené spořiče obrazovek chráněné heslem po 15 minutách nečinnosti,
- zajištění zálohy mimo firmu,
- zajištění repliky dat do datového centra NWT a možnost zprovoznit firmu pomocí této repliky z datového centra,
- dvě na sobě nezávislé připojení k Internetu, atd.

3.2.3 Bezpečnost lidských zdrojů

Společnost má velmi dobře fungující personální oddělení. Ve smlouvách se již řeší právní aspekt z hlediska mlčenlivosti zaměstnance, jenž zaručuje možný postih zaměstnance v případě úniku informací ze společnosti. Při ukončení pracovního vztahu musí zaměstnanec projít všechny útvary a odpovědné osoby mu dají potvrzení, že nemá již žádné závazky v tomto útvaru vůči společnosti. Jednou z podmínek výstupního listu je u útvaru IS/IT blokace veškerých práv, které měl zaměstnanec k dispozici a odevzdání přístupových karet (v případě ztráty provedena okamžitá blokace). Mlčenlivost zaměstnance je samozřejmě smlouvou vyžadována i po určitou dobu skončení jeho pracovního poměru.

3.2.4 Řízení přístupu a ochrana osobních údajů

Proti neoprávněnému přístupu k informacím jsou všechny PC v doméně chráněny heslem a přes GPO je zajištěno spuštění spořiče obrazovky po 15 minutách nečinnosti uživatele. Všechny databáze jsou chráněny přístupovými hesly, která jsou svázány s rolemi uživatelů a tím i právy v těchto databázích. Všechna činnost uživatelů je monitorována pomocí Monitoringu od firmy Alvao. Jakýkoliv výskyt nelegálního software je ihned řešen jako incident.

Všechny osobní údaje zaměstnanců jsou bezpečně uchovávány a zajištěny proti přístupu neoprávněnou osobou. To se vše děje v souladu se zákonem o ochraně osobních údajů. Zaměstnanci, kteří přijdou do styku s osobními informacemi, jsou povinni řídit se organizačními pokyny pro ochranu těchto dat. Jakékoliv porušení této politiky společnosti je bráno jako hrubé porušení pracovní kázně.

Pokud jsou zaměstnanci svědky porušení této politiky společnosti, jsou povinni tento incident hlásit svému nadřízenému.

4 VLASTNÍ NÁVRHY INFORMAČNÍ BEZPEČNOSTI

Úkolem je navrhnout taková bezpečnostní opatření, aby se minimalizovaly největší rizika ve společnosti. Prvním krokem bude provedení analýzy rizik. Je zapotřebí identifikovat všechny aktiva společnosti a tato aktiva ohodnotit a to vše za spolupráce vrcholového managementu. Potom se musí identifikovat hrozby a stanovit s jakou pravděpodobností se mohou vyskytnout. Dalším krokem je ohodnocení zranitelnosti aktiv vůči možným hrozbám a vypočítá se míra rizika. Na základě těchto bezpečnostních rizik se vyberou vhodná bezpečnostní opatření, která budou sloužit k zajištění akceptovatelné bezpečnosti.

4.1 Provedení analýzy rizik

V první fázi analýzy se identifikují aktiva organizace. Tato tabulka byla sestavena na základě konzultace a komunikace s vrcholovým managementem společnosti (vedením společnosti), za účasti majitele společnosti. Potom je vzápětí provedeno ohodnocení aktiv, a to podle dopadu na společnost, jenž se děje v důsledku porušení důvěrnosti, integrity a dostupnosti daného aktiva. Pro ohodnocení aktiv je použita škála 1 až 5. nejdůležitější aktiva jsou ohodnocena „5“ na škále.

Tabulka 1 : Škála ohodnocení aktiv

Popis dopadu	Hodnota aktiva
žádný dopad na organizaci	1
minimální dopad na organizaci	2
střední potíže a možnost finančních ztrát	3
velké potíže a finanční ztráty	4
existenční potíže organizace	5

Škála hodnocení aktiv je k dispozici a nyní je dalším krokem analýzy rizik identifikace aktiv organizace, která musí probíhat ve spolupráci s vrcholovým managementem organizace. Identifikované aktiva jsou v následující tabulce 2:

Tabulka 2 – Identifikované aktiva organizace

Skupina	Aktivum (A)
DATA	Databáze ABAS
	Databáze Datapoint
	Databáze Teamcenter
	Databáze RQM
	Databáze Forge
	Databáze FK
	Databáze BNS
	Databáze aktion
	Data File-Server2
	Databáze SAFEQ
	Účetní doklady/papírově
	Personální data
	Data FORGE
	Programy CNC
	Měření 3D
	Technická data - lisy
	technická data - ohřevy
	Autentizační údaje
Hardware	Počítače Embeded
	Počítače Office
	Pracovní stanice
	Průmyslové PC
	Servery
	Switche
	přístupové čtečky karet
	Kamerové DVR
	VoIP ústředna
	Kamery
	Přenosnná zařízení
	Router
	Tiskárny
	Kabeláž
	Síťová infrastruktura
	Přenosná média
Software	Operační systém
	Kancelářské programy
	ABB studio
	Step -Simatic
	Účetní programy
Služby	Elektronická pošta
	Office 365
	Webové stránky
	Připojení k internetu

Nyní se musí tyto aktiva ohodnotit a pomocí součtového algoritmu se vypočte hodnota aktiva: **Hodnota aktiva = (Dostupnost + Důvěrnost + Integrita) /3**

Tabulka 3 – Ohodnocení aktiv

Skupina	Aktivum (A)	Důvěrnost	Integrita	Dostupnost	Hodnota aktiva
DATA	Databáze ABAS	5	5	5	5
	Databáze Datapoint	4	5	5	5
	Databáze Teamcenter	5	5	5	5
	Databáze RQM	4	5	4	4
	Databáze Forge	4	5	4	4
	Databáze FK	5	5	5	5
	Databáze BNS	5	5	4	5
	Databáze aktion	4	5	4	4
	Data File-Server2	4	4	4	4
	Databáze SAFEQ	4	4	4	4
	Účetní doklady/papírově	5	4	4	4
	Personální data	5	5	4	5
	Data FORGE	4	5	4	4
	Programy CNC	5	5	5	5
	Měření 3D	5	5	5	5
	Technická data - lisy	3	4	3	3
	technická data - ohřevy	3	4	3	3
	Autentizační údaje	5	4	4	4
Hardware	Počítače Embeded	4	4	4	4
	Počítače Office	5	4	4	4
	Pracovní stanice	4	3	3	3
	Průmyslové PC	4	4	4	4
	Servery	5	5	5	5
	Switche	5	5	5	5
	přístupové čtečky karet	3	3	3	3
	Kamerové DVR	4	4	3	4
	VoIP ústředna	5	5	5	5
	Kamery	3	3	3	3
	Přenosnná zařízení	4	4	4	4
	Router	4	3	3	3
	Tiskárny	4	5	5	5
	Kabeláž	3	4	3	3
	Síťová infrastruktura	4	4	3	4
	Přenosná média	5	4	3	4
Software	Operační systém	3	4	4	4
	Kancelářské programy	3	3	3	3
	ABB studio	5	5	5	5
	Step -Simatic	5	5	5	5
	Účetní programy	5	3	3	4
Služby	Elektronická pošta	3	3	2	3
	Office 365	4	5	5	5
	Webové stránky	3	3	4	3
	Připojení k internetu	3	4	4	4

Nyní musí být stanovena škála pro pravděpodobnosti hrozeb. Je to škála 1-5 s tím, že jedna je nejmenší pravděpodobnost hrozby a pět je nejvyšší pravděpodobnost hrozby.

Tabulka 4 – Škála pravděpodobnosti hrozeb

Popis	Hodnota
velmi malá pravděpodobnost hrozby	1
malá pravděpodobnost hrozby	2
střední pravděpodobnost hrozby	3
vysoká pravděpodobnost hrozby	4
velmi vysoká pravděpodobnost hrozby	5

Musí být následně vytvořena tabulka hrozeb, které mohou aktiva organizace ohrozit a tím i poškodit nebo způsobit přímo ztrátu. Pro vypracování tabulky hrozeb je možné použít i katalog hrozeb, jenž je obsahem normy ČSN ISO/IEC TR 13335 nebo BS 7799-3. K vypracování tabulky hrozeb bylo použito letitých zkušeností vrcholového managementu organizace.

Tabulka 5 – Identifikace a ohodnocení hrozeb

Hrozba	Pravděpodobnost
Útok z vnějšku	2
Neoprávněný přístup do prostor firmy	1
Požár	1
Poškození vodou	1
Úder bleskem	1
Krádež zařízení	4
Krádež dokumentů	3
Porucha hardwaru	3
Poškození hardware/neúmyslné	2
Poškození hardware /úmyslné	1
Poškození LAN/neúmyslné	2
Poškození LAN//úmyslné	1
Počítačový virus	2
Výpadek internetu	2
Výpadek pevné linky	2
Výpadek elektrického proudu	3
Prozrazení autentizačních údajů	3
Chybné zaslání citlivých dat	3
Porušení mlčenlivosti zaměstnance	3
Nedostupnost webových stránek	3
Poškození zálohovacího média	2
Útok /SPAM	2
Útok z vnějšku na Wifi	2
Výpadek termokamerového systému	2
Výpadek kamerového systému	2
Modifikace záloh	2
Ztráta záloh	1
Modifikace databází	1
Nefunkčnost přístupového systému	1
Útok z vnitřku organizace	3
Neúmyslná modifikace dokumentů	2
Zneužití přenosného zařízení pro špionáž	4

V dalším kroku analýzy se musí posoudit zranitelnost jednotlivých aktiv jednotlivými hrozbami a tím vlastně doplnit buňky vytvořené tabulky. Tím se vytvoří matice zranitelností, která je znázorněna v příloze **P II**.

