Projekt přípravy společnosti English Editorial Services, s. r. o. na zavedení systému managementu se zaměřením na bezpečnost dat

Petra Stodůlková

Diplomová práce
2010

Univerzita Tomáše Bati ve Zlíně
Fakulta managementu a ekonomiky

Univerzita Tomáše Bati ve Zlíně
Fakulta managementu a ekonomiky
Ústav managementu a marketingu
akademický rok: 2009/2010

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Petra STODŮLKOVÁ**
Osobní číslo:	**M080647**
Studijní program:	**N 6208 Ekonomika a management**
Studijní obor:	**Management a marketing**
Téma práce:	**Projekt přípravy společnosti English Editorial Services, s.r.o. na zavedení systému managementu se zaměřením na bezpečnost dat**

Zásady pro vypracování:

Úvod

I. Teoretická část

- **Vypracujte literární rešerši na dané téma na základě studia literatury k řešené problematice včetně aktuálních standardů, dle kterých lze systém managementu ve firmě zavést.**

II. Praktická část

- **Analyzujte nynější stav řízení ve firmě.**
- **Zhodnoťte výsledky analýzy a navrhněte východiska pro zlepšení situace.**
- **Navrhněte projekt zavedení systému managementu se zaměřením na bezpečnost dat.**
- **Zpracujte harmonogram projektu včetně jednotlivých kroků při implementaci.**
- **Zhodnoťte přínos navrženého projektu pro činnost společnosti.**

Závěr

Rozsah diplomové práce: **70 stran**

Rozsah příloh:

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

Seznam odborné literatury:

[1] BRIŠ, Petr. Management kvality. 1. vyd. Zlín: Univerzita Tomáše Bati, 2005. 213 s. ISBN 80-7318-312-9.
[2] MLÝNEK, Jaroslav. Zabezpečení obchodních informací: Výběr a realizace bezpečnostních opatření k zajištění důvěrnosti, celistvosti a dostupnosti informací. 1. vyd. Brno: Computer Press, 2007. 154 s. ISBN 978-80-251-1511- 4.
[3] NENADÁL, Jaroslav. Měření v systémech managementu jakosti. 2. dopl. vyd. Praha: Management Press, 2006. 336 s. ISBN 80-7261-110-0.
[4] PLURA, Jiří. Plánování a neustálé zlepšování jakosti. 1. vyd. Praha 4: Computer Press, 2001. 244 s. ISBN 80-7226-543-1.
[5] TOŠENOVSKÝ, Josef, et al. Moderní management jakosti: principy, postupy, metody. 1. vyd. Praha: Management Press, 2008. 380 s. ISBN 978-80-7261-186-7.

Vedoucí diplomové práce: **Ing. Dušan Shejbal, Ph.D.**
Ústav výrobního inženýrství

Datum zadání diplomové práce: **29. března 2010**

Termín odevzdání diplomové práce: **3. května 2010**

Ve Zlíně dne 29. března 2010

L.S.

doc. Dr. Ing. Drahomíra Pavelková
děkanka

Ing. Pavla Staňková, Ph.D.
ředitel ústavu

PROHLÁŠENÍ AUTORA DIPLOMOVÉ PRÁCE

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 [1)];
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k nahlédnutí;
- 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 [2)];
- podle § 60 [3)] odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 [3)] odst. 2 a 3 mohu užít své dílo – diplomovou/bakalářskou práci - nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům.

Ve Zlíně 5.5.2010 ..... Šlodičková .....

1) zákon č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, § 47b Zveřejňování závěrečných prací:

(1) Vysoká škola nevýdělečně zveřejňuje disertační, diplomové, bakalářské a rigorózní práce, u kterých proběhla obhajoba, včetně posudků oponentů a výsledku obhajoby prostřednictvím databáze kvalifikačních prací, kterou spravuje. Způsob zveřejnění stanoví vnitřní předpis vysoké školy.

(2) Disertační, diplomové, bakalářské a rigorózní práce odevzdané uchazečem k obhajobě musí být též nejméně pět pracovních dnů před konáním obhajoby zveřejněny k nahlížení veřejnosti v místě určeném vnitřním předpisem vysoké školy nebo není-li tak určeno, v místě pracoviště vysoké školy, kde se má konat obhajoba práce. Každý si může ze zveřejněné práce pořizovat na své náklady výpisy, opisy nebo rozmnoženiny.

(3) Platí, že odevzdáním práce autor souhlasí se zveřejněním své práce podle tohoto zákona, bez ohledu na výsledek obhajoby.

2) 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, § 35 odst. 3:

(3) Do práva autorského také nezasahuje škola nebo školské či vzdělávací zařízení, užije-li nikoli za účelem přímého nebo nepřímého hospodářského nebo obchodního prospěchu k výuce nebo k vlastní potřebě dílo vytvořené žákem nebo studentem ke splnění školních nebo studijních povinností vyplývajících z jeho právního vztahu ke škole nebo školskému či vzdělávacího zařízení (školní dílo).

3) 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, § 60 Školní dílo:

(1) Škola nebo školské či vzdělávací zařízení mají za obvyklých podmínek právo na uzavření licenční smlouvy o užití školního díla (§ 35 odst. 3). Odpírá-li autor takového díla udělit svolení bez vážného důvodu, mohou se tyto osoby domáhat nahrazení chybějícího projevu jeho vůle u soudu. Ustanovení § 35 odst. 3 zůstává nedotčeno.

(2) Není-li sjednáno jinak, může autor školního díla své dílo užít či poskytnout jinému licenci, není-li to v rozporu s oprávněnými zájmy školy nebo školského či vzdělávacího zařízení.

(3) Škola nebo školské či vzdělávací zařízení jsou oprávněny požadovat, aby jim autor školního díla z výdělku jím dosaženého v souvislosti s užitím díla či poskytnutím licence podle odstavce 2 přiměřeně přispěl na úhradu nákladů, které na vytvoření díla vynaložily, a to podle okolností až do jejich skutečné výše; přitom se přihlédne k výši výdělku dosaženého školou nebo školským či vzdělávacím zařízením z užití školního díla podle odstavce 1.

ABSTRAKT

Účelem mé diplomové práce je vytvoření podkladového (informačního) materiálu, pomocí něhož a v něm uvedených příkladů, ukázek analýz a metod aplikovaných na danou firmu, by se zjistil nejen současný stav řízení ve firmě, ale také její možnosti, které má z hlediska implementace a certifikace. Což by následně mohlo vést k rozhodnutí, zdali vůbec, a potažmo jaký druh certifikace by byl pro ni vhodný. Teoretická část se zabývá shromážděním informací a podkladů týkajících se kvality a bezpečnosti informací. Cílem je tyto materiály poté zpracovat a na jejich základě provést vyhodnocení současného stavu v dané společnosti, která je již součástí samotné projektové části. Dle zjištěných ukazatelů a skutečností následně sestavit přehled jednotlivých kroků při případné implementaci a v závěru zhodnotit přínos projektu pro činnost společnosti.

Klíčová slova:

Systémy managementu, bezpečnost informací, ISO 9001, ISO 27001, analýza rizik

ABSTRACT

The purpose of this diploma thesis is to create base (information) material to find out the current status of a company´s management as well as its possibilities concerning the implementation and certification. Examples, analyses and methods are applied on a specific company. This procedure should subsequently lead to a decision whether and what kind of certificate is suitable. In the theoretical part, information and facts are collected as regards the quality of information security. The objective is to process these materials and evaluate the current status in the given company. This already constitutes an independent project part. Then, according to the facts ascertained, the work aims to make a list of individual steps for the potential implementation and evaluates the benefits of the project for the company´s activities.

Keywords:

Management systems, data security, ISO 9001, ISO 27001, risk analysis

Ráda bych na tomto místě poděkovala za odbornou pomoc, cenné připomínky a rady panu Ing. Dušanu Shejbalovi, Ph.D.

V neposlední řadě bych ráda také poděkovala vedení společnosti a kolegům za spolupráci při tvorbě projektu.

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

OBSAH

ÚVOD

Nacházíme se v době, která nutí nejen nás, občany, ale také firmy a instituce, aby produkovaly statky vysoké kvality. Nejedná se o něco, co bychom mohli považovat za nepodstatnou věc, ale jde o důležitou složku našeho života. Pokud si kladete otázku, proč tomu tak je, tak odpověď je nasnadě. Konkurenceschopnost. Ať již se jedná o jednotlivce nebo korporaci, tak pokud kvalita naší produkce je nízká, tak nás konkurence velmi snadno smete. Navíc existují instituce, které v případě, že kvalita produktů je nevyhovující a mnohdy i zdraví ohrožující, jsou schopny zakročit a tyto produkty nejen stáhnout z trhu, ale také danou firmu penalizovat, a to nemalou částkou. Můžeme říci, že takto náš stát brání občany, instituce a hlavně jejich uspokojování potřeb jako spotřebitelů a uživatelů.

V České republice došlo 10. května 2000 k vyhlášení oficiální státní politiky jakosti a současně k harmonizace s Evropskou chartou kvality (EOQ, Paříž, 23. října 1998). Toto se odehrálo na základě usnesení vlády č. 458/2000.

Dle charty je kvalita:

- cestou k dokonalosti organizace, protože pro konkurenceschopnost musíme reagovat přesně na potřeby a očekávání zákazníků a uživatelů
- metodologií, která podporuje účast, protože nelze žádat plnou angažovanost pracovníků bez současného rozvoje odpovídajících pracovních podmínek. Kvalita zahrnuje motivaci a odpovědnost, a proto metody a chování organizace musí být založeny na iniciativně a zájmu zákazníka.[1]

Při snaze firem navzájem si konkurovat dochází také k tomu, že firmy na výrobcích šetří (např. na výrobním materiálu), aby snížily výrobní nákladnost. Tímto jednáním může docházet k tomu, že to bude právě spotřebitel, který levně nakoupí, ale daným výrobkem může ohrozit svoje zdraví. Zajímavých výsledků dosáhly výzkumy realizované v minulých letech v zemích Evropské unie (dále jen EU), které odhalily, že

[1] Ryšánek (1998), s. 10

66 % ztrát trhů připadá na vrub nízké kvality produktů. Podrobnějším výzkumem se prokázalo, že také zde je rozhodující podíl nedostatků v etapách předvýroby.[2]

Zbožím naší doby se staly informace. Na tom, jak zvládnout proces tvorby, zpracování, ukládání a distribuce informací, jsou podniky a instituce životně závislé. Stále aktuálněji proto vystupuje do popředí otázka ochrany a bezpečnosti informací. Vedení mnohých organizací si uvědomuje, že ochrana a bezpečnost informací je jednou z priorit v systému řízení organizace. Právě proto, že pracuji ve společnosti, která je s tímto obeznámena, jsem se rozhodla, že také já mohu svým výzkumem přispět k dané problematice.

[2] www.businessinfo.cz

I. TEORETICKÁ ČÁST

1 LITERÁRNÁ REŠERŠE NA DANÉ TÉMA VČETNĚ AKTUÁLNÍCH NOREM, PODLE KTERÝCH LZE SYSTÉM MANAGEMENTU VE FIRMĚ ZAVÉST

1.1 Úvod do problematiky kvality

1.1.1 Česká republika a Evropská společenství

V prosinci 1990 zahájilo Československo s Evropským společenstvím (ES) rozhovory o uzavření asociační dohody, kterou o rok podepsalo.

Po rozpadu Československa ES ratifikační proces pozastavila. V roce 1993 obě strany podepsaly dohodu „zakládající přidružení mezi Českou republikou na jedné straně a ES a jejich členskými státy na straně druhé". Smlouva vstoupila v platnost 1. února 1995. Do té doby se vzájemné vztahy řídily Prozatímní dohodou.

Na svém zasedání v Kodani v červnu 1993 rozhodla Evropská rada, že asociované země ze střední a východní Evropě, které si to přejí, se mohou stát členy Evropské unie. Zároveň bylo stanoveno, že ke vstupu dojde, jakmile bude země schopná přijmout všechny povinnosti spojené se členstvím, bude splňovat ekonomické a politické podmínky a bude mít dostatečnou administrativní a soudní kapacitu potřebnou k převzetí acquis.

17. ledna 1996 podala Česká republika přihlášku ke členství v Evropské unii.

V červenci 1997 zveřejnila Evropská komise materiál Agenda 2000, ve kterém se přihlásila k myšlence „silnější a větší unie", a zveřejnila Posudky o připravenosti všech kandidátských zemí.

Agenda 2000

Agenda 2000 je akční program, přijatý Evropskou komisí 15. července 1997. Je to oficiální odpověď na požadavky, formulované na zasedání Evropské rady v Madridu v prosinci 1995, všeobecný dokument o rozšíření a o reformě společných politik a zpráva o finančním rámci Evropské unie po 31. prosinci 1999. Agenda 2000 se dotýká všech otázek, s nimiž se unie musí vyrovnávat na počátku 21. století. Součástí dokumentu jsou posudky zemí, které se v té době ucházely o členství v Unii (posudky, které vypracovala EK).

Agenda 2000 má tři části:

- První projednává o vnitřních mechanismech unie, zejména se zabývá reformou společné zemědělské politiky a politiky sociální a hospodářské soudržnosti. Obsahuje také doporučení, jak se nejlépe vyrovnat s nadcházejícím rozšířením a navrhuje vytvoření nové finanční perspektivy (tj. rozpočtu) na období 2000-2006.
- Druhá část navrhuje zesílenou předvstupní strategii, zahrnující dva nové prvky: přístupové partnerství a rozšířenou účast kandidátských zemí v programech Společenství - a vytvoření mechanismu pro uplatňování acquis Společenství.
- Třetí část představuje studii o vlivu rozšíření na politiky EU.

V prosinci 2002 byly uzavřeny všechny vyjednávací kapitoly včetně přechodných období, která poskytla novým členským zemím delší lhůtu k úspěšnému vyrovnání se všemi závazky vyplývajícími z členství v EU. Evropská rada rozhodla v souladu se stanoviskem Komise o přijetí 10 nových členských států k datu 1. 5. 2004. Dne 1. května 2004 se Evropská unie rozrostla na společenství 25 členských států.

13. prosince 2007 byla v Lisabonu podepsána Lisabonská smlouva (též Reformní smlouva). Lisabonská smlouva má zajistit efektivní fungování EU a jejích institucí do budoucna. Lisabonská smlouva je novelizací zakládajících smluv, které nadále zůstanou v platnosti.

Lisabonská smlouva obsahuje články pozměňující:

1) Smlouvu o EU (Smlouvu o EU, Maastrichtskou smlouvu)

2) Smlouvu o založení Evropského společenství (Smlouvu o ES, Římská smlouva)

Dále Smlouva nově stanovuje, že na těchto dvou smlouvách je Evropská unie (EU) založena, že nahrazuje Evropské společenství (ES) a je jeho nástupkyní. Evropská unie by tak měla mít jednotnou právní subjektivitu, jak už navrhovala Ústava EU.

Listina základních práv a svobod sice není - odlišně od Ústavy EU - částí textu Reformní smlouvy, ale je její nedílnou přílohou právně závaznou pro všechny členy, s výjimkou Velké Británie a Polska.

ES dále vydává tyto dokumenty:

- Zelené knihy vydává Komise. Jsou to dokumenty, které mají podpořit debatu a zahájit konzultace na evropské úrovni o určitém tématu (jako je například sociální politika, jednotná měna, telekomunikace, doprava, vzdělávání). Tyto konzultace mohou následně vyústit v publikaci BÍLÉ KNIHY, která již předkládá praktické návrhy.
- Bílé knihy Evropské komise jsou dokumenty, které obsahují návrhy na činnost Společenství v určité oblasti. V některých případech Bílá kniha následuje po vydání Zelené knihy, jejímž cílem je zahájit proces konzultací o daném tématu na evropské úrovni. Příkladem jsou Bílé knihy o završení jednotného trhu, o růstu, konkurenceschopnosti a zaměstnanosti, o sbližování práva v přidružených státech střední a východní Evropy v oblastech týkajících se vnitřního trhu. Vysloví-li souhlas Evropská rada, může se z Bílé knihy stát akční program Unie pro danou oblast.[3]

1.1.2 Nový přístup a Globální přístup

Technická harmonizace v Evropské unii - Technickou harmonizací se rozumí sjednocení technických právních předpisů, technických norem a postupů pro posuzování shody vlastností produktů, které jsou předpisy či normami upraveny. Harmonizace má být zajištěna do té míry, aby byly odstraněny technické překážky obchodu, které díky rozdílným národním požadavkům existují.

Principy pro odstraňování technických překážek obchodu byly v Evropském společenství založeny již v zakládající Římské smlouvě v r. 1957, s cílem vytvořit jednotný vnitřní trh s volným oběhem zboží, kapitálu, služeb a osob. Tento proces byl ovšem velmi dlouhý a nesnadný.

Do r. 1985 byly technické překážky odstraňovány zejména vydáváním harmonizujících technických předpisů (na úrovni tehdejšího Evropského hospodářského sdružení), které přímo upravovaly podrobné technické specifikace výrobků. Tento přístup však vylučoval postižení všech individuálních požadavků pro jednotlivé kategorie výrobků. Technické

---

[3] *Euroskop.cz:Věcně o Evropě* [online]. 2005 [cit.2010-03-03]. Vstup ČR do EU. Dostupné z WWW:<http://www.euroskop.cz/803/sekce/vstup-cr-do-eu/>

specifikace navíc s pokrokem zastarávají a podrobné závazné předpisy je pak nutno často aktualizovat, aby se nestaly brzdou inovací produktů i výrobních metod. V roce 1985 byl proto v zájmu rychlejšího a účinnějšího postupu, který byl naprosto nezbytný pro zajištění správné funkce vnitřního trhu v ES, přijat nový systém - *„Nový přístup k technické harmonizaci a normám“* (Usnesení Rady ze 7. května 1985 č. 85/C/136/01).

Nový přístup je založen na následujících principech:

- harmonizace právních předpisů (směrnic) je omezena na přijímání základních požadavků podstatných pro zajištění bezpečnosti výrobků, popř. dalších hledisek veřejné ochrany. Tyto základní požadavky musí výrobek splňovat a pak může být umístěn na trh v kterémkoli členském státě,
- podrobné technické specifikace, jejichž dodržení zaručuje splnění základních požadavků směrnic, jsou upraveny evropskými technickými normami,
- tyto normy, zvané harmonizované, jsou zásadně nezávazné, jejich dodržení však dává předpoklad, že základní požadavky směrnic byly splněny,
- výrobci je ponechána volba, zda bude postupovat podle harmonizovaných norem nebo zda zvolí jiné řešení, které je pro něj výhodnější; v takovém případě však musí soulad s požadavky směrnic prokázat.

Pro ty skupiny produktů, které obecně představují vyšší stupeň rizik, však zůstává i nadále systém závazných předpisů s podrobnými specifikacemi zachován. Tyto směrnice, zpravidla nazývané sektorové, platí např. pro motorová vozidla, potraviny, chemické látky a humánní i veterinární léčiva, a tento přístup k harmonizačnímu procesu se nazývá „starý“.

Nový přístup byl v r. 1989 doplněn „Globálním přístupem k posuzování shody“ (Usnesení Rady z 21. prosince 1989 č. 90/C10/01), který se zabývá obecnými principy zkoušení a certifikace, především pak prvky, které zajišťují důvěryhodnost systému a jsou předpokladem pro uznávání certifikátů mezi členskými státy. K těmto prvkům patří mj. akreditace zkušebních a certifikačních orgánů a certifikace systémů kvality u výrobce.

Rozhodnutím Rady č. 90/683/EHS, resp. 93/465/EHS byl přijat systém modulů, které lze k posouzení shody použít. Zpravidla existuje volba mezi moduly, které jsou považovány za rovnocenné. Postupy jsou přesně stanoveny v každé jednotlivé směrnici nového přístupu.

Výrobek, který splňuje požadavky směrnice, popř. více směrnic, se opatřuje označením CE.

