

Příloha č. 2 – Technická specifikace Jednotný informační systém práce a sociálních věcí (dále v rámci této Přílohy č. 2 jen „Příloha“)

1. Integrovaná podpůrná a provozní data IPPD

1.1. Evidence subjektů a napojení na registry

Pro návrh a implementaci základní vrstvy Evidence subjektů a napojení na registry bude využit již existující framework Společného zemědělského registru (dále jen „SZR“), který je již od roku 2005 implementován a v provozu na Ministerstvu zemědělství ČR, a který je evidencí s totožným účelem jako IS IPPD MPSV.

Níže uvedený popis tak představuje nejen tento systém a jeho funkcionality, které jsou – z principu – totožné s požadavky IPPD Objednatele, ale uvádí také závazek Poskytovatele k úpravám „na klíč“, které vyplývají ze ZD a budou ve frameworku provedeny tak, aby mohl být nasazen jako požadované plnění.

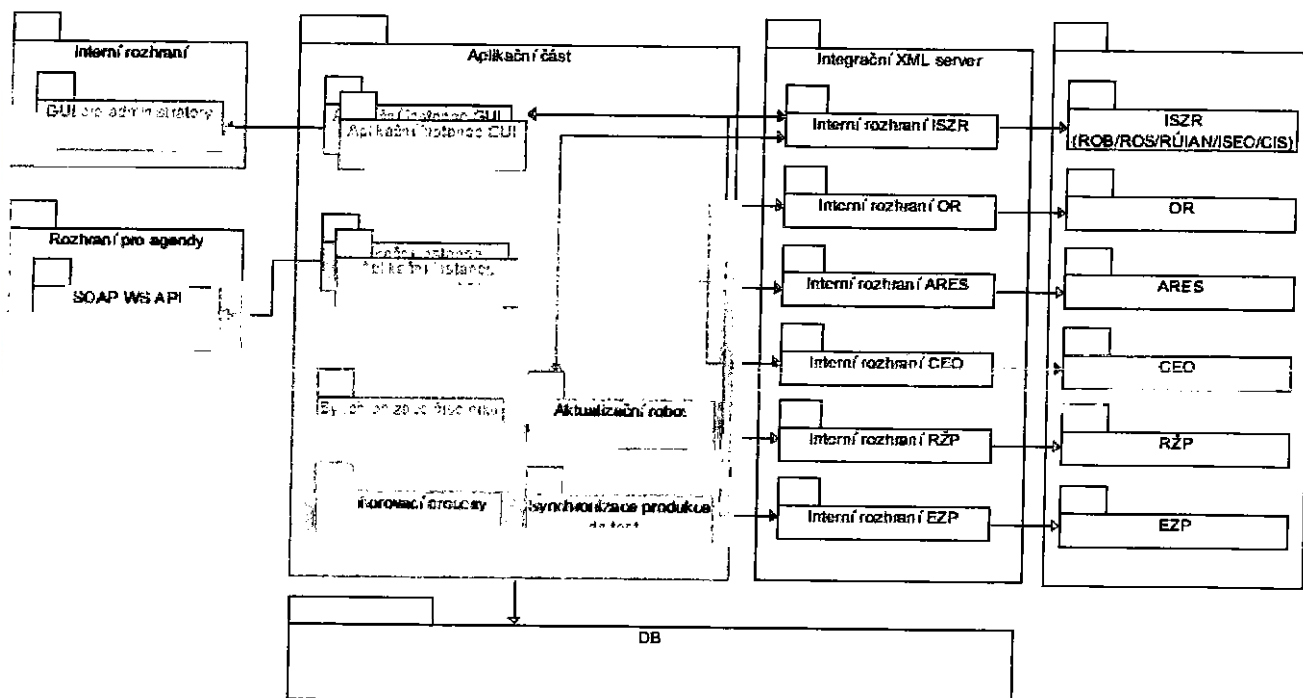
Systém SZR MZe byl navržen ještě před příchodem Základních registrů ČR a plnil následující účely v rámci resortu zemědělství:

- Ztotožnění subjektů v různých evidencích s různými identifikátory
- Aktualizace údajů vzdor heterogenitě prostředí a zdrojových systémů
- Vznik autoritativního zdroje údajů v resortu

První a třetí cíl je totožný s požadavky Objednatele a dodávaný registr je také v souladu s požadavky Objednatele bude plnit.

1.1.1. Architektura

Následující diagram zobrazuje nejen stávající architekturu SZR MZe, ale také základ nabízeného řešení, ze kterého budou odebrány prvky nepodstatné pro MPSV a které bude naopak rozšířeno o specifické požadavky MPSV, jak je uváděno níže:



Aplikační část zahrnuje programy podporující procesy fungování systému SZR. Aplikační vrstva je realizována v modulární vícevrstvé architektuře. Součásti aplikační vrstvy jsou následující:

- Webový server pro provoz interního rozhraní a rozhraní pro agendy v resortu.
- Aktualizační proces zajišťující načítání změnových informací ze Základních registrů a aktualizaci subjektů v evidenci.
- Proces synchronizace číselník s centrálním úložištěm číselníku.
- Synchronizační proces zajišťující přenos změn z produkční databáze do testovací.

Architektura systému IPPD bude postavena obdobně systému SZR a bude splňovat následující požadavky:

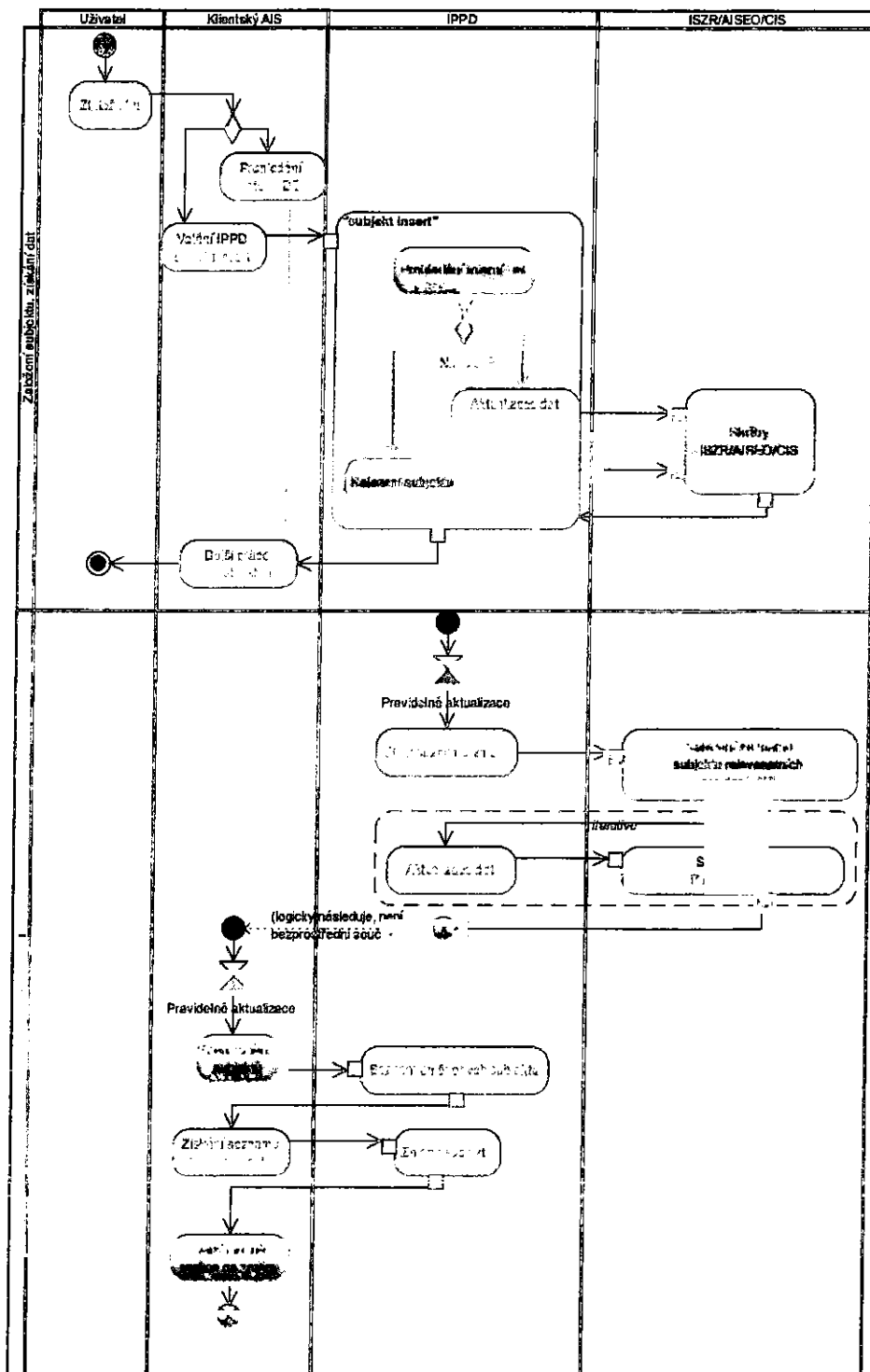
Architektura klient-server s oddělenou aplikační a databázovou částí.

- Pro databázovou část bude využito relačního databázového systému. Přístup k databázi bude vůči konzumentům zapouzdřen prostřednictvím aplikačních procesů.
- Systém bude provozován ve dvou prostředích – produkčním a testovacím, vždy v clusteru (primární a záložní prostředí). Pro vysokou dostupnost systému je počítáno se souběžným provozem primárního a záložního prostředí. Testovací prostředí bude provozováno v totožné architektuře s výjimkou procesů, které v testovacím prostředí nebude možné či smysluplné provozovat – například aktualizace subjektů vůči Základním registrům (lze nahradit např. synchronizačním procesem IPPD vůči produkčnímu prostředí či aktualizací testovacího prostředí vůči testovacím ISZR, dle vhodnosti pro splnění podmínky totožnosti obou prostředí).
- Systém bude integrován do zálohovacího prostředí Objednatele.
- Paralelní zpracování a škálovatelnost a vysoká dostupnost bez ztráty kontextu v případě výpadku (jak vyplývá z kap. 1.1.2)

Integrační XML server je proprietární avšak plně otevřená platforma Poskytovatele, na které budou provozovány služby střední vrstvy. XML server zprostředkovává rozhraní pro vnější přístup k systému SZR (v kontextu MPSV: kompozitní služby ISZR, služby poskytované třetím stranám na základě oborových zákonů MPSV či jiných práv) z ostatních systémů a naopak je prostředníkem komunikace s externími systémy, ze kterých SZR čerpá data. V rámci dodávky Evidence subjektů IPPD budou implementována následující rozhraní:

- Rozhraní pro Informační systém základních registrů
 - Registr obyvatel (ROB) – načítání dat o fyzických osobách
 - Registr osob (ROS) – načítání dat o právnických osobách
 - Informační systém evidence obyvatel (ISEO)
 - Cizinecký informační systém (CIS)
 - Registr územní identifikace adres a nemovitostí (RÚIAN) – získávání údajů o adresách osob obyvatel
- Pokud se ukáže jako potřebné, bude implementováno rozhraní externích registrů ARES, OR a RŽP (případně pouze některá z nich) a to především kvůli zakládání právnických osob, jejichž data nejsou zapsána v ROS.
- Integrace na rozhraní spisové služby Objednatele.

lyze systému bude přesně specifikováno za jakých podmínek budou načítány subjekty ze Základních registrů a jakým způsobem bude vyplňována kategorie dotazu do ZR.



3

identity vůči ISZR, včetně zabezpečení neoprávněného přístupu. V rámci procesu pak bude návrhem v analýze vyřešeno i nesdružování osobních údajů, které byly získány k rozdílným účelům (dle písm. h) odst. (1) § 5 zák. 101/2000 Sb. O ochraně osobních údajů v návaznosti na legislativě pokrývající daný klientský AIS v kontextu legislativy IPPD.

Důležitou informací je fakt, že pro IPPD bude transparentní režim zakládání, ztotožnění a nebo vyhledání subjektu (pozn.: navíc je takto i ošetřena editace těch údajů které jsou načítány z jiných evidencí a není požadavek na jejich úpravy ze stran klientských systémů). Požadavek na subjekt obecně ústí v jeho vyhledání a – pokud by shodou okolností ještě nebyl zaveden v DB IPPD – zavedení údajů do IPPD. Pokud subjekt již existuje v IPPD, jsou tyto údaje pouze aktualizovány.

Systém pak pro pravidelnou aktualizaci (zpravidla v nočních hodinách) využívá automatizovaného volání změnových služeb ISZR, kdy jsou notifikovány identifikátory těch subjektů, u kterých došlo ke změnám. Stejný princip pak používá IPPD i dovnitř resort k integrovaným systémům, kterým předává identifikátory těch subjektů, které se změnily a systémy mají možnost – v návaznosti na svůj business process a jeho relevantní předpisy - údaje aktualizovat.

1.1.2. Architektura serverového řešení

Pozn.: Toto řešení bude sloužit i pro aplikace Právních agend, s ohledem na překryv problematiky jej Poskytovatel uvádí pouze jednou a to v celé šíři v této kapitole u IPPD. Předpokládáme využití současné virtualizované infrastruktury zadavatele, která je provozována za použití hypervisoru Microsoft Hyper-V. V tomto prostředí budou vytvořeny virtuální stroje dle definice v následujících kapitolách tohoto dokumentu. Jako serverový operační systém byl vybrán Microsoft Windows Server 2012 R2 Standart, databázový server byl vybrán Microsoft SQL Server Standart.

1.1.2.1. Popis základní myšlenky architektury serverového řešení

Aby byla splněna podmínka požadavku na vysokou dostupnost řešení, využíváme technologii Microsoft Server Cluster Server (MSCS) jak pro Microsoft SQL, tak i pro Microsoft Internet Information Server (IIS).

Pro realizaci clusteru v navržené formě tak, aby splňovala požadavky ZD na vysokou dostupnost (zejména AR008 a AR009) je nezbytné, aby v souladu s popisem možností „Záložního produkčního prostředí“ (kap. 1.3.1. Příl. 6 ZD) byly systémy virtuálních serverů Poskytovatele v „Záložním produkčním prostředí“ provozovány souběžně (aktivně) s jejich ekvivalenty v primárním produkčním prostředí. Tím je dotčena možnost je dle požadavků AR008 a AR009 provozovat – z pohledu aplikací – jak jako active-active tak jako active-passive (pokrytí licencemi aplikací i OS s tím počítá v souladu s dopl. dotazy č. X, dotaz č. 2, tj. licence v „záložním produkčním prostředí“ se pokrývají z 3-násobku licencí navíc), kdy ale v obou případech (tj. aplikačního režimu active-active i active-passive) je nutný aktivní provoz guestů (hostovaných OS) pro zajištění funkcionality vysoké dostupnosti.

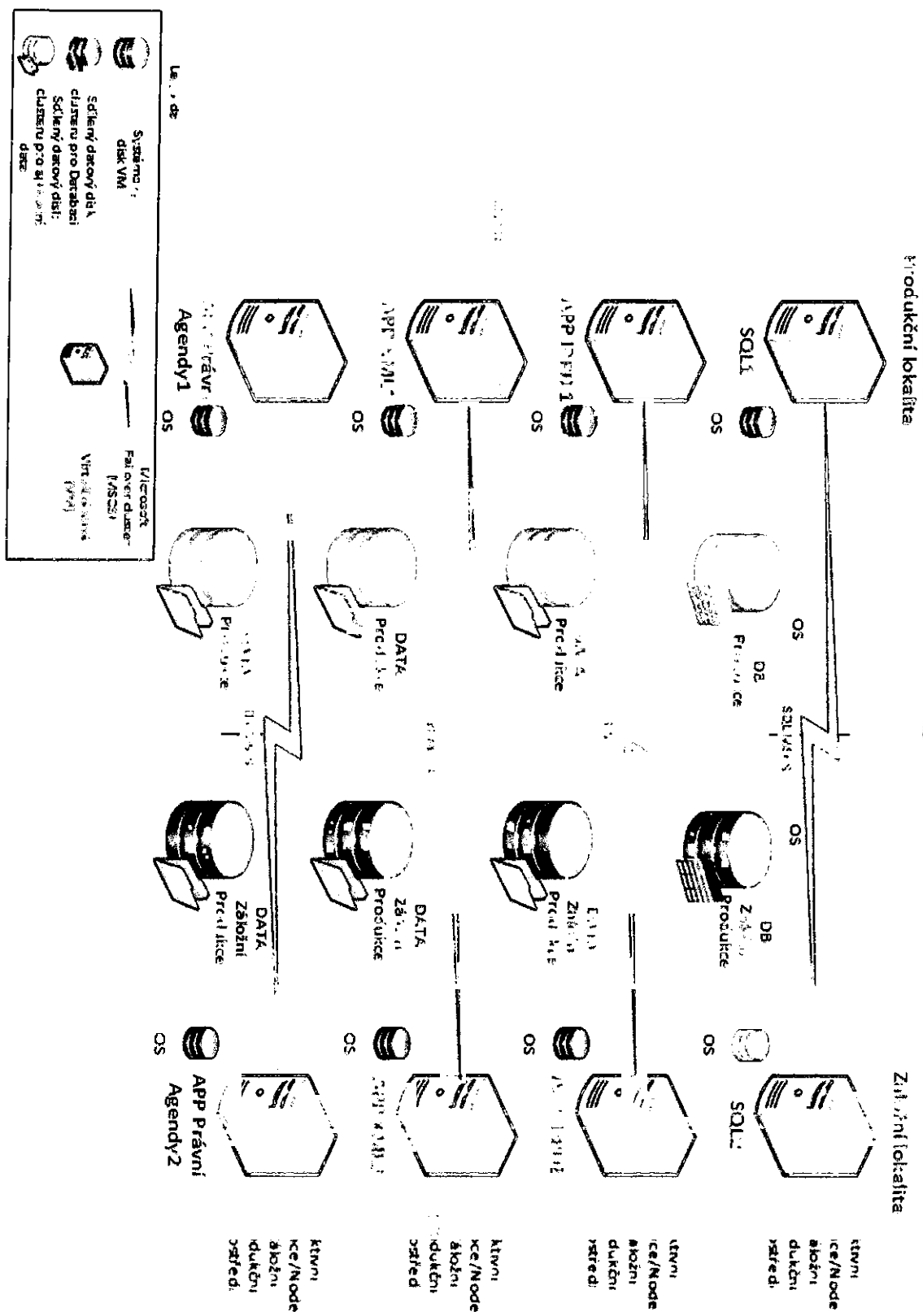
1.1.2.2. Produkční + záložní produkční prostředí

Je koncipováno jako active-active geografický cluster. Pro Produkční prostředí bude vyhrazena jedna instance a pro Záložní produkční prostředí druhá instance. Obě instance jsou na sobě nezávislé. To předpokládá, že poskytnutá infrastruktura umožňuje propojení pro LAN i SAN plnohodnotně v obou lokalitách. To umožňuje optimálně škálovat a zároveň poskytnout vysokou dostupnost.

Předpokládaná konfigurace:

Role	Počet vCPU 2,4GHz	R A M	HDD OS GB	HDD Data GB	HDD Archiv TB	Licen ce OS	Licence SQL Core	poznámka	umístění
SQL 1	16	96	60	1024	8	1	16	Aktivní instance pro produkce	produkční lokalita
SQL 2	16	96	60	1024	8	1	16	Aktivní instance pro záložní produkce	záložní lokalita
APP IPPD 1	16	32	60	100	0	1	0	Aktivní instance pro produkce	produkční lokalita
APP IPPD 2	16	32	60	100	0	1	0	Aktivní instance pro záložní produkce	záložní lokalita
APP XML 1	12	32	60	100	0	1	0	Aktivní instance pro produkce	produkční lokalita
APP XML 2	12	32	60	100	0	1	0	Aktivní instance pro záložní produkce	záložní lokalita
APP Právní Agendy 1	12	32	60	100	0	1	0	Aktivní instance pro produkce	produkční lokalita
APP Právní Agendy 2	12	32	60	100	0	1	0	Aktivní instance pro záložní produkce	záložní lokalita

Předpokládá se, že produkční prostředí při standartním provozu poběží na zdrojích poskytovaných na primární lokalitě a pomocné produkční prostředí poběží při standartním provozu ze záložního prostředí. V případě výpadku jedné z lokalit bude provoz „překlopen“ na druhou přeživší lokalitu. SQL cluster bude v tomto prostředí provozován jako active-active.



1.1.2.3. Testovací prostředí

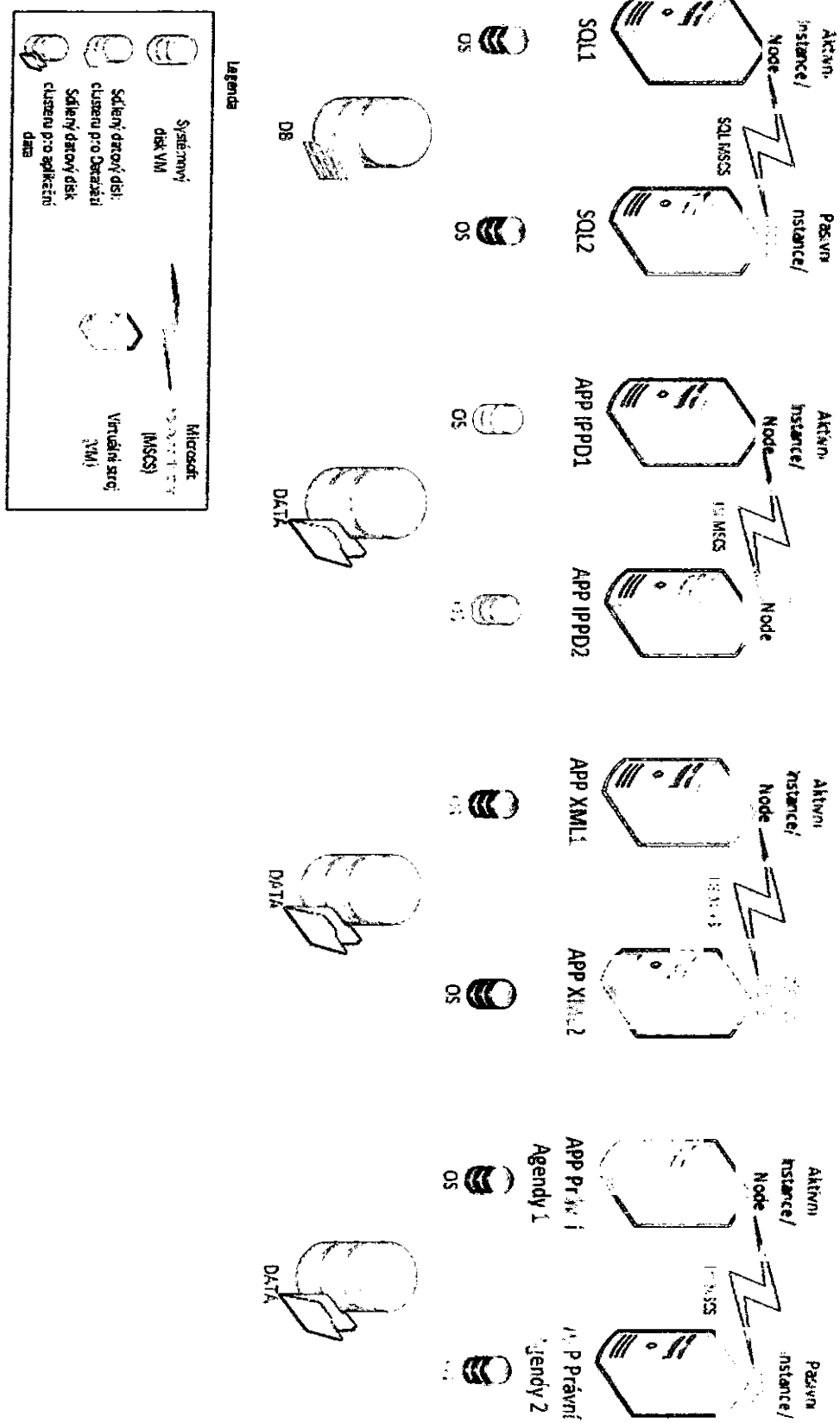
Je koncipováno jako standartní active-pasive MSCS v rámci jedné lokality – jedna instance.

Předpokládá se provozovat celé na produkční lokalitě. Jeho implementace je naprosto srovnatelná (jedna vyhrazená instance) s Produkčním (vlastní instance) a Záložním produkčním (vlastní instance) prostředím. Jeho výkon je možné kdykoliv rozšířit na výkon srovnatelný s Produkčním a Záložním produkčním prostředím. Toho dosáhneme čerpáním licencí z 2. nebo 3. 1/3 licencí.

Předpokládaná konfigurace

Role	Počet vCPU 2,4GHz	RAM	HDD OS GB	HDD Data GB	HDD Archiv TB	Licenc e OS	Licence SQL Core	poznám ka	umístění
SQL 1	8	96	60	1024	8	1	8	Aktivní	produkční lokalita
SQL 2	8	96	60			1		Pasivní/ Aktivní	produkční lokalita
APP IPPD 1	4	8	60	100	0	1	0	Aktivní	produkční lokalita
APP IPPD 2	4	8	60		0	1	0	Aktivní	produkční lokalita
APP XML 1	4	8	60	100	0	1	0	Aktivní	produkční lokalita
APP XML 2	4	8	60		0	1	0	Aktivní	produkční lokalita
APP Právní Agendy 1	4	8	60	100	0	1	0	Aktivní	produkční lokalita
APP Právní Agendy 2	4	8	60		0	1	0	Aktivní	produkční lokalita

Detailní náčrpes prostředí



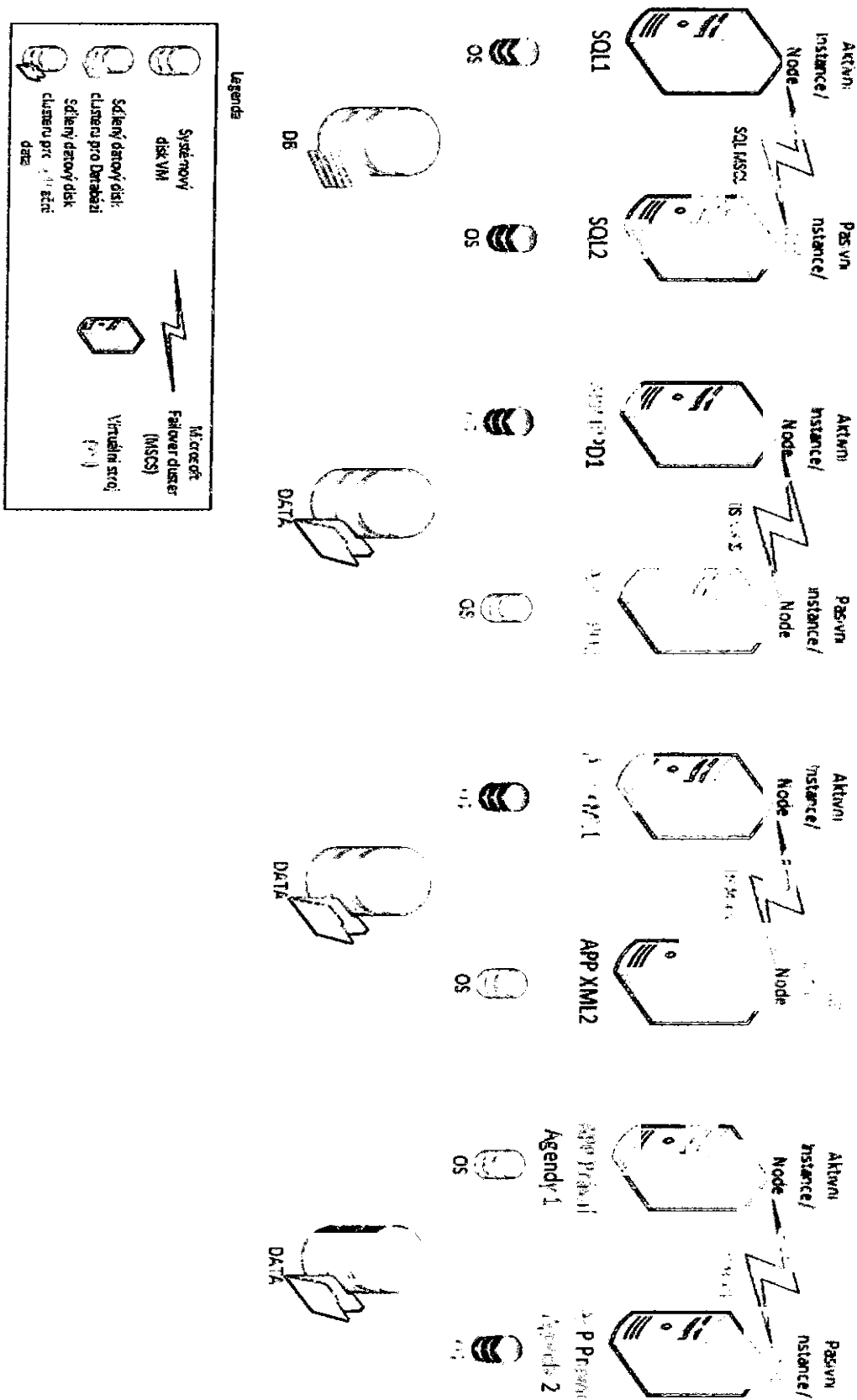
1.1.2.4. Testovací prostředí

Je koncipováno jako standartní active-pasive MSCS v rámci jedné lokality – jedna instance.

Předpokládá se provozovat celé na produkční lokalitě. Jeho implementace je naprosto srovnatelná (jedna vyhrazená instance) s Produkčním (vlastní instance) a Záložním produkčním (vlastní instance) prostředím. Jeho výkon je možné kdykoliv rozšířit na výkon srovnatelný s Produkčním a Záložním produkčním prostředím. Toho dosáhneme čerpáním licencí z 2. nebo 3. 1/3 licencí. Předpokládaná konfigurace

Role	Počet vCPU 2,4GHz	RAM	HDD OS GB	HDD Data GB	HDD Archiv TB	Licenc e OS	Licence SQL Core	poznám ka	umístění
SQL 1	8	96	60	1024	8	1	8	Aktivní	produkční lokalita
SQL 2	8	96	60			1		Pasivní	produkční lokalita
APP IPPD 1	4	8	60	100	0	1	0	Aktivní	produkční lokalita
APP IPPD 2	4	8	60		0	1	0	Aktivní	produkční lokalita
APP XML 1	4	8	60	100	0	1	0	Aktivní	produkční lokalita
APP XML 2	4	8	60		0	1	0	Aktivní	produkční lokalita
APP Právní Agendy 1	4	8	60	100	0	1	0	Aktivní	produkční lokalita
APP Právní Agendy 2	4	8	60		0	1	0	Aktivní	produkční lokalita

Detailní náčrtek prostředí:



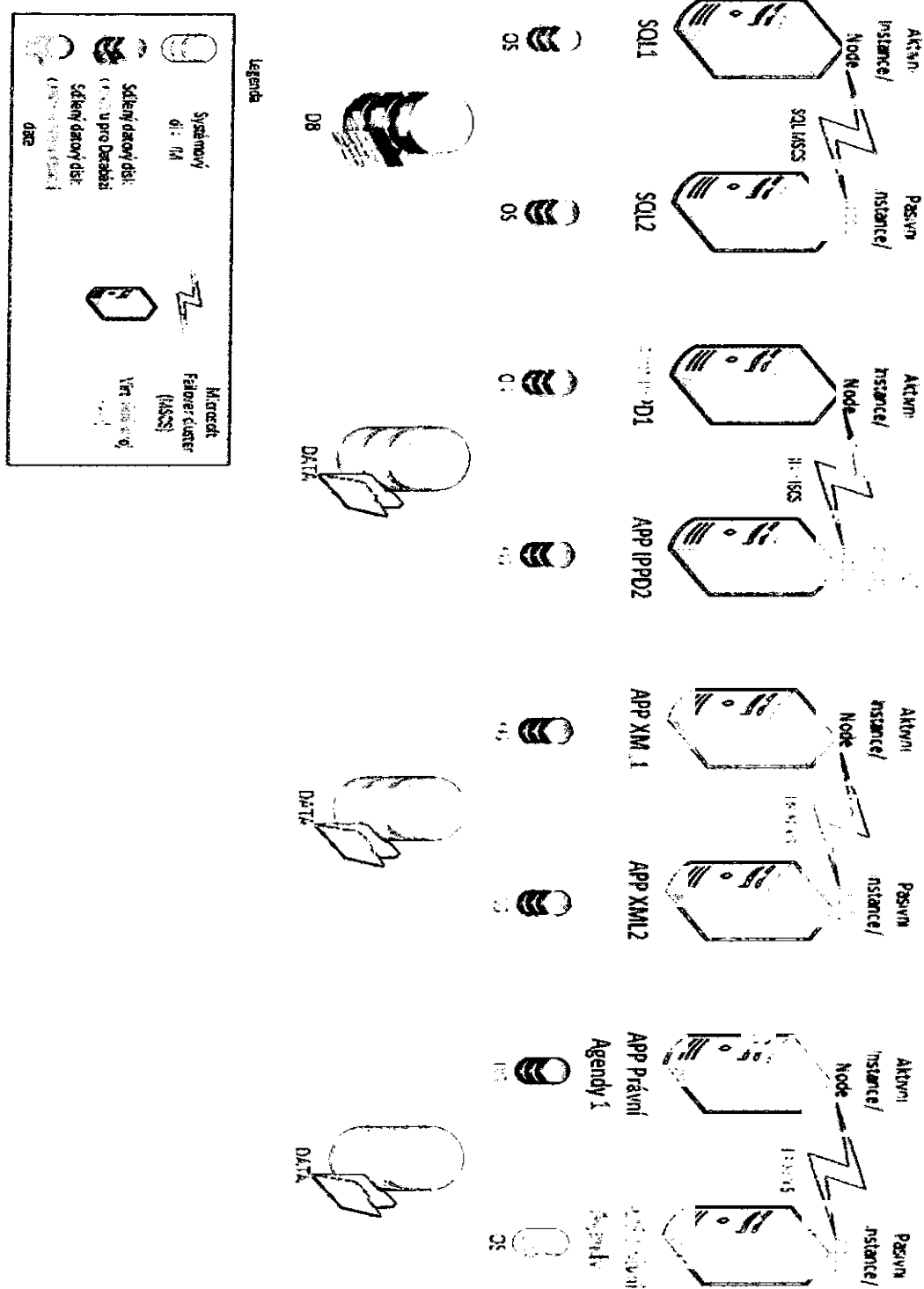
1.1.2.5. Vývojové prostředí

Je koncipováno jako standartní active-pasive MSCS v rámci jedné lokality – jedna instance.

Předpokládá se provozovat celé na produkční lokalitě. Jedna instance je naprosto srovnatelná (jedna vyhrazená instance) s Produkčním (vlastní instance) a s Testovacím produkčním (vlastní instance) prostředím.

Předpokládaná konfigurace

Role	Počet vCPU 2,4GHz	RAM	HDD OS GB	HDD Data GB	HDD Archivační TB	Licence OS	Licence SQL Core	poznámka	umístění
SQL 1	4	96	60	1024	4	1	4	Aktivní	Testovací lokalita
SQL 2	4	96	60			1		Pasivní	Testovací lokalita
APP IPPD 1	4	8	60	100	0	1	0	Aktivní	Testovací lokalita
APP IPPD 2	4	8	60		0	1	0	Pasivní	Testovací lokalita
XML 1	4	8	60	100	0	1	0	Aktivní	Testovací lokalita
XML 2	4	8	60		0	1	0	Pasivní	Testovací lokalita
Právní fondy 1	4	8	60	100	0	1	0	Aktivní	Testovací lokalita
Právní fondy 2	4	8	60		0	1	0	Pasivní	Testovací lokalita



1.1.2.6.

Nabízené licence

Jak již bylo zmíněno, předpokládáme použití operačního systému Microsoft Windows Server Standard a Microsoft SQL standart. Všechny licence, jak vychází z požadavků ze ZD, jsou opatřeny softwarovou maintenance ve formě Software Assurance (SA). Vzhledem k dvouletému inkrementu/skoku SA je celková doba trvání nabízených licencí + SA na dobu 6ti let.

Pro realizaci clusteru v navržené formě tak, aby splňovala požadavky ZD na vysokou dostupnost (zejména AR008 a AR009) je nezbytné, aby v souladu s popisem možností „Záložního produkčního prostředí“ (kap. 1.3.1. Příl. 6 ZD) byly systémy virtuálních serverů Poskytovatele v „Záložním produkčním prostředí“ provozovány souběžně (aktivně) s jejich ekvivalenty v primárním produkčním prostředí. Tím je dotčena možnost je dle požadavků AR008 a AR009 provozovat – z pohledu aplikací – jak jako active-active tak jako active-pasive (pokrytí licencemi aplikací i OS s tím počítá v souladu s dopl. dotazy č. X, dotaz č. 2, tj. licence v „záložním produkčním prostředí“ se pokrývají z 3-násobku licencí navíc), kdy ale v obou případech (tj. aplikačního režimu active-active i active-passive) je nutný aktivní provoz guestů (hostovaných OS) pro zajištění funkcionality vysoké dostupnosti.

Pro zajištění množstevního rozsahu licencí, který je potřebný k pokrytí potřeb Objednatele ke dni uzavření smlouvy je 32ks licencí operačního systému Microsoft Windows Server Standart. Toto číslo je součtem všech instancí operačního systému ve všech prostředích. Tím pádem je trojnásobkem těchto potřeb množství odpovídající 96ks licencí Microsoft Windows Server + patřičné množství dvou-letých inkrementů Software Assurance.

Pro zajištění množstevního rozsahu licencí, který je potřebný k pokrytí potřeb Objednatele ke dni uzavření smlouvy je 36ks core licencí databázového systému Microsoft SQL Server Standart. Toto je součet všech potřebných core pro Produkční prostředí + testovací prostředí a vývojové prostředí. Tím pádem je trojnásobkem těchto potřeb množství odpovídající 108ks core licencí Microsoft SQL Server + patřičné množství dvou-letých inkrementů Software Assurance. Vzhledem k tomu, že výrobce SW prodává licence SQL serveru po dvou-core inkrementech, je tím pádem nabízeno 96ks SKUs (Stock keeping Units). Zbývá prostředí jsou, na základě odpovědi na doplňující dotazy č. X, dotaz č. 2, tj. licence v „záložním produkčním prostředí“ se pokrývají z 3-násobku licencí navíc, licencovány z 2. a 3. 1/3 dodaných licencí.

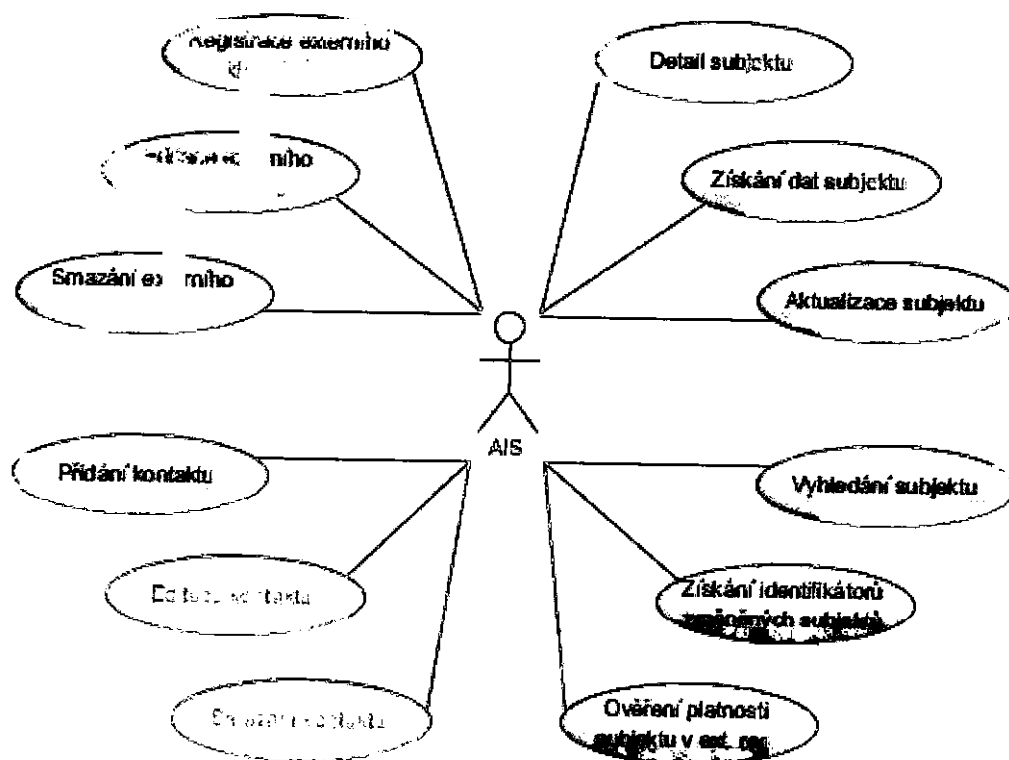
1.1.2.7. Zálohování

Zálohování považujeme za jednu ze samozřejmostí bezpečnosti celého systému. Předpokládáme, že námi navrhovaný systém bude začleněn do zálohovacího systému zadavatele. Zálohy předpokládáme provádět jak na úrovni celé VM, tak i na úrovni aplikační, především SQL databáze. Pokud zálohovací systém zadavatele disponuje možností granulárního restore z filesystému uvnitř VM, nevyžadujeme tuto zálohu separátně. Pokud to neumožňuje, předpokládáme provádění i separátní zálohy filesystému uvnitř VM.

Zálohovací scénář bude prováděn v definovaných intervalech pro plné (Full) a inkrementální/rozdílové zálohy.

- Konec subkapitoly 1.1.2. Architektura serverového řešení, pokračují subkapitoly z kapitoly 1.1.
Evidence subjektů a napojení na registry -

1.1.3. Rozhraní pro agendy



Pokud některá agenda v resortu zavede subjekt do své evidence, registruje v SZR svůj externí identifikátor. Tím je v centrální databázi SZR k dispozici informace o tom, ve kterých agendách je daný subjekt evidován.

V rámci dodávky IPPD bude dodáno principiálně identické rozhraní systému, upravené dle specifických potřeb Objednatel. Rozhraní systému IPPD bude specifikováno v rámci analýzy.

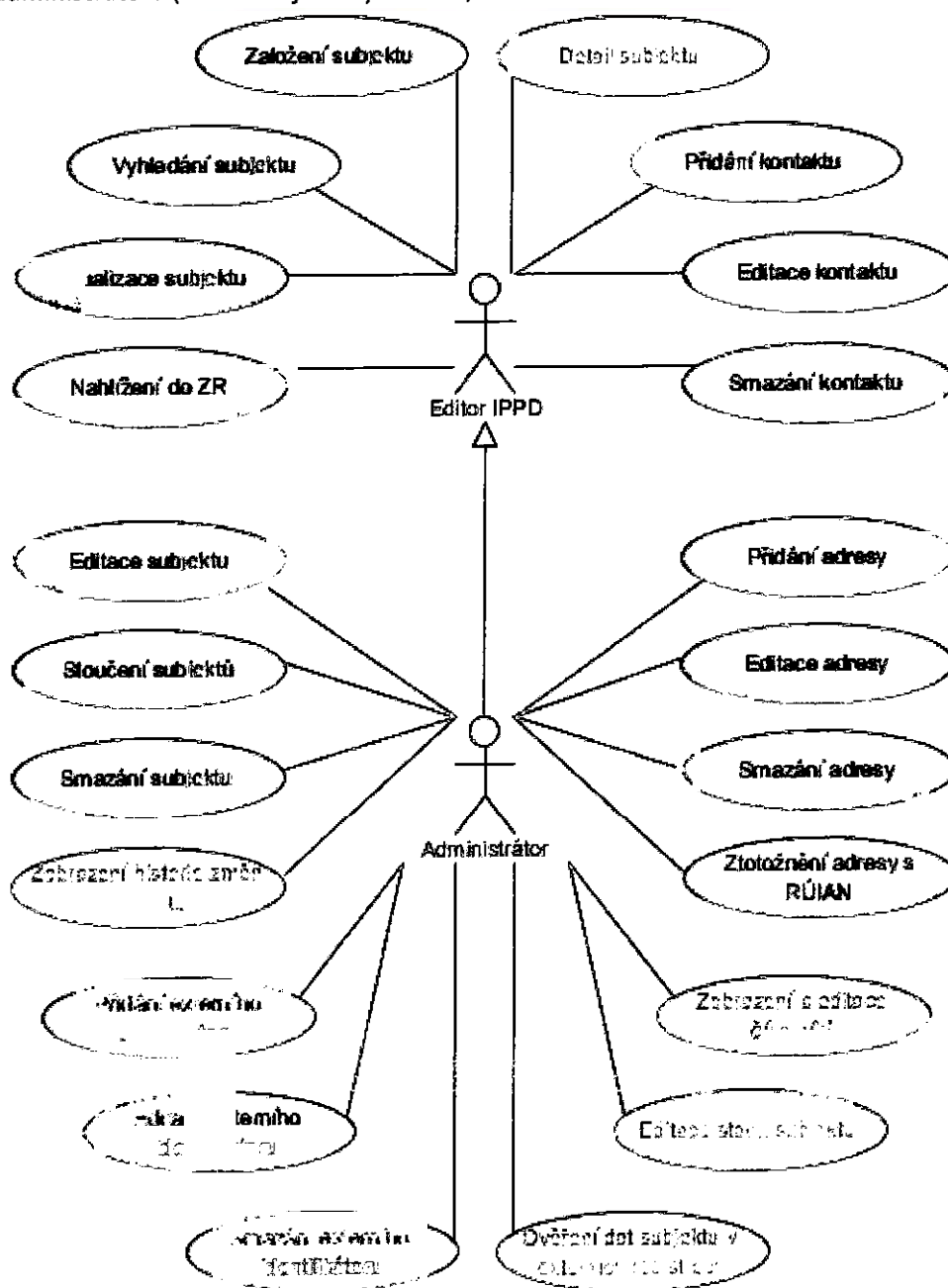
Oproti základu platformy pro evidenci subjektů budou také navíc v rámci této zakázky implementovány služby (a jim odpovídající datové entity v rámci IPPD) sloužící pro evidenci rozhodných skutečností. Dle detailní specifikace pak bude možné, aby do těchto atributů subjektů jednotlivé integrované agendové systémy zapisovaly či načítaly tyto údaje (rozsah evidence v souladu POD0079), nebo v případě potřeby může tyto údaje aktualizovat automatizovaný proces dle pravidel poskytovaných dat na rozhraní té které evidence.

V souladu s požadavky ZD a při zohlednění principů a využití nástrojů platformy, na kterých je systém založen (viz kap 3.1) budou veškeré metody (tím se myslí metody webových služeb nebo metody tříd controllerů MVC) opatřeny mechanismem, který platforma ASP.NET poskytuje pro explicitní definování povolených rolí či jiných definovaných entit dle implementace u metod a jejich srovnání s předanými údaji

uživatelského sezení získaných při autentizaci implementovatelnými způsobem dle analýzy, čímž bude zabráněno využití kódu dané metody neoprávněnými přistupujícími entitami. S pomocí entit vstupujících do tohoto mechanismu bude řešeno také jejich předání programovým modulům pro logování (bezpečnostní a výkonnostní monitoring vč. podkladů pro audit), implementovaným v každé metodě, čímž bude zajištěna funkcionality bezpečnostního dohledu.

1.1.4. Aplikace pro administraci evidence subjektů

Pro správce evidence subjektů bude dodáno administrační rozhraní postavené na webových technologiích implementující následující případy užití pro roli editora a administrátora (obdobně jako nyní v SZR).



V následující části bude ukázáno, jak vypadá řešení grafického uživatelského rozhraní administrátorské aplikace v případě SZR MZe. Řešení této aplikace v rámci dodávky IPPS pro Objednatele bude přizpůsobeno jeho požadavkům.

SPOLEČNÝ ZEMĚDĚLSKÝ REGISTR

MINISTERSTVO ZEMĚDĚLSTVÍ

Přihlášení uživatele
Ověřte šablonu
za subjektu

[Zpět](#)

Vyhledání subjektu

SZR-ID: _____ Obchodní jméno: PDS s.r.o.
 IČO: _____ Jméno: _____
 Rodné číslo: _____ Příjmení: _____
 Datum narození: _____ Obec: _____
 Právní forma: _____ Ulice: _____
 Externí identifikátor: _____ Kraj: _____
 Typ: (neurčeno) PSČ: _____
 Hodnota: _____ Identifikátor DS: _____

[Hledat](#) [vytisknout formulář](#)

SZR-ID	Obchodní jméno ^	Příjmení, Jméno	Rodné číslo	IČO	Adresa	Akce
1000946200	PDS s.r.o.			25523121	Viniční 6, Brno, 61500	Detail

Strana 1 [10](#) Zobrazeno 1 - 1 z 1 záznamů

[nahoru](#)

Na uvedeném snímku je vidět formulář pro vyhledání subjektu s tabulkou nalezených výsledků. V tabulce je ikona pro přechod na detailní informace o subjektu s možností editovat data. V levé části je v menu jednořádkový formulář, s pomocí kterého lze při znalosti některého identifikátoru okamžitě přejít na detail subjektu. Dále je v menu odkaz na formulář pro založení subjektu a také odkaz pro nahlížení do Základních registrů.

Monitorování

Subjekty

Vhledat subjekty

- Vyhledávání
- Zabíjení subjektu
- Data pro MF
- Občanská
- Výsledky synchronizace
- Dotazy
- Základní registry

Provozování

- Vyhledávání
- Import

Vyhledávání DS

Restriktivní DS

LDAP farmář

- Zabíjení
- Vyhledávání
- Sestavy

Čestník

- Běžné formy
- Dotazníky
- Dotazníky podrobnosti
- Běžné identifikátory
- Typy adres
- Zobrazit
- Obory
- Systémy
- Účty
- Čestník BOP
- SLE - přímý odkaz

Ke stažení

PDS s.r.o. (SZR-ID 1000946200)

Stav

Zablokovat Smazat Sloučit Aktualizovat Historie

SZR EDP

Obchodní jméno: PDS s.r.o.

Seznam obch. jmen: PDS s.r.o. (A120) PDS s.r.o. (A120)

Obchodní jm. - zkratka:

Titul před jménem:

Jméno: 1. 2.

Příjmení: 1. 2.