Podobným způsobem se sestavuje matice rizik, v níž jsou míry rizika a to jak pro kombinaci aktiv, tak i pro kombinaci hrozeb. Pro výpočet míry rizika se použije tento vzorec:

R = T * A * V, kde „T“ je pravděpodobnost, „A“ je aktivum a „V“ je zranitelnost. Výsledné hodnoty tohoto vzorce jsou vyjádřeny třemi kategoriemi rizik:

Tabulka 6 – Kategorie rizik

Rozmezí možného rizika	Stupnice míry rizik
1 – 40	**Nízká míra rizika**
41 – 80	**Střední míra rizika**
81 – 125	**Vysoká míra rizika**

Pokud se v matici rizik neobjeví vysoká míra rizika, znamená to pro organizaci, že bude mít velmi dobrou výchozí pozici pro zavedení ISMS do celé organizace (holdingu) bez velkých komplikací.

V příloze **P III** – je uvedena tabulka matice rizik. Zde je již jasně vidět že v organizaci opravdu nejsou dosaženy vysoké míry rizik.

4.2 Zavedení bezpečnostních opatření

Na základě analýzy rizik v organizaci je potřeba zavádět bezpečnostní politiky a jejich opatření a to v souladu s přílohou A normy ISO/IEC 27001. Všechna opatření a pokyny k implementaci bezpečnosti informací, jsou přímo odvozeny a propojeny z normy ČSN ISO/IEC 27002.[7]

Vzhledem k tomu, že organizace chce do budoucna získat certifikaci v oblasti bezpečnosti informací, je nutné postupně zavést a splnit všechny cíle opatření a jednotlivá opatření, které jsou uvedeny v tabulce A.1 normy ISO/IEC 27001. Vzhledem k tomu, že se při zavádění této normy nedoporučuje ihned zavést všechny cíle a opatření bezpečnosti informací, protože tak velký záběr na organizaci může být spíše kontraproduktivní a může dojít k určité apatii ze strany zaměstnanců i zaměstnavatele tyto opatření neplnit, nebo je dokonce bojkotovat.

Tabulka 7 – ČSN ISO/IEC 27001 Příloha A (normativní) [8]

ČSN ISO/IEC 27001
Příloha A (normativní)

Tabulka A.1- Cíle opatření a jednotlivá opatření		zavádět	Počet hodin	Zavedeno	zavádět později
A.5	**Politiky bezpečnosti informací**				
A.5.1	Směřování bezpečnosti informací vedením organizace				
A.5. 1.1	Politiky pro bezpečnost informací	zavádět	15		
A.5. 1.2	Přezkoumání politik pro bezpečnost informací	zavádět	20		
A.6	**Organizace bezpečnosti informací**				
A.6.1	Interní organizace				
A.6.1.1	Role a odpovědnosti bezpečnosti informací	zavádět	5		
A.6.1.2	Princip oddělení povinnosti	zavádět	15		
A.6.1.3	Kontakt s příslušnými orgány a autoritami	zavádět	1		
A.6.1.4	Kontakt se zájmovými skupinami				později
A.6. 1.5	Bezpečnost informací v řízení projektů	zavádět	3		
A .6.2	**Mobilní zařízení a práce na dálku**				
A.6.2.1	Politika mobilních zařízení	zavádět	20		
A.6.2.2	Práce na dálku			zavedeno	
A.7	**Bezpečnost lidských zdrojů**				
A.7. 1	Před vznikem pracovního vztahu	zavádět	3		
A.7.1.1	Prověřování				později
A.7.1.2	Podmínky pracovního vztahu			zavedeno	
A .7.2	Během pracovního vztahu			zavedeno	
A.7.2.1	Odpovědnosti vedení organizace	zavádět	15		
A.7.2.2	Povědomí, vzdělávání	zavádět	18		
A .7.2.3	Disciplinární řízení	zavádět	10		
A.7.3	Ukončení a změna pracovního vztahu			zavedeno	
A .7.3.1	Odpovědnosti při ukončení			zavedeno	
A.8	**Řízení aktiv**				
A.8.1	**Odpovědnost za aktiva**				
A.8. 1.1	Seznam aktiv	zavádět	6		
A.8.1.2	Vlastnictví aktiv	zavádět	2		
A.8.1.3	Přípustné použití aktiv	zavádět	8		
A.8.1.4	Navrácení aktiv	zavádět	2		
A.8.2	**Klasifikace informací**				
A.8 .2.1	Klasifikace informací	zavádět	15		
A.8 .2.2	Označování informací	zavádět	8		
A.8.2.3	Manipulace s aktivy	zavádět	10		
A.8.3	**Manipulace s médii**				
A.8.3.1	Správa výměnných médií	zavádět	6		
A.8 .3.2	Likvidace médií	zavádět	2		
A.8.3.3	Přeprava fyzických médií	zavádět	3		
A.9	**Řízení přístupu**				
A.9.1	Požadavky organizace na řízení přístupu				
A.9.1.1	Politika řízení přístupu	zavádět	10		
A.9.1.2	Přístup ksítím a síťovým službám			zavedeno	
A.9.2	**Řízení přístupu uživatelů**				
A.9.2.1	Registrace a zrušení registrace uživatele			zavedeno	
A.9.2 .2	Správa uživatelských přístupů			zavedeno	
A.9.2.3	Správa privilegovaných přístupových práv			zavedeno	
A.9.2.4	Správa tajných autentizačních informací uživatelů			zavedeno	
A.9.2.5	Přezkoumání přístupových práv uživatelů	zavádět	5		
A.9.2.6	Odebrání nebo úprava přístupových práv			zavedeno	

A.9.3	**Odpovědnosti uživatelů**				
A.9.3.1	Používání tajných autentizačních informací	zavádět	2		
A.9.4	Řízení přístupu k systému a aplikacím			zavedeno	
A.9.4 .1	Omezení přístupu k informacím			zavedeno	
A.9.4.2	Bezpečné postupy přihlášení			zavedeno	
A.9.4.3	Systém správy hesel			zavedeno	
A.9.4.4	Použití privilegovaných programových nástrojů			zavedeno	
A.9.4.5	Řízení přístupu ke zdrojovým kódům programu			zavedeno	
A.10	**Kryptografie**				
A.10.1	Kryptografická opatření				
A.10. 1.1	Politika pro použití kryptografických opatření	zavádět	6		
A.10.1.2	Správa klíčů	zavádět	6		
A.11	**Fyzická bezpečnost a bezpečnost prostředí**				
A.11.1	**Bezpečné oblasti**				
A.11.1.1	Fyzický bezpečnostní perimetr			zavedeno	
A. 11.1.2	Fyzické kontroly vstupu			zavedeno	
A. 11.1.3	Zabezpečení kanceláří, místností a vybavení			zavedeno	
A.11.1.4	Ochrana před vnějšími hrozbami a hrozbami prostředí			zavedeno	
A.11.1.5	Práce v bezpečných oblastech			zavedeno	
A.11.1.6	Oblasti pro nakládku a vykládku			zavedeno	
A.11.2	**Zařízení**				
A.11.2.1	Umístění zařízení a jeho ochrana			zavedeno	
A.11.2.2	Podpůrné služby			zavedeno	
A.11.2.3	Bezpečnost kabelových rozvodů			zavedeno	
A. 11.2.4	Údržba zařízení			zavedeno	
A. 11.2.5	Přemístění aktiv			zavedeno	
A.11.2.6	Bezpečnost zařízení a aktiv mimo prostory			zavedeno	
A.11.2.7	Bezpečná likvidace nebo			zavedeno	
A.11.2.8	Uživatelská zařízení bez			zavedeno	
A .11.2.9	Zásada prázdného stolu			zavedeno	
A.12	**Bezpečnost provozu**				
A.12.1	Provozní postupy a odpovědnosti				
A.12. 1.1	Dokumentované provozní postupy	zavádět	4		
A.12.1.2	Řízení změn	zavádět	6		
A.12.1.3	Řízení kapacit	zavádět	2		
A.12.1.4	Princip oddělení prostředí			zavedeno	
A.12.2	**Ochrana proti malwaru**				
A.12.2.1	Opatření proti mawaru			zavedeno	
A.12.3	**Zálohování**				
A.12 .3.1	Zálohování informací			zavedeno	
A.12.4	**Zaznamenávání formou logů a monitorování**				
A.12.4.1	Zaznamenávání událostí formou logů			zavedeno	
A.12.4.2	Ochrana logů			zavedeno	
A.12.4 .3	Logy o činnosti administrátorů a operátorů			zavedeno	
A.12.4.4	Synchronizace hodin			zavedeno	
A.12.5	**Správa provozního softwaru**				
A.12.5.1	Instalace softwaru na provozní systémy	zavádět	2		
A.12.6	**Řízení technických zranitelností**				
A.12.6.1	Řízení technických zranitelností			zavedeno	
A. 12.6.2	Omezení instalace			zavedeno	
A.12.7	**Hlediska auditu informačních systémů**				
A. 12.7.1	Opatření k auditu informačních systémů				později
A.13	**Bezpečnost komunikací**				