V září 1997 nabyl účinnosti zákon č. 22/1997 Sb., o technických požadavcích na výrobky a o změně některých zákonů a na jeho základě byla schválena celá řada nařízení vlády, transponujících jednotlivé směrnice nového přístupu. [4]

New Approach - „vylepšení“ Nového Přístupu v datech:

- Zahájení 7. 5. 2003 - Evropská komise zaslala Radě a EP sdělení (Communication) ‘Enhancing the Implementation of the New Approach Directives’
- Zahájení procesu 10. 11. 2003 - Rada EU potvrdila ve své rezoluci, že New Approach (dosavadní stav) je vhodný nástroj pro regulaci vnitřního trhu EU a „jen“ je třeba jej vylepšit, zejména v oblasti posuzování shody (CE), akreditace a dozoru nad trhem.
- Ukončení technických prací: 14. 2. 2007 - Günter Verheugen (za EK) prezentoval na tiskové konferenci účel a cíle této nové legislativy
- Ukončení legislativních prací v EU: 13. 8. 2008 - V úředním věstníku EU (Official Journal OJ L 218, pp. 21, 30, 82) byl publikován soubor 3 aktů ve vztahu k uvádění výrobků na trh v EU, akreditaci a dozoru nad trhem.
- 31. 12. 2009 legislativní proces v ČR ukončen

[4] Technická harmonizace v Evropské unii. In ŠAFAŘÍK-PŠTROSZ, Alexander. Sborník dokumentů technické harmonizace: Nový přístup a globální přístup. svazek č.4. Praha: ÚNMZ, 2004. s. 11, s. 12. Dostupné z WWW:<http://www.unmz.cz/sborniky_th/04/0400.pdf>

Nový legislativní rámec (platný od 01. 01. 2010) - New legislative framework (NLF) je založen na:

- Regulation (EC) No 764/2008[5] - laying down procedures relating to the application of certain national technical rules to products lawfully marketed in another Member State

  Nařízení EP a Rady (EC) č. 764/2008 - kterým se stanoví postupy týkající se uplatňování některých vnitrostátních technických pravidel u výrobků uvedených v souladu s právními předpisy na trh v jiném členském státě a kterým se zrušuje rozhodnutí č. 3052/95/ES

- Regulation (EC) No 765/2008[6] - setting out the requirements for accreditation and market surveillance relating to the marketing of products

  (Nařízení EP a Rady (EC) č. 765/2008 - kterým se stanoví požadavky na akreditaci a dozor nad trhem týkající se uvádění výrobků na trh a kterým se zrušuje nařízení (EHS) č. 339/93)

  Jedná se o Nařízení, tzn. realizace je přímou aplikovatelností v členských státech bez nutnosti implementace. Platnost od 1.1.2010.

  Hlavní oblasti změn:

  - Definice – nové/upravené/doplněné
  - Akreditace
  - Dozor nad trhem

---

[5] EU. Regulation (EC) No 764/2008 Of the European Parlament and of the Council. In Official Journal of the European Union. 13.8.2008, L218/21, s. 218. Dostupný také z WWW: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:218:0021:0029:EN:PDF>.

[6] EU. Regulation (EC) No 765/2008 Of the European Parlament and of the Council. In Official Journal of the European Union. 13.8.2008, L218/30, s. 218. Dostupný také z WWW: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:218:0030:0047:EN:PDF>.

- Řízení výrobků dovážených ze třetích zemí (mimo EU a EFTA)
- Obecné principy označování výrobků CE
  - značka CE bude pod právní ochranou, sankce při zneužití
  - CE na výrobek smí připojit pouze výrobce nebo autorizovaný zástupce
  - CE označuje shodu s požadavky platných právních a technických předpisů (ne kvalita). Primárně je určena pro státní orgány (ne pro spotřebitele).
  - CE značku je možno umístit pouze na výrobky, u kterých to příslušné směrnice předpokládají. Jinde je to zakázáno.
  - Označením CE výrobce přebírá plnou právní odpovědnost za shodu výrobku se stanovenými požadavky, zejména za bezpečnost výrobku a splnění všech administrativních náležitostí (např. příbalový leták…)

- Decision No 768/2008/EC - on a common framework for the marketing of products

  Rozhodnutí EP a Rady č. 768/2008/EC - o společném rámci pro uvádění výrobků na trh a o zrušení rozhodnutí Rady 93/465/EHS[7]

  - Rozhodnutí 768/2008/EC se vztahuje pouze k regulované sféře (Nařízení (EC) č. 765/2008 se vztahuje na všechny oblasti)
  - Rozhodnutí 768/2008/EC je „sui generis“ legislativní akt. To znamená, že principy zde uvedené by měly být použity při tvorbě podřízených/následujících legislativních aktů (zejména novelizací směrnic nového přístupu). Toto rozhodnutí platí de jure ihned, de facto až po zapracování principů do nové legislativy.

[7] Interní dokumenty ITC a www.esipa.cz (placená služba)

- „Rozhodnutí o modulech – postupech posuzování shody“ No. 93/465/EEC je zrušeno a nahrazeno tímto novým rozhodnutím, tedy moduly se budou měnit.
- *Nejdůležitější ustanovení jsou v přílohách*:
    - Annex I – Referenční ustanovení pro harmonizační právní předpisy společenství týkající se výrobků
    - Annex II – Postupy posuzování shody
    - Annex III – ES prohlášení o shodě

Právní úprava v ČR vztahující se k ochraně spotřebitele a kvalitě produktů (základní výčet):

- Zákon č. 634/1992 Sb. o ochraně spotřebitele v platném znění
- Novela občanského zákoníku č. 367/2000
- Zákon č. 505/1990 Sb. o metrologii v platném znění
- Zákon č. 102/2001 Sb. o obecné bezpečnosti výrobků a o změně některých zákonů (o obecné bezpečnosti výrobků) v platném znění
- zákon č. 59/1998 Sb. o odpovědnosti za škodu způsobenou vadou výrobku v platném znění
- zákon č. 22/1997 Sb. o technických požadavcích na výrobky v platném znění

Kromě výše uvedených zákonů existuje řada evropských směrnic a národních vyhlášek, které dané zákony upřesňují nebo doplňují.

Politiku ochrany spotřebitele u nás podporuje také rozvoj různých sdruženích, které se touto problematikou přímo zabývají. V současné době se u nás vyskytuje několik těchto subjektů a zhruba 50 poradenských pracovišť, jejichž úkolem je hájit a pomáhat spotřebitelům při řešení problematických situací.

K nejznámějším patří:

- *Sdružení obrany spotřebitelů České republiky* – www.spotřebitele.info
- *Občanské sdružení spotřebitelů TEST – www.dtest.cz*

Důležité instituce politiky kvality v ČR:

- *Ministerstvo průmyslu a obchodu* (MPO) – www.mpo.cz
    - *Úřad pro technickou normalizaci, metrologii a státní zkušebnictví* (ÚNMZ) – www.unmz.cz
    - *Český institut pro akreditace, o. p. s.* (ČIA) – www.cia.cz
    - *Český metrologický institut* (ČMI) – www.cmi.cz

- *Česká obchodní inspekce* (ČOI) – www.coi.cz
- *Národní informační středisko pro podporu jakosti* – www.npj.cz
- *Asociace akreditovaných a autorizovaných organizací* (AAAO) – www.aaao.cz

1.2 Historický vývoj kvality

Názory na kvalitu prodělaly dlouhý historický vývoj, který se datuje až do dob prvobytně pospolné společnosti, kdy si lidé začali zhotovovat nástroje pro lov, oděvy pro ochranu těla, obydlí, pomůcky pro zpracování přírodních produktů.[8] Další příklady můžeme nalézt také na reliéfech z egyptských Théb[9] (2. stol. př. n. l.). Zde je zobrazen kontrolor na stavbě pyramidy, kdy kontroluje rozměry kamenných kvádrů. Také definice kvality Aristotelem je důkazem toho, že lidský zájem o kvalit není jen novodobou záležitostí. Ze záznamů z Chammurapiho zákoníku (ze staré Mezopotámie 1792 – 1750 před Kristem)[10] víme, že zde byly navrženy tresty smrti za to, když stavitel postavil obydlí s nevyhovující konstrukcí, jež zapříčinila zřícení domu a usmrcení jeho obyvatel.

Jak docházelo k rozvoji obchodu a používání měr a váh, začali se lidé zajímat také o kontrolu těchto veličin. V době středověku byla kvalita hlídána a kontrolována nařízením řemeslnických cechů (např. zákaz výroby zlata s ryzostí nižší než 16 karátů v Německu).[11] V jiných krajích se za šizení a vady výrobků usekávaly ruce nebo docházelo dokonce k popravám. Český král Václav IV zavedl trest v podobě nápravných koupelí nepoctivých obchodníků ve Vltavě.[12]

S čím se také postupně setkáváme, je zasahování státu do oblastí kvality. Nejdříve byla důvodem podpora rozvoje výroby a obchodu, ze kterých postupně zesílily důvody ochranářské. Příklad zásahu ze strany státu do oblasti kvality můžeme sledovat v roce 1887 ve Velké Británii, kdy britská dolní sněmovna odhlasovala, že zboží importované do země musí mít označení původu (dodnes přetrval způsob označení *„made in...“*).[13]

---

[8] Briš (2005), s. 6

[9] Zídková (2003), s. 7

[10] Veber (2007), s. 14

[11] Veber (2007), s. 19

[12] Zídková (2003), s. 7

[13] Veber (2007), s. 14

Dalším milníkem se stalo období, kdy vznikl vztah poskytovatele produktu – zákazník, kde byl produkt předmětem směny. V případě řemeslné výroby víme, že byl zhotovitel v přímém kontaktu se zákazníkem, znal jeho požadavky a přání. Průmyslová revoluce přinesla sebou nárůst jak manufaktur, tak i kontroly. Setkáváme se zde s hlubší dělbou práce, kdy dělník nebyl již v přímém kontaktu se zákazníkem. Došlo k předávání výrobku mezi spolupracovníky, čímž se ztratil pocit vlastnictví a hrdosti na daný výrobek. Komplexní přístup byl narušen, načež bylo nutné implementovat průběžnou kontrolu, která měla zajistit dosahování požadovaných charakteristik produktu. Tato kontrola byla nejdříve zajištěna dělníky a mistry popřípadě majiteli. Za zmínku jistě stojí, že Henry Ford jako první použil ve svých závodech funkce technických kontrol, kdy nejzkušenější pracovníci (z řad dělníků) měli na starosti i zodpovědnost za kvalitu.

Milníkem bylo také období druhé světové války, kdy důrazy na kvalitu zesílily, a to proto, že byla enormní spotřeba válečného materiálu. Byly vytvořeny normy s technickými požadavky na jednotlivé produkty, vše bylo pečlivě monitorováno, měřeno a vyhodnocováno.

Další zlom nastal ve 30. letech minulého století, kdy se objevili zásluhou Američanů Shewharta a Romiga první statistické metody kontroly výrobních procesů.[14] Při nich docházelo ke kontrolám jen některých produktů, a to z toho důvodu, že v důsledku navýšení produktů stejného provedení nebylo možno překontrolovat každý výrobek samostatně. V poválečném období dochází k růstu požadavků na produkty a jejich kvalitu, kdy výrobci postupně zjišťovali, že produkt bez vad ještě nezaručuje to, že bude na trhu úspěšný. Začínal se klást důraz nejen na kvalitu, ale také na design, spolehlivost, funkčnosti a úspornost. Zde hrála také důležitou roli kvalita procesů, kterými produkty vznikají, což se pomalu dostává do popředí zájmu managementu a jeho odpovědnosti za kvalitu.

Jednou z prvních zemí, která si uvědomila přínos kvality a její význam z konkurenčního hlediska, a to nejen pro podnik, ale také pro společnost, bylo Japonsko. K tomuto došlo po druhé světové válce, kdy v zemi docházelo k masivnímu zavádění statistické regulace

[14] Nenadál (2008), s. 16

a kdy získané poznatky byly aplikovány nejen v dané firmě, ale také v každodenní praxi (i v neziskovém sektoru). Tento příklad zaveden v Japonsku v 70. letech byl příkladem i pro ostatní průmyslové podniky, které si začaly uvědomovat, že produkty, které produkují, nemusejí být konkurenceschopné na trhu. Dochází ke zlomu, kdy se podniky nažily prokázat, že dodávají kvalitní produkty (výrobky a služby). Toto dalo základ podnikovým a odvětvovým standardům, které dané požadavky obsahovaly. Pokud bychom se pokusili o stručné zmapování cesty k řízení kvality, tak bychom mohli říci, že je následovná:

zjištění (popř. predikce) požadavků zákazníků – vývoj – nákup – realizace (výroba) – skladování – prodej – doprava – instalace – technická podpora – likvidace – zpětná vazba od zákazníka[15]

Z literatury víme, že tyto požadavky managementu kvality byly poprvé formulovány v normách AQAP (Allied Quality Assurance Publications) pro organizaci NATO, dále se připojila NASA. Poté došlo k jejich aplikaci také do civilního sektoru.[16] Na konci 80. let dochází k dalšímu vývoji, kdy vzniká technická komise ISO/TC 176 (roku 1980), která navrhla akceptaci norem ISO 9000 (v roce 1987).

Druhy norem pro řízení kvality se liší dle požadavku na její řízení:[17]

- *AQAP* – pro NATO, NASA
- *ISO 9000*
- *QSF* – pro letectví a kosmonautiku
- *GMP* – pro potraviny a léky (stanovené WHO)
- *VDA, QS-9000, ISO/TS 16949* – pro automobilový průmysl

V současné době, charakteristické rychlým rozvojem jak vědy (můžeme sledovat rapidní nárůst zájmu a požadavků na ochranu životního prostředí), tak techniky (rozvoj počítačové

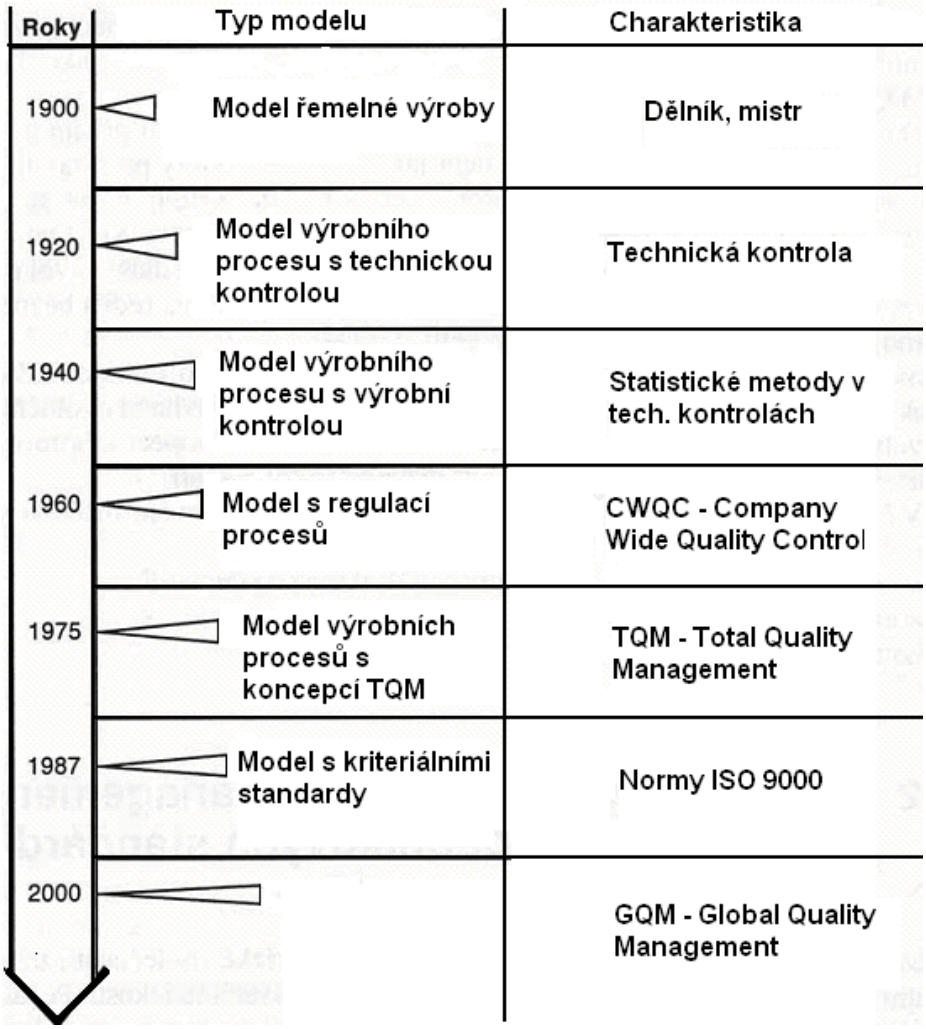
[15] Veber (2007), s. 16

[16] Veber (2007), s. 16

[17] Veber (2007), s. 16

a čipové technologie), která klade vysoké nároky nejen na jednotlivce, ale také na organizace v ní působící, je důležité, aby firmy začlenily také do svých procesů otázky ekologie i bezpečnosti práce či bezpečnosti a ochrany informací.

Obr. 1. Časový sled vývoje managementu kvality ve 20. století[18]



Kvality se staly základním pilířem řízení společnosti, nástrojem jejich rozvoje a také jsou využívány jako konkurenční výhody v úsilí o získání zákazníků na svou stranu. Nakonec

[18] Nenadál (1998)

ten, kdo není schopen garantovat standardní úroveň kvality, má minimální naději na úspěch. Vztahují se nejen k výrobkům, službám, činnostem a procesům, ale také k výzkumu nových metod a přístupů k aplikacím v různých oblastech, kde bychom donedávna kvality ani neočekávali (činnost policie, státní správa).[19]

1.3 Objasnění pojmu kvalita

V literárních zdrojích se můžeme setkat s různými definicemi objasňujícími a vymezujícími pojem kvalita (dříve také jakost). Dalo by se říci, že co autor, tak to jiná definice. Jinými slovy její definice není jednoznačně stanovena a existuje mnoho různorodých přístupů k vymezení pojmu kvalita (jakost).

Uveďme si na příkladech:

- *Kvalita (jakost) je minimum ztrát, které výrobek od okamžiku své expedice dále společnosti způsobí.* (Genichi Taguchi)
- *Kvalita (jakost) je shoda s požadavky.* (Phil Crosby)
- *Kvalita (jakost) je to, co za ni považuje zákazník.* (Armand V. Feigenbaum)
- *Kvalita (jakost) je vhodnost pro použití.* (Joseph M. Juran)
- *Kvalita (jakost) je stupeň splnění požadavků souborem inherentních charakteristik.* (ČSN EN ISO 9000:2006)
- *Kvalita (jakost) je souhrn vlastností a charakteristických rysů produktu nebo služby, které vytvářejí schopnost uspokojovat dané nebo vyvolené potřeby.* (Americká společnost pro jakost)

[19] Veber (2007), s. 14

Výrazy jakost i kvalita jsou latinského původu a jsou si navzájem synonymem.[20] Proto jsou v předešlém výčtu uvedeny pospolu. Jak vidíme v přehledu vybraných definic, tak se tyto navzájem výrazně neodlišují, spíše si můžeme povšimnout snahy o vylepšení jejich přesnosti a srozumitelnosti. Také je zde v pozadí patrné zahlédnout zákazníka (osobu, která přijímá produkt). Jeho požadavky, kterých se ve vztahu ke kvalitě domáhá, se liší, jsou časově proměnlivé a ovlivněny řadou faktorů.[21]

- *Biologických* (věk, zdravotní stav, pohlaví)
- *Demografických* (zvyky, klima, lokalita)
- *Společenských* (veřejné mínění, názory odborníků, reklama, hnutí)
- *Sociálních* (vzdělání, zaměstnání, společenské postavení)

Orientace na zákazníka je charakteristickým rysem současné doby a snahou podniků je podřídit výrobní programy, vývoj produktů, služeb a stanovením cen, požadavkům zákazníka.

S pojmy kvalita (jakost) se v posledních letech setkáváme stále častěji a náš pohled na posuzování kvality produktů je subjektivní a odlišný. Toto je způsobeno tím, že jsme ve svém každodenním životě postaveni do dvou různých rolí – role *dodavatele produktu* (výrobku a služby) a role *zákazníka*.[22] Z vlastních zkušeností je známo, že zákazník vyžaduje kvalitní zboží a služby za nízké ceny. Kdežto v roli výrobce již nejsme tak důslední.

Smyslem systémů managementu není vytvářet rozsáhlé dokumentační řetězce a pyramidy ani samotná certifikace, ale ve výsledku dosáhnout co nejvyšší úrovně spokojenosti a následně i loajality ze strany zákazníků při oboustranně akceptovatelné ceně produktu. Toto vše při minimálních nákladech, zato co nejefektivnějším způsobem. Jak je známo, tak

[20] Nenadál (2008), s. 13

[21] Veber (2007), s. 19

[22] Zídková (2003), s. 6

nízké náklady a šťastní zákazníci tvoří předpoklad toho, že firma bude ekonomicky úspěšná. Ovšem toho, že zákazníci jsou spokojeni, nedosáhneme pouze náhodně, ale prostřednictvím učení se ze zkušeností. Čili zde nezanedbatelnou úlohu hraje *zpětná vazba*, která je tvořena kanály sloužícími k systematickému výzkumu. Tento výzkum následně odhalí míru spokojenosti zákazníků s produkty jim nabízenými. Systém je tvořen procesy (mnohdy velmi náročnými a obsáhlými) v různých etapách životního cyklu produktu – od marketingového výzkumu trhu až po záruční servis a likvidaci produktu.

Nuton zmínit také pojem *absolutní kvalita*, který znamená ideál, ke kterému se snaží výrobce přiblížit. To, zdali se toto přiblížení uskuteční a jeho míra, závisí na dokonalosti podnikového systému managementu kvality. Z dosavadních poznatků je známo, že skutečnost vnímaná zákazníkem na trhu (tzn. výsledná kvalita), je asi 50 % z daného ideálu. Zbývajících 50 % znamenají ztráty. [23]

1.4 Tři základní koncepce managementu kvality

Podnikové standardy

Podnět ke vzniku byl dán hlavně ze stran amerických společností, načež se následně přidávaly další. Požadavky byly uvedeny v normách platných jak v rámci firem, tak se jimi museli řídit také všichni jejich dodavatelé. Jedná se o např. standardy VDA, AQAP, QS-9000, IFS, BRC, standardy IKEA apod.