Rodné příjmení:

Titul za jménem:

Datum narození:

Číslo dokladu:

Typ dokladu:

Státní příslušnost: 112 - Společnost s ručením omezeným

Právní forma: 112

Plátce DPH: Ne

Finanční úřad:

Kód plátce daně:

DIČ:

Na snímku obrazovky je hlavní stránka s daty subjektu se zobrazením všech administrátorských funkcí. Pod názvem subjektu jsou záložky, na kterých se nacházejí další data subjektu. Na zobrazené záložce je nástrojová lišta, která umožňuje provést blokaci subjektu (zamezení aktualizace dat subjektu), smazání subjektu, sloučení s jiným subjektem, aktualizaci dat subjektu ze Základních registrů a zobrazení historie změn subjektu. Pod nástrojovou lištou je tabulka, která zobrazuje údaje subjektu, jak jsou uloženy v SZR. Do dalších sloupců je možné načíst data z různých registrů a jednoduše pohledem srovnat shodnost údajů v různých evidencích. Na uvedeném snímku jsou vidět údaje evidované v SZR a data načtená z ROS. Po načtení údajů z externích registrů má administrátor možnost zobrazit si přímo XML odpovědi patřičné webové služby (ikona v záhlaví sloupců externích registrů).



SPOLEČNÝ ZEMĚLSKÝ REGISTR
 MINISTERSTVO ZEMĚLSTVÍ

Přidání uživatel
 Ověření účtu
 Zpět

Monitoring

Subjekty

- Vyhledávání
- Zakázání subjektu
- Data pro MF
- Chybovka
- Výsledky synchronizace
- Doklady
- Základní registry
- Provozovny
- Vyhledávání
- IMOD
- Vyhledávání DS
- Režimové tresty
- LDAP farmář
- Zakázání
- Vyhledávání
- Systém
- Časová osa
- První form
- Doklady provozovny
- Doklady podnikavny
- Externí identifikatory
- Doklady

Subjekt Identifikatory Adresy Kontakty Finance

Filtr podle typu

Zobrazit historii ☐

p	Typ	Hodnota	Platnost od	Platnost do	Důvod	Akce
1	ICO	25523121	17. 3. 1998			☐
4	EAG	1000946200	16. 1. 2010			☐
5	ADP	1000946200	30. 12. 2011			☐
6	ADP	1000946200	31. 12. 2011			☐
7	JIA	1001119509	11. 2. 2014			☐

Strana 1 z 1

Zobrazeno 1 - 5 z 5 záznamů

Doklady totožnosti

Typ

Filtr podle typu

Zobrazit historii ☐

Typ	Číslo	Platnost od	Platnost do

Strana 1 z 0

Nenalezeny žádné záznamy

Snímek obrazovky zobrazuje externí identifikátory subjektu. V nástrojové liště má administrátor tlačítko pro přidání dalšího externího identifikátoru. V tabulce je seznam evidovaných identifikátorů subjektu s jejich platností a možnostmi jejich editace či smazání. Dle typů externích identifikátorů je možné zjistit, ve kterých agendách resortu je subjekt evidován. Dále jsou zde identifikátory IČO, u fyzických osob rodné číslo načtené ze Základních registrů, respektive z ISEO. V druhé tabulce se zobrazují u fyzických osob údaje o dokladech totožnosti načtené ze Základních registrů. U obou tabulek je možné filtrovat podle typu a zobrazovat historii změn údajů.



SPOLEČNÝ ZEMĚLSKÝ REGISTR
 MINISTERSTVO ZEMĚLSTVÍ

Zpět

Monitoring

Subjekty

Hledat subjekt

- Vyhledávání
- Zakázání subjektu
- Data pro MF
- Chybovka
- Výsledky synchronizace
- Doklady
- Základní registry
- Provozovny
- Vyhledávání
- IMOD
- Vyhledávání DS
- Režimové tresty
- LDAP farmář
- Zakázání
- Vyhledávání
- Systém
- Časová osa
- První form
- Doklady provozovny
- Doklady podnikavny
- Externí identifikatory
- Doklady

Filtr podle typu

Zobrazit historii ☐

Typ	Agenda	Kraj	Okres	Obec, část	Ulice	Č.p./č. or.
100: Primární adresa SZR		Jihomoravský kraj	Brno-město	O: Brno ČO: Židenice MČ: Brno-Židenice	Viniční	6/20
301: A120		Jihomoravský kraj	Brno-město	O: Brno ČO: Židenice MČ: Brno-Židenice	Viniční	6/20

Strana 1 z 1

Zeleně podbarvené řádky obsahují hodnoty (uvedené kurzívou), které nejsou uloženy v SZR, pouze byly dočasně načteny z RÚIAN dle kódu adresy.

Na uvedeném snímku jsou zobrazeny adresy subjektu uložené v evidenci SZR. Opět jsou zde k dispozici administrátorské funkce pro přidání, editaci a mazání adres. K dispozici je filtr podle typu adresy a volba pro zobrazení historie změn. Adresu, která je zadána pomocí textových údajů, může administrátor ztotožnit s RÚIAN pomocí dialogu pro vyhledání adresy RÚIAN.

Grafické rozhraní systému IPPD nabídne uživateli funkci pro nahlášení rozporu v údajích evidovaných v Základních registrech (zpochybnění údajů).

Grafické rozhraní umožní zobrazení a náhled případných navázaných dokumentů a písemností ze spisové služby Objednatele. Přesná specifikace integrace na spisovou službu bude definována v analýze.

V souladu s požadavky ZD a při zohlednění principů a využití nástrojů platformy, na kterých je systém založen (viz kap 3.1) budou veškeré metody (tím se myslí metody webových služeb nebo metody tříd controllerů MVC) opatřeny mechanismem, který platforma ASP.NET poskytuje pro explicitní definování povolených rolí či jiných definovaných entit dle implementace u metod a jejich srovnání s předanými údaji uživatelského sezení získaných při autentizaci implementovatelnými způsobem dle analýzy, čímž bude zabráněno využití kódu dané metody neoprávněnými přístupujícími entitami. S pomocí entit vstupujících do tohoto mechanismu bude řešeno také jejich předání programovým modulům pro logování (bezpečnostní a výkonnostní monitoring vč. podkladů pro audit), implementovaným v každé metodě, čímž bude zajištěna funkcionality bezpečnostního dohledu.

1.1.5. Databázový model

Na následujícím diagramu jsou zobrazeny základní entity týkající se evidence subjektů a jejich vazby.

Pozn.: Níže uvedené schéma je z pohledu závaznosti Smlouvy ilustrativní (demonstrativní) a vychází ze stávající zkušenosti registru SZR MZe a může se v rámci dokumentu „Návrh realizace“ změnit i rozšířit, bude-li taková změna či rozšíření v souladu s některým požadavkem ZD či Smlouvy nebo její Přílohy, ze kterého toto plnění vychází. Poskytovatel se ovšem zavazuje, že takto koncipovaná databáze, realizovaná pomocí RDBMS, bude součástí dodávky a to v souladu se všemi jejími požadavky.

- Externí identifikátory – pro uložení identifikátorů jako IČO, rodné číslo a dalších agendových identifikátorů.
Státní příslušnosti – kolekce státních příslušností subjektu.
Doklady – kolekce dokladů načítaných ze Základních registrů (například číslo OP, číslo pasu, číslo pobytového štítku, apod.).
- Obchodní jména – kolekce obchodních jmen. Základní registry umožňují evidovat různá obchodní jména subjektu pro různé agendy. Proto jsou obchodní jména evidována v samostatné entitě, aby bylo možné načíst všechna obchodní jména subjektu.
- Kontakty – kolekce kontaktů subjektu včetně evidence datových schránek.
- Vazby – tabulka umožňuje evidovat vazby mezi jednotlivými subjekty (například zákonný zástupce, opatrovník osoby, jednatel společnosti a podobně)
- Rozhodné skutečnosti – tabulky pro evidenci těch skutečností, které popisuje ZD a které mohou upravovat či načítat integrované agendové systémy.

U všech uvedených datových tabulek bude vedena historie všech změn v datech subjektu. Po přesném návrhu databázového modelu v rámci analýzy bude specifikován seznam entit, pro které bude vedena historie a verze změn. Díky tomu bude možné nahlížet na historii údajů subjektu včetně změn vazeb subjektu. Dále vedení historie umožní nahlížet na údaje subjektu, jak byly platné k určitému datu. U všech změn v evidenci subjektů IPPD bude zaznamenána identifikace osoby či procesu, který změnu provedla, případně bude vyznačeno, odkud byla změna načtena (změna ze Základních registrů, změna načtena z jiného externího zdroje, apod.). Na historii údajů a identifikaci, kým byly změny provedeny, bude možné nahlížet skrze uživatelské rozhraní pro správce IPPD.

Výše uvedené entity budou rozšířeny o další entity a atributy dle zadávací dokumentace a požadavků, které vyplynou v rámci analýzy.

Systém IPPD bude evidovat všechny požadované referenční údaje ze Základních registrů (ROB, ROS, odkaz do RÚIAN) a dále údaje nad rámec referenčních údajů, které budou získávány prostřednictvím rozhraní na další externí systémy či interní systémy Objednatele. U údajů, které nejsou načítány ze Základních registrů, umožní systém úpravu na základě písemného ohlášení změny. V systému bude zaevidována písemnost, na základě které byla změna údaje provedena.

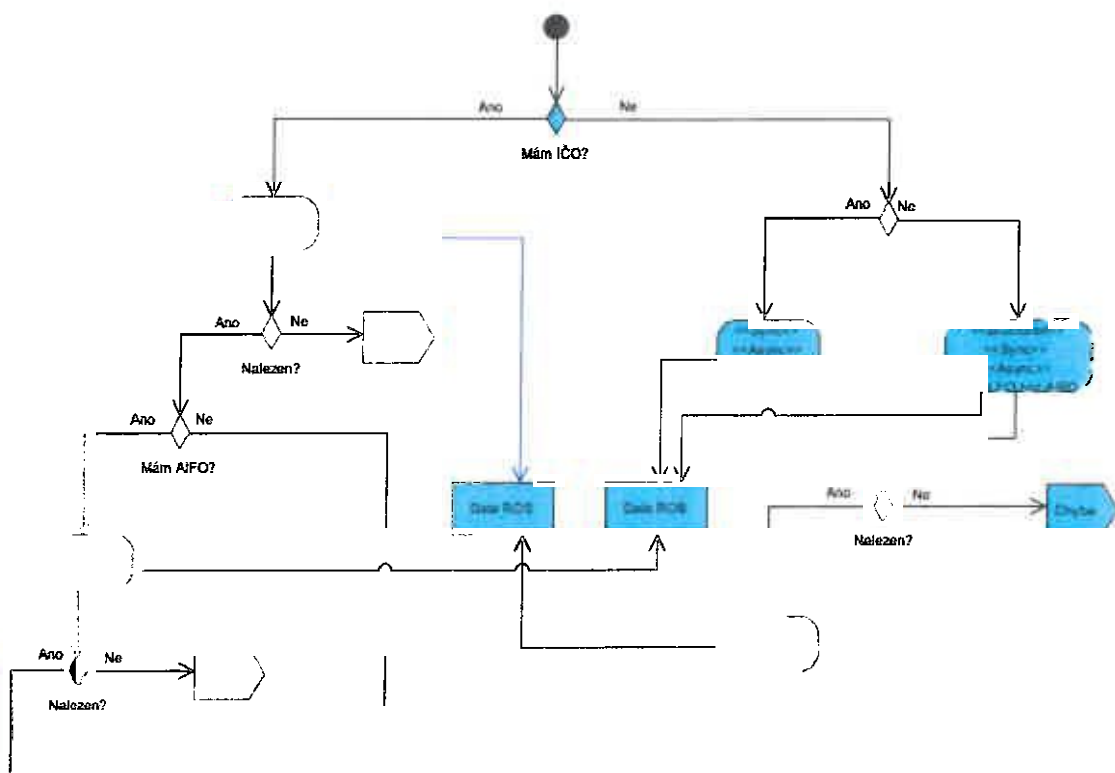
Systém bude pro jednotlivé subjekty evidovat doby zaměstnání a druhy důchodů a to u občanů v rámci EU.

Součástí systému IPPD bude i lokální kopie Registru územní identifikace adres a nemovitostí (RÚIAN). Systém IPPD umožní evidovat i adresy, které v RÚIAN nebudou existovat.

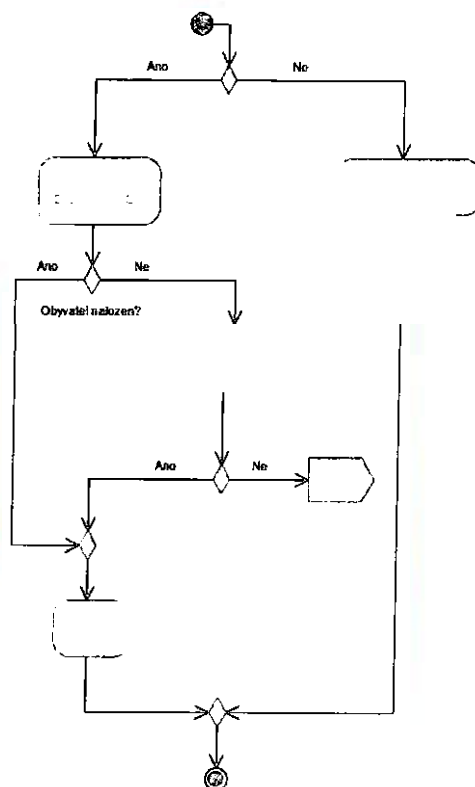
1.1.6. Zakládání subjektu

Zakládání subjektů v SZR realizuje webová služba „subject insert“. Subjekty jsou do SZR zakládány primárně s pomocí Základních registrů, konkrétně Registru obyvatel („ROB“), Registru osob („ROS“), Informačního systému evidence obyvatel („ISEO“) a Cizineckého informačního systému („CIS“). Rozhraní ISEO a CIS je implementováno

Následující diagram ukazuje schéma procesu založení subjektu do evidence s využitím Základních registrů:



Samostatný diagram pak prezentuje založení fyzické osoby v případě, kdy není znám agendový identifikátor fyzické osoby („AIFO“).



V případech, kdy je při zakládání subjektu použito rodné číslo, je volán Informační systém evidence obyvatel, případně Cizinecký informační systém. S pomocí služby „RobCtiPodleUdaju“ je možné získat data subjektu s pomocí jména, příjmení, data narození, kódu adresy a státní příslušnosti. Pro vyhledání službou „RobCtiPodleUdaju“ nemusí být všechny uvedené údaje zadány.

Následuje ukázka dotazu na webovou službu „subject insert“, s pomocí které se zakládají osoby do evidence SZR (jedná se o fiktivní osobu vedenou v testovacích Základních registrech; v ukázce je možné si povšimnout faktu, že SZR je integrováno s pomocí principů integračních sběrnic typu ESB a v implementaci na MZe jejich služeb i aktivně využívá v souvislosti se zajištěním mj. například způsobu volání ISZR a podobně – takové funkcionality mohou být dle požadavků a jejich zakotvení v dokumentu „Návrh realizace“ realizovány i pro Objednatele):


```

<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <soap:Body>
    <ESBServerEnvelopeRes xmlns="http://schemas.xmlsoap.org/soap/envelope/">
      <Service ID="SZR" />
      <Inquirer ID="SZR" CorrelationID="0700092-9700-4200-A000-000000000000"
        Version="0.1" Timestamp="2015-01-23T08:14:05.7613577+01:00"/>
      <SourceSystems>
        <SourceSystem ID="SZR" Version="0.0.0.0" Timestamp="2015-01-23T08:14:05.7613577+01:00"/>
      </SourceSystems>
      <ESBServer CorrelationID="0700092-9700-4200-A000-000000000000" />
      <Data Content="xml">
        <Response xmlns="http://schemas.xmlsoap.org/soap/envelope/">
          <SZR>
            9363164954
            " " 1995-06-06
            " " 163
            " Podnikající fyzická osoba tuzemská
            " " ESOŘICH
            " " ESOŘIVA
            2014-12-11
            " true
            " 2015-01-23T08:14:05.7613577+01:00
            " 67173
          </SZR>
        </Response>
      </Data Content>
    </ESBServerEnvelopeRes>
  </soap:Body>
</soap:Envelope>

```

4

V odpovědi služby pro zakládání subjektů do SZR je u všech elementů uveden atribut „iszr“, který říká, zda se jedná o referenční údaj načítaný ze Základních registrů. Elementy s neplatnou hodnotou atributu „iszr“ pochází z evidence subjektů SZR nebo jsou načítány z jiných nereferenčních systémů, než ze Základních registrů. Elementy s platnou hodnotou atributu „iszr“ jsou přebírány ze Základních registrů a je u nich dále uveden atribut „stav“, který říká, zda je či není daná hodnota v Základních registrech zpochybněna.

Pro již založené subjekty umožňuje služba volání v režimu aktualizace, kdy provede ověření údajů a případnou aktualizaci ze Základních registrů.

1.1.7. Aktualizace subjektů

Evidence subjektů systému IPPD bude sloužit jako primární zdroj v něm evidovaných údajů a proto budou všechny údaje udržované jako aktuální. Aktualizace subjektů ztotožněných se Základními registry je v SZR realizována prostřednictvím výměny informací prostřednictvím patřičných služeb Základních registrů (RobCtiZmeny a RosCtiZmeny). Změnové služby Základních registrů vrací identifikátory AIFO, respektive IČO na základě kterých je vyhledán subjekt v evidenci a následně je aktualizován vůči Základním registrům.

V samotné evidenci subjektů jsou vedeny data a časy změn údajů subjektů. Na základě těchto časů vystavuje změnová služba informace o změnách podřízeným agendám. Tímto způsobem bude systém IPPD zabezpečovat propagaci změn do

podřízených agend. U změnové služby systému IPPD je možné zvážit vstupní parametr, který určí rozsah sledovaných změn. Systémy, které budou čerpat data o subjektech z evidence IPPD budou povinny načítat údaje ze změnové služby IPPD a na jejich základě provádět následnou aktualizaci údajů ve svých agendách.

Konec subkapitoly 1.1. Evidence subjektů a napojení na registry, pokračují subkapitoly z kapitoly 1. Integrovaná podpůrná a provozní data IPPD -

1.2. Sdílené a kompozitní služby

Implementace evidence IPPD nabídne prostřednictvím Integrovaného XML serveru SOAP WS rozhraní (viz. diagram architektury v bodě 1a). Toto rozhraní bude plnit následující účely:

- Rozhraní pro služby Základních registrů
- Rozhraní poskytované třetím stranám na základě oborových zákonů MPSV
- Rozhraní poskytované třetím stranám na základě jiných práv

Přesná specifikace jednotlivých rozhraní bude provedena v rámci fáze analýzy projektu. Rozhraní bude navrženo tak, aby byla umožněna integrace s požadovanými externími i interními systémy a evidencemi. Rozhraní umožní integraci s jinými OVM a to prostřednictvím referenčního rozhraní.

XML integrační server bude prostředníkem komunikace na těchto rozhraních a zabezpečí logování a archivaci dotazů na jednotlivé služby rozhraní. XML server bude provádět dva typy logování:

Systémový log – slouží pro zápis informací, varování a chyb z procesu XML serveru LAR (logování archivace) – pro zápis zpráv a komunikace procházející XML serverem, zpravidla se do LAR zapisuje každý požadavek, transformovaný požadavek na koncový systém, odpověď koncového systému a transformovaná odpověď pro konzumenta. Základním prvkem interní databáze XML serveru (LAR) je tabulka zpráv, která se dále rozšiřuje podle instalovaných modulů.

Log a archiv XML serveru zároveň umožňují monitorování všech dotazů na systém Základních registrů.

Implementace rozhraní bude splňovat následující požadavky na integraci s ostatními systémy a subsystémy:

- Komunikace prostřednictvím HTTP(S), FTP(S) a SMB/CIFS. Pro jednotlivé body rozhraní budou podporované protokoly specifikovány v rámci analýzy.
- Integrace do provozního prostředí Objednatele (včetně provozního a bezpečnostního monitoringu, zálohovacího systému apod.).
- Komunikace s dalšími systémy prostřednictvím ESB.

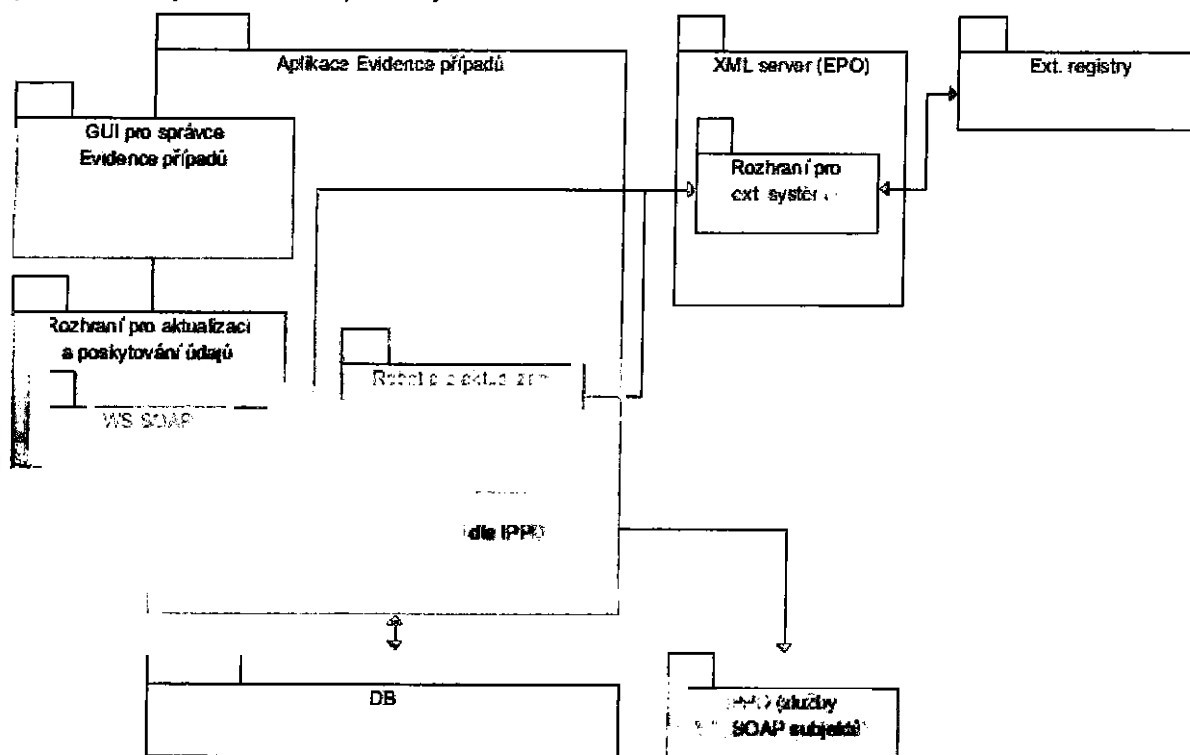
Systém bude pro všechny dotazy na rozhraní vyžadovat patřičná oprávnění. Způsob ověřování autorizace a autentizace u dotazů na rozhraní systému IPPD bude specifikován v analýze.

1.3. Evidence případů

Součástí dodávky bude také systém pro evidenci případů, který bude sloužit k evidenci informací o pravomocných rozhodnutích. Systém bude plně integrován na evidenci IPPD, ze které bude čerpat údaje o subjektech. Systém bude načítat změnové informace o subjektech z evidence subjektů IPPD a promítat je do evidence tak, aby měl neustále platné údaje.

Systém umožní evidovat žádosti, rozhodnutí, údaje o výplatách dávek, předpisy plateb a výplatní kalendáře, exekuční požadavky a rozhodnutí. Rozsah a přesná specifikace evidovaných entit bude popsána v analýze projektu.

V evidenci případů budou udržovány platné a aktuální údaje a tato bude sloužit jako primární zdroj zde evidovaných údajů.



Evidence případů nabídne rozhraní pro ostatní systémy, prostřednictvím kterého umožní zapisovat informace o platných rozhodnutích, jež jsou v danou chvíli v právní moci, ale i o rozhodnutích historických. Dále evidence případů nabídne rozhraní, kterým umožní zjišťovat údaje ostatním systémům. Rozsah a oprávnění přístupu k tomuto rozhraní bude podrobněji specifikováno v rámci analýzy. Rozhraní ale nabídne například informace pro ověření, zda subjekt pobírá nějakou dávku, či zda čerpá nějakou službu ze sociálního systému. V rámci analýzy také bude přesně specifikováno, ze kterých externích registrů bude Evidence případů čerpat údaje.

Uživatelské rozhraní pro správu evidence případů umožní vyhledávání a zobrazení údajů vedených v evidenci. Dále systém umožní v rámci integrace na spisovou službu zobrazení návazných písemností a digitalizovaných dokumentů.

Evidence případů bude poskytovat údaje s historickými konsekvencemi a to v rozsahu, který vyplýne z analýzy. U všech změn v evidenci bude zaznamenána identifikace osoby, která změnu provedla, případně bude zaznamenáno, odkud byla změna načtena (změna načtená z Základních registrů, změna načtená z jiného externího zdroje, apod.). Na historii údajů a identifikaci, kým byly změny provedeny, bude možné nahlížet skrze uživatelské rozhraní Evidence případů.

1.4. Číselníky a datové prvky

Součástí dodávky bude systém pro centrální správu a poskytování číselníků a datových prvků.

Rozhraní pro aktualizaci číselníků

- Bude umožněn import z formátů CSV, XLS a XML. Import bude umožněn pomocí grafického rozhraní. Pokud se v rámci analýzy ukáže jako účelné umožnit import i jiným způsobem, bude umožněn i tento způsob.
- Systém umožní aktualizaci číselníků prostřednictvím SOAP WS rozhraní.
- Rozhraní pro export a poskytování číselníků
 - Bude umožněn export do formátů CSV, XLS a XML. Exportovat bude možné i skupiny číselníků dle výběru a dále bude možné exportovat stav číselníku k určitému datu. Exporty budou dostupné přes grafické uživatelské rozhraní správy číselníků. Zda bude možné exportovat číselníky i jiným způsobem bude specifikováno v analýze.
 - Poskytování číselníků dálkovým přístupem – Poskytovatel zde předpokládá primárně realizaci s pomocí SOAP WS rozhraní. V rámci analýzy bude způsob (či způsoby) tohoto poskytování upřesněn.

Systém bude poskytovat změnové informace k jednotlivým číselníkům tak, aby je konzumentské systémy mohly aktualizovat. S pomocí atributů platností jednotlivých položek bude možné řídit, v jaký časový okamžik budou změny v číselnících zveřejňovány.

Přístup k jednotlivým číselníkům bude řízen oprávněními a to na úroveň jednotlivých položek. Bude možné definovat oprávnění pro čtení, zápis a změnu hodnot. Objednatel bude moci přesným specifikováním skupin (dle modelu oprávnění) a jejich pozitivních práv řídit, k jakým položkám či číselníkům mají jaká oprávnění.

Přesný seznam číselníků, které budou evidovány v centrální databázi číselníků bude specifikován v analýze a bude vycházet ze seznamu v zadávací dokumentaci.

Součástí Centrální databáze číselníků bude také datová struktura, udržující informaci o tom, ve kterých datových prvcích a vstupních polích formulářů jednotlivých modulů jsou jednotlivé číselníky používány.

Ostatní dodávané systémy budou využívat při zadávání údajů výběr z centrální databáze číselníků.

1.5. Komponenta kalendář uživatele

Systém umožní zadávání seznamu různorodých druhů záznamů vázících se k datu a času harmonogramu konkrétního (přihlášeného) uživatele. Jejich součástí budou (pro druh záznamu „jednání“) i mandatorní údaje typu jednání, identifikace klienta (z IPPD), stavu jednání, jeho délky, a uživatelem definované oblasti v návaznosti na hodnoty z číselníků. Mandatorním údajem všech položek bude definice agendy.

Tento seznam bude možné vyfiltrovat podle uvedených mandatorních údajů. V kalendáři uživatele se zobrazí také ty položky, které zadal jeho nadřízený jako skupinové jednání a daného uživatele do něj přiřadil (což bude funkcionality, kterou bude moci udělat každý uživatel na základě výběru ze seznamu svých podřízených).

Zadávat hodnoty data a času každé položky kalendáře bude možné provést z grafického kalendáře nebo přímo zadáním do textového pole.

Kalendář bude možné sdílet konkrétně specifikovanému uživateli a zobrazit plánované události i pro jiné uživatele v rámci identického atributu agendy. Toto zobrazení bude možné s využitím uvedených filtrů měnit. Zda si kalendář zobrazí bude záviset na přihlášeném uživateli, jakýkoliv jiný uživatel (např. nepřihlášený) nebude mít možnost si kalendář zobrazit.

2. Další systémy (Kontroly, Exekuce a insolvence, Agendy právních služeb)

Všeobecné poznámky ke všem systémům a údajům uvedeným v této kapitole:

- Systémy zobrazené jako balíčky nevyplněné (tj. vyplněné bílou barvou) nejsou předmětem dodávky Poskytovatele a představují rozhraní integrovaných systémů (ať již volané nebo volající).
- Systém „Integrační XML Server“ je zástupcem platformy dodávané v rámci zakázky, avšak v konkrétním integračním scénáři se nemusí využít tak, jak je zakreslen v průvodních schématech. Pro integrační scénáře budou existovat v zásadě tato řešení, v závislosti na charakteru a stavu integrovaného systému:
 - Integrovaný systém je napojen na ESB (Integrační Broker, Enterprise Service Bus), tj. integrační sběrnici MPSV vytvářenou v rámci jiného projektu a je s ní plně v souladu. V takovém případě může být integrace provedena:
 - Přímě: tj. Systém bude přes ESB komunikovat přímo (=na úrovni business logiky, nikoliv na úrovni technologické) s daným systémem a moduly systému musejí tuto logiku znát – abstrakce, která má zajistit, aby při změnách integrovaných systémů NEmusel být měněn i vnitřek logiky dodávaného systému, bude provedena na úrovni objektového návrhu aplikace, to neplatí, pokud dojde ke změnám v logice či definici vlastních přenášovaných datových entit takovým způsobem, který musí reflektovat i vnitřní procesy/algoritmy dodávaných systémů či jejich částí.
 - Kompozitně: Systém právních agend bude komunikovat s abstraktním zdrojem dat na ESB, který bude slučovat tato data do jednodílného datového zdroje pro moduly Systém právních agend

POZOR! Součást „XML Server“ v takovém případě nebude součástí daného řešení! Na jejím místě ovšem bude integrační systém „ESB systém“ takže logika postupu zůstane nezměněna.

To platí i pro integraci na ty systémy, které jsou předmětem této dodávky. Zde je v obrazových materiálech zakreslena „přímá vazba“, lze ale odůvodněně očekávat, že tato vazba bude (ať už technologicky nebo i business-logikou) podléhat integračním pravidlům zadavatele a tedy může být realizována s pomocí systému ESB (Integrační sběrnice), což v případě, že bude vyžadováno, také bude.

- Integrovaný systém nebude podléhat řízení MPSV pokud se týká integrace, nebo bude poskytovat data takovým způsobem, který není vhodný a (časově či ekonomicky) efektivní pro implementaci na ESB. Systém „integrační XML server“ v takovém případě převezme tu část práce s integrovaným systémem, kterou nebude

vhodné implementovat na ESB. Systém „Integrační XML Server“ vystaví své služby (zprostředkující komunikaci s integrovaným systémem) do vnitřní sítě MPSV a to tak, že – v návaznosti na integrační politiku Zadavatele – bude s těmito službami komunikovat:

Budto přímo daný dodávaný systém (právních agend, kontroly, IPPD, číselníky a ostatní) – v tom případě bude řešení postaveno přesně tak, jak je na obrázku.

Nebo pouze integrační ESB systém, který teprve zprostředkuje uvedené služby volajícímu dodávanému systému. V tom případě si je nutno na každém obrázku mezi komponentou „XML Server“ a volajícími moduly dodávaného systému představit ještě systém ESB. Jeho zpodobnění je ale z důvodu opakování tohoto principu a zvýšení přehlednosti schémat vynecháno, i když se pak v řešení samozřejmě přenosu dat (a dalších eventuálních operací nad nimi) účastní.

- Je-li uvedeno v názvu balíčku „DB“ jedná se o RDBMS, se kterým aplikace (jak automatizované procesy, tak GUI) komunikuje prostřednictvím odpovídajících protokolů (např. TDS – Tabular Data Stream v případě MS SQL). Tím není dotčena abstrakce uvnitř aplikace, kde je využito technologie ORM na platformě NHibernate, jak popisuje kapitola 3.1. této Přílohy). Tato součást systému je pak z hlediska technologické architektury umístěna jako příslušná databáze na databázových serverech navrhovaných dle technologické architektury uvedené v kap. 1.1.2. **Architektura serverového řešení**
- Má-li být součástí takovéto databáze nějaký číselník z centrální databáze číselníků, není zde integrace na tuto centrální databázi explicitně uváděna, ale samozřejmě bude provedena dle specifikace v dokumentu „Návrh realizace“ v některé s preferovaných možných variant (robotem (pravidelnou dávkovou službou) synchronizovaná kopie, pouze logická vazba s tím, že data číselníku budou vždy získávána odpovídající webovou službou atp.)
- Je-li uvedeno v názvu balíčku „Grafické uživatelské rozhraní“ nebo „GUI“, jedná se o webovou aplikaci zobrazitelnou webovým prohlížečem dle specifikace (nebude-li v rámci analýzy zjištěno, že je vhodnější pro danou část/aplikaci/modul klientské rozhraní jiné). Webové aplikace a jejich rozhraní budou ve všech případech odpovídat všem požadavkům specifikovaným v ZD stejně jako v této Smlouvě a jejich přílohách. Toto rozhraní z balíčku aplikace částečně „vystupuje“, čímž je naznačeno, že se jedná o součást aplikace fungující směrem k uživateli a kde je část funkcionality (v souladu s kapitolou 3.1. této Přílohy) přenesena do technologií na straně webového prohlížeče (vykreslování zadaných ovládacích prvků, některé druhy validací, některé interaktivní funkce, vložené objekty atp.). Tato součást systémů níže popsanych v této kapitole je pak z hlediska technologické architektury umístěna jako aplikace IIS na aplikačních serverech kódového jména „Právní agendy“ (ale to se týká i Kontrol a Exekucí/insolvencí) navrhovaných dle technologické architektury uvedené v kap. 1.1.2. **Architektura serverového řešení** a to jako serverové aplikace IIS s výstupem určeným pro webové prohlížeče. Takové části řešení GUI pak také přímo spoléhají na funkcionality platformy klientského prohlížeče na jednotlivých klientských stanicích uživatelů. Pro přehlednost byla ale tato část ze schématu vypuštěna, neboť klientské stanice ani jejich prohlížeče nejsou (s výjimkou SK0007) součástí dodávky a ani řešení, mimoto veškeré součásti dodávky jsou implementovány na serverech a do prohlížečů se dostávají běžnými již existujícími a u Objednatele provozovanými mechanismy HTTP(S), URL/URI atp.

Takovéto rozhraní GUI vždy – není-li nakreslen specifický konektor – komunikuje přímo s databází dané aplikace (pro přehlednost nejsou konektory do DB vedeny od jednotlivých vnitřních modulů, ale od GUI jako celku).

- Je-li uvedeno v názvu balíčku „Rozhraní“ (bez přízviska „grafické/grafický“) který je součástí balíčku (řešení) „XML Server“, pak se jedná o standardizovanou WS SOAP, která v případě jejího napojení na ESB systém (viz výše) odpovídá i požadavkům tohoto ESB systému. Na druhé (externí) straně pak splňuje ty požadavky integrovaného systému, které integrovaný systém na své spojení klade. Tím není dotčena možnost jiného provedení integrace (viz výše v tomto seznamu odrážek). Tato součást systémů níže popsanych v této kapitole je pak z hlediska technologické architektury umístěna jako aplikace IIS na aplikačních serverech kódového jména „XML server“ navrhovaných dle technologické architektury uvedené v kap. 1.1.2. **Architektura serverového řešení** a to jako kombinace serverové aplikace IIS s výstupem určeným pro libovolné ale zpravidla automatizované (bezobslužné) SW či HW prostředky nebo dávkové automaty (roboty) v souladu s požadavky integrace. Toto se netýká „EPO – XML služby“, kdy bude vždy použito XML Serveru a některých jeho vlastností „Elektronické podatelny“ (viz 2.2. Exekuce, insolvence)

Nesplňuje-li balíček žádnou z výše uvedených podmínek a je-li umístěn uvnitř zastřešujícího „balíčku“ (aplikace), pak se jedná o automatizovanou službu (tzv. robota) provádějícího pravidelné dávkové operace v daném systému tak, jak je požadováno. Takovýto robot má vždy ve svém názvu slovo slovesného původu jako „Monitoring“, „Aktualizace“, „Aktualizátor“, „Výpočet“, „Notifikátor“, „Robot“ atp. Tato součást systémů níže popsanych v této kapitole je pak z hlediska technologické architektury umístěna jako samostatná aplikace (eventuálně jako aplikace v podobě „Služby“ tak, jak ji chápe terminologie „OS Windows“) na aplikačních serverech navrhovaných dle technologické architektury uvedené v kap. 1.1.2. **Architektura serverového řešení** a to jako binární (MSIL) aplikace platformy Microsoft .NET.

- Směr šipek na schématech uvedených v této kapitole pouze naznačuje logickou nebo technologickou komunikaci a není v této Příloze vymezující pro dané řešení jinak, než jako vazba ilustrující tok dat a/nebo spoluúčast/spolupráci jednotlivých částí systému na daném úkolu (tj. kdo co volá, odkud čte data, kam je zapisuje).

Následující jednotlivé sub-kapitoly uvádějí již jen specifické vlastnosti jednotlivých uvedených součástí dodávky (Díla), k jejichž realizaci se Poskytovatel zavazuje zcela v souladu se ZD a Smlouvou. Na všechny se ovšem vztahují ty všeobecné poznámky, které jsou uvedeny v seznamu odrážek nad tímto odstavcem.

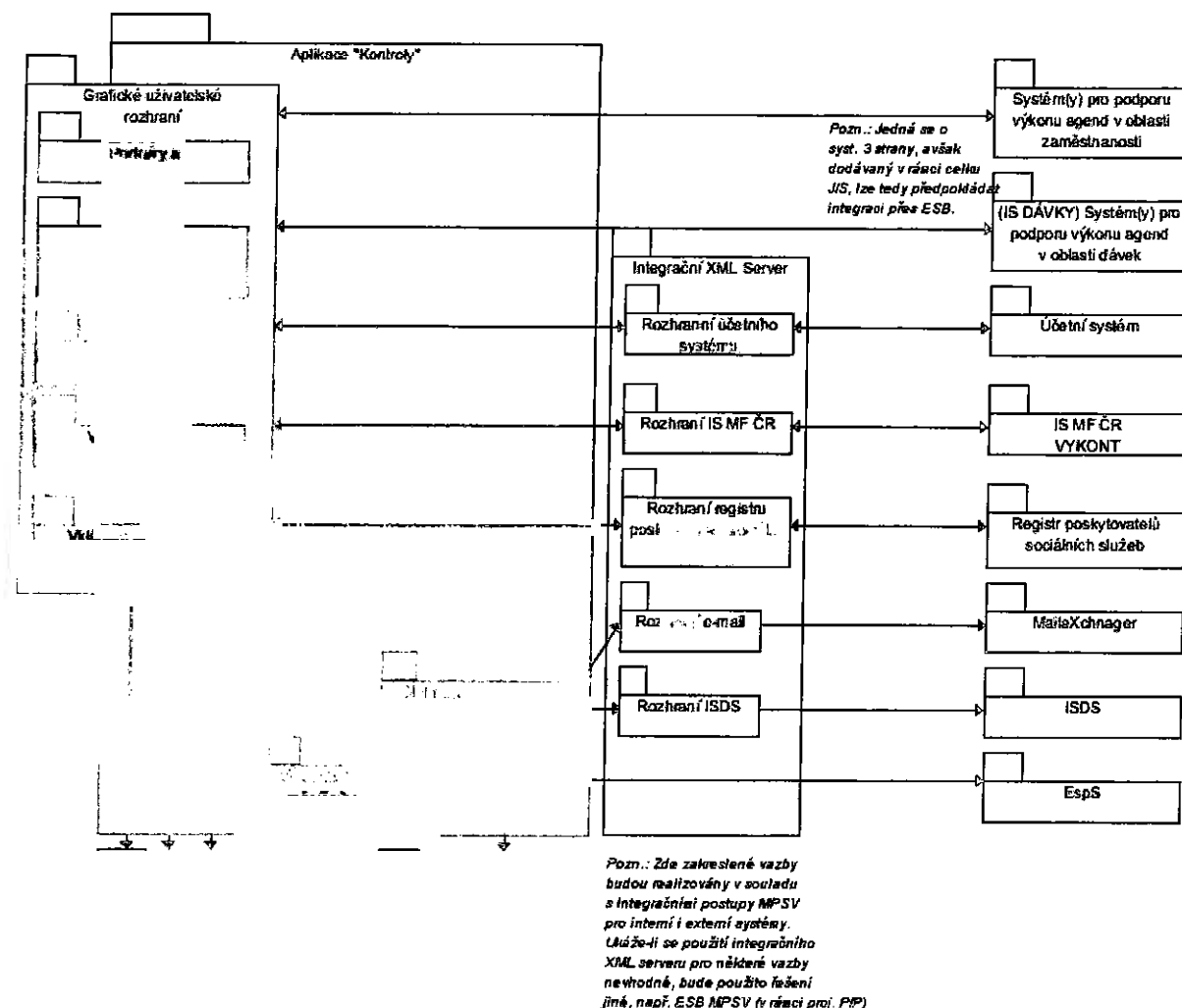
Systémy těchto níže uvedených agend všeobecně, tam kde to bude v rámci analýzy „Návrhu realizace“ specifikováno jako k dané problematice jako relevantní, budou integrován na externí systémy (jediný úřad pro postoupení pohledávek, insolvenční rejstřík pro kontroly a načtení insolvenčních řízení dlužníků, INFOSUD pro načítání informací o soudních sporech identifikovaných dle IČO, ČSSZ za účelem získávání dat o dalších postižitelných příjmech, o zaměstnavateli nebo údaje OSVČ, centrální registr vozidel a katastr nemovitostí pro získávání údajů o vlastněných nemovitostech a vozidlech formou dotazu).

2.1. Kontroly

Provedení systému „Kontroly“ je určeno pro splnění podpory obchodního procesu (business proces) výkonu kontrolní činnosti ÚP ČR a dalších věcných útvarů, které vykonávají kontrolní činnost.

Funkcionalita níže uvedených částí bude v souladu se zákony a vyhláškami uvedenými v kap. 2.2.2.4.1. Přílohy č. 6 ZD.

Logická architektura systému bude navržena následovně:



Aplikace Kontroly, stejně jako následující aplikace v této kapitole, bude aplikací třívrstvou, tedy aplikační logika v podobě webové aplikace bude umístěna na aplikačním (webovém) serveru, kde veškerá aplikační logika je zakódována a provozována v rámci této platformy (webových serverů) a do klientského prohlížeče jsou k provedení/vykreslení adresářů pouze ty části aplikační logiky a dat či metadat, které slouží pro vykreslování a poskytování stupeň interaktivity práce na klientské stanici. Na aplikačním serveru se pak budou také nacházet některé automatizované dávkové procesy (zkráceně „roboti“), jejichž úkolem je provádění pravidelných dávkových úloh takového charakteru, kdy je nutné procházet větší množství dat z nějakého datového zdroje větu po větě a na základě hodnot v těchto větách uvedených dále reagovat (například i prací s dalšími datovými zdroji).

Systém bude v grafickém uživatelském rozhraní poskytovat možnosti pro:

- Podněty a jejich příjem, zobrazení/vyhledání/filtrování a vypořádání (včetně zařazení do kategorií)
- Kontroly a jejich zadávání, zobrazování/vyhledávání/filtrování, zadávání informací k jejich provádění (postupu), opatření k nápravě, ukládání pokut a evidenci pověření ke kontrole v rámci ÚP ČR (číselná řada).
- Ke každé kontrole bude možné zadávat údaje postupu pro specifikované fáze v souladu s odpovídající legislativou a umožní evidovat spolu související řízení. Zobrazení (v seznamu i detailů) a možnosti editace kontrol budou filtrovány nejen na základě předmětu kontroly ale také dle oprávnění jednotlivých ÚP ke kontrolám daného typu.
- Pro výše uvedené funkcionality bude v rámci dat s nimi souvisejících využívat údaje společné Evidence subjektů
- Pro kontroly umožní sestavovat plán kontrol dle typů a oblastí kontrol a jejich konsolidaci tak, jak jsou sbírány na KOP a krajských pobočkách a GŘ ÚP ČR a to včetně aktualizace.
- Modul statistik umožní výpočet počtů jednotlivých datových entit dle specifikace a to v agregaci na v požadavku specifikované úrovni pracovišť ÚP.
Informace dle specifikace v analýze Návrhu realizace bude možné vkládat také pomocí tabulek. V analýze specifikované informace bude možné konvertovat do MS Word a PDF.

Systém bude obsahovat robota pro periodické monitorování Objednatelem v rámci analýzy specifikovaných dat ze specifikovaných datových zdrojů pro výpočet průměrného měsíčního čistého výdělku na základě Objednatelem daných algoritmů. Tyto údaje bude ukládat v rámci DB Kontroly.

Stejně tak bude notifikátor notifikovat uživatele o zvolených typech událostí a to vybranými možnými komunikačními kanály.

Pro ty kontroly, ke kterým byly již zadány výsledky, bude provádět automatický robot předání těchto zjištění věcným útvarům ÚP (jejich věcná příslušnost bude specifikována v rámci analýzy.

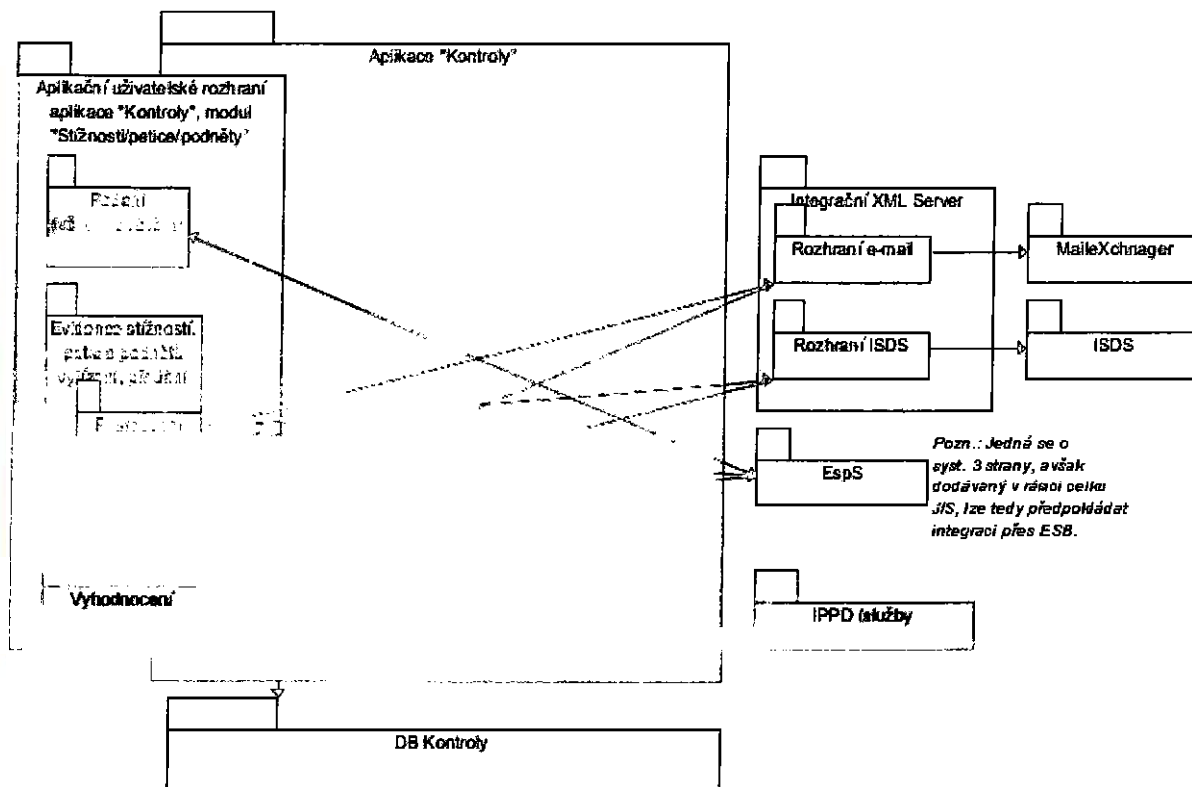
Pokud se týká modulu (součásti) systému Právních agend, odpovědného za evidenci pohledávek, bude tento – způsobem jak je uvedeno níže v souladu se specifickými požadavky na tento systém – integrován na všechny oblasti, v nichž vznikají pohledávky EKIS.

Tam, kde bude relevantní přikládání dokumentů k jednotlivým soudním sporům, bude možné ukládat tyto dokumenty prostřednictvím a do Elektronické spisové služby (ESPS) a nebo také přidávat vazby na dokumenty stávající. Pro poskytnutí informace (při zobrazení údajů soudního sporu) nebo tvorbě vazby na dokument (při editaci údajů soudního sporu) umožní systém vyhledávání podkladů a to s pomocí různých způsobů filtrování zobrazených sestav při vyhledávání dokumentů.

Ty části systému, kterých se dotýkají požadavky na přehledové sestavy a kombinované výběry, je budou poskytovat, stejně jako s možností jejich exportů (či jejich vybraných částí)

do formátu vhodného pro zpracování v MS Excel (např. CSV) a to ze všech disponibilních dat systémů níže kategorizovaných v souladu se strukturou požadavků ZD jako součásti aplikace „Právní služby“.

2.1.1. Stížnosti, petice, podněty



Pozn.: V této kapitole je za účelem dosažení souladu se ZD a hodnotitelnosti nabídky využito stejné dělení, jako v ZD a to včetně obrazových materiálů. Ačkoliv pro „Stížnosti, petice a podněty“ je pro lepší přehlednost zobrazeno oddělené schéma, bude se jednat o jeden systém a jeho různé moduly.

Součástí aplikace kontroly je i evidence dalších podnětů než těch, které vstupují do aplikace Kontrola. Jedná se jmenovitě o stížnosti, petice a podněty. Tyto budou vstupovat do aplikace primárně skrz podatelnu spisové služby (odkud mohou být získávány ať už např. pollingem nějaké služby nebo naopak voláním zpřístupněných služeb aplikace „Kontrola“ spisovou službou). Aplikace „Kontrola“ povede evidenci těchto stížností/petic/podnětů a v kooperaci se službami IPPD k nim bude schopen ztotožnit jejich pisatele, podle jehož identifikace pak bude schopen prohledávat systémy.