A.13.1	**Správa bezpečnosti sítě**				
A. 13.1.1	Opatřeni v sitich			zavedeno	
A.13.1.2	Bezpečnost síťových služeb			zavedeno	
A.13.2	**Přenos informací**				
A.13.2.1	Politiky a postupy při přenosu informaci	zavádět	8		
A.13.2.2	Dohody o přenosu informaci	zavádět	3		
A. 13.2.3	Elektronické předáváni	zavádět	2		
A.13.2.4	Dohody o utajeni nebo o mlčenlivosti			zavedeno	
A .14	**Akvizice, vývoj a údržba systémů**				
A .14.1	**Bezpečnostní požadavky informačních systémů**				
A.14.1.1	Analýza a specifikace požadavků bezpečnosti informaci			zavedeno	
A.14.1.2	Zabezpečeni aplikačních služeb ve veřejných sítich			zavedeno	
A.14.1.3	Ochrana transakci aplikačních služeb			zavedeno	
A.14.2	**Bezpečnost v procesech vývoje a podpory**				
A.14.2.1	Politika bezpečného vývoje				později
A.14.2.2	Postupy řízeni změn systémů				později
A.14.2 .3	Technické přezkoumáni aplikaci po změnách provozni				později
A.14.2.4	Omezeni změn softwarových balíků				později
A.14.2.5	Principy budováni bezpečných systémů				později
A.14.2.6	Prostředi bezpečného vývoje				později
A.14 .2.7	Outsourcovaný vývoj				později
A.14.2.8	Testováni bezpečnosti systémů				později
A.14.2.9	Testováni akceptace systémů				později
A.14.3	**Data pro testování**				
A.14.3.1	Ochrana dat pro testování				později
A.15	**Dodavatelské vztahy**				
A.15.1	**Bezpečnost informací v dodavatelských vztazích**				
A.15.1.1	Politika bezpečnosti informaci pro dodavatelské vztahy				později
A. 15.1.2	Bezpečnostni požadavky v dohodách s dodavateli				později
A. 15.1.3	Dodavatelský řetězec informačnich				později
A.15.2	**Řízeni dodávek služeb dodavatelů**				
A.15.2.1	Monitorováni a přezkoumáváni služeb dodavatelů				později
A.15.2.2	Řízeni změn ve službách dodavatelů				později
A.16	**Řízeni incidentů bezpečnosti informací**				
A.16.1	**Řízeni incidentů bezpečnosti informací a zlepšování**				
A. 16.1.1	Odpovědnosti a postupy	zavádět	4		
A.16 .1.2	Hlášeni události bezpečnosti informaci	zavádět	2		
A.16.1.3	Hlášeni slabých mist bezpečnosti informaci	zavádět	2		
A.16.1.4	Posouzeni a rozhodnuti	zavádět	6		
A.16 .1.5	Reakce na incidenty bezpečnosti informaci	zavádět	2		
A.16.1.6	Ponaučeni z incidentů bezpečnosti informaci	zavádět	2		
A.16.1.7	Shromažďováni důkazů	zavádět	4		
A.17	**Aspekty řízeni komtinuity činností organizace z hlediska bezpečnosti informací**				
A. 17.1	**Kontinuita bezpečnosti informací**				
A.17.1.1	Plánováni kontinuity bezpečnosti informaci				později
A.17.1.2	Implementace kontinuity bezpečnosti informaci				později
A.17.1.3	Verifikace, přezkoumáni a vyhodnoceni kontinuity bezpečnosti informaci				později
A .17.2	**Redundance**				
A. 17.2.1	Dostupnost vybaveni pro zpracováni informaci			zavedeno	
A.18	**Soulad s požadavky**				
A.18.1	**Soulad s právními a smluvními požadavky**				

A.18.1.1	Identifikace odpovidajici legislativy a smluvnich požadavků	zavádět	3		
A.18. 1.2	Ochrana duševního vlastnictvi	zavádět	4		
A.18.1.3	Ochrana záznamů	zavádět	2		
A.18.1.4	Soukromi a ochrana osobnich údajů			zavedeno	
A. 18.1.5	Regulace kryptografických opatřeni	zavádět	4		
A.18.2	**Přezkoumání bezpečnosti informací**				
A.18.2.1	Nezávislá přezkoumání bezpečnosti informaci	zavádět	2		
A.18.2.2	Shoda s bezpečnostními politikami a normami	zavádět	4		
A. 18.2.3	Přezkoumání technické shody	zavádět	2		
	Celkem hodin na zavedeni		286		

4.2.1 Politiky bezpečnosti informací (A.5)

Zavedením těchto opatření je určit směr a vyjádřit podporu bezpečnosti informací ze strany vedení v souladu s požadavky týkající se činnosti organizace, příslušnými zákony a směrnicemi. Důležitým bodem po zavedení opatření je jejich plánované přezkoumávání.

Politiky pro bezpečnost informací (A.5.1.1)

Zde je prvořadým úkolem definovat „politiku bezpečnosti informací“ v souladu s příslušnými zákony, směrnicemi a požadavky týkající se činnosti organizace. Tuto sadu politik pro bezpečnost informací schválit vrcholným managementem organizace a seznámit s ní všechny zaměstnance formou školení.

Vydat jeden dokument „Politiku bezpečnosti informací“. Každá politika má vlastníka, který schválí odpovědnost managementu za vývoj, přezkoumávání a vyhodnocování politik. Přezkoumávání politik pro bezpečnost bere v úvahu výsledky přezkoumávání prováděné managementem. Všechny revidované politiky jsou opět schvalovány managementem. Politika bezpečnosti řeší požadavky vyvolané:

- podnikatelskou strategií,
- předpisy, legislativou a smlouvami,
- prostředím současných a očekávaných hrozeb bezpečnosti informací.

Politika bude obsahovat prohlášení k definici bezpečnosti informací, cílů, principů a postupy pro zacházení s odchylkami a výjimkami. Na nižší úrovni musí politika bezpečnosti pokrýt řešení potřeb určitých cílových skupin v rámci organizace nebo určité témata.

Časová náročnost vypracování: **15 hodin**.

Přezkoumání politik pro bezpečnost informací (A.5.1.2)

Pro zajištění neustálé vhodnosti, přiměřenosti a efektivnosti bezpečnosti informací se vypracuje plán vývoje, přezkoumání a vyhodnocování politik s periodicitou tři krát ročně. Za každou přezkoumanou politiku odpovídá vlastník. Revidované politiky budou schvalovány managementem.

Časová náročnost přezkoumání a revize politik: **20 hodin**

4.2.2 Organizace bezpečnosti informací (A.6)

Ustanovit řídící rámec pro zahájení a řízení implementace a provozu bezpečnosti informací v rámci organizace. V této části jsou opatření stanovující odpovědnosti, povinnosti v oblasti bezpečnosti informací, a to zabezpečení práce na dálku a bezpečnost použití mobilních zařízení.

Role a odpovědnosti bezpečnosti informací (A.6.1.1)

Definovat odpovědnosti určeným pracovníkům za činnosti v oblasti řízení rizik bezpečnosti informací, a zejména za přijetí zbytkového rizika. Doplnit odpovědnosti podrobnějšími pokyny pro specifická pracoviště. Zodpovědná osoba může delegovat úkoly na jinou osobu, ale tím se nezbavuje zodpovědnosti za řešený úkol.

Časová náročnost zavedení: **5 hodin**

Princip oddělení povinností (A.6.1.2)

Striktně oddělit jednotlivým osobám konfliktní povinnosti a oblasti působnosti, aby nemohly přistupovat k aktivům a následně je upravovat, nebo je používaly bez oprávnění a detekce. Tím se zabrání náhodnému nebo úmyslnému zneužití aktiv ve vlastnictví organizace.

Časová náročnost zavedení : **15 hodin**

Kontakt s příslušnými orgány a autoritami (A.6.1.3)

Zavést kontaktní osoby, které budou mít pověření od organizace kontaktovat autority (např. dodavatel elektřiny, mobilní operátor, orgán vymáhající právo, atd.). V organizaci jsou určeny kontaktní osoby, ale není vypracována konkrétní směrnice, která komplexně shrnuje všechny kontaktní osoby.

Časová náročnost zavedení: **1 hodina**

Bezpečnost informací v řízení projektů (A.6.1.5)

Řešit bezpečnost informací začleněním do metody (metod) řízení projektů v organizaci a tím zajistit identifikaci rizik bezpečnosti informací a jejich řešení jako součást projektu. Používané metody řízení projektů musí vyžadovat, aby:

- cíle bezpečnosti informací byly zahrnuty do projektových cílů,
- posuzování rizik bezpečnosti informací se provádělo již v rané fázi projektu, aby se identifikovala nezbytná opatření,
- bezpečnost informací byla součástí všech fází použité projektové metodiky.

Časová náročnost zavedení: **3 hodiny**

Politika mobilních zařízení (A.6.2.1)

Zamezit riziku ztráty firemních informací různého stupně důležitosti pro firmu. Proškolit osoby používající mobilní zařízení na možné bezpečnostní riziko úniku informací. Šifrovat přenosná zařízení (notebook, tablet, externí HDD, flash disk, atd.) a tím zamezit ztrátě firemních informací. Poučit osoby o nebezpečí připojení mobilního zařízení přes bezdrátové sítě ve veřejných zařízeních (kavárny, rychlé občerstvení, počítačové herny, atd.). Zabezpečení mobilních zařízení na hotelích (použití sejfu). Nebezpečí ponechání mobilního zařízení ve veřejném dopravním prostředku nebo automobilu. Snažit se zpracovávat data online nebo zpracovat offline a ihned odeslat na server. Tím zamezit ponechání informací na mobilním zařízení.

Časová náročnost zavedení: **20 hodin**

4.2.3 Bezpečnost lidských zdrojů (A.7.1)

Určitě této části opatření věnovat velkou pozornost, protože tady je velké potenciální riziko narušení bezpečnosti informací. Budování důvěry v pracovníky firmy a majitelem je zdlouhavý a složitý proces. Předejít možným problémům se dá již dodržením určitého postupu ověřování nových pracovníků již při nástupu:

- dostupnost uspokojivých osobních nebo profesních posudků,
- doporučení od důvěryhodné osoby,
- ověření životopisu žadatele,

- podrobnější ověření, jako jsou posouzení finanční situace nebo výpis z rejstříku trestů, atd.

Časová náročnost zavedení: **3 hodiny**

Odpovědnosti managementu organizace (A.7.2.1)

Management musí vyžadovat od všech zaměstnanců a smluvních stran, aby po náležitém informování o svých rolích a odpovědnostech v oblasti bezpečnosti informací, aplikovali bezpečnost informací se zavedenými politikami a postupy organizace. Právě neuvědomění zaměstnanců o svých odpovědnostech v oblasti bezpečnosti informací může vést ke značným škodám pro organizaci.

Samozřejmostí se musí stát i to, že management musí jít příkladem v dodržování politik bezpečnosti informací. I tady se může stát, že nespolehlivý management může způsobit organizaci bezpečnostní riziko a tím i finanční ztrátu.

Management musí zaměstnance motivovat a zajistit vysokou úroveň povědomí o bezpečnosti informací a to celou řadou osvětových aktivit, jako jsou kampaně, školení vydávání brožur, atd. Program zvyšování povědomí musí být pravidelně aktualizován

K oznamování nedodržování politik nebo vznik nových rizik využít metodu Kaizen (může být vytvořen i anonymní informační kanál), která v organizaci funguje v oblasti zlepšování kontroly ve výrobě a bezpečnosti na pracovišti.

Časová náročnost vytvoření programu a seznámení zaměstnanců s ním: **15 hodin**

Povědomí, vzdělávání a školení bezpečnosti informací (A.7.2.2)

Sestavit program školení zvyšování povědomí v oblasti bezpečnosti informací a zaměřit se nejen na faktory „co“ a „jak“, ale také na faktor „proč“. Je důležité, aby zaměstnanci pochopili cíl bezpečnosti informací a možný dopad, pozitivní a negativní, na organizaci jejich vlastního chování. Školení musí probíhat minimálně třikrát za rok. Činnosti pro zvyšování povědomí, vzdělávání a školení musí být vhodné a relevantní pro role, odpovědnosti a schopnosti jednotlivce a samozřejmě být též v souladu s bezpečnostními politikami organizace.

Časová náročnost vypracování programu: **18 hodin**

Časový fond na roční školení: **12 hodin**

Disciplinární řízení (A.7.2.3)

Vypracování formálního disciplinárního procesu, oznámeného všem, pro podniknutí kroků vůči zaměstnancům, kteří se dopustili narušení bezpečnosti informací. Formální disciplinární proces musí zajistit správné a spravedlivé zacházení pro zaměstnance, kteří jsou podezřelí z narušení bezpečnosti informací. Před zahájením procesu je důležité ověření, zda opravdu vzniklo bezpečnostní riziko pro organizaci. Formální disciplinární proces stanoví odstupňované reakce, které berou v úvahu určité faktory provinění (první incident, nevznikla organizaci žádná finanční ztráta, atd.). Disciplinární proces musí být použit jako odstrašující prostředek odrazující zaměstnance z porušení politik a postupů organizace v oblasti bezpečnosti informací.

Časová náročnost zavedení: **10 hodin**

4.2.4 Řízení aktiv (A.8)

Tato bezpečnostní opatření si kladou za cíl identifikovat aktiva organizace definovat odpovědnosti za jejich přiměřenou ochranu.

Seznam aktiv (A.8.1.1)

Organizace by měla identifikovat aktiva relevantní v životním cyklu informací a dokumentovat jejich význam. Životní cyklus informací zahrnuje vytvoření, zpracování, ukládání, přenos, vymazání a zničení. Dokumentace je udržována ve vyhrazených nebo stávajících inventářích. Seznam aktiv je přesný, aktuální, konzistentní a uspořádaný s dalšími inventáři.

Aktualizace seznamu aktiv: **6 hodin**

Vlastnictví aktiv (A.8.1.2)

Jednotlivci, jakož i jiné subjekty jsou odpovědni za správu a řízení aktiva po dobu jeho životnosti, jsou kvalifikováni, aby byli určeni jako vlastníci aktiva.

Vlastník aktiv musí:

- zajistit, že aktiva jsou inventarizována,
- zajistit, že aktiva jsou náležitě klasifikována a chráněna,
- stanovit a pravidelně přezkoumávat omezení přístupu k důležitým aktivům a jejich klasifikaci, s přihlédnutím k doposud platným politikám přístupu,
- Zajistit správný postup zacházení, pokud je aktivum vymazáno nebo zničeno.

Časová náročnost zavedení: **2 hodiny**

Přípustné použití aktiv (A.8.1.3)

Sestavení pravidel pro zacházení s utajovanými informacemi (obchodní tajemství, konstrukční informace automobilek, atd.) a to jak pro zaměstnance tak i uživatele externích stran. Obě strany musí být seznámeny s opatřeními, které vyplynuly z bezpečnosti informací.

Časová náročnost zavedení: **8 hodin**

Vrácení aktiv (A.8.1.4)

Proces ukončení vztahu by měl být zdokumentován na výstupním formuláři, kde zaměstnanci se zadokumentují všechna aktiva, které předal. Ve výpovědní době nasadit zaměstnanci omezený režim, aby bylo zamezeno neoprávněnému kopírování dat a jiným bezpečnostním rizikům. Zaměstnanec je povinen předat i své znalosti, které jsou důležité pro probíhající operace, musí být zdokumentovány a předány organizaci.

Časová náročnost zavedení: **2 hodiny**

Klasifikace informací (A.8.2.1)

Vytvoření stupnice a podle ní klasifikovat informace. Tím se určí jak s kterými informacemi zacházet v návaznosti na bezpečnost informací. Jakým způsobem je nutné tyto oceněné informace chránit. Ideální je vytvoření skupiny informací s podobnými nebo stejnými potřebami ochrany. Individuální posuzování informací by spíše vedlo k přehnané informační bezpečnosti a zbytečné komplikaci při zpracování těchto dat zaměstnanci. Protože informace

může v průběhu roku ztrácet na významu, je nutné na konci roku (nebo i během roku), provést revizi těchto kvalifikací. Informace stačí rozdělit na tři úrovně, a to veřejné, citlivé a utajované.

Časová náročnost zavedení: **15 hodin**

Označování informací (A.8.2.2)

Vypracování postupů pro označování informací, které musí zahrnovat informace a související aktiva a to jak ve fyzické tak i v elektronické podobě. Označení by mělo odpovídat schématu pro klasifikaci. Označení musí být snadno rozpoznatelné. Vynecháním označení dat, která jsou veřejná, se sníží pracovní zátěž. Označování informací a s nimi souvisejících aktiv může mít i negativní dopady. Klasifikovaná aktiva jsou snadněji identifikovatelná, a tudíž cílem krádeží interních pracovníků nebo externích útočníků.

Časová náročnost vypracování postupů: **8 hodin**

Manipulace s aktivy (A.8.2.3)

Vypracování postupu pro zacházení, zpracování, ukládání a předávání informací v souladu s jejich klasifikací. Vzít v úvahu následující položky:

- udržování formálního záznamu o oprávněných příjemcích aktiv,
- omezení přístupu v rámci ochrany na každé úrovni klasifikace,
- ochrana dočasných nebo trvalých kopií informace na úrovni odpovídající ochraně původní informace (nesnižovat úroveň zabezpečení kopie),
- skladování IT aktiv v souladu se specifikacemi výrobce,
- zřetelné označení všech kopií médií pro upoutání pozornosti oprávněného příjemce.

Časová náročnost zavedení: **10 hodin**

Správa výměnných médií (A.8.3.1)

Vypracování postupů pro správu médií a vzít do úvahy následující pokyny:

- obsah jakýchkoliv opakovaně použitelných médií, která mají být z organizace odstraněna, by měl být učiněn neobnovitelným, pokud již tento obsah již organizace nepotřebuje,
- provedení záznamu o odstraněných mediích pro potřeby auditu,
- uložení médií v souladu se specifikacemi výrobce,
- pokud jsou na médiích důležitá data, tak použít v zájmu ochrany kryptografické techniky,
- pokud jsou data uchovávána na médiích, u kterých může dojít časem k degradaci záznamu, provést přenesení dat na nová média,
- vícenásobné kopie cenných dat ukládat na oddělených médiích,
- zvážit registraci výměnného média,
- mechaniky pro výměnná média povolit jen tehdy, je-li pro to důvod vyplývající z činnosti organizace,
- používaná výměnná média by měly mít monitorovaný přenos informací do těchto médií.

Časová náročnost vypracování postupů: **6 hodin**

Likvidace médií (A.8.3.2)

Stanovení formálního postupu pro bezpečnou likvidaci médií a tím zamezit úniku důvěrných informací k neoprávněným osobám. Vzít do úvahy tyto body:

- bezpečné skladování a likvidace médií s důvěrnými daty,
- jednodušší je hromadná likvidace médií, než se snažit oddělit média s citlivými daty,
- zavedení postupů pro identifikaci médií, která zaručuje bezpečnou likvidaci,
- pokud se využije služba likvidace médií u externí organizace, musí to být organizace s odpovídajícími opatřeními a zkušenostmi,
- likvidace médií s citlivými daty by měla být zaznamenaná formou logu pro případ auditu.

Časová náročnost vypracování: **2 hodiny**

Přeprava fyzických médií (A.8.3.3)

Vypracování postupy s následujícími zásadami:

- použití spolehlivé přepravní nebo kurýrní služby,
- seznam autorizovaných kurýrních služeb schválit managementem,
- vypracovat postup pro ověření kurýrů,
- chránit data takovým obalem, aby nedošlo k poškození média,
- uchovávání záznamů formou logů identifikující obsah médií, požitou ochranu, čas předání správci přepravy a čas přijetí na místě určení.

Časová náročnost zavedení: **3 hodiny**

4.2.5 Řízení přístupu (A.9)

Cílem opatření je omezení přístupu k informacím a k vybavení pro zpracování informací neoprávněným osobám. Povolit přístup pouze osobám, které informace zpracovávají a mají k tomu oprávnění od svých nadřízených a ti mají svolení od managementu organizace.

Politika řízení přístupu (A.9.1.1)

Vlastníci aktiv musí stanovit vhodná pravidla řízení přístupu, přístupová práva a omezení pro specifické uživatelské role ve vztahu k jejich aktivům, s přesností a přísností opatření související rizika v oblasti bezpečnosti informací. Z toho plyne, že uživatel by měl mít jen přístupy a práva k informacím, které nezbytně potřebuje pro svoji pracovní činnost, nebo dočasný přístup nebo právo pro vykonání úkolu, který mu byl svěřen. Může se uplatnit pravidlo principu, jenž zakazuje vše, co není výslovně povoleno.

Časová náročnost vypracování: **10 hodin**

Přezkoumání přístupových práv uživatelů (A.9.2.5)

Proces by měl zahrnovat:

- pokud uživatelé sdílejí autentizační informace v rámci skupiny, měl by být tento podepsaný závazek o mlčenlivosti mimo skupinu zahrnut do pracovní smlouvy,
- při první autentizaci dát uživateli ihned možnost změny těchto údajů,

- ověřit si stanoveným postupem identitu uživatele před změnou autentizačních údajů,
- předání autentizačních údajů bezpečnou formou uživateli,
- uživatel by měl potvrdit příjem autentizační informace,
- dočasné autentizační informace musí být neodhalitelné a jedinečné,
- výchozí autentizační informace od výrobce software by měly být po instalaci změněny.