[23] BusinessInfo.cz [online]. 1997-2010 [cit. 2010-03-03]. Kvalita, jakost. Dostupné z WWW:<http://www.businessinfo.cz/cz/clanek/kvalita-jakost/system-managementu-jakosti/1000513/16924/#b02>.

TQM (Total Quality Management)[24]

Total – úplné zapojení všech pracovníků (administrativa, ostraha, servis, marketing)

Quality – splnění očekávání zákazníka (výrobek, služba), ale i proces, činnost

Manangement – řízení jak z pohledu strategického, taktického a operativního, tak z pohledu manažerských aktivit (plánování, motivace, vedení, kontrola, atd.)

Jedná se o manažerský přístup, koncipovaný zejména v Japonsku, poté USA a Evropě, jehož cílem je neustálé zlepšování ve všech oblastech. Na tomto systému se podílí všichni zaměstnanci firmy za účelem maximálně uspokojit požadavky zákazníků a souběžně se snaží o dosažení ekonomického přínosu. Jedná se o využití všeho pozitivního, co může být použito pro rozvoj podniku. Jelikož není ovlivněn žádnou normou nebo směrnicí, je zde otevřený prostor pro kreativitu. Tato koncepce se orientuje na:[25]

- *Zákazníka* (partnerství s dodavateli)
- *Prevenci* (orientace na procesy)
- *Neustálé zlepšování a inovace*
- *Účast všech zaměstnanců* (vedení lid, týmová práce, rozvoj angažovanosti)
- *Komunikace a informace* (měřitelnost výsledků)
- *Vliv a odpovědnost vůči okolnímu prostředí*

ISO (International Organization for Standardization)

Tato mezinárodní organizace sídlící v Ženevě a její technická komise ISO/TC 176 *Management kvality a prokazování kvality* v roce 1987 uvedla skupinu norem (původně pět norem) výhradně se zabývajících požadavky na *„management quality" – systém kvality*.

---

[24] překlad do češtiny používá označení komplexní (úplné, integrované) řízení jakosti. Můžeme se take setkat s výrazy TOC (Total Quality Control) a CWQCM (Company Wide Quality Control Management).

[25] Jedná se o šest základních pilířů. Většina těchto principů byla převzata normou ISO řady 9000 z roku 2000.

Jedná se o koncepci, která má univerzální charakter, a to proto, že může být použita bez ohledu na velikost organizace, její výrobní program nebo službu. Nicméně by tato koncepce měla být brána jako počáteční bod na cestě ke špičkové kvalitě, a to z toho důvodu, že ani v případě jejich striktního dodržování nelze zaručit plnou spokojenost, loajalitu ani splnění hospodářských cílů.

Vzhledem k existenci několika norem a předpisů, které se odlišovaly pouze strukturu, ale ne požadavky, vznikla potřeba na jejich sjednocení, a tím byly vytvořeny normy ISO řady 900x. Závaznost norem na tyto normy není aplikovatelná, mají pouze doporučující charakter a obsahují minimální požadavky, které by měly být ve firmě zavedeny. Závazným by se staly v případě jejich uvedení v podmínkách obchodní smlouvy. Organizace ISO provádí revize norem v pětiletých periodách.

Pokud se podíváme na dané koncepce (ISO, TQM, podnikové/oborové standardy), tak zjistíme, že jejich společnou a hlavní prioritou je, co nejvíce spokojený zákazník. Jeho monitoring mají pevně zakotven a jsou i případy, kdy je pojat také jako součást povinného měření výkonnosti dané organizace.

1.5 Management

Japonský pohled na management je vysoce pozitivní a nazývá se *kaizen*. Jeho principem je zdokonalování všeho, po celou dobu a všemi.[26] Lze jej chápat jako proces tvorby a následného rozvíjení podnikatelsky orientovaného chování společností. Jedná se o činnosti (např. rozhodování, organizování, práce s inovacemi, plánování, implementace, kontrola) zabezpečující chod organizace, které slouží jako výchozí pro práci manažera.

Chápání managementu může být rozděleno do následujících skupin:

Zdůrazňující vedení lidí - tvorba a udržování prostředí umožňující jednotlivcům pracovat společně ve skupinách a uskutečňovat dané cíle.

[26] Kotler (2003), s. 100

Z pohledu specifických funkcí vykonávaných vedoucími pracovníky – jedná se o proces plánování, organizování, vedení a kontroly činností, s cílem dosažení organizačních úkolů.

Předmět studia a důraz na jeho účel - věnuje se stanovením nejlepších postupů k dosažní cíle organizace.

1.5.1 Pohled na službu (produkt) z hlediska kvality

Kvalita služby = skutečný služba – očekávaná služby

Kotler definuje službu jako „jakoukoli činnost nebo výhodu, kterou může nabídnout jedna strana druhé, je v zásadě nehmotná a nevytváří žádné nabyté vlastnictví. Její realizace může, ale nemusí být spojena s fyzickým produktem.[27]

Z literatury dále také známe základní vlastnosti služeb:

Nehmotnost:

- není možné ji předem poslechnout, ochutnat, očichat, prohlédnout a málokdy ji lze vyzkoušet. Posuzovat ji však lze na základě personálu, místa, propagačních tiskovin, ceny.

Neoddělitelnost:

- nelze oddělit od prodávajícího. Díky tomu se zákazník může stát spoluproducentem služby a někdy se i podílet na její tvorbě (např. koncert). Služby jsou totiž obvykle prodány a teprve poté produkovány a spotřebovány.

Proměnlivost:

- neboli heterogenita znamená, že kvalita služby se odvíjí od toho, kdo ji poskytuje. Není snadné předvídat chování spotřebitelů, provádět výstupní kontroly před jejím dodáním. Z tohoto lze usoudit to, že služba může být poskytnuta s rozdílným výsledkem, a proto i jejich standardizace je velmi složitá.

---

[27] Kotler (1992), s 789

Pomíjivost:

- službu nelze skladovat nebo opětovně prodávat. Mělo by se dbát na její dostupnost a tím vyrovnání fluktuace poptávky (např. lístky do kina). Tato vlastnost také udává, že ji lze velmi těžko reklamovat (jsou i případy, kdy může být nahrazena novou službou).

Nemožnost vlastnictví:

- tím, že je nehmotná a nelze ji skladovat, tak ji nelze také vlastnit. Kupujeme si pouze právo na její poskytnutí (užívání) a přístup k ní (např. hotelový pokoj, sedadlo v letadle).

Základní vlastností produktu (či služby) je uspokojovat lidské potřeby. Můžeme říci, že každý produkt (služba) uspokojuje jiné potřeby (např. biologické, sociální, estetické), a také že má určitou úroveň znaků kvality. Základní členění je na skupiny *kvalitativních* znaků (např. image, technická kvalita, funkčnost) a skupinu *kvantitativních* znaků (např. objem služeb, časová dimenze a tok služeb). Rozdíl, mezi kvalitativními a kvantitativními znaky je jejich vyjádřitelnosti v číselné hodnotě (kvalitativní vyjádřit nelze). Zato v očích spotřebitele mohou hrát rozhodující roli (např. chování personálu, vůně, chuť). Každý produkt má tyto vlastnosti jedinečné a vypovídající o jeho charakteru.

Dle *„filozofie vrstev,“* která se zabývá užitnými vlastnostmi produktu a popisuje jeho vlastnosti z pohledu zákazníka, se produkt skládá z vrstev.

Kde dle Leeflangovi teorie máme:

- *Fyzický produkt* – rysy objektivně zjistitelné (např. barva, tvar).
- *Rozšířený produkt* – zde vstupuje marketing (např. obal, značka, služby).
- *Totální produkt* – rysy připisované produktu zákazníkem (např. životnost, modernost).

Kotler chápe danou problematiku následovně:

- *Základní produkt* – jedná se o základní potřebu, požadovanou uživatelem po výrobku k tomu, aby jeho potřeby byly uspokojeny (konečný prospěch)
- *Vnímatelný produkt* – hlavně fyzické vlastnosti a charakteristiky (např. design, styl)

- *Zvětšený (rozšířený) produkt* – soubor služeb, které s výrobkem souvisí (např. záruky, instalace, náhradní díly, ekologické parametry)

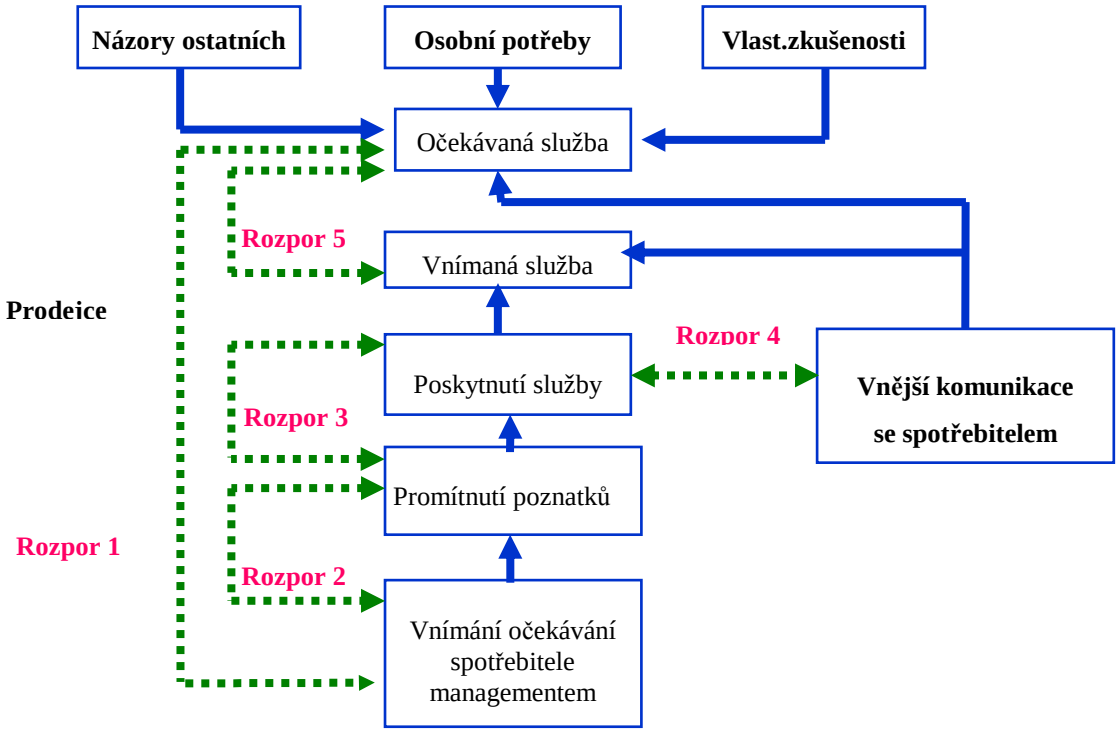
Služby jako takové mohou být rozděleny na:

- *Základní* (klíčové, elementární) – jsou hlavním důvodem pro zákazníka
- *Periferní* (doplňkové) – nedílná součást služby, dotváří její hodnotu
- *Globální* – základní a periferní, které vytváří nabídku

Požadavky zákazníka na kvalitu služeb:

- Spolehlivost a pružnost
- Vhodné prostředí a odborná způsobilost
- Vlídné zacházení
- Dostupnost

Obr. 2. Model popisující kvalitu služeb



Zdroj: přednášky Marketingu obchodu a služeb, rok 2001

V modelu popisujícím kvalitu služeb je znázorněno také pět rozporů ve vnímání kvality u služeb:

Rozpor 1 – mezi očekáváním spotřebitele a tím, co vnímá management

Rozpor 2 – mezi vnímáním managementu a očekávanou kvalitou služeb

Rozpor 3 – mezi specifikovanou kvalitou služeb a poskytováním služeb

Rozpor 4 – mezi vnější komunikací se spotřebitelem a poskytovanou službou

Rozpor 5 – mezi očekávanou službou a vnímanou službou

V dřívějších dobách zákazníkovi postačovalo, aby produkt splňoval základní (funkční) požadavky (např. ochrana před chladem). Postupem času začal zákazník požadovat i další užitné vlastnosti (např. u služeb spolehlivost, dostupnost, pružnost, odbornost apod.) a navíc vyžadoval, aby produkt byl dodáván včas, za odpovídající cenu a kvalitu. Hovoříme o *„triádě úspěšnosti,“* jejíž splnění v 90. letech bylo předpokladem úspěchu. Nedlouho na to, a to je počátkem 20. století, byla do ní přidána kvalita, a to proto, že opakovaná produkce je výhodná nejen pro společnost, ale také koncového zákazníka (snižuje náklady => nižší cena pro kupujícího). Z hlediska kvality to také znamená postupné odstranění nedostatků, které se zprvu při výrobě mohou objevovat, ale s další výrobou se eliminují, čímž může docházet až ke zlepšování vlastností koncového produkt (např. kvality, funkčnosti).

V případě služeb by neměla být opomenuta ani tvorba *„package“*. To proto, že služba může vystupovat jako jeden produkt nebo komplex služeb jednoho produktu. Dle definice package představuje kombinaci souvisejících a vzájemně se doplňujících služeb do komplexní nabídky. toto si získalo oblibu u zákazníka pro větší pohodlí, hospodárnost, lepší možnosti plánování prostředků, uspokojování zájmů, a také zajištění trvalé kvality. Pro organizaci má význam hlavně například pro zvyšování poptávky mimo sezónu, působí přitažlivěji, umožňuje jednoduší předvídání vývoje podnikání, a také díky ní roste spokojenost zákazníka a tvorba kladných vztahů s veřejností.

V dnešní době je zákazník ten, kdo stanovuje pravidla a klade požadavky na společnosti. Proto je důležité, aby si firmy uvědomovali nebo alespoň byly schopny rozpoznat, co zákazník od nich chce kupovat, co vyžaduje, potřebuje a jak vnímá kvalitu jimi poskytovaných produktů. Velké firmy si stále více tuto skutečnost uvědomují.

Několik příkladů:

Motorola*: „Naši zákazníci určují kvality norem. Naší prací je, je dodržet.“*[28]

Siemens: *„Kvalita znamená, že naši zákazníci se k nám vracejí, ale naše výrobky ne.“*[29]

[28] Kotler (2003), s. 148. “Our customers set our quality standards. Our job is to meet them.

[29] Kotler (2003), s 148. “Quality is when our customers come back and our products don’t.”

2 SYSTÉM MANAGEMENTU VE SPOLEČNOSTI POSKYTUJÍCÍ REDAKČNÍ, PŘEKLADATELSKÉ A GRAFICKÉ SLUŽBY

„Ne vždy vysoká cena je známkou kvality.“

Také trh s překladatelskými službami se v posledních letech rozrostl o desítky překladatelských agentur a tisíce nezávislých překladatelů. Tento jev však může pro koncového uživatele působit velmi nepřehledně.

Výběr překladatelské agentury či překladatele není snadný a hledání optimálního poměru kvalita. Na českém trhu působí desítky překladatelských agentur a tisíce nezávislých překladatelů, kteří poskytují služby nejrůznější kvality.

Překladatelské služby – požadavky na poskytování služby

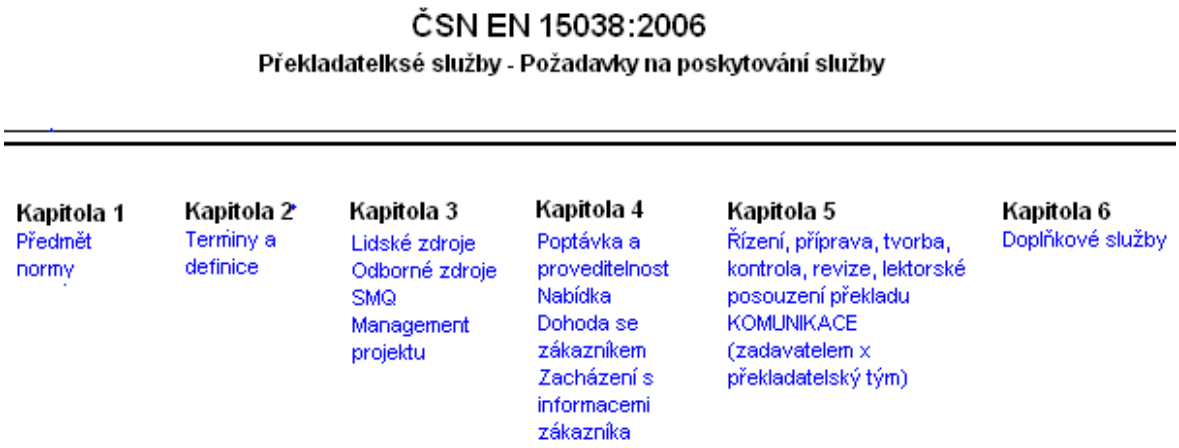
Od listopadu 2006 platí evropská norma EN 15038 i v České republice pod označením ČSN EN 15038:2006 Překladatelské služby – Požadavky na poskytování služby. Norma stanovuje požadavky na překladatelské služby z hlediska zabezpečení lidských a technických zdrojů, managementu kvality a projektů, rámcových smluvních podmínek a postupů poskytování služby (pozor nevztahuje se na tlumočnické služby). Pozornost je věnována také vymezení vztahu mezi zákazníkem a poskytovatelem překladatelských služeb. Norma nezapomíná ani na velice důležité téma vzájemné kooperace všech zainteresovaných stran v průběhu tvorby překladu. Norma určuje nový, doposud ne příliš často využívaný prvek procesu tvorby překladu, kterým je revize revizním pracovníkem. Revizní pracovník, který má odbornou způsobilost ve zdrojovém i cílovém jazyce, překlad kontroluje z hlediska vhodnosti pro stanovený účel, porovnává zdrojový i cílový text s ohledem na jednotnost terminologie, registr a styl. Na základě kontroly pak navrhuje případná opatření k nápravě, která mohou v krajním případě znamenat i nový překlad.

Norma ČSN EN 15038 není určena k certifikaci konkrétního hmotného produktu - tj. překladu, ale k certifikaci služby, která jako taková v sobě obsahuje požadavek na zavedení takového postupu, který musí zajistit výběr osob s potřebnými dovednostmi a kvalifikací

pro konkrétní překladatelské projekty. Norma definuje odbornou způsobilost překladatele/týmu překladatelů na základě 5ti oblastí[30]:

- překladatelská odborná způsobilost
- jazyková a stylistická odborná způsobilost ve zdrojovém a cílovém jazyce
- výzkumná odborná způsobilost, získávání a zpracování informací
- kulturní odborná způsobilost a konečně
- technická odborná způsobilost.

Obr. 3. Znázornění struktury normy ČSN EN 15038



Z grafického znázornění vidíme, že norma je rozdělena do 6 kapitol a každá kapitola následně obsahuje specifické podkapitoly.

Kapitola 3 definuje minimální profesionální odbornou způsobilost překladatelů, revizních pracovníků a lektorů, minimální požadavky na systém managementu kvality (SQM) a projektu.

Kapitola 4 se zabývá od vztahů se zákazníky, poptávky až po nakládání s informacemi klienta.

[30] www.csq-cert.cz

Kapitola 5 se mimo jiné zabývá vzájemnou kooperací všech zainteresovaných stran během práce s textem, což je důležité pro produkci vysoce kvalitního překladu. Významnou roli zde hraje také revizní pracovník, který má odbornou způsobilost ve zdrojovém i cílovém jazyce, tudíž může překlad kontrolovat z hlediska vhodnosti pro stanovený účel, porovnat dodržení jednotné terminologie a stylu. Je schopen navrhnout opatření k nápravě (např. nový překlad).

Zástupci překladatelských agentur si jsou plně vědomi, že bez stanoveného postupu pro dělení překladů dle oborů a stanovení odborné způsobilosti pro překladatele, nemůže agentura řádně fungovat. Proces překladu je značně závislý na dobré komunikaci mezi překladatelem a zákazníkem, kdy je nutné především stanovit účel překladu, případné nejasnosti ve výchozím textu či vyjasnit terminologii.
Čím odbornější je překládané téma, tím hlubší věcnou znalost problematiky musí mít překladatel.

Komunikujte s překladateli. Měli by dobře znát překládanou problematiku. V opačném případě je na čase změnit dodavatele překladů. Překladatelé by si neměli odborné problematice učit na váš účet. Není-li to ovšem s vaším výslovným souhlasem, například když si chcete vychovat vlastní překladatelský tým.
Každý realizovaný překlad je vždy závislý na obou stranách - zákazníkovi i překladatelské agentuře/překladateli. Certifikace překladatelských služeb dle normy ČSN EN 15038:2006 může zvýšit předpoklad, že výběr překladatelské agentury/poskytovatele překladatelských služeb nebude rizikem, ale stane se informovanou a důvěryhodnou volbou.