Tyto stížnosti/podněty/petice bude možné v systému aplikace Kontrola zpracovávat v tom smyslu, že bude možné je buďto předat (postoupení v souladu se spisovým a skartačním řádem a dalšími požadavky Objednatele) nebo stejným způsobem odbavené vyrozumění o prošetření či stanovisku (zde je nutno v souladu s druhou a třetí větou POD0060 podotknout, že systém umožní využití všech (druhů) kontaktů uložených u daného subjektu v IPPD a podporovat jejich odeslání s využitím služeb infrastruktury zadavatele –ilustrace těch součástí, které systém má již implementované, avšak také závisejí na dostupných

službách infrastruktury Zadavatele, je k vidění na schématu výše, tím není dotčena implementace podpory ostatních kanálů v souladu s POD0060).

V návaznosti na datové atributy jednotlivých stížností/petic/podnětů, bude možné statisticky vyhodnocovat dle těchto datových atributů jednotlivých záznamů tak, jak bude definováno v analýze Návrhu realizace (pozn.: potřebou explicitní specifikace ovšem není dotčeno splnění požadavku POD0037 neboť specifikovány mohou být jakékoliv, tj. „všechny“ dostupné parametry, ani dalších relevantních požadavků ZD).

Přístupová oprávnění (tj. filtrace seznamu a možností operací nad jednotlivými položkami) se budou lišit v návaznosti na příslušnost uživatele ke skupinám/rolím (dle modelu autorizačních informací) a typu dané stížnosti/petice/podnětu.

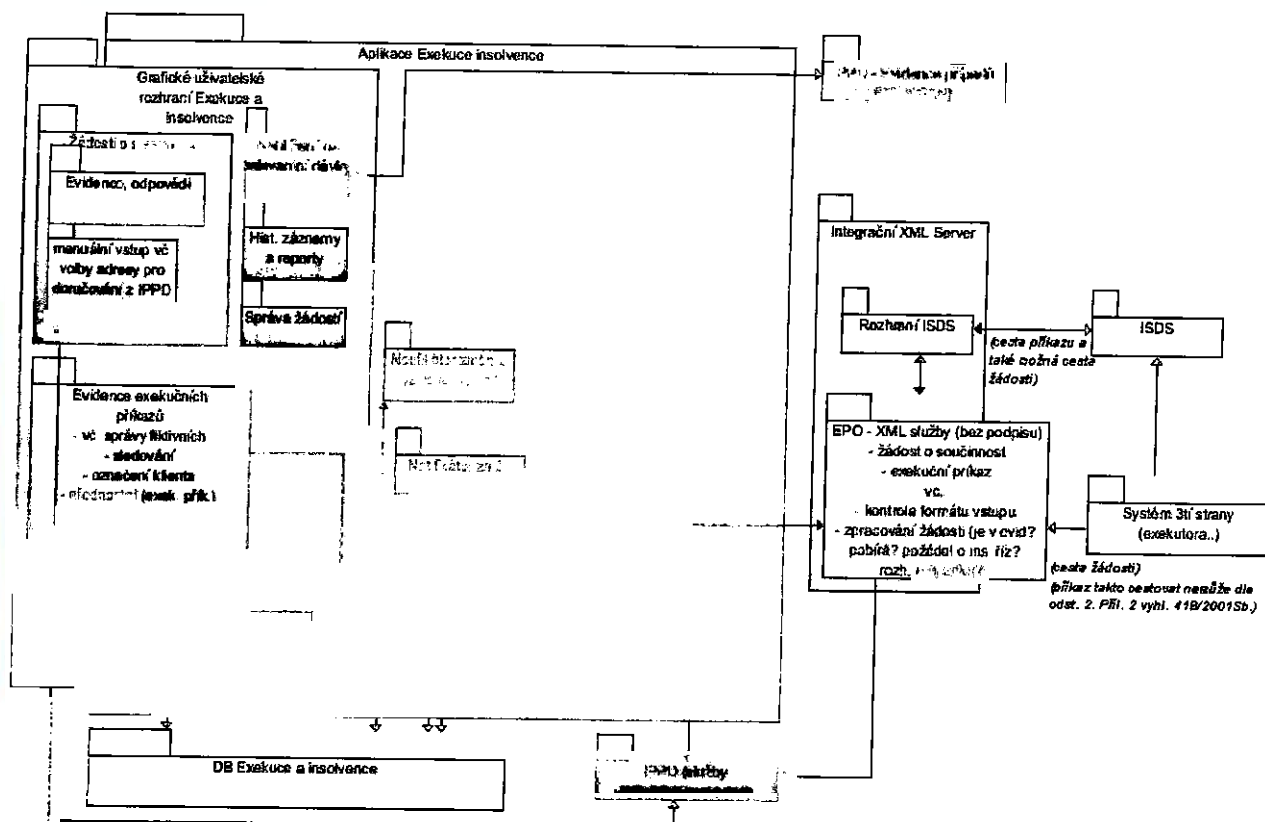
2.2. Exekuce, insolvence

Tento systém je určen pro plnou podporu cyklu exekučních příkazů nad subjekty (klienty), kde se tyto exekuce dotýkají plateb a/nebo pohledávek Objednatele pro tyto / za těmito subjekty (klienty) a to takovým způsobem, aby prováděné srážky/pohledávané částky současně vyhověly všem v ZD uváděným a navazujícím legislativním předpisům týkajících se sociální politiky ČR.

Systém aplikace „Exekuce, insolvence“ se tak bude skládat ze dvou větších celků:

- Evidence (vč. příjmu a zpracování) žádostí o součinnost a exekučních příkazů a to jak elektronicky i manuálně a to včetně jejich správy (i fiktivních) sledování, označení přednostních atp. v souladu s požadavky
- Exekuce výplat, využívající nejen funkcí evidence exekučních příkazů, ale také provádějící evidenci a zpracování realizace srážek (při spolupráci s informačními systémy IS DÁVEK), přihlašování těchto pohledávek atp. a také evidenci a administraci výplat a deponací těchto srážek ve prospěch jednotlivých exekučních příkazů. Toto provádění výplat a deponací bude systém řešit v závislosti na provedeném zadání srážek automatizovaně v kooperaci se specifikovaným externím systémem (externími systémy).

2.2.1. Příjem a zpracování žádosti



Základním vstupem do systému bude vstup v podobě:

- Žádosti o součinnost
- Exekučního příkazu

Výše uvedené vstupy budou do systému vstupovat:

Skrze WS SOAP služby integračního XML serveru, zde v roli elektronické podatelny

Skrze rozhraní (vč. robotů pollingu datové schránky MPSV atp.) ISDS integračního XML server

- (obě výše uvedená rozhraní při přijetí požadavku ve strukturovaném formátu dle §5a + přílohy č. 2 vyhl. 418/2001 Sb. provedou jeho validaci, tj. kontrolu formátu vstupu, a z databáze aplikace „Exekuce a insolvence“ a IPPD po ztotožnění subjektů vyhodnotí pro dlužníka požadované stavy(*) včetně rozhodných skutečností, které vedou v přímé automatizované odpovědi Exekutorovi)

*) zda je či není v evidenci, zda pobírá nějaké dávky, nebo se nachází v nějakém stavu insolvenčního řízení či bylo již rozhodnuto o jeho úpadku

- Skrze rozhraní pro evidenci žádostí o součinnost – manuálním zadání
- Na výše uvedené žádosti umožní systém v rámci jejich evidence připravit odpověď s pomocí načtení údajů z Evidence případů.

Systém bude pro práci s exekučními příkazy poskytovat evidenci exekučních příkazů a evidenci žádostí o součinnost, kde z druhé jmenované bude také možné připravit odpověď na každou jednu tuto žádost, a to na základě načtených informací o klientovi z Evidence případů. Z první jmenované evidence bude možné také nahlížení do této Evidence případů na data stavu žádostí o dávky. K subjektu (klientovi), který je již nějakým způsobem účasten evidencí žádostí či exekucí, bude systém notifikovat (v analýze určeným způsobem v souladu

Evidence exekučních příkazů pak bude podporovat všechny stavy (a s nimi bezprostředně související požadované funkce) jednotlivých exekučních příkazů a to včetně možnosti zadání i fiktivních exekučních příkazů, sledování exekuce jako takové po nezbytnou zákonnou dobu (dle POD0232) označení klienta s podaným Oznámením o zahájení insolvenčního řízení, možností zavedení přednostního exekučního příkazu, evidenci příznaků „řádné ukončení“ a „předčasné ukončení“ či pozastavení, a nebo znovuoobnovení realizace srážek a načtení exekučních příkazů z insolvenčního rejstříku MF ČR.

Modul realizace srážek nabídne přehled a správu srážek v rámci exekučních příkazů včetně jejich pozastavení či obnovení a náhledu plánovaných srážek na příští měsíc.

Tento modul také umožní v integraci na Právní služby a rozhraní ISDS (či Spisovou službu) provedení přihlášky pohledávky ÚP, kterou nejen odešle insolvenčnímu soudu (přes ISDS či zvolený jiný kanál) ale také ji automaticky zaregistruje do modulu Správa pohledávek.

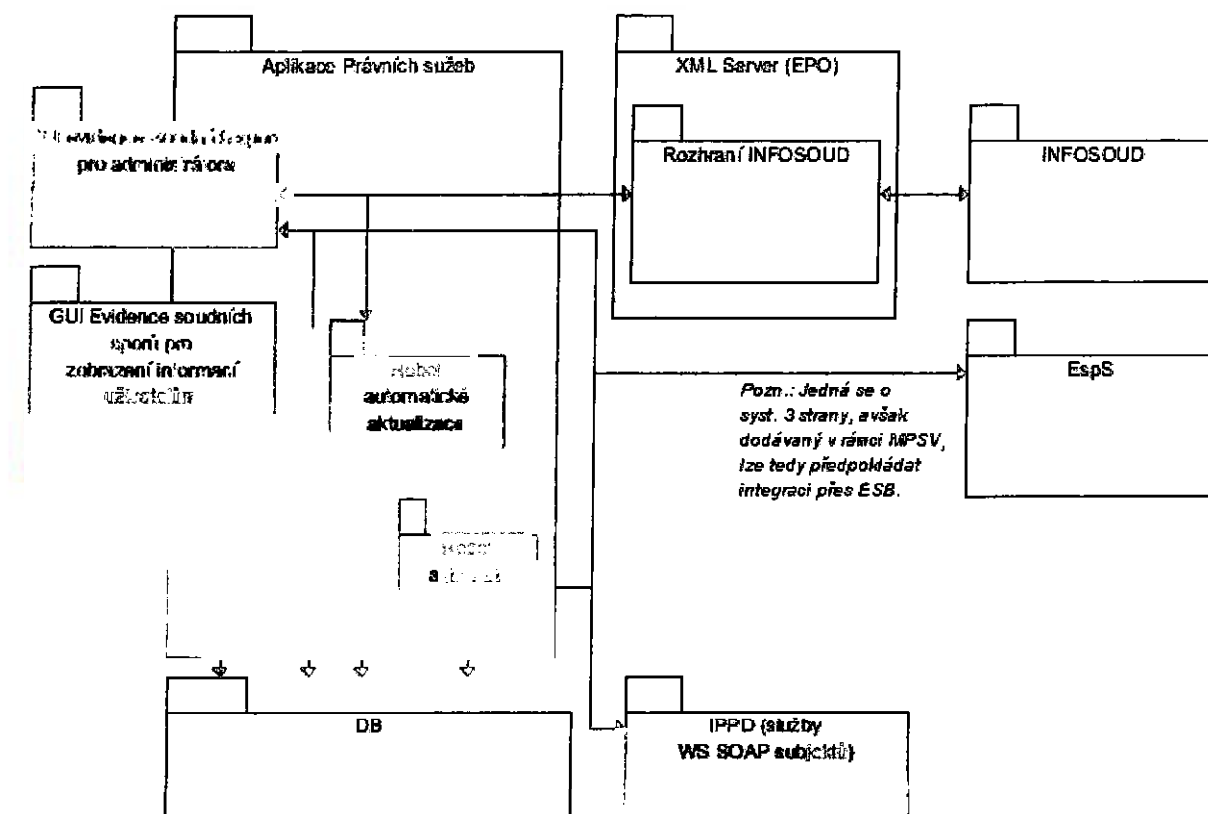
Automatizovaný robot pak zajistí provádění výplat částek ve prospěch exekučních příkazů, včetně automatického pozastavení (spravovatelné dále přes grafické rozhraní evidence výplat), a nebo zpětného proplacení deponovaných částek v případě změny stavu insolvenčního návrhu.

2.3. Systém právních agend

Pozn.: V této kapitole je za účelem dosažení souladu se ZD a snazší hodnotitelnosti Přílohy v rámci nabídky využito stejné dělení, jako v ZD a to včetně obrazových materiálů. Ačkoliv jsou tyto rozděleny, bude se jednat o jeden systém a jeho různé moduly.

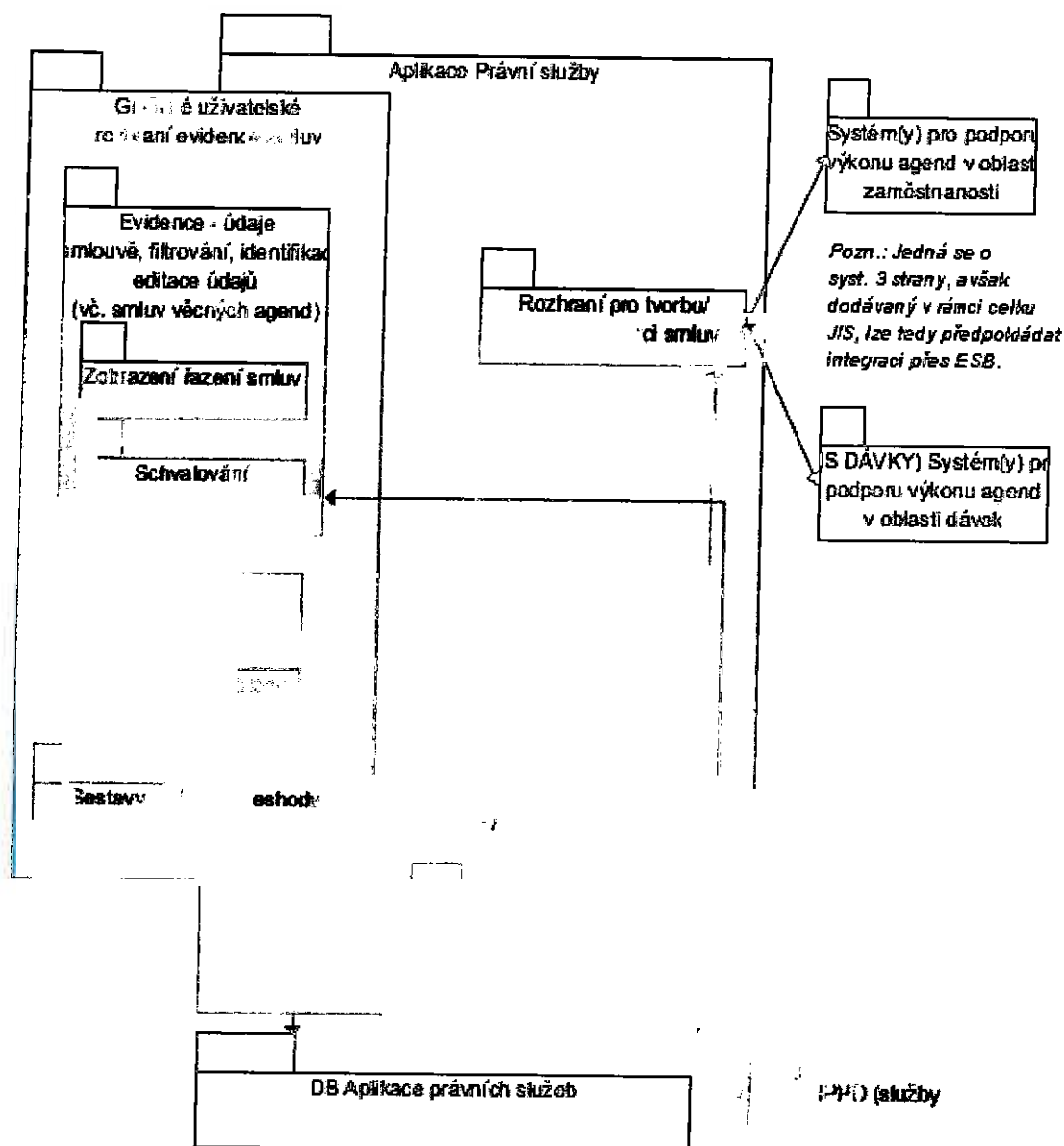
Tam, kde je v obrazových materiálech v této nabídce nějaký element/součást systému/modul rozdělen (tj. zobrazen jako dvě různé entity) a během analýzy či i přímo vývoje se ukáže jako účelné jeho technologické a/nebo logické sloučení, bude toto provedeno.

2.3.1. Evidence soudních sporů



Tato součást systému aplikace „Právní služby“ bude určena pro jednoduchou evidenci soudních sporů, kde je jedním z účastníků subjekt Objednatele. Cílem systému aplikace bude evidence soudních sporů (ať již manuálním zadáním, nebo načtením či spárováním dle pravidel určeným v analýze s údaji z aplikace INFOSUD, na základě převzetí informace z INFOSUD dle IČO) a jejich zpřístupnění oprávněným uživatelům organizací rezortu. Další skupina oprávněných uživatelů pak bude mít možnost filtrovat, zobrazovat a editovat údaje o soudních sporech (včetně možnosti editace stavu, nezávisle na stavu přebíraném z INFOSUD a včetně možnosti editovat další doplňující údaje, které do struktury evidence přidá administrátor) a také je mezi sebou navzájem spárovávat. Evidované soudní spory bude také možné provázat s odpovídajícími dokumenty ze spisové služby.

2.3.2. Přehled o aplikaci



Pro evidenci subjektů ve vztazích organizace resortu v rámci smluvních vztahů bude existovat systém Evidence smluv. Tento systém umožní nejen jejich evidenci (vyhledávání, filtrování a editaci údajů záznamů jejich evidence) za použití společné Evidence subjektů (IPPD) pro identifikaci smluvních stran, ale také umožní vytvářet, spravovat a archivovat smlouvy připravované i na základě podnětu jednotlivých věcných agend z oblasti zaměstnanosti i dávek. Systém bude pro vybraného partnera resortu umožňovat zobrazení všech smluv a dodatků a dalších v analýze definovaných skutečností ve formě grafického stromu s možností tisku a exportu.

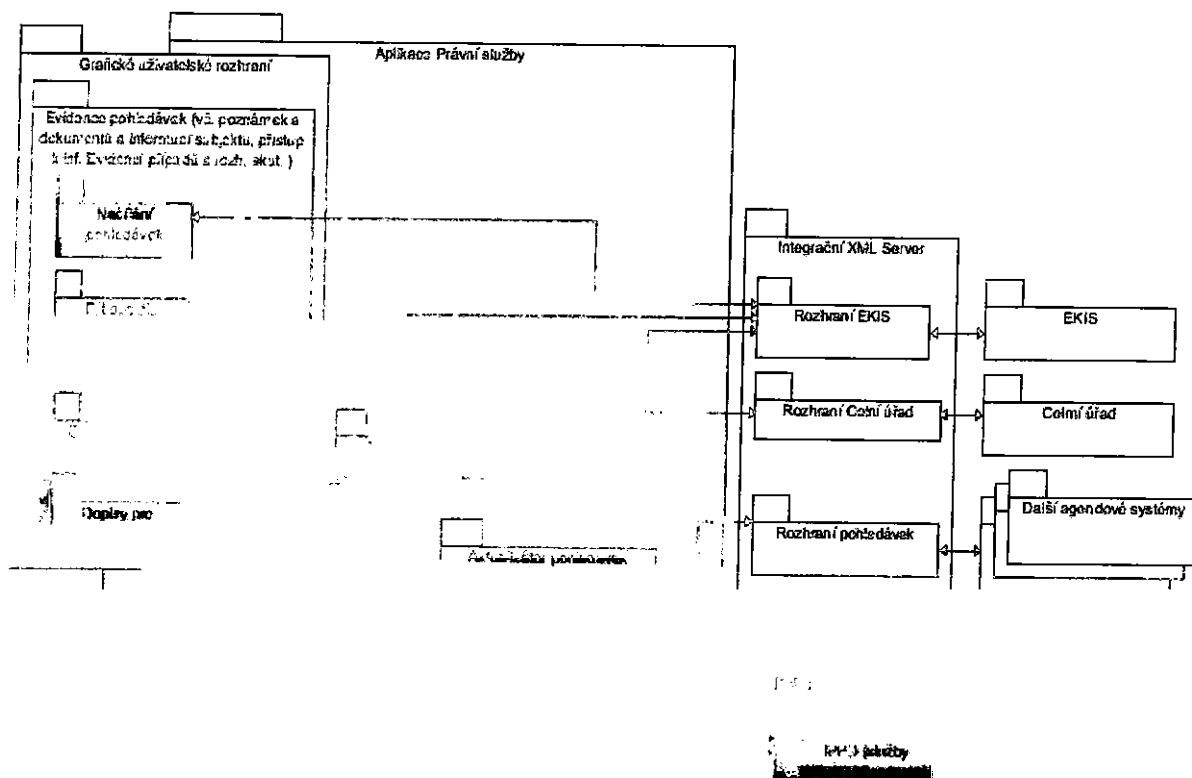
Pro každou organizaci resortu využívající tento systém bude definován postup schvalování. Systém k tomu nabídne rozhraní pro jeho editaci na úrovni rolí či uživatelů (dle architektury bezpečnostního modelu) administrátorem za danou organizaci resortu. S využitím šablon bude možné v systému vytvářet verzované dokumenty. Kromě originálních dokumentů v elektronické podobě bude možné ukládat také jejich skenované podepsané ekvivalenty ve formátu PDF

Automatický robot bude dle pravidel zakotvených v analýze „Návrhu realizace“ verifikovat termíny a zadané údaje a o jejich neshodách informovat v analýze zvolenou cestou (v souladu s POD0060 tak je to například u notifikátoru v kap. 2.1.1). Termíny budou u každého evidovaného záznamu smlouvy libovolně definovatelné.

Přístup k vlastním smlouvám bude pak nastavitelný správcem za danou organizaci resortu až na úroveň jednotlivých uživatelů resortu v závislosti na to, pod kterou organizaci resortu smlouva spadá.

V rámci výstupů sestav a přehledů bude možné zobrazit (vyfiltrovat) přehledy smluv platných k určitému datu, uzavřených s určitým zvoleným subjektem, platných po daném datu, dle jejich typů a kategorií. (Pozn.: vybraná pevná položka jinak variabilního seznamu termínů smluv, která bude v tomto vyhledávání použita jako datum platnosti bude určena v rámci analýz „Návrhu řešení“)

2.3.3. Správa pohledávek



Vedení evidence pohledávek (včetně vytváření historie dat v souladu s dalšími požadavky ZD) a to včetně jejich načítání a spárovávání s údaji z EKIS (tj. stažení v pravidelných časových intervalech údaje typ, výše, dlužník a datum splatnosti a následné úpravy stavu pohledávky, vč. evidence vzniku přeplatku a uložených pokut). Tyto pohledávky bude moci převzít právní odbor a dále je zpracovat (tj. vyhotovit výkaz nedoplatků podle daňového řádu a postoupí je celnímu úřadu k vymáhání nebo k vlastnímu vymáhání, takové informace bude opět zpětně zavedena do EKIS, pokud to systém EKIS umožní).

Specifikem tohoto systému bude pravidelná aktualizace (prováděná Aktualizátorem pohledávek) pohledávek nejen z EKIS, ale také z rozhraní Evidence rozhodných skutečností IPPD ale i z širší sady (určené v analýze) dalších agentových systémů. Za tímto účelem pro splnění požadavku POD0280 bude v rámci Integračního XML Serveru implementována univerzální služba (univerzální svým konstantním rozhraním dovnitř rezortu, tedy vůči apl. Právní služby a eventuálně i využitě ESB), která zprostředkuje dovnitř rezortu konzistentní spojení s jednotlivými dalšími agendovými systémy, evidujícími pohledávky či jejich atributy (to neplatí v případě, kdy by charakter přístupu k danému agendovému systému znemožňoval implementaci procesního modelu zvoleného pro toto rozhraní).

Informace evidované k dané pohledávce v Evidenci případů, Evidenci rozhodných skutečností a o subjektu z Evidence subjektů budou systémem zpřístupněny.

Součástí systému bude i automat na monitorování lhůt jednotlivých pohledávek, včetně upozornění (v souladu s POD0060 tak je to například u notifikátoru v kap. 2.1.1) v případě jejich uplynutí.

3. Obecné požadavky na systémy JISPSV

3.1. Použité technologie, požadavky na uživatelská rozhraní a architektura

Uživatelské rozhraní systémů bude implementováno jako webové aplikace postavené na technologiích Microsoft .NET framework. Pro vývoj těchto aplikací bude dále využito následujících technologií:

ASP .NET MVC

jQuery, jQuery UI, jqGrid

NHibernate

Vybraná platforma umožňuje zajištění škálovatelnosti a zabezpečení vysoké dostupnosti bez ztráty kontextu v případě výpadku. Blíže popsáno v kapitole **1.1.2 Architektura serverového řešení**. Platforma také umožňuje u aplikační a prezentační logiky využít souběžného zpracování požadavků více vláken.

S ohledem na plánovanou architekturu aplikací bude pro práci s databází vyžit ORM systém, který bude dále zabezpečovat i automatické zápisy do historie. V místech, kde by využití ORM mohlo ohrozit dodržení reakční doby systému, bude načítání dat optimalizováno. Způsob těchto optimalizací se může v jednotlivých případech lišit. Možnosti optimalizací budou specifikovány v analýze. Využití ORM nabízí nezávislost na variantě databázového systému.

Grafické zpracování uživatelských rozhraní systémů bude podléhat grafickému manuálu Objednatel a bude řešeno s pomocí responzivního vzhledu.

Další parametry uživatelských rozhraní:

- Aplikace budou řešeny jako webové, ovládání tedy bude obdobné běžným zvyklostem při ovládání webových aplikací.
- Webové aplikace z principu umožňují spuštění více instancí jedné aplikace na jedné pracovní stanici, jak je požadováno v zadávací dokumentaci. Dodávané aplikace to tedy budou umožňovat.

- Vzhledem k využití webových technologií bude síťový přenos realizován prostřednictvím http, případně šifrovaného http protokolu prostřednictvím síťového protokolu TCP.
- Responzivní design webových aplikací nabízí možnost pracovat s aplikací i na tabletech a obdobných zařízeních. V rámci analýzy bude specifikována míra podpory těchto zařízení.

Formuláře v aplikacích budou obsahovat validační mechanismy a to jak na straně klienta (u položek, u kterých to bude možné), tak na straně serveru. Vstupní pole ve formuláři budou v případě chyby zvýrazněna a na vhodném místě bude výrazně zobrazen text vysvětlující chybu.

- Při implementaci vyhledávání bude v místech, kde se to v rámci analýzy ukáže jako účelné, využito podobnostní vyhledávání založené na databázové funkci SOUNDEX. Podobnostní vyhledávání bude také využito s ohledem na výkonnostní požadavky na systém.
- Výběr kalendářního data bude uživatelským rozhraní řešen s ohledem na požadavek UR008 v zadávací dokumentaci.
Aktualizace údajů bude vždy, když to bude možné, probíhat asynchronně.
Texty v uživatelských rozhraních budou vypisovány s ohledem na případnou lokalizaci do více jazyků.
V jednotlivých částech aplikací bude k dispozici kontextová nápověda. Kontextová nápověda bude i u jednotlivých vstupních polí. Přesný rozsah nápovědy v systémech bude specifikován v analýze daných systémů.
- Veřejné části uživatelských rozhraní systémů budou vyhovovat „vyhláše o přístupnosti“, kterou vymezuje „Předpis č. 64/2008 Sb. – Vyhláška o formě uveřejňování informací souvisejících s výkonem veřejné správy prostřednictvím webových stránek pro osoby se zdravotním postižením“.
- V místech, kde to bude účelné, bude využito našeptávače pro zrychlení zadávání hodnot.
- Systémy v případech, kdy to bude vyžadováno a bude to vhodné, umožní uživateli vlastní nastavení uživatelského rozhraní. Rozsah a přesná specifikace nastavení uživatelských rozhraní bude uvedena v analýze jednotlivých systémů.
- Uživatelská rozhraní systémů budou nabízet možnost úplného a bezpečného odhlášení uživatele.

Dodávané systémy budou dále splňovat následující požadavky na architekturu řešení:

Architektura klient-server

Obsluha uživatelského požadavku bude primárně umístěna v aplikační vrstvě. V situacích, kdy to bude účelné a neohrozí to požadavky na odezvy systému, může být část požadavku zpracovávána na straně klienta.

- Systémy budou k perzistenci dat využívat relační databázový systém (s dotazovacím jazykem SQL), ke kterému bude přístupováno výhradně prostřednictvím aplikačního serveru. Mimo databáze budou ukládána pouze data určená pro archivaci a dokumenty umístěné ve společném úložišti.

Dodávané systémy budou v místech specifikovaných v rámci jednotlivých analýz a návrhů řešení podporovat vyhledávání podle obsahu dokumentů a to jak u

dokumentů uložených přímo v databázi, tak skrze rozhraní spisové služby Objednatele v dokumentech uložených v této spisové službě. U dokumentů bude možné ukládat metadata, s pomocí kterých bude možné dokument rovněž vyhledávat.

- Tam, kde se to v rámci analýzy ukáže jako účelné, bude umožněna hromadná editace údajů.
- Pokud bude potřebné v některých dodávaných systémech ukládat nestrukturovaná data do relačního databázového systému, budou tato data ukládána jako binární objekty (BLOB), nebo volitelně ve spisové službě Objednatele. Systémy budou případně podporovat obě varianty a bude možné konfigurovat využívání těchto variant (pro uživatele to ovšem bude transparentní).
- Celé řešení bude podporovat používání národních znakových sad minimálně v rozsahu UTF8, Win1250-1251, ISO 8859-1 a 8859-2.

Systém bude v případech specifikovaných v Návrhu realizace poskytovat možnost pro snadný import dat. Struktura importovaných dat bude rovněž specifikována v Návrhu řešení. Dále bude systém podporovat exporty dat do formátů určených v Návrhu realizace. Pokud to bude účelné a není-li v ZD řečeno jinak, budou podporovány minimálně formáty CSV, PDF a XML. Při výstupech do XML bude Poskytovatelem dodáno patřičné DTD.

Systém umožní administraci parametrů systému uživatelskými rozhraními dle specifikace v Návrhu realizace, ať již se bude jednat o strukturovaná webová rozhraní, webová rozhraní s přímou editací konfiguračních sad nebo jiný způsob přístupu. Parametry systému se myslí takové parametry systému, které ovlivňují jeho chování a toto ovlivnění chování je pro daný systém/modul relevantní (např. workflow pro POD029 Schvalování smluv atp., úroveň detailu správy integračních rozhraní API v případě systémů, které API dle požadavků definují atp.). Naopak některé parametry mohou být editovatelné pomocí generických komponent využitých napříč všemi relevantními systémy, jako je například správa reportů.

- Systém bude mít jasně dokumentované API, které bude používáno pro potřeby komunikace s jinými systémy.

3.2.

Systémy, u kterých je požadována integrace se spisovou službou, budou integrovány na spisovou službu Objednatele a to v rozsahu, který bude přesně specifikován v rámci analýzy a návrhu řešení jednotlivých systémů. Systémy budou při nakládání se spisem primárně využívat funkcí rozhraní spisové služby. Pokud se v rámci analýzy ukáže, že některé části procesu nakládání s písemnostmi bude nezbytné implementovat v rámci dodávaných systémů, budou tyto části součástí dodávky. V rámci integrace na spisovou službu budou řešeny například následující funkcionality:

- Založení spisu a zahájení správního řízení
- Evidence písemností, ukládání dokumentů
- Ukládání popisných informací k písemnostem
- Vyhledávání ve spise
- Výpis obsahu spisu

- Tisk obsahu spisu

Podpora tisku písemností
Doplňování čárových kódů do písemností
Archivace spisu
Zobrazení písemností
Podepisování vytvářených písemností

V rámci integrace na spisovou službu budou dále implementovány funkcionality pro nakládání s digitálními písemnostmi. Opět je možné, že bude některé tyto funkcionality implementovat v rámci dodávaných systémů, ale primárně se očekává využití spisové služby Objednatele. Vše bude podrobně specifikováno v analýze systémů. Mezi funkcionality pro nakládání s digitálními písemnostmi budou například patřit následující:

- Načtení, zpracování a tisk čárového kódu určeného k označení písemnosti, přiřazení čárového kódu ke spisové značce a k digitálnímu obrazu písemnosti
Zobrazení digitální písemnosti, zobrazení písemností ve spise
Vyhledání písemnosti dle čárového kódu
Vytváření a tisk obálek dle definovaných šablon
- Doručování písemností – mezi podporované doručovací kanály budou patřit datová schránka, pošta do vlastních rukou adresáta na doručovací adresu, hybridní poštou na doručovací adresu nebo tisk a příprava pro osobní převzetí
- Doručování do ciziny, na vojenské újezdy či na PO BOXy
Doručování veřejnou vyhláškou
- Systém umožní zadání způsobu převzetí a data doručení, dále bude podporovat zpracování elektronických dodejek
- Systém umožní kontrolu doručení písemností, bude evidovat nedoručené písemnosti spolu s jejich typem a důvodem nedoručení

3.3. Šablony a generování písemností

Systémy, u kterých je požadováno generování písemností dle šablon, umožní vytváření a písemností dle šablon a to v rozsahu, který bude specifikován v analýze jednotlivých systémů. Pro generování šablon bude vytvořen obecný koncept využitelný napříč jednotlivými systémy. Tento koncept bude přesně vymezen v návrhu řešení, ale mezi podporovanými funkcionalitami budou například následující:

Vytvoření písemnosti dle předdefinované šablony
Automatické předvyplňování údajů z evidencí či vypočítaných údajů do písemností
Umožnění editace některých polí v generované písemnosti, možnost konfigurovat, které části písemnosti budou citovatelné
Centrální správa šablon s verzováním a ukládáním metadat k šablonám
Úpravy šablon
Export šablon
Sdílení šablon
Historizace šablon
Uživatelská databáze textů

Systémy rovněž umožní tisk písemností.

Ukáže-li se to v rámci analýzy možným a vhodným či účelným, budou tyto funkcionality či některé jejich části na základě dohody s Objednatelem realizovány pomocí integrace na

logických funkcí. Dotaz je možné uložit, zobrazit výsledek do tabulky v prostředí aplikace a také výsledek exportovat. Uložené dotazy nadále zobrazuje systém pouze uživateli, který je vytvořil. Uživatel může dotazy upravovat, ale může je také konkrétní dotazy zpřístupnit i jiným uživatelům. V rámci komponenty Dotazovač může uživatel sestavit i vlastní SQL dotaz ručně, ale vždy je omezen „Relačním stromem“ a nemá tedy k dispozici skutečnou databázovou strukturu.

Při sestavování je možné definovat omezující podmínky a to dle libovolných atributů, na které má daný uživatel oprávnění. Pro některé sestavy může být vhodné vytvořit databázové pohledy a to zejména ve chvíli, kdy jsou dané sestavy využívány při omezování jiných sestav. Vytvoření databázových pohledů v takovém případě zjednoduší sestavování dotazů v průvodci dotazovače. Seznamy často používaných atributů pro definování podmínek budou součástí analýzy a budou vycházet z požadavků v zadávací dokumentaci.

Komponentu bude třeba rozšířit o zobrazování výstupů do grafů, o podporu šablon a o podporu sestav s proměnnými parametry, tak aby plně odpovídala požadavkům Objednatele. Dále bude umožněn export sestav do různých formátů (například Excel, PDF a Word), systém umožní filtrování dat, upřesnění vyhledávání a tisk sestav. Přesná specifikace úprav bude provedena v rámci analýzy.

Při sestavování a provádění dotazů pro vytváření sestav budou hlídána přístupová práva uživatele k jednotlivým požadovaným datovým položkám.

Systém bude dále rozšířen o podporu přenosu sestav prostřednictvím emailu, publikace na Portál, uložení na souborový server či odeslání pomocí FTP.

3.5. Výměna údajů s ostatními OVM - Požadované a poskytované údaje

Integrační XML server je proprietární avšak plně otevřená platforma Poskytovatele, na které budou provozovány služby střední vrstvy. XML server zprostředkovává rozhraní pro vnější přístup k systému SZR (v kontextu MPSV: kompozitní služby ISZR, služby poskytované třetím stranám na základě oborových zákonů MPSV či jiných práv) z ostatních systémů a naopak je prostředníkem komunikace s externími systémy, ze kterých SZR čerpá data. V rámci dodávky Evidence subjektů JIS IS IPPD budou implementována následující rozhraní:

- Rozhraní pro Informační systém základních registrů (ROB, ROS, ISEO, CIS, RÚIAN)
- Pokud se ukáže jako potřebné, bude implementováno rozhraní externích registrů ARES, OR a RŽP (případně pouze některá z nich) a to především kvůli zajištění právnických osob, jejichž data nejsou zapsána v ROS.
- V rámci analýzy bude také specifikována implementace dalších potřebných rozhraní pro požadované či poskytované údaje, předpokládají se následující:
 - MOČR – evidence výplat důchodů z Vojenského úřadu sociálního zabezpečení
 - MSČR – evidence výplat důchodů, poskytování údajů v požadovaném rozsahu
 - MFČR – údaje o příjmech klientů žádajících o některé typy dávek
 - MDČR – údaje z evidence motorových vozidel
 - MVČR – evidence výplat důchodů z Odboru sociálního zabezpečení, poskytování údajů v požadovaném rozsahu

- ČSSZ – potvrzení o nároku na dávky, potvrzení o denním vyměřovacím základu, potvrzení o bezdlužnosti, potvrzení o výši vyměřovacího základu DP OSVČ, informace o vyplacených dávkách NP a DP pojištěnci za období
- BIS – tam, kde se to bude týkat dodávky systému IPPD, bude poskytnuto rozhraní pro BIS
- Rozhraní pro další externí systémy (IKMPSV, CEDR, ČSÚ, PSS, AP, DotInfo, Insolvenční rejstřík, Katastr nemovitostí, MŠMT, MZČR, NÚV, Registr pojištěnců)
- Rozhraní pro interní systémy a evidence (AccessPoints, centrální úložiště číselníků, ČSSZ, EKIS MPSV, EKIS ÚP, Identity management MPSV, NSP, JVM, IKMPSV, IS ESF 2014+, IS SD, IS ZAM, Portál MPSV, SÚIP)
- Rozhraní pro spisovou službu MPSV a centrální úložiště dokumentů a dalších systémů, které uvádí v souladu s požadavky ZD kapitola 2 této Přílohy)
- Rozhraní pro spisovou službu ÚP

V rámci analýzy bude specifikováno, zda některá rozhraní budou implementována prostřednictvím Informačního systému základních registrů nebo jiným způsobem (viz úvodní část kapitoly 2 této Přílohy). Dále bude v analýze specifikován rozsah načítaných údajů.

U rozhraní pro poskytování údajů se předpokládá využití jednotného referenčního rozhraní systému IPPD.

V rámci Návrhů realizací jednotlivých evidencí a systémů bude specifikováno, které systému budou implementovat která rozhraní.

Integrační XML server bude provádět transformaci XML zpráv prostřednictvím XSLT transformací. XML server umožní validaci XML zpráv prostřednictvím XSD schémat.

Integrační XML server je jako produkt postaven na společném jádře (z pohledu programového kódu realizovaného objektovým návrhem od společných datových entit a jejich procesů; z pohledu databáze se jedná o kořenové databázové entity LAR (Log a ARchiv – interní název), poskytující společnou množinu služeb pro výměnu a stav zpráv mezi systémy) a doplňovaný jednotlivými moduly, což jsou soustavy služeb či jiného kódu, realizujícího – s pomocí rozšiřování implementace funkcionalit předků OOP společného jádra a entit tohoto jádra a s pomocí doplňkových knihoven – komunikaci s jednotlivými systémy ať už konzumací jejich služeb různého typu nebo naopak poskytování služeb těmto systémům.

Ačkoliv je systém „proprietárním“ systémem Poskytovatele, jeho kód je otevřený a/nebo splňující některou z podmínek odst. 14.3.7. Smlouvy.

Jak již vyplývá z výše uvedeného, databáze LAR XML Serveru je určena i pro archivaci zpráv, avšak v souladu s požadavkem PRO004 „Archivace dat“ je systém vybaven i modulem pro provádění off-line archivace dat. Rozšířením tohoto modulu pro ostatní součásti systému bude dosaženo požadavků na archivaci, vč. podpory šifrování s pomocí kombinací funkcí MS SQL a použité ORM platformy. Systém IPPD bude mít k šifrovaným přístup z aplikační části a všechny externí systémy budou mít šifrovaná data k dispozici pouze prostřednictvím rozhraní aplikační části systému s ohledem na bezpečnostní požadavky Objednatele.

XML server a jeho moduly či součásti rovněž poskytují nástroje pro práci s časovými razítky a podpisy dokumentů PDF a XML (ověřování podpisů/označení časovými razítky, provádění podpisování a označování časovými razítky). Těmito nástroji se myslí nástroje v rozsahu ať už

přidělování přístupových oprávnění a/nebo předpokládaného/očekávaného/požadovaného/dodaného návrhu struktur entit AD dodavatelským subjektem realizujícím infrastrukturu část JIS.

- Jednak strukturu aplikační, reprezentující jednotlivé aplikace, volitelně rozdělené i na jednotlivé moduly (např. \Systém právních agend\Evidence soudních sporů) a evidující role v systému. Tyto „role“ budou klíčovými textovými řetězci, rozpoznávanými pro ověřování přístupu k jednotlivým funkcím v systémech jeho zdrojovým kódem.

Tyto 2 stromové struktury pak budou rovněž v rámci LDAP spojeny dohromady přiřazením „rolí“ konkrétním uživatelům nebo jejich pracovním pozicím (abstraktním či konkrétním, viz. předchozí odrážky). Toto přiřazení pak využijí dodávané systémy Poskytovatele při načítání údajů pro (v daném okamžiku již autentizovaného uživatele). Filtrací na Systém a modul získají seznam jeho rolí, které budou moci využít. Nastavení těchto údajů (vazeb) bude probíhat v rámci administrátorských rozhraní specifikovaných v příslušné zadávací dokumentaci jednotlivých zakázek.

S ohledem na specifické požadavky Objednatele pak k této struktuře musí existovat specifická struktura přímo v databázi (číselníkové, jako doplněk k Objednatelem již v ZD specifikovaným číselníkům), kterou dodá Poskytovatel v souladu s požadavky Objednatele a která vyjde z požadovaného seznamu datových atributů a jejich místech použití v dodaných systémech. A to ve třech specifických větvích:

- Číselníkové položky „typů kontrol“ a typů „stížností a petic“, ke kterým budou existovat databázové entity, odkazující se do DN na záznamy organizací/útvárů a tím budou reprezentovat oprávnění přístupů všech uživatelů z daných útvarů/organizací k daným typům kontrol či stížností a petic.
- Seznam datových tabulek a jejich atributů a to v konkrétním použití v aplikaci (tak jak vyžaduje ZD). Mezi každým použitím datové entity a atributu bude existovat vazba v datové entitě uložené v DB na pracovní pozici nebo konkrétního uživatele s informací, zda daný uživatel smí tuto datovou entitu zapisovat nebo jen číst (v případě neexistence vazby ji nebude moci ani číst). Vazba na pozici či uživatele bude realizována v rámci DB jako atribut (=sloupec tabulky) obsahující DN dané entity v LDAP.
- Seznam specifických datových tabulek a atributů patřících číselníkovým datovým entitám v DB bude základem pro entitu zachycující jejich vazbu na konkrétní uživatele, kterým bude možné takto přidělit oprávnění číst, vytvářet nebo editovat danou položku v administraci číselníků.

Specifickým autorizačním prostředkem pak bude evidence smluv, umožňující jednotlivým osobám nastavit přístupová oprávnění ke smlouvám jednotlivých organizací či jejich útvarů.

Veškeré výše uvedené hodnoty se budou nastavovat v administračním rozhraní dodávaným k jednotlivým modulům v souladu s požadavky ZD.

Za účelem oddělení pravomocí pro ty autorizační údaje, které budou spravovány přímo dodávaným systémem a budou v souladu s terminologií požadavku BEZ005 souviset s rolí,

platí, že k nim bude lze definovat role i oprávnění (oprávnění = datová entita role-oprávnění-cílová entita), které nesmějí být definovány současně.

3.8. Audit

Některé systémy budou podporovat evidenci informací pro audit prováděných činností. Činnosti každého uživatele budou evidovány a to v rozsahu prováděných operací, identity uživatele a data a času provedení operace. Systémy umožní konfiguraci auditu. Přesná specifikace provádění auditu a poskytování auditních informací bude specifikována v analýze. Podpora auditu jednotlivými systémy bude specifikována na základě požadavků Objednatele v analýzách.

3.9. Monitoring

Systémy budou poskytovat informace pro provozní a bezpečnostní monitoring. Budou logovány všechny operace ohledně přístupu a oprávnění uživatelů a to jak úspěšné, tak neúspěšné. Specifikace rozsahu logovaných informací bude v analýze.

3.10. Dokumentace

K systémům bude dodána dokumentace následujících typů: instalační příručka, provozní příručka, příručka správce aplikace, uživatelský manuál, analytická dokumentace a vývojářská dokumentace.

Instalační příručka, provozní příručka a uživatelský manuál budou dodány formou dokumentů ve formátech Microsoft Word a PDF. V těchto formátech bude dodána i doplňková dokumentace ve vztahu ke zdrojovým kódům, vývojovému prostředí a softwarovým knihovnám. Přesný rozsah a způsob předání jednotlivých dokumentací bude specifikován v analýze a bude respektovat požadavky Objednatele vycházející ze zadávací dokumentace.

Součástí dodávky budou zdrojové kódy vytvořené v rámci plnění. Dále bude dodána dokumentace popisující instalaci, konfiguraci a způsob použití prostředí pro vývoj systému.

Při tvorbě analytické dokumentace bude využito nástroje SparxSystems Enterprise Architect. Pro analytickou dokumentaci bude využita notace Archimate a pro model procesů notace BPMN vždy ve verzi požadované Objednatelem. Pro vývojářskou dokumentaci bude využito notace UML 2.0. Konečná struktura a rozsah použitých typů schémat bude stanovena v průběhu analýzy projektu dle informací, které vyplynou z potřeb Objednatele.

3.11. Testování

Pro potřeby provedení funkčních testů v rámci akceptací budou připraveny testovací plány a sady testovacích scénářů ke každému případu užití. Součástí dodávky budou také testovací skripty a to v rozsahu, který bude specifikován v rámci analýzy jednotlivých projektů.

Dále bude poskytnuta součinnost pro provedení bezpečnostních a výkonnostních testů.

3.12. Školení

Pro dodávané systémy budou vytvořeny podklady pro školení ve formě prezentací. Tyto prezentace budou vytvořeny v produktu Microsoft PowerPoint. Součástí podkladů budou interaktivní eLearning kurzy ve formátu SCORM. Součástí dodávky bude jednoduchá portálová aplikace pro podporu školení, ve které budou dostupné školící podklady a

uživatelské dokumentace. Školení budou probíhat na místech v rozsahu specifikovaným Objednatel. Přesná specifikace průběhu školení bude stanovena v analýze.

V rámci školení bude podáváno drobné občerstvení ve dvou stravovacích fázích rozdělené na dopolední přesnídávku cca mezi 9 a 10 hodinou a odpolední přesnídávku mezi cca 3-4 hodinou (pokud to plánovaný čas a délka školení umožní).

Pro Objednatel specifikované klíčové uživatele bude v rámci těchto školení (již ve fázi školení k prototypu) dodáno 30 mobilních pracovišť v souladu se specifikací Objednatele.

3.13. Provozní a výkonnostní požadavky

Součástí dodávky bude dodání všech potřebných licencí pro provoz systému a to včetně licencí vývojářských nástrojů a knihoven, s pomocí kterých bude možné nainstalovat stanici vývojáře. Současně bude dodán obraz virtuální pracovní stanice vývojáře a obrazy virtuálních serverů pro nasazení systému v konfiguraci pro vývoj (v prostředí Oracle VirtualBox nebo Microsoft Virtual PC).

Systémy budou provozovány ve dvou prostředích – produkčním a testovacím – vždy v clusteru – primární a záložní. U primárního a záložního prostředí se předpokládá souběžný provoz kvůli požadované vysoké dostupnosti systémů. Dále bude k dispozici možnost zprovoznit vývojové prostředí. Součástí dodávky bude plně funkční testovací prostředí včetně všech produktových licencí. Poskytovatel dodá obrazy virtuálních serverů pro nasazení systému v konfiguraci pro testování.

Systémy v účelných případech umožní řešení dávkových úloh, které bude možné plánovat na určitý čas, aby nebyla ovlivněna výkonnost systémů.

Systémy budou koncipovány a nastaveny dostatečně robustně s ohledem na výkonnostní požadavky Objednatele. Uživatelská rozhraní budou řešena tak, aby doba zpracování operací u koncového uživatele netrvala déle než 4 vteřiny (vyjma například generování sestav či dávkových operací). V případě požadavků na WS SOAP služby budou systémy připraveny reagovat v řádu milisekund. Do uvedených dob se v souladu s doplňujícími dotazy ZD nezapočítávají ty vlivy, na které Poskytovatel nemohl mít vliv (rychlost síťového spojení atp.). Systémy budou dále minimalizovat používání databázových zámků, aby tím nedocházelo ke znemožnění souběžné práce. Poskytovatel provede primární výkonnostní testování a dále nabídne součinnost a podklady pro zátěžové testování prováděné třetí stranou.

Systémy, u kterých to bude vyžadováno, budou disponovat modulem pro archivaci dat podle zadaných parametrů do externího úložiště. Archivovaná data budou šifrována a to s využitím odlišného klíče od klíče pro aktivní data. V archivních datech bude možné vyhledávat podle shodných kritérií jako v samotné aplikaci, ale nahlížení do archivních dat nebude probíhat skrze aplikace pracující nad aktivními daty. Nahlížení do archivních dat bude možné například prostřednictvím vlastních instancí aplikací. Přístup k archivním datům bude možný pouze vlastními oprávněními a může být vyčleněn pouze pro uživatelské účty sloužící pouze k tomuto účelu. Veškeré akce nad archivními daty budou auditovány. Systém umožní mazání archivních dat po definované době.

3.14. Migrace dat

U některých systémů bude třeba provést migrace dat ze systémů stávajících. Přesná specifikace, rozsah a způsob migrací bude popsán v analýzách jednotlivých projektů.

Migrace je možné provést některým z následujících způsobů:

4. DB link – připojení k databázi stávajícího systému a převod dat pomocí SQL skriptů do nových struktur s provedením čištění a potřebných úprav dat a vymezení chybných množin pro následné zpracování. K databázovému schématu původního systému dodá Objednatel Poskytovateli dokumentaci v souladu s kapitolou 8. **Zajištění provozu a podpora řešení**

4.1. Zajištění provozu řešení

4.1.1. Přístup S&T CZ k outsourcingu ICT

K outsourcingu nelze v současné době přistoupit jinak než komplexně. Takový přístup ale jednoznačně vyžaduje veliký rozsah kompetencí, kterými je schopna společnost pokrýt veškeré požadavky Zadavatele z vlastních zdrojů, a to jak v oblasti kapacitní, tak především kompetenční. Tímto Zadavateli plně garantujeme, že naše společnost tuto podmínku splňuje a vyhovujeme všem požadavkům kladeným v Zadávací dokumentaci.

Vzhledem k tomu, že uchazeč disponuje certifikovanými a zkušenými odborníky v oblasti ITIL (Information Technology Infrastructure Library – jedná se o soubor konceptů a postupů, které umožňují lépe plánovat, využívat a zkvalitňovat využití informačních technologií a to jak ze strany Uchazeče, tak i z pohledu Zadavatele), bude Uchazeč využívat tato doporučení pro poskytování, evidenci a reporting dodávaných služeb.

Tento rámec souborů a postupů je celosvětově osvědčen a uznáván jako soubor nejlepších doporučení pro řízení a dodávku příslušných služeb, což Zadavateli garantuje maximální možnou efektivitu a záruku velmi kvalitního řízení a plnění požadovaných činností. Dále pak ve svém realizačním týmu disponuje Uchazeč vysoce zkušenými pracovníky s certifikacemi, kteří mají dlouhodobou zkušenost se zavedenými procesy.

4.1.2. Široké kompetence společnosti S&T

Službou Outsourcing obecně přebíráme částečnou nebo úplnou odpovědnost za definované oblasti IT/IS. Poskytování outsourcingu probíhá tak, že na jedné straně procesu stojí zákazník se svými požadavky, a na druhé straně je dodavatel služeb, který tyto zákaznické potřeby uspokojuje. Dodavatel těchto služeb může být interní nebo externí.

Outsourcing IT/IS nepovažujeme za monolitickou dodávku jednoho systému, naopak ho vidíme jako stavebnici složenou z několika komponent, a záleží jen na budoucím uživateli outsourcingu, kterou část svého IS vyčlení vně své organizace a nahradí ji přiměřenou komponentou této stavebnice.

Firmy specializující se na daný obor mají zavedla mnohem lépe proškolené pracovní síly, které se v dané problematice orientují. Odpovědnost za problematiku nese jiný subjekt a výchozí firma se může plně věnovat svému hlavnímu oboru. Náklady na zajištění specializované činnosti jsou při využití outsourcingu zpravidla výrazně nižší. Zajišťování služeb pomocí outsourcingu je celosvětově se zvyšujícím trendem.

V oblasti outsourcingu infrastruktury a standardních aplikací se zaměřujeme na společnosti středně velké a velké ze všech segmentů trhu v ČR. V oblasti aplikačního a procesního outsourcingu jsme díky našim referencím schopni poskytnout vysokou

kvalitu outsourcingových služeb pro společnosti ze segmentů financí, telekomunikací, výroby, stavebnictví a státní správy.

V IT existuje nepřehledné množství technologií, systémů a aplikací. Jako jeden z velkých integrátorů v České republice vlastníme na většinu z těch klíčových vlastní školené specialisty a v ostatních případech doplňujeme naše řady o externí spolupracovníky a využíváme subdodávek našich dlouhodobých partnerů. Díky takovému přístupu zajistíme vždy kvalitní podporu všech technologií klientů.

Naše společnost mimo certifikace ISO 9001 získala také významnou certifikaci ISO 20000 se zaměřením specificky na outsourcing IT/IS a certifikaci ISO 27000 se zaměřením na informační bezpečnost.

V oblasti podnikových systémů jsou našimi partnery SAP, INFOR, COGNOS a LCS. V oblasti technické infrastruktury také spolupracujeme se špičkovými dodavateli a jsme držiteli nejvyšších certifikací – našimi partnery jsou společnosti HP, IBM, Fujitsu, DELL, Microsoft, CheckPoint, EMC, VMware a další.

Bezpečnostní řešení, poskytovaná našim klientům, jsou založena na nejnovějších technologiích společností CISCO, CITRIX, McAfee, Symantec, ISS, BlueCoat a dalších. Mezi naše osvědčené partnery z oblasti sítí patří například společnosti CISCO, Allied Telesyn, HP, 3COM a RIT.

V oblasti servisu, podpory a služeb naše aktivity zahrnují například péči o produkty společností IBM, HP, NetApp, Dell, Fujitsu Siemens Computers, Xerox, Acer, Lexmark, Olivetti a dalších.

Systém řízení kvality podle S&T

4.1.3. Model projektového a procesního řízení

Uchazeč k efektivnímu řízení smluvního vztahu, resp. k efektivnímu řízení dodávky outsourcingových služeb přistupuje na základě níže popsaného modelu, který je založen na dlouholetém vývoji, vzhledem k jeho efektivitě a upravován na základě aktuálních zkušeností a hodnocení našich zákazníků. Tento model je používán mnoha outsourcingovými organizacemi.

Používaná architektura řízení umožňuje včasnou identifikaci potenciálního výskytu problému a jeho řešení od nejnižší úrovně řízení až po jeho eskalaci na nejvyšší možnou úroveň. Tento proces bude detailně popsán v Provozní dokumentaci vznikající v rámci fáze tranzice.

Řízení vztahu se zákazníkem – v terminologii Uchazeče "Governance model", tvoří formální řídicí rámec a strukturu, které vychází ze standardních procesů a osvědčených zkušeností Uchazeče. Governance model umožní oběma stranám efektivní vzájemné řízení vztahu, očekávání, smluvních závislostí a služeb.

Procesy Governance jsou dobře dokumentované, opakovatelné a flexibilní. Úspěšná implementace Governance je úzce závislá na návrhu optimálního modelu, který umožní splnit požadavky obou stran a zajistí proaktivní a oboustranně výhodný partnerský vztah mezi oběma organizacemi.

Na základě zkušeností Uchazeče s obdobnými komplexními vztahy řešícími poskytování dlouhodobých outsourcingových služeb srovnatelného objemu a vzhledem ke stávajícímu organizačnímu zajištění služeb v prostředí Zadavatele navrhujeme ustanovit následující:

Výkonný Management (frekvence schůzek 1–2x ročně)

- Strategické řízení vztahu
- Dlouhodobé plánování aktivit, zpravidla na roční období

Řídící výbor (frekvence schůzek kvartálně)

Taktické řízení vztahu

Střednědobé plánování aktivit, zpravidla na kvartální období

Vyžadována přítomnost tzv. Sponzora projektu ze strany Zadavatele

Hlavní tým projektu (frekvence schůzek měsíčně)

Operativní řízení vztahu

Krátkodobé plánování aktivit, zpravidla na měsíční bázi

Průběžné hodnocení dodávky dohodnutých služeb dle SLA

Dále pak garantujeme na vyžádání Zadavatele účast odpovědného zástupce Uchazeče na tzv. Pracovních skupinách, které jsou v současné době pořádány Zadavatelem na týdenní (příp. 14 denní) bázi a řeší zcela operativní záležitosti, které se týkají běžného provozu všech provozovaných služeb napříč celým Ministerstvem zemědělství. Z těchto schůzek jsou eskalovány problémy na vyšší úroveň řízení, jako jsou výše zmíněný Hlavní tým projektu, případně Řídící výbor projektu.

Uchazeč garantuje objednateli součinnost a komunikaci v rámci osobních jednání na kontrolních dnech, operativních ad-hoc schůzkách na vyžádání a v průběhu poskytování činností v rámci provádění služeb, což objednateli zajistí v maximální možné míře průběžné zvyšování efektivity řízení poskytovaných služeb.

Uchazeč se zavazuje předložit objednateli jedenkrát ročně celkovou výroční zprávu obsahující přehled poskytnutých služeb, ve které přehledným způsobem popíše realizované činnosti v uplynulém období dle jednotlivých klíčových oblastí, shrnutí měsíčních vyhodnocení SLA parametrů, doporučí objednateli případné oblasti služeb vhodné pro zlepšení a poskytne objednateli celkovou zpětnou vazbu vycházející ze zkušeností provozu služeb za uplynulé období.

Blokový obrázek modelu dodávky služeb

4.1.4. Procesy a pracovní postupy

Naše společnost se již od svého založení zaměřovala především na oblast poskytování služeb IT. Díky této striktní orientaci jsme se již od roku 2005 začali intenzivně věnovat školením a procesním změnám směrem k rámci ITIL. Procesní rámec ITIL byl víceméně jako jeden celek využit k vytvoření evropské normy známou pod značkou ISO 20000. Protože naše procesy a postupy již splňovaly náročná kritéria procesního rámce ITIL, požádali jsme jako druhá společnost na českém trhu o certifikaci dle této ISO normy a v

roce 2006 jsme obdrželi akreditaci ISO 20000 na služby, mezi kterými je mimo jiné také poskytování outsourcingu IT. Náš přístup k procesnímu řízení je standardizován a podrobně popsán v dokumentaci ISO 20000. Tak, jak je popsáno v zadání, nebudeme se v následujících kapitolách dopodrobna věnovat procesním modelům řízení jednotlivých disciplín IT služeb, ale zdůrazníme náš přístup a vyzdvihneme výhody a vylepšení, která jsme za dobu poskytování služeb outsourcingu dosáhli. Z těchto bohatých zkušeností budou čerpat členové našeho týmu a garantujeme tímto Zadavateli poskytování všech požadovaných služeb v souladu se Zadávací dokumentací.

Vrcholový pohled na procesy ISO 20000 certifikované v S&T

4.1.5. Incident management

Účel procesu:

Maximálně rychle obnovit službu s ohledem na smluvní termíny, s minimálním dopadem na uživatele a za co nejnižších nákladů. Incident je specifický typ události nebo uživatelského hlášení, obvykle spojeného s výpadkem služby nebo se snížením její kvality. Správa incidentů tvoří další větev podpory uživatelů. Vstupy od uživatelů nebo dohledované IT infrastruktury jsou buď vyřešeny přímo pracovníky Service Desku, a nebo předány specialistům druhé a třetí úrovně podpory, případně předány externím řešitelům.

Uchazeč zastává přístup, že Incident Management přináší kvalitu, efektivitu a tedy i cenovou konkurenceschopnost způsobem maximální standardizace. S&T má tisíce incidentů měsíčně od stovek klientů. Tato čísla se rychle zvyšují a naše procesy se stále musí zlepšovat. Naši manažeři kvality a manažeři jednotlivých disciplín mají za cíl dále zlepšovat vlastní IMS systém a procesy na něj navázané. Incident Management máme standardně rozdělen do tří úrovní dle doporučení ITIL a to 1st level – ServiceDesk; 2nd level – On-Site/Off-Site specialista; 3rd line – eskalace na vendora a podporu třetích stran.

Závěr:

Vzhledem k tomu, že schválený proces incident managementu v prostředí Zadavatele je plně v souladu s doporučeními ITIL, které má uchazeč jako svůj firemní standard a na který je certifikován, garantujeme Zadavateli, že budeme plně integrováni na tento proces a budeme postupovat plně v souladu s uvedeným diagramem:

4.1.6. Change management

Účel procesu:

Obhospodařovat změny v infrastruktuře IT s ohledem na neustále se měnící obchodní potřeby a očekávání uživatelů, aby se minimalizoval negativní dopad na existující služby IT. Změnová řízení jsou kvůli rostoucím požadavkům na efektivitu provozu IT a důrazu na vysokou dostupnost služeb stále důležitější. Proces Správa změn vzájemně spojuje a propojuje procesy inicializace, sběr informací, vyhodnocování, plánování, řízení, implementace a testování změn v IT infrastruktuře. Je prakticky nemožné ve složitějším

prostředí provádět jakékoliv změny, pokud daný pracovník nemá například dostatečné informace o tom, jaké technické vybavení, kdy a kde a jakým způsobem má vyměnit či nainstalovat.

Změnová řízení jsou v případě naší společnosti více "customizovaná" proti vysoce standardizovanému procesu Incident Managementu. Důvodem je, že zde klademe více důraz na rychle se vyvíjející obchodní cíle klientů, které se většinou diametrálně liší ve všech parametrech. I zde existují ale výjimky, kdy například u vysoce centralizovaných a manažersky globalizovaných mezinárodních společností náš model standardního řízení změn byl použit v plném míře.

Podstatnou výhodou naší implementace této disciplíny je flexibilita, kterou našim klientům nabízíme za využití standardních a vyzkoušených postupů na oborově širokém vzorku našich outsourcingových klientů.

Závěr:

Vzhledem k tomu, že schválený proces change managementu v prostředí Zadavatele je plně v souladu s doporučeními ITIL, které má uchazeč jako svůj firemní standard a na který je certifikován, garantujeme Zadavateli, že budeme plně integrováni na tento proces a budeme postupovat plně v souladu s uvedeným diagramem:

4.1.7. Service level management

Účel procesu:

Připravit, poskytovat a vyhodnocovat úroveň dodávaných služeb, které jsou zakotveny písemnými smluvními vztahy.

Klíčovým nástrojem pro správu, řízení, evidenci, kontrolu, reporting a zajištění požadované úrovně poskytovaných služeb je tzv. Service Level Management, jehož hlavním účelem je připravit, poskytovat a vyhodnocovat úroveň dodávaných služeb, které jsou zakotveny ve Smlouvě.

Uchazeč dlouhodobě praktikuje a důsledně dodržuje propracované praktiky ServiceLevel Managementu ve všech poskytovaných a provozovaných službách, což přináší Zadavateli následující hlavní výhody:

Lepší vyváženost přínosů ICT proti nákladům,

Zvýšení výkonnosti i prestiže ICT a zlepšení služeb, které poskytuje,

Zásadní zkrácení doby pro obnovu služeb při jejich výpadku.

Pro maximálně efektivní evidenci služeb využívá Poskytovatel Katalog služeb, který obsahuje jednotlivé katalogové listy s jejich příslušnými atributy pro měření a definici úrovně služeb. Níže uvádíme základní atributy služeb, které běžně v jiných projektech

Uchazeč eviduje a využívá k reportingu:

Jméno služby/Service Name

Popis služby/Service description

Typ služby/Service type

Kterých odborných útvarů se služba týká/Business Unit(s)

Manažeři služby/Service Manager(s)

Dopad na odborné útvary a jejich agendy/Business Impact

Priorita agendy (procesu)/Business priority

Provozní doba služby/Service hours
Kontakty na zástupce odborných útvarů/Business contacts
Eskalační kontakty/Escalation Contacts
Reporty o službě/Service Reports
Revize služby/Service Reviews
Bezpečnostní kategorie/Security Rating
Garantovaná úroveň služby (SLA)/Service Level Agreement)

Service Level Management je zastřešen metodicky a personálně Service manažery, kteří nejsou jmenováni jen na straně Uchazeče, ale také na straně našich klientů. Naši Service manažeři jsou certifikováni ITIL profesionálové, kteří se řídí doporučeními ITIL a interními směrnici ISO 20000 naší společnosti.

Dedikovaný Service manažer má za úkol kontinuálně měřit, řídit, vyhodnocovat a především zlepšovat průběžně poskytované služby. Dále pak zastřešuje další definované role pro poskytování služeb definovaných Zadavatelem v Zadávací dokumentaci.

Jako jedno z našich vylepšení postupů můžeme uvést například standardizovaný proces SIP [Service Improvement Program], který metodicky zvyšuje kvalitu služeb tam, kde není dostatečná.

Díky moderním technologiím a informačním systémům mají naši Service manažeři okamžitý přístup k vyhodnocování všech KPI [Key Performance Indikátory], které jsou uvedeny v jednotlivých SLA [Service Level Agreement] nebo Katalogu služeb.

Příklad on-line reportu dostupného pro všechny Service Manažery

Závěr:

Vzhledem k tomu, že schválený proces service level managementu v prostředí Zadavatele je plně v souladu s doporučeními ITIL, které má uchazeč jako svůj firemní standard a na který je certifikován, garantujeme Zadavateli, že budeme plně integrováni na tento proces a budeme postupovat plně v souladu s uvedeným diagramem:

4

Service Manažer (dále jen SM) je jmenovaný Uchazečem za účelem zajištění standardní úrovně poskytovaných služeb, zvyšováním spokojenosti Zákazníka a pro koordinaci a řízení všech aspektů se službou související. Mezi hlavní povinnosti patří pravidelné governance meetingy se zástupci Zadavatele, interním personálem dodavatele, dále pak řešení všech nestandardních situací (projekty, změny služeb, procesů) včetně průběžné dokumentace a pravidelného vyhodnocování. SM má přiděleny od dodavatele vysoké pravomoci, které mu umožňují ve většině běžných případů rozhodovat rychle a efektivně, bez nutnosti eskalace a tvorby interních žádostí o změny.

Vysoká úroveň kvalifikace a zkušenosti SM jsou zárukou zajištění kontinuity a dlouhodobé kvality služeb poskytovaných dodavatelem. Všichni SM jsou certifikováni dle ITIL (standard na řízení IT používaný dodavatelem) s minimální 5letou praxí v řízení dodávek outsourcingu, správy systémů nebo projektového managementu v IT oboru.

Při startu nebo přebírání poskytování nové služby je role SM definována takto:

- Představit manažera služeb – jediný kontakt v S&T pro IT/SM manažera Zadavatele
- Seznámit se s korporátními normami IT Zadavatele a s jeho postupy spojenými s IT a požadavky
- Nastavení podpory a eskalačních cest
- Připravit, optimalizovat a implementovat postupy pro poskytování služby
- Seznámit odpovědné zaměstnance S&T s výše uvedenými informacemi
- Zajistit funkčnost náběhu příslušných postupů
- Připravit strukturu pravidelného reportování, dokumentace, eskalace
- Vytvoření datového prostoru na intranetu a vložení dat (smlouva, zápisy, reporty atd.)
- Zajistit shodu s procesními a metodickými pokyny S&T a Zadavatele

Pravidelné governance aktivity vykonávané SM:

Popis				
Provozní schůzky (analogie Pracovní skupiny v prostředí MZe)	1x 14dní	• Řízení incidentů • Změnová řízení • Bezpečnostní incidenty • Průběžná kontrola služby • Doporučení na zlepšení • Krátkodobé plánování služby • Kontrola plnění KPI parametrů	• Ad-Hoc reporty • Konzultace s vlastníky služeb • Interní vyhodnocení s pracovníky dodavatele • Výstupy z procesů změn, releasů a problémů • Minulý zápis s úkolovníkem	• Zápis z jednání • Rozdělovník úkolů • Stav úkolů • Distribuce zápisu dle rozdělovníku • Návrh eskalace na SLM • Žádosti o změny
Jednání SL komise (analogie Hlavního týmu projektu v prostředí Mze)	měsíčně	• Vyhodnocení KPI/SLA • Revize změnových požadavků • Schválení změn • Finanční sumarizace/faktura	• Měsíční reporty • Zápisy z provozních schůzek • Finanční podklady • Seznam úkolů • Eskalace na SLM • Změnové žádosti	• Zápis z jednání • Rozdělovník úkolů • Stav úkolů • Distribuce zápisu dle rozdělovníku • Vyřešení eskalace • Návrh eskalace na IT komisi • Žádosti o změny
Jednání komise	ročně	• Vyhodnocení dlouhodobých cílů • Finanční management • Revize smluvních	• Roční souhrnné reporty • Audit report (je-li) • Eskalace na IT komisi • Cíle na předchozí	• Zápis z jednání • Rozdělovník úkolů • Stav úkolů • Distribuce zápisu dle rozdělovníku



	podmínek	rok	• Vyřešení eskalace
	•	•	•
	•		•
	další rok		inovace

Governance aktivity lze realizovat dle dohody mezi Uchazečem a Zadavatelem na místě, telefonicky a nebo videokonferencí, dle požadavku a aktuální potřeby. Pravidelnost a dodržování termínů je primární odpovědností SM a pouze na žádost Zákazníka lze pravidelné termíny rušit nebo přesunovat.

4.1.9. Service Continuity Management

Kontinuita poskytovaných služeb a podnikání našich klientů je jedním z cílů naší společnosti. Řešení Disaster Recovery současně nabízíme našim klientům jako součást našeho standardního produktového portfolia. Interní systémy a podpůrné procesy (CallCentrum, Informační systémy, datová konektivita) jsou zajištěny i pro případy havárie. Máme vypracovány havarijní plány pro jednotlivé disciplíny dle ISO 20000.

Kontinuitu námi poskytování služeb, tedy z pohledu klienta i kontinuitu jeho podnikání, chápeme jako neustále se vyvíjející se proces.

Business Continuity / DR metodologie dle NIST 800.34

Tento obecný proces je shodný pro jakoukoli organizaci či podnik a liší se až v technické realizaci.

4.1.10. Bezpečnost a důvěrnost informací

Bezpečnost a důvěrnost informací je klíčovou devizou naší společnosti. Bez garance vysoké úrovně bezpečnosti bychom nemohli splňovat vysoké nároky, které na nás kladou naši současní zákazníci.

Naši zaměstnanci, přicházející do styku s důvěrnými i utajovanými informacemi, a proto někteří z nich prošli bezpečnostními prověrkami a byli náležitě proškoleni. Organizace jako celek disponuje zaměstnanci certifikovanými NBÚ od úrovně D (důvěrný) až po T (tajný).

Zaměstnanci používají šifrované připojení k internetu, zabezpečené počítače a šifrují data na nosičích. Přístup k datům je obvykle řešen "pohledy" do databáze a bezpečnostními politikami v rámci stromové struktury dat. Zaměstnanec nemá přístup k datům, která bezprostředně nepotřebuje k řešení svého úkolu v rámci týmu.

Na úrovni jednotlivých prvků architektury – aplikací – bezpečnost zajištěna následovně:

- Bezpečnost dat je zajištěna robustními prostředky SQL datového enginu
- Bezpečnost komunikace klient – server je zajištěná na úrovni variantního kódování tohoto protokolu
- Bezpečnost na úrovni logiky aplikace je zajištěná robustním, nastavitelným auditem jednotlivých procesů na straně jedné a systémem nastavování skupinových a uživatelských profilů na straně druhé

Přesné definice rozsahu, hloubce, technikách a penalizacích jsou ukotveny ve vzájemné smlouvě o utajovaných skutečnostech, která je obvykle připravována a podepsána na úvod procesu Due Diligence.

4.1.11. CSI – Index spokojenosti Zákazníka

Pro vyhodnocování služeb předpokládáme použití intranetového dotazníku, který bude připravovat MZe. Níže uvádíme naše standardní procesy a postupy.

Mezi standardní reporty patří výstupy z pravidelných průzkumů spokojenosti uživatelů Zákazníka. Reporty vznikají z odpovědí na dotazníky, které jsou zasílány pravidelně elektronicky emailem, obvykle jednou za půl roku, na uživatele, kteří využili službu – tedy pouze těm, kteří mohou na zaslaný průzkum spokojenosti kvalifikovaně odpovědět.

Počet a znění dotazů které se uživatelům pokládají, jsou definovány na začátku poskytování služby. Aby bylo možné srovnávat výsledky jednotlivých průzkumů v průběhu let poskytování služby, je třeba, aby znění dotazů zůstalo po celou dobu služby ideálně nezměněno. Hodnocení obvykle probíhá na tzv. školní stupnici, kde 1 znamená nejlepší a 5 nejhorší. CSI, tedy index spokojenosti Zákazníka je spočten jako absolutní průměr hodnocení všech účastníků a všech položených dotazů. Tento index jako jedna hodnota je součástí DashBoardu, jenž je určen pro Manažerský přehled. Detailní výsledky hodnocení a výsledky po jednotlivých odpovědích jsou k dispozici Service Manažerům obou smluvních stran.

Logo Zpěva

Odeslat Odpověď Převést Odložit Přesunout do složky Vytvořit pravidlo Vložit do adresáře Sdílet Sdílet adresou Zládit do Zpracovat Odeslat jako nepřečtené Odeslat Souhrnný výhled

Od: Komu: Zpráva: Předmět: Průzkum spokojenosti s IT

Vážený IT uživatel,

V rámci zlepšení kvality poskytovaných IT služeb plánujeme převést službu IT HelpDesk na externího dodavatele (společnost S&T CZ, s.r.o.). Naším cílem je zvýšit dostupnost služeb, které Vám IT poskytuje, rozšířit dobu pokrytí a zejména snížit reakční dobu řešení Vámi nahlášených IT problémů a tím minimalizovat případné finanční ztráty.

Ti z vás, kteří již od pondělního poledne hlásili IT incident, jistě zaznamenali změnu. Společnost S&T CZ, s.r.o. disponuje profesionálním call centrem a pro Vaši podporu dedikovala několik pracovníků, kteří jsou schopni pokrýt více hovorů paralelně.

Rádi bychom pravidelně hodnotili Vaši spokojenost s poskytovanými IT službami a za tímto účelem s Vámi dovoluujeme poslat následující link

Webový formulář průzkumu Vaší spokojenosti s IT službami je umístěn ZDE.

Na této adrese je třeba odpovědět na uvedené dotazy a ohodnotit jak vnímáte stávající kvalitu poskytovaných IT služeb. Tento průzkum plánujeme opakovat pravidelně jednou za půl roku, aby vedení společnosti získalo náhled zdali tato změna je správná.

Předem děkujeme za Vaši reakci, po uzavření průzkumu dojde ke slosování všech odpovědí a pět vylosovaných uživatelů bude odměněno zajímavou věcnou cenou od společnosti S&T CZ

Děkuji,

Patička s logem a podpisem

Příklad zasláního emailu na uživatele průzkumu

Příklad dotazů pokládaných v jednom ze současných průzkumů. Dotazy by měli být jednoznačné krátké a srozumitelné.

- Jak jste celkově spokojeni s poskytováním IT služeb?
- V případě, že kontaktujete vaši IT podporu, je vždy někdo, kdo by se vám věnoval?
- Jste spokojeni s kvalitou komunikace ze strany vaší IT podpory?
Jste spokojeni s dobou řešení vámi nahlášených požadavků?

Webový formulář průzkumu spokojenosti

Detail vyhodnocení dotazníku průzkumu spokojenosti

CSI uvedený v DashBoardu

4.1.12. Správa problémů

Účel procesu: identifikovat a řešit chyby v infrastruktuře IT, aby se zabránilo opakovanému výskytu incidentů vztažených k těmto chybám. Tento proces je velmi často též nazýván správou kvality (Quality Management), protože je zaměřen na analýzu velkých, opakujících se nebo podobných incidentů. Výsledkem analýzy je pak nalezení a definice systémové příčiny tzv. známé chyby (Known Error). Proces Správa problému má jak reaktivní, tak i proaktivní aspekty. Reaktivní činnosti se soustřeďují na řešení problémů vyvolaných incidenty, proaktivní činnosti se zaměřují na identifikaci a řešení problémů a známých chyb ještě předtím, než se stanou incidenty. Zatímco účelem procesu Správa incidentů je obnovit službu jak nejrychleji je to možné, proces Správa problémů se zaměřuje na důkladnou analýzu klíčové příčiny selhání, a podporuje tak maximální stabilitu poskytovaných služeb IT.

4.1.13. Správa konfigurace

Účel procesu: zabezpečit centrální správu IT infrastruktury tak, aby se podpořila dodávka kvalitních a efektivních služeb IT. Správa konfigurace je proces, který zajišťuje identifikaci, řízení, vykazování stavu a kontrolu nad infrastrukturou IT a všemi aktivy IT v organizaci v průběhu jejich životního cyklu. Kromě podpory dalších procesů, jako je Správa problémů a Správa změn, zajišťuje také snadný přístup k informacím, jako jsou smlouvy o poskytování služeb, vazby/závislosti mezi konfiguračními položkami a organizačními informacemi. U procesu Správa změn zabezpečuje proces Správa konfigurace pracovníkům zodpovědným za změny, aby byli aktuálně informováni o jednotlivých zařízeních, uživateli a službách. V důsledku toho mohou provádět odpovídající analýzu rizik a dopadů. Tato integrace zároveň zaručuje aktuální stav

konfigurační databáze. Účinné řízení konfigurace zajišťuje nejlepší využití, rozmístění a využívání všech IT aktiv.

4.1.14. Řízení projektů

Pomocí projektových manažerů pomáháme u našich zákazníků zavést nebo zdokonalit projektovou kulturu, aby pomocí efektivních a kontrolovatelných procesů a metod řídili své projekty v daném čase, v rámci rozpočtu a v požadované kvalitě. Dále pak pomáháme projekty kvalifikovaně a maximálně efektivně řídit plně v souladu s principy metodiky IPMA.

4.1.15. Provozní deník

Uchazeč bude vést Provozního deník a zaznamenávat do něj minimálně následující skutečnosti:

Výskyt havarijních stavů;

Výskyt anomálií a nestandardních stavů systémů, které mají dopad na plnění SLA;

Zprovoznění nového nebo dočasně odstaveného systému a odstavení systému; Spuštění, vypnutí a restart systému.

Uchazeč garantuje, že provozní deník bude obsahovat minimálně následující informace:

Datum a čas pořízení záznamu;

Identifikace osoby pořizující záznam;

V případě událostí trvajících více než 1 hodinu také čas začátku a konce události;

Popis události.

4.1.16. Integrace interních procesů hlášení incidentů, přijímání změnových požadavků na stávající procesy a systémy zadavatele

Interní procesy hlášení požadavků, přijímání změnových požadavků vycházejí z procesů požadovaných zadavatelem v zadávací dokumentaci. Interní procesy uchazeče budou flexibilně přizpůsobeny potřebám MPSV a budou plně reflektovat i požadavky na případné úpravy procesů.

Poskytované služby zajištění předmětu VZ jsou řízeny procesními standardy postavené na sadě doporučení ITIL v3. Interní procesy Zadavatele pro hlášení incidentů, změnových požadavků případně problémů budou jedna ku jedné navázány na procesy Uchazeče, který provozuje plnohodnotné service deskové SW řešení. V inicializační části projektu počítáme s provedením integrace mezi SW nástroji Zadavatele a Uchazeče tak aby byli jednotlivé procesy provázány.

Tímto postupem zajistíme vedení evidence o probíhajících řešení jednotlivých požadavků nebo skupin požadavků v service desku Zadavatele v dostatečné úrovni informací tak aby bylo možno provádět měření a vyhodnocování podpory jednotlivých služeb a řešení jednotlivých požadavků.

4.1.17. Komunikační kanály a jejich integrace s komunikačními kanály zadavatele

Komunikační kanály na straně dodavatele budou plně integrovány s komunikačními kanály zadavatele a přizpůsobeny jeho potřebám. Pro komunikaci s uživateli uchazeč předpokládá využití telefonu, faxu, e-mailu a případně webového rozhraní. Pro interní komunikaci mezi dodavatelem a objednatelem předpokládá dodavatel využití Pracovního týmu (PT), Hlavního týmu projektu (HTP) a Řídícího Výboru (ŘV).

4.1.18. Dokumentace projektu

Průběh projektu a podstatné výstupy projektu jsou ukládány do centrálního úložiště dokumentace, které je přístupné všem osobám podílejícím se na projektu.

Struktura úložiště je následující:

- Společná projektová dokumentace
 - Provozní deník
 - SLA reporting
 - Požadavky na změnu
 - Záписy z porad (jednání ŘV a pracovního týmu)
 - Komunikační matice – složení jednotlivých týmů a kontaktní údaje účastníků
 - Procesní dokumentace – popisy procesů, katalog služeb, konfigurační databáze

Systémová dokumentace a složky jednotlivých systémů

- Administrátorské, instalační a uživatelské příručky
- Testovací a akceptační protokoly

Všechny dokumenty zaznamenávající dohody mezi objednatelem a poskytovatelem implementace změn (např. zápisy z jednání), výstupy poskytovatele (dokumenty analýzy a návrhu) jsou pojmenovávány stejnou konvencí a ukládány na úložišti Projektové dokumentace.

V případě oponentury a upřesňování obsahu dokumentu týkajícího se implementace změn jsou změny zachycované formou revizí (pokud to daný formát dokumentu umožňuje) a v úvodu dokumentu je doplněno datum oponentury a souhrn připomínek. Opakovaně předávané dokumenty objednateli jsou verzovány a nová verze bude obsahovat stručný popis změn navíc ještě v komentáři verze na portálu.

Konvence pojmenování souboru je "Název dokumentu_identifikace týmu_verze (případně pořadí)_datum předání", kde verze je znázorněna konvencí XvY a datum je ve formátu rrrmdd (bez diakritiky).

Soubory jsou na úložiště ukládány ve standardních formátech – MS Office verze 2003 včetně (.doc, .docx, .xls, .ppt, .msg atd.), MS Project (.mpp), obrázky (.jpeg, .tif, .gif, .pdf), MS Visio (.vsd), XML služby (.wsdl, .xml, .html, .css).

4.1.19. Strukturované e-maily

Na základě schválených plánů změn a plánů odstávek zasílá technický specialista případně Manažer řízení služeb v dostatečném předstihu na HD MPSV informační e-mail v předem definované struktuře o plánované odstávce systému (případně plánované změně). HD MPSV si odstávku/update zkontroluje z hlediska plánů odstávek a změn, případně si vyžádá souhlas odborného garanta IS nebo Manažera řízení služeb

poskytovatele. Rovněž si může vyžádat doplnění e-mailu o dodatečné informace, pokud není informace kompletní.

Minimální rozsah strukturovaného e-mailu je následující:

- Identifikace systému, kterého se informace týká a identifikace, zda se jedná o produkční či testovací prostředí.

Rozsah prací.

Dopad prací (např. úplná nedostupnost, omezení rychlosti aplikace apod.).

Plánovaný začátek a plánovaný konec prací (datum a čas).

Kontaktní osoba odpovědná za provedení prací a kontaktní údaje (mobil a e-mail).

Následně HD MPSV rozešle oznámení e-mailem na kontaktní osoby dle komunikační a eskalační matice (filtrované dle druhu upozornění (odstávka/update) a dotčeného systému).

Strukturované e-maily jsou prostřednictvím HD MPSV rozesílány i v případě výpadku systému, kdy je součástí zprávy dotčený systém a určení prostředí (produkční/testovací). Zpráva je zasílána na konkrétní osoby určené v komunikační a eskalační matici (druh upozornění "výpadek"). Zpráva je zasílána při vzniku takového stavu a po vyřešení incidentu je oznámeno ukončení výpadku.

4.2. Způ:

4.2.1

Jako primární monitorovací nástroj infrastruktury a aplikací byl zvolen S&T Spectator. Spectator je řešení, jenž umožňuje monitorovat chování komponent informačního systému od hardware až po aplikace. Dává možnost, v co nejkratší době, detekovat reálné ale i potenciální problémy, které se mohou vyskytnout v každodenních činnostech IT systémů. Nonstop monitorování zajistí bezpečnost a efektivitu práce IT systémů – 7 dnů v týdnu, 365 dní v roce.

Hlavní vlastnosti řešení Spectator:

Dohled nad zařízeními a dostupností služeb v síťovém prostředí

Kontrola UPS, teploty v serverových místnostech, routerů

- Aktivní i pasivní sběr informací

- Použití vlastních agentů nebo SNMP protokolu

- Možnost vývoje agentů nových (pro zařízení i aplikace) Notifikace

Notifikace

Oznámí problém před tím, ještě než je uživateli vůbec zjištěn

Definice alertů (OK, WARNING, CRITICAL, UNKNOWN)

Různé způsoby oznámení (e-mail, SMS...) Webová konzole operátora

Webová konzole administrátora

Aktuální stav zařízení a služeb

Historie všech záznamů

Reporty o dostupnosti zařízení služeb

Reporty o závadách a problémech

Reporty o oznámeních/notifikacích

Výhody platformy Nagios

Plně škálovatelná – systém roste s potřebami společnosti bez nutnosti vybavování novou technickou infrastrukturou či nákupem licencí
Využívá současné infrastruktury k přenosu dat (vyžaduje IP síťové prostředí)
Umožňuje rychlou implementaci s minimálním vlivem na monitorované systémy
Běží na Linuxu – operační systém s nízkým TCO
Jednoduše adaptabilní na specifické potřeby klienta
Má pokročilé metody analýzy problémů (zabraňuje falešným notifikacím apod.)
Umožňuje eskalaci notifikací dle definovaných kritérií
Nevyžaduje instalaci žádného specifického software (pro dohledový server je třeba jen – C compiler, Perl interpreter, WWW server)
Díky otevřenému kódu není zákazník závislý na jedné vývojářské společnosti/dodavateli

4.2.2

S&T CZ provozuje ve vlastních prostorách ServiceDesk, který je rozdělen na několik virtuálních týmů dle klienta a typu práce (HelpDesk, Kvalifikace, Dispečink, Dohled). Všechny členy ServiceDesku spojuje jedna technologická základna telefonického CallCentra od společnosti Alcatel s nadstavbou pro profesionální CallCentra Genesys. ServiceDesk pracuje s vlastním IMS společnosti stejně jako s informačními systémy našich klientů. Plné služby ServiceDesku poskytujeme v době 8x10 a 24x7 v stand-by režimu s dohledem systémů našich klientů v nonstop režimu. Procesy ServiceDesku jsou standardizovány s tím, že pro každého klienta jsou upraveny v průběhu implementace služby tzv. "na míru" klienta a jeho požadavků.

IT ServiceDesk představuje provoz centrálního místa Dodavatele pro hlášení a evidenci požadavků Objednatele souvisejících s plněním Služby ve lhůtách uvedených v SLA. Součástí této Dílčí služby je zejména:

Příjem požadavků na odstranění vad

- Evidence požadavků na straně S&T
- Evidence průběhu řešení a výsledného řešení požadavků na odstranění vad
- Technická podpora zaměstnanců odboru ICT Zadavatele
- Spolupráce s pracovníky odboru ICT Zadavatele a s dodavateli třetích stran při odstraňování problémů
- Poskytování informací o dodávaných službách pro odbor ICT Zadavatele
- Příprava podkladů pro reporting

Hlavními charakteristickými rysy služeb ServiceDesk jsou:

- Užívání metodických standardů a ověřené procesní metodologie ITSM
- Víceúrovňová struktura umožňující typovou segmentaci a vyšší efektivitu práce

S&T poskytuje komplexní služby outsourcingu, které pokrývají celý životní cyklus od návrhu řešení a architektury, přes poskytování technologií formou služby, řízení změn v průběhu životního cyklu až po provozování a podporu infrastruktury. Funkce ServiceDesku je nedílnou součástí provozu a podpory a S&T takový IT ServiceDesk provozuje pro řadu významných klientů v České republice, srovnatelných co do velikosti se Zadavatelem.

ServiceDesk S&T je jeden tým pracující ve sdíleném režimu pro více zákazníků, fyzicky umístěný v prostorách S&T. ServiceDesk je organizován do několika vrstev rozdílnými rolemi v rámci procesů ITIL.

Název	
	Primární kontaktní místo pro Incident Management, Request uživatele IT Fulfillment, Access Management
	Management, Release and Deployment, Operations Management (provozní)
Level 3	

4.2.2.1. Incident Management Solvedirect

Solvedirect je plně webová online aplikace specificky vytvořená pro práci s požadavky. Je jedním z nejčastěji užívaných systémů outsourcingovými společnostmi a společnostmi poskytujícími servisní služby více zákazníkům z jednoho nástroje. Systém jako takový je provozován buď formou Cloudu (SaaS) nebo méně častou formou instalované vlastní instalované stand-alone aplikace.

Systém Solvedirect obsahuje všechny klíčové funkcionality pro management požadavků tedy:

Databáze kontaktů, lokalit, zařízení, software, výrobců atd.

Procesní workflow, které lze libovolně měnit a upravovat

Eskalační a notifikační nástroje (SMS, mail atd.)

Měření SLA (hodnoty odezva, oprava/náprava)

Silný reporting všech hodnot souvisejících s požadavky (kvantitativní, kvalitativní)

Webové rozhraní jak pro běžné prohlížeče, tak pro přístup z mobilních zařízení

Znalostní databáze

A mnoho dalších funkcí. Detaily lze nalézt na stránkách výrobce <http://www.solvedirect.com>

Reporting a evidence

Reporting a evidence zahrnuje vedení evidence Zařízení přenechaných k užívání Objednateli a vytvoření sady pravidelných reportů, které zahrnují informace a to zejména:

Reporting

- Počtu servisních požadavků a reklamací
 - Seznam s počty roztríděný po jednotlivých měsících a letech
 - Pole detailního seznamu budou obsahovat všechna data relevantní k daným požadavkům a reklamacím
 - Řešeno on-line reportem z logického celku reportingu "Množství Volání" viz. metodika níže
- Plnění SLA parametrů u incidentů a reklamací
 - Seznam s procentem plnění SLA po jednotlivých měsících a letech
 - Pole detailního seznamu budou obsahovat časová razítka ze který je proveden výpočet procenta dosaženého SLA
 - Řešeno on-line reportem z logického celku reportingu "Úroveň Služby" viz. metodika níže
- Přehled obnovy techniky v případě havárie včetně plnění SLA
 - Seznam s počty a plněním SLA roztríděný po jednotlivých měsících a letech
 - Řešeno on-line kombinací reportů z celků "Množství Volání" a "Úroveň Služby"
- Přehled plnění harmonogramu obnovy techniky
 - Report s plánem harmonogramu a časovými razítky finální realizace
 - Řešeno on-line reportem exportovaným z CMDB s časovými razítky
- Přehled instalací jednotlivých Image na zařízeních.
 - Seznam zařízení s detaily ze CMDB mezi které patří i verze image
 - Řešeno on-line reportem exportovaným z CMDB s detaily o verzích image
- Přehled dostupných opravných balíčků k centrální distribuci včetně údajů o případné distribuci

- Seznam všech opravných balíčků s uvedeným stavem
- Stav: žádost na balíček, v přípravě, testování, připraveno k distribuci, distribuováno
- Přehled dostupných opravných balíčků; které nelze distribuovat centrálně včetně údajů o případné distribuci
 - Rozšířený seznam viz. bod výše o stav nelze distribuovat s uvedením důvodu
 - Jelikož se jedná o balíčky nedistribuované automaticky bude řešeno seznamem udržovaným Service Manažerem s využitím odpovídajícího SW nástroje
- Přehled využívání služeb dodavatele podle jednotlivých katalogových listů
 - Report s počty požadavků na každý katalogový list po jednotlivých měsících a letech – KL bude zaveden do systému jako PrvekSmlouvy viz. metodika níže
 - Řešeno on-line reportem z logického celku reportingu "Množství Volání" viz. metodika níže

Evidence SW

- Evidence SW instalovaného v místě odběratele
 - Podle druhů SW
 - Podle HW na kterém je instalován

Evidence SW bude realizována na vstupu typováním použité verze SW do CMDB. Změna zařízení, SW nebo reinstalace povede vždy k aktualizaci dat v CMDB. Každé HW má v CMDB vlastní sadu polí mezi které patří i pole pro uložení potřebných informací o SW.

Seznam bude obsahovat detaily o HW i SW (výrobní číslo, typ, verze atd.) s uvedením verze image/SW.

- Řešeno on-line reportem ze CMDB

Evidence HW

- Evidence HW instalovaného v místě odběratele, která bude obsahovat minimálně tyto povinná pole:
 - Konfigurace
 - TypUmístění
 - Výměna
 - Vyřazení
 - Servis

Stejně jako evidence SW je detailní evidence všech atributů HW výše uvedených, součástí CMDB. Mimo výše uvedená datové pole bude seznam rozšířen o další důležité informace např.: Inventární číslo, model/typ, odpovídající servisní SLA, datum a jméno k poslední editaci záznamu v CMDB.

- Řešeno on-line reportem ze CMDB

4.2.2.2. Metodika poskytování a příklady reportů

Vytváření reportů je v kompetenci role Service Manažera. Jedná se o klíčovou službu pro měření kvalitativních a kvantitativních parametrů dodávaných služeb.

Vstupy do procesu měření a reportingu kvalitativních a kvantitativních parametrů jsou především:

- SLA – tedy klientem smluvně definované parametry, jež služba musí dlouhodobě splňovat
- OLA – interní mimo smlouvu definované parametry, které slouží k měření návazných služeb
- CSI – subjektivní hodnocení spokojenosti zákazníka nebo uživatelů s poskytovanými službami
- CMDDB – databáze obsahující veškerá a detailní data o HW, SW a všech realizovaných službách a aktivitách

Výstupy z procesu měření a reportingu kvalitativních a kvantitativních parametrů se předkládají ve dvou informačních vrstvách. První je tzv. souhrnný jednostránkový DashBoard, jež slouží k rychlému shrnutí celkové kvality všech poskytovaných dílčích služeb a je využíván především managementem zákazníka a dodavatele. Druhá informační vrstva je mnohem detailnější (až na úroveň dat z CMDDB). Tuto vrstvu reportů a detailu využívají především nominovaní Service Manažeři k detailní analýze trendů, problémů, návrhů na zlepšení atd.

Základem druhé vrstvy nebo také úrovně reportingu jsou on-line generované reporty u kterých jsou k dispozici následující funkcionality:

Jedním klikem export do Excelu, CSV a XML souborů

Jedním klikem export do PDF

Drill–Down funkcionality

Seznam instalované báze HW/SW

Drill–Down umožňuje z každého on-line reportu proklikáváním vstupovat do dat ze kterých je report složen nebo vypočítán. Tedy lze jedním klikem z přehledové tabulky např. s počty instalací/oprav v jednotlivých měsících vstoupit do detailního seznamu s popisy jednotlivých instalací/oprav, a dalším klikem zobrazit úplný detail jedné jediné instalace nebo opravy včetně všech příloh, časů a komentářů techniků i uživatelů.

První úroveň reportingu – DashBoard

V první vrstvě (tzv. DashBoard) jsou prezentována především tyto data:

Percentuální plnění SLA

Index hodnocení zákazníka a uživatelů

Součástí bývá i souhrn finanční kalkulace/podklad pro fakturaci

Screenshot DashBoardu – záložky obsahují další detaily

DashBoard je generován na konci každého kalendářního měsíce a je podkladem pro pravidelné měsíční vyhodnocování poskytovaných služeb smluvními stranami včetně odsouhlasení souvisejících finančních podkladů.

DashBoard může být se základními parametry poskytovaných služeb generován kdykoli v průběhu i on-line. Tento on-line náhled může být zobrazen na dohledovém displeji

nebo mobilním zařízením Service Manažera dodavatele pro aktuální přehled stavu všech klíčových parametrů poskytovaných služeb.

Screenshot on-line pohledu na webový DashBoard

Druhá úroveň reportingu – detailní reporty

Ve druhé vrstvě jsou prezentována především detailní přehledové reporty ze CMDB obsahující počty incidentů, kategorie, aktivity, lokality atd. Všechny reporty z této vrstvy jsou k dispozici vždy (24x7) on-line Service Manažerovi zákazníka i odběratele.

V této úrovni reportingu je rozsah možností pro generování různých reportů natolik rozsáhlá, že umožňuje on-line přístup k více jak 200 kusům reportů. Tuto rozmanitost a hloubku získá i neškolený Service Manažer zákazníka přes intuitivní on-line webové rozhraní které je zdarma bez limitu počtu Service Manažerů nebo jiných uživatelů ze strany zákazníka.

Webové rozhraní obsahuje desítky parametrů, kterými lze výsledný report ovlivňovat (filtrovat, omezovat, třídit, zobrazovat). Sady reportů jsou zde rozděleny do tří logických celků:

1. Množství Volání – výstupem této skupiny reportů jsou vždy počty (součty incidentů, změn apod.)
2. Úroveň Služby – výstupem této skupiny jsou procenty vyjádřené hodnoty proti nastaveným SLA
3. Čas Služby – výstupy z této skupiny jsou časové hodnoty v minutách a hodinách (např. délka trvání oprav atd.)

Screenshot třech základních kategorií on-line reportingu

Množství Volání

Základní logika reportů je postavena na dvou částech. První část, první třetina níže uvedeného screenshotu určuje, jaký typ reportu bude vygenerován (seskupení reportu). Parametry v další, tedy spodní části, určují filtry obsahu reportu samotného.



Hlavní pohled na tvorbu reportů ze skupiny Množství Volání

Níže uvádíme kompletní seznam možných reportů (tedy seskupení podle pole) v celku Množství Volání:

- | | | |
|------------------------------------|-----------------------|-------------------------------|
| ◦ Poskytovatel | ◦ Umístění | ◦ ProvincieKontaktu |
| ◦ ProvinciePoskytovatele | ◦ ProvincieUmístění | ◦ KategorieKontaktu |
| ◦ KategoriePoskytovatele | ◦ KategorieUmístění | ◦ ProvincieOperátoraHelpDesku |
| ◦ StátPoskytovatele | ◦ Komponenta | ◦ KategorieOperátoraHelpDesku |
| ◦ OrganizacePoskytovatele | ◦ DruhZařízení | ◦ Fronta |
| ◦ KategorieOrganizacePoskytovatele | • Výrobce | ◦ Fronta2 |
| ◦ ProvincieOrganizacePoskytovatele | ◦ KategorieVolání | ◦ Fronta3 |
| ◦ Zákazník | ◦ KategorieVolání1+2 | ◦ ÚroveňFronty |
| ◦ KategorieZákazníka | • KategorieVolání1–3 | ◦ Řešitel |
| ◦ ProvincieZákazníka | ◦ KategorieVolání1–4 | ◦ Řešitel2 |
| ◦ StátZákazníka | ◦ KategorieVolání1–5 | ◦ Řešitel3 |
| ◦ Organizace Zákazníka | ◦ KategoriePříčiny | ◦ DruDodavateležadavku |
| ◦ KategorieOrganizaceZákazníka | ◦ KategoriePříčiny1+2 | ◦ SkupinaStavůVolání |
| ◦ ProvincieOrganizaceZákazníka | ◦ KategoriePříčiny1–3 | ◦ SkupinaPriorit |
| ◦ Smlouva | • KategoriePříčiny1–4 | ◦ TypSkupinyProblému |
| ◦ PrvekSmlouvy | ◦ KategoriePříčiny1–5 | ◦ SkupinaTypůChyb |
| ◦ Priorita | ◦ PříjmeníVolajícího | ◦ SkupinaZávažnosti |
| ◦ DruDodavateleproblému | ◦ PoskincieVolajícího | |
| ◦ DruhChyby | ◦ KategorieVolajícího | |
| ◦ Závažnost | | |

• StavVolání

Základní filtry pro reporty (seskupení podle) v této skupině jsou:

- Otevřená Volání – do reportu jsou zahrnuty všechna vytvořená volání
Uzavřená Volání – do reportu jsou zahrnuty již jen ukončená volání
Časové hodnoty – vymezení hodnot od kdy, do kdy má report být vygenerován
- Časová granularita – vymezení detailu
 - na rok
 - na měsíce a roky
 - na pracovní dny v měsíci a roce
 - na dny

V této sadě reportů "Množství Volání" jsou položky typu reportu (seskupení reportu) a parametry pro kompletní seznam filtrů obsahu reportu shodné.

Níže uvádíme nejčastěji využívané reporty ze sady Množství Volání:

Počet požadavků rozdělený podle typu požadavku

Počet požadavků rozdělený podle jejich priority

Počet požadavků podle kategorie zařízení

Počet požadavků podle druhu/typu zařízení a SW

Úroveň služby

Základní logika reportů této skupiny je postavena stejně jako ta předchozí na dvou částech. První část, první třetina níže uvedeného screenshotu určuje, jaký typ reportu bude vygenerován (seskupení reportu). Parametry v další, tedy spodní části, určují filtry obsahu reportu samotného.

Hlavní pohled na tvorbu reportů ze skupiny Úroveň Služby

Níže uvádíme kompletní seznam možných reportů (tedy seskupení podle pole) ve skupině Úroveň Služby:

- SLA
- Poskytovatel
- OrganizacePoskytovatele
- KategorieOrganizacePoskytovatele
- Zákazník
Organizace Zákazníka
- KategorieOrganizaceZákazníka
- Smlouva
- PrvekSmlouvy
- Naplnění
- Odchylka
- Distribuce

Základní filtry pro reporty (seskupení podle) v této skupině jsou:

- Otevřená Volání – do reportu jsou zahrnuta všechna vytvořená volání
- Uzavřená Volání – do reportu jsou zahrnuta již jen ukončená volání
- Rozsah Distribuce – v procentech, nastavení pro vyobrazení jak daleko od předepsaného SLA se nachází reálně dosažená hodnota kvality služby
- Typ SLA – zda bude generován report nad parametrem Odezva (Response Time) nebo Obnovení (oprava, Fix Time)
- Časové hodnoty – vymezení hodnot od kdy, do kdy má report být vygenerován
- Časová granularita – vymezení detailu
 - na rok
 - na měsíce a roky
 - na měsíc
 - na dny

V této sadě reportů "Úroveň Služby" jsou k dispozici tyto parametry pro tvoření filtrů obsahu reportu:

• Poskytovatel	Umístění	ProvincieKontaktu
• ProvinciePoskytovatele	ProvincieUmístění	KategorieKontaktu
• KategoriePoskytovatele	KategorieUmístění	ProvincieOperátoraHelpDesku
• StátPoskytovatele	Komponenta	KategorieOperátoraHelpDesku
• OrganizacePoskytovatele	DruhZařízení	Fronta
• KategorieOrganizacePoskytovatele	Výrobce	Fronta2
• ProvincieOrganizacePoskytovatele	KategorieVolání	Fronta3
• Zákazník	KategorieVolání1+2	ÚroveňFronty
• KategorieZákazníka	KategorieVolání1–3	Řešitel
• ProvincieZákazníka	KategorieVolání1–4	Řešitel2
• StátZákazníka	KategorieVolání1–5	Řešitel3
• Organizace Zákazníka	KategoriePříčiny	DruDodavateložadavku
• KategorieOrganizaceZákazníka	KategoriePříčiny1+2	SkupinaStavůVolání
• ProvincieOrganizaceZákazníka	KategoriePříčiny1–3	SkupinaPriorit
• Smlouva	KategoriePříčiny1–4	TypSkupinyProblému
• PrvekSmlouvy	KategoriePříčiny1–5	SkupinaTypůChyb
• Priorita	PříjmeníVolajícího	SkupinaZávažnosti
• DruDodavatelroblému	ProvincieVolajícího	
• DruhChyby	KategorieVolajícího	
• Závažnost		
• StavVolání		

Níže uvádíme nejčastěji využívané reporty ze sady Množství Volání:

Celkový pohled na procentuální plnění SLA parametrů Odezva a Obnova

Screenshot zachycující percentuální plnění SLA po jednotlivých měsících s rozdělením na jednotlivé poskytované služby

Percentuální přehled plnění SLA za jednotlivé měsíce včetně procenta ještě rozpracovaných požadavků

Odchylka od definovaného SLA v hodinách – slouží k analýze trendu kvality služby

Report distribuce plnění definovaných SLA – jak percentuálně je rychlé plnění SLA v rozsahu –50% až +50% (volitelné)

Čas služby

Základní logika reportů této skupiny je postavena stejně jako ta předchozí na dvou částech. První část, první třetina níže uvedeného screenshotu určuje, jaký typ reportu bude vygenerován (seskupení reportu). Parametry v další, tedy spodní části, určují filtry obsahu reportu samotného.

Hlavní pohled na tvorbu reportů ze skupiny Úroveň Služby

Níže uvádíme kompletní seznam možných reportů (tedy seskupení podle pole) ve skupině Úroveň Služby:

- Poskytovatel
- OrganizacePoskytovatele
- KategorieOrganizacePoskytovatele
- Zákazník
- Organizace Zákazníka
- KategorieOrganizaceZákazníka
- Smlouva
- PrvekSmlouvy
- Distribuce

Základní filtry pro reporty (seskupení podle) v této skupině jsou:

Otevřená Volání – do reportu jsou zahrnuty všechna vytvořená volání

Uzavřená Volání – do reportu jsou zahrnuty již jen ukončená volání

Rozsah Distribuce – v hodinách, nastavení pro vyobrazení jak dlouho od předepsaného SLA se nachází reálně dosažený čas

Typ SLA – zda bude generován report nad parametrem Odezva (Response Time) nebo Obnovení (oprava, Fix Time)

- Časové hodnoty – vymezení hodnot od kdy, do kdy má report být vygenerován
- Časová granularita – vymezení detailu
 - na rok
 - na měsíce a roky
 - na měsíc

V této sadě reportů "Úroveň Služby" jsou k dispozici tyto parametry pro tvoření filtrů obsahu reportu:

• Poskytovatel	• Umístění	ProcincieKontaktu
• ProvinciePoskytovatele	ProvincieUmístění	KategorieKontaktu
KategoriePoskytovatele	KategorieUmístění	ProvincieOperátoraHelpDesku
StátPoskytovatele	Komponenta	KategorieOperátoraHelpDesku
OrganizacePoskytovatele	DruhZařízení	Fronta
KategorieOrganizacePoskytovatele	Výrobce	Fronta2
ProvincieOrganizacePoskytovatele	KategorieVolání	Fronta3
Zákazník	KategorieVolání1+2	ÚroveňFronty
KategorieZákazníka	KategorieVolání1–3	Řešitel
ProvincieZákazníka	KategorieVolání1–4	Řešitel2
StátZákazníka	KategorieVolání1–5	Řešitel3
Organizace Zákazníka	KategoriePříčiny	DruDodavateležadavku
KategorieOrganizaceZákazníka	KategoriePříčiny1+2	SkupinaStavůVolání
ProvincieOrganizaceZákazníka	KategoriePříčiny1–3	SkupinaPriorit
Smlouva	KategoriePříčiny1–4	TypSkupinyProblému
PrvekSmlouvy	KategoriePříčiny1–5	SkupinaTypůChyb
Priorita	PříjmeníVolajícího	SkupinaZávažnosti
DruDodavatelroblému	PoskincieVolajícího	
DruhChyby	KategorieVolajícího	
Závažnost		
StavVolání		

Níže uvádíme nejčastěji využívané reporty ze sady Množství Volání:

V hodinách vyjádřená doba potřebná k vyřešení požadavků v jednotlivých měsících na všechny typy SLA

V hodinách vyjádřená doba potřebná k vyřešení požadavků v jednotlivých měsících v detailu podle SLA

Počty a procentuálně vyjádřená distribuce délky řešení SLA v krocích a rozsahu od 10 do 480 hodin (volitelné)

CMDb – online přístup k instalované bázi

Součástí reportingu jsou i data z CMDb, tedy databáze, která obsahuje informace o instalované bázi. Ke každému zařízení je přiřazeno smluvně stanovené SLA a další informace. Tento přehled je k dispozici on-line přes webové rozhraní a poskytuje plnou funkcionalitu obvyklou pro ostatní reporty tedy především:

- Fulltextové vyhledávání

- Vyspělou filtraci (část řetězce, hodnoty, limity, prázdné/plné hodnoty atd.)
- Seskupování (grouping) podle polí viz. níže

Export do Excelu, CSV a XML následujících polí:

- Zkrácený název
- Typ/Model
- Sériové číslo
- IPAdresa
- Produktová skupina
- Výrobce
- Smlouva SLA
- Lokalita
- Ulice
- Město
- JeAktivní
- ZačátekZáruky
- KonecZáruky
- ÚdržbaDo
- HlavníOčekávání
- HlavníDatum
- MěsíceÚdržby
- PlánovanýPočetÚdržby
- OtevřenýPočetÚdržby
- ÚdržbaJeAktivní

Seznam informací které lze na požádání a zdarma do reportů pro Service Manažery přidat je velmi rozsáhlý a obsahuje přes 50 dalších polí z databáze CMDb. Pole, jež budou využita pro poskytování služby odpovídají požadavkům na informační hodnotu reportů a jsou součástí dohody na počátku poskytování služeb.

Přehled nad celou instalovanou bází

Seskupení zařízení podle SLA; znaménkem "+" vlevo se zobrazí seznam zařízení s daným SLA

Seskupení instalované báze podle Modelu; znaménkem "+" vlevo se zobrazí seznam zařízení daného Modelu

Seskupení zařízení podle lokality, na které jsou nainstalována; znaménkem "+" vlevo se zobrazí seznam

4.3. Havarijní scénáře

4.3.1. Metodika zpracování analýzy rizik

Každý projekt je ovlivněn řadou faktorů, které mohou mít negativní vliv na dosažení cíle. Řízením rizik se snažíme eliminovat či zmírnit výskyt nemilých překvapení a to po celou dobu provozu IS. Prvním krokem je určení odpovědných osob za všechny zúčastněné strany, které se řízením rizik budou zabývat.

Při samotném řízení rizik, které bude probíhat nejen na začátku projektu, ale v celém průběhu poskytování podpory IS, budou prováděny tyto činnosti:

4.3.1.1. Identifikace/analýza rizik

Identifikaci rizik můžeme charakterizovat jako pravidelné a kontinuální monitorování všech probíhajících interních a externích událostí, které ovlivňují naplňování cílů. U těchto událostí pak rozlišujeme pozitivní nebo negativní dopad. Události, které mají negativní dopad, jsou rizika.

4.3.1.2. Zpracování analýzy rizik a hodnocení rizik

Vzhledem k množství rizik je třeba je zanalyzovat a určit jejich pravděpodobnost a dopad, tím určit jejich významnost a prioritu jejich řešení.

Rizika mohou být vyjádřena kvalitativně a kvantitativně. V rámci počáteční fáze projektu i fáze podpory IS zvolíme kvalitativní vyjádření – malý, střední, velký, kritický. Vyhodnocení významnosti rizik může provádět buď dostatečně odborně vybavený jednotlivec, nebo skupina odborníků, v případě tohoto projektu hodnocení provádí pracovní tým projektu a schvaluje ŘV.

4.3.1.3. Strategie zvládnutí rizik

Jedná se o určení způsobu, jak se s daným rizikem vypořádáme, jak ovlivníme jeho dopad a pravděpodobnost – zda se ho raději vyvarujeme, akceptujeme ho, minimalizujeme ho či ho přeneseme.

Výsledek identifikace, vyhodnocení a strategie zvládnutí rizik je zaznamenán do tzv. registru rizik, který je veden v elektronické formě.

Kromě klasifikace rizik obsahuje i nápravná opatření a sledování jejich úspěšné aplikace. Důležité je také určit odpovědnou osobu spojenou s provedením preventivního opatření.

4.3.1.4. Monitorování, vykazování a reportování

Pravidelná aktualizace registru rizik je potřebná pro včasnou identifikaci případných nových rizik, přehodnocování dříve identifikovaných rizik, posuzování opatření na jeho zvládnutí (původní strategie funguje, není potřeba nějaká změna?), aktualizace dokumentace, komunikace.

Během jakéhokoli projektu se mohou objevit další rizikové události, a proto musejí být rizika stále monitorována.

Registr rizik bude mít minimálně tyto položky (příklad v tabulce níže).

Riziko	Popis Rizika		Dopad	Váha Rizika		Řešení	Vlastník
	Popis	Událost					
1.	Dostupnost všech SW nástrojů a přístupů	Spatné plnění SLA s možným dopadem na koncové uživatele (Zadavatel/S&P)	Vysoký: 3			Zajištění že	
			Střední: 2	X		jsou všem	

	Malé	Malé změny, které mají dokumentovaný a vyzkoušený postup implementace s <i>velmi malým</i> dopadem na podnikání.	S&T upozorní Zadavatele <i>pět dní před</i> provedením změny. Postačuje zpráva Zadavatele bez potvrzení o jejím přijetí.	Instalování nového service packu na server.
	Střední	Změny, které mohou ohrozit vícero aplikací a mají <i>širší</i> dopad na podnikání.	S&T upozorní Zadavatele <i>pět dní před</i> provedením změny. Zadavatel <i>musí</i> potvrdit přijetí zprávy.	Instalace nebo reinstalace serveru, změny v LAN.
		Změny, které mohou ohrozit vícero aplikací skrze celou společnost a mají <i>signifikantní dopad</i> na podnikání.	S&T upozorní Zadavatele <i>deset dní před</i> provedením změny. Zadavatel <i>musí</i> potvrdit přijetí zprávy.	Spuštění nového antiviru, změna IS. Komplexní výměna HW včetně SW.
	Kritické (mimo prac. dobu)	Změny, které musí být provedeny za účelem zprovoznění havarované IT služby s <i>nějakým dopadem</i> na podnikání.	S&T <i>co nejdříve</i> po zjištění nutnosti takové změny informuje Zadavatele. Potvrzení takové zprávy od Zadavatele je preferováno.	"Zatuhlá" služba na serveru – musí být opraveno ještě před začátkem zálohování.
		Změny, které musí být	S&T informuje Zadavatele	Útok viru.

5. Projektové řízení, organizace a harmonogram projektu

Uchazečem navrhované řešení bude respektovat požadavky zadavatele a to zejména s ohledem na co nejvyšší kvalitu a propracovanost metodiky projektového řízení a organizace projektu včetně účinné kontroly a navržených opatření k zajištění cílů projektu, dále na komplexnost a propracovanost navrženého harmonogramu a přístupů pro zajištění realizovatelnosti projektu.

Zhotovitel bude celý projekt implementovat a řídit primárně dle mezinárodně uznávané metodiky IPMA, a dále dle dalších specifických metodik a standardů zohledňující dlouholeté působení uchazeče ve státní správě, které jsou nejvhodnější pro specifické dílčí části plnění cílů projektu.

5.1. Popis způsobu a metodiky projektového řízení, organizace účastníků projektu

5.1.1. Organizace

Řízení projektu bude založeno na tříúrovňové hierarchii, bude tedy zabezpečeno prostřednictvím tří základních řídicích úrovní.

Nejnižší úroveň řízení jsou **pracovní týmy (PT)**, které jsou ustaveny k plnění konkrétního rozsahu úkolů v předem určených dílčích oblastech. Úkolem pracovních týmů je řešení běžných operativních, výrobních, logistických a dalších záležitostí, kontrola plnění dílčích úkolů dle harmonogramu a vytváření případných zadání požadavků na změnu na základě předložených návrhů. Výstupy z pracovních týmů a záležitosti, které potřebují rozhodnutí vyšší úrovně řízení, včetně požadavků na změnu, se ke schválení předávají na vyšší úroveň řízení a to na **Hlavní tým projektu (HTP)**.

Hlavní tým projektu (HTP) je základní řídicí platformou projektu, která má za úkol zajistit soulad postupu prací na projektu se schváleným věcným a časovým plánem. Hlavní tým projektu zároveň schvaluje všechny požadavky na změnu, financované z prostředků příslušné smlouvy. Nejvyšší strategickou úroveň řízení projektu pak zajišťuje **Řídicí výbor projektu (ŘV)**.

Řídicí výbor projektu (ŘV) řeší na nejvyšší řídicí úrovni zásadní otázky týkající plnění či neplnění hlavních záměrů projektu jako celku. Zároveň přijímá opatření definuje další postup v případě krizových stavů v rámci projektu.

Ze všech jednání týmů na všech úrovních jsou odpovědnými osobami dodavatele pořizovány zápisy, které jsou distribuovány k oponentuře všem členům příslušného týmu. Po zpracování připomínek je zápis schválen a uložen.

5.1.2. Struktura a kompetence orgánů řízení projektu

5.1.2.1. Řídicí výbor projektu (ŘV)

Nejvyšší strategická úroveň řízení projektu, na které se řeší zásadní otázky týkající se plnění či neplnění hlavních záměrů projektu jako celku, rozhoduje o případech eskalovaných z úrovně HTP, které se nepodařilo vyřešit na nižších úrovních a přijímá opatření a definuje další postup v případě krizových stavů. ŘV zpravidla rozhoduje na základě připravených podkladů vypracovaných hlavním týmem projektu nebo pro tyto účely ustavenými poradními či pracovními skupinami.

ŘV se bude scházet pravidelně nejméně 1× za čtvrtletí. V případě potřeby může podat návrh na svolání mimořádné schůzky ŘV vedoucí projektu objednatele nebo vedoucí projektu dodavatele s uvedením důvodů pro mimořádnou schůzku. Uskutečnění mimořádné schůzky a její termín schvaluje vedoucí projektu objednatele.

Dodavatel navrhuje následující minimální složení ŘV:

- Zástupci objednatele
 - Zástupce vrcholového vedení Objednatele
 - Vedoucí projektu Objednatele
- Zástupci dodavatele
 - Vedoucí projektu dodavatele (Řídicí manažer ŘV)
 - Zástupce vedoucího projektu dodavatele
 - Zástupce vrcholového managementu dodavatele

Na jednání ŘV mohou být fakultativně přizváni i další zástupci objednatele a dodavatele dle projednávané problematiky (zástupci odborných útvarů objednatele, garant infrastruktury dodavatele apod.).

5.1.2.2. Hlavní tým projektu (HTP)

Základní řídicí platforma projektu, na které jsou projednávány výstupy z pracovních týmů a záležitosti, které potřebují rozhodnutí vyšší úrovně řízení. Hlavní tým projektu zároveň schvaluje všechny požadavky na změnu, financované z prostředků příslušné smlouvy.

Dodavatel navrhuje následující složení HTP:

- Zástupci objednatele
 - Vedoucí projektu objednatele
 - Zástupci zainteresovaných odborů poskytovatele (vedoucí nebo jimi delegovaní zástupci)
 - Odborní garanti odběratele:
 - Garant IS (osoba odpovědná za provoz ICT objednatele)
 - Garant provozu aplikační vrstvy
 - Garant bezpečnosti objednatele
 - atd.
- Zástupci dodavatele
 - Zástupce vedoucího projektu dodavatele (řídicí manažer HTP)
 - Vedoucí projektu dodavatele
 - Odborní garanti dodavatele dle časových etap a věcné problematiky:
 - Garant IS
 - Garant provozu
 - Garant bezpečnosti
 - atd.

Jednání HTP se mohou účastnit podle potřeby i další zástupci objednatele, to pravidelně či pouze pro potřeby projednání specifického tématu, avšak vždy se souhlasem vedoucího projektu objednatele. Obdobně se jednání HTP mohou účastnit podle potřeby i další zástupci dodavatele, a to pravidelně či pouze pro potřeby projednání specifického tématu, avšak vždy se souhlasem vedoucího projektu dodavatele nebo zástupce vedoucího projektu poskytovatele.

Jednání HTP se koná pravidelně nejméně 1x za dva týdny.

Pro každé jednání HTP bude připravena ze strany dodavatele agenda; z každého jednání dodavatel zpracuje zápis, který bude po kontrole vedoucím projektu objednatele za obě strany podepsán. Výstupy z jednání budou promítány i do další projektové dokumentace.

HTP využívá pro svou práci výstupů činnosti z úrovně pracovních či poradních týmů (PT) nebo jednotlivců.

Minimální agenda pravidelného jednání HTP o stavu projektu bude v rozsahu:

- Projednání a schválení zdroje financování předložených požadavků na změnu (jsou-li předloženy).
- Projednání a odsouhlasení dokumentů/návrhů připravených pracovními týmy.
- Kontrola plnění úkolů – za období od předchozího jednání.

Pokud mají projednávání skutečnosti dopad na celkový časový, finanční nebo věcný rozsah plnění dle smlouvy, je nutné jejich projednání a schválení na ŘV.

5.1.2.3. Pracovní týmy

Pracovní týmy představují nejnižší úroveň řízení a jsou ustaveny k plnění konkrétního rozsahu úkolů v předem určených dílčích oblastech. Úkolem pracovních týmů je řešení běžných provozních záležitostí, kontrola plnění dílčích úkolů dle harmonogramu a vytváření zadání požadavků na změnu na základě předložených návrhů.

Úkolem pracovního týmu je především:

- kontrola plnění dílčích úkolů,
řešení běžných provozních problémů,
vytváření a připomínkování dílčích výstupů projektu,
eskalace nestandardních/neplánovaných situací a zjištěných rizik, které vznikly nebo byly identifikovány v průběhu realizace projektu,
vytváření zadání požadavků na změnu, schvalování požadavků na změnu z věcného hlediska, návrh způsobu financování pro požadavky na změnu k předložení na jednání HTP,
- příprava podkladů pro Hlavní tým projektu.

Schůzky pracovního týmu navrhujeme v týdenních intervalech, pokud nebude dohodnuto jinak. Z jednání pracovních týmů bude vždy pořízen zápis, který bude distribuován k připomínkám všem zúčastněným osobám a jiným zainteresovaným stranám.

Dodavatel navrhuje následující složení PT:

Vedoucí pracovního týmu dodavatele

Zástupce vedoucího projektu dodavatele

Dle konkrétní situace delegování pracovníci Zadávatelie

Na jednání jednotlivých pracovních týmů mohou být fakultativně přizváni další zástupci objednatele a dodavatele dle projednávané problematiky.

5.1.3. Hlavní role projektu

5.1.3.1. Vedoucí projektu objednatele

Vedoucí projektu objednatele je zástupce objednatele, odpovědný za koordinaci činností, spojených s realizací projektu na straně objednatele na úrovni Hlavního týmu projektu.

Zejména se jedná o:

- určení a koordinaci jednotlivých odborných garantů relevantních systémů na straně objednatele,
- zajištění součinností na straně objednatele,
- kontrolu přidělených úkolů a odpovědnost za splnění těchto úkolů vůči HTP,
- koordinaci časových možností na straně objednatele (řešení časových kolizí s jinými pracovními úkoly),
- koordinaci oponentury jednotlivých výstupů odbornými guaranty na straně objednatele.

Vedoucí projektu objednatele je členem Řídícího výboru a Hlavního týmu projektu. Do pracovního týmu jmenuje svého odpovědného zástupce, odpovědného na úrovni pracovního týmu za koordinaci činností spojených s realizací projektu.

5.1.3.2. Vedoucí projektu dodavatele

Zástupce dodavatele, odpovědný za koordinaci činností spojených s realizací projektu.

Především jde o:

- koordinaci aktivit celého realizačního týmu, včetně podřízených dodavatelů,
- kontrolu přidělených úkolů a odpovědnost za splnění těchto úkolů vůči HTP,
- koordinaci přípravy výstupů k oponentuře.

Vedoucí projektu dodavatele je řídícím manažerem Řídícího výboru a členem Hlavního týmu projektu.

5.1.3.3. Odborný garant IS objednatele

Zástupce objednatele, jmenovaný pro každý podporovaný či implementovaný systém.

V rámci jemu svěřenému systému odpovídá zejména za:

- definici funkčních požadavků,
- posouzení návrhů na změnu systému,
- spolupráci při zpracování zadání požadavku na změnu,
- v rámci pracovního týmu je odpovědný za schválení požadavků na změnu z věcného hlediska,
- přípravu potřebných podkladů a znalostí na schůzku (tj. přípravu na jednání dle avizované agendy schůzky pracovního týmu),
- přípravu a provedení funkčních a následně akceptačních testů dle dodavatelem zpracovaných a objednatelem schválených testovacích scénářů,

splnění úkolů definovaných na schůzce pracovního týmu v dohodnutém rozsahu a čase.

Účastní se schůzek pracovního týmu, ve výjimečných případech písemně jmenuje svého zástupce na konkrétní schůzku, které se nemůže zúčastnit. Na schůzku si může přizvat potřebný počet spolupracovníků v dané oblasti. Stále je ale jedinou odpovědnou osobou za dohodnuté závěry v rámci jemu svěřené oblasti.

5.1.3.4. Systémový a aplikační architekt

Zástupce dodavatele, který podléhá řízení Vedoucího projektu dodavatele a odpovídá za odborné činnosti a návrh i implementaci řešení v oblasti síťové a aplikační infrastruktury, databází, konsolidace datových zdrojů, serverových farem, operačních systémů, uživatelských rozhraní atd.

5.1.3.5. Garant bezpečnosti dodavatele

Pracovník na této pozici je odpovědný za zajištění procesu řízení bezpečnosti, včetně kontrol, zpracování pravidelných reportů, nezbytné dokumentace apod. V rámci své činnosti spolupracuje s garantem bezpečnosti objednatele, se kterým projednává návrhy na bezpečnostní opatření a spolupracuje při zpracování bezpečnostních auditů. Garant bezpečnosti je dále odpovědný za posuzování aktivit jednotlivých procesů řízení služeb provozu ICT z hlediska jejich vlivu na bezpečnost, tzn. za identifikaci bezpečnostních rizik, která včas eskaluje na příslušné orgány řízení projektu.

5.1.3.6. Technický specialista dodavatele

Technický specialista je odborným pracovníkem v jednotlivých oblastech realizace projektu (administrátor, analytik, architekt, operátor, konzultant) na straně dodavatele a jeho subdodavatelů. Techničtí specialisté zároveň zastávají role specialistů v jednotlivých procesech implementace a řízení služeb.

5.1.4. Projektová jednání

Rozlišují se následující dva základní typy jednání:

- kontrolní a řídicí jednání (jednání ŘV a HTP),
- pracovní schůzka – jednání pracovního týmu.

Příprava podkladů (rozbory, vypracování návrhu atd.) probíhá výhradně mimo jednání. Zajištění podkladů je vždypovinností toho, kdo jednání vede (v případě HTP je to zpravidla vedoucí projektu dodavatele), aby nedocházelo k prolínání kontrolní a řídicí činnosti s řešením konkrétních pracovních podkladů. U ad-hoc svolaných jednání zajišťuje podklady vždy ten pracovník, který jednání inicioval.

5.1.4.1. Příprava na projektová jednání

Každé jednání musí být připraveno realizováno minimálně v následujícím rozsahu:

Činnost	Odpovědnosti – ŘV	Odpovědnosti – HTP	Odpovědnosti – PT
Návrh termínu a délky	Vedoucí projektu	Vedoucí projektu	Odborný garant, Vedoucí

Činnost	Odpovědnosti – ŘV	Odpovědnosti – HTP	Odpovědnosti – PT
schůzky	objednatele	objednatele	pracovního týmu (řídící manažer)
Příprava agendy	Vedoucí projektu dodavatele	Vedoucí projektu dodavatele	Vedoucí pracovního týmu (řídící manažer)
Zajištění jednací místnosti	Vedoucí projektu objednatel	Vedoucí projektu objednatel	Odborný garant
Osobní příprava na schůzku dle agendy	Vedoucí projektu a přizvání členové	Vedoucí projektu a přizvání členové	Odborný garant, Vedoucí pracovního týmu, členové týmu dle pokynů garanta
Provedení jednání	Vedoucí projektu objednatel, Vedoucí projektu dodavatele a přizvání členové	Vedoucí projektu objednatel, Vedoucí projektu dodavatele a přizvání členové	Odborný garant, Vedoucí pracovního týmu a přizvání členové
Zpracování návrhu zápisu	Vedoucí projektu objednatel	Vedoucí projektu objednatel	Vedoucí pracovního týmu (řídící manažer)
Oponentura a odsouhlasení zápisu	Vedoucí projektu objednatel, Vedoucí projektu dodavatele	Vedoucí projektu objednatel, Vedoucí projektu dodavatele	Odborný garant, Vedoucí pracovního týmu
Realizace úkolů vyplývajících ze schůzky	Vedoucí projektu objednatel, Vedoucí projektu dodavatele	Vedoucí projektu objednatel, Vedoucí projektu dodavatele	Odborný garant a vedoucí pracovního týmu

5.1.4.2. Oponentura a schvalování zápisů

Z každého jednání připravuje příslušná odpovědná osoba ze strany dodavatele zápis.

V případě Řídícího výboru nebo Pracovního týmu je návrh zápisu zaslán e–mailem odpovědné osobě za stranu objednatel elektronickou poštou k oponentuře a je vyžádáno potvrzení o přečtení této zprávy (případně je u odpovědné osoby ověřeno, že tento zápis obdržela). Objednatel je povinen v dohodnutém termínu se k zápisu vyjádřit nebo jej odsouhlasit zpět e–mailem odesílateli zápisu, který potvrzuje vypořádání připomínek.

Zápis z pracovního týmu se stává platným a závazným již po tomto e–mailovém odsouhlasení nebo po uplynutí lhůty 3 pracovních dnů po odeslání zápisu, pokud nepřišla od odpovědné osoby objednatel zpět žádná reakce (kromě potvrzení přijetí e–mailu). Finální schválení zápisu z Řídícího výboru se provádí podpisem zápisu odpovědnými zástupci za stranu dodavatel objednatel.

V případě možnosti budou zápisy zpracovávány s využitím dataprojektoru tak, že mají možnost se k zápisu v aktuálním čase vyjádřit všechny zúčastněné strany. Zápis je pak podepisován na místě.

Zápisy jsou po schválení uloženy jako součást dokumentace projektu na dokumentačním úložišti zřízeném pro účel centrální evidence dokumentace projektu. Za ukládání a správu zápisů z jednání odpovídá až do aktivace Projektové kanceláře pracovní tým PT ADMIN.

5.2. Šablony projektových dokumentů

Uchazeč bude v rámci plnění předmětu smlouvy po celou dobu trvání projektu aplikovat metodiky a best practices projektového řízení dle standardů IPMA a ISO10.006.

Administraci projektu bude zajišťovat projektová kancelář prostřednictvím projektového manažera. Projektová kancelář umožní přístup oprávněných subjektů řízení projektu k potřebným uloženým informacím o projektu, jako jsou zejména:

- Harmonogram projektu (vzor viz kap.8.8),
- Projektová dokumentace - Analýza, Funkční specifikace, Technická specifikace, Uživatelská, Školící, Administrátorská dokumentace, apod. (dokumenty poskytnuté Zadavatele),
- Projektové výkazy činností,
Komunikační matice,
Zápisy z jednání projektových týmů (na úrovni řídicího výboru a pracovních skupin),
Zpráva o stavu projektu,
Předávací protokoly,
Akceptační protokoly,
Změnové požadavky,
Testovací protokoly,
Zpráva o ukončení projektu (předání do provozu).

5.3.

Riziko je nejistá událost nebo podmínka, která když nastane, ovlivní nepříznivě projekt z pohledu naplnění jeho cílů. Řízení rizik je soubor postupů a nástrojů sloužících k identifikaci rizik, jejich vyhodnocení a přijetí opatření k jejich omezení z pohledu vyhodnocení událostí, které mohou mít nepříznivý vliv na jakékoli události, které jsou předmětem řízení projektu.

Cílem řízení rizik je identifikace a specifikace jednotlivých rizik projektu včetně posouzení jejich dopadu a celkové závažnosti a vymezení vhodných opatření na prevenci daného rizika nebo omezení následků při reálném uplatnění daného rizika. Na základě identifikace a specifikace jsou následně vybraná opatření plánována v rámci projektu.

Některá identifikovaná rizika mohou být záměrně akceptována bez jakýchkoli opatření (nebo jen s omezenými opatřeními) s ohledem na přílišnou (danému riziku neadekvátní) náročnost některých opatření (zejména nároky na časové, finanční a lidské zdroje).

Řízení rizik projektu bude provádět průběžně Vedení projektových týmů a jejich zjištění bude konsolidováno Vedením projektu. Tuto činnost koordinuje Projektový manažer tak, aby se plně prošetřila možná rizika. Zjištěná závažná rizika, jejich dopady a návrhy na jejich řešení či omezení jsou neprodleně předkládány k posouzení a případnému rozhodnutí Řídícímu výboru projektu.

Každý projekt, bez ohledu na velikost, vždy přináší rizika a problémy spojené s jeho realizací. Je nezbytné je rozpoznat a zvládat tak, aby se minimalizovaly škody a maximalizovaly šance na úspěch.

Rizika se hodnotí podle dvou faktorů:

- Pravděpodobnosti, že se něco stane
- Důsledku, jaký bude na projekt mít to, že se to stane

5.3.1. Identifikace rizik

Metodika rozlišuje pro účely řízení rizik dvě základní skupiny:

- **Externí rizika:** rizika působící na projekt z vnějšího prostředí, které je nezávislé na bezprostředních smluvních závazcích, které spolu smluvní strany uzavřely, jejich splnitelnost však může podmiňovat. Možnost ovlivňovat výskyt externích rizik (prevence) je (s ohledem na jejich charakter) velmi omezená. V případě externích rizik jsou dominantní opatření na omezení jejich dopadů.
- **Interní rizika:** rizika projektu mající rámec ve smluvních vztazích mezi smluvními stranami. Výskyt interních rizik je možno do značné míry ovlivnit vzhledem k tomu že přímo souvisí s průběhem a vývojem projektu. V případě interních rizik jsou kombinována opatření na omezení výskytu rizik a opatření na omezení jejich dopadů.

Každé jednotlivé identifikované riziko musí být specifikováno v následujícím rozsahu:

- **Vymezení:** popis rizika a jeho projevů, na jehož základě lze riziko identifikovat,
- **Dopady:** popis možných dopadů rizika na projekt,
- **Opatření:** návrh opatření, která mohou riziko vyloučit nebo podstatně omezit jeho působení a dopady,
- **Závažnost:** určení aktuální míry ohrožení projektu daným rizikem, která je posouzena a stanovena na základě aktuální pravděpodobnosti výskytu rizika a na základě aktuální závažnosti potenciálních dopadů rizika do projektu. Zejména závažnost rizik ve škále Nízká / Střední / Vysoká je nutné přehodnocovat průběžně.

Analýza rizik bude dále prováděna na úrovni vedení projektových týmů a koordinována na úrovni vedení projektu průběžně vzhledem k tomu, že rizika projektu se mohou měnit jak co do struktury (vznik a zánik rizik), tak do povahy existujících rizik (změna specifikace rizik a to zejména aktuální závažnosti).

V průběhu projektu bude nutné rizika přehodnocovat zejména v případech přechodu mezi jednotlivými fázemi realizace projektu.

Každý člen projektového týmu je povinen neprodleně informovat nadřízeného vedoucího projektového týmu o skutečnostech, které mohou reálně negativně ovlivnit projekt. Každý vedoucí projektového týmu je povinen neprodleně zvážit informace o skutečnostech, které mohou reálně negativně ovlivnit projekt a vyhodnotí-li je jako riziko projektu, pak o tomto riziku neprodleně informovat vedoucí projektového týmu. Vedení projektu je povinno zvážit dané riziko a informovat o něm Řídící výbor projektu.

Každé jednotlivé identifikované riziko musí být vedením projektu specifikováno ve výše uvedeném rozsahu. V případě závažných rizik projektu ovlivňujících rámec projektu daný smluvní dokumentací nebo zásadně ovlivňující organizaci Zadavatele musí být Řídící výbor projektu informován neprodleně.

Za výkon identifikace rizik odpovídají všechny zainteresované strany v projektu, tj. včetně všech členů projektového týmu Dodavatele a Zadavatele. Projektový manažer udržuje celkový "Registr rizik" projektu.

5.3.2. Hodnocení rizik

Hodnocení rizik rozdělujeme následujícím způsobem na:

- Kvantitativní
 - Určíme pravděpodobnost a hodnotu ztráty, vytvoříme součin jehož hodnota je vyjádřena v peněžních jednotkách.

Kvalitativní

- Dopad a pravděpodobnost se určí verbálně (velký, malý apod.) nebo s pomocí bodovací stupnice bez peněžního významu. Tato metoda slouží k určení priority rizik.

Tato tabulka je finálním produktem identifikační části analýzy a následuje finální analytická činnost představující zatřídění rizik do jednotlivých tříd.

V praxi vypadá hodnocení rizik ze strany uchazeče následujícím způsobem. Tato tabulka je také součástí registru rizik:

Riziko1	Garant1	10	10	100		Opatření1
Riziko2	Garant2	30	5	150	1.	Opatření2
Riziko3	Garant3	15	8	120	2.	Opatření3
Riziko4	Garant3	5	2	10	4.	Opatření4
...						

Ve výše uvedené tabulce si pro každý faktor rizika (riziko) určíme:

- Pravděpodobnost výskytu rizika (Pravděpodobnost) a to v hodnotách od 0 až do 100%
- Potenciál poškození a to například v hodnotách od 1 (nejmenší) až 10 (největší)

Míru důležitosti (Důležitost) poté vypočítáme jako součin hodnot Pravděpodobnost krát (*) Potenciál poškození

- Následně z těchto hodnot určíme pořadí rizik podle důležitosti a vybereme rizika, která zařadíme do plánu rizik

5.3.3. Opatření na eliminaci rizik

V rámci opatření rizik bude uchazeč používat dále současně preventivní (proaktivní) a následný (reaktivní) přístup k odezvě na riziko:

- **Proaktivní přístup** (prevence vzniku této situace)
 - Identifikace, eliminace a řízení rizik

Identifikace rizik

Vytvoření rizikové analýzy

Vytvoření mechanismu hodnocení rizik

Určení výše dopadu a pravděpodobnosti vzniku rizik

▪ Eliminace rizik

- Vyloučení rizika – zákaz vybraných rizikových aktivit a procesů
- Snížení rizika – snížení velikosti dopadu např. pojištěním rizika
- Přenos rizika – redukce rizika snížením pravděpodobnosti nežádoucích událostí
- Přijetí rizika – akceptace rizika na stávající úrovni bez dalších aktivit
- Uplatňování zásad projektové řízení, správné nastavení úrovně řízení projektu, pravidelný Řídící výbor projektu, ustanovení sponzora projektu

Kontrolní den na měsíční bázi

Pravidelný reporting a průběžné sledování požadavků uživatelů v HelpDeskovém systému zadavatele

- Využití projektových a procesních manažerů uchazeče disponujících mezinárodně uznávanými certifikacemi ITILv3, ISO 10.006 a IPMA

- Uplatňování zásad procesního řízení (ITIL)
- Řízení subdodavatelů a řízení kvality
- Pojištění – tento nástroj řešení rizik v sobě zahrnuje aktivní složku prevence, tj. minimalizace ztrát v případě výskytu rizika

Reaktivní přístup (řešení situace až v případě vzniku rizika s cílem minimalizovat dopady). Uchazeč bude reagovat průběžně s ohledem na aktuální vývoj výskytu vybraných rizik v rámci projektu, které nelze řešit proaktivně a to např. z důvodu neekonomičnosti (tj. neúměrně vysokých nákladů na eliminaci těchto rizik), atd.

Když byla vyhodnocena pravděpodobnost a dopady každého rizika, je potřeba konkrétně naplánovat, jak se na dané riziko bude reagovat. Reakce na rizika má buď

snížit jejich pravděpodobnost nebo omezit jejich nepříznivé důsledky, ev. oboje. Reakce na rizika v projektu mohou být následující:

- Akceptace – nebude se dělat nic. Znamená to, že projekt dané riziko toleruje, s tím, že pokud by se naplnilo, zvládnou se případné důsledky pomocí zavedených postupů.
- Ošetření rizika – naplánují se a provedou opatření snižující pravděpodobnost naplnění daného rizika. Například se naplánuje nějaká rezerva nebo dodatečné zdroje.
- Přenesení rizika – speciální forma snížení rizika, při níž se důsledky daného rizika převedou na nějakou třetí stranu. Například se použije penále vůči dodavateli.
- Ukončení činnosti, z níž dané riziko vyplývá. Jinými slovy taková změna rozsahu projektu, že se možnost naplnění rizika vyloučí.

Vedle zřejmých negativních efektů rizik mohou někdy z nejistoty vyplývat i pozitivní příležitosti. Hledání příležitostí vyžaduje uvažovat o věcech, u kterých nebyla zjištěna žádná rizika.

Řízení rizik tedy znamená:

Přidělení rizika konkrétní osobě (vlastníkovi), zodpovídající pak za schválené (re)akce

Hodnocení výsledků, které provedené akce přinesly

Opakované vyhodnocování rizik a rozhodování o případných dalších opatřeních

Kontrola toho, jestli neexistují ještě další, zatím neidentifikovaná rizika (příležitosti)

Veškeré informace o rizicích a plánovaných i provedených opatřeních se zaznamenávají do Evidence rizik.

- **Součinnost Objednatele.**

6. Prostřednictvím implementace migračního procesu, který může načítat data z databáze, ale i z jiných zdrojů a provádí transformaci dat do nových struktur. Takovýmito zdroji dat mohou být soubory ve formátu CSV nebo XML (v případě poskytnutí dat v některém z uvedených formátů, bude vyžadována dokumentace formátu souboru v souladu s 8. **Zajištění provozu a podpora**

K outsourcingu nelze v současné době přistoupit jinak než komplexně. Takový přístup ale jednoznačně vyžaduje veliký rozsah kompetencí, kterými je schopna společnost pokrýt veškeré požadavky Zadavatele z vlastních zdrojů, a to jak v oblasti kapacitní, tak především kompetenční. Tímto Zadavateli plně garantujeme, že naše společnost tuto podmínku splňuje a vyhovujeme všem požadavkům kladeným v Zadávací dokumentaci.

Vzhledem k tomu, že uchazeč disponuje certifikovanými a zkušenými odborníky v oblasti ITIL (Information Technology Infrastructure Library – jedná se o soubor konceptů a postupů, které umožňují lépe plánovat, využívat a zkvalitňovat využití informačních technologií a to jak ze strany Uchazeče, tak i z pohledu Zadavatele), bude Uchazeč využívat tato doporučení pro poskytování, evidenci a reporting dodávaných služeb.

Tento rámec souborů a postupů je celosvětově osvědčen a uznáván jako soubor nejlepších doporučení pro řízení a dodávku příslušných služeb, což Zadavateli garantuje maximální možnou efektivitu a záruku velmi kvalitního řízení a plnění požadovaných činností. Dále pak ve svém realizačním týmu disponuje Uchazeč vysoce zkušenými pracovníky s certifikacemi, kteří mají dlouhodobou zkušenost se zavedenými procesy.

6.1.2. Široké kompetence společnosti S&T

Službou Outsourcing obecně přebíráme částečnou nebo úplnou odpovědnost za definované oblasti IT/IS. Poskytování outsourcingu probíhá tak, že na jedné straně procesu stojí zákazník se svými požadavky, a na druhé straně je dodavatel služeb, který tyto zákaznické potřeby uspokojuje. Dodavatel těchto služeb může být interní nebo externí.

Outsourcing IT/IS nepovažujeme za monolitickou dodávku jednoho systému, naopak ho vidíme jako stavebnici složenou z několika komponent, a záleží jen na budoucím uživateli outsourcingu, kterou část svého IS vyčlení vně své organizace a nahradí ji přiměřenou komponentou této stavebnice.

Firmy specializující se na daný obor mají zpravidla mnohem lépe proškolené pracovní síly, které se v dané problematice orientují. Odpovědnost za problematiku nese jiný subjekt a výchozí firma se může plně věnovat svému hlavnímu oboru. Náklady na zajištění specializované činnosti jsou při využití outsourcingu zpravidla výrazně nižší. Zajišťování služeb pomocí outsourcingu je celosvětově se zvyšujícím trendem.

V oblasti outsourcingu infrastruktury a standardních aplikací se zaměřujeme na společnosti středně velké a velké ze všech segmentů trhu v ČR. V oblasti aplikačního a procesního outsourcingu jsme díky našim referencím schopni poskytnout vysokou kvalitu outsourcingových služeb pro společnosti ze segmentů financí, telekomunikací, výroby, stavebnictví a státní správy.

V IT existuje nepřeberné množství technologií, systémů a aplikací. Jako jeden z velkých integrátorů v České republice vlastníme na většinu z těch klíčových vlastní školené specialisty a v ostatních případech doplňujeme naše řady o externí spolupracovníky a využíváme subdodávek našich dlouhodobých partnerů. Díky takovému přístupu zajistíme vždy kvalitní podporu všech technologií klientů.

Naše společnost mimo certifikace ISO 9001 získala také významnou certifikaci ISO 20000 se zaměřením specificky na outsourcing IT/IS a certifikaci ISO 27000 se zaměřením na informační bezpečnost.

V oblasti podnikových systémů jsou našimi partnery SAP, INFOR, COGNOS a LCS. V oblasti technické infrastruktury také spolupracujeme se špičkovými dodavateli a jsme držitelé nejvyšších certifikací – našimi partnery jsou společnosti HP, IBM, Fujitsu, DELL, Microsoft, CheckPoint, EMC, VMware a další.

Bezpečnostní řešení, poskytovaná našim klientům, jsou založena na nejnovějších technologiích společností CISCO, CITRIX, McAfee, Symantec, ISS, BlueCoat a dalších. Mezi naše osvědčené partnery z oblasti sítí patří například společnosti CISCO, Allied Telesyn, HP, 3COM a RIT.

V oblasti servisu, podpory a služeb naše aktivity zahrnují například péči o produkty společností IBM, HP, NetApp, Dell, Fujitsu Siemens Computers, Xerox, Acer, Lexmark, Olivetti a dalších.

Systém řízení kvality podle S&T

6.1.3. Model projektového a procesního řízení

Uchazeč k efektivnímu řízení smluvního vztahu, resp. k efektivnímu řízení dodávky outsourcingových služeb přistupuje na základě níže popsaného modelu, který je založen na dlouholetém vývoji, vzhledem k jeho efektivitě a upravován na základě aktuálních zkušeností a hodnocení našich zákazníků. Tento model je používán mnoha outsourcingovými organizacemi.

Používaná architektura řízení umožňuje včasnou identifikaci potenciálního výskytu problému a jeho řešení od nejnižší úrovně řízení až po jeho eskalaci na nejvyšší možnou úroveň. Tento proces bude detailně popsán v Provozní dokumentaci vznikající v rámci fáze tranzice.

Řízení vztahu se zákazníkem – v terminologii Uchazeče "Governance model", tvoří formální řídicí rámec a strukturu, které vychází ze standardních procesů a osvědčených zkušeností Uchazeče. Governance model umožní oběma stranám efektivní vzájemné řízení vztahu, očekávání, smluvních závislostí a služeb.

Procesy Governance jsou dobře dokumentované, opakovatelné a flexibilní. Úspěšná implementace Governance je úzce závislá na návrhu optimálního modelu, který umožní splnit požadavky obou stran a zajistí proaktivní a oboustranně výhodný partnerský vztah mezi oběma organizacemi.

Na základě zkušeností Uchazeče s obdobnými komplexními vztahy řešícími poskytování dlouhodobých outsourcingových služeb srovnatelného objemu a vzhledem ke stávajícímu organizačnímu zajištění služeb v prostředí Zadavatele navrhujeme ustanovit následující:

Výkonný Management (frekvence schůzek 1–2x ročně)

- Strategické řízení vztahu
- Dlouhodobé plánování aktivit, zpravidla na roční období

Řídicí výbor (frekvence schůzek kvartálně)

Taktické řízení vztahu

Střednědobé plánování aktivit, zpravidla na kvartální období

Vyžadována přítomnost tzv. Sponzora projektu ze strany Zadavatele

Hlavní tým projektu (frekvence schůzek měsíčně)

Operativní řízení vztahu

- Krátkodobé plánování aktivit, zpravidla na měsíční bázi
- Průběžné hodnocení dodávky dohodnutých služeb dle SLA

Dále pak garantujeme na vyžádání Zadavatele účast odpovědného zástupce Uchazeče na tzv. Pracovních skupinách, které jsou v současné době pořádány Zadavatelem na týdenní (příp. 14 denní) bázi a řeší zcela operativní záležitosti, které se týkají běžného provozu všech provozovaných služeb napříč celým Ministerstvem zemědělství. Z těchto schůzek jsou eskalovány problémy na vyšší úroveň řízení, jako jsou výše zmíněný Hlavní tým projektu, případně Řídící výbor projektu.

Uchazeč garantuje objednateli součinnost a komunikaci v rámci osobních jednání na kontrolních dnech, operativních ad-hoc schůzkách na vyžádání a v průběhu poskytování činností v rámci provádění služeb, což objednateli zajistí v maximální možné míře průběžné zvyšování efektivity řízení poskytovaných služeb.

Uchazeč se zavazuje předložit objednateli jedenkrát ročně celkovou výroční zprávu obsahující přehled poskytnutých služeb, ve které přehledným způsobem popíše realizované činnosti v uplynulém období dle jednotlivých klíčových oblastí, shrnutí měsíčních vyhodnocení SLA parametrů, doporučí objednateli případné oblasti služeb vhodné pro zlepšení a poskytne objednateli celkovou zpětnou vazbu vycházející ze zkušeností provozu služeb za uplynulé období.

Blokový obrázek modelu dodávky služeb

6.1.4. Procesy a pracovní postupy

Naše společnost se již od svého založení zaměřovala především na oblast poskytování služeb IT. Díky této striktní orientaci jsme se již od roku 2005 začali intenzivně věnovat školením a procesním změnám směrem k rámci ITIL. Procesní rámec ITIL byl víceméně jako jeden celek využit k vytvoření evropské normy známou pod značkou ISO 20000.

Protože naše procesy a postupy již splňovaly náročná kritéria procesního rámce ITIL, požádali jsme jako druhá společnost na českém trhu o certifikaci dle této ISO normy a v roce 2006 jsme obdrželi akreditaci ISO 20000 na služby, mezi kterými je mimo jiné také poskytování outsourcingu IT.

Náš přístup k procesnímu řízení je standardizován a podrobně popsán v dokumentaci ISO 20000. Tak, jak je popsáno v zadání, nebudeme se v následujících kapitolách dopodrobna věnovat procesním modelům řízení jednotlivých disciplín IT služeb, ale zdůrazníme náš přístup a vyzdvihneme výhody a vylepšení, která jsme za dobu poskytování služeb outsourcingu dosáhli. Z těchto bohatých zkušeností budou čerpat členové našeho týmu a garantujeme tímto Zadavateli poskytování všech požadovaných služeb v souladu se Zadávací dokumentací.

Vrcholový pohled na procesy ISO 20000 certifikované v S&T

6.1.5. Incident management

Účel procesu:

Maximálně rychle obnovit službu s ohledem na smluvní termíny, s minimálním dopadem na uživatele a za co nejnižších nákladů. Incident je specifický typ události nebo uživatelského hlášení, obvykle spojeného s výpadkem služby nebo se snížením její kvality. Správa incidentů tvoří další větev podpory uživatelů. Vstupy od uživatelů nebo dohledované IT infrastruktury jsou buď vyřešeny přímo pracovníky Service Desku, a nebo předány specialistům druhé a třetí úrovně podpory, případně předány externím řešitelům.

Uchazeč zastává přístup, že Incident Management přináší kvalitu, efektivitu a tedy i cenovou konkurenceschopnost způsobem maximální standardizace. S&T má tisíce incidentů měsíčně od stovek klientů. Tato čísla se rychle zvyšují a naše procesy se stále musí zlepšovat. Naši manažeři kvality a manažeři jednotlivých disciplín mají za cíl dále zlepšovat vlastní IMS systém a procesy na něj navázané.

Incident Management máme standardně rozdělen do tří úrovní dle doporučení ITIL a to 1st level – ServiceDesk; 2nd level – On-Site/Off-Site specialista; 3rd line – eskalace na vendora a podporu třetích stran.

Závěr:

Vzhledem k tomu, že schválený proces incident managementu v prostředí Zadavatele je plně v souladu s doporučeními ITIL, které má uchazeč jako svůj firemní standard a na který je certifikován, garantujeme Zadavateli, že budeme plně integrováni na tento proces a budeme postupovat plně v souladu s uvedeným diagramem:

6.1.6. Change management

Účel procesu:

Obhospodařovat změny v infrastruktuře IT s ohledem na neustále se měnící obchodní potřeby a očekávání uživatelů, aby se minimalizoval negativní dopad na existující služby IT. Změnová řízení jsou kvůli rostoucím požadavkům na efektivitu provozu IT a důrazu na vysokou dostupnost služeb stále důležitější. Proces Správa změn vzájemně spojuje a propojuje procesy inicializace, sběr informací, vyhodnocování, plánování, řízení, implementace a testování změn v IT infrastruktuře. Je prakticky nemožné ve složitějším prostředí provádět jakékoliv změny, pokud daný pracovník nemá například dostatečné informace o tom, jaké technické vybavení, kdy a kde a jakým způsobem má vyměnit či nainstalovat.

Změnová řízení jsou v případě naší společnosti více "customizovaná" proti vysoce standardizovanému procesu Incident Managementu. Důvodem je, že zde klademe více důraz na rychle se vyvíjející obchodní cíle klientů, které se většinou diametrálně liší ve všech parametrech. I zde existují ale výjimky, kdy například u vysoce centralizovaných a manažersky globalizovaných mezinárodních společností náš model standardního řízení změn byl použit v plném měřítku.

Podstatnou výhodou naší implementace této disciplíny je flexibilita, kterou našim klientům nabízíme za využití standardních a vyzkoušených postupů na oborově širokém vzorku našich outsourcingových klientů.

Závěr:

Vzhledem k tomu, že schválený proces change managementu v prostředí Zadavatele je plně v souladu s doporučeními ITIL, které má uchazeč jako svůj firemní standard a na který je certifikován, garantujeme Zadavateli, že budeme plně integrováni na tento proces – budeme postupovat plně v souladu s uvedeným diagramem:

6.1.:

Připravit, poskytovat a vyhodnocovat úrovně dodávaných služeb, které jsou zakotveny písemnými smluvními vztahy.

Klíčovým nástrojem pro správu, řízení, evidenci, kontrolu, reporting a zajištění požadované úrovně poskytovaných služeb je tzv. Service Level Management, jehož hlavním účelem je připravit, poskytovat a vyhodnocovat úrovně dodávaných služeb, které jsou zakotveny ve Smlouvě.

Uchazeč dlouhodobě praktikuje a důsledně dodržuje propracované praktiky ServiceLevel Managementu ve všech poskytovaných a provozovaných službách, což přináší Zadavateli následující hlavní výhody:

Lepší vyváženost přínosů ICT proti nákladům,

Zvýšení výkonnosti i prestiže ICT a zlepšení služeb, které poskytuje,

Zásadní zkrácení doby pro obnovu služeb při jejich výpadku.

Pro maximálně efektivní evidenci služeb využívá Poskytovatel Katalog služeb, který obsahuje jednotlivé katalogové listy s jejich příslušnými atributy pro měření a definici úrovně služeb. Níže uvádíme základní atributy služeb, které běžně v jiných projektech

Uchazeč eviduje a využívá je při reportingu:

Jméno služby/Service Name

Popis služby/Service description

Typ služby/Service type

Kterých odborných útvarů se služba týká/Business Unit(s)

Manažeři služby/Service Manager(s)

Dopad na odborné útvary a jejich agendy/Business Impact

Priorita agendy (procesu)/Business priority

Provozní doba služby/Service hours

Kontakty na zástupce odborných útvarů/Business contacts

Eskalační kontakty/Escalation Contacts

Reporty o službě/Service Reports

Revize služby/Service Reviews

Bezpečnostní kategorie/Security Rating

Garantovaná úroveň služby (SLA)/Service Level Agreement)

Service Level Management je zastřešen metodicky a personálně Service manažery, kteří nejsou jmenováni jen na straně Uchazeče, ale také na straně našich klientů. Naši Service manažeři jsou certifikováni ITIL profesionálové, kteří se řídí doporučeními ITIL a interními směrnicemi ISO 20000 naší společnosti.

Dedikovaný Service manažer má za úkol kontinuálně měřit, řídit, vyhodnocovat a především zlepšovat průběžně poskytované služby. Dále pak zastřešuje další definované role pro poskytování služeb definovaných Zadavatelem v Zadávací dokumentaci.

Jako jedno z našich vylepšení postupů můžeme uvést například standardizovaný proces SIP [Service Improvement Program], který metodicky zvyšuje kvalitu služeb tam, kde není dostatečná.

Díky moderním technologiím a informačním systémům mají naši Service manažeři okamžitý přístup k vyhodnocování všech KPI [Key Performance Indikátory], které jsou uvedeny v jednotlivých SLA [Service Level Agreement] nebo Katalogu služeb.

Příklad on-line reportu dostupného pro všechny Service Manažery

Závěr:

Vzhledem k tomu, že schválený proces service level managementu v prostředí Zadavatele je plně v souladu s doporučeními ITIL, které má uchazeč jako svůj firemní standard a na který je certifikován, garantujeme Zadavateli, že budeme plně integrováni na tento proces a budeme postupovat plně v souladu s uvedeným diagramem:

6.1.8. Service manažer

Service Manažer (dále jen SM) je jmenovaný Uchazečem za účelem zajištění standardní úrovně poskytovaných služeb, zvyšováním spokojenosti Zákazníka a pro koordinaci a řízení všech aspektů se službou související. Mezi hlavní povinnosti patří pravidelné governance meetingy se zástupci Zadavatele, interním personálem dodavatele, dále pak řešení všech nestandardních situací (projekty, změny služeb, procesů) včetně průběžné dokumentace a pravidelného vyhodnocování. SM má přiděleny od dodavatele vysoké pravomoci, které mu umožňují ve většině běžných případů rozhodovat rychle a efektivně, bez nutnosti eskalace a tvorby interních žádostí o změny.

Vysoká úroveň kvalifikace a zkušenosti SM jsou zárukou zajištění kontinuity a dlouhodobé kvality služeb poskytovaných dodavatelem. Všichni SM jsou certifikováni dle ITIL (standard na řízení IT používaný dodavatelem) s minimální 5letou praxí v řízení dodávek outsourcingu, správy systémů nebo projektového managementu v IT oboru.

Při startu nebo přebírání poskytování nové služby je role SM definována takto:

- Představit manažera služeb – jediný kontakt v S&T pro IT/SM manažera Zadavatele
- Seznámit se s korporátními normami IT Zadavatele a s jeho postupy spojenými s IT a požadavky
Nastavení podpory a eskalačních cest
Připravit, optimalizovat a implementovat postupy pro poskytování služby
Seznámit odpovědné zaměstnance S&T s výše uvedenými informacemi
Zajistit funkčnost náběhu příslušných postupů
Připravit strukturu pravidelného reportování, dokumentace, eskalace

- Vytvoření datového prostoru na intranetu a vložení dat (smlouva, zápisy, reporty atd.)
- Zajistit shodu s procesními a metodickými pokyny S&T a Zadavatele

Pravidelné governance aktivity vykonávané SM:

Popis				
Provozní schůzky (analogie Pracovní skupiny v prostředí MZe)	1x 14dní	- Řízení incidentů - Změnová řízení - Bezpečnostní incidenty - Průběžná kontrola služby - Doporučení na zlepšení - Krátkodobé plánování služby - Kontrola plnění KPI parametrů	- Ad-Hoc reporty - Konzultace s vlastníky služeb - Interní vyhodnocení s pracovníky dodavatele - Výstupy z procesů změn, releasů a problémů - Minulý zápis s úkolovníkem	- Zápis z jednání - Rozdělovník úkolů - Stav úkolů - Distribuce zápisu dle rozdělovníku - Návrh eskalace na SLM - Žádosti o změny
Jednání komise (analogie Hlavního t projektu v prostředí Mze)	měsíčně	- Vyhodnocení KPI/SLA - Revize změnových požadavků - Schválení změn - Finanční sumarizace/fakturace	- Měsíční reporty - Zápisy z provozních schůzek - Finanční podklady - Seznam úkolů - Eskalace na SLM komisi - Změnové žádosti	- Zápis z jednání - Rozdělovník úkolů - Stav úkolů - Distribuce zápisu dle rozdělovníku - Vyřešení eskalace z provozu - Návrh eskalace na IT komisi - Žádosti o změny
Jednání komise	ročně	- Vyhodnocení dlouhodobých cílů - Finanční management - Revize smluvních podmínek - Aktualizace dlouhodobého plánu - Stanovení cílů na další rok	- Roční souhrnné reporty - Audit report (je-li) - Eskalace na IT komisi - Cíle na předchozí rok - Finanční podklady	- Zápis z jednání - Rozdělovník úkolů - Stav úkolů - Distribuce zápisu dle rozdělovníku - Vyřešení eskalace ze SLM - Cíle na další rok - Návrhy na zlepšení a inovace

Governance aktivity lze realizovat dle dohody mezi Uchazečem a Zadavatelem na místě, telefonicky a nebo videokonferencí, dle požadavku a aktuální potřeby. Pravidelnost a dodržování termínů je primární odpovědností SM a pouze na žádost Zákazníka lze pravidelné termíny rušit nebo přesunovat.

6.1.9. Service Continuity Management

Kontinuita poskytovaných služeb a podnikání našich klientů je jedním z cílů naší společnosti. Řešení Disaster Recovery současně nabízíme našim klientům jako součást našeho standardního produktového portfolia. Interní systémy a podpůrné procesy (CallCentrum, Informační systémy, datová konektivita) jsou zajištěny i pro případy havárie. Máme vypracovány havarijní plány pro jednotlivé disciplíny dle ISO 20000. Kontinuitu námi poskytování služeb, tedy z pohledu klienta i kontinuitu jeho podnikání, chápeme jako neustále se vyvíjející se proces.

Business Continuity / DR metodologie dle NIST 800.34

Tento obecný proces je shodný pro jakoukoli organizaci či podnik a liší se až v technické realizaci.

6.1.10. Bezpečnost a důvěrnost informací

Bezpečnost a důvěrnost informací je klíčovou devizou naší společnosti. Bez garance vysoké úrovně bezpečnosti bychom nemohli splňovat vysoké nároky, které na nás kladou naši současní zákazníci.

Naši zaměstnanci, přicházející do styku s důvěrnými i utajovanými informacemi, a proto někteří z nich prošli bezpečnostními prověrkami a byli náležitě proškoleni. Organizace jako celek disponuje zaměstnanci certifikovanými NBÚ od úrovně D (důvěrný) až po T (tajný).

Zaměstnanci používají šifrované připojení k internetu, zabezpečené počítače a šifrují data na nosičích. Přístup k datům je obvykle řešen "pohledy" do databáze a bezpečnostními politikami v rámci stromové struktury dat. Zaměstnanec nemá přístup k datům, která bezprostředně nepotřebuje k řešení svého úkolu v rámci týmu.

Na úrovni jednotlivých prvků architektury systému je bezpečnost zajištěna následovně:

Bezpečnost dat je zajištěna robustními prostředky SQL datového enginu
Bezpečnost komunikace klient – server je zajištěná na úrovni variantního kódování tohoto protokolu

- Bezpečnost na úrovni logiky aplikace je zajištěná robustním, nastavitelným auditem jednotlivých procesů na straně jedné a systémem nastavování skupinových a uživatelských profilů na straně druhé

Přesné definice rozsahu, hloubce, technikách a penalizacích jsou ukotveny ve vzájemné smlouvě o utajovaných skutečnostech, která je obvykle připravována a podepsána na úvod procesu Due Diligence.

6.1.11. CSI – Index spokojenosti Zákazníka

Pro vyhodnocování služeb předpokládáme použití intranetového dotazníku, který bude připravovat IviZe. IviZe uvádíme naše standardní procesy a postupy.

Mezi standardní reporty patří výstupy z pravidelných průzkumů spokojenosti uživatelů Zákazníka. Reporty vznikají z odpovědí na dotazníky, které jsou zasílány pravidelně elektronicky emailem, obvykle jednou za půl roku, na uživatele, kteří využili službu – tedy pouze těm, kteří mohou na zaslaný průzkum spokojenosti kvalifikovaně odpovědět.

Počet a znění dotazů které se uživatelům pokládají, jsou definovány na začátku poskytování služby. Aby bylo možné srovnávat výsledky jednotlivých průzkumů

v průběhu let poskytování služby, je třeba, aby znění dotazů zůstalo po celou dobu služby ideálně nezměněno. Hodnocení obvykle probíhá na tzv. školní stupnici, kde 1 znamená nejlepší a 5 nejhorší. CSI, tedy index spokojenosti Zákazníka je spočten jako absolutní průměr hodnocení všech účastníků a všech položených dotazů. Tento index jako jedna hodnota je součástí DashBoardu, jenž je určen pro Manažerský přehled. Detailní výsledky hodnocení a výsledky po jednotlivých odpovědích jsou k dispozici Service Manažerům obou smluvních stran.

Průzkum spokojenosti s IT

Vážený IT uživatel,

V rámci zlepšení kvality poskytovaných IT služeb plánujeme převést službu IT HelpDesk na externího dodavatele (společnost S&T CZ, s.r.o.). Naším cílem je zvýšit dostupnost služeb, které Vám IT poskytuje, rozšířit dobu pokrytí a zejména snížit reakční dobu řešení Vámi nahlášených IT problémů a tím minimalizovat případné finanční ztráty.

Ti z vás, kteří již od pondělního poledne hlásili IT incident, jistě zaznamenali změnu. Společnost S&T CZ, s.r.o. disponuje profesionálním call centrem a pro Vaši podporu dedikovala několik pracovníků, kteří jsou schopni pokrýt více hovorů paralelně.

Rádi bychom pravidelně hodnotili Vaši spokojenost s poskytovanými IT službami a za tímto účelem si Vám dovoluujeme poslat následující link

Webový formulář průzkumu Vaší spokojenosti s IT službami je umístěn ZDE.

Na této adrese je třeba odpovědět na uvedené dotazy a ohodnotit jak vnímáte stávající kvalitu poskytovaných IT služeb. Tento průzkum plánujeme opakovat pravidelně jednou za půl roku, aby vedení společnosti získalo náhled zdali tato změna je správná.

Předem děkujeme za Vaši reakci, po uzavření průzkumu dojde ke slosování všech odpovědí a pět vylosovaných uživatelů bude odměněno zajímavou věcnou cenou od společnosti S&T CZ.

Děkují,

Petička s logem a podpisem

Příklad zaslání emailu na uživatele průzkumu

Příklad dotazů pokládaných v jednom ze současných průzkumů. Dotazy by měli být relevantní a stručné.

- Jak jste celkově spokojeni s poskytováním IT služeb?
- V případě, že kontaktujete vaši IT podporu, je vždy někdo, kdo by se vám věnoval?
- Jste spokojeni s kvalitou komunikace ze strany vaší IT podpory?
- Jste spokojeni s dobou řešení vámi nahlášených požadavků?

CSI uvedený v DashBoardu

6.1.12. Správa problémů

Účel procesu: identifikovat a řešit chyby v infrastruktuře IT, aby se zabránilo opakovanému výskytu incidentů vztahených k těmto chybám. Tento proces je velmi často též nazýván správou kvality (Quality Management), protože je zaměřen na analýzu velkých, opakujících se nebo podobných incidentů. Výsledkem analýzy je pak nalezení a definice systémové příčiny tzv. známé chyby (Known Error). Proces Správa problému má jak reaktivní, tak i proaktivní aspekty. Reaktivní činnosti se soustřeďují na řešení problémů vyvolaných incidenty, proaktivní činnosti se zaměřují na identifikaci a řešení problémů a známých chyb ještě předtím, než se stanou incidenty. Zatímco účelem procesu Správa incidentů je obnovit službu jak nejrychleji je to možné, proces Správa problémů se zaměřuje na důkladnou analýzu klíčové příčiny selhání, a podporuje tak maximální stabilitu poskytovaných služeb IT.

6.1.13. Správa konfigurace

Účel procesu: zabezpečit centrální správu IT infrastruktury tak, aby se podpořila dodávka kvalitních a efektivních služeb IT. Správa konfigurace je proces, který zajišťuje identifikaci, řízení, vykazování stavu a kontrolu nad infrastrukturou IT a všemi aktivy IT v organizaci v průběhu jejich životního cyklu. Kromě podpory dalších procesů, jako je Správa problémů a Správa změn, zajišťuje také snadný přístup k informacím, jako jsou smlouvy o poskytování služeb, vazby/závislosti mezi konfiguračními položkami a organizačními informacemi. U procesu Správa změn zabezpečuje proces Správa konfigurace pracovníkům zodpovědným za změny, aby byli aktuálně informováni o jednotlivých zařízeních, uživateli a službách. V důsledku toho mohou provádět odpovídající analýzu rizik a dopadů. Tato integrace zároveň zaručuje aktuální stav konfigurační databáze. Účinné řízení konfigurace zajišťuje nejlepší využití, rozmístění a využívání všech IT aktiv.

6.1.14. Řízení projektů

Pomocí projektových manažerů pomáháme u našich zákazníků zavést nebo zdokonalit projektovou kulturu, aby pomocí efektivních a kontrolovatelných procesů a metod řídili své projekty v daném čase, v rámci rozpočtu a v požadované kvalitě. Dále pak pomáháme projekty kvalifikovaně a maximálně efektivně řídit plně v souladu s principy metodiky IPMA.

6.1.15. Provozní deník

Uchazeč bude vést Provozní deník a zaznamenávat do něj minimálně následující skutečnosti:

Výskyt havarijních stavů;

Výskyt anomálií a nestandardních stavů systémů, které mají dopad na plnění SLA;

Zprovoznění nového nebo dočasně odstaveného systému a odstavení systému;
Spuštění, vypnutí a restart systému.

Uchazeč garantuje, že provozní deník bude obsahovat minimálně následující informace:

Datum a čas pořízení záznamu;

Identifikace osoby pořizující záznam;

V případě událostí trvajících více než 1 hodinu také čas začátku a konce události;

- Popis události.

6.1.16. Integrace interních procesů hlášení incidentů, přijímání změnových požadavků na stávající procesy a systémy zadavatele

Interní procesy hlášení požadavků, přijímání změnových požadavků vycházejí z procesů požadovaných zadavatelem v zadávací dokumentaci. Interní procesy uchazeče budou flexibilně přizpůsobeny potřebám MPSV a budou plně reflektovat i požadavky na případné úpravy procesů.

Poskytované služby zajištění předmětu VZ jsou řízeny procesními standardy postavené na sadě doporučení ITIL v3. Interní procesy Zadavatele pro hlášení incidentů, změnových požadavků případně problémů budou jedna ku jedné navázány na procesy Uchazeče, který provozuje plnohodnotné service deskové SW řešení. V inicializační části projektu počítáme s provedením integrace mezi SW nástroji Zadavatele a Uchazeče tak aby byli jednotlivé procesy provázány.

Tímto postupem zajistíme vedení evidence o probíhajících řešení jednotlivých požadavků nebo skupin požadavků v service desku Zadavatele v dostatečné úrovni informací tak aby bylo možno provádět měření a vyhodnocování podpory jednotlivých služeb a řešení jednotlivých požadavků.

6.1.17. Komunikační kanály a jejich integrace s komunikačními kanály zadavatele

Komunikační kanály na straně dodavatele budou plně integrovány s komunikačními kanály zadavatele a přizpůsobeny jeho potřebám. Pro komunikaci s uživateli uchazeč předpokládá využití telefonu, faxu, e-mailu a případně webového rozhraní. Pro interní komunikaci mezi dodavatelem a objednatelem předpokládá dodavatel využití Pracovního týmu (PT), Hlavního týmu projektu (HTP) a Řídícího Výboru (ŘV).

6.1.18. Dokumentace projektu

Průběh projektu a podstatné výstupy projektu jsou ukládány do centrálního úložiště dokumentace, které je přístupné všem osobám podílejícím se na projektu.

Struktura úložiště je následující:

- Společná projektová dokumentace
 - Provozní deník
 - SLA reporting
 - Požadavky na změnu

Zápisy z porad (jednání ŘV a pracovního týmu)

Komunikační matice – složení jednotlivých týmů kontaktní údaje účastníků

Procesní dokumentace – popisy procesů, katalog služeb, konfigurační databáze

- Systémová dokumentace a složky jednotlivých systémů
 - Administrátorské, instalační a uživatelské příručky
 - Testovací a akceptační protokoly

Všechny dokumenty zaznamenávající dohody mezi objednatelem a poskytovatelem implementace změn (např. zápisy z jednání), výstupy poskytovatele (dokumenty analýzy a návrhu) jsou pojmenovávány stejnou konvencí a ukládány na úložišti Projektové dokumentace.

V případě oponentury a upřesňování obsahu dokumentu týkajícího se implementace změn jsou změny zachycované formou revizí (pokud to daný formát dokumentu umožňuje) a v úvodu dokumentu je doplněno datum oponentury a souhrn připomínek. Opakovaně předávané dokumenty objednateli jsou verzovány a nová verze bude obsahovat stručný popis změn navíc ještě v komentáři verze na portálu.

Konvence pojmenování souboru je "Název dokumentu_identifikace týmu_verze (případně pořadí)_datum předání", kde verze je znázorněna konvencí XvY a datum je ve formátu rrrmmdd (bez diakritiky).

Soubory jsou na úložiště ukládány ve standardních formátech – MS Office verze 2003 včetně (.doc, .docx, .xls, .ppt, .msg atd.), MS Project (.mpp), obrázky (.jpeg, .tif, .gif, .pdf), MS Visio (.vsd), XML služby (.wsdl, .xml, .html, .css).

6.1.19. Strukturované e-maily

Na základě schválených plánů změn a plánů odstávek zasílá technický specialista případně Manažer řízení služeb v dostatečném předstihu na HD MPSV informační e-mail v předem definované struktuře o plánované odstávce systému (případně plánované změně). HD MPSV si odstávku/update zkontroluje z hlediska plánů odstávek a změn, případně si vyžádá souhlas odborného garanta IS nebo Manažera řízení služeb poskytovatele. Rovněž si může vyžádat doplnění e-mailu o dodatečné informace, pokud není informace kompletní.

Minimální rozsah strukturovaného e-mailu je následující:

Identifikace systému, kterého se informace týká a identifikace, zda se jedná o produkční či testovací prostředí.

Rozsah prací.

Dopad prací (např. úplná nedostupnost, omezení rychlosti aplikace apod.).

Plánovaný začátek a plánovaný konec prací (datum a čas).

Kontaktní osoba odpovědná za provedení prací a kontaktní údaje (mobil a e-mail).

Následně HD MPSV rozešle oznámení e-mailem na kontaktní osoby dle komunikační a eskalační matice (filtrované dle druhu upozornění (odstávka/update) a dotčeného systému).

Strukturované e-maily jsou prostřednictvím HD MPSV rozesílány i v případě výpadku systému, kdy je součástí zprávy dotčený systém a určení prostředí

(produkční/testovací). Zpráva je zasílána na konkrétní osoby určené v komunikační a eskalační matici (druh upozornění "výpadek"). Zpráva je zasílána při vzniku takového stavu a po vyřešení incidentu je oznámeno ukončení výpadku.

6.2. Způsob monitoringu, měření a vyhodnocování provozních parametrů řešení

6.2.1. Centrální monitorovací nástroj

Jako primární monitorovací nástroj infrastruktury a aplikací byl zvolen S&T Spectator. Spectator je řešení, jenž umožňuje monitorovat chování komponent informačního systému od hardware až po aplikace. Dává možnost, v co nejkratší době, detekovat reálné ale i potenciální problémy, které se mohou vyskytnout v každodenních činnostech IT systémů. Nonstop monitorování zajistí bezpečnost a efektivitu práce IT systémů – 7 dnů v týdnu, 365 dní v roce.

Hlavní vlastnosti řešení Spectator:

- Dohled nad zařízeními a dostupností služeb v síťovém prostředí
Kontrola UPS, teploty v serverových místnostech, routerů
Aktivní i pasivní sběr informací
Použití vlastních agentů nebo SNMP protokolu
- Možnost vývoje agentů nových (pro zařízení i aplikace) Notifikace

Notifikace

Oznámí problém před tím, ještě než je uživateli vůbec zjištěn

Definice alertů (OK, WARNING, CRITICAL, UNKNOWN)

Různé způsoby oznámení (e-mail, SMS...) Webová konzole operátora

Webová konzole administrátora

- Aktuální stav zařízení a služeb
Historie všech záznamů
Reporty o dostupnosti zařízení a služeb
- Reporty o závadách a problémech
Reporty o oznámeních/notifikacích

Výhody platformy Nagios

- Plně škálovatelná – systém roste s potřebami společnosti bez nutnosti vybavování novou technickou infrastrukturou či nákupem licencí
- Využívá současné infrastruktury k přenosu dat (vyžaduje IP síťové prostředí)
- Umožňuje rychlou implementaci s minimálním vlivem na monitorované systémy
- Běží na Linuxu – operační systém s nízkým TCO
- Jednoduše adaptabilní na specifické potřeby klienta
- Má pokročilé metody analýzy problémů (zabraňuje falešným notifikacím apod.)
- Umožňuje eskalaci notifikací dle definovaných kritérií

- Nevyžaduje instalaci žádného specifického software (pro dohledový server je třeba jen – C compiler, Perl interpreter, WWW server)
- Díky otevřenému kódu není zákazník závislý na jedné vývojářské společnosti/dodavateli

6.2.2. Servicedesk

S&T CZ provozuje ve vlastních prostorách ServiceDesk, který je rozdělen na několik virtuálních týmů dle klienta a typu práce (HelpDesk, Kvalifikace, Dispečink, Dohled). Všechny členy ServiceDesku spojuje jedna technologická základna telefonického CallCentra od společnosti Alcatel s nadstavbou pro profesionální CallCentra Genesys. ServiceDesk pracuje s vlastním IMS společnosti stejně jako s informačními systémy našich klientů. Plné služby ServiceDesku poskytujeme v době 8x10 a 24x7 v stand-by režimu s dohledem systémů našich klientů v nonstop režimu. Procesy ServiceDesku jsou standardizovány s tím, že pro každého klienta jsou upraveny v průběhu implementace služby tzv. "na míru" klienta a jeho požadavků.

IT ServiceDesk představuje provoz centrálního místa Dodavatele pro hlášení evidenci požadavků Objednatele souvisejících s plněním Služby ve lhůtách uvedených SLA. Součástí této Dílčí služby je zejména:

- Příjem požadavků na odstranění vad
- Evidence požadavků na straně S&T
- Evidence průběhu řešení a výsledného řešení požadavků na odstranění vad
- Technická podpora zaměstnanců odboru ICT Zadavatele
- Spolupráce s pracovníky odboru ICT Zadavatele a s dodavateli třetích stran při odstraňování problémů
- Poskytování informací o dodávaných službách pro odbor ICT Zadavatele
- Příprava podkladů pro reporting

Hlavními charakteristickými rysy služeb ServiceDesk jsou:

- Užívání metodických standardů a ověřené procesní metodologie ITSM
- Víceúrovňová struktura umožňující typovou segmentaci a vyšší efektivitu práce

S&T poskytuje komplexní služby outsourcingu, které pokrývají celý životní cyklus od návrhu řešení a architektury, přes poskytování technologií formou služby, řízení změn v průběhu životního cyklu až po provozování a podporu infrastruktury. Funkce ServiceDesku je nedílnou součástí provozu a podpory a S&T takový IT ServiceDesk provozuje pro řadu významných klientů v České republice, srovnatelných co do velikosti se Zadavatelem.

ServiceDesk S&T je jeden tým pracující ve sdíleném režimu pro více zákazníků, fyzicky umístěný v prostorách S&T. ServiceDesk je organizován do několika vrstev s rozdílnými rolmi v rámci procesů ITIL.

Název		
Level 1	Primární kontaktní místo pro uživatele IT	Incident Management, Request Fulfillment, Access Management
Level 2	Technické řízení	Incident Management, Problem Management, Release and Deployment, Operations Management (provozní činnosti)
Level 3	Technická autorita	Change Management, Design

6.2.2.1. Incident Management System SolveDirect

Solvedirect je plně webová online aplikace specificky vytvořená pro práci s požadavky. Je jedním z nejčastěji užívaných systémů outsourcingovými společnostmi a společnostmi poskytujícími servisní služby více zákazníkům z jednoho nástroje. Systém jako takový je provozován buď formou Cloudu (SaaS) nebo méně častou formou instalované vlastní instalované stand-alone aplikace.

Systém Solvedirect obsahuje všechny klíčové funkcionality pro management požadavků tedy:

- Databáze kontaktů, lokalit, zařízení, software, výrobců atd.
- Procesní workflow, které lze libovolně měnit a upravovat
- Eskalační a notifikační nástroje (SMS, mail atd.)
- Nastavení SLA (hodnoty odezva, oprava/náprava)
- Sliný reporting všech hodnot souvisejících s požadavky (kvantitativní, kvalitativní)
- Webové rozhraní jak pro běžné prohlížeče, tak pro přístup z mobilních zařízení
- Znalostní databáze
- A mnoho dalších funkcí. Detaily lze nalézt na stránkách výrobce <http://www.solvedirect.com>

Reporting a evidence

Reporting a evidence zahrnuje vedení evidence Zařízení přenechaných kužívání Objednateli a vytvoření sady pravidelných reportů, které zahrnují informace a to zejména:

Počtu servisních požadavků a reklamací

- Seznam s počty roztríděný po jednotlivých měsících a letech
- Pole detailního seznamu budou obsahovat všechna data relevantní k daným požadavkům a reklamacím
- Řešeno on-line reportem z logického celku reportingu "Množství Volání" viz. metodika níže

Plnění SLA parametrů u incidentů a reklamací

- Seznam s procentem plnění SLA po jednotlivých měsících a letech
- Pole detailního seznamu budou obsahovat časová razítka ze který je proveden výpočet procenta dosaženého SLA
- Řešeno on-line reportem z logického celku reportingu "Úroveň Služby" viz. metodika níže

- **Přehled obnovy techniky v případě havárie včetně plnění SLA**
 - Seznam s počty a plněním SLA roztríděný po jednotlivých měsících letech
 - Řešeno on-line kombinací reportů z celků "Množství Volání" a "Úroveň Služby"
- **Přehled plnění harmonogramu obnovy techniky**
 - Report s plánem harmonogramu a časovými razítky finální realizace
 - Řešeno on-line reportem exportovaným z CMDB s časovými razítky
- **Přehled instalací jednotlivých Image na zařízeních.**
 - Seznam zařízení s detaily ze CMDB mezi které patří i verze image
 - Řešeno on-line reportem exportovaným z CMDB s detaily o verzích image
- **Přehled dostupných opravných balíčků k centrální distribuci včetně údajů o případné distribuci**
 - Seznam všech opravných balíčků s uvedeným stavem
 - Stav: žádost na balíček, v přípravě, testování, připraveno k distribuci, distribuováno

Přehled dostupných opravných balíčků; které nelze distribuovat centrálně včetně údajů o případné distribuci

- Rozšířený seznam viz. bod výše o stav nelze distribuovat s uvedením důvodu
- Jelikož se jedná o balíčky nedistribuované automaticky bude řešeno seznamem udržovaným Service Manažerem s využitím odpovídajícího SW nástroje

Přehled využívání služeb dodavatele podle jednotlivých katalogových listů

- Report s počty požadavků na každý katalogový list po jednotlivých měsících a letech – KL bude zaveden do systému jako PrvekSmlouvy viz. metodika níže

- Řešeno on-line reportem z logického celku reportingu "Množství Volání" viz. metodika níže

Evidence SW instalovaného v místě odběratele

- Podle druhů SW
- Podle HW na kterém je instalován

Evidence SW bude realizována na vstupu typováním použité verze SW do CMDB. Změna zařízení, SW nebo reinstalace povede vždy k aktualizaci dat v CMDB. Každé HW má v CMDB vlastní sadu polí mezi které patří i pole pro uložení potřebných informací o SW.

Seznam bude obsahovat detaily o HW i SW (výrobní číslo, typ, verze atd.) s uvedením verze image/SW.

- Řešeno on-line reportem ze CMDB

Evidence HW

Evidence HW instalovaného v místě odběratele, která bude obsahovat minimálně tyto povinná pole:

- Konfigurace
- TypUmístění
- Výměna
- Vyřazení
- Servis

Stejně jako evidence SW je detailní evidence všech atributů HW výše uvedených, součástí CMDB. Mimo výše uvedená datové pole bude seznam rozšířen o další důležité informace např.: Inventurní číslo, model/typ, odpovídající servisní SLA, datum a jméno k poslední editaci záznamu v CMDB.

- Řešeno on-line reportem ze CMDB

6

Vytváření reportů je v kompetenci role Service Manažera. Jedná se o klíčovou službu pro měření kvalitativních a kvantitativních parametrů dodávaných služeb

Vstupy do procesu měření a reportingu kvalitativních a kvantitativních parametrů jsou především:

- SLA – tedy klientem smluvně definované parametry, jež služba musí dlouhodobě splňovat
- OLA – interní mimo smlouvu definované parametry, které slouží k měření návazných služeb
- CSI – subjektivní hodnocení spokojenosti zákazníka nebo uživatelů s poskytovanými službami

CMDB – databáze obsahující veškerá a detailní data o HW, SW a všech realizovaných službách a aktivitách

Výstupy z procesu měření a reportingu kvalitativních a kvantitativních parametrů se předkládají ve dvou informačních vrstvách. První je tzv. souhrnný jednostránkový DashBoard, jež slouží, k rychlému shrnutí celkové kvality všech poskytovaných dílčích

služeb a je využíván především managementem zákazníka a dodavatele. Druhá informační vrstva je mnohem detailnější (až na úroveň dat z CMDB). Tuto vrstvu reportů a detailů využívají především nominovaní Service Manažeři k detailní analýze trendů, problémů, návrhů na zlepšení atd.

Základem druhé vrstvy nebo také úrovně reportingu jsou on-line generované reporty u kterých jsou k dispozici následující funkcionality:

- Jedním klikem export do Excelu, CSV a XML souborů
 - Jedním klikem export do PDF
- Drill-Down funkcionality
Seznam instalované báze HW/SW

Drill-Down umožňuje z každého on-line reportu proklikáváním vstupovat do dat ze kterých je report složen nebo vypočítán. Tedy lze jedním klikem z přehledové tabulky např. s počty instalací/oprav v jednotlivých měsících vstoupit do detailního seznamu s popisy jednotlivých instalací/oprav, a dalším klikem zobrazit úplný detail jedné jediné instalace nebo opravy včetně všech příloh, časů a komentářů techniků i uživatelů.

První úroveň reportingu – DashBoard

V první vrstvě (tzv. DashBoard) jsou prezentována především tyto data:

- Percentuální plnění SLA
- Index hodnocení zákazníka a uživatelů
Součástí bývá i souhrn finanční kalkulace/podklad pro fakturaci

Screenshot DashBoardu – záložky obsahují další detaily

DashBoard je generován na konci každého kalendářního měsíce a je podkladem pro pravidelné měsíční vyhodnocování poskytovaných služeb smluvními stranami včetně odsouhlasení souvisejících finančních podkladů.

DashBoard může být se základními parametry poskytovaných služeb generován kdykoli v průběhu i on-line. Tento on-line náhled může být zobrazen na dohledovém displeji nebo mobilním zařízení Service Manažera dodavatele pro aktuální přehled stavu všech klíčových parametrů poskytovaných služeb.

Screenshot on-line pohledu na webový DashBoard

Druhá úroveň reportingu – detailní reporty

Ve druhé vrstvě jsou prezentována především detailní přehledové reporty ze CMDB obsahující počty incidentů, kategorie, aktivity, lokality atd. Všechny reporty z této vrstvy jsou k dispozici vždy (24x7) on-line Service Manažerovi zákazníka i odběratele.

V této úrovni reportingu je rozsah možností pro generování různých reportů natolik rozsáhlá, že umožňuje on-line přístup k více jak 200 kusům reportů. Tuto rozmanitost a hloubku získá i neškolený Service Manažer zákazníka přes intuitivní on-line webové rozhraní které je zdarma bez limitu počtu Service Manažerů nebo jiných uživatelů ze strany zákazníka.

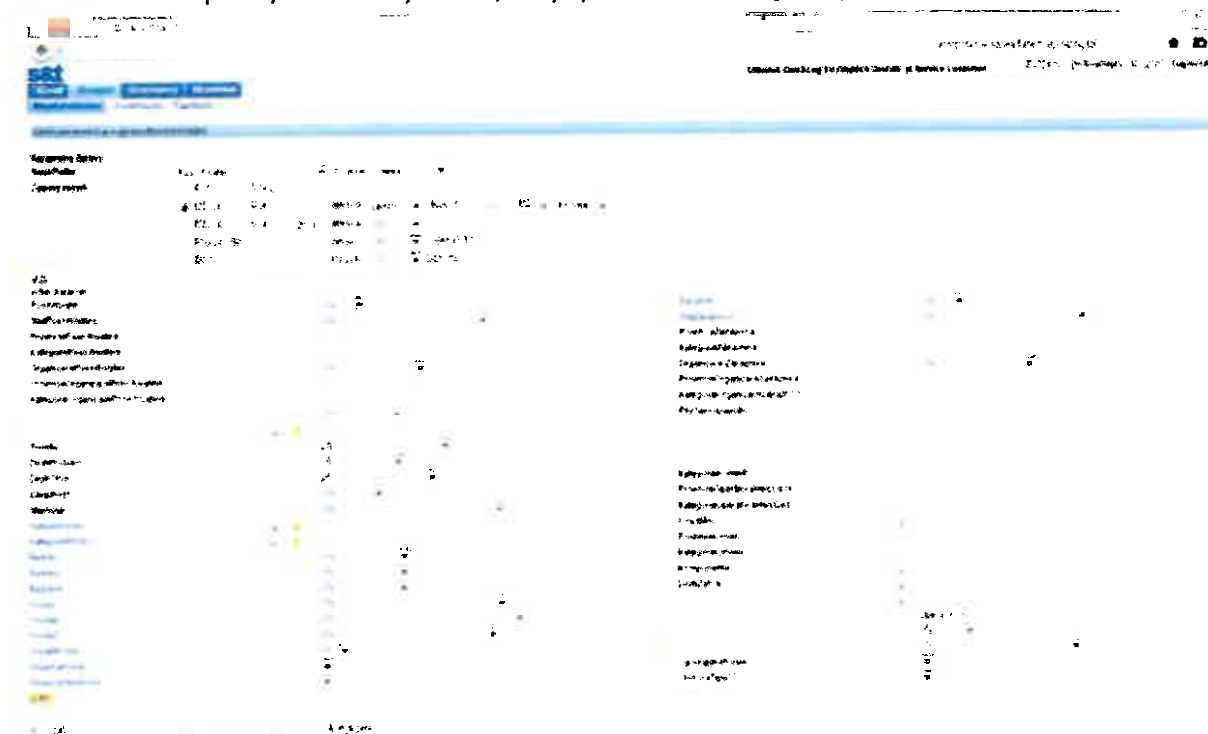
Webové rozhraní obsahuje desítky parametrů, kterými lze výsledný report ovlivňovat (filtrovat, omezovat, třídit, zobrazovat). Sady reportů jsou zde rozděleny do tří logických celků:

4. Množství Volání – výstupem této skupiny reportů jsou vždy počty (součty incidentů, změn apod.)
5. Úroveň Služby – výstupem této skupiny jsou procenty vyjádřené hodnoty proti nastaveným SLA
6. Čas Služby – výstupy z této skupiny jsou časové hodnoty v minutách a hodinách (např. délka trvání oprav atd.)

Screenshot třech základních kategorií on-line reportingu

Množství Volání

Základní logika reportů je postavena na dvou částech. První část, první třetina níže uvedeného screenshotu určuje, jaký typ reportu bude vygenerován (seskupení reportu). Parametry v další, tedy spodní části, určují filtry obsahu reportu samotného.



Hlavní pohled na tvorbu reportů ze skupiny Množství Volání

Níže uvádíme kompletní seznam možných reportů (tedy seskupení podle pole) v celku Množství Volání:

- | | | |
|------------------------------------|---------------------|-------------------------------|
| • Poskytovatel | • Umístění | • ProvincieKontaktu |
| • ProvinciePoskytovatele | • ProvincieUmístění | • KategorieKontaktu |
| • KategoriePoskytovatele | • KategorieUmístění | • ProvincieOperátoraHelpDesku |
| • StátPoskytovatele | • Komponenta | KategorieOperátoraHelpDesku |
| • OrganizacePoskytovatele | • DruhZařízení | Fronta |
| • KategorieOrganizacePoskytovatele | • Výrobce | • Fronta2 |
| | • KategorieVolání | Fronta3 |

• ProvincieOrganizacePoskytovat ele	KategorieVolání1+2	ÚroveňFronty
• Zákazník	KategorieVolání1–3	Řešitel
• KategorieZákazníka	KategorieVolání1–4	Řešitel2
• ProvincieZákazníka	KategorieVolání1–5	Řešitel3
• StátZákazníka	KategoriePříčiny	DruDodavateložadavku
• Organizace Zákazníka	KategoriePříčiny1+2	SkupinaStavůVolání
• KategorieOrganizaceZákazníka	KategoriePříčiny1–3	SkupinaPriorit
• ProvincieOrganizaceZákazníka	KategoriePříčiny1–4	TypSkupinyProblému
• Smlouva	KategoriePříčiny1–5	SkupinaTypůChyb
• PrvekSmlouvy	PříjmeníVolajícího	SkupinaZávažnosti
• Priorita	PoskincieVolajícího	
• DruDodavatelproblému	KategorieVolajícího	
• DruhChyby		
• Závažnost		
• StavVolání		

Základní filtry pro reporty (seskupení podle) v této skupině jsou:

- Otevřená Volání – do reportu jsou zahrnuty všechna vytvořená volání
- Uzavřená Volání – do reportu jsou zahrnuty již jen ukončená volání
- Časové hodnoty – vymezení hodnot od kdy, do kdy má report být vygenerován
- Časová granularita – vymezení detailu
 - na rok
 - na měsíce a roky
 - na pracovní dny v měsíci a roce
 - na dny

V této sadě reportů "Množství Volání" jsou položky typu reportu (seskupení reportu) a parametry pro kompletní seznam filtrů obsahu reportu shodné.

Níže uvádíme nejčastěji využívané reporty ze sady Množství Volání:

Počet požadavků rozdělený podle typu požadavku

Počet požadavků rozdělený podle jejich priority

Počet požadavků podle kategorie zařízení

Počet požadavků podle druhu/typu zařízení a SW

Úroveň služby

Základní logika reportů této skupiny je postavena stejně jako ta předchozí na dvou částech. První část, první třetina níže uvedeného screenshotu určuje, jaký typ reportu bude vygenerován (seskupení reportu). Parametry v další, tedy spodní části, určují filtry obsahu reportu samotného.

Hlavní pohled na tvorbu reportů ze skupiny Úroveň Služby

Níže uvádíme kompletní seznam možných reportů (tedy seskupení podle pole) ve skupině Úroveň Služby:

SLA
Poskytovatel
OrganizacePoskytovatele
KategorieOrganizacePoskytovatele
Zákazník
Organizace Zákazníka
KategorieOrganizaceZákazníka
Smlouva
PrvekSmlouvy
Naplnění
Odchylka
Distribuce

Základní filtry pro reporty (seskupení podle) v této skupině jsou:

- Otevřená Volání – do reportu jsou zahrnuty všechna vytvořená volání
 - Uzavřená Volání – do reportu jsou zahrnuty již jen ukončená volání
- Rozsah Distribuce – v procentech, nastavení pro vyobrazení jak daleko od předepsaného SLA se nachází reálně dosažená hodnota kvality služby
- Typ SLA – zda bude generován report nad parametrem Odezva (Response Time) nebo Obnovení (oprava, Fix Time)
- Časové hodnoty – vymezení hodnot od kdy, do kdy má report být vygenerován
- Časová granularita – vymezení detailu
- na rok
 - na měsíce a roky
 - na měsíc
 - na dny

V této sadě reportů "Úroveň Služby" jsou k dispozici tyto parametry pro tvoření filtrů obsahu reportu:

• Poskytovatel	Umístění	ProvincieKontaktu
• ProvinciePoskytovatele	ProvincieUmístění	KategorieKontaktu
• KategoriePoskytovatele	KategorieUmístění	ProvincieOperátoraHelpDesku
• StátPoskytovatele	Komponenta	KategorieOperátoraHelpDesku
• OrganizacePoskytovatele	DruhZařízení	Fronta
• KategorieOrganizacePoskytovatele	Výrobce	Fronta2
	KategorieVolání	Fronta3
• ProvincieOrganizacePoskytovatele	KategorieVolání1+2	ÚroveňFronty
	KategorieVolání1–3	Řešitel
• Zákazník	KategorieVolání1–4	Řešitel2
• KategorieZákazníka	• KategorieVolání1–5	• Řešitel3
• ProvincieZákazníka	KategoriePříčiny	DruDodavateložadavku

StátZákazníka	KategoriePříčiny1+2	• SkupinaStavůVolání
Organizace Zákazníka	KategoriePříčiny1–3	• SkupinaPriorit
KategorieOrganizaceZákazníka	KategoriePříčiny1–4	• TypSkupinyProblému
ProvincieOrganizaceZákazníka	KategoriePříčiny1–5	• SkupinaTypůChyb
Smlouva	PříjmeníVolajícího	• SkupinaZávažnosti
PrvekSmlouvy	PoskincieVolajícího	
Priorita	KategorieVolajícího	
DruDodavatelroblému		
DruhChyby		
Závažnost		
StavVolání		

Níže uvádíme nejčastěji využívané reporty ze sady Množství Volání:

Celkový pohled na percentuální plnění SLA parametrů Odezva a Obnova

Screenshot zachycující percentuální plnění SLA po jednotlivých měsících s rozdělením na jednotlivé poskytované služby

Percentuální přehled plnění SLA za jednotlivé měsíce včetně procenta ještě rozpracovaných požadavků

Odchylka od definovaného SLA v hodinách – slouží k analýze trendu kvality služby

Report distribuce plnění definovaných SLA – jak percentuálně je rychlé plnění SLA v rozsahu –50% až +50% (volitelné)

Čas služby

Základní logika reportů této skupiny je postavena stejně jako ta předchozí na dvou částech. První část, první třetina níže uvedeného screenshotu určuje, jaký typ reportu bude vygenerován (seskupení reportu). Parametry v další, tedy spodní části, určují filtry obsahu reportu samotného.

Hlavní pohled na tvorbu reportů ze skupiny Úroveň Služby

Níže uvádíme kompletní seznam možných reportů (tedy seskupení podle pole) ve skupině Úroveň Služby:

Poskytovatel
OrganizacePoskytovatele
KategorieOrganizacePoskytovatele
Zákazník
Organizace Zákazníka
KategorieOrganizaceZákazníka

Smlouva
PrvekSmlouvy
Distribuce

Základní filtry pro reporty (seskupení podle) v této skupině jsou:

- Otevřená Volání – do reportu jsou zahrnuty všechna vytvořená volání
- Uzavřená Volání – do reportu jsou zahrnuty již jen ukončená volání
- Rozsah Distribuce – v hodinách, nastavení pro vyobrazení jak dlouho od předepsaného SLA se nachází reálně dosažený čas
- Typ SLA – zda bude generován report nad parametrem Odezva (Response Time) nebo Obnovení (oprava, Fix Time)
- Časové hodnoty – vymezení hodnot od kdy, do kdy má report být vygenerován
- Časová granularita – vymezení detailu
 - na rok
 - na měsíce a roky
 - na měsíc

V této sadě reportů "Úroveň Služby" jsou k dispozici tyto parametry pro tvoření filtrů obsahu reportu:

• Poskytovatel	Umístění	ProcincieKontaktu
• ProvinciePoskytovatele	ProvincieUmístění	KategorieKontaktu
• KategoriePoskytovatele	KategorieUmístění	ProvincieOperátoraHelpDesku
• StátPoskytovatele	Komponenta	KategorieOperátoraHelpDesku
• OrganizacePoskytovatele	DruhZařízení	Fronta
• KategorieOrganizacePoskytovatele	Výrobce	Fronta2
• ProvincieOrganizacePoskytovatele	KategorieVolání	Fronta3
• Zákazník	KategorieVolání1+2	ÚroveňFronty
• KategorieZákazníka	KategorieVolání1–3	Řešitel
• ProvincieZákazníka	KategorieVolání1–4	Řešitel2
• StátZákazníka	KategorieVolání1–5	Řešitel3
• Organizace Zákazníka	KategoriePříčiny	DruDodavateležadavku
• KategorieOrganizaceZákazníka	KategoriePříčiny1+2	SkupinaStavůVolání
• ProvincieOrganizaceZákazníka	KategoriePříčiny1–3	SkupinaPriorit
• Smlouva	KategoriePříčiny1–4	TypSkupinyProblému
• PrvekSmlouvy	KategoriePříčiny1–5	SkupinaTypůChyb
• Priorita	PříjmeníVolajícího	SkupinaZávažnosti
• DruDodavateleproblému	PoskincieVolajícího	
• DruhChyby	KategorieVolajícího	
• Závažnost		
• StavVolání		

Níže uvádíme nejčastěji využívané reporty ze sady Množství Volání:

V hodinách vyjádřená doba potřebná k vyřešení požadavků v jednotlivých měsících na všechny typy SLA

V hodinách vyjádřená doba potřebná k vyřešení požadavků v jednotlivých měsících v detailu podle SLA

Počty a procentuálně vyjádřená distribuce délky řešení SLA v krocích a rozsahu od 10 do 480 hodin (volitelné)

CMDB – online přístup k instalované bázi

Součástí reportingu jsou i data z CMDB, tedy databáze, která obsahuje informace o instalované bázi. Ke každému zařízení je přiřazeno smluvně stanovené SLA a další informace. Tento přehled je k dispozici on-line přes webové rozhraní a poskytuje plnou funkcionalitu obvyklou pro ostatní reporty tedy především:

Fulltextové vyhledávání

- Vyspělou filtraci (část řetězce, hodnoty, limity, prázdné/plné hodnoty atd.)
- Seskupování (grouping) podle polí viz. níže
- Export do Excelu, CSV a XML následujících polí:
 - Zkrácený název
 - Typ/Model
 - Sériové číslo
 - IPAdresa
 - Produktová skupina
 - Výrobce
 - Smlouva SLA
 - Lokalita
 - Ulice
 - Město
 - JeAktivní
 - ZačátekZáruky
 - KonecZáruky
 - ÚdržbaDo
 - HlavníOčekávání
 - HlavníDatum
 - MěsíceÚdržby
 - PlánovanýPočetÚdržby
 - OtevřenýPočetÚdržby
 - ÚdržbaJeAktivní

Seznam informací které lze na požádání a zdarma do reportů pro Service Manažery přidat je velmi rozsáhlý a obsahuje přes 50 dalších polí z databáze CMDB. Pole, jež budou využita pro poskytování služby odpovídají požadavkům na informační hodnotu reportů a jsou součástí dohody na počátku poskytování služeb.

Přehled nad celou instalovanou bází

Seskupení zařízení podle SLA; znaménkem "+" vlevo se zobrazí seznam zařízení s daným SLA

Seskupení instalované báze podle Modelu; znaménkem "+" vlevo se zobrazí seznam zařízení daného Modelu

Seskupení zařízení podle lokality, na které jsou nainstalována; znaménkem "+" vlevo se zobrazí seznam

6.3. Havarijní scénáře

6.3.1. Metodika zpracování analýzy rizik

Každý projekt je ovlivněn řadou faktorů, které mohou mít negativní vliv na dosažení cíle. Řízením rizik se snažíme eliminovat či zmírnit výskyt nemilých překvapení a to po celou dobu provozu IS. Prvním krokem je určení odpovědných osob za všechny zúčastněné strany, které se řízením rizik budou zabývat.

Při samotném řízení rizik, které bude probíhat nejen na začátku projektu, ale v celém průběhu poskytování podpory IS, budou prováděny tyto činnosti:

6.3.1.1. Identifikace/analýza rizik

Identifikaci rizik můžeme charakterizovat jako pravidelné a kontinuální monitorování všech probíhajících interních a externích událostí, které ovlivňují naplňování cílů. U těchto událostí pak rozlišujeme pozitivní nebo negativní dopad. Události, které mají negativní dopad, jsou rizika.

6.3.1.2. Zpracování analýzy rizik a hodnocení rizik

Vzhledem k množství rizik je třeba je zanalyzovat a určit jejich pravděpodobnost a dopad, tím určit jejich významnost a prioritu jejich řešení.

Rizika mohou být vyjádřena kvalitativně a kvantitativně. V rámci počáteční fáze projektu i fáze podpory IS zvolíme kvalitativní vyjádření – malý, střední, velký, kritický. Vyhodnocení významnosti rizik může provádět buď dostatečně odborně vybavený jednotlivec, nebo skupina odborníků, v případě tohoto projektu hodnocení provádí pracovní tým projektu a schvaluje ŘV.

6.3.1.3. Strategie zvládnutí rizik

Jedná se o určení způsobu, jak se s daným rizikem vypořádáme, jak ovlivníme jeho dopad a pravděpodobnost – zda se ho raději vyvarujeme, akceptujeme ho, minimalizujeme ho či ho přeneseme.

Výsledek identifikace, vyhodnocení a strategie zvládnutí rizik je zaznamenán do tzv. registru rizik, který je veden v elektronické formě.

Kromě klasifikace rizik obsahuje i nápravná opatření a sledování jejich úspěšné aplikace. Důležité je také určit odpovědnou osobu spojenou s provedením preventivního opatření.

6.3.1.4. Monitorování, vykazování a reportování

Pravidelná aktualizace registru rizik je potřebná pro včasnou identifikaci případných nových rizik, přehodnocování dříve identifikovaných rizik, posuzování opatření na jeho zvládnutí (původní strategie funguje, není potřeba nějaká změna?), aktualizace dokumentace, komunikace.

Během jakéhokoli projektu se mohou objevit další rizikové události, a proto musejí být rizika stále monitorována.

Registr rizik bude mít minimálně tyto položky (příklad v tabulce níže).

		Dopad	Váha Rizika	Řešení	Vlastník
Riziko 1		Vysoký: 3		veškeré potřebné SW a přístupy jsou všem k dispozici	
			X		
		Nízký: 1			
Riziko 2			Váha	Řešení	Vlastník
		Vysoký: 3		Včasná definice pravidel a procesů s následnými testy a odsouhlasením uživateli jejich funkce v systémech	Projektový Manažer a Manažer ServiceDesk

Registr rizik připraví a bude aktualizovat pracovní tým projektu. ŘV bude registr rizik schvalovat, tzn. schvalovat identifikovaná rizika, jejich klasifikaci a přijatá opatření.

6.4. Postup zajištění procesu změnových řízení

Tento proces řídí veškeré změny oproti stávajícímu stavu IT, které nějakým způsobem mohou nebo zasáhnou do činností Zadavatele. Změnová řízení platí pro změny v IT službách,

software, hardware, síti. S&T zajistí co nejmenší dopad změn za využití standardních procesů jak komunikovat a implementovat takové změny.

	Dopad na podnikání (Business impact)	Komunikace a schvalování Zadavatelem	Příklad
	Velmi malé nebo se opakující změny, jenž jsou běžného provozního charakteru, <i>bez jakéhokoli dopadu</i> na podnikání.	Není třeba.	Vytvoření účtu novému zaměstnanci.
Malé	Malé změny, které mají dokumentovaný a vyzkoušený postup implementace s <i>velmi malým</i> dopadem na podnikání.	S&T upozorní Zadavatele <i>pět dní před</i> provedením změny. Postačuje zpráva Zadavatele bez potvrzení o jejím přijetí.	Instalování nového service packu na server.
Střední	Změny, které mohou ohrozit vícero aplikací a mají <i>širší</i> dopad na podnikání.	S&T upozorní Zadavatele <i>pět dní před</i> provedením změny. Zadavatel <i>musí</i> potvrdit přijetí zprávy.	Instalace nebo reinstalace serveru, změny v LAN.
	Změny, které mohou ohrozit vícero aplikací skrze celou společnost a mají <i>signifikantní dopad</i> na podnikání.	S&T upozorní Zadavatele <i>deset dní před</i> provedením změny. Zadavatel <i>musí</i> potvrdit přijetí zprávy.	Spuštění nového antiviru, změna IS. Komplexní výměna HW včetně SW.
Kritické (mimo prac. dobu)	Změny, které musí být provedeny za účelem zprovoznění havarované IT služby s <i>nějakým dopadem</i> na podnikání.	S&T <i>co nejdříve</i> po zjištění nutnosti takové změny informuje Zadavatele. Potvrzení takové zprávy od Zadavatele je preferováno.	"Zatuhlá" služba na serveru – musí být opraveno ještě před začátkem zálohování.
	Změny, které musí být provedeny za účelem zprovoznění havarované IT služby s <i>kritickým dopadem</i> na podnikání. Dopad na podnikání vyžaduje okamžité řešení.	S&T informuje Zadavatele až po samotném vyřešení problému. Potvrzení takové zprávy od Zadavatele je preferováno.	Útok viru.

7. Projektové řízení, organizace a harmonogram projektu

Uchazečem navrhované řešení bude respektovat požadavky zadavatele a to zejména s ohledem na co nejvyšší kvalitu a propracovanost metodiky projektového řízení a organizace projektu včetně účinné kontroly a navržených opatření k zajištění cílů projektu, dále na komplexnost a propracovanost navrženého harmonogramu a přístupů pro zajištění realizovatelnosti projektu.

Zhotovitel bude celý projekt implementovat řídit primárně dle mezinárodně uznávané metodiky IPMA, a dále dle dalších specifických metodik a standardů zohledňující dlouholeté působení uchazeče ve státní správě, které jsou nejvhodnější pro specifické dílčí části plnění tohoto projektu.

7.1. Popis způsobu a metodiky projektového řízení, organizace účastníků projektu

7.1.1. Organizace

Řízení projektu bude založeno na tříúrovňové hierarchii, bude tedy zabezpečeno prostřednictvím tří základních řídicích úrovní.

Nejnižší úroveň řízení jsou **pracovní týmy (PT)**, které jsou ustaveny k plnění konkrétního rozsahu úkolů v předem určených dílčích oblastech. Úkolem pracovních týmů je řešení běžných operativních, výrobních, logistických a dalších záležitostí, kontrola plnění dílčích úkolů dle harmonogramu a vytváření případných zadání požadavků na změnu na základě předložených návrhů. Výstupy z pracovních týmů a záležitosti, které potřebují rozhodnutí vyšší úrovně řízení, včetně požadavků na změnu, se ke schválení předávají na vyšší úroveň řízení a to na **Hlavní tým projektu (HTP)**.

Hlavní tým projektu (HTP) je základní řídicí platformou projektu, která má za úkol zajistit soulad postupu prací na projektu se schváleným věcným a časovým plánem. Hlavní tým projektu zároveň schvaluje všechny požadavky na změnu, financované z prostředků příslušné smlouvy. Nejvyšší strategickou úroveň řízení projektu pak zajišťuje **Řídicí výbor projektu (ŘV)**.

Řídicí výbor projektu (ŘV) řeší na nejvyšší řídicí úrovni zásadní otázky týkající se plnění či neplnění hlavních záměrů projektu jako celku. Zároveň přijímá opatření a definuje další postup v případě krizových stavů v rámci projektu.

Ze všech jednání týmů na všech úrovních jsou odpovědnými osobami dodavatele pořizovány zápisy, které jsou distribuovány k oponentuře všem členům příslušného týmu. Po zapracování připomínek je zápis schválen a uložen.

7.1.2. Struktura a kompetence orgánů řízení projektu

7.1.2.1. Řídicí výbor projektu (ŘV)

Nejvyšší strategická úroveň řízení projektu, na které se řeší zásadní otázky týkající se plnění či neplnění hlavních záměrů projektu jako celku, rozhoduje o případech eskalovaných z úrovně HTP, které se nepodařilo vyřešit na nižších úrovních a přijímá opatření a definuje další postup v případě krizových stavů. ŘV zpravidla rozhoduje na základě připravených podkladů vypracovaných hlavním týmem projektu nebo pro tyto účely ustavenými poradními či pracovními skupinami.

ŘV se bude scházet pravidelně nejméně 1× za čtvrtletí. V případě potřeby může podat návrh na svolání mimořádné schůzky ŘV vedoucí projektu objednatele nebo vedoucí projektu dodavatele s uvedením důvodů pro mimořádnou schůzku.

Uskutečnění mimořádné schůzky a její termín schvaluje vedoucí projektu objednatele.

Dodavatel navrhuje následující minimální složení ŘV:

- Zástupci objednatele
 - Zástupce vrcholového vedení Objednatele
 - Vedoucí projektu Objednatele
- Zástupci dodavatele
 - Vedoucí projektu dodavatele (Řídící manažer ŘV)
 - Zástupce vedoucího projektu dodavatele
 - Zástupce vrcholového managementu dodavatele

Na jednání ŘV mohou být fakultativně přizváni i další zástupci objednatele a dodavatele dle projednávané problematiky (zástupci odborných útvarů objednatele, garant infrastruktury dodavatele apod.).

7.1.2.2. Hlavní tým projektu (HTP)

Základní řídicí platforma projektu, na které jsou projednávány výstupy z pracovních týmů a záležitosti, které potřebují rozhodnutí vyšší úrovně řízení. Hlavní tým projektu zároveň schvaluje všechny požadavky na změnu, financované z prostředků příslušné smlouvy.

Dodavatel navrhuje následující složení HTP:

- Zástupci objednatele
 - Vedoucí projektu objednatele
 - Zástupci zainteresovaných odborů poskytovatele (vedoucí nebo jimi delegovaní zástupci)
 - Odborní garanti odběratele:
 - Garant IS (osoba odpovědná za provoz ICT objednatele)
 - Garant provozu aplikační vrstvy
 - Garant bezpečnosti objednatele
 - atd.
- Zástupci dodavatele
 - Zástupce vedoucího projektu dodavatele (řídící manažer HTP)
 - Vedoucí projektu dodavatele
 - Odborní garanti dodavatele dle časových etap a věcné problematiky:
 - Garant IS
 - Garant provozu
 - Garant bezpečnosti
 - atd.

Jednání HTP se mohou účastnit podle potřeby i další zástupci objednatele, a to pravidelně či pouze pro potřeby projednání specifického tématu, avšak vždy se souhlasem vedoucího projektu objednatele. Obdobně se jednání HTP mohou účastnit podle potřeby další zástupci dodavatele, a to pravidelně či pouze pro

potřeby projednání specifického tématu, avšak vždy se souhlasem vedoucího projektu dodavatele nebo zástupce vedoucího projektu poskytovatele.

Jednání HTP se koná pravidelně nejméně 1x za dva týdny.

Pro každé jednání HTP bude připravena ze strany dodavatele agenda; z každého jednání dodavatel zpracuje zápis, který bude po kontrole vedoucím projektu objednatele za obě strany podepsán. Výstupy z jednání budou promítány i do další projektové dokumentace.

HTP využívá pro svou práci výstupů činnosti z úrovně pracovních či poradních týmů (PT) nebo jednotlivců.

Minimální agenda pravidelného jednání HTP o stavu projektu bude v rozsahu:

- Projednání a schválení zdroje financování předložených požadavků na změnu (jsou-li předloženy).
- Projednání a odsouhlasení dokumentů/návrhů připravených pracovními týmy.
- Kontrola plnění úkolů – za období od předchozího jednání.

Pokud mají projednávání skutečnosti dopad na celkový časový, finanční nebo věcný rozsah plnění dle smlouvy, je nutné jejich projednání a schválení na ŘV.

7.1.2.3. Pracovní týmy

Pracovní týmy představují nejnižší úroveň řízení a jsou ustaveny k plnění konkrétního rozsahu úkolů v předem určených dílčích oblastech. Úkolem pracovních týmů je řešení běžných provozních záležitostí, kontrola plnění dílčích úkolů dle harmonogramu a vytváření zadání požadavků na změnu na základě předložených návrhů.

Úkolem pracovního týmu je především:

- kontrola plnění dílčích úkolů,
- řešení běžných provozních problémů, vytváření a připomínkování dílčích výstupů projektu, eskalace nestandardních/neplánovaných situací a zjištěných rizik, které vznikly nebo byly identifikovány v průběhu realizace projektu, vytváření zadání požadavků na změnu, schvalování požadavků na změnu z věcného hlediska, návrh způsobu financování pro požadavky na změnu k předložení na jednání HTP,
- příprava podkladů pro Hlavní tým projektu.

Schůzky pracovního týmu navrhujeme v týdenních intervalech, pokud nebude dohodnuto jinak. Z jednání pracovních týmů bude vždy pořízen zápis, který bude distribuován k připomínkám všem zúčastněným osobám a jiným zainteresovaným stranám.

Dodavatel navrhuje následující složení PT:

- Vedoucí pracovního týmu dodavatele
- Zástupce vedoucího projektu dodavatele
- Dle konkrétní situace delegování pracovníci Zadavatele

Na jednání jednotlivých pracovních týmů mohou být fakultativně přizváni i další zástupci objednatele a dodavatele dle projednávané problematiky.

7.

Vedoucí projektu objednatele je zástupce objednatele, odpovědný za koordinaci činností, spojených s realizací projektu na straně objednatele na úrovni Hlavního týmu projektu.

Zejména se jedná o:

- určení a koordinaci jednotlivých odborných garantů relevantních systémů na straně objednatele, zajištění součinností na straně objednatele,
- kontrolu přidělených úkolů a odpovědnost za splnění těchto úkolů vůči HTP, koordinaci časových možností na straně objednatele (řešení časových kolizí s jinými pracovními úkoly),
- koordinaci oponentury jednotlivých výstupů odbornými guaranty na straně objednatele.

Vedoucí projektu objednatele je členem Řídícího výboru a Hlavního týmu projektu. Do pracovního týmu jmenuje svého odpovědného zástupce, odpovědného na úrovni pracovního týmu za koordinaci činností spojených s realizací projektu.

7.1.3.2. Vedoucí projektu dodavatele

Zástupce dodavatele, odpovědný za koordinaci činností spojených s realizací projektu.

Především jde o:

- koordinaci aktivit celého realizačního týmu, včetně podřízených dodavatelů,
- kontrolu přidělených úkolů a odpovědnost za splnění těchto úkolů vůči HTP,
- koordinaci přípravy výstupů k oponentuře.

Vedoucí projektu dodavatele je řídícím manažerem Řídícího výboru a členem Hlavního týmu projektu.

7.1.3.3. Odborný garant IS objednatele

Zástupce objednatele, jmenovaný pro každý podporovaný či implementovaný systém.

V rámci jemu svěřenému systému odpovídá zejména za:

- definici funkčních požadavků,
- posouzení návrhů na změnu systému,

- spolupráci při zpracování zadání požadavku na změnu,
- v rámci pracovního týmu je odpovědný za schválení požadavků na změnu z věcného hlediska, přípravu potřebných podkladů a znalostí na schůzku (tj. přípravu na jednání dle avizované agendy schůzky pracovního týmu), přípravu a provedení funkčních a následně akceptačních testů dle dodavatelem zpracovaných a objednatelem schválených testovacích scénářů,
- splnění úkolů definovaných na schůzce pracovního týmu v dohodnutém rozsahu a čase.

Účastní se schůzek pracovního týmu, ve výjimečných případech písemně jmenuje svého zástupce na konkrétní schůzku, které se nemůže zúčastnit. Na schůzku si může přizvat potřebný počet spolupracovníků v dané oblasti. Stále je ale jedinou odpovědnou osobou za dohodnuté závěry v rámci jemu svěřené oblasti.

7.1.3.4. Systémový a aplikační architekt

Zástupce dodavatele, který podléhá řízení Vedoucího projektu dodavatele a odpovídá za odborné činnosti a návrh i implementaci řešení v oblasti síťové a aplikační infrastruktury, databází, konsolidace datových zdrojů, serverových farem, operačních systémů, uživatelských rozhraní atd.

7.1.3.5. Garant bezpečnosti dodavatele

Pracovník na této pozici je odpovědný za zajištění procesu řízení bezpečnosti, včetně kontrol, zpracování pravidelných reportů, nezbytné dokumentace apod. V rámci své činnosti spolupracuje s garantem bezpečnosti objednatele, se kterým projednává návrhy na bezpečnostní opatření a spolupracuje při zpracování bezpečnostních auditů. Garant bezpečnosti je dále odpovědný za posuzování aktivit jednotlivých procesů řízení služeb provozu ICT z hlediska jejich vlivu na bezpečnost, tzn. za identifikaci bezpečnostních rizik, která včas eskaluje na příslušné orgány řízení projektu.

7.1.3.6. Technický specialista dodavatele

Technický specialista je odborným pracovníkem v jednotlivých oblastech realizace projektu (administrátor, analytik, architekt, operátor, konzultant) na straně dodavatele a jeho subdodavatelů. Techničtí specialisté zároveň zastávají role specialistů v jednotlivých procesech implementace a řízení služeb.

7.1.4. Projektová jednání

Rozlišují se následující dva základní typy jednání:

- kontrolní a řídicí jednání (jednání ŘV a HTP),
- pracovní schůzka – jednání pracovního týmu.

Příprava podkladů (rozbor, vypracování návrhu atd.) probíhá výhradně mimo jednání. Zajištění podkladů je vždy povinností toho, kdo jednání vede (v případě HTP je to zpravidla vedoucí projektu dodavatele), aby nedocházelo k prolínání

kontrolní a řídicí činnosti s řešením konkrétních pracovních podkladů. U ad-hoc svolaných jednání zajišťuje podklady vždy ten pracovník, který jednání inicioval.

7.1.4.1. Příprava na projektová jednání

Každé jednání musí být připraveno a realizováno minimálně v následujícím rozsahu:

Činnost	Odpovědnosti – ŘV	Odpovědnosti – HTP	Odpovědnosti – PT
Návrh termínu a délky schůzky	Vedoucí projektu objednatele	Vedoucí projektu objednatele	Odborný garant, Vedoucí pracovního týmu (řídící manažer)
Příprava agendy	Vedoucí projektu dodavatele	Vedoucí projektu dodavatele	Vedoucí pracovního týmu (řídící manažer)
Zajištění jednací místnosti	Vedoucí projektu objednatele	Vedoucí projektu objednatele	Odborný garant
Osobní příprava na schůzku dle agendy	Vedoucí projektu a přizvaní členové	Vedoucí projektu a přizvaní členové	Odborný garant, Vedoucí pracovního týmu, členové týmu dle pokynů garanta
Provedení jednání	Vedoucí projektu objednatele, Vedoucí projektu dodavatele a přizvaní členové	Vedoucí projektu objednatele, Vedoucí projektu dodavatele a přizvaní členové	Odborný garant, Vedoucí pracovního týmu a přizvaní členové
Zpracování návrhu zápisu	Vedoucí projektu objednatele	Vedoucí projektu objednatele	Vedoucí pracovního týmu (řídící manažer)
Oponentura a odsouhlasení zápisu	Vedoucí projektu objednatele, Vedoucí projektu dodavatele	Vedoucí projektu objednatele, Vedoucí projektu dodavatele	Odborný garant, Vedoucí pracovního týmu
Realizace úkolů vyplývajících ze schůzky	Vedoucí projektu objednatele, Vedoucí projektu dodavatele	Vedoucí projektu objednatele, Vedoucí projektu dodavatele	Odborný garant a vedoucí pracovního týmu

7.1.4.2. Oponentura a odsouhlasení zápisů

Z každého jednání připravuje příslušná odpovědná osoba ze strany dodavatele zápis.

V případě Řídícího výboru nebo Pracovního týmu je návrh zápisu zaslán e-mailem odpovědné osobě za stranu objednatele elektronickou poštou k oponentuře a je vyžádáno potvrzení o přečtení této zprávy (případně je u odpovědné osoby ověřeno, že tento zápis obdržela). Objednatel je povinen v dohodnutém termínu se k zápisu vyjádřit nebo jej odsouhlasit zpět e-mailem odesílateli zápisu, který potvrzuje vypořádání připomínek.

Zápis z pracovního týmu se stává platným a závazným již po tomto e-mailovém odsouhlasení nebo po uplynutí lhůty 3 pracovních dnů po odeslání zápisu, pokud nepřišla od odpovědné osoby objednatele zpět žádná reakce (kromě potvrzení přijetí e-mailu). Finální schválení zápisu z Řídícího výboru se provádí podpisem zápisu odpovědnými zástupci za stranu dodavatele objednatele.

V případě možnosti budou zápisy zpracovávány s využitím dataprojektoru tak, že mají možnost se k zápisu v aktuálním čase vyjádřit všechny zúčastněné strany. Zápis je pak podepisován na místě.

Zápisy jsou po schválení uloženy jako součást dokumentace projektu na dokumentačním úložišti zřízeném pro účel centrální evidence dokumentace projektu. Za ukládání a správu zápisů z jednání odpovídá až do aktivace Projektové kanceláře pracovní tým PT ADMIN.

7.2. Šablony projektových dokumentů

Uchazeč bude v rámci plnění předmětu smlouvy po celou dobu trvání projektu aplikovat metodiky a best practices projektového řízení dle standardů IPMA a ISO10.006.

Administraci projektu bude zajišťovat projektová kancelář prostřednictvím projektového manažera. Projektová kancelář umožní přístup oprávněným subjektů řízení projektu k potřebným uloženým informacím o projektu, jako jsou zejména:

- Harmonogram projektu (vzor viz kap.8.8),
- Projektová dokumentace - Analýza, Funkční specifikace, Technická specifikace, Uživatelská, Školící, Administrátorská dokumentace, apod. (dokumenty poskytnuté Zadavatele),
- Projektové výkazy činností,
Komunikační matice,
Zápisy z jednání projektových týmů (na úrovni řídicího výboru a pracovních skupin),
Zpráva o stavu projektu,
Předávací protokoly,
Akceptační protokoly,
Změnové požadavky,
Testovací protokoly,
Zpráva o ukončení projektu (předání do provozu).

7.3. Analýza rizik

Riziko je nejistá událost nebo podmínka, která když nastane, ovlivní nepříznivě projekt z pohledu naplnění jeho cílů. Řízení rizik je soubor postupů a nástrojů sloužících k identifikaci rizik, jejich vyhodnocení a přijetí opatření k jejich omezení z pohledu vyhodnocení událostí, které mohou mít nepříznivý vliv na jakékoli události, které jsou předmětem řízení projektu.

Cílem řízení rizik je identifikace a specifikace jednotlivých rizik projektu včetně posouzení jejich dopadů a celkové závažnosti a vymezení vhodných opatření na prevenci daného rizika

nebo omezení následků při reálném uplatnění daného rizika. Na základě identifikace a specifikace jsou následně vybraná opatření plánována v rámci projektu.

Některá identifikovaná rizika mohou být záměrně akceptována bez jakýchkoli opatření (nebo jen s omezenými opatřeními) s ohledem na přílišnou (danému riziku neadekvátní) náročnost některých opatření (zejména nároky na časové, finanční a lidské zdroje).

Řízení rizik projektu bude provádět průběžně Vedení projektových týmů a jejich zjištění bude konsolidováno Vedením projektu. Tuto činnost koordinuje Projektový manažer tak, aby se plně prošetřila možná rizika. Zjištěná závažná rizika, jejich dopady a návrhy na jejich řešení či omezení jsou neprodleně předkládány k posouzení a případnému rozhodnutí Řídícímu výboru projektu.

Každý projekt, bez ohledu na velikost, vždy přináší rizika a problémy spojené s jeho realizací. Je nezbytné je rozpoznat a zvládat tak, aby se minimalizovaly škody a maximalizovaly šance na úspěch.

Rizika se hodnotí podle dvou faktorů:

Pravděpodobnosti, že se něco stane

Důsledku, jaký bude na projekt mít to, že se to stane

7.3.1. Identifikace rizik

Metodika rozlišuje pro účely řízení rizik dvě základní skupiny:

- **Externí rizika:** rizika působící na projekt z vnějšího prostředí, které je nezávislé na bezprostředních smluvních závazcích, které spolu smluvní strany uzavřely, jejich splnitelnost však může podmiňovat. Možnost ovlivňovat výskyt externích rizik (prevence) je (s ohledem na jejich charakter) velmi omezená. V případě externích rizik jsou dominantní opatření na omezení jejich dopadů.
- **Interní rizika:** rizika projektu mající rámec ve smluvních vztazích mezi smluvními stranami. Výskyt interních rizik je možno do značné míry ovlivnit vzhledem k tomu že přímo souvisí s průběhem a vývojem projektu. V případě interních rizik jsou kombinována opatření na omezení výskytu rizik a opatření na omezení jejich dopadů.

Každé jednotlivé identifikované riziko musí být specifikováno v následujícím rozsahu:

- **Vymezení:** popis rizika a jeho projevů, na jehož základě lze riziko identifikovat,
- **Dopady:** popis možných dopadů rizika na projekt,
- **Opatření:** plánovaná opatření, která mohou riziko vyloučit nebo podstatně omezit jeho působení a dopady,
- **Závažnost:** určení aktuální míry ohrožení projektu daným rizikem, která je posouzena a stanovena na základě aktuální pravděpodobnosti výskytu rizika a na základě aktuální závažnosti potenciálních dopadů rizika do projektu. Zejména závažnost rizik ve škále Nízká / Střední / Vysoká je nutné přehodnocovat průběžně.

Analýza rizik bude dále prováděna na úrovni vedení projektových týmů a koordinována na úrovni vedení projektu průběžně vzhledem k tomu, že rizika projektu se mohou měnit jak co do struktury (vznik a zánik rizik), tak do povahy existujících rizik (změna specifikace rizik a to zejména aktuální závažnosti).

V průběhu projektu bude nutné rizika přehodnocovat zejména v případech přechodu mezi jednotlivými fázemi realizace projektu.

Každý člen projektového týmu je povinen neprodleně informovat nadřízeného vedoucího projektového týmu o skutečnostech, které mohou reálně negativně ovlivnit projekt. Každý vedoucí projektového týmu je povinen neprodleně zvážit informace o skutečnostech, které mohou reálně negativně ovlivnit projekt a vyhodnotí-li je jako riziko projektu, pak o tomto riziku neprodleně informovat vedoucí projektového týmu. Vedení projektu je povinno zvážit dané riziko a informovat o něm Řídící výbor projektu.

Každé jednotlivé identifikované riziko musí být vedením projektu specifikováno ve výše uvedeném rozsahu. V případě závažných rizik projektu ovlivňujících rámec projektu daný smluvní dokumentací nebo zásadně ovlivňující organizaci Zadavatele musí být Řídící výbor projektu informován neprodleně.

Za výkon identifikace rizik odpovídají všechny zainteresované strany v projektu, tj. včetně všech členů projektového týmu Dodavatele a Zadavatele. Projektový manažer udržuje celkový "Registr rizik" projektu.

7.3.2. Hodnocení rizik

Hodnocení rizik rozdělujeme následujícím způsobem na:

- Kvantitativní
 - Určíme pravděpodobnost a hodnotu ztráty, vytvoříme součin jehož hodnota je vyjádřena v peněžních jednotkách.
- Kvalitativní
 - Dopad a pravděpodobnost se určí verbálně (velký, malý apod.) nebo s pomocí bodovací stupnice bez peněžního významu. Tato metoda slouží k určení priority rizik.

Tato tabulka je finálním produktem identifikační části analýzy a následuje finální analytická činnost představující zatřídění rizik do jednotlivých tříd.

V praxi vypadá hodnocení rizik ze strany uchazeče následujícím způsobem. Tato tabulka je také součástí registru rizik:

Riziko	Garant	Pravdě podob nost [%]	Potenciál poškození	Důležitost	Pořadí	Opatření proti riziku
Riziko1	Garant1	10	10	100	3.	Opatření1
Riziko2	Garant2	30	5	150	1.	Opatření2
Riziko3	Garant3	15	8	120	2.	Opatření3
Riziko4	Garant3	5	2	10	4.	Opatření4

Ve výše uvedené tabulce si pro každý faktor rizika (riziko) určíme:

Pravděpodobnost výskytu rizika (Pravděpodobnost) a to v hodnotách od 0 až do 100%

Potenciál poškození a to například v hodnotách od 1 (nejmenší) až 10 (největší)

Míru důležitosti (Důležitost) poté vypočítáme jako součin hodnot Pravděpodobnost krát (*) Potenciál poškození

Následně z těchto hodnot určíme pořadí rizik podle důležitosti a vybereme rizika, která zařadíme do plánu rizik

7.3.3. Opatření na eliminaci rizik

V rámci opatření rizik bude uchazeč používat dále současně preventivní (proaktivní) a následný (reaktivní) přístup k odezvě na riziko:

- **Proaktivní přístup** (prevence vzniku této situace)
 - Identifikace, eliminace a řízení rizik

Identifikace rizik

Vytvoření rizikové analýzy

Vytvoření mechanismu hodnocení rizik

Určení výše dopadu a pravděpodobnosti vzniku rizik

Eliminace rizik

- Vyloučení rizika zákaz vybraných rizikových aktivit a procesů
- Snížení rizika snížení velikosti dopadu např. pojištěním rizika
- Přenos rizika – redukce rizika snížením pravděpodobnosti nežádoucích událostí
- Přijetí rizika – akceptace rizika na stávající úrovni bez dalších aktivit
- Uplatňování zásad projektové řízení, správné nastavení úrovně řízení projektu, pravidelný Řídící výbor projektu, ustanovení sponzora projektu
 - Kontrolní den na měsíční bázi
 - Pravidelný reporting a průběžné sledování požadavků uživatelů v HelpDeskovém systému zadavatele
 - Využití projektových a procesních manažerů uchazeče disponujících mezinárodně uznávanými certifikacemi ITILv3, ISO 10.006 a IPMA
- Uplatňování zásad procesního řízení (ITIL)
- Řízení subdodavatelů a řízení kvality
- Pojištění – tento nástroj řešení rizik v sobě zahrnuje aktivní složku prevence, tj. minimalizace ztrát v případě výskytu rizika

Reaktivní přístup (řešení situace až v případě vzniku rizika s cílem minimalizovat dopady). Uchazeč bude reagovat průběžně s ohledem na aktuální vývoj výskytu vybraných rizik v rámci projektu, které nelze řešit proaktivně a to např. z důvodu neekonomičnosti (tj. neúměrně vysokých nákladů na eliminaci těchto rizik), atd.

Když byla vyhodnocena pravděpodobnost a dopady každého rizika, je potřeba konkrétně naplánovat, jak se na dané riziko bude reagovat. Reakce na rizika má buď snížit jejich pravděpodobnost nebo omezit jejich nepříznivé důsledky, ev. oboje. Reakce na rizika v projektu mohou být následující:

- Akceptace – nebude se dělat nic. Znamená to, že projekt dané riziko toleruje, s tím, že pokud by se naplnilo, zvládnou se případné důsledky pomocí zavedených postupů.

Ošetření rizika – naplánují se a provedou opatření snižující pravděpodobnost naplnění daného rizika. Například se naplánuje nějaká rezerva nebo dodatečné zdroje.

- Přenesení rizika – speciální forma snížení rizika, při níž se důsledky daného rizika převedou na nějakou třetí stranu. Například se použije penále vůči dodavateli.

Ukončení činnosti, z níž dané riziko vyplývá. Jinými slovy taková změna rozsahu projektu, že se možnost naplnění rizika vyloučí.

Vedle zřejmých negativních efektů rizik mohou někdy z nejistoty vyplývat i pozitivní příležitosti. Hledání příležitostí vyžaduje uvažovat o věcech, u kterých nebyla zjištěna žádná rizika.

Řízení rizik tedy znamená:

- Přidělení rizika konkrétní osobě (vlastníkovi), zodpovídající pak za schválené (re)akce

Hodnocení výsledků, které provedené akce přinesly

Opakované vyhodnocování rizik a rozhodování o případných dalších opatřeních

Kontrola toho, jestli neexistují ještě další, zatím neidentifikovaná rizika (příležitosti)

Veškeré informace o rizicích a plánovaných i provedených opatřeních se zaznamenávají do Evidence rizik.

Součinnost Objednatele). Takové řešení umožňuje implementaci komplexnější logiky transformace a čištění dat a zaznamenávání případných nekonzistencí a problémů ve stávajících datech.

Preferovaným formátem poskytnutí dat pro migraci je přímý přístup k databázím stávajících systémů a dodání patřičné dokumentace.

V analýzách jednotlivých projektů bude dále specifikováno:

- Jednotlivé zdroje dat pro migraci

Definice obsahu a struktury přenášených dat

Způsob konsolidace dat

Způsob čištění dat – jak bude zajištěno řešení duplicitních záznamů, řešení neaktuálních záznamů a řešení dalších nekonzistencí

V době přípravy i v době provádění migrace dat bude nutná součinnost Objednatele. Při migraci bude zajištěna integrita migrovaných dat, případné nekonzistence a problémové záznamy mohou být dále čištěny ručně za součinnosti Objednatele. Migrovaná data budou s ohledem na jejich charakter dělena na data aktuální a archivní. Aktuální data budou ukládána do aktivních produkčních databází, archivní data budou ukládána do archivu. Průběh migrace dat nebude ohrožovat činnost stávajících systémů.

Navrhovaný migrační plán uchazeče má 3 vrstvy, které je potřeba zohlednit:

- Plánování z pohledu harmonogramu projektu – postup hlavních částí:
 - Dodržení dodání dokumentace struktury a rozsahu dat Objednatelem v požadovaném termínu (viz harmonogram, nejpozději k začátku tvorby analýzy Návrhu realizace)
 - Dodržení dodání vzorku dat a jejich odpovídající dokumentace Objednatelem v požadovaném termínu (viz harmonogram, nejpozději k začátku tvorby prototypu) formátu struktury a kvalitě
 - Dodržení dodání dat a jejich odpovídající dokumentace Objednatelem v požadovaném termínu (viz harmonogram, nejpozději k začátku migrace) formátu struktury a kvalitě
 - Dodržení termínů migrace s ohledem na celkový projekt (data výkonnostních testů, školení,
 - Dodržení výkonnostních parametrů rychlosti migrace.
- Plánování z pohledu postupu realizace pro splnění podmínek ZD – detailní postup provedení:
 - Analýza struktury a rozsahu dat, úplnosti dokumentace, návrh a odsouhlasení výkonnostních parametrů prostředí provádějících migraci (pouze v případě, že by dodané informace o datech znamenaly nějak výrazněji překročené parametry prostředí tak, jak jsou předpokládány v návrhu architektury, zejména u RDBMS či systému archivů)
 - Plánování postupu (na úrovni jednotlivých datových entit) s ohledem na vazby dat a možnosti a potřeby paralelizace (škálování) importu, tj. v jakém pořadí je možné/nutné data importovat tak, aby byly paralelizovatelné na úrovni ať už datových entit nebo sad záznamů atp. + plánování provedení migrace finálního stavu (zda jsou data natolik malá a čistá, že je možné je importovat po definitivním opuštění starých systémů, nebo zda je potřeba řešit formou např. rozdílového importu, nebo následného do-importu typováním atp.)
 - Analýza vzorku dat – souhlasnost s dokumentací (a to včetně např. povolených či logických intervalů hodnot atp.)
 - Příprava testovacího importu v rámci prototypu.
 - Testování a akceptace importu prototypu.

- Příprava řešení hlavního importu dat (vč. řešení rozdělení dat na archivní a produkční).
- Testování řešení hlavního importu pro detekci tříd chyb (viz detailní třetí úroveň plánu)
- Řešení (plánování v rámci PT) třetí vrstvy plánu migrace – řešení detekovaných neintegrit.
- Implementace doplňkových řešení pro automatizované odstraňování chyb.
- Příprava denního či týdenního harmonogramu (v závislosti na výkonnostních parametrech) pro provedení iniciálního importu včetně provedení iniciálního importu do již finální DB (produkce i archiv).
- Provedení akceptačních testů a vstup řešení do produkce.
- Odstávka původních systémů v detailní koordinaci s přípravou opakované migrace již „definitivních“ dat ať již celkovou, rozdílovou nebo jiným zvoleným způsobem.
- Plánování z pohledu vlastních dat a jejich vad a neintegrit jako jsou duplicity, chybějící reference atp. – postup řešení čistoty dat:
 - Určení tříd chyb v datech
 - Určení rozsahu jednotlivých tříd (= počet dotčených záznamů)
 - Určení řešení jednotlivých tříd (např.: pro malé třídy či pro specifické třídy vyžadující odborný zásah garanta a zhodnocení/rozhodnutí (ne ve smyslu správ. řádu)/dohlední/doplnění informací je vhodné/nutné typování, naopak například pro velké obsahy dat s chybami odstranitelnými snadno algoritmizovatelným způsobem je vhodnější implementace takového algoritmu do modulu provádějícího import dat).
 - Realizace řešení při migraci.

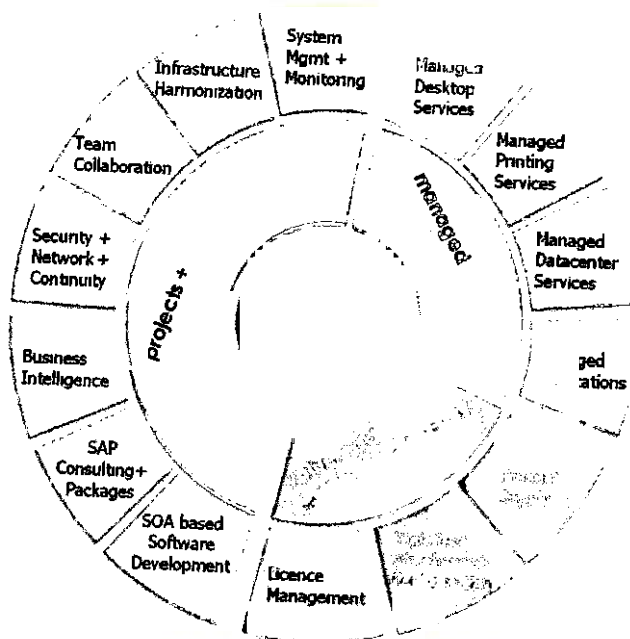
Detailní zakotvení absolutních termínů bude provedeno v rámci analýzy Návrhu realizace tj. bude obsahovat výše uvedené body zakotvené již ke konkrétním kalendářním datům v návaznosti na datum podpisu smlouvy a harmonogram, konkrétní datové entity, pokud to bude možné tak i konkrétní vady atp.

8. Zajištění provozu a podpora řešení

8.1. Zajištění provozu řešení

8.1.1. Přístup S&T CZ k outsourcingu ICT

K outsourcingu nelze v současné době přistoupit jinak než komplexně. Takový přístup ale jednoznačně vyžaduje veliký rozsah kompetencí, kterými je schopna společnost pokrýt veškeré požadavky Zadavatele z vlastních zdrojů, a to jak v oblasti kapacitní, tak především kompetenční. Tímto Zadavateli plně garantujeme, že naše společnost tuto podmínku splňuje a vyhovujeme všem požadavkům kladeným v Zadávací dokumentaci.



Vzhledem k tomu, že uchazeč disponuje certifikovanými a zkušenými odborníky v oblasti ITIL (Information Technology Infrastructure Library – jedná se o soubor konceptů a postupů, které umožňují lépe plánovat, využívat a zkvalitňovat využití informačních technologií a to jak ze strany Uchazeče, tak i z pohledu Zadavatele), bude Uchazeč využívat tato doporučení pro poskytování, evidenci a reporting dodávaných služeb.

Tento rámec souborů a postupů je celosvětově osvědčen a uznáván jako soubor nejlepších doporučení pro řízení a dodávku příslušných služeb, což Zadavateli garantuje maximální možnou efektivitu a záruku velmi kvalitního řízení a plnění požadovaných činností. Dále pak ve svém realizačním týmu disponuje Uchazeč vysoce zkušenými pracovníky s certifikacemi, kteří mají dlouhodobou zkušenost se zavedenými procesy.

8.1.2. Široké kompetence společnosti S&T

Službou Outsourcing obecně přebíráme částečnou nebo úplnou odpovědnost za definované oblasti IT/IS. Poskytování outsourcingu probíhá tak, že na jedné straně procesu stojí zákazník se svými požadavky, a na druhé straně je dodavatel služeb, který tyto zákaznické potřeby uspokojuje. Dodavatel těchto služeb může být interní nebo externí.

Outsourcing IT/IS nepovažujeme za monolitickou dodávku jednoho systému, naopak ho vidíme jako stavebnici složenou z několika komponent, a záleží jen na budoucím uživateli outsourcingu, kterou část svého IS vyčlení vně své organizace a nahradí ji přiměřenou komponentou této stavebnice.

Firmy specializující se na daný obor mají zpravidla mnohem lépe proškolené pracovní síly, které se v dané problematice orientují. Odpovědnost za problematiku nese jiný subjekt a výchozí firma se může plně věnovat svému hlavnímu oboru. Náklady na zajištění specializované činnosti jsou při využití outsourcingu zpravidla výrazně nižší. Zajišťování služeb pomocí outsourcingu je celosvětově se zvyšujícím trendem.

V oblasti outsourcingu infrastruktury a standardních aplikací se zaměřujeme na společnosti středně velké a velké ze všech segmentů trhu v ČR. V oblasti aplikačního a procesního outsourcingu jsme díky našim referencím schopni poskytnout vysokou kvalitu outsourcingových služeb pro společnosti ze segmentů financí, telekomunikací, výroby, stavebnictví a státní správy.

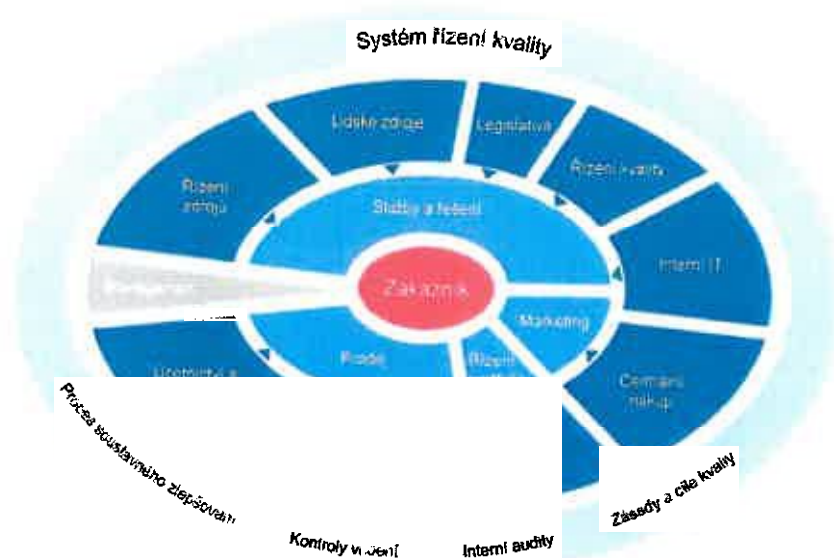
V IT existuje nepřeberné množství technologií, systémů a aplikací. Jako jeden z velkých integrátorů v České republice vlastníme na většinu z těch klíčových vlastní školené specialisty a v ostatních případech doplňujeme naše řady o externí spolupracovníky a využíváme subdodávek našich dlouhodobých partnerů. Díky takovému přístupu zajistíme vždy kvalitní podporu všech technologií klientů.

Naše společnost mimo certifikace ISO 9001 získala také významnou certifikaci ISO 20000 se zaměřením specificky na outsourcing IT/IS a certifikaci ISO 27000 se zaměřením na informační bezpečnost.

V oblasti podnikových systémů jsou našimi partnery SAP, INFOR, COGNOS a LCS. V oblasti technické infrastruktury také spolupracujeme se špičkovými dodavateli a jsme držiteli nejvyšších certifikací – našimi partnery jsou společnosti HP, IBM, Fujitsu, DELL, Microsoft, CheckPoint, EMC, VMware a další.

Bezpečnostní řešení, poskytovaná našim klientům, jsou založena na nejnovějších technologiích společností CISCO, CITRIX, McAfee, Symantec, ISS, BlueCoat a dalších. Mezi naše osvědčené partnery z oblasti sítí patří například společnosti CISCO, Allied Telesyn, HP, 3COM a RIT.

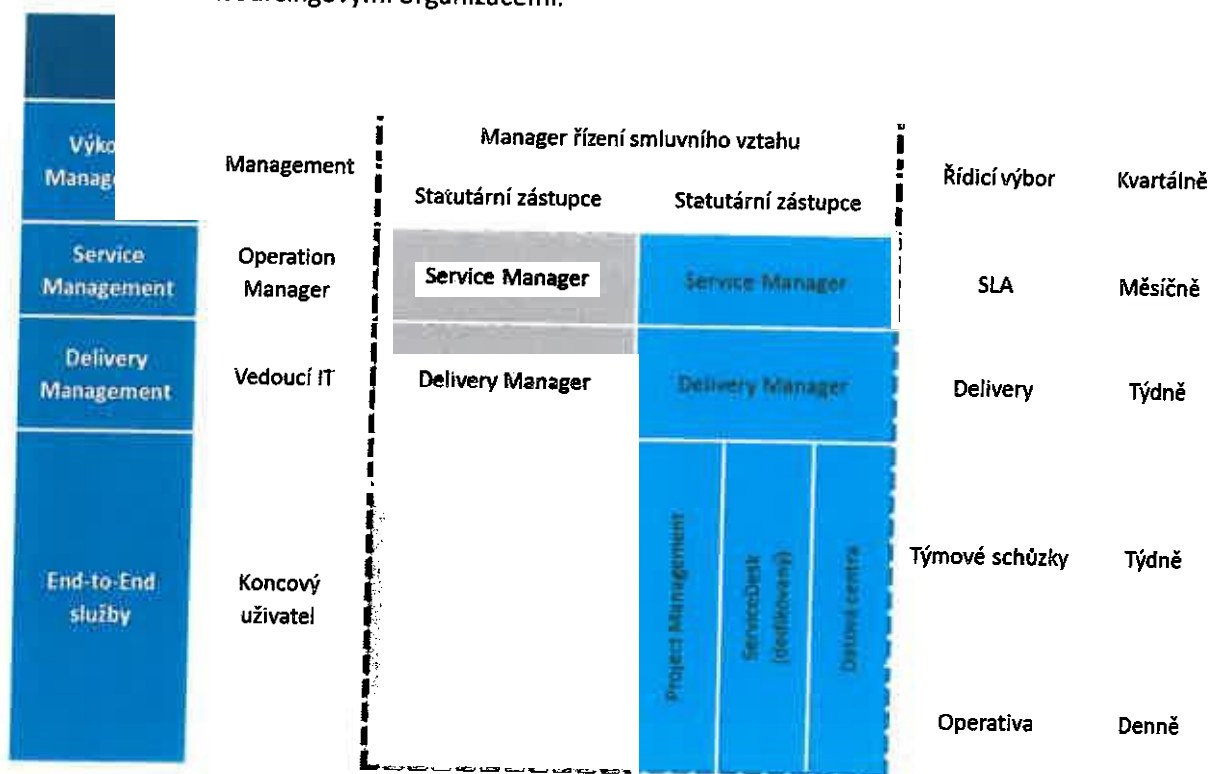
V oblasti servisu, podpory a služeb naše aktivity zahrnují například péči o produkty společností IBM, HP, NetApp, Dell, Fujitsu Siemens Computers, Xerox, Acer, Lexmark, Olivetti a dalších.



Systém řízení kvality podle S&T

8.1.3. Model projektového a procesního řízení

Uchazeč k efektivnímu řízení smluvního vztahu, resp. k efektivnímu řízení dodávky outsourcingových služeb přistupuje na základě níže popsaného modelu, který je založen na dlouholetém vývoji, vzhledem k jeho efektivitě a upravován na základě aktuálních zkušeností a hodnocení našich zákazníků. Tento model je používán mnoha outsourcingovými organizacemi.



Používaná architektura řízení umožňuje včasnou identifikaci potenciálního výskytu problému a jeho řešení od nejnižší úrovně řízení až po jeho eskalaci na nejvyšší možnou

úroveň. Tento proces bude detailně popsán v Provozní dokumentaci vznikající v rámci fáze tranzice.

Řízení vztahu se zákazníkem – v terminologii Uchazeče "Governance model", tvoří formální řídicí rámec a strukturu, které vychází ze standardních procesů a osvědčených zkušeností Uchazeče. Governance model umožní oběma stranám efektivní vzájemné řízení vztahu, očekávání, smluvních závislostí a služeb.

Procesy Governance jsou dobře dokumentované, opakovatelné a flexibilní. Úspěšná implementace Governance je úzce závislá na návrhu optimálního modelu, který umožní splnit požadavky obou stran a zajistí proaktivní a oboustranně výhodný partnerský vztah mezi oběma organizacemi.

Na základě zkušeností Uchazeče s obdobnými komplexními vztahy řešícími poskytování dlouhodobých outsourcingových služeb srovnatelného objemu a vzhledem ke stávajícímu organizačnímu zajištění služeb v prostředí Zadavatele navrhujeme ustanovit následující:

Výkonný Management (frekvence schůzek 1–2x ročně)

- Strategické řízení vztahu
- Dlouhodobé plánování aktivit, zpravidla na roční období

Řídicí výbor (frekvence schůzek kvartálně)

- Taktické řízení vztahu
Střednědobé plánování aktivit, zpravidla na kvartální období
Vyžadována přítomnost tzv. Sponzora projektu ze strany Zadavatele

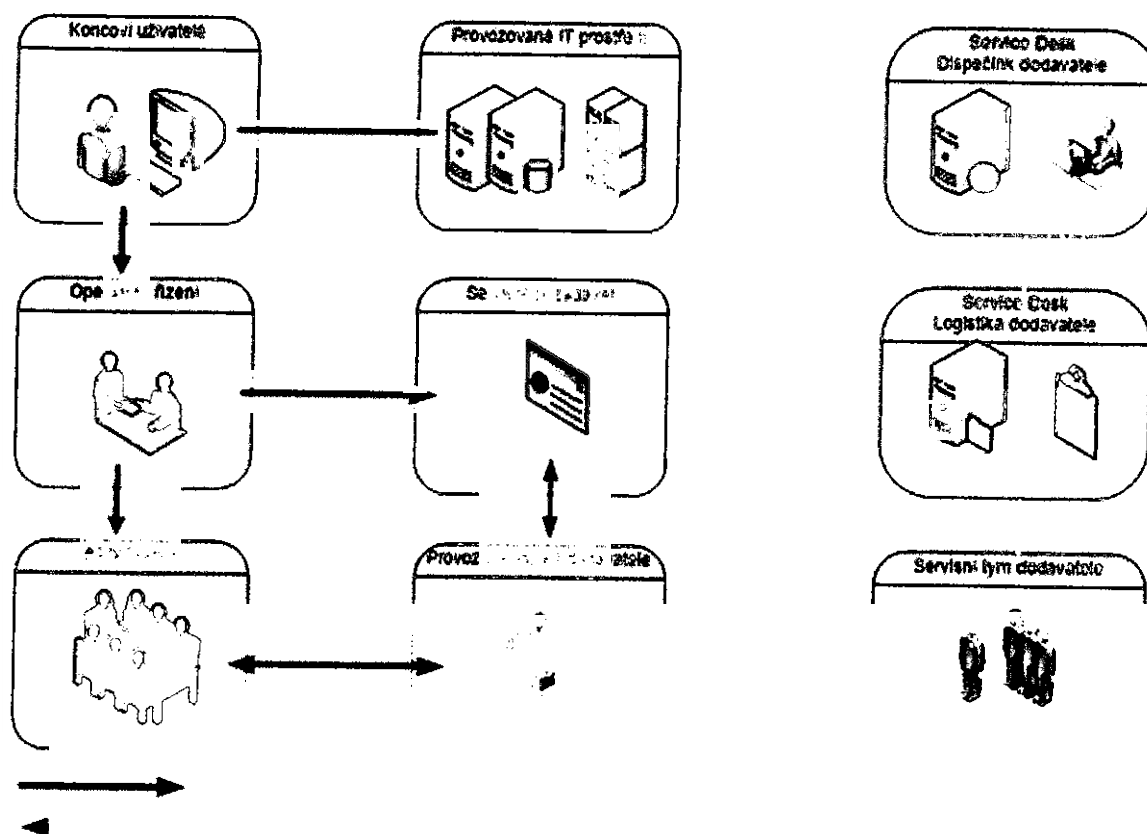
Hlavní tým projektu (frekvence schůzek měsíčně)

- Operativní řízení vztahu
Krátkodobé plánování aktivit, zpravidla na měsíční bázi
Průběžné hodnocení dodávky dohodnutých služeb dle SLA

Dále pak garantujeme na vyžádání Zadavatele účast odpovědného zástupce Uchazeče na tzv. Pracovních skupinách, které jsou v současné době pořádány Zadavatelem na týdenní (příp. 14 denní) bázi a řeší zcela operativní záležitosti, které se týkají běžného provozu všech provozovaných služeb napříč celým Ministerstvem zemědělství. Z těchto schůzek jsou eskalovány problémy na vyšší úroveň řízení, jako jsou výše zmíněný Hlavní tým projektu, případně Řídicí výbor projektu.

Uchazeč garantuje objednateli součinnost a komunikaci v rámci osobních jednání na kontrolních dnech, operativních ad-hoc schůzkách na vyžádání a v průběhu poskytování činností v rámci provádění služeb, což objednateli zajistí v maximální možné míře průběžné zvyšování efektivity řízení poskytovaných služeb.

Uchazeč se zavazuje předložit objednateli jedenkrát ročně celkovou výroční zprávu obsahující přehled poskytnutých služeb, ve které přehledným způsobem popíše realizované činnosti v uplynulém období dle jednotlivých klíčových oblastí, shrnutí měsíčních vyhodnocení SLA parametrů, doporučí objednateli případné oblasti služeb vhodné pro zlepšení a poskytne objednateli celkovou zpětnou vazbu vycházející ze zkušeností provozu služeb za uplynulé období.

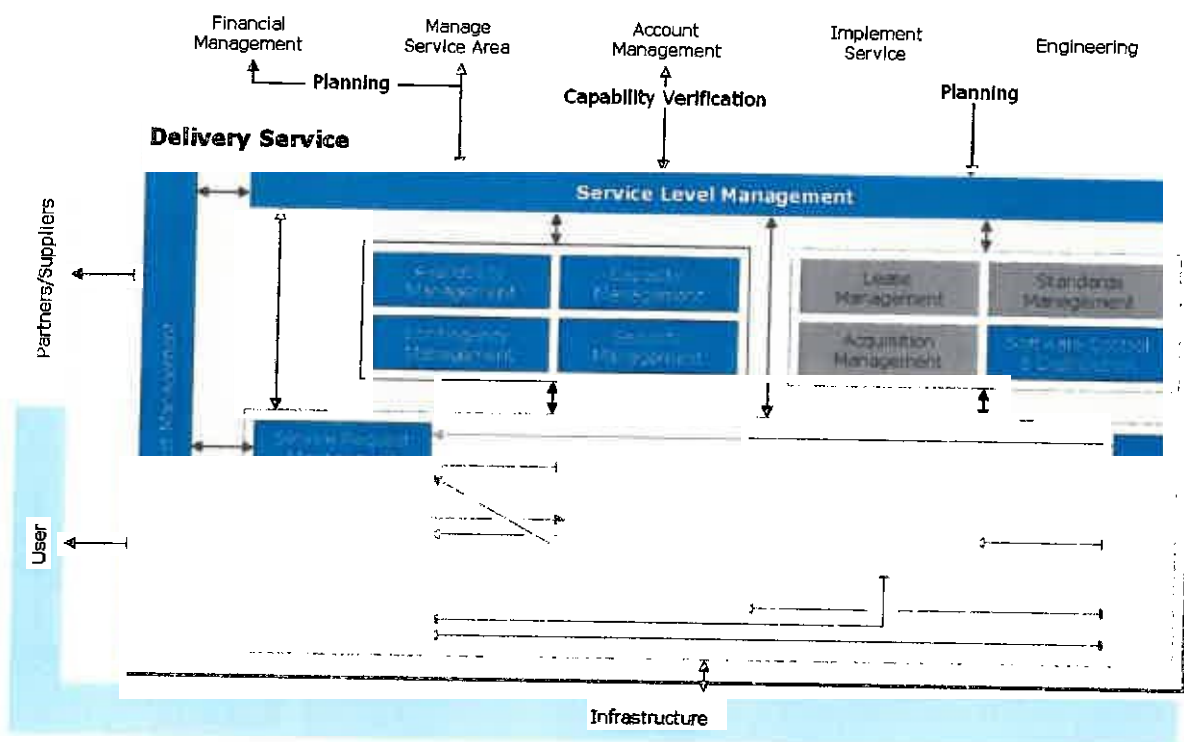


Blokový obrázek modelu dodávky služeb

8.1.4. Procesy a pracovní postupy

Naše společnost se již od svého založení zaměřovala především na oblast poskytování služeb IT. Díky této striktní orientaci jsme se již od roku 2005 začali intenzivně věnovat školením a procesním změnám směrem k rámci ITIL. Procesní rámec ITIL byl víceméně jako jeden celek využit k vytvoření evropské normy známou pod značkou ISO 20000. Protože naše procesy a postupy již splňovaly náročná kritéria procesního rámce ITIL, požádali jsme jako druhá společnost na českém trhu o certifikaci dle této ISO normy a v roce 2006 jsme obdrželi akreditaci ISO 20000 na služby, mezi kterými je mimo jiné také poskytování outsourcingu IT.

Náš přístup k procesnímu řízení je standardizován a podrobně popsán v dokumentaci ISO 20000. Tak, jak je popsáno v zadání, nebudeme se v následujících kapitolách dopodrobna věnovat procesním modelům řízení jednotlivých disciplín IT služeb, ale zdůrazníme náš přístup a vyzdvihneme výhody a vylepšení, která jsme za dobu poskytování služeb outsourcingu dosáhli. Z těchto bohatých zkušeností budou čerpat členové našeho týmu a garantujeme tímto Zadavateli poskytování všech požadovaných služeb v souladu se Zadávací dokumentací.



Vrcholový pohled na procesy ISO 20000 certifikované v S&T

8.1.5. Incident management

Účel procesu:

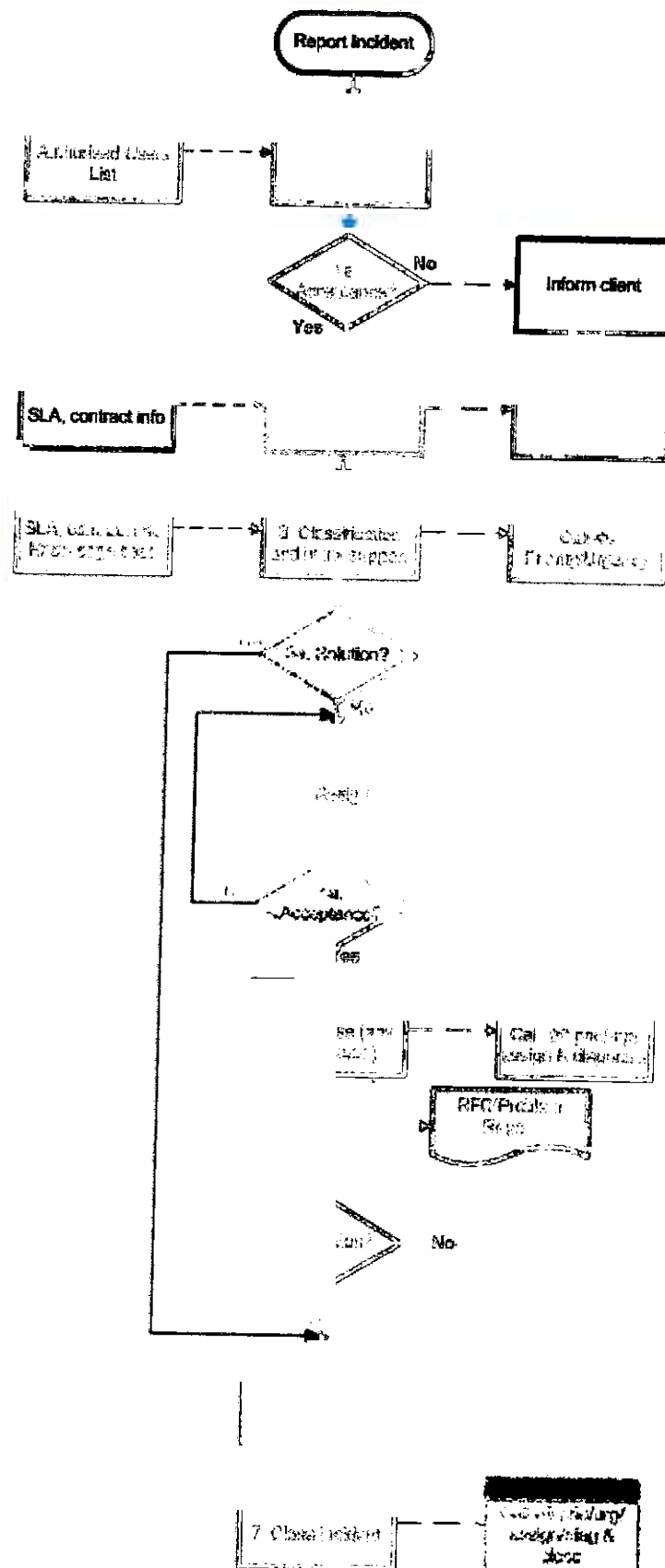
Maximálně rychle obnovit službu s ohledem na smluvní termíny, s minimálním dopadem na uživatele a za co nejnižších nákladů. Incident je specifický typ události nebo uživatelského hlášení, obvykle spojeného s výpadkem služby nebo se snížením její kvality. Správa incidentů tvoří další větev podpory uživatelů. Vstupy od uživatelů nebo dohledované IT infrastruktury jsou buď vyřešeny přímo pracovníky Service Desku, a nebo předány specialistům druhé a třetí úrovně podpory, případně předány externím řešitelům.

Uchazeč zastává přístup, že Incident Management přináší kvalitu, efektivitu a tedy i cenovou konkurenceschopnost způsobem maximální standardizace. S&T má tisíce incidentů měsíčně od stovek klientů. Tato čísla se rychle zvyšují a naše procesy se stále musí zlepšovat. Naši manažeři kvality a manažeři jednotlivých disciplín mají za cíl dále zlepšovat vlastní IMS systém a procesy na něj navázané.

Incident Management máme standardně rozdělen do tří úrovní dle doporučení ITIL a to 1st level – ServiceDesk; 2nd level – On-Site/Off-Site specialista; 3rd line – eskalace na vendora a podporu třetích stran.

Závěr:

Vzhledem k tomu, že schválený proces incident managementu v prostředí Zadavatele je plně v souladu s doporučeními ITIL, které má uchazeč jako svůj firemní standard a na který je certifikován, garantujeme Zadavateli, že budeme plně integrováni na tento proces a budeme postupovat plně v souladu s uvedeným diagramem:



8.1.6. Change management

Účel procesu:

Obhospodařovat změny v infrastruktuře IT s ohledem na neustále se měnící obchodní potřeby a očekávání uživatelů, aby se minimalizoval negativní dopad na existující služby IT. Změnová řízení jsou kvůli rostoucím požadavkům na efektivitu provozu IT a důrazu na vysokou dostupnost služeb stále důležitější. Proces Správa změn vzájemně spojuje a propojuje procesy inicializace, sběr informací, vyhodnocování, plánování, řízení, implementace a testování změn v IT infrastruktuře. Je prakticky nemožné ve složitějším prostředí provádět jakékoliv změny, pokud daný pracovník nemá například dostatečné informace o tom, jaké technické vybavení, kdy a kde a jakým způsobem má vyměnit či nainstalovat.

Změnová řízení jsou v případě naší společnosti více "customizovaná" proti vysoce standardizovanému procesu Incident Managementu. Důvodem je, že zde klademe více důraz na rychle se vyvíjející obchodní cíle klientů, které se většinou diametrálně liší ve všech parametrech. I zde existují ale výjimky, kdy například u vysoce centralizovaných a manažersky globalizovaných mezinárodních společností náš model standardního řízení změn byl použit v plném měřítku.

Podstatnou výhodou naší implementace této disciplíny je flexibilita, kterou našim klientům nabízíme za využití standardních a vyzkoušených postupů na obrově širokém vzorku našich outsourcingových klientů.

Závěr:

Vzhledem k tomu, že schválený proces change managementu v prostředí Zadavatele je plně v souladu s doporučeními ITIL, které má uchazeč jako svůj firemní standard a na který je certifikován, garantujeme Zadavateli, že budeme plně integrováni na tento proces a budeme postupovat plně v souladu s uvedeným diagramem:

8.1.7. Service level management

Účel procesu:

Připravit, poskytovat a vyhodnocovat úrovně dodávaných služeb, které jsou zakotveny písemnými smluvními vztahy.

Klíčovým nástrojem pro správu, řízení, evidenci, kontrolu, reporting a zajištění požadované úrovně poskytovaných služeb je tzv. Service Level Management, jehož hlavním účelem je připravit, poskytovat a vyhodnocovat úrovně dodávaných služeb, které jsou zakotveny ve Smlouvě.

Uchazeč dlouhodobě praktikuje a důsledně dodržuje propracované praktiky ServiceLevel Managementu ve všech poskytovaných a provozovaných službách, což přináší Zadavateli následující hlavní výhody:

Lepší vyváženost přínosů ICT proti nákladům,

Zvýšení výkonnosti i prestiže ICT a zlepšení služeb, které poskytuje,

Zásadní zkrácení doby pro obnovu služeb při jejich výpadku.

Pro maximálně efektivní evidenci služeb využívá Poskytovatel Katalog služeb, který obsahuje jednotlivé katalogové listy s jejich příslušnými atributy pro měření a definici úrovně služeb. Níže uvádíme základní atributy služeb, které běžně v jiných projektech

Uchazeč eviduje a využívá je při reportingu:

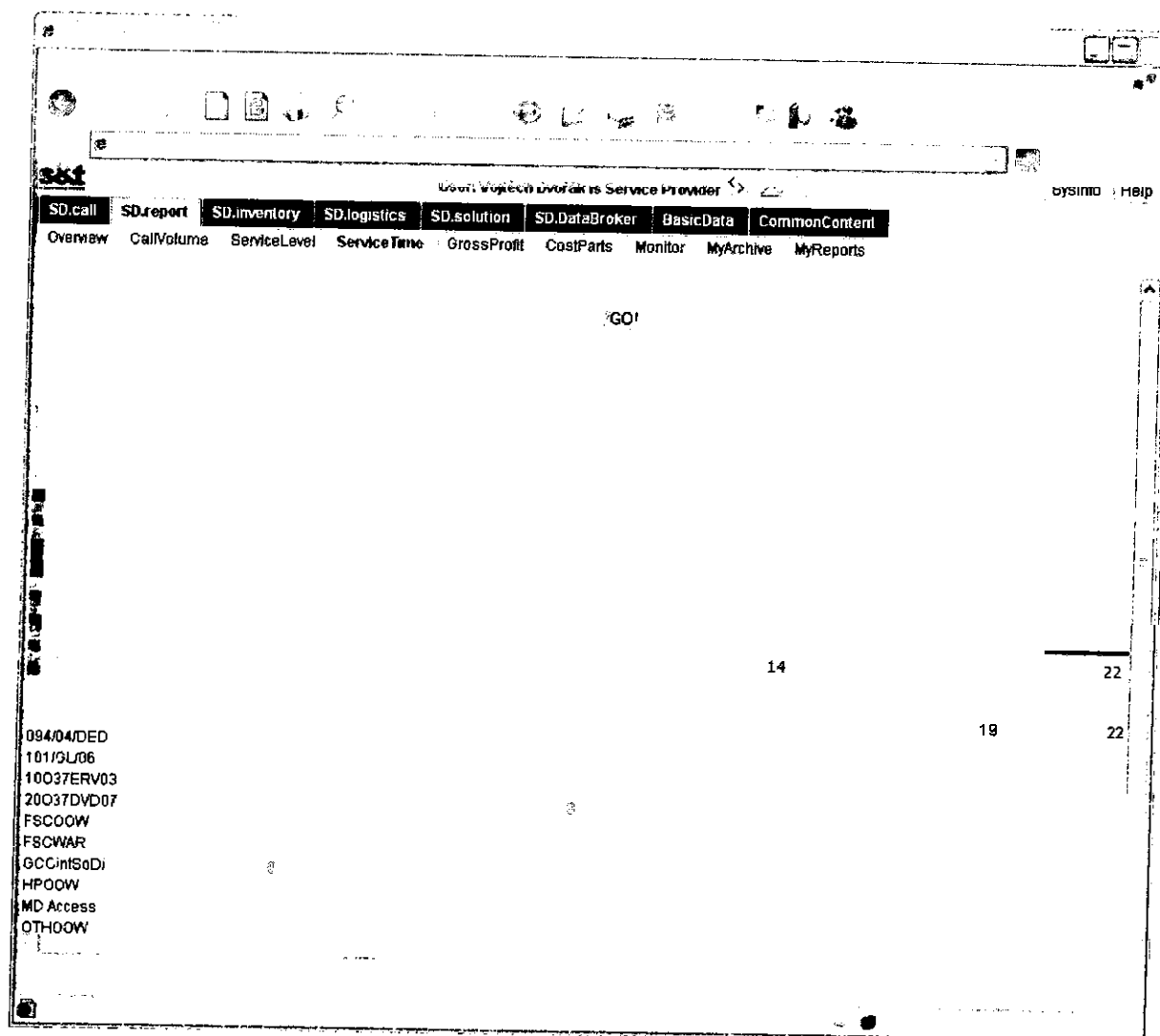
- Jméno služby/Service Name
- Popis služby/Service description
 - Typ služby/Service type
 - Kterých odborných útvarů se služba týká/Business Unit(s)
 - Manažeři služby/Service Manager(s)
 - Dopad na odborné útvary a jejich agendy/Business Impact
 - Priorita agendy (procesu)/Business priority
 - Provozní doba služby/Service hours
 - Kontakty na zástupce odborných útvarů/Business contacts
 - Eskalační kontakty/Escalation Contacts
 - Reporty o službě/Service Reports
- Revize služby/Service Reviews
- Bezpečnostní kategorie/Security Rating
- Garantovaná úroveň služby (SLA)/Service Level Agreement)

Service Level Management je zastřešen metodicky a personálně Service manažery, kteří nejsou jmenováni jen na straně Uchazeče, ale také na straně našich klientů. Naši Service manažeři jsou certifikováni ITIL profesionálové, kteří se řídí doporučeními ITIL a interními směrnicemi ISO 20000 naší společnosti.

Dedikovaný Service manažer má za úkol kontinuálně měřit, řídit, vyhodnocovat a především zlepšovat průběžně poskytované služby. Dále pak zastřešuje další definované role pro poskytování služeb definovaných Zadavatelem v Zadávací dokumentaci.

Jako jedno z našich vylepšení postupů můžeme uvést například standardizovaný proces SIP [Service Improvement Program], který metodicky zvyšuje kvalitu služeb tam, kde není dostatečná.

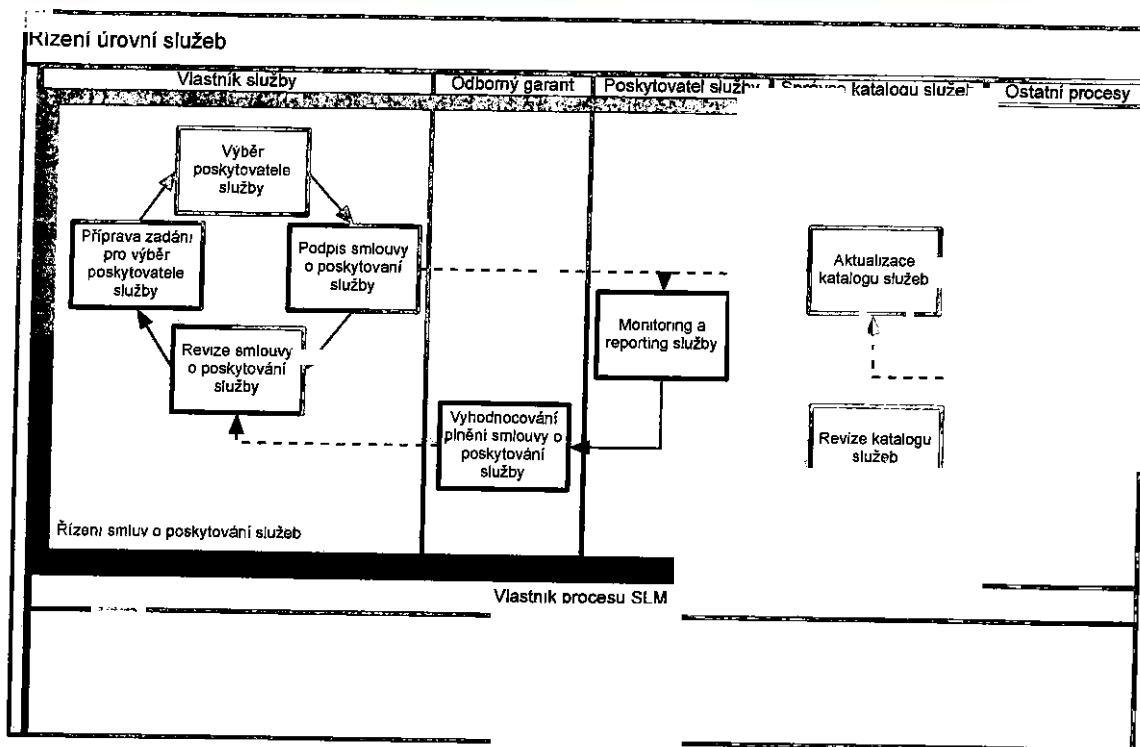
Díky moderním technologiím a informačním systémům mají naši Service manažeři okamžitý přístup k vyhodnocování všech KPI [Key Performance Indikátory], které jsou uvedeny v jednotlivých SLA [Service Level Agreement] nebo Katalogu služeb.



Průhled online reportu dostupného pro všechny Service Manažery

Závěr:

Vzhledem k tomu, že schválený proces service level managementu v prostředí Zadavatele je plně v souladu s doporučeními ITIL, které má uchazeč jako svůj firemní standard a na který je certifikován, garantujeme Zadavateli, že budeme plně integrováni na tento proces a budeme postupovat plně v souladu s uvedeným diagramem:



8.1.8. Service manažer

Service Manažer (dále jen SM) je jmenovaný Uchazečem za účelem zajištění standardní úrovně poskytovaných služeb, zvyšováním spokojenosti Zákazníka a pro koordinaci a řízení všech aspektů se službou související. Mezi hlavní povinnosti patří pravidelné governance meetingy se zástupci Zadavatele, interním personálem dodavatele, dále pak řešení všech nestandardních situací (projekty, změny služeb, procesů) včetně průběžné dokumentace a pravidelného vyhodnocování. SM má přiděleny od dodavatele vysoké pravomoci, které mu umožňují ve většině běžných případů rozhodovat rychle a efektivně, bez nutnosti eskalace a tvorby interních žádostí o změny.

Vysoká úroveň kvalifikace a zkušenosti SM jsou zárukou zajištění kontinuity a dlouhodobé kvality služeb poskytovaných dodavatelem. Všichni SM jsou certifikováni dle ITIL (standard na řízení IT používaný dodavatelem) s minimální 5letou praxí v řízení dodávek outsourcingu, správy systémů nebo projektového managementu v IT oboru.

Při startu nebo přebírání poskytování nové služby je role SM definována takto:

- Představit manažera služeb – jediný kontakt v S&T pro IT/SM manažera Zadavatele
- Seznámit se s korporátními normami IT Zadavatele a s jeho postupy spojenými s IT a požadavky
Nastavení podpory a eskalačních cest
- Připravit, optimalizovat a implementovat postupy pro poskytování služby
- Seznámit odpovědné zaměstnance S&T s výše uvedenými informacemi
- Zajistit funkčnost náběhu příslušných postupů
- Připravit strukturu pravidelného reportování, dokumentace, eskalace

- Vytvoření datového prostoru na intranetu a vložení dat (smlouva, zápisy, reporty atd.)
- Zajistit shodu s procesními a metodickými pokyny S&T a Zadavatele

Pravidelné governance aktivity vykonávané SM:

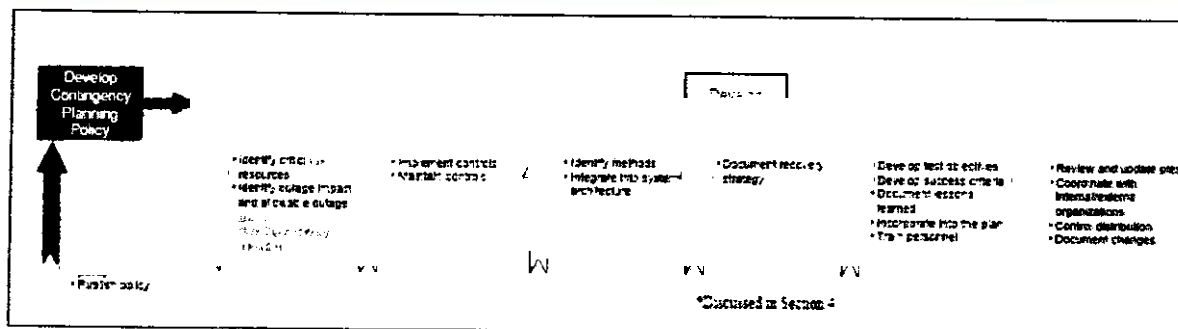
Popis				
Provozní schůzky (analogue Pracovní skupiny v prostředí MZe)	1x 14dní	• Řízení incidentů • Změnová řízení • Bezpečnostní incidenty • Průběžná kontrola služby • Doporučení na zlepšení • Krátkodobé plánování služby • Kontrola plnění KPI parametrů	• Ad-Hoc reporty • Konzultace s vlastníky služeb • Interní vyhodnocení s pracovníky dodavatele • Výstupy z procesů změn, releasů a problémů • Minulý zápis s úkolovníkem	• Zápis z jednání • Rozdělovník úkolů • Stav úkolů • Distribuce zápisu dle rozdělovníku • Návrh eskalace na SLM • Žádosti o změny
Jednání komise (analogue Hlavního projektu v prostředí Mze)	měsíčně	• Vyhodnocení KPI/SLA • Revize změnových požadavků • Schválení změn • Finanční sumarizace/faktura	• Měsíční reporty • Zápisy z provozních schůzek • Finanční podklady • Seznam úkolů • Eskalace na SLM komisi • Změnové žádosti	• Zápis z jednání • Rozdělovník úkolů • Stav úkolů • Distribuce zápisu dle rozdělovníku • Vyřešení eskalace z provozu • Návrh eskalace na IT komisi • Žádosti o změny
Jednání komise	ročně	• Vyhodnocení dlouhodobých cílů • Finanční management • Revize smluvních podmínek • Aktualizace dlouhodobého plánu • Stanovení cílů na další rok	• Roční souhrnné reporty • Audit report (je-li) • Eskalace na IT komisi • Cíle na předchozí rok • Finanční podklady	• Zápis z jednání • Rozdělovník úkolů • Stav úkolů • Distribuce zápisu dle rozdělovníku • Vyřešení eskalace ze SLM • Cíle na další rok • Návrhy na zlepšení a inovace

Governance aktivity lze realizovat dle dohody mezi Uchazečem a Zadavatelem na místě, telefonicky a nebo videokonferencí, dle požadavku a aktuální potřeby. Pravidelnost a dodržování termínů je primární odpovědností SM a pouze na žádost Zákazníka lze pravidelné termíny rušit nebo přesunovat.

8.1.9. Service Continuity Management

Kontinuita poskytovaných služeb a podnikání našich klientů je jedním z cílů naší společnosti. Řešení Disaster Recovery současně nabízíme našim klientům jako součást našeho standardního produktového portfolia. Interní systémy a podpůrné procesy (CallCentrum, Informační systémy, datová konektivita) jsou zajištěny i pro případy havárie. Máme vypracovány havarijní plány pro jednotlivé disciplíny dle ISO 20000.

Kontinuitu námi poskytování služeb, tedy z pohledu klienta i kontinuitu jeho podnikání, chápeme jako neustále se vyvíjející se proces.



Business Continuity / DR metodologie dle NIST 800.34

Tento obecný proces je shodný pro jakoukoli organizaci či podnik a liší se až v technické realizaci.

8.1.10. Bezpečnost a důvěrnost informací

Bezpečnost a důvěrnost informací je klíčovou devizou naší společnosti. Bez garance vysoké úrovně bezpečnosti bychom nemohli splňovat vysoké nároky, které na nás kladou naši současní zákazníci.

Naši zaměstnanci, přicházející do styku s důvěrnými i utajovanými informacemi, a proto někteří z nich prošli bezpečnostními prověrkami a byli náležitě proškoleni. Organizace jako celek disponuje zaměstnanci certifikovanými NBÚ od úrovně D (důvěrný) až po T (tajný).

Zaměstnanci používají šifrované připojení k internetu, zabezpečené počítače a šifrují data na nosičích. Přístup k datům je obvykle řešen "pohledy" do databáze a bezpečnostními politikami v rámci stromové struktury dat. Zaměstnanec nemá přístup k datům, která bezprostředně nepotřebuje k řešení svého úkolu v rámci týmu.

Na úrovni jednotlivých prvků architektury systému je bezpečnost zajištěna následovně:

- Bezpečnost dat je zajištěna robustními prostředky SQL datového enginu
- Bezpečnost komunikace klient – server je zajištěná na úrovni variantního kódování tohoto protokolu
- Bezpečnost na úrovni logiky aplikace je zajištěná robustním, nastavitelným auditem jednotlivých procesů na straně jedné a systémem nastavování skupinových a uživatelských profilů na straně druhé

Přesné definice rozsahu, hloubce, technikách a penalizací jsou ukotveny ve vzájemné smlouvě o utajovaných skutečnostech, která je obvykle připravována a podepsána na úvod procesu Due Diligence.

8.1.11. CSI – Index spokojenosti Zákazníka

Pro vyhodnocování služeb předpokládáme použití intranetového dotazníku, který bude připravovat MZe. Níže uvádíme naše standardní procesy a postupy.

Mezi standardní reporty patří výstupy z pravidelných průzkumů spokojenosti uživatelů Zákazníka. Reporty vznikají z odpovědí na dotazníky, které jsou zasílány pravidelně elektronicky emailem, obvykle jednou za půl roku, na uživatele, kteří využili službu – tedy pouze těm, kteří mohou na zaslaný průzkum spokojenosti kvalifikovaně odpovědět.

Počet a znění dotazů které se uživatelům pokládají, jsou definovány na začátku poskytování služby. Aby bylo možné srovnávat výsledky jednotlivých průzkumů v průběhu let poskytování služby, je třeba, aby znění dotazů zůstalo po celou dobu služby ideálně nezměněno. Hodnocení obvykle probíhá na tzv. školní stupnici, kde 1 znamená nejlepší a 5 nejhorší. CSI, tedy index spokojenosti Zákazníka je spočten jako absolutní průměr hodnocení všech účastníků a všech položených dotazů. Tento index jako jedna hodnota je součástí DashBoardu, jenž je určen pro Manažerský přehled. Detailní výsledky hodnocení a výsledky po jednotlivých odpovědích jsou k dispozici Service Manažerům obou smluvních stran.

Vážený IT uživateli,

V rámci zlepšení kvality poskytovaných IT služeb plánujeme převést službu IT HelpDesk na externího dodavatele (společnost S&T CZ, s.r.o.). Naším cílem je zvýšit dostupnost služeb, které Vám IT poskytuje, snížit dobu pokrytí a zejména snížit reakční dobu řešení Vámi nahlášených IT problémů a tím minimalizovat případné finanční ztráty.

Ti z vás, kteří již od pondělního poledne hlásili IT incident, jistě zaznamenali změnu. Společnost S&T CZ, s.r.o. disponuje profesionálním call centrem a pro Vaši podporu dedikovala několik pracovníků, kteří jsou schopni pokrýt více hovorů paralelně.

Rádi bychom pravidelně hodnotili Vaši spokojenost s poskytovanými IT službami a za tímto účelem si Vám dovoluujeme poslat následující link

Webový formulář průzkumu Vaší spokojenosti s IT službami je umístěn ZDE.

Na této adrese je třeba odpovědět na uvedené dotazy a ohodnotit jak vnímáte stávající kvalitu poskytovaných IT služeb. Tento průzkum plánujeme opakovat pravidelně jednou za půl roku, aby vedení společnosti získalo náhled zdali tato změna je správná.

Předem děkujeme za Vaši reakci, po uzavření průzkumu dojde ke sklosování všech odpovědí a pět vylosovaných uživatelů bude odměněno zajímavou věcnou cenou od společnosti S&T CZ

Děkují,

Patička s logem a podpisem

Příklad zaslaného emailu na uživatele průzkumu

Příklad dotazů pokládaných v jednom ze současných průzkumů. Dotazy by měli být jednoznačné krátké a srozumitelné.

- Jak jste celkově spokojeni s poskytováním IT služeb?
- V případě, že kontaktujete vaši IT podporu, je vždy někdo, kdo by se vám věnoval?
- Jste spokojeni s kvalitou komunikace ze strany vaší IT podpory?
-

OMV - průzkum spokojenosti

Dotazník spokojenosti prokrm vyplňuje jako vy křídle.
1 = výborně, 5 = naderazetně

1. Jak jste celkově spokojeni s poskytováním IT služeb?

1 2 3 4 5

2. V případě, že kontaktujete vaši IT podporu, je vždy někdo, kdo by se vám věnoval?

1 2 3 4

3. Jste spokojeni s kvalitou komunikace ze strany vaší IT podpory?

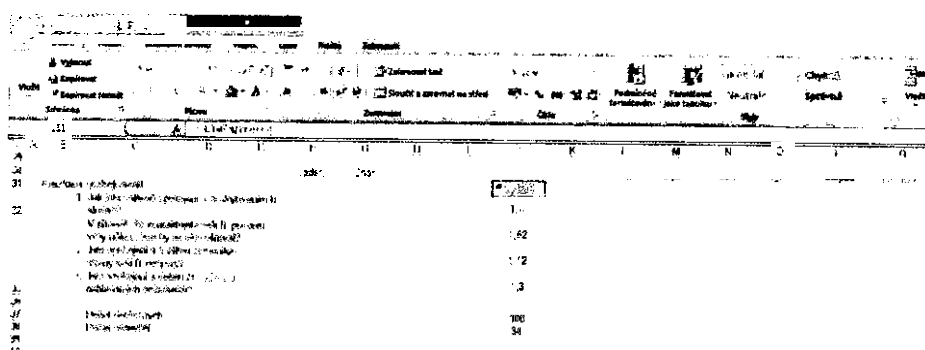
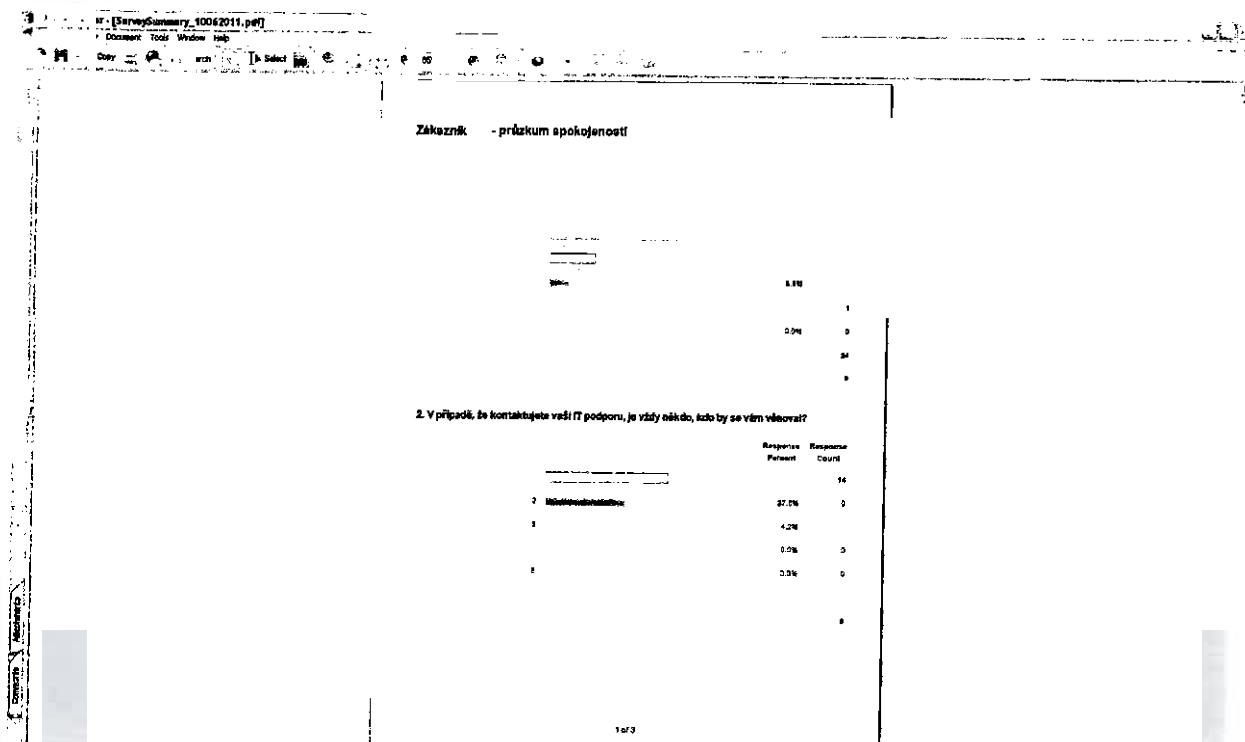
1 2 3 4 5

4. Jste spokojeni s dobou řešení vami nahlášených požadavků?

1 2 3 4 5

5. Máte momentálně nějaké IT problémy, které nejsou vyřešeny?

Webový formulář průzkumu spokojenosti



CSI uvedený v DashBoardu

8.1.12. Správa problémů

Účel procesu: identifikovat a řešit chyby v infrastruktuře IT, aby se zabránilo opakovanému výskytu incidentů vztahených k těmto chybám. Tento proces je velmi často též nazýván správou kvality (Quality Management), protože je zaměřen na analýzu velkých, opakujících se nebo podobných incidentů. Výsledkem analýzy je pak nalezení a definice systémové příčiny tzv. známé chyby (Known Error). Proces Správa problému má jak reaktivní, tak i proaktivní aspekty. Reaktivní činnosti se soustřeďují na řešení problémů vyvolaných incidenty, proaktivní činnosti se zaměřují na identifikaci a řešení problémů a známých chyb ještě předtím, než se stanou incidenty. Zatímco účelem procesu Správa incidentů je obnovit službu jak nejrychleji je to možné, proces

Správa problémů se zaměřuje na důkladnou analýzu klíčové příčiny selhání, a podporuje tak maximální stabilitu poskytovaných služeb IT.

8.1.13. Správa konfigurace

Účel procesu: zabezpečit centrální správu IT infrastruktury tak, aby se podpořila dodávka kvalitních a efektivních služeb IT. Správa konfigurace je proces, který zajišťuje identifikaci, řízení, vykazování stavu a kontrolu nad infrastrukturou IT a všemi aktivy IT v organizaci v průběhu jejich životního cyklu. Kromě podpory dalších procesů, jako je Správa problémů a Správa změn, zajišťuje také snadný přístup k informacím, jako jsou smlouvy o poskytování služeb, vazby/závislosti mezi konfiguračními položkami a organizačními informacemi. U procesu Správa změn zabezpečuje proces Správa konfigurace pracovníkům zodpovědným za změny, aby byli aktuálně informováni o jednotlivých zařízeních, uživateli a službách. V důsledku toho mohou provádět odpovídající analýzu rizik a dopadů. Tato integrace zároveň zaručuje aktuální stav konfigurační databáze. Účinné řízení konfigurace zajišťuje nejlepší využití, rozmístění a využívání všech IT aktiv.

8.1.14. Řízení projektů

Pomocí projektových manažerů pomáháme u našich zákazníků zavést nebo zdokonalit projektovou kulturu, aby pomocí efektivních a kontrolovatelných procesů a metod řídili své projekty v daném čase, v rámci rozpočtu a v požadované kvalitě. Dále pak pomáháme projekty kvalifikovaně a maximálně efektivně řídit plně v souladu s principy metodiky IPMA.

8.1.15. Provozní deník

Uchazeč bude vést Provozní deník a zaznamenávat do něj minimálně následující skutečnosti:

Výskyt havarijních stavů;

Výskyt anomálií a nestandardních stavů systémů, které mají dopad na plnění SLA;

Zprovoznění nového nebo dočasně odstaveného systému a odstavení systému;
Spuštění, vypnutí a restart systému.

Uchazeč garantuje, že provozní deník bude obsahovat minimálně následující informace:

Datum a čas pořízení záznamu;

Identifikace osoby pořizující záznam;

V případě událostí trvajících více než 1 hodinu také čas začátku a konce události;

- Popis události.

8.1.16. Integrace interních procesů hlášení incidentů, přijímání změnových požadavků na stávající procesy a systémy zadavatele

Interní procesy hlášení požadavků, přijímání změnových požadavků vycházejí z procesů požadovaných zadavatelem v zadávací dokumentaci. Interní procesy uchazeče budou

flexibilně přizpůsobeny potřebám MPSV a budou plně reflektovat i požadavky na případné úpravy procesů.

Poskytované služby zajištění předmětu VZ jsou řízeny procesními standardy postavené na sadě doporučení ITIL v3. Interní procesy Zadavatele pro hlášení incidentů, změnových požadavků případně problémů budou jedna ku jedné navázány na procesy Uchazeče, který provozuje plnohodnotné service deskové SW řešení. V inicializační části projektu počítáme s provedením integrace mezi SW nástroji Zadavatele a Uchazeče tak aby byli jednotlivé procesy provázány.

Tímto postupem zajistíme vedení evidence o probíhajících řešení jednotlivých požadavků nebo skupin požadavků v service desku Zadavatele v dostatečné úrovni informací tak aby bylo možno provádět měření a vyhodnocování podpory jednotlivých služeb a řešení jednotlivých požadavků.

8.1.17. Komunikační kanály a jejich integrace s komunikačními kanály zadavatele

Komunikační kanály na straně dodavatele budou plně integrovány s komunikačními kanály zadavatele a přizpůsobeny jeho potřebám. Pro komunikaci s uživateli uchazeč předpokládá využití telefonu, faxu, e-mailu a případně webového rozhraní. Pro interní komunikaci mezi dodavatelem a objednatelem předpokládá dodavatel využití Pracovního týmu (PT), Hlavního týmu projektu (HTP) a Řídícího Výboru (ŘV).

8.1.18. Dokumentace projektu

Průběh projektu a podstatné výstupy projektu jsou ukládány do centrálního úložiště dokumentace, které je přístupné všem osobám podílejícím se na projektu.

Struktura úložiště je následující:

- Společná projektová dokumentace
 - Provozní deník
 - SLA reporting
 - Požadavky na změnu
 - Zápisy z porad (jednání ŘV a pracovního týmu)
 - Komunikační matice – složení jednotlivých týmů a kontaktní údaje účastníků
 - Procesní dokumentace – popisy procesů, katalog služeb, konfigurační databáze
- Systémová dokumentace a složky jednotlivých systémů
 - Administrátorské, instalační a uživatelské příručky
 - Testovací a akceptační protokoly

Všechny dokumenty zaznamenávající dohody mezi objednatelem a poskytovatelem implementace změn (např. zápisy z jednání), výstupy poskytovatele (dokumenty analýzy a návrhu) jsou pojmenovávány stejnou konvencí a ukládány na úložišti Projektové dokumentace.

V případě oponentury a upřesňování obsahu dokumentu týkajícího se implementace změn jsou změny zachycované formou revizí (pokud to daný formát dokumentu umožňuje) a v úvodu dokumentu je doplněno datum oponentury a souhrn připomínek. Opakovaně předávané dokumenty objednateli jsou verzovány a nová verze bude obsahovat stručný popis změn navíc ještě v komentáři verze na portálu.

Konvence pojmenování souboru je "Název dokumentu_identifikace týmu_verze (případně pořadí)_datum předání", kde verze je znázorněna konvencí XvY a datum je ve formátu rmmdd (bez diakritiky).

Soubory jsou na úložiště ukládány ve standardních formátech – MS Office verze 2003 včetně (.doc, .docx, .xls, .ppt, .msg atd.), MS Project (.mpp), obrázky (.jpeg, .tif, .gif, .pdf), MS Visio (.vsd), XML služby (.wsdl, .xml, .html, .css).

Na základě schválených plánů změn a plánů odstávek zasílá technický specialista případně Manažer řízení služeb v dostatečném předstihu na HD MPSV informační e-mail v předem definované struktuře o plánované odstávce systému (případně plánované změně). HD MPSV si odstávku/update zkontroluje z hlediska plánů odstávek a změn, případně si vyžádá souhlas odborného garanta IS nebo Manažera řízení služeb poskytovatele. Rovněž si může vyžádat doplnění e-mailu o dodatečné informace, pokud není informace kompletní.

Minimální rozsah strukturovaného e-mailu je následující:

- Identifikace systému, kterého se informace týká a identifikace, zda se jedná o produkční či testovací prostředí.

Rozsah prací.

Dopad prací (např. úplná nedostupnost, omezení rychlosti aplikace apod.).

Plánovaný začátek a plánovaný konec prací (datum a čas).

Kontaktní osoba odpovědná za provedení prací a kontaktní údaje (mobil a e-mail).

Následně HD MPSV rozešle oznámení e-mailem na kontaktní osoby dle komunikační a eskalační matice (filtrované dle druhu upozornění (odstávka/update) a dotčeného systému).

Strukturované e-maily jsou prostřednictvím HD MPSV rozesílány v případě výpadku systému, kdy je součástí zprávy dotčený systém a určení prostředí (produkční/testovací). Zpráva je zasílána na konkrétní osoby určené v komunikační a eskalační matici (druh upozornění "výpadek"). Zpráva je zasílána při vzniku takového stavu a po vyřešení incidentu je oznámeno ukončení výpadku.

8.2. Způsob monitoringu, měření a vyhodnocování provozních parametrů řešení

8.2.1. Centrální monitorovací nástroj

Jako primární monitorovací nástroj infrastruktury a aplikací byl zvolen S&T Spectator. Spectator je řešení, jenