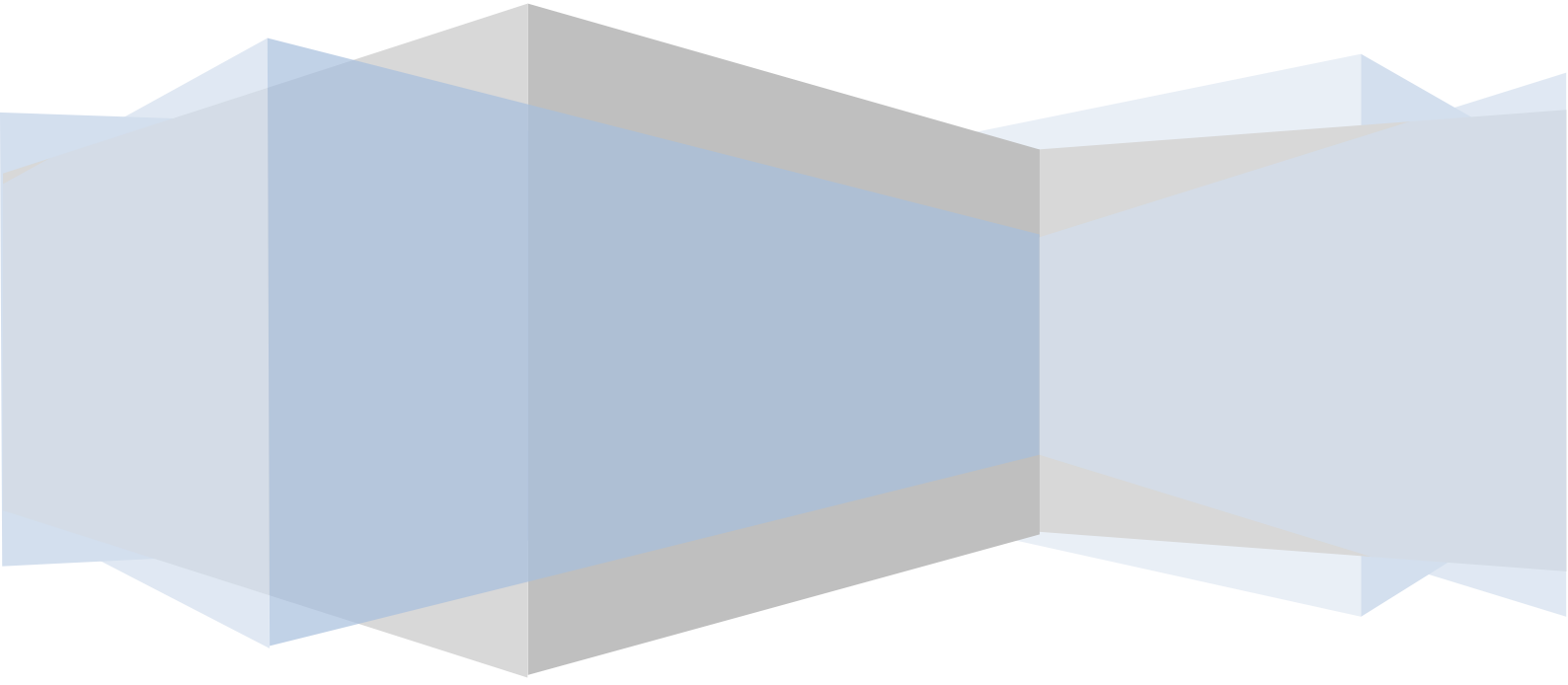
RIADENIE IT PROSTREDIA

Skriptá k predmetu

Martin Sarnovský
Karol Furdík
Erika Školová



Ing. Martin Sarnovský, PhD.

Katedra kybernetiky a umelej inteligencie,
Fakulta elektrotechniky a informatiky
Technická univerzita v Košiciach

Skriptá boli vytvorené v rámci projektu KEGA grantu MŠVVaŠ SR č. 065TUKE-4/2011 „Virtuálne laboratórium hospodárskej informatiky“.

Obsah

Úvod 6
ITIL a ITSM Model 7
Služby a riadenie služieb 7
ITIL 8
História vzniku ITIL 9
Charakteristické črty 10
ITIL V2 vs. ITIL V3 11
Stratégia služieb 14
Návrh služieb 15
Prechod služieb 16
Prevádzka služieb 16
Neustále zlepšovanie služieb 17
Aplikačná podpora ITIL 17
Stratégia služby 19
Úvod 19
Účel 19
Ciele 20
Použité koncepty 21
Stratégia štyroch P 21
Aktíva, zdroje a schopnosti 22
Stanovenie hodnoty služby 23
Balíčky 26
Konkurencia a priestor na trhu 27
Modely poskytovateľov služieb 27
Modely poskytovania služieb 28
Outsourcing služieb, štruktúra alokácie zdrojov (sourcing) 28
Návratnosť investícií 30
Rozvoj organizácie 31
Portfólio a katalóg služieb 31
Procesy Stratégie služby 33
Správa financií IT (IT Financial Management) 35
Správa požiadavok (Demand Management) 35
Správa portfólia služieb (Service Portfolio Management – SPM) 36
Role stratégie služby 37
Návrh služby 38
Úvod 38
Účel 38
Princípy návrhu služby 39
Pri identifikácia požiadaviek na službu roznávame tieto dva druhy požiadaviek: 41
Požiadavky kvality: 41
Podporné systémy – Portfólio služieb 43
Procesy návrhu služby 45
Správa katalógu služieb 46
Manažment úrovní služieb 46
Manažment kapacít 47
Manažment dostupnosti 47
Manažment kontinuity IT služieb 48
Manažment informačnej bezpečnosti 48
Manažment dodávateľov 48

Role Návrh služby ... 48
Prechod služby ... 50
Úvod ... 50
Účel ... 50
Ciele a prínosy prechodu služby ... 50
Procesy prechodu služby ... 52
Plánovanie a podpora prechodu (Transition Planning and Support) ... 53
Manažment zmien (Change management) ... 54
Manažment aktív a konfigurácií (Service Asset and Configuration Management) ... 56
Manažment vydaní a nasadení (Release and Deployment Management) ... 58
Validácia a testovanie služby (Service Validation and Testing) ... 59
Vyhodnotenie (Evaulation) ... 60
Manažment znalostí (Knowledge management) ... 61
Roly prechodu služby ... 62
Záver ... 64
Prevádzka služby ... 65
Úvod ... 65
Manažment udalostí ... 67
Manažment incidentov ... 70
Ciele a prínosy implementácie manažmentu incidentov ... 75
Manažment problémov ... 76
Spracovanie požiadaviek ... 80
Správa prístupov ... 82
Service Desk ... 82
Lokálny service desk ... 84
Centrálny service desk ... 85
Virtuálny service desk ... 85
Role Service desku ... 86
Meranie výkonnosti Service desku ... 87
Záver ... 89
Nepretržité zlepšovanie služieb ... 90
Úvod ... 90
Účel nepretržitého zlepšovania služieb ... 90
Ciele nepretržitého zlepšovania služie ... 91
Pôsobnosť nepretržitého zlepšovania služieb v organizáciách ... 91
Prístup a zmysel nepretržitého zlepšovania služieb ... 93
Prínosy zavedenia nepretržitého zlepšovania služieb ... 94
Zásady nepretržitého zlepšovania služieb ... 97
7 fáz procesu nepretržitého zlepšovania služieb ... 100
Metódy a techniky CSI ... 101
Implementácia procesu neustáleho zlepšovania služieb IT ... 102
Kritické faktory a riziká CSI v praxi ... 105
Záver ... 106
Normalizácia z pohľadu IT prostredia ... 107
Základné princípy štandardizácie a normalizácie ... 108
Norma a štandard ... 108
Úloha, obsah a druhy noriem ... 109
Štandardizácia a tvorba noriem, životný cyklus normy ... 114
Štandardizačné organizácie ... 118
Medzinárodná normalizácia ... 119

Regionálna normalizácia v Európe 124
Národná normalizácia 126
Záväznosť a legislatívny rámec noriem 128
Normalizácia v oblasti IT prostredia a služieb 130
Vývoj noriem v oblasti manažmentu IT služieb 132
Normy pre manažment kvality 134
Normy pre modelovanie a riadenie podnikových procesov 136
Normy pre IT služby a ich riadenie 138
Normy pre bezpečnosť IT systémov 143
Niektoré normy pre technológie IT systémov 144
Certifikácia súladu s normami v oblasti IT prostredia a služieb 146
IT Bezpečnosť a ITIL 151
Úvod 151
Normy a štandardy 153
ISO/IEC 20000 - IT service management 153
ISO/IEC 2700x 154
ISO/IEC 13335 – Smernice pre riadenie bezpečnosti IT 155
COBIT security baseline 156
ITIL 2011 158
Úvod 158
Stratégia služby 158
Návrh služby 160
Prechod služby 162
Prevádzka služby 164
Neustále zlepšovanie služby 167
Záver 167
Referencie 168
Zoznam skratiek 172

Úvod

Hlavným cieľom každej organizácie je dosahovanie zisku, udržanie a zvyšovanie podielu na trhu. Ak chce podnik obstáť v konkurenčnom prostredí, musí dodávať na trh služby kvalitatívne a cenovo zaujímavé pre zákazníka. Znižovanie priamych nákladov má častokrát vplyv na kvalitu. Z tohto dôvodu podnik zväčša znižuje nepriame náklady. Dobre riadené firmy už oddávna dokázali znižovať výrobne náklady, čím získavali vedúce postavenie na trhu. V súčasnosti sa už takmer nenájde firma, ktorá by nebola závislá od informačných a komunikačných technológií (Information and Communication Technology, ďalej len IKT). Ak chcú takéto organizácie dosahovať svoje ciele a obstáť v konkurenčnom prostredí potrebujú, aby tieto technológie boli kvalitné. Z toho vyplýva nevyhnutnosť podniku investovať do nových IKT. Od takýchto investícií podnik očakáva ich návratnosť, ktorá sa posudzuje podľa toho, ako kvalitné a spoľahlivé služby mu tieto informačné a komunikačné technológie môžu poskytnúť. Z tohto dôvodu je nutné sa systematicky zaoberať riadením poskytovania IT služieb tak, aby výsledkom bola nákladovo optimálna dodávka týchto služieb, ktorú obchodné útvary podniku budú môcť použiť k tomu, aby podnik obstál v konkurenčnom prostredí a dosiahol zisk. Pre riadenie IKT sa zaužívala skratka ITSM (IT Service Management). Skúsenosti s organizáciou prevádzky a podpory používateľov IKT, ktoré odborníci zozbierali sa postupom času stali bežne používanými štandardami (napr. BS15000, ISO20000). Štandardom k riadeniu ICT sa stal ITIL (Information Technology Infrastructure Library), ktorý predstavuje sadu publikácií, ktorá obsahuje odporúčania overené praxou, k riadeniu IKT.

ITIL a ITSM Model

Služby a riadenie služieb

Služba vo svojej podstate je definovaná ako akákoľvek činnosť, úžitok či výhoda, ktorá má nemateriálnu povahu a jej výsledkom nie je nadobudnutie vlastníctva. Produkcia služby môže a nemusí byť spojená s hmotným produktom [1]. Zároveň môžeme službu definovať aj ako prostriedok dodávania hodnoty zákazníkovi tým, že sprostredkuje výstupy, ktoré chce zákazník dosiahnuť tak, aby nemusel znášať špecifické náklady a riziká. Ak služba nejakým spôsobom využíva IKT technológie, hovoríme o IT službách. Z iného pohľadu je možné IT službu zadefinovať aj ako jeden, alebo viac IT systémov a mechanizmov, ktoré podporujú jednotlivé podnikové procesy organizácie. IT službami môžeme mať na mysli prevádzku aplikácií, správu dát, zabezpečenie komunikácie a mnoho iných.

Definícia pojmu ITSM o ňom hovorí ako o schopnosti *zabezpečiť dodávku kvalitných IT služieb podporujúcich podnikateľské ciele organizácie použitím nákladovo optimálnych prostriedkov.* ITSM sa teda zaoberá riadením IT služieb a to tak, aby tieto služby boli poskytované efektívne a kvalitne. ITSM tento cieľ dosahuje pomocoi riadenia interakcie medzi ľuďmi, procesmi a technológiami.

ITSM je výrazne zákaznícky orientované, pričom zákazníkom je ten, kto službu odoberá a kto za jej odber platí, pričom môže ísť o zákazníka externého, tak interného:

- *Externý zákazník* je obchodným partnerom podniku, ktorý si kupuje niektorý z podnikových produktov (výrobok alebo službu).
- *Interný zákazník* je predstaviteľom užívateľov podnikovej ICT infraštruktúry (t.j. v zásade vedúci pracovník niektorého podnikového obchodne - prevádzkového útvaru).

Charakteristickou črtou ITSM je poskytovať iba také služby, ktoré sú požadované. Je dôležité pochopiť obchodné procesy firmy a jej strategický plán pre správne pochopenie požadovaných služieb. Taktiež je nevyhnutná neustála komunikácia s

odberateľom vo všetkých štádiách dodávky IT služieb. Snahou ITSM je dodávať nákladovo optimálne služby. Veľkosť nákladov na poskytované IT služby závisí od typu, prosperity a vedenia firmy. Je dôležité informovať odberateľa IT služieb o veľkosti nákladov spojených s dodavkov týchto služieb. Odberatelia IT služieb si taktiež musia uvedomiť, že čím viac do týchto služieb investujú, tým kvalitnejšie služby dostanú. Medzinárodne platnou normou pre ITSM je 2005 ISO/IEC 20000. Vychádza už z existujúcej normy British Standard, BS 15000. V roku 2005 bola vyhlásená za medzinárodne platnú normu ITSM. Podobne ako BS 15000 sa skladá z dvoch častí:

- ISO/IEC 20000-1:2005 – IT service management – Špecifikácia pre service management
- ISO/IEC 20000-2:2005 – IT service management – Predpis pre vykonávanie service manažmentu

ITIL

ITIL (Information Technology Infrastructure Library) je súbor najlepších postupov (Best Practice) pre riadenie IKT služieb. Vznikol v 80. rokoch 20. storočia vo Veľkej Británii a dnes ide o medzinárodne uznávaný štandard v oblasti riadenia IKT. Pôvodne vznikal, ako snaha britskej agentúry CCTA (Central Computer and Telecommunication Agency) o štandard podobný ISO 9000, ale zameraný na poskytovanie služieb. Informácie popísané v ITIL sú šírené formou kníh, CD, školení, konzultácií a certifikácií. ITIL však nie je metodika, ale rámec pre návrh ITSM procesov. Vychádza z najlepších praktických skúsenosti, pričom ponecháva veľkú voľnosť pri implementácií týchto procesov.

Hlavným prínosom je predovšetkým jasné pochopenie k čomu jednotlivé procesy slúžia a aké väzby medzi nimi sú, aké role by sa mali podieľať a aké parametre má mať proces. ITIL nie je len návodom ako dobre riadiť IT služby, ale obsahuje tiež návody k poskytovaniu a zlepšovaniu IT služieb. Mechanizmus na zlepšovanie činností je priamo v jednotlivých procesoch a implementácia podľa ITILu je zárukou priebežného zlepšovania kvality a produktivity.

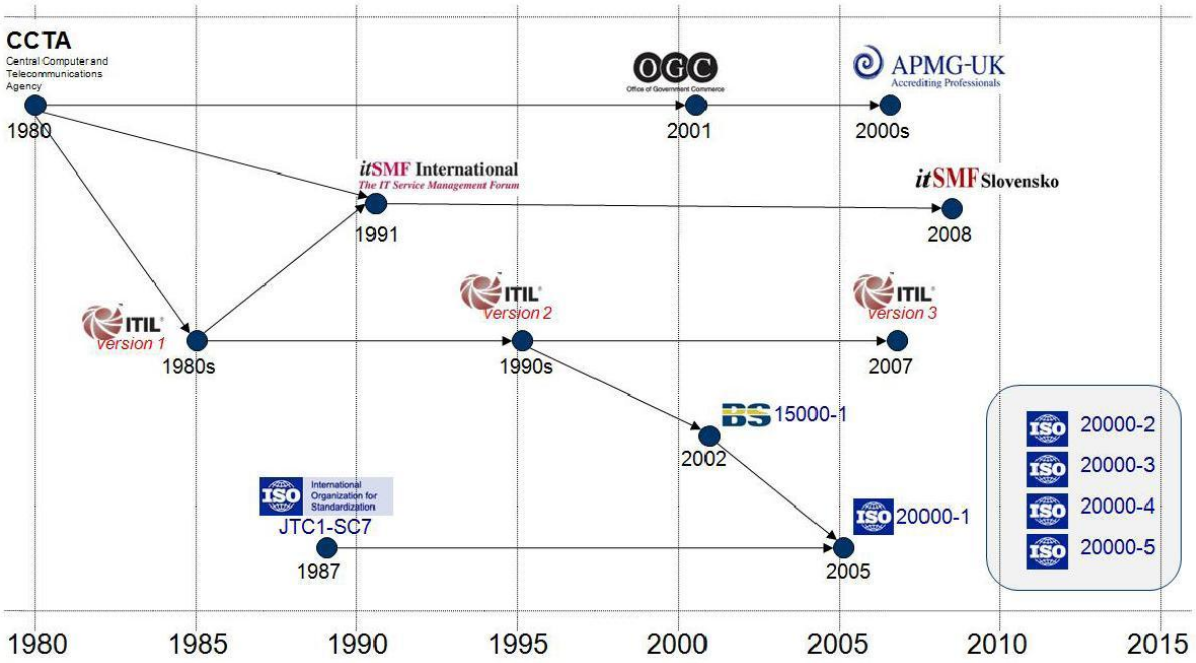
História vzniku ITIL

V rokoch 1989 až 1995 vo svete narastá závislosť na informačné a komunikačné technológie a z toho vyplývajúci rast požiadaviek na kvalitu IT služieb.
Najprv to bolo zo strany britskej vládnej agentúry CCTA (Central Communications and Telecommunications Agency), ktorá neskôr vydá 46 knižných zväzkov obsahujúci najlepšie praktiky z oblasti IT služieb z čoho vznikne ITIL vo verzii 1.0.

V 90. rokoch sa zlúčili tri britské vládne agentúry spolu s CCTA z čoho vzniká OGC (Office of Government Commerce) a stávajú sa hlavnou autoritou pre reedície a vydávanie ďalších publikácií ITIL. V tom čase vzniká itSMF (IT Service Management Forum) a stáva sa medzinárodnou komunitou profesionálov a odbornej verejnosti z oblasti ITSM a ITIL. Sféru ITIL preberajú súkromné i verejné subjekty, ktoré začínajú vydávať prvé certifikáty odbornej spôsobilosti pre oblasť ITSM podľa ITIL.

Na prelome storočia (2000-2004) prichádza k zredukovaniu 46 knižných publikácii na sedem knižníc, kde základom sú knižnice Service Support a Service Delivery, ktoré definujú oblasť ITSM z čoho následne vzniká ITIL vo verzii 2.0. Táto druhá verzia začala byť univerzálne akceptovaná v mnoho krajinách a tisícky organizáciami ako základňu pre efektívne poskytovani služieb IT.

V novembri 2004 OGC začína projekt s názvom Scoping Proces, ktorého cieľom bolo pracovať na tretej aktualizácii knižnice ITIL. V auguste 2005 OGC zverejňuje podrobnosti o ITIL verzie 3, kde celá knižnica bude rozdelená do štyroch blokov. Ešte v Decembri toho roku je vydaná medzinárodná norma pre časť ITSM – ISO/EIC 20000. Rok 2006 prináša celosvetové rozšírenie normy ISO/IEC 20000 a práce na druhom bloku ITIL verzie 3. V 2007 bol ITIL verzie 2 vystriedaný treťou verziou ITIL.



Obr. 1 História vzniku ITIL

Charakteristické črty

ITIL používa moderne procesne orientovaný prístup k riadeniu IT služieb (na rozdiel od tradičného funkcionálneho riadenia). Proces je logický sled úloh transformujúcich určitý vstup na určitý výstup, pričom plnenie jednotlivých úloh v procese je zaisťované úlohami s jasne definovanými zodpovednosťami. Celý proces je riadený, monitorovaný, meraný, vyhodnocovaný a neustále vylepšovaný, a to má na starosti vlastník tohto procesu. ITIL je orientovaný na zákazníka. Tento rys vyplýva priamo zo samotnej podstaty ITSM a to, že všetky procesy sú navrhnuté s ohľadom na potreby zákazníka, tzn. každá aktivita, každý úkon v každom procese musí prinášať určitú pridanú hodnotu pre zákazníka - ak neprináša, potom je taká činnosť nadbytočná. Rámec ITSM procesov podľa ITIL je nezávislý na akejkoľvek platforme. Dokonca je možné ITIL použiť i pre návrh procesov (úplne mimo oblasť ICT) v akejkoľvek firme, ktorá podniká v oblasti služieb. Knižnica je voľne dostupná, čo znamená, že každý si môže knihy ITIL kúpiť a procesy ITSM podľa ITIL vo svojom podniku implementovať. Táto skutočnosť okrem iného prispela aj k rýchlemu celosvetovému rozšíreniu ITIL.

Formálne deklarované ciele ITIL sú:

- zvýšenie kvality,
- zníženie nákladov,
- zlepšenie dostupnosti,
- vyladenie kapacity,
- zvýšenie výkonu,
- optimalizácia využitia zdrojov,
- vysoká škálovateľnosť.

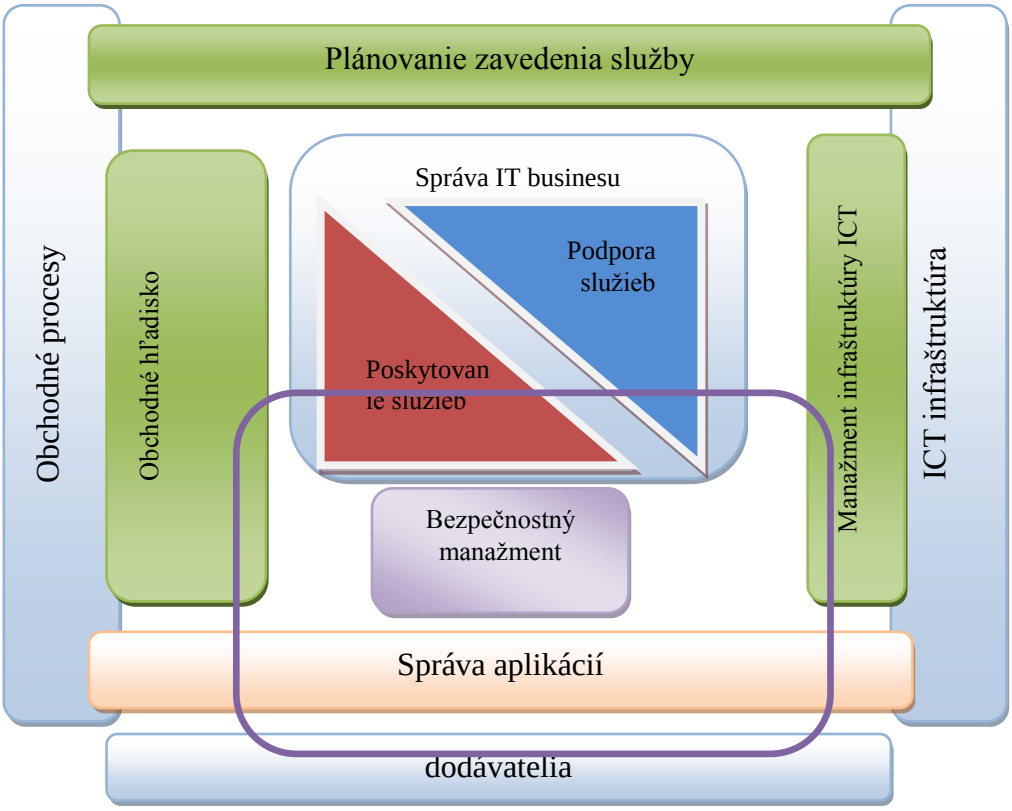
ITIL vo verzii 3 bol publikovaný v máji 2007 a skladá sa z troch oddelených častí:

• Kľúčové publikácie (Core) - tvoria jadro a pokrývajú jednotlivé časti životného cyklu služby.
• Doplnkové publikácie (Complementary) - tvoriace nadstavbu nad jadrom, popisujú špecifiká ITIL v závislosti od konkrétnej oblasti, prostredia či situácie. Zahŕňajú v sebe detailnejšie procesné mapy, mapovanie ITIL na oblasť IT governance a ďalšie rámcové modely a techniky.
• Dokumentácia na webe (Web based material) - budú ju tvoriť doplnkové dynamické zdroje ako šablóny, dokumenty typu „White paper“ či prípadové štúdie sa výhradne distribuuje prostredníctvom webu. Zahŕňa pravidelne aktualizácie, čo prináša lepšie a aktuálnejšie návody.

ITIL V2 vs. ITIL V3

ITIL vo svojej druhej verzii pozostával z 8 základných zväzkov, ktoré môžete vidieť na Obr. 2.. Hlavnou zmenou oproti verzii 2 je prechod od procesného riadenia k životnému cyklu služieb. Ďalšou zmenou je rozšírenie obsahu, a to rozšírením o fázu ako je návrh služieb a ich stratégie. Celkový cyklus môžete vidieť na Obrázku č.4. najvýraznejšou zmenou oproti ITIL V2 je pridanie celej rady nových procesov, funkcií, procesných aktivít či rolí. Na druhej strane klesla úroveň detailov popisujúcich jednotlivé elementy – napr. procesov (a to v časti týkajúcej sa potenciálnych rizík, problémov a doporučení pre implementáciu – v oblasti, kde sa najčastejšie vyskytujú chyby). Celkovo ITIL V3 je rozšírením V2. Obrázok č.4 zobrazuje dátové a procesné toky medzi jednotlivými časťami životného cyklu služieb a ich výstupy. ITIL V3 je

rozšírená o 12 procesov, ktoré posilňujú riadenie celého životného cyklu služby a kladú dôraz na vytváranie obchodnej hodnoty a zlepšovanie výkonu procesov. Tieto doplnkové procesy, publikácie pozostávajú zo znalostí a získaných skúseností, špeciálnych tém (outsourcing), nových šablón, detailov použitých metód v minulosti, ktoré sa určitým spôsobom stali štandardom. Ďalším rozšírením je súlad s medzinárodnými normami, alebo sady rôznych užívateľských príručiek, či už pre manažérov, alebo pre potreby študentov. Nové publikácie popisujú ako rýchlo a efektívne dosiahnuť prínosy v malých, ale i veľkých organizáciách.

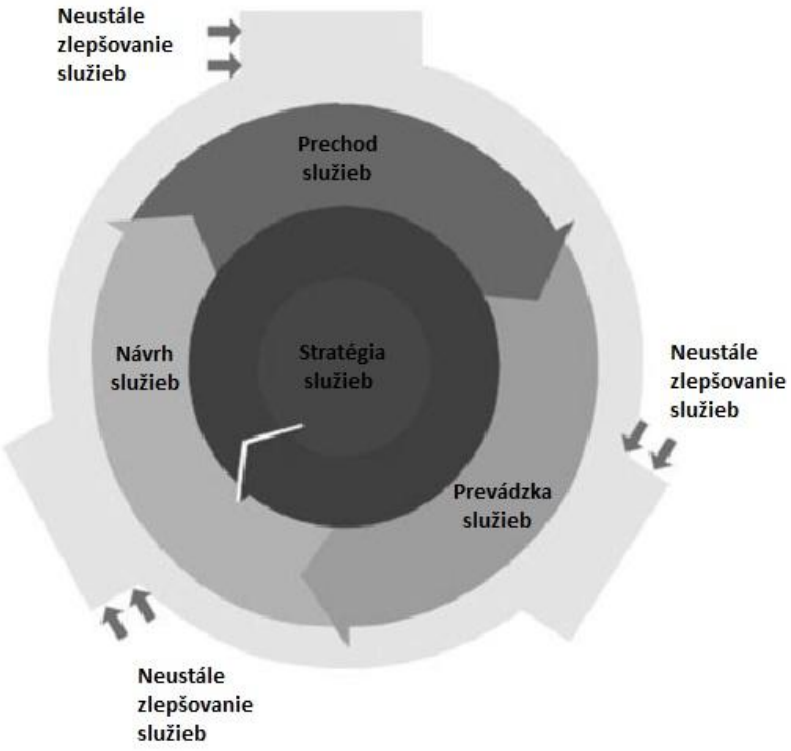


Obr. 2 ITIL V2

Kľúčové publikácie tvorí séria piatich kníh (Obr. 3). Každá z nich dáva užitočné pokyny pre dosiahnutie integrovaného prístupu podľa štandardu ISO/IEC 20000:

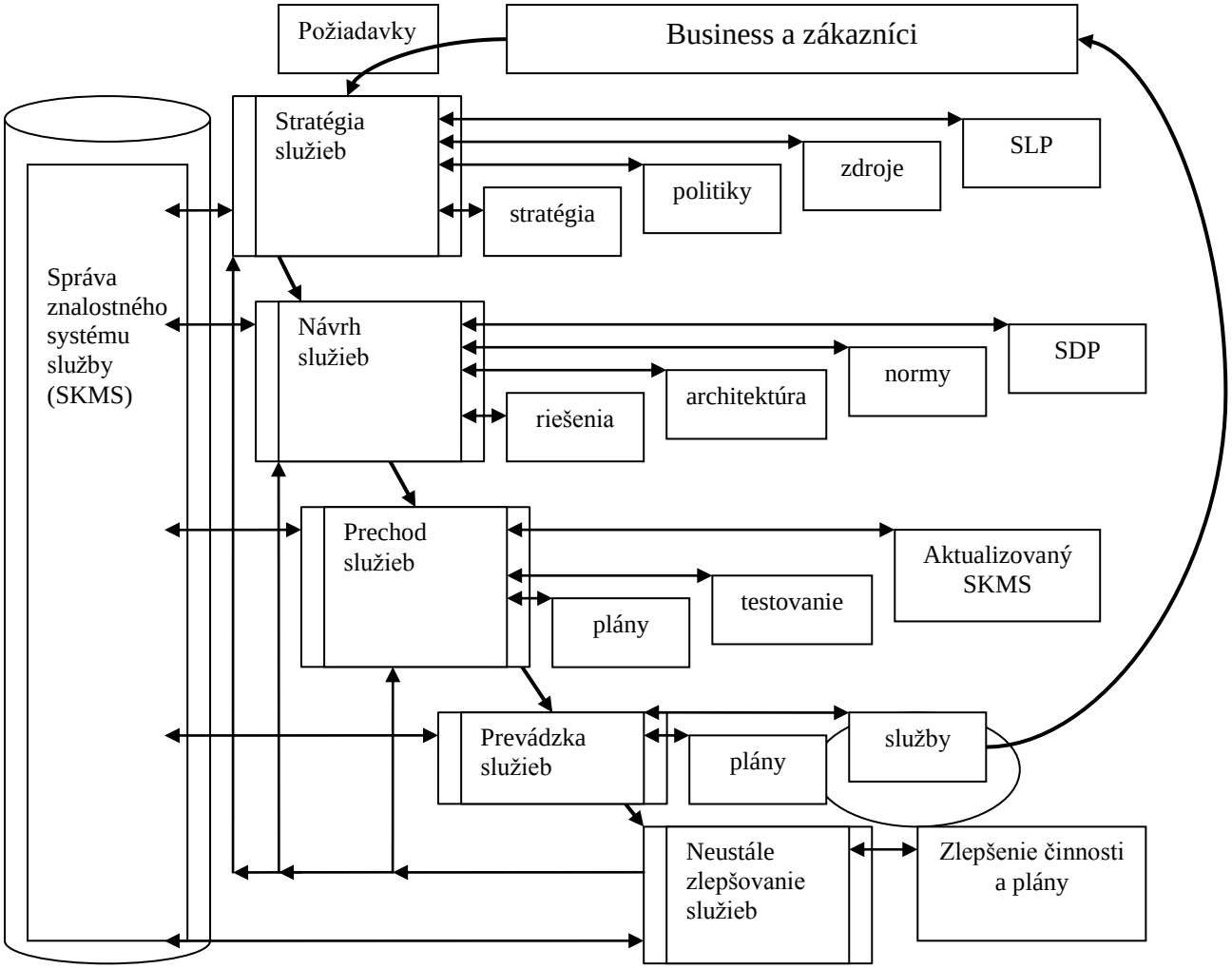
- Stratégia služby (Service Strategy)
- Návrh služby (Service Design)

- Prechod služby (Service Transition)
- Prevádzka služby (Service Operation)
- Neustále zlepšovanie služby (Continual Service Improvement)



Obr. 3 ITIL V3

Životný cyklus služby sa začína knihou *Stratégia služieb*, kde sa plánuje podniková stratégia a z nej vyplývajúca stratégia IT služby. Nasledujúca publikácia *Návrh služieb* definuje vlastný návrh služieb, infraštruktúry, podporných procesov a podporných systémov. Ďalším pokračovaním je kniha *Prechod služieb*, ktorá sa zaoberá prechodom služby do prevádzkového prostredia, ktorý zahŕňa testovanie, vlastné nasadenie, školenie a validáciu. Ďalej nadväzuje publikácia *Prevádzka služieb*, ktorá pokrýva všetky prevádzkové aspekty služby. Celý cyklus uzatvára kniha *Neustále zlepšovanie služieb*, ktorá sa zaoberá priebežným vylepšovaním služby.



Obr. 4 Životný cyklus riadenia služieb podľa ITIL V3

Stratégia služieb

Ústredná publikácia poskytujúca praktický rámec pre návrh, vývoj a implementáciu riadenia služieb nielen z pohľadu organizačného, ale aj z pohľadu zdroja strategickej výhody. Kniha obsahuje definície služieb, stratégie ITSM a plánovanie pridanej hodnoty, definície typov poskytovateľov služieb a obchodných stratégií a stratégií služieb. Stratégia poskytovateľa služieb musí byť založená na tom, že zákazník nekupuje produkty, ale uspokojuje konkrétne potreby. Preto pre dosiahnutie úspechu musia byť poskytované služby vnímané zákazníkom tak, že ponúkajú dostatočnú hodnotu, ktorú zákazník požaduje.

Aby sme dosiahli úplné porozumenie, zákazníkovi musíme podať odpovede na otázky, čo sú potreby, kedy a prečo sa vyskytujú a tiež musíme vedieť zhodnotiť zákazníka alebo potenciálneho zákazníka pre dosiahnutie úplného uspokojenia. To zároveň znamená, že poskytovateľ musí rozumieť širšiemu kontextu aktuálnych a potenciálnych trhov, kde operuje alebo plánuje poskytovať takéto služby.

Stratégia služieb nemôže existovať samostatne niekde mimo podniku, organizácie. Poskytovateľ služby môže existovať v rámci organizácie jedine pre dodávanie služieb v špecifickom odbore obchodu, zároveň je tu možnosť vytvoriť stredisko, ktoré bude zastrešovať niekoľko pobočiek danej organizácie. Čím sa zároveň dosiahne minimalizovanie nákladov. Daná stratégia by mala poskytovať dostatočnú kvalitu všetkým zainteresovaným stranám poskytovania služieb.

Návrh služieb

Táto publikácia poskytuje rámec pre návrh a vývoj služieb a procesov ich riadenia. Zahrňuje princípy a metódy pre prechod strategických cieľov do portfólia služieb. Nesústredí sa iba na nové služby, ale obsahuje i procesy zmeny a procesy priebežného zlepšovania už poskytovaných služieb. Tieto procesy sú potrebné pre udržanie alebo prípadné zvýšenie úrovne služieb, zvýšenie pridanej hodnoty pre zákazníka a v neposlednom rade aj pre ich súlad s právnymi normami a štandardmi.

Hlavným zámerom a cieľom je navrhnúť všetky služby tak, aby vyhovovali dohodnutým výstupom a podporovali životný cyklus služieb. Určitým spôsobom ako dokumentovať návrh služieb je *Service Model*. Predstavuje grafickú reprezentáciu komponentov, ktoré službu tvoria. Zobrazuje nielen komponenty, ale i vzťahy a interakcie medzi nimi a tiež spôsob ako službu používa užívateľ. Základ service modelu môže vzniknúť pri prvých diskusiách o tom, ako bude služba fungovať. Vytvára ho architekt alebo obchodník na podporu dohody s ostatnými zamestnancami, ktorí sa budú podieľať na vývoji a prevádzkovaní služby [2]. ITIL neurčuje detailne ako má service model vyzerať, ale necháva priestor pre kreativitu tvorcov. Pri jeho tvorbe môžeme využívať metódy a nástroje systémového inžinierstva, workflow diagramov alebo procesných máp. Sám o sebe service model nestačí na implementovanie služieb preto je doplnený detailnými informáciami ako sú

biznis, funkčné a prevádzkové požiadavky, akceptačné kritéria a plány pre nasadenie služby do prevádzky. Všetky tieto dokumenty vytvorené vo fáze Návrh služieb tvoria balíček návrhu služby (Service Design Package). Tento balíček je posunutý do ďalšej fázy, a to Prechod služieb [6].

Prechod služieb

Publikácia obsahuje postup, akým spôsobom požiadavky definované v rámci Service Strategy efektívne zrealizovať v priebehu Service Operation (reálne prostredie) za súčasného riadenia rizík porúch a výpadkov služieb. Úlohou je teda na základe balíčka návrhu služby (či už novej, alebo aktualizovanej) uviesť ju do praxe tak, aby ju užívatelia mohli začať používať. Publikácia poskytuje rámec pre riadenie komplexnej problematiky spojenej so zmenami v službách a v procesoch ich riadenia.

Poskytuje aj procesy spojené so zavedením fázy s názvom *Počiatočná podpora*, ktorá začína okamžite ako sa uvedie služba do ostrej prevádzky. Kombinuje postupy Správy verzií (Release Management), Riadenia programu (Programme Management) a Správy rizík (Risk Management) a transformuje ich do praktického kontextu riadenia služieb ako celku. Okrem toho publikácia popisuje procesy súvisiace s manažmentom zmien a poskytuje štandardné metódy pre zabezpečenie riadenie zmien. Nemenej dôležitou časťou je v tejto fáze zavedenie pojmu konfuguračná databáza, čo predstavuje databázu, ktorá dokumentuje atribúty každého komponentu IT infraštruktúry a poskytuje model jednotlivých komponentov a ich vzájomných vzťahov a závislostí.

Prevádzka služieb

Táto publikácia obsahuje postupy pre riadenie služieb v produkčnom prostredí, dosiahnutie výkonnosti a účinnosti v dodávke služieb a v ich podpore tak, aby bola vyprodukovaná hodnota ako pre zákazníka tak i pre poskytovateľa služby. Táto časť

ITIL V3 v najväčšom rozsahu preberá knihy Service Strategy a Service Delivery ITIL V2. Procesy, ktoré sú v publikácii popísané, slúžia k monitorovaniu, údržbe a zlepšovaniu služieb. Zahrňujú správu incidentov a požiadaviek na služby, správu problémov a správu prevádzky. Tento proces pracuje s každodennými požiadavkami zákazníka na službu či servis a stará s o to, aby kvalita poskytovaných služieb dosahovala požadovanú úroveň [7]. Vo fáze prevádzky služieb sa kľúčové procesy ITIL venujú najmä riadeniu udalostí, incidentov a problémov. ITIL tu poskytuje rámec na ich spracovávanie, ktoré spočíva hlavne v ich filtrácií, kategorizovaní a pod..

Neustále zlepšovanie služieb

Táto publikácia obsahuje prostriedky pre vytváranie a udržovanie pridanej hodnoty služby pre zákazníka prostredníctvom zvyšujúcej sa kvality služieb a efektivity ich prevádzky. Kombinuje princípy, praktiky a metódy z riadenia kvality, správy zmien a zlepšenie kapacít, pričom pracuje na zlepšení každej fázy životného cyklu, ako aj aktuálnych služieb, procesov- Obsahuje prostriedky pre vytváranie a udržovanie hodnoty služby prostredníctvom zvyšujúcej sa kvality služieb a efektivity prevádzky.

Kľúčové procesy a činnosti:

- meranie služieb (Service Measurement),
- reportovanie služieb (Service Reporting),
- zlepšovanie služieb (Service Improvement).

Hlavným procesom je tzv. 7-Step Improvement Process. Ide o sedem krokov, ktoré pokrývajú zlepšovacie aktivity, od definície metrík a zberu dát až po implementáciu. Mimo aktivít v jednotlivých fázach životného cyklu ITIL poskytuje rámec pre *Riadenie rizík* (Risk Management) v priebehu všetkých fáz života služby, pričom je riziko chápané nielen ako potenciálna hrozba, ale tiež ako nevyužitá príležitosť [6].

Aplikačná podpora ITIL

Certifikáciou a verifikáciou súladu softvérových nástrojov s myšlienkami ITIL sa zaoberá portál *PinkElephant* so svojim certifikačným programom *PinkVerify* [6]. Softvérové nástroje môžu získať nasledovné stupne certifikácie:

● *PinkVerify™ Service Support* Enhanced – tento certifikát je softvérovému nástroju udelený, ak pokrýva Manažment incidentov, Manažment problémov, Manažment zmien, Manažment konfigurácií a minimálne jeden z manažmentov: Manažment úrovne služieb, Manažment vydaní alebo Manažment dostupnosti.

● *PinkVerify™ Service Support* – sa udeľuje softvérovému nástroju, ak pokrýva manažmenty incidentov, problémov, zmien a konfigurácii.

● PinkVerify™ *Service Monitoring* – sa udeľuje softvérovému nástroju, ak je kompatibilný s procesmi Manažmentu dostupnosti a Manažmentu kapacít.

● *PinkVerify™ Service Deployment* – sa udeľuje softvérovému nástroju, ak je kompatibilný s procesmi Manažmentu zmien a Manažmentu vydaní.
Pre porovnanie ponúkame dva zásadne odlišné pohľady, na jednej strane komerčný produkt s veľkou oblasťou záberu a širokou funkcionalitou a na strane druhej jednoduchý voľne dostupný nástroj s menšími nárokmi no s menšími možnosťami nasadenia.

Stratégia služby

Úvod

Publikácia sa zaoberá súčasnými a budúcimi obchodnými požiadavkami podniku, rozoberá návrh a vývoj služieb a procesov riadenia IT. Cieľom je poskytnúť návody na tvorbu a údržbu stratégií a architektúry IT a dokumentovať návrh adekvátnych a inovatívnych riešení služieb a procesov IT. Zameriava sa nielen na nové služby, ale aj zmeny v existujúcich službách a rôzne vylepšenia smerujúce k tomu, aby sa zachovala, resp. zvýšila pridaná hodnota pre zákazníkov v priebehu životného cyklu služby. V princípe by sa dalo povedať, že publikácia mieri na vývoj a prevádzku. Obsahuje pôvodnú knihu Dodávka služby z predchádzajúcej verzie knižnice ITIL, ale rozšírenú o nový obsah. Publikácia obsahuje a popisuje procesy, ktoré sú aktualizované z verzie ITIL v2:

- Správa kapacít (Capacity management)
- Správa dostupnosti (Availability Management)
- Správa úrovní služieb (Service Level Management)
- Správa kontinuity služieb IT (IT Service Continuity Management)
- Správa informačnej bezpečnosti (Information Security Management)

Ďalej definuje nové procesy, ktorými sú:

- Správa katalógu služieb (Service Catalogue Management)
- Správa dodavateľov (Supplier Management)

Výstupom tejto fázy životného cyklu je samotný návrh riešenia (nielen služieb, ale aj procesov, meraní, systémov, atď.), návrh architektúry, definícia štandardov a tzv. balíček návrhu služby (Service Design Package/SDP).

Účel

Stratégia služieb akéhokoľvek poskytovateľa služieb by mala byť založená na zásadnom princípe - zákazník nekupuje produkty, ale uspokojenie svojich konkrétnych (častokrát špecifických) potrieb prostredníctvom nejakej služby. Pre dosiahnutie úspechu je preto potrebné, aby boli poskytované služby vnímané

zákazníkom ako „produkty“, ktoré poskytujú dostatočnú hodnotu vo forme výsledkov, ktoré chce zákazník dosiahnuť. Aby sme lepšie pochopili aké sú presne potreby zákazníka, musíme porozumieť tomu, aké sú jeho potreby, čo pre neho znamenajú a kto sú naši existujúci a potenciálny zákazníci. To vyžaduje, aby poskytovateľ služieb rozumel širšiemu kontextu aktuálnych a potenciálnych trhov, kde je poskytovateľ služieb činný, alebo kde plánuje pôsobiť. Stratégiu služieb nie je možné vytvoriť, rovnako ako zaistiť jej existenciu, v izolácii mimo celkovú stratégiu, resp. podnikovú kultúru, ku ktorej poskytovateľ služieb patrí. Poskytovateľ služby môže existovať v rámci organizácie výlučne pre dodávku služieb špecifickej jednotke businessu (typ I), pre poskytovanie služby viacerým jednotkám businessu (typ II), alebo môže operovať ako externý poskytovateľ služby, ktorý poskztuje služby viacerým externým businessom (typ III). Prijatá stratégie však musí vždy poskytovať dostatočnú hodnotu zákazníkom a všetkým zainteresovaným stranám – musí spĺňať strategický zámer poskytovateľa služieb.

Ciele

Stratégia služieb by mala byť založená na jasnom uznaní existencie konkurencie na trhu, nezávisle od kontextu, v ktorom fungujeme ako poskytovateľ služieb; na poznaní, že každá strana má možnosť výberu, a na zámere, ako sa chceme ako poskytovateľ služieb odlíšiť od konkurencie. Všetci poskytovatelia služieb potrebujú definovať stratégiu služieb. Z tohto dôvodu tvorí publikácia SS skutočné jadro životného cyklu ITIL v3. Zameriava sa na návody pre všetkých poskytovateľov služieb IT a ich zákazníkom, ako prevádzkovať a dlhodobo udržať jasnú stratégiu služieb. V praxi to znamená mať presné porozumenie:

- aké služby poskytovať (portfólio a katalóg služieb)
- komu tieto služby ponúkať (zákazníci)
- ako rozvíjať vnútorné a vonkajšie trhy pre tieto služby existujúce a potenciálne konkurencie na týchto trhoch a ciele, ktoré odlíšia

hodnotu toho, čo robíme, alebo ako to robíme

- ako môžeme vytvárať obchodné prípady pre investície v oblasti správy služieb
- ako budú zákazníci a zainteresované strany vnímať a merať hodnotu (výkonnosť služieb), a ako bude táto hodnota vytváraná
- ako budú zákazníci rozhodovať o zdrojoch služieb s ohľadom na využitie rôznych typov poskytovateľov služieb
- ako dosiahnuť priehľadnosti a kontroly vytváraní hodnôt prostredníctvom správy financií
- ako by malo byť nastavené rozmiestnenie dostupných zdrojov pre dosiahnutie optimálneho efektu s ohľadom na celkové portfólio služieb, vrátane riešenia prípadných konfliktov

Publikácia sa zaoberá v tomto kontexte strategickým plánovaním a berie do úvahy určité faktory, akými sú napr. silné a slabé stránky, unikátnosť na trhu, stratégia businessu, kritické faktory úspechu a možné hrozby a príležitosti a ich vplyv na stratégiu služieb.

Použité koncepty

Stratégia štyroch P

Jedným zo základných konceptov používaných v časti Stratégie služieb je tzv. Koncept štyroch P. Tento koncept je použitý v kontexte nosnej myšlienky pre

stanovenie úspešnej a integrovanej stratégie, ktorá pomôže udržať stanovené ciele. 4P je v tomto prípade skratka štyroch slov:

- perspektíva: príznačná vízia a smer. Vo všeobecnosti platí, že ak spoločnosť má ucelenú víziu toho, čo chce dosiahnuť, má aj lepší pohľad na ciele podnikania. Spoločnosť majúca jasnú víziu služieb, ktoré chce poskytovať vie svoje podnikanie vhodnejšie cieliť na skupinu svojich zákanzíkov a je schopná s nimi lepšie interagovať. Takýmto postojom vie poskytovateľ služieb vytvoriť charakteristický rozdiel od ostatných konkurentov na trhu a pomôže mu v okruhu zákazníkov získať stabilné miesto.

- pozícia: základňa, kde bude poskytovateľ pôsobiť. Najmä v oblasti IT je pre úspešného IT poskytovateľa podstatné definovať spôsob podnikania. Tento koncept Stratégie služby hovorí práve o nutnosti poznať pozíciu spoločnosti vo všetkých aspektoch. Spoločnosť poskytujúca služby by sa mala pevne rozhodnúť čo najskôr aké služby bude poskytovať a ako bude ich hodnota mapovaná na užitočnosť resp. záruku.

- plán (strategický): ako poskytovateľ dosiahne svoje vízie. Predstauje kľúčový faktor úspechu a to vytvorenie detailného plánu, akým spôsobom bude všetko stanovené dosiahnuté. To teda znamená aké metódy resp. fomry rozhodovania sa bude podnik používať, resp. zvažovať.

- profil (pattern): zásadný spôsob realizácie vecí – charakteristické znaky pri rozhodovaní a správanie sa v priebehu doby. Pod pojmom profil, aleb vzor sa tu definje nejaká množina po vykonávaných akcií a úprav, ktoré poskytovateľ vykonáva a ktoré umožňujú chod spoločnosti. Ak spoločnosť vie, ktoré vzory sú pre ňu vhodné, napomáha to fungovaniu spoločnosti. Poskytovateľ sa musí rozhodnúť, ktoré politiky, techológie, ostatné koncepty ako model poskytovateľa, služieb atď. sú preň ideálne.

Aktíva, zdroje a schopnosti

Jedným zo základných použitých konceptov naprieč fázou Stratégie služby je definícia aktív, zdrojov a schopností. Pod pojmom aktívum môžme rozumieť ľubovoľný zdroj, alebo schopnosť, ktoú má podnik k dispozícii. Zdroj je definovaný ako všeobecný termín, ktorý zahŕňa infraštruktúru, ľudí, financie, alebo čokoľvek iné, čo môže prispieť k dodávke služby. Schopnosť na druhej strane vyjadruje ako je daný proces, služba, aplikácia, osoba schopná vykonávať aktivitu.

Schopnosti a zdroje sú využívané na vytváranie hodnoty, ktorá je dodávaná prostredníctvom služby. Zdroje podniku sú relatívne jednoducho získateľné prostriedky, zatiaľčo schopnosti sa získavajú a formujú časom. Schopnosti tak vlastne reflektujú skúsenosť podniku a umožňujú premeniť zdroje na služby. Príklady rôznych zdrojov a schopností sú uvedené v tabuľke Tab. 1

Zdroje	Schopnosti
Kapitál	Manažment
Infraštruktúra	Organizácia
Aplikácie	Procesy
Informácie	Znalosti
Ľudia	Ľudia

Tab. 1. Príklady rôznych zdrojov a schopností

Stanovenie hodnoty služby

Použitým konceptom je stratégia správy služieb a plánovanie podľa pridanej hodnoty (tzv. value planning). Toto plánovanie používa vždy orientovanú dvojicu *funkčnosť* (utility) a *záruka* (warranty). Funkčnosť definuje, či služba vyhovuje pre účely biznisu, a záruka definuje, či služba vyhovuje z hľadiska použitia (požadovaná dostupnosť, kapacita, kontinuita a bezpečnosť). Ďalej je tu použitý aj koncept „agentúry poskytujúcej agentov“, ktorá funguje tak, že majiteľ firmy buď najíma alebo zamestnáva agentov, ktorí jednajú v jeho záujme v určitej oblasti. Agenti môžu byť zamestnanci, konzultanti, poradcovia, alebo poskytovatelia služieb. Agenti sú jednak

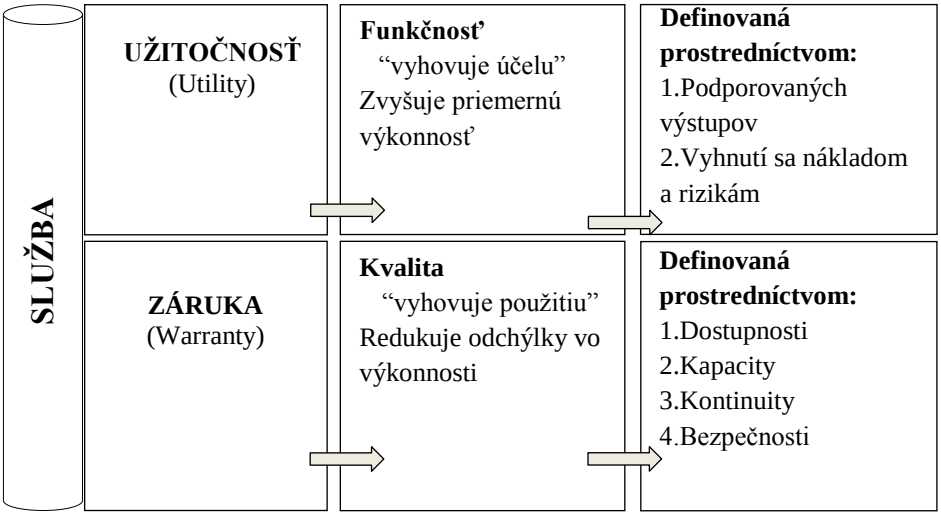
za svoju funkciu platení a na druhej strane je to v ich vlastnom záujme (napr. ak agentmi sú zamestnanci, alebo koncový používateľ). Publikácia popisuje plánovanie a stratégiu služieb – previazanie plánov biznisu a smerníc na stratégiu IT, portfólio služieb a katalóg služieb či rôzne stratégie sourcingu. Kategorizuje poskytovateľov služieb (interný, externý, zdieľaný). Sú tu definované rôzne alternatívy modelov dodávky služieb a modely služieb ako také. Kniha operuje s termínmi ako je zapúzdrenie (encapsulation), kde vlastne ide o modularitu služieb, slabé väzby (Loose coupling) – koncept využívaný v SOA a oddelenie záujmov (separation of concerns). Drvivá väčšina tém je úplne nová a nikdy nebola v ITIL V2 rozoberaná.