Národní specifikace CEPRES:2007

Aby mohla být nová evropská norma EN 15038 zavedena do praxe, vytvořila pracovní skupina Regionálního evropského centra mezinárodní Federace tlumočníků a překladatelů (FIT) prováděcí doporučení. Pracovní skupina v ČR, která v pozměněné sestavě založila Národní radu pro certifikaci překladatelských služeb, vytvořila paralelně s EN specifikaci CEPRES:2007 jako nástroj pro certifikaci podle EN doplněný o další požadavky nezbytné pro český překladatelský trh. Specifikace si tak neklade za cíl nahradit výše zmiňovanou

evropskou normu, nebo snad hledat nějakou jinou cestu – velmi vhodně tuto normu však doplňuje a upřesňuje.

Certifikace poskytovatelů překladatelských služeb podle specifikace CEPRES:2007 je čistě dobrovolnou záležitostí ve firmách (tzn. je nepovinná), nicméně bude pro potenciální klienty silnějším signálem záruky kvality než přihlášení se „pouze“ k mezinárodní normě ISO 9001, Systémy managementu jakosti.

Specifikace CEPRES:2007 je výsledkem spolupráce odborníků z oblasti překladatelských služeb a oblasti certifikací. Na společném díle se formou připomínek a pohledu praktiků podíleli i samotní překladatelé.

Specifikace CEPRES:2007 je tedy koncipována jako doplnění a zpřesnění požadavků procesních norem. Může však být aplikována také samostatně, neboť obecná pravidla procesního řízení (např. ve formě struktury mezinárodní normy ISO 9001:2008 i ČSN EN 15038) již v sobě obsahuje. [31]

[31] Text specifikace verze 2007 je veřejně dostupný na: http://www.cepres.cz/index.php?action=3&action2=1

3 ZPŮSOBY SYSTÉMOVÉHO ŘEŠENÍ VEDOUCÍ K OCHRANĚ DAT V PRAXI

3.1 Možné varianty přístupu k systémovému nastavení managementu ochrany dat v organizacích

Rozhodne-li se firma k systémovému přístupu u procedury tvorby, zpracování, ukládání a distribuce informací, jejíž nedílnou a velmi významnou oblastí je ochrana a bezpečnost informací může využít principy těchto produktů nebo se může rozhodnout pro jejich plnou aplikaci (pokud jsou vhodné pro její předmět podnikání) a realizovaný systém si nechat posoudit třetí stranou. V případě naplnění požadavků bývá o takovém prověření vystaven dokument – zpravidla Certifikát nebo Osvědčení.

- **APEK**

  Asociace pro elektronickou komerci (APEK) je sdružením firem, podnikatelů a odborníků v oboru elektronického obchodu.

  Certifikační pravidla jsou vytvořena na základě platných zákonů – zejména Směrnice Evropského parlamentu a Rady o elektronickém obchodu, Směrnice o prodeji na dálku, občanského zákoníku, zákona o ochraně spotřebitele – stávajících pravidel APEK a certifikačních pravidel zemí EU.[32]

- **Q-Web**

  Q-web je služba IQNetu pro hodnocení a certifikaci elektronického obchodu (e-commerce) a elektronického podnikání (e-business). Je založena na mezinárodních standardech a vlastních IQNet technických specifikacích.

  Q-web cerifikační služba byly vyvinuta pod vedením IQNetu podle existujících platných cerifikačních zásad.

[32] Plné znění pravidel je k dispozici na: http://www.apek.cz/gallery/0/141-certifikace_pravidla_v2_1.pdf

Q-web služba je nabízena prostřednictvím partnerů IQNetu všem zákazníkům IQNetu, jako nový mezinárodně uznávaný postup uspokojující potřeby a požadavky všech, kteří se účastní internetové ekonomiky.[33]

Obr. 4. Základní princip QWeb

Základní princip	Moduly		jedna hvězda *	dvě hvězdy **	tři hvězdy ***
Q-web, certifikace elektronického obchodování je dostupná ve třech úrovních	Identifikace a obsah		●	●	●
	Ochrana osobních dat		●	●	●
	Bezpečnost IT	bezpečné placení	●	●	●
		proces audit (BS 7799)		●	●
		Certifikace ISMS (BS 7799)			●
	Kvalita obchodního procesu	systém řešení stížností	●	●	●
		procesní audit (ISO 9001)		●	●
		Certifikace systému managementu kvality (ISO 9001)			●
	Funkčnost a spolehlivost software			●	●
	Použitelnost (ISO 9241-10/ -11)				●

ISMS = Information Security Management Systém (Systém managementu pro zajištění bezpečnosti informací)

QMS = Quality Management Systém (Systém managementu kvality Q-web je jeden produkt, který má tři úrovně. Ty jsou zobrazeny na obrázku níže:

[33] http://www.iqnet-ltd.com/ a interní dokumenty ITC

Zákazník si může vybrat ze tří možných úrovní. Jsou zaměřeny na rozdílné typy elektronického obchodu a služeb.

Obr. 5. Moduly QWeb a příklady

MODUL	Příklad
jedna hvězda *	elektronický obchod nebo služba s relativně malým obratem (B2C a B2B)
dvě hvězdy **	elektronické obchodování s vyšším obratem (B2B) a s vyššími potřebami na bezpečnost aplikací (B2G, C2G) webovské aplikace, které jsou zřídka používány a mají malé požadavky na použitelnost (ASP)
tři hvězdy ***	aplikace elektronického obchodu s velmi vysokým obratem (B2B) nebo s velmi vysokými požadavky na bezpečnost (B2G, C2G) webovské aplikace, které jsou používány pravidelně a mají vysoké požadavky na použitelnosti (ASP)

Poznámka:

B2C = Business to Consumer – vztah: obchod-spotřebitel

B2B = Business to Business – vztah: obchod-obchod

B2G = Business to Government – vztah: obchod -vládní organizace

C2G = Citizens to Government – vztah: občané - vládní organizace

ASP = Application Service Providers – aplikace poskytovatelů internetových služeb

Zákon č. 412/2005 Sb.[34]. o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

[34] http://www.nbu.cz a www.rac.cz

Ochrana utajovaných informací je zajišťována komplexním systémem opatření personální, průmyslové, administrativní a fyzické bezpečnosti, bezpečností informačních nebo komunikačních systémů a kryptografické ochrany.

Způsobilost zabezpečit ochranu utajovaných informací je jednou ze základních podmínek získání osvědčení podnikatele, o které musí organizace (podnikatel) zažádat, pokud požaduje přístup k utajované informaci.

Podnikateli lze umožnit přístup k utajované informaci, jestliže jej nezbytně potřebuje k výkonu své činnosti a je držitelem platného osvědčení podnikatele příslušného stupně utajení.

Stručná charakteristiky oblastí ochrany utajovaných informací:

- personální bezpečnost (získání přístupu fyzické osoby k utajované informaci daného stupně utajení, při poučení, proškolení nebo kontrole plnění povinností fyzické osoby ze zákona.
- průmyslová bezpečnost (svědčení podnikatele dle §96 zákona – obsahuje: výčet utajovaných informací uložených u podnikatele, analýzu možného ohrožení utajovaných informací, vhodná a účinná ochranná opatření ke snížení rizik, způsoby realizace jednotlivých druhu zajištění ochrany utajovaných informací, časový harmonogram realizace bezpečnostní dokumentace a seznam funkcí a osob, u kterých se předpokládá přístup k utajovaným informacím
- administrativní bezpečnost (systém opatření pro tvorbu, příjem, evidenci a další manipulaci s utajovanou informací, včetně evidence a vedení administrativních pomůcek a dále naplnění povinností organizace vyplývajících ze zákona a vyhlášky č. 529/2005 Sb. o administrativní bezpečnosti)
- fyzická bezpečnost (projekt fyzické bezpečnosti - určení objektu a zabezpečených oblastí (ZO), včetně jejich hranic a určení kategorií a tříd ZO, vyhodnocení rizik, způsob použití opatření fyzické bezpečnosti, provozní řád objektu a plán zabezpečení objektu a zabezpečených oblastí v krizových situacích a povinnosti organizace vyplývajících ze zákona a vyhlášky č. 528/2005 Sb. o fyzické bezpečnosti.
- bezpečnost informačních systémů (IS) (certifikace IS, zapracování změn, schváleném do provozu, opakovaná certifikace IS)

- bezpečnost komunikačních systémů (KS) (schválení projektu bezpečnosti KS a/nebo jejich změn).[35]

- **GoodPriv@cy**

  Produkt Good Priv@cy je služba IQNetu pro hodnocení a certifikaci, která specifikuje požadavky na ochranu dat a bezpečnost informací.

  Značka Good Priv@cy umožňuje organizacím soukromého i veřejného sektoru objektivně doložit a komunikovat účinnost jejich systému ochrany dat tváří v tvář zákazníkům a vlastníkům. Je to cesta pro reprezentaci a ochranu dobrého jména.

  Požadavky systému Good Priv@cy

  Charakteristické aspekty zpracování dat:

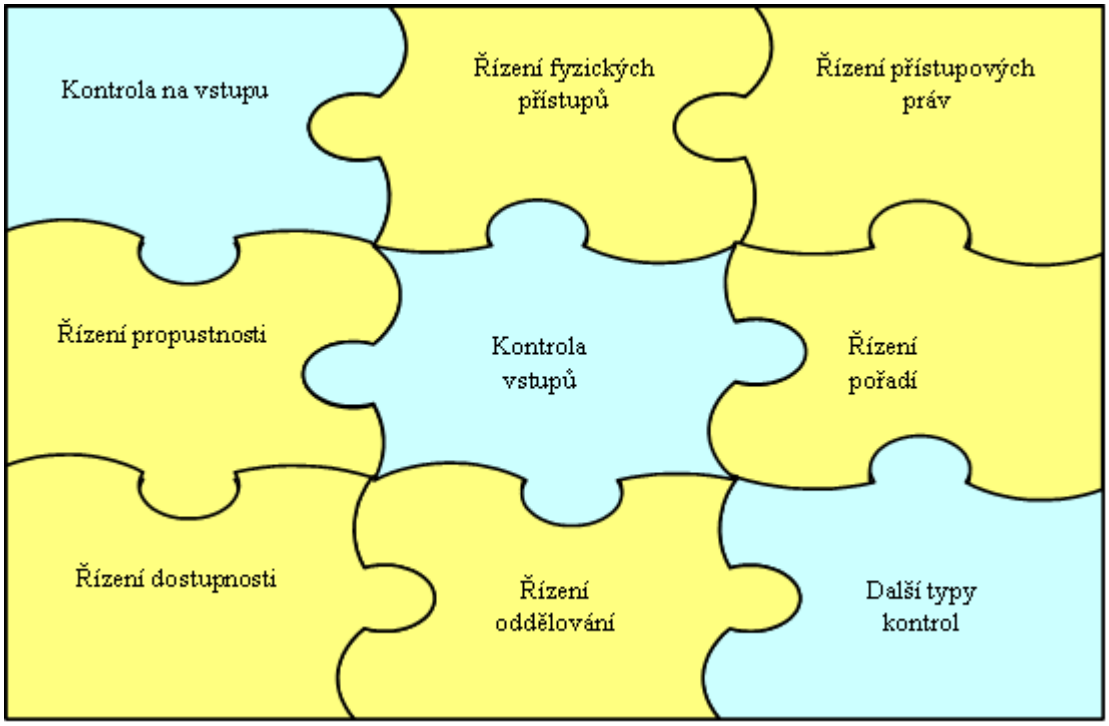
  - Vhodné metody zpracování dat
  - Zákonnost zpracování dat
  - Přesné plnění zadání
  - Regulované uchovávání a užívání dat

  Aspekty bezpečnosti informací:

  - Důvěrnost, integrita a autenticita osobních dat
  - 9 kontrolních mechanismů pro bezpečnost dat (viz obrázek)

[35] Zdroj informací: http://www.nbu.cz a www.rac.cz

Obr. 6. Kontrolní mechanismy pro bezpečnost dat



Požadavky, které musí být splněny k získání značky Good Priv@cy jsou následující:

- Formulovaná a implementovaná politika ochrany dat
- Provozuschopný a dokumentovaný systém řízení ochrany dat
- Shoda s právními nebo smluvními požadavky na ochranu dat
- Zajištění bezpečnosti informací vhodnými organizačními, personálními a technickými opatřeními
- Účinná kontrola a monitorování procesů
- Hodnocení a neustálé zlepšování ochrany dat a soukromí

Certifikace Good Priv@cy potvrzuje:

- že k osobním datům a bezpečnosti informací je přistupováno v souladu právními a ostatními předpisy

- neustálé zlepšování
- že systém řízení ochrany dat je kompletní (PLÁNUJ-DĚLEJ-KONTROLUJ-JEDNEJ), je pochopen a je účinný v celé organizaci.[36]

- **ISMS** - Information Sercurity Management System – Požadavky na ISMS jsou uvedeny v normě ISO/IEC 27001:2005. Stručný popis uvádí následující kapitola.

- **ITIL - Best practices**

  ITSM je zkratkou pro IT Service Management, (Řízení služeb informačních technologií). Obsah ITSM je definován následujícími britskými normami (vydanými British Standard Institute v roce 2000):

  - BS 15000-1:2002 - IT service management. Specification for service management
  - BS 15000-2:2003 - IT service management. Code of practice for service management

  Výše uvedené základní normy definující disciplínu ITSM a jsou dále doplněny dalšími dvěma předpisy:

  - BIP 0005:2004 – A Managers‘ Guide to Service Management
  - PD 0015:2002 – IT service management. Self-assessment workbook

Normy BS 15000 definují disciplínu ITSM velice obecně, zatímco ITIL® publikace tyto obecné normy blíže specifikují a popisují. ITIL® je zkratkou pro Information Technology Infrastructure Library, (knihovna infrastruktury informačních technologií). ITIL® vznikl jako sada knižních publikací popisujících způsob řízení IT služeb a ICT infrastruktury. ITIL® je zcela samostatným oborem činnosti a podnikání a zahrnuje v druhé verzi

[36] http://www.iqnet-ltd.com/ a interní dokumenty ITC

knihovnu čítající 8 svazků. V roce 2005 společnost OGC zahajuje projekt „ITIL Refresh“, jehož cílem je vývoj třetí verze knihovny ITIL, která je v roce 2007 vydána.[37]

ITIL® předkládá sadu osvědčených Best Practices z oblasti řízení služeb ICT, které, jsou-li implementovány, napomáhají dosažení kvality. ITIL® je rámec pro design procesů.

ČSN ISO/IEC 20000-1: 2006 a ČSN ISO/IEC 20000-2:2007

V těchto normách je popsán „Management služeb IT“. Normy se uplatní především v odběratelsko-dodavatelských vztazích. Jedná se o soubor technických norem, které vznikly na základě BS 15000-1 a BS 15000-2. Původní britské normy vymezily racionální a přesná pravidla pro plánování a realizaci služeb IT poskytovaných uživatelům (zákazníkům).

Norma ISO/IEC DIS 20000-1:2004 (ČSN ISO/IEC 20000-1:2006) stanovuje přesná kritéria pro organizace, dodávající služby IT v předem definované a přesně řízené kvalitě, plně akceptovatelné pro její zákazníky.

Norma ISO/IEC DIS 20000-2:2004 (ČSN ISO/IEC 20000-2:2007) poskytuje podrobný návod, jak zajistit nejlepší možnou službu IT (deklarovanou podle ISO/IEC 20000-1:2004), která je v souladu s podnikatelskými potřebami organizace v rámci odsouhlasených úrovní zdrojů, tj. službu, která je profesionální, efektivní z hlediska nákladů a s riziky, která jsou pochopena a řízena.

Normy předkládají srozumitelné požadavky umožňující objektivní ověření toho, že Best Practices byly skutečně aplikovány, tzn. umožňuje provedení nezávislé certifikace procesů řízení ICT služeb.[38]

---

[37] Zdroj: www.itil.cz a http://www.itil.org.uk

[38] Podrobné informace najdete na: http://www.bsi-global.com/

3.2 Informační bezpečnost podle ISO/IEC 27001:2006

„Systém je tak stabilní jako jeho nejslabší článek.“

Toto tvrzení se vztahuje na bezpečnost informací asi nejvíce. Proto je implementace ISMS (Information Sercurity Management System) logickým krokem ve snaze systémového pojetí řízení informační bezpečnosti. Požadavky pro ISMS jsou uvedeny v normě ISO/IEC 27001:2005 (ČSN ISO/IEC 27001:2006), která vycházejí z principu ISO 9001. ISMS klade důraz na přesné definování rizik poškození, zneužití a napadání informací společnosti. Za tímto účelem je vytvořen soubor pokynů (pravidel) napomáhajících efektivitě řízení a minimalizování potencionálních hrozeb. Navíc musí obsahovat soubor opatření k zajištění významných aktiv firmy (např. digitálních a tištěných informací, know-how, projektových metod).

Subjektům, které zpracovávají informace a data třetích stran, se doporučuje harmonizace ISMS s ISO 27001. Důvod je prostý, jedná se o snížení rizikových faktorů, mezi něž hlavně patří ať už vlastní, či bývalí pracovníci (nejrizikovější skupinou jsou správci IT a vývojáři) a zvenčí firmy se jedná např. o hackery, viry, informační „špionáž“, apod.

Původ standardu ISO/IEC 27001:2005 je v britských normách BS 7799. U nás ji známe jako ISO IEC 17799. Normy řady ISO/IEC 2700x mají pomoci k posílení bezpečnosti systémů zejména v oblasti ICT a jsou v souladu i s principy v praxi rozšířených standardů systémů řízení (jako ISO 9001 a ISO 14001). Stejně jako tyto standardy, tak i ISO 27001 v sobě zahrnuje management, politiku, organizaci i pravidelné přezkoumávání tedy principy tzv. PDCA (Plan – Do – Check – Act) modelu.[39]

[39] Standardy ISO/IEC 27001

Standardy ISO/IEC 2700x:

- ISO/IEC 27000:2009 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary
- ISO/IEC 27001:2005 Information technology -- Security techniques -- Information security management systems – Requirements
- ISO/IEC 27003:2010 Information technology -- Security techniques -- Information security management system implementation guidance
- ISO/IEC 27004:2009 Information technology -- Security techniques -- Information security management – Measurement
- ISO/IEC 27005:2008 Information technology -- Security techniques -- Information security risk management
- ISO/IEC 27006:2007 Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems

- ČSN ISO/IEC 27001:2006 - Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací – Požadavky
- ČSN ISO/IEC 27005:2009 - Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací
- ČSN ISO/IEC 27006:2008 - Informační technologie - Bezpečnostní techniky - Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací[40]

[40] Pozn. Celou rodinu norem, které mají souvislost s problematikou bezpečnosti informací obsahuje třída 36, skupina 97 českých technických norem. Viz. http://csnonline.unmz.cz/.

3.2.1 Struktura normy ČSN ISO/IEC 27001:2006 - Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací – Požadavky

4 Systém managementu bezpečnosti informací

4.1 Všeobecné požadavky

4.2 Ustavení a řízení ISMS

4.2.1 Ustavení ISMS

4.2.2 Zavádění a provozování ISMS

4.2.3 Monitorování a přezkoumání ISMS

4.2.4 Udržování a zlepšování ISMS

4.3 Požadavky na dokumentaci

4.3.1 Všeobecně

4.3.2 Řízení dokumentů

4.3.3 Řízení záznamů

5 Odpovědnost vedení

5.1 Závazek vedení

5.2 Řízení zdrojů

5.2.1 Zajištění zdrojů

5.2.2 Školení, informovanost a odborná způsobilost

6 Interní audity ISMS

7 Přezkoumání ISMS vedením organizace

7.1 Všeobecně

7.2 Vstup pro přezkoumání

7.3 Výstup z přezkoumání

8 Zlepšování ISMS

8.1 Neustálé zlepšování

A.10.8 Výměna informací

A.10.9 Služby elektronického obchodu

A.10.10 Monitorování

A.11 Řízení přístupu

A.11.1 Požadavky na řízení přístupu

A.11.2 Řízení přístupu uživatelů

A.11.3 Odpovědnosti uživatelů

A.11.4 Řízení přístupu k síti

A.11.5 Řízení přístupu k operačnímu systému

A.11.6 Řízení přístupu k aplikacím a informacím

A.11.7 Mobilní výpočetní zařízení a práce na dálku

A.12 Akvizice, vývoj a údržba informačních systémů

A.12.1 Bezpečnostní požadavky informačních systémů

A.12.2 Správné zpracování v aplikacích

A.12.3 Kryptografická opatření

A.12.4 Bezpečnost systémových souborů

A.12.5 Bezpečnost procesů vývoje a podpory

A.12.6 Řízení technických zranitelností

A.13 Zvládání bezpečnostních incidentů

A.13.1 Hlášení bezpečnostních událostí a slabin

A.13.2 Zvládání bezpečnostních incidentů a kroky k nápravě

A.14 Řízení kontinuity činností organizace

A.14.1 Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací

A.15 Soulad s požadavky

A.15.1 Soulad s právními normami

A.15.2 Soulad s bezpečnostními politikami, normami a technická shoda

A.15.3 Hlediska auditu informačních systémů

V rámci zavádění ISMS podle normy ČSN ISO/IEC 27001:2006 je nutno popsat způsob realizace požadavků jednotlivých kapitol normy a její přílohy. Pokud to norma umožňuje lze aplikovat vyloučení některých požadavků. Aplikovaná vyloučení musí být v dokumentaci ISMS zdůvodněna.

3.2.2 Zabezpečení informací a jejich klasifikace

Základní charakteristiky zabezpečení informací jsou důvěrnost, integrita a dostupnost.[41]

- *Důvěrnost* – prevence proti neoprávněnému užití informace
- *Integrita* – prevence proti neautorizované modifikaci informace
- *Dostupnost* – prevence proti znemožnění neoprávněného použití informace a současně zajištění včasné a úplné informace oprávněnému uživateli.

Klasifikace informací je důležitá proto, aby se zajistila jejich dostatečná ochrana, a to ve všech formách, ve kterých se vyskytují ve firmě. Na základě předešlého rozdělení se jednotlivé body dále dělí na třídy:[42]

Důvěrnost:

- *Třída veřejných informací* (tvoří zhruba 10% informací) – nevyžaduje zvlášntní ochranu, slouží ke zveřejnění (reklama, výroční zprávy, informace z tisku, webu, apod.)

[41] MLÝNEK(2007). str. 5.

[42] MLÝNEK(2007). str. 52, str. 53, str. 54, str. 55.

- *Třída informací pro vnitřní potřebu* (80% informací) – interní informace, které je nutné chránit a poskytnuty externě mohou být za předpokladu mlčenlivosti (údaje o klientech, zaměstnancích, audity, aj.)
- *Třída informací omezeného užití* (cca 10% informací společnosti) – velmi důvěrné, mohou ohrozit, poškodit až způsobit likvidaci firmy. Přístup je co nejvíce omezován (strategické, finanční, marketingové plány, havarijní a bezpečnostní plány, kryptografické klíče)

Integrita:

- *Třída informací autentických* – důležité zaručení zdroje (příkaz k transakci, nastavení přístupu, apod.)
- *Třída informací cenných* – nutná celistvost a neporušenost obsahu. Jsou nosičem hodnoty a nutné pro rozhodování (kurzovní lístek, zápis z jednání)
- *Třída informací ostatních* – monitoring tisku, možnost podnikové rekreace

Dostupnosti:

- *Třída informací kritických* – dělí se dle dostupnosti na částečnou (15 min.) a úplnou (3 hodiny). Patří sem obchodování na internetu, transakce, apod.
- *Třída informací prioritních* – částečná dostupnost (1 den), úplná (1 týden). Informace o klientech, mzdách zaměstnanců
- *Třída informací potřebných* – částečná dostupnost (1 týden), úplná (2 měsíce). Zahrnuje evidenci majetku, nabídka rekreace

3.2.3 Data a informace

- *Data* – formalizovaná reprezentace skutečností, pojmů či údajů, které vznikají, jsou uchovávány a zpracovávány v rámci výkonu činnosti společnosti nebo v přímé

souvislosti s ní tak, aby bylo možné jejich zpřístupňování, interpretace či zpracování lidmi nebo automatizovanými prostředky.[43]

- *Informace* – data, jejichž obsah je srozumitelný lidem. Jsou nejdůležitější aktiva IS (Informační systém)[44]. Jedná se o texty, číselné údaje, e-mailové zprávy, počítačové soubory apod.

Nacházíme se v době, která vyniká svou rychlostí a neustálým pokrokem. K tomu, aby firma byla úspěšná na trhu je také důležité to, jak nakládá s informacemi a daty. Nejenže stát skrze svoji legislativu určuje adekvátní správu informací (např. Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých předpisů), ale jsou to také závazky společnosti, které plynou z podmínek ve smlouvách. Nadto se jedná také o interní obchodní zájmy (např. „konw – how“).

Obecně můžeme říci, že ve firmě se nachází informace[45]:

- *Interní*, o společnosti (její záměry a plány)
- *Know-how*, které je nedostupné konkurenci
- *Zaměstnanci* společnosti
- *Databázové*, a to o klientech a jiných kooperujících subjektech
- *Volně* dostupné (odborné publikace, tisk, internet)

3.2.4 Přehled zákonů a vyhlášek, které lze aplikovat pro oblast bezpečnosti informací

Právo v Česku upravující ochranu spotřebitele vychází z občanského zákoníku a ze zákona na ochranu spotřebitele. Koncepci spotřebitelské politiky stanovuje ministerstvo průmyslu a obchodu.

---

[43] MLÝNEK(2007). str. 6.

[44] MLÝNEK(2007). str. 7.

[45] MLÝNEK(2007). str. 5.

Informace jsou právně upravovány a chráněny:

- Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů;
- Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů;
- Zákon č. 227/2000 Sb., o elektronickém podpisu, ve znění pozdějších předpisů;
- Zákon č. 499/2004 Sb., o archivnictví a spisové službě
- Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů
- Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti
- Zákon č. 227/2000 Sb., o elektronickém podpisu v aktuálním znění
- Zákon č. 513/1991 Sb., obchodní zákoník. Řeší otázku obchodního tajemství
- Zákon č. 365/2000 Sb., o informačních systémech veřejné správy

V kapitole 3. jsou uvedeny výsledky provedené literární rešerše, které dávají východisko pro realizaci praktické části DP v podmínkách praxe.

II. PRAKTICKÁ ČÁST

4 ANALÝZA AKTUÁLNÍHO STAVU ŘÍZENÍ VE FIRMĚ

4.1 Představení firmy English Editorial Services, s.r.o.

Motto:

„Vaše sdělení je důležité.

Dojem, který zanecháte, je nesmírně cenný.

Vy víte, co chcete sdělit.

My vám to pomůžeme vyjádřit.“46

Historie:

English Editorial Services, s. r. o. se sídlem v Brně a vedená v obchodním rejstříku u Krajského soudu v Brně, byla založena v roce 2003. Zakladatelem je bývalý novinář (deset let v rodných Spojených státech), finanční analytik a manažer s praxí v různých zemích světa (od roku 1992 vedl týmy investičních analytiků jak u nás, tak na Ukrajině) Gale A. Kirking, CFA, MBA.

Od svého založení se společnost progresivně vyvíjí a do budoucna se uvažuje o růstu, co do počtu zaměstnanců.

Poslání:

Pomoci klientům s konečnou úpravou dokumentů tak, aby byl jasně, správně a účinně vyjádřen jejich záměr.

[46] Your message is important. Your image is precious. You know what to communicate. We help you to say it.

Portfolia služeb:

Firma poskytuje nejen redakční a překladatelské služby, ale také zajišťuje celou škálu prací, které souvisejí s publikováním dokumentů:

- copywriting, redigování, korektura, překlady, lokalizace, grafický design, DTP, předtiskovou přípravu, projektové úkoly

Klienti společnosti:

Hlavní oblast zakázek pochází z finančího sektoru (banky, obchodníci s cennými papíry, správci fondů, společnosti působící v oblasti firemních financí). Služby jsou založeny na naprosté diskrétnosti. Do dalších oblastí spadá:

- Firemní a marketingová komunikace
- Právo
- IT
- Telekomunikace
- Státní správa
- Zahraniční obchod
- Life sciences (vědci a akademičtí pracovníci)

Organizační struktura:

Nejedná se o velkou společnost. Hierarchie zde je velmi jasná a zřetelná. Společnost tvoří 5 (a 2 externí) pracovníků, z čehož 3 jsou v managementu a zastávají také funkce tomu odpovídající. Zbývající 2 (a 2 externí dodavatelé) jsou řadoví zaměstnanci.

4.2 Analýzy stavu řízení ve firmě

4.2.1 SWOT analýza společnosti

Silné stránky

- tým vysoce kvalifikovaných pracovníků s dlouholetou praxí (hlavní editor má 30 let praxe s editací odborných textů)
- Znalosti z široké škály oblastí a schopnost je precizně zpracovat (od finanční po vědeckou)
- poskytování balíčků služeb (překlad, DTP, tisk, rozesílka) a koordinace mezinárodních projektů i v malém týmu
- dodržení termínů zakázek a jejich doručení i mimo pracovní dny
- možnost otevření kreditu klientem, který následně čerpá
- asistence a pomoc klientům při hledání vhodného časopisu k publikaci jejich rukopisů (v ČR i v zahraničí)
- finální revize hlavním editorem před předáním každé zakázky klientovi je samozřejmostí
- údaje o klientech (jméno) poskytujeme třetím osobám pouze se souhlasem daného klienta
- zneužití informací o klientech ze stran interních pracovníků ošetřeno smluvně pod pokutou
- vývoj vlastního slovníku
- veškerá data (zakázky klientů a informace o nich) jsou denně zálohovaná
- férovost ke klientům (kalkulace normostran za překlad vychází z původního textu, který bývá obecně kratší, při editaci se počítá skutečný čas práce)
- nepotřebné tištěné materiály jsou před vyhozením zkratovány

Slabé stránky

- Sídlo firmy v rodinném domě
- Externí DTP pracovník
- Základní zabezpečení firmy
- Neschopnost zajistit (ihned) každou zakázku z kapacitních důvodů
- Cena (pevně stanovená) na základě poskytovaných služeb a firemní klientely
- Uložení hlavního serveru
- Malá propagace firmy (pouze vlastní aktivitou a „Word of mouth“)

Příležitosti

- spolupráce s vydavatelstvími
- větší angažovanost před rozdělováním grantů na akademické půdě
- rozšíření služeb o další jazyk(y)
- efektivnější zpracování legalizovaných dokumentů (interní pracovník)
- prohloubení spolupráce se zahraničními klienty
- získání dlouhodobé spolupráce se státním sektorem
- noví pracovníci
- účast firmy na vědeckých a jiných odborných konferencích

Hrozby

- počítačové víry, piráti
- ztráta hardware při manipulaci s ním
- zneužití dat interními pracovníky
- ztráta kvalifikovaného a vyškoleného zaměstnance

4.2.2 Analýzy stavu řízení ve firmě k požadavkům normy ISO 9001

Pro analyzování současného stavu řízení firmy jsem zvolila metodu checklistů, a to proto, abych zjistila, jak firma splňuje požadavky daných norem. Tyto checklisty se vztahují k normám ISO 9001a ISO 27001. Normu ISO 9001 jsem použila jako základní a normu ISO 27001 jsem k ní přiřadila pro srovnání. Mojí snahou bylo zjistit, které požadavky normy již firma naplňuje, a v čem se současný management s požadavky norem rozchází.

Norma ISO 9001 Všeobecné požadavky (kap. normy 4)

K tomu, aby řízení společnosti bylo efektivní, měly by být identifikovány firemní procesy a jednotlivé vazby mezi nimi. Pro tento účel je také důležité nejen jejich správné řízení, ale také dokumentace, která nám usnadní a zajistí lepší orientaci v propojenosti procesů a jejich posloupnosti, určení vstupního zdroje (ať už interního nebo externího) a v neposlední řadě monitoring a následné analyzování stavu ve společnosti jako prvku významného pro zlepšování.

Současný stav ve společnosti English Editorial Services, s. r. o. – ISO 9001

Firma jako taková ISO ani jinou certifikaci nemá, nicméně se snaží dodržovat zásady správné evidence požadavků klientů. Určení firemních procesů není formálně upraveno. Dokumentace nových zakázek se uskutečňuje na několika místech, a to nejprve do knihy zakázky, kde se fyzicky zapíše, poté se uvede do elektronické podoby do souboru přehledu zakázek. Druhy zakázky jsou rozlišeny na vědecké a ostatní, u každé zakázky se vždy přesně eviduje: *název instituce, či jméno firmy* (respektive fyzické osoby), *jméno zadavatele zakázky, označení zakázky, datum obdržení, vyhotovení a odeslání, druh vyžadované služby, rozsah zakázky, dvojí evidenční číslo zakázky přiděleno odpovědnou osobou ve firmě:*

- nejprve se vyplní předtištěný formulář, tzv. *evidenční list* zakázky
- zakázka je zavedena do evidenčního systému v PC
- zakázka spolu s evidenčním listem je předána překladateli, který ho po jejím zpracování odevzdá specialistovi péče o zákazníky.

Velmi důležitá je skutečnost, že tento evidenční systém urychluje a zpřehledňuje práci na zakázkách a zároveň umožňuje stanovení priorit. Toto firma ocení zejména v době, kdy má zpracovat velké množství objednávek v krátkém časovém horizontu.

Při dokončení zakázky a její předání klientovi se daný klient kontaktuje (telefonicky nebo e-mailem), aby se zjistilo, zdali a jak byl s danou prací spokojen (zpětná vazba hraje roli v budování dobrého vztahu s klientem). V případě, že klient měl výhrady, tak se toto zapíše pod jeho číslo zakázky pro případ budoucích potřeb.

Služby společnosti jsou popsány v její nabídce, která je dostupná na jejích webových stránkách. Zde ovšem není uveden ceník, ten je přístupný pouze interně. Ocenění zakázek probíhá až po jejich zaslání firmě, a to proto, že dříve ji firma není schopna určit. Je to z toho důvodu, že něco se může účtovat dle hodin (času). V tom případě se jedná o předběžný odhad. Vytvoří se cenová kalkulace (a to na základě jak dané zakázky, tak také dohody s klientem a jeho požadavcích), která se posléze zašle zájemci k odsouhlasení. Tvorba kalkulace se klientovi neúčtuje, jedná se o naši nabídku.

Zásady jednání s klientem nejsou písemně formulovány, ale vycházejí z obecných pravidel jako je slušné, asertivní jednání, vstřícnost, ochota pomoci.

Neshody s normou:

I přes současná opatření nejsou procesy ve firmě přesně definovány a popsány. Chybí prohlášení o politice kvality a příručka kvality, nejsou přesně stanoveny cíle organizace a dokumentované postupy. Můžeme říci, že firma provádí svoji činnost na základě zkušeností a hlavně požadavků svých klientů, kterým se snaží maximálně přizpůsobit a uspokojit jejich potřeby. Uvedení odpovědnosti není příliš jasné a občas způsobuje chaos. Obecné povědomí zaměstnanců o postupech, jak jednat s klienty, a jak dokumentovat zakázky by mohlo být prohloubeno, ve firmě je aplikováno řízení založené na zvyklostech pracovníků vrcholového vedení. Definování náležitostí procesního řízení je pouze částečné a opět výhradně slovní. Zajišťování procesů pomocí externích zdrojů je evidováno, ale i zde by tento postup mohl být zlepšen. Společnost není schopna plně zaručit, že tyto (externí) procesy jsou řízeny odpovídajícím způsobem.

Možná opatření:

Jasnější identifikace procesů, a to nejen pro odpovědného pracovníka, ale celý pracovní tým. Dále je nutná zavedení systematického monitoringu nebo měření procesů a tvorba

analýz sloužících k následnému zlepšování. Měla by být vytvořena a soustavně řízena náležitá dokumentace včetně příručky kvality. Nevyhnutelné bude také provedení školení zaměstnanců, aby se rozšířilo jejich povědomí o podnikových procesech a jejich náležitostech. Jelikož se firma snaží o dodržování vlastních zásad kvality, které nejsou však nikde oficiálně písemně deklarovány, bylo by jistě dobré tyto zásady seskupit také do psané podoby.

Odpovědnost managementu (kap. normy 5):

Neshoda s normou:

Rozpor je zde v tom, že firma sice deklaruje, že vedení vychází a naplňuje požadavky zákazníka, ale příslušná dokumentace o tomto je nedostačující. Není stanovena odpovědná osoba za kvalitu a způsob jejího sledování ani se neprovádí systematická kontrola plnění úkolů a evidence o ní. Firma jako taková nemá formalizovanou politiku kvality a sledování kvality jako takové neprobíhá jen částečně.

Možná opatření:

Stanovení odpovědné osoby za kvalitu, vymezení odpovědností a pravomocí při interní komunikaci. Důrazné zapojení majitele firmy do implementace systému kvality do života organizace a jeho následný rozvoj. Neméně důležitá je také interní komunikace, která by měla být také vymezena a definovány její způsoby. Jelikož se jedná o velmi malou firmu, tak by komunikace měla být jasná a přímo směřovaná.

Zajištění zdrojů (kap. normy 6):

Firma požaduje od svých zaměstnanců určitou kvalifikovanost pro výkon dané práce a má na ně stanoveny minimální požadavky. V této souvislosti také o nich udržuje odpovídající záznamy (o školení, vzdělání, kvalifikaci, aj.). Snaží se také o rozvoj a zvyšování kvalifikace svých zaměstnanců (různá překladatelská školení, grafická, aj.) prostřednictvím plánu výcviku. Pro zajištění provozu má firma k dispozici potřebné technické vybavení, které prochází pravidelnými měsíčními kontrolami. Přístup zaměstnanců k potřebným informacím a jejich ochrana proti zneužití je definována.

Neshoda s normou:

Plánovité zajištění zdrojů pro systém kvality se neprovádí. Nejsou přesně identifikování zaměstnanci, kteří mohou ovlivnit kvalitu. I přes to, že firma podporuje vzdělávání svých zaměstnanců, tak záznamy o školeních, se sice provádějí, ale jsou vedeny jen velmi obecně. Není také sestaven a propracován celkový přehled školení, která byla již realizována a těch plánovaných. Analýza pracovního prostředí z hlediska normy se neprovádí.

Možná opatření:

Tvorba dokumentu, který bude jasně a přehledně definovat způsob řízení a plán rozvoje zaměstnanců. Také je nutné vytvořit dokument, obsahující podobu pracoviště (jak z pohledu bezpečnosti, tak ergonomie).

Realizace produktu (kap. normy 7):

- *Procesy týkající se realizace produktu* – snahou firmy je poskytovat a zajistit vysoce kvalitní produkt a tím dosáhnout spokojenosti zákazníka. Důležitou roli zde hraje kontrola hlavním editorem, který před zasláním překladu, ale také v jeho průběhu dohlíží na to, aby úroveň jazyka byla co nevyšší. Žádná zakázka neopustí kancelář, aniž by nebyla jím revidována. Tento postup není však zdokumentován ani jinak zaznamenán.
- *Procesy vztahující se k zákazníkovi* – snahou organizace je zajistit, aby výsledný produkt byl v souladu s požadavky zákazníka. Dále také dodržení časového rámce na zpracování zakázky, pokud není schopna dodat produkt včas nebo v požadované kvalitě, ihned klienta informuje a navrhne relevantní řešení. Snahou je toto vyřešit ještě před začátkem práce na zakázce. Jak již bylo zmíněno, každá zakázka má svůj evidenční list obsahující veškeré důležité náležitosti pro její zpracování. I zde se jedná o postupy, které jsou obecně zaužívané pro všechny zaměstnance, ale jejich dokumentace (která by popisovala přesný postup) schází.
- *Komunikace se zákazníkem* – na komunikaci se zákazníky je ustanoven pracovník, který řeší veškeré záležitosti týkající se zakázek, spokojenosti, stížností, smluv, změn, atd. Tento pracovník udržuje spojení s klienty prostřednictvím e-mailu, ale hlavně

telefonicky, a to proto, že je to osobnější a rychlejší. Zákazníci toto vítají hlavně proto, že mnohdy je pro ně snažíš domluvit náležitosti zakázky ústně. Upevňuje to také vztahy se zákazníky z pohledu marketingu. Dokumentace, která by stanovila, jak se zákazníky jednat nebyla však doposud vytvořena.

- *Vztahy s dodavateli* – jsou známi klíčoví dodavatelé, se kterými společnost spolupracuje. Jedná se však o velmi málo zakázek. Organizace spolupráce se uskutečňuje přes specialistu péče o zákazníky do jehož kompetence toto také patří. Jejich hodnocení se vůbec neprovádí a není ani zavedena žádná dokumentace.
- *Realizace výroby a služby* – již bylo řečeno, že se každá zakázka dokumentuje, a tento evidenční list je její součástí až do doby, než je vyfakturována. Nejen že daný list obsahuje podstatné náležitosti zakázky, ale také její jednoznačnou identifikovatelnost. Tento postup je však realizován fyzicky, nikoli dokumentován. Pokud při zpracování zakázky vzniknou nesrovnalosti, ihned se řeší, buď v rámci firmy, nebo přímo s klientem. Toto se však nikde nedokumentuje. Není poté možné provést analýzu problému.

Měření, statistické metody, analýzy a zlepšování (kap. normy 8):

Měřidla jako taková se ve firmě nepoužívají, interní audity neprobíhají, probíhající procesy se neměří. Spokojenost zákazníků se odhaduje nejen na jejich opakovaných zakázkách, ale také po každé předané zakázce se daný klient kontaktuje telefonicky, aby se zjistila zpětná vazba, případně odstranily nesrovnalosti. V průběhu práce na zakázce v případě nutnosti probíhají diskuse mezi překladateli a hlavním editorem, aby se případné nedostatky odstranily již během procesu překladu. Před zasláním konečného překlad hlavní editor provede závěrečnou revizi, případně doladění. Neprobíhá zde žádné řízení neshodných produktů. Řízení neshodných produktů se neprovádí, a tudíž nemůže být provedena analýza. Ani zde není dostatečná dokumentace, která by identifikovala jednotlivé kroky. Snaha o zlepšení produktu se uskutečňuje pomocí dodatečných služeb (zpracování zakázky i přes víkend; možnost otevření kreditu a jeho následného čerpání; hledání periodik, kde by případný rukopis mohl být vydán; kontaktování zahraničních institucí a vydavatelství; aj.).