Časová náročnost vypracování procesu: **5 hodin**

Používání tajných autentizačních informací (A.9.3.1)

Všichni uživatelé musí být poučeni:

- udržovat v tajnosti své autentizační údaje a neprozradit je jiné osobě,
- neuchovávat své autentizační údaje na papíře, v souboru nebo v přenosných zařízeních,
- okamžitě změnili své autentizační údaje, pokud mají podezření na prozrazení,
- zvolili kvalitní heslo s dostatečnou délkou a tím zamezili možnému prozrazení,
- nesdíleli své heslo s ostatními uživateli,
- zajistili řádnou ochranu hesel, pokud jsou používána v automatických postupech,
- nepožívali stejnou autentizační informaci pro další přístupy (např. do banky).

Časová náročnost vypracování poučení: **2 hodiny**

4.2.6 Kryptografie (A.10)

Cílem kryptografických opatření je zajistit správné a efektivní využití kryptografie na ochranu důvěrnosti, autenticity a také integrity informací.

Politika pro použití kryptografických opatření (A10.1.1)

Při vytváření politiky v oblasti kryptografie musí být zváženo:

- manažerský přístup ve vztahu k používání kryptografických opatření v rámci celé organizace,
- na základě posouzení rizik by měl být zvolen kvalitní šifrovací algoritmus,

- použití šifrování pro ochranu informací na mobilních zařízeních nebo výměnných médiích,
- přístup ke správě klíčů, včetně metod zabývající se jejich ochranou,
- stanovit role kdo je odpovědný za implementaci a kdo za správu klíčů,
- normy, které budou převzaty pro účinnou implementaci,
- dopad na kontrolu malware na zašifrovaném mobilním zařízení nebo médii

Časová náročnost vypracování: **6 hodin**

Správa klíčů (A.10.1.2)

Tato politika zahrnuje požadavky na správu kryptografických klíčů během celého jejich životního cyklu, včetně generování, ukládání, archivace, znovuzískání, distribuce, vyřazení a zničení klíče. Kryptografické algoritmy, délky klíčů a postupy použití by měly být vybrány v souladu s doporučenými postupy. Všechny kryptografické klíče musí být chráněny před modifikací a ztrátou. Navíc tajné a soukromé klíče potřebují ochranu proti neoprávněnému použití, jakož i zveřejnění. Zařízení sloužící ke generování, ukládání a archivaci klíčů musí být fyzicky chráněno.

Časová náročnost vypracování postupů správy: **6 hodin**

4.2.7 Bezpečnost provozu (A.12)

Cílem těchto politik je zajištění správného a bezpečného provozování vybavení pro zpracování dat.

Dokumentace provozních postupů (A.12.1.1)

Provozní postupy musí být řádně dokumentovány a být k dispozici všem uživatelům, kteří je potřebují. Pro provozní činnosti spojené s vybavením pro zpracování informací a s komunikačním vybavením by měly být připraveny dokumentované postupy, jako jsou postupy pro ovládání počítače, zálohování, monitorování, údržba zařízení, zacházení s médii, správa počítačové místnosti, zacházení s poštou, nakládání s chybami, instalace a konfigurace systémů a bezpečnost práce.

Časová náročnost zavedení: **4 hodiny**

Řízení změn (A.12.1.2)

Jedná se o zdokumentování kompletního změnového řízení v podnikových procesech, vybaveních pro zpracování informací a systémech, které mají vliv na bezpečnost informací. Tyto změny musí být řízeny a kontrolovány. Důležité je tyto změny předem plánovat a testovat. Po otestování provést zkušební provoz a až potom přejít do ostrého provozu. Nedostatečná kontrola změn vybavení pro zpracování informací a systémů je často příčinou systémových a bezpečnostních selhání. Změny v provozním prostředí, zejména při převádění systému z fáze vývoje do provozní fáze, mohou mít vliv na spolehlivost aplikací.

Časová náročnost zavedení: **6 hodin**

Řízení kapacit (A.12.1.3)

Toto opatření se v první řadě týká sledování a monitorování kapacit (diskového prostoru), které jsou přiděleny aplikacím a řídicím systémům. Opatření počítá s nasazením monitorovacího zařízení, které upozorní včasným varováním na nedostatečné kapacity. Absence těchto nástrojů může vést ke kolapsu některých důležitých systémů a jejich nedostupnosti. Toto opatření se samozřejmě týká i kapacit lidských zdrojů, kanceláří a jejich vybavení.

Časová náročnost vypracování**: 2 hodiny**

Instalace software na provozních systémech (A12.5.1)

Zavedení postupů pro řízení a kontrolu instalace software na provozních systémech. Dodaný software používaný v provozních systémech musí být udržován na úrovni podporované dodavatelem. Při ukončení podpory software ze strany dodavatele, musí organizace zvážit nákup nové podporované verze software. Software záplaty musí být použity, pokud se tím odstraní slabá místa v oblasti bezpečnosti informací.

Časová náročnost vypracování: **2 hodiny**

4.2.8 Bezpečnost komunikací (A13)

Zde je důležité zajistit ochranu informací v sítích a podpůrném síťovém vybavení pro zpracování informací. Organizace již má monitoring a kontrolu sítě v sytému NAGIOS.

NAGIOS je software nástroj, který umožňuje monitorovat počítačovou síť a v ní poskytované služby a v případě jakéhokoliv výskytu problému okamžitě informovat administrátora, který na základě vyhodnoceného incidentu může rychle zasáhnout.

Politiky a postupy při přenosu informací (A.13.2.1)

Vypracování pokynů, postupů a opatření navržených k ochraně přenosu informací prostřednictvím všech druhů komunikačních zařízení. Tyto postupy musí chránit přenášené informace a to zejména před odposloucháváním, kopírováním, pozměněním, chybným směrováním a zničením. Organizace by měla zvážit tyto opatření:

- detekce a ochrana před malwarem, při elektronické komunikaci,
- přeposílání dat na soukromé maily,
- přípustné použití komunikačních zařízení,
- použití kryptografických technik,
- zákaz nechávání důvěrných zpráv na záznamníku telefonu,
- posílání citlivých materiálů ve formě přílohy,
- nakládání s podnikovou korespondencí,
- odpovědnosti zaměstnanců nekompromitovat a nepomlouvat organizaci, atd.

Časová náročnost zavedení: **8 hodin**

Dohody o přenosu informací (A.13.2.2)

Musí být stanoveny a udržovány politiky, postupy a normy pro ochranu informací a fyzických médií během přepravy. Dohody o přenosu informací by měly zahrnovat:

- odpovědnost managementu za řízení a oznamování přenosu,
- postupy k zajištění dohledatelnosti a nepopiratelnosti,
- normy pro balení a přenos,
- zásady identifikace kurýra,
- odpovědnosti a povinnosti v případě incidentů bezpečnosti informací,
- technické normy pro záznam a čtení informací a software, atd.

Smlouvy mohou být v elektronické podobě nebo papírové podobě a mohou mít podobu formálních smluv.

Časová náročnost vypracování: **3 hodiny**

Elektronické předávání zpráv (A.13.2.3)

V tomto opatření je velmi důležité, aby elektronicky předávané zprávy byly přiměřeně chráněny. Důležité je zvážit tyto aspekty bezpečnosti informací:

- ochrana zpráv před neoprávněným přístupem, změnou nebo odmítnutím služby a to úměrně ke klasifikačním schématu přijatému organizací,
- zajištění správného adresování a přepravy zprávy,
- spolehlivost a dostupnost služby,
- požadavky na elektronické podpisy,
- **získání předchozího svolení k užívání externích veřejných služeb** jako je možnost zasílání zpráv prostřednictvím **služby „instant messaging", sociální sítě nebo sdílení souborů, atd.**

Časová náročnost zavedení: **2 hodiny**

4.2.9 Řízení incidentů bezpečnosti informací

Cílem je zajištění důsledného a efektivního přístupu k řízení incidentů bezpečnosti informací, včetně komunikace ohledně bezpečnostních událostí a slabých míst.

Odpovědnosti a postupy (A.16.1.1)

Zde je důležité vypracovat tyto postupy:

- pro plánování a přípravu odezvy na incidenty,
- pro monitorování, detekci a analýzu a podávání zpráv o incidentech spadajících do bezpečnosti informací,
- pro zaznamenání a řízení incidentů (formou logů),
- pro zacházení s forenzními důkazy,
- pro posuzování a rozhodování o incidentech a posuzování slabých míst v oblasti bezpečnosti informací.

Důležité je stanovení kontaktního místa pro hlášení incidentů. Udržovat kontakt s experty zabývající se incidenty a jejich eliminací v oblasti bezpečnosti informací.

Časová náročnost zavedení: **4 hodiny**

Podávání zpráv o událostech bezpečnosti informací (A16.1.2)

Cílem je dosáhnutí rychlého hlášení událostí bezpečnosti informací ze strany všech zaměstnanců a smluvních stran. Všechna tato hlášení směřovat do jednoho kontaktního místa podle postupu, s kterým musí být seznámeni. Závada nebo nestandardní chování systému, může být indikací o možném útoku na bezpečnost systému.

Časová náročnost zavedení: **2 hodiny**

Podávání zpráv o slabých místech bezpečnosti informací (A.16.1.3)

Všichni zaměstnanci a smluvní strany musí hlásit všechny slabá místa (a to i domnělá) bezpečnosti informací. Podávání zpráv by mělo být rychlé, snadné a kontaktní místo by mělo být snadno přístupné a co nejvíce dostupné. Zaměstnanci by se neměli pokoušet sami testovat slabá místa, ale přenechat testování osobám k tomu delegovaným.

Časová náročnost zavedení: **2 hodiny**

Posuzování a rozhodování o událostech bezpečností informací (A.16.1.4)

Kontaktní místo musí posoudit bezpečnostní událost a rozhodnout, zda se jedná o incident a s jakým dopadem na organizaci. Všechny výsledky řešení událostí se musí podrobně zaznamenat za účelem budoucí reference a ověření.

Časová náročnost zavedení: **6 hodin**

Odezva na incidenty bezpečnosti informací (A.16.1.5)

Vypracování dokumentovaných postupů jak reagovat na incidenty bezpečnosti informací. Kontaktní místo musí ihned reagovat a odezva by měla zahrnovat:

- shromáždění důkazů ihned po nahlášení incidentu,
- provedení forenzní analýzy bezpečnosti informací
- eskalace je-li vyžádána,
- řádný záznam formou logu všech činností pro pozdější analýzu,

- oznámení existence incidentu dalším externím osobám nebo organizacím splňujícím požadavek „potřeba znát“.

Časová náročnost zavedení: **2 hodiny**

Ponaučení z incidentů bezpečnosti informací (A.16.1.6)

Pro prevenci incidentů bezpečnosti informací je důležité použít všechny znalosti z řešení a analýzy předchozích incidentů. Tyto znalosti pomáhají k identifikaci opakujících se incidentů a incidentů s velkým dopadem. Události, které předcházely incidentům bezpečnosti informací a jsou zdokumentovány, mohou posloužit jako podklad pro školení zaměstnanců.

Časová náročnost zavedení: **2 hodiny**

Shromažďování důkazů (A.16.1.7)

Organizace musí definovat a aplikovat postupy pro identifikaci, shromažďování, získávání a uchovávání informací, které mohou sloužit jako důkaz. Postupy by měly brát v úvahu bezpečnost důkazů a personálu. Při prvním zjištění bezpečnosti informací nemusí být zřejmé, zda incident se bude řešit soudní cestou. Potom je důležité ochránit důkazy pro budoucí soudní spor.

Časová náročnost vypracování: **4 hodiny**

4.2.10 Soulad s požadavky (A.18)

Cílem je zamezit porušení právních, zákonných, předpisových nebo smluvních povinností, které souvisejí s bezpečností informací a jakýchkoliv požadavků bezpečnosti.

Identifikace příslušné legislativy a smluvních požadavků (A.18.1.1)

Musí být splněny všechny zákonné, předpisové, smluvní požadavky příslušné legislativy. Potom organizace musí vše dokumentovat a udržovat v aktuálním stavu pro každý informační systém. Pokud organizace podniká v dalších zemích, musí manažeři zvážit soulad všech příslušných zemí.

Časová náročnost zavedení: **3 hodiny**

Práva k duševního vlastnictví (A.18.1.2)

Vypracovat politiku kontroly neoprávněného zneužití duševního vlastnictví. To zahrnuje používání legálního software. Nepřekračování licencí software, který nemá dokonalé hlídání licenční politiky. Prokázat se při jakékoliv kontrole ze strany certifikovaného kontrolního orgánu, že má organizace v pořádku všechny licence (a doklady k nim) a má účinné monitorování na odhalení nelegálního software. Provést vždy přezkoumání software, který je zdarma, zda je možné jej bezplatně využívat i v komerční sféře.

Časová náročnost vypracování: **4 hodiny**

Ochrana záznamů (A.18.1.3)

Všechny důležité záznamy roztřídit podle typů a podle zákonné délky jejich uchování. Vzít v úvahu na jakém médiu jsou uchovány a zaručit včasné opětovné uložení záznamů na novější média, aby byla zaručena čitelnost i po letech skladování. Vzhledem k tomu že organizace má stanovenou životnost hardware ve firmě na 4-5 let nemá s tímto krokem problém. Při skladování médií musí být dodrženy postupy od výrobce. Organizace uchovává tyto záznamy na HDD a datových páskách a díky stanovené životnosti všech hardware zařízeních nedochází v průběhu uchovávání k žádné ztrátě dat, která by byla způsobena nekompatibilními technologiemi.

Časová náročnost zavedení: **2 hodiny**

Regulace kryptografických opatření (A.18.1.5)

Vypracování postupu pro regulaci kryptografických opatření, aby byla v souladu se všemi příslušnými dohodami, legislativou a předpisy. Jedná se hlavně o zneužití kryptografie ke krytí trestní činnosti nebo terorismu, atd. Použití by se mělo omezovat pouze na firemní informace a nerozšiřovat jeho použití k jiným účelům, které by přesahovaly hranici jurisdikce.

Časová náročnost zavedení: **4 hodiny**

4.2.11 Přezkoumání bezpečnosti informací (A.18.2)

Cílem je zajisti, že bezpečnost informací je implementována a provozována v souladu (shodě) s politikami a postupy organizace. Protože organizace chce přistoupit k certifikaci a získat certifikát je nutné splnit i následující opatření.

Nezávislé přezkoumání bezpečnosti informací (A18.2.1)

Management organizace musí iniciovat nezávislé přezkoumání. Toto přezkoumání by mělo být provedeno nezávislým orgánem (auditor interní, externí firma, nezávislý manažer). Pokud audit bezpečnosti informací shledá závažné neshody, musí managementem organizace zvážit nápravná opatření. Audity přezkoumání bezpečnosti informací by se měly naplánovat s půlroční periodicitou nebo při výrazných změnách.

Časová náročnost vypracování harmonogramu nezávislých auditů: **2 hodiny**

Shoda s bezpečnostními politikami a normami (A.18.2.2)

Vedoucí pracovníci by měli pravidelně přezkoumávat soulad se zpracováním informací a postupy, v rámci své působnosti se všemi požadavky na bezpečnost. Taky by měli identifikovat, z jaké příčiny vznikl nesoulad, a dosáhnou nápravnými kroky opět souladu. Potom ještě přezkoumat efektivitu nápravného opatření.

Časová náročnost zavedení: **4 hodiny**

Přezkoumání technické shody (A.18.2.3)

Informační systémy, které organizace vlastní, musí být periodicky přezkoumávány, zda jsou stále v souladu s politikami a normami bezpečnosti informací organizace. Toto přezkoumání musí být zdokumentováno a výsledky předány vrcholovému managementu organizace. Ta musí ze závěru vyvodit opatření, pokud byla narušena bezpečnost informací.

Časová náročnost zavedení: **2 hodiny**

Časový fond pro kontroly: 10 hodin / rok

4.3 Zavedení servisních služeb podle metodiky ITIL

Jak již bylo zmíněno v analýze, je velkým problémem v organizaci dosavadní způsob fungování servisních služeb oddělení IS/IT. Zavedení všech politik a opatření v rámci bezpečnosti informací vše nekončí. Pokud v organizaci není správně fungující oddělení IS/IT, na které se dá spolehnout a je plně funkční i po servisní stránce. Tady dostává své místo metodika ITIL, která právě funkčnost IS/IT rozebírá z hlediska servisních služeb tohoto oddělení. V tomto případě je důležité si uvědomit několik věcí:

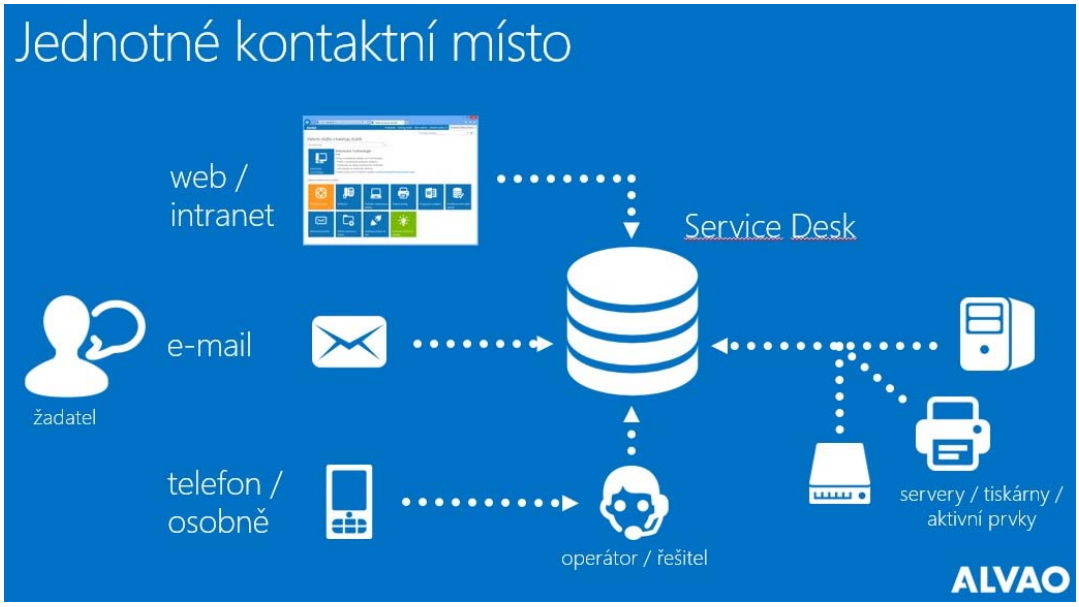
- změnit dosavadní stav funkčnosti IS/IT a vytvořit vztah dodavatel-odběratel,
- definovat oblasti dodávaných služeb,
- nastavit si procesy, workflow a měřitelné parametry pro vyhodnocení funkčnosti procesu,
- schopnost IS/IT plánovat si svou činnost,
- dodávat služby v dohodnutém čase a kvalitě.

V první fázi je důležitým krokem definice IT služeb potřebných pro fungování jednotlivých oddělení, ale i služby spadající do správy IT. V druhé fázi je dalším krokem definice SLA (dohoda o úrovni poskytovaných služeb) pro jednotlivé služby:

- jak je služba důležitá
- jaký je čas reakce a vyřešení
- jaká je cena služby
- nutná spolupráce jednotlivých útvarů na definicích SLA

Další fází je naplnění katalogu služeb do správy servisních požadavků (firma ALVAO). Posledním krokem je spuštění celé správy servisních požadavků přes podnikový Intranet. Naznačení funkčnosti je na následujícím obrázku poskytnutém od firmy ALVAO. Na obrázku je vidět, že je stanoveno jenom jedno kontaktní místo a v případě nefunkčnosti Intranetu je možné sdělit incident jinou komunikační cestou. Prioritní cestou sdělení incidentu ale stále zůstává podnikový Intranet, který bude uživatelům sloužit i k tomu, že budou moci sledovat, jak se jejich servisní požadavek plní, nebo v jaké fázi rozpracovanosti se nachází.

Pro IS/IT vznikne nástroj, kterým si oddělení lépe naplánuje plnění servisních požadavků a nebude se dostávat do pracovního přetlaku a tím i do špatného světla vůči vrcholovému managementu.



Obrázek 16: Princip servisní služby [ALVAO]

Časová náročnost zavedení servisních služeb: **60 hodin**

4.4 Postup při zavádění bezpečnostních opatření

Jak již bylo zmíněno v předcházejících kapitolách 4.2 a 4.3 chce organizace zavést popsaná bezpečnostní opatření. V kapitole 4.3 se jedná o kompletní řízení servisních služeb oddělení IS/IT, které je koncipováno podle metodiky ITIL. Společnost chce provést kompletní certifikaci ISMS a proto jako první krok k tomuto cíli vidí zavedení ISMS podle normy ČSN ISO/IEC 27001.

Před začátkem zavádění ISMS je důležité všechny zaměstnance proškolit a seznámit je se záměrem společnosti dodržovat a neustále prohlubovat politiku bezpečnosti informací podle dokumentu vypracovaného podle opatření s označením A.5.1.1.

Postup zavádění je stanoven podle matice rizik od nejvyšších až po nejnižší rizika. Vzhledem k tomu, že se ve společnosti vyskytují pouze střední rizika, bude společnost zavádět od těchto rizik. Důležitým bodem bude taky zavedení opatření, kterým se zavede šifrování přenosných zařízení.

V tabulce 7 jsou přesně zapsány politiky a jejich opatření, které je nutné zavést, aby plně fungovaly ve společnosti. I když si tyto politiky vezme za své vrcholový management společnosti, je velmi důležité, aby se s těmito politikami ztotožnili i všichni zaměstnanci. Všichni si musí uvědomit, že zavedením a fungováním tento proces nekončí, ale začíná dlouhá cesta monitorování, vyhodnocování, zlepšování a dalšího zavádění opatření podle Demingova modelu.

Celkový součet hodin, který je potřeba pro zavedení ISMS podle normy ČSN ISO/IEC 27001 je vyčíslen na konci tabulky 7. Jedná se o 286 hodin zavádění opatření a politik ISMS. **Na školení** je stanoveno 12 hodin, které jsou brány jako minimum, ale bude počítáno s dvanácti až padesát hod školení. **Pro monitoring a přezkoumávání politik** je počítáno s 10 hod/rok, ale podle potřeb to může být až 70 hod/rok. Při plánování finančního rozpočtu na každý rok se bude počítat s maximálním počtem hodin pro tyto činnosti. To bude činit **každý rok 120 hodin.**

4.5 Ekonomické zhodnocení zavedení ISMS a časový plán

V tabulce 8 je celkový počet hodin na zavedení ISMS stanoven na 286 hodin a roční náročnost na udržování těchto opatření je stanovena na 120 hodin. Vrcholový management určil dvě zodpovědné osoby, které se budou na zavádění podílet a budou podávat po celou dobu své činnosti pravidelné reporty vrcholovému managementu společnosti písemnou formou.

Každá z těchto osob bude mít k dispozici pro zavádění časový 25 hodin týdně, z čeho vyplývá celkem 50 hodin týdně pro zavádění ISMS. Ekonomický ředitel společnosti stanovil hodinovou mzdu těchto osob na 500,- Kč/hod. Při 286 hodinách zavádění bude tato práce ohodnocena částkou **143 000,- Kč bez DPH**. Celková částka za zavedení funkčního servisního střediska pro IS/IT ve společnosti od firmy ALVAO bude činit **334 538,- Kč bez DPH**. **Zakoupení šifrovacího software** od firmy Symantec je ohodnoceno částkou **25 000,-Kč** bez DPH. To je výčet jednorázových nákladů na zavedení ISMS. Na údržbu celého ISMS bude potřeba každý rok podle stanovené mzdy 500,- Kč/hod a časovému fondu 120 hod vyčlenit částku **60 000,-Kč/rok**. Celková jednorázová částka bude činit **502 538,- Kč bez DPH**.

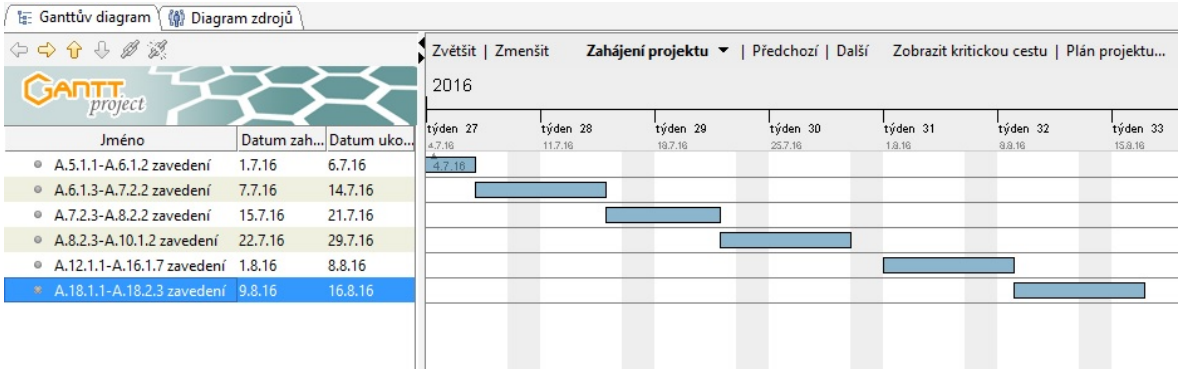
V následující tabulce 8 jsou shrnuty všechny náklady, které představuje implementace ISMS ve společnosti.

Tabula 8 – Náklady společnosti na zavedení, udržování a neustálé zlepšování ISMS

	Jednorázové náklady	Každoroční náklady
Zavedení / udržování politik bezpečnosti	**143 000,-Kč**	**60 000,-Kč**
Zakoupení šifrovacího software Symantec	**25 000,-Kč**	**0,-Kč**
Zavedení servisního střediska IT útvaru	**334 538,-Kč**	**0,-Kč**
Celkové náklady	**502 538,-Kč**	**60 000,-Kč**
Poměr nákladů k ročnímu obratu	**0,20%**	**0,016%**
Pozn. Všechny uvedené ceny jsou bez DPH		

Celkový čas na zavedení celého ISMS je rozvržen do šesti týdnů. V následující tabulce 10 je zobrazen časový plán zavedení pomocí Ganttova diagramu.

Tabulka 9 – Časový plán zavedení ISMS ve společnosti



ZÁVĚR

Cílem této práce bylo vypracovat v dané společnosti podrobný postup zavedení systému řízení bezpečnosti ISMS podle normy ČSN ISO/IEC 27001. Vzhledem k tomu, že jsem nechtěl opomenout i metodiku ITIL, protože se silně tato metodika sbližuje s metodikou COBIT, využil jsem toho, že společnost již plně uvažovala o zavedení servisních služeb IT útvaru. Software, který je přesně podle vzoru metodiky ITIL v rámci servisních služeb, je od dodavatelské firmy ALVAO. Zavedením by se měl kompenzovat přetlak servisních požadavků a tím dojít k tomu, že začne útvar opravdu servisní požadavky vykrývat plánovaně a s předstihem. Tím poroste i efektivita práce v tomto útvaru a s tím ruku v ruce by měla stoupnout produktivita plnění servisních požadavků.

Zavedením ISMS bude mít vedení společnosti i majitelé větší jistotu v ochraně svého majetku, know - how, obchodního a výrobního tajemství. Vzhledem k tomu, že společnost má velký progres jak po obchodní stránce, tak po stránce nových technologií, bude bezpečnost ISMS pro ni velkým přínosem nejen po zavedení, ale také do budoucna. Společnost chce v brzké době taky dosáhnout certifikace ISMS a tím dát svým obchodním partnerům signál, že je silná nejenom v oblasti kvality výroby, životního prostředí, výrobních procesů (certifikace EN ISO 9001:2008, EN ISO 14001:2004, ISO/TS 16949:2009), ale i v oblasti systému řízení bezpečnosti informací. Obchodní partneři tak budou mít jistotu, že i jejich dat jsou v bezpečí.

Je pravdou, že určitě neexistuje naprosto ideální bezpečnost informací a technologií. To by muselo být ve sterilním prostředí s osobami, které by byly plně tomuto programu loajální. I když se množí různé útoky na podnikové sítě zvenčí, pořád je největším nebezpečím zaměstnanec firmy a tedy útok zevnitř společnosti. Díky Internetu jsou mladým lidem představeny některé hackerské praktiky a možnosti jak zaútočit uvnitř jakékoliv firmy. Proto získání loajality zaměstnanců by mělo být prvořadým úkolem vrcholového managementu, který by měl jít všem příkladem. Právě i zavedení ISMS je dalším krokem jak získat z hlediska bezpečnosti informací přehled o dění ve firmě a o kontrole komunikace i toku dat.

Vzhledem k tomu, že informační technologie jdou ve vývoji stále vpřed, tak se tomu musí neustále přizpůsobovat i systém bezpečnosti informací. A tady vidím sílu Demingova cyklu, neustálého zlepšování systému řízení bezpečnosti informací, ale i kvality, životního prostředí, atd.

SEZNAM POUŽITÉ LITERATURY

[1] MATES, Pavel a Vladimír SMEJKAL. *E-government v České republice: právní a technologické aspekty*. 2., podstatně přeprac. a rozš. vyd., V nakl. Leges vyd. 1. Praha: Leges, 2012, 464 s. Teoretik. ISBN 978-80-87576-36-6.

[2] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 4., aktualiz. a rozš. vyd. Praha: Grada, 2013, 483 s. Expert (Grada). ISBN 978-80-247-4644-9.

[3] BUCKSTEEG, Martin. *ITIL 2011*. 1. vyd. Brno: Computer Press, 2012, 216 s. ISBN 978-80-251-3732-1.

[4] LUKÁČ, Ľubomír. *IT management: jak na úspěšnou kariéru*. Vyd. 1. Brno: Computer Press, 2011, 208 s. ISBN 978-80-251-3378-1.

[5] SELECKÝ, Matúš. *Penetrační testy a exploitace*. 1. vyd. Brno: Computer Press, 2012, 303 s. ISBN 978-80-251-3752-9.

[6] POŽÁR, Josef. *Informační bezpečnost*. 1.vyd. Plzeň: Aleš Čeněk, 2005. ISBN 978-80-86898-38-5.

[7] DOUCEK, Petr. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM*. 2., přeprac. vyd. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.

[8] *ISO/IEC 27001*. Druhé vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

[9] *ČSN ISO/IEC 27002*. Druhé vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

[10] *Sbírka zákonů Česká republika: Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).*, 2014. Břeclav: Moraviapress. ISSN 12111244.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ISMS	Information Security Management System
ISO	International Organization of Standardization
IS	Informační systémy
IT	Informační systém
ICT	Information and Communication Technologies
GPO	Group Policy Object
CISCO	Největší počítačová firma na poli síťových prvků
CLOUD	Computing funguje na principu sdílení hardwarovýcha softwarových prostředků prostřednictvím sítě
HDD	Hard Disc Drive
USB	Universal Seriál Bus
MERAKI	Firma zabývající se výrobou špičkových aktivních prvků v oblasti počítačových sítí. Dnes již pod firmou CISCO (koupilo ji v roce 2012 za 1,2 miliardy $)
SLA	Service-level agreement

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: HISTORICKÝ VÝVOJ NOREM ŘÍZENÍ BEZPEČNOSTI INFORMACÍ [7]

Rok	Slovník	Požadavky	Soubor postupů	Implementace	Měření	Řízení rizik	Certifikace	Audit
1995			BS 7799					
1996	ISO/IEC TR 13335-1							
1997	ISO/IEC TR 13335-2							
1998						ISO/IEC TR 13335-3	c:cure	
1999		BS 7799-2	BS 7799-1				EA7/03	
2000			ISO/IEC 17799			ISO/IEC TR 13335-4		
2001						ISO/IEC TR 13335-5		
2002		BS 7799-2 v2						
2004	ISO/IEC 13335-1							
2005		ISO/IEC 27001	ISO/IEC 17799 v2					
2006						BS 7799-3		
2007			ISO/IEC 27002				ISO/IEC 27006	
2008						ISO/IEC 27005		
2009	ISO/IEC 27000				ISO/IEC 27004			
2010				ISO/IEC 27003				
2011						ISO/IEC 27005 v2		ISO/IEC 27007
2012		ISO/IEC 27001 v2	ISO/IEC 27002 v2					ISO/IEC TR 27008
2013	ISO/IEC 27000 v2						ISO/IEC 27006 v2	

PŘÍLOHA P II: MATICE ZRANITELNOSTI

Popis aktiva		Databáze ABAS	Databáze Datapoint	Databáze Teamcenter	Databáze RQM	Databáze Forge	Databáze FK	Databáze BNS	Databáze akcion	Data File-Server2	Databáze SAFEQ	Účetní doklady/papírové	Personální data	Data FORGE	Programy CNC	Měření 3D	Technická data - lisy	technická data - ohřevy	Autentizační údaje	Počítače Embeded	Počítače Office	Pracovní stanice	Průmyslové PC	Servery	Switche	přístupové čtečky karet	Kamerové DVR	VoIP ústředna	Kamery	Přenosná zařízení	Router	Tiskárny	Kabeláž	Síťová infrastruktura	Přenosná média	Operační systém	Kancelářské programy	ABB studio	Step -Simatic	Účetní programy	Elektronická pošta	Office 365	Webové stránky	Připojení k internetu
	Hodnota aktiva (A)	5	5	5	4	4	5	5	4	4	4	4	5	4	5	5	3	3	4	4	4	3	4	5	5	3	4	5	3	4	3	5	3	4	4	4	3	5	5	4	3	5	3	4
Popis hrozby	Pravděpodobnost hrozby (T)																																											
Útok z vnějšku	2	1	1	1	1	1	1	1	1	1	1		1	1	2	2	2	2	2					1	1	1	1	2	1	4	2	2				2	1	1	1	1	1	1	2	
Neoprávněný přístup do prostor firmy	1											2				2										1			1	1		1												
Požár	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Poškození vodou	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Úder bleskem	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Krádež zařízení	4																			2	4	4	2			1			1	4					3									
Krádež dokumentů	3											1				1																												
Porucha hardwaru	3	1	1	1	1	1	1	1	1	1	1		1	1	1	1	1	1		1	1	1	1	1	1	1	1	1	1	2	1	2				1	2	2	1	2	2	2	1	2
Poškození hardware/neúmyslné	2																			1	1	1	1	1	1	1	1	1	1	1	1	1												
Poškození hardware /úmyslné	1																																											
Poškození LAN/neúmyslné	2																																											
Poškození LAN//úmyslné	1																																				1	1	1	1	1	2	2	2
Počítačový virus	2																				1	1								3					3							2	2	
Výpadek internetu	2																																								2	2	2	
Výpadek pevné linky	2																																											
Výpadek elektrického proudu	3	1	1	1	1	1	1	1	1	1	1			1	1	1	1	1		2	2	2	2	2	2	2	1	2	1	1		2					1	2	1	2	3	3	1	
Prozrazení autentizačních údajů	3																			2	2	2	2							2		2									2	2	2	
Chybné zaslání citlivých dat	3																																							2	1	1	1	
Porušení mlčenlivosti zaměstnance	3												3	2	2																									2	2	2		
Nedostupnost webových stránek	3																											2													3	3	3	
Poškození zálohovacího média	2	1	1	1	1	1	1	1	1	1	1		1	1	1	1																												
Útok /SPAM	2																																											
Útok z vnějšku na Wifi	2																																											
Výpadek termokamerového systému	2																																											
Výpadek kamerového systému	2																1	1																										
Modifikace záloh	2																																											
Ztráta záloh	1																																											
Modifikace databází	1																																											
Nefunkčnost přístupového systému	1																																											
Útok z vnitřku organizace	3													2	2	2	2	2	2	3	3	3	3	1						3		2			2									
Neúmyslná modifikace dokumentů	2																																											
Zneužití přenosného zařízení pro špionáž	4												2	2	2	2	2	2	2	2	2	2	2							3		2			2									

PŘÍLOHA P III: MATICE RIZIK

RIZIKO (R)	Popis aktiva	Databáze ABAS	Databáze Datapoint	Databáze Teamcenter	Databáze RQM	Databáze Forge	Databáze FK	Databáze BNS	Databáze aktion	Data File-Server2	Databáze SAFEQ	Účetní doklady/papírově	Personální data	Data FORCH	Programy CNC	Měření 3D	Technická data - lisy	technická data - ohřevy	Autentizační údaje	Počítače Embeded	Počítače Office	Pracovní stanice	Průmyslové PC	Servery	Switche	přístupové čtečky karet	Kamerové DVR	VoIP ústředna	Kamery	Přenosná zařízení	Router	Tiskárny	Kabeláž	Síťová infrastruktura	Přenosná média	Operační systém	Kancelářské programy	ABB studio	Step -Simatic	Účetní programy	Elektronická pošta	Office 365	Webové stránky	Připojení k internetu
	Hodnota aktiva (A)	5	5	5	4	4	5	5	4	4	4	4	5	4	5	5	3	3	4	4	4	3	4	5	5	3	4	5	3	4	3	5	3	4	4	4	3	5	5	4	3	5	3	4
Popis hrozby	**Pravděpodobnost hrozby (T)**																																										
Útok z vnějšku	2	10	10	10	8	8	10	10	8	8	8		10	8	20	20	20	20	20					10	10	6	8	20	6	32	12	20				16	6	10	10	8	6	10	12	
Neoprávněný přístup do prostor firmy	1											8				10										3			3	4		5												
Požár	1	5	5	5	4	4	5	5	4	4	4	4	5	4	5	5	3	3	4	4	4	3	4	5	5	3	4	5	3	4	3	5	3	4	4	4	3	5	5	4	3	5	3	4
Poškození vodou	1	5	5	5	4	4	5	5	4	4	4	4	5	4	5	5	3	3	4	4	4	3	4	5	5	3	4	5	3	4	3	5	3	4	4	4	3	5	5	4	3	5	3	4
Úder bleskem	1	5	5	5	4	4	5	5	4	4	4	4	5	4	5	5	3	3	4	4	4	3	4	5	5	3	4	5	3	4	3	5	3	4	4	4	3	5	5	4	3	5	3	4
Krádež zařízení	4																			32	64	48	32			12			12	64					48									
Krádež dokumentů	3											12				15																												
Porucha hardwaru	3	15	15	15	12	12	15	15	12	12	12		15	12	15	15	9	9		12	12	9	12	15	15	9	12	15	9	24	9	30				12	18	30	15	24	18	30	9	32
Poškození hardware/neúmyslné	2																			8	8	6	8	10	10	6	8	10	6	8	6	10												
Poškození hardware /úmyslné	1																																										
Poškození LAN/neúmyslné	2																																										
Poškození LAN//úmyslné	1																																		3	5	5	4	3	10	6	8
Počítačový virus	2																				4	3								12				12							10	6	
Výpadek internetu	2																																							12	20	12	
Výpadek pevné linky	2																																										
Výpadek elektrického proudu	3	15	15	15	12	12	15	15	12	12	12			12	15	15	9	9		12	12	9	12	15	15	18	12	30	9	12		30				9	30	15	24	27	45	9	
Prozrazení autentizačních údajů	3																			24	24	18	24							24		30									18	30	18	
Chybné zaslání citlivých dat	3																																						24	9	15	9	
Porušení mlčenlivosti zaměstnance	3												45	24	30																								24	18	30			
Nedostupnost webových stránek	3																											30												27	45	27	
Poškození zálohovaciho média	2	10	10	10	8	8	10	10	8	8	8		10	8	10	10																												
Útok /SPAM	2																																										
Útok z vnějšku na Wifi	2																																										
Výpadek termokamerového systému	2																6	6																										
Výpadek kamerového systému	2																																										
Modifikace záloh	2																																										
Ztráta záloh	1																																										
Modifikace databází	1																																										
Nefunkčnost přístupového systému	1																																										
Útok z vnitřku organizace	3													24	30	30	18	18	24	36	36	27	36	15						36		30			24					27	45	27	
Neúmyslná modifikace dokumentů	2																																										
Zneužití přenosného zařízení pro špionáž	4												40	32	40	40	24	24	32	32	32	24	32							48		40			32								