Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informačních technologií

Implementace konceptů ITIL do HZS ČR

Diplomová práce

Autor: Bc. Roman Fiedler
Studijní obor: K-IM-2

Vedoucí práce: Mgr. Josef Horálek, Ph.D.

Velké Poříčí duben 2015

Prohlášení:

Prohlašuji, že jsem diplomovou práci zpracoval samostatně a s použitím uvedených zdrojů a literatury.

Ve Velkém Poříčí dne 21. dubna 2015 Bc. Roman Fiedler

Poděkování:

Mé poděkování patří Mgr. Josefu Horálkovi, Ph.D., za odborné vedení, trpělivost, cenné rady a ochotu, kterou mi v průběhu zpracování diplomové práce věnoval. Poděkování patří též mjr. Ing. Martinu Řehákovi za spolupráci při získávání údajů pro praktickou část práce. V neposlední řadě také děkuji za podporu mé rodině a mé přítelkyni za jejich trpělivost, kterou mi věnovali při psaní práce.

Anotace práce:

Diplomová práce se zabývá analýzou a návrhem řešení implementace konceptů ITIL ve vybrané organizaci. Práce je rozdělena na dvě části. Teoretickou a praktickou.

V teoretické části se práce soustřeďuje na základní principy řízení informačních technologií a konceptů ITIL. Popisuje jednotlivé metodiky, rámce a uplatnění jednotlivých procesů.

Praktická část analyzuje stávající stav v organizaci a přináší podklady pro zlepšení a optimalizaci.

Annotation:

Title: Implementation of ITIL concepts to FR CZ

The diploma thesis deals with the analysis and proposal for a solution of ITIL concepts implementation in a chosen organization. The thesis is divided into two parts – the theoretical and practical one.

The theoretical part focuses on basic principles of IT management and ITIL concepts. It describes specific methodologies, framework and application of particular processes.

The practical part analyses the current state of the organization and provides groundwork for improvement and optimization.

Obsah

Úvod

V dnešní ekonomicky náročné době hledá organizace jakoukoliv možnost, jak snížit provozní náklady firmy na minimum. Efektivní používání vnitropodnikových procesů je jedním z nástrojů, jak lze tohoto stavu docílit. Nezbytnou součástí zefektivňujících procesů jsou informační a komunikační technologie (dále jen ICT). Tyto služby se již staly nedílnou součástí organizací a pouze málo z nich by se bez těchto služeb obešlo. Diplomová práce je zaměřena na prostředí Hasičského záchranného sboru Královéhradeckého kraje a zabývá se implementací metodického rámce ITIL do prostředí sboru. Navrhuje kroky založené nad metodickým rámcem ITIL, které povedou ke zlepšení stávajícího stavu.

Teoretická část práce obsahuje čtyři kapitoly. V první a druhé kapitole popisuje základní principy řízení informačních technologií z hlediska managementu. Druhá kapitola je rozšířena o další metodické rámce, jejich historii a základní struktury.

Třetí a čtvrtá kapitola jsou zaměřeny na seznámení se s koncepty ITIL v aktuální třetí verzi dle základních procesů. Metodický rámec ITIL je v současné době nejpoužívanější sbírka nejlepších praktik pro řízení IT služeb v rámci organizace. Na konci kapitoly je provedeno porovnání jednotlivých procesních rámců.

Praktická část se skládá ze dvou kapitol, které využívají poznatky z předchozích částí práce. Pátá kapitola se zabývá případovou studií implementace ITIL do prostředí Hasičského záchranného sboru Královéhradeckého kraje. Popisuje aktuální stav v prostředí organizace a analyzuje možná rizika při implementaci. Dále navrhuje vhodná opatření při zavádění správy softwarového majetku.

Druhá část praktické části se zabývá samotnou implementací Software Asset Managementu do prostředí Hasičského záchranného sboru a popisuje jednotlivé fáze zavádění příslušného software.

1 Principy IT managementu

Základním stavebním prvkem IT managementu je spojení znalostí z oblastí informatiky, marketingu, ekonomie a managementu. Náplní IT manažera není jenom informatika, jako je vývoj softwaru apod., ale zároveň zastává i funkci manažerů nebo vedoucích oddělení. Proto se také manažeři během svého studia věnují oborům jako je sociologie, mezinárodní obchod, komunikační dovednosti, psychologie, principy PR a další. [1]

1.1 Úkoly manažera IT

V této kapitole jsou vysvětleny důležité pojmy související s managementem informačních technologií.

1.1.1 Tým

Základním pilířem úspěchu manažera je jeho kvalitní tým, na který se může spolehnout. Dynamicky se tak kariérní postavení mění ruku v ruce s jeho podřízenými. Je to právě manažer, který řídí a plánuje, aby jeho podřízení plnili své termíny včas a v odpovídající kvalitě. Je to právě manažer, který svůj tým musí motivovat, podporovat a dle jejich výkonů i ohodnocovat.

IT manažer by měl úzce spolupracovat s personálním oddělením firmy, a to především při výběru nových kandidátů do svého týmu. Důležitý by měl být vstupní pohovor, který je úzce spojený s životopisem. Ovšem ne vždy je životopis opravdu pravdivý a není „vylepšený“.

Existují prý tři druhy lží: obyčejná lež, proklatě veliká lež a životopis. Proto mnoho lidí takový životopis hodně nadsadí. Ale i malá lež je také lež, jak můžeme vidět v následující tabulce. [1]

Pravdivý životopis	„Vylepšený“ životopis
Učitel informatiky - výuka základů informatiky na základní škole - teoretická i praktická výuka žáků - příprava testů a testovacích příkladů - vedení administrativní agendy spojené s výukou	**Profesor IT** - odborná výuka různých oblastí IT - zkoušení studentů - příprava osnov
Operátor Call centra - aktivní obvolávání stávajících zákazníků a nabídka produktů nadnárodních společností (operátoři, banky)	**Zástupce vedoucího provozu Call centra** - odpovědnost za velké zákazníky (operátoři, banky)
Kopáč na stavbě - kopání výkopů dle nakresleného plánku	**Stavbyvedoucí** - poradce architekta se specializací na stabilitu budovy

Tabulka 1: Běžný způsob „vylepšování“ životopisů[1]

Z vlastní zkušenosti mohu také čerpat. Mám kamaráda, který bez jakéhokoliv vysokoškolského titulu zkusil přijímací pohovor do jedné z největších firem v oblasti tvorby webových prezentací. Byl přijat jako junior web developer. Po 7 letech je z něj senior web developer a má svůj tým. Od mládí se totiž věnoval programování webových prezentací jako svému koníčku. Správný manažer tedy musí vybírat dle své intuice a dle osobního pohovoru.

[1] Zpracováno dle [1].

1.1.2 Manažer

IT manažer si musí uvědomit, že s programováním a vývojem softwaru je konec. Jednou z výhod IT manažera je fakt, že neztratí krok s neustále dynamicky se vyvíjejícími technologiemi.

Správný manažer musí být především vůdčí typ. Je to člověk, který za každé situace zachová chladnou hlavu a ví naprosto přesně, co má dělat. Nezbytná je přirozená autorita. Velice důležitou oblastí, kterou je nutno brát v potaz, je plán na další období, nebo chcete-li, strategie. Manažer si nesmí své myšlenky nechat pro sebe, ale jít s nimi ven. Strategie musí být dynamická a musí se přizpůsobovat aktuálním trendům a vyvíjet se společně s vývojem společnosti. Pokud se takový manažer nebude zúčastňovat vrcholových jednání vedení firmy, jen těžko bude schopen zajistit optimální požadovaný výsledek v oblasti IT. [1]

2 Řízení IT managementu

Výpočetní technika prodělala během dvacátého století mohutný rozvoj od sálových počítačů až po osobní počítače připojené do celosvětové sítě internet. Pomocí osobních počítačů, laptopů, chytrých telefonů a tabletů pronikají stále více do běžného života všech lidí. Lidé, ale i firmy, neustále pociťují čím dál větší nutnost využívání těchto technologií. Vidí potenciál ve využívání chytrých telefonů, přístupu k podnikovým sítím i z domu. Firmy si uvědomují, že využívání IT technologií jim umožňuje pracovat podstatně efektivněji a rychleji, a také náklady na výměnu dat mezi jednotlivými podniky se snížily. [2]

2.1 IT Governance

IT Governance je v oblasti IT technologií velice rozšířený pojem, který vyjadřuje dlouhodobý přístup k řízení informačních technologií v rámci organizace. Řízení IT chápe z pohledu taktického, strategického a operativního řízení služeb. IT Governance nám pomáhá sjednotit způsob řízení IT se strategií a cílem firmy v jeden celek. V podstatě se opírá o tvrzení, že IT Governance stejně jako metodiky a standardy jsou závislé a odpovědnost za ně nenesou pouze IT manažeři, ale odpovědnost nese také vrcholový management. Právě vrcholový management by se měl podílet na tvorbě IT strategie a držet dozor nad fungováním IT. [2]

2.2 Postavení informatiky ve firmě

Řízení IT patří mezi nejtěžší disciplíny díky neustále rostoucímu vývoji nových technologií. Nejčastějším problémem dnešního řízení IT ve firmě je přehlížení současných trendů managementem firmy. Vrcholový management nemá zájem o IT, nepřijde mu tato oblast důležitá, a tak odsunuje tuto oblast do střední vrstvy problémů. To může mít za následek nízkou konkurenceschopnost, a z toho plynoucí ohrožení firmy na trhu. Dalším problémem může být pojetí řízení IT. Vedení má sice zájem o IT a její rozšiřování, ale nemá jasný způsob řízení. V neposlední řadě může mít špatný dopad podceňování vlastních sil. Vedení firmy nedůvěřuje svým zaměstnancům a jejich znalostem. Proto si najme cizího dodavatele služeb, který ale nemusí být dostatečně detailně seznámen se specifiky firmy. To může mít za

následek, že vlastní nasazení nového systému bude řešeno direktivním způsobem namísto efektivního. Všechny tyto problémy jsou typickým rysem zastaralého způsobu řízení firmy. [1]

Způsob řízení IT musí jít ruku v ruce se strategií řízení firmy. Vzhledem k neustálému vývoji moderních technologií je nutné, aby se řízení IT přesunulo ze střední vrstvy do vrcholového managementu firmy. IT oddělení, včetně jejich manažera, by mělo detailně znát cíle firmy a spolupracovat na dalších strategických záměrech firmy. V případě této práce nasazení řízení IT do prostředí HZS (Hasičského záchranného sboru), kde není jednoznačně daná strategie firmy díky jejímu postavení jako bezpečnostní složky státu, je nutné se soustředit na budoucnost IT technologií, její bezpečnost a především co nejnižší poruchovost.

Hlavním problémem, před kterým stojí dnešní manažeři, je fakt, že firma chce snižovat náklady na pořízení IT, ale vyžaduje zvyšování výkonu. Což v naší oblasti není přímá úměrnost. Pro manažera je tak opravdu složité obhájit u vedení firmy vysoké investice do oblasti IT a to především do oblasti hardware. [1]

2.3 IT metodiky, rámce a standardy

Jak jsem zmínil v předchozích kapitolách, růst IT technologií vedl také k nutnosti zavedení a vzniku různých metodik, rámců a norem jako pomůcek pro řízení IT. [3]

- **Metodika** – metodikou se rozumí série několika doporučených postupů, které mohou být více či méně strukturované. Některé metodiky jsou přesně nastavené, jiné jsou benevolentní.

- **Rámec** – rámce jsou mnohem obsáhlejší než metodiky. Jedná se o „vodítko“ k budování něčeho (například aplikace, systému nebo metodiky).

    - ITIL – Information Technology Infrastructure Library
    - CobiT – Control Objectives for Information and related Technology

- MOF – Microsoft Operations Framework
- PRMIT – IBM Process Reference Model For IT

- **Standard** – jasně definovaný na základě sady metod nebo kritérií.
  - ISO 20000, ISO 9000 a další

Tyto metodiky a rámce budu porovnávat vzhledem k použití v praktické části práce, kde bude použit rámec ITIL na implementaci do firemního prostředí. Rámec ITIL tedy rozebírat nijak podrobně v této části kapitoly nebudu. V následujících kapitolách bude podrobně rozebrán na jednotlivé procesy.

2.3.1 CobiT

Druhým nejrozšířenějším rámcem řízení IT je rámec CobiT. Tento rámec byl vyvinut neziskovou a nezávislou organizací ISACA (Information System Audit and Control Association).[2] Organizace ISACA využívala při tvorbě standardů nejlepší zkušenosti řízení a auditu v oblasti informačních technologií. CobiT byl proto přijat jako všeobecný standard jak správně řídit, kontrolovat a provádět audit. [4], [5]

2.3.2 Historie CobiTu

V roce 1996 organizace ISACA vydala první sadu rámce pro řízení podnikové informatiky. V roce 1998 vydala druhé vydání, do kterého přidala postupy auditu, implementační sadu a detailní cíle IT procesů s rozpracovanou kontrolou. V roce 2000 vyšlo třetí vydání s přidáním manažerských postupů a došlo k aktualizaci rámce řízení podnikové informatiky. V témže roce přebírá organizaci pod svá křídla ITGI (IT Governance Institute). V roce 2003 je zpřístupněna on-line verze. V roce 2005 byla vydána čtvrtá verze, která v roce 2007 byla zaktualizována na verzi 4.1. Aktuální verzí je CobiT 5, která spojuje CobiT 4.1, Val IT 2.0 a Risk IT. [4], [5]

2.3.3 Struktura CobiTu

CobiT verze 5 je rámcem procesním. Definuje procesy řízení IT na čtyři domény, které obsahují třicet sedm procesů. Pro každý proces můžeme měřit

[2] ISACA. [online]. [cit. 2015-04-15]. Dostupné z: https://www.isaca.org/Pages/default.aspx

výkonnost a rizika spojená s navrženými kritérii. Všechny tyto procesy jsou, ale navrženy tak, aby při dosažení podnikových cílů byla minimalizována rizika pro jejich dosažení. Tyto čtyři procesní domény jsou[3] [5], [6], [7]:

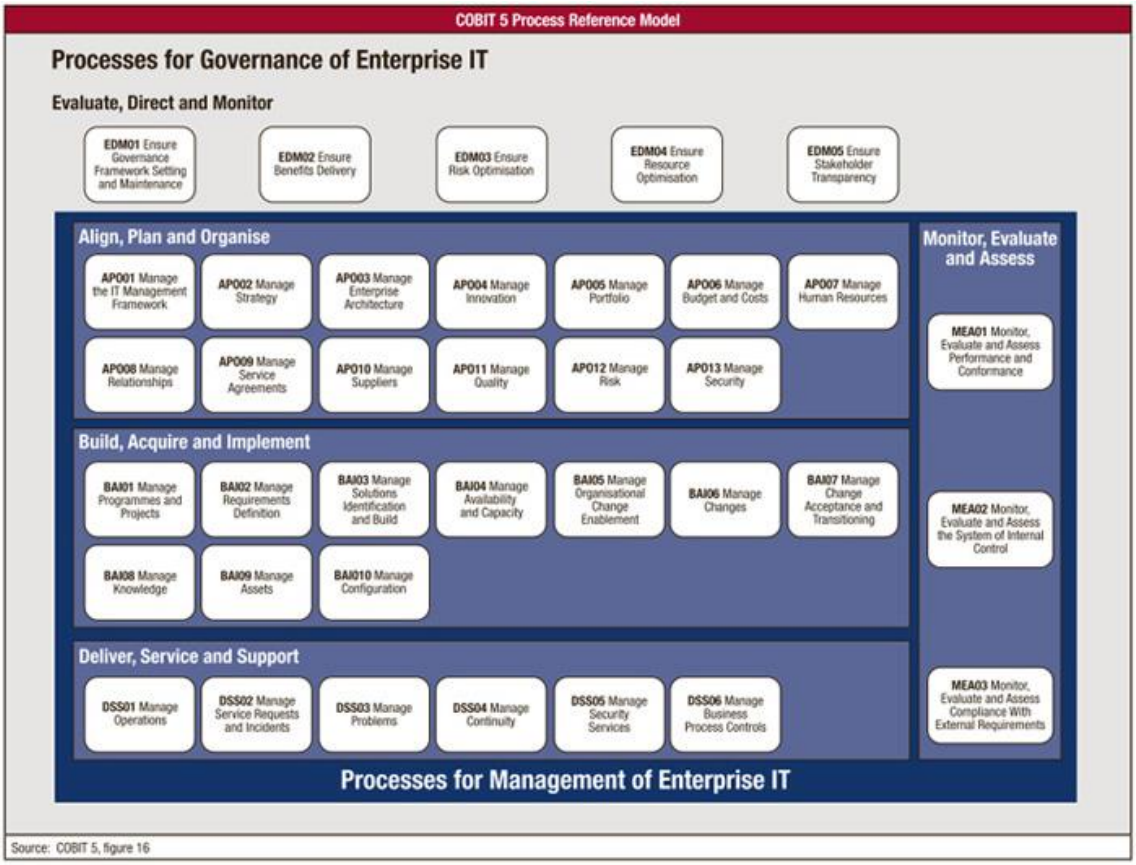
1. **Align, Plan and Organize (Příprava, plánování a organizace)** – oblast strategického a taktického plánování. Soustřeďuje se na co nejlepší způsoby využití informačních technologií v celkem 13 procesech.

2. **Build, Acquire and Implement (Stavění, pořízení a implementace)** – doména hledá vhodné řešení pro realizaci IT strategie, která vznikla v předchozí doméně. Implementuje navrhované řešení a udržuje jej funkční při zachování co nejdelší životnosti. Doména obsahuje celkem 13 procesů.

3. **Deliver, Service and Support (Dodávka, služba a podpora)** – třetí procesní doména se zabývá specifikací dodávky služby a řízením služeb IT od jejich poskytování až po podporu uživatelům. Zabezpečuje správu dat a řízení bezpečnosti služeb pomocí 10 procesů.

4. **Monitor, Evaluate and Assess (Monitorování, hodnocení a posouzení)** – doména se zabývá neustálou kontrolou, zda jsou aktuální služby stále v mezích požadavků organizace a to ve třech procesech. Všechny služby a procesy je nutno neustále kontrolovat a vyhodnocovat.

[3] Volně přeloženo autorem



Obrázek 1: Struktura CobiT 5[4]

Na obrázku č. 1 jsou znázorněny jednotlivé domény a jejich procesy dle rámce CobiT.

CobiT se zaměřuje na top manažery a auditory. Pro manažery je vhodným nástrojem k nalezení rovnováhy mezi investicemi, řízením IT a vzniku rizik. Auditorům pak poskytuje nástroje vedoucí při navrhování kontrol a jejich optimalizací. Proto se CobiT velice často používá jako nástroj auditu podnikové informatiky. CobiT je na rozdíl od ITIL více určen pro manažera IT, ale je také vhodným doplňkem rámce ITIL.