Neshoda s normou:

Také zde schází dokumentované postupy a některé procesy ve firmě vůbec neprobíhají. Dostatečně se nevedou a nedokumentují informace o produktech nesplňujících požadavky a následkem toho je neschopnost provedení analýzy a zjištění jejich příčin.

Možná opatření:

Vytvoření dokumentace a směrnic, dle kterých by se dalo postupovat při řešení postupů vedoucích k zlepšování.

4.2.3 Analýzy stavu řízení ve firmě k požadavkům normy ISO 27001

Norma ISO 27001: Všeobecné požadavky (kap. normy 4)

Současný stav:

Situace ve firmě týkající se zajištění bezpečnosti informací je ošetřena pouze velmi jednoduše. Zaměstnanci firmy mají zakázáno hovořit o klientech s jinými zákazníky. Je dovoleno sdělovat pouze sektor, ve kterém se daný subjekt pohybuje. Mlčenlivost je ošetřena smluvně pod pokutou. Další zabezpečení je pomocí šifrování, které se ke komunikaci s některými klienty používá. Dokumenty v papírové podobě se ukládají pouze po dobu nezbytně nutnou a poté se skartují. K ochraně počítačů se používá antivirový program v aktuální verzi (zaplacena licence). Veškerá data, a to nejen o klientech, se zálohují a daný nosič je ukládán na určené místo. Veškeré smluvní dokumenty jsou uschovány v uzamykatelných skříňkách. Je zavedena klíčová politika.

Přístup zaměstnanců do adresářů datového úložiště je prováděn řízením přístupů.

Přístup na internet není omezen z důvodu použití tohoto nástroje při hledání informací nutných pro práci. Umístění kanceláří se nachází v rodinném objektu.

Neshoda s normou:

Řízení, ustavení a politika ISMS se ve firmě vůbec neprovádí dle požadavků normy. Totéž se vztahuje také k implementaci, monitorování, přezkoumávání udržování a zlepšování ISMS. Patřičná dokumentace zde také není nebo je pouze částečná. Rizika a plánování jejich zvládání se rovněž neprovádí. Náležitosti kladené ve všeobecných požadavcích normy, firma nesplňuje vůbec.

Možnosti nápravy:

Zdokumentované postupy zavedení, monitorování a přezkoumání ISMS a jeho následná udržování a zlepšování. Dokumentovaný postup při identifikování a analýze rizik, jejich zvládání. Zde vedení firmy navrhuji využití externí firmy, která by se zavedením mohla firmě pomoci, a také proškolení pracovníka(ů), který by měl toto posléze v kompetenci.

Odpovědnost vedení, interní audity, přezkoumání a zlepšování ISMS (kap. normy 5, 6, 7, 8):

Závazek vedení se provádí pouze částečně. Informovanost pracovníků, jejich školení se v této oblasti téměř vůbec neprovádí. ISMS není vůbec ve firmě propracován ani nijak zlepšován, o čemž svědčí také odpovědi v checklistech. Preventivní opatření se provádí pouze částečně nebo vůbec s nedostatečnou dokumentací.

Možná opatření:

Proškolení pracovníků, zavedení procedury do praxe firmy.

Cíle opatření a jednotlivá bezpečnostní opatření (příloha A normy ISO 27001)

Bezpečnostní politika, organizace bezpečnosti informací (příloha normy A.5):

Dokumentace je pouze částečná, přezkoumání bezpečnosti politiky informací se neprovádí, koordinace bezpečnosti je opět neúplná. Přidělení odpovědností je nejasné. Pravidla o ochraně důvěrných informací jsou vytvářeny částečně.

Externí subjekty, identifikace rizik plynoucích z jejich přístupů (příloha normy A.6):

Uzavírání dohod se třetí stranou, které také obsahují bezpečnostní požadavky, se provádí jen částečně nebo vůbec.

Možná opatření:

Proškolení pracovníků, zavedení a řádné zpracovávání interní dokumentace vztahující se k tomuto tématu.

Řízení aktiv (příloha normy A.7):

Evidence aktiv se provádí pouze částečně a z hlediska vlastnictví se neprovádí vůbec. Doporučení pro klasifikaci informací se neaplikuje vůbec a označování a nakládání s informacemi je prováděno pouze částečně.

Aktiva hrají důležitou roli při zavádění ISMS, a to proto, že je nutné jejich ocenění z hlediska hrozeb a rizik. Proto by se jejich evidence měla vést velmi zodpovědně a pokud možno přesně dokumentovat jejich cyklus ve firmě.

Bezpečnost lidských zdrojů (příloha normy A.8):

- *Před zahájením pracovního procesu*– role, odpovědnosti, prověřování a ověřování podmínek pracovní činnosti se provádí pouze částečně. Dokumentace není kompletní.
- *Během pracovního procesu* – vedoucí pracovníci a jejich odpovědnosti za ISMS jsou zmíněny v interních dokumentech pouze okrajově. Odborné vzdělávání v této oblasti (bezpečnosti informací) se provádí jen výjimečně a v nezbytně nutných případech. Dokumentace je většinou velmi obecná a nepřesná.
- *Po skončení pracovního poměru* – v případě užívání firemních prostředků je povinován tyto navrátit zpět společnosti, což je ošetřeno smluvně. Danému pracovníkovi je zrušen e-mail a přístupová hesla. Interní dokumentace postupů při odchodu zaměstnance z firmy není předem dána.

Fyzická bezpečnost, bezpečnost prostředí a zařízení (příloha normy A.9):

Zabezpečení objektu je jednoduché. Každý zaměstnanec vlastní klíč k dané nemovitosti a při vstupu se dostane přímo do kanceláří. Osobní prohlídky se zde neprovádějí. Kanceláře jsou otevřené, a tudíž neustále přístupné. Je zde omezený počet skříní, které se dají uzamknout. Zbylé jsou neustále přístupné. Umístění kancelářského vybavení a jeho ochrana je neodpovídající. Kabeláž je volně přístupná a není zabezpečená. Hlavní server je nevhodně umístěn. Servis zařízení je prováděn odborným zaměstnancem naší dodavatelské firmy.

Dokumentace zařízení se provádí jen částečně a měla by se dokompletovat. Informace o výměnách přístrojů nebo jejich opravy nejsou evidovány nebo jen částečně. Nebyl ani vytvořen dokument, který by takový postup popsal.

Řízení komunikací a řízení provozu (příloha normy A.10):

Provozní procesy jsou dokumentovány pouze částečně a řízení změn se neprovádí vůbec. Přezkoumání služeb třetích stran se uskutečňuje také jen částečně. Dokumentace popisující ochranu proti škodlivým virům a mobilním kódům se nevytváří vůbec.

Zálohování se provádí a správa výměnných počítačových médií je prováděna. Ani o jednom procesu se však nevede detailní záznam. Postupy při výměně informací se provádí jen částečné, služby elektronického obchodu se nevyužívají vůbec.

Řízení přístupů (příloha normy A.11):

Politika řízení přístupů se provádí jen zčásti, a to pomocí uživatelských práv. Registrace uživatelů a používání hesel se provádí, ale příslušná dokumentace nebyla vytvořena. Pravidlo prázdného stolu je zaměstnancům obecně známo, ale nedodržuje se. Veškeré správa sítí je ošetřena externí firmou.

Oddělení citlivých systémů se neprovádí vůbec (pouze jsou omezena přístupová práva uživatelů) a stejně tak práce na dálku. Neexistuje dokumentace, která by toto ošetřovala nebo objasňovala.

Akvizice, vývoj a údržba informačních systémů (příloha normy A.12):

Ve firmě se neprovádí vůbec nebo jen částečně a opět schází potřebná dokumentace. Řízení, správa a kontrola technických zranitelností se provádí částečně externí firmou. Dokumentace vedena nedostatečně.

Zvládání bezpečnostních incidentů (příloha normy A.13):

Jsou obecně známy postupy a odpovědnosti, jak v daných situacích jednat, ale písemně stanovené normy neexistují. Shromažďování důkazů se provádí jen částečné, a to proto, že není zaměstnancům firmy přesně známo, co a jak by se mělo evidovat. Potřebná dokumentace není.

Řízení kontinuity činnosti organizace (příloha normy A.14):

Dodržují se nepsaná pravidla, která však v souladu s normou nejsou. Z hlediska normy se tento bod vůbec neprovádí a ani není dokumentován.

Soulad s požadavky, soulad s právním normami (příloha normy A.15):

Firma dodržuje ochranu duševního vlastnictví a svých interních záznamů, není však přesně stanoveno a dokumentováno, jak se toto má provádět a dodržovat, čímž může vznikat rozpor v chápání daných požadavků mezi zaměstnanci firmy. Ochrana dat a soukromých informací se neprovádí nebo jen omezeně a patřičná dokumentace nebyla vytvořena. Preventivní opatření, která by měla zabránit případnému zneužití prostředků pro zpracování informací se také neprovádí (kromě opět přístupových práv uživatelů a AVG).

Firma se s požadavky normy a bezpečnostními politikami shoduje jen omezeně a spíše se rozchází.

4.3 Zhodnocení výsledku analýzy a návrh východiska pro zlepšení situace

Po vyhodnocení checklistů a jejich následné analýze vztahující se k požadavkům normy ISO 9001 a ISO 27001 lze konstatovat, že:

- Zájmem firmy je dodržovat kvalitu a zlepšovat její služby, ale toto probíhá v mnoha oblastech v rozporu s požadavky norem ISO 9001 a ISO 27001 (chybí patřičná dokumentace).
- Definice procesů ve firmě není dostačující.
- Pravomoci a odpovědnosti pracovníků nejsou jednoznačně stanoveny.
- Informace o dodavatelích nejsou dostatečně dokumentovány, a tudíž schází údaje pro jejich hodnocení.
- Zaměstnanci firmy a také vedení se při vyplňování checklistů v některých bodech neshodovali, což bylo hlavně nedostatečnou znalostí dotazované problematiky.
- Standardizované postupy a vhodná dokumentace až na drobné výjimky je zpracována přiměřeně s možností vylepšení. Záznamy o činnostech ve firmě se nevytvářejí v normou požadovaném rozsahu a záznamy se neudržují, a proto chybí podklady pro analyzování a vyhodnocení příčin a následků.
- Aplikovaná bezpečnostní opatření jsou v současnosti vyhovující jen do jisté míry.

- Z výše uvedené analýzy je nutno konstatovat, že v současnosti firma nemá dostatečné personální zdroje, pomocí kterých by byla schopna sama zavést všechny požadavky norem ISO 9001 a ISO 27001 do praxe.

4.3.1 Návrh metodiky analýzy rizik pro firmu English Editorial Services, s.r.o.

Analýzu rizik lze provádět několika způsoby:

Hrubá úroveň

- bere v úvahu hodnotu systému IT z pohledu činnosti společnosti
- odpovídá na otázku, který přístup je pro který systém IT vhodný
- základní rozdělení nám pomůže k zjištění, které systémy jsou vhodné a u kterých je nutné provést podrobnou analýzu

Neformální přístup

- nejedná se o strukturované metody, ale o využití zkušeností jednotlivců
- k analýze není potřeba nových dovedností, je provedena rychle
- vzniká zde však nebezpečí opomenutí některých důležitých detailů

Kombinovaný přístup

- jedná se o kombinaci nejlepších charakteristik možností s minimalizací času a úsilí
- provede se počáteční analýza rizik na hrubé úrovni a u systému IT identifikovaných jako významné nebo vystaveny vysokým rizikům by měla být provedena podrobná analýza

Podrobný přístup

- analýza se skládá z identifikace souvisejících rizik a odhadem jejich velikosti
- zkoumá se atraktivita aktiva pro útočníka, výskyt hrozeb a snadnost, se kterou mohou být zranitelnosti využity

Další možný přístup

- provedení analýzy rizik pomocí specializovaného programu (např. CRAMM)[47]

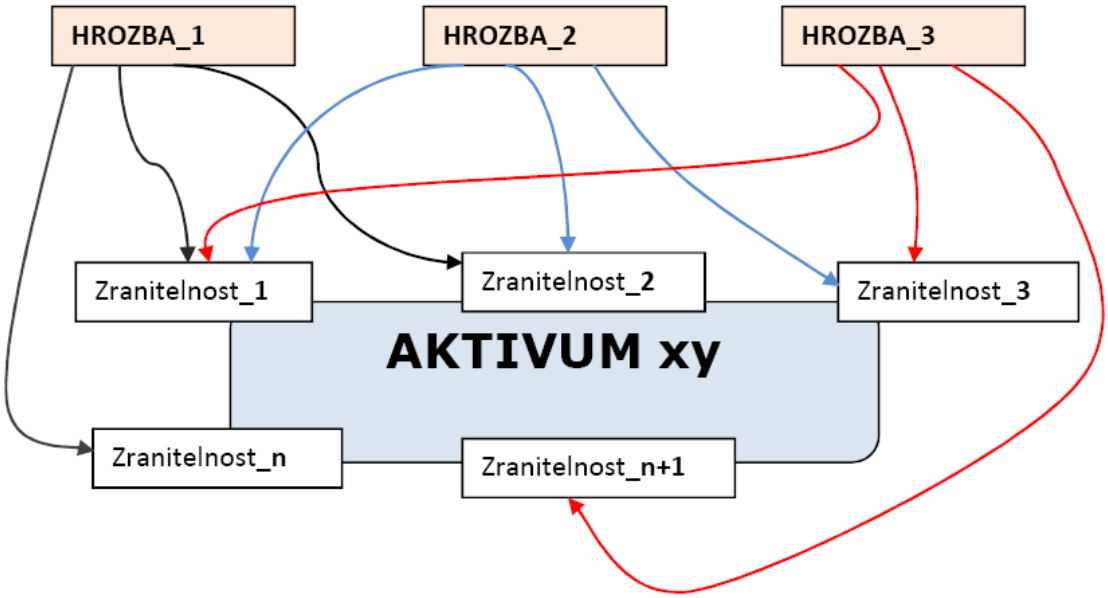
[47] CCTA Risk Analysis and Management Method. Jedná se o metodiku a soubor softwarových nástrojů pro zavádění a podporu řízení bezpečnosti informací, pro provádění identifikace a ohodnocení aktiv, analýzy rizik informačních systémů a sítí, k návrhu bezpečnostních protiopatření, určování havarijních požadavků na informační systémy a k návrhům na řešení havarijních situací.

- nebo použitím tabulkového editoru a aplikací principu:
  Riziko = (hrozba x zranitelnost x možné následky)

Analýza rizik je jednou z nejdůležitějších částí při zavádění systému řízení bezpečnosti, provádí se za účelem odhalení zranitelných a slabých míst Informačního systému organizace. Při analýze rizik musíme vycházet z ohodnocení aktiv, která jsou přehledem toho, co má pro organizaci cenu z hlediska jejího obchodního zaměření.

- *AKTIVUM* je něco, co pro organizaci přináší přidanou hodnotu a organizace si to musí chránit
- *HROZBA* = potenciální příčina nežádoucího incidentu na aktivum, která může mát za následek jeho poškození
- *ZRANITELNOST* = slabé místo aktiva nebo skupiny aktiv, které může být využito hrozbou

Obr. 7. Grafické znázornění principu analýzy rizik



Riziko = Hodnota aktiva * Pravděpodobnost výskytu hrozby * Dopad zranitelnosti

Zdroj: vlastní

Tab.1. Navrhované klasifikační škály pro výpočet Hodnoty Rizika

Pravděpodobnost výskytu hrozby

	váha
Prakticky nemožný výskyt	1
Není běžné, ale může nastat za zvláštních okolností	2
Možný výskyt, již se vyskytl	3
Častý výskyt	4
Příliš častý výskyt, stále se opakující výskyt	5

Dopad zranitelnosti

úroveň	Charakter	Závažnost (váha)
1	Zanedbatelný (nevýznamný)	1
2	Vyšší (malý)	2
3	Značný (střední)	3
4	Existenční (velký)	4
5	Totální (katastrofální)	5

Riziko **R=** *Hodnota aktiva * Pravděpodobnost výskytu hrozby * Dopad zranitelnosti*

úroveň	riziková skupina	rizikový faktor
1	akceptovatelná rizika	<= 100
2	úroveň rizika, u nichž je nutno dodržovat stanovená (ovládací) opatření	=> 100

Zdroj: vlastní

Aktiva

Na podkladě analýzy uvedených v předcházejících kapitolách lze doporučit zahrnout do analýzy rizik tato aktiva:

Tab. 2. Aktiva

Aktivum číslo	Název aktiva
1	Personál a „know-how“ firmy
2	Informace – marketingová data (identifikační údaje o zákaznících)
3	Informace – data zakázek
4	Smlouvy - (s klienty, dodavateli, zaměstnanci, externími spolupracovníky, nabídky)
5	Hardware (PC, notebooky, tiskárna, skener, skartovací zařízení)
6	Software (grafické aplikace – InDesign, Photoshop, Adobe – PDF creator, slovníky, MS Office)
7	Komunikační zařízení (sítě, telefony – klasické, IP a mobilní, modemy)
8	Image firmy

Zdroj: vlastní

Pokusím se nyní o nástin analýzy rizik ve firmě. Nejprve musí být tedy vytvořeno ohodnocení aktiv. Vzhledem k velikosti firmy navrhuji využití metody tvorby tabulek v MS Excel s aplikací stupnice od 1 do 5, kde 1 by znamenala nejnižší dopad na společnost a 5 nejvyšší, hraničící se schopností přežití firmy. Barevné rozlišení je zvoleno pro lepší orientaci a přehlednost v případě, že máme více tabulek.

Tab. 3. Kvalitativní ohodnocení a barevné rozlišení aktiv

Hodnocení	Popis
1	Změny nejsou patrné a dopad na organizaci není žádný
2	Zanedbatelný dopad
3	Zatížení finanční ztrátou a potížemi
4	Podstatné finanční ztráty a vážné potíže
5	Vážné ohrožení firmy až existenční potíže

Zdroj: vlastní

Podklad pro hodnocení získáme na základě *součtového algoritmu*, který patří mezi nejjednodušší a nejpoužívanější. Jeho tvorba spočívá v součtu:

Dostupnost + Důvěrnost + Integrita

x + y + z

Aktiva v průběhu hodnocení mohou mít několik výstupů, záleží totiž, z jakého hlediska je hodnotíme. Má analýza je následující:

Aktivum:

Personál a know-how firmy

- Hodnota z hlediska dostupnosti: 5
- Hodnota z hlediska důvěrnosti: 5
- Hodnota z hlediska integrity: 4
- Celková váha: 5 + 5 + 4 = **14**

Ohrožení tohoto aktiva může znamenat pro firmu značné finanční náklady a vážné potíže. Personál firmy je velmi ceněn, a to z toho důvodu, že zkušenosti, které nabude během zkušební doby a v průběhu pracovního poměru z jednotlivých zakázek a od hlavního editora a editora jsou vysoce cenné. Jedná se o investovaný čas, který školení jednotlivého pracovníka stojí. Překladatel s každou novou zakázkou získává poznatky, které jsou evidovány ve firemním slovníku k dalšímu využití. Význam dosažených znalostí hraje velkou roli hlavně při zakázkách stejného nebo podobného typu od zadavatele, se kterým pracuje průběžně. V tom případě ví, jaké termíny daná firma používá, v jakých souvislostech, což nejen urychluje a usnadňuje překlad, ale také zaručuje, že klient obdrží zakázku zpracovanou dle jeho požadavků a představ. Jde o efektivitu práce překladatele.

Informace – data o zákaznících

Tab. 4. Hodnocení aktiv o zákaznících

Aktivum	Zdroj	Dostupnost	Důvěrnost	Integrita	Váha
Informace o zákaznících	PC a notebooky	5	5	4	14
	Zálohovací zařízení	4	5	5	14
	Kniha zakázek	2	1	2	5
	Síťové disky	5	5	3	13
	Evidenční listy	1	1	1	3
	Tištěné smlouvy	3	2	5	10

Zdroj: vlastní

Z tabulky jsou patrné váhy jednotlivých aktiv. Je z ní zřejmé, že nejvíce do nesnází by se firma dostala při nedostupnosti ať už samotných PC nebo disků, kde jsou veškerá data uložena. Tato data jdou totiž více do hloubky než ta, co jsou v papírové podobě.

Hardware

Tab. 5. Hodnocení jednotlivých hardware

Aktivum	Zdroj	Dostupnost	Důvěrnost	Integrita	Váha
Hardware	PC a notebooky	5	5	4	14
	Tiskárna	1	1	1	3
	Skener	1	1	1	3
	Skartovací zařízení	2	2	2	6

Zdroj: vlastní

Opět je zde vidět, že významnou roli hrají PC a notebooky. Význam ostatního zařízení je velmi malý.

Software

Tab. 6. Hodnocení jednotlivých software

Aktivum	Zdroj	Dostupnost	Důvěrnost	Integrita	Váha
Software	InDesign	2	2	1	5
	Photoshop	1	1	1	3
	Adobe	3	2	3	8
	Slovníky	4	4	4	12
	MS Office	4	4	3	11

Zdroj: vlastní

Vidíme, že ze software, které firma využívá nejvíce patří slovníkům hlavní priorita a ztráta těchto dat by způsobila značné komplikace v pracovním procesu, jež by mohly vést až k finančním ztrátám.

Dokumenty

Tab. 7. Váha jednotlivých zdrojů uložených dokumentů

Aktivum	Zdroj	Dostupnost	Důvěrnost	Integrita	Váha
Dokumenty	PC - elektronická podoba	3	3	4	10
	Archiv - fyzická podoba	2	3	4	9

Zdroj: vlastní

Vidíme, že význam uložení dokumentů se pro společnost z hlediska daného místa (PC nebo archivu) neliší. Obě váhy jsou totožné. Je důležité, aby se k daným informací dostala oprávněná osoba včas bez rozdílu, zdali jsou uvedeny v PC nebo fyzicky zavedeny v archivu.

Komunikační zařízení

Tab. 8. Hodnocení komunikačních zařízení

Aktivum	Zdroj	Dostupnost	Důvěrnost	Integrita	Váha
Komunikační zařízení	Sítě	3	4	4	11
	Telefony - IP	2	2	1	5
	Mobilní telefony	1	2	1	4
	Modemy	3	3	2	8

Zdroj: vlastní

Z komunikačních zařízení pro firmu jsou nejvýznamnější sítě a modemy. Dále pak vidíme, že pro společnost mají větší význam IP telefony než klasické mobilní. To proto, že využívání IP telefonů je velmi výhodné, co se týče nákladů. Jelikož společnost spolupracuje s firmami, které mají pobočky po celé Evropě, stalo se využívání IP telefonů nezbytně nutnou záležitostí. Volání nejen do evropských zemí, ale také do USA se pohybuje v haléřových položkách za minutu a hovory místní (celá ČR) jsou do 30 minut zdarma. Proto je snahou firmy omezovat používání mobilních telefonů a přesunout se raději na plné využívání IP telefonů.

Image společnosti

Bych ohodnotila nejvyšší vahou – 5. A to z toho důvodu, že pro společnost je její dobrý image vysoce důležitý v konkurenčním boji. Hlavním způsobem jak oslovuje potencionální klienty, je druh telemarketingu a na základě osobních kontaktů, návštěv odborných veletrhů a konferencí. Investování do reklamy je minimální až nulové. Za dobu své

působnosti na trhu si společnost vybudovala dobré jméno a dostala se do povědomí zákazníků z nejrůznějších sfér, kteří jsou ochotni investovat do vysoce profesionálních služeb, čímž se společnost odlišuje od klasických překladatelských agentur. Nejběžnějším způsobem, jak se informace o společnosti šíří je na základě doporučení stávajících klientů („Word of mouth“). Dle mého názoru je tento druh reklamy pro společnost a její prezentaci velmi přínosné. Společnost se nesnaží uspokojit masový trh s překlady, ale specifický okruh zákazníků (manažeři, vědci, právníci, ekonomové, státní sektor, aj.).

Nyní máme za sebou identifikaci aktiv a jejich ocenění. Dalším důležitým bodem je vypracování analýzy rizik. Významnost tohoto dokumentu spočívá v tom, že je na něm postaven celý systém bezpečnosti informací, a tudíž je jeho důležitost vysoká.
Před tím, než je analýza rizik provedena, bychom mohli uskutečnit odhad rizik, která mohou být vyvolány jednou nebo více událostmi. Měli bychom se podívat na současný stav společnosti a zjistit, jaké hrozby jsou pro ni aktuální.

Hrozby se mohou dělit na:

- Přírodní – blesk, povodeň
- Úmyslné – požár, záměrná chyba pracovníka
- Náhodné – odstranění složky
- Lidské – odcizení vybavení

Při posuzování hrozeb by mělo být provedeno minimálně ohodnocení kritických systémů. Jelikož si v našem případě provádí společnost toto hodnocení vlastními silami, je v tomto případě dobré použít jako návod, jak postupovat normu ISO/IEC TR 13335-3 (příloha C), kde jsou možné formy hrozeb vymezeny. Struktura hrozeb, které by se daly aplikovat na naši firmu, může být následující (variantní příklad):
Lidské hrozby úmyslné

- Krádež (informací nebo vybavení)
- Úmyslná škoda
- Chyba zaměstnanců
- Chybné směrování zpráv
- Hacking

Neúmyslné

- Vymazání
- Selhání dodávky energie
- Chyba uživatele
- Nesprávné použití zdrojů
- Neškolení uživatelé
- Nedostatečné zabezpečení přístupu na Internet

Náhodné

- Selhání dodávek (voda, energie)
- Selhání hardwaru, softwaru
- Viry
- Chyba přenosu
- Chyba údržby
- Nedostatek zaměstnanců

Přírodní

- Blesk
- Požár
- Povodeň
- Vichřice

Z výčtu hrozeb můžeme vidět, že jsou některé aplikovatelné na různé druhy hrozeb. Hlavně co se týče lidského faktoru, tak zde je možnost vzniku hrozby úmyslně či neúmyslně.
Při hodnocení rizika budeme opět vycházet z údajů (váhy aktiv), které jsme si již zjistili z předešlých výpočtů, a také z tabulky 1, kde jsou uvedeny úrovně pravděpodobnosti výskytu hrozeb a dopad zranitelnosti. K jednotlivým škálám jsem přiřadila váhy, a to opět od 1 (nejmenší zátěže) po váhu 5 (nejrizikovější).

Na příkladu aktiva Informace o zákaznících bych uvedla, jak daný výpočet provést.
V tabulce vidíme, že nejvyšší váhy jsou ve zdrojích PC a notebooky a Zálohovací zařízení. Obě mají shodně hodnotu váhy 14. To znamená, že tyto zdroje jsou velmi cenné pro

společnost a měla by jim být věnována zvýšená pozornost, ale tak, aby nebyly opomenuty také ostatní zdroje.

Známe hodnotu zdroje aktiva a nyní si musíme položit otázky:

„Jaká je pravděpodobnost výskytu hrozby pro dané aktivum a zdroj?“

„Jaký bude dopad zranitelnosti daného aktiva a jeho zdroje na společnost?“

Pomocí těchto otázek provedeme analýzu rizika, kdy použijeme rovnici:

Riziko = Hodnota aktiva x Pravděpodobnost výskytu hrozby x Dopad zranitelnosti

- Hodnota aktiva je **14** (bereme nejvyšší hodnotu);
- Pravděpodobnost výskytu hrozby je **3** (možný výskyt, již se vyskytl)
- Dopad zranitelnosti je **3** (značný, střední)

Výpočet bude následný:

Riziko = 14 x 3 x 3 = 84 rizikový faktor

Nyní je nutné údaj, který jsme si výpočtem zjistili, porovnat s hodnotou rizikového faktoru. Použila jsem hodnotu rizikového faktoru 100, s tím, že pokud se v průběhu analýzy rizik aktiv vyskytnou hodnoty, které tento rámec překročí, bude to signál proto, aby se navrhla a následně zavedla do praxe potřebná opatření ke snížení rizika. Před započetím je však nutné, aby byla určena osoba, která bude za tyto činnosti odpovědná.

V našem případě jsem zjistila, že hodnota je 84. Tedy **84 < 100**

Z hlediska přehlednosti a množství údajů, navrhuji řešení s podporou strukturované tabulky:

Tab. 9. Znázornění výpočtu rizikového faktoru

Aktivum	Zdroj	Hodnota aktiva **A**	Pravděpod. výskytu **B**	Dopad zranitelnosti **C**	Riziko **(A x B x C)**	Rizikový faktor
Informace o zákaznících	Zálohovací zařízení	14	3	3	84	**84 < 100**

Zdroj: vlastní

Můžeme říci, že riziko je akceptovatelné. Pokud se podíváme na dané údaje z jiného úhlu, tak vidíme, že rozdíl mezi naším výsledkem a hranicí 100 není až tak příliš velký. Proto bych si troufla říci, že, i když dle naší tabulky se jedná o akceptované riziko, tak by se toto nemělo podceňovat, obzvláště, když pro společnost toto aktivum (a jeho daný zdroj) hraje jednu z klíčových rolí.

Stejně jako jsem postupovala v tomto případě, by se provedla analýza na zbývající aktiva a jejich zdroje. Z nich bychom poté zjistili celkový přehled o riziku ve společnosti a na jeho základě by se mohla budovat preventivní opatření.

Nutno podotknout, že dané hodnoty a škály si subjekt, který danou analýzu provádí, stanoví sám na základě zkušeností nebo po rozhovoru s ať již majitelem společnosti nebo s uživateli (zaměstnanci). Vždy je lépe danou problematiku prodiskutovat s oběma stranami (majitel a zaměstnanci), abychom se vyhnuli případnému zaujetí z jedné strany. Jedná se o druh křížové konfrontace. Tímto získáme objektivnější pohled a následná analýza je více přesná.

Současný stav a návrh možných opatření:

Jelikož firma využívá a kumuluje velké množství informací a dat je zálohovací systém pro ni nezbytností. V současné době je řešení tohoto aktiva pro společnost nevýhodné. Každý den se kontroluje, zdali proces zálohování proběhl a v případě, že ne, tak musí být přizván externí specialista ze společnosti, která je poskytovatelem odborného servisu, aby našel příčinu a problém odstranil. I když může být řešení velmi snadné, musí tento pracovník přesto přijít osobně, protože hlavní management společnosti nesouhlasí s tím, aby byl na hlavní server vytvořen tzv. vzdálený přístup umožňující odstraňování a práci na daných počítačích na dálku.

Další problém spatřuji v tom, že firma nemá svého interního IT specialistu. Zpráva počítačů a systému formou vzdáleného přístupu se jeví efektivnější z pohledu zajištění kontinuity činností, ale přinesla by s sebou další rizika pro jednotlivá aktiva, která by se musela zohlednit v analýze rizik.

Výhody:

- Rychlý přístup
- Průběžná kontrola a tím větší pravděpodobnost předejetí incidentů (např. při napadení systému virem je spuštěn varovný signál, který upozorní dané IT pracovníky, že se něco děje)
- Aktualizace nejen antivirových programů přes hlavní server, čímž se předejde zdlouhavější instalaci na každém počítači zvlášť
- Flexibilita
- Menší časová náročnost
- Možnost instalace programů na dálku

Nevýhody:

- Přístup dalšího subjektu z venčí
- Možnost úniku informací
- Nemožnost osobní kontroly toho, co daný pracovník provádí
- Pocit nejistoty ze strany společnosti, zdali nedošlo k úniku informací

Uveďme si nyní opačnou situaci, kdy by hodnota rizikového faktoru přesáhla 100.

Tab. 10. Rizikový faktor u dokumentů na PC

Aktivum	Zdroj	Hodnota aktiva **A**	Pravděpod. výskytu **B**	Dopad zranitelnosti **C**	Riziko **(A x B x C)**	Rizikový faktor
Dokumenty	PC - elekt. Podoba	10	3	4	120	**120 > 100**

Zdroj: vlastní

Zde vidíme opačný efekt. Rizikový faktor je zde větší, a to proto, že veškeré dokumenty, které firma má jsou z větší části uloženy (buď naskenované nebo v PDF) v počítači. Tiskopisů ve fyzické podobě je jen velmi málo a tvoří je hlavně smlouvy, které jsou také po naskenování uloženy do počítače a originály jsou uzamčeny ve skříni.
Opatření dvou záloh může vypadat zprvu jako dobré řešení, ale i zde jsou nedostatky.

Současný stav:

- Organizace datového prostoru je nejednotná a uživatelsky složitá na orientaci.
- Postup při přijímání dokumentů je velmi složitý (od jejich převzetí po uložení čítá několik etap evidence)
- Není jednoznačně (písemně) stanoveno, které dokumenty ukládat a které nikoli.

Návrh možných opatření:

- Stanovení dokumentu postupu, jak materiály kategorizovat, nakládat s nimi a jak je evidovat (nejen fyzicky, ale také elektronicky)
- Vytvoření přílohy postupu, jak nakládat s citlivými dokumenty
- Na základě daného rozhodnutí vytvořit dokument a obeznámit s ním zaměstnance tak, aby každý byl schopen provedení evidence. Jelikož je firma malá, dle mého názoru by měli všichni interní zaměstnanci být schopni zvládat základy administrativních prací pro případ nutného zastoupení administrativního pracovníka
- Nákup uzamykatelné skříně a vytvoření řízeného přístupu osob
- Ukládání všech dokumentů stejné povahy na vyhrazeném datovém úložišti v počítači.

Jelikož se jedná o hlavně administrativní úkony, bylo by dle mého názoru vhodné, aby odpovědnou osobou byl administrativní pracovník. Ten by na základě zkušeností a ve spolupráci s ostatními zaměstnanci a vedením firmy, vytvořil dokument, který by dané postupy sjednotil a stal se vodítkem nejen pro stávající zaměstnance, ale také pro nové. Provedl by také školení, kde by zaměstnanci byli s danými skutečnostmi obeznámeni a podpisem by stvrdili, že danému systému rozumí a budou se jej snažit dodržovat. Dalším jeho úkolem by také bylo monitorování dodržování postupů a případné inovace.
Postup, který jsem zde uvedla na příkladu by měl být aplikován pokaždé, když se provádí hodnocení aktiv a rizik.

4.3.2 Komentář ke stavu řízení firmy

Vzhledem k tomu, že se jedná o malou firmu, tak její řízení je přímé, nejsou zde žádné komplikované vazby mezi jednateli či zaměstnanci. Organizační struktura je jasná a vymezuje přesně vazby mezi jednotlivými zaměstnanci a také jejich odpovědnosti.
Rozdělování úkolů probíhá směrem shora dolů, tzn., že ředitel ustanovil osobu odpovědnou za rozdělování úkolů a jejich přiřazování. V případě nejasností je to ředitel, kdo dělá konečná rozhodnutí, většinou však po konzultaci se zaměstnanci.

Snahou firmy je vystupovat jako komunikační firma a tím se odlišit od ostatních překladatelských agentur, což se jí daří. Vzhledem k velikosti týmu je občas o něco složitější skloubit práci na zakázkách a projektech tak, aby nedošlo ke snížení kvality služby, ale i zde si společnost vede velmi zdatně a profesionálně bez negativních ohlasů z venčí. Snahou firmy je, aby úroveň práce a výsledků se stále zvyšovala, což podporuje umožněním zaměstnancům se účastnit vzdělávacích kurzů a jiných školení. I když certifikace nebyla zatím provedena, tak zájem ze strany společnosti je v tomto směru vysoký. Hlavně, co se týče bezpečnosti dat. Vedení společnosti je si vědomo významu bezpečnosti v současné době a snaží se o shodu provozu s požadavky normy.

Při zpracovávání checklistů jsem měla možnost se obeznámit s tím, jak nejen vedení, ale také zaměstnanci chápou působení společnosti, zdali mají přehled o postupech, které se ve společnosti odehrávají, o jejím vybavení (hmotném, nehmotném) a dalších aspektech, které jsou uvedeny v normách a musí být plněny, aby mohla proběhnout certifikace.

Vyhodnocením checklistů jsem zjistila, že zaměstnanci povědomí o požadavcích normy a stavu ve firmě mají, ale není jednotné. V některých případech bylo pro ně obtížné porozumět otázce, jinde se lišili v odpovědích (kde jeden uvedl, že ano, druhý odpověděl vůbec ne). Většinou byla odpověď nevím. Vyskytly se však i odpovědi kladné, které se shodovali.

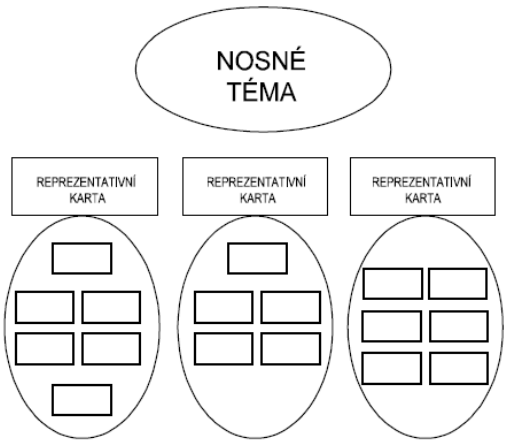
4.3.3 Návrh nástrojů a/nebo metodik pro zlepšování systému řízení ve firmě

Vzhledem k velikosti firmy a pracovního týmu bych navrhla následný postup přístupu k pojetí neustálé zlepšování.

Brainstorming („bouření mozků") - nejdříve bych použila této metody k zjištění nápadů a nových myšlenek od všech členů kolektivu. Navržené zadání by mohlo znít: „Systém evidence zakázek ve firmě." Všichni by se měli tak možnost vyjádřit k danému tématu, které má také na ně dopad a navrhnout řešení. Tato metoda může být velmi účinná, ale je nutné, aby se všichni oprostili od zábran a ostychu, že jejich nápad může být považován za hloupý. Brainstormingu by se účastnili všichni, tedy i vedení a nápady by se zaznamenávaly na papír. Jednoduše řečeno, každý by napsal to, co ho v souvislosti s daným tématem (např. problém dokumentace) napadne. Smyslem je myšlenky pouze kumulovat a ne je také ihned hodnotit. Poté, co již produktivita nových nápadů stagnuje, by se přikročilo k druhé etapě – jejich kritickému vyhodnocení. Před tím bychom mohli využít *diagram afinity*, abychom získané myšlenky utřídili.

Diagram afinity – je užitečnou pomůckou pro rozdělení myšlenek do logických skupin. Tím se naskytne možnost lépe vidět jednotlivé skupiny a dále je v případě nutnosti doplňovat.

Obr. 8. Možnost grafického znázornění „Diagramu afinity"

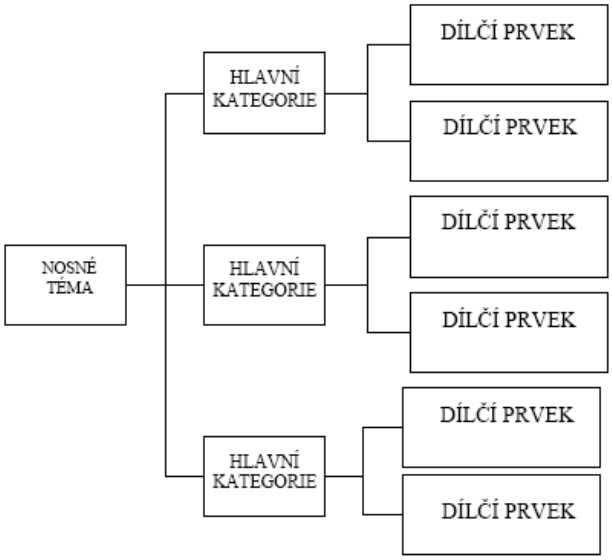


Zdroj: vlastní

A/nebo

Stromový diagram – daný problém lze rozložit do linie od obecného ke konkrétnímu. Vznikne nám druh větvení, se který můžeme následně pracovat. Tento diagram lze aplikovat jak na výrobek, jeho základní funkce, tak proces nebo cíl a myšlenku.

Obr. 9. Znázornění „Stromového diagramu“

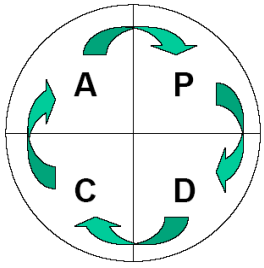


Zdroj: vlastní

Na základě těchto nových myšlenek, jejich roztřídění a vyhodnocení, by se dle mého názoru a dosavadních zkušeností, mohla ve společnosti využít metoda PDCA.

Jedná se o obecnou metodu složenou ze čtyř kroků, jejíž bezesporu výhodou je její jednoduchost. Dalším plusem této metody je skutečnost, že sama firma si může vypracovat podrobnější návody na řešení nelezených problémů. Firma si může „ušít na míru“ jednotlivé kroky PDCA:

Obr. 10. Jedno z možných znázornění metody PDCA



Zdroj: vlastní

- Plan – plánuj a urči záměr, cílem je návrh řešením problému
- Do – proveď, uskutečni zvolený záměr, smyslem je provedení rozhodnutí, a sledování jeho následků. Vše musíme měřit a pečlivě zaznamenávat.
- Check – kontroluj, analyzuj a vyhodnocuj dosažené výsledky a změny. V případě, že se potvrdí zlepšení, pak následuje poslední krok
- Action – trvalé zavedení

4.4 Návrh projektu „Zavedení systému managementu se zaměřením na bezpečnost dat

K zavedení systému managementu bezpečnosti informací lze přistoupit z různých hledisek. Tím základním přístupem může být právě již aplikace principu PDCA.

Plan - ustavení ISMS:

- Stanovení rozsahu ISMS a strategie informační bezpečnosti
- Management rizik
- Návrh bezpečnostní politiky, systémových směrnic, plánu řízení kontinuity činností
- Bezpečnostní plán a plán implementace ISMS

Do - zavádění a provozování ISMS:

- Implementace procedur a postupů ISMS
- Školení
- Provoz

Check - monitorování a přezkoumání ISMS:

- Audit a/nebo penetrační testy
- Testy procesů
- Testy techniky
- Testy metodami sociálního inženýrství a další testy

Act - udržování a zlepšování systému

Jiný přístup by mohl být definován na podkladě principů projektového řízení - systém managementu jakosti projektů:

1. Charakteristiky projektu
2. Management zdrojů
   - Procedury vztahující se ke zdrojům
   - Procedury vztahující se k zaměstnancům
3. Realizace produktu
   - Procedury vztahující se k vzájemné závislosti
   - Procedury vztahující se k předmětu
   - Časově závislé procedury
   - Procedury vztahující se k nákladům
   - Procedury vztahující se ke komunikaci
   - Procedury vztahující se k riziku
   - Procedury vztahující se k nakupování
4. Měření, analýza a zlepšování
   - Měření a analýza
   - Neustálé zlepšování

4.4.1 Analýza možností zavedení systému managementu se zaměřením na bezpečnost dat vlastními silami ve firmě

Na základě poznatků uvedených v kapitole 4.3 vyvozuji, že stávající personální kapacity neumožňují zavedení systému managementu bezpečnosti informací s využitím jen vlastních personálních zdrojů a to z důvodů časové kapacity taky důvodu nedostatečných odborných znalostí v oblasti ICT a praktických zkušeností a dovedností.

Lze doporučit tyto kroky:

- proškolit zaměstnance, vysvětlit jim, proč a o jakou certifikaci má firma zájem, jaké kroky budou muset být udělány, aby tento proces mohl být uveden do chodu a aby v závěru mohla proběhnout (za splnění všech podmínek a s přispěním všech zaměstnanců) samotná certifikace. Zaměstnanci by sami měli poznat přínosy celého projektu a postupu, čímž by se do jisté míry usnadnila celá organizace, a to z důvodu nutné spolupráce všech osob bez výjimky.
- Stanovení rozsahu ISMS
- Výběr konzultační firmy, která povede celý projekt implementace a pomůže s řešením odborných otázek ICT a s vlastní implementací bezpečnostních opatření
- Realizace projektu
- Validace projektu a jeho ukončení.

Rizika plynoucí ze spoluúčasti externího subjektu v projektu musí být ošetřena ve smlouvě o spolupráci a to jak na úrovni naší firmy s dodavatelem (právní subjekt) tak na úrovni naše firma a jednotlivý zaměstnanci dodavatele. Dále musí být ustanovena politika bezpečnosti pro období trvání projektu pro pracovníky dodavatele, tak aby byly eliminovány rizika úniku, zneužití nebo ztráty dat pracovníky dodavatele.

4.5 Zpracování harmonogramu projektu včetně jednotlivých kroků při implementaci

Pokud by se společnost rozhodla pro zavedení certifikace, bylo by nutné vytvořit předběžný harmonogram prací a postupů jednotlivých etap. Nezbytně nutné před samotným počátkem by také bylo informovat zaměstnance o všem, co se ve společnosti bude v nejbližších měsících odehrávat, aby se zajistila jejich maximální spolupráce.

Tento návrh by mohl vypadat následovně:

1. Fáze – zahrnovala by sběr informací o aktivech, dále by tato aktiva byla oceněna a ohodnocena vlastníky. Ukázka postupu, jak by sběr a hodnocení mohl vypadat

jsem již provedla v kapitole 4.3. Bylo by také nutné, spolu s IT techniky ze společnosti, která zajišťuje IT servis společnosti, přezkoumat stav bezpečnostních opatření a standardů a hlavně bezpečnost sítě.

2. Fáze – tato část by se soustředila hlavně na dokumentaci jednotlivých postupů a procesů. Načež by sloužila jako podklad k tvorbě platformy pro provoz ISMS. Další důležitou součástí tohoto bodu by bylo vytvoření plánu na zvládaní zjištěných rizik na aktivech a tvorbě bezpečnostní politiky a návrh technických opatření.

3. Fáze – týkala by se hlavně auditů a testování. Poté přípravě k certifikaci. Proběhlo by školení pracovníků, jak nakládat s informacemi a dále by se také školení provedlo pro správce aktiv.

Harmonogram by mohl být:

Dne 1.1.2011 by mohlo být provedeno setkání se zaměstnanci a také by byli přizváni IT technici. Následně by se provedlo výběrové řízení na dodavatele této služby. Dostačující výběrové řízení by mohlo trvat v délce 1 měsíc, poté by se provedlo vyhodnocení jednotlivých uchazečů a následný výběr dodavatele, se kterým by byla sepsána smlouva. Predikce časového hlediska plnění dalších bodů je velmi těžko v tuto chvíli odhadnutelná, ale jednalo by se řádově roky (+2roky) než by mohla být provedena certifikace. Tedy pokud by počátek procesu byl v roce 2011, tak v případě, že vše půjde dobře a bez větších komplikací, by mohlo dojít k certifikaci na konci roku 2013 (jedná se však o velmi hrubý odhad).

Fáze 1 – Analýza současného stavu ITC

- Nejdříve by bylo nutné definovat základní pojmy
- Zvolení vlastní metodiky analýzy rizik (možnost použití normy ČSN ISO/TR 13335). Postupů pro analýzy je několik a záleží na posouzení firmy o vhodnosti či nevhodnosti dané metody. Navrhovala bych provedení analýzy hodnot k jednotlivým aktivům (viz. předchozí kapitoly). Z časového hlediska by analýza rizik u tak malé společnosti měla trvat zhruba 1 měsíc.
- Hodnocení aktiv – hardware, software, informace, zaměstnanci
- Identifikace, hodnocení hrozeb a zranitelností

Dokumenty, které by měly být vytvořeny:

- Slovník pojmů a jejich definice
- Dokument týkající se metod při analýze rizik, obsahující postupy analýz
- Rozbor analýzy rizik – tabulky, grafy, dle požadavků společnosti
- Protokol o provedené analýze rizik
- Harmonogram popisující další etapu – požadavky a zdroje
- Závěrečný dokument obsahující výsledky první etapy

Fáze 2 – Zvládání rizik a politika bezpečnosti

- Zprvu nutnost vytvoření postupů (plánů) pro zvládání rizik, a to individuálně pro jednotlivá rizika, která byla zjištěna z předchozí analýzy. Opět je nutná tvorba dokumentace, která by zahrnovala opatření pro řízení rizik a jejich časový a nákladový rámec.
- Při analýze bychom nalezli jak neakceptovatelná rizika, tak akceptovatelná, která je také nutné identifikovat
- Rozdělení odpovědností

  - ředitel firmy by měl být odpovědný za prosazování bezpečnostních zásad (direktivně-osobní přístup), implementaci bezpečnostní politiky, vyhodnocování rizik a způsoby jejich pokrytí). Zde nám hrozí riziko kumulace práv a pravomocí, s čímž je nutné počítat již od započetí projektu.
- Vytvoření dokumentu týkajícího se bezpečnostní politiky a rozhodnutí o hranicích a rozsahu ISMS

Dokumenty, které by měly z dané etapy být vytvořeny:

- Písemný postup při zvládání rizik, který také by měl zahrnovat cíle, opatření a rozsah ISMS. V potaz je nutno brát např. rysy společnosti, aktiva, technologie.
- Dokument obsahující bezpečnostní politiku (metody řešení bezpečnosti, hlavní cíle při ochraně informací, odpovědnosti a pravomoci)
- Návrhy na provádění interních auditů (procesy a zdroje)
- Bezpečnostní standardy

- Dokument o aplikovatelnosti
- Zápis o schválení poznatků a výsledků z dané etapy (Fáze 2)
- Návrh postupu následných prací ve fázi 3

Fáze 3 Implementace a provoz ISMS

- Objasnění zásad interního auditu a postupu jeho realizace
- Školení zaměstnanců a správců aktiv
- Doporučení a zavedení opatřeních týkajících se organizace a procedur

Výsledná dokumentace:

- Potvrzení o proškolení interních auditorů
- Zápisy z interních auditů a jejich ohodnocení
- Analýza interních auditů a případná doporučení ke změnám
- Zpráva o hrozbách, které vznikly v analyzované oblasti od zahájení Fáze 2
- Aktualizovaná dokumentace o aktivech a práci s nimi ve vztahu k bezpečnosti (např. směrnice, příručky, aj.)
- Protokol o schválení daných výsledků Fáze 3

Postup, který jsem zde uvedla je ukázkou toho, jak by vše mohlo být provedeno. Ve výsledku však rozhodnutí závisí na dané firmě. I v případě, že firma projde všemi etapami a připraví dané dokumenty, které jsou vedením přijaty a slouží jako podklady pro zahájení procesu certifikace, neznamená to, že v konečné fázi k certifikaci dojde. Rozhodnutí, zdali se tomu tak stane či nikoli závisí na firmě.
Pokud ohlas bude negativní, neznamená to, že celá práce byla zbytečná. Ve výsledku firma jistě získá znalosti o slabinách současného systému, na jejichž základech se může lépe rozhodnout v případě investic do daného systému a jeho rozvoje. Vzniklá dokumentace postupů, procesů a odpovědností bude přínosná ke zvyšování bezpečnosti.

V teoretické části kapitoly 3 jsem hovořila o možných přístupech k systému nastavení managementu ochrany dat. Zde by bylo opět vhodné se k tomuto bodu vrátit, abychom dle zjištěných poznatků mohli stanovit, které z dalších metod by společnost mohla využít, pokud by se nerozhodla pro ISO 9001 nebo ISO 27000. Záleží totiž na společnosti, který certifikát se jí (tedy jejímu managementu) bude zdát více přínosný.

Co se týče metody QWeb a Apek, tak jsou tyto přístupy nevyhovující, protože jsou vhodnější pro firmy zabývající se činností elektronického obchodu na internetu a zde naše společnost nepůsobí. Zákon vztahující se k ochraně utajovaných informací – 412/2005 Sb. by se dal aplikovat z důvodů občasné práce s údaji, které dočasně podléhají utajení, tedy před tím, než jsou oficiálně zveřejněny. Jak již jsem uvedla dříve, v těchto případech se využívá šifrování, kdy heslo je známo pouze vybraným subjektům.

ITIL – Best practise a Good Priv@cy jsou dalšími přístupy, které by mohly být použity. ITIL proto, že více do hloubky specifikuje a popisuje řízení služeb informačních technologií a Good Priv@cy se zaměřuje na reprezentaci a ochranu dobrého jména.

ZÁVĚR

Záměrem předložené diplomové práce bylo vypracovat vstupní materiál pro firmu English Editorial Services, s. r. o. obsahující rešerši systémových přístupů k problematice bezpečnosti informací. Tento dokument bude sloužit jako informační text pro získání základní představy, co kvalita a bezpečnost v oblasti informací znamenají a obnášejí, a možnosti, které firma v této oblasti má (druhy možných certifikací) a jejich vhodnost.

Diplomová práce vznikala za definovaných vymezených podmínek, které jsou dány charakteristikou firmy – předmět činnosti, počat pracovníků, zvyklosti a záměry majitelů. Cílem diplomové práce nebylo provedení implementace ISMS podle ISO 27001.

Na základě struktury zadání diplomové práce a po následném prostudování materiálů, byly nejprve provedeny analýzy systému kvality (podle norem ISO 9001 a ISO 27001) pomocí checklistů. Checklisty byly zpracovány z části s využitím ne veřejně dostupných informací. Ze strany poskytovatele nebyl udělen souhlas k prezentování checklistů v diplomové práci. Analýzou bylo zjištěno, že současný stav řízení firmy se z pohledu požadavků daných norem nenachází v souladu: požadavky – jejich dokladování – a zjištěný stav praxe. Následně byly provedeny u daných bodů, kde docházelo k rozporům, návrhy na jejich možná opatření a doporučení. Byl také proveden návrh metodiky ohodnocení aktiv a analýzy rizik s využitím excelových tabulek a hodnotových koeficientů.

Jak je v práci popsáno význam certifikace bezpečnosti informací v posledních letech výrazně roste. Není to pouze z důvodů konkurenceschopnosti firem, ale také z marketingového hlediska, kde snahou je maximální uspokojení zákazníka, a tím získání jeho loajality. Jelikož v dnešní době je trh přeplněn a zahlcen firmami poskytujícími podobné služby, může být pro zákazníka, který hledá opravdu kvalitu rozhodující fakt, že daná firma má nebo jedná v souladu s určitým standardem a tento stav prokazuje například certifikací (platným certifikátem). I když se nedá jednoznačně odpovědět na to, zdali je v konečné fázi sama certifikace nutná, tak dle mého názoru pro danou firmu by bylo vlastnictví certifikátu přínosné, už jen z toho důvodu, že uchovává a kumuluje data svá a data a informace o klientů (i když se jedná z části o data veřejně dostupná). I v případě, že by v konečné fázi k certifikaci nedošlo, tak přínosem bude důkaz, že firma má zájem o zvyšování kvality a snaží se následovat a dodržovat požadavky norem (ať už se jedná o ISO 9001, ISO 27001 nebo o best practices v daném oboru).

Poznatkem bylo také zjištění, že systém řízení a samotná certifikace ještě nezaručují kvalitní zvýšení základních požadavků managementu bezpečnosti informací (dostupnost, důvěrnost, integrita), ale poskytují informace a přehled o činnostech a odpovědnostech, které jsou již v dané firmě zavedeny, ale většinou nejednotně.

Přínosem této práce pro firmu English Editorial Services, s. r. o. je zpracování základní analýzy stavu řízení ke standardům ISO 9001 a ISO 27001, návrh možných opatření pro zvýšení souladu mezi praxí a požadavky uvedených norem a zpracování harmonogramu prací spojených se zavedením funkčního systému řízení podle požadavků těchto norem. Kritickým bodem, který byl v průběhu zpracování diplomové práce analyzován je zjištění nedostatečných kapacit personálního charakteru s potřebnou hloubkou znalostí problematiky ICT. Pro úspěšné zvládnutí celého projektu, jehož započetí je na rozhodnutí majitelů firmy, bude nutné vybrat vhodnou poradenskou firmu. Závěrem je nutno konstatovat, že normy ISO procházejí periodickým cyklem aktualizací, které by do nich měly přinášet aktuální poznatky z best practices daného oboru. Pokud bude zahájení projektu implementace oddalováno, může dojít ke změně rozsahu požadavků obsažených v aktualizovaných technických normách.

SEZNAM POUŽITÉ LITERATURY

Monografie:

[1] RYŠÁNEK, Pavel a kol. Kvalita v podmínkách Evropské unie. 1. vydání. Ostrava: Montanex, 1998. 190 s. ISBN 80-7225-010-8

[2] BusinessInfo.cz: oficiální portál pro podnkání a export [online].Český institut pro akreditaci (ČOI), 22.6.2004, 2010 [cit. 2010-02-12]. Systém managementu jakosti. Dostupné z WWW: <http://www.businessinfo.cz/cz/clanek/kvalita-jakost/system-managementu-jakosti/1000513/16924/>.

[3] KOTLER, Philip. *Marketing insights from A - Z: 80 concepts every manager needs to know*. I. Title. New Jersey (United States of America): John Wiley & Sons, Inc., 2003. 206 s. ISBN 0-471-26867-4.

[4] VEBER, Jaromír, et al. Řízení jakosti a ochrana spotřebitele. 2., aktulizované vydání. Praha: Grada Publishing, 2007. 204 s. ISBN 978-80-247-1782-1.

[5] MLÝNEK, Jaroslav. Zabezpečení obchodních informací. Vydání první. Brno: Computer Press, a. s., 2007. 154 s. ISBN 978-80-251-1511-4.

[6] PLURA, Jiří. Plánování a neustálé zlepšování jakosti. Vydání první. Praha: Computer Press, a. s., 2001. 244 s. ISBN 80-7226-543-1.

[7] DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana. Vydání první. Brno: Computer Press, a. s., 2004. 182 s. ISBN 80-251-0106-1.

[8] BRIŠ, Petr. Management kvality. první. Zlín: Univerzita Tomáše Bati ve Zlíně, 2005. 213 s. ISBN 80-7318-312-9.

[9] ZÍDKOVÁ, Helena; ZVONEČEK, František. Jakost - styl života pro třetí tisíciletí. 2. vydání. Plzeň: Západočeská univerzita v Plzni, 2003. 139 s. ISBN 80-7043-243

Internetové zdroje:

[10] Certifikace Apek [online]. 2008 [cit. 2010-03-02]. Apek.cz. Dostupné z WWW: <http://www.apek.cz/8482/2041/clanek/o-certifikaci-apek-certifikovany-obchod/>.

[11] Oborová certifikace [online]. 2007 [cit. 2010-03-02]. Národní rada pro certifikaci překladatelských služeb. Dostupné z WWW: <http://www.cepres.cz/index.php?action=3&action2=1>.

[12] E-Trust: QWeb [online]. 2009 [cit. 2010-03-02]. IQNet. Dostupné z WWW: <http://www.iqnet-ltd.com/index.php?liv1=5&liv2=63>.

[13] E-Trust: GoodPriv@cy [online]. 2009 [cit. 2010-03-02]. IQNet. Dostupné z WWW: <http://www.iqnet-ltd.com/index.php?liv1=5&liv2=62&liv3=1>.

[14] GoodPriv@cy. In GoodPriv@cy: Trustworthiness in business. Switzerland: IQNet, 1.7.2003 [cit. 2010-03-02]. Dostupné z WWW: <http://www.iqnet-ltd.com/userfiles/GoodPriv@cy/goodprivacy.pdf>.

[15] QWeb: Trust in e-business. In IQNet. Switzerland: IQNet, 15.4.2005 [cit. 2010-03-02]. Dostupné z WWW: <http://www.iqnet-ltd.com/userfiles/GoodPriv@cy/goodprivacy.pdf>.

[16] ITIL - IT Service Management Books [online]. 2006 [cit. 2010-03-02]. ITIL® and IT Service Management. Dostupné z WWW: <http://www.itil.org.uk/>.

[17] Euroskop.cz:Věcně o Evropě [online]. 2005 [cit.2010-03-03]. Vstup ČR do EU.Dostupné z WWW:<http://www.euroskop.cz/803/sekce/vstup-cr-do-eu/>.

[18] Technická harmonizace v Evropské unii. In ŠAFAŘÍK-PŠTROSZ, Alexander. Sborník dokumentů technické harmonizace: Nový přístup a globální přístup. svazek č.4. Praha: ÚNMZ, 2004. s. 11, s. 12. Dostupné z WWW:<http://www.unmz.cz/sborniky_th/04/0400.pdf>.

[19] Národní rada pro certifikaci překladatelských služeb: Oborová certifikace CEPRES:2007 [online]. 2007 [cit. 2010-03-03]. Dokumenty ke stažení. Dostupné z WWW: <http://www.cepres.cz/download/CEPRES_2007.pdf>.

Právní předpisy

[20] Česká republika. Zákon č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. In *Sbírka zákonů, Česká republika*. 21. září 2005, 143, s. 7526-7596. Dostupný také z WWW: <http://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=2005&typeLaw=zakon&what=Rok&stranka=5>.

[21] EU. Regulation (EC) No 764/2008 Of the European Parlament and of the Council. In Official Journal of the European Union. 13.8.2008, L218/21, s. 218. Dostupný také z WWW: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:218:0021:0029:EN:PDF>

[22] EU. Regulation (EC) No 765/2008 Of the European Parlament and of the Council. In Official Journal of the European Union. 13.8.2008, L218/30, s. 218. Dostupný také z WWW: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:218:0030:0047:EN:PDF>

Interní dokumenty

[23] Interní dokumenty společnosti ITC

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AAAO	Asociace akreditovaných a autorizovaných organizací
APEK	Asociace pro elektronickou komerci
AQAP	Allied Duality Assurance Publications
ASP	Application Service Providers (Aplikace poskytovatelů internetových služeb)
BRC	British Retail Consortium
B2C	Business to Consumer (vztah obchod-spotřebitel)
B2B	Business to Business (vztah obchod-obchod)
B2G	Business to Government (vztah obchod-vládní organizace)
C2G	Citizen to Government (vztah občané-vládní organizace)
CRAMM	CCTA Risk Analysis and Management Method
CWQC	Copany Wide Quality Control
ČOI	Česká obchodní inspekce
ČSN	České normy
EU	European Union (Evropská unie)
ES	Evropská společenství
EP	Evropský parlament
GQM	Global Quality Management
IS	Information system (Informační systém)
IFS	International Food Standard
ITSM	IT Service Management (Řízení služeb informačních technologií)
ISO	International Organization for Standardization
ISMS	Information Security Management System (Systém managementu pro zajištění bezpečnosti informací)
KS	Komunikační systém

MPO	Ministerstvo průmyslu a obchodu
NLF	New Legislative Framework (Nový legislativní rámec)
PDCA	Plan-Do-Check-Act (Plánuj-Dělej-Kontrolu-Jednej)
QS	Quality Standard (Standard kvality)
TQM	Total Quality Management (Řízení kvality)
ÚNMZ	Úřad pro technickou normalizaci, metrologii a státní zkušebnictví
VDA	Verand der Automobilindustrie

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM TABULEK

Nenalezena položka seznamu obrázků.