Pre efektívny chod služby je podstatné poznať jej podstatu a účel v pojmoch výsledku a/alebo odstránenia obmedzení businessu (to vyjadruje kocept užitočnosti) a nejakým spôsobom potvrdiť, že táto užitočnosť bude dodaná v definovanej kvalite (toto popisuje záruka). Nározný príklad ako môže byť pri službe definovaná jej užitočnosť a funkčnosť je možné vidieť v tabuľke Tab 2.

Hodnota služby je definovaná v pojmoch výstupov businessu, tak ako ich vníma zákazník, a popísaná pomocou dvoch základných charakteristík:

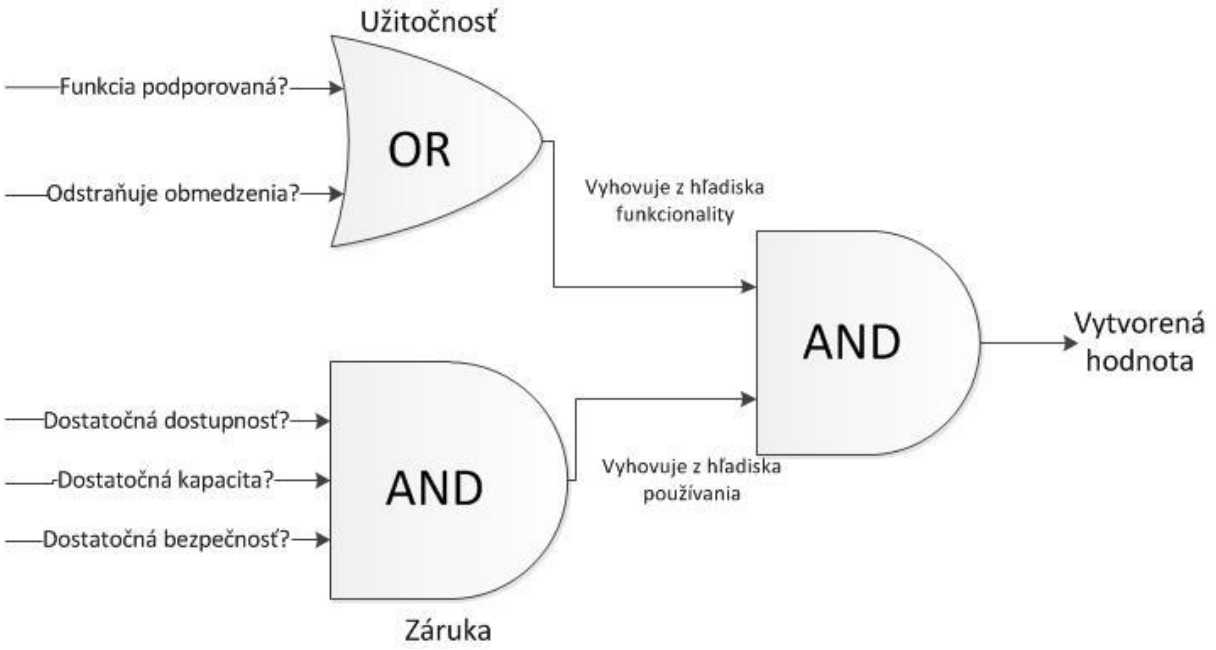
- *Užitočnosť služby* (service utility): je to to, čo zákazník dostáva v zmysle podporovaných výstupov a/alebo odstránených obmedzení. Niekedy sa tiež označuje ako funkčnosť.

- *Záruka služby* (service warranty): ako je služba dodávaná a jej vhodnosť pre použitie, vyjadrená v pojmoch dostupnosti, kapacity, kontinuity a bezpečnosti.



Tab. 2. Definícia hodnoty služby

Jednoducho povedané, užitočnosť určuje, čo zákazník dostane a záruka určuje, akým spôsobom to dostane. Detailné vysvetlenie je uvedené na v obrázku 5 tejto kapitoly. Hodnota služby mimo iného závisí aj na vlastných aktívach zákazníka, pretože bez týchto aktív nie je možné v niektorých prípadoch hodnotu vytvárať. Vytváranie hodnoty môže v praxi znamenať využitie ITIL pre transformáciu schopností správy služieb do strategických aktív, využitie Správy služieb pre vytvorenie základne pre kľúčové kompetencie, typický výkon a trvalé výhody pre nárast potenciálu poskytovateľa služieb. Deje sa tak prostredníctvom: schopností: schopnosť poskytovateľa (vyjadrenia pojmov správa, organizácie, procesov, znalostí a personálu) koordinovať, kontrolovať a implementovať zdroje zdrojov: priame vstupy pre produkciu služieb, napr. vstupy finančné, kapitálové, infraštruktúrne, aplikácie, informácie a personál.



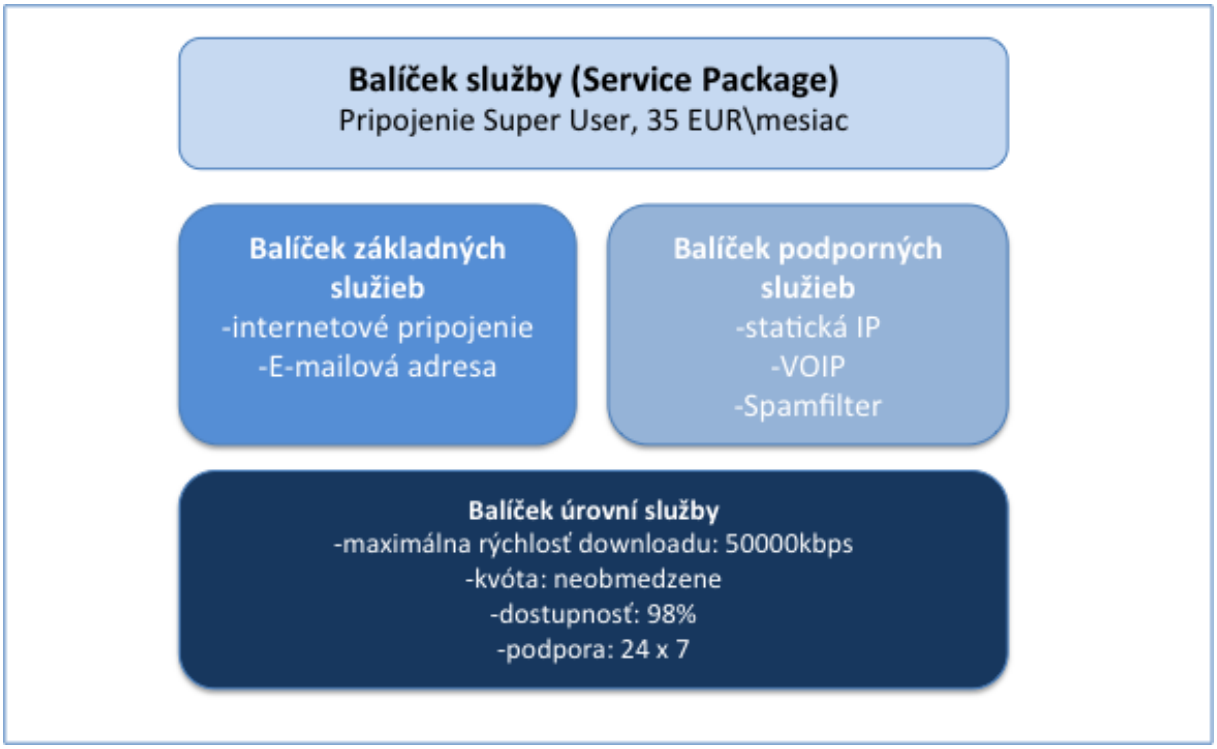
Obr. 5. Vytváranie hodnoty služby

Balíčky

Balíčky (z angl. packages) predstavujú návrhové dokumenty, ktoré špecifikujú navrhované služby a ich požiadavky naprieč celým životným cyklom služby. Balíček úrovní služieb (Service Level Package, SLP) je definovaný ako úroveň (miera) užitočnosti a záruky pre určitú službu (balíček služieb). Každý SLP sa definuje tak, aby zodpovedal určitej vzorke obchodných aktivít. SLP je vždy prepojený s tzv. balíčkom základných služieb. Balíček základných služieb (Core Service Package, CSP) je balík služieb poskytujúci platformu užitočnosti a záruky pre 2 a viac SLP. Kombinácia CSP a SLP sa používa k pokrytiu špecifických zákazníckych segmentov. Balíček pdporných služieb (Supporting Service Package) zahŕňa služby, ktoré umožňuje resp. vylepšuje balíček CSP. Celkový Balíček služby (Service Package) je detailný popis konkrétnej IT služby, ktorá je dostupná zákazníkovi. Zahŕňa v sebe SLP, jeden alebo viac CSP a podporných balíčkov.

Pre lepšiu názornosť si ilustrujeme ako takéto balíčky môžu vyzerať v praxi. V danom prípade pôjde ukážkovú službu poskytovateľa internetového pripojenia. Ako je uvedené vyššie, Balíček služby poskytuje detailný popis služieb poskytovaných zákazníkom a pozostáva z CSP, SLP a Podporných služieb. SLP špecifikuje mieru

užitočnosti a záruky. Teda jasne stanovuje kritéria dostupnosti, kapacity, bezpečnosti, prípadne dostupnej podpory. CSP obsahuje základné služby, tzn. Také, ktoré môžu byť využité pri budovaní viacerých služieb daného poskytovateľa. Balík podporných služieb definuje služby, ktoré pridávajú funkcionalitu a rozširujú Balík základných služieb o špecifické vlastnosti. Ak by sme teda použili príklad služby internetového pripojenia, mohli by jednotlivé balíky vyzerať pre takúto službu takto.



Obr. 6. Príklad balíčkov pre konkrétnu službu

Konkurencia a priestor na trhu

- každý poskytovateľ služieb je predmetom konkurenčných síl

- všetci poskytovatelia služieb a zákazníci operujú v jednom alebo vo viacerých vnútorných/externých trhoch. Poskytovateľ služieb sa viac ako jeho konkurenti musí snažiť dosiahnuť lepšieho porozumenia dynamiky tržného priestoru, jeho zákazníkov a kombinácii kritických faktorov úspechu, ktoré sú pre tento trhový priestor unikátne.

Modely poskytovateľov služieb

Z hľadiska stanovenia typu poskytovateľa služieb, ITIL v tejto časti stanovuje tri rôzne modely poskytovateľov na základe toho ako a komu svoje služby poskytujú.

- Interný poskytovateľ služieb existuje v rámci jednej organizácie a poskytuje služby výhradne pre jednu organizačnú jednotku.

- Zdieľaný poskytovateľ služieb existuje v rámci jednej organizácie, avšak posktytuje služby pre viac ako jednu obchodnú jednotku.

- Externý poskytovateľ služieb existuje mimo organizácie.

Modely poskytovania služieb

Pri modeloch poskytovania služieb sa jedná o kategorizáciu a analýzu rôznych modelov, ktoré si zákazníci môžu vybrať a ktoré môžu použiť poskytovatelia služieb za účelom zaistenia zdrojov a dodávky služieb, rovnako ako pre finančný manažment pri zhodnotení dopadov rôznych variánt sourcingu on–shore, off–shore alebo near–shore. Vo všeobecnosti ale definuje dva rôzne typy poskytovaných služieb.

Spravovaná služba (managed service): používa sa tam, kde podniková jednotka požadujúca službu úplne financuje poskytovanie tejto služby pre sebe.

Zdieľaná služba (shared service): zaisťovanie viacerých služieb pre jednu alebo viac podnikových jednotiek prostredníctvom zdieľanej infraštruktúry a zdrojov Utilita: služby sú poskytované na základe toho, koľko každý zákazník požaduje, ako často a kedy ich zákazník potrebuje.

Outsourcing služieb, štruktúra alokácie zdrojov (sourcing)

V časti Stratégie služby sa ITIL venuje aj alokácii zdrojov. Tá súvisí so spôsobom poskytovania služieb a modelmi ako sú služby poskytované a modelmi poskytovateľov. Outsourcing je kombináciou slov *out* a *source* (vonkajší, externý; zdroj). Outsourcing ako taký je pojem, ktorý v ekonómii označuje odovzdanie vnútropodnikových aktivít na externý subjekt. V oblasti IT sa outsourcing aplikuje

načastejšie na prevádzku IT infraštruktúry. Outsourcing IT služieb dáva firmám možnosť sa plne sústrediť na samotné podnikanie a zároveň im zabezpečuje dostupnosť a podporu tímu vysoko kvalifikovaných odborníkov, ktorí preberú zodpovednosť za prevádzku ich služieb. V tejto podkapitole uvedieme niekoľko najčastejšie používaných foriem alokácie zdrojov.

Interný (typ I) - Provízia a dodávka internými zamestnancami, nezahŕňa štandardizáciu služieb naprieč obchodnými/podnikovými útvarmi. Poskytuje najväčší stupeň kontroly, ale je limitovaný v možnostiach škálovania.

Zdieľané služby (typ II) - Interný podnikový útvar. Typicky funguje na princípe profitu a strát a má stanovený mechanizmus platieb za služby (ak nie, patrí do predchádzajúceho typu). Nižšie náklady ako Typ I s podobným stupňom kontroly, zlepšená štandardizácia,, ale obmedzená v možnostiach škálovania.

Plný outsourcing služby - Jeden kontrakt s jedným poskytovateľom služby. Spravidla zahŕňa prevod časti majetku. Zlepšuje škálovanie, ale obmedzenie existuje v zmysle najlepších služieb. Riziko dodávky je vyššie ako u primárneho kontraktora, konzorcia alebo selektívneho outsourcingu, pretože sa prepnúť na iného poskytovateľa je veľmi náročné.

Prime - Jeden kontrakt s jedným poskytovateľom služby, ktorý riadi dodávky, ale angažuje do toho viacero poskytovateľov. Kontrakt je postavený tak, že primárny kontraktor sa bude snažiť využiť tých najlepších dodávateľov. Schopnosti a riziká sa zlepšujú na rozdiel od situácie s jedným dodávateľom, ale zvyšuje sa komplexnosť.

Konzorcium - Množina poskytovateľov služieb je explicitne vybraná odberateľom služby. Všetci poskytovatelia sú povinní poskytnúť jednotné rozhranie pre správu. Spĺňa požiadavky, ktoré nie je možné splniť s jedným dodávateľom. Poskytuje tie najlepšie schopnosti s lepšou kontrolou ako v predchádzajúcom prípade. Zvyšujú sa ale riziká a to tým, že nútime poskytovateľov spolupracovať s konkurenciou.

Selektívny outsourcing - Množina poskytovateľov služieb je explicitne vybraná a riadená odberateľom služby. Toto predstavuje najzložitejšiu štruktúru pre riadenia, pretože príjemca služby funguje ako integrátor služieb a je zodpovedný za medzery a riešenie potenciálnych konfliktov medzi poskytovateľmi služieb. Termín „co-sourcing“ sa viaže k špeciálnemu prípadu selektívneho outsourcingu. V tejto variante príjemca služby udržiava interné, alebo zdieľané štruktúry služieb a kombinuje ich s externými poskytovateľmi. Príjemca služby je integrátor služieb.

Návratnosť investícií

ROI je koncept resp. ukazovateľ vyjadrujúci hodnotu investície, či jej úspešnosti. Môže sa tiež využiť ako vyjadrenie výkonnosti nejakej podnikateľskej aktivity, projektu či činností spojených s konkrétnymi investíciami. Jeho použitie a význam však nie je vždy úplne presný, resp. jeho vnímanie rôznymi stranami nie je vždy rovnaké. V terminológii napr. finančných riaditeľov sa spravidla jedná o ROIC (Return On Invested Capital), meraní výkonnosti businessu. V oblasti správy služieb sa ROI spravidla používa k meraniu schopnosti používať aktíva pre generovanie pridanej hodnoty. V najjednoduchšom prípade to znamená čistý zisk delený čistým majetkom spoločnosti. Výsledné percento sa aplikuje buďto na celkový príjem, alebo eliminációui s tým spojených nákladov.

ITIL V3 nepredpokladá, že sa organizácie budú snažiť aplikovať ROI pri rozhodovanie o prijatie správy služieb (realita nás však niekedy presvedčuje o opaku). ROI je metóda, pretože je jednoducho vysvetliteľná a vyčísliteľná. Meranie buď spĺňa, alebo nespĺňa stanovené numerické kritériá. Výzvou je to však vtedy, pokiaľ sa zameriavate s vyčíslením ROI na krátkodobý horizont. Uplatnenie správy služieb má odlišné stupne ROI, v závislosti na obchodnom dopade, realizovanej výslednej hodnote, stratégii služieb v spoločnosti a celej rade ďalších faktorov, ktoré nemusia logicky implikovať priamy finančný efekt. Naviac sú s tým veľmi často spojené rôzne problémy pri implementácii. ITIL SS operuje s dvoma klasickými metódami vyčíslenia návratnosti investícií – Net Present Value/NPV a Internal rate of Return/IRR. Častějšou a doporučenou metódou je NPV.

Rozvoj organizácie

ITIL sa tu koncentruje na potrebu vykonávania organizačných zmien. Tá však nie je nikdy okamžitá a nenastane tak, že ju manažment formálne vyhlási. Neexistuje tu univerzálne platná metóda, rozsah a štruktúra sú naplno závislé na podnikovej stratégii. Zatiaľ čo je pomerne jednoduché spravovať nejakú organizáciu pomocou funkcií, kde líniová štruktúra odpovedá adekvátnym kompetenciám a zodpovednosť. Ak však pre nejakú elementárnu funkciu (typickým príkladom môže byť Incident Management) potrebujeme podporu naprieč organizačnou štruktúrou, naprieč niekoľkými oddeleniami je koncept správy pomocí líniového riadenia a priradených funkcií už ďalej neudržateľný. ITIL V3 SS v tomto kontexte uvažuje použitie funkcií, produktov (organizácia je orientovaná podľa nejakých produktových radov – spravidla v oblasti priemyslovej výroby), trhového priestoru, alebo zákazníkov (organizačná štruktúra zodpovedá štruktúre zákazníckej báze), geografii (napr. pobočky medzinárodných firiem a pod.).

Portfólio a katalóg služieb

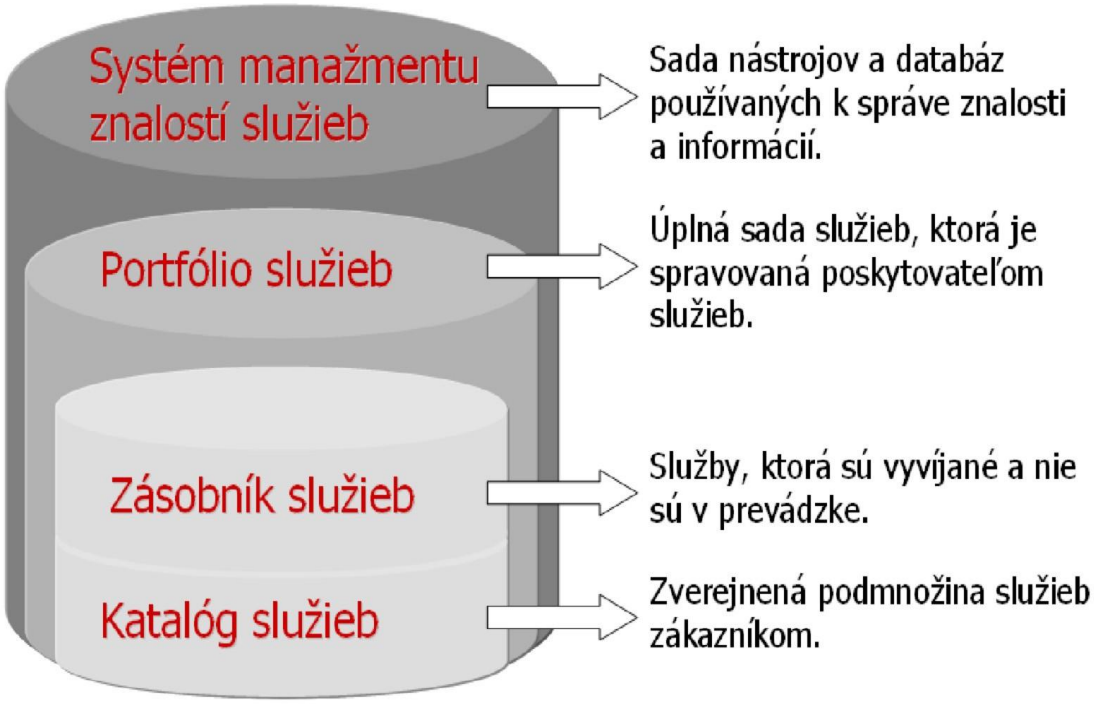
ITIL v časti Stratégia služby predstavuje aj dva koncepty, ktoré sa neskôr využívajú v ostatných fázach životného cyklu služby. Jedná sa o Katalóg a Portfólio služieb.

Portfólio služieb predstavuje množinu všetkých budúcich požiadavok na služby a katalóg služieb by mal obsahovať údaje o všetkých službách, poskytovaných v súčasnosti, alebo pripravovaných, súhrn ich vlastností, informácie o zákazníkoch a ich údržbe. Podstatný rozdiel je ten, že katalóg služieb predstavuje tú podmnožinu portfólia, ktorá je jediná viditeľná zákazníkom. Portfólio obsahuje všetky služby vo všetkých fázach vývoja a nasadenia, vrátane služieb, ktoré sú už vyradené, alebo služieb, ktoré sa ešte nedostali do prevádzky. Len čo je služba vyvíjaná pre použitie zákazníkmi a sú vytvorené špecifikácie pre službu, tak služba by mala byť pridaná do portfólia služieb.

Správne navrhnutý katalóg služieb môže organizácií priniesť množstvo hmotných a nehmotných prínosov. Katalóg služieb slúži ako zdroj informácií pre zákazníka, aby mal prehľad, ktoré služby sú k dispozícii a ako ich získať a používať. Pri tvorbe

katalógu služieb sa berie do úvahy pohľad zákazníka a to prispieva k jeho spokojnosti. Očakávania zákazníkov sa stavajú realistickejšími, férovými, predvídateľnými a služby, ktoré im boli dodané sa dajú vyčísliť.

Cieľom teda je maximalizovať úžitkovú hodnotu katalógu služieb vzhľadom na to, ake služby sa v ňom nachádzajú. Toto je už ale úlohou procesu Správy portfólia služieb, ktorý je popísaný nižšie.



Obr. 7. Zjednodušená schéma vzťahov medzi Portfóliom a Katalógom služieb

Pre organizáciu je dôležite definovať čo je to vlastne služba. Dobrým spôsobom je získať túto informáciu priamo od zákazníka, ktorý je užívateľom služby a vie aké výstupy chce od tejto služby dosiahnuť.

Katalóg služieb podľa [6] ma dva aspekty:

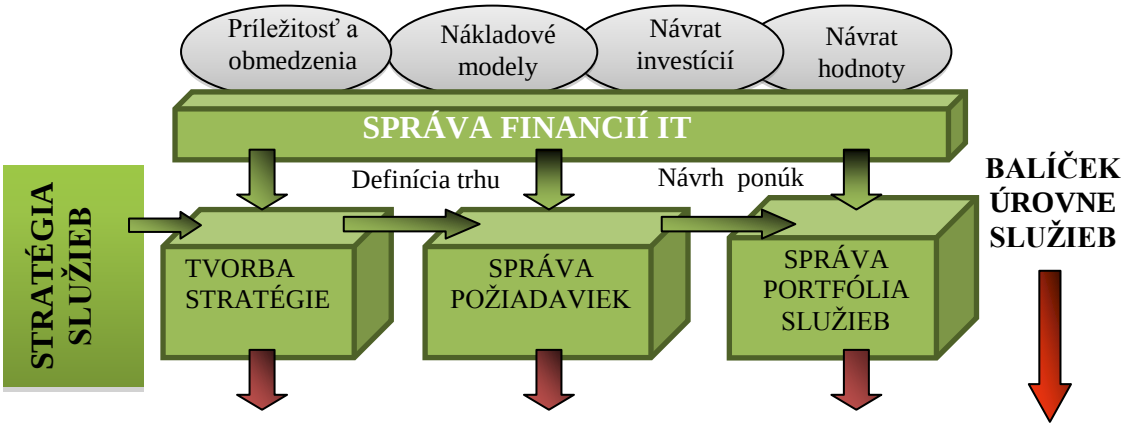
Katalóg biznis služieb: obsahuje údaje o všetkých IT službách dodávaných zákazníkovi spolu s vzťahmi s obchodnými jednotkami a procesmi, ktoré sa spoliehajú na IT služby. Je to pohľad zákazníka na katalóg služieb.

Katalóg technických služieb: obsahuje údaje o všetkých IT službách dodávaných zákazníkovi spolu s vzťahmi podpory služieb, zdieľania služieb a komponentov nutných pre podporu služieb podniku. Mal by podporovať Katalóg biznis služieb.

Hlavným rizikom spojeným s katalógom služieb je nepresnosť údajov v katalógu a podcenená kontrola dát. Rizikom pre spoločnosť býva aj slabé prijatie vytvoreného katalógu služieb a jeho využitie vo všetkých prevádzkových procesov.

Procesy Stratégie služby

Príklad možného generického workflow. Detaily – viz obr. 8.



Obr. 8. Zjednodušený workflow procesov stratégie služby.

Celý proces je započatý definovaním požiadaviek businessu (proces Správy požiadavok). Nasleduje aktivita, ktorá reprezentuje špecifikáciu zákazníkov a ich potrieb, konkurencie, rizika a spôsobu, ako vytvoriť balíčky služieb a balíčky úrovní služieb atď. Tieto kroky sú v diagrame reprezentované aktivitami Definícia trhu a Definícia štruktúry služieb (proces Tvorba stratégie). Tok ďalej pokračuje vývojom modelu nákladov (proces Finančný manažment), čo zahŕňa návrh obchodného prípadu, výpočet možnej návratnosti investícií a predbežné schválenie zámeru. Ďalším krokom je Vývoj portfólia služby (proces SPM), ktorý zahŕňa naplánovanie služby, plánovanie zdrojov a Vývoj strategických aktív služby. Poslednou aktivitou je potom Ustanovenie služby, čo zvyčajne znamená finálne schválenie služby. V tomto kontexte je potrebné zdôrazniť, že služba v tomto momente ešte neexistuje, existuje jej návrh je popísaný až v procesoch, ktoré popisuje publikácia Návrh služby. Celkový diagram je zachytáva postupný prechod bez iterácií, no v skutočných prípadoch tu takéto vzťahy existujú.

Publikácia obsahuje aj niekoľko procesov, ktoré sa naprieč textom spomínajú, no nie sú explicitne definované. Jedná sa o tieto procesy:

- Vytváranie stratégie (Strategy generation)
- Správa financií (Financial Management)
- Správa požiadaviek (Demand Management)
- Správa portfólia služieb (Service Portfolio Management – SPM)

Správa financií IT (IT Financial Management)

Cieľom tohto procesu je poskytovať obchodným útvarom a IT finančné vyjadrenie hodnoty poskytovaných služieb, hodnoty aktív, ktoré podporujú poskytovanie týchto služieb a základnú kvalifikáciu pre prevádzkové plánovanie (prognózy). Správa financií zahŕňa funkcie a procesy, ktoré u poskytovateľa služieb IT zodpovedajú za správu rozpočtu, účtovanie a spoplatňovanie. Interní poskytovatelia služieb (nielen IT) sú stále viac a viac vystavovaní požiadavkám fungovať z hľadiska finančnej transparentnosti ako všetky ostatné obchodné útvary. Zodpovednosti a činnosti Správy financií IT neexistujú výlučne v doméne financií a účtovanie IT. Na tvorbe a využívaní finančných informácií IT spolupracujú mnohé časti organizácie. Zbierajú, zdieľajú a udržujú finančné dáta, ktoré potrebujú, a pritom umožňujú šírenie informácií ako podkladov pre kritické rozhodnutia a činnosti. Proces zahŕňa vyčíslenie hodnoty služieb a ich komponentov vo finančnom vyjadrení. Zahŕňa to stanovenie nákladov rôznych typov, priradenie týchto nákladov k službám, klasifikáciu týchto nákladov (kapitálové vs. prevádzkové, fixné vs. variabilné, priame vs. nepriame atď.). Zahŕňa aj dynamiku variabilných nákladov, čo v praxi môže znamenať porozumenie faktorom, ktoré môžu ovplyvniť služby z hľadiska nákladov, ako sú tieto faktory citlivé na odchýlky. Závisí to na veciach ako je počet používateľov, počtu SW licencií, náklady na prevádzku dátových centier, mechanizmu dodávky služby, počtu a typu zdrojov a inkrementálnych nákladoch pri zvýšení týchto hodnôt.

Správa požiadavok (Demand Management)

Správa požiadaviek je kritickým aspektom ITSM. Nedostatočne či neadekvátne špecifikované požiadavky so sebou nesú riziko, že požiadavka nebude riadne uspokojená.

Cieľom Správy požiadaviek je porozumieť zákazníkovým požiadavkám na služby a ovplyvňovať ich a zabezpečovať kapacitu pre naplnenie týchto požiadaviek. Na strategickej úrovni to môže zahŕňať analýzu charakteru obchodnej činnosti a užívateľských profilov. Na taktickej úrovni to môže zahŕňať využitie napríklad

diferencovaného spoplatnenia pre motiváciu zákazníkov k využitiu služieb v menej exponovaných časoch.

Správa portfólia služieb (Service Portfolio Management – SPM)

SPM proaktívne riadi investície v priebehu životného cyklu služby aj vrátane tých služieb, ktoré sú vo fáze koncepcie, návrhu a prechodu, rovnako ako tých živých, definovaných v rôznych katalógoch a aj služieb vyradených.

Portfólio služieb reprezentuje všetky zdroje, ktoré sú nejako použité alebo uvoľnené v rozličných fázach životného cyklu služieb. Každá fáza vyžaduje nejaké zdroje pre dokončenie projektov, iniciatív a kontraktov. Toto je veľmi dôležitý aspekt v oblasti e-governance. Každý vstup, plnenie a ukončenie sú schválené s patričným financovaním a finančným plánom rovnako, ako s tým spojené náklady uhradiť, resp. priniesť zisk. Portfólio služieb by mala byť primeraná kombinácia služieb vo vývoji pre rôzne typy trhov (zákazníkov) a katalógu (katalógov) služieb, ktorý reprezentuje finančnú "životaschopnosť" poskytovateľa služieb. Katalóg služieb je podmnožinou portfólia služieb a je to jediná časť portfólia, ktorá je viditeľná pre zákazníka a časť, ktorá buď len zabezpečuje úhradu vynaložených nákladov, alebo generuje zisk. Služby obsiahnuté v katalógu služieb je možné nastavovať podľa konkrétnych potrieb zákazníkov. Katalóg je tiež dôležitým ukazovateľom poskytovateľa služieb navonok, pretože reprezentuje schopnosti tohto poskytovateľa ponúkať služby. SPM je kontinuálnym procesom, ktorý obsahuje:

- Definovanie: katalógových služieb, zaistenie obchodných prípadov a potvrdenie dát v portfóliu
- Analýzu: maximalizácie hodnoty portfólia, zladenie, prioritizáciu a vyváženie dodávky a dopytu
- Schválenie: dokončenie navrhnutého portfólia, potvrdenie služieb a zdrojov
- Ustanovenie: komunikácie rozhodnutí, priradenie zdrojov a dohodnutých služieb.

Role stratégie služby

Publikácie Stratégia služby definuje niektoré špecifické úlohy a zodpovednosti spojené s realizáciou úspešnej stratégie, a to:

Manažér vzťahov s biznisom (Business Relationship Manager - BRM): Manažéri BRM (niekedy sa používa aj termín Account manager) vytvárajú silný vzťah so zákazníkom tým, že sa orientujú v biznise zákazníka a jeho výstupom. V záujme zákazníkov tesne spolupracujú s produktovými manažérmi.

Produktový manažér (Product Manager - PM): Produktoví manažéri preberajú zodpovednosť za rozvoj a správu služieb počas ich životného cyklu a majú zodpovednosť za produkčné kapacity, plánované služby (service pipeline) a tie služby, riešenia a balíky, ktoré sú prezentované v katalógoch.

Hlavný špecialista pre zdroje (Chief Sourcing Officer - CSO): CSO je špecialistom pre stratégiu zdrojov v organizácii, je zodpovedný za vedenie a nasmerovanie útvaru zdrojov a rozvoj stratégie zdrojov.

Návrh služby

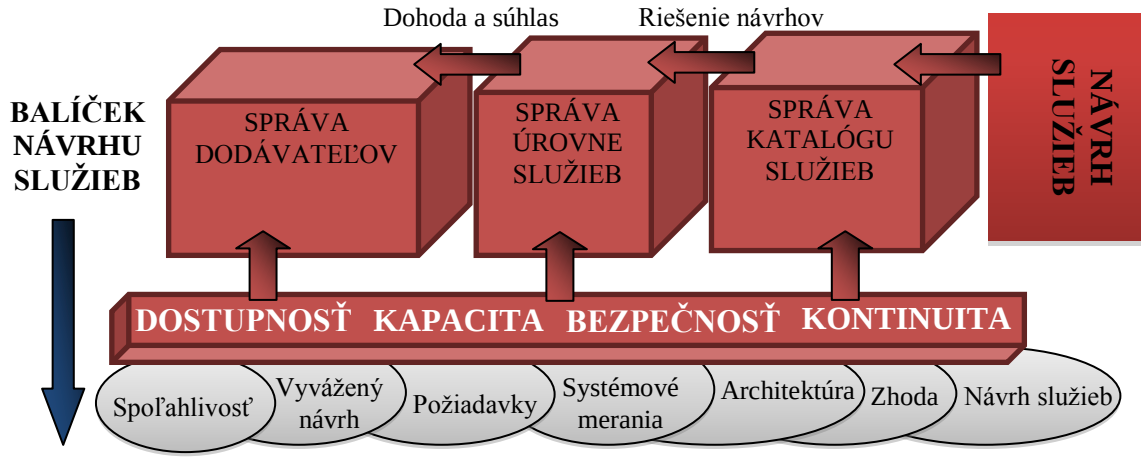
Úvod

Táto kapitola je primárne zameraná na vysvetlenie a popis základných konceptov a myšlienok, ktoré sú spôaté s návrhom služby. Zameriava sa na návrh služieb, ktoré podporujú hlavnú podnikovú stratégiu organizácie. Návrh služby popisuje, akým spôsobom sú implementované výstupy zo Stratégie služby pochopením zdrojov a schopností organizácie pre dodávku služby a následným zabezpečením IT zdrojov, ktoré budú tieto služby zabezpečovať. IT služby by mali byť navrhované tak, aby v nasledujúcej fáze (Prechod služby) bol zabezpečený hladký prechod do „živého“ prostredia a aby vyhovovali dohodnutým výstupom a podporovali životný cyklus služieb. Medzi hlavné princípy fázy Návrhu služieb teda patrí sledovanie postupov a metód, ktorými sa strategické a podnikové ciele orgnizácie transformujú na portfólio služieb a aktíva služieb a návody, ako vytvoriť kapacity pre manažment služieb v orgnizácii. Okrem iného publikácia popisuje ako transformovať súčasné a budúce obchodné požiadavky, návrh a vývoj služieb procesov IT, poskytuje návody na tvorbu a údržbu stratégii, architektúry IT a dokumentuje návrh inovatívnych riešení služieb a procesov IT.

Účel

Stratégia služieb akéhokoľvek poskytovateľa služieb by mala byť založená na zásadnom princípe - zákazník nekupuje produkty, ale uspokojenie svojich potrieb.
Návrh služby poukazuje na to, ako sa výstup z fázy Stratégie služieb pretransformuje na novú službu. Zameriava sa na zmeny a rôzne zlepšenia, ktoré smerujú k zvýšeniu pridanej hodnoty pre zákazníka v priebehu životného cyklu služby. Návrh služieb obsahuje princípy a metódy pre prevod strategických cieľov do portfólia služieb.
Cieľom tejto fázy životného cyklu je návrh novej alebo zmena existujúcej služby. Aplikuje sa holistický prístup pre všetky aspekty návrhu služby, aby sa zabezpečila konzistencia a integrácia s ostatnými aktivitami a procesmi. t.j. nie v izolácii, ale s ohľadom na iné služby, systémy riadenia a nástroje (napr. portfólio služieb, katalóg služieb), architektúry, technológie. Nie každá zmena vyžaduje úplný postup podľa

aktivít Návrhu služieb, týka sa to iba podstatných zmien. Ktoré to sú, to by mala definovať organizácia (viď Manažment zmien, v časti Prechod služby)



Obr. 9. Zjednodušený workflow procesov návrhu služby.

Kroky pri návrhu služieb vychádzajú zo strany biznisu. Ten generuje nové požiadavky, resp. sa tieto priebežne menia. Na návrh novej, resp. zmenenej služby môžeme pozerať z viacerých aspektov:

- Na novú resp. menenú službu samu o sebe
- Na systémy a nástroje pre manažment služieb, najmä Portfólio služieb: konzistencia s inými službami (rozhrania, závislosti, podpora)
- Na technológie, architektúry a systémy riadenia: konzistencia s technickými prostriedkami (dostatočnosť technického a riadiaceho vybavenia)
- Na procesy a zabezpečenie, že sú k dispozícii všetky prostriedky (procesy, roly, zodpovednosti, skúsenosti, či znalosti)
- Metódy merania a metriky: overenie, či je možné úspešne merať novú službu vzhľadom na požiadavku biznisu (zabezpečiť súlad so SLA, kvalita “v jazyku” biznisu, mapovanie biznis procesov na IT infraštruktúru a na metriky, priebežné monitorovanie výkonnosti)

Novo navrhnutá alebo zmenená služba potom prechádza do časti fázy Prechod služby na vyhodnotenie, testovanie a jej nasadenie.

Princípy návrhu služby

Návrh služby spočíva v návrhu vhodných a inovatívnych IT služieb, ich architektúry, procesov, vykonávacej politiky a dokumentácie tak, aby sa naplnili požiadavky biznisu. Kroky by sa dali zhrnúť do týchto bodov**:**

- pridanie do Portfólia služieb (už v čase návrhu)
- špecifikácia resp. porozumenie SLR (Service Level Requirements)
- manažment kapacít vzhľadom na súčasnú IT infraštruktúru
- finančný manažment (pri nárokoch na doplnenie infraštruktúry)
- analýza vplyvu na biznis a rizík (Business Impact Analysis, Risk Analysis)
- príprava Service Desku a školenie ľudí
- príprava implementácie (Prechod služby)
- manažment dodávateľov.

Hlavné ciele a faktory pri návrhu služby sú:

- Súlad s cieľmi biznisu na základe definovaných požiadaviek na kvalitu, zhodu (compliance), riziká a bezpečnosť
- Jednoduchosť a efektivita vývoja, t.j. nie dlhotrvajúce náklady na dodávku, vývoj či poskytovanie služby
- Efektívne procesy pre návrh, prechod, prevádzku a vylepšenia služby
- Identifikácia a manažment rizík tak, aby riziká boli odstránené resp. eliminované pred spustením služby
- Zabezpečená bezpečná a flexibilná IT infraštruktúra, prostredie, aplikácie, dátové a informačné zdroje, a to v súlade so súčasnými aj budúcimi požiadavkami biznisu
- Definované metódy merania a metriky na určenie efektívnosti procesov
- Zabezpečená kvalita IT riešení pomocou plánov, politík, procesov, architektúr, rámcov a dokumentácie (v súlade s biznisom); štandardizácia riešení
- Rozvoj schopností a zručností v IT presunom aktivít stratégie a návrhu do operačných úloh
- Zlepšenie celkovej kvality IT služieb, redukcia požiadaviek na zmeny, prepracovanie a doplnenie.

Pri identifikácia požiadaviek na službu roznávame tieto dva druhy požiadaviek:

Požiadavky kvality:

- *Škálovateľnosť* vzhľadom na budúce biznis ciele
- *Biznis procesy* ktoré sú podporované službou
- Súlad biznis požiadaviek so službou, t.j. ako ich služba spĺňa
- *Služba samotná*, jej SLR (Service Level Requiement) alebo SLA (Service Level Agreement)
- Technologické komponenty pre nasadenie služby
- *Vnútorné služby / komponenty* a ich OLA (Operational Level Agreement)
- Externé služby / komponenty a ich kontrakty
- *Metrika výkonnosti*, ktorá je požadovaná pre službu
- *Úroveň bezpečnosti*, požadovaná biznisom alebo legislatívou

Technologické oblasti ovplyvňujúce požiadavky na službu sú:

- Infraštruktúra: servre, sieťové vybavenie, DB systémy, úložiská
- Prostredie: miestnosti, priestory, el. zdroje, kabeláž, fyz. bezpečnosť
- Údaje: manažment informácií a údajov, vrátane napr. testovacích dát
- Aplikácie: manažment aplikačného softvéru (kúpeného, aj in-house)

Pri návrhu služby nie je kladený dôraz na požiadavky funkcionality, ale rovnako na všetky aspekty. Cieľom je dodržať jednoduchosť návrhu a nešpecifikovať príliš zložité a teoretické návrhy. Aktivity pri samotnom návrhu služby by sa dali sumarizovať do týchto bodov:

- Zbieranie požiadaviek, ich analýza a dokumentovanie,
- Návrh služieb, technológií, procesov, informačných zdrojov a tokov,
- Prehodnotenie procesov a dokumentov návrhu,
- Spojenie s ďalšími aktivitami / rolami plánovania a návrhu,
- Tvorba a správa IT politík, návrh dokumentov,
- Revízia všetkých dokumentov, plán nasadenia,
- Zohľadnenie a manažment rizík,
- Zabezpečenie súladu so stratégiami IT a organizácie (Service Strategy)

Vstupy do týchto aktivít predstavujú výstupy z fázy Stratégie služby. Jedná sa o vízie, stratégie a biznis ciele organizácie, rôzne ohraničenia stanovené napr. štandardmi alebo legislatívou a IT stratégie a dokumenty zo Stratégie služieb:

- Všetky IT stratégie, politiky, strategické plány
- Detailné požiadavky biznisu
- Ohraničenia: finančný rozpočet, finančné plány
- Portfólio služieb
- Plány prechodu služieb: manažment zmeny, konfigurácie, nasadenia,
- Procesy manažmentu IT a služieb, riziká
- Plány bezpečnosti, politiky a príručky
- IT biznis plány a plány, politiky IT kvality
- Plány manažmentu služieb:
- plány manažmentu úrovne služieb (SLM), SLA, SLR
- plány zlepšovania služieb (SIP)
- plány kapacít, dostupnosti, kontinuity IT služieb
- Nástroje a techniky merania (metriky, kritériá kvality)

Plán na návrh novej služby vychádza vždy z požiadavok biznisu, nie IT. Plán sa tvorí vzhľadom na uvedených 5 aspektov návrhu služby a zahŕňa:

- Prístup (approach) k návrhu a časové hľadisko (timescales),
- Organizačné, komerčné, technické dopady zavedenia služby
- Komerčné overenie vhodnosti služby vzhľadom na existujúci biznis (z pohľadu IT aj procesov manažmentu služby, zahŕňa kapacitu aj výkonnosť)
- Vplyv a migráciu rizík, príslušné aktivity manažmentu služby
- Plánovanie komunikácie, aktérov - dotknuté strany
- Vplyv na kontrakty a dohody (existujúce, budúce)
- Očakávané výstupy z prevádzky služby, merateľne vyjadrené: SLA, úrovne služieb, spokojnosť zákazníkov
- Tvorbu Súboru dokumentov návrhu služby (SDP, Service Design Package)
- Tvorbu Akceptačných kritérií služby (SAC, Service Acceptance Criteria)

Podporné systémy – Portfólio služieb

Už v predchádzajúcej časti sme sa stretli s pojmami Katalóg a Portfólio služieb. Popísali sme si ich ako jedny z najdôležitejších systémov manažmentu. Svoju rolu zohráva Portfólio aj vo fáze pri návrhu služieb, kde podporuje všetky procesy návrhu a vytára platformu pre popis služieb podľa ich hodnoty pre zákazníka. Týmto v podstate dáva odpoveď na otázku, prečo by zákazník mal kúpiť práve túto službu. Portfólio služieb je uplatňované pri riadení celého životného cyklu všetkých služieb a obsahuje:

Zásobník služieb (Service Pipeline) – zoznam pripravovaných služieb. Je to databáza štruktúrovaných dokumentov s prehľadom všetkých IT služieb, ktoré sú vo fáze vývoja a ešte nie sú zatiaľ dostupné pre zákazníkov. Tento zoznam poskytovaných služieb poskytuje podnikový pohľad na možné budúce IT služby;

Katalóg služieb (Service Catalogue) – databáza alebo štruktúrovaný dokument s informáciami o aktívnych IT službách, vrátane tých, ktoré sú vhodné pre nasadenie. Ako jediná časť Portfólia dostupná zákazníkom a je tak priamou podporou predaja a dodávky IT služieb. Štandardným obsahom by mali byť informácie o dodávkach, cenách, SLA, objednávaní či požiadavkách na procesy;

Vyradené služby (Retired Service) – databáza už vyradených služieb.

Neodmysliteľnou súčasťou každého Katalógu služieb má byť jasná definícia *SLA (Service Level Agreement)* a *OLA (Operational Level Agreement)* zmlúv, prípadne aj kontraktu, tzv. UC (Underpinning Contract), ktorá predstavuje zmluvu medzi poskytovateľom IT služby a treťou stranou (externým poskytovateľom) o doručení jednej alebo viacerých služieb.

Servisná (SLA) a Operačná úroveň služieb (OLA) predstavujú dohody, ktoré sú široko používané v odvetví informačných technológií. SLA je dohoda o úrovni poskytovaných služieb, ktorá je zameraná na servisnú časť, čiže na dobu prevádzkyschopnosti služieb a na ich výkon. Ide o písomnú zmluvu medzi poskytovateľom služieb a zákazníkom, ktorá môže byť právne záväzná, kedy ide o tzv. formálnu dohodu, alebo môže predstavovať len určitú právne neoverenú zmluvu medzi oboma stranami, tzv. neformálnu dohodu. Obe dohody, či už formálne, alebo neformálne, zabezpečujú udržiavanie a spravovanie všetkých počítačových komponentov a ich vybavenia. SLA spája poskytovateľov služieb so zákazníkmi a nachádza sa v servisnej zmluve, kde je táto úroveň služieb definovaná a odkazuje sa

na dohodnutú dodaciu lehotu služby, alebo jej výkonu. Servisná úroveň služieb spravidla obsahuje tri časti**:**

Strednú dobu medzi poruchami, ktorá predstavuje čas, za aký sa má systém súvisiaci so službou začať opravovať

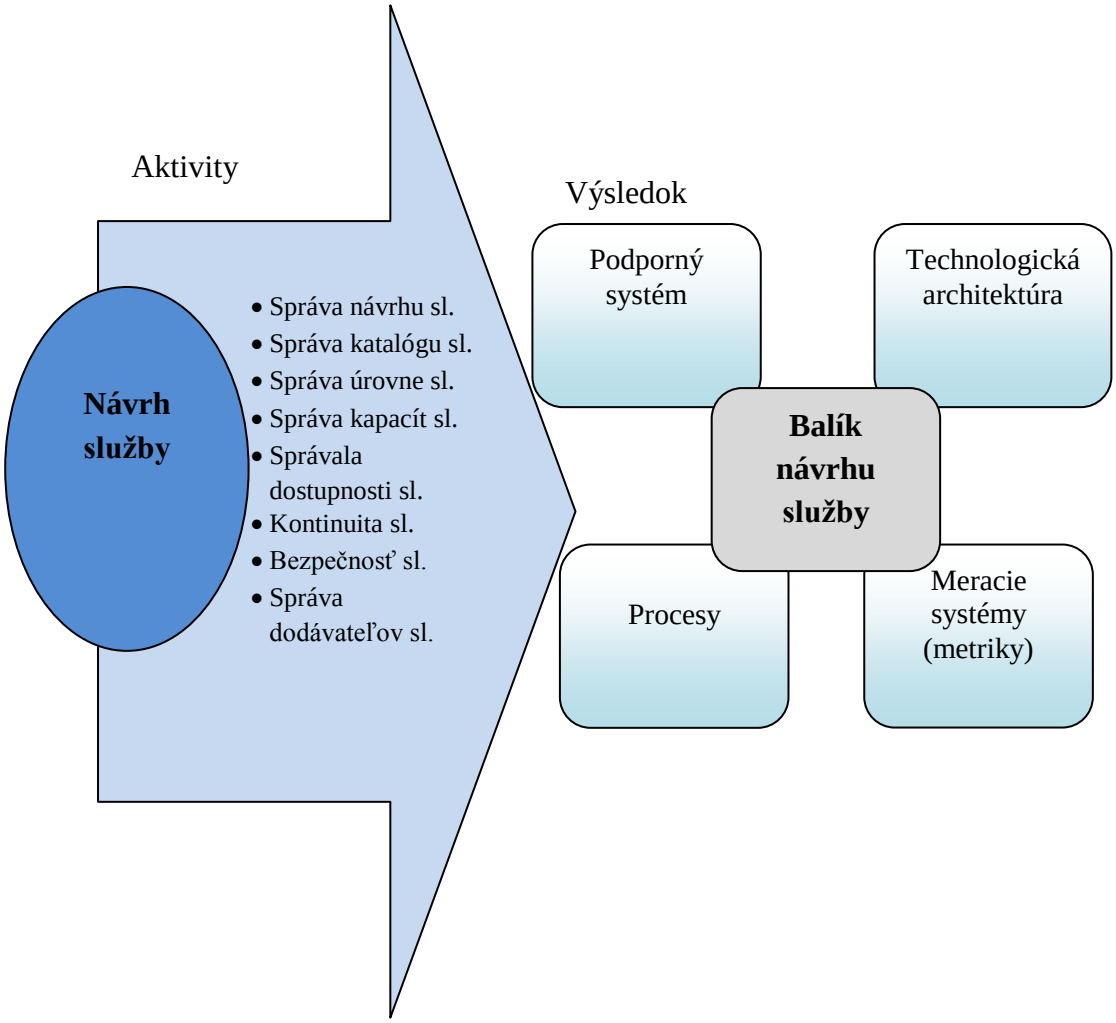
Stredná doba opravy, ktorá predstavuje dobu, za ako dlho dôjde v prípade výpadku k obnoveniu služby

Stredná dobu obnovy, ktorá vyjadruje čas, za aký sa dostaví prvé odstránenie poruchy

SLA popisuje priority služieb a je aplikovaná na celý proces riešenia požiadaviek. Definuje, kto je za služby zodpovedný, ich garanciu, záruku a určuje úroveň prístupnosti k službám, ich použiteľnosť a výkon.

Operačná úroveň služieb predstavuje dohodu o prevádzkovej úrovni a údržbe služieb, je špecifikovaná pre podpornú skupinu, ktorej je daná požiadavka pridelená. Ide o dohodu medzi internou podporou a inštitúciami, ktoré podporujú SLA, z čoho vyplýva, že je technicky orientovaná. Podľa dohody OLA každá vnútorná podporná skupina má povinnosti voči inej skupine. Zreteľne zobrazuje výkonnosť a vzťahy vnútorných skupín a jej hlavným cieľom je zabezpečenie, aby všetky podporné skupiny poskytovali určené SLA. Operačná úroveň služieb definuje vzájomné pomocné vzťahy medzi skupinami organizácie, ktoré pracujú na úrovni podpory SLA. Táto dohoda opisuje zodpovednosť každého člena zo skupiny, ku každému členovi inej skupiny, vrátane procesu a časového rámca pre poskytovanie svojich služieb [8] [9] [10].

Procesy návrhu služby



Obr. 10. Procesy návrhu služby.

Určitým spôsobom ako dokumentovať návrh služieb je Model služby (Service Model). Ten predstavuje grafickú reprezentáciu komponentov, ktoré službu tvoria. Zobrazuje nielen komponenty, ale i vzťahy a interakcie medzi nimi a tiež spôsob ako službu používa používateľ. Základ Modelu služby môže vzniknúť pri prvých diskusiách o tom, ako bude služba fungovať. Vytvára ho architekt, alebo obchodník na podporu dohody s ostatnými zamestnancami, ktorí sa budú podieľať na vývoji a prevádzkovaní služby [6].

ITIL neurčuje detailne ako má Model služby vyzerať, ale necháva priestor pre kreativitu tvorcov. Pri jeho tvorbe môžeme využívať metódy a nástroje systémového

inžinierstva, workflow diagramov alebo procesných máp. Sám o sebe service model nestačí na implementovanie služieb preto je doplnený detailnými informáciami ako sú funkčné a prevádzkové požiadavky, akceptačné kritéria a plány pre nasadenie služby do prevádzky. Všetky tieto dokumenty vytvorené vo fáze Návrh služby tvoria Balík návrhu služby (Service Design Package - SDP). Tento balík je posunutý do ďalšej fázy v rámci ITIL V3, do Prechodu služby.

Správa katalógu služieb

Správa katalógu služieb (Service Catalogue Management, SCM) zabezpečuje vytvorenie katalógu služieb, jeho aktuálnosť. Katalóg služieb je centrálnym zdrojom informácií o službách IT poskytovaným používateľom služieb a umožňuje získať presný a úplný obraz o dostupných službách IT a ich stavu business centrám.

Účelom SCM je poskytnúť jediný a konzistentný zdroj informácií o všetkých službách a tiež dohliada na to, aby boli dostupné všetky informácie všetkým, ktorí majú povolený prístup.

Hlavným vstupom tohoto procesu sú výstupy z úvodnej fázy životného cyklu (Stratégia služby), Portfólio služieb a tiež výstupy Manažmentu vzťahov s businessom (Business Relationship Management, BRM), alebo od procesu Manažmentu úrovne služieb (Service Level Management, SLM).

Manažment úrovní služieb

Manažment úrovní služieb (Service Level Management, SLM), je proces zabezpečujúci vytvorenie dohôd o úrovni služieb (SLA) a zabezpečenie ich dodržiavania. Hlavným cieľom tohoto procesu je definovať, zjednávať, monitorovať, vykazovať a mať pod kontrolou úrovne poskytovaných IT služieb, ktoré sú šité na mieru jednotlivým zákazníkom. Kvalita poskytovaných služieb sa pritom musí pohybovať na začiatku v stanovených hraniciach.

Zvláštny význam má vzájomná súvislosť medzi procesmi Plánovania služieb a Riadenia úrovne služieb. Vďaka podrobným špecifikáciám služieb dokáže proces riadenia úrovne služieb stanoviť merateľné a dosiahnuteľné ciele pre úrovne služieb poskytované potenciálnym zákazníkom. Vedenie oddelenia IT potom môže súhlasiť s dodávkou služieb podľa rozumných dohôd o úrovni služieb SLA (Service Level

Agreement). Plánovanie služieb a riadenie úrovne služieb závisí na výsledkoch vzájomného pôsobenia s ostatnými procesmi IT.

Manažment kapacít

Proces Manažmentu (Capacity management) slúži na zabezpečenie toho, aby kapacita IT služieb a IT infraštruktúry bola dostatočná vzhľadom na stanovené ciele (t.j. cenová efektivita, čas, atď.). Vďaka tomuto procesu môže oddelenie IT definovať, sledovať a riadiť kapacitu služieb. Tiež môže všetky služby zabezpečiť, aby ich prevádzkové zaťaženie odpovedalo požiadavkám výkonnosti, ktoré sú definované v zmluvách o úrovni poskytovaných služieb (SLA).

Kapacita systémov a sietí je kľúčový faktor celkovej kapacity služieb IT. Vzhľadom k tomu, že kapacita služieb ovplyvňuje vývoj nových služieb a tvorbu zmlúv prebieha tento proces spoločne s procesmi Plánovanie služieb a Manažment úrovne služieb (podobne ako Manažment dostupnosti).

Manažment dostupnosti

Proces Manažmentu dostupnosti (Availability management) zabezpečuje návrh, analýzu, plánovanie, meranie a zlepšovanie všetkých aspektov dostupnosti IT služieb. Rovnako zabezpečuje, že IT infraštruktúra, procesy, nástroje, roly atď. sú v zhode s dohodnutou cieľovou úrovňou.

Tento proces umožňuje oddeleniu IT definovať, sledovať a riadiť prístup zákazníka k jednotlivým službám. Je potrebné zdôrazniť, že zaistenie dostupnosti služieb koncovému používateľovi (tzv. end-to-end availability) sa nezaobíde bez zaistenia dostupnosti systému a siete.

V rámci správy dostupnosti sa pracovníci IT zaoberajú správou príspevku jednotlivých subdodávateľov k celej službe a ďalej kontrolujú a analyzujú plány služieb, ktoré sú výstupom procesu Plánovania služby. Vďaka tomu môžeme plány upravovať tak, aby odrážali požiadavky na dostupnosť služieb. Všimnite si, že Manažment úrovní služieb, čo je súčasťou procesu zaistenia dodávky služieb, musí zahrňovať také požiadavky na dostupnosť služieb zakotvené v zmluvách o úrovni poskytovaných služieb (SLA).

Manažment kontinuity IT služieb

Manažment kontinuity služieb zabezpečuje riadenie rizík, ktoré môžu mať vážny dopad na IT služby. Implementácia procesu zaručuje, že poskytovateľ IT služieb môže vždy poskytnúť minimálne dohodnuté úrovne služieb, a to redukovaním rizika na akceptovateľnú úroveň a plánovaním obnovy IT služieb.

Tento proces popisuje schopnosť oddelenia IT pokračovať v dodávaní definovaných služieb na dohodnutých úrovniach i v prípade, že dôjde k sérii výpadkov, alebo k nejakej havárii infraštruktúry IT. Aby bol tento proces úplne efektívny, mal by byť zahrnutý ako neoddeliteľná súčasť väčšieho podnikového procesu Manažmentu kontinuity biznisu (Business Continuity Management, BCM).

Manažment informačnej bezpečnosti

Proces manažmentu informačnej bezpečnosti (Information security management) zabezpečuje dôvernosť, integritu a dostupnosť aktív organizácie, informácií, dát a IT služieb. Vďaka tomuto procesu môže oddelenie IT definovať, sledovať a riadiť zabezpečenie firemných informácii a služieb. Tento proces zahrnuje implementáciu, riadenia a údržbu celej bezpečnostnej infraštruktúry. Všetky služby musia vyhovovať prísnym firemným štandardom na zabezpečenie informácii.

Manažment dodávateľov

Manažment dodávateľov (Supplier management) je proces, ktorý by mal zapezpečovať záruku, že všetky zmluvy s dodávateľmi podporujú potreby podniku a že všetci dodávatelia plnia zmluvné záväzky. Na takmer každej poskytovanej službe sa podieľajú aj externí dodávatelia, preto tento proces poskytuje návod na riadenie dodávateľov tak, aby všetky dodávky vychádzali potrebám firmy.

Ukazuje ako uzatvoriť zmluvy, ktoré budú dodávatelia rešpektovať a plniť svoje ciele a za dohodnutých podmienok a termínov. Zároveň nám poskytuje informácie o kontaktoch na dodávateľov a tiež iné informácie s nimi spojené.

Role Návrh služby

Každý proces, Návrhu služby, má vytvorené sebe prislúchajúce kľúčové úlohy a zodpovednosti:

- *Manažér návrhu služby* – jeho úlohou je zabezpečovať koordináciu a rozmiestňovanie kvalitných riešení a postupov, pre IT služby a procesyô
- *Architekt IT* – hlavnou zodpovednosťou je návrh potrebných a požadovaných technológií, architektúry, stratégií a plánov;
- *Manažér Katalógu služieb* – hlavnou zodpovednosťou je riadiť vytváranie, aktualizáciu a údržbu Katalógu služieb;
- *Manažér SLA*, resp. úrovne služieb – má zabezpečovať docielene požadovanej úrovne služieb;
- *Manažér bezpečnosti* –má za úlohu zosúladiť bezpečnosť IT s rizikami, dopadmi a požiadavkami, ktoré boli dohodnuté v bezpečnostnej politike organizácie;
- *Manažér dostupnosti* – má za úlohu to, aby služby dosahovali dohodnuté kvalitatívne ciele;
- *Manažér kontinuity IT služieb* – má v kompetencii zaistenie ich obnovy, ktorá má byť v súlade s dohodnutými požiadavkami a potrebami;
- *Manažér kapacity* – musí zaistiť to, aby IT budú napĺňali požiadavky obchodu

Prechod služby

Úvod

Prechod služieb je podporovaný základnými princípmi, ktoré uľahčujú efektívne a hospodárne využitie služieb. Medzi kľúčové princípy sa zahrňuje porozumenie všetkých služieb a ich užitočnosť, zriadenie formálnej politiky pre implementáciu všetkých potrebných zmien, podpora prenosu znalostí, podpora rozhodovania, predvídanie a riadenie, zaistenie spolupráce prechodu služby a požiadaviek na prechod služby v celom životnom cykle. Niektoré procesy prechodu služieb sú zapojené do celého životného cyklu a úvahy ohľadne ich dopadu, vstupov, monitorovania a riadenia sa týkajú všetkých fáz životného cyklu.

Účel

Prechod služby slúži na poskytnutie služby do prevádzkového využitia. Táto fáza sa realizuje potom ako prechod služby obdrží *Súbor dokumentov návrhu služby,* ktorý je výstupom fázy *Návrhu služby*. Prechod služieb po prevzatí tohoto súboru dodá do prevádzkovej fázy každý potrebný element potrebný pre súvislú prevádzku a jeho podporu. Ak sa po návrhu služby zmenia nejaké okolnosti, alebo požiadavky podniku, tak sa vo fáze Prechodu služby môžu modifikovať položky tak, aby zodpovedali danej požiadavke. Navrhnutá služba by mala byť navrhnutá tak, aby vedela čeliť možným komplikáciám a nepredvídaným udalostiam.

Ciele a prínosy prechodu služby

Prechod služby sa zameriava na implementáciu všetkých aspektov služieb, nie iba na ich aplikáciu a na to, ako je služba využívaná v tzv. normálnych podmienkach. Úlohou fázy prechodu služby je vziať do úvahy aj predvídateľné extrémne podmienky, rovnako ako je jej úlohou zabezpečiť dostupnosť podpory v prípade porúch, alebo chýb. Prechod služieb je podporovaný základnými princípmi, ktoré uľahčujú efektívne a hospodárne využitie nových/zmenených služieb. Medzi tieto kľúčové princípy patria:

- Porozumenie všetkým službám, ich užitočnosti a zárukám – pre efektívny prechod služby je podstatné poznať jej podstatu a účel v pojmoch výsledku a/alebo odstránenie obmedzení businessu (užitočnosti) a potvrdenie, že táto užitočnosť bude dodaná v patričnej kvalite (záruka)

- Zriadenie formálnej politiky a spoločného rámca pre implementáciu všetkých potrebných zmien – konzistentného a úplného, takého, aby zaručil, že sa nevynechá žiadna služba, zainteresovaná osoba, príležitosť atď. A nespôsobí sa tak porucha služby

- Podpora prenosu znalostí, podpora rozhodovania a opätovného využitia procesov, systémov, služieb a ostatných elementov – hospodárny Prechod služieb funguje za participácie všetkých zúčastnených strán, pri zaistení dostupnosti potrebných znalostí a možnosti opakovaného použitia za podobných okolností v budúcnosti.

- Predvídanie a riadenie „korekcií smeru“ – byť proaktivný a zisťovať pravdepodobné požiadavky na korekciu smeru, pokiaľ je potrebné prvky služby doladiť, je to vykonané logicky a s kompletnou dokumentáciou.

- Zaistenie participácie Prechodu služieb a požiadavkov na prechod v celom životnom cykle služby.

Životný cyklus prechodu služby by sa teda dal zosumarizovať takto:

Vstup: Súbor dokumentov návrhu služby (Service Design Package)

Etapy životného cyklu:

- Získanie a testovanie vstupných konfiguračných jednotiek a komponentov,

- Zostavenie (build) a testovanie

- Test vydania služby
- Test pripravenosti na prevádzku (operational readiness)
- Nasadenie
- Podpora v úvodnej fáze nasadenia (early life support)
- Zhodnotenie a skončenie prechodu služby.

Výstup: dodanie všetkých súčastí služby v prevádzkyschopnom stave pre fázu Service Operation.

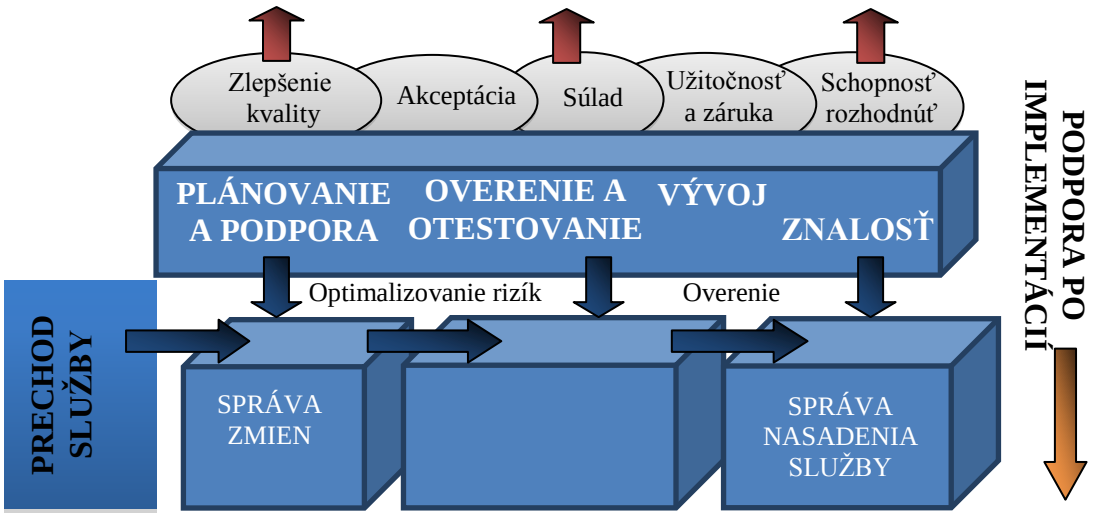
Procesy prechodu služby

Ako už bolo vyššie spomenuté, publikácia Prechodu Služieb sa primárne zaoberá aspektami umiestnenia služieb, či už nových, tak aj aktualizovaných, do prevádzakového prostredia. V tejto podkapitole si definujeme a vysvetlíme zásadné procesy popísané v tejto publikácii. Medzi týmito procesmi existuje niekoľko z nich, ktoré sú zapojené do celého životného cyklu služby a úvahy ohľadom ich dopadu, vstupov, monitorovania a riadenia sa tak dotýkajú všetkých fáz životného cyklu služby. Medzi tieto procesy patria:

- Manažment zmien
- Manažment aktív a konfigurácií
- Manažment znalostí

Okrem týchto komplexných procesov Prechod služieb zahŕňa ešte niekoľko procesov:

- Plánovanie a podpora prechodu
- Manažment vydaní a nasadení
- Overenie a testovanie služby
- Vyhodnotenie



Obr. 11. Zjednodušený workflow procesov prechodu služby.

Plánovanie a podpora prechodu (Transition Planning and Support)

Hlavné ciele a účely procesu Plánovania prechodu služby by sa dali zhrnúť do týchto bodov:

- Plánovanie kapacít a zdrojov pre vývoj, implementáciu, vydanie, testovanie a nasadenie služby do prevádzky,
- Podpora pre tímy prechodu služby, t.j. pre ľudí vykonávajúcich aktivity pri prechode služby,
- Plánovanie zmien na zabezpečenie integrity s aktívami zákazníka, aktívami a konfiguráciami služby, ich správa počas prechodu služieb,
- Zabezpečenie správ o priebehu prechodu, rizikách a odchýlkach pre všetky relevantné zúčastnené strany, najmä pre ľudí s rozhodovacou právomocou,
- Koordinácia aktivít v projektoch, zabezpečenie súhry vývojárov a dodávateľov,

Cieľom je teda naplánovať a koordinovať zdroje tak, aby bolo zaistené, že požiadavky zo *Stratégie služieb* rozpracované v *Návrhu služieb* budú v tejto fáze efektívne realizované. To samozrejme zahŕňa aj identifikáciu a manažment rizík, porúch a prerušení dodávky služieb behom činností spojených s prechodom.
Efektívne plánovanie prechodu služby v sebe však zahŕňa aj:

- Definovanie a aplikáciu politiky prechodu služby (Service Transition Policy)
- Definovanie politiky vydania

Manažment zmien (Change management)

Manažment zmien je proces, ktorý má za úlohu zaistiť, aby všetky zmeny boli zaznamenané, vyhodnotené, autorizované, aby im bola priradená priorita, aby boli otestované, implementované, dokumentované a revidované kontrolovaným spôsobom. Zmena služby je v tomto prípade jasne definovaná a hovorí sa o nej ako *o pridaní, modifikácii, alebo odstránení autorizovanej, plánovanej, alebo podporovanej služby, alebo jej komponenty a dokumentácie, ktorá k nej prislúcha.* Potom je hlavným cieľom Manažmentu zmien uskutočnenie užitočných zmien pri čo najkratšom prerušení IT služieb.

Zmeny samé o sebe môžu vznikať dvoma druhmi spôsobov:

- *Proaktívne* - napr. hľadaním výhod pre biznis: znižovanie nákladov, zlepšovanie servisu, zvýšenie efektívnosti,
- *Reaktívne* – ako odozva na chyby alebo adaptácia na zmeny zvonka.

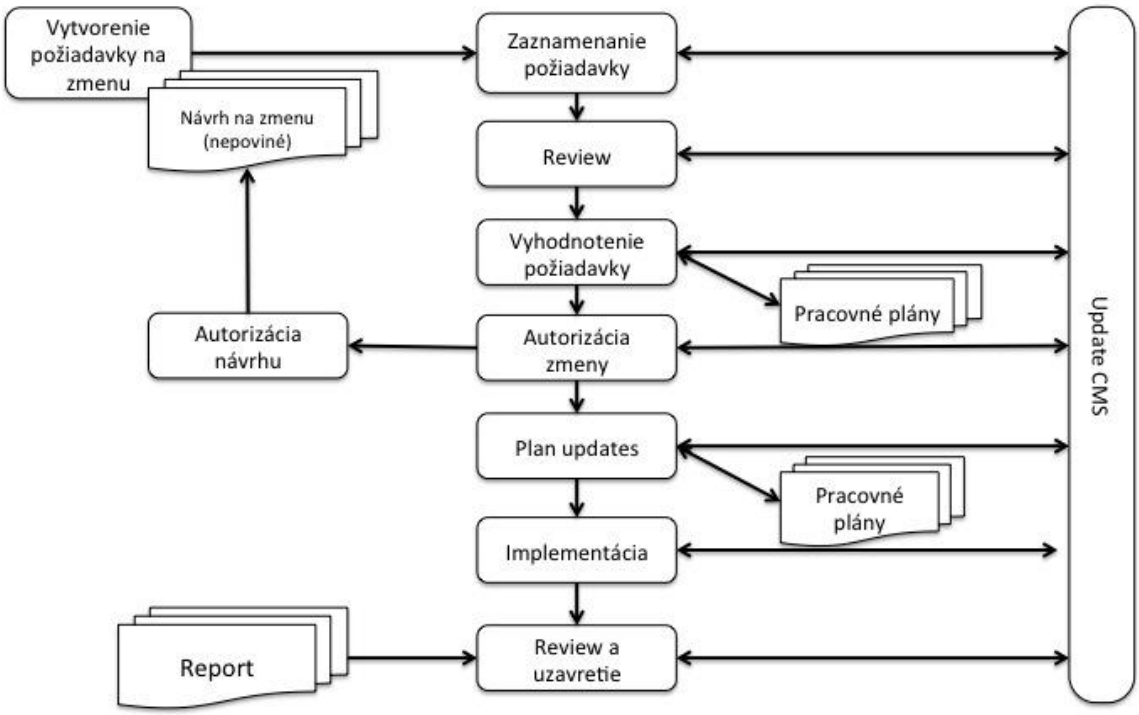
Proces manažmentu zmien sa teda zaoberá zmenami všetkých typov. Jeho cieľom je zaistiť, aby sa pre efektívnu a promptnú manipuláciu so zmenami využívali štandardizované metódy a postupy. Rovnako je cieľom zaistiť, aby všetky zo zmien boli zaznamenané v systéme pre správu konfigurácií (CMS) a aby celkové riziko pri implementácii zmien bolo optimalizované.

Manažment zmien je tak relevantný počas celého životného cyklu služby, vzťahuje sa ku všetkým úrovniam správy služieb – k strategickej, taktickej aj prevádzkovej úrovni. Manažment zmien poskytuje businessu nástroj, ako znížiť počet chýb pri nových, alebo menených službách, rýchlejšiu a presnejšiu implementáciu zmien. Rovnako poskytuje mechanizmy, ktoré umožňujú sa pri obmedzených fondoch

a zdrojoch koncentrovať práve na tie zmeny, ktoré dosiahnu najväčší prospech pre business.

Malé zmeny sa môžu zdať neškodné, ale pritom môžu spôsobiť veľké škody. Je dobrou praxou používať pri posúdení zmeny aj aspekty rizika. Pozornosť by mala byť zameraná najmä na hľadanie faktorov, ktoré môžu prerušiť business procesy, brániť dodávke služieb, alebi inak ovplyvniť ciele organizácie.

Problematika rizík musí byť zvážená, než dôjde k odsúhlaseniu zmeny. Organizácie ku kategorizácii rizík požívajú maticu P x D – *pravdepodobnosť* x *dopad*, ktorá každé riziko zaradí do niektorej z kategórií podľa odhadnutého dopadu a pravdepodobnosti jeho vzniku. Relevantné rizika, teda tie s vysokou mierou koeficientu P x D, je potrebné posúdiť a príslušným spôsobom schváliť zodpovednou osobou za danú business službu. Inou metódou môže byť *Stredná doba obnovy služby* (Mean Time to Restore Service, MTRS), čo je priemerný čas trvania obnovy konfiguračnej položky alebo IT služby po zlyhaní.



Obr.12 Proces manažmentu zmien

Celý proces pozostáva z viacerých krokov a podprocesov ako je možno vidieť na obrázku. Jedným z hlavných je proces zodpovedný za filtrovanie požiadavok na zmenu a zaznamenaie zmien. *Požiadavka na zmenu* (Request for Change, RFC) predstavuje formálny návrh na vykonanie zmeny. Požiadavka na zmenu obsahuje detaily navrhovanej zmeny a môže byť zaznamenaná v papierovej alebo elektronickej forme. Výraz požiadavka na zmenu sa často nesprávne používa na vyjadrenia záznamu o zmene, alebo na vyjadrenie samotného výrazu zmena. Až po zaznamenaná požiadavky na zmenu sa táto vyhodnocuje a evaluuje a v prípade schválenia naplánuje a implementuje.

Manažment aktív a konfigurácií (Service Asset and Configuration Management)

Proces manažmentu aktív a konfigurácií je zásadný proces Prechodu služieb. Bez neho nie je možné rozumne vykonávať zmeny infraštruktúry, aktualizácie nových verzií aplikačných softvérov a ostatných aktivít. Je to proces, ktorý podporuje business tým, že poskytuje presné informácie a kontrolu nad všetkými existujúcimi aktívami a vzťahmi, ktoré tvoria infraštruktúru organizácie. Zavedenie Manažment konfigurácii poskytuje logický model infraštruktúry a služieb, identifikuje, zabezpečuje kontrolu a údržbu všetkým konfiguračným položkám a stará sa o konfiguračnú databázu (CMDB). Podporuje ostatné procesy poskytovaním vierohodných informácií o konfiguračných položkách infraštruktúry a o ich dokumentácii. Vo všeobecnosti by sme tento proces mohli rozdeliť do dvoch celkov:

- Konfiguračný manažment
- Manažment aktív

Z prvého hľadiska sa naň pozeráme ako na proces zodpovedný za udržiavanie informácií o *konfiguračných položkách* (CI) vyžadovaných na dodávku IT služieb, vrátane ich vzájomných vzťahov, počas celého cylku CI. Z hľadiska manažmentu aktív ide o proces zodpovedný za sledovanie a reportovanie hodnoty a vlastníctva finančných aktív. Rozsah tohoto procesu sa rozširuje aj o aktíva, ktoré neprináležia IT a o interných a externých poskytovateľov služieb, kde je nutné kontrolovať zdieľané aktíva.

Konfiguračná položka je aktívum, predstavuje ľubovoľnú časť vývojového prostredia a/alebo dodávky, ktorá musí byť samostatne identifikovaná, uchovávaná, testovaná, preverená, používaná, menená, dodávaná a udržiavaná. Pokiaľ pri identifikácii nevieme presne určiť, či sa jedná o konfiguračnú položku, môžeme si položiť otázku: Ovplyvnilo by našu schopnosť dodať službu v poriadku, včas a bez dodatočných nákladov, keby sa táto položka (súbor, HW atď.) stratila (resp. bola nesprávne použitá, poškodená)? Pokiaľ dostaneme kladnú odpoveď, jedná sa o konfiguračnú položku. Jednotlivé konfiguračné položky sa môžu navzájom výrazne odlišovať, či už zložitosťou, veľkosťou, či typom:

- v rozsahu od kompletnej služby, alebo systému (vrátane všetkých HW, SW, dokumentácie a podporného personálu)
- až po samostatný SW modul, alebo malú časť HW.

Múžu takisto obsahovať aj iné položky v rámci konfiguračnej hierarchie. Konfiguračné položky by mali byť volené pomocou stanoveného výberu kritérií, zoskupované, klasifikované a identifikované takým spôsobom, aby ich bolo možné raidiť v priebehu ich životného cyklu.

1. Konfiguračné položky teda možno rozdeliť do niekoľkých kategórií:
2. Konfiguračné položky životného cyklu služby (Service lifecycle CIs)
3. Konfiguračné položky služieb (Service CIs)
4. Konfiguračné položky organizácie (Organization CIs)
5. Interné konfiguračné položky (Internal CIs)
6. Externé konfiguračné položky (External CIs)

Konfiguračná databáza (Configuration management database (CMDB)) je úložisko informácií vzťahujúcich sa k všetkým komponentom IS. Aj napriek tomu, že boli a sú úložiská podobné CMDB používané IT oddeleniami už dlho, pochádza termín CMDB z ITILu. V súvislosti s ITILom predstavuje CMDB schválenú konfiguráciu významných komponentov v IT prostredí. Hlavným cieľom CMDB je pomáhať organizáciám pochopiť vzťahy medzi komponentami a sledovať ich konfiguráciu. CMDB je základnou zložkou ITIL rámca a celkovo procesu manažmentu konfigurácií.

Implementácia CMDB často zahŕňa integráciu s ostatnými systémami, napr. so systémami riadenia aktív. Záznamy v CMDB (konfiguračné položky) obsahujú detaily o dôležitých vlastnostiach a vzťahoch medzi CI. Manažéri konfigurácií obvykle popisujú CI pomocou troch typov atribútov:

- Technické
- Vlastníctvo
- Vzťahy

Kľúčovým faktorom úspechu pri implementácii CMDB je schopnosť automaticky odhaliť informácie o CI a sledovať zmeny ihneď keď nastanú.

Pre riadenie veľkých a komplexných služieb a infraštruktúr IT vyžaduje tento proces aj podporu *systému pre správu konfigurácií* (CMS). CMS je v podstate súbor nástrojov a databáz, ktoré sú používané na manažovanie konfiguračných údajov poskytovateľa IT služieb. CMS tiež zahŕňa informácie o incidentoch, problémoch, známych chybách, zmenách a vydaniach. Systém môže obsahovať údaje o zamestnancoch, dodávateľoch, umiestneniach, podnikových jednotkách, zákazníkoch a používateľoch a zahŕňa nástroje pre zber, uchovávanie, manažovanie, aktualizáciu a prezentáciu údajov o konfiguračných položkách a o ich vzájomných vzťahoch. CMS je udržiavaný konfiguračným manažmentom a je využívaný všetkými procesmi manažmentu IT služieb. Model, s ktorým CMS pracuje je CMDB. Obvykle systém CMS udržuje jednu, alebo viac CMDB, pričom každá CMDB uchováva atribúty konfiguračných položiek (CI) a ich vzájomné vzťahy s inými konfiguračnými položkami. Záznam o konfigurácii (Configuration Record) je potom záznam obsahujúci detaily o konfiguračnej položke - každý konfiguračný záznam dokumentuje životný cyklus jednej CI.

Je tu definovaná aj Definite Media Library (DML), čo je záložná databáza schválených CI a obsahuje kópie CI všetkých verzií a ich kvality nezávisle na originálov v správe jednotlivých služieb.

Manažment vydaní a nasadení (Release and Deployment Management)

Cielom proces Manažnemtu vydaní a nasadení je spojiť všetky pohľady na služby, umiestniť ich do produkcie a zabezpečiť, aby sa nové alebo zmenené služby efektívne využívali. Inými slovami je to proces, ktorý je zodpovedný za plánovanie, zostavovanie rozvrhov a riadenie presunu vydaní do testovacieho a živého prostredia tak, aby bola chránená integrita celého prostredia a aby boli vydávané správne komponenty. Manažment vydaní je riadený politikami vydávania (Release Policies) a rozlišuje niekoľko úrovní vydaní služieb:

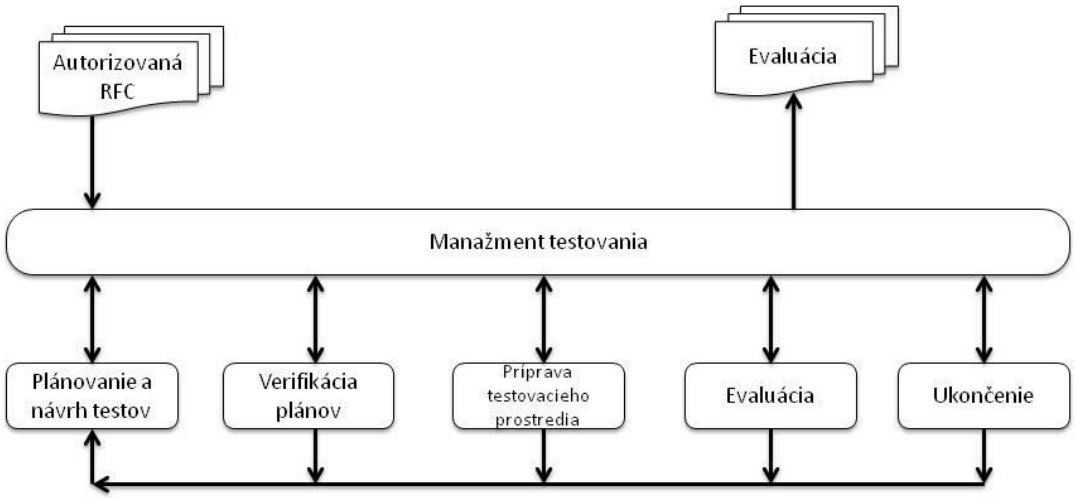
- *Hlavné vydania* (Major releases) – rozsiahle rozšírenia, zvyčajne o nové funkcionality, môžu odstraňovať niektoré chyby a problémy,
- *Vedľajšie vydania* (Minor releases) – menšie rozšírenia a opravy, niektoré z nich mohli byť predtým uverejnené ako poruchové vydania.
- *Poruchové vydania* (Emergency releases) – korekcie menšieho počtu známych chýb, resp. Rozšírenia smerom k prioritným business požiadavkám.

Proces manažmentu vydaní zaisťuje hladký priebeh distribúcie nového hardvéru, softvéru, prípadne nových verzií existujúceho hardvéru a softvéru, do IT infraštruktúry na základe schválených zmien. Úlohou manažmentu vydaní je správa Definite Software Library (DSL), kde je uchovávaný, alebo interne vyvíjaný softvér (respektíve inštalačné médiá, kódy, dokumentácia), a správa Definite Hardware Store (DHS), teda rezervného, práve nepoužívaného hardvéru. Aktivita *Nasadenie* (Deployment, tiež Rollout) je potom zodpovedná za presun nového alebo zmeneného hardvéru, softvéru, dokumentácie, procesu a pod. do živého prostredia.

Validácia a testovanie služby (Service Validation and Testing)

Všetky služby musia byť vždy presne testované, aby sa potvrdilo, že boli splnené požiadavky podniku a že uvedenie služby do prevádzky bude v rozpätí dohodnutých obchodných rizík. Testovanie služby je najmä potrebné preto, aby sa v prípade poruchy mohol doložiť dôkaz, že daná služba bola podporovaná všetkými požiadavkami podniku. Testovanie v sebe zahŕňa testovanie obchodnej funkčnosti, dostupnosť, bezpečnosť a použiteľnosť služby.

Úspešné otestovanie zároveň závisí na komplexnom porozumení služby – ako bude využívaná, akým spôsobom je konštruovaná. Všetky služby, či už interné, alebo outsourcované musia byť náležite otestované, pričom tieto testy potvrdia, že požiadavky businessu môžu byť pomocou tejto služby dosiahnuté v plnom rozsahu očakávaných situácií a prevádzka služby neprekročí dohodnuté riziko. Hlavným cieľom validácie a testovania je poskytnôť objektívny dôkaz, že nová/zmenená služba podporuje požiadavky businessu, vrátane dohodnutých SLA.

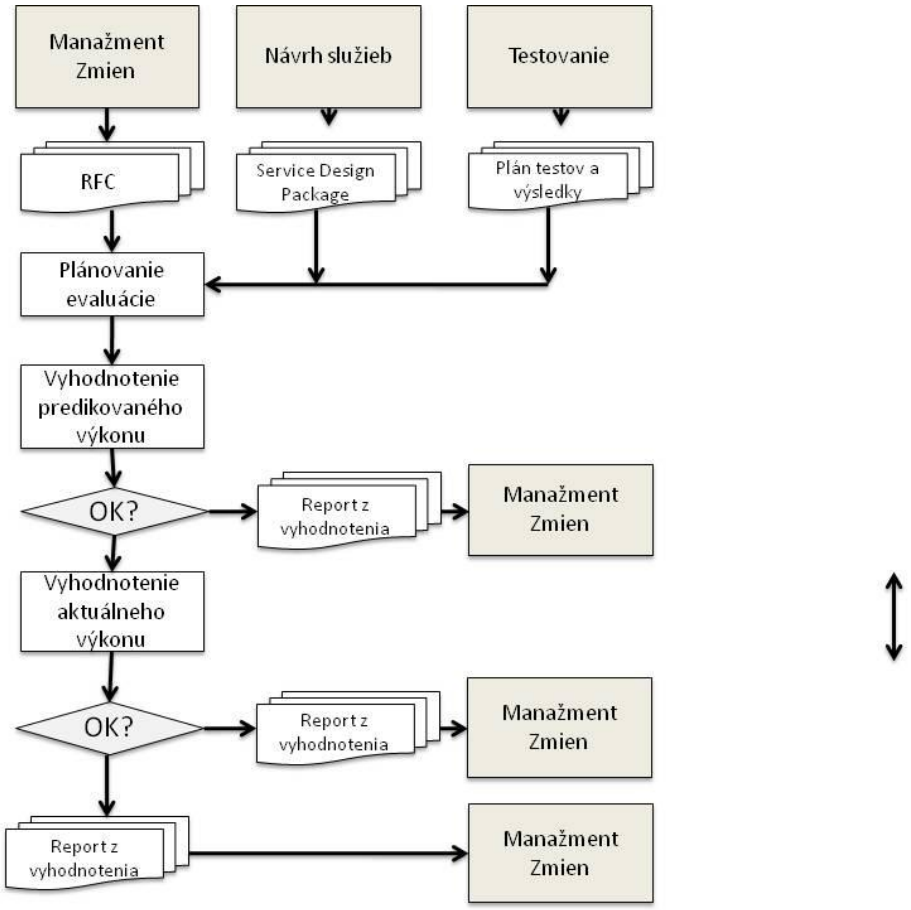


Obr. 13 Príklad procesu validácie a testovania

Vyhodnotenie (Evaulation)

Hodnotenie je všeobecný proces, či konkrétna služba je prijateľná. V tejto súvislosti je potrebné vziať do úvahy, že každá odchýlka od predpokladaného a aktuálneho stavu musí byť posúdená zákazníkom a zároveň prijatá. Proces Vyhodnotenia sa zaoberá tým, či je daná služba akceptovateľná v očakávanom prostredí podniku. Jeho cieľom je teda posúdiť nové/zmenené IT služby. Proces má zabezpečiť, že riziká boli spracované a napomáha rozhodnúť sa, či pokračovať ďalej so zmenou,

alebo bez nej. Vyhodnotenie tuto rovnako znamená aj porovnanie aktuálnych výstupov služby s plánovanými výstupmi, alebo porovnávanie viacerých alternatív.



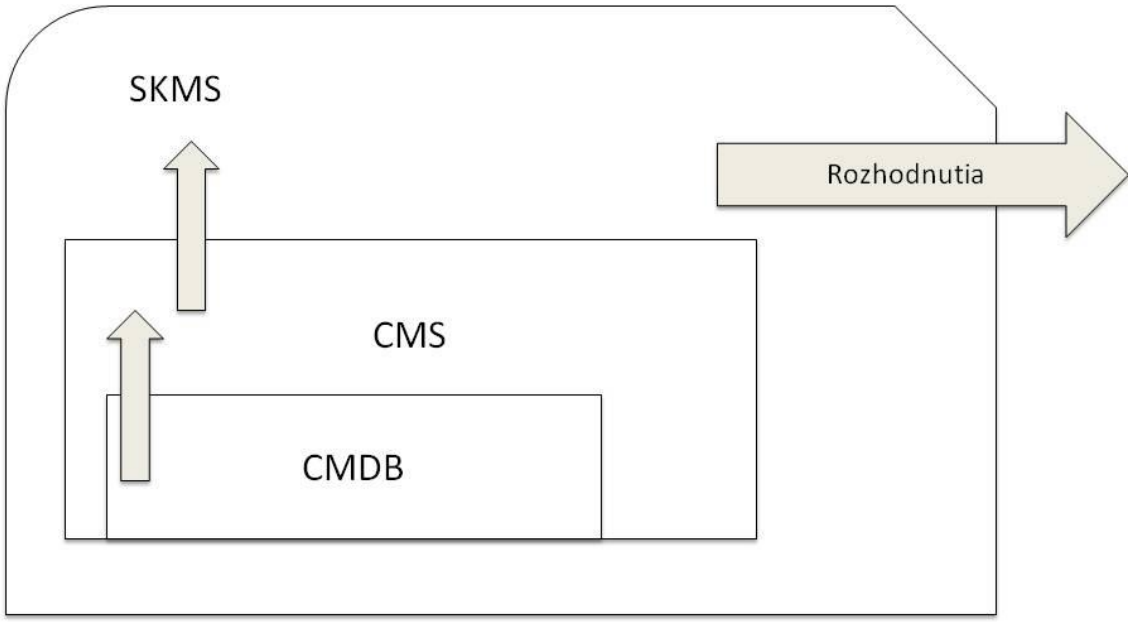
Obr. 14 Proces vyhodnotenia

Manažment znalostí (Knowledge management)

Proces Manažmentu znalostí je zodpovedný za zber, analýzu, ukladanie a zdieľanie znalostí a informácií v rámci organizácie. Hlavným dôvodom manažmentu znalostí je zlepšovať efektívnosť znižovaním nutného znovuobnovovania znalostí. Cieľom procesu je teda zabezpečiť, aby správne osoby mali správne znalosti v správny čas a mohli tak efektívne podporiť služby požadované businessom. To napomôže k získaniu:

- Hospodárnejších služieb so zvýšenou kvalitou
- Jasnému a všeobecnému poruzumeniu hodnotám, ktoré služby prinášajú
- Relevantných informácií, ktoré sú kedykoľvek dostupné

Jadrom celého procesu je štruktúra DIKW (Data-Information-Knowledge-Wisdom), ktorá kondenzuje surové, nespracované a nevyužiteľné dáta do hodnotných aktív. Toto je zabezpečené systémom Manažmentu znalostí, ktorý obsahuje relevantné informácie a znalosti odvodené z množiny dáť o aktívach a konfiguračných položkách. *Systém manažmentu znalostí služieb* (SKMS – Service Knowledge Management System) je teda množina nástrojov a databáz, ktoré sa používajú na riadenie znalostí a informácií. SKMS obvykle v sebe integruje a pokrýva systém konfiguračného manažmentu obohatený o ďalšie nástroje a databázy. Systém má za úlohu ukladať, manažovať, aktualizovať a prezentovať všetky informácie, ktoré poskytovateľ IT služieb potrebuje na riadenie úplného životného cyklu služby.



Obr. 15 Vzťah medzi SKMS a CMS/CMDB

Roly prechodu služby

- Manažér zmien (Change Manager): úlohou je povoľovať a dokumentovať všetky zmeny IT infraštruktúry (Konfiguračne položky), aby bolo zaistené minimálne narušenie služieb v prípade výroby. V prípade požiadavok na zmeny, ktoré môžu mať významný dopad sa manažér zmien obracia Schvaľovaciu komisiu pre naliehavé zmeny (Emergency Change Advisory Board (ECAB)).

- Komisia pre naliehavé zmeny (Emergency Change Advisory Board): ECAB je skupina ľudí, ktorých cieľom je upozorniť manažment na zmeny v hodnotení, priority a plánovaní zmien. Táto komisia sa skládá zo zástupcov všetkých oddelení IT služieb a zástupcov externých dodávateľov, v případě potřeby.

- Service transition manager: je zodpovedný za pravidelnú kontrolu aktivít ostatných pracovníkov zapojených vo fáze prechodu služieb. Má na starosti celkové plánovanie a riadenie prechodu služieb a riadenie činností s tým spätých vrátane plánovania rozpočtu. Slúži ako jediné rozhranie pre komunikáciu s vyšším manažmentom.

- Service Asset Manager: implementuje štandardy riadenia aktív, evaluuje existujúce spôsoby riadenia aktív a navrhuje a implementuje vylepšenia.

- Configuration Control Board: definuje a riadi správu konfigurácií v oblasti hlavných a podporných služieb, aplikácií a infraštruktúry.

- Configuration Manager: je zodpovědný za zachovanie integrity údajov o CI vrátane tých, ktoré musí dodať do IT služieb. Vytvára logický dátový model, ktorý obsahuje zložky IT infraštruktúry (CI) a ich vzťahy.

- Configuration analyst: má za úlohu vytvárať procesy riadenia aktív a konfigurácií tak, aby boli v súlade s definovanými rolami a zodpovednosťami. Pomáha vytvárať plány riadenia aktív a konfigurácií a princípy ich implementácie.

- Configuration administrator: hlavnou úlohou je riadiť ukadanie všetkých CI, poskytuje informácie o jednotlivých CI.

- CMS/tools administrator: monitoruje výkonnosť a kapacitu CMS a vytvára v prípade potreby odporúčania na možnosti vylepšenia.

- Performance and risk evaluation manager: jeho úlohou je vytvoriť plán evaluácie pre testovanie služby a identifikovať možné riziká a problémy spojené s jej používaním.

- Manažér znalostí (Knowledge Management process owner): úlohou je zaistiť, že IT organizácia je schopná zhromažďovať, analyzovať, ukladať a zdieľať znalosti a informácie. Jeho hlavním cieľom je zlepšiť účinnosť znížením využívaním existujúcich znalostí.

- Service Test Manager: úlohou je zaistiť, že verzie služby, ktoré sú nasadené splňujú ciele sledované klientmi. Kontroluje tiež, že prevádzka IT je schopná podporovať novú službu.

- Release and deployment manager: je zodpovedný za plánovanie, návrh, konfiguráciu a testovanie všetkého softvéru a hardvéru potrebného pre vytvorenie vydania pre dodanie služby.

Záver

V tejto kapitole boli popísané základné koncepty fázy prechodu služby. Táto pokrýva implementáciu do prevádzkového prostredia vrátane testovania, samotného nasadenia, validácie a iných. Prakticky nadväzuje na predchádzajúcu kapitolu, vychádza z návrhu služieb. Výstupmi z tejto fázy potom sú samotné plány prechodu a nasadenia, otestované riešenia a zavedený a aktualizovaný SKMS. Publikácia sa venuje popisu taktýchto procesov nielen pre nové, ale aj pre služby zmenené. Na publikáciu popisujúcu prechod služby nadväzuje publikácia popisujúca fázu prevádzky služieb.

Prevádzka služby

Úvod

Prechod služieb je podporovaný základnými princípmi, ktoré uľahčujú efektívne a hospodárne využitie služieb. Medzi kľúčové princípy sa zahrňuje porozumenie všetkých služieb a ich užitočnosť, zriadenie formálnej politiky pre implementáciu všetkých potrebných zmien, podpora prenosu znalostí, podpora rozhodovania, predvídanie a riadenie, zaistenie spolupráce prechodu služby a požiadaviek na prechod služby v celom životnom cykle. Niektoré procesy prechodu služieb sú zapojené do celého životného cyklu a úvahy ohľadne ich dopadu, vstupov, monitorovania a riadenia sa týkajú všetkých fáz životného cyklu.

Služby vo fáze prevádzky produkujú hodnotu pre zákazníka. IT infraštruktúra je ako organizmus, ktorý žije, no je potrebné tento organizmus sledovať, aby sme zistili, či funguje normálne. Preto je dôležité poznať stav služieb a infraštruktúry, ktoré vplývajú na celkovú prevádzku, ale aj na celú infraštruktúru. Nie je potrebné monitorovať celú infraštruktúru, ale zamerať sa na dôležité časti, ktoré sú kritickými oblasťami v IT podnikaní. Hlavným cieľom je dodať zákazníkovi dohodnutú úroveň služieb.

Služby nachádzajúce sa v životnom cykle prevádzky sú poskytované zákazníkom. Z tohoto hľadiska je fáza prevádzky služby najdôležitejšia z toho dôvodu, že procesy a koncepty popisované v tejto časti sú jediné nielen viditeľné, ale priamo sa týkajúce zákazníka. Jak procesy, tak napr. konkrétne pracovisko Service Desk popisované v tejto časti ITIL knižnice sa priamo zaoberajú spôsobom komunikácie so zákazníkom. Aj z tohoto dôvodu sa častokrát procesy popisované v tejto časti implementujú medzi prvými, resp. pri implementáciách v malých podnikoch sú implementované iba tieto.

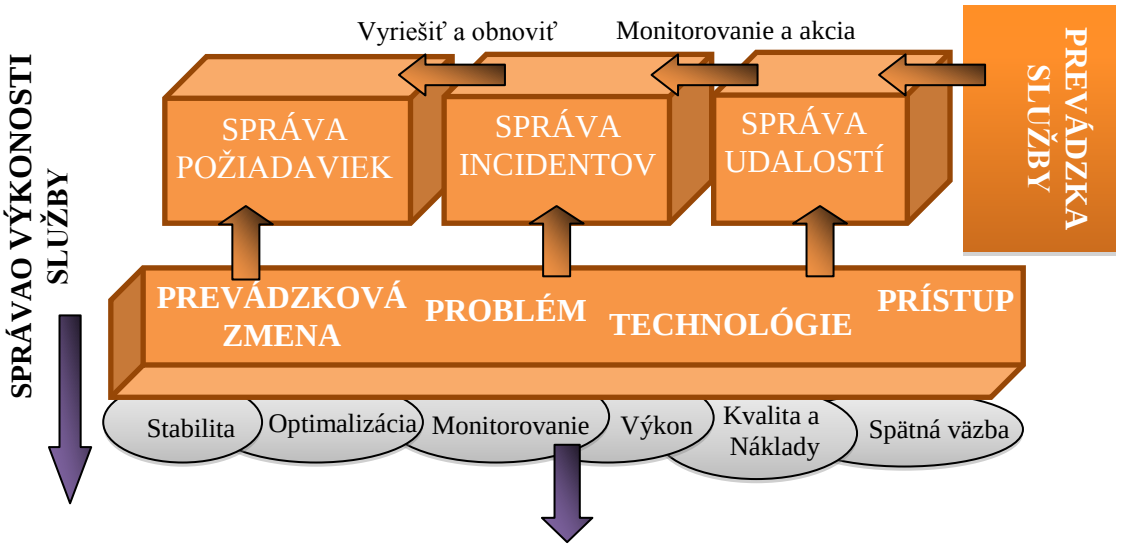
Ciele prevádzky služby sa teda dajú označiť aj ako metódy ako identifikovať a udržať podstatné príznaky pre tzv. „zdravie prevádzky IT“. To môže mať viacero podôb, napríklad zabezpečenie rovnováhy medzi vnútorným pohľadom na IT v organizácii a biznis pohľadom organizácie celkovo, zohľadňovaním kvality poskytovaných

služieb a nákladov na ňu, či nájdením vhodného balansu medzi reaktívnym a proaktívnym riešením situácií.

Medzi najdôležitejšie koncepty (resp. funkcií) a procesy popisované v ITIL Prevádzka služby patria tieto:
Service Desk – ITIL defininuje pracovisko, ktoré predstavuje spôsob kontaktu, pre všetkých používateľov a zákazníkov s IT oddelením. Riadi interakciu s používateľmi na základe definovaných procesov a informuje používateľov o stave služieb a ich požiadavie,
Manažment aplikácií (Application Management) – zamerané na softvérové aplikácie a zahŕňa ľudí, ktorí poskytujú technickú odbornosť a správu týchto aplikácii,
Správa technológií (Technical Management) – zahŕňa personál s technickou odbornosťou a správu infraštruktúry IT. Pomáha plánovať a pokračovať v stabilizácii technickej infraštruktúry,
Správa dodávky IT (IT Operations Management) – zodpovedá za správu a údržbu infraštruktúry IT, ktorá je potrebná pre dodávku dohodnutej úrovne IT služieb pre biznis. Správu dodávky IT vykonávajú operátori svojimi rutinnými úlohami, ktorými sú hlavne monitorovanie a kontrola.

Medzi procesy spadajúce do tejto fázy životného cylku služby patria:

- Manažment udalostí
- Manažment incidentov
- Manažment problémov
- Správa požiadaviek
- Správa prístupov



Obr. 15. Zjednodušený workflow procesov prevádzky služby.

Manažment udalostí

Manažment udalostí definuje *udalosť* (Event), ako zmenu stavu, ktorá ovplyvňuje správu konfiguračných položiek, alebo IT služieb. Udalosť môže indikovať, že niečo nefunguje korektne, kedy sa jedná o zaznamenanie incidentu, alebo udalosť môže zaznamenať normálnu aktivitu, či hlásenie potreby rutinného zásahu, ktoré môže predstavovať. Odpovede na udalosti môžu byť manuálne, alebo sa dajú automatizovať.

Proces Manažmentu udalostí je úzko prepojený s ostatnými aktivitami manažmentu IT služieb, najmä však s monitorovaním. Zásadný rozdiel spočíva v tom, že na rozdiel od monitorovania tento proces nekontroluje stav komponentov infraštruktúry, keď k ničomu nedochádza.

Proces je obvykle spustený výskytom udalosti ako takej. Nie všetky udalosti sú detekované a registrované. Notifikácia udalosti je vygenerovaná konkrétnou konfiguračnou položkou. Schopnosť konfiguračných položiek generovať udalosti ale musí byť vopred zohľadnená pri návrhu konfiguračnej databázy a návrhu infraštruktúry. Akonáhle je vygenerovaná notifikácia, detekuje sa udalosť. V reálmych prostrediach sú udalosti sú generované mnohými komponentami infraštruktúry v pravidelných okamihoch, kvantum dát, ktoré generujú by bolo obtiažne spracovávať separátne. Aj z toho dôvodu je jedným z prvých krokov tohoto procesu filtrovanie udalostí na základe ich dôležitosti. Pri filtrácií udalostí je cieľom rozhodnúť, či udalosť zaradíme na spracovanie, alebo či vzniknutú udalosť môžeme ignorovať. Úlohou je

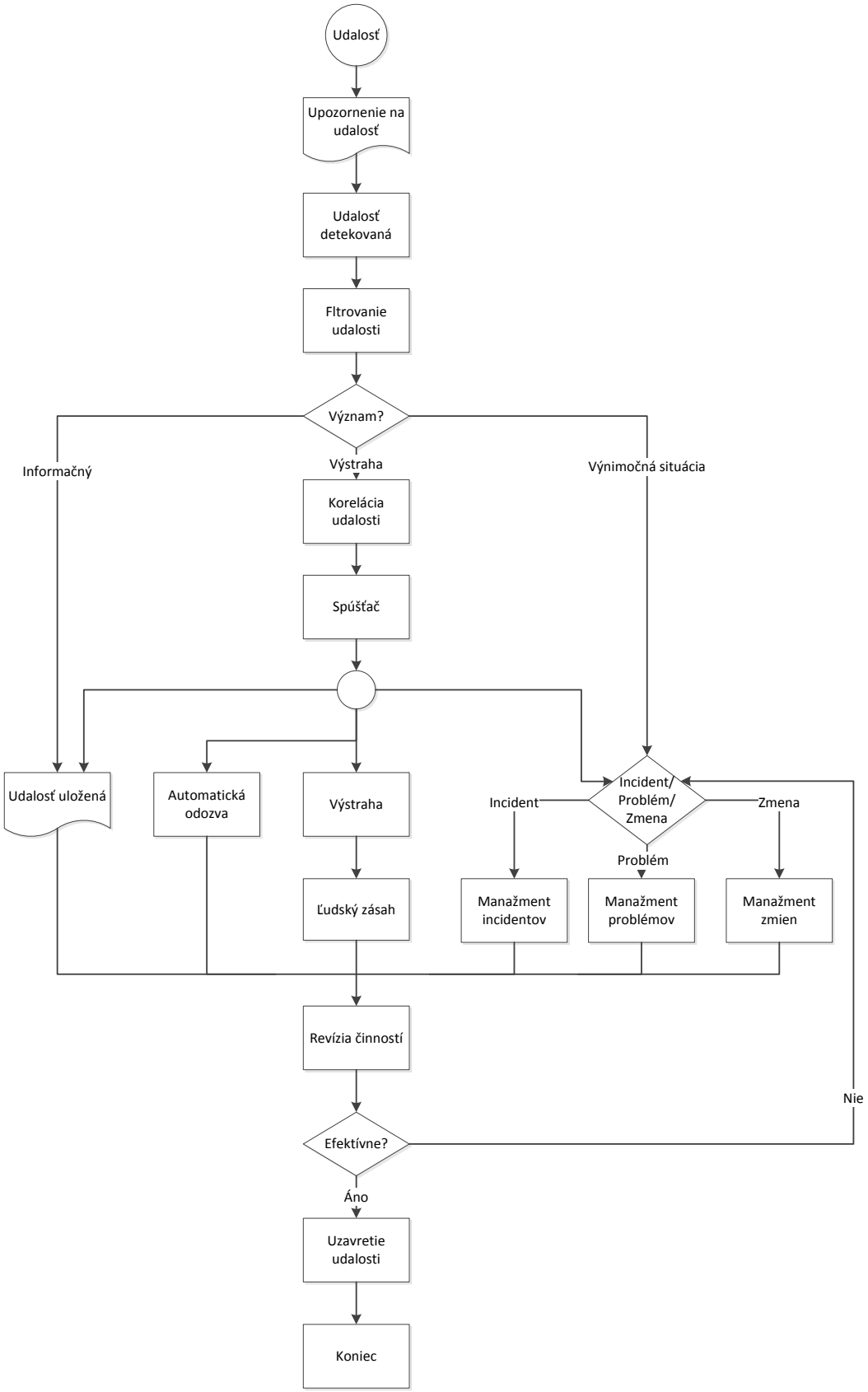
rozdeliť udalosti podľa kategórie, ITIL špecifkuje tieto tri hlavné kategórie udalostí, pre ktoré následne odporúča štandardné posupy ich spracovania:

Informatívna – tento typ udalosti podáva informáciu o stave infraštruktúry, resp. konkrétnej konfiguračnej položky (napr. prihásenie sa používateľa, logy zo sieťových komponentov, atď.). Nenesie signifikantný význam, ale je potrebné takúto udalosť zaznamenať, napr. pre účely ďalšej analýzy. Udalosti tohoto typu sú poväčšinou automaticky ukladané niektorým z nástrojov pre podporu riadenia IT do databázy, z nej sú po uplynutí určitej doby (závislé od zákazníka a poskytovateľa) odstránené a nahradené aktuálnymi záznamami;

Varovanie – signalizuje dosiahnutie prednastavenej východiskovej hodnoty (zaťaženie CPU, RAM, doba odozvy), ktorá môže predchádzať vzniku incidentov (napr. varovanie pri zaťažení procesora na 65% ak bude 75% kritický stav). Pre tento typ udalosti je potrebné vykonať činnosť. Akú, je potrebné rozhodnúť. To je náplň tzv. Korelačného nástroja, (Correlation Engine), čo vo všeobecnosti znamená porovnanie udalosti, ktorá nastala s existujúcimi udalosťami v báze. Cieľom je rozhodnúť, ako veľmi a aké akcie je pre jej vyriešenie potrebné uplatniť. Takúto udalosť na základe jej charakteristík možno vyriešiť bez potrebných úkonov, teda iba uložením do databázy, automatickou odpoveďou (z množiny vopred preddefinovaných štandardných riešení), vygenerovaním upozornenia (upozornenie, že sa blíži moment, kedy je možné na danej konfiguračnej položke očakávať incident, napr. voľné miesto na disku pod 5%), alebo riešiť udalosť ako incident/zmenu/problém, ak sa ukáže, že je jedným z nich;

Výnimka – signalizuje neštandardný stav. Vo všeobecnosti znamená, že udalosť reprezentuje incident, problém, alebo požiadavku na zmenu. V takom prípade sa potom podľa typu výnimky spúšťa konkrétny proces manažmentu incidentov, manažmentu zmien, alebo manažmentu problémov.

Po spracovaní udalosti je potrebné skontrolovať a preveriť akcie, ktoré k vyriešeniu udalosti videli. Ak bola udalosť vyriešená a bola vyriešená efektívne, riešenie udalosti sa uzatvára.



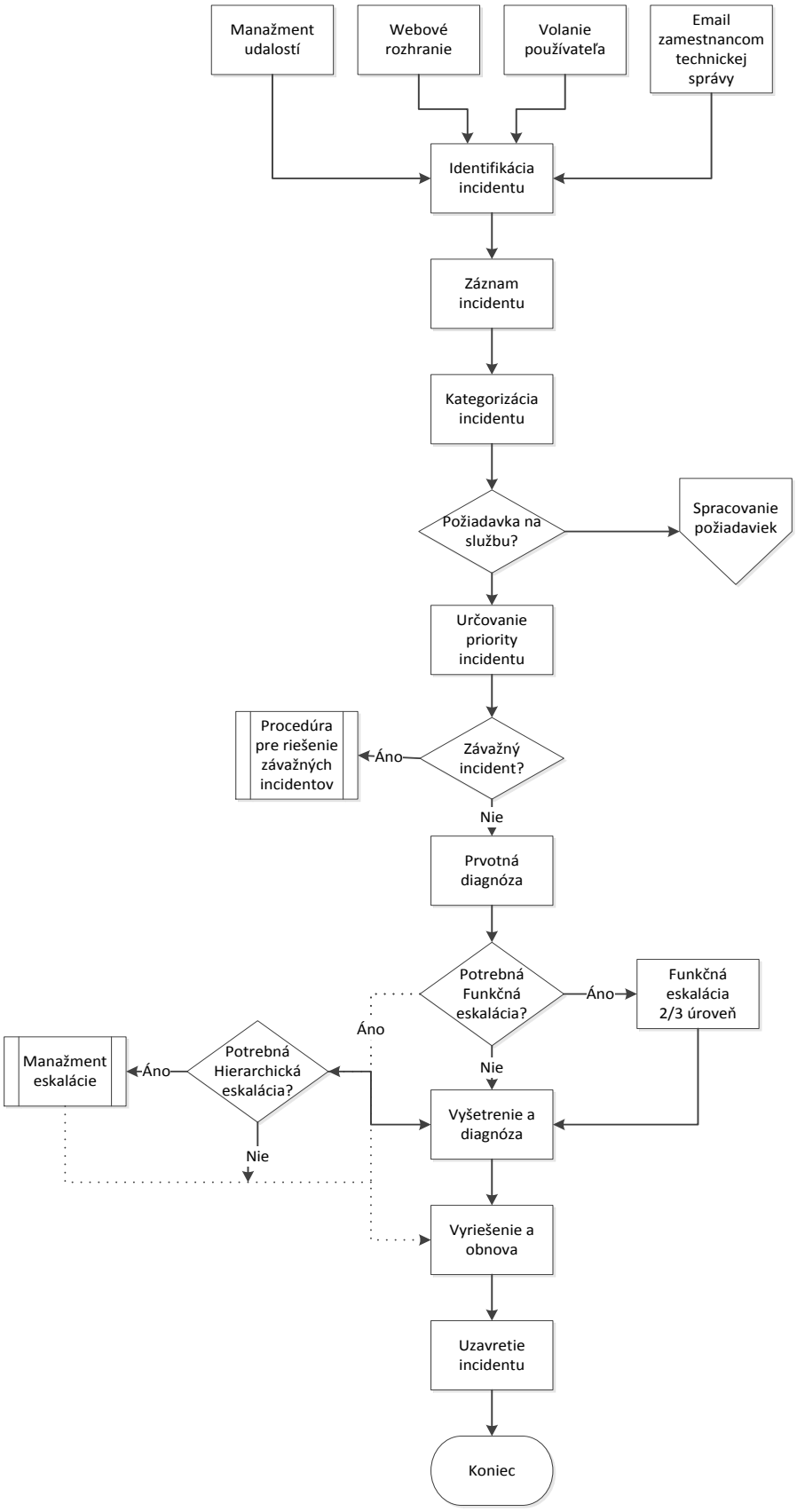
Obr. 16. Proces manažmentu udalostí.

Manažment incidentov

Manažment incidentov (Incident Management, ďalej IM) je procesom z oblasti ITSM, ktorý je zodpovedný za včasnú detekciu incidentov, ich zaznamenávanie a riadenie ich životného cyklu. IM sa zaoberá všetkými incidentmi, čo zahŕňa zlyhania, otázky a dotazy oznámené užívateľmi, technickou podporou alebo automaticky detekované a zaznamenané nástrojmi na monitorovanie udalostí. V ITIL terminológii je *incident* definovaný ako akákoľvek udalosť, ktorá nie je súčasťou štandardnej činnosti IT služby a ktorá spôsobí alebo môže spôsobiť prerušenie IT služby, prípadne zníženie kvality IT služby. Taktiež zlyhanie konfiguračnej položky, ktorá ešte neovplyvňuje IT službu, sa označuje ako incident. V zásade IM vôbec neskúma prečo k incidentom dochádza, ale hľadá akékoľvek riešenie vedúce k obnoveniu služby. Jedná sa o jednu z najdôležitejších častí riadenia IT, najmä kvôli jej tzv. „vysokej viditeľnosti“ pre biznis. Inými slovami, je veľmi ľahké demonštrovať hodnotu tohoto procesu pre zákazníka nakoľko sa proces zaoberá práve neštandardnými stavmi služby, ktorú od poskytovateľa kupuje.
ITIL špecifikuje ako hlavné ciele a hlavné aktivity tohto procesu nasledovne:
Obnoviť normálnu prevádzku služby, a to čo najrýchlejšie pri súčasnej minimalizácii dôsledkov výpadku služby na prevádzku (tzn. na zákazníkov a používateľov)
Zabezpečovať, aby služby dodávané zákazníkom spĺňali kvalitu podľa dohodnutých SLA

Normálnou prevádzkou služby tu rozumieme prevádzku služby v rámci SLA. Incidenty, ktoré nemôžu byť vyriešené priamo na Service desku (pozri kap. 6.), sú odtiaľ okamžite presmerované na špecialistov technickej podpory. Mnoho zaznamenaných incidentov nie je nových, ale zaoberajú sa niečím, čo sa stalo a riešilo už predtým, a môže sa to stať znovu. Preto vidia organizácie dôležitosť v preddefinovaných štandardných modeloch incidentov. Tie potom môžu priamo aplikovať na vzniknuté incidenty. Modely incidentov môžu zahŕňať kroky, ktoré je treba podniknúť pre spracovanie incidentov, zoznamy zodpovedných osôb za jednotlivé činnosti, eskalačné procedúry a kontakty, iné dôležité náležitosti. Modely by mali byť importované do podporných nástrojov pre prácu s incidentmi, aby mohli tieto nástroje zautomatizovať spracovanie incidentov aj proces eskalácie.

Procesný tok manažmentu incidentov vizualizuje nasledujúci procesný diagram (Obr.).



Obr. 17. Proces manažmentu incidentov.

Pokiaľ je to možné, všetky kľúčové komponenty by mali byť monitorované, aby v prípade zlyhania alebo možného zlyhania mohol byť incident čo najrýchlejšie identifikovaný a proces manažmentu incidentov čo najrýchlejšie spustený. Všetky incidenty musia byť dôkladne zalogované, musia byť zaznamenané všetky relevantné informácie o incidente, aby pomohli k vyriešeniu vzniknutého incidentu. Každý zalogovaný incident by mal obsahovať tieto potrebné informácie: unikátne referenčné číslo, kategorizáciu incidentu, naliehavosť incidentu, dopad incidentu, prioritu incidentu, dátum a čas zaznamenania, meno osoby, ktorá incident zaznamenala, metódu ohlásenia, kontakt na užívateľa na danej lokalite, popis príznakov incidentu, stav incidentu, meno riešiteľskej skupiny alebo riešiteľa, súvisiace problémy, riešiteľské aktivity, dátum a čas vyriešenia, kategória uzavretia, dátum a čas uzavretia incidentu.

Počiatočné zaznamenanie musí obsahovať aj informáciu o kategorizácii incidentu pre štatistické účely. Klasifikácia incidentov, (samozrejme iba v prípade, ak sa nejedná o servisnú požiadavku) je dôležitá z hľadiska správneho určenia služieb IT a komponentov IT infraštruktúry, ktorých sa incident týka. Týmto je možné stanoviť prioritu riešenia a prípadne ďalšie vzťahy, ktoré môžu byť použité pri porovnávaní s databázou známych chýb. Mnoho nástrojov umožňuje aj viacúrovňovú kategorizáciu incidentov. Ďalším dôležitým aspektom je stanovenie priority incidentu, ktorá sa používa pri určení relatívnej dôležitosti incidentu. Je založená na dopade a závažnosti a zvykne identifikovať čas, ktorý si činnosti vyžadujú. Dopad predstavuje mieru vplyvu incidentu, problému alebo zmeny na podnikové procesy. Dopad sa často zakladá na tom, ako budú ovplyvnené úrovne služieb. Na druhej strane naliehavosť je miera, ktorá vyjadruje dobu potrebnú pre incident, problém alebo zmenu (napr. vysoko významný incident môže mať nízku naliehavosť, ak sa dopad neprejaví do konca finančného roka). Existuje niekoľko stupňov dopadu:

malý vplyv (3) – služba je degradovaná, ale stále funguje v rámci SLA špecifikácií;

stredný vplyv (2) – služba nepracuje v rámci dohodnutej úrovne služieb, vykonáva sa len minimálna úroveň;

vysoký vplyv (1) – služba nie je k dispozícií.

Rovnako, závažnosť incidentu, resp. miera do akej výsledok môže byť odložený, môže byť klasifikovaná nasledovne:

malá (3) – incident zabráni používateľovi vykonávať svoje povinnosti;

stredná (2) – incident zabráni užívateľovi vykonávať časovo kritické funkcie;

vysoká (1) – služba alebo hlavná časť služby nie je k dispozícií.

Prvotná klasifikácia nemusí byť definitívna a v priebehu riešenia môže byť aktualizovaná podľa novo zistených skutočností.

Určenie priority incidentu		Vplyv "Impact"		
		Vysoký	Stredný	Malý
Závažnosť "Urgency"	Vysoká	1	2	3
	Stredná	2	3	4
	Malá	3	4	5

Obr. 18 Prioritizácia incidentu

Závažný incident (Major incident) predstavuje najvyššiu kategóriu vplyvu na mimoriadnu udalosť. Takýto incident vedie k významnému narušeniu podnikania a má kritický dopad na zákazníka. Takéto typy incidentov nepodliehajú štandardnému pracovnému toku procesu pre ostatné incidenty. Spravocanie závažných incidentov je v procesných diagramoch reprezentované samotnou aktivitou. Určenie typu incidentu vykoná Service desk na základe klasifikácie – môže to byť Servisná požiadavka, incident so známym postupom riešenia, alebo incident, u ktorého je riešenie doteraz neznáme. V prípade Servisnej požiadavky sa použije štandardný postup (Spracovanie požiadaviek) a požiadavka je vo väčšine prípadov vyriešená a následne uzavretá hneď v prvej úrovni podpory, alebo sa presunie k vyriešeniu pracovníkovi druhej úrovne podpory. Rovnako sa postupuje u incidentov, u ktorých je známy postup riešenia. V prípade, že pre vzniknutý incident nie je známe priame riešenie, nasledujú aktivity, ktoré spoločne vykonávajú Manažment incidentov s Manažmentom problémov. V tomto procese sa príznaky incidentu porovnávajú s databázou známych chýb (Known Error DB). Pokiaľ je niektorej príčine (Známej chybe) priradený, je v databáze nájdené aj zapísané riešenie, pracovník Service desku buď priamo zákazníka o riešení informuje, alebo riešenie priradí špecializovanej skupine podpory. Ak nedôjde k úspešnému priradeniu k niektorej zo

známych chýb, porovná sa incident s databázou problémov, kde sa vyšetruje, či existujú incidenty, ktoré vykazujú rovnaké príznaky a dá sa tak predpokladať, že sú spôsobené rovnakým, ešte nevyriešeným problémom. Obe znalostné bázy (Known Error DB a Problem DB) spravuje Manažment problémov. Ak ani v jednej nedôjde k nájdeniu odpovedajúceho záznamu, je vytvorený nový problém v databáze problémov a je o ňom informovaný Manažment problémov, ktorý ďalej riadi aktivity s ním spojené.

Pri zisťovaní príčin incidentu môže dôjsť k *eskalácii* – aktivite, ktorá zaistí dodatočné zdroje, ak sú potrebné na dosiahnutie cieľovej úrovne služieb alebo očakávaní zákazníka. Existujú dva typy eskalácie, ***funkčná*** eskalácia a *hierarchická* eskalácia. Funkčná eskalácia presúva riešenie incidentu, problému alebo zmeny na technický tím, ktorý je v rámci organizácie na vyššom stupni odbornej znalosti. Hierarchická eskalácia je naproti tomu proces informovania alebo zapojenia viacerých nadriadených úrovní manažmentu pri riešení eskalácie. Oba typy eskalácie je možné vykonávať manuálne alebo zavedením automatickej eskalácie. Automatická eskalácia je väčšinou vedená na základe prekročenia časového limitu pre riešenie incidentu, preto je v tomto prípade nutné zaznamenávať i čas strávený nad jeho riešením, rovnako je podmienená vlastníctvom vhodného softvérového nástroja, ktorý automatizáciu umožňuje.

Podporné riešiteľské skupiny incident podrobne preskúmajú a vykonajú potrebnú diagnostiku incidentu. Detaily z týchto činností a zistení priebežne dokumentujú v záznamoch o incidente. Keď sa objaví možné riešenie, aplikuje sa na incident a otestuje sa správnosť riešenia. Môže ísť o dočasné riešenie (tzv. workaround) alebo jednoduchú permanentnú úpravu. Ak sú potrebné zmeny v infraštruktúre, aby sa už incidenty rovnakého typu viac neobjavovali, je do systému vložená Požiadavka na zmenu a zmena je potom riešená v rámci procesu Manažment zmien. Potom je ešte potrebné uistiť sa, či bola obnova funkčnosti služby kompletná. Posledným krokom je uzavretie incidentu, ktoré vykonáva Service desk po overení úspešnosti vyriešenia incidentu so zákazníkom. Neriadené incidenty sa “strácajú”, pri zle riadených incidentoch sa predlžuje doba ich odstránenia, a tým sa predlžuje aj doba výpadku služby. Neexistencia eskalačných procedúr spôsobuje, že sa z drobných incidentov stávajú incidenty závažné, ktoré významne ovplyvňujú kvalitu služieb. Špecialisti v skupinách podpory sú neustále vyrušovaní zo svojej práce, a tým sa dostávajú do časového tlaku. Vyrušovanie pracovníkov obchodu, na ktorých sa obracajú ich

kolegovia so žiadosťou o radu. Manažment incidentov je zodpovedný za včasnú detekciu incidentov, ich zaznamenávanie a riadenie ich životného cyklu. Úlohou procesu je zaistiť čo najrýchlejšie obnovenie dodávky služby a minimalizovať dôsledky výpadku služby na obchodnú činnosť. Často ide len o implementáciu dočasného náhradného riešenia, ktoré ma za úlohu čo najrýchlejšie aspoň čiastočne sprístupniť dotknutú službu. Jeho cieľom je "byť čo najrýchlejší" a proces v zásade vôbec neskúma prečo k incidentom dochádza, ale hľadá akékoľvek riešenie vedúce k obnoveniu služby (za hľadanie príčin incidentov je zodpovedný proces manažmentu problémov).

Ciele a prínosy implementácie manažmentu incidentov

Pre obchodné podnikanie organizácie je možné sformulovať niekoľko zásadných prínosy implementácie tohto procesu. Medzi hlavnými je schopnosť detekovať a riešiť incidenty, ktorá vedie k zvýšeniu dostupnost poskytovaných služieb. Správnym zavedením štandardizovaných procesov je možné znížiť čas potrebný na reakciu, keď k incidentu dôjde. Pochopením, prečo incidenty vznikajú je zase možné hnachádzať možnosti ako vylepšiť samotné služby.

Pri nasadzovaní procesu je však potrebné dbať na niekoľko problémov, ktoré pri implementácii v reálnom prostredí môžu nastať. Jedná sa o obchádzanie procesných krokov zamestnancami, ale aj samotnými používateľmi služby a tým spôsobená strata cenných informácií o nezaznamenaných incidentoch, ktorá by následne mohla byť vhodná pri analýzach počas manažmentu problémov, alebo manažmente zmien. Rovnako môže problémy spôsobiť aj neodhadnutie kapacity Service Desku, ktoré môže viesť k jeho zahlteniu a preťaženiu vplyvom priveľkého množstva incidentov a z toho vyplývajúce problémy s ich nepresnou evidenciou a nevhodnými riešeniami. Pri realizácii týchto činností sa rovnako prejavia aj chyby v katalógu služieb, či nepresne a nejasne definované zmluvy SLA resp. OLA.

Na druhej strane, pre úsek informačných technológii môžu byť zaujímavé tieto prínosy:

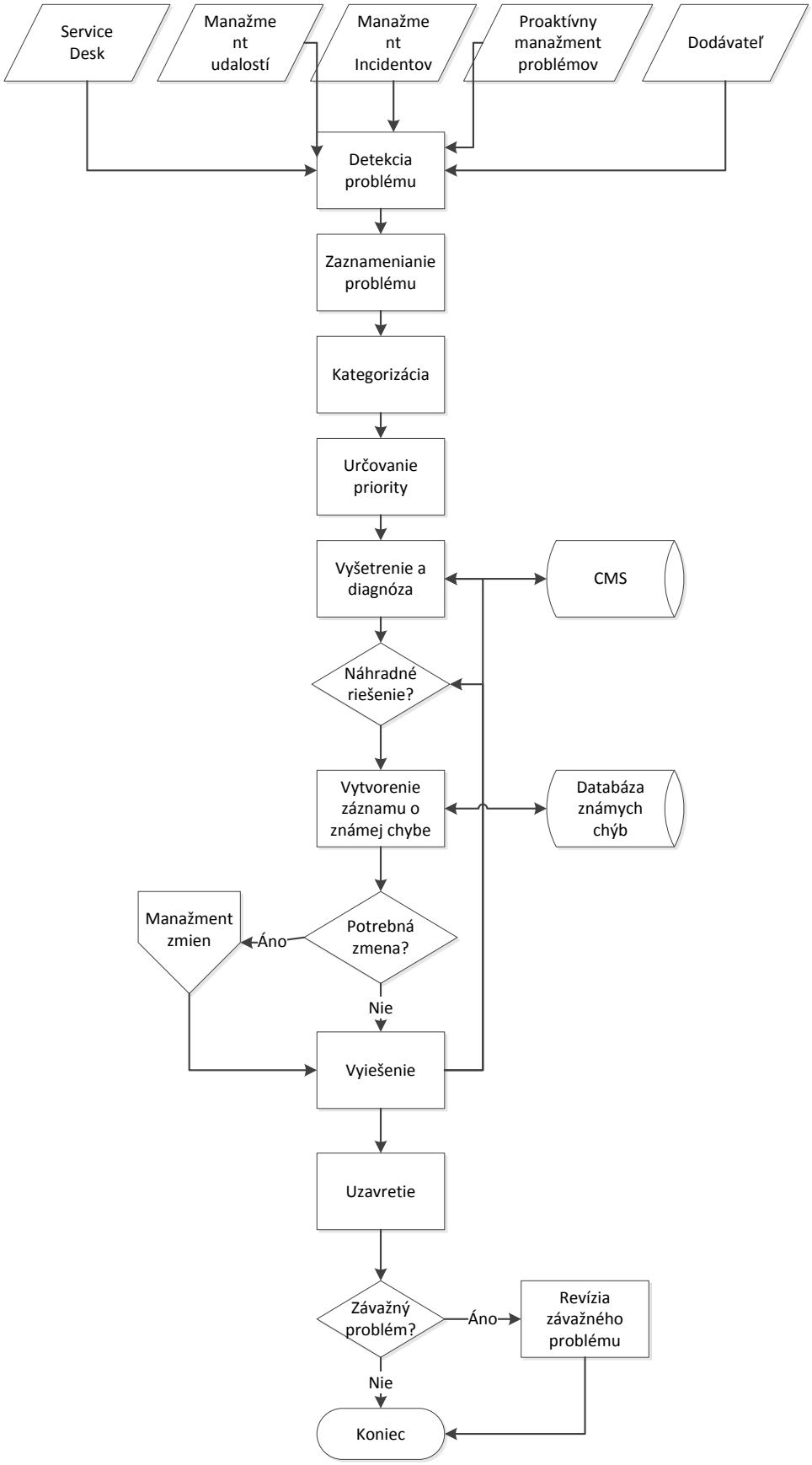
- Presné meranie miery plnenia SLA
- Manažérske informácie o aspektoch kvality služieb
- Lepšie využitie zdrojov, zvýšenie efektivity práce
- Eliminácia "stratených incidentov"

- Vierohodnejší obsah CMDB
- Zvýšenie spokojnosti zákazníkov a používateľov

Manažment problémov

Manažment problémov (Problem management) je proces, ktorého cieľom je identifikácia problémov problémov a ich incidentom, ktoré spôsobujú. ITIL tu definuje problém ako neznámu a základnú príčinu jedného alebo viacerých incidentov. Príčina spravidla nie je známa v dobe, kedy je vytváraný záznam o probléme. Manažment incidentov má minimalizovať dopady u tých incidentov, ktorým sa nedá zabrániť. Diagnostikuje ich príčiny a stanovuje riešenia, pre ich odstránenie. Problém by mal byť vytvorený vždy, keď sa incident alebo skupina incidentov vyrieši len dočasným náhradným riešením, aby sa čo najrýchlejšie zabezpečila funkčnosť produkčnej prevádzky. Vtedy je už známe dočasné náhradné riešenie incidentu (napríklad sa problém dočasne vyrieši vypnutím a novým naštartovaním servera) a jeho opätovný vznik už nemá taký veľký vplyv na produkciu. Preto má Manažment problémov priestor a čas na analýzu opakujúceho sa incidentu, nájdenie a elimináciu jeho hlavnej príčiny. Rola Manažéra problémov by sa nemala prekrývať s rolou Manažéra incidentov, pretože musia mať na rovnakú vec rozdielny pohľad. Manažérovi incidentov ide o rýchlosť riešenia a manažérovi problémov o jeho kvalitu. Problémov v organizácii vzniká rádovo menej ako incidentov, preto je možné, aby riešitelia Manažmentu incidentov boli zároveň riešiteľmi problémov. V takom prípade by ale mali mať presne zadefinované časy, kedy sa ktorej z činností venujú, aby nevznikol problém s nekonečným odsúvaním riešenia problémov kvôli vždy práve dôležitejším incidentom. Organizácia môže posúdiť potrebu zdieľania či rozdelenia zamestnancov medzi manažmenty podľa pomeru vzniknutých incidentov k problémom v testovacej prevádzke zákazníckeho centra.Podnik je schopný reagovať na problémy až po tom, keď už došlo k prerušeniu dodávky služby zákazníkom (ak keď v organizácii proces manažmentu problémov neexistuje, obvykle sa určitá skupina pracovníkov podpory zaoberá hľadaním príčin problémov a ich štrukturálnym riešeniam, ale väčšinou až potom, keď dôsledok opakujúcich sa incidentov a

dôsledok výpadkov prekročí istú



Obr. 17. Proces manažmentu problémov

únosnú mieru - tzn. obvykle na popud manažmentu podniku). Neustálym opakovaním sa stále rovnakých incidentov stráca organizácia dôveru svojich zákazníkov v kvalitu svojich služieb. Neexistencia štrukturálnych riešení a nutnosť opakovane riešiť stále rovnaké incidenty domotivuje personál a zvyšuje fluktuáciu, čím sa podpora užívateľov stáva vysoko neefektívna s vysokými nákladmi.

Cieľom implementácie procesu manažmentu problémov teda je je:

- Zabrániť opakovaniu Incidentov súvisiacich s poruchami. Tento cieľ dosahuje proces tým, že analyzuje incidenty, snaží sa nájsť ich základnú príčinu a následne iniciuje kroky vedúce k náprave
- Minimalizovať obchodný dopad incidentov a problémov spôsobených poruchami ICT infraštruktúry a zaistiť účelné využívanie zdrojov
- Starať sa o znalostnú bázu a informácie v nej uložené sprístupňovať špecialistom podpory v procese manažmentu incidentov a pracovníkom Service desku.

Manažment problémov svojou činnosťou tak v podstate zaisťuje stabilitu IT infraštruktúry.

Medzi hlavné prínosy implementácie tohto procesu patria:

- Zvýšenie kvality IT služieb (naštartovanie cyklu neustáleho zlepšovania kvality)
- Zníženie počtu incidentov (vďaka zisteniu a odstráneniu ich základných príčin)
- Trvalé štrukturálne riešenie, zaisťovanie stability infraštruktúry
- Zvýšenie úspešnosti Service Desku v ukazovateli tzv. first-time fix (ako dôsledok doplňovania znalostnej databáze)

Proces manažmentu problémov ako ho definuje ITIL je možné vidieť na obr. 17. Proces je spustený detekciou samotného problému. To, akým spôsobom je problém detekovaný, závisí na konkrétnej situácii. Problém môže byť detekovaný Service Deskom, udalosť v procese manažmentu udalostí môže byť ako problém

identifikovaná, môže vyplynúť z riešenia incidentu, alebo môže byť výsledkom tzn. proaktívneho manažmentu problémov, čo predstavuje aktivity pre nachádzanie problémov ešte predtým, ako spôsobia incident.

Problém sa potom spracováva podobne ako udalosť, či incident. Ukladá sa do databázy spolu s informáciami o čase výskytu, službe, ktorej sa môže týkať, konfiguračných položiek, ale aj informáciami o incidentoch, ktoré môžu byť naviazané na tento problém (ak také sú). Prebehne prioritizácia a kategorizácia problému, kde sa navyše k ostatným procesom prevádzky služby predvída, ako náročné bude riešenie problému (časovo aj finančne) a odhaduje sa personál potrebný na vyriešenie problému. Do úvahy sa taktiež berie aj spôsob jeho vyriešenia – či bude na základe dostupných informácií vhodnejšia náhrada systému, resp. jeho časti, alebo oprava.

Na analýzu a vyriešenie problému sa používajú štandardné metódy, vrátane analytických a štatistických metód, analýz časových radov, brainstorming a podobne. Cieľom je tu aplikovať trvalé riešnenie na rozdiel od manažmentu incidentov, kde sa v snahe čo najrýchlejšie obnoviť dodávku služby používajú riešenia dočasné.

Pre každú zámu chybu musí byť existovať záznam v databáze známych chýb. Známa chyba (Known error) je tu definovaná ako incident, alebo problém, pre ktorý je známa hlavná príčina vzniku a pre ktorý už existuje dočasné náhradné riešenie, alebo už bola v minulosti zaistená trvalá náhrada. Incidenya a problémy, ktoré sa opakujú je takto možno efektívne riešiť pomocou znalostí uložených v tejto báze.

Pre odstránenie problému a jeho celkové vyriešenie sú niekedy nevyhnutné zmeny v infraštruktúre, resp. zmeny jednotlivých komponentov. Tieto zodpovedajú zmenám konfiguračných položiek v CMDB, čo si môže vyžiadať naplánovanie a implementáciu zmeny tak, ako je popísaná v časti Prechod služby. Po implementácii zmien (ak sú potrebné) je aplikované riešenie problému, ktorý sa následne uzavrie. Uzatvorenie problému by malo obsahovať informácie o krokoch, ktoré k jeho riešeniu viedli. To zahŕňa rovnako sled správnych aktivít, ktoré k riešeniu prispeli, ale takisto aj nesprávne zvolené kroky. Tie sú podstatné pre ďalšie možnosti využitia týchto informácií a odvodenie znalostí, ako by problém mohol byť vyriešený

lepšie v prípade, že sa v budúcnosti zopakuje. Ostatné informácie získané v procese analýzy a riešenia problému môžu slúžiť aj ako prevencia zopakovania sa problému.

Vo všeobecnosti je možné zhrnúť dva aspekty prístupu k manažmentu problémov. Ten sa skladá z reaktívnych činností, ktoré sú zväčša súčasťou popisovaného procesného modelu. Jedná sa o identifikáciu a zaznamenávanie problémov analýzou detailov jednotlivých incidentov. Medzi reaktívne činnosti patrí aj poskytovanie odporúčaní a poradenstva smerom k manažmentu incidentov spolu s informáciami o náhradných dočasných riešeniach, ktoré boli identifikované, rovnako ako aj s riešeniami známych chýb. Nemalým prostriedkom, ktorý napomáha sú aj dokumentácie a výkazy obsahujúce postupy pri riešení problémov. Z preventívnych činností sú podstatné aktivity smerujúce k identifikácii trendov, ktoré môžu viesť k potenciálnym problémom a odhaliť tak ich zdroje v predstihu, predtým, ako dôjde k samotnému incidentu. Do týchto aktivít spadá aj návrh a implementácia rôznych preventívnch opatrení, ktorých cieľom je vyhnúť sa možným problémom v budúcnosti. Sem spadá napr. rozširovanie a aktualizácia systémov.

Manažment problémov je oblasť úzko prepojená s manažmentom incidentov. Tu môžu v prevádzke nastať aj niektoré problémy späté s nedôslednou, resp. chýbajúcou väzbou medzi nimi. Vzájomné prepojenie je nutné najmä medzi záznamami o incidentoch a informáciami o problémoch. Časté je rovnako aj slabé vzájomné informovanie o známych chybách medzi vývojárskym a produkčným prostredím. Aplikačný softvér a technickú infraštruktúru prechádzajúcu do produkčného prostredia by mala sprevádzať informácia o známych chybách. Takáto informácia v budúcnosti ušetrí čas strávený nad hľadaním príčiny chyby, ktorá už je vlastne známa.

Spracovanie požiadaviek

Proces spracovania požiadaviek umožňuje používateľom prijímať a žiadať o štandardné služby. *Servisná požiadavka* (Service Request) používateľa predstavuje požiadavku o informácie, rady, štandardné zmeny, alebo o prístup k IT službe. Proces má používateľom poskytovať informácie o službách a tiež o postupoch, ktoré sú spojené so získavaním služieb. Umožňuje používateľom vyžiadať si použitie

služby a prijímať štandardné služby. Servisné požiadavky sú sledované a archivované. V tomto procese sa môžeme stretnúť aj s modelmi požiadaviek, ktoré definujú často sa vyskytujúce požiadavky a spôsob ich jednotného spracovávania. Používatelia generujú servisné požiadavky spolu so zoznamom očakávaní, ktoré je pred samotným vykonaním procesu nutné schváliť a vykonávanie samotného procesu závisí od typu požiadavky. Ak by sme to mohli zhrnúť, účelom tohoto procesu je:

- Umožniť používateľom vyžiadať si použitie služby
- Príjmať štandardné služby
- Poskytovať informácie o službách používateľom, rovnako ako aj informácie o postupoch pre ich získanie

Vyšším cieľom tohoto procesu je aj redukovať byrokraciu v organizácii spojenú s poskytovaním služieb. Tá sa redukuje aj vďaka modelom požiadaviek (Request models). Tieto spočívajú v podstate v jasnej definícii požiadaviek, ktoré sa vyskytujú najčastejšie a spôsobu ich jednotného a konzistentného spracovávania.

Samotný proces je v ITIL popísaný nasledovne. Pozostáva z niekoľkých hrubých krokov. Prvým je generovanie samotnej požiadavky od používateľa. Najčastejším spôsobom ako toho docieliť je vygenerovať požiadavku priamo v nástroji pre podporu IT riadenia. Tieto častokrát obsahujú interfejs umožňujúci zvoliť rôzne typy požiadaviek z poskytovaných a podporovaných typov. Vstupom by mal byť aj zoznam splnených očakávaní.

Pred samotným vykonaním procesu je nutné požiadavku schváliť. Schvaľovanie požiadaviek môžme rozdeliť do dvoch základných typov. Prvým je finančné schvaľovanie, ktoré predstavuje typ schvaľovania, ktorý je nutné vykonať pri každej požiadavke. Tieto totiž môžu mať finančný dopad na organizáciu poskytujúcu IT služby, z toho dôvodu je potrebné zakaždým tento krok vykonať. Ostatné typy schvaľovaní sú nepovinné a poväčšinou špecifické pre konkrétnu implementáciu v procese. Pri návrhu procesu schvaľovania požiadaviek preto netreba zabúdať na ich definíciu.

Posledným krokom je samotné vykonanie požiadavky, v prípade, že táto bola schválená. Typ vykonania je závislý na povahe požiadavky. Tie jednoduché je možné riešiť priamo na Service Desku a je za ne zodpovedná prvá línia podpory. Tie zložitejšie si môžu vyžadovať eskaláciu na vyššiu úroveň, alebo špecializovaný personál.

Správa prístupov

Proces *Správy prístupov* (Access management) riadi práva používateľov tak, aby boli schopní pristupovať k službe, alebo určitej skupine služieb, ale zároveň, aby prístup nebol umožnený neautorizovaným používateľom. Táto oblasť sa prekrýva s oblasťou informačnej bezpečnosti a dôvery. Celý proces definuje niekoľko konceptov:

- Identita individuí
- Práva prístupu
- Overovanie identity a práv prístupu

Hlavným cieľom je zvýšiť efektivitu využívania poskytovaných služieb a to tak, že bude zabezpečený prístupu a autorizácia k týmto službám. Súčasťou procesu je minimalizovať s tým spojené chyby a schopnosť jednoducho odhaliť nekorektné použitie služby.

Samotný proces pozostáva z niekoľkých krokov. Prístup je vyžiadaný používateľom a následne je verifikovaný. Verifikácia je overenie toho, či používateľ je skutočne ten, za ktorého sa vydáva (napr. login a heslo) a či vlastní legitímne oprávnenie na používanie služby. ITIL konkrétne metódy nešpecifikuje, spomína iba viacero rôznych typov verifikácie podľa typu požiadavky, napr. autorizáciu služby od určitého stupňa, či definíciu politík, ktoré stanovujú oprávnenia používateľov k službám. So samotným procesom úzko súvisia aj monitorovacie aktivity stavu identity používateľa. Toto je spojené najmä s úkonmi súvisiacimi so zmenami prístupu k službám po určitej udalosti, napr. povýšenie/degradácia, odchod do dôchodku, či disciplinárne akcie, kedy sa stav prístupu k službe môže dočasne alebo trvalo zmeniť.

Service Desk

V úvode tejto kapitoly sme spomenuli *Service Desk* ako jeden z najdôležitejších konceptov, ktoré ITIL v časti Prevádzka služby popisuje. Service Desk predstavuje najdôležitejšiu časť IT oddelenia v organizácii, pretože poskytuje primárny centrálny bod kontaktu pre všetkých používateľov s IT. Service desk je zároveň tzv. „*Single Point of Contact"*, teda jednotný kontaktný bod medzi poskytovateľom služieb a používateľom služieb. Primárne slúži na zaznamenávanie a riadenie všetkých prichádzajúcich incidentov a požiadaviek zákazníka. Tieto transformuje na vstupy do jednotlivých procesov IT riadenia, môžme tak povedať, že je rozhraním pre ostatné procesy a aktivity Prevádzky služieb.

Service desk je teda miesto, kde sa odohráva komunikácia so zákazníkom. Navyše je Service Desk nástrojom komplexnej integrácie ďalších procesov v manažmente IT služieb, ktorý dodáva rozmedzie pre jeho aktivity a je zdrojom informácii medzi vzájomne prepojenými vzťahmi týchto procesov a ich týkajúcich sa činnosti. Zo strategického hľadiska je Service Desk najdôležitejším miestom v organizácii. Pre zákazníka a používateľa je Service Desk jediným oknom do organizácie - úroveň poskytovaných služieb, profesionalita a odbornosť pracovníkov organizácie je používateľmi a zákazníkmi meraná ich pohľadom na fungovanie Service Desku a podľa technických aspektov a parametrov infraštruktúry hoci aj tej najvyššej úrovne. Pracovníci Service desku sú zodpovední na aktivity príjmania, zaznamenávania, prioritizácie tzv. volaní, alebo „service calls". Service desk predstavuje aj prvú líniu podpory pri manažmente incidentov. Realizuje eskaláciu v rámci organizácie a má za úloju aj sledovanie a monitoring statusu všetkých registrovaných volaní. Jeho úlohou je neustále informovať zákazníka o priebehu a stave jeho požiadavky, statuse v akom sa nachádza a progrese vybavovania. Koordinuje druhú líniu podporty pri eskalácii rovnako ako aj podporu tretích strán. Service desk je zodpovedný aj za uzatváranie volaní a následnú komunikáciu so zákazníkom za účelom získania spätnej väzby.

Z hľadiska organizačnej štruktúry nie je Service desk novou myšlienkou. Callcentrum je podniková jednotka, ktorá sa zameriava na kvalifikovanú obsluhu veľkého množstva prichádzajúcich alebo odchádzajúcich telefonických volaní, prípadne e-mailov. Otázky a požiadavky zákazníkov a používateľov služieb rieši reaktívnym spôsobom, čo znamená, že sa buď okamžite vyriešia, poskytnú odpoveď alebo sa eskalujú. Podobne Helpdesk predstavuje kontaktný bod pre používateľov, kde môžu

zaznamenávať hlásenia. Helpdesk je zvyčajne viac technicky zameraný než Service Desk a neposkytuje jednotný kontaktný bod pre všetky interakcie. Úloha pracoviska Service Desk je oproti Callcentru a Helpdesku rozmanitejšia. Zahŕňa v sebe funkcie predošlých kategórií a pridáva mnohé ďalšie. Zahŕňa v sebe totiž pohľad na IT ako na služby a umožňuje integráciu IT procesoc do infraštruktúry riadenia. Navyše dojem používateľov a zákazníkov zo Service Desku je celkovým dojmom z celého IT oddelenia.

Medzi prínosy zavedenia takéhoto riešenia do podniku patria:

- Zvýšenie spokojnosti zákazníkov
- Zvýšenie dostupnosti podpory, zlepšenie komunikácie
- Vyššia kvalita a rýchlosť vybavovania požiadaviek
- Zlepšenie tímovej práce a internej komunikácie
- Proaktívny prístup k poskytovaniu služieb
- Minimalizácia negatívnych dopadov
- Lepšie riadenie infraštruktúry
- Lepšie využitie IKT zdrojov, zvýšenie produktivity
- Dostupnosť informácií s vyššou vypovedajúcou hodnotou

Dôsledky ne-existencie štrukturálneho riešenia podpory:

- Nízka spokojnosť zákazníkov i vlastného personálu
- Nesystémové riadenie pracovníkov podpory
- Nepretržité "hasenie požiarov"
- Opakujúce sa riešenia rovnakých incidentov a problémov
- Závislosť na kľúčových zamestnancoch
- Nekoordinované a neriadené zmeny sú bežnou záležitosťou
- Neschopnosť reagovať na nové obchodné požiadavky
- Nejasné a nepreukázateľné vyťaženie zdrojov

Podľa toho, ako je samotný Service desk organizovaný ITIL definuje niekoľko rôznych druhov Service desku.

Lokálny service desk

Charakteristickým znakom je to, že je fyzicky umiestnený blízko používateľov. Jeho hlavnou výhodou je tzv. „visible presence“, teda akási fyzická prítomnosť pre používateľov. Je vhodný predovšetkým pre menšie organizácie, v ktorých sa pracovníci podpory nachádzajú v rovnakej lokalite ako služby, ktoré podporujú. Pre organizácie, ktoré potrebujú podporu vo viacerých lokalitách, sa stáva nepraktickým, pretože dochádza k zvyšovaniu nákladov. Tie sa prejavujú hlavne v nadbytočných zdrojoch rovnakého charakteru (ľudia, znalosti, zručnosti). Dôležité je tiež zaistiť kompatibilitu hardvérových a softvérových nástrojov s aplikovaním rovnakých aktivít a procesov. Nedostatkom je tiež zložitá orientácia používateľov služieb, ktorí nevedia, aké IT oddelenie majú v prípade vzniknutých problémov, incidentov alebo servisných požiadaviek kontaktovať. Medzi dôvody, kedy zvoliť lokálny Service desk patria napr. podpora podnikových jednotiek v krajinách so špecifikcými kultúrnymi rozdielmi, prípadne iným jazykom, tvorba lokálnych Service deskov so špecializovaným personálom pre riešenie iba určitého typu hlásením, alebo špecializovaný lokálny Service desk pre kritických používateľov.

Centrálny service desk

Táto forma je prispôsobená pre prijímanie a zaznamenávanie všetkých servisných požiadaviek a vzniknutých incidentov na jednom fyzickom mieste, pričom pracovníci podpory sa môžu nachádzať v rozdielnych lokalitách. Používateľovi umožňuje kontaktovať jedno centrálne miesto, ktoré vzniknuté incidenty a servisné požiadavky buď priamo vyrieši, prípadne ich posunie ďalšej úrovni podpory, ktoré je zvyčajne viac technicky orientované. Používatelia vedia, koho majú v takýchto situáciách kontaktovať, pretože tieto problémy riešia priamo pracovníci Service Desku. Redukuje sa tak počet Service Deskov do jedného, podporujú všetkých používateľov, zvyšuje sa efektivita využitých nákladov.

Virtuálny service desk

Pre organizácie, ktoré majú svoje pobočky nielen doma, ale aj v zahraničí, je vhodnou alternatívou virtuálny Service desk. Samotné zvýšenie efektivity podpory IT služieb, ako aj zníženie nákladov, je prospešné zaistiť jednou globálnou podporou, ktorá bude zdieľať informácie, používať jeden komunikačný jazyk a bude postupovať v rámci rovnako definovaných procesov. Výraz „virtuálny“ v tejto rovine definuje, že

neexistuje jedna centrálna fyzická lokalizácia Service desku, avšak podpora navonok ako jednotná vystupuje. Vytvára teda dojem jedného Service desku (napr. prístupom cez jedno tel. číslo, resp. e-mail kontakt), v skutočnosti jednotlivé Service desky geograficky distribuované. Musí sa však rátať s dostatočnou kapacitou a najmä so spoločnými procedúrami v rámci jednotlivých Service deskov. To miestami môže prinášať komplikácie vzhľadom na možnú existenciu kultúrnych rozdielov medzi jednotlivými lokalitami v ktorých sú Service desky umiestnené.

Špeciálnym typom virtuálneho Service desku je *Follow the sun*. Jedná sa skôr o metodológiu použitia Service Desk-ov a podporných skupín po celom svete na poskytovanie konzistentnej služby 24 hodín denne, 7 dní v týždni. Volania, incidenty, problémy a požiadavky na službu sa posúvajú medzi skupinami v rôznych časových pásmach.

Role Service desku

Kľúč k efektívnemu ITSM je zaistenie toho, že je jasná zodpovednosť a roly definované na vykonávanie praxe, postupov Prevádzky služieb. Rola je často zaviazaná k popisu práce alebo popisu pracovnej skupiny, ale nie sú nevyhnutne potrebné byť plnené, obsadené jedným jednotlivcom. Veľkosť organizácie, ako je štruktúrovaná, existencia vonkajších partnerov a iné faktory ovplyvnia ako sú roly priradené. Či je konkrétna rola plnená, obsadená jediným jedincom, osobou alebo zdieľaná medzi dvoma a viacerými, dôležitosť, význam je zhoda zodpovednosti a vykonávania popri interakcii s inými rolami v organizácii.

Service Desk Manažér – vo veľkých organizáciách, kde je pracovisko Service Desk dôležitou časťou, môže byť rola Service Desk Manažéra totožná s rolou Service Desk kontrolóra. V takých prípadoch táto rola môže prevziať zodpovednosť za riadenie aktivít v rámci celkového Service desku, hlásenie problémov pre Vyšší manažment, ktoré môžu mať podstatný dopad na biznis, preberanie zodpovednosti za incidenty a servisné požiadavky slúžiace na Service Desku.

Service Desk supervízor – vo veľmi malých oddeleniach je možné, že najvyšší Service desk analytik bude tiež pôsobiť ako supervízor – ale vo veľkých oddeleniach

je to pravdepodobne rola špecializovaného Service Desk supervízora, ktorá bude potrebná. Táto rola zahŕňa zaistenie rozdelenia pracovných funkcií, úrovní zručností, predstavujú eskaláčný bod v prípade niektorých volaní, tvorby štatistík a manažérskych hlásení. Ďalšou náplňou je reprezentácia pracoviska Service Desk na stretnutiach, úprava personálnych školení, spojenie s vyšším manažmentom a manažmentom služieb, realizovanie porád s personálom Service Desku. Asistuje analytikom v poskytovaní prvej línie podpory, ak je pracovná záťaž vysoká alebo ak sú vyžadované dodatočné skúsenosti.

Service Desk analytik – táto rola poskytuje prvú líniu podpory cez preberanie hovorov a narábanie s vyplývajúcimi incidentmi alebo servisnými požiadavkami používajúci ohlasujúce incidenty a procesy spracovania požiadaviek.

Superpoužívateľ (Superuser) – umožňuje komunikáciu medzi IT a biznisom na úrovni prevádzky, posilňuje očakávania používateľov s ohľadom na úroveň služieb, či boli odsúhlasené, tréning personálu pre používateľov v ich oblasti, poskytovanie podpory pre malé incidenty alebo jednoduché spracovanie požiadaviek

Meranie výkonnosti Service desku

Výkonnosť Service desku je možné merať dvoma spôsobmi. Metriky, tzv. „*hard performance*“ merajú výkon Service desku pomocou merateľných ukazovateľov a štatistík. Na druhej strane tzv. „*soft performance*“ metriky umožňujú zistiť ako na Service desk reagujú samotní používatelia služieb. Oba prístupy teda zohľadňujú rozdielne aspekty toho, ako Service desk funguje.

Pri prvej skupine je dôležité metriky definovať. Evaluácia Service desku musí byť jasne definovaná, ktorými metrikami a ako sa bude merať. Rovnako podstatné je zabezpečiť, aby merania prebiehali v pravidelných intervaloch. Metriky by mali byť zvolené realisticky vzhľadom na doménu poskytovaných služieb. Mali by byť volené tak, aby neviedli k nesprávnym, alebo mylným informáciám. Medzi najčastejšie používané ukazovatele výkonnosti Service desku patria tieto skupiny metrík:

- Množstvo vyriešení na prvej úrovni

  - Koľko volaní vyriešených počas prvého kontaktu so Service deskom
  - Koľko volaní vyriešených priamo na Service desk bez nutnosti iných skupín
- Priemerný čas na vyriešenie incidentu
- Priemerný čas potrebný na eskaláciu incidentu
- Priemerný čas na review a uzatvorenie incidentu
- Počet nesprávne priradených incidentov/požiadaviek
- Podiel používateľských updatov vykonaných mimo v SLA definovaných časoch
- Priemerné náklady Service Desku na spracovanie incidentu
  - Celkové náklady na Service desk/Počet volaní

Z nameraných metrík je potom možné stanoviť kľúčové ukazovatele výkonu (Key Performance Identifiers, KPI). Jedná sa o pomerové kritériá berúce metriky v kontexte ostatných. Medzi niektoré používané KPI pri evaluácii Service desku patria:

% úspešnosti vyriešených incidentov a požiadavok na službu (podľa kategórií a priorít)

% incidentov/požiadavok vyriešených na prvej úrovni

% nesprávne priradených incidentov a požiadavok na služby na druhej/tretej úrovni

% incidentov/požiadavok vyriešených bez návštevy používateľa

% znovuotvorených incidentov/požiadavok

% mimoriadne dlhých dôb riešenia

% neúspechu včasného vyriešenia incidentu/požiadavky

Evaluáciou Service desku „soft metrikami“ získavame spätnú väzbu od používateľov a obraz o tom, ako reagujú na Service desk. Sú realizované väčšinou dotazníkmi, alebo telefonickými prieskumami po uzavretí volania na Service desk. Voľba metód závisí na konkrétnej implementácii. Medzi najčastejšie implementované partia:

- After-Call Surveys – telefonické dotazník prebiehajúce hneď po volaní na Service desk, vysoká návratnosť, no obsah môže byť ovplyvnený negatívnym zážitkom (samotné volanie na Service desk z dôvodu vypadku služby)

- Outbound Phone Surveys - hovory so zákazníkmi, ktorí niekedy v minulosti kontaktovali Service desk, majú nižšiu návratnosť ako predchádzajúci spôsob, no vnem z komunikácie so Service deskom je zbavený počiatočných negatívnych emócií. Existuje tu aj možnosť kontaktovať špecifické skupiny používateľov, no respondentov môže rušiť a môže dôjsť k zmene vnímania celej komunikácie so Service deskom zo strany používateľa.
- Rozhovory – interviews sprostredkujú aj neverbálne informácie, respondenti majú celkovo lepší pocit, no negatívnou stránkou je časová náročnosť ich zorganizovania
- Skupinové rozhovory – sú výhodnejšie vzhľadom na možnosť osloviť väčšiu skupinu používateľov, no hrozí nemožnosť vypočutia všetkých názorov, rovnako ako aj zmena názorov v skupine
- Poštové/e-mailové dotazníky – poskytujú možnosť osloviť veľké skupiny, výhodou je anonymita, automatizácia, no negatívom nízky počet odpovedajúcich a možnosť zlej interpretácie odpovede
- On-line dotazníky

Záver

V tejto kapitole boli popísané základné koncepty fázy prechodu služby. Táto pokrýva implementáciu do prevádzkového prostredia vrátane testovania, samotného nasadenia, validácie a iných. Prakticky nadväzuje na predchádzajúcu kapitolu, vychádza z návrhu služieb. Výstupmi z tejto fázy potom sú samotné plány prechodu a nasadenia, otestované riešenia a zavedený a aktualizovaný SKMS. Publikácia sa venuje popisu taktýchto procesov nielen pre nové, ale aj pre služby zmenené. Na publikáciu popisujúcu prechod služby nadväzuje publikácia popisujúca fázu prevádzky služieb.

Nepretržité zlepšovanie služieb

Úvod

Nepretržité zlepšovanie služieb (Continual Service Improvment) zodpovedá za manažovanie zlepšení v procesoch riadenia IT služieb a v IT službách samotných. Na dosiahnutie požadovaných zlepšení ako napr. zvýšenie účinnosti, nákladovej efektívnosti, dostupnosti služby a pod. je potrebné kvalitu IT služieb kontinuálne merať, zisťovať aktuálnu úroveň služieb, priestor na ich zlepšenie ako aj dosiahnuté zlepšenia. Výsledky sa zaznamenávajú a zapracúvajú do procesov poskytovateľa, služieb a infraštruktúry IT, čím nepretržité zlepšovanie služieb nekončí.

Organizácie o zlepšovaní služieb hovoria mnoho rokov, ale u väčšiny zlepšovanie nebolo koncepčné a zostávalo len na hovorenej úrovni. Často sa ním začali zaoberať až po vzniku alebo prekonaní neúspechov, ktoré vážne ovplyvnili ich podnikanie. Nakoniec sa po vyriešení problémov použitá koncepcia dostávala do zabudnutia, nevyužívali sa v plnej miere zistenia z predchádzajúcich skúseností.

Organizácie bývajú často presvedčené, že potom ako prešli procesom vytvárania a definovania poskytovaných služieb a procesmi podporujúcimi realizáciu služieb, majú hlavnú časť riadenia a tvrdú prácu za sebou. Skutočná práca a dosahovanie požadovaných výsledkov prichádza až potom. Prostredníctvom informácii, dát a opatrení je možné zabezpečiť zlepšovanie nových ale aj zabehnutých poskytovaných služieb - vyžaduje si to ale vedomé rozhodnutia prijaté s jasne definovanými cieľmi, dokumentované postupy, vstupy, výstupy, identifikované role, kompetencie a zodpovednosti. Pre dosiahnutie úspechu, musí byť nepretržité zlepšovanie služieb začlenené do každej zložky organizácie s väzbami na hlavné potreby organizácie a plnenia obchodných plánov a cieľov.

Účel nepretržitého zlepšovania služieb

Hlavným účelom CSI je priebežne prispôsobovať IT služby meniacim sa potrebám podniku prostredníctvom identifikácie a zavádzania zlepšení, ktoré podporujú podnikové procesy. Tieto činnosti vedúce k zlepšeniam je nutné zavádzať počas celoživotného cyklu služby od samotnej stratégie služby, cez návrh a prechod služby až po jej prevádzku. V skutočnosti CSI je o hľadaní spôsobov, ako zlepšiť

proces a dosiahnuť vyššiu efektívnosť, dostupnosť, spoľahlivosť a ďalšie parametre kvality poskytovanej služby.

Ak procesy v organizácii nie sú známe, riadené a podporované pomocou jasne definovaných cieľov a príslušných meraní zameraných na zisťovanie aktuálneho stavu a plánovaných zlepšení, negatívne to vplýva na jej dlhodobé obchodné výsledky. V závislosti od konkrétnej IT služby môže organizácia znižovať svoje náklady, zvyšovať produktivitu, či dokonca predísť strate dobrého mena. To sú dôvody, prečo je veľmi dôležité poznať, zistiť a porozumieť, čo v danej organizácii merať, prečo to merať a vedieť definovať úspešný výsledok.

Ciele nepretržitého zlepšovania služieb

Aby bolo zlepšovanie IT služieb efektívne, musia sa pred jeho zavedením stanoviť ciele, ktoré sa majú dosiahnuť dôsledkom jeho zavedenia. Tieto ciele by mali byť zároveň špecifické, merateľné, dosiahnuteľné, realistické, časovo ohraničené (vychádza sa z metódy SMART) ako aj nadviazané na podnikateľské ciele. Bývajú zdokumentované v pláne zlepšovania služieb.

- preskúmať a analyzovať úrovne poskytovanej služby, so zameraním na analýzu, návrh a predkladanie príležitostí a odporúčaní na zlepšenie v každej fáze životného cyklu služby,
- identifikovať potenciálne zlepšenia kvality IT služieb a zavedenie vybraných zlepšení do jednotlivých činností procesov organizácie,
- merať účinnosť zavedených opatrení na zlepšenie kvality IT služieb
- zlepšiť súčasnú efektívnosť nákladov na poskytovanie IT služieb, bez negatívneho dopadu na spokojnosť zákazníkov,
- výber vhodných metód riadenia kvality a ich implementácia na podporu dlhodobého zlepšovania činností.

Zlepšenie služieb by sa malo aktívne riadiť a jeho vývoj je nutné monitorovať oproti formálne odsúhlaseným cieľom.

Pôsobnosť nepretržitého zlepšovania služieb v organizáciách

Ak má CSI priniesť úspech a merateľné výsledky, je dôležité pochopiť rôzne aktivity, ktoré do procesu zlepšovania služieb vstupujú alebo ho priamo podporujú:

■ riadenie informácií a trendov poukazujúcich na práve aktuálnu, očakávanú alebo požadovanú úroveň poskytovaných služieb IT,

■ pravidelné hodnotenie činností a výsledkov úloh realizačných procesov voči definovaným oblastiam zlepšovania, alebo naopak hodnotenie požadovaných oblastí zlepšenia voči realizovaným úlohám,

■ pravidelný výkon interných auditov zameraných na overenie plnenia poverených činností zamestnancov,

■ preskúmavanie existujúcich výsledkov získaných z meraní z pohľadu ich vypovedacej schopnosti a relevantnosti,

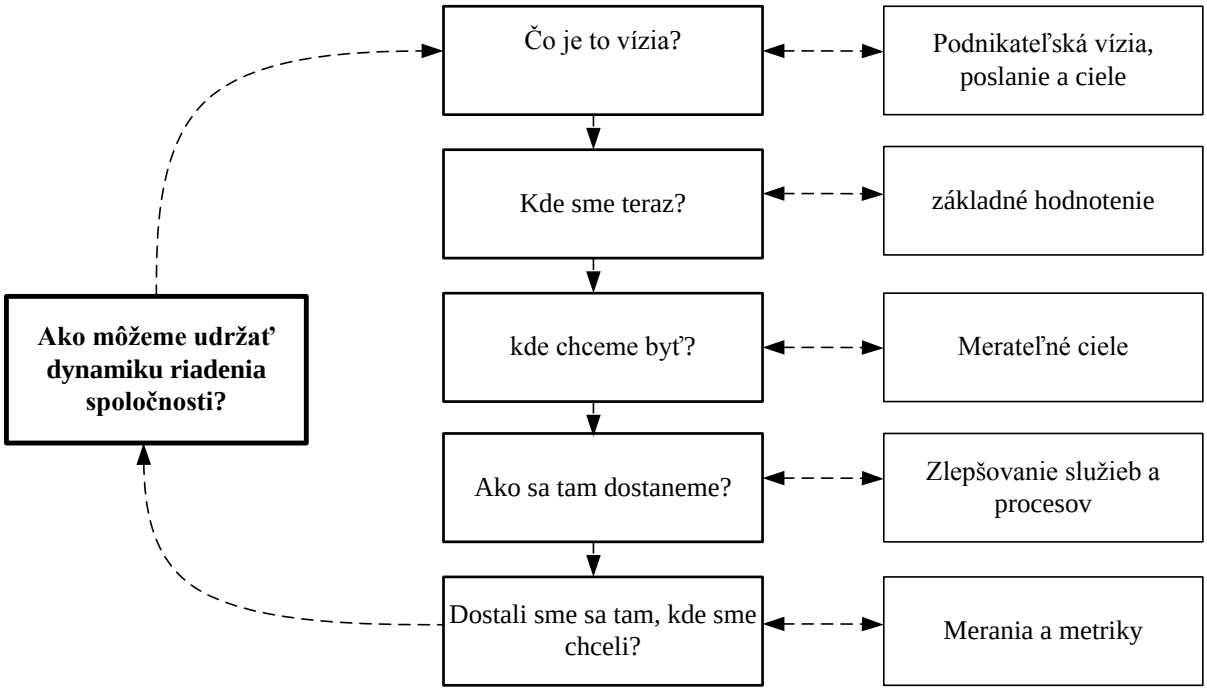
■ tvorba a navrhovanie okamžitých odporúčaní a ich predkladanie na schválenie,

■ pravidelný výkon prieskumu spokojnosti zákazníkov vhodne zvolenou formou, vyhodnocovanie jeho parametrov úspešnosti, očakávaní pred prieskumom a získané informácie analyzovať, preskúmavať a implementovať do návrhov odporúčaní,

■ vykonávanie preskúmavanie vonkajších a vnútorných služieb, ktoré identifikuje príležitosti na CSI.

Tieto činnosti sa v organizáciách nevykonávajú automaticky. V IT organizácii je z pravidla určená konkrétna osoba, tím pracovníkov alebo dokonca vybudované samostatné oddelenie schopné niesť zodpovednosť za dosiahnutie definovaných cieľov zlepšenia služieb. Ich činnosti musia byť taktiež plánované, riadené a pravidelne vyhodnocované, čím sa zlepšovanie služieb stáva procesom v rámci IT s definovanými činnosťami, vstupmi, výstupmi, parametrami, rolami a zodpovednosťami. Pri tom CSI musí zabezpečiť, aby všetky procesy organizácie boli navrhnuté a nasadené na priamu podporu správy služieb poskytovaných konečným zákazníkom. Výstupy z CSI musia byť preskúmavané, priebežne overované z pohľadu úplnosti, funkčnosti, relevantnosti, použiteľnosti a realizovateľnosti. Je tiež dôležité zabezpečiť, aby sledované parametre kvality a metriky dokázali identifikovať oblasti pre zlepšovanie procesu.

Vzhľadom k tomu, že sa v IT organizácii predpokladajú rôzne iniciatívy na zmeny procesov vychádzajúce z podnetov z vonka alebo z vnútra organizácie, proces kontinuálneho zlepšovania služieb je nutné vždy zaradiť hneď za procesom riadenia zmien.



Obr.18 Model nepretržitého zlepšovania služieb

Prístup a zmysel nepretržitého zlepšovania služieb

Ako bolo v predchádzajúcej časti naznačené, existuje mnoho príležitostí pre CSI. Je nutné si uvedomiť, že CSI je konštantný cyklus. Implementáciu procesu zlepšovania IT služieb možno zhrnúť do šiestich krokov:

■ 1. krok: prijať dlhodobé vízie požadovanej úrovne zlepšenia služieb a porozumieť im na najvyššej úrovni obchodných cieľov. Vízia by mala zosúladiť obchodné a IT stratégie.

■ 2. krok: na základe presne získaných a nezaujatých dôkazov, zhodnotiť súčasnú situáciu, kde sa organizácia práve nachádza (analýza z pohľadu organizácie, pracovníkov, procesov a technológií),

■ 3. krok: dohodnúť sa na prioritách a princípoch zlepšenia služieb vychádzajúcich z dlhodobej vízie cez stanovenie konkrétnych cieľov a kratšieho časového rámca.

■ 4. krok: vypracovať detailný plán CSI na dosiahnutie požadovanej kvality služieb v procesoch organizácie,

■ 5. krok: overiť, či budú navrhované činnosti, míľniky, stanovené úrovne služieb, merania a metriky podporovať samotné plnenie obchodných cieľov organizácie,

■ 6. krok: zabezpečiť implementáciu overených zmien v procesoch, za účelom zlepšenia alebo udržateľnosti kvality služieb.

Tak ako všetky činnosti aj CSI musí pre organizáciu preukázať svoj prínos, aby malo zmysel pokračovať vo svojej existencii. Je nutné definovať účel CSI s jasne identifikovanými výhodami a zrozumiteľným spôsobom dosiahnutia zlepšovania služieb. Často ide napr. o požadované zníženie nákladov pri zavádzaní služby, zvýšenie spokojnosti zákazníkov s poskytovaním existujúcich služieb, viac agility pri riešení požiadaviek zákazníkov nových služieb, alebo spoľahlivejšie IT služby na podporu hlavných obchodných procesov zákazníka.

IT organizácia musí porovnávať svoje náklady a príjmy z poskytovaných služieb. To sú pomerne jednoducho merateľné a dostupné parametre. Oveľa ťažšie je však exaktne kvantifikovať napr. zvýšenie príjmov organizácie v dôsledku implementácie plánu zlepšovania služieb alebo zavedenia niektorého odporúčania na zlepšenie.

Odberatelia IT služieb si čoraz viac uvedomujú dôležitosť informačných technológií a v niektorých prípadoch až závislosť na IT. Totiž poskytovatelia IT služieb sú súčasťou nie len obchodných operácií svojich zákazníkov, ale aj zmien, ktoré sa v nich dejú a bez kvalitných IT služieb by mnohé firmy nedokázali prežiť. Preto dnes obchodní lídri na trhu očakávajú od IT oveľa viac, ako len podporu. Požadujú priamo vyriešiť otázky týkajúce sa schopnosti a efektivity ich podnikania pozitívnym vplyvom kvalitných IT služieb. Poskytovateľom IT služieb tak tento vyšší stupeň a komplexnosť požiadaviek na informačné technológie rozširuje nutnosť implementácie nepretržitého zlepšovania ich služieb.

Preto si je nutné uvedomiť, že:

- IT robí viac, než aby podporovalo existujúce obchodné operácie, umožňuje zmeny vo firmách, a je teda neoddeliteľnou súčasťou manažmentu zmien vo firmách,
- kvalita IT sa posudzuje z hľadiska spoľahlivosti, dostupnosti, stability, kapacity, bezpečnosti a najmä rizík na podnikanie,
- IT a správa IT je integrálnou súčasťou podnikového riadenia,
- výkon IT sa stáva viditeľnejší cez technické výpadky a nespokojnosť zákazníkov,
- pre elektronické obchodovanie je IT kľúčovým predpokladom existencie.

Prínosy zavedenia nepretržitého zlepšovania služieb

Od zavedenia CSI sa očakávajú mnohé priame i nepriame prínosy:

pre zákazníka:

■ celkové zlepšenie alebo udržanie kvality obchodných operácií aj po zavádzaní interných zmien alebo dôsledkom vplyvu externého prostredia,

■ zlepšenie kvality služieb a dostupnosti služieb, čo vedie k lepšej produktivite a zvýšeniu príjmov,

■ priama podpora obchodných procesov,

■ rýchlejšie a kvalitnejšie reakcie na potreby trhu

■ väčšia flexibilita a adaptabilita podnikania prostredníctvom pochopenia výhod, ktoré služby IT ponúkajú,

■ pochopenie, čo možno očakávať od IT a čo od nich, aby to bolo možné dodať,

■ zvýšenie produktivity personálu vďaka zvýšeniu spoľahlivosti a dostupnosti IT služieb,

■ lepšie pracovné vzťahy medzi zákazníkmi a dodávateľmi IT služieb,

■ lepšie plánovanie nákupov a definovanie požiadaviek na vývoj a implementácie IT,

finančné výhody:

■ rentabilné poskytovania IT služieb,

■ výdavky na IT služby a ich kontinuitu sú úmerné kritickosti podporovaných podnikových procesov,

■ lepšie pochopenie dôvodov pri investovaní do IT infraštruktúry a služieb a ľahšie rozhodovanie pri výške investícií,

■ zníženie nákladov pri zavádzaní zmien služieb bez negatívneho dopadu na ich kvalitatívnu úroveň,

■ lepšie pridelenie a využitie zdrojov,

pre inovácie:

■ jasnejšie chápanie obchodných požiadaviek, ktoré zabezpečujú, aby IT služby úspešne podporovali podnikové procesy,

■ vyššia informovanosť o kvalitatívnej úrovni aktuálne poskytovaných služieb s možným získaním potenciálneho prínosu a vyššieho úžitku,

■ vyššia flexibilita pre podnikanie prostredníctvom lepšieho chápania IT služieb a podpory,

■ zvýšenie flexibility a adaptability IT služieb,

■ vyššie ambície firiem,

■ lepšia schopnosť rozpoznať meniace sa trendy a rýchlejšie sa prispôsobiť novým požiadavkám a vývojom trhu,

pre prevádzku IT:

■ lepšie metriky a manažment správy IT služieb,

■ lepšie informácie o aktuálne poskytované služby a o tom, kde zmeny v životnom cykle IT služby prinesú najväčší úžitok,

■ zvýšenie výkonnosti procesov a vytvorenie nových obchodných modelov alebo kanálov na základe riadenia procesov v reálnom čase,

■ jasnejší pohľad na aktuálne možnosti IT a budúci potenciál IT služieb,

■ štruktúrovaný prístup k zberu údajov, sústruženie dát do informácií a ich analýzou vytváranie cenných znalostí podľa toho, čo sa v rámci organizácie deje, čoho výsledkom by mali byť získané hodnotenia a cenné informácie o tom, kde sa môžu použiť prostriedky na zlepšenie služieb s väčším pozitívnym vplyvom na podnikanie,

■ znalosti o nástrojoch a zdrojoch potrebných na podporu činností CSI,

■ aktívnejší rozvoj a zdokonaľovanie IT technológií a služieb,

■ zladenie štruktúry nákladov na poskytovanie IT (technológie, ľudia a pod.) s obchodnými potrebami,

■ zlepšenie komunikácie, tímová práca, firemná kultúra a interaktivity prístup,

■ motivovanejší zamestnanci – vyššia spokojnosť s ich prácou vďaka lepšiemu porozumeniu ich schopností a očakávaní,

■ zvýšenie efektivity zamestnancov - zlepšenia ich produktivity, spolupráce, komunikácie a inovácie,

■ stanovenie jasnejších zodpovedností, povinností a úloh,

■ lepšie využitie zdrojov,

■ nízka fluktuácia zamestnancov,

■ lepšie riadenie dodávateľov s ich vyššou výkonnosťou,

■ zníženie rizika neúspechu pri plnení záväzkov,

■ lepšie pracovné vzťahy s podnikateľským sektorom.

Zásady nepretržitého zlepšovania služieb

Zlepšenie služieb sa zaoberá predovšetkým zvýšením celkovej efektivity, efektivity nákladov, účinnosti zmien a optimalizácie procesov, čo je možné dosiahnuť:

- *organizačnými zmenami:*

Ľudia vo všeobecnosti nemajú radi zmeny a keď je to možné, vyhýbajú sa im. Zmeny v organizácii musia byť jasne vysvetlené všetkým zainteresovaným osobám, aby porozumeli čo nové sa od nich očakáva. Ak sa aspoň vzorke zainteresovaných osôb umožní priestor vstúpiť do navrhovaných zmien ešte vo fáze návrhu, podrobne sa oboznámi s dôvodmi a potrebami zmien, je nútená zamyslieť sa nad riešeniami a oveľa rýchlejšie a jednoduchšie sa potom získa ich podpora pri samotnom zavádzaní dohodnutých zmien. Ľahšie sa tak zabezpečí aj odstránenie starých neželaných pracovných postupov. To všetko často súvisí so zmenami zodpovedností a rolí v rámci organizácie a projektov.

- *určením vlastníctiev za proces zlepšovania služieb:*

Princíp vlastníctva je zásadný pre akékoľvek zlepšenie stratégie. Jedným z kľúčov k úspešnej realizácii CSI je zabezpečiť, aby konkrétny manažér bol v pozícii manažéra CSI (alebo bola menovaná samostatná osoba) so zodpovednosťou za prijaté a trvalo zlepšované zmeny v celej organizácii. Správca CSI sa stáva vlastníkom CSI a hlavný obhajca, je zodpovedný za úspech a neustále zlepšovanie služieb v organizácii.

- *poznaním, čo ovplyvňuje úroveň služieb:*

Sú dva druhy vplyvov, ktoré pôsobia na úroveň služieb, vonkajšie a vnútorné. Vonkajšie aspekty pôsobia z vonku, teda mimo organizácie, ako napr. nariadenia, legislatíva, predpisy, hospodárska súťaž, externé požiadavky zákazníkov, tlaky trhu a stav ekonomiky spoločnosti. Vnútorné aspekty sú vnútornou záležitosťou každej organizácie, ako je organizačná štruktúra , firemná kultúra, schopnosť prijať zmenu, nové pravidlá, existujúci a navrhovaný počet zamestnancov atď. V niektorých prípadoch tieto aspekty môžu brániť objavovať priestory na zlepšenie služieb. Významné príležitosti pre zlepšovanie služieb sa dajú identifikovať napr. SWOT analýzou, ktorá pracuje so silnými a slabými stránkami, príležitosťami a hrozbami. Silné a slabé stránky sa zameriavajú na vnútorné aspekty organizácie, kým príležitosti a hrozby sa zameriavajú na vonkajšie aspekty.

- *riadením úrovne služieb:*

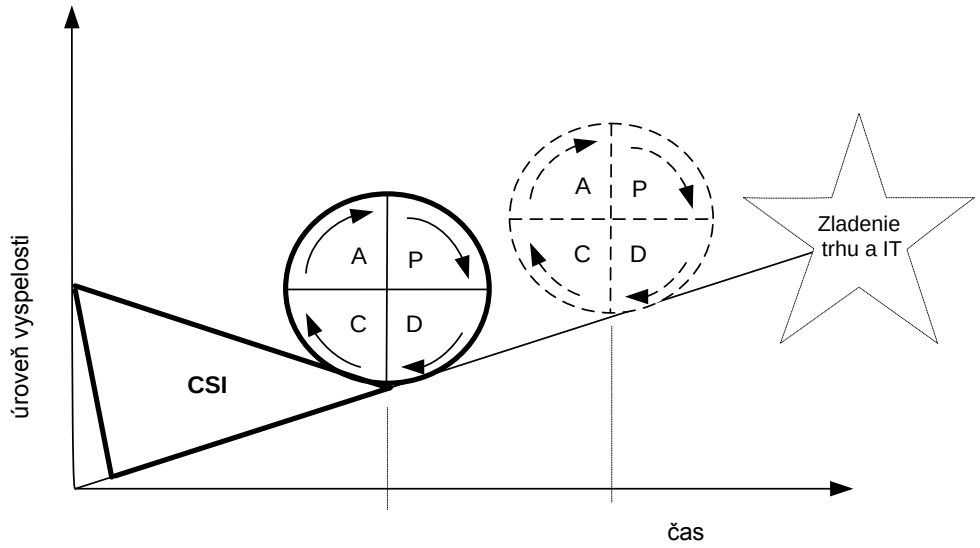
Proces riadenia úrovne služieb (Service Level Management) je kľúčovým princípom CSI. Zatiaľ čo v minulosti veľa IT organizácií považovalo riadenie služieb len za

izolované dohody dostupnosti systému alebo help desk hovorov, dnes to už často nestačí. Dnešné požiadavky zákazníkov sú nastavené tak, aby IT služby poháňali obchodný model. Táto služba orientácie smerom k podnikaniu sa stáva základom pre dôveryhodné partnerstvo, ktoré sa svet IT musí snažiť vytvoriť. IT si už nemôže dovoliť byť izolované vo svojom vlastnom svete ale naopak, snaží sa byť súčasťou každého komunikačného kanálu, na každej úrovni rozhodovania.

Potom, ako sa poskytovatelia IT a ich obchodní partneri začali zaoberať riadením úrovne služieb (Service Level Management), manažéri IT si uvedomijú, že dovtedy známe definície úspešnosti IT sa dostávajú na vedľajšiu koľaj. Totiž konečným cieľom už nie je len dosiahnuť určité percento dostupnosti služieb, alebo želanú úroveň spokojnosti zákazníkov meranej v pravidelných intervaloch. To sú len pozitívne ukazovatele na dosiahnutie komplexnej úrovne služieb. Definícia úspechu v IT je potom jasná, dosiahnuť požadovanú úroveň služieb, teda súbor dohodnutých očakávaní poskytovateľa IT a jeho zákazníka. Dohodnutá úroveň služieb je potom štruktúrovaná, riadená, implementovaná, financovaná, a prevádzkovaná tak, aby spĺňala prípadne aj prekračovala dohodnuté úrovne služieb.

- *pochopením prínosu Demingovho cyklu:*

W. Edwards Deming je známy vďaka jeho filozofii ako sa dopracovať k vyššej kvalite, zvýšenej produktivite a lepšiemu konkurenčnému postaveniu na trhu. V rámci tejto filozofie formuloval 14 poznatkov pre manažérov. Pre zlepšenie kvality navrhoval tzv. Demingov cyklus, známy tiež ako PDCA cyklus (Plan, Do, Check, Act), ktorý pozostáva zo štyroch základných fáz: plánuj, urob, over, konaj, pričom po fáze konaj sa dostávame opäť od fázy plánovania a však nie na začiatok cyklu, ale akoby špirálovite posunutý o úroveň vyššie s nadobudnutými vedomosťami a skúsenosťami z predchádzajúcich fáz a teda po posune v zlepšovaní služieb.



Obr.19 Demingov cyklus

- *Riadením znalostí:*

Hovorí sa, že tí, ktorí sa nepoučili z histórie, sú odsúdení zopakovať si ju. Riadenie znalostí zohráva ďalšiu kľúčovú úlohu CSI. V rámci každej fázy životného cyklu služby, by mali byť získané údaje súvisiace s úrovňou poskytovaných služieb zachytené a zaznamenané, následne analyzované a spracované na informácie vedúce k vedomostiam a pochopeniu, čo sa v poskytovaní IT služieb deje. Tieto získané múdrosti povedú k lepšiemu rozhodovaniu pri zlepšovaní služieb IT a ich poznanie je nepochybne tiež konkurenčnou výhodou poskytovateľa IT.

- *Využitím benchmarkingu:*

Benchmarking je proces používaný najmä v oblasti strategického riadenia, v ktorom organizácia hodnotí rôzne aspekty svojich procesov v súvislosti s osvedčenými postupmi. Organizácie majú rastúcu potrebu získavať jasný a nezávislý pohľad na ich vlastnú úroveň kvality služieb v porovnaní s konkurenciou. Výsledky porovnávacej analýzy a seba-hodnotenie môže viesť k identifikácii medzier, pokiaľ ide o ľudí, procesy a technológie.

Benchmark môže byť katalyzátorom na určenie priorít, kde začať implementovať formálny proces zlepšovania. Výsledkom tejto porovnávacej analýzy musí byť identifikácia priestorov na zlepšenia, určenie rizík, ktoré nie sú pokryté slabými miestami, uľahčenie stanovenia priorít rozvojových aktivít a výsledky dostatočne a vhodne komunikované.

7 fáz procesu nepretržitého zlepšovania služieb

Je zrejmé, že všetky činnosti procesu zlepšovania môžu pomôcť k celkovému kontinuálnemu zlepšovaniu IT služieb. Je pomerne jednoduché zistiť, čo sa vplyvom týchto činností deje, ale náročnosť spočíva v pochopení, akým spôsobom zlepšenie prebieha a teda aj opačne, ako zlepšenie dosiahnuť. Zistiť to môžeme postupnými siedmymi fázami procesu nepretržitého zlepšovania IT služieb:

1. *fáza: Definovať, čo by sa malo merať*

Na začiatku životného cyklu služby by mali byť tieto informácie určené. Kontinuálne zlepšovanie služieb potom môže nájsť počiatočný bod úrovne služieb. Bude tak možné odpovedať si na otázku: „Kde sme teraz?“

2. *fáza: Definovať, čo môžete merať*

Z požiadaviek na podnikanie a výpočtovú techniku identifikovaných počas návrhu a prechodu služieb dochádza k určeniu novej úrovne služieb. Mali by sme si tak vedieť odpovedať na otázku: „Kde sa chceme dostať?“' Vďaka tomu sa môže vykonať analýza nedostatkov, aby sa zistili príležitosti pre zlepšenia, rovnako ako odpovede na otázku: „Ako sa tam dostaneme?“

3. *fáza: Zber údajov*

Aby bolo možné správne odpovedať na otázku: „Mali sme sa tam dostať?“, musia sa najskôr získať údaje o kvalite a úrovni služieb z reálnej prevádzky. Tieto dáta sa zhromažďujú na základe vopred stanovených cieľov a sú v surovom stave, teda neopierajú sa o žiadne závery. Odpovedať si pritom na túto otázku vieme až neskôr.

4. *fáza: Spracovanie dát*

Cieľom tohto kroku je spracovávať dáta z viacerých rôznorodých zdrojov do porovnateľných kategórií. Keď sú dáta racionálne a relevantné, môže sa začať s ich analýzou.

5. *fáza: Analýza dát*

V tomto kroku sa z dát stáva informácia, akou môže byť identifikovaná medzera služby, jej vývoj a vplyv na podnikanie. Tento krok je najčastejšie podceňovaný alebo zabudnutý v zhone, aby sa v požadovanom termíne predložili dáta na riadenie služieb IT.

6. *fáza: Prezentácia a využitie informácií*

Už poznáme odpoveď na otázku „Mali sme sa tam dostať?“, ale treba ju ešte naformulovať a oznámiť vhodným spôsobom rôznym zainteresovaným stranám s cieľom podať presný obraz o výsledkoch úsilia zlepšení.

7. *fáza: Vykonávacie opatrenia na nápravu*

Získané poznatky z predchádzajúcich krokov sa používajú pri optimalizácii a zlepšení služieb. Manažéri by mali v tejto fáze identifikovať problémy a prezentovať svoje riešenia vo forme návrhov nápravných alebo preventívnych opatrení, ktoré považujú za potrebné prijať na zlepšenie služieb. Nemali by pri tom zabudnúť vysvetliť v súvislostiach dôvody a očakávané dopady ich návrhov. Po tomto kroku často formou schválenia opatrení vyšším manažmentom organizácia zavádza nový cyklus a začína nanovo.

Aj keď sa zdá, že týchto sedem fáz meraní tvorí kruhový súbor činností, v skutočnosti predstavuje špirálu. V praxi sa tak vedomosti a poznatky zhromaždené z týchto znalostí na jednej úrovni organizácie stávajú vstupnými dátami pre ďalšie opakované kroky. Ak by sa niektorá z fáz vynechala, existuje tu potom riziko, že by pri plnení cieľov CSI ani ostatné fázy neboli efektívne.

Metódy a techniky CSI

V činnostiach nepretržitého zlepšovania služieb môže byť použitá nepretržitá škála metód a techník od príliš všeobecných až po vecné až vedecké. Všetky by mali poskytovať kvalitatívne alebo kvantitatívne výsledky meraní resp. ich kombináciu.

Aby sa zabezpečil súlad realizácie merania a efektívnosť merania potrebná najmä pre činnosti zberu a spracovania dát, mali by sa zvolené techniky a metódy merania v predstihu jasne zdokumentovať a oznámiť pracovníkovi, ktorý bude zodpovedný za ich vykonanie a dodržanie. Pre zvýšenie dôveryhodnosti nazbieraných a dodaných údajov do ďalších procesov, môže byť na viac potrebné vykonávať kontroly dodržiavania dohodnutých a predpísaných metód a techník merania.

V súčasnej dobe sa na dosiahnutie zlepšenia služieb preferujú postupy a medzinárodne uznávané štandardy ITIL, ISO / IEC 20000, CMMI, COBIT, VALIT a ďalšie. Posúdenie ich vhodnosti, účinnosti, prínosu, stavu plnenia požadovaných cieľov ako aj objektívnosti týchto hodnotení je možné vykonávať z vnútra organizácie, kedy ale môže dôjsť k narušeniu objektívnosti hodnotení, alebo s pomocou tretej

strany formou pravidelných externých auditov. Hodnotenie by pri tom malo byť efektívny spôsob odpovede na otázku *„Kde sme teraz?“* a pochopenie, ako sú existujúce služby poskytované a vykonávané, alebo ako efektívne a účinne sú procesy služieb IT riadené. Tento stav je dôležitý aj pre určenie prínosu CSI rozdielom medzi miestom, kde sme boli na začiatku a kde sme po zavedení plánovaného procesu zlepšovania služieb, resp. kde sme teraz a kde chceme byť.

Implementácia procesu neustáleho zlepšovania služieb IT

Jedným z najnovších medzinárodne uznávaných systémov implementácie procesu neustáleho zlepšovania služieb do života spoločnosti poskytovanej IT služby je ISO 38500, zaoberá sa ňou aj ITIL.

Kde a ako treba s CSI začať?

Organizácie si môžu vybrať rôzne spôsoby vykonávania činností CSI:

■ jednou z možností je identifikovať určité problémové služby, ktoré nespĺňajú požadované finančné alebo nefinančné výsledky. Vyžaduje si to samozrejme poznať požadované výsledky a trendy a mať k dispozícii overenie ich stavu počas niekoľkých posledných mesiacov. Je potrebné vrátiť sa na všetky dostupné reporty a realizovaný monitoring, pri čom sa zamerať nie na to, čo bolo monitorované a merané, ale hlavne či existujú konzistentné problémy, ktoré vedú k nižšej úrovni služieb ako boli očakávané a definované na začiatku alebo sú aktuálne požadované. Ak nedôjde k žiadnym výrazným zisteniam, je nutné nezabudnúť skontrolovať záznamy v incident manažmente, zaoberať sa dôvodmi ich vzniku, prípadnými trendmi ich vývoja, ako aj konzistentnými konfiguráciami, ktoré majú vplyv na služby. Tiež je treba preskúmať zmeny záznamov pre rôzne konfigurácie, ktoré spoločne podporujú službu. Výsledkom týchto snažení sú zistenia, čo je nutné sledovať cez definované požiadavky na monitoring. Následne na to sa tím poverený monitoringom často zaoberá zavažovaním, či doteraz používané postupy, metódy a technológie sú postačujúce. Začínajú sa používať alebo zavádzať nové technológie potrebné na monitoring spĺňajúci definované požiadavky.

Pred tým sa však treba ešte uistiť, či získané dáta, informácie a trendy majú zmysel, treba ich analyzovať a spracovať do komplexnej správy o získaných existujúcich, konzistentných zlyhaniach alebo odchýlkach od očakávaných výsledkov a identifikovať príležitosti na zlepšenie.

■ druhá z možností začatia zavádzania procesu zlepšovania vychádza z postoja celoživotného prístupu k službe. Vtedy sa hľadané zistenia stavu úrovne služieb a príležitosti na zlepšenia vykonávajú v každej časti životného cyklu, najmä v návrhu služby (Service Design), prechode služby (Service Transition) a prevádzke služby (Service Operation). Výsledky takéhoto priebežného zlepšovania sa môžu pozitívne prejaviť ešte pred nasadením služby do produkčného prostredia zákazníka, keď dochádza k zlepšovaniu ešte v čase návrhu služby vo vývojom prostredí poskytovateľa IT služby vďaka jeho interným testovaniam.

■ ďalší spôsob zistenia, čo a ako začať zlepšovať vyplýva z problémov funkčnosti a teda následnej nedostupnosti služby, ktoré môžu byť spôsobené napríklad zlyhaniami serverov. V takom prípade ide skôr o krátkodobé riešenie zlepšovania IT služieb a z pohľadu koncového odberateľa IT služieb často prvý ale zďaleka nepostačujúci krok k skutočnému vnímaniu zlepšovania služieb.

Ako pokračovať s CSI po vykonaní prvých krokov?

■ strategický pohľad na identifikované príležitosti zlepšení služieb

Je nevyhnutné všetky relevantné zistenia a hlavne identifikované príležitosti na zlepšenia spracovať do správy zistení aj zo strategického pohľadu. Neraz organizácie čelia potrebám rozšíriť svoje IT stratégie z prevádzkovej úrovne na správu služieb, musia tak riešiť automatizáciu obchodných procesov, trhovú globalizáciu a zvyšujúcu sa závislosť na IT pre efektívne a spoľahlivé riadenie a poskytovanie základných služieb obchodnej povahy, čo neraz vyžaduje transformáciu vnútornej kultúry IT a projektového manažmentu.

■ proces zmeny

Implementácia CSI bude priamo vplývať na procesy, pracovníkov, používané technológie ako aj riadenie zdrojov poskytovateľa IT služieb. CSI sa tak musí stať spôsobom života v rámci organizácie, čo môže vyžadovať novú štruktúru riadenia, nové technológie, zmeny procesov na podporu CSI a ľudia budú musieť byť dobre informovaní o zámeroch a cieľoch CSI.

■ tvorba tímu pre CSI

Pre dosiahnutie úspešných výsledkov CSI je nutné stanoviť tím zložený s viacerých úrovní riadenia poskytovateľa IT služieb, ktorý bude mať viac než len formálne právomoci ale aj skúsenosti, rešpekt, dôveru a vierohodnosť a vedúce osobnosti tímu by mali mať spoločné chápanie naliehavosti a toho, čo chcú dosiahnuť. Tento tím

musí byť pripravený vynaložiť čas a úsilie presvedčiť a motivovať ostatných pracovníkov spoločnosti k primeranej účasti na CSI, nemal by sa na čas implementácie zlepšení izolovať od ostatných pracovníkov. Potrebné je tiež formálne aj neformálne sa pýtať, či sú v tíme tí správni ľudia a ak nie, kto by tam mal byť.

■ vytvorenie víze pre CSI

Vedenie tímu CSI by malo byť zodpovedné za zabezpečenie toho, že vízia CSI priamo súvisí s cieľmi a účelom CSI. Táto vízia by mala predstavovať dobré videnie a tvrdenie realizácie zlepšení služieb a jej účelom je objasniť smer CSI, motivovať ľudí na zapojenie sa správnym smerom a koordinovať ich činnosti a mal by byť vstupom do cieľov vrcholového vedenia spoločnosti. Musí byť však ľahko pochopiteľné a tiež ľahko vysvetliteľné do piatich minút.

■ komunikácia víze

Hoci vízia je mocný nástroj, ktorý pomáha koordinovať zmeny v organizácii, stráca svoju silu, keď nie je účinne zainteresovaným stranám oznámená a pochopená. Komunikácia vízie CSI by mala byť zameraná na motiváciu, inšpiráciu a vytvorenie potrebnej energie a odhodlania k prijatiu potreby na zmeny.
Je dôležité využiť všetkých komunikačné kanály vo vnútri spoločnosti sa dostať tieto informácie naprieč spoločnosťou.

■ poskytnutie zdrojov na CSI

Na realizáciu vízie CSI treba podporiť existujúce zdroje v organizácii, teda poskytnúť ľuďom nástroje, školenia, smer, a ubezpečenie, že budú mať jasné a jednoznačne stanovené ciele. V momente, keď sú ľudia na niečo konkrétne splnomocní, sú aj za to zodpovední. To je dôvod, prečo treba potvrdiť ich dôveru pred začatím požadovaných zmien.

■ krátkodobé plánovanie zmien a tvorby CSI

Samotné CSI je zdĺhavý program zmien. Je dôležité mať definované krátkodobé úspechy, uvedomovať si ich a oznamovať ich zainteresovaným stranám, čo pomáha, aby ľudia nestrácali príliš skoro nadobudnutú energiu a chuť zmeny realizovať a prispôsobovať sa im.

■ upevnenie zlepšovania služieb

Úspechy plnenia krátkodobých plánov a cieľov umožňujú udržiavať dynamiku priebehu CSI, sú presvedčivejšie, ukazujú okamžité výhody i zisky a vytvárajú priestor na väčšie zmeny. V procese nepretržitého zlepšovania služieb si je tiež dôležité uvedomovať aj prínosy plnenia stredných a dlhodobých plánov, ktoré

prinášajú pracovníkom dôveru, istoty, a prejavuje sa to ich ochotou a prirodzenou snahou samovzdelávať sa v tom, čo sa od nich požaduje, aby to boli schopní robiť na požadovanej úrovni, ak nie aj vyššej. Ale to už je stav pracovníkov, kedy nie len skutočne pochopili význam ich činností ale sa s ním aj stotožnili. Je to ako snažiť sa dosiahnuť olympijskú medailu ešte pred tréningom. Prirodzene takýto stav nie je v praxi možné reálne dosiahnuť u všetkých pracovníkov, na všetkých úrovniach riadenia, či pre všetky poskytované služby vplyvom podnetov z vnútra i z vonku spoločnosti. Aj preto musí byť zlepšovanie služieb proces kontinuálny a v podstate nikdy sa nekončiaci, ak je to v súlade s obchodným a podnikateľským zámerom.

Kritické faktory a riziká CSI v praxi

Každá organizácia má svoj vlastný a jedinečný súbor problémov. Z pohľadu času a náročnosti je jedna z najväčších výziev pre riadiacich manažérov práve riadenie zmien myslenia a správania. Ak sa podarí táto fáza, teda ľudia chápu prečo sa na dané problémy treba pozerať inak a aj inak k nim pristupovať, bude pre nich prirodzenejšie si dané zmeny aj osvojiť a riadiť sa nimi.

Ďalší zásadný problém je, keď CSI si už vyžaduje mať náležité technické nástroje pre monitorovanie a zhromažďovanie väčšieho množstva údajov, vyhodnocovanie a podávanie správ o dátach a trendoch. Naopak to ale neznamená, že CSI sa dosiahne len vďaka automatizácii zberu údajov. Je nevyhnutné mať potrebné zdroje a zručnosti na výkon činností, úloh a zodpovedností CSI.

V praxi môžu počas nepretržitého zlepšovania služieb nastať nasledovné kritické faktory, riziká a problémy negatívne ovplyvňujúce výsledky činností zlepšovania služieb IT:

- nedostatok firemných cieľov, stratégií, politík a nejasné obchodné smerovanie,
- nedostatok nástrojov, znalostí, a zručností počas zlepšovania služieb,
- nedostatočné zdroje, rozpočet alebo čas,
- nedostatočné plnenie záväzkov vyplývajúcich z externého prostredia,
- vysoká odolnosť proti zmenám podporovaná silnou vnútornou kultúrou,
- nedostatočná komunikácia a spolupráca medzi IT a zákazníkom,
- slabá motivácia a neschopnosť dodávať služby v požadovanom čase, rozsahu a rozpočte,

■ chýbajúce alebo zlé riadenie dodávateľov s dopadom na výkonnosť a efektivitu celkového výsledku,

■ chýbajúce menovanie manažéra pre nepretržité zlepšovanie služieb alebo jeho nejasné úlohy, zodpovednosti a hlavne nedostatočné kompetencie,

■ chýbajúce riadenie záväzkov cez vytváranie a obnovovanie vízie pre CSI, v prípade potreby aj oznamovanie tejto vízia do vnútra organizácie, smeru ktorým sa organizácia rozhodla ísť,

■ nejasné vymedzenie kritérií na stanovenie priorít zlepšovania,

■ priveľké očakávania z procesu zlepšovania bez jasne definovaných čiastkových krokov a cieľov,

■ nedostatok IT cieľov, stratégií a politík,

■ využívanie zložitých a technologických nástrojov na evidenciu údajov o poskytovaných alebo plánovaných službách, čo komplikuje ba až znemožňuje merať a monitorovať úroveň služieb,

■ vysoké náklady na údržbu a ďalší vývoj nástrojov na meranie úrovne služieb,

■ všetka pozornosť venovaná na nové služby IT na úkor starých a zabehnutých služieb, čím môže dôjsť k výraznému zníženiu ich kvality,

■ nedostatok informácií, ich podcenené sledovanie a meranie,

■ nedostatočné riadenie znalostí,

■ nezrozumiteľné a nejednotné informácie vstupujúce do tvorby plánov, ktoré nemajú vypovedaciu hodnotu pri porovnávaní so skutočnosťou a následná neochota neporozumenie zmyslu vypracúvania nových plánov

Záver

Vykonávacie CSI nie je z ďaleka ľahká úloha, lebo vyžaduje zmenu v riadení, postojov zamestnancov a neraz i hodnôt a priorít. Nepretržité zlepšovanie je potrebné urobiť aktívne a nie reaktívne. Prvým kľúčovým krokom pred implementáciou CSI je identifikácia rizík a výziev. Tieto položky možno identifikovať pomocou SWOT analýzy služieb poskytovateľa. Je dôležité pri tom definovať stratégiu, ako zmierniť identifikované riziká a stanoviť, ako najlepšie môže organizácia predísť prípadne prekonať možné problémy, ktoré jej hrozia. Druhým krokom je poznanie a zaujatie stanoviska k riešeniu kritických faktorov CSI, čo výrazne napomáha schopnosti riadiť nové výzvy a riziká.

Normalizácia z pohľadu IT prostredia

Pod pojmom *normalizácia* rozumieme tvorbu a aplikáciu noriem, štandardov, odporúčaní a predpisov v určitej oblasti; v našom prípade v oblasti nasadenia a využívania informačných a komunikačných technológií (IKT, resp. IT) v organizácii. Normalizácia v tomto zmysle predstavuje vymedzenie rámca, ktorý zabezpečuje dodržanie minimálnej požadovanej úrovne kvality, technologických či manažérskych postupov a procesov, systémov riadenia, poskytovaných rozhraní, a podobne. Cieľom implementácie normy, sústavy predpisov a odporúčaní formulovaných v procese normalizácie, je v konečnom dôsledku zvýšenie konkurencieschopnosti organizácie, v ktorej sú normy zavedené. Správna implementácia normy by mala garantovať predpísanú kvalitu výstupných produktov či poskytovaných služieb, mala by zefektívniť a optimalizovať riadiace a rozhodovacie procesy, a napokon by mala zvýšiť prestíž a kredit organizácie voči konkurentom, ktorí danú normu implementovanú nemajú.

Na to, aby implementácia noriem prinášala konkurenčné výhody, musia normy spĺňať viaceré predpoklady. Norma má byť progresívna, zodpovedajúca najnovším poznatkom a trendom, čo je mimoriadne dôležité v takej dynamicky sa rozvíjajúcej oblasti, akou sú informačné technológie. Keďže poznatky vo všetkých oblastiach ľudskej činnosti sa vyvíjajú, normalizácia je iteratívnym procesom, pri ktorom norma prechádza etapami od návrhu a rozpracovania cez zavedenie do praxe až po ukončenie platnosti normy (časť 2.1.3). Norma však musí byť aj dostatočne ustálená, akceptovaná širokým spektrom odborníkov a preverená aplikáciami v praxi. Má tiež byť dostatočne jasná, zrozumiteľná, explicitná a kontrolovateľná – má teda obsahovať návody na implementáciu, príklady aplikácie, a tiež je vhodné ak jej súčasťou je odporúčaný postup certifikácie (porov. časť 2.2.7).

Pre oblasť riadenia služieb v IT prostredí je v súčasnosti základným štandardizačným rámcom norma ISO/IEC 20000, ktorá je založená na knižnici ITIL vo verzii 2. Tento prístup začleňuje infraštruktúru IT do celkovej štruktúry organizácie, orientuje služby IT smerom k podpore podnikových procesov a strategických cieľov. Z hľadiska normalizácie sa tým rozširuje záber o normy vymedzujúce riadenie kvality, monitorovanie podnikových procesov, bezpečnosť IT systémov, a tiež príslušné podporné technológie pre riešenia zodpovedajúce odporúčaniam rámca ITIL.

V ďalších častiach tejto kapitoly prezentujeme v uvedenom kontexte prehľad informácií o normalizácii v IT prostredí. Najprv, v časti 2.1, popisujeme problematiku normalizáce vo všeobecnosti. Definované sú základné pojmy a princípy normalizácie, druhy noriem a ich charakteristiky. Vymenované sú niektoré dôležité štandardizačné organizácie a stručne je popísaná ich činnosť. V závere prvej časti kapitoly je prezentovaná u nás platná legislatíva v oblasti technickej normalizácie.

V časti 2.2 sú predstavené konkrétne normy, ktoré sú relevantné pre manažment IT prostredia a služieb. Ťažiskovou je norma ISO/IEC 20000 a rámec ITIL. V tomto kontexte sa prezentujú ďalšie normy a štandardizačné dokumenty, napríklad normy pre manažment kvality (skupina noriem ISO 9000), štandardy pre modelovanie a riadenie podnikových procesov, norma ISO/IEC 38500 pre komplexné riadenie IT, ďalej normy pre informačnú bezpečnosť (ISO/IEC 27000) a štandardy niektorých technológií pre informačné systémy orientované na služby. Na záver je popísaný proces certifikácie na normu ISO/IEC 20000.

Základné princípy štandardizácie a normalizácie

Norma a štandard

Pre popis všeobecných princípov štandardizácie a normalizácie je potrebné definovať a vymedziť niektoré kľúčové pojmy, predovšetkým termíny *norma* a *štandard*. V slovenčine sa významy týchto termínov definujú takto:

> *Norma*: záväzné pravidlo ustálené predpismi, zvykom a podobne, resp. súbor takých pravidiel. Napr. *mravná, spoločenská, právna, štátna (technická) norma* [24].
>
> - *Technická norma*: predpis technického riešenia výrobku, zariadenia, technológie a pod. [29].
>
> *Štandard*: bežná (dobrá) úroveň, ustálená, normálna miera, stupeň ako základ hodnotenia niečoho [24].
>
> - *Technický štandard*: bežná, ustálená miera, vzor, podľa ktorého sa riadi výroba tak, aby sa vyrábali výrobky určitého typu, kvality, zloženia alebo rozmerov; (v niektorých krajinách) označenie technickej normy [29].

Z uvedených definícií vyplýva, že *norma* je „prísnejší“ pojem, obsahujúci črtu záväznosti. Termín *štandard* má v slovenskom prostredí všeobecnejší, voľnejší význam, zodpovedajúci širšie akceptovanému a rešpektovanému vzoru, ktorý však nemusí byť nevyhnutne záväzný, povinný. Skutočne, v minulosti boli u nás technické normy STN záväzné. Od 1.1.2001 však platí zákon č. 264/1999 Z. z. o technických požiadavkách na výrobky a o posudzovaní zhody, podľa ktorého je zhoda so slovenskými technickými normami dobrovoľná okrem prípadov, keď ich dodržiavanie vyžaduje tento zákon alebo iný technický predpis (napr. v oblasti bezpečnosti, elektrických inštalácií, v spojitosti s verejným obstarávaním, atď.). Viac o záväznosti technických noriem a predpisov uvádzame samostatne, v časti 2.1.5.

V anglicky písanej literatúre sa takmer výlučne na označenie pojmu norma používa termín *standard*[1]. Tento sa spätne sa do slovenčiny prekladá tvarovo blízkym termínom *štandard*, pričom sa zanedbáva príslušný významový rozdiel. Avšak túto nepresnosť je azda možné tolerovať, a to aj vzhľadom na vyššie spomínaný významový posun termínu *norma*, pri ktorom sa stráca rozlišovací aspekt záväznosti. Preto v ďalšom, ak nebude povedané inak, budeme používať termíny *štandard* / *štandardizácia* a *norma* / *normalizácia* ako synonymá.

Za referenčnú definíciu termínu norma možno považovať definíciu uvedenú v slovníku štandardizačnej organizácie ISO [13]. Podľa tejto definície: norma je dokument, vytvorený na základe dohody a schválený uznaným orgánom, ktorý poskytuje na bežné a opakované používanie pravidlá, usmernenia, návody alebo charakteristiky pre činnosti alebo ich výsledky tak, aby sa dosiahol optimálny stupeň usporiadania v danom kontexte.

Úloha, obsah a druhy noriem

Úlohou (technických) noriem je sprostredkovať presnú špecifikáciu danej oblasti priemyslu, obchodu či služieb, ktorá slúži ako referenčný rámec pre uplatnenie sa vo výrobnej či obchodnej praxi. Dôležité teda je, aby norma bola výsledkom čo najširšieho konsenzu zainteresovaných odborníkov a subjektov pôsobiacich v oblasti, aby mohla byť široko akceptovateľná a pre prax prijateľná. Zároveň norma musí byť progresívna, čiže má zodpovedať najnovším trendom a poznatkom v špecifikovanej oblasti. Tieto požiadavky sú však do istej miery

[1] Vyskytujú sa aj tvary *specification* a *norm*, tie sú však oproti tvaru *standard* oveľa zriedkavejšie.

antagonistické, protichodné. Nové poznatky a trendy sa do normy dostávajú až vtedy, ak sú aspoň do určitej miery verifikované, overené v praxi, a sú akceptované širším konzorciom odborníkov či používateľov (porov. časť 2.1.3). Pritom by však norma mala byť dostatočne prediktívna, zameraná do budúcnosti, smerom k predpokladaným a najpravdepodobnejším smerom budúceho vývoja v oblasti.

Súhrnne možno dôležité črty technickej normy vzhľadom na jej úlohy v priemysle a obchode popísať v nasledujúcich bodoch [34]:

- Norma reprezentuje určitú úroveň know-how a technológie, ktorá má byť čo najprogresívnejšia, avšak v technologickej praxi už overená. Preto je pri príprave normy nevyhnutná prítomnosť širšieho konzorcia zástupcov priemyslu a odborníkov.
- Norma je výsledkom spolupráce, odráža výsledky spoločnej práce všetkých zainteresovaných strán a je potvrdená dohodou konzorcia tak, aby reprezentovala všetky relevantné záujmy: výrobcov, používateľov, laboratórií, verejnej správy, spotrebiteľov, atď.
- Norma nie je nikdy neutrálna, nie je kompromisom. Naopak, v norme je vyjadrená presná a konkrétna špecifikácia určitého smeru či postupu (výrobného, technologického, riadiaceho, a pod.).
- Norma je koherentná a kozistentná. Je tvorená technickými komisiami, ktoré sú koordinované špecializovanými orgánmi a zabezpečujú, aby sa prekonali prekážky či rozdielnosti medzi rôznymi oblasťami činností a rôznymi typmi obchodných aktivít.
- Norma je referenčným dokumentom používaným osobitne v súvislosti s verejnými kontraktmi medzi obchodnými či priemyselnými partnermi, pri kontraktoch v medzinárodnom obchode alebo pri uzatváraní obchodných zmlúv.
- Norma je používaná priemyselníkmi ako nediskutabilná referencia, ktorá zjednodušuje a zjednoznačňuje zmluvný vzťah medzi ekonomickými partnermi.
- Aj keď norma nie je nevyhnutne právne záväzná (porov. časť 2.1.5), je to všeobecne akceptovaný dokument, ktorý možno použiť napríklad aj pri právnych sporoch.
- Normy sú všeobecne dostupné, môžu sa študovať alebo kupovať bez obmedzenia. Nie je však dovolené ich kopírovanie a zverejňovanie.

Štruktúra existujúcich noriem je v súčasnosti veľmi komplikovaná a rozsiahla. Vo všeobecnosti sa normy zaoberajú prakticky všetkými technickými, ekonomickými a sociálnymi aspektami činnosti ľudí, pokrývajú nielen technické či ekonomické oblasti, ale zahŕňajú všetky základné disciplíny ako sú jazyk, matematika, fyzika, a podobne. Z toho vyplýva, že noriem existuje veľké množstvo[2] a nie je v zásade jednoduché sa v nich orientovať. Naviac, tvorba noriem, ktorej sa podrobnejšie venujeme v časti 2.1.3, je živým procesom. Normy sa pravidelne revidujú, dopĺňajú sa alebo zanikajú. Podľa priebežne sa vyvíjajúcich poznatkov v oblasti sa normy menia tak, aby boli čo najviac aktuálne. Normy sa členia podľa zamerania, predmetu (oblasti), stupňa rozpracovanosti, geografickej platnosti a spôsobu šírenia.

Podľa obsahového zamerania (charakteru) sa normy rozdeľujú do štyroch hlavných druhov [34]:

- *Základné normy* pokrývajúce terminológiu, metrológiu, konvencie, značky a symboly, apod. Obyčajne sú to normy so širokým záberom, ktorý obsahuje všeobecné ustanovenia pre jednu konkrétnu oblasť.
- *Skúšobné metódy a normy pre analýzy*, pomocou ktorých sa merajú kľúčové vlastnosti, charakteristiky v danej oblasti.
- *Normy výrobkov a služieb* definujúce parametre jednotlivého typu výrobku (normy na výrobky) alebo obsahujúce špecifikáciu služieb. Tieto normy definujú najnižšiu prípustnú úroveň parametrov, ktoré služby alebo výrobky musia dosahovať (napr. vhodnosť použitia, ochrana zdravia, bezpečnosť, ochrana životného prostredia, dokumentácia prikladaná k výrobku, a pod.).
- *Organizačné normy,* ktoré sa zaoberajú opisom funkcie firmy a jej vzťahov, a tiež modelovaním rôznych činností vo vnútri firmy (napr. manažérstvo a zabezpečenie kvality, udržiavanie, hodnotová analýza, logistika, manažérstvo projektov a systémov, riadenie a organizácia výroby, atď.).

Podľa geografickej pôsobnosti, teritoriálnej platnosti, resp. podľa pôvodu vzniku sa normy členia na:

- *národné* (u nás STN, ďalej napr. ANSI – USA, DIN – Nemecko, BS – Veľká Británia, Ö NORM – Rakúsko, NF – Francúzsko, JISC – Japonsko),
- *regionálne* (napr. európske – EN, ETS a pod.),
- *medzinárodné* (napr. ISO, IEC, IEEE, W3C a ďalšie).

[2] Napríklad sústava STN v súčasnosti obsahuje asi 30 000 platných technických noriem, ročne pribúda okolo 2000 nových noriem [35].

Označenie normy príslušnou skratkou je dané legislatívne (napr. skratka STN – Slovenská technická norma, § 5 zákona NR SR č. 264/1999 Z. z.), alebo zodpovedá názvu organizácie, ktorá normu eviduje (ISO, IEC a ďalšie, prehľad najdôležitejších organizácií zaoberajúcich sa štandardizáciou uvádzame v časti 2.1.4). Pôvod a geografická pôsobnosť danej normy sú takto zrejmé z jej označenia.

Tvorba a modifikácia noriem je dynamický proces (porov. časť 2.1.3), pričom snahou je do čo najväčšej miery zosúladiť normy buď celosvetovo, alebo aspoň v rámci prirodzených geografických či hospodársko-politických celkov. Najčastejšie sa normy definované na medzinárodnej alebo regionálnej úrovni preberajú do sústavy národných noriem. Napríklad v priestore Európskej únie platí *princíp technickej harmonizácie noriem*, podľa ktorého sú na európskej úrovni definované spoločné technické špecifikácie, tzv. *harmonizované normy.* Na základe Rámcového dohovoru s Európskou komisiou z 13. novembra 1984 tieto normy pripravujú európske normalizačné organizácie [26]. Národné štandardizačné organizácie preberajú tieto harmonizované normy do vlastných štruktúr pomocou kvalifikovaného prekladu pôvodnej európskej normy a zosúladenia ostatných noriem a predpisov s touto normou. U nás sa táto činnosť vykonáva na základe zákona č. 264/1999 Z. z., pričom výsledkom tohto procesu sú *harmonizované slovenské technické normy*.

Normy definované na úrovni vyššej teritoriálnej platnosti sa pomerne často preberajú do nižších úrovní aj inak ako v procese harmonizácie. Menej častým spôsobom zmeny geografickej pôsobnosti je prechod z nižšej, napr. národnej úrovne na vyššiu regionálnu alebo medzinárodnú úroveň. Táto norma bola pôvodne definovaná ako národná norma Veľkej Británie pod označením BS 15000. Z nej vznikla medzinárodná norma ISO 20000, ktorá bola následne prebratá do európskej sústavy noriem ako ISO/IEC 20000, a neskôr sa stala aj súčasťou slovenských technických noriem pod označením STN ISO/IEC 20000.

Normy vydávané danou štandardizačnou organizáciou v príslušných katalógoch sa ďalej vnútorne členia podľa parametrov definovaných touto organizáciou. Pozícia normy v katalógu je vyjadrená jej *označením*, ktoré slúži ako kód obsahujúci informáciu o poradí, type a zameraní normy. Ako príklad uvedieme formát označenia a parametre noriem STN a ISO:

Formát označenia normy STN:

Celé označenie noriem STN nepreberajúcich medzinárodnú alebo európsku normu prekladom sa skladá zo značky STN a šesťmiestneho čísla:

- STN XX XX XX – pôvodná národná norma (neprevzatá), dvojčíslia vyjadrujú triedu, skupinu a poradie v katalógu (cca 40% noriem z celkového počtu STN).

Pri normách preberaných do sústavy STN z iných európskych či medzinárodných noriem nasleduje za značkou STN značka a číslo pôvodnej normy:

- STN EN XXXXX resp. STN ISO/IEC XXXXX – prevzatá európska resp. medzinárodná norma, päťčíslie vyjadruje číslo pôvodnej európskej alebo medzinárodnej normy (cca 60% noriem).

Za označením noriem preberajúcich medzinárodnú alebo európsku normu je v zátvorke uvedený triediaci znak zodpovedajúci označeniu (kódu) národnej STN, pod ktorým je norma zatriedená do sústavy STN, napríklad:

STN ISO/IEC 20000-1 (36 9788)

V tomto prípade ide o medzinárodnú ISO normu, ktorá bola pripravená v spolupráci s Medzinárodnou elektrotechnickou komisiou IEC. Pôvodná norma ISO má číslo 20000, tvorí ju však súbor viacerých dokumentov. Uvedené označenie sa vzťahuje na prvý z dokumentov, ktorý má číslo 20000-1. Názov tohto dokumentu je „Informačné technológie. Manažment služieb. Časť 1: Špecifikácia“. Pri zaradení do sústavy STN bola táto norma pridelená do STN triedy 36: Elektrotechnika, Informačné technológie, do skupiny 97, poradové číslo 88.

Parametre normy ISO:

Označenie normy ISO (reference number) sa skladá z prefixu, poradového čísla a roku publikovania. Vyššie spomínaná norma, ktorá bola publikovaná v roku 2005, má v ISO kódovaní označenie:

ISO/IEC 20000-1:2005

Prefix je zložený reťazec, ktorý označuje pôvod normy (ISO, resp. spločné štandardy ISO/IEC, ISO/IEEE, ISO/OECD, atď.) a môže obsahovať aj určenie typu dokumentu. Typy dokumentov ISO noriem môžu byť napríklad:

- *R* – odporúčanie (Recommendation),
- *TR* – technická správa (Technical Report),
- *TS* – technická špecifikácia (Technical Specification), a niektoré ďalšie.

Okrem samotného označenia je publikovaná ISO norma zaradená do štruktúry ISO katalógu podľa ďalších parametrov, napríklad:

- *ICS* (International Classification of Standards): kódové označenie predmetu normy, resp. oblasti, do ktorej norma spadá. Používajú sa kódy podľa medzinárodnej klasifikácie [8]. Norma ISO/IEC 20000 je priradená do oblastí 03.080.99: Services a 35.020: Information technology in general.
- *TC/SC* (Technical committee / Subcommittee): kód technickej komisie (podkomisie), ktorá je zodpovedná za jednotlivé etapy tvorby normy. Pre normu ISO/IEC 20000 je určená komisia JTC 1/SC 7: Software and systems engineering.
- *stav* (status): jednoduché označenie stavu rozpracovanosti normy, napr. „v príprave“ (Under development), „publikované“ (Published), a pod.
- *stupeň* (stage): komplexné označenie stavu rozpracovanosti a vývoja normy podľa medzinárodnej kódovej tabuľky [9] spolu s dátumom poslednej zmeny.

Ďalšie parametre publikovanej ISO normy sú popisné, určujú formát a spôsob prístupu k norme. Do tejto skupiny parametrov patrí jazyk (ISO normy sú publikované v angličtine, francúzštine a ruštine), abstrakt (skrátený obsah normy), počet strán a formát (PDF alebo tlačená verzia).

Štandardizácia a tvorba noriem, životný cyklus normy

Štandardizácia (resp. *normalizácia*) je cielená činnosť, ktorou sa vytvárajú a do praxe zavádzajú štandardy (resp. normy), čiže všeobecne platné ustanovenia pre konkrétne a opakované použitie v danej oblasti, napríklad v priemysle, obchode, službách, a podobne. Štandardizácia je zameraná na dosiahnutie optimálneho stupňa poriadku v príslušnej oblasti, a to s ohľadom na aktuálny stav poznania v oblasti, na riešenie známych problémov a na predpokladaný výhľad do budúcnosti. Aktivity spojené so štandardizačnou činnosťou pozostávajú predovšetkým z vypracovania návrhu normy, jej oficiálneho vydania a zavedenia do praxe.

Dôležitým prínosom technickej štandardizácie je zlepšenie vhodnosti výrobkov, procesov a služieb pri ich použití pre zamýšľané účely, predchádzanie prekážkam v obchode a uľahčenie technickej spolupráce. Pre ekonomických, výrobných či obchodných partnerov zúčastňujúcich sa na tvorbe alebo aplikácii noriem sa štandardizácia zameriava na splnenie viacerých faktorov [34]:

- *Faktor odôvodňujúci produkciu*. Norma umožňuje dosiahnuť žiadané technické parametre, uspokojiť zákazníka, potvrdiť spôsob výroby, ovplyvňovať rast produktivity a poskytovať obsluhe stanovenú úroveň kvality a bezpečnosti.
- *Faktor na sprehľadnenie transakcie*. Existencia systému referenčných dokumentov, noriem a predpisov, umožňuje lepšie vyhodnotiť ponuku a redukovať neistotu v obchodných vzťahoch, pomáha pri definovaní potrieb firmy, pri optimalizovaní vzťahov s dodávateľmi a zákazníkmi, dovoľuje produkovať výrobky bez ďalšieho dodatočného skúšania.
- *Faktor inovácie a ďalšieho vývoja výrobkov*. Účasť na normalizačnej práci umožňuje predvídať budúci vývoj v oblasti, a teda aj priebežne inovovať výrobok či službu. Normy pomáhajú získavať relatívnu konkurenčnú výhodu vďaka prenosu znalostí.
- *Faktor prenosu nových technológií*. Normalizácia uľahčuje a urýchľuje prenos technológií v oblastiach dôležitých ako pre firmy, tak aj pre osoby (nové materiály, informačné systémy, biotechnológie, elektronika, výroba pomocou počítačov, riadenie IT služieb, a pod.).
- *Faktor ovplyvňujúci strategické rozhodnutia firiem*. Účasť na normalizačnej práci robí významnou potrebu zaviesť prijaté riešenie do firmy, čím sa táto vybaví nástrojom pre lepšiu konkurencieschopnosť. Toto zvýrazňuje potrebu aktívne sa zúčastňovať na normalizácii, a nie ju iba trpieť.

Uvedené faktory poukazujú na charakter normy ako kolektívneho diela viacerých organizácií, jednotlivcov a záujmových skupín (dobrovoľných aj profesionálnych), pričom ich úsilie je zastrešované a koordinované príslušnou štandardizačnou organizáciou (porov. časť 2.1.4). Pre zainteresovanú organizáciu, firmu alebo záujmovú skupinu, je výhodné aktívne sa podieľať na príprave a následnej aplikácii technickej normy predovšetkým vzhľadom na faktory inovácie, prenosu nových technológií a úspešného strategického rozhodovania.

Štandardizácia je pomerne komplexný proces, ktorého konkrétne aktivity sa líšia v závislosti od druhu normy a pravidiel platných pre tú-ktorú štandardizačnú organizáciu. Vo všeobecnosti však možno vyčleniť niekoľko základných (typických) etáp [30], v ktorých sa proces štandardizácie najčastejšie vykonáva:

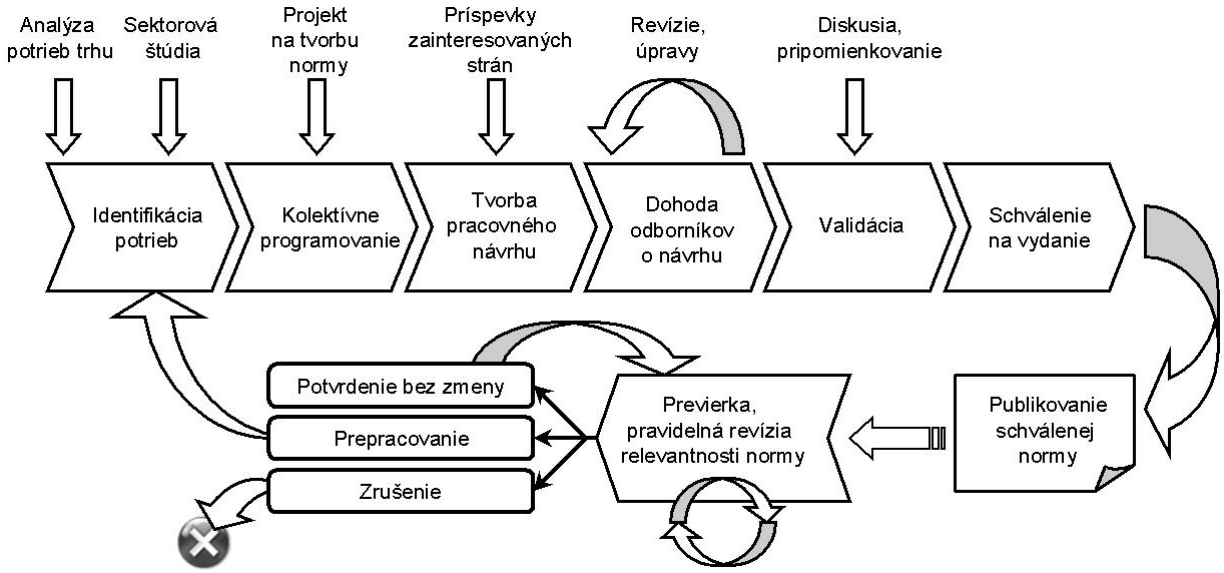
1. *Návrh normy*. Od myšlienky k pracovnému návrhu.

- Identifikácia potreby trhu pre vznik nového štandardu, ktorú určuje dostatočne reprezentatívne množstvo relevantných partnerov, organizácií pôsobiacich v danej oblasti.
- Definícia požiadaviek (komerčných, používateľských, funkčných, resp. technických), ktoré sú vyjadrením konkrétnej potreby trhu a slúžia ako podklad pre vypracovanie normy.
- Prvý pracovný návrh (draft specification) normy, ktorý vznikne ako konsenzus partnerov zainteresovaných na tvorbe normy. Návrh je formulovaný skupinou expertov, ustanovenou partnermi.

2. *Rozpracovanie a oficiálne vydanie*. Od návrhu k výslednej formulácii normy.
   - Proces schvaľovania návrhu v širšom konzorciu odborníkov a zainteresovaných skupín, obyčajne koordinovaných príslušnou štandardizačnou organizáciou.
   - Posudzuje sa širší dopad normy na danú oblasť i mimo nej, a tiež aj na celkovú štruktúru existujúcich noriem. Prípadné konflikty sa riešia prepracovaním návrhu normy a jeho opätovným posúdením v rámci tejto etapy.
   - Oficiálne vydanie normy jej začlenením do katalógu noriem spravovaných danou štandardizačnou organizáciou.
3. *Zavedenie do praxe*. Od formulácie normy k jej praktickej implementácii.
   - Špecifikácia testovania a certifikácie, ktorá sa najčastejšie publikuje vo forme dodatkov k norme. Môže obsahovať aj viac či menej podrobné návody na praktickú implementáciu normy a príklady typickej (referenčnej) implementácie. Týmito dodatkami sa zabezpečuje interoperabilita, čiže súlad medzi rôznymi implementáciami.
   - Proces priebežného a periodického posudzovania súladu normy s praxou, pravidelné vyhodnocovanie aplikácie normy, najmä vzhľadom k meniacim sa potrebám a požiadavkám trhu. Výsledkom tohto procesu môžu byť návrhy na aktualizáciu, zmeny a doplnenia normy (prípadne aj návrh na zrušenie normy pre jej neaktuálnosť).

Procesne orientovaný pohľad na štandardizáciu dovoľuje riadiť aktivity vytvárania normy pomocou samostatného projektu, v rámci ktorého sa dá plánovať časová náročnosť jednotlivých aktivít, optimalizovať rozloženie zdrojov, stanovovať priority a verifikovať výsledky čiastkových činností.

Treba pripomenúť, že uvedený proces štandardizácie je zovšeobecnením najdôležitejších a typických aktivít tvorby a aplikácie noriem. Rôzne štandardizačné organizácie však často definujú vlastné špecifické činnosti, a to v závislosti od pôsobnosti organizácie (medzinárodná, regionálna, národná), od oblasti (priemysel, obchod, manažment, atď.), miery formalizácie (formálne normy, technické špecifikácie, dohody konzorcií, technické správy, odporúčania), a podobne. Naviac, štandardizácia v širšom zmysle zahŕňa aj osobitné spôsoby tvorby, modifikácie a adaptácie noriem, pod ktoré možno zaradiť harmonizáciu noriem, respektíve preberanie noriem definovaných na úrovni vyššej alebo nižšej teritoriálnej platnosti (porov. v časti 2.1.2).



Obr. 20 Schéma životného cyklu normy

Počas procesu štandardizácie sa mení a vyvíja vytváraná norma, preto sa dá popísať tzv. *životný cyklus normy* [34]. Tento cyklus, schematicky zobrazený na Obr. 2-1, sa vo všeobecnosti skladá zo siedmich hlavných etáp:

1. *Identifikácia potrieb partnerov*. Analýza potreby trhu a technicko-ekonomická štúdia po sektoroch, ktorá má odpovedať na dve základné otázky:
   - Poskytne norma technické a ekonomické „plus“ danému sektoru, oblasti?
   - Sú k dispozícii znalosti potrebné na vypracovanie normy?
2. *Kolektívne programovanie*, návrh a správa projektu na tvorbu normy. Odrážať sa tu majú identifikované potreby a priority definované všetkými zúčastnenými

stranami, nasleduje formálne zaevidovanie projektu (pracovného programu na tvorbu normy) príslušnou štandardizačnou organizáciou.

3. *Vypracovanie pracovného návrhu normy* zainteresovanými stranami, zastúpenými odborníkmi (vrátane výrobcov, distribútorov, používateľov, spotrebiteľov, administráciou, laboratóriami, atď.), ktorí sú zhromaždení v príslušnej technickej komisii ustanovenej štandardizačnou organizáciou na prípravu normy.
4. *Dohoda odborníkov o návrhu normy*. Revízie a modifikácie návrhu normy, schválenie jej finálnej podoby v rámci technickej komisie.
5. *Validácia (potvrdenie)*. Široká diskusia na národnej alebo medzinárodnej úrovni formou verejného pripomienkovania, ktorá zahrnie všetkých ekonomických partnerov, aby sa zaistilo, že návrh normy je v súlade so všeobecným záujmom a nevyvolá žiadne závažné námietky. Preskúmanie pripomienok. Dokončenie definitívneho textu návrhu normy.
6. *Schválenie textu na vydanie ako normy*. Publikovanie normy k katalógu štandardizačnej organizácie.
7. *Previerka*. Používanie normy vytvára podmienky na pravidelnú revíziu jej relevantnosti štandardizačnou organizáciou, čo umožňuje stanoviť čas, keď je potrebné normu prispôsobiť novým potrebám. Po previerke môže byť norma potvrdená bez zmeny, daná na revíziu alebo na zrušenie.

Tvorba noriem je teda iteratívny proces. Pravidelným monitorovaním a vyhodnocovaním prínosov normiem implementovaných v praxi a následnými korekciami sa zabezpečuje aktuálnosť, súlad s progresívnymi technológiami a trendmi, a najmä s reálnymi potrebami organizácií pôsobiacich v danom sektore.

Štandardizačné organizácie

Organizácie zaoberajúce sa štandardizáciou, riadením štandardizačných aktivít a zverejňovaním noriem sa členia podľa teritoriálnej pôsobnosti na medzinárodné, regionálne a národné. Koordinácia prác na všetkých troch úrovniach sa zabezpečuje spoločnými štruktúrami a dohodami o spolupráci. U nás je hlavnou štandardizačnou organizáciou Slovenský ústav technickej normalizácie, ktorý je aj reprezentantom Slovenskej republiky v príslušných medzinárodných organizáciách.

SÚTN, Slovenský ústav technickej normalizácie, http://www.sutn.sk

SÚTN bol zriadený Úradom pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky (ÚNMS SR, http://www.unms.sk) dňa 1. januára 1993. Od 1. 1. 1999 je SÚTN štátnou príspevkovou organizáciou hospodáriacou podľa vlastného rozpočtu, ktorý schvaľuje zriaďovateľ, čiže ÚNMS SR.

Činnosť SÚTN sa riadi zákonom č. 264/1999 Z. z., ktorý poveril SÚTN funkciou národného normalizačného orgánu Slovenskej republiky. Na základe tohto zákona je SÚTN určenou právnickou osobou na tvorbu, schvaľovanie a vydávanie slovenských technických noriem, plnenie povinností vyplývajúcich z medzinárodných zmlúv a členstva v medzinárodných a európskych normalizačných organizáciách (ISO, IEC, CEN, CENELEC a ETSI).

Hlavnou úlohou SÚTN v súčasnosti je zabezpečenie plnej harmonizácie národnej sústavy technických noriem preberaním európskych noriem a postupné aktívne zapojenie sa do tvorby európskych noriem [33]. V tomto kontexte sa činnosť SÚTN zameriava na tvorbu a správu slovenských technických noriem STN (porov. v časti 2.1.2), vydávanie a distribúciu slovenských technických noriem a iných dokumentov súvisiacich s normalizáciou, plnenie funkcií národného informačného strediska a národného normalizačného orgánu.

V ďalšom stručne predstavíme niektoré vplyvné a ťažiskové štandardizačné organizácie, rozdelené podľa teritoriálnej pôsobnosti (od medzinárodnej po národnú úroveň). Sústredíme sa na organizácie, ktorých členom je SÚTN, a tiež tie, ktoré sa aktívne zaoberajú štandardizáciou v oblasti elektrotechniky, elektroniky, informatiky a IKT, vrátane štandardov pre riadenie IT prostredia a služieb.

Medzinárodná normalizácia

ISO, Medzinárodná organizácia pre normalizáciu
International Organization for Standardization, http://www.iso.org

ISO je svetová federácia národných normalizačných orgánov, je v súčasnosti zrejme najvýznamnejšou autoritou v oblasti normalizácie. Bola založená v roku 1947, jej centrálny sekretariát sídli v Ženeve, Švajčiarsko, odkiaľ sa koordinuje celý systém.

Pokrýva 163 krajín, za každú krajinu je členom ISO jedna normalizačná inštitúcia. Prostredníctvom SÚTN je Slovenská republika riadnym členom ISO od 1. júla 1993.

ISO je mimovládna organizácia, ktorá v oblasti normalizácie spája verejné a vládne inštitúcie so súkromným sektorom. Na jednej strane, mnoho členov ISO je súčasťou vládnej štruktúry svojich krajín, alebo má mandát od príslušnej vlády. Na druhej strane, iní členovia ISO majú zázemie v súkromnom sektore, kde boli zvolení národným spoločenstvom priemyselných inštitúcií. Teda ISO umožňuje dosiahnuť konsenzus, kde budú splnene požiadavky podnikov a aj širšie potreby spoločnosti.

Úlohou ISO je podporovať rozvoj normalizácie a súvisiacich činností v celosvetovom meradle s cieľom uľahčiť medzinárodnú výmenu tovaru a služieb a dosiahnuť spojenectvo v intelektuálnej, vedeckej, technickej a hospodárskej oblasti. Činnosť ISO je zameraná na všetky oblasti normalizácie [8], pričom oblasť elektrotechniky, elektroniky a informačných technológií sa rieši v úzkej spolupráci s organizáciou IEC.

Vývoj medzinárodných noriem ISO je organizovaný do štruktúry technických komisií a podkomisií [6]. V súčasnosti je aktívnych 210 technických komisií, 519 subkomisií a 2443 pracovných skupín v najrôznejších oblastiach, napríklad poľnohospodárstvo a konštrukcia, strojné inžinierstvo, chémia, finančné služby, lekárske pomôcky, atď. Oblasť informačných technológií zastrešuje komisia JTC1, ktorá je spoločnou komisiou organizácií ISO a IEC. V rámci tejto komisie sa vyvíja aj norma ISO/IEC 20000, zameraná na oblasť riadenia IT prostredia.

Samotný vývoj ISO normy sa člení do stupňov [9], ktoré zodpovedajú životnému cyklu normy (porov. časť 2.1.3):

1. *Návrh* (Proposal stage), prijatie návrhu nového projektu na tvorbu normy, hlasovanie o prijatí na riešenie, určenie vedúceho projektu (project leader).
2. *Príprava* (Preparatory stage), vytvorenie pracovnej skupiny (working group) v rámci niektorej z technických komisií, tvorba pracovného návrhu (working draft) novej normy.
3. *Komisia* (Committee stage), posúdenie pracovného návrhu normy v technickej komisii, hlasovanie o prijatí, registrácia návrhu na úrovni centrálneho sekretariátu ISO. Publikovanie návrhu vo forme predbežnej medzinárodnej normy (DIS – draft International Standard).
4. *Pripomienky* (Enquiry stage), ISO sekretariát distribuuje DIS normy medzi členské organizácie ISO na pripomienkovanie a hlasovanie o prijatí. Technická

komisia zapracuje získané pripomienky do normy. Tento proces trvá päť mesiacov. Po schválení dvoma tretinami členov ISO je norma publikovaná vo forme finálnej predbežnej medzinárodnej normy (FDIS – final draft International Standard).

5. *Schvaľovanie* (Approval stage), ISO sekretariát distribuuje FDIS normy medzi členské organizácie ISO na záverečné hlasovanie o prijatí (áno / nie). Tento proces trvá dva mesiace. Po schválení dvoma tretinami členov ISO je norma pripravená na zverejnenie. Ak sa FDIS neschváli, posiela sa späť technickej komisii na prepacovanie.
6. *Zverejnenie* (Publication stage), ISO sekretariát publikuje normu v ISO katalógu.
7. *Priebežné posudzovanie* (Review – Confirmation, Revision, Withdrawal stages). Všetky publikované ISO normy sa znova posudzujú v období do troch rokov po zverejnení, a následne každých päť rokov po prvom posúdení. Jednoduchá väčšina členov ISO rozhoduje, či norma môže byť potvrdená bez zmeny (Confirmation), či sa má aktualizovať (Revision) alebo stiahnuť (Withdrawal).

Celkovo bolo od roku 1949 až po súčasnosť vydaných viac než 18000 ISO noriem, v roku 2009 pribudlo 1038 noriem a štandardizačných dokumentov.

IEC, Medzinárodná elektrotechnická komisia
International Electrotechnical Commission, http://www.iec.ch

IEC je medzinárodnou organizáciou s celosvetovou pôsobnosťou, ktorá pripravuje a vydáva medzinárodné štandardy pre všetky elektrické, elektronické a súvisiace technológie, súhrnne označované pojmom elektrotechnológie. Premet činnosti IEC zahŕňa elektrotechnológie vrátane elektroniky, magnetizmu a elektromagnetiznu, alektroakustiky, telekomunikácií, výroby a rozvodu energie, a tiež súvisiace všeobecné disciplíny ako je terminológia, symboly, meranie a funkčné parametre, závislosti, návrh a vývoj, bezpečnosť a ochrana životného prostredia. Do sféry záujmu IEC spadá aj oblasť informatiky a riadenia IT prostredia.

IEC bola založená v roku 1906 v Londýne, od roku 1948 sídli riaditeľstvo IEC v Ženeve. Členmi IEC sú národné komisie (committies), vždy jedna za každú krajinu. V súčasnosti je v IEC združených 59 riadnych a 22 asociovaných členov. Ich úlohou je medzinárodná odborná spolupráca na tvorbe noriem a presadzovanie spoločne

vytvorených štandardov v jednotlivých krajinách. Slovenská republika, v zastúpení SÚTN , je riadnym členom IEC od 1. januára 2003.

Štandardizácia IEC sa uskutočňuje, podobne ako v organizácii ISO, v rámci technických komisií, pracovných skupín a projektov pre jednotlivé vytvárné normy. Ku koncu roka 2009 bolo aktívnych 174 technických komisií a vyše 600 pracovných skupín a projektov. Okrem členských národných komisií IEC úzko spolupracuje s mnohými medzinárodnými a regionálnymi štandardizačnými organizáciami, napr. s ISO, ITU, WHO, WTO, CENELEC, atď. Pre oblasť informačných technológií bola na základe dohody s ISO v roku 1986 vytvorená spoločná komisia ISO/IEC JTC1 (viď aj vyššie pri popise ISO), v rámci ktorej sa IEC podieľa aj na vývoji a správe normy ISO/IEC 20000. Od svojho vzniku IEC publikovala a spravuje vše 6000 štandardizačných dokumentov – medzinárodných noriem, technických špecifikácií a správ. V roku 2009 bolo v IEC publikovaných 441 štandardizačných dokumentov.

ITU, Medzinárodná telekomunikačná únia
International Telecommunication Union, http://www.itu.int

ITU je špecializovanou agentúrou Organizácie spojených národov v oblasti telekomunikácií a rádiokomunkácií so sídlom v Ženeve. Vznikla v roku 1865 (vtedy pod názvom Medzinárodná telegrafná únia), agentúrou OSN je od roku 1947. ITU je celosvetovou medzivládnou organizáciou s účasťou členských krajín OSN a rôznych organizácií pôsobiacich v sektoroch telekomunikácií a rádiokomunkácií. V súčasnosti ITU reprezentuje 191 členských štátov a viac než 700 členov sektorov. Slovenská republika je riadnym členom ITU od 23. februára 1993.

Organizačne sa ITU člení na tri sektory, z ktorých najvýznamnejším z hľadiska normalizácie je sektor štandardizácie telekomunikácií (ITU-T) [21]. Tento sektor vydáva medzinárodné odporúčania, technické špecifikácie a štandardy v oblasti telekomunikačných systémov, informačných a kommunikačných sietí, organizované do hierarchickej štruktúry 23 skupín [20]. V súčasnosti je publikovaných vyše 3000 odporúčaní pokrývajúcich definíciu telekomunikačných služieb, sieťovú achitektúru a bezpečnosť, rôzne druhy sietí od širokopásmových DSL cez optické siete a siete novej generácie, a mnoho ďalších aspektov moderného využívania informačných a komunikačných technológií. Odporúčania ITU sú voľne a bez poplatku prístupné vo formáte PDF.

IEEE, Inštitút pre elektrotechnické a elektronické inžinierstvo
Institute for Electrical and Electronics Engineers, http://www.ieee.org

IEEE je medzinárodná nezisková profesná organizácia usilujúca o vzostup technológií súvisiacich s elektrotechnikou. Vznikla v USA v roku 1963, v súčasnosti má viac ako 395 tisíc členov zo 160 krajín sveta (45% členov je z iných krajín ako z USA). Sídlo IEEE je v USA v štáte New York.

Normalizácii sa v rámci IEEE venuje samostatná organizácia s názvom IEEE Standards Association (IEEE-SA, http://standards.ieee.org). V súčasnosti spravuje cca 900 platných publikovaných štandardov, ďalších zhruba 500 štandardov je vo vývoji. Ročne sa v rámci IEEE-SA spracuje okolo 200 návrhov štandardov.

Štandardy IEEE-SA pokrývajú široké spektrum oblastí, napríklad počítačové siete, inteligentné systémy na riadenie dopravy, distribuovanú produkciu obnoviteľnej energie, systémy na prenos a výmenu údajov, a ďalšie. Jedným z dôležitých štandardov IEEE je skupina štandardov IEEE 802 LAN/WAN, ktorá zahŕňa IEEE 802.3 Ethernet a IEEE 802.11 Wireless Networking štandardy.

W3C, Konzorcium svetového webu
World Wide Web Consortium, http://www.w3.org

W3C je medzinárodné združenie záujmových organizácií a jednotlivcov, ktoré sa zaoberá tvorbou štandardov pre prostredie webu (World Wide Web, skr. WWW, resp. W3). Bolo založené v roku 1994 na pôde Massachusettského technologického inštitútu v USA, v spolupráci s Európskou organizáciou pre jadrový výskum CERN a s podporou Európskej komisie a americkej Agentúry pre výskum pokročilých obranných projektov DARPA.

W3C definuje a spravuje štandardy definujúce základy WWW, architektúry a návrhu web aplikácií (napr. HTML, XHTML, DOM, CSS), sémantického webu (napr. RDF, OWL, WSMO, SKOS, SPARQL), XML technológií (XML, XSLT, XPath, XQuery), webových služieb (SOAP, WSDL), a podobne. Práca na štandardoch sa vykonáva v pracovných, záujmových a koordinačných skupinách členených podľa tématických oblastí.

Proces štandardizácie W3C sa uskutočňuje v piatich fázach, zodpovedajúcich životnému cyklu vytváraného štandardu. Začína ako pracovný návrh (Working Draft), nasleduje posledná výzva na úpravu pracovného návrhu (Last Call Working Draft), kandidát na odporúčanie (Candidate Recommendation, CR) a návrh odporúčania

(Proposed Recommendation, PR). Poslednou fázou štandardu je odporúčanie (Recommendation, REC), ktorého verzie sa môžu publikovať vo viacerých vydaniach (Editions), prípadne môžu byť doplnené poznámkami (Notes). V súčasnosti W3C spravuje viac ako 1500 štandardizačných dokumentov, z toho okolo 200 odporúčaní. V roku 2010 bolo zatiaľ (do konca augusta) vydaných 12 odporúčaní.

Regionálna normalizácia v Európe

CEN, Európsky výbor pre normalizáciu
European Committee for Standardization, http://www.cen.eu

CEN je najdôležitejšou normalizačnou inštitúciou v Európe. Založená bola v roku 1961 a sídli v Bruseli, v Belgicku. CEN je nezisková organizácia, ktorá združuje 31 národných členov vrátane Slovenskej republiky (v zastúpení SÚTN). Pridruženými členmi sú aj niektoré krajiny mimo Európskej únie a európskeho hospodárskeho priestoru, napríklad Rusko, Ukrajina, Egypt, Turecko, Austrália, atď.

Náplňou práce CEN je tvorba a správa európskych noriem EN vo všetkých oblastiach, v ktorých sa štandardizácia uplatňuje, okrem oblastí elektrotechniky (ktorú zastrešuje CENELEC) a telekomunikácií (ktorou sa zaoberá ETSI). Sú to napríklad oblasti zdravotníctva, výživy, energie, materiálov, inovácií, služieb, a ďalšie. CEN svojou štandardizačnou činnosťou v týchto oblastiach vytvára platformu pre progresívny a koordinovaný vývoj európskych krajín vo viac-menej jednotnom ekonomicko-sociálnom priestore.

Za koordináciu, plánovanie a programovanie prác zodpovedá Technická rada (Technical Board). Práce vykonávajú odborné orgány, technické komisie, subkomisie a pracovné skupiny, ktorých sekretariáty sú decentralizované v členských krajinách. V súčasnosti je aktívnych do 300 technických komisií a do 1400 pracovných skupín. Celkovo spravuje CEN cca 14000 štandardizačných dokumentov, ročne sa vytvorí okolo 1000-1500 noriem EN, technických špecifikácií a ďalších typov dokumentov.

CENELEC, Európsky výbor pre normalizáciu v elektrotechnike
European Committee for Electrotechnical Standardization, http://www.cenelec.eu

CENELEC je nezisková organizácia pôsobiaca ako hlavná európska štandardizačná inštitúcia pre oblasť elektrotechniky. Spolu s CEN a ETSI tvorí *európsky systém technickej štandardizácie*. CENELEC bola založená v roku 1973 a

sídli v Bruseli. Plné členstvo v CENELEC má 31 krajín Európskej únie a európskeho hospodárskeho priestoru, vrátane Slovenskej republiky (v zastúpení SÚTN). Pridružené členstvo má ďalších 12 krajín mimo EÚ.

Práca CENELEC sa sústreďuje najmä na tvorbu dvoch hlavných typov štandardizačných dokumentov, a to na európske normy EN a harmonizačné dokumenty HD. Tieto dokumenty majú charakter záväzných noriem, ktoré sú členské krajiny CENELEC povinné implementovať a ktorým musia prispôsobiť iné národné normy. Okrem týchto dvoch typov dokumentov publikuje CENELEC technické špecifikácie, technické správy, manuály a dohody z pracovných skupín.

Formát označenia noriem EN je v zásade rovnaký ako pri normách ISO a IEC (porov. v časti 2.1.2), pozostáva z označenia EN, poradového čísla normy a dvojbodkou oddeleného roku vydania, napr. EN 50225:1996. Európske normy EN pre oblasť elektrotechniky sú číslované v rozsahu od 40000 do 69999. Rozsah od 40000 do 44999 je vymedzený pre spoločné CEN/CENELEC normy z oblasti informačných technológií, od 45000 do 49999 pre spoločné CEN/CENELEC normy mimo oblasti informačných technológií, od 50000 do 59999 pe samostatné štandardizačné projekty CENELEC a od 60000 do 69999 pre CENELEC implementácie noriem IEC.

ETSI, Európsky inštitút pre telekomunikačné normy
European Telecommunications Standards Institute, http://www.etsi.org

ETSI je nezisková organizácia, ktorá vypracúva európske normy ETS pre telekomunikačnú oblasť. Vznikla v roku 1988 a sídli vo Francúzsku v Sophia Antipolis. Združuje do 700 členov v rôznych kategóriách z vyše 60 krajín. Členmi ETSI za Slovenskú republiku sú Ministerstvo dopravy, pôšt a telekomunikácií SR a Slovak Telecom, a.s. ETSI v rámci európskeho systému technickej štandardizácie úzko spolupracuje s organizáciami CEN a CENELEC.

Normy ETS sú zamerané na informačné a komunikačné technológie v oblastiach telekomunikácií, vysielania a masmédií, inteligentných dopravných systémov a medicínskej elektroniky. ETSI sa venuje aj progresívnym a inovatívnym smerom v techológiách Internetu (Internet of Things), softvérového inžinierstva a IT (Grid computing, Clouds), prenosu digitálneho obsahu (Media Content Distribution), inžinierstva v oblasti životného prostredia, a podobne [36]. Celkovo ETSI spravuje do 24000 štandardizačných dokumentov rôznych typov, z toho je 610 ETS noriem. V

roku 2009 bolo vypracovaných 2480 štandardizačných dokumentov, z toho bolo 26 ETS noriem, 2192 technických špecifikácií, 191 technických správ a 71 ostatných typov dokumentov.

Národná normalizácia

Každá krajina má vlastný normalizačný systém, ktorý je obyčajne koordinovaný na úrovni vlády (napr. u nás ÚNMS SR a SÚTN). Ústredná alebo najreprezentatívnejšia národná normalizačná inštitúcia sa zúčastňuje na práci v regionálnych a medzinárodných organizáciách, pričom tam presadzuje záujmy danej krajiny. Zároveň je úlohou národnej normalizačnej inštitúcie aj aplikácia noriem z vyšších úrovní do prostredia vlastnej krajiny, napríklad podľa princípu harmonizácie noriem v rámci Európskej únie, alebo podľa záväzkov vyplývajúcich z členstva národnej inštitúcie v medzinárodných organizáciách.

V ďalšom bližšie predstavíme národné normalizačné organizácie USA a Veľkej Británie, ktoré možno považovať za azda najvplyvnejšie aj v celosvetovom kontexte (t.j. normy a dokumenty vytvárané týmito organizáciami sa často využívajú ako podklady pre tvorbu regionálnych alebo aj medzinárodných noriem). Okrem týchto dvoch organizácií majú pomerne veľký vplyv normalizačné organizácie Nemecka (Deutsches Institut für Normung, http://www.din.de), Francúzska (Association française de normalisation, http://www.afnor.org), alebo Japonska (Japanese Industrial Standards Committee, http://www.jisc.go.jp).

ANSI, Americký národný štandardizačný inštitút
American National Standards Institute, http://www.ansi.org

ANSI je národná štandardizačná organizácia USA. Vznikla v roku 1918 a pôsobí ako súkromná nezisková organizácia, ktorá vytvára a spravuje technické normy a priemyselné štandardy v USA. Ústredie ANSI sídli vo Washingtone, D.C., pracovné úrady sú lokalizované v New Yorku.

V ANSI sa rozlišuje šesť typov členstva. Členmi sú vládne agentúry USA, záujmové neziskové organizácie, komerčné spoločnosti a korporácie, výskumné a vzdelávacie inštitúcie, medzinárodné organizácie aj jednotlivci – spolu viac než 125 tisíc spoločností a 3,5 milióna individuálnych členov.

Činnosť ANSI pokrýva tvorbu a správu štandardov vo všetkých oblastiach. V rámci domácej, národnej štandardizácie v rámci USA je vytvorených sedem panelových fór zameraných na normy v oblasti bezpečnosti, nanotechnológií, zdravotnej starostlivosti, osobnej identity, biopalív, chémie a nukleárnej energie. Na regionálnej úrovni pôsobí ANSI v programoch štandardizácie pre Európu, Stredný východ a Afriku, a pre Ázijsko-Pacifické teritórium. Na medzinárodnej úrovni je ANSI popredným a aktívnym členom organizácií ISO a IEC. Zúčastňuje sa na celom technickom programe oboch medzinárodných organizácií a riadi okolo 20% komisií, subkomisií a pracovných skupín. Normy ANSI sa v mnohých prípadoch presadzujú v ISO a/alebo v IEC ako normy medzinárodné. Príkladom sú kódové tabuľky ANSI (ASA X3.4-1963), ktoré boli prijaté ako skupina noriem ISO 8859, ďalej možno spomenúť štandardizáciu programovacieho jazyka C (ANSI X3.159-1989) alebo iniciatívu ANSI na sprístupnenie ISO noriem pomocou on-line knižnice [4].

BSI, Britský štandardizačný inštitút
British Standards Institution, http://www.bsigroup.com

BSI je národná normalizačná organizácia Spojeného kráľovstva Veľkej Británie a Severného Írska, ktorá pôsobí ako nezávislá a nezisková inštitúcia. Jej základnou činnosťou je produkcia štandardov a dodávanie služieb spojených so štandardmi. BSI bola založená v Londýne v roku 1901 a je tak prvou národnou štandardizačnou organizáciou na svete. Od svojho vzniku postupne rozširovala svoju štandardizačnú činnosť, roku 1929 získala kráľovskú listinu ako ocenenie svojej kvality a dôležitého postavenia. Revízia listiny v roku 1998 umožnila diverzifikáciu a rozšírenie štandardizačnej činnosti o ďalšie formy podnikania. Obchodné meno BSI sa zmenilo na BSI Group.

Normy BSI, označované ako BS (British Standard), sú vyvíjané pre dobrovoľné použitie a nepredpisujú žiadne nariadenia. Avšak rôzne zákony, predpisy a regulačné nariadenia môžu odkazovať na niektoré z týchto noriem a určiť zhodu s nimi ako povinnú. BSI Group zabezpečuje aj služby certifikácie a testovania zhody výrobkov a služieb s BS normami.

BSI Group, ako inštitúcia pre národné štandardy Veľkej Británie, je zodpovedná predovšetkým za tvorbu, správu a publikovanie britských štandardov. Je však aj aktívnym členom vo všetkých hlavných medzinárodných a európskych

organizáciách pre štandardy, napr. v ISO, IEC, CEN, CENELEC a ETSI, kde reprezentuje záujmy Veľkej Británie.

Formálne sú britské štandardy označované reťazcom BS XXXX[-P]:YYYY, kde BS znamená British Standard, XXXX je číslo štandardu, P je číslo časti štandardu (ak tento je rozdelený na viacero častí) a YYYY je rok publikovania. V prípade prebratých (harmonizovaných) noriem sa medzi označenie BS a číslo štandardu vkladajú pôvodné identifikačné označenia, z ktorých bola daná norma odvodená. Ako príklad možno uviesť normu pre formát a charakteristiky kreditných kariet, ktorá má v britskom systéme označenie BS EN ISO/IEC 7810:1996. Táto norma je vyvíjaná organizáciami ISO a IEC, pričom príslušná pracovná skupina je koordinovaná zástupcami BSI Group.

Škála oblastí, v ktorých BSI Group pripravuje normy, pokrýva prakticky všetky sféry života, v ktorý sa uplatňuje štandardizácia. V súčasnosti je v správe BSI Group celkovo viac ako 46000 noriem. Dôležitosť a kvalitu činnosti BSI Group dokumentuje skutočnosť, že viaceré BS normy boli prijaté na európskej a medzinárodnej úrovni a sú dnes široko akceptované. Okrem už spomínanej normy ISO/IEC 20000, ktorá pôvodne vznikla ako britská norma BS 15000, je to napríklad skupina noriem pre manažment systémov kvality ISO 9000 (pôvodne BS 5750), norma pre bezpečnosť informačných systémov ISO/IEC 27001 (pôvodne BS 7799), a viaceré ďalšie.

Záväznosť a legislatívny rámec noriem

V predchádzajúcich častiach sme viackrát spomínali, že normy nemajú v zásade záväzný charakter a ich dodržiavanie je dobrovoľné. To však neznamená, že používanie noriem je ľubovoľné a neriadi sa žiadnymi pravidlami. Naopak, existuje pomerne presný legislatívny rámec, ktorý funkciu a aplikáciu noriem v právnom zmysle vymedzuje. Do tohto rámca spadá definícia normy a jej typov, základné ustanovenia tvorby a dodržiavania noriem, určenie práv, povinností i zodpovednosti subjektov vytvárajúcich a aplikujúcich normy. Za širšiu súčasť legislatívneho rámca normalizácie možno považovať aj právnu špecifikáciu autorstva noriem, definovanie procesu posudzovania zhody a certifikácie.

Na Slovensku technickú normalizáciu legislatívne upravuje zákon č. 264/1999 Z. z. o technických požiadavkách na výrobky a o posudzovaní zhody, v znení ďalších nadväzujúcich zákonov. Tento zákon v § 7 ustanovuje, že zhoda s normami STN a

tiež dodržiavanie noriem STN sú dobrovoľné okrem prípadov, keď ich dodržiavanie vyžaduje tento zákon alebo iný technický predpis. Okrem toho zákon upravuje:

- spôsob ustanovenia technických požiadaviek na výrobky, ktoré by mohli ohroziť zdravie, bezpečnosť alebo majetok osôb, alebo životné prostredie,
- práva a povinnosti SÚTN ako právnickej osoby určenej na činnosti súvisiace s tvorbou, schvaľovaním a vydávaním slovenských technických noriem,
- postupy posudzovania zhody výrobkov s technickými požiadavkami noriem,
- práva a povinnosti subjektov, podnikateľov resp. zriadených právnických osôb, ktoré súvisia s posudzovaním zhody,
- z noriem vyplývajúce práva a povinnosti podnikateľov, ktorí vyrábajú, dovážajú alebo uvádzajú výrobky na trh,
- pôsobnosť ústredného orgánu štátnej správy a ďalších orgánov štátnej správy na úseku technickej normalizácie a posudzovania zhody,
- dohľad nad dodržiavaním zákona vrátane ukladania pokút.

Zákon č. 264 upravuje aj vzťah medzi slovenskými a inými normami, harmonizáciu a preberanie noriem. Podľa §4 tohto zákona sa medzinárodné alebo európske normy vydávajú a sú platné v Slovenskej republike iba ako normy STN a sú súčasťou sústavy slovenských technických noriem. Pri ich preberaní možno použiť všetky formy preberania určené medzinárodnými, resp. európskymi normalizačnými organizáciami.

Vo všeobecnosti platí, že norma je výsledkom práce kolektívu autorov [31]. Preto je norma chránená už v etapách návrhu autorským právom, vlastníkom ktorého je, v prípade národnej normy, národná normalizačná organizácia. Podobne je aj medzinárodná norma chránená autorským právom príslušnej normalizačnej organizácie. Právo na využívanie takejto normy pri preberaní do sústavy národných noriem je automaticky prenesené na tie národné normalizačné organizácie, ktoré sú členmi medzinárodnej organizácie a podieľajú sa na tvorbe národnej normy. Národná normalizačná organizácia musí prijať všetky opatrenia, ktoré sú potrebné na ochranu duševného vlastníctva medzinárodnej organizácie na území vlastného štátu. Každý návrh medzinárodnej normy a každá vydaná medzinárodná norma obsahuje ochrannú formulu so symbolom medzinárodnej ochrany, meno vydavateľa a rok vydania. Ak nie je v norme uvedené inak, žiadna norma ani jej časť nesmie byť reprodukovaná, zaznamenaná alebo šírená v akejkoľvek forme alebo akýmkoľvek

prostriedkom, elektronicky alebo mechanicky, bez písomného súhlasu príslušnej národnej alebo medzinárodnej normalizačnej organizácie.

V zákone č. 264 sa vymedzujú aj ďalšie pojmy, ktoré sú dôležité pre používanie noriem v praxi, kontrolu ich dodržiavania. Je to najmä autorizácia, posudzovanie zhody a certifikácia:

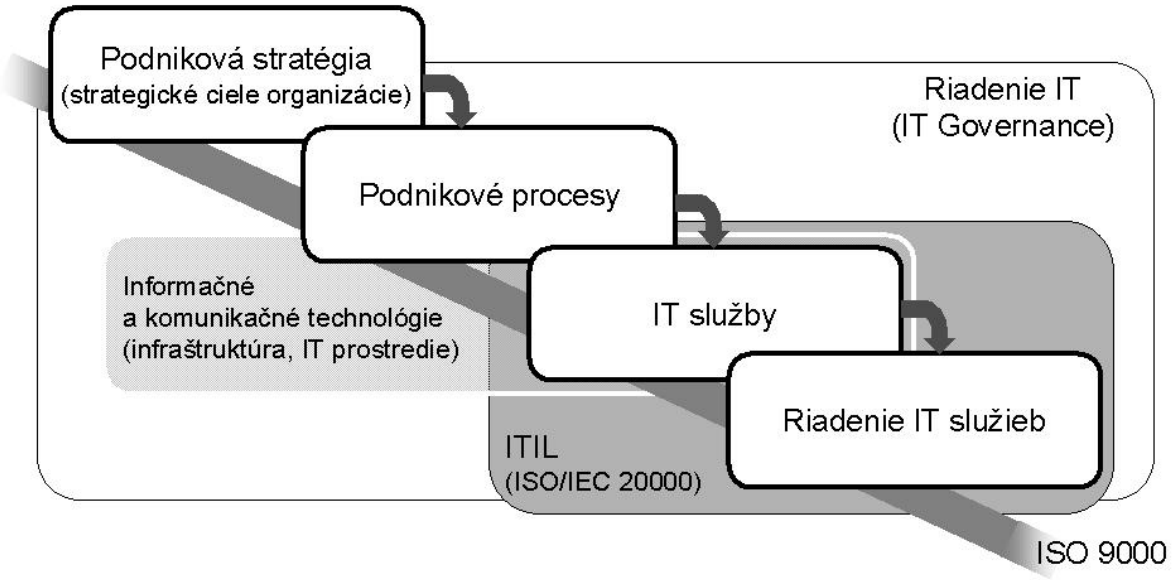
- *Autorizácia*, podľa § 11, je poverenie podnikateľa alebo inej právnickej osoby na vykonávanie posudzovania zhody. Poverenie vydáva úrad alebo príslušné ministerstvo rozhodnutím. Držiteľ poverenia (t.j. „autorizovaná osoba“) môže byť podľa rozsahu poverenia a obsahu činnosti pri posudzovaní zhody autorizovaný na certifikáciu, posudzovanie zhody, posudzovanie činností súvisiacich s výrobou určeného výrobku, na vykonávanie inšpekcie a na skúšanie určených výrobkov.
- *Posudzovanie zhody*, podľa § 12, je zisťovanie, či skutočné vlastnosti určeného výrobku zodpovedajú ustanoveným technickým požiadavkám na určený výrobok. Na posudzovanie zhody sa používajú presne stanovené postupy, ktoré sú v §12 uvedené v odsekoch 3 a 4. Výsledkom úspešného posúdenia zhody je výrobcom alebo dovozcom vydané *vyhlásenie o zhode* (§13 zákona č. 264), ktoré je podmienkou uvedenia výrobku na národný trh.
- *Certifikácia*, podľa § 14, je činnosť autorizovanej osoby, ktorá vydaním certifikátu osvedčí, že vlastnosti určeného výrobku a/alebo činnosti súvisiace s jeho výrobou sú v súlade s technickými požiadavkami na určené výrobky v technických predpisoch.

V oblasti informačných technológií sú procesy posudzovania zhody a certifikácie podľa národných noriem STN a prevzatých medzinárodných noriem rovnaké ako v iných oblastiach. Proces certifikácie a súvisiacich činností, spolu s postupom cerifikácie na normu ISO/IEC 20000, podrobnejšie popisujeme v časti 2.2.7.

Normalizácia v oblasti IT prostredia a služieb

IT prostredie je možné charakterizovať ako infraštruktúru, v rámci ktorej sa využívajú informačné a komunikačné technológie v danej organizácii na dosiahnutie špecifických podnikových cieľov (t.j. na tvorbu zisku, dlhodobý rozvoj, a pod.). Ciele organizácie sa definujú na úrovni *podnikovej stratégie*, čiže koncepcie jej zamerania v strednodobom a dlhodobom horizonte. Stratégia okrem iného definuje, čo je

predmetom podnikania, akými činnosťami sa organizácia zaoberá, ako je riadená, aké sú jej ciele v oblasti marketingu, obchodu, výroby, prevádzky, financií, atď. Podniková stratégia sa následne konkretizuje a realizuje pomocou príslušných *podnikových procesov* (business processes), čiže postupností aktivít, činností a úloh potrebných na vytvorenie určitého produktu alebo služby pre konkrétneho zákazníka. Konkrétna podoba podnikových procesov je daná prijatou podnikovou stratégiou, pričom kritériom kvality a adekvátnosti procesov je miera súladu so strategickými cieľmi organizácie.



Obr. 21 Schéma postupného riadenia služieb informačných technológií

V súčasnosti je prakticky nevyhnutné pre zmysluplné a efektívne fungovanie podnikových procesov využívať rôzne služby informačných a komunikačných technológií, skrátene nazývané *IT službami*. Všetky tieto služby sú prevádzkované na konkrétnej *infraštruktúre informačných a komunikačných technológií*, ktorá v súhrne tvorí IT prostredie organizácie. Infraštruktúra IT služieb je vždy určitým spôsobom *riadená*, pričom za jej riadenie je obyčajne zodpovedný špecializovaný IKT úsek organizácie. Úlohou riadenia IT prostredia je zosúladenie jednotlivých komponentov infraštruktúry tak, aby boli čo najvhodnejšie, efektívne a optimálne podporované podnikové procesy organizácie. V konečnom dôsledku má teda riadenie IT prostredia podporovať podnikovú stratégiu organizácie, ako je to schématicky znázornené hierarchiou na Obr. 2-2.

Celkové riadenie prostriedkov IT však nie je obmedzené iba na riadenie samotnej technickej a technologickej podstaty infraštruktúry IKT. Pre správne fungovanie IT služieb tak, aby boli v súlade s podnikovými procesmi a strategickými cieľmi organizácie, je totiž potrebné určitým spôsobom riadiť (monitorovať, kontrolovať a usmerňovať) aj vlastné IT služby, kvôli ktorým táto infraštruktúra IKT existuje. Toto komplexné riadenie sa nazýva *riadenie IT služieb* (angl. IT Service Management, ITSM) [15]. Štandardizačným rámcom pre riadenie IT služieb je v súčasnosti predovšetkým knižnica ITIL.

Ak je riadenie IKT rozšírené z úrovne IT služieb a podpornej infraštruktúry aj na podnikové procesy a strategické ciele organizácie, t.j. je chápané z pozície vrcholového manažmentu ako súčasť celkového riadenia organizácie zameraného na dosahovanie globálnych cieľov [22], potom sa označuje všeobecnejším termínom *riadenie IT*. Ako medzinárodný metodický rámec pre štandardizáciu procesov riadenia IT sa používa metodika COBIT [5]. Súčasťou riadenia IT sú však aj požiadavky na kvalitu IT služieb a podpornej infraštruktúry, primeraná úroveň informačnej bezpečnosti, vhodné formálne vyjadrenie podnikových procesov na zabezpečenie ich súladu s IT službami aj so strategickými cieľmi organizácie. Najdôležitejšie normy, ktoré tvoria referenčný rámec pre tieto čiastkové úlohy riadenia IT a ITSM, predstavíme v nasledujúcich častiach tejto kapitoly.

Vývoj noriem v oblasti manažmentu IT služieb

Narastajúca závislosť podnikov a rôznych organizácií na IKT sa začala intenzívne pociťovať začiatkom 80. rokov 20. storočia [16]. Z tejto závislosti zákonite vznikol tlak na definovanie širšie akceptovateľných požiadaviek na kvalitu IT služieb, ktorý vyústil do poverenia od vlády Veľkej Británie pre agentúru CCTA (Central Computer and Telecommunications Agency[3]) na vypracovanie záväznej príručky pre dodávateľov IT služieb pre britskú vládu. Vydaných bolo postupne 46 zväzkov, ktoré sústreďovali najlepšie skúsenosti (angl. Best Practices) z oblasti riadenia IT služieb a infraštruktúry pre potreby britských vládnych úradov a podnikateľských subjektov dodávajúcich IT služby vláde. Tento súbor bol v roku vydaný koncom 80. rokov, pôvodne pod názvom GITIM (Government Information Technology Infrastructure Management), ktorý sa neskôr zmenil na ITIL (IT Infrastructure Library), verzia 1.

[3] CCTA je od r. 2000 súčasťou Office of Government Commerce, http://www.ogc.gov.uk.

Počas 90. rokov sa rámec ITIL rozšíril medzi mnohé organizácie súkromného aj verejného sektora a stal sa akceptovaným „de facto“ štandardom v oblasti ITSM. V roku 2001 bola vydaná verzia 2 knižnice ITIL, ktorá bola už aj formálne začlenená do štruktúry britských noriem pod označením BS 15000 IT service management. Táto norma pozostáva z častí:

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

Tieto dve základné normy, ktoré definujú disciplínu ITSM, boli doplnené ďalšími dvoma vysvetľujúcimi predpismi, a to:

- BS PD 0005:2003. Management guide to IT service management,
- BS PD 0015:2002. IT service management. Self-assessment workbook.

Paralelne, v roku 1987, vznikla na pôde ISO a v spolupráci s IEC subkomisia JTC 1/SC 7 Software and systems engineering, ktorá zastrešovala tvorbu medznárodných štandardov pre oblasť informačných systémov a softvérového inžinierstva. Táto subkomisia vydala v decembri 2005 normu ISO/IEC 20000, ktorá vychádza z normy BS 15000 a zodpovedá teda knižnici ITIL vo verzii 2 (označenie ITIL v2). Norma ISO/IEC 20000 (u nás pod označením STN ISO/IEC 20000) sa tým stala oficiálnym medzinárodne platným štandardom pre ITSM.

V roku 2007 bola vydaná verzia 3 knižnice ITIL (t.j. ITIL v3). Verzie 2 a 3 sú vzájomne kompatibilné, hoci ITIL v3 je rozsiahlejší, podrobnejší, viac procesne zameraný (popisuje cca trikrát viac procesov a funkcií než verzia 2) a s väčším dôrazom na prepojenie IT služieb so strategickými cieľmi organizácie [7]. Vo všeobecnosti sa dá pohľad ITIL v3 na IT služby charakterizovať ako modernejší, vertikálny, odvodený od podnikových procesov a stratégií, kým pohľad ITIL v2 je horizontálny, zameraný na vyčlenenie typov služieb, ktoré je potrebné implementovať [23]. Norma ISO/IEC 20000 teda, v súlade s ITIL v2, špecifikuje, aké typy IT služieb sa majú pre procesy riadenia IT prostredia implementovať. Oproti ITIL v2 obsahuje norma v dokumente ISO/IEC 20000-2:2005. *Part 2: Code of practice* aj návod, metodiku, akým spôsobom je potrebné vytvoriť a nasadiť požadované služby. Akokoľvek, vývoj knižnice ITIL aj príslušnej normy pokračuje a možno očakávať, že norma sa bude v nasledujúcich rokoch aktualizovať smerom k progresívnejšej verzii ITIL v3, kým rámec ITIL sa zrejme bude vyvíjať, podľa poznatkov získaných z nasadenia ITIL v3 v praxi, smerom k novej verzii 4.

Okrem rámca ITIL a základnej normy ISO/IEC 20000 pre riadenie IT prostredia existuje škála ďalších noriem vymedzujúcich (v zmysle ITIL v3) širší kontext pre plánovanie, návrh a manažment IT služieb a prostredia v organizácii. Tento kontext zahŕňa manažérske normy pre riadenie kvality vo všeobecnosti, pre modelovanie a manažment podnikových procesov, pre riadenie informačnej bezpečnosti, a tiež normy pre niektoré technológie vhodné na návrh a prevádzku systémov orientovaných na IT služby. Najdôležitejšie z týchto noriem postupne popíšeme v nasledujúcich častiach.

Normy pre manažment kvality

Globálny rámec pre efektívne riadenie podnikového prostredia, vrátane stratégií, procesov a podporných IT služieb, určujú najmä medzinárodné normy ISO. Z nich azda najvýznamnejšou je známa skupina noriem **ISO 9000**, ktorá definuje tzv. *systém riadenia kvality* [25]. Tieto normy obsahujú súbor odporúčaní na dokumentovanie procesov potrebných pre riadenie kvality na všetkých úrovniach. Využíva sa procesný prístup, pričom kritériom kvality je orientácia na zákazníka, spotrebiteľa. Znamená to, že pohľad zákazníka je určujúci pri definovaní požiadaviek na kvalitu v procesnom systéme.

Dokumentácia predpisovaná normami umožňuje identifikovať všetky z hľadiska kvality relevantné procesy v organizácii, určiť ich postupnosť a interakciu, určiť kritériá a metódy potrebné na efektívnu prevádzku týchto procesov, zaistiť dostupnosť zdrojov a informácií nevyhnutných na zabezpečenie prevádzky a monitorovania procesov. Ďalej sa normou predpisujú spôsoby samotného monitorovania, merania, analyzovania a vyhodnocovania procesov, a napokon sa zavádzajú činnosti na zabezpečenie trvalého zlepšovania procesov [27].

V kontexte problematiky riadenia IT prostredia a služieb však treba zdôrazniť, že normy skupiny ISO 9000 majú široký a všeobecný záber, pokrývajú všetky procesy v organizácii, vrátane procesov ITSM (porov. Obr. 2-2). Pritom však platí, že knižnica ITIL je plne kompatibilná s normami ISO 9000 [19]. Základné rozdiely medzi ISO 9000 a ITIL sú prezentované v Tab. 2-1, podrobný popis mapovania procesov ITSM na jednotlivé ustanovenia noriem skupiny ISO 9000 možno nájsť v [37].

Tab. 2-1. Porovnanie základných charakteristík ISO 9000 a ITIL

ISO 9000	ITIL
Určuje povinnosť popísať, zdokumentovať, riadiť a priebežne zlepšovať všetky existujúce procesy v organizácii, predpisuje formu dokumentácie a spôsob jej riadenia.	Definuje, akým spôsobom sa majú navrhovať procesy ITSM, aby viedli k nákladovo efektívnemu poskytovaniu IT služieb, tiež zavádza nepretržtý cyklus neustáleho zvyšovania ich účinnosti a efektivity.
Má širší záber, pokrýva vo všeobecnosti všetky podnikové procesy.	Pokrýva iba procesy ITSM, ktoré sú len časťou podnikových aktivít.
Je to všeobecná norma, ktorá nešpecifikuje, aké konkrétne procesy majú byť popísané.	Presne definuje, ktoré procesy majú byť vytvorené a implementované.

Normy ISO 9000 boli koncipované na základe britskej normy BS 5750 a boli prvýkrát publikované už v roku 1987, a to ako súbor odporúčaní na dokumentáciu v systéme riadenia kvality. Procesný prístup sa uplatnil v revízii ISO 9000:2000. V roku 2005 bol súbor noriem kvalitatívne prepracovaný a zverejnený bol štandard ISO 9000:2005, ktorý definuje základné pojmy, princípy a ciele riadenia kvality. Aktualizované boli normy definujúce požiadavky kladené na organizáciu (ISO 9001), návody na riadenie kvality (ISO 9004) a návody na vykonávanie interných auditov (ISO 19011). Normy ISO 9000 boli prijaté na úrovni európskej organizácie EN a boli začlenené aj do sústavy slovenských technických noriem. Skupinu noriem ISO 9000 tvoria u nás nasledujúce predpisy:

- STN EN ISO 9000:2005. Systémy manažérstva kvality. Základy a slovník.
- STN EN ISO 9001:2008. Systémy manažérstva kvality. Požiadavky.
- STN EN ISO 9004:2009. Manažérstvo trvalého úspechu organizácie. Prístup na základe manažérstva kvality.
- STN EN ISO 19011:2002. Návod na auditovanie systému manažérstva kvality a/alebo systému environmentálneho manažérstva.

Keďže je súbor noriem ISO 9000 koncipovaný všeobecne, z praktických dôvodov vznikli na jeho základe špecializované normy kvality pre jednotlivé odvetvia. Napríklad pre oblasť softvérového inžinierstva je to norma:

- STN ISO/IEC 90003:2004. Softvérové inžinierstvo. Návod na aplikáciu normy ISO 9001:2000 na počítačový softvér.

Z ďalších súvisiacich noriem možno spomenúť napríklad normu:

- STN ISO 10006:2003. Systémy manažérstva kvality. Návod na manažérstvo kvality v projektoch.

Okrem noriem skupiny ISO 9000 definujúcich princípy riadenia kvality existuje široké spektrum ISO noriem pre rôzne ďalšie globálne aspekty riadenia podniku či organizácie. Niektoré z týchto noriem, aj keď azda okrajovo, môžu mať istý vplyv na riadenie podnikového prostredia. Medzi takéto normy patria napríklad:

- STN EN ISO 14001:2004. Systémy environmentálneho manažérstva. Požiadavky s pokynmi na použitie.
- ISO 26000:2010. Spoločenská zodpovednosť firiem.

Normy pre modelovanie a riadenie podnikových procesov

Úspešné a efektívne riadenie IT je zamerané na zabezpečenie súladu medzi strategickými cieľmi organizácie, z nich vyplývajúcimi podnikovými procesmi, a IT službami podporujúcimi tieto procesy (porov. Obr. 2-2 a časť 2.2). *Podnikové procesy* (angl. Business Processes) majú teda pri riadení IT centrálne postavenie, dá sa povedať, že definovaným spôsobom „riadia“ život organizácie a zhromažďujú štatistiky o priebehu činností [23]. Je teda mimoriadne dôležité *optimalizovať podnikové procesy* a nastaviť tým základné oblasti činnosti na najvhodnejšiu mieru kvality, výkonnosti a efektívnosti z pohľadu času, zdrojov a nákladov. Potrebné je tiež zvážiť možnosti automatizácie podnikových procesov a zvoliť primeranú mieru ľudskej interakcie. Všetky tieto opatrenia sa súhrnne označujú pojmom *manažment podnikových procesov* (angl. Business Process Management).

Základným nástrojom pre návrh, riadenie, monitorovanie a validáciu podnikových procesov je vhodná formálna reprezentácia procesu, tzv. *procesný model*. Pomocou modelu sa pre proces definuje pracovný tok (angl. workflow), pozostávajúci z časovej následnosti čiastkových úloh (podprocesov alebo akcií), aktorov zúčastňujúcich sa na procese, udalostí, ohraničení, a podobne.

Na modelovanie podnikových procesov existuje viacero rôznych formalizmov, avšak najpoužívanejšie sú špecifikované vo forme otvorených štandardov. Vytvára a publikuje ich najmä konzorcium OMG (Object Management Group, http://www.omg.org), ktoré je medzinárodným neziskovým združením s otvoreným členstvom. Pôvodne bolo OMG zamerané na vytváranie štandardov pre

distribuované objektovo orientované softvérové systémy, v súčasnosti sa však venuje najmä modelovaniu systémov a procesov. Najznámejšie a najpoužívanejšie OMG štandardy na modelovanie procesov sú:

- **BPMN** (Business Process Model and Notation, http://www.bpmn.org) je špecifikácia grafického formalizmu pre modelovanie abstraktných[4] podnikových procesov. Verzia BPMN 1.2 bola publikovaná v roku 2009 ako OMG štandard [3], v súčasnosti sa pripravuje vydanie verzie 2.0.
- **BPDM** (Business Process Definition Metamodel, http://www.omg.org/spec/BPDM/) je rozšírením BPMN o modelovanie interakcií medzi jednotlivými procesmi v rámci jednej organizácie (tzv. *orchestrácia*) aj medzi procesmi rôznych organizácií (tzv. *choreografia*). Štandard bol vydaný v novembri 2008 vo verzii 1.0.
- **UML** (Unified Modeling Language, http://www.uml.org) je populárny a často používaný súbor grafických a formálnych notácií pre modelovanie procesov a komplexných systémov v všeobecnosti. Tradične sa využíva v softvérovom inžinierstve, avšak je rovnako vhodný pre tvorbu modelov podnikových procesov a servisne orientovaných systémov. V súčasnosti je UML k dispozícii vo verzii 2.3 [38], pričom príslušný OMG štandard zahŕňa dve navzájom sa doplňujúce špecifikácie: 1) Infraštruktúra, kde sa definujú základné konštrukty formalizmu, a 2) Nad-štruktúra, obsahujúca popis UML diagramov z hľadiska používateľa, tvorcu modelov. Verzia UML 1.4.2 bola vydaná aj ako norma ISO/IEC 19501:2005.

Vývojom štandardov pre modelovanie procesov a pracovných tokov sa zaoberá aj organizácia WfMC (Workflow Management Coalition, http://www.wfmc.org). Poskytuje technické špecifikácie, ktoré dopĺňajú formát BPMN:

- **XPDL** (http://www.wfmc.org/xpdl.html), definuje formát pre uloženie a výmenu reprezentácií procesov. Štandard bol vydaný v októbri 2008 vo verzii 2.1.
- **BPAF** (Business Process Analytics Format, http://www.wfmc.org/business-process-analytics-format.html), špecifikácia XML schémy pre posudzovanie a hodnotenie efektívnosti procesov. Verzia 2.0 bola zverejnená vo februári 2009.

[4] Procesy sú abstraktné v tom zmysle, že ich modely neobsahujú primo vykonateľný kód. Existujú aj formalizmy pre vykonateľné procesy, najznámejším je BPEL, resp. WS-BPEL [39]. Medzi BPMN a BPEL je možná transformácia, hoci táto nie je úplne priamočiara a dá sa vykonať iba pri splnení určitých obmedzujúcich podmienok.

Modely podnikových procesov sú nástrojmi najmä pre manažérov (sledovanie denných operácií a činností v organizácii), analytikov (dokumentácia a vyhodnocovanie procesov) a IT architektov (návrh IT aplikácií a služieb na podporu procesov) [23]. Simulácia rôznych potenciálnych či skutočných stavov a situácií, ktorú procesný model umožňuje, dovoľuje využiť získané údaje a štatistiky na dynamickú anaýzu, plánovanie a v konečnom dôsledku na prispôsobovanie procesov strategickým zámerom organizácie.

Normy pre IT služby a ich riadenie

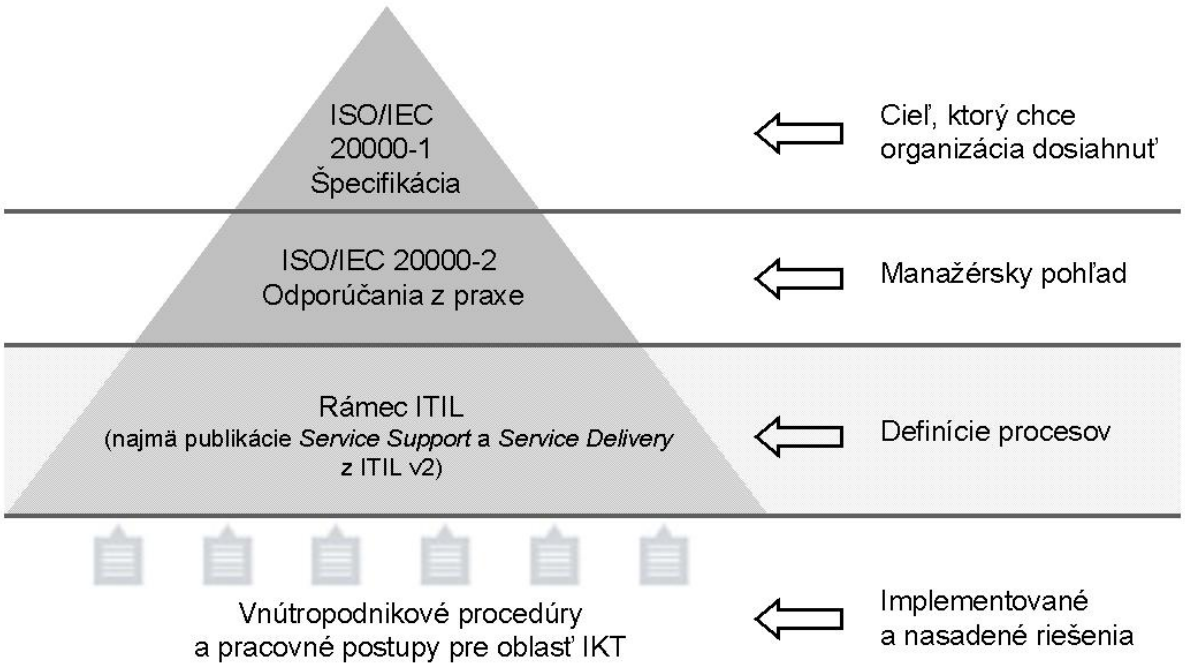
Základnou normou pre manažment IT služieb a k nim príslušnej IT infraštruktúry je norma **ISO/IEC 20000**. Táto norma, pôvodne vytvorená na základe britskej normy BS 15000, je v zásadnej zhode s ITIL v2, pričom zhoda je 90 až 95% [40]. V norme ISO/IEC 20000 sú definované kvalitatívne a procesné požiadavky na dodávateľov a poskytovateľov IT služieb pre interných alebo externých zákazníkov. Norma je procesne orientovaná a nezaoberá sa konkrétnymi IT technológiami, nástrojmi, či ich posudzovaním [40]. Obsah normy tvoria tieto časti:

1. *Úvod*: definícia účelu, rozsahu a možností použitia normy.
2. *Termíny a definície*: vymedzenie základnej terminológie.
3. *Požiadavky na systém riadenia*: definícia zodpovedností vrcholového manažmentu v oblasti riadenia kvality služieb, požiadavky na dokumentáciu, prideľovanie kompetencií a povinnosť školení personálu.
4. *Plánovanie a implementácia*: definuje sa systém priebežného zlepšovania metódou PDCA (plan – do – check – act, t.j. plánuj – konaj – kontroluj – zlepšuj).
5. *Nové služby a zmeny*: definícia požiadaviek na plánovanie a posudzovanie nákladov, dopadov a rizík zmien.
6. *Procesy dodávania služieb*: definícia procesov taktického plánovania služieb (riadenie úrovní služieb, reporting, manažment kontinuity, riadenie finančných zdrojov, riadenie kapacít, manažment informačnej bezpečnosti).
7. *Procesy vzťahov*: definícia procesov pre riadenie vzťahov so zákazníkom, vzťahov s dodávateľmi a s tretími stranami.
8. *Procesy obnovy*: definícia procesov operatívneho riadenia služieb (manažment incidentov a problémov).

9. *Procesy kontroly*: definícia procesov informačnej podpory, zabezpečenia kontroly a zmien (konfiguračný manažment, manažment zmien).
10. *Proces nasadenia*: definícia požiadaviek na proces, ktorý fyzicky vykonáva, implementuje a nasadzuje zmeny (manažment vydaní).

Prínosy a konkrétne výhody implementácie normy ISO/IEC 20000 závisia od tej-ktorej organizácie, avšak je možné určiť niektoré všeobecné praktické a formálne prínosy [18]. Formálnymi prínosmi sú najmä vytvorenie konkurenčnej výhody, zvýšenie reputácie organizácie, posun k proaktívnemu zmýšľaniu, automatizácia procesov riadenia služieb a zvýšenie interoperability podporou štandardizovaných medzipodnikových procesov. K praktickým výhodám patrí zosúladenie stratégie poskytovania IT služieb s celkovou podnikovou stratégiou organizácie, rýchla odozva IT služieb na zmeny v stratégii, zníženie nákladov na IT služby pri zachovaní požadovanej úrovne kvality, určenie konkrétnych zodpovedností za procesy a služby, možnosť monitorovania, hodnotenia a porovnávania služieb voči najlepším skúsenostiam, pochopenie a riadenie rizík, a ďalšie.

Napriek tomu, že norma ISO/IEC 20000 vychádza z rámca ITIL v2, nie sú tieto špecifikácie totožné. Je to dané ich rôznym určením. ITIL je súbor najlepších skúseností z praxe, avšak nie je metodikou ani pracovným postupom pre riadenie IT služieb. Naopak, norma ISO/IEC 20000 obsahuje konkrétne požiadavky a odporúčania, pri ktorých je možné preukázať (v procese *certifikácie*, porov. časť 2.2.7) mieru implementácie všetkých normou definovaných procesov. Knižnica ITIL prináša bližšiu špecifikáciu a detailný popis týchto procesov v kontexte ITSM. Spoločným cieľom normy ISO/IEC 20000 aj rámca ITIL je vytvorenie prostredia pre poskytovanie takých IT služieb, ktoré budú podporovať existujúce vnútropodnikové procesy a ktoré budú v súlade s celopodnikovými strategickými cieľmi (Obr. 2-3, porov. aj Obr. 2-2).



Obr. 22 Vzťah normy ISO/IEC 20000, rámca ITIL a vnútropodnikových procesov

V súčasnosti celý súbor noriem radu ISO/IEC 20000 *Information technology – Service management* tvorí päť základných dokumentov:

- ISO/IEC 20000-1:2005. *Part 1: Specification*. Definuje základné požiadavky na systém riadenia IT služieb v organizácii a slúži ako referenčný rámec pre certifikáciu poskytovateľo IT služieb.
- ISO/IEC 20000-2:2005. *Part 2: Code of practice* (slov. návod na použitie). Poskytuje návod na podporu a zavedenie systému ITSM v organizácii.
- ISO/IEC TR 20000-3:2009. *Part 3: Guidance for the scoping and applicability of ISO/IEC 20000-1*. Definuje sa rozsah a aplikovateľnosť ITSM v organizácii.
- ISO/IEC TR 20000-4:2010. *Part 4: Process reference model*. Definuje sa logická reprezentácia abstraktných procesov ITSM a ich častí, vrátane cieľov a požadovaných výstupov procesov.
- ISO/IEC TR 20000-5:2010. *Part 5: Exemplar implementation plan for ISO/IEC 20000-1*. Vzorový príklad plánu implementácie procesov ITSM.

Norma ISO/IEC 20000 bola v auguste 2008 preložená do slovenčiny a zaradená do sústavy STN, kde ju tvoria tieto predpisy:

- STN ISO/IEC 20000-1:2005. Informačné technológie. Manažment služieb. Časť 1: Špecifikácia.

- STN ISO/IEC 20000-2:2005. Informačné technológie. Manažment služieb. Časť 2: Odporúčania z praxe.

Ďalšie tri časti, teda definícia rozsahu a aplikovateľnosti, procesný referenčný model a príklad implementačného plánu, sú v príprave na schválenie za normy STN. Zároveň v rámci ISO komisie JTC 1/SC 7 prebieha aktualizácia prvých dvoch častí normy smerom k verzii 3 knižnice ITIL.

Vyššiu úroveň riadenia IT prostredia a služieb, vrátane manažmentu podnikových procesov a strategických cieľov organizácie v zmysle riadenia IT, pokrýva norma **ISO/IEC 38500** (http://www.38500.org). Táto norma je odvodená z austrálskej normy AS 8015:2005 a do štruktúry ISO noriem bola zapracovaná zmiešanou komisiou ISO/IEC JTC 1. Oficiálny názov normy je ISO/IEC 38500:2008. Corporate governance of information technology. V súčasnosti ešte táto norma nie je začlenená do STN, avšak pracuje sa na jej preklade a v najbližšom čase sa pripravuje jej zaradenie pod označením STN ISO/IEC 38500 [2].

Norma ISO/IEC 38500 je založená na metodike COBIT vo verzii 4.1 [5]. Cieľom normy je poskytnúť vrcholovému manažmentu súbor princípov na využívanie, vyhodnocovanie, riadenie a monitorovanie IT v rôznych typoch organizácií. Za jeden z kľúčových aspektov tejto normy možno považovať skutočnosť, že táto norma po prvýkrát pripustila, že riadenie IT by mali vlastniť tí, ktorí sú zodpovední za efektívne dodávanie podnikateľských systémov [2].

Obsah normy ISO/IEC 38500 je rozdelený do troch častí. Prvá časť popisuje predmet normy, jej použitie a ciele. Sú v nej upresnené prínosy jej používania, definície jednotlivých pojmov, a tiež referencie na použité dokumenty. V druhej časti je popísaný rámec pre správne *riadenie IT v organizácii* (angl. IT corporate governance), pričom sa zdôrazňuje šesť základných prícipov: zodpovednosť, stratégia, akvizícia, výkon, súlad a správanie sa ľudí. Súčasťou tejto časti normy je aj interpretácia a detailný popis modelu pre tzv. EDM cyklus riadenia IT (evaluate – direct – monitor, t.j. hodnotiť – nariadiť – monitorovať). Tretia časť normy je venovaná návodom pre správne riadenie IT v organizácii a postupom potrebným na ich implementáciu. V tejto časti sa interpretujú jednotlivé pricípy uvedené v druhej časti z pohľadu EDM cyklu riadenia IT, pričom sa detailne popisujú jednotlivé aktivity.

Procesy, v rámci ktorých sa IT služby vykonávajú, sú definované vo viacerých normách a špecifikáciách, v závislosti od zvoleného prístupu. Medzi dôležité štandardy v tejto oblasti patrí norma **ISO/IEC 15504**, ktorá je tiež známa pod akronymom SPICE (z angl. Software Process Improvement and Capability dEtermination). Norma definuje referenčný model pre organizačné procesy, pre procesy riadenia, vytvárania, dodávky, podpory a prevádzky, a to v dimenziách procesných typov a ich výkonnosti.

Do štruktúry STN bola norma ISO/IEC 15504 zaradená v apríli 2010 pod označením STN ISO/IEC 15504. Informačné technológie. Hodnotenie procesov. Člení sa na päť dokumentov a dve technické správy:

- STN ISO/IEC 15504-1:2004. Časť 1: Koncepty a slovník. Všeobecný úvod do konceptov hodnotenia procesov a slovník pre termíny súvisiace s hodnotením.
- STN ISO/IEC 15504-2:2003. Časť 2: Vykonávanie hodnotenia. Popisuje základné princípy a spôsoby hodnotenia procesov vrátane požiadaviek kladených na rôzne typy procesov.
- STN ISO/IEC 15504-3:2004. Časť 3: Návod na vykonávanie hodnotenia.
- STN ISO/IEC 15504-4:2004. Časť 4: Návod na vykonávanie hodnotenia zlepšovania procesov a určenia miery spôsobilosti procesov.
- STN ISO/IEC 15504-5:2006. Časť 5: Príklad modelu hodnotenia procesov.
- TNI ISO/IEC TR 15504-6:2008. Časť 6: Posúdenie životného cyklu modelu hodnotenia procesov.
- TNI ISO/IEC TR 15504-7:2008. Časť 7: Posúdenie zrelosti organizácie. Určujú sa podmienky posúdenia zrelosti organizácie, definuje sa rámec pre stanovenie zrelosti organizácie založený na profiloch spôsobilosti procesov odvodených z posudzovania procesov a definujú sa podmienky, za ktorých sú tieto hodnotenia platné.

Popis procesov v rámci životného cyklu umelých, ľuďmi konštruovaných systémov je predmetom normy **ISO/IEC 15288**. Táto norma definuje procesy životného cyklu systémov v štyroch kategóriách: technické, projektové, zmluvné a organizačné podporné procesy. Každý z popisov procesov v týchto kategóriách obsahuje určenia príslušných cieľov, výstupov a čiastkových aktivít. Väčšina z definovaných projektov je relevantná aj z hľadiska riadenia IT služieb. Sú to napríklad organizačné podporné procesy riadenia infraštruktúry, kvality, či ľudských zdrojov,

ďalej projektové procesy riadenia informácií, konfigurácie, rizík, rozhodovania či plánovania projektu, a tiež technické procesy návrhu architektúry, integrácie, verifikácie, prechodu, validácie, prevádzky, údržby a vyraďovania.

Norma bola začlenená do štruktúry STN v decembri 2009 pod označením STN ISO/IEC 15288. Systémové a softvérové inžinierstvo. Procesy životného cyklu systému. Od roku 2004 je začlenená aj do systému IEEE štanadrdov pod označením IEEE 15288. Úzko súvisiacou normou je ISO/IEC 12207, ktorá definuje procesy životného cyklu softvéru pre oblasť systémového a softvérového inžinierstva.

Normy pre bezpečnosť IT systémov

Manažment informačnej bezpečnosti je mimoriadne dôležitým aspektom riadenia IT prostredia a služieb, preto je tiež definovaný a vyžadovaný ako samostatný proces v metodike ITIL. *Informačná bezpečnosť*, resp. v širšom zmysle *bezpečnosť IT*, je súhrnom procesov a činností, ktoré zahŕňajú ochranu informačných aktív, stanovenie miery ich zabezpečenia, definíciu opatrení na ochrannu informačných aktív, riadenie bezpečnostných incidentov, výber, nasadzovanie a zaistene prevádzky bezpečnostných technológií, vykonávanie bezpečnostných testov systémov a aplikácií, audit a kontrolu bezpečnostných opatrení. Štandardy pre oblasť bezpečnosti IT určuje sústava ISO noriem, z ktorých najdôležitejšie uvádzame v nasledujúcom prehľade.

Systém riadenia informačnej bezpečnosti je definovaný súborom noriem **ISO/IEC 27000** (http://www.27000.org), ktorú tvoria dokumenty:

- ISO/IEC 27000:2009. *Information security management systems. Overview and vocabulary*. Definície pojmov a terminológie.
- ISO/IEC 27001:2005. *Information security management systems. Requirements*. Hlavná norma systému riadenia informačnej bezpečnosti, odvodená od britskej normy BS 7799-2. Predstavuje ucelený systémom riadenia informačnej bezpečnosti od realizácie, udržiavania, a priebežného zlepšovania v organizáciách. Norma sa zaoberá aj povahou zmluvných vzťahov pre informačnú bezpečnosť v obchodnom styku, a tiež aj zmluvných vzťahov pri správe a servise spracovávaných citlivých informácií.

- ISO/IEC 27002:2005. *Code of practice for information security management*. Súbor postupov pre riadenie informačnej bezpečnosti, ktorý určuje hlavné smery a všeobecné zásady pre iniciovanie, zavedenie, udržiavanie a zlepšovanie riadenia bezpečnosti informácií v organizácii. Nahrádza staršie normy ISO/IEC 17799 (predtým BS 7799-1), pričom obsah tejto normy je totožný s ISO/IEC 17799:2005.
- ISO/IEC 27003:2010. *Information security management system implementation guidance*. Obsahuje návod na implementáciu manažmentu informačnej bezpečnosti podľa normy ISO/IEC 27001. Využíva sa procesný prístup a metodika PDCA.
- ISO/IEC 27004:2009. *Information security management. Measurement*. Návod na zavedenie a využívanie štandardných ukazovateľov a spôsobov merania efektívnosti implementovaného systému informačnej bezpečnosti.
- ISO/IEC 27005:2008. *Information security risk management*. Poskytuje doporučenia a techniky pre analýzu a riadenie bezpečnostných rizík na základe súvisiacich noriem ISO/IEC 13335-4:2008 a ISO/IEC 13335-3:1998.
- ISO/IEC 27006:2007. *Requirements for bodies providing audit and certification of information security management systems*. Obsahuje požiadavky a návody na certifikáciu informačnej bezpečnosti, určená je najmä akreditovaným certifikačným autoritám.
- ISO/IEC 27011:2008. *Information security management guidelines for telecommunications organizations based on ISO/IEC 2700*. Určuje spôsoby riadenia informačnej bezpečnosti v telekomunikáciách.
- ISO 27799:2008. *Information security management in health using ISO/IEC 27002*. Obsahuje odporúčania pre riadenie informačnej bezpečnosti v zdravotníckych zariadeniach.

V súčasnosti sú rozpracované aj ďalšie normy súboru ISO/IEC 27000 [10], ktoré by mali zahŕňať audit, riadenie, poradenstvo a viaceré iné aspekty informačnej bezpečnosti.

Niektoré normy pre technológie IT systémov

Z hľadiska efektívneho a moderného manažmentu IT prostreda a služieb je dôležitý aj vhodný výber technológií, ktoré by mali podporovať automatizáciu podnikových procesov a umožňovať integráciu na úrovniach údajov, aplikácií,

procesov a používateľov [23]. Integračná platforma má v cieľovom stave zabezpečovať návrh, realizáciu a prevádzku scenárov zodpovedajúcich podnikovým procesom a podporených príslušnými IT službami. Technologickým rámcom, ktorý umožňuje vybudovanie takejto integračnej platformy, sú *webové služby*, architektúry orientované na služby a rôzne ďalšie všeobecne akceptované štandardy, napríklad HTML, XML, SOAP, WSDL, SAWSDL, a podobne. V tohto kontexte je kľúčovým pojmom *interoperabilita*, čiže schopnosť rôznych súčastí IT infraštruktúry, informačných systémov a služieb vzájomne spolupracovať, komunikovať, odovzdávať si údaje a služby vo vzájomnej súčinnosti. Štandard pre interoperabilitu webových služieb určujú napríklad normy spoločnej komisie ISO a IEC:

- ISO/IEC 29361-29363:2008. *Web Services Interoperability*. Tieto tri normy definujú profily webových služieb, pozostávajúce zo súboru voľných, neproprietárnych špecifikácií. Popisuje sa komunikácia webových služieb cez SOAP protokol, popis parametrov služieb pomocou WSDL schémy, previazanie odovzdávaných a prijímaných parametrov cez SOAP binding, a ďalšie. Normy obsahujú aj vysvetlenia a dodatky k špecifikáciám, ktoré smerujú k podpore interoperability v riešeniach založených na webových službách.

Špecifikácie, na ktoré sa odvolávajú normy ISO/IEC 29361-29363, sú definované v odporúčaniach konzorcia W3C:

- **SOAP** (Simple Object Access Protocol, http://www.w3.org/TR/soap12/). *W3C Recommendation: SOAP Version 1.2*, vydané v apríli 2007. Odporúčanie definuje protokol na výmenu štruktúrovaných informácií v decentralizovanom, distribuovanom prostredí. Štandard pozostáva zo štyroch dokumentov, ktoré špecifikujú komunikačnú plaformu (messaging framework), údajový model, spôsob kódovania, testovacie kolekcie a procesný model protokolu.
- **WSDL** (Web Services Description Language, http://www.w3.org/TR/wsdl20/). *W3C Recommendation: Web Services Description Language Version 2.0*, vydané v júni 2007. Odporúčanie špecifikuje údajový model a príslušný XML formát pre popis webových služieb. Definovaný je formálny jazyk pre reprezentáciu abstraktnej funkcionality služieb, a tiež platforma pre popis detailov služby pomocou jej parametrov.
- **SAWSDL** (http://www.w3.org/TR/sawsdl/). *W3C Recommendation: Semantic Annotations for WSDL and XML Schema*, vydané v auguste 2007. Odporúčanie

definuje súbor rozširujúcich atribútov pre WSDL, ktorými možno popísať význam (sémantiku) parametrov webových služieb.

K týmto, možno povedať, základným a rámcovým štandardom ponúka W3C viacero špecifikácií pre transformáciu a prístup k údajom v XML formáte, napríklad XPath, XSLT, XQuery, XForms, atď. Technológie vytvárané na báze týchto a ďalších súvisiacich špecifikácií dovoľujú vytvárať, spravovať a udržiavať IT infraštruktúru ako modulárny systém nezávislých, avšak navzájom funkčne prepojených služieb. Toto progresívne a vďaka svojej flexibilite čoraz častejšie využívané riešenie sa označuje ako *architektúra orientovaná na služby* (SOA, Service Oriented Architecture). Štandardizačný rámec a referenčný model pre SOA poskytuje združenie OASIS (Organization for the Advancement of Structured Information Standards, http://www.oasis-open.org):

- **SOA** (http://docs.oasis-open.org/soa-rm/v1.0/). *OASIS standard: Reference Model for Service Oriented Architecture 1.0*, vydaný v októbri 2006. Štandard vymedzuje základné pojmy, objekty a vzťahy v rámci SOA, čím definuje všeobecné prostredie pre konkrétne implementácie na princípoch SOA.

SOA, v kombinácii s webovými službami a ďalšími štandardizovanými technológiami, následne umožňuje implementáciu riešení podporujúcich interoperabilitu IT služieb [23], napríklad aplikačnej integrácie na báze jednotnej zbernice (ESB, Enterprise Service Bus), údajovej integrácie pomocou dátových modelov a pracovných tokov (MDM, Master Data Management), a podobne.

Certifikácia súladu s normami v oblasti IT prostredia a služieb

Certifikácia je proces, pri ktorom sa preukazuje a potvrdzuje, že vlastnosti posudzovaného výrobku, služby, systému alebo činnosti spĺňajú požiadavky definované a vyžadované príslušnou normou. Súčasťou certifikácie je *posudzovanie zhody*, t.j. porovnávanie skutočných parametrov výrobku, služby, systému, alebo činnosti s parametrami vyžadovanými normou. Posudzovanie zhody a certifikáciu vykonáva na tieto činnosti kvalifikovaná a poverená právnická alebo fyzická osoba, tzv. *autorizovaná osoba*. Predpokladom pre výkon týchto činností je osvedčenie o spôsobilosti na vykonávanie certifikácie, inšpekcie či skúšok potrebných na posudzovanie zhody, ktoré získava daná právnická alebo fyzická osoba v procese

tzv. *akreditácie*. Štandardizačný rámec pre posudzovanie zhody a certifikáciu vymedzuje medzinárodná norma ISO /IEC 17000:2004, ktorá bola začlenená do sústavy STN v roku 2005 pod označením STN EN ISO/IEC 17000. Táto norma špecifikuje všeobecné termíny a definície súvisiace s posudzovaním zhody vrátane akreditácie orgánov posudzovania zhody a využívania posudzovania zhody pri uľahčovaní obchodu.

Certifikáciu, posudzovanie zhody, akreditáciu a ďalšie súvisiace činnosti spravidla nevykonávajú štandardizačné organizácie. Tieto kompetencie sú zväčša delegované na rôzne vládne a súkromné spoločnosti, pričom rámcové pravidlá sú nastavené legislatívne v rámci tej-ktorej krajiny. U nás pojem certifikácie a ďalšie súvisiace pojmy vymedzuje zákon č. 264/1999 Z. z. o technických požiadavkách na výrobky a o posudzovaní zhody, a to najmä v § 11, § 12, § 14 a § 22 (porov. v časti 2.1.5). Ústredným orgánom štátnej správy na úseku technickej normalizácie a posudzovania zhody je u nás, podľa § 3 zákona č. 264, ÚNMS SR. Týmto orgánom bola zriadená Slovenská národná akreditačná služba (SNAS, http://www.snas.sk), ktorá od 1. januára 2010 vykonáva činnosť podľa zákona č. 505/2009 Z. z. o akreditácii orgánov posudzovania zhody. SNAS je nezávislá príspevková organizácia, ktorá udeľuje osvedčenia o akreditácii orgánom posudzovania zhody, čím oficiálne potvrdzuje ich spôsobilosť vykonávať deklarované činnosti nestranne, nezávisle a na požadovanej odbornej úrovni, ktoré sú uznávané v Slovenskej republike i v zahraničí [1]. Pre činosti v oblastiach manažérstva kvality a riadenia IT prostredia sú u nás akreditovanými certifikačnými autoritami napríklad spoločnosti Bureau Veritas (http://www.bureauveritas.sk) a TÜV NORD Slovakia (http://www.tuvnord.sk). Aktuálny zoznam akreditovaných organizácií a certifikačných orgánov, členený podľa predmetov činnosti, možno nájsť na web stránke SNAS[5].

Niekedy, najmä pri rozsiahlejších a manažérsky orientovaných normách, býva odporúčaný postup implementácie špecifikovaný priamo ako súčasť normy. Napríklad pri normách skupiny ISO 9000 je návod na zavedenie manažmentu kvality publikovaný ako norma ISO 9004 (resp. STN EN ISO 9004). Takýto návod je možné voľne využiť pri internom posudzovaní zhody, resp. pri vnútornom audite v danej organizácii [28]. Avšak oficiálny certifikát môže udeliť iba akreditovaná certifikačná

[5] Podobne, ako medzinárodné štandardizačné organizácie (napr. ISO), ani SÚTN neposkytuje služby certifikácie a posudzovania zhody pre všetky normy, ktoré spravuje a publikuje. V rámci SÚTN však existuje špecializovaný Certifikačný orgán SÚTN [32], ktorý je akreditovaný SNAS pre certifikáciu úzkeho okruhu služieb (konkrétne pre prekladateľské služby, organizovanie jazykových študijných pobytov a pre pohrebné služby).

autorita, ktorá môže mať vypracované vlastné postupy a pravidlá certifikácie. Súlad týchto postupov a pravidiel s predmetnou normou zaručuje akreditácia.

V oblasti manažmentu IT prostredia a služieb platia pre certifikáciu v zásade rovnaké pravidlá. Norma ISO/IEC 20000, ktorú možno považovať v tejto oblasti za najvýznamnejší štandardizačný predpis, však má vytvorený vlastný certifikačný systém, tzv. certifikačnú schému. *Certifikačná schéma ISO/IEC 20000* bola navrhnutá organizáciou itSMF UK (http://www.itsmf.co.uk) v novembri 2003, do praxe bola zavedená v roku 2005. V súčasnosti je vlastníkom a prevádzkovateľom tejto schémy medzinárodná spoločnosť APMG-International (http://www.apmg-international.com). V rámci tejto certifikačnej schémy je akreditovaná skupina audítorských organizácií, tzv. certifikačných autorít (angl. Registered Certification Bodies, RCB), ktoré sú oprávnené posudzovať a certifikovať súlad ďalších organizácií s požiadavkami normy ISO/IEC 20000. Pritom sa vyžaduje, aby RCB bola akreditovaná aj na národnej úrovni, t.j. u nás orgánom SNAS. Zoznam certifikačných autorít pre ISO/IEC 20000 možno nájsť na web stránke APMG-International[6].

Certifikácia podľa normy ISO/IEC 20000 sa môže týkať buď podnikov, alebo jednotlivcov [14]. Na úrovni certifikácie jednotlivcov, pri ktorej sa skúma osobná znalosť normy a rámca ITIL, je možné dosiahnuť dva základné certifikačné stupne:

- *Certified ISO20000 Consultant*. Certifikačný stupeň určený pre konzultantov poskytujúcich služby v oblasti prípravy podniku na audit (interný audit).
- *Certified ISO20000 Auditor*. Certifikačný stupeň pre audítorov pracujúcich pre certifikačné autority, t.z. RCB, ktoré vykonávajú audit zhody s ISO 20000.

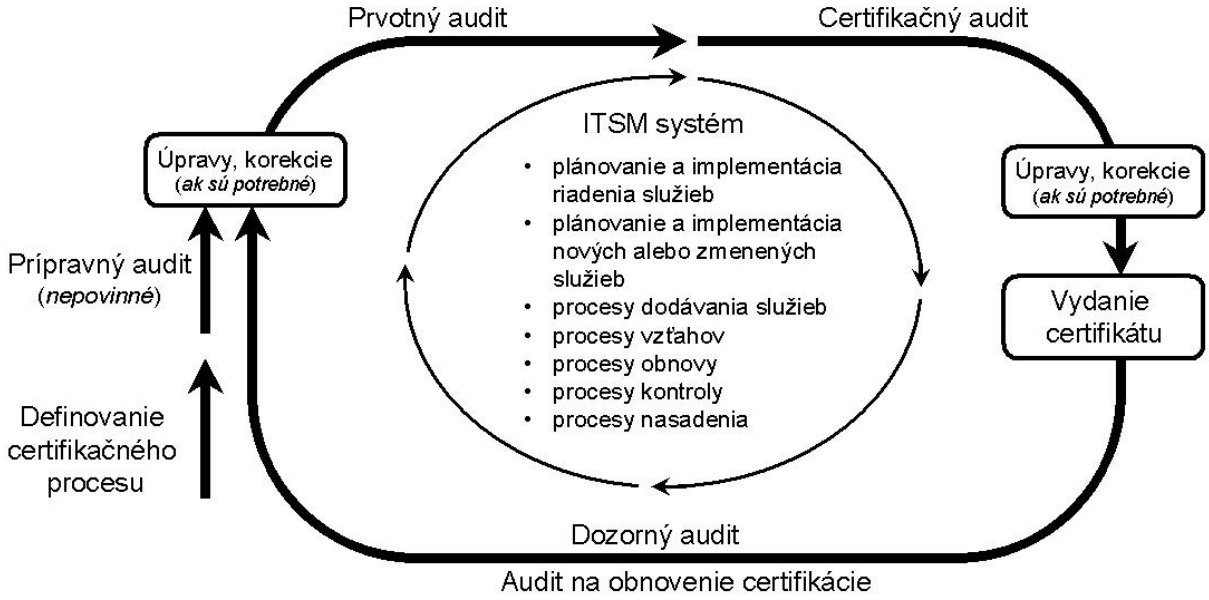
Na úrovni certifikácie podnikov, organizácií, je certifikácia dlhodobejší proces, ktorého predpokladom je zavedenie služby, dodávka, riadenie, uvoľnenie, rozlíšenie a vzťahy procesov [11]. Následne je certifikácia vykonávaná v nasledujúcich krokoch [12], graficky znázornených aj na Obr. 2-4:

1. *Definovanie certifikačného procesu*, spracovanie prvotných informácií.
2. *Prípravný audit* (nepovinný krok). Diferenčná analýza, zisťovanie pozície súčasného stavu oproti norme.
3. *Prvotný audit*. Overenie základnej štruktúry systému ITSM.

[6] Kým bola certifikačná schéma ISO/IEC 20000 prevádzkovaná organizáciou itSMF UK, zoznam certifikačných autorít bol dostupný na stránke http://www.isoiec20000certification.com. Táto stránka je v súčasnosti presmerovaná na web APMG-International, http://www.apmg-international.com/home/Qualifications/ISOIEC20000/RCBs.asp.

4. *Certifikačný audit*. Posudzovanie zhody s normou, overenie implementácie cieľového systému ITSM, ku ktorému sa požaduje vydanie certifikátu.
5. *Vydanie certifikátu*.

Certifikát je platný tri roky, je však potvrdzovaný každoročnými *dozornými auditmi*, pri ktorých sa sleduje priebežné zlepšovanie IT služieb. Po troch rokoch sa vykonáva *audit na obnovenie certifikácie*. V priebehu procesu certifikácie je možné vykonať aj *rozširovacie audity*, a to v prípade zmien ovplyvňujúcich rozsah a obsah certifikácie (napr. zavedenie nových technológií, rozšírenie priestorov, a pod.).



Obr. 23 Schéma procesu certifikácie organizácie na normu ISO/IEC 20000

Z praktického hľadiska sa na strane organizácie, ktorá sa uchádza o certifikáciu ITSM systému podľa normy ISO/IEC 20000, odporúčajú nasledujúce kroky [40]:

1. Navodiť v organizácii správnu a zmene prístupnú atmosféru, získať správnych ľudí, zabezpečiť podporu vedenia.
2. Podrobne sa oboznámiť s požiadavkami normy ISO/IEC 20000-1. Brať do úvahy skutočnosť, že normou je vyžadovaná preukázateľná implementácia *všetkých* (t.j. nie iba niekoľkých) normou definovaných procesov.
3. Podrobne sa oboznámiť s odporúčaniami normy ISO/IEC 20000-2, ktoré uľahčia implementáciu.

4. Príprava na certifikáciu je projekt ako každý iný, preto je potrebné definovať ciele a žiadané výstupy projektu certifikácie, zabezpečiť ľudí a financie, a pripraviť časový plán implementácie (od 6 do 36 mesiacov, podľa veľkosti organizácie).
5. Realizovať vyškolenie všetkých zúčastnených aktérov, t.j. projektového tímu, vlastníkov a kľúčových účastníkov jednotlivých procesov, a to buď priamo na ISO/IEC 20000, alebo na ITIL.
6. Vykonať objektívne posúdenie súčasného stavu ITSM v organizácii, ideálne s pomocou externého nezávislého a akreditovaného konzultanta.
7. Implementovať všetky vyžadované procesy v zmysle definovaného rozsahu, prípadne upraviť existujúce procesy podľa požiadaviek normy.
8. Vykonať interný audit procesov oproti požiadavkám normy, pričom k auditu je potrebné predložiť dôkazy o fungovaní týchto procesov. Vhodné je opäť využiť služby akreditovaného konzultanta.
9. Spustiť aktivity priebežného zlepšovania (PDCA).
10. Osloviť spoločnosť, ktorá je akreditovaná ako RCB, čiže má oprávnenie vykonávať audit a na udeľovať certifikáciu podľa ISO/IEC 20000.
11. Ak sa počas procesu certifikácie vyskytli vážnejšie nedostatky, tieto je potrebné odstrániť približne do 1 až 2 mesiacov. Certifikát je možné získať aj pri nesplnení určitých menej závažných požiadaviek normy, vtedy je však podmienkou kontrolný audit po jednom roku.
12. Aj po získaní certifikátu, tak ako pre ostatné normy ISO, je vyžadovaný audit na obnovenie certifikácie (tzv. recertifikácia), a to každé 3 roky.

Všeobecnou zásadou pri snahe o certifikáciu podľa normy ISO/IEC 20000, podobne ako pri každej inej norme, predpise, či dobrej iniciatíve, je uvedomenie si, že *ISO/IEC 20000 nie je cieľ, ale cesta* [40]. Čiže nie je správne nechať sa viesť výlučne snahou o zvýšenie prestíže spojenej so získaním certifikátu, skôr je potrebné snažiť sa dosiahnuť čo najlepšie výsledky cez porozumenie podnikovým procesom a požiadavkám zákazníkov, efektívne riadenie IT služieb smerom k splneniu týchto požiadaviek, vytvorenie vhodnej firemnej kultúry a celkovej atmosféry v organizácii.

IT Bezpečnosť a ITIL

Úvod

IT bezpečnosť je vsúčasnosti veľmi frekventovaný pojem. Niekedy sa IT bezpečnosť považuje iba za počítačovú bezpečnosť. Toto tvrdenie je však zavadzajúce pretože informácie existujú nielen v elektronickej podobe, ale aj v podobe papierovej, vo forme znalostí zamestnancov. Informácie a schopnosť s týmito informáciami pracovať predstavujú pre každú organizáciu konkurenčnú výhodu. Neschopnosť organizácii tieto informácie uchrániť môže viesť k strate dobrej povesti organizácie prípadne až ku krachu. Na IT bezpečnosť sa dá nazerať z rôznych pohľadov. Má rôzne úrovne a to technologickú, právnu, koncepčnú a ľudskú. Ľudský faktor je najproblematickejší, čo vedie k tvrdeniu že informačná bezpečnosť je ľudským aspektom. Predovšetkým však rozlišujeme bezpečnosť fyzickú a softvérovú (resp. informačnú). Fyzickú bezpečnosť môžeme definovať ako "systém opatrení slúžiaci na ochranu aktív spo- ločnosti pred nepovolanými osobami a pred neoprávnenou manipuláciou s nimi v objektoch a chránených priestoroch spoločnosti." Ide teda o: "ochranu aktív, objektov a chránených priestorov." [1]

Informačnú bezpečnosť môžeme definovať ako "schopnosť siete alebo informačného systé- mu ako celku odolať s určitou úrovňou spoľahlivosti náhodným udalostiam, alebo nezákonnému, alebo zákernému konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu a dôvernosť uchovávaných alebo prenášaných údajov a súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a systémov." [2]

V rámci efektívneho systému riadenia bezpečnosti (IT Security Management - ITSM) sa na zachovanie bezpečnosti využíva súbor metód ITIL. ITIL je súbor konceptov a postupov, ktorý umožňuje lepšie plánovať, využívať a skvalitňovať využitie informačných technológií. ITIL pre riadenie bezpečnosti vychádza z noriem ISO. Systém riadenia informačnej bezpečnosti (Information Security Management System - ISMS) definovaný ISO má nasledujúce základné ciele [3]:

- Zmiernenie hrozieb a rizík pre zachovanie dôvernosti, integrity a dostupnosti majetku vrátane informácií, ľudí, systému - softvér, hardvér, telekomunikácií na prijateľnú úroveň.
- Zlepšiť efektívnosť a účinnosť riadenia informačnej bezpečnosti – ISM (Information Security Management)

- Vylepšiť účinnosť a výkonnosť existujúceho bezpečnostného mechanizmu.
- Zdokonaliť testovanie a validáciu výsledkov z interných a externých auditov.

Hlavné ciele systému riadenia bezpečnosti - ITSM definovaný v rámci ITIL má dve hlavné ciele podobné cieľom ISMS [6] [7]:

Realizácia bezpečnostných požiadaviek definovaných v zmluve SLA. Realizá- cia ostaných externých požiadaviek, ktoré sú špecifikované v kontraktoch, v legislatíve apod.

Poskytovať základnú úroveň bezpečnosti čo je dôležité a nevyhnutné aj pre zabezpečenie kontinuity riadenia organizácie - Service Level Management (kap.2)

Platí, že ak sa zvyšuje objem a zložitosť spracovania informácií potom sa zvyšujú aj nároky na efektívne riadenie a bezpečnostný prehľad. Riadenie informačnej bezpečnosti je komplex činností v spoločnosti ako celku, do ktorej musia byť zapojené všetky zložky spoločnosti. Zvyšovaním objemu a náročnosti informačnej bezpečnosti logicky rastú aj nároky na jej efektívnosť riadenia. Ako základný kameň riadenia informačnej bezpečnosti sa považuje splnenie základných podmienok:

- pochopenie princípov, metódy riadenia a implementácia štruktúr riadenia informačnej bezpečnosti,
- efektívne meranie, spätné vyhodnocovanie a odstraňovanie slabín informačnej bezpečnosti (podľa kritérií hodnotenia informačnej bezpečnosti daných systémov a podľa metriky informačnej bezpečnosti ako celku). [5]

Na úspešne riadenie informačnej bezpečnosti v spoločnosti, je tiež nevyhnutné vychádzať z podmienok a vplyvov na spoločnosť, ktoré pomáhajú pri určení metódy riadenia. Prirodzeným výsledkom je realizácia informačnej bezpečnosti prepletením pracovných štruktúr spoločnosti, ktoré ovplyvňujú jej fungovanie. Nie však v rámci normatívnych oblastí bezpečnosti kde je priamo ovplyvnené jej fungovanie.

Bezpečnosť je riešená v rámci ITIL zväčša u stredných a vo veľkých spoločnostiach. Potreba komplexnosti v tejto oblasti je u menších spoločností len marginálna. ISM má vzťah a prepojenie so skoro všetkými ostatnými ITIL procesmi. Najväčšie prepojenie má s manažmentom incidentov, manažmentom zmien a manažmentom úrovní služby.

Pri zavádzaní systému riadenia informačnej bezpečnosti by sme mali zvážiť tieto kritické faktory úspechu:

- Ciele aaktivity bezpečnostnej politiky by mali odrážať biznis ciele podniku
- Implementácia by mala brať v úvahu kultúrne aspekty organizácie
- Požadovaná otvorená pomoc od vyššieho manažmentu organizácie
- Dostatočná znalosť bezpečnostných požiadaviek a odhadnutie rizík
- Používatelia by mali byť dostatočne vyškolený na používanie
- Dostupnosť systému na meranie výkonnosti, ktorý by mal napomáhať nepretržitému zlepšovaniu

Normy a štandardy

Normy a štandardy slúžia ako spôsob postupu pri riadení informačnej bezpečnosti. K nim možno zaradiť aj “best practices”, teda zoznam praktických skúseností, ktoré možno využiť. [4]

ITIL pre riadenie bezpečnosti vychádza z normy ISO 27001. Podľa ISO.ORG "ISO / IEC 27001:2005 sa vzťahuje na všetky typy organizácií (napr. obchodné podniky, vládne agentúry, neziskových organizácií). ISO / IEC 27001:2005 špecifikuje požiadavky pre stano- venie, realizáciu, operačné sledovanie, preskúmanie, udržiavanie a zlepšovanie systému ria- denia informačnej bezpečnosti v rámci organizácie celkových podnikateľských rizík. Stano- vuje požiadavky na vykonávanie bezpečnostných kontrol, ktoré sú prispôsobené potrebám jednotlivých organizácií alebo ich častí. ISO / IEC 27001:2005 je navrhnutý tak, aby zabezpe- čoval výber vhodných a primeraných bezpečnostných kontrol, ktoré by mali chrániť infor- mačné aktíva a dávať dôveru zúčastneným stranám.

ISO/IEC 20000 - IT service management

Norma ISO/IEC 20000 je medzinárodná štandarda pre riadenie IT služieb (ITSM – IT Servi- ce Management). Vychádza priamo z knižnice ITIL- Best Practice.

Výhody:

- odlíšenie sa od konkurencie a zlepšenie postavenia na trhu;
- rýchlosť odozvy na zmenu;
- formálny rámec na stále zvyšovanie kvality IT služieb;

- pochopenie a riadenie rizík;
- definovanie zodpovednosti na všetkých úrovniach zlepšuje firemnú kultúru a vzťahy;
- štandardný prístup k zvládnutiu organizačných zmien;
- rámec na vzdelávanie ľudí a automatizovanie procesov riadenia služieb.

ISO/IEC 2700x

Tieto normy konkretizujú činnosti IKT v oblasti informačnej bezpečnosti a jej samotného riadenia (normy sú v súlade s ISO/IEC 20000). Základ normy vychádza z britských štandardov. Patria tu normy:

- ISO/IEC 27001: – Systém manažérstva informačnej bezpečnosti (ISMS – Information security management system). Je to ,,top – level'' špecifikácia a certifikácia štandardu pre efektívny ISM pre všetky typy organizácií.

  Popisuje model ISMS – PDCA (plan-do-check-act);

  Zahŕňa:
  - definíciu termínov
  - všeobecné požiadavky
  - riadenie
  - implementáciu a prevádzku o monitorovanie a kontrolu
  - dokumentovanie požiadaviek
  - dokumentovanie a zaznamenávanie kontrol o Zodpovednosti a povinnosti
  - interné audity
  - manažérske kontroly
- ISO/IEC 27002: – známa aj ako ISO/IEC 17799 – „best practices“, Zoznam použiteľných praktických skúseností manažérstva informačnej bezpečnosti. Je to zbierka postupov, ktoré popisujú čo je dôležité robiť aby sa zvládli rôzne špecifikácie podľa ich dôležitosti. Štandard ISO/IEC 27002 bol vydaný v roku 2000. V roku 2005 bola vydaná jeho aktualizovaná verzia ISO/IEC 2700:2005. Je to zbierka najlepších bezpečnostných praktík a môže byť použitá ako kontrolný zoznam všetkého správneho, čo je nutné pre bezpečnosť informácii v organizácii urobiť. Jeho cieľom je poskytnutie informácii zložkám zodpovedným za udržiavanie informačnej bezpečnosti v organizácii. Napomáha pri vývoji

informačnej bezpečnosti a zároveň aj pri zlepšovaní spoľahlivosti informačnej bezpečnosti vo vzťahu k iným organizáciám. Táto norma celkovo obsahuje 11 základných oddielov bezpečnosti:

- Bezpečnostná politika
- Organizácie bezpečnosti
- Klasifikácia a riadenie aktív
- Bezpečnosť ľudských zdrojov
- Fyzická bezpečnosť a bezpečnosť prostredia
- Riadenie komunikácii a riadenie chodu organizácie
- Riadenie prístupu
- Vývoj, údržba a rozšírenie informačného systému
- Riadenie kontinuity činnosti organizácie
- Súlad s požiadavkami

□

Týchto 11 hlavných oddielov definuje celkovo 39 cieľov a opatrení pre ochranu informačnej bezpečnosti aktív. Tieto ciele opatrení zároveň zahŕňajú funkčné požiadavky pre architektúru bezpečnosti informácii organizácie.
ISO/IEC 27002 taktiež zahŕňa najlepšie praktiky pre zabezpečenie bezpečností informácii, ktoré by mala organizácia použiť pre zabezpečenie kontrolných cieľov. Aktualizovaná verzia obsahuje 133 základných opatrení, ktoré sa ďalej rozdeľujú na stovky ďalších opatrení.

Zvládanie bezpečnostných incidentov na základe minulého vývoja sa dá predikovať, že významné štandardy postupne vytlačí súbor noriem ISO/IEC 2700x aspoň v európskom meradle určite. Výhodou týchto noriem je aj sú- lad s ISO 9000 a ISO 14000, čo ponúka možnosť zaviesť a certifikovať procesy riadenia in- formačnej bezpečnosti aj už v existujúcom normatívnom prostredí. Ostatným štandardom táto výhoda komplexnosti chýba. [4]

ISO/IEC 13335 – Smernice pre riadenie bezpečnosti IT

Zahrňuje neoddeliteľnú súčasť riešenia informačnej bezpečnosti, predovšetkým v jej projek- tovaní. Normu odporúčajú v projektoch na ochranu osobných údajov, projektoch s ochranou utajovaných skutočností, no aj v ostatných zákonom

nešpecifikovaných oblastiach. Nevýho- dou tejto normy je jej špecifikácia na určitú oblasť IT bezpečnosti, pokrýva veľkú časť informačnej bezpečnosti, no nie celú oblasť. Norma sa preto používa ako doplnok k iným štandardom. Skladá z 5 častí:

- ISO/IEC TR 13335-1: Koncepcie a modely bezpečnosti IT: definovanie pojmov, mo- delov a vzťahov IT bezpečnosti k iným oblastiam IT,
- ISO/IEC TR 13335-2: Riadenie a plánovanie bezpečnosti IT: popis riadiacich a pláno- vacích aspektov.
- ISO/IEC TR 13335-3: Techniky riadenia bezpečnosti IT: popis bezpečnostných tech- ník pre pracovníkov. Takto sú priamo zapojený v životnom cykle riešenia informač- nej bezpečnosti: plánovanie - návrh - implementácia - testovanie - prevádzka. Tvorí základ pre pochopenie riešenia informačnej bezpečnosti a celej ISMS.
- ISO/IEC TR 13335-4: Výber ochranných opatrení: návod na výber ochranných opat- rení, základných modelov a opatrení na kontrolu. Rovnako slúži ako popis modelov a opatrení kontroly, doplňujú bezpečnostné techniky(ISO/IEC TR 13335-3).
- ISO/IEC TR 13335-5: Pokyny pre bezpečné pripojenie siete s IT systémami. [4]

COBIT security baseline

COBIT je framework vytvorený medzinárodnou asociáciou ISACA pre správu a riadenie informatiky (IT Governance). Jedná sa o súbor praktík, ktoré by mali umožniť dosiahnutie strategických cieľov organizácie vďaka efektívnemu využitiu dostupných zdrojov a minimalizáciu IT rizík. Prakticky je teda určený predovšetkým top manažérom na hodnotenie prevádzky IKT a audítorovi pre vykonávanie auditu systému riadenia IKT. Na rozdiel od ITIL, ktorý je určený viac manažérovi IT (CIO).

COBIT podobne ako ITIL vychádza zo skutočnosti, že aby podnik mohol dosahovať svoje ciele (Business goals), vznáša business požiadavky (Business Requirements), ktoré generujú požiadavky na IT zdroje (IT resources), ktoré sú zapojené do IT procesov (IT processes) prinášajúci businessu požadovanú službu a informácie (Enterprise Information).

Z hľadiska IT bezpečnosti obsahuje COBIT tzv. security baseline. Bola pridaná k verzii 4.1 a zahŕňa bezpečnosť rovnako ako iné riziká, ktoré sa môžu objaviť s využívaním informačných technológii. Je to príručka, ktorá sa zameriava na špecifické riziká informačnej bezpečnosti. Má byť využívaná profesionálnymi používateľmi a manažmentom veľkých podnikov. Zahŕňa 12 kapitol od úvodu, definícii informačnej bezpečnosti. Popis rizík pre informačnú bezpečnosť obsahuje 44 krokov k dosiahnutiu informačnej bezpečnosti. Ďalej obsahuje návod na informačnú bezpečnosť pre jednotlivé typy používateľov.

ITIL 2011

Úvod

ITIL 2011 predstavuje aktualizáciu, nie novú verziu, neobsahuje ani žiadne úplne nové koncepcie. Cieľom tejto aktualizácie je vyriešenie nezrovnalostí, prípadne oprava chýb v textoch a schémach. Podstatou je zlepšiť zrozumiteľnosť a štruktúru verzie ITIL v3. Celý názov nového vydania znie ITIL 2011 Edition, ktorý sa skracuje na "ITIL 2011", alebo jednoduchšie "ITIL", zatiaľ čo termín "ITIL 2007" sa používa pre vydanie ITIL v3. Aktualizácia zohľadňuje spätnú väzbu od používateľov a vzdelávacích komunít. Je odpoveďou na:

- problémy vznikajúce cez Change control log
- odporúčanie od Change Advisory komisie
- spätná väzba od komunity

Medzi prvé rozdiely, ktoré si je možné všimnúť v aktualizácií ITIL 2011 patrí väčší počet strán s hrubším papierom a väčšími písmenami. Väčšina procesov je detailnejšie popísaná a vzniklo v nej aj niekoľko nových procesov.

Aktualizované publikácie ITIL v3 zdieľajú spoločnú štandardnú štruktúru pre zlepšenie jednotnosti. Niektoré časti boli reorganizované pre zlepšenie čitateľnosti a plynulosti textu. Autorom išlo hlavne o zabezpečenie zhody naprieč knihami, ktoré zahrňujú ujasnenie okolo rozhraní, vstupov a výstupov naprieč celým životným cyklom služby. Terminológia je ujasnená a modifikovaná tak, aby bola konzistentná naprieč všetkými publikáciami i ITIL slovníkom.[1][2][3]

Stratégia služby

Koncepty v rámci publikácie Stratégia služieb boli objasnené bez toho, aby sa celkový odkaz zmenil. Pôvodných 373 strán bolo kompletne prepracovaných na 483 a aktualizácia v sebe prináša viac praktických návodov s viacerými relevantnými príkladmi. ITIL 2011 zaviedol a jasne definoval nový systém strategických procesov. V Stratégii sluţžeb vznikli aj nové procesy, ako sú *Manažment stratégie pre IT služby*

Strategy Management for IT Services a *Riadenie vzťahov* Business Relationship management .[2][3]

Manažment stratégie pre IT služby (Strategy management for IT services)

Kým vo verzii ITIL V3 bolo strategické hodnotenie a rozvoj stratégie služieb vykonávaný pod správou portfólia služieb, v ITIL 2011 je zavedený nový postup správy a riadenia IT služieb, ktorý je zodpovedný za rast a údržbu podnikania a IT stratégií. V aktualizácií je oddelený popis podnikateľskej stratégie od IT stratégie. Na podporu stratégie riadenia IT služieb bola zavedená aj nová rola Service Strategy Manager. [2][3]

Správa portfólia (Service portfolio management)

Správa portfólia je ITIL 2011 znovu zameraná na činnosti, ktoré sú spojené s riadením portfólia služieb a nadväzuje na zavedenie procesu Manažmentu stratégie pre IT služby. Cieľom je zaistenie, že poskytovateľ služieb má správnu kombináciu služieb s požadovanými obchodnými výsledkami na zodpovedajúcej úrovni investícií. Z procesu bolo odstránené strategické hodnotenie a rozvoj služieb. Naopak pridané boli skutočné pracovné toky a nové výstupy *Service Charter* a model poskytovania služieb *Service Model*. [3][2]

Riadenie dopytu (Demand management)

Jeho cieľom je pochopiť, naučiť sa predvídať a ovplyvňovať dopyt zákazníkov po službách. Z predchádzajúceho vydania ITIL V3 bola mapa procesov Riadenia dopytu ošetrená a spojená so Správou kapacít (Capacity Management). ITIL 2011 tiež obsahuje vysvetlenie a rozdiely medzi dopytom a riadením kapacít. Riadenie dopytu ako špecializovaný proces bol zavedený ako súčasť Stratégie služieb. Pre výkon činností v tomto procese vznikla nová rola, tzv. manažér dopytu (Demand Manager). V riadení dopytu sú uvedené príklady a vzor obchodnej činnosti (Pattern of Business Activity (PBA)). [2]

Finančné riadenie pre IT služby (Financial management for IT services)

V tomto procese nenastali žiadne významné rozdiely medzi ITIL V3 a ITIL 2011. Cieľom tohto procesu ostáva spravovanie rozpočtu poskytovateľa služieb a jeho účtovníctva. V tomto procese nastalo rozšírenie a boli popísané skutočné workflow (Accounting, Budgeting, Charging). [2][3]

Riadenie vzťahov s biznisom (Business relationship management)

Tento proces je v ITIL 2011 zavedený ako nový. Jeho cieľom je identifikovanie potrieb súčasných , ako aj potenciálnych zákazníkov a zaistenie, že príslušné služby boli vyvinuté na uspokojenie ich potrieb. Veľký dôraz kladie na prieskum spokojnosti zákazníkov a schopnosť vybavovať sťažnosti v rámci riadenia obchodných vzťahov, v čoho dôsledku sa príslušné postupy na tieto úlohy presunuli z neustáleho zlepšovania služieb do tohto procesu. Na základe toho, vznikli nové výstupy, ako portfólio zákazníkov (Customer Portfolio) a požadované výsledky služby (Desired Service Outcomes). [2][3]

Návrh služby

Aktualizácia ITIL 2011 kládla dôraz na zjednotenie Návrhu služby s ITIL Stratégiou služby. Tu nastalo rozšírenie z pôvodných 334 strán na 441. Návrh služby predstavuje proces s novým návrhom rolí, v ktorom sa objasnilo množstvo konceptov a princípov. [2][3]

Koordinácia návrhu (Design Coordination)

Tento proces bol pridaný ako nový proces. Jeho cieľom je zodpovednosť za koordináciu projektovej činnosti vykonávanú inými procesmi v dizajne služby. Vo verzii 2007 boli niektoré z týchto činností, resp. úloh, vykonávané ako súčasť procesu Service Level Management. Predstavuje projektový prístup pre riadenie zdrojov, rizík a na revíziu riešenia. Ďalšou novinkou je *politika návrhu služby* (Service Design

Policy) , ktorá predstavuje návod, ako zabezpečiť jednotný prístup aplikovaný na všetky projektové činnosti. [2][3]

Správa Katalógu služieb (Service Catalogue Management)

Žiadne významné zmeny oproti verzii ITIL V3 nenastali, iba sa jasnejšie definoval Katalóg služieb. Vymedzilo sa jeho použitie, čím došlo k špecifikácií na tzv. Veľkoobchodný a Maloobchodný Katalóg služieb. [3]

Správa úrovne služieb (Service Level Management)

Správa úrovne služieb bola v aktualizácii kompletne prepracovaná po zavedení procesu Návrh koordinácie. Z pôvodného procesu boli odstránené koordinácie aktivít. Novou hlavnou úlohou Správy úrovne služieb je zhromažďovanie, sledovanie a podávanie správ o požiadavkách na servis s prihliadnutím na dohodnutú úroveň služieb. [2][3]

Procesy Správa rizík (Risk Management), (IT Service Continuity Management), (Compliance Management) a Správa architektúry (Architecture Management) neobsahujú žiadne významné zmeny v novej aktualizácii ITIL 2011 v porovnaní s vydaním ITIL V3. [2][3]

V procesoch Správa kapacít (Capacity Management), Správa dostupnosti (Availability Management) a Správa informačnej bezpečnosti (Information Security Management) nedošlo k významnejším zmenám. Za spomenutie však stoja pridané výstupy, ako filtrovanie udalostí (Event Filtering) a korelačné pravidlá (Correlation Rules), ktoré boli pridané každému procesu. [2][3]

Správa dodávateľov (Supplier Management) taktiež neobsahuje výrazné zmeny oproti ITIL V3. Všetci dodávatelia a ich zmluvy sú spracované v rámci Správy zákazky s dodávateľom a informačným systémom (Supplier and Contract Management Information System (SCMIS)), ktorý v ITIL V3 bol známy ako "Supplier & Contract Database (SDC)”. [2][3]

Prechod služby

Štruktúra, obsah a vzťah medzi CMS SKMS boli objasnené, aby uľahčili čitateľovi chápanie kľúčových konceptov. V publikácií Prechod služieb bol pridaný nový obsah a z pôvodných 270 strán vzniklo rozšírenie na 348 strán. [1][2][3]

Manažment zmien (Change Management)

Štruktúra procesu Manažment zmien bola upravená tak, aby zdôraznila, že na významné zmeny je potrebné povolenie vo všetkých etapách životného cyklu. V aktualizácii bol taktiež pridaný nový obsah tohto procesu, ktorý vysvetľuje, ako sa tento proces má používať. Pridané boli aj nové čiastkové procesy (Assessment of Change Proposals) a (Minor Change Deployment), ktoré majú vykonávať drobné zmeny a posudzovať návrh zmien. V tomto procese nastalo rozdelenie autorizácie, ktoré zdôrazňuje etapu build s testovaním a až potom nasleduje etapa deployment so schválením. Zmena plánovania (Change Scheduling) je v aktualizácii ITIL 2011 prepracovaná tak, aby podrobné zmeny, plánovanie a správa releasov zodpovedne vykonával proces Správa releasov (Release Management). Zmena modelov (Change Models) dostala v aktualizácií významnejšiu úlohu v procese Správy zmien ako mala doposiaľ. Využíva sa nie len pri štandardných zmenách s nízkym rizikom zmeny na prevádzkovej úrovni, ale je možné ju použiť, aj pri opakovaných a tiež významných zmenách. [1][2][3]

Pri procese Vyhodnotenie zmien (Change Evaluation) došlo k spresneniu názvu kľúčových termínov procesu a k sprehľadneniu pracovného toku. Cieľom tohto procesu je hodnotenie závažných zmien na rôznych miestach v životnom cykle služby. Výsledky formálneho hodnotenia zmien sú zdokumentované v Správe hodnotenia zmien (Change Evaluation Report). [2][3]

Projektový manažment –Plánovanie prechodu služieb a ich podpora-Project Management (Transition Planning and Support)

Tento proces prešiel zmenou natoľko, aby zdôraznil, že jeho hlavnou úlohou je koordinovať rôzne projekty služieb, ich prechody a riešenie konfliktov. Projekty začínajú, ak je v Správe portfólia objednaná nová služba, alebo sa služba podstatne mení. Proces Projektový manažment v aktualizácií ITIL 2011 vyzýva ďalšie procesy Koordináciu návrhov a Manažment vydaní k vykonávaniu plánovacích aktivít na podrobnej úrovni. [2][3]

Manažment vydaní (Release Management)

V ITIL 2011 je tento proces vyzdvihnutý z Projektového riadenia (prechod, plánovanie a podpora služieb) na vykonávanie skúšobných verzií a verzií nasadenia. Medzi ním a Projektovým riadením boli zavedené aj doplnkové rozhrania, ktoré slúžia na zabezpečenie a ubezpečenie, že Projektovému riadeniu sú neustále poskytované aktuálne informácie o plánovaní. Ďalej aktualizácia stanovuje, že drobné zmeny sú realizované procesom Správa zmien bez účasti procesu Manažmentu vydaní. [2][3]

Validácia a testovanie Služby (Service Validation and Testing)

Aktualizácia ITIL 2011 vyžaduje ďalšie rozhranie medzi procesmi Validačné služby a testovanie a riadenie projektov, ktoré boli pridané pre zabezpečenie, že Projektovému riadeniu sú neustále poskytované aktuálne informácie o plánovaní. ITIL 2011 pridal aj nový čiastkový proces Návrh Validovania-Overenia Služieb (Service Design Validation), ktorý prebieha ako súčasť procesu Hodnotenie zmien. [2][3]

Manažment aktív a konfigurácií služby (Service Asset and Configuration Management)

Aj medzi týmito procesmi sa podľa aktualizácie ITIL 2011 vyžaduje nové rozhranie, ktoré má slúžiť na zabezpečenie poskytovania neustále aktuálnych informácií o plánovaní pre proces Projektové riadenie a proces Hodnotenie zmien. Ďalšou zmenou v aktualizácií je jasné zadefinovanie pojmov (Service asset -Configuration item - Configuration record) a tiež vysvetlenie vzťahu SCM a SKMS, s tým, čo tam

patrí. V procese je dodatočný obsah, ktorý sa vzťahuje prevažne na Manažment aktív, v ktorom došlo ku celistvosti množstva procesov, ktoré pozostávajú zo Manažmentu zmien, Manažmentu vydaní, Manažmentu zmien a Hodnotenia zmien. [2][3]

Vývoj aplikácií (Application Development) a Manažment znalostí (Knowledge Management)

Aktualizácia ITIL 2011 v týchto procesoch nepriniesla žiadne významnejšie zmeny, ani vylepšenia. [2][3]

Prevádzka služby

V tejto publikácií sa všetky pôvodné procesy upravili a z pôvodných 263 strán vzniklo 370. Publikácia bola upravená tak, aby jasne vysvetlila a poskytla zmysluplné informácie o udalostiach. Ďalšie vylepšenia obsahujú rozšírenú sekciu techník pre analýzu a porovnanie problémov a incidentov. Zlepšením prešli aj návody na eskalovanie incidentov v procese Manažment problémov. [1][2][3]

Manažment udalostí (Event management)

ITIL 2011 priniesol zmenu procesného toku, ktorá umožňuje teraz dvojitú koreláciu udalosti (1st Level Correlation and 2nd Level Correlation). Prvý stupeň korelácie zvažuje, či sa jedná naozaj o zmysluplnú udalosť a druhý stupeň porovnáva udalosť s nastavenými kritériami a pravidlami. Aktualizácia ITIL 2011 v tomto procese poskytuje aj podrobnejší popis a pokyny týchto procesných tokov. [2][3]

Manažment incidentov (Incident management)

V tomto procese aktualizácia odstránila nedostatky v procesnom toku a priniesla jasnejšie pokyny pre zvládanie a stanovenie priorít incidentov. Bol pridaný aj nový kontrolovaný zoznam (Incident Prioritization Guideline).

Ďalšie kroky zlepšenia boli vnesené do 1. úrovne podpory (1st Level Support), v ktorej je jasnejšie vysvetlené, za aké incidenty, existujúce problémy a známe chyby, by mala zodpovedať. 2. úroveň podpory (2nd Level Support) je značne rozšírená, pretože bolo nutné jasnejšie zadefinovať, kedy sa jedná o Manažmentu problémov a kedy o Manažmentu incidentov. Hlavnými úlohami 2. úrovne podpory je obnova služieb za čo najkratší možný čas a hľadanie pomoci u Manažmentu problémov, ak príčinu incidentu nie je možţné vyriešiť menšími zmenami. V rámci identifikácie incidentu v aktualizácií ITIL 2011 prebieha overenie, či sa skutočne jedná o incident, ak áno, pokračuje sa v procese, ak nie, tak sa automaticky presúva na proces Vykonávanie požiadaviek. [2][3]

Vykonávanie požiadaviek (Request Fulfilment)

Kľúčový proces Vykonávanie požiadaviek bol kompletne prepracovaný a odráža najnovšie pokyny a podrobný opis všetkých činností pre jednoduchšie pochopenie jeho piatich čiastkových procesov. Proces ďalej obsahuje rozhranie so Správu incidentov (pre prípad, že sa z požiadavky o službu vykľuje incident) a Prechodom služieb (v prípade, že si vykonávanie požiadaviek vyžaduje zapojenie procesu Správa zmien).

Aktualizácia ďalej prináša jasnejší opis požiadaviek a ich životný cyklus - prijatie, overenie, ich záznam a potvrdenie, kategorizácia a prioritizácia požiadaviek, schválenie/neschválenie, ako a kedy požiadavky vrátiť žiadateľovi, uzavretie požiadaviek. Zadefinované je aj potrebné overenie splnenia požiadaviek, resp. pravidlá na ich znovuotvorenie. Detailnejšie je vysvetlená aj koncepcia Modelu požiadavky (Request Model). [2][3]

Manažment prístupov (Access Management)

V tomto procese bolo v ITIL 2011 pridané rozhranie medzi ním a Manažmentom udalostí, ktoré zdôrazňuje, že niektoré filtrovanie udalostí a korelačné pravidlá by mali byť navrhnuté priamo v ňom pre podporu detekcie neoprávneného prístupu k službám. Špecializovaná činnosť a jasnejší popis bol pridaný k bodu zrušenie

prístupových práv. Žiadosť o povolenie prístupových práv musí byť kontrolovaná. [2][3]

Manažment problémov (Problem Management)

Aktualizácia priniesla nový čiastkový proces *Proaktívna identifikácia problému* (Proactive Problem Identification), ktorý má zdôrazniť význam aktívneho procesu Správa problémov. Ďalšou zmenou je úprava workflow a tiež stanovenie, že ak v rámci riešenia problému je potrebné riešenie, je potrebné ho implementovať. Taktiež bola kompletne prepracovaná časť diagnostika problému a jeho riešenie, aby bolo jasnejšie, ako tento proces spolupracuje s procesom Správa incidentov. ITIL 2011 obsahuje rozšírenú časť, v ktorej sa nachádzajú metódy pre analýzu problémov s príkladmi situácií, kedy sa tieto techniky a metódy dajú aplikovať. Aktualizácia poukazuje na to, že priorita problému sa dá znižovať jeho čiastočnými riešeniami. [2][3]

V procesoch Správa prevádzky IT (IT Operations Control) a Správa budov (Facilities Management) nenastali žiadne významné rozdiely medzi ITIL 2007 a aktualizáciou ITIL 2011. [2]

Manažment aplikácií (Application Management)

Proces Manažment aplikácií je spracovaný v ITIL ako “funkcia”, ktorá zohráva dôležitú úlohu pri správe aplikácií a systémov. Nie všetky činnosti pre správu aplikácií sú pokryté inými procesmi ITIL, preto sa pre tieto činnosti vytvorili v ITIL 2011 procesné mapy a vznikol proces Správa aplikácií. [2][3]

Správa IT infraštruktúry (Technical Management)

Proces Správa IT infraštruktúry je spracovaný v ITIL ako “funkcia”, ktorá zohráva dôležitú úlohu pri správe IT infraštruktúry. Keďže nie všetky činnosti pre technické zabezpečenie sú pokryté v iných ITIL procesoch, boli pre túto správu vytvorené procesné mapy a rozhodlo sa zaviesť samostatný proces. [2][3]

Neustále zlepšovanie služby

Aktualizácia ITIL 2011 kladie úplne nový dôraz na neustále zlepšovanie služby a procesov, ako to bolo predchádzajúcich vydaniach, či už v ITIL V2, alebo ITIL V3. Procesy Hodnotenie služieb a Plán zlepšovania služieb sa stali zásadnou disciplínou procesu - Neustále zlepšovanie služieb. Ide o jedinú publikáciu, v ktorej došlo k redukcii rozsahu z pôvodných 308 na 246 strán, pretože mnohé odseky sa v pôvodnej publikácií ITIL V3 opakovali. Zlepšený bol 7 krokový proces zlepšovania vo vzťahu k Demingovmu cyklu a k znalostnému manažmentu. Model CSI bol premenovaný na CSI prístup a ďalšou novinkou je predstavenie konceptu pre zaznamenanie iniciatív na zlepšovanie v rámci organizácie - CSI register. K minimálnym zmenám došlo v publikácií pre zlepšenie čitateľnosti a jednoznačne boli zmeny orientované na dokumentovanie vzťahov medzi CSI a ostatnými úrovňami životného cyklu služby. [1][2][3]

Záver

Aktualizácia ITIL 2011 priniesla mnoho nových zmien, ktoré sprehľadnili a zjednodušili správu procesov, workflow a služieb. Svojou inováciou sa chce viac priblížiť svojim používateľom a vo svojom obsahu zohľadnila ich návrhy a pripomienky. Recenzenti si hlavne pochvaľujú pridanú zrozumiteľnosť a súdržnosť medzi piatimi publikáciami a tiež zlepšenie čitateľnosti. Podstatou aktualizácie ITIL 2011 je tiež odstránenie nezrovnalostí, ktoré vznikli vo vydaní ITIL 2007. [4]

Jazyk a popisy sú tak jasné, že dávajú čitateľovi omnoho jasnejší zmysel pre procesy. V publikácií Stratégia Služby sa dosiahlo výrazné zlepšenie a poukázanie na to, ako robiť veci ľahšie, čím sa stratégia stala oveľa dostupnejšou. Za pochválenie stojí aj prepracovanie diagramov, ktoré sú lepšie a jednoduchšie nakreslené s jasnejšími popismi. [4]

Celkovo môžeme povedať, že aktualizácia je prínosom a je bližšie k používateľom, pričom stále predstavuje štandardný rámec pre riadenie IT služieb, ktorý môže byť prijatý a prispôsobený ako veľkým organizáciám, tak i malým.

Referencie

1) Akreditácia a poslanie SNAS [online]. Slovenská národná akreditačná služba, Bratislava. [cit. 2010-12-07]. Dostupné na internete: <http://www.snas.sk/index.php?page=1&page_sub=63>.
2) BALCO, P.: IT Governance - STN ISO/IEC 38500 [online]. ÚNMS SR, Newsletter / NL_17_09. [cit. 2010-09-30]. Dostupné na internete: <http://www.unms.sk/?it-governance-stn-iso-iec-38500>.
3) Business Process Model and Notation (BPMN), Version 1.2. OMG Standard, January 2009 [online]. [cit. 2010-10-21]. Dostupné na internete: <http://www.omg.org/spec/BPMN/1.2/>.
4) Citation Technologies and ANSI Partner to Bring Full Collection of ISO Standards to Market on Robust citation® Web-based Platform. ANSI Press Release, New York, 2009.
5) COBIT Framework for IT Governance and Control [online]. ISACA, May 2007. [cit. 2010-11-25]. Dostupné na internete: <http://www.isaca.org/Knowledge-Center/COBIT/>.
6) General information on the list of technical committees [online]. International Organization for Standardization [cit. 2010-10-06]. Dostupné na internete: <http://www.iso.org/iso/standards_development/technical_committees.htm>.
7) HAVELKA, M.: Hlavné rozdiely ITIL V3 verzus ITIL V2. eFocus 3/2008, s. 12-14.
8) International Classification for Standards. 6th Edition. International Organization for Standardization, Genève, Switzerland, 2005.
9) International harmonized stage codes [online]. International Organization for Standardization [cit. 2010-09-22]. Dostupné na internete: <http://www.iso.org/iso/stage_codes.pdf>.
10) International organization for security and crisis planning - Normy ISO 27000 [online]. KORAK Slovakia, s.r.o., Banská Bystrica. [cit. 2010-11-05]. Dostupné na internete: <http://www.korak.sk/~milan/index.php/sk/normy-iso-27000>.
11) ISO 20000 - Systém manažérstva informačných technológií (SMIT) [online]. TÜV NORD Slovakia, s.r.o., Bratislava. [cit. 2010-12-15]. Dostupné na internete: <http://www.tuvnord.sk/mnu1700.htm>.

12) ISO 20000 Certification & IT Service Management. Bureau Veritas Services, 2007.
13) ISO/IEC Guide 2:2004. Standardization and related activities - General vocabulary. International Organization for Standardization / International Electrotechnical Commission, 2004.
14) IT Service Management - Certifikácia podnikov a jednotlivcov podľa normy ISO 20000 [online]. OMNICOM, s.r.o., Bratislava. [cit. 2010-12-15]. Dostupné na internete: <http://www.itsm.sk/sk/Certifikacie/Certifikacia-podnikov-a-jednotlivcov-podla-normy-ISO-20000.alej>.
15) IT Service Management - Čo je to ITSM [online]. OMNICOM, s.r.o., Bratislava. [cit. 2010-09-24]. Dostupné na internete: <http://www.itsm.sk/sk/ITSM/Co-je-to-ITSM.alej>.
16) IT Service Management - História a vývoj ITIL [online]. OMNICOM, s.r.o., Bratislava. [cit. 2010-09-29]. Dostupné na internete: <http://www.itsm.sk/sk/ITIL/Historia-a-vyvoj-ITIL-.alej>.
17) IT Service Management - ISO/IEC 20000 [online]. OMNICOM, s.r.o., Bratislava. [cit. 2010-09-30]. Dostupné na internete: <http://www.itsm.sk/sk/ISO-IEC-20000.alej>.
18) IT Service Management - Prínosy implementácie normy [online]. OMNICOM, s.r.o., Bratislava. [cit. 2010-09-30]. Dostupné na internete: <http://www.itsm.sk/sk/ISO-IEC-20000/Prinosy-implementacie-normy.alej>.
19) IT Service Management - Vzťah ITIL® a noriem kvality podľa ISO 9000 [online]. OMNICOM, s.r.o., Bratislava. [cit. 2010-09-29]. Dostupné na internete: <http://www.itsm.sk/sk/ITIL/Vztah-ITIL-a-noriem-kvality-podla-ISO-9000.alej>.
20) ITU-T Recommendations [online]. International Telecommunication Union [cit. 2010-10-14]. Dostupné na internete: <http://www.itu.int/itu-t/recommendations/index.aspx>.
21) ITU-T Standardization Sector [online]. International Telecommunication Union [cit. 2010-10-14]. Dostupné na internete: <http://www.itu.int/net/about/itu-t.aspx>.
22) JANÁČ, R.: Riadenie IT služieb. eFocus 3/2008, s. 26-29.
23) JANÁČ, R.: Význam BPM pre riadenie IT. eFocus 3/2008, s. 30-34.
24) Krátky slovník slovenského jazyka. Štvrté, doplnené a upravené vydanie. Bratislava, Veda 2003.

25) MATEDIES, A. a kol.: Manažérstvo kvality. Bratislava, Epos 2006.
26) New Approach Standardisation in the Internal Market [online]. [cit. 2010-11-09]. Dostupné na internete: <http://www.newapproach.org>.
27) POLÁK, R.: Procesný model SMK podľa STN EN ISO 9001 [online]. POLING, Čadca. [cit. 2010-11-10]. Dostupné na internete: <http://www.poling.sk/procesny-model.php>.
28) Publicizing your ISO 9000 or ISO 14000 certification [online]. ISO Central Secretariat, Genève, Switzerland. [cit. 2010-12-07]. Dostupné na internete: <http://www.simplyquality.org/publicity.pdf>.
29) Slovník cudzích slov (akademický). Druhé, doplnené a upravené slovenské vydanie. Bratislava, SPN 2005.
30) Standardization guidelines for IST research projects interfacing with ICT standards organizations. COPRAS consortium, 2007.
31) SÚTN - Autorské právo a právo na používanie technických noriem [online]. Slovenský ústav technickej normalizácie, Bratislava. [cit. 2010-12-07]. Dostupné na internete: <http://www.sutn.sk/default.aspx?page=fb39909f-66d1-490c-811a-1a403672ca07>.
32) SÚTN - Certifikačný orgán Slovenského ústavu technickej normalizácie [online]. Slovenský ústav technickej normalizácie, Bratislava. [cit. 2010-12-07]. Dostupné na internete: <http://www.sutn.sk/default.aspx?page=6cb4107b-a582-4b69-a9df-ceedbea8171c>.
33) SÚTN - História a poslanie organizácie [online]. Slovenský ústav technickej normalizácie, Bratislava. [cit. 2010-10-18]. Dostupné na internete: <http://www.sutn.sk/default.aspx?page=179cad9a-a1e0-4e89-860f-e9d2d4d8568c>.
34) SÚTN - Úloha normalizácie [online]. Slovenský ústav technickej normalizácie, Bratislava. [cit. 2010-10-18]. Dostupné na internete: <http://www.sutn.sk/default.aspx?page=81f79981-12c5-491e-87e3-491c73710141>.
35) SÚTN - Výročná správa za rok 2009. Bratislava, Slovenský ústav technickej normalizácie, 2009.
36) The Annual Report of ETSI, 2009. European Telecommunications Standards Institute, Sophia Antipolis Cedex, France, ETSI 2009.

37) The Business Perspective: The IS View on Delivering Services to the Business. Office of Government Commerce, UK. Stationery Office Books, 2005.
38) Unified Modeling Language (UML), Version 2.3. OMG Standard, May 2010 [online]. [cit. 2010-10-21]. Dostupné na internete: <http://www.omg.org/spec/UML/2.3>.
39) Web Services Business Process Execution Language Version 2.0. OASIS Standard, 11 April 2007 [online]. [cit. 2010-10-21]. Dostupné na internete: <http://docs.oasis-open.org/wsbpel/2.0/>.
40) ZVIJÁK, O.: Ako postupovať pri implementácii ISO 20000. eFocus 3/2008, s. 39-40
41) KOSTERCOVÁ, E., Informačná bezpečnosť [on-line] [cit 2012.4.12]. Dostupné na internete: <http://download.matus.in/security/Informacna%20bezpecnost%20-%20predmet%20na%20FEI/2008.06.ppt >
42) Bíro,P., INFORMATIZÁCIA - Informačná bezpečnosť [on-line] [cit 2012.4.12]. Dostupné na internete: < http://www.informatizacia.sk/informacna-bezpecnost/>
43) Information Security Management System versus ITIL – IT Security Management. Do- stupné na internete: <http://www.slideshare.net/Billy82/isoiec-27001-information- security-management-system-vs-itil>
44) Security Revue [on-line] [cit 2012.3.18]. Dostupné na internete: <http://www.securityrevue.com/article/2008/07prehlad-metodik-metrik-a-kriterii-hodnorenia-efektivneho-isms-cast-i/>
45) ITIL webportal - ITSM [on-line] [cit 2012.3.18]. Dostupné na internete: <http://www.itsm.sk/sk/Poradenstvo/ISO-IEC-20000-Pre-Audit.alej>
46) Clinch, Jim. ITIL v3 and Information Security. Best management practise: 2009
47) ITIL security management. Dostupné na internete: <http://en.wikipedia.org/wiki/ITIL_security_management>
48) ITIL 2011. In: Wikipedia: the free encyclopedia [online]. Wikimedia Foundation, 2001-2012, 20 December 2011 [cit. 2012-03-14]. Dostupné z: http://wiki.en.it-processmaps.com/index.php/ITIL_2011

49) ITIL Publication Updates: ITIL 2011 Summary of Updates - English. In: Itil-officialsite [online]. [cit. 2012-03-14]. Dostupné z: http://www.itil-officialsite.com/Publications/ITILPublicationUpdates.aspx

50) ITIL Aktualizácia. 2011, 13 s. Dostupné z: www.tempest.sk/ext_dok-itservices2011_itil-aktualizacia/950c

51) BEST MANAGEMENT PRACTICE. ITIL 2011 gets a warm welcome from reviewers [online]. [cit. 2012-03-14]. Dostupné z: http://www.best-management-practice.com/Knowledge-Centre/News/ITIL-News/?DI=630839

52) ITIL – výkladový slovník a zkratky v češtině. In: ITIL – výkladový slovník a zkratky v češtině [online]. [cit. 2012-05-06]. Dostupné z: http://www.itil-officialsite.com/InternationalActivities/ITILGlossaries_2.aspx

53) Slovník ITIL® v3. In: Slovník ITIL® v3 [online]. 23.3.2009 [cit. 2012-05-06]. Dostupné z: http://www.itsmf.sk/sk/itSMF-IT-Service-Management-Forum.alej

54) Service Management Body of Knowledge (SMBOK.). Service management 101 [online]. 1996-2011 [cit. 2012-05-06]. Dostupné z: http://www.servicemanagement101.net/pages/home

Zoznam skratiek

CCTA **C**entral **C**ommunications and **T**elecommunications **A**gency

ICT **I**nformation and **C**ommunication **t**echnology

IS **I**nformačný **S**ystém

IT **I**nformation **T**echnology

ITIL **I**nformation **T**echnology **I**nfrastructure **L**ibrary

ITSM **IT S**ervice **M**anagement

itSMF **IT S**ervice **M**anagement **F**orum

OGC **O**ffice of **G**overnment **C**ommerce

OLA **O**perational **L**evel **A**greement

PDCA **P**lan **D**o **C**heck **A**ct

PRINCE Projects **in C**ontrolled **E**nvironment

RAM **R**andom **A**ccess **M**emory

SDP **S**ervice **D**esign **P**ackage

SPOC **S**ingle **P**oint **o**f **C**ontact

SLA **S**ervice **L**evel **A**greement

SLP **S**ervice **L**evel **P**ackage

CMS systém pre správu konfigurácií (Configuration Management System)

CMDB konfiguračná databáza (Configuration database)

CI konfiguračná položka (configuration item)

DML Definitive Media Library

ECAB Komisia pre naliehavé zmeny (Emergency Change Advisory Board)

SKMS Systém manažmentu znalostí služieb (Service Knowledge Management System)