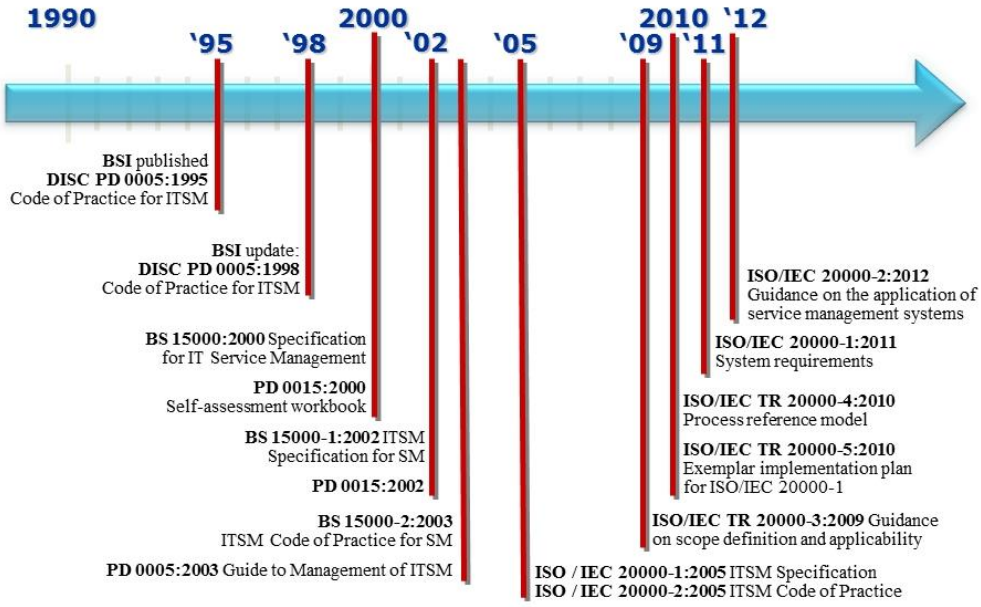
[4] Zdroj: ISANA Now. *ISACA Now* [online]. [cit. 2015-04-15].
Dostupné z: http://www.isaca.org/Knowledge-center/Blog/Lists/Posts/Post.aspx?ID=193

2.3.4 ISO 20000

Norma ISO je mezinárodní standard, který vydává organizace pro standardizaci ISO (International Organization for Standardization).[5] Norma je z velké části inspirována ITILem a obsahově se jím řídí. [9]

Organizace si může po aplikování norem ISO 20000 slibovat zefektivnění činnosti při poskytování IT služeb, řízení IT služeb od strategie až k vlastní tvorbě a tím získání konkurenční výhody na trhu. Také minimalizuje výpadky podstatným zvýšením kvality podnikových procesů. Vlastník certifikace ISO 20000 prokazuje, že organizace opravdu dodržuje principy ITILu. [9], [11]

2.3.5 Historie ISO 20000



Obrázek 2: Diagram historie ISO 20000[6]

[5] Zdroj: *ISO: International Organization for Standardization* [online]. [cit. 2015-04-15]. Dostupné z: http://www.iso.org/iso/home.html

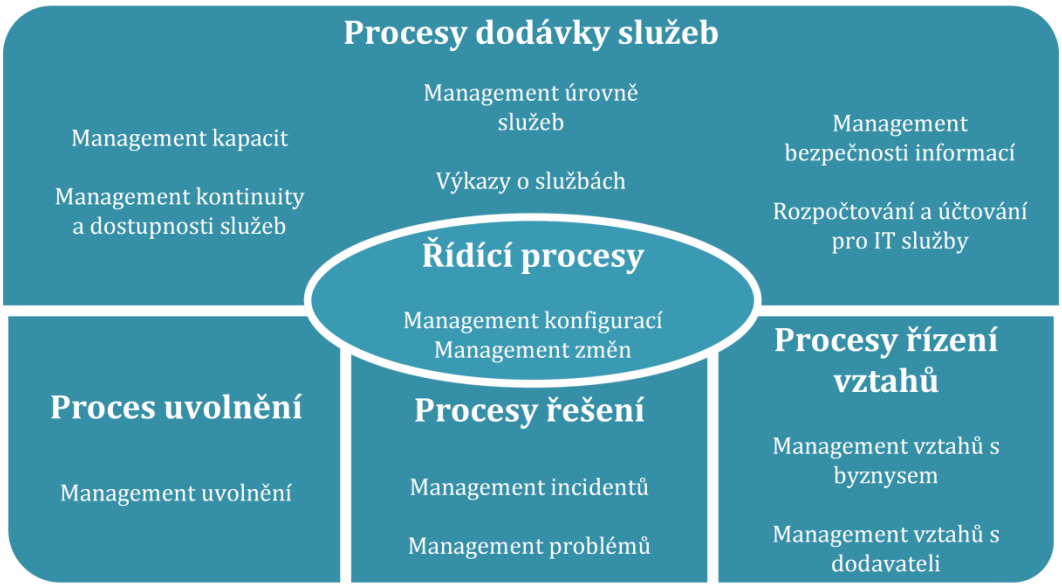
[6] Zdroj: [10]

V osmdesátých letech pracoval institut BSI (British standard institution) na sborníku řízení služeb. V roce 1995 vydal BSI publikaci nazvanou DISC PD 0005:1995, kterou v roce 1998 vydal aktualizovanou s názvem DISC PD 0005:1998.Tu tvořilo 13 procesů. V podstatě jsou to dnešní procesy, které tvoří normu ISO 20000. V roce 2000 vydal institut BSI další sbírku, která se jmenovala BS 15000:2000 a vytvořil tak standard shodný s ITIL v2, o kterém si řekneme více v kapitole 3. V roce 2005 vydal standard ISO 20000 a od té doby v podstatě vydává pouze aktualizace shodné s vývojem ITILu.

2.3.6 Struktura normy ISO 20000

Struktura ISO 20000 je tvořena dvěma částmi [9], [11]:

- ISO/IEC 20000-1:2005 Information technology – Service management – Part 1: Specification (specifikace řízení IT služeb)
- ISO/IEC 20000-2:2005 Information technology – Service management – Part 2: Code of Practise (praktická doporučení)



Obrázek 3: Struktura normy ISO 20000[7]

[7] Zpracováno a volně přeloženo ze [13].

Struktura se skládá ze čtyř procesních oblastí a jedné kontrolní oblasti (Řídící procesy). Norma převzala a mírně upravila procesy dle ITIL verze 2 a doplnila o procesy řízení vztahů a bezpečnosti. Obecně by se ale dalo říci, že norma ISO 20000 je plně v souladu s ITIL verze 2 a verze 3.

3 Koncepty ITIL

Odvětví IT služeb je často řízeno neefektivně a centrálně. Proto pro správné fungování IT služeb je zapotřebí řídit přímo IT služby. Toto řízení se nazývá IT Service Management (dále jen ITSM).

ITIL působí jako jeden z představitelů procesních rámců, který se těmito praktikami zabývá. Je to soubor světově nejuznávanějších praktik (best practice), který je založen na principu řízení. Celý soubor je poměrně rozsáhlý a především obsahuje doporučení jak tyto procesy implementovat, čeho se vyvarovat apod. Hlavní podstatou ITIL je souhrn doporučení, které vycházejí z praxe a jeho hlavním přínosem je mít tato doporučení v ucelené podobě. Tato ucelená podoba obsahuje v ITIL verze tři pět hlavních knih, které právě tento rámec obsahují. Tyto knihy jsou uspořádány do životního cyklu a mapují všechny principy, procesy, funkce, organizační a technologické aspekty. Jednotlivé verze ITIL budou nastíněny v následujících kapitolách. [14]

Mezi přední výhody ITILu se řadí například následující:

- Orientace poskytování služeb
- Využití již vymyšlených a osvědčených metodik
- Komunikace ve společnosti
- Flexibilita a škálovatelnost
- Měřitelná kvalita služeb
- Snížení rizik na úrovni procesů

3.1 Historie

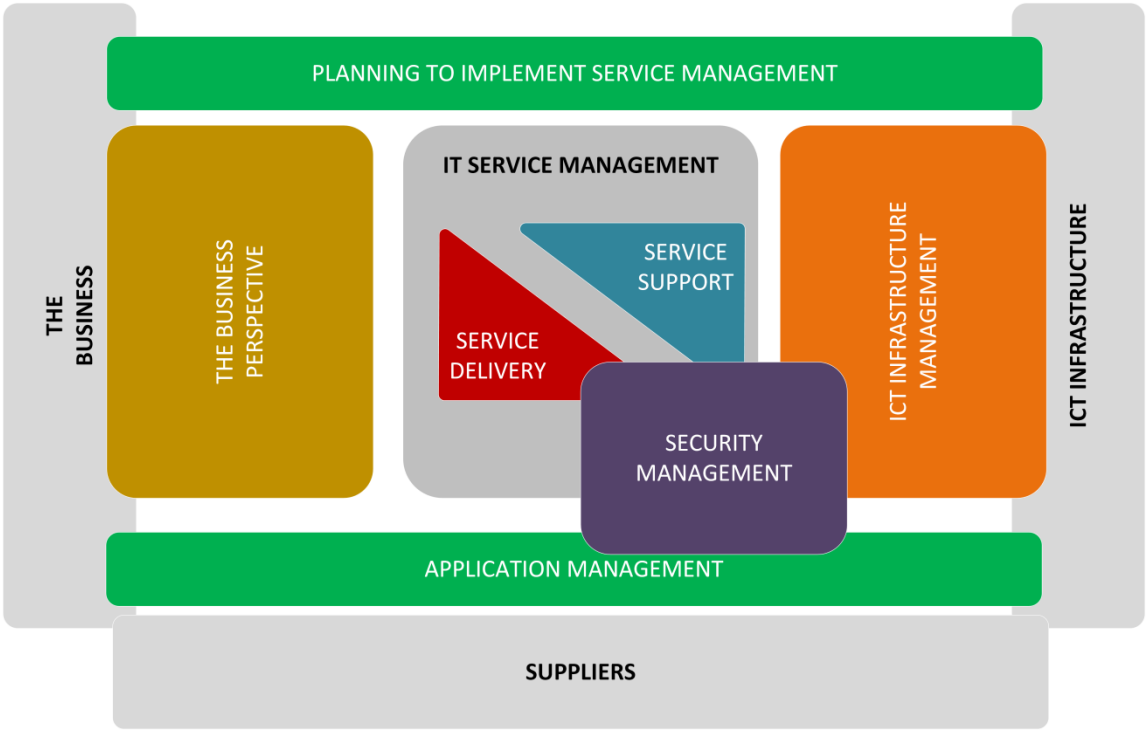
Počátky ITIL se datují až do 80. let minulého století. Firmy z celého světa řešily problémy se závislostmi na IT technologiích a s tím také souvisela otázka řešení kvality těchto služeb. Velká Británie a zaměstnanci její veřejné správy byli pověřeni vládou snížit ve státním sektoru náklady na IT. V roce 1986 odstartoval projekt Government Information Technology Infrastructure Management Method (GITIMM) pro zaměření v oblasti dodávky a podpory služeb IT. [14]

V roce 1989 vyšla první sbírka knih ITIL v1, která čítala čtyřicet šest knih o správě služeb IT. V 90. letech vzniká britská kancelář Office of Government Commerce (OGC), která sloučila prozatímní tři vládní agentury a sehrála nejdůležitější úlohu. Také v těchto letech vzniklo uživatelské fórum itSMF (IT Service Management Forum), které dodnes existuje. Toto fórum bylo komunitou pro profesionály a recenzenty a dodnes sdružuje IT manažery a ITSM specialisty.

V letech 1999 - 2004 byla v důsledku adaptace aktuální situace na poli IT vydaná zmodernizovaná, přepracovaná a rozšířená sbírka ITIL v2. Ta byla původně vydaná v osmi knihách. Klíčovým stavebním kamenem byly dvě knihy a to Service Support a Service Delivery. Někdy se také používá název Červená a Modrá kniha. Tyto dvě knihy převážně obsahují původních 46 knih a reprezentují prakticky kompletní IT Service Management. Podrobněji si povíme o ITIL v2 v následující kapitole. [14]

V roce 2004 zahájila britská kancelář OGC přípravu nové verze ITIL v3. Ta byla vydána v roce 2007. Tato verze přepracovala strukturu předešlé verze dle životních cyklů IT služeb. Předchozí verze totiž předpokládali

3.2 ITIL verze 2



Obrázek 4: Schéma ITIL verze 2[8]

ITIL ve verzi 2 obsahuje základních 8 knih. Vazby těchto knih je možné vidět na obrázku č. 4. Každá část je jinak barevně odlišena a věnuje se jí jedna publikace. Okolo těchto barevných částí je šedé okolí, které znázorňuje prostředí, kterého se dané publikace týkají. Tuto verzi zmíníme také, protože je stále mnoho firem, pro které je tato verze dostačující a používají ji v praxi. [15]

Publikace, které tvoří ITIL verze 2 a jejich základní přehled:

- **Service Support (Podpora služeb)** – každodenní podpora a údržba při poskytování IT služeb.

[8] Zdroj: ITIL - Information Technology Infrastructure Library. *TRIZ SIGMA* [online]. 2008 [cit. 2015-04-15]. Dostupné z: http://www.trizsigma.com/itil.html

- **Service Delivery (Dodávka služeb)** – procesy potřebné k plánování a dodání IT služeb v uspokojivé kvalitě. Jedná se o dlouhodobější plánování vedoucí k neustálému zlepšování.

- **ICT Infrastructure Management (Management infrastruktury ICT)** – popisuje řízení infrastruktury od zákaznických požadavků přes výběrová řízení, testování řešení, instalaci, nasazení a další rozšíření jednotlivých IT služeb.

- **The Business Perspective (Obchodní perspektiva) -** jedná se o návod pro pracovníky oddělení IT, jakým způsobem mohou přispět k plnění cílů firmy. Vede je k dalšímu poznání, jak by mohly jejich služby vést k maximalizování užitku firmy.

- **Planning to Implement Service Management (Plánování implementace managementu služeb)** – zabývá se popisem zavádění procesů ITIL do organizace. Jedná se především o úlohy plánování, zavedení a zlepšováním procesů managementu služeb v organizaci.

- **Security Management (Management bezpečnosti)** – detailně popisuje, jak zavést procesy řízení bezpečnosti informací a služeb na dané úrovni zabezpečení.

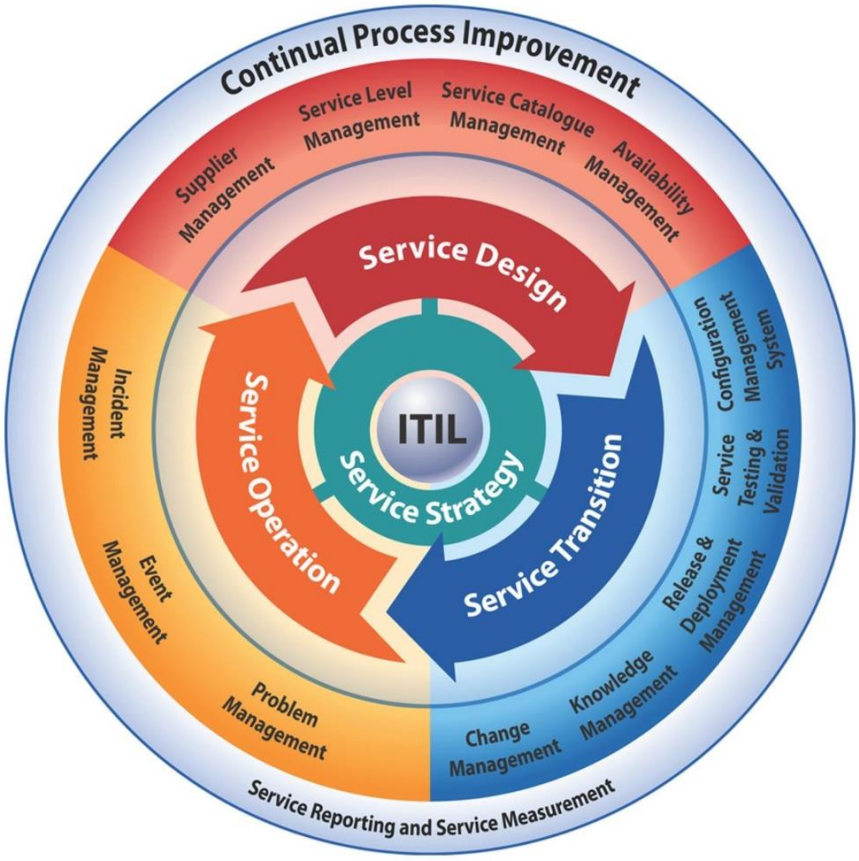
- **Application Management (Management aplikací)** – popisuje celý životní cyklus aplikace od sběru požadavků na aplikaci po její vývoj. Také popisuje řízení dodávky softwarových řešení).

- **Software Asset Management (Řízení softwarových aktivit)** – u verze č. 2 se jedná o doplňující blok, který popisuje efektivní řízení a správu infrastruktury softwarových aktivit ve všech fázích životního cyklu aplikací.

Srdcem celého rámce jsou dva základní moduly Podpora služeb a Dodávka služeb. Oba se staly nejpoužívanějšími knihami ITIL. Protože ITIL verze 3 vychází z verze 2, nebudu jednotlivé publikace podrobně vysvětlovat v této kapitole, ale v kapitole 4, kde se budu věnovat ITIL verzi 3.

4 ITIL verze 3

Pojem ITIL lze popsat mnoha definicemi, avšak nejvýstižnější je ta, která se nachází v oficiální knize o ITIL verzi 3. Ta říká, že ITIL je soubor konceptů a postupů, které nám umožní efektivněji plánovat, využívat a zlepšovat využití informačních technologií při zohlednění z pohledu zákazníka i dodavatele IT služeb.



Obrázek 5: Architektura ITIL a životní cyklus služby[9]

Celkovou architekturu ITIL verze tři znázorňuje obrázek č. 5. Knihovna ITIL se skládá ze třech částí. Jádro ITIL tvoří těchto pět knih a na obrázku č. 5 je představuje vnitřní kruh. Toto jádro představuje životní cyklus služby. [14], [15]

[9] Obrázek převzat z: Certificado Itil V3. *Certificado Itil V3* [online]. 2013 [cit. 2015-04-15]. Dostupné z: http://www.rogergrossi.com/certificado-itil-v3/

Výčet služeb, které jsou popsány v jednotlivých knihách ITIL:

- **Service Strategy (Strategie služeb)**– hlavní kniha ITILu, která je určena především pro top-management.

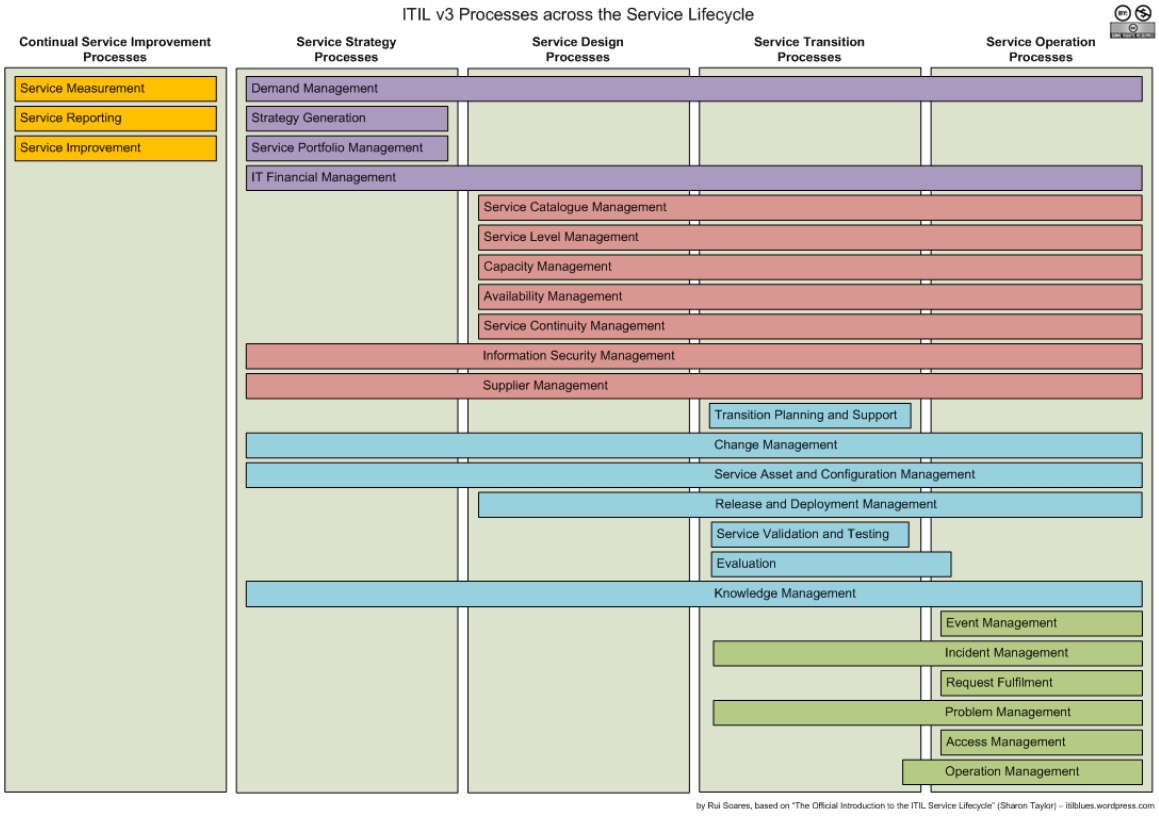
- **Service Design (Návrh služeb)** – popis návrhu procesů, jejichž cíl je navrhování takových služeb, které uspokojí aktuální i budoucí požadavky.

- **Service Transition (Přechod služeb)** – kniha, která popisuje proces zavedení služeb.

- **Service Operation (Provoz služeb)** – provoz služeb, který si klade za cíl poskytovat služby v požadované kvalitě.

- **Continual Service Improvement (Neustálé zlepšování služeb)** – kniha zabývající se neustálým zlepšováním služeb.

Nyní si jednotlivé knihy popíšeme podrobněji s ohledem na jednotlivé služby a jejich procesy.



Obrázek 6: Rozložení procesů napříč životním cyklem služby[10]

Obrázek č. 6 znázorňuje procesy jednotlivých knih ITIL dle životního cyklu služby. Zobrazuje také návaznost služeb a jejich prolínání.

4.1.1 Service Strategy (Strategie služeb)

Strategie služeb je první kniha z rámce ITIL. Je základem pro životní cyklus služby, kde vyvíjí, navrhuje a definuje její cíle a strategie. Funguje jako osa životního cyklu služby, která ovlivňuje všechny další fáze.

Jedná se o pět oblastí [14], [15]:

1. **Demand Management (Správa požadavků)** – porozumění a předvídání poptávky zákazníků po službách. Služba úzce spolupracuje se správou

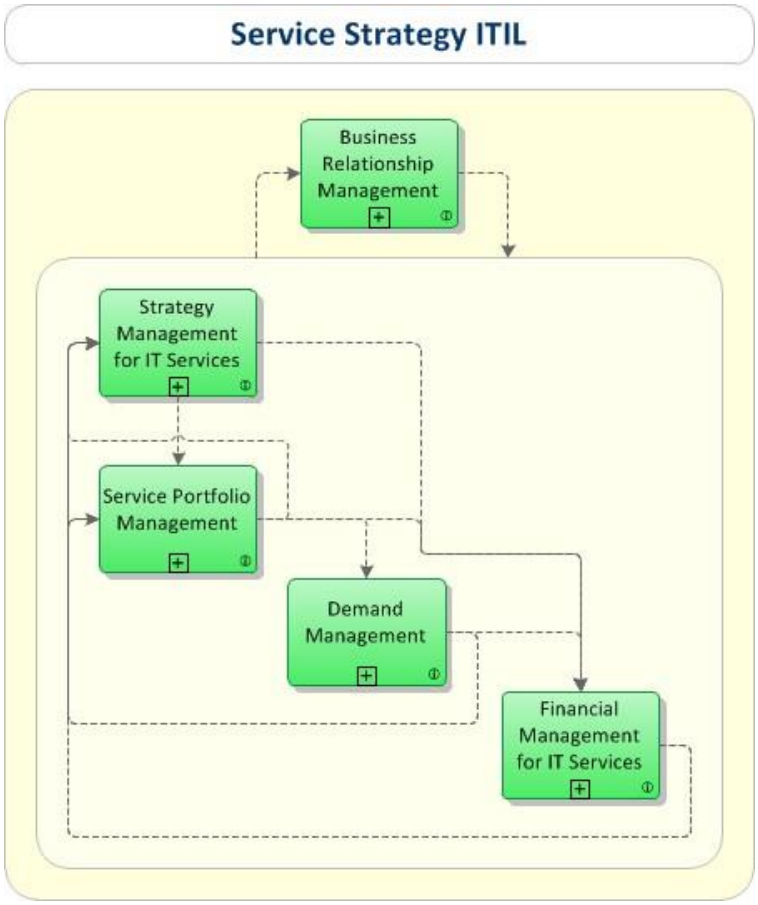
[10] Obrázek převzat z: ITIL 2011 edition Processes along the Service Lifecycle Diagram. *ITIL Blues* [online]. 2011 [cit. 2015-04-15]. Dostupné z: https://itilblues.wordpress.com/2007/10/13/itil-v3-processes-along-the-service-lifecycle-diagram/

kapacit (Capacity Management), aby zajistila, že poskytovatel služeb má dostatečnou kapacitu pro splnění požadované poptávky.

2. **Strategy Generation (Správa strategie služeb)** – strategie služeb si klade za cíl dlouhodobý přínos pro zákazníka. Říká, jak správně vytvořit strategii služeb ve všech životních cyklech služby.

3. **Service Portfolio Management (Správa portfolia služeb)** – řízení a správa sbírky služeb. Zajišťuje, aby poskytovatel služeb měl správnou kombinaci služeb a aby splnil všechny požadované obchodní výsledky na odpovídající úrovni investic.

4. **IT Financial Management (Správa financí služeb IT)** – správa rozpočtu, účtování a požadavků poskytovatele IT služeb.



Obrázek 7: Diagram Service Strategy[11]

4.1.2 Service Design (Návrh služeb)

Návrh nových služeb nebo úprava a vylepšení stávajících služeb. Procesy, které obsahuje návrh služeb [14], [15]:

1. **Service Catalogue Management (Správa katalogu služeb)** – proces, který odpovídá za udržování přesných informací katalogu služeb. Zároveň také zajišťuje dostupnost tohoto katalogu těm, kteří jsou oprávnění k němu přistupovat.

2. **Service Level Management (Správa úrovně služeb)** – proces, ve kterém se smluvně vyjednávají dohody a požadavky zákazníků. Dále proces zahrnuje kontrolu dodržování těchto smluvních podmínek.

[11] Obrázek převzat z [16].

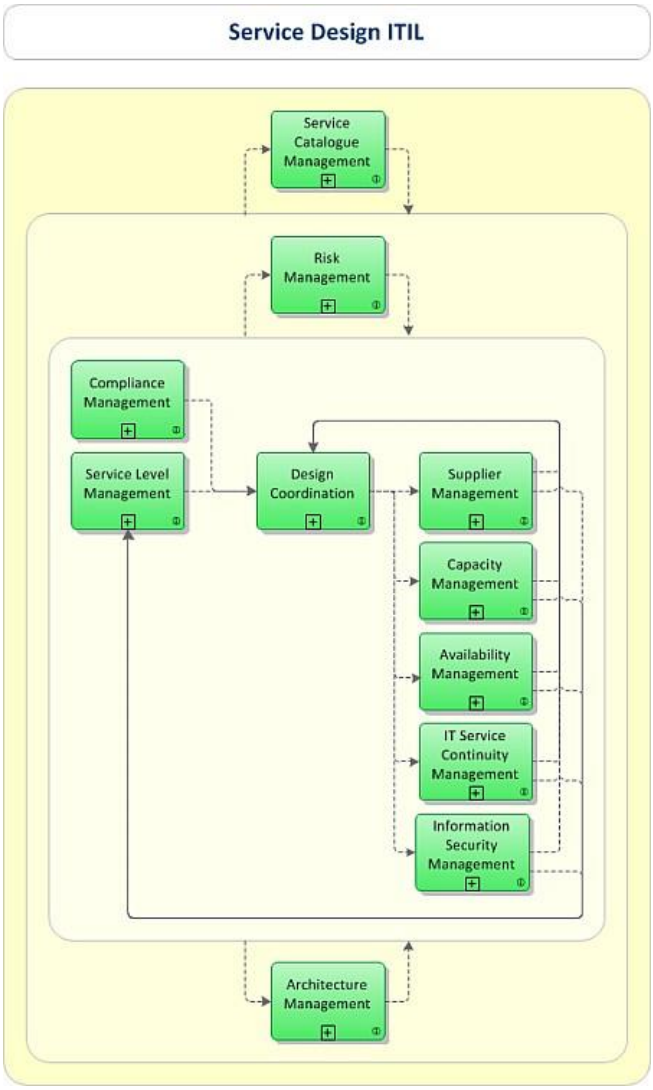
3. **Capacity Management (Správa kapacit)** – správa kapacit je proces, který odpovídá za to, že budou kapacity IT služeb dosahovat dohodnutých cílů při přiměřených nákladech a včas. Správa kapacit bere v úvahu všechny zdroje potřebné pro dodávku služeb při krátkých, středních a dlouhodobých požadavcích.

4. **Availability Management (Správa dostupnosti)** – správa dostupnosti zodpovídá za to, aby všechny služby odpovídaly dohodnuté dostupnosti. Klade si za cíl definovat, analyzovat, plánovat, měřit a zlepšovat všechny aspekty dostupnosti IT služeb.

5. **Service Continuity Management (Správa kontinuity služeb)** – správa kontinuity služeb vede k opatření ke snižování rizik, která by mohla vážně ohrozit IT služby. Poskytovatel zajišťuje poskytnutí minimální dohodnuté úrovně služeb a omezuje rizika v případě mimořádných událostí na přijatelnou úroveň.

6. **Information Security Management (Správa bezpečnosti informací)** – správa bezpečnosti informací umožňuje řešení bezpečnosti informací pro organizaci. Jedná se o velmi důležitou součást všech procesů. Správa bezpečnosti informací je integrována ve strategické, taktické i provozní úrovni.

7. **Supplier Management (Správa dodavatelů)** – proces zajišťující dodržení všech smluv mezi dodavatelem a zákazníkem. Aby mohl zákazník dosáhnout předem stanovených cílů, musí dodavatelé plnit veškerá ujednání, která mají dohodnutá ve smlouvách.



Obrázek 8: Diagram Service Design[12]

4.1.3 Service Transition (Přechod služeb)

Cílem úkolu přechodu služby je dodat služby požadované kvality. Je to část ITILu, která se zabývá zavedením služby do provozu. Do tohoto procesu patří kroky, které pracují s managementem zdrojů, testování, implementací a další aktivity spojené s nasazením služby. [14], [15]

[12] Obrázek převzat z [16]

1. **Transition Planning and Support (Plánování a podpora přechodu)** – plánování a podpora přechodu připravuje celkový plán nasazení a přechodu služby v rámci předpokládaných nákladů a přiměřeného času.

2. **Change Management (Správa změn)** – správa změn si klade za cíl řízení cyklu změn. Primárně se snaží o minimalizaci počtu výpadků a incidentů s minimálním narušením IT služeb.

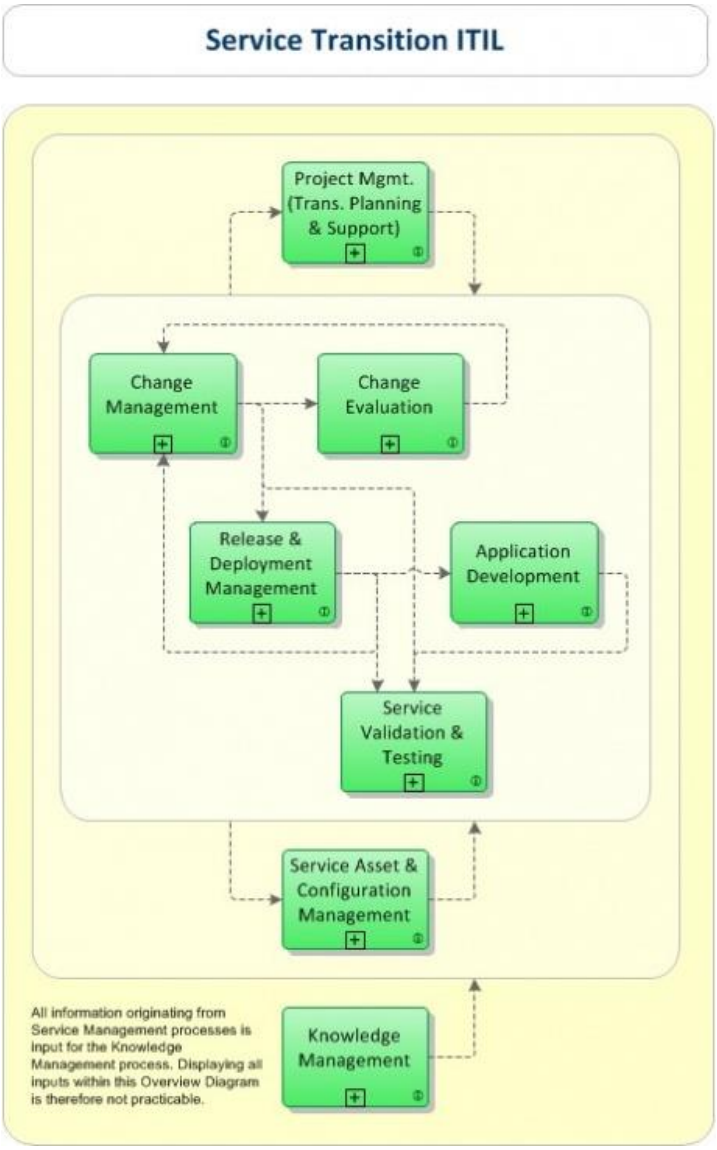
3. **Service Asset and Configuration Management (Správa aktiv služeb a konfigurací)** – správa aktiv služeb a konfigurací udržuje informace o konfiguracích potřebných pro poskytování IT služeb a zajišťuje, aby tyto informace byly správné.

4. **Release and Deployment Management (Správa releasů a provozního nasazení)** – správa releasů a provozního nasazení má za cíl plánování a řízení sestavení včetně testování v reálném prostředí. Musí při tom dodržet původní zadání zákazníka.

5. **Service Validation and Testing (Validace a testování služby)** – validace a testování služby zajišťuje, aby nasazená verze služby splňovala očekávání dle požadavků zákazníka. Ověřuje zda při dodání nebo změně služby právě tyto požadavky splňuje.

6. **Change Evaluation (Vyhodnocení změny)** – vyhodnocení změny má za cíl zhodnocení významných změn, vyhodnocení zavedení nové služby nebo zásadní změny v již zavedených službách.

7. **Knowledge Management** (**Správa znalostí)** – správa znalostí shromažďuje, analyzuje, ukládá a sdílí veškeré informace získané v rámci organizace. Je potřeba mít tyto informace k dispozici v co nejkratším možném čase. Hlavním úkolem správy znalostí je zlepšit účinnost služby tím, že sníží potřebu znovu objevovat nové znalosti.



Obrázek 9: Diagram Service Transition[13]

4.1.4 Service Operation (Provoz služeb)

Čtvrtá kniha rámce ITIL se zaměřuje na splnění požadavků při dodání uživateli. Toto dodání musí splňovat požadavky na kvalitu. Monitoruje selhání služby a také spojení nákladů s provozem. [14], [15]

1. **Event Management (Správa událostí)** – proces správa událostí analyzuje a monitoruje konfigurační služby. Nabízí možnosti včasného odhalení

[13] Obrázek převzat z [16]

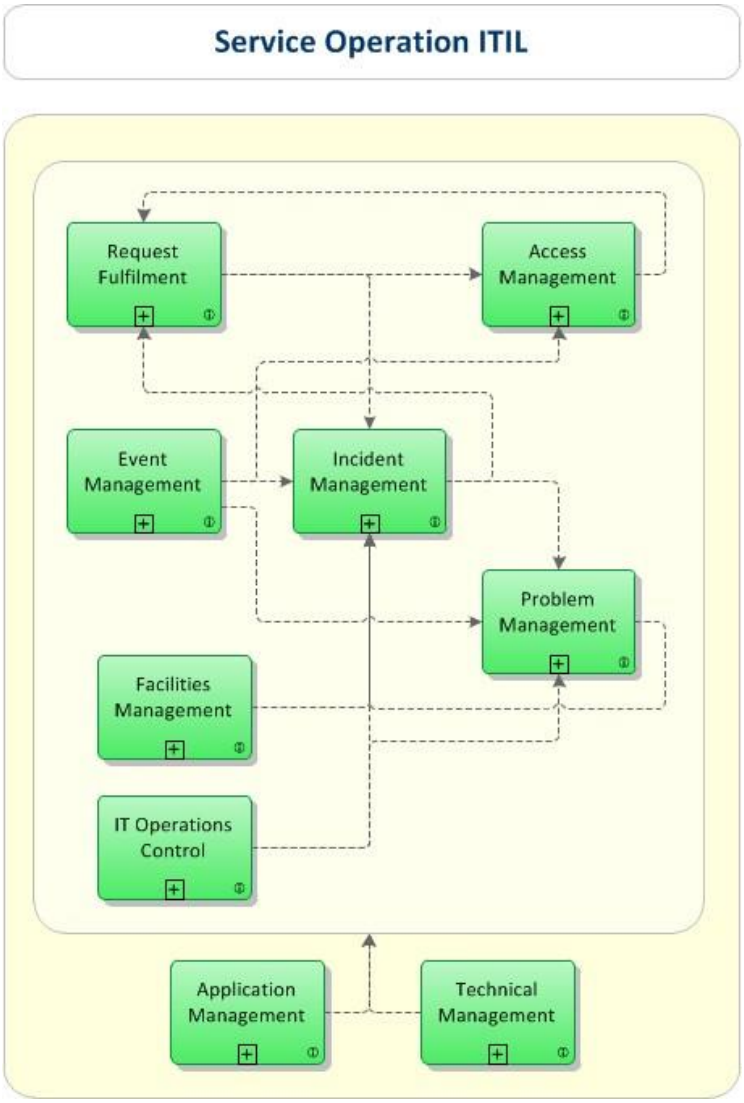
problémů a incidentů. Třídí akce s cílem kvalitně rozhodnout o vhodných opatřeních.

2. **Incident Management (Správa incidentů)** – proces správa incidentů se zaměřuje na správu životního cyklu incidentů. Analyzuje a monitoruje poruchy služeb tak, aby je bylo možné obnovit co nejdříve do původního stavu.

3. **Request Fulfilment (Plnění požadavků)** – proces plnění požadavků je odpovědný za řízení životního cyklu všech žádostí o službu.

4. **Problem Management (Správa problémů)** – správa problémů řídí životní cyklus všech problémů. Jejím primárním cílem je zamezit výskytu incidentů a minimalizovat jejich dopad. Proces správa problémů také analyzuje záznamy o již uskutečněných incidentech, a to od jeho identifikace až po odstranění příčiny problémů.

5. **Access Management (Správa přístupů)** – správa přístupů si klade za cíl poskytnout oprávněným uživatelům právo na použití služby a zároveň zabránit k přístupu neautorizovaným osobám. K řízení přístupu využívá politiky vymezené ve správě informační bezpečnosti.



Obrázek 10: Diagram Service Operation[14]

4.1.5 Continual Service Improvement (Neustálé zlepšování služeb)

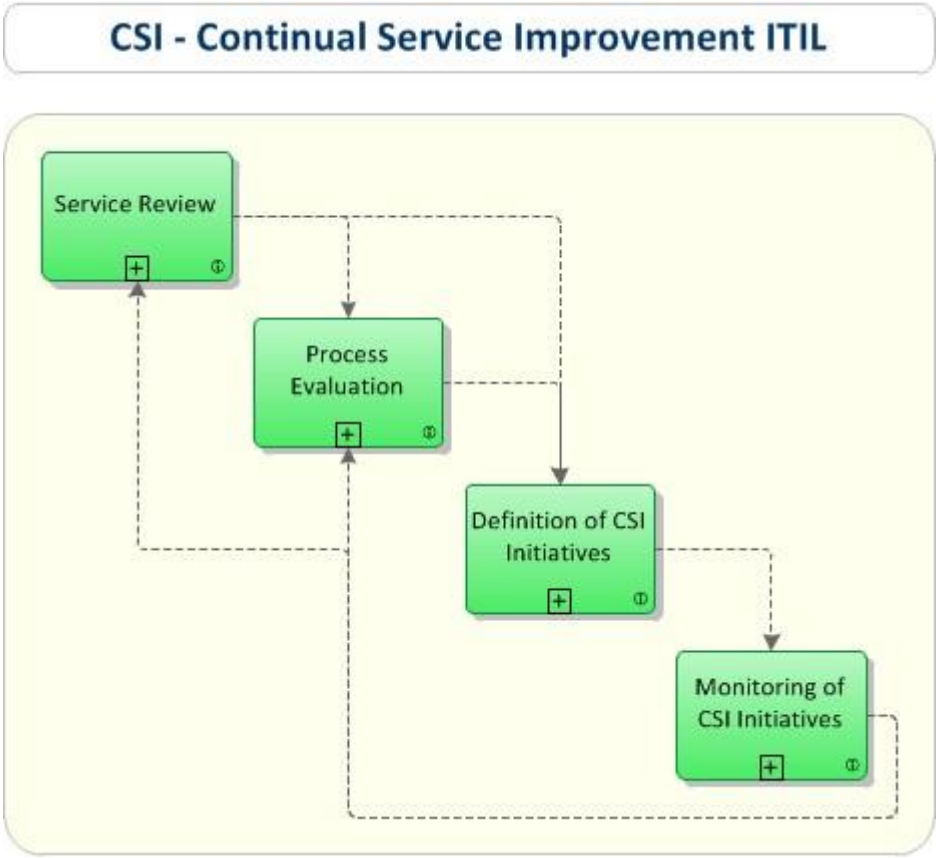
Pátá kniha popisuje procesy, které využívají metody v oblasti řízení kvality. Klade si za cíl neustálé zlepšování efektivity procesů na základě minulých úspěchů a neúspěchů. [14], [15]

1. **Service Measurement (Měření služby)** – monitorování a měření je základním předpokladem pro správu služeb a procesů.

[14] Obrázek převzat z [16]

2. **Service Reporting (Hlášení služby)** – služba, která zabezpečuje veškeré činnosti, které dodávají výkazy o výkonech služeb a porovnává je s určitou úrovní služeb.

3. **Service Improvement (Zlepšení služby)** – proces, který v sobě zahrnuje proces zlepšování služeb v sedmi krocích, které jsou požadované pro sběr a analýzu dat.



Obrázek 11: Diagram CSI[15]

[15] Obrázek převzat z [16]

4.2 ITIL verze 3 jednoduše

Pro jednoduší pochopení a seznámení se s jednotlivými procesy ITIL cituji konkrétní příklad převzatý z [17].

„Uživateli nefunguje aplikace a závadu hlásí na Service Desk (z pohledu ITIL je Service Desk funkce, jejíž pojem jsme si definovali výše). Service Desk zakládá ve svém systému tzv. incident, který řeší v rámci procesu ***Incident Management.*** *Tento incident však byl IT již jednou řešen a způsob řešení byl příslušným pracovníkem popsán a díky výstupům z procesu* ***Knowledge Management*** *operátor Service Desku snadno dohledá, že existuje řešení v podobě workaroundu, takže služba (rozuměj funkčnost aplikace) může být obnovena velice rychle (ITIL o všem, co IT poskytuje, hovoří jako o službě) v souladu s uzavřeným SLA a incident může být uzavřen. Vše, co souvisí SLA, je řešeno v rámci procesu* ***Service Level Management.*** *Vzhledem k tomu, že stále více uživatelů hlásí na Service Desk stejnou závadu, rozhodne se Service Desk založit ke stávajícím incidentům tzv. „problem“, který by měl odhalit skutečnou příčinu závady. Tím se startuje proces* ***Problem Management.*** *Ještě téhož dne je příčina závady odhalena. Bude nutné přepsat kód jedné knihovny, kterou aplikace používá. Tím se rozjíždí proces* ***Change Management.*** *Úprava knihovny vývojářům netrvala dlouho. Po důkladném otestování je k dispozici nová verze, která může být nasazena nejen na stanice postižených uživatelů, ale všem, kteří aplikaci používají. Uvolnění a nasazení nové verze popisuje proces* ***Release and Deployment Management****. IT musí vědět, na jakých stanicích je daná aplikace nainstalována, aby mohlo provést její upgrade na novou verzi. Vzhledem k tomu, že naše IT má zaveden proces* ***Service Asset and Configuration management****, má přehled nejen o veškerém majetku, ale i o vazbách mezí jednotlivými komponentami, takže to pro něj nebude problém. V okamžiku, kdy je na všech stanicích nainstalována nová verze aplikace, objeví se tato informace i v databázi Asset and Configuration Management nástroje a Service Desk „problem“ uzavírá. Ve stejnou dobu však do firmy nastupuje nový zaměstnanec a jeho manažer žádá o instalaci aplikace, kterou našel v katalogu služeb, které IT nabízí. Netřeba asi dodávat, že katalog je udržován v rámci procesu* ***Service Catalogue Management****. Tento požadavek již nemusí nikdo další schvalovat a tak je tento*

*požadavek řešen v rámci procesu **Request Fullfilment**. Prostřednictvím aplikace však uživatel přistupuje k datům o zákaznicích firmy a proto musí být jeho přístup k datům řízen. Manažer proto o příslušné přístupy požádá v rámci procesu **Access Management**. V aplikaci pracuje velké množství uživatelů a databáze, kterou aplikace využívá, obsahuje čím dál tím více dat. Je zřejmé, že stávající HW nebude v brzké době stačit a bude nutné provést upgrade dříve, než systém spadne. Je zřejmé, že se není možné soustředit jen na zajištění aktuální dostupnosti IT služeb v rámci procesu **Availability Management,** ale je nutné myslet i na budoucnost a včas alokovat potřebné zdroje, čemuž by se měli věnovat odpovědní pracovníci v rámci procesu **Capacity Management.** Toto IT však nechce spoléhat jen na to, že incident někdo nahlásí, ale raději by incidentům předešlo a proto používá monitorovací nástroje, které odpovědným pracovníkům zasílají hlášení o nestandardních událostech v systému, toto se řeší v rámci procesu **Event Management.** Firma si je vědoma, že v jejich systémech jsou obsažena cenná data, která ohodnotila v rámci Business Impact Analysis a proto věnuje dostatek pozornosti vypracování plánů kontinuity pro případ útoku, havárie nebo přírodní katastrofy v rámci procesu **IT Service Continuity Management**. Mnohým bezpečnostním incidentům však může společnost předejít implementací základní sady opatření v rámci procesu **Information Security Management**, jehož cílem je zajistit bezpečnost informací během celého jejich životního cyklu. Ne všechny služby si je však firma schopna zajistit sama a proto využívá služeb mnoha různých dodavatelů, které řídí v rámci procesu **Supplier management.** Aby IT mohlo dodávat službu, kterou si zákazník objednal, musí se věnovat běžné správě a o tom pojednává proces **IT Operations Management**. Návrhu infrastruktury se věnuje proces **Technical Management**, samotným aplikacím se pak logicky věnuje proces **Application Management**. Je zřejmé, že všechno něco stojí a někdo musí finance spravovat a na to máme proces **Financial Management**. Pokud jde o proklamované soustavné zlepšování, nejedná se v podstatě o nic jiného, než o klasický Demingův PDCA cyklus uplatňovaný na všechny procesy a služby, jejichž vyzrálost můžeme měřit např. za použití CMM (Capability Maturity Model) v rámci procesu **Service Measurement** a výsledky těchto měření poté analyzovat a prezentovat v rámci procesu **Service Reporting**."*

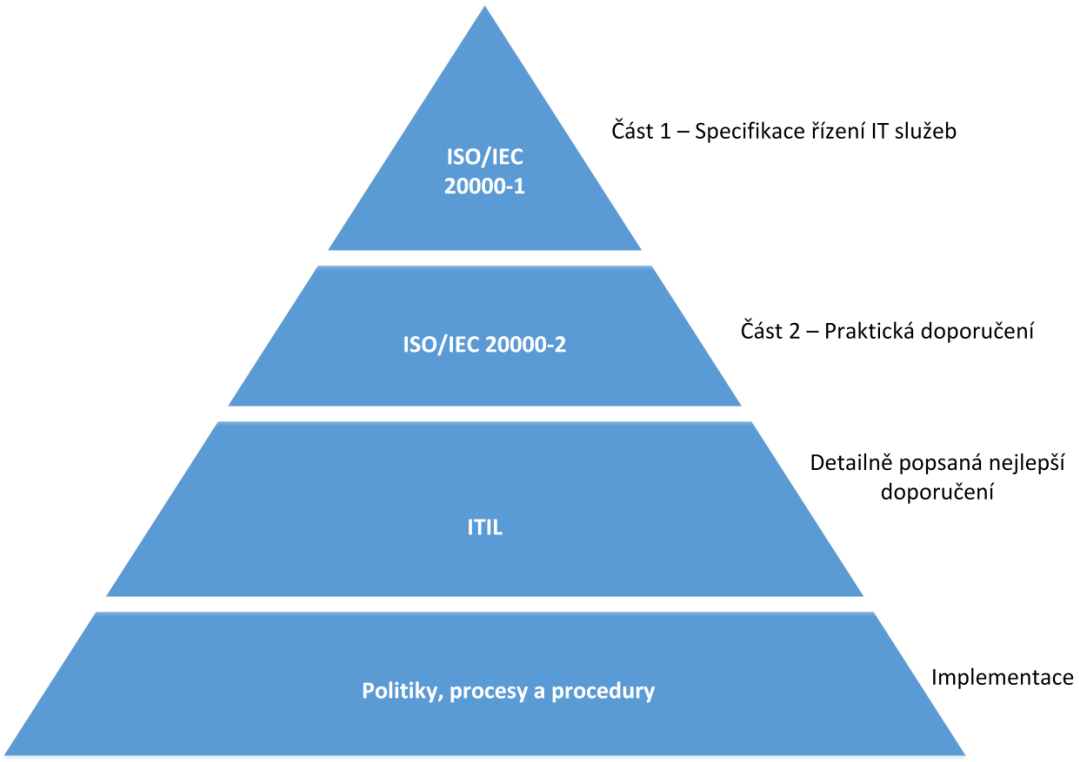
4.3 Porovnání ITIL v2 a ITIL v3

Při porovnání obou verzí jsem zjistil, že hlavní myšlenky knihovny verze 2 jsou obsaženy také ve verzi 3, ale z jiného úhlu pohledu. Hlavní dvě knihy ve verzi 2 na rozdíl od ostatních knih mají strukturu rozdělenou na procesy. Na rozdíl od verze 3, která nemá procesní strukturu a tím je čtení informací z nich problematičtější. Proto jsem také popsal knihovnu ITIL verze 3 podrobně, aby vynikl obsah jednotlivých procesů. Obě verze, ale vycházejí z procesního přístupu k řízení IT služeb. Třetí verze není tolik direktivní, jako tomu bylo ve verzi 2. Zabývá se spíše řízením životního cyklu služby, na rozdíl od řízení podnikové informatiky. Při návrhu služeb je kladen velký důraz na budoucí hodnotu pro cílového zákazníka.

Hlavním a základním rozdílem tedy je, že ve verzi 2 byly nejdříve popsány procesy jednotlivě a až později byla uspořádaná spojitost mezi nimi. Verze 3, jak jsem již zmínil, se zabývá řízením životního cyklu služby, a tak se mohou jednotlivé procesy objevit i vícekrát v různých kapitolách nebo knihách. [18]

4.4 Porovnání ITIL a ISO 20000

ISO 20000 a ITIL jsou, jak již jsem zmínil, v kapitole 2.3.6. ISO 20000 vychází z ITILu a také se na něj odkazuje ve svých publikacích. ISO 20000 popisuje „co“ musí organizace splňovat a ITIL říká „jak“ toho dosáhnout. ISO 20000 není tedy přímo metodikou, ale standardem, který slouží k certifikaci organizací. [11], [14]



Obrázek 12: Vztahy mezi ISO 20000 a ITIL[16]

Vztahu ITILu a ISO 20000 je možno také vidět na diagramu výše. Pokud organizace chce být certifikována dle ISO 20000, musí zavést všechny procesy v první části normy. Na rozdíl od toho v ITILu organizace zavádí pouze vybrané části. Certifikaci ISO dostává organizace jako celek, u ITIL certifikaci získávají jednotlivci.

4.5 Porovnání ITIL a CobiT

Hlavním rozdílem je, že ITIL je nástrojem ICT oddělení společnosti a jejího IT managementu. CobiT jako nástroj ICT používá vrcholový management (tzv. IT Governance). Z toho vyplývá, že CobiT má širší uplatnění než ITIL. Velice zajímavé je vzájemné doplňování ITILu a CobiTu. Strategické dlouhodobé řízení může být implementováno pomoci CobiT, ale operativní procesy dle ITIL. Oba dva rámce jsou vzájemně kompatibilní. Dalším podstatným rozdílem je, že CobiT nevychází z praxe, ale je dílem několika profesionálních auditorských společností.[17] Proto mohou být

[16] Zdroj: ISO/IEC 20000 and ITIL. *TSO Shop* [online]. 2015 [cit. 2015-04-15]. Dostupné z: http://www.tsoshop.co.uk/parliament/bookstore.asp?FO=1229332&DI=571307
[17] ISACA. [online]. [cit. 2015-04-15]. Dostupné z: https://www.isaca.org/Pages/default.aspx

procesy CobiT hůře pochopitelné, oproti procesům dle ITIL. Hlavní výhodou CobiT je ale fakt, že publikace jsou volně dostupné ke stažení na internetu.

5 Případová studie implementace ITIL do HZS KH kraje

5.1 Charakteristika organizace

Hasičský záchranný sbor Královéhradeckého kraje patří do Integrovaného záchranného systému České Republiky. Poslání hasičů chránit životy, zdraví obyvatel a jejich majetek před mimořádnými událostmi je základním stavebním prvkem organizace. Dále se také HZS Královéhradeckého kraje zabývá státním požárním dozorem, prevencí a řízením krizových událostí. To by v dnešní době nebylo možné bez výpočetních systémů a proto je součástí organizace i oddělení ICT. Výpočetní systémy se v organizaci používají na všech úsecích napříč organizací.

5.2 Organizační složky organizace

Ředitel HZS Královéhradeckého kraje

Zodpovídá za problematiku informační bezpečnosti HZS KH kraje vůči nadřízeným a kontrolním orgánům.

Top-Management (náměstci ředitele a ředitel kanceláře ředitele)

Za strategii rozvoje a plánování ICT v rámci HZS KH kraje je zodpovědný náměstek úseku IZS a operačního řízení. Strategické záměry a plány týkající se informační bezpečnosti předkládá ke schválení krajskému řediteli. V rámci jednotlivých organizačních úseků má primární zodpovědnost za bezpečnost provozovaných informačních systémů příslušný náměstek nebo ředitel kanceláře.

Ostatní vedoucí pracovníci

Vedoucí pracovníci všech stupňů definovaní organizačním řádem HZS KH kraje odpovídají za realizaci bezpečnostní politiky v rámci své působnosti.

Vedoucí pracovníci odpovídají za kontrolu dodržování stanovených zásad v každodenní praxi jejich podřízených a za aplikaci postihů v případě nedodržení těchto zásad.

Správci systémů informačních a komunikačních technologií

Správce systémů informačních a komunikačních technologií (dále jen „administrátor ICT“) je určený příslušník, jehož úkolem je odborná správa, obsluha a údržba systémů ICT.

Administrátor ICT odpovídá za provoz ICT v souladu s platnými pracovními postupy. Je povinen ve své činnosti prosazovat informační bezpečnost stanovenou bezpečnostní politikou a bezpečnostní dokumentací.

Aby administrátor ICT mohl úspěšně vykonávat svoji práci, musí být náležitě kvalifikován. Je povinen se stále odborně vzdělávat a sledovat nejnovější vývoj v oblasti svěřených technologií tak, aby byl schopen samostatně reagovat na nově vznikající rizika v IS. Ve spolupráci s bezpečnostním správcem a bezpečnostním manažerem navrhuje opatření přesahující jeho působnost k zajištění informační bezpečnosti IS.

