Fakulta informatiky MU

Komentovaný výklad norem ISO 20000

Studijní materiál

2008

©Masarykova universita 2008

Předmluva

Cílem komentovaného vydání souhrnu norem ISO 20000 je vytvořit v rámci projektu FRVŠ 1613/2008 pro studenty Masarykovy university studijní materiál, který jim umožní seznámit se co nejrychleji se souborem norem v oblasti poskytování služeb informačních technologií (IT) a seznámit je s praxí, především probelmatikou odběratelsko dodavatelských smluv v této velmi se rozvíjející oblasti aplikace moderních informačních a komunikačních technologií. Tento soubor norem, které vznikly původně v osmdesátých letech minulého století ve Velké Británii jako normy BS 15000-1 a 15000-2, stanovuje velmi racionální a přesná pravidla plánování a realizace služeb IT, poskytovaných uživatelům (zákazníkům).

Služby IT jsou poměrně sofistikované a vyžadují dobře nastavená pravidla od stanovení rozsahu služby, plánu jejího zavedení přes implementaci až po tzv. regulace incidentů a řešení problémů. Obě normy ISO/IEC 20000-1 a 20000-2 vycházejí z nejlepších zkušeností praktik, známých ve firmách, zabývajících se informačními technologiemi. V oblasti normalizace služeb IT je v současné době celosvětovou normou procesní rámec pro poskytování IT služeb ITIL (Information Technology Infrastructure Library). Již méně je známa skutečnost, že hlavní doporučení tohoto rámce byly shrnuty v další britské normě BS 15000. Tyto normy budou zahrnuty do přenášek „Integrovaného systému managementu“ na Fakultě informatiky Masarykovy university a zpřístupněny v rámci Informačního systému Masarykovy university všem jejím studentů. Analogie s jinými normami pro systémy managementu jakosti je nabíledni. Stejně jako norma ISO 9001, která je základem pro uzavírání bilaterálních vztahů a ISO 9004, která je návodem, jak je optimálně plnit i zde je norma ISO/IEC 20000-1:2005 (Information technology – Service management – Part 1: Specification) zásadní, stanovující kritéria, zatímco norma ISO/IEC 20000-2:2005 (ISO/IEC 20000-2:2005 Information technology – Service management – Part 2: Code of practice) je více návodem, jak je plnit. Norma ISO/IEC 20000-1:2005 je oproti normě ISO 9001:2000 mnohem zásadovější, obsahuje velké množství povinných dokumentů i záznamů.

Vzhledem k tomu, že se jedná o normy, se kterými se mají seznámit studenti bakalářského a magisterského studia, kteří studují oblasti IT, nesnažili jsme se jednoznačně a přesně překládat všechny výrazy z angličtiny do češtiny, ale vyšly jsem z podobného přístupu jako v [10]. Tam, kde jsme se domnívali, že studenti spíše využívají anglické výrazy, ponechali jsme je i v textu, který vycházel z anglických originálů. Proto je v úvodu i tabulka ekvivalentních výrazů (českých, anglických a „počeštěných“ anglických) a doufáme, že jazykovědci nám některé zavedené slangové výrazy prominou.

Obsah

1 Úvod

V oblasti standardizace služeb informačních technologií (IT) je celosvětovou normou procesní rámec pro poskytování informačních (IT) služeb knihovna ITIL® (Information Technology Infrastructure Library)[1], která má následující charakteristické rysy:

1. **Procesní řízení** - ITIL používá moderní procesně orientovaný přístup k řízení IT služeb (na rozdíl od tradičního funkcionálního řízení). Proces je logický sled úkolů transformujících nějaký vstup na nějaký výstup, přičemž plnění jednotlivých úkolů v procesu je zajišťováno rolemi s jasně definovanými odpovědnostmi. Celý proces je řízen, monitorován, měřen, vyhodnocován a neustále vylepšován, což je odpovědností vlastníka procesu.
2. **Zákaznicky orientovaný přístup** - tento rys vyplývá přímo ze samotné podstaty managementu služeb IT; všechny procesy jsou designovány s ohledem na potřeby zákazníka, tzn. každá aktivita, každý úkon v každém procesu musí přinášet nějakou přidanou hodnotu pro zákazníka - pokud ne, pak je taková činnost nadbytečná.
3. **Jednotná terminologie** - jednotná terminologie je někdy málo doceňovanou nebo úplně opomíjenou charakteristikou ITIL, ale jen do té doby, než budeme poprvé v praxi řešit nedorozumění plynoucí z toho, že někdo používá stejný termín v jiném významu, než očekáváme.
4. **Nezávislost na platformě** - rámec procesů managementu IT služeb podle ITIL je nezávislý na jakékoliv platformě. Dokonce je možné ITIL použít i pro designování procesů (úplně mimo oblast informačních a komunikačních technologií - ICT) v jakékoliv organizaci, která podniká ve službách.
5. **Public Domain** - knihovna je volně dostupná, což znamená, že každý si může knihy ITIL koupit a procesy managementu služeb IT podle ITIL ve své organizaci implementovat. Tato skutečnost mj. přispěla k rychlému celosvětovému rozšíření ITIL.

Rámec ITIL byl vyvinut v osmdesátých letech minulého století pro účely britské vlády. Od té doby byl dále rozvíjen i dalšími organizacemi a konzultačními společnostmi. V současné době tvoří defacto celosvětově nejrozšířenější normou pro regulaci a poskytování IT služeb. Z principů stanovovaných v tomto rámci vychází i norma ISO 20000 (zkráceně 20k).

1.2 Důležité zkratky a pojmy

Dostupnost - schopnost prvku nebo služby plnit svou určenou funkci ve stanovený okamžik nebo během stanoveného období.

Položka konfigurace (CI) - prvek infrastruktury nebo položka, která je nebo bude řízena v procesu managementu konfigurací.

Konfigurační databáze (CMDB) - databáze obsahující všechny důležité informace o každé položce konfigurace a podrobnosti o zásadních vzájemných vztazích mezi nimi.

Incident - jakákoli událost, která není součástí běžného fungování služby, a která způsobí nebo může způsobit přerušení dodávky nebo snížení kvality služby.

Problém - neznámá základní příčina jednoho nebo více incidentů.

Uvolnění - soubor nových a/nebo změněných položek konfigurace, které jsou společně testovány a implementovány do produkčního prostředí.

Požadavek na změnu - formulář nebo obrazovka používané k záznamu požadavku na každou změnu jakékoliv položky konfigurace v rámci služby nebo infrastruktury.

[1] http://www.itil-officialsite.com/AboutITIL/WhatisITIL.asp

Dohoda o úrovni služeb (SLA) - písemná dohoda mezi poskytovatelem služeb a zákazníkem, která obsahuje popis služby a dohodnuté úrovně služeb.

POZNÁMKA: V rámci dodržení srozumitelnosti normy v organizacích v oblasti informačních a komunikačních technologií (ICT) jsou ponechány v tomto učebním textu některé v IT běžně používané termíny v anglickém jazyce. Důvodem je především to, že tyto pojmy jsou dlouhodobě používány v odborné veřejnosti a v obecně uznávané metodologií. ITIL (Information Technology Infrastructure Library). Český význam a souvislost s procesy a terminologií využitou v ITIL jsou:

Termín	**Přípustné použití termínu**	**Ekvivalent v ITIL**
Procesy zajišťující dodávku služeb	Service Delivery Processes	Service Delivery (název jednoho svazku z ITIL)
Management kapacit	Capacity Management	Capacity Management
Management kontinuity dodávky služeb Management dostupnosti	Service Continuity and Availability Management	IT Service Continuity Management Availability Management
Management úrovně služeb	Service Level Management	Service Level Management
Hlášení o úrovni služeb	Service Reporting	Není stanovován jako samostatný proces
Management informační bezpečnosti	Information Security Management	Security Management (název jednoho svazku z ITIL)
Rozpočtování a účtování IT služeb	Budgeting and Accounting for IT services	Financial Management for IT Services
Kontrolní procesy	Control Processes	Tato oblast je řešena v „Service Support" svazku
Management konfigurace	Configuration Management	Configuration Management
Management uvolňování jednotlivých verzí	Release Process	Release Management (součást Service Support)
Procesy řešení požadavků a problémů	Resolution Processes	Tato oblast je řešena v „Service Support" svazku
Management incidentů	Incident management	Incident management
Management problémů	Problem Management	Problem Management
Procesy řízení vztahů	Relationship Processes	Tato oblast je řešena v „Business Perspective: The IS View on Delivering Services to the Business"
Management vzájemných vztahů	Business Relationship Management	Business Perspective
Management vztahů s dodavateli	Supplier Management	Supplier Relationship Management

Hlavní doporučení tohoto rámce byly shrnuty v normě ISO/IEC 20000-1, česká verze viz [1], která má analogii s jinými normami pro systémy managementu kvality. Stejně jako norma ISO 9001, která je základem pro uzavírání bilaterálních vztahů a ISO 9004, která je návodem, jak je optimálně plnit, i zde je norma ISO/IEC 20000-1 zásadní, která stanovuje kritéria, zatímco norma ISO/IEC 20000-2, česká verze viz [2], je více návodem, jak je plnit. Norma ISO/IEC 20000-1 je oproti normě ISO 9001 mnohem zásadovější, obsahuje velké množství povinných dokumentů i záznamů. Normy ISO 20000 prosazují přijetí integrovaného procesního přístupu k efektivnímu dodávání řízených služeb, aby byly splněny podnikatelské požadavky a požadavky zákazníků. Aby organizace fungovala efektivně, musí identifikovat a kontrolovat řadu vzájemně souvisejících činností. Činnost využívající zdroje, a je řízena za účelem umožnění přeměny vstupů ve výstupy, může být považována za proces. Výstup z jednoho procesu tvoří často vstup do dalšího.

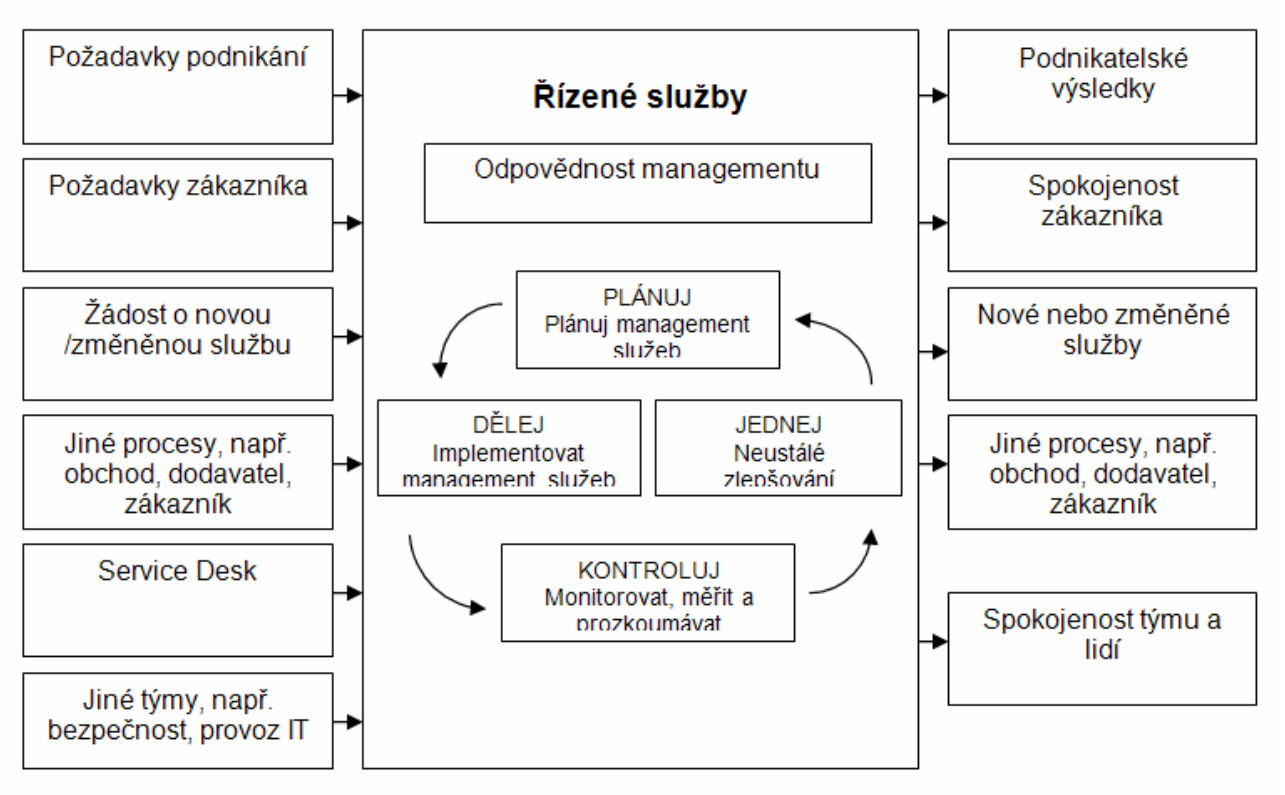
Norma ISO 20000 prosazuje přijetí integrovaného procesního přístupu k efektivnímu poskytování řízených informačních služeb, respektive informačních technologií (IT), aby byly splněny

podnikatelské požadavky a požadavky zákazníků. Aby organizace fungovala efektivně, musí identifikovat a kontrolovat řadu vzájemně souvisejících činností. Činnost využívající zdroje, a je řízena za účelem umožnění přeměny vstupů ve výstupy, může být považována za proces. Výstup z jednoho procesu tvoří často vstup do dalšího.

Koordinovaná integrace a implementace procesů managementu informačních (IT) služeb poskytuje trvalou kontrolu, větší účinnost a příležitost pro neustálé zlepšování. Provádění činností a procesů vyžaduje, aby lidé pracující v týmech „service desk[2]“, „service support“, „service delivery“ a v provozních týmech byli dobře organizovaní a koordinovaní. K zajištění efektivních účinných procesů jsou požadovány vhodné nástroje.

POZNÁMKA: Metodologie Deminga známá jako Plánuj-Dělej-Kontroluj-Jednej (PDCA - Plan-Do-Check-Act) může být aplikována na všechny procesy řízení informačních služeb. PDCA schéma může být popsáno následovně:

- *Plánuj (Plan)*: stanovit cíle a procesy nezbytné pro dosažení výsledků podle požadavků zákazníka a politiky organizace;
- *Dělej (Do)*: implementovat procesy;
- *Kontroluj (Check)*: monitorovat a měřit procesy a služby vzhledem k zásadám, cílům a požadavkům a reportovat výsledky;
- *Jednej (Act)*: provádět činnosti vedoucí k neustálému zlepšování dosaženého stavu.



Obrázek 1: Metodika Plánuj-Dělej-Kontroluj-Jednej pro jednotlivé procesy IT služeb.

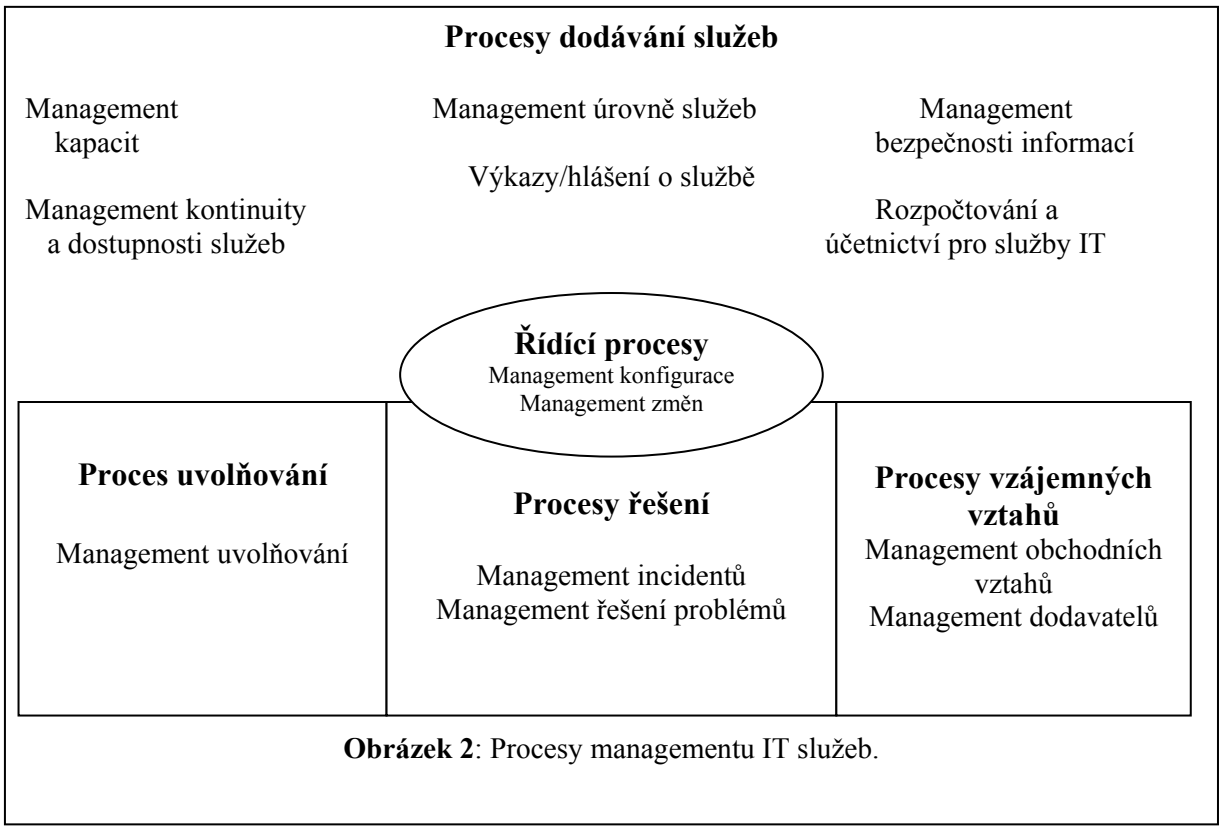
Metodika PDCA je podrobně popsána v obou normách ISO 20000-1 a ISO 20000-2 a shoduje se s metodikou systému řízení jakosti proto ji nebudeme podrobně popisovat a přejdeme rovnou na procesy v systému řízení informačních služeb, které bude zkráceně uvádět jako služby.

[2] skupina podpory pro první kontakt se zákazníkem, která provádí vysoký podíl celkových podpůrných prací.

2 Procesy podle normy ISO 20000

Specifikace procesů podle ITIL respektive podle normy ISO 2000 stanovuje požadavky na organizaci[3] s ohledem na dodání kontrolovaných informačních (IT) služeb v kvalitě přijatelné pro její zákazníky. Může být použita:

- organizacemi, které vstupují do výběrových řízení se svými informačními (IT) službami;
- organizacemi, které vyžadují důsledný přístup od všech poskytovatelů služeb v dodavatelském řetězci;
- poskytovateli služeb pro benchmarking jejich managementu IT služeb ;
- jako základ ohodnocení, které může vést k formální certifikaci;
- organizací, která potřebuje prokázat schopnost poskytovat IT služby, které splňují požadavky zákazníků;
- organizací, která usiluje o zlepšení IT služeb pomocí efektivní aplikace procesů pro monitorování a zlepšování kvality služeb.



Obrázek 2: Procesy managementu IT služeb.

Norma ISO 20000 specifikuje několik vzájemně úzce souvisejících procesů managementu informačních (IT) služeb, jak je znázorněno na obrázku (Obrázek 2.).

Vztahy mezi procesy závisejí na způsobu aplikace v rámci organizace a jsou obecně příliš složité na modelování, a proto nejsou vztahy mezi procesy v tomto diagramu ukázány.

Norma nespecifikuje vyčerpávající seznam cílů a organizace může zvážit, zda existují další cíle a opatření nezbytné ke splnění jejich konkrétních podnikatelských potřeb. Podstata obchodního vztahu mezi poskytovatelem služeb IT a organizací využívající tyto služby určí, jak budou implementovány požadavky této normy, aby byly splněny celkové cíle.

[3] Společnost, sdružení, firma, podnik, úřad nebo instituce, nebo jejich část nebo kombinace, ať už zapsané do obchodního rejstříku nebo ne, veřejné nebo soukromé, které mají své vlastní funkce a správu.

2.1 Odpovědnost vedení

Uplatňováním vedoucí role a svou činností musí vrcholové vedení poskytnout důkazy o svém závazku k rozvoji, implementaci a zlepšování své schopnosti v managementu služeb v rámci kontextu podnikání organizace a požadavků zákazníků. Vedení musí:

- stanovit politiku managementu IT služeb, cíle a plány;
- komunikovat důležitost plnění cílů managementu IT služeb a potřebu neustálého zlepšování;
- zajistit, aby požadavky zákazníků byly určeny a splněny v rámci cíle zlepšovat spokojenost zákazníků;
- určit člena vedení odpovědného za koordinaci a sledování a udržování všech služeb;
- určit a poskytnout zdroje pro plánování, implementaci, monitorování, přezkoumání a zlepšování poskytování, sledování a udržování služeb IT, např. získání vhodného personálu, kontrolu fluktuace personálu;
- řídit rizika v organizaci managementu IT služeb a ve službách samotných;
- provádět přezkoumání managementu IT služeb v plánovaných intervalech pro zajištění neustálé vhodnosti, přiměřenosti a efektivnosti.

2.2 Požadavky na dokumentaci

Vrcholové vedení organizace musí zajistit, aby byly pro audit k dispozici doklady o politice, plánech, postupech managementu služeb a jakýchkoliv souvisejících činností.

Většina dokladů o plánování a provozu managementu informačních (IT) služeb musí existovat ve formě dokumentů, které mohou být jakéhokoliv druhu, v jakékoliv formě a na jakémkoliv médiu vhodném pro jejich využití. Následující dokumenty jsou běžně považovány jako vhodné pro doklad o plánování managementu služeb:

- politiky a plány;
- dokumentace služeb;
- postupy;
- procesy;
- záznamy o řízení procesu.

Musí být stanoveny postupy a odpovědnosti pro tvorbu, přezkoumání, schvalování, udržování a řízení různých typů dokumentů a záznamů.

2.3 Řízené dokumenty

V organizaci poskytující IT služby musí být definován proces pro vytváření a řízení dokumentů, které pomohou zajistit, aby byly splněny popsané charakteristiky.

Dokumentace musí být chráněna proti zničení v důsledku, například špatných environmentálních podmínek a počítačových selhání.

2.4 Kvalifikace, povědomí a školení/výcvik

Vrcholové vedení organizace musí zajistit, aby si jejich zaměstnanci byli vědomi významnosti a důležitosti jejich činností a toho, jak přispívají k dosažení cílů managementu IT služeb.

Zaměstnanci pracující v oblasti managementu služeb musí získat svou kompetenci na základě odpovídajícího vzdělání, školení, dovedností a zkušeností. Organizace by měla:

- určit potřebnou kvalifikaci pro každou roli v managementu služeb;
- zajistit, aby si pracovníci uvědomovali významnost a důležitost jejich činností v rámci širšího podnikatelského kontextu a jejich přínos k dosažení cílů kvality;
- udržovat vhodné záznamy o vzdělání, školení, dovednostech a zkušenostech;
- poskytovat výcvik nebo přijmout jiná opatření k zajištění těchto potřeb;
- hodnotit efektivitu přijatých opatření.

Poskytovatel IT služeb musí rozvíjet a zvyšovat profesionální kvalifikaci svých zaměstnanců. Mezi opatřeními přijatými k dosažení tohoto záměru se poskytovatel služeb musí vypořádat s následujícím činnostmi:

- *náborem zaměstnanců*: s cílem ověření platnosti detailů údajů uchazečů o práci (včetně jejich profesní kvalifikace) a identifikace silných stránek, slabých stránek a potenciálních schopností žadatele v porovnání s popisem/profilem práce, s cíli managementu služeb a s celkovými cíli kvality služeb;
- *plánováním jejich kariérního růstu*: s cílem personálního zajištění nových nebo rozšiřujících se služeb (také kontrahovaných služeb), používání nové technologie, přiřazení pracovníků managementu služeb k týmům vývojových projektů, následného plánování a vyplnění jiných mezer v důsledku očekávané fluktuace pracovníků;
- *školením a rozvojem znalostí zaměstnanců*: s cílem identifikace požadavků na školení a rozvoj jako je plán školení a rozvoje a zajišťování včasného a efektivního dosažení cílů školení a rozvoje.

Pracovníci musí být vyškoleni v odpovídajících aspektech managementu služeb (např. pomocí formálních kurzů, samostudiem, instruktáží a výcvikem při práci) a jejich týmová práce a manažerské schopnosti musí být rozvíjeny. Chronologické záznamy o výcviku musí být udržované pro každého jedince společně s popisem poskytnutého výcviku.

Z důvodu dosažení náležité úrovně kvalifikace týmů musí poskytovatel služeb rozhodnout o optimálním mixu dočasných a trvalých členů týmu. Poskytovatel služeb musí také optimalizovat poměr mezi náborem nových pracovníků s požadovanými schopnostmi a přeškolením stávajícího personálu.

U všech zaměstnanců musí poskytovatel služeb přezkoumat úroveň každého jednotlivce nejméně jedenkrát ročně a přijmout náležitá opatření.

3 Procesy dodávání služeb

V této kapitole popíšeme jednotlivé hlavní procesy, které se mohou vyskytovat v poskytování/dodávání IT služeb. Jedná se o procesy: *Management úrovně služeb* (Service level management); *Hlášení/zprávy o službách* (Service reporting); *Management dostupnosti a kontinuity* (Availability and service kontinuity management); *Rozpočtování a účetnictví ve službách IT* (Budgeting and accounting for IT services); *Management kapacit* (Capacity management); *Management bezpečnosti informací* (Information security management).

3.1 Management úrovně služeb

Cíl: Stanovovat, odsouhlasit, zaznamenávat a regulovat úrovně služeb.

Celý sortiment informačních služeb, který má být poskytován, musí být odsouhlasen všemi stranami společně se souvisejícími cíli a charakteristikami pracovní zátěže. O odsouhlasení stranami musí být veden záznam. Každá poskytovaná služba musí být stanovena, odsouhlasena a dokumentována v jedné nebo více *dohodách o úrovni poskytnutých služeb* (Service Level Agreements) dále zkráceně SLA. SLA společně s podpůrnými smlouvami o službách, smlouvami se třetími stranami a souvisejícími postupy, musí být odsouhlasena všemi relevantními stranami a zaznamenány. SLA musí být spravovány procesem pro řízení změn.

Smlouvy SLA musí být udržovány pravidelným přezkoumáním zúčastněnými stranami, aby bylo zajištěno, že jsou aktuální a zůstávají efektivní po celou dobu trvání.

Úrovně služeb musí být monitorovány a porovnávány s cíli tak, aby byla zřejmá aktuální informace a informace o trendech. Důvody pro neshody musí být zaznamenány a přezkoumány a musí poskytovat vstup do plánu zlepšování služeb.

3.1.1 Katalog služeb

Katalog služeb musí určit všechny služby. Může na něj být odkaz ze SLA a měl by být použit jako často se měnící materiál ve vztahu k vlastní SLA.

Katalog služeb musí být udržován a aktualizován. Katalog služeb je klíčový dokument pro stanovení očekávání zákazníků a musí být snadno a široce dostupný jak pro zákazníky, tak pro pracovníky podpory.

3.1.2 Dohody o úrovni služeb

Služba musí být formálně dokumentovaná v dohodě o úrovni služeb (SLA). SLA musí být formálně potvrzená zodpovědným manažerem zákazníka a poskytovatele služby. SLA musí být řízena v rámci managementu změn, stejně jako i služba, kterou popisuje. SLA musí zahrnovat pouze takovou podskupinu cílů, která zajistí soustředění zájmu pouze na nejdůležitější stránky služby.

Minimální obsah, který musí být v SLA nebo který může být ze SLA přímo odkazován je:

- krátký popis služby;
- doba platnosti a/nebo mechanismus řízení změny SLA;
- detaily autorizace;
- stručný popis komunikace, včetně reportingu;
- kontaktní údaje osob pověřených jednat při mimořádných událostech, účastnit se při řešení incidentů a problémů, při obnově služby nebo nalezení náhradního řešení;
- provozní doba služby, např. 09:00 hodin až 17:00 hodin, data výjimek (např. víkendy, státní svátky), pokrytí kritických podnikatelských období a mimopracovní doby;
- plánovaná a dohodnutá přerušení, včetně upozornění, které musí být učiněno, četnost za období;

- odpovědnosti zákazníka, např. bezpečnost;
- závazky a povinnosti poskytovatele služby, např. bezpečnost;
- pravidla pro určení priority a dopadu;
- postupy práce se stížnostmi;
- cíle služby;
- limity pracovního zatížení (horní a dolní), např. schopnost služby podporovat odsouhlasený počet zákazníků/objem práce, průchodnost systému;
- vysoká úroveň detailů finanční kontroly, např. kódy sazeb atd.,
- opatření, která musí být přijata v případě přerušení služby;
- postupy v hospodaření;
- slovníček pojmů;
- podpůrné a související služby;
- jakékoliv výjimky v podmínkách stanovených v SLA.

3.1.3 Proces řízení úrovně služeb

Zásadní změny podnikání v důsledku, například růstu, reorganizací a fúzí společností, a měnících se požadavků zákazníků, mohou vyžadovat úpravu úrovně služeb, jejich opětné určení nebo dokonce dočasné přerušení. Proces *řízení úrovně služeb* (Servis level management) zkráceně SLM, musí být pružný, aby se přizpůsobil těmto změnám. SLM proces musí zajistit, aby poskytovatel informačních (IT) služeb zůstal zaměřený na zákazníka po celou dobu plánování, implementace a v trvalém řízení dodávky služeb.

Proces SLM musí motivovat jak poskytovatele služeb, tak zákazníka k využívání aktivnějšího přístupu, který zajistí, aby přijali společnou odpovědnost za služby.

3.1.4 Smlouvy o podpůrných službách

Podpůrné služby, na kterých závisí dodávané služby, musejí být dokumentované a odsouhlasené s každým dodavatelem služeb. Jsou typicky nazývané „Operational Level Agreement" (OLAs).

Praktický příklad „Managementu úrovně služeb“:

Ve většině případů se u organizace jedná o obchodní závazkové vztahy uvedené v zákoně č. 63/2001 Sb., obchodní zákoník, ve znění pozdějších předpisů, a to i s přihlédnutím k ustanovením § 729 (závazkové vztahy v mezinárodním obchodu).

Bez takové „smlouvy“ je jakékoliv hodnocení úrovně poskytovaných služeb v podstatě znemožněno. To platí i v případě poskytování služeb „internímu“ zákazníkovi.

Každý smluvní vztah organizace s dodavatelem (SLA) je řešen samostatně v rámci kontraktačního řízení, které je součástí jednotlivých procesů (projektů) se stanovenými rolemi a specifickými činnostmi, jež jsou však pro každý projekt jedinečné.

Popisy procesů, včetně určujících faktorů obsahu, struktury a cílů SLA, jsou součástí projektové dokumentace.

Cílem organizace je, aby SLA uzavírané s klienty obsahovaly (mimo formálních náležitostí) následující kategorie údajů: stručný popis IT služby, její požadavky, rozsah, úroveň; cíle služby; stručný popis komunikace a její vykazování; provozní doba IT služby, výjimky z této doby (například víkendy, státní svátky), pokrytí kritických časových úseků z pohledu byznysu a mimopracovní doby; způsob měření a vykazování dosažených úrovní služeb; plánovaná a dohodnutá přerušení, včetně způsobu vyrozumění, četnost za období; akce prováděné v případě přerušení služby, doba zahájení nápravných opatření; podpůrné a související služby; základní charakteristiky a limity pracovní zátěže, např. garantovanou rychlost přenosu dat, rychlost odezvy, max. počet současně připojených uživatelů, objem práce, výkonnost systému apod.; jakékoli výjimky v podmínkách stanovených v SLA; kontaktní údaje na osoby oprávněné jednat v naléhavých situacích a podílet se na nápravě, obnově nebo náhradním pracovním postupu při incidentech a problémech; mechanismus řízení změn SLA; finanční

plnění; práva a odpovědnosti společnosti; práva a odpovědnosti zákazníka (smluvního partnera); formální postup pro řešení stížnosti týkajících se služby; informace o finančních aspektech, výše a způsob plateb; případné administrativní postupy; bezpečnostní ujednání; sankce; doba platnosti SLA.

3.2 Výkazy/hlášení/zprávy o službách

Cíl: Vytvářet dohodnuté, aktuální, spolehlivé a přesné zprávy pro kvalifikované rozhodování a pro efektivní komunikaci.

3.2.1 Politika

Součástí politiky musí být odsouhlasené a zaznamenané požadavky na podávání zpráv (reporting) o informačních (IT) službách jak pro zákazníky, tak vnitřní management organizace. Monitorování a reporting služeb zahrnuje všechny měřitelné stránky služeb, poskytující aktuální a časové analýzy.

Tam, kde se využívají společní poskytovatelé služeb, dodavatelé a dodavatelé třetích stran, musí zprávy odrážet vztahy mezi dodavateli. Například, vedoucí dodavatel musí podávat zprávu za celou informační (IT) službu, kterou poskytuje, včetně všech služeb od dodavatelů třetích stran, které kontroluje jako součást zákaznických služeb.

3.2.2 Účel a kontrola kvality u zpráv o službách

Zprávy o informačních (IT) službách musí být včasné, jasné, spolehlivé a stručné. Musí být přiměřené k potřebám příjemce a dostatečně správné, aby byly využitelné jako podpůrný nástroj pro rozhodování managementu. Prezentace musí napomáhat pochopení zpráv, aby byly snadno přijatelné, např. včetně použití grafů (nebylo by lepší třeba: včetně grafických vizualizací výsledků?).

Typy zpráv se dělí podle toho, co mělo být reportováno na:

- *reaktivní zprávy*, které ukazují, co se již stalo;
- *proaktivní zprávy*, které dávají předběžné upozornění na důležité události, čímž umožňují, aby byla přijata preventivní opatření (například zprávy o hrozícím nedodržení SLA);
- předem *plánované zprávy* obsahující plánované činnosti.

3.2.3 Zprávy o službách

Vedoucí dodavatel musí vytvořit zprávy pro zákazníky a management, které budou zahrnovat:

- dosažený stav vzhledem k cílovým úrovním informačních (IT) služeb, např. zprávy o výpadcích, dosažených hodnotách služeb;
- neshody s normami;
- typické pracovní zatížení a informace o objemech, např. incidentů, problémů, změn a úkolů, klasifikaci, umístění, zákazníkovi, sezónních trendech, mixu priorit, počtu žádostí o podporu;
- hlášení o dosaženém stavu následující po významných událostech, např. změny a nové release;
- periodické informace o trendech (např. den, týden, měsíc, jiné období); trendy jsou dlouhodobé, spíš: trendech a výkyvech (např. den, týden, měsíc, jiné období);
- reporty, které zahrnují informace ze všech procesů, např. počet incidentů a nejčastěji pokládané otázky, nespolehlivé komponenty infrastruktury, úkoly náročné na zdroje/náklady;

Příklad realizace „Zpráv o službách“:

Každá změna v SLA je přímo v dokumentech SLA přesně datována a popsána. V rámci každoročních interních auditů jsou SLA prozkoumávány a počty změn jsou zaznamenávány do daného dokumentu, který je archivován.

Změna v naléhavé situaci je mimořádná událost a jako taková je zaznamenávána v samostatném dokumentu, které jsou ukládány např. do adresáře konfigurační databáze. Jejich počet se

vyhodnocuje každých 6 měsíců počtem dokumentů v uvedeném adresáři. Výsledek je zaznamenán do speciálního souboru, který je archivován.

Každá stížnost je zaznamenána do speciálního formuláře pojmenovaného např. „Záznam o stížnosti.doc“. V rámci interního auditu jednou ročně jsou tyto záznamy přezkoumány a jejich počet je zaznamenán ve zprávě z auditu.

Dosažené cíle IT služeb jsou srovnávány s cíli, které jsou definované v SLA. V rámci každoročního přezkoumávání SLA je kvalifikovaným odhadem stanoveno procento jejich dosažení. Výsledek je pak uveden ve zprávě z přezkoumávání SLA.

3.3 Management dostupnosti a kontinuity služeb

Cíl: Zajistit, aby odsouhlasené závazky vůči zákazníkům mohly být splněny za všech okolností.

3.3.1 Obecně

Požadavky na kontinuitu a dostupnost informační (IT) služby musí být identifikovány na základě zákaznických podnikatelských priorit, smluv o úrovni služeb a ohodnocených rizik. Poskytovatel služeb musí udržovat dostatečnou úroveň služeb společně s proveditelnými plány navrženými k zajištění toho, že odsouhlasené požadavky mohou být splněny za všech okolností od normálních podmínek až po závažné výpadky služeb. Poskytovatel služeb musí plánovat na základě známých údajů, podle růstu nebo poklesu zátěže, podle očekávaných špiček, tj. nejvyšší a nejnižší úrovně zátěže nebo průchodnosti, a podle dalších známých budoucích změn. Požadavky musí zahrnovat přístupová práva a čas odezvy, stejně jako celkovou dostupnost komponent systému.

Řízení dostupnosti a kontinuity služeb musí fungovat společně s cílem zajistit, aby dohodnuté úrovně služeb byly dodržované. Tyto požadavky musí mít významný vliv na činnosti, úsilí a přidělované zdroje k dosažení dostupnosti služeb, které jsou podporovány.

3.3.2 Monitorování dostupnosti a činností

Řízení dostupnosti musí:

- monitorovat a zaznamenávat dostupnost služeb;
- udržovat správná historická data;
- provádět srovnání s požadavky stanovenými v SLA k identifikaci neshod s dohodnutými cíli dostupnosti;
- dokumentovat a přezkoumávat neshody;
- předpovídat budoucí dostupnost.

Musí zajistit dostupnost všech komponent služby, se zaznamenanými nápravnými opatřeními a jejich provedením.

3.3.3 Strategie kontinuity služeb

Poskytovatel informačních (IT) služeb musí rozvíjet a udržovat strategii, která stanovuje obecný přístup, jaký má být přijat, aby byly splněny závazky kontinuity služeb. To musí zahrnovat hodnocení rizika a musí vzít v úvahu dohodnutou dobu poskytování služeb a kritická období podnikání. Poskytovatel služeb musí odsouhlasit pro každou skupinu zákazníků a služeb:

- maximální přijatelnou nepřetržitou dobu ztracené služby;
- maximální přijatelnou dobu zhoršené služby;
- přijatelnou zhoršenou úroveň služby během doby obnovy služby.

Strategie kontinuity musí být revidována v dohodnutých intervalech, nejméně jednou ročně. Jakékoliv změny ve strategii musí být formálně odsouhlaseny.

3.3.4 Plánování a testování kontinuity služeb

Plány kontinuity služeb a související dokumenty (např. smlouvy) musejí být ohodnoceny z hlediska jejich dopadu před tím, než jsou odsouhlaseny změny systému. Plány kontinuity služeb a související dokumenty (např.smlouvy) musejí být ohodnoceny z hlediska jejich dopadu před tím, než jsou odsouhlaseny změny systému a služeb, a před tím, než jsou odsouhlaseny významné nové nebo pozměněné požadavky zákazníka.

Testování musí být prováděno s frekvencí a důsledností dostatečnou pro získání jistoty, že plány kontinuity jsou efektivní a zůstávají takové i vůči měnícím se systémům, procesům, personálu a potřebám podnikání. Testování musí být společnou aktivitou zákazníka a poskytovatele služeb založená na dohodnutém souboru cílů. Nedostatky odhalené v testu musí být dokumentovány a přezkoumávány, aby mohly být vstupem pro plán zlepšování služeb.

Příklad:

Organizace zahrnuje do procesu řízení dostupnosti služeb zejména:

- *monitorování (měření) a zaznamenávání dostupnosti informačních (IT) služeb;*
- *provádění srovnání s požadavky uvedenými v SLA s cílem zjištění neshod se stanovenými cíli dostupnosti;*
- *dokumentování a přezkoumávání neshod;*
- *udržování autentických záznamů o historických datech v oblasti dostupnosti služeb;*
- *zajištění dostupnosti všech prvků služby a dokumentování realizací nápravných opatření;*
- *anticipace budoucí dostupnosti služby (potenciálních problémových záležitostí) a realizace preventivních opatření.*

Veškeré tyto činnosti jsou zaznamenávány do dokumentů „Záznam o problému“, „Záznam o stížnosti“, popř. „Záznam o neshodě“ (jako v QMS – V systému řízení jakosti), „Záznam o řešení opatření k nápravě a preventivních opatření“ (QMS) a jejich vyřízení je realizováno v souladu s ustanovením dokumentů „Řízení incidentů a problémů“, „DP Řízení neshod, opatření k nápravě a preventivních opatření” (QMS) a „Přezkoumání ITSM (Integrovaného systémů managementu)“.

Dokumenty pro plánování a testování kontinuity IT služeb pak obsahují:

- *popis rychlé dostupnosti záloh dat, dokumentů a software a jakékoli zařízení a personálu nezbytného pro obnovení služby;*
- *údaje o bezpečném vzdáleném místě, kde je uložena kopie plánu a všech dokumentů kontinuity služeb, spolu se zařízením, které je nezbytné pro jejich použití;*
- *popis postupu postup navrácení do normálního stavu;*
- *jsou posuzovány (spolu s dalšími souvisejícími dokumenty, např. smlouvami) z hlediska dopadu změn ve službách ještě před schválením a realizací těchto změn;*
- *jsou testovány dále po provedení každé závažné změny ve službách;*
- *jsou uloženy tak, aby nejméně jedna kopie (a všech dalších dokumentů kontinuity služeb) byla uložena a udržována na bezpečném vzdáleném místě, spolu se zařízením, které je nezbytné pro jejich použití.*

3.4 Rozpočtování a účetnictví v IT službách

Cíl: Rozpočtovat a účtovat náklady poskytování služeb.

Musí existovat organizací definované politika a postupy pro:

- rozpočtování a účetnictví všech komponent včetně IT aktiv, sdílených zdrojů, režijních nákladů, služeb dodávaných třetí stranou, lidí, pojištění a licencí;
- rozdělení a alokace všech nepřímých nákladů na příslušné služby;
- efektivní finanční kontrolu a autorizaci.

Náklady musí být rozpočteny v dostatečném detailu, aby byla umožněna efektivní finanční kontrola a rozhodování.

Politika musí také stanovovat úroveň podrobnosti, s jakou je rozpočetnictví a účetnictví prováděno, a bere přitom v úvahu:

- typy nákladů, které mají být účtovány;
- rozdělení režijních nákladů, např. paušální úroková sazba, fixní úročení, nebo na základě velikosti variabilních prvků;
- členění pohledu na business zákazníka, na kterého je zpoplatnění uvaleno, např. obchodní jednotka jako jedna jednotka, nebo rozdělení podle útvarů, případně rozdělení podle sídla;
- pravidla pro management řešení rozdílů oproti rozpočtu, např. velikost rozdílu, při kterém bude řešení postoupeno vrcholovému vedení; spojitost s řízením úrovně služeb.

Úroveň investice do procesů rozpočtování a účetnictví a jejich finančních detailů musí být založena na potřebách jak zákazníků, tak dodavatelů jak je stanoveno v politice.

Poskytovatel služeb musí monitorovat a zaznamenávat náklady vůči rozpočtu, revidovat finanční předpověď a odpovídajícím způsobem regulovat náklady.

Změnám ve službách musí být přiřazeny náklady a musejí být potvrzeny v rámci procesu managementu změn.

3.5 Management kapacit

Cíl: Zajistit, aby organizace měla po celou dobu dostatečnou kapacitu ke splnění dohodnutých současných a budoucích požadavků podnikání.

Současné a očekávané podnikatelské požadavky na služby musí být chápány z hlediska toho, co bude firma potřebovat, aby je byla schopná dodávat svým zákazníkům.

Předpověď podnikání a odhady pracovního zatížení musí být převedeny do specifických požadavků a musí být dokumentovány. Výsledky proměnlivosti v pracovním zatížení nebo v prostředí musí být předvídané; data týkající se současného a předchozího využívání komponent a zdrojů na odpovídající úrovni musí být zachycena a analyzována za účelem podpory procesu.

Management kapacity musí být ohniskovým bodem ve všech záležitostech dosaženého stavu a kapacity. Proces musí poskytovat přímou podporu vývoji nových a změněných služeb zajišťováním tzv. „sizingu“ (určení potřebné kapacity zdrojů a komponent infrastruktury) a modelováním služeb.

Dokumentace kapacitního plánování současné úrovně infrastruktury a očekávaných požadavků musí být zhotovována s vhodnou frekvencí, když přitom bere v úvahu míru změny ve službách a objemech služeb, informace z reportů o managementu změn a podnikání zákazníka. Toto musí být zhotovováno nejméně jednou ročně. Musí dokumentovat nákladové možnosti splnění obchodních požadavků a doporučená řešení, s cílem zajistit dosažení dohodnutých cílů úrovně služeb, jak je stanoveno v SLA. Technická infrastruktura a její současné a projektované kapacity musí být jasně pochopeny.

Výsledkem managementu kapacit musí být vytvoření a udržování kapacitního plánu. Management kapacit musí odrážet podnikatelské potřeby a musí zahrnovat:

- současné a předvídané požadavky na kapacitu a dosažený stav;
- identifikovaný časový rozsah, limity a náklady na vylepšování služeb;
- hodnocení předpokládaných upgrade služeb, požadavků na změny, nových technologií a technik z hlediska jejich vlivu na kapacitu;
- předpokládaný vliv externích změn, např. legislativních;
- data a procesy, které umožní analýzy budoucího vývoje.

Musí být identifikovány metody, postupy a techniky pro monitorování kapacity služeb, vyladění dosaženého stavu služeb a poskytování odpovídající kapacity.

Příklad:
Plán obsahuje v závislosti na charakteru aktuálně poskytovaných nebo aktuálně plánovaných IT služeb zejména údaje v rozsahu:

- *stručné zhodnocení současné výkonnosti infrastruktury po kategoriích (personální obsazení, HW, OS, aplikace, pracovní zatížení, ...) v rozsahu:*
  - *plně zabezpečuje;*
  - *zabezpečuje;*
  - *zabezpečuje s nedostatky;*
  - *nezabezpečuje;*
- *stručný popis očekávaných změn služeb (důvod, míra změny, objem služby apod.) v nadcházejícím roce, příp. odkaz na SLA;*
- *stručná předpověď kapacitních nároků v nadcházejícím roce;*
- *popis navrhovaných změn v reorganizaci stávajících zdrojů včetně časového harmonogramu a finančních požadavků;*
- *popis očekávaných a navrhovaných požadavků na nové kapacitní zdroje včetně časového harmonogramu a finančních požadavků.*

3.6 Management bezpečnosti informací

Cíl: Bezpečnost informací v rámci všech činností efektivně řídit.

Vedení s náležitou pravomocí musí potvrdit bezpečnostní politiku ve vztahu k informacím, která musí být, pokud je to vhodné, komunikovaná všem příslušným zaměstnancům a zákazníkům. Na bezpečnost informačních služeb a informací se vztahuje rodina norma ISO 27000, jejímž cílem je zavedení jednotného systému řízení pro všechny oblasti a umožnění budování integrovaného systému řízení. Jedná se o normy:

- ISO 27000, která uvádí definice pojmů a terminologický slovník pro všechny ostatní normy z této série.
- ISO 27001, která je hlavní normou pro systém řízení bezpečnosti informací (ISMS), dříve to byla norma BS 7799 část 2, podle které byly ISMS certifikovány. Norma ISO 27001 byla publikována koncem října 2005.
- ISO 27002 (dříve normy ISO/IEC 17799 a BS7799-1), která je aktuální verzí normy, která byla vydána v červnu 2005 jako ISO/IEC 17799:2005 a označena ISO 27002:2005 v roce 2007.
- ISO 27003, která je návodem k implementaci ostatních norem a očekává se její publikace počátkem roku 2009.
- ISO 27004, která bude vydána pod názvem "Information Security Management Metrics and Measurement". (Metriky a měření).
- ISO 27005 (dříve BS 7799-3) , která bude vydána pod názvem "Information Security Management Systems - Guidelines for Information Security Risk Management" a měla by nahradit BS 7799 část 3. (Informační technologie - bezpečnostní techniky - mezinárodní uznávaná směrnice pro uznání osob pro řízení certifikace / registrace zabezpečení systémů řízení informací).
- ISO 27006, která bude vydána pod názvem “Information technology - Security techniques - International accreditation guidelines for the accreditation of bodies operating certification / Registration of information security management systems”.
- ISO 27007, která uvádí doporučení pro auditování ISMS.

Proto uvedeme v této kapitole jen stručně základní zásady bezpečnosti informací.

Náležitá bezpečnostní opatření musí být použita k:

- implementaci požadavků výše uvedené bezpečnostní politiky;

- řízení rizik spojených s přístupem ke službám nebo systémům.

Bezpečnostní opatření musí být dokumentovaná. Dokumentace musí popisovat rizika, ke kterým se opatření vztahuje, a způsob provozování a udržování tohoto opatření. Vliv změn na opatření musí být ohodnocen před tím, než jsou změny implementovány.

Uspořádání, které zahrnuje přístup třetích stran k informačním systémům a službám, musí být založeno na formální smlouvě, která stanovuje všechny nezbytné požadavky na bezpečnost.

Bezpečnostní incident musí být oznámen a zaznamenán v souladu s postupem pro management incidentů ihned, jak je možné. Musí existovat postupy, které zajistí, že všechny bezpečnostní incidenty jsou prošetřeny a že jsou přijata opatření v oblasti kontroly. Musí existovat mechanismy, které zajistí, že typy, objemy a vlivy bezpečnostních incidentů a selhání jsou kvantifikovány a monitorovány, a poskytují vstupy do plánů zlepšování služeb.

4 Procesy řízení vzájemných vztahů

V této kapitole popíšeme jednotlivé hlavní procesy, které se mohou vyskytovat v procesech řízení vzájemných vztahů, které se týkají komunikace se zákazníky a dodavateli. Jedná se o procesy: *Management obchodních vztahů* (Business relationship management) a *Management dodavatelů* (Supplier Management).

4.1 Management obchodních vztahů

Cíl: Vybudovat a udržovat dobré vztahy mezi poskytovatelem služeb a zákazníkem, založené na chápání potřeb zákazníků a hnacích sil jejich podnikání.

Poskytovatel informačních (IT) služeb musí identifikovat a dokumentovat zainteresované strany a zákazníky informačních (IT) služeb.

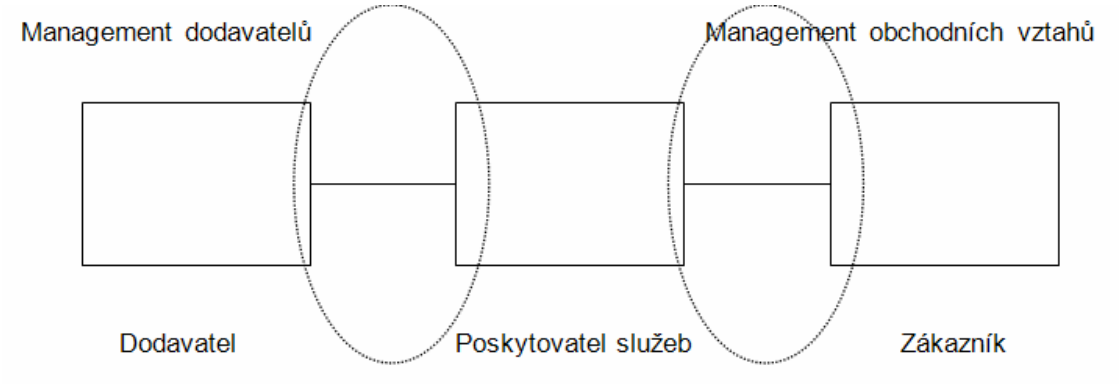
Poskytovatel informačních (IT) služeb a zákazník se musí věnovat přezkoumání služeb, aby prodiskutovali změny v rozsahu služeb, v SLA, ve smlouvách (pokud existují) nebo v obchodních potřebách nejméně jednou ročně a musí pořádat průběžná jednání v dohodnutých intervalech, aby diskutovali o dosaženém stavu, dosažených výsledcích, problémech a akčních plánech. Tato jednání musejí být dokumentována. Na jednání mohou být také pozvány ostatní zainteresované strany. Pokud je to potřebné musí následovat po těchto jednáních změny ve smlouvách, pokud existují, a v SLA. Tyto změny musí být předmětem managementu změn.

Poskytovatel informačních (IT) služeb si musí udržet povědomí o obchodních potřebách a významných změnách, aby byl schopen reagovat na tyto potřeby. Musí existovat postup na vypořádání stížností. Musí být se zákazníkem dohodnuto stanovení formálního postupu v případě stížnosti. Všechny formální stížnosti na služby musí poskytovatel služeb zaznamenat, prověřit, reagovat na ně, podat o nich zprávu a formálně je uzavřít. Pokud není stížnost vyřešena za pomoci běžných postupů, musí být zákazníkovi k dispozici možnost eskalace.

Poskytovatel informačních (IT) služeb musí jmenovat osobu nebo osoby, které jsou odpovědné za kontrolu spokojenosti zákazníků a za celý proces obchodních vztahů. Musí existovat proces získávání zpětné vazby z pravidelného měření spokojenosti zákazníků a reakce na ni.

Činnosti pro zlepšování služeb, identifikované během tohoto procesu, musí být zaznamenány a vloženy do plánu zlepšování služeb.

Poskytovatel informačních (IT) služeb musí mít dokumentované procesy managementu dodavatelů a musí jmenovat manažera pro smlouvy s dodavateli, který je zodpovědný za každého dodavatele.



Obrázek 3: Zjednodušené znázornění vztahů.

Jak je na obrázku 3 znázorněno, poskytovatel informačních (IT) služeb plní v rámci dodavatelského řetězce roli, kde v každém kroku v řetězci musí přidávat výhodu, když poskytovatel služeb přijímá služby nebo zboží od dodavatele a když dodává rozšířené služby zákazníkovi. Pro vysvětlení, v rámci této kapitoly je pojem poskytovatel služby vždy užíván k popisu organizace, pro kterou je určen tento dokument, bez ohledu na roli nebo řízení, které přebírá v popisovaném procesu. V praxi bude vztah zřídkakdy takto jednoduchý. Bude zahrnovat mnoho účastníků, přebírajících role jak dodavatelů, tak zákazníků s obchodními vazbami přímo mezi mnohými z nich stejně jako vazbami zprostředkovanými poskytovatelem.

Řízení vzájemných vztahů mezi procesy musí zajistit, aby všechny strany:

- chápaly a plnily podnikatelské potřeby;
- chápaly schopnosti a omezení;
- chápaly odpovědnosti a povinnosti.

Musí také zajistit, aby úrovně uspokojení zákazníka byly přiměřené a aby budoucí obchodní potřeby byly komunikovány a pochopeny.

4.1.1 Přezkoumání služeb

Poskytovatel informačních (IT) služeb a zákazník (zákazníci) musí provádět přezkoumání služeb nejméně jednou ročně, a to před a po významných změnách. Přezkoumání musí brát v úvahu dosaženou úroveň v minulosti, diskutovat současné a plánované obchodní potřeby a navrhovat jakékoliv změny v rozsahu služeb a ve smlouvách SLA Ostatní zainteresované strany, např. subdodavatelé, zákazníci, uživatelské skupiny a ostatní zástupci zainteresovaných stran mohou být pozváni k účasti na schůzkách, kde přezkoumáni probíhá.

Poskytovatel informačních (IT) služeb a zákazník (zákazníci) se musí také dohodnout na postupech průběžného přezkoumání zahrnujících diskusi o vývoji, dosažených cílech a problémech. Tato jednání musí být plánována a oznámena zainteresovaným stranám.

Poskytovatel informačních (IT) služeb musí plánovat a zaznamenávat všechna formální jednání, uveřejňovat záznamy a plnit v odsouhlasené činnosti.

Poskytovatel služeb musí vybudovat vztah se svými zákazníky tak, aby se dalo očekávat, že si je vědom podnikatelských potřeb a významných změn a že je schopen reagovat na takovou potřebu.

4.1.2 Stížnosti na služby

Poskytovatel informačních (IT) služeb a zákazník (zákazníci) musí odsouhlasit formální postup pro případ stížností, aby neexistovala pochybnost o podstatě stížnosti a způsobu, jak má být vyřízena. Poskytovatel služeb musí stanovit proces pro přijetí vhodného opatření k řešení této záležitosti.

Poskytovatel služeb musí pravidelně analyzovat záznamy o stížnostech, aby identifikoval trendy a podal zprávu o této analýze zákazníkům. Výsledky takové analýzy musí být použité tam, kde je to vhodné a musí být využity pro plán na zlepšení služeb.

4.1.3 Měření spokojenosti zákazníků

Spokojenost zákazníků musí být měřena, aby umožnila poskytovateli služeb porovnat dosaženou úroveň s cíli spokojenosti zákazníků a s předchozími průzkumy. Rozsah a složitost průzkumu musí být navrženy tak, aby zákazník mohl jednoduše a bez nadměrného časového zatížení správně odpovědět na tento průzkum.

Příklad:
Agenda vedená v souvislosti s těmito činnostmi je součástí dokumentace standardního řízení organizace (jako jsou v QMS dokumenty „Plány práce“, „Porada vedení“ apod.).

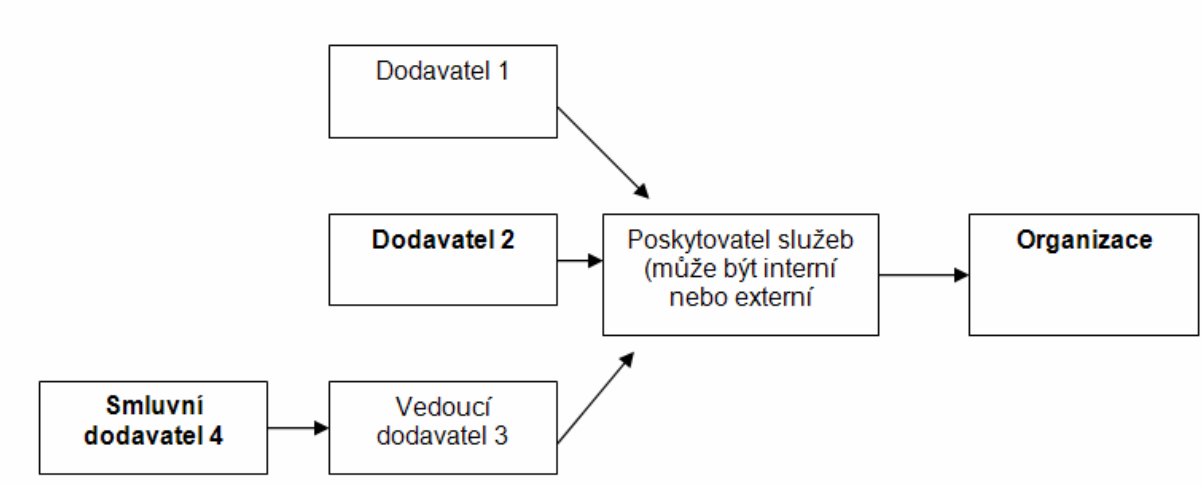
Při jednání se zákazníky a dalšími zainteresovanými stranami, které jsou konány se zaměřením na obsah a kvalitu poskytovaných služeb, je povinností zaměstnanců společnosti, vedoucích tato jednání, projednávat zejména následující tématiku:

- *dosažené výsledky;*
- *předcházející výkonnost;*
- *vzniklé problematické záležitosti;*
- *současné a plánované potřeby byznysu;*
- *plány činnosti;*
- *návrhy změn v rozsahu služeb;*
- *návrhy změn v SLA;*
- *dotazníkové šetření spokojenosti zákazníků.*

Zaměstnanci společnosti, vedoucí jednání se zákazníky jsou povinní vést o výsledcích jednání přiměřené záznamy.

4.2 Management dodavatelů

Cíl: Řídit dodavatele třetích stran tak, aby bylo zajištěno poskytování nepřerušovaných kvalitních služeb.



Obrázek 4: Dodavatelé a odběratelé.

Poskytovatel informačních (IT) služeb musí mít dokumentované procesy managementu dodavatelů a musí jmenovat manažera pro smlouvy s dodavateli, který je zodpovědný za každého dodavatele.

Požadavky, rozsah, úroveň služeb a procesy komunikace poskytované dodavateli musí být dokumentované v SLA nebo jiných dokumentech a odsouhlaseny všemi stranami.

SLA s dodavateli musí být v souladu se SLA uzavřenými s organizací. Rozhraní mezi procesy užívanými každou stranou musí být dokumentované a odsouhlasené.

Všechny role a vztahy mezi vedoucím a smluvními dodavateli musí být jasně dokumentované. Vedoucí dodavatelé musí být schopni prokázat procesy, které zajišťují, že smluvní dodavatelé plní smluvní požadavky.

Musí existovat proces základního přezkoumání smlouvy nebo formální dohody nejméně jedenkrát ročně, aby bylo zajištěno, že podnikatelské potřeby a smluvní závazky jsou stále naplňovány.

Změny ve smlouvách s dodavateli, pokud existují, a v SLA musí vycházet buď z těchto přezkoumání nebo požadavků na jiné termíny tak, jak je to zapotřebí. Jakékoliv změny musí být předmětem procesu managementu změny.

Musí existovat formální proces pro řešení smluvních sporů. Musí existovat proces pro vypořádání očekávaného ukončení služeb, předčasného ukončení služeb nebo převod služeb na jiný subjekt.

Musí být monitorována a přezkoumána výkonnost vzhledem k požadované úrovni služeb. Podněty pro činnosti ke zlepšování, identifikované během tohoto procesu, musí být zaznamenány a zahrnuty do plánu zlepšování služeb.

Příklad:

Managera kontraktu stanovuje vrcholové vedení organizace (např. zástupce ředitele pro ICT) svým rozhodnutím. Manager kontraktu je v rámci organizace současně kontaktní osobou pro dodavatele.

Každý smluvní vztah organizací a dodavatelem je řešen samostatně v rámci kontraktačního řízení, které je součástí jednotlivých procesů (projektů) se stanovenými rolemi a specifickými činnostmi, jež jsou však pro každý projekt jedinečné.

Popisy procesů jsou součástí projektové dokumentace.

Dokumentovaný postup uplatňovaný u organizace při řešení smluvních sporů a ukončení poskytované služby je obsahem kapitoly Management smluvních sporů tohoto dokumentu.

Každá „aktivní“ smlouva s dodavatelem je zařazena do procesu pravidelného přezkoumávání ITSM, které provádí zástupce ředitele pro ICT.

V rámci přezkoumání je položen důraz na zjištění podnětů, jejichž případná existence je uplatněna při tvorbě dokumentu „Plán pro zlepšování služeb“.

5 Procesy řešení

V této kapitole popíšeme jednotlivé hlavní procesy, které se mohou vyskytovat v procesech řešení informačních služeb. Jedná se o procesy: *Management incidentů* (Incident management) a *Management řešení problémů* (Problem management).

Stanovení priorit

Cíle v procesech řešení musí být založeny na prioritách organizace. Priority musí být založeny na jejich dopadu a naléhavosti. Dopady musí být založeny na rozsahu aktuálního a potenciálního poškození podnikání zákazníka. Naléhavost musí být založena na časovém období mezi zjištěním problému nebo incidentu a okamžikem, kdy je podnikání zákazníka tímto ovlivněno.

Plánování v procesech řešení incidentu nebo problému musí brát v úvahu přinejmenším následující položky:

- prioritu;
- dostupné schopnosti;
- protichůdné požadavky na zdroje;
- úsilí/náklady na použitou metodu řešení;
- celkovou dobu na poskytnutí metody řešení.

Náhradní pracovní postupy

Tam, kde je to vhodné, musí proces řízení problémů zajistit stanovení a udržování náhradních pracovních postupů, které umožní řešení incidentů tak, aby služba mohla být obnovena uživateli z řad zaměstnanců.

Známá chyba může být uzavřena pouze tehdy, když byla úspěšně použita opravná změna, nebo chyba již dále není platná, např. protože služba již dále není používána.

Proces řešení problémů musí mít zajištěn přístup k informacím o podnikatelských oblastech postižených problémem.

Informace o náhradních pracovních postupech uložené ve znalostní databázi, o jejich aplikaci a efektivitě musí být uloženy a udržovány.

5.1 Management incidentů

Cíl: Co nejdříve obnovit dohodnuté služby pro organizaci nebo reagovat na požadavky na služby.

Všechny incidenty musí být zaznamenány. Musí být stanoveny postupy pro sledování a řízení dopadu incidentů. Postupy musí stanovovat způsob zaznamenávání, určování priorit, vliv na podnikání, klasifikaci, aktualizaci, eskalaci, vyřešení a formální ukončení všech incidentů.

Zákazník musí být informován o postupu řešení incidentů, které nahlásil, nebo o požadavku na služby. Předem musí být upozorněn, pokud úroveň služeb nemůže být dodržena, a musí postup odsouhlasit.

Všichni pracovníci podílející se na managementu incidentů musí mít přístup k odpovídajícím informacím, jako jsou známé chyby, řešení problémů a k databázi konfiguračního managementu (CMDB – Configuration Management of Data Base).

Významné incidenty musí být klasifikované a řízené podle stanovovaného procesu.

Řízení procesu incidentů musí:

- být jak procesem proaktivním, tak reaktivním, odpovídajícím na incidenty, které ovlivňují nebo potenciálně mohou ovlivnit služby;
- se zabývat obnovením zákaznických služeb, ne určováním příčin incidentů.

Proces řízení incidentů musí zahrnovat následující činnosti:

- přijímání telefonátů, zaznamenávání, stanovení priorit, klasifikaci;
- první linii rozhodnutí nebo doporučení;
- zvážení otázek bezpečnosti;
- sledování incidentu a řízení jeho životního cyklu;
- ověření a uzavření incidentu;
- první linie kontaktu se zákazníkem;
- eskalace řešení.

Incidenty mohou být ohlášeny telefonicky, hlasovou schránkou, osobně, písemně, faxem nebo e-mailem nebo mohou být zaznamenány přímo uživatelem s přístupem do systému pro záznam incidentů nebo automaticky monitorovacím software. Všechny incidenty musí být zaznamenány způsobem, který dovoluje, aby důležité informace byly nalezeny a analyzovány.

Pokrok (nebo jeho absence) v řešení incidentů musí být oznamován těm osobám, které jsou aktuálně nebo mohou být potenciálně ovlivněni. Všechny činnosti musí být zaznamenány do záznamu o incidentu. Pracovníci týmu „Incident management“ musí mít přístup do aktualizované znalostní databáze, kde jsou uchovávány informace o technických specialistech, předchozích incidentech, souvisejících problémech a známých chybách, náhradních pracovních postupech a kontrolních seznamech, které pomohou při obnovení služeb pro business.

Kdekoliv je to možné, musí být zákazníkovi poskytnuty prostředky k pokračování podnikatelské činnosti, dokonce i se zhoršenou kvalitou služby, např. vyřazením vadného prvku z činnosti. Motivem je minimalizace vlivu na podnikatelské aktivity zákazníka. Když příčina zůstává neurčena, ale je stanoven náhradní pracovní postup, detaily musí být zaznamenány pro použití při probíhajícím určování problému a pro případ, že se bude opakovat podobný incident.

Konečné uzavření incidentu může nastat pouze tehdy, když iniciující uživatel dostal příležitost potvrdit, že incident je vyřešen a služba je obnovena.

Příklad:

V rámci organizace jsou mezi standardní incidenty zařazeny zejména následující události, požadavky a hlášení:

- *ztráta počítačového média nebo jiné písemnosti s manuálem, pracovním postupem apod., bez něhož klient nemůže využívat službu v plném rozsahu;*
- *nedosažitelnost uživatelských dat nebo jejich ztráta;*
- *projev počítačového viru nebo jiného zlomyslného programu, který způsobuje problémy ve využívání služby;*
- *nefunkčnost Internetu na klientské stanici;*
- *nefunkčnost elektronické pošty na klientské stanici;*
- *opakované potíže při síťovém připojení;*

Závažný incident je událost nebo hlášení systému, které signalizují, že poskytovaná služba není zcela evidentně vůbec poskytována nebo vykazuje nedostatky, jež jsou v zásadním rozporu s garantovanými parametry této služby (výpadky se opakují nebo jejich trvání značně přesahuje tolerovanou a garantovanou dobu výpadku poskytované služby, popř. poskytovaná služba neobsahuje všechny kvalitativní a kvantitativní prvky). Jedná se zejména o:

- *nemožnost přihlásit se ke službě obvyklým způsobem;*
- *nemožnost editace dat, jež jsou předmětem poskytované služby;*
- *nečitelnost dat, jež jsou předmětem poskytované služby;*

- *opakované výpadky v připojení se k poskytované službě;.*
- *poškození databáze;*
- *zhroucení centrálních serverů*

Všechny požadavky jsou přijímány od různých subjektů a několika nezávislými komunikačními cestami (telefonicky, e-mailem, jiným způsobem). Evidence požadavků je pak vedena centrálně.

Každý přijatý požadavek je evidován v centrálním databázovém systému - aplikaci „CleverDesk“, který je dostupný na dané webové adrese.

SW aplikace „CleverDesk“ je helpdeskový systém pro podporu řešení většiny problémových situací mezi koncovými uživateli služeb a řešiteli, který zajišťuje přesnou evidence celého průběhu problému v definovaném formuláři. Systém navíc umožňuje řešiteli přístup do vlastní znalostní databáze v minulosti už obdobně řešených problémů.

Přístup do systému je řízen prostřednictvím přidělení uživatelských a administrátorských práv managerem HelpDesku, který je zároveň zodpovědný za definování sledovaných parametrů v „CleverDesku“ a celý chod úseku HelpDesku.

Každý požadavek je evidován pod svým jedinečným číslem, které je tvořeno kontinuální posloupností zvyšující se vždy o jedničku s každým novým požadavkem. U každého požadavku je také evidován:

- *přesný čas jeho zadání;*
- *jméno zadávajícího uživatele;*
- *řešitelský tým (řešitel);*
- *stav požadavku.*

5.2 Management řešení problémů

Cíl: Minimalizovat přerušení podnikání proaktivní identifikací a analýzou příčin incidentů a řízením problémů k jejich ukončení.

Management řešení problémů je vhodně rozdělit na dva poměrně nezávislé subprocesy. Jedním z nich je *řízení problému* (Problem Control) a druhým pak *řízení chyb* (Error Control). Cílem procesu řízení problému je nalezení zdroje problému ve formě tzv. „Známé chyby" a případná identifikace náhradního pracovního postupu, který je uplatněn při výskytu incidentu způsobeného touto chybou. Tyto informace se pak zapisují do znalostní databáze, kterou pro svou práci využívá především Service desk. Ve fázi řízení chyb se řeší vlastní odstranění známé chyby obvykle formou řízené změny infrastruktury nebo procesů. Subproces řízení chyby ale může být ukončena i bez odstranění této chyby (chyba tedy není uzavřena). To se může stát v případě, že je např. odstranění chyby tak náročné na zdroje a finance, že se vyplatí zůstat u náhradního pracovního postupu. Po odstranění známé chyby by mělo rovněž proběhnout uzavření všech incidentů, které s chybou souvisely.

5.2.1 Rozsah řízení problémů

Proces managementu problémů musí zjistit základní příčiny incidentů.

Management problémů musí proaktivně předcházet opakování incidentů nebo známých chyb podle podnikatelských požadavků.

5.2.2 Zahájení řízení problému

Incidenty musejí být klasifikovány, aby pomohly určit příčinu problémů. Klasifikace může odkazovat na existující problémy a změny.

5.2.3 Známé chyby

Když v rámci managementu problémů byla vyšetřováním zjištěna základní příčina incidentu a metoda řešení incidentu, pak problém musí být klasifikován jako známá chyba.

Všechny známé chyby musejí být zaznamenány ve vztahu k současným a potenciálně ovlivněným službám a navíc k položkám konfigurace, které jsou podezřelé ze závadnosti.

Informace o známých chybách ve službách, které byly uvedeny do produktivního prostředí, musí projít managementem služeb a musí být zaznamenány do znalostní báze spolu s jakýmikoliv náhradními pracovními postupy.

Známá chyba by neměla být uzavřena do doby úspěšného vyřešení.

5.2.4 Řešení problému

Když byla identifikována základní příčina a bylo přijato rozhodnutí o řešení, toto řešení musí být řízeno v rámci procesu managementu změny.

Informace o náhradních pracovních postupech, trvalých opravách nebo vývoj problémů musí být komunikovány těm, kteří byli postiženi nebo požadovali podporu postiženými službami.

Postup řešení problémů musí být sledován. Všechny okolnosti problému musí být dále předávány příslušným stranám.

5.2.5 Uzavření záznamu o incidentu a problému

Postup uzavření záznamu musí zahrnovat kontrolu, která zajistí, že:

- detaily řešení byly přesně zaznamenány;
- příčina je kategorizována pro usnadnění analýzy;
- pokud je to vhodné, pak zákazník a pracovníci podpory jsou informováni o řešení;
- zákazník souhlasí, že bylo dosaženo řešení;
- pokud řešení není možné dosáhnout nebo není možné, pak je zákazník informován.

5.2.6 Přezkoumání problému

Přezkoumávání problému musí být provedeno, pokud je k tomu důvod z hlediska zkoumání problémů nevyřešených, neobvyklých nebo problémů s velkým dopadem. Účelem je hledat zlepšení procesu a předcházet opakování incidentů nebo chyb.

Typickým přezkoumáním problému je:

- přezkoumání jednotlivých úrovní incidentu a stavu problému vzhledem k úrovním služeb;
- přezkoumání vedením, která zdůrazní ty problémy, které vyžadují okamžitou reakci;
- přezkoumání vedením, která určí a analyzují trendy a poskytují vstup pro další procesy, jako vzdělávání zákazníků.

5.2.7 Prevence problému

Proaktivní management problémů musí vést k redukci incidentů a problémů. Musí zahrnovat odkazy na informace, které pomáhají při analýze, jako jsou:

- aktiva a konfigurace;
- management změny;
- publikované známé chyby, informace o náhradních pracovních postupech poskytnutých dodavateli;
- historické informace o podobných problémech.

Prevence problémů musí zahrnovat vše od prevence jednotlivých incidentů, jako jsou opakované potíže s určitou částí systému, až po strategická rozhodnutí. To posledně jmenované může vyžadovat

významné výdaje na implementaci jako je investice do lepší sítě. Na této úrovni proaktivní management problémů do procesu Availability managementu. ???-není sloveso

Prevence problémů také zahrnuje informace poskytované zákazníkům, které znamenají, že nemusejí žádat o pomoc v budoucnu, např. předcházení incidentům způsobených nedostatkem znalostí nebo školení uživatelů.

Příklad:

Problém se obvykle řeší ve třech fázích: fázi stanovení řešitele a identifikace problému; fázi řešení problému a fázi uzavření problému

*V rámci **fáze stanovení řešitele** a identifikace problému (vypořádaného incidentu) se provádí zejména:*

- *stanovení managera problému (vedoucího řešitelského týmu);*
- *specifikace incidentu včetně jeho kategorie a způsobu jeho nápravy.*

*V rámci **fáze řešení** problému se provádí zejména:*

- *stanovení příčiny (příčin) vzniku incidentu;*
- *stanovení návrhu opatření k předcházení vzniku nebo uplatnění příčiny (proaktivní aspekt);*
- *stanovení návrhu opatření ke zvýšení efektivity obnovy služby (reaktivní aspekt);*
- *případný způsob aktualizací;*
- *schválení návrhu.*

*V rámci **fáze uzavření** problému:*

- *realizace opatření;*
- *stanovení výstupu do dokumentu „Plán pro zlepšování služeb“ a následně pak do databáze známých chyb a vyřešených problémů a do procesů řízení změn, řízení konfigurací, řízení úrovně služeb apod.;*
- *vyrozumění zainteresovaných osob (i v případě, že řešení není dosažitelné nebo neexistuje);*
- *případný záznam o souhlasu zákazníka, že bylo dosaženo řešení;*
- *založení dokumentu „Záznam o problému“.*

6 Řídicí procesy

V této kapitole popíšeme jednotlivé hlavní procesy, které se mohou vyskytovat v řídících procesech poskytování informačních služeb. Jedná se o procesy: *Management konfigurace* (Configuration management) a *Management změn* (Change management).

6.1 Management konfigurace

Cíl: Stanovovat a řídit jednotlivé komponenty služeb a infrastruktury a udržovat přesné informace o konfiguraci.

6.1.1 Plánování a implementace managementu konfigurace

Management konfigurace musí být plánován a implementován spolu s managementem změny a managementem uvolňování, aby bylo zajištěno, že organizace může efektivně sledovat a udržovat své IT aktiva a jejich konfiguraci. Musí být k dispozici přesné informace o konfiguraci, pro podporu plánování, řízení změn jako je vytváření a distribuce nových a aktualizovaných release služeb a systémů. Výsledkem musí být účinný systém, který integruje procesy konfigurace informací samotné organizace, svých zákazníků a pokud je to vhodné, tak i dodavatelů.

Za všechna významná aktiva a konfiguraci musí být stanovena odpovědnost a musí mít odpovědného vedoucího, který zajišťuje, že je udržována vhodná ochrana a systém řízení, např. změny jsou autorizované před implementací. Dílčí odpovědnosti při implementaci systému řízení mohou být delegovány, ale celková zodpovědnost musí zůstat u odpovědného vedoucího. Odpovědný vedoucí musí mít k dispozici nezbytné informace k uplatnění této odpovědnosti, např. osoba schvalující změny může požadovat informace o nákladech, rizicích, dopadu změny a zdrojích potřebných pro implementaci.

Infrastruktura a/nebo služby musí mít aktualizované plány managementu konfigurace, které mohou být samostatné nebo tvoří část jiných plánovacích dokumentů. Tyto plány musí zahrnovat nebo popisovat:

- rozsah, cíle, politiky, stanovení rolí a odpovědností;
- procesy managementu konfigurace pro stanovení konfiguračních položek ve službách a infrastruktuře, řízení změn v konfiguracích, záznamy a reporty stavu konfiguračních položek a ověřování úplnosti a správnosti konfiguračních položek;
- požadavky na zodpovědnost, sledovatelnost, kontrolovatelnost, např. z důvodů bezpečnostních, právních, regulatorních nebo obchodních;
- management konfigurace (řízení přístupu, ochrany, verzí, vývojových verzí tzv. „builds", release);
- proces řízení rozhraní, který zajišťuje identifikaci, záznam a řízení konfiguračních položek a informací a určuje hranice dvou nebo více organizací, např. systémová rozhraní, release;
- plánování a alokování zdrojů pro řízení aktiv a konfigurací a udržování systému managementu konfigurace, např. školení;
- procesy řízení dodavatelů a subdodavatelů, kteří se podílí na managementu konfigurace.

6.1.2 Identifikace konfigurace

Všechny konfigurační položky musí být jednoznačně identifikované a stanovené pomocí atributů, které popisují jejich funkční a fyzické charakteristiky. Informace musí být relevantní a kontrolovatelné. Příslušné značení nebo jiné metody identifikace musí být zaznamenány v databázi managementu konfigurací (CMDB). Položky, které mají být řízeny, musí být identifikované za použití stanovených výběrových kritérií a musí zahrnovat:

- všechna vydání a release informačních systémů a software (včetně software třetích stran) a vydané dokumentace k systému, např. požadavky specifikací, návrhy, zprávy z testů, dokumentace release;
- konfigurační „baseline" nebo popis vývojové verze SW pro jednotlivá prostředí, normalizovanou konfiguraci a release hardware;
- původní verze a elektronické knihovny, např. Definitive Software Library (DSL)[4];
- použité balíky nebo nástroje managementu konfigurace;
- licence;
- bezpečnostní komponenty, např. firewalls;
- fyzická aktiva, která musí být sledována z důvodu řízení finančních aktiv nebo z obchodních důvodů, např. zabezpečení magnetických médií, zařízení;
- dokumentace týkajících se služeb, např. SLA, postupy;
- podpůrná zařízení nebo příslušenství např. elektřina pro místnost s počítači;
- vztahy a závislosti mezi konfiguračními položkami.

Musí být identifikovány příslušné vztahy a závislosti mezi konfiguračními položkami, aby mohla být zajištěna nezbytná úroveň řízení. Tam, kde je požadovaná sledovatelnost, musí proces zajistit, aby mohly být konfigurační položky sledovány v rámci celého životního cyklu, od požadavků na dokumentaci až po vydání záznamů, např. využití matice sledovatelnosti.

Další položky, které mohou být považované za konfigurační položky, jsou:
- další dokumentace;
- další aktiva;
- další zařízení, např. místnosti;
- podnikatelské jednotky;
- lidé.

6.1.3 Řízení konfigurace

Proces musí zajistit, že pouze schválené a identifikovatelné konfigurační položky jsou akceptované a zaznamenané. Žádné konfigurační položky nesmí být přidány, modifikovány, nahrazeny nebo přemístěny/odstraněny bez náležité kontrolní dokumentace, např. schválený požadavek na změnu, aktualizace informace o release. K ochraně integrity systémů, služeb a infrastruktury, musí být konfigurační položky udržovány ve vhodném a bezpečném prostředí, které:
- je chrání proti neautorizovanému přístupu, změnám nebo porušení např. virům;
- poskytuje prostředky pro obnovení provozu;
- povoluje řízené přístupy k původním verzím, např. software.

6.1.4 Popis stavu konfigurace a reporting

Aktuální a přesné konfigurační záznamy musí být udržovány, aby zohledňovaly změny stavu, změny umístění a změny verzí konfiguračních položek. Práce se stavy musí zajistit poskytnutí informací o současných a historických datech týkajících se každé konfigurační položky v průběhu jejího životního cyklu. Toto musí umožnit, aby změny konfiguračních položek byly sledovány v různých stavech, např. objednání, dodávka, akceptační testy, živý provoz, změny, odstranění, likvidace.

Informace o konfiguracích musí být udržovány a dány k dispozici pro plánování, rozhodování a řízení změn u stanovených konfigurací. Pokud je to požadováno, informace o konfiguraci musí být přístupné uživatelům, zákazníkům, dodavatelům a partnerům s cílem pomoci jim v jejich plánování a

[4] Pojem Definitive Software Library (DSL) se používá k označení knihovny všech tzv."Master" kopií programů, aplikací a dalšího SW, které jsou v organizaci využívány. Pod pojmem „Master" rozumíme originální jedinečnou verzi, ze které mohou být pořízeny kopie např. pro instalaci SW na koncovou stanici uživatele. Současně je tam uložena i aktuální verze dokumentace k tomuto SW vybavení včetně poznámek k release, licencím apod. Při vyřazení SW z používání by měly být všechny položky týkající se tohoto SW rovněž vyřazeny (může to být např. do archivních databází, které ale nemusí podléhat tak přísným pravidlům řízení jako DSL).

rozhodování. Například, externí poskytovatel služeb, aby zajistil poskytování služby v celém jejím rozsahu, může zákazníkům a jiným stranám umožnit přístup k informacím o konfiguraci.

Reporty o řízení konfigurace musí být k dispozici všem relevantním stranám. Reporty musí zahrnovat identifikaci a stav konfiguračních položek, jejich verze a související dokumentaci. Reporty musejí zahrnovat:

- poslední verze konfiguračních položek;
- umístění konfiguračních položek a u software také umístění "Master" verzí;
- vzájemné závislosti;
- historii verzí.

Kdykoliv musí být možné shromáždit stavy konfiguračních položek, které dohromady tvoří:

- konfiguraci služby nebo systému;
- změnu, baseline (pozn. Překladatele: v tomto případě výchozí stav), vývojové verze nebo release;
- verzi nebo variantu.

6.1.5 Ověření a audit konfigurace

Procesy ověřování a auditu konfigurace, fyzické i funkční, musí být naplánovány a kontrolovány takovým způsobem, aby bylo zajištěno, že odpovídající procesy a zdroje jsou použity k:

- ochraně fyzické konfigurace a intelektuálního kapitálu organizace;
- zajištění, že organizace má kontrolu nad svými konfiguracemi, master kopiemi a licencemi;
- poskytnutí jistoty, že informace o konfiguraci jsou přesné, kontrolované a jsou k dispozici;
- zajištění, že změna, release, systému nebo prostředí odpovídají smluvním nebo specifikovaným požadavkům, a že záznamy konfigurace jsou přesné.

Audity konfigurace musí být prováděny pravidelně, před a po významných změnách, po katastrofách a v náhodných intervalech.

Nedostatky nebo neshody musí být zaznamenány, ohodnoceny a musí být vyvolána opatření k nápravě, tato i realizována a podána zpětná vazba relevantním stranám a programům pro zlepšování služeb.

Příklad:

Identifikace konfigurace se provádí před každým nasazením nové služby nebo jejího podpůrného prostředku a před každou implementací nového uvolnění do produkčního prostředí (viz příslušná kapitola dokumentu „Řízení uvolnění“).

Součástí identifikace je popis jednotlivých položek (podstatných prvků) systémů, jejich evidence do konfigurační databáze a identifikace vztahů mezi nimi.

Kritéria pro výběr konfigurační položky:

- *důležitost položky pro poskytování služby / chod systému;*
- *cenová a časová nákladnost na opravu či změnu položky;*
- *aj.*

Vypracování záznamu prvotní identifikace výchozího stavu a stanovení klíčových konfiguračních položek provádí „řešitel“ stanovený vedením organizace (např. zástupcem ředitele pro ICT).

6.2 Management změn

Cíl: Zajistit, aby všechny změny byly ohodnoceny, schváleny implementovány a přezkoumány řízeným způsobem.

6.2.1 Plánování a implementace

Procesy a postupy managementu změn musí zajistit, že:

- změny a dokumentovaný rozsah mají jasně stanoveny;
- schváleny jsou pouze změny, které přinášejí podnikatelský přínos, např. obchodní, právní, regulatorní, statutární;
- změny jsou naplánovány na základě priorit a rizik;
- změny v konfiguraci mohou být ověřeny během implementace;
- čas pro implementaci změn je monitorován a podle požadavků i zlepšován.

Proces managementu změn musí být schopný prokázat, jak je změna:

- vyvolána, zaznamenána a klasifikována (s odkazem na dokumenty, které změnu vyvolaly);
- ohodnocena z hlediska dopadu, naléhavosti, nákladů, přínosů a rizika dopadu změny na služby, zákazníka a plány release;
- zrušena nebo upravena, pokud je neúspěšná;
- dokumentována, např. požadavek na změnu se přímo dotýká konfigurační položky a aktualizace verze plánu implementace a release;
- schválená nebo zamítnutá osobou odpovědnou za změnu, v závislosti na typu, velikosti a riziku změny;
- implementována určeným vlastníkem s využitím pracovních skupin, které jsou odpovědné za změnu každé komponenty;
- testována, ověřována a ukončena;
- uzavřena a přezkoumána;
- plánována, monitorována a reportována;
- spojena s incidentem, problémem a pokud je potřeba, tak s jinými záznamy o změnách a konfiguračních položkách.

Stav změn a plánovaná data implementace musí být použity jako základ pro plánování změn a release.

Informace o plánování změny musí být k dispozici osobám, kterých se změna týká. Pokud při implementaci změny může dojít k výpadku v průběhu běžné pracovní doby, pak osoby, kterých se to týká, musí s touto implementaci předem souhlasit.

6.2.2 Uzavření a přezkoumání požadavku na změnu

Všechny změny musí být přezkoumány z hlediska úspěšnosti nebo neúspěšnosti implementace a všechna zlepšení musí být zaznamenána.

Přezkoumání po implementaci musí proběhnout minimálně u významných změn, aby se ověřilo, že:

- změna splnila cíle;
- zákazníci jsou spokojeni s výsledky;
- nenastaly neočekávané vedlejší dopady.

Všechny neshody musí být zaznamenány a odstraněny.

Slabé stránky nebo nedostatky, zjištěné při přezkoumání procesu managementu změny, by měly být předány do plánu na zlepšování služeb.

6.2.3 Naléhavé změny

Někdy je požadováno provedení naléhavé změny, proces změny musí být sledován, avšak některé detaily mohou být dokumentovány zpětně. Když proces v případě naléhavé změny obchází jiné požadavky managementu změny, musí tyto požadavky splnit zpětně a to ihned jak jen to bude možné.

Naléhavé změny musí být odůvodněné implementující osobou a přezkoumány po implementaci, aby se ověřilo, že se jednalo skutečně o naléhavou změnu.

6.2.4 Reportování, analýza a provádění změny

Záznamy o změnách musí být pravidelně analyzovány, aby byly zjištěny zvyšující se úrovně prováděných změn, pravidelně se opakující typy, nově vznikající trendy a další důležité informace. Výsledky a závěry získané z analýzy změn musí být zaznamenány a musí se podle nich jednat.

Příklad z praxe:

Požadavek na změnu může být:

- *ze strany zákazníka;*
- *ze strany zaměstnanců a managementu;*
- *ze strany třetích osob (správní úřady, odborná ale i laická veřejnost);*
- *z objektivní příčiny (např. novela právního předpisu, existence nových technologií, materiálů);*

Registrace požadavku v organizaci:

- *provádí „správce požadavků“, což může být:*
  - *Helpdesk;*
  - *sekretářka;*
  - *vlastník procesu nebo činnosti;*
  - *určený zaměstnanec.*

Potvrzení přijetí požadavku:

- *provádí „správce požadavků“.*

Posouzení požadavku:

- *provádí „řešitel“, což může být:*
  - *určený zaměstnanec nebo skupina;*
  - *vlastník procesu nebo činnosti;*
- *jehož obsahem je:*
  - *posouzení podkladů, sil a prostředků, nástrojů, rozpočtu, termínu, kvality, efektivnosti apod.;*
  - *analýzu dopadu jak z hlediska technického, tak z hlediska zdrojů a času;*
  - *případný návrh požadavku za zpracování „havarijního plánu“ - popis způsobu, kterým vše bude uvedeno do původního stavu nebo napraveno v případě, že nastane případ selhání postupu implementace;*
  - *požadavky na doplnění.*

Schválení požadavku:

- *provádí:*
  - *příslušný vedoucí zaměstnanec (většinou zástupce ředitele pro ICT);*
  - *ředitel;*
- *jehož obsahem je:*
  - *vyčlenění zdrojů;*
  - *stanovení způsobů implementace;*
  - *rozdělení kompetencí.*

7 Procesy uvolňování

V této kapitole popíšeme hlavní proces, který se vyskytuje v procesech uvolňování informačních (IT) služeb. Jedná se o proces: *Management uvolňování* (Release management).

Management uvolňování musí koordinovat činnosti poskytovatele služeb, dodavatelů a podnikání při plánování a dodání release do produktivního prostředí.

Dobré plánování, řízení jsou nezbytné pro tvorbu balíčků a úspěšnou distribuci release a pro řízení souvisejících dopadů a rizik na podnikání a IT. Uvolňování týkající se informačních systémů, infrastruktury, služeb a dokumentace musí být plánované v společně s obchodováním.

Management uvolňování musí být integrován s procesy managementu konfigurace a managementu změny. Všechny související aktualizace dokumentace musí být zahrnuty v uvolňování, např. podnikatelské procesy, podpůrná dokumentace a SLA. Musí být ohodnocen vliv všech nových nebo změněných konfiguračních položek, u kterých je požadována autorizace změn. Poskytovatel služeb musí zajistit, že jak technické, tak netechnické aspekty uvolňování jsou zvažovány společně.

Položky uvolňování musí být sledovatelné a zabezpečené proti modifikaci. Pouze patřičně otestovaná a potvrzená uvolňování mohou být schválena do produktivního prostředí.

7.1 Management uvolňování

Cíl: Dodat, distribuovat a sledovat jednu nebo více změn obsažených v jednom release do produktivního prostředí.

7.1.1 Politika uvolňování

Musí existovat politika uvolňování, která zahrnuje:

- frekvenci a typ release;
- role a odpovědnosti pro release management;
- pravomoc pro schválení release do akceptačních testů a produktivního prostředí;
- jedinečná identifikace a popis všech release;
- přístupy ke skupinovým změnám v release;
- preferenci automatizace procesů tvorby vývojových verzí, instalace, distribuce release za účelem opakovatelnosti a efektivnosti;
- ověření a schválení release.

7.1.2 Plánování a nasazení uvolňování do produktivního prostředí

Poskytovatel služeb musí provádět činnosti s ohledem na podnikání, aby bylo zajištěno, že položky konfigurace, které jsou předmětem release, jsou kompatibilní s cílovým prostředím. Plánování release musí zajistit, aby změny, které ovlivní informační systémy, infrastrukturu, služby a dokumentaci byly odsouhlaseny, povoleny, naplánovány, koordinovány a sledovány.

Nasazení release do produktivního prostředí musí být plánované po etapách, protože detaily nasazení nemusí být zpočátku známé.

Plánování nasazení release do produktivního prostředí musí typicky zahrnovat:

- termíny vydání release a popis výstupů;
- související změny, problémy a známé chyby uzavřené nebo vyřešené touto release a známé chyby, které byly identifikované během testování této release;
- související procesy pro implementaci release napříč všemi podnikatelskými a geografickými jednotkami;
- způsob, jakým bude release zálohovaná nebo opravena, pokud bude neúspěšná;
- proces ověření a přijetí;

- komunikace, příprava, dokumentace a školení zákazníků a pracovníků podpory;
- logistika a procesy nákupu, skladování, expedice, spojení, přijímání a likvidace zboží;
- zdroje pro podporu potřebnou pro zajištění požadované úrovně služeb;
- identifikace závislostí, souvisejících změn a spojených rizik, které mohou ovlivnit hladký přenos release do akceptačních testů a produktivního prostředí;
- ukončení relese;
- plán auditů produkčního prostředí, kde se u významných aktualizací požaduje, aby bylo zajištěno, že produktivní prostředí je po nasazeni release v očekávaném stavu.

7.1.3 Vývoj nebo pořízení software

Release informačních systémů a software dodané od vlastních týmů, tvůrců systémů, systémových integrátorů nebo jiných organizací musí být ověřeny při přijetí. Celkový proces musí být dokumentován v plánu řízení konfigurace.

7.1.4 Návrh, vytváření a konfigurace uvolňování

Release a distribuce musejí být navrženy a implementovány, aby:

- vyhovovaly architektuře systému organizace, managementu služeb a normalizované infrastruktuře;
- zajistily integritu v průběhu tvorby vývojové verze, instalace, manipulace, vytvoření instalačního balíčku a dodávky;
- během procesu tvorby vývojové verze a nasazení release byly použity softwarové knihovny a související úložiště k řízení a kontrole komponent;
- byla jasně identifikována rizika a pokud to bude potřeba, tak aby byla přijata opatření k nápravě;
- umožnily ověření, že cílová platforma vyhovuje nezbytným předpokladům pro instalaci;
- umožnily ověření, že release je úplná v době, kdy se dostala na místo určení.

Výstupy z tohoto procesu musí zahrnovat poznámky k release, instalační instrukce, instalovaný software a hardware s příslušnou konfigurační baseline.

Výstupy z release musí být předány skupině odpovědné pro testování.

Procesy vytváření vývojové verze, instalace a distribuce by měly být automatizovány, aby byly omezeny chyby a aby bylo zajištěno, že proces je opakovatelný a že nové release mohou být rychle nasazeny do produktivního prostředí.

7.1.5 Ověření a akceptace uvolňování

Konečný výsledek musí být zakončen odsouhlasením úplnosti celého balíku release v porovnání s požadavky. Procesy ověření a akceptace musí:

- ověřit, že řízená akceptace v testovacím prostředí souhlasí s požadavky cílového produktivního prostředí;
- zajistit, že release je vytvořena z verzí podléhajících managementu konfigurace a je instalována v akceptačním testovacím prostředí používajícím plánované produkční procesy;
- ověřit, že požadovaná dílčí úroveň testování byla dokončena, např. funkční a nefunkční testování, obchodní akceptační testování, testování postupů vytváření vývojové verze, vydání release, distribuce a instalace;
- zajistit, aby release byla testována na spokojenost business zákazníků a personálu poskytovatele služeb;
- zajistit, že každé ukončení fáze akceptačního testování bude schváleno autorizovanou osobou;
- ověří, že cílový prostor uspokojuje nezbytné požadavky pro instalaci v oblasti hardware i software;
- ověřit, že release je úplná v době, kdy se dostala na místo určení.

K danému uvolnění (release) musí být vytvořena a být k dispozici vhodná dokumentace. Tato dokumentace musí být v rámci managementu konfigurace uložena ke konfigurační položce dané release a musí zahrnovat:

- podpůrnou dokumentaci, např. SLA;
- podpůrnou dokumentaci, např. přehled systému, instalační a podpůrné postupy, diagnostické nástroje, provozní a administrační instrukce;
- procesy vytváření vývojové verze, release, instalace a distribuce;
- contingency[5] a záložní plány;
- plán školení pro management služeb, pracovníky podpory a zákazníky;
- konfigurační baseline pro release včetně souvisejících položek konfigurace jako je systémová dokumentace, testovací prostředí, testovací dokumentace, verze nástrojů použitých při tvorbě a vývoji;
- související změny, problémy a známé chyby;
- důkazy o autorizaci release a související důkazy o ověření a přijetí.

Systém nebo služba, která ne zcela splňuje své specifické požadavky, musí být identifikována a zaznamenána v rámci managementu konfigurace a managementu problémů předtím, než vstoupí do produktivního provozu. Informace o známých chybách musejí být komunikovány incident managementu.

Pokud je release odmítnuta, opožděna nebo zrušena, musí být o tomto informován management změn.

7.1.6 Nasazení do produkčního prostředí, distribuce a instalace

Plán nasazení do produktivního prostředí musí být přezkoumán a musí být přidány potřebné detaily, aby bylo zajištěno, že všechny nezbytné činnosti budou provedeny.

Je důležité, aby release byla dodána bezpečně do místa určení a ve svém předpokládaném stavu. Procesy nasazení do produkčního prostředí distribuce a instalace musí zajistit, že:

- všechny oblasti skladování hardware a software jsou bezpečné;
- existují vhodné postupy pro skladování, expedici, přijeti a likvidaci zboží;
- kontroly instalací, prostředí, elektrického napájení a kontroly zařízení jsou plánované a provedené;
- zákazník a poskytovatel služeb jsou upozorněni na novou release;
- nadbytečné produkty, služby a licence jsou vyřazeny z provozu.

Po distribuci software přes počítačovou síť je důležité zkontrolovat, zda je release úplná a provozuschopná poté, co se dostanou do místa určení. Po úspěšné instalaci musí být aktualizovány záznamy aktiv a položek managementu konfigurace týkající se umístění a odpovědné osoby za hardware a software.

Mohou být použity zákaznické dotazníky o akceptaci a spokojenosti, a tím zaznamenat úspěch nebo neúspěch nasazení release. Výsledky zákaznických průzkumů musí být předány útvaru řízení obchodních vztahů.

7.1.7 Situace po uvolnění do produkčního prostředí

Počet incidentů souvisejících s release v období bezprostředně následujícím po nasazení do produktivního prostředí musí být měřen a analyzován, aby byl ohodnocen jejich vliv na obchodní činnost, na provoz a na zdroje pracovníků podpory.

[5] Pojmem „contingency plány“ se zde rozumí plány takových aktivit, které se začnou provádět v okamžiku vzniku významné havárie. V podstatě se jedná o havarijní plány, které mají za cíl, zajistit fungování základních služeb třeba v omezeném rozsahu v případě havárie.

Proces managementu změny musí zahrnovat poimplementační přezkoumání. Doporučení musí být předána do plánů zlepšení služeb.

Příklad:

Vzhledem k určitým specifikám poskytovaných IT služeb je četnost uvolnění plánována většinou zvlášť pro každý projekt podle smluvené frekvence vydávání nových a aktualizovaných verzí, a je tedy implicitně uvedena buď přímo v SLA nebo v příslušné projektové dokumentaci.

K dalšímu uvolnění u společnosti dochází na základě vzniklé potřeby vydání nové verze služby, infrastruktury IT, informačních systémů (SW a HW) a dokumentace (bezpečnostní záplata, oprava, ...).

U organizace je pro potřeby plánování uvolnění zaveden formulář „Plán uvolnění“, ale vzhledem k výše uvedenému jsou údaje související s plánováním uvolnění uváděny jako součást projektové nebo smluvní dokumentace. V určitých případech jsou nezbytné údaje o plánování uvolnění prováděny přímo v aplikaci MarkTime.

K nezbytným údajům pro plánování uvolnění patří zejména:

- *plánované datum vydání uvolnění;*
- *popis změn, odstranění problémů a známých chyb opravených plánovaným uvolněním;*
- *seznam potřebných zdrojů a evidenci požadavků pro nákup, včetně kompetenčních otázek.*

Za plánování uvolnění je zodpovědný manager projektu (manager uvolnění) nebo zaměstnanec podepsaný za společnost na SLA. V případě tvorby dokumentu „Plán uvolnění“ je to ředitel společnosti.

V organizaci jsou používány celkem 3 typy uvolnění:

- *Ostré uvolnění - uvolnění do provozního prostředí – nejsou označována typovým znakem;*
- *Release Candidate (kandidát na uvolnění) – verze připravená k distribuci, která je v režimu ověřování a schvalování;*
- *Betaverze – verze, která není určena pro nasazení do provozního prostředí a slouží pouze pro testování (tyto verze mohou být nestabilní a mohou vykazovat chyby).*

8 Literatura

[1] ČSN ISO/IEC 20000-1:2006: Informační technologie - Management služeb - Část 1: Specifikace.

[2] ČSN ISO/IEC 20000-2:2007: Informační technologie - Management služeb - Část 2: Soubor postupů.

[3] Office of Government Commerce (2000). Service Support, The Stationery Office. ISBN 0-11-330015-8.

[4] Office of Government Commerce (2001). Service Delivery. IT Infrastructure Library, The Stationery Office. ISBN 0-11-330017-4.

[5] Office of Government Commerce (2002). Planning To Implement Service Management, The Stationery Office. ISBN 0-11-330877-9.

[6] Office of Government Commerce (2002). ICT Infrastructure Management, The Stationery Office. ISBN 0-11-330865-5.

[7] Office of Government Commerce (2005). The Business Perspective, The Stationery Office. ISBN 0-11-330894-9.

[8] Office of Government Commerce (2002). Application Management, The Stationery Office. ISBN 0-11-330866-3.

[9] Office of Government Commerce (2005). ITIL Small Scale Implementation, The Stationery Office. ISBN 0-11-330980-5.

[10] Šebestová, M., Sedláček, M., Váňa, V. (2005) Management služeb IT, komentované vydání souboru ISO/IEC/DIS 20000:2004, ČNI Praha, 66 s.