Administrátor ICT má ve své roli zpravidla určeného zástupce. Seznam administrátorů ICT a jejich zástupců je vydáván pokynem krajského ředitele.

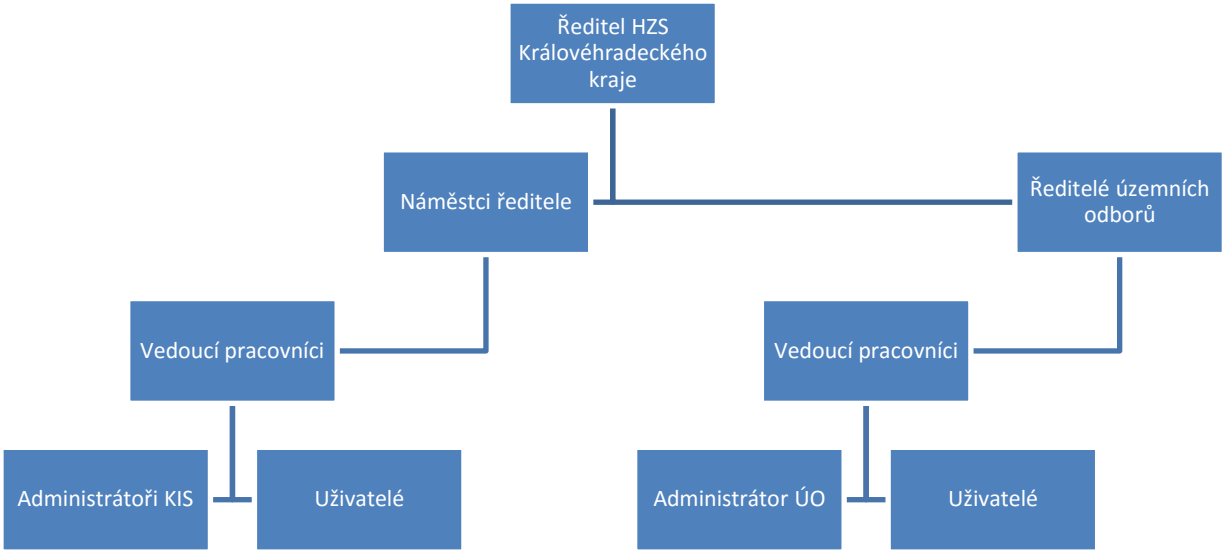
Uživatelé informačního systému

Uživatelé informačního systému jsou fyzické osoby, které mají právo v předem definovaném rozsahu používat prostředky informačního prostředí, zejména využívat a pořizovat informace.

Uživatelem informačního systému může být:

- Příslušník ve služebním poměru nebo občanský zaměstnanec v pracovním či obdobném poměru k HZS KH kraje; základní rozsah informací potřebných k výkonu činností příslušných funkčnímu místu zaměstnance a rozsah přístupu tohoto uživatele k informacím v informačním systému je stanoven v popisu jeho pracovní náplně.

- Jiná fyzická osoba, které byl povolen přístup k informačnímu prostředí HZS KH kraje na základě formálního smluvního nebo na jiné úrovni definovaného vztahu, který přesně stanoví přidělená přístupová práva.



Obrázek 13: Zjednodušený diagram organizace pro SAM

5.3 Přehled platné právní úpravy

- **Zákon č. 121/2000 Sb.,** o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).

„V souladu se zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), jsou počítačové programy, pokud splňují znaky autorského díla, chráněny zákonem. Jejich ochrana, shodná jako ochrana literárního díla, vyplývá také z mezinárodních úmluv závazných pro Českou republiku. Platné právní předpisy chrání všechny aspekty nakládání s počítačovým programem jako autorským dílem, zejména pak právo na integritu díla a právo na jeho šíření.

Platné právní předpisy zajišťují nositeli autorských práv k softwaru řadu výhradních práv s tím, že z pohledu zajištění oprávněnosti užívání počítačových

programů v informačních systémech lze za nejdůležitější považovat právo na šíření počítačových programů, kdy šíření počítačových programů bez souhlasu oprávněné osoby, vyplývajícího většinou z licenčních ujednání, je nezákonné a může být dokonce trestné.

K šíření dochází tehdy, pokud je počítačový program kopírován, kopie počítačového programu je pak pořízena tehdy, když:

a) počítačový program je nahrán do paměti počítače (včetně RAM či podobně) při spuštění programu z disku;
b) počítačový program je instalován (kopírován) na pevný disk počítače nebo výměnné disky přidělené k počítači;
c) počítačový program je spuštěn na příslušném počítači ze síťového serveru, na kterém je uložen nebo instalován.

Šířením v souladu s autorským zákonem není zhotovení záložní kopie počítačového programu pro účely jeho obnovy v případě poruchy a je-li to potřebné pro jeho užívání.“

- **Zákon č. 140/1961 Sb.,** trestní zákon, ve znění pozdějších předpisů.

„Neoprávněné užívání a šíření počítačových programů může být zejména posuzováno, za předpokladu, že jsou splněny všechny znaky skutkové podstaty trestného činu, jako trestný čin porušení autorského práva podle ustanovení § 152 zákona č. 140/1961 Sb., trestního zákona, ve znění pozdějších předpisů. Za tento trestný čin je možné uložit trest odnětí svobody až na 5 let, peněžitý trest a trest propadnutí věci.

Neoprávněné užívání a šíření počítačových programů může mít dále za následek odpovědnost za škodu ve smyslu příslušných právních předpisů, a to jak odpovědnost ve vztahu k nositeli autorských práv k softwaru, tak případnou odpovědnost zaměstnance vůči zaměstnavateli podle platných pracovně-právních předpisů.“

Další související zákony:

- Zákon č. 227/2000 Sb., o elektronickém podpisu.
- Zákon č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů.
- Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

5.4 Analýza současného stavu

Diplomová práce je zpracována na současný stav reálné organizace k únoru 2015, působící v České Republice, konkrétně na Hasičský záchranný sbor Královéhradeckého kraje. Jedná se o bezpečnostní složku státu, proto mohou být některé údaje vynechány.[18]

Tato organizace je velice vhodným adeptem na nasazení správy softwarových aktivit, protože veškerá činnost organizačního i operačního řízení je závislá na ICT. Pro zjednodušení budu v této práci zmiňovat pouze jedinou organizační strukturu organizace, a to oddělení komunikačních a informačních systémů (KIS). Analýza bude prováděna na základě konzultací se zaměstnanci KIS.

Oddělení KIS disponuje vypracovanou IT strategií, kterou spravuje. Stará se o její aktualizaci, komunikaci a naplňování. Donedávna ale nedisponovala efektivní správou softwaru a licencí. Vše se dělo na základě interních databází oddělení. Neustálá úsporná opatření vedla vrcholový management k zamyšlení se nad optimalizací IT procesů.

[18] Nekomerční Software, speciální software, apod.

Cílem bylo tedy zpracování důležitých zásad správy SW a jejich šíření napříč celou organizací:

- **Ochrana a bezpečnost dat a informací**
- **Ochrana přístupu a hesel k informačním systémům**
- **Pravidla používání sítě internet**
- **Používání softwaru**
- **Elektronická pošta**
- **Tiskárny**
- **Manipulace s počítačem**
- **Monitoring pracovníků**

5.5 Specifikace požadovaných funkcí na SW nástroj

Zásady správy SW jsou umístěny na firemním intranetu. Každý zaměstnanec k nim má možnost neustálého přístupu. Každý nový zaměstnanec musí projít úvodním školením a tato pravidla podepsat. Při porovnání místních zásad SAM dle ITIL jsem zjistil, že většina zásad je zde uvedena, ale některá pouze z části. Chybí zde informace o licencích, zda je software freeware nebo shareware. Dále zde chybí systém podrobnějšího oprávnění a přístupu.

Software Asset Management (dále již jen SAM), je nedílnou součástí ITIL. Je to metodika správy softwaru v organizaci dle jejich požadavků a možností. Výstižná je tato definice dle [19].

„Software Asset Management je souhrnem veškeré infrastruktury a procesů nezbytných pro efektivní řízení, kontrolu a ochranu softwarových aktiv ve všech fázích životního cyklu v rámci podniku.“

5.6 Analýza rizik

Používání softwaru je také spojeno s riziky, která je nutno včas odhalit, specifikovat a nalézt způsoby, jak tyto rizika minimalizovat. Pro tuto analýzu byla vybrána metoda polokvantitivní. [20]

Existence rizika se zde testuje pomocí tří složek:

- Pravděpodobnost vzniku (P) – jaká je pravděpodobnost, že ohrožení nastane
- Pravděpodobnost následků (N) – jak velká je závažnost škod způsobené ohrožením
- Názor hodnotitelů (H) – míra závažnosti ohrožení, stáří a technický stav technologických zařízení apod.

Slovní vyjádření	Stupnice
Nahodilá	1
Nepravděpodobná	2
Pravděpodobná	3
Velmi pravděpodobná	4
Trvalá	5

Tabulka 2: P - Pravděpodobnost vzniku a existence nebezpečí [20]

Slovní vyjádření	Stupnice
Vznik nízkých nákladů u jednotlivce	1
Vznik vysokých nákladů u jednotlivce	2
Vznik nákladů s vlivem na chod podniku	3
Vznik nákladů ohrožujících podnik	4
Likvidační následky	5

Tabulka 3: N – Možné následky ohrožení [20]

Slovní vyjádření	Stupnice
Zanedbatelný vliv na míru nebezpečí a ohrožení	1
Malý vliv na míru nebezpečí a ohrožení	2
Slovní vyjádření	**Stupnice**
Větší, nezanedbatelný vliv na míru ohrožení a nebezpečí	3
Velký a významný vliv na míru ohrožení a nebezpečí	4
Více významných a nepříznivých vlivů na závažnost a následky ohrožení a nebezpečí	5

Tabulka 4: H – Názor hodnotitelů [5]

Výsledná míra rizika (R) se spočítá součinem všech tří složek.

$$R = P \times N \times H$$

Míru rizika určuje její stupeň, který spadá do intervalu míry rizika. Čím větší je míra rizika (R) tím je zásah proti riziku naléhavější.

Rizikový stupeň	Rozpětí rizika	Hodnocení rizika
I.	> 100	Nepřijatelné riziko
II.	51 – 100	Nežádoucí riziko
III.	11 – 50	Mírné riziko
IV.	3 – 10	Akceptovatelné riziko
V.	< 3	Bezvýznamné riziko

Tabulka 5: R – Stupeň rizikovosti [5]

5.6.1 Analýza rizik v organizaci

Ve spolupráci s oddělení KIS byla provedena analýza rizik při použití software v organizaci:

- Zrušení vzájemné spolupráce s firmou Microsoft při nedodržení licenčních podmínek.
- Při reinstalaci počítače se neprovede odebrání instalace.
- Koupě nových licencí vlivem špatného přehledu o stavu licencí v organizaci.
- Náklady při poškození počítačů při použití nelegálního software.

5.6.2 Opatření rizik v organizaci

Ke každému z výše uvedených rizik byla vytvořena opatření k zabránění či omezení těchto rizik. Byla proto doporučena následující opatření:

- Centrální evidence software a hardware
- Evidence instalovaného software
- Evidence licenčních ujednání a smluv
- Pravidelné měsíční kontroly počítačů
- Pravidelné měsíční kontroly instalovaného software
- Ochrana počítačů technickými prostředky
- Okamžité odstranění nelegálního software
- Omezení práv k instalaci
- Optimalizace nákupu software a hardware
- Pravidelné školení uživatelů
- Postihy za instalaci nelegálního software

Veškerá opatření budou vydána sbírkou interních aktů řízení krajského ředitele.

5.7 Správa SAM

Při vytváření zásad je nutné dodržovat základní doporučení, která vycházejí dle ITIL a stanovených cílů organizace pro minimalizaci rizik.

5.7.1 Vytvoření evidence SW a HW

Jednou z nejdůležitějších věcí, kterou je nutné vědět, je aktuální stav licencí daného software s jejich následnou potřebnou dokumentací. Je potřeba zajistit, aby všechna data byla aktuální, a proto musí být do systému SAM zavedena ihned po nákupu. Zároveň je potřeba provádět pravidelnou kontrolu těchto licencí a také kontrolu ostatních verzí freeware programů. Kopie výsledků inventarizace je také nutné pravidelně zálohovat. Proto je doporučeno tyto výsledky udržovat i v papírové podobě v archívu KIS. Přístup k tomuto archívu mají pouze pověření pracovníci oddělení KIS a krajského ředitelství.

5.7.2 Evidence médií

Instalační média musí být také ochráněna a zabezpečena pro případ nenadálé události. Bylo zjištěno, že jsou uchovávána pouze na instalačních discích. Doporučuji proto vytvořit záložní bitové kopie instalačních médií a také uložení ISO obrazů disků na centrální zabezpečený server. Všechny kopie musí být provedeny na základě pravidel výrobce software.

5.7.3 Certifikáty o vlastnictví

Dokumenty opravňující k nabytí licence software jsou nejdůležitějším prvkem. Všechny originály jsou skladovány na centrálním místě na oddělení KIS. Výjimku tvoří certifikáty jednotlivých OEM licencí a licencí, jejichž doložení je nezbytné při případném auditu softwaru.

5.7.4 Role v SAM

V organizaci je nutné nastavit jasně definované odpovědnosti za procesy SAM. Je vhodné stanovit hlavního správce SAM, který bude zodpovědný za celkový stav i za podřízené správce. Dle pokynu krajského ředitele HZS Královéhradeckého kraje je to příslušník zařazený k výkonu služby v odborném útvaru, který je dle náplně služební činnosti osobou určenou k provádění úkonů instalace, konfigurace, oprav, aktualizace a odinstalování počítačových programů, na územních odborech zaměstnanec stanovený ředitelem příslušného územního odboru.

5.7.5 Software Brainstorming

Další důležitou součástí je tzv. software Brainstorming, kdy se zástupci oddělení KIS sejdou se zaměstnanci organizace a zjišťují, jaký software by mohli zaměstnanci využívat, který již nepoužívají a další připomínky k software. Brainstorming je vhodné provádět v pravidelných cyklech s ročním intervalem.

5.7.6 Inventarizace SAM

Pravidelná inventarizace SAM je nastavena v organizaci v ročních intervalech. Při pořízení nového software je nutné stanovit pravidla pro okamžité zapsání

software do evidence. Tímto by se mělo zamezit rizikům spojeným s neevidovaným software.

5.7.7 Kontrola SAM v organizaci

V kapitole 5.6 se budu zabývat implementací vhodného SW nástroje pro evidenci. Takový nástroj by dle požadavků měl provádět kontroly automaticky a samostatně. Je však vhodné v ročních intervalech stanovit namátkové kontroly na náhodném výběru vzorku počítačů. Po kontrole je nutné také zpracovat zápis a výsledky z namátkové kontroly. Přílohou této práce je vzor zápisu.

5.7.8 Nelegální software

Je nezbytné zabezpečit veškerý software tak, aby byl v souladu s právní úpravou. Je tedy nutno používat pouze legální software. Veškerý software má svou vlastní licenci a je nainstalován pouze na daném počítači, pro který je licence určena. V organizace jsou i licence, kdy si uživatel může danou licenci převzít i na přenosný počítač. Tuto činnost uživatel nesmí provádět sám, ale pouze se souhlasem hlavního správce SAM. Neoprávněné zacházení s chráněným softwarem je porušení zákona a také v rozporu s vnitřní směrnicí. Zaměstnanec, který takto bude činit, bude okamžitě disciplinárně potrestán, toto chování vést může k okamžitému ukončení pracovního nebo služebního poměru.

5.7.9 Školení SAM

Úvodní proškolení zaměstnanců k legálnímu používání počítačových programů zajišťuje odborný útvar. Provádí se před prvním použitím prostředků ICT určených k použití zaměstnancem, na základě předchozí žádosti vedoucího zaměstnance nadřízeného zaměstnanci, který má být proškolen. Za účelem proškolení všech zaměstnanců zaměstnavatele poskytují odbornému útvaru vedoucí zaměstnanci jiných odborných útvarů potřebnou součinnost, zejména hlášení potřeby proškolení nově příchozích zaměstnanců.

O provedeném proškolení se sepisuje písemný zápis, který podepisuje proškolený zaměstnanec a správce počítačových programů, který školení prováděl. Aktuální tematický plán proškolení uživatele ICT a formulář dokladu o proškolení je

uložen v tištěné podobě na odborném útvaru a v elektronické podobě je k dispozici na Intranetu HZS Královéhradeckého kraje. Hlavní body plánu školení jsou:

1. **Uživatel je oprávněn:**
   - Využívat služeb a prostředků počítačové sítě v rozsahu přidělených oprávnění a proškolení.
   - Požadovat po správci počítačových programů odstranění závad, pro které nemůže plně využívat služeb lokální počítačové sítě.
   - Požadovat po odborném pracovišti odstranění závad na počítačové sestavě.

2. **Uživatel je povinen:**
   - Respektovat pokyny správce počítačových programů.
   - Zabránit přístupu do lokální počítačové sítě neoprávněným osobám a to zejména tím, že neponechá připojenou počítačovou sestavu ve volně přístupných místnostech bez dozoru, nejsou-li použity jiné způsoby bránící používání počítače a neoprávněnému přístupu do počítačové sítě.
   - Užívat prostředky lokální počítačové sítě a výpočetní techniky pouze a jen v rámci své pracovní náplně a v rámci svých přidělených oprávnění a takovým způsobem, aby nedocházelo k zaviněným technickým nebo softwarovým poruchám.
   - Neměnit technické vybavení a konfiguraci počítačové sestavy a nepřipojovat k ní další zařízení.
   - Neměnit topologii počítačové sítě a neprovádět zásahy do technických prostředků sítě.
   - Neměnit přidělenou identifikaci počítače vůči počítačové síti (IP adresu).
   - Utajovat svá konta a hesla pro přístup do systémů.
   - Neumísťovat do blízkosti počítačové sestavy a magnetických médií (nosičů dat) předměty vytvářející silnější elektromagnetické pole (transformátory, elektromotory, magnety apod.).

- Nevystavovat počítač a magnetická média (nosiče dat) působení silnějšího tepelného záření (vařiče, radiátory).
- Dbát, aby nedošlo k fyzickému poškození počítače, nevystavovat přívodní a propojovací kabely ani další části počítačové sestavy nadměrnému mechanickému namáhání.
- Nezakrývat větrací otvory počítače.
- Nevystavovat počítačovou sestavu otřesům, zvýšené prašnosti, nebezpečí polití tekutinou nebo posypání sypkým materiálem (např. blízkost květin).
- Dbát základního principu antivirové ochrany.
- Oznámit neprodleně svému přímému nadřízenému nebo správci počítačových programů, zjistí-li porušení tohoto pokynu, nebo ostatních závazných pokynů souvisejících s problematikou informačních technologií.

3. Uživatel sítě nesmí

- Zneužívat nedbalosti jiných uživatelů k přístupu k cizím datům pod jinou identitou.
- Obtěžovat ostatní uživatele počítačové sítě zejména hromadným rozesíláním zpráv nesouvisejících s plněním služebních úkolů případně netýkajících se činností HZS, řetězových zpráv, a používat počítačovou síť k šíření, prohlížení nebo ukládání komerčních nebo osobních oznámení, žádostí a propagací.
- Připojovat se do lokální počítačové sítě nebo k jejím prostředkům pod jiným uživatelským jménem než přiděleným.
- Odposlouchávat komunikaci jiných uživatelů, zejména za účelem zjištění jejich přístupových hesel a instalovat takové prostředky, které toto umožňují nebo usnadňují.
- Instalovat počítačové programy na soupravě výpočetní techniky (včetně počítačů nepřipojených do sítě HZS HK), není-li správcem počítačových programů, a provádět jakékoliv změny nebo zasahovat do konfigurace technického prostředku výpočetní techniky.

- Šířit a ukládat destruktivní kódy (jako jsou viry apod.), pornografické texty a obrázky nebo jakékoliv nepovolené materiály.
- Vykonávat vědomě takové úkony, které vedou k dlouhodobému časovému omezování práce ostatních uživatelů lokální počítačové sítě zejména při užívání služeb Internetu (příjem audio a video souborů, správcování vlastních WWW stránek atd.).

5.7.10 Optimalizace nákupu SAM

Organizace musí stanovit roční plán nákupů SAM. Tento plán musí schválit vedení KIS a vedení krajského ředitelství. Plán by měl pokrývat aktuální požadavky na nákup a neměl by být nadhodnocen nebo podhodnocen. Veškeré změny provedené v oblasti SAM by se měly pravidelně zveřejňovat pro všechny zaměstnance organizace.

5.8 Výběr vhodného SW nástroje

Při výběru jsem vycházel ze tří nejznámějších a nejpoužívanějších produktů pro správu SAM na českém trhu a to:

- AuditPro
- AW Caesar
- ALVAO Asset Management

5.8.1 Komparace vhodných SW nástrojů

Porovnání jednotlivých produktů bylo převzato z [21]:

Název produktu	AW Caesar	ALVAO Asset Management	AuditPro
Rok uvedení na trh	2002	1999	2001
Počet konzultantů produktu v ČR	12 + 98	15	Více než 1000
VYBRANÉ FUNKCE - EVIDENCE A SPRÁVA HW MAJETKU			
Inventarizace majetku	ANO	ANO	ANO
Přehled konfigurací počítačů	ANO	ANO	ANO
Ekonomické údaje (dodavatel, faktura, cena, záruka, …)	ANO	ANO	ANO

Název produktu	AW Caesar	ALVAO Asset Management	AuditPro
Sledování historie počítače (uvedení do provozu, opravy, upgrade, zapůjčení, převody, servisy, revize, likvidace)	ANO	ANO	ANO
Elektronická dokumentace (naskenované faktury, texty smluv, fotky, …)	ANO	ANO	ANO
Sledování nákladů na údržbu	ANO	ANO	ANO
Podpora technologie čárových kódů	ANO	ANO	ANO
Možnost propojení na SAP	ANO	ANO	NE
Přehled SW na jednotlivých PC a jeho licencí	ANO	ANO	ANO
Evidence všech typů licencí (OEM, Upgrade, Downgrade, Maintenance)	ANO	ANO	ANO
Sledování využití licencí	ANO	ANO	ANO
Porovnání stavu PC proti vzoru	ANO	ANO	ANO
Historie licence software (instalace, odinstalace, zapůjčení, převody, roční servisy)	Částečně	ANO	ANO
Elektronická dokumentace k software (naskenované faktury, texty smluv, licenční ujednání, …)	ANO	ANO	ANO
Sledování upgrade (Windows 95 – 98 – XP)	ANO	ANO	ANO
Evidence a správa multilicencí	ANO	ANO	ANO
Pevné přiřazení OEM licence k počítači nebo příslušenství	ANO	ANO	ANO

Název produktu	AW Caesar	ALVAO Asset Management	AuditPro
UŽIVATELSKÉ ROZHRANÍ A VÝSTUPY			
Grafické přehledy a výstupy	ANO	ANO	ANO
Webové rozhraní	ANO (nadstavba)	ANO	ANO
Standardní sestavy (předávací protokol, pasportní list, specifikační list, inventární sestavy, sestavy oprav)	ANO	ANO	ANO
Souhrnné sestavy dle organizačních složek podniku	ANO	ANO	ANO
Vlastní uživatelské sestavy (generátor sestav)	ANO	ANO	ANO
Aktivní reporting (e-mailové reporty)	NE	Částečně (pomocí uživatelských skriptů)	ANO
Exporty pro MS Excel	ANO	ANO	ANO
Další exportní formáty (CSV, PDF, XML, HTML...)	CSV, XML, HTML, PDF	Export do formátů: CSV, XML, HTML, DOC, TXT. Publikování výsledků na MS Share Point Server.	csv;xml;mdb;html; grafické reporty pro management; napojení reportovacího centra s MS Office; publikace reportů v prostředí intranetu

5.8.2 Výběr vhodného nástroje pro implementaci

Pro implementaci vhodného nástroje byl vybrán ALVAO Asset Management. Do užšího kola se dostal společně s programem AuditPro, který také splňuje očekávání IT managementu. V konečné fázi rozhodování bylo rozhodnuto

ekonomickým oddělením HZS vzhledem k možné propojenosti s ekonomickým systémem SAP[19]. Vzájemná asociace s programem SAP je zatím v dlouholetých vizích Hasičského záchranného sboru Královéhradeckého kraje, proto se jí nadále nebudu ve své práci zabývat.

5.8.3 ALVAO Asset Management

Tento komplexní informační systém je určen pro pracovníky oddělení správy výpočetní a komunikační techniky v organizaci. Jeho hlavními funkcemi je evidence zařízení, předmětů a software z hlediska použitelnosti pro oddělení ICT.

5.8.4 Možnosti evidence pomocí SAM ALVAO

- **Počítače** – veškerá kompletní evidence komponentů uvnitř počítačů (základní deska, procesor, pevný disk, paměti, grafické karty, zvukové karty apod.). Veškeré parametry zjišťuje systém ALVAO pomocí Collectoru a automaticky tyto parametry vkládá do systému automaticky. Jsou ovšem výjimečné případy, kdy je nutno tyto parametry potvrdit ručně. Další parametry jako inventární čísla, data pořízení, umístění objektu je nutné vkládat ručně.
- **Nainstalovaný software** – jedná se o seznam programů, které jsou nainstalovány na jednotlivých počítačích. Jejich detekování probíhá automaticky z registrů systémů. Je možno také sledovat historii instalací software na jednotlivých počítačích. Dále je možno v systému Active Directory (AD) sledovat, který uživatel nebo administrátor software nainstaloval.
- **Nakoupený software** – seznam dokumentů koupeného software, resp. licencí k software. Zohledňuje se zde také možnost downgrade nebo upgrade licencí.
- **Další majetek** – mobilní telefony, síťové prvky, tiskárny, kopírky, brašny apod.
- **Spotřební materiál** – je možno evidovat stav zásob spotřebního materiálu jako jsou tonery, inkoustové náplně to tiskáren a další.

[19] Zdroj: *SAP* [online]. 2015 [cit. 2015-04-15]. Dostupné z: http://go.sap.com/index.html

Systém ALVAO tedy splňuje veškeré požadavky, které byly při nasazování systému vzneseny. Dále je možno pomocí software vytvářet tiskové sestavy (inventární sestavy, přesuny majetků, předávací protokoly), provádět audit software, evidovat závady a opravy, service desk a také vést inventury.

5.8.5 Minimální nároky na použití SAM ALVAO

V této části musíme vzít v úvahu tři různé typy požadavků. A to pro serverovou část, administrátorskou část a ostatní účastnické stanice v síti.

5.8.6 Servery

- Microsoft Windows Server 2012, Microsoft Windows 2008 Server (R2)
- Microsoft Windows 2003 Server (R2)[20]
- Microsoft SQL Server 2012
- Microsoft .NET Framework 4.0, 3.5
- Microsoft Internet Information Server (IIS)

5.8.7 Administrátorské počítače

- Microsoft Windows 8 Pro, Enterprise
- Microsoft Windows 7 Professional, Enterprise, Ultimate
- Microsoft Windows Vista Business, Ultimate
- Microsoft Windows XP Professional
- Microsoft .NET Framework 4.0, 3.5
- Microsoft Internet Explorer 8 nebo vyšší

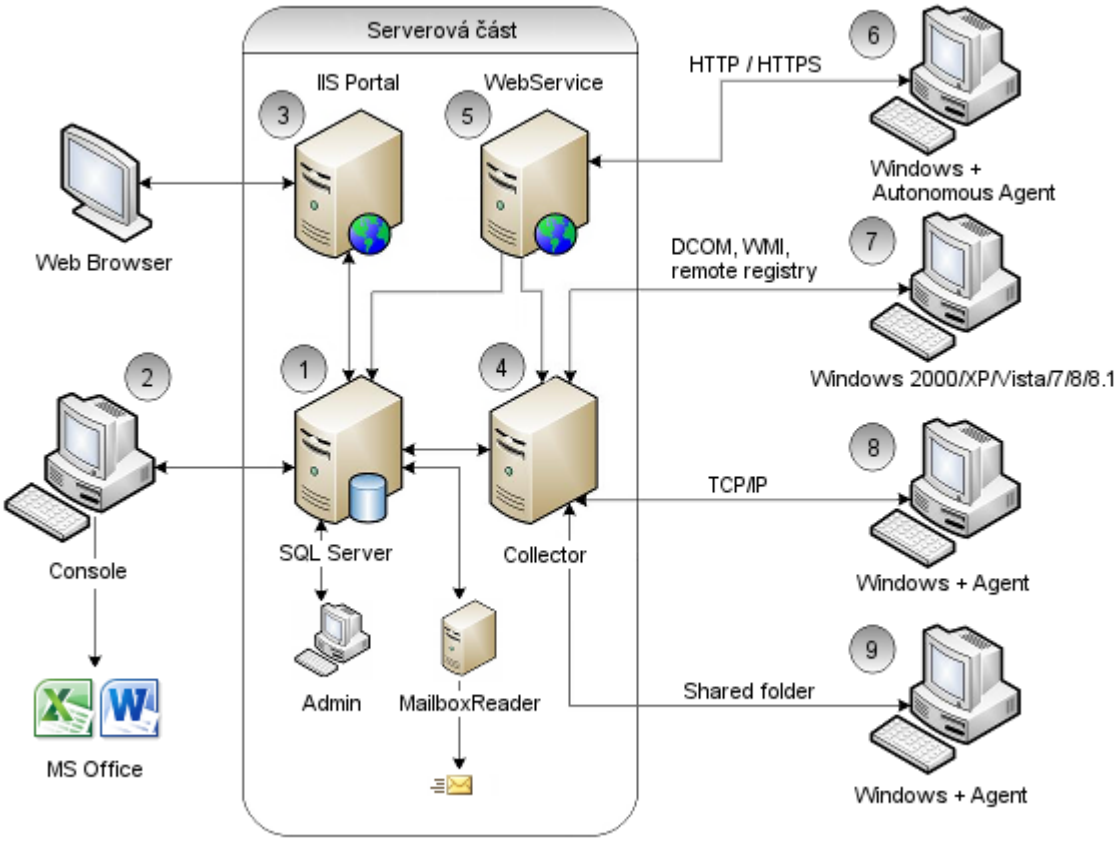
5.8.8 Ostatní účastnické stanice

Pro evidování a automatickou detekci hardware a software je nutno, aby klientské počítače splňovaly pouze podmínku podporovaného operačního systému od Windows 2000 SP4 a vyšší.

[20] Od verze OS WIN 8.1 končí podpora, a proto se již nedoporučuje pro zavedení systému ALVAO

6 Implementace Software Asset Managementu do prostředí HSZ KHK

6.1 Architektura systému



Obrázek 14: Architektura systému ALVAO Asset Management

Veškeré zachycované údaje se ukládají do databáze, která je společná pro všechny uživatele. V prostředí HZS byl zřízen server, který poběží na operačním systému Windows Server 2008 R2 a na verzi MS SQL server 2012 R2 express. Collector je aplikace, která úzce spolupracuje s databází a provádí vzdálenou detekci hardware a software počítačů v síti. K detekci dochází na základě požadavku od správce ICT přes Konzoli. Detekovat lze pomocí několika způsobů.

- **Detekce pomocí autonomního Agenta** – na konečné pracovní stanici je nainstalován Agent, který sám provádí detekci a poté odesílá získaná

data na server pomocí protokolu HTTP / HTTPS. Výhodou této detekce je, že může konečný klient být kdekoliv, kde je připojen k internetu.

- **Detekce bez Agenta** – Collector je schopen detekovat údaje bez nutnosti instalace autonomního agenta. Detekce je prováděna pomocí protokolů DCOM, WMI a vzdáleného registru.

- **Detekce s Agentem přes TCP/IP** – Agent je implantován na konečnou stanici jako systémová služba. Collector provádí komunikaci pomocí TCP/IP.

- **Detekce s Agentem přes sdílenou složku** – Agent provádí komunikaci pomocí sdílené složky na serveru. Jedná se o nejméně používanou variantu, ale je zachována z důvodu kompatibility se staršími verzemi operačního systému.

V našem prostředí byla vybrána implementace detekování konečných stanic pomocí Agenta přes TCP/IP, protože žádná stanice není umístěna mimo podnikovou síť.

6.2 Zavedení SAM a jeho nejvhodnější opatření

V této kapitole se zabývám návrhem doporučení pro zlepšení situace v organizaci. Jedním ze zjištěných problémů byla chybná SW politika organizace a s ní spojené další aspekty. Chyběly zde konkrétní zásady týkající se licencování a typů software používaných v organizaci. Tato skutečnost má za následek neinformovanost zaměstnanců a tím i následné prodloužení doby trvání vyřízení požadavku vzhledem k jejich špatné interpretaci při školení SAM. Navrhuji tedy zpravovat také interní směrnice pro řízení software.

		Měsíc											
Fáze	**Aktivita**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
Plánování	Ustanovení týmu	■											
	Analýza vhodného SW řešení		■										
	Výběr vhodného řešení		■										
Nasazení	Analýza rizik		■	■									
	Zavádění opatření			■	■								
	Zavedení SW řešení					■	■	■					
Kontrola	Kontrola funkcí							■	■	■			
	Testování									■	■	■	■

Tabulka 6: Harmonogram prací

V současné době se časový harmonogram nachází ve fázi testování a kontroly funkcí. Je to také nejdelší období implementace SAM. Časový harmonogram je pouze rámcový, ale dle skutečných stavů.

6.3 Interní směrnice řízení SAM

Tuto část práce tvoří vypracovaná směrnice pro vedoucí pracovníky oddělení KIS, kteří budou pracovat s určeným software společnosti ALVAO. Tato struktura byla vypracována na základě pohovorů s oddělením KIS v organizaci a administrátory územních odborů.

6.3.1 Činnosti SAM dle typů

1. Detekce software automatická
2. Detekce software ruční

3. Evidence instalací
4. Licenční audit software
5. Pravidelná kontrola licenční čistoty
6. Nákup software
7. Nasazení software
8. Údržba software
9. Vyřazení software

6.3.2 Popisy jednotlivých činností SAM dle typu

Jednotlivé popisy činností dle typu uvedených v bodě 6. 3. 1.

1. Detekce software automatická

Popis činnosti

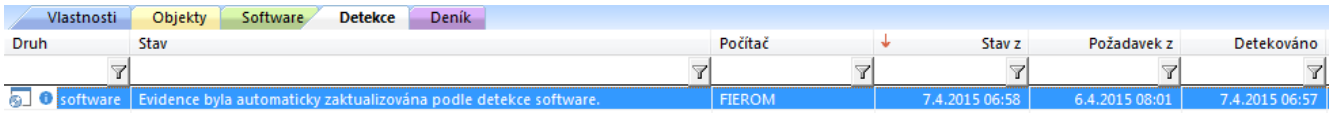
Automatická detekce software slouží k získání informací o nainstalovaném software na počítačích v organizaci. Toto je standardní postup, který se bude uplatňovat u HZS Královéhradeckého kraje. Tento postup bude dle plánu SAM automaticky spuštěn každý měsíc. Systém si pak zabezpečuje veškeré činnosti sám a administrátor pouze kontroluje chyby při detekci.

Předpoklady činnosti

- Distribuce instalačního balíčku přes Doménovou politiku
- Počítače jsou připojeny do místní sítě pomocí protokolu TCP/IP
- Databáze SAM je přístupná a zřízená
- Aplikace ALVAO je dostupná

Postup činnosti

1. Přihlášení ke konzoli aplikace ALVAO.
2. Zkontrolování chyb o neúspěšných automatických detekcích.



Obrázek 15: Automatická detekce agentem

Na obrázku č. 15 je záznam o automatické detekci Agentem včetně data požadavku na detekci, čas vyřízení požadavku a aktuálního stavu.

2. Detekce software ruční

Popis činnosti

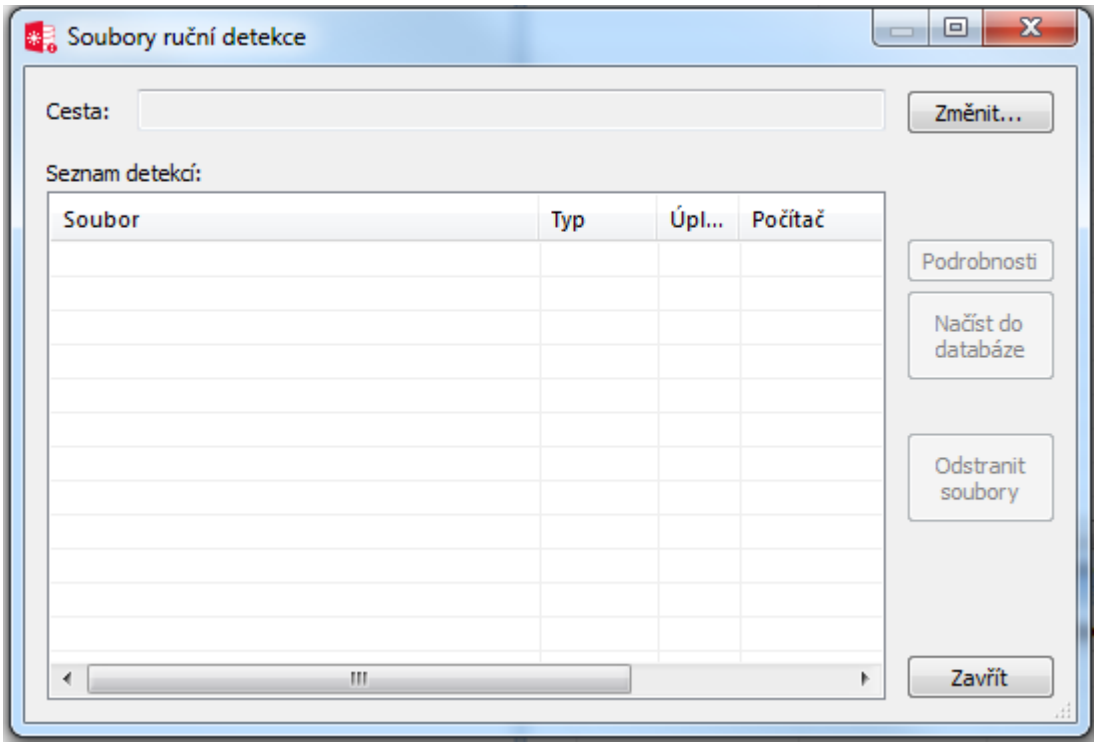
Ruční detekce software slouží k získání informací o nainstalovaném software na počítačích v organizaci. Ruční detekci použijeme v případě, že počítač není připojen do domény HZSHK.CZ nebo není připojen v síti. Takto získané informace z detekce uložíme do souboru a poté importujeme ručně s databází.

Předpoklady činnosti

- Administrátor má přístup k počítačům
- Databáze SAM je přístupná a zřízená
- Aplikace ALVAO je dostupná

Postup činnosti

1. Přihlášení ke kontrolovanému počítači pod administrátorským účtem.
2. Spouštění Collectoru a ruční spuštění detekce.
3. Po kompletní detekci uložit detekci do souboru.
4. Načtení detekce do inventáře .



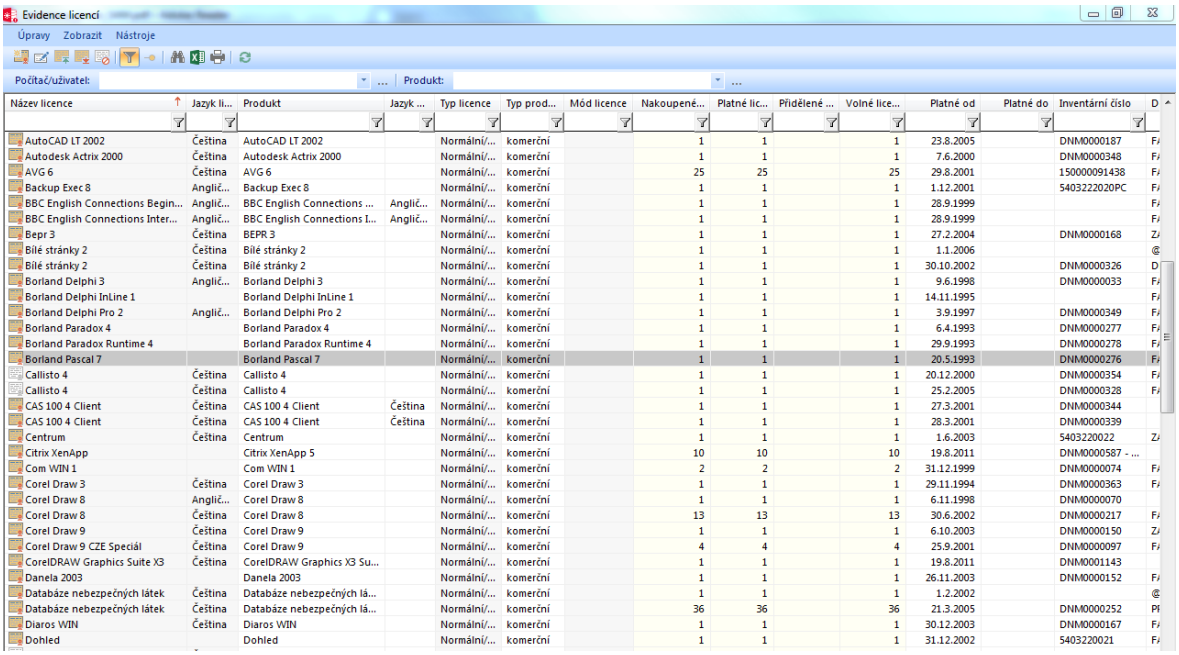
Obrázek 16: Importování ruční detekce

Na obrázku č. 16 je zobrazeno dialogové okno pro import ručního souboru s detekcí provedenou pomocí Collectoru.

3. Evidence instalací

Popis činnosti

Činnosti zabezpečující získávání informací o licencích, které organizace vlastní a se kterými může nakladádat. Veškeré informace jsou uloženy do aplikace pro správu. Evidence instalací si aktualizuje počty licencí automaticky na základě automatické detekce. Pokud detekce zjistí nesrovnalost, administrátor tuto skutečnost musí opravit ručně.



Název licence	Jazyk li...	Produkt	Jazyk ...	Typ licence	Typ prod...	Mód licence	Nakoupené...	Platné lic...	Přidělené ...	Volné lice...	Platné od	Platné do	Inventární číslo	D
AutoCAD LT 2002	Čeština	AutoCAD LT 2002		Normální/...	komerční		1	1		1	23.8.2005		DNM0000187	F
Autodesk Actrix 2000	Čeština	Autodesk Actrix 2000		Normální/...	komerční		1	1		1	7.6.2000		DNM0000348	F
AVG 6	Čeština	AVG 6		Normální/...	komerční		25	25		25	29.8.2001		150000091438	F
Backup Exec 8	Angličt...	Backup Exec 8		Normální/...	komerční		1	1		1	1.12.2001		5403222020PC	F
BBC English Connections Begin...	Angličt...	BBC English Connections ...	Angličt...	Normální/...	komerční		1	1		1	28.9.1999			F
BBC English Connections Inter...	Angličt...	BBC English Connections I...	Angličt...	Normální/...	komerční		1	1		1	28.9.1999			F
Bepr 3	Čeština	BEPR 3		Normální/...	komerční		1	1		1	27.2.2004		DNM0000168	Z
Bílé stránky 2	Čeština	Bílé stránky 2		Normální/...	komerční		1	1		1	1.1.2006			@
Bílé stránky 2	Čeština	Bílé stránky 2		Normální/...	komerční		1	1		1	30.10.2002		DNM0000326	D
Borland Delphi 3	Angličt...	Borland Delphi 3		Normální/...	komerční		1	1		1	9.6.1998		DNM0000033	F
Borland Delphi InLine 1		Borland Delphi InLine 1		Normální/...	komerční		1	1		1	14.11.1995			F
Borland Delphi Pro 2	Angličt...	Borland Delphi Pro 2		Normální/...	komerční		1	1		1	3.9.1997		DNM0000349	F
Borland Paradox 4		Borland Paradox 4		Normální/...	komerční		1	1		1	6.4.1993		DNM0000277	F
Borland Paradox Runtime 4		Borland Paradox Runtime 4		Normální/...	komerční		1	1		1	29.9.1993		DNM0000278	F
Borland Pascal 7		Borland Pascal 7		Normální/...	komerční		1	1		1	20.5.1993		DNM0000276	F
Callisto 4	Čeština	Callisto 4		Normální/...	komerční		1	1		1	20.12.2000		DNM0000354	F
Callisto 4	Čeština	Callisto 4		Normální/...	komerční		1	1		1	25.2.2005		DNM0000328	F
CAS 100 4 Client	Čeština	CAS 100 4 Client	Čeština	Normální/...	komerční		1	1		1	27.3.2001		DNM0000344	
CAS 100 4 Client	Čeština	CAS 100 4 Client	Čeština	Normální/...	komerční		1	1		1	28.3.2001		DNM0000339	
Centrum	Čeština	Centrum		Normální/...	komerční		1	1		1	1.6.2003		5403220022	Z
Citrix XenApp		Citrix XenApp 5		Normální/...	komerční		10	10		10	19.8.2011		DNM0000587 - ...	
Com WIN 1		Com WIN 1		Normální/...	komerční		2	2		2	31.12.1999		DNM0000074	F
Corel Draw 3	Čeština	Corel Draw 3		Normální/...	komerční		1	1		1	29.11.1994		DNM0000363	F
Corel Draw 8	Angličt...	Corel Draw 8		Normální/...	komerční		1	1		1	6.11.1998		DNM0000070	
Corel Draw 8	Čeština	Corel Draw 8		Normální/...	komerční		13	13		13	30.6.2002		DNM0000217	F
Corel Draw 9	Čeština	Corel Draw 9		Normální/...	komerční		1	1		1	6.10.2003		DNM0000150	Z
Corel Draw 9 CZE Speciál	Čeština	Corel Draw 9		Normální/...	komerční		4	4		4	25.9.2001		DNM0000097	F
CorelDRAW Graphics Suite X3	Čeština	CorelDRAW Graphics X3 Su...		Normální/...	komerční		1	1		1	19.8.2011		DNM0001143	
Danela 2003		Danela 2003		Normální/...	komerční		1	1		1	26.11.2003		DNM0000152	F
Databáze nebezpečných látek	Čeština	Databáze nebezpečných lá...		Normální/...	komerční		1	1		1	1.2.2002			@
Databáze nebezpečných látek	Čeština	Databáze nebezpečných lá...		Normální/...	komerční		36	36		36	21.3.2005		DNM0000252	P
Diaros WIN	Čeština	Diaros WIN		Normální/...	komerční		1	1		1	30.12.2003		DNM0000167	F
Dohled		Dohled		Normální/...	komerční		1	1		1	31.12.2002		5403220021	F

Obrázek 17: Evidence instalací a licencí

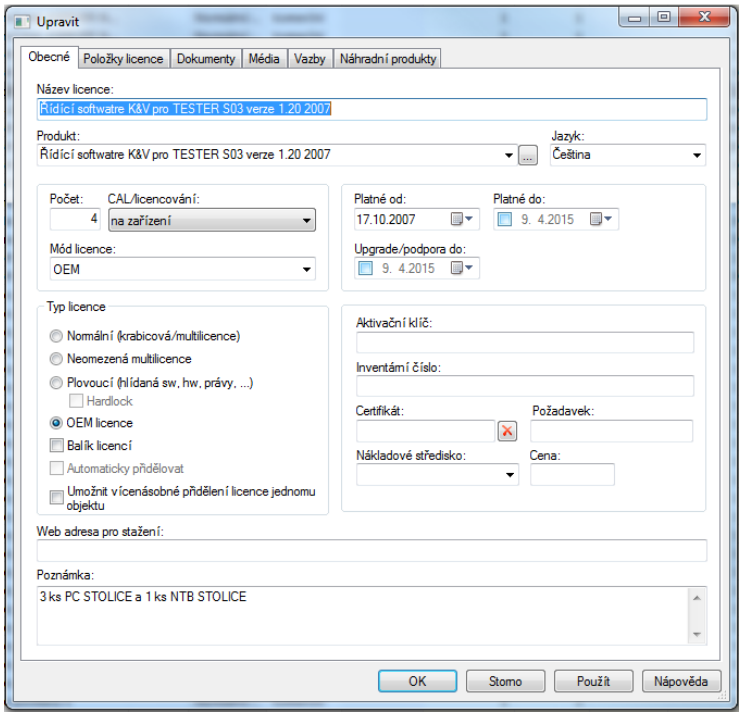
Zobrazení nainstalovaného software a počty jejich licencí. V přehledovém okně je zobrazen název licence, jazyk produktu, název produktu, typ licence, počet nakoupených licencí, počet platných licencí a počet volných licencí. Dále je zde možno sledovat data vypršení platností licencí a inventární čísla nákupů.

Předpoklady činnosti

- Databáze SAM je přístupná a zřízená
- Aplikace ALVAO je dostupná

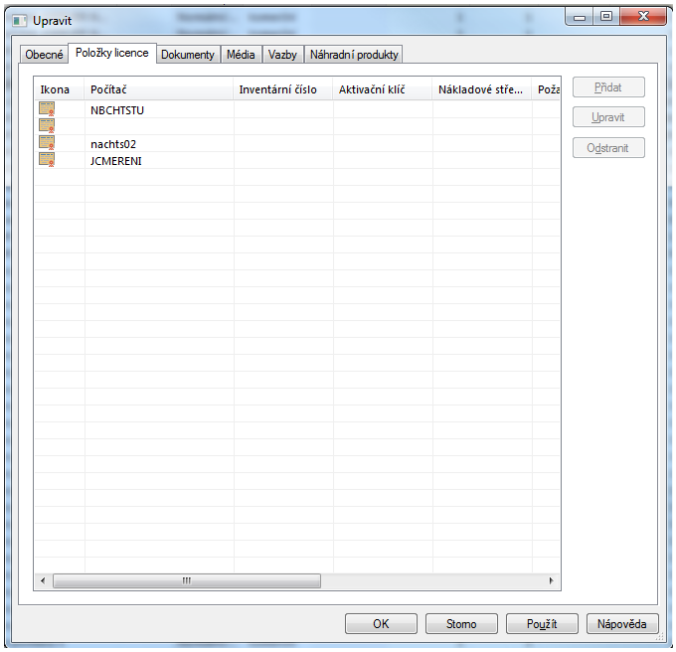
Postup činnosti

1. Při prvním spuštění musí administrátor zkompletovat veškeré licence v organizaci a ručně zadat počty licencí do konzole.
2. Otevření modulu Evidence licencí.
3. Zajišťuje doplnění kompletních údajů v evidenci.
4. Tisk inventárního seznamu s podpisem odpovědné osoby.



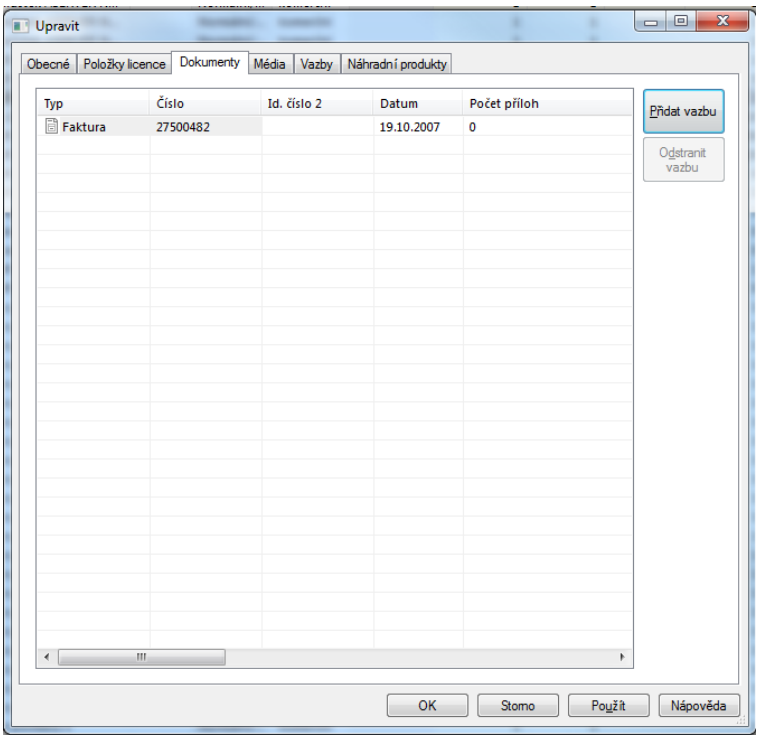
Obrázek 18: Zobrazení detailu licence

Zobrazení detailu licence, jejího módu, data platnosti licence, počtu licencí a dalších atributů, které lze nastavit. Dále je zde možno přiřazovat aktivační klíče, certifikáty, nákladová střediska, cenu produktu a uživatelskou poznámku.



Obrázek 19: Položky licence

V záložce položky licence v detailu licence je možno sledovat na kterém počítači je daný software nainstalován a je právě na něj tato licence použita.



Obrázek 20: Přidružené doklady k licenci

U každého software se také evidují veškeré doklady spojené s nákupem licencí. Datum pořízení, číslo faktur a také počet příloh dokumentace.

4. Licenční audit software a pravidelná kontrola licenční čistoty

Popis činnosti

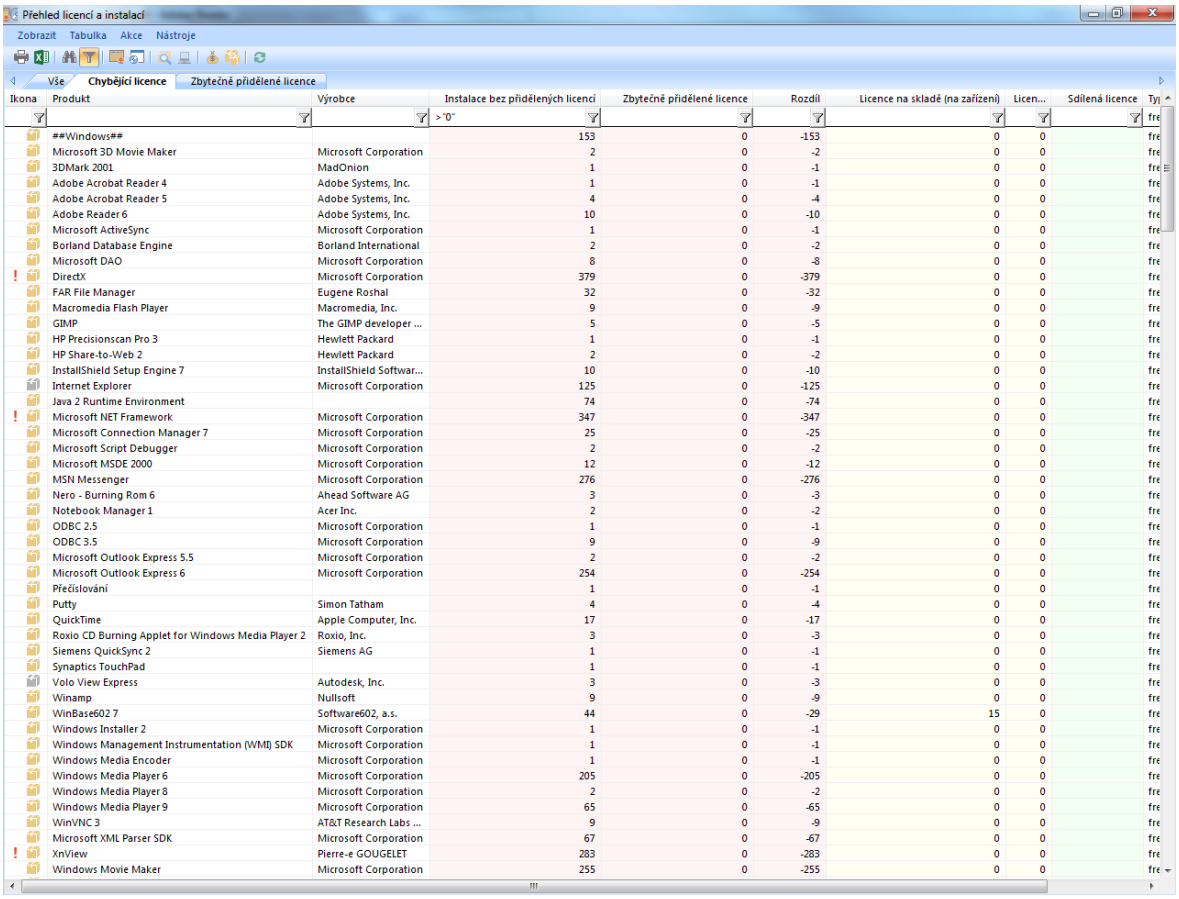
Administrátor pravidelně provádí licenční audit a kontrolu licenční čistoty. Využívá k tomu model konzole ALVAO.

Předpoklady činnosti

- Databáze SAM je přístupná a zřízená
- Aplikace ALVAO je dostupná

Postup činnosti

1. Otevření modulu Přehled licencí a instalací.
2. Kontrola chybějících licencí.
3. Kontrola zbytečně přidělených licencí.
4. Úprava stavu licencí nebo zajištění odinstalace programu bez platné licence.
5. Tisk protokolu s podpisem odpovědné osoby.



Ikona	Produkt	Výrobce	Instalace bez přidělených licencí	Zbytečně přidělené licence	Rozdíl	Licence na skladě (na zařízení)	Licen...	Sdílená licence	Ty
			> "0"						
	##Windows##		153	0	-153	0	0		fre
	Microsoft 3D Movie Maker	Microsoft Corporation	2	0	-2	0	0		fre
	3DMark 2001	MadOnion	1	0	-1	0	0		fre
	Adobe Acrobat Reader 4	Adobe Systems, Inc.	1	0	-1	0	0		fre
	Adobe Acrobat Reader 5	Adobe Systems, Inc.	4	0	-4	0	0		fre
	Adobe Reader 6	Adobe Systems, Inc.	10	0	-10	0	0		fre
	Microsoft ActiveSync	Microsoft Corporation	1	0	-1	0	0		fre
	Borland Database Engine	Borland International	2	0	-2	0	0		fre
	Microsoft DAO	Microsoft Corporation	8	0	-8	0	0		fre
!	DirectX	Microsoft Corporation	379	0	-379	0	0		fre
	FAR File Manager	Eugene Roshal	32	0	-32	0	0		fre
	Macromedia Flash Player	Macromedia, Inc.	9	0	-9	0	0		fre
	GIMP	The GIMP developer ...	5	0	-5	0	0		fre
	HP Precisionscan Pro 3	Hewlett Packard	1	0	-1	0	0		fre
	HP Share-to-Web 2	Hewlett Packard	2	0	-2	0	0		fre
	InstallShield Setup Engine 7	InstallShield Softwar...	10	0	-10	0	0		fre
	Internet Explorer	Microsoft Corporation	125	0	-125	0	0		fre
	Java 2 Runtime Environment		74	0	-74	0	0		fre
!	Microsoft NET Framework	Microsoft Corporation	347	0	-347	0	0		fre
	Microsoft Connection Manager 7	Microsoft Corporation	25	0	-25	0	0		fre
	Microsoft Script Debugger	Microsoft Corporation	2	0	-2	0	0		fre
	Microsoft MSDE 2000	Microsoft Corporation	12	0	-12	0	0		fre
	MSN Messenger	Microsoft Corporation	276	0	-276	0	0		fre
	Nero - Burning Rom 6	Ahead Software AG	3	0	-3	0	0		fre
	Notebook Manager 1	Acer Inc.	2	0	-2	0	0		fre
	ODBC 2.5	Microsoft Corporation	1	0	-1	0	0		fre
	ODBC 3.5	Microsoft Corporation	9	0	-9	0	0		fre
	Microsoft Outlook Express 5.5	Microsoft Corporation	2	0	-2	0	0		fre
	Microsoft Outlook Express 6	Microsoft Corporation	254	0	-254	0	0		fre
	Přečíslování		1	0	-1	0	0		fre
	Putty	Simon Tatham	4	0	-4	0	0		fre
	QuickTime	Apple Computer, Inc.	17	0	-17	0	0		fre
	Roxio CD Burning Applet for Windows Media Player 2	Roxio, Inc.	3	0	-3	0	0		fre
	Siemens QuickSync 2	Siemens AG	1	0	-1	0	0		fre
	Synaptics TouchPad		1	0	-1	0	0		fre
	Volo View Express	Autodesk, Inc.	3	0	-3	0	0		fre
	Winamp	Nullsoft	9	0	-9	0	0		fre
	WinBase602 7	Software602, a.s.	44	0	-29	15	0		fre
	Windows Installer 2	Microsoft Corporation	1	0	-1	0	0		fre
	Windows Management Instrumentation (WMI) SDK	Microsoft Corporation	1	0	-1	0	0		fre
	Windows Media Encoder	Microsoft Corporation	1	0	-1	0	0		fre
	Windows Media Player 6	Microsoft Corporation	205	0	-205	0	0		fre
	Windows Media Player 8	Microsoft Corporation	2	0	-2	0	0		fre
	Windows Media Player 9	Microsoft Corporation	65	0	-65	0	0		fre
	WinVNC 3	AT&T Research Labs ...	9	0	-9	0	0		fre
	Microsoft XML Parser SDK	Microsoft Corporation	67	0	-67	0	0		fre
!	XnView	Pierre-e GOUGELET	283	0	-283	0	0		fre
	Windows Movie Maker	Microsoft Corporation	255	0	-255	0	0		fre

Obrázek 21: Licenční audit

Licenční audit pro chybějící licence. Na výše uvedeném obrázku sledujeme název produktu, jeho výrobce, počet instalací bez přidělených licencí, zbytečně přidělené licence a jejich rozdíl. Na obrázku jsou všechny instalace bez přidělených licencí, protože se jedná o freeware.

Přílohou č. 2 je praktická ukázka výstupu z tiskových sestav.

5. Párování software s licencí

Popis činnosti

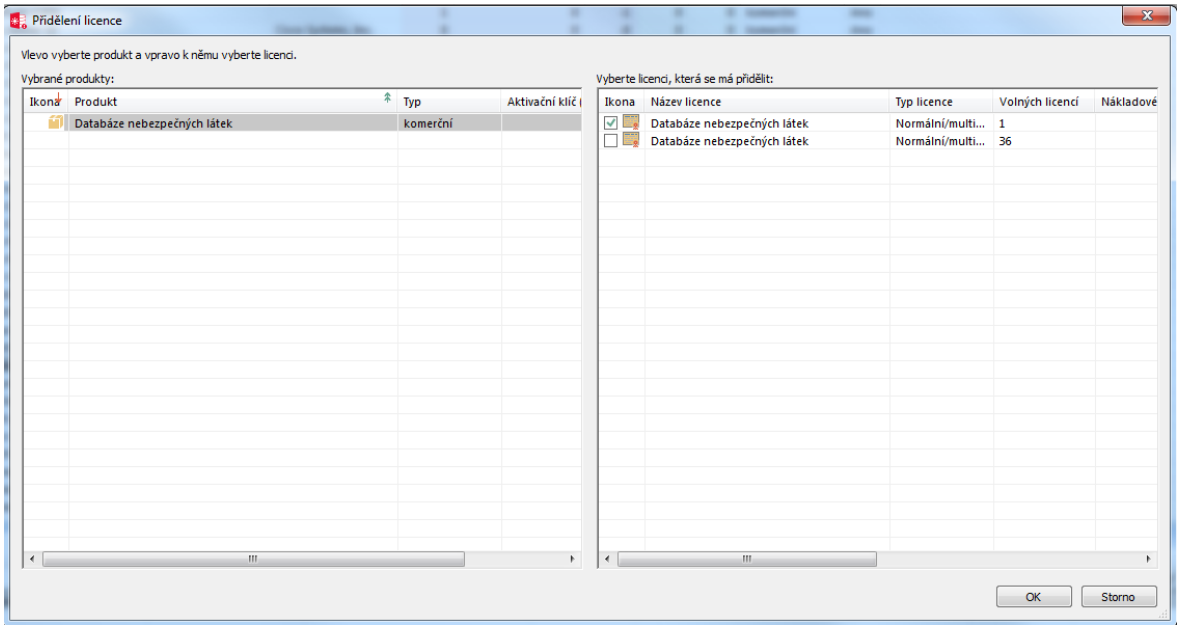
Administrátor kontroluje shodu instalovaného software a dostupné licence, které má k dispozici.

Předpoklady činnosti

- Databáze SAM je přístupná a zřízená
- Aplikace ALVAO je dostupná
- Proveden audit licencí a jejich počtů

Postup činnosti

1. Kontrola automatického přidělení licencí detekcí.
2. Přiřazení licencí ručně.
3. Tisk seznamu přidělených licencí s podpisem odpovědné osoby.



Obrázek 22: Ruční přidělení licence

Licenci, kterou nemůžeme spárovat automaticky je nutno přiradit ručně. K tomu nám slouží výše uvedené dialogové okno přidělení licence.

6. Nákup a nasazení software

Popis činnosti

Činnost sloužící k nákupu nového software a jeho zařazení do užívání v organizaci.

Předpoklady činnosti

- Databáze SAM je přístupná a zřízená
- Aplikace ALVAO je dostupná
- Nový software byl objednán

Postup činnosti

1. Příchozí balík je nutno zkontrolovat na veškeré doklady k dodanému software (dodací list, faktura, licenční karty).
2. Vytvoření kopií všech důležitých dokumentů.
3. Pokud to dovolují licenční podmínky, vytvořit kopii instalačního média.
4. Zadat údaje o software do konzole a přiřadit k němu licenci.
5. Změnit počet využitých licencí v auditu licencí.

7. Údržba a vyřazení software

Popis činnosti

Činnosti sloužící k aktuálnosti přehledu o nainstalovaném software. S údržbou souvisí také odebrání nepoužívaných licencí. Může nastat situace, kdy se počítač kompletně vyřadil bez konečné detekce a tím pádem mohou nastat nesrovnalosti s detekcí počtu licencí. Činnost vyřazení software vede ke smazání nepotřebného nebo nadbytečného software z evidence.

Předpoklady činnosti

- Databáze SAM je přístupná a zřízená
- Aplikace ALVAO je dostupná
- Počítače jsou dostupné v síti

Postup činnosti

1. Pravidelné kontroly dle plánu v (kapitola 6.4)
2. Provedení případných změn
3. Informování vedení organizace při porušení
4. V případě vyřazení zkontrolovat odstranění software z počítače
5. Odstranění dokladů a instalačních médií
6. Oznámení o vyřazení ekonomickému oddělení

6.4 Plán SAM

Jako další krok pro úspěšnou implementaci SAM do podniku je vytvoření plánu, jak časté bude plnění jednotlivých bodů. Níže uvedená tabulka představuje dohodnutý plán s vedením KIS. Je možné, že tato tabulka bude po ročním používání upravena dle požadavků organizace.

Četnost	Název aktivity	Popis aktivity
Měsíčně	Detekce software automatická	Automatické detekce a aktualizace instalovaného software a porovnání zjištěného stavu s databází. Systém si zabezpečuje veškeré činnosti sám a administrátor pouze kontroluje chyby při detekci.
Dle potřeby	Detekce software ruční	Dle potřeby ruční spuštění detekce. Výjimku tvoří měsíční kontrola na počítačích mimo síť HZS KHK.
Měsíčně	Inventarizace licencí	Provedení auditu licencí. Evidence instalací si aktualizuje počty licencí automaticky na základě automatické detekce.
Čtvrtletně	Přehled porušení pravidel	Přehled porušení pravidel pro potřeby vedení organizace. Po provedení přehledu je také nutno informovat nadřízené pracovníky o míře závažnosti porušení pravidel.
Měsíčně	Kontrola automatické detekce	Namátková kontrola automatické detekce na 10% počítačů. Kontrola chybovosti automatické detekce a informace pro nadřízené pracovníky při závažnější chybovosti.
Ročně	Školení v oblasti SAM	Školení pro zaměstnance organizace a jejich seznámení s provozním řádem SAM v podniku.
Ročně	Přehled využívání licencí	Provedení přehledu využívaných kapacit software v organizaci. Vyhodnocení nevyužívaných kapacit s návrhem na jejich vyřazení.

Tabulka 7: Tabulka plánu SAM

7 Závěr

Cílem této práce byla implementace metodického rámce ITIL do reálného prostředí Hasičského záchranného sboru Královéhradeckého kraje. Práce je rozdělena na teoretickou a praktickou část. Teoretická část se zabývá popisem řízení informačních technologií a procesy řízení dle metodik. Popisuje historii jednotlivých nejrozšířenějších metodik a standardů a jejich základní procesní rámce. Pomocí získaných poznatků z rámce ITIL

V praktické části byla představena cílová organizace, její organizační struktura a popis právní úpravy z hlediska implementace konceptů ITIL. Dále vhodně analyzuje a navrhuje bezpečnostní opatření a analýzu rizik. Popisuje práva a povinnosti správců a uživatelů softwarových aktivit a dílčích procesů řízení softwarových aktivit dle ITIL. Posuzuje výběr softwarového řešení pro správu software k implementaci. V závěru praktické části se práce zabývá vhodnou implementací vybraného software ke správě softwarových aktivit

Hlavním přínosem pro organizaci je soubor doporučení a opatření z hlediska správy softwarových aktivit, které při realizaci tohoto opatření vedou ke snížení nákladů organizace, a tím ke zefektivnění procesů dle ITIL. Tato doporučení mohou být inspirací pro využití v řadě dalších středních a velkých organizací.

Dle doporučení zmíněných v této diplomové práci se plánuje reálné nasazení a využívání procesů řízení softwarových aktivit u Hasičského záchranného sboru Královéhradeckého kraje.

8 Seznam použitých zdrojů

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

[2] IT governance pro každého. [online]. [cit. 2015-04-15]. Dostupné z: http://www.systemonline.cz/sprava-it/it-governance-pro-kazdeho.htm

[3] Rámce a metodiky. [online]. [cit. 2015-04-10]. Dostupné z: https://managementmania.com/cs/ramce-a-metodiky

[4] COBIT. [online]. [cit. 2015-04-10]. Dostupné z: http://en.wikipedia.org/wiki/COBIT

[5] COBIT 5. [online]. [cit. 2015-04-10]. Dostupné z: https://managementmania.com/cs/cobit-control-objectives-for-information-and-related-technology

[6] *COBIT: An ISACA Framework* [online]. [cit. 2015-04-15]. Dostupné z: https://cobitonline.isaca.org/

[7] *SOX-online: The Vendor-Neutral Sarbanes-Oxley Site* [online]. [cit. 2015-04-15]. Dostupné z: http://www.sox-online.com/cobit.html

[8] ISANA Now. *ISACA Now* [online]. [cit. 2015-04-15]. Dostupné z: http://www.isaca.org/Knowledge-center/Blog/Lists/Posts/Post.aspx?ID=193

[9] ISO/IEC 20000 Essentials. [online]. [cit. 2015-04-10]. Dostupné z: http://itservicemngmt.blogspot.cz/2008/02/isoiec-20000-essentials.html

[10] ISO/IEC 20000 A Brief History. [online]. [cit. 2015-04-15]. Dostupné z: http://itservicemngmt.blogspot.cz/2011/05/isoiec-20000-brief-history.html

[11] BON, Jan Van a Leo Van SELM. *ISO/IEC 20000 an Introduction*. Zaltbommel: Van Haren Pub, 2008, 238 s. ISBN 90-875-3194-X.

[12] *ISO: International Organization for Standardization* [online]. [cit. 2015-04-15]. Dostupné z: http://www.iso.org/iso/home.html

[13] ISO/IEC 20000. [online]. [cit. 2015-04-15]. Dostupné z: http://cfnpeople.com/our_toolbox/iso_20000/

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

[15] COMMERCE, Office of Government and. *The official introduction to the ITIL service lifecycle*. 2. publ. London: Stationery Office/TSO, 2007, 238 s. ISBN 978-011-3310-616.

[16] *IT Process Maps* [online]. 2015 [cit. 2015-04-15]. Dostupné z: http://wiki.en.it-processmaps.com/

[17] ITIL tajemství zbavený. *Clever And Smart* [online]. 2009 [cit. 2015-04-15]. Dostupné z: http://www.cleverandsmart.cz/itil-tajemstvi-zbaveny/

[18] Comparison between ITIL V3 and ITIL V2. *IT Process Maps* [online]. 2015 [cit. 2015-04-15]. Dostupné z: http://wiki.en.it-processmaps.com/index.php/Comparison_between_ITIL_V3_and_ITIL_V2_-_The_Main_Changes

[19] RUDD, Colin. *ITIL® V3 guide to software asset management*. London: TSO, 2009, 178 s. ISBN 978-011-3311-064.

[20] KOUDELKA, Ctirad. *Rizika a jejich analýza*. Ostrava, 2006. Dostupné z: [20] http://fei1.vsb.cz/kat420/vyuka/Magisterske%20nav/prednasky/web/RIZIKA.pdf. VŠB – TU Ostrava

[21] *System On Line* [online]. 2015 [cit. 2015-04-15]. Dostupné z: http://www.systemonline.cz/

9 Seznam obrázků

10 Seznam tabulek

Příloha č. 1 – Zápis z provedené namátkové kontroly

Zápis z kontroly

Kontrola dle pokynu č. 62 / 2002 počítačových sestav.

Cíl kontroly: prověření shody hardwaru a softwaru s evidenční kartou počítačové sestavy.

1. **sestava:** PS Jaromer01
   zodpovědná osoba: npor. Bc. Pavel Čižmář

   rozdíly: nejsou rozdíly s evidenční kartou

2. **sestava:** PS Jaromer02
   zodpovědná osoba: npor. Bc. Pavel Čižmář

   rozdíly: nejsou rozdíly s evidenční kartou

3. **sestava:** nbPacVit
   zodpovědná osoba: por. Ing. Vít Paclík

   rozdíly: nejsou rozdíly s evidenční kartou

Ve Velkém Poříčí dne 19.1.2009

mjr. Ing. Martin Řehák
vedoucí pracoviště IZS a služeb

Příloha č. 2 – Tiskový výstup automatické detekce software

Nainstalovaný software

Název v síti: **FIEROM**	Inventární číslo počítače:	Sériové číslo počítače: **CZC8142FZN**
Uživatel: **Fiedler Roman** Název organizace: ÚO Náchod	Budova: Budova (1) Poschodí: Podlaží (2) Místnost: Místnost (106) FIEROM	

Operační systém

Microsoft Windows 7 Professional

Komerční software

##Computer games##	Microsoft Office 2010 Standard
Microsoft Office Excel 2010	Microsoft Office Outlook 2010
Microsoft Office PowerPoint 2010	Microsoft Office Publisher 2010
Microsoft Office Word 2010	ALVAO Asset Management Console 8
ALVAO Asset Management Collector 8	ALVAO Asset Management Agent 8
ESET Remote Administrator Console 5	ESET Endpoint Security 5
Cisco Jabber 10	Zoner Photo Studio 17

Příloha č. 2 - pokračování

Freeware

DirectX	Macromedia Flash Player
GIMP	Microsoft NET Framework
PSPad	7-Zip
Firefox	Salamander
UltraVNC	Adobe Flash Player
CDBurnerXP 4	ImgBurn
Google Chrome	Microsoft Office OneNote 2010
Windows Media Player 12	Adobe Reader XI
Internet Explorer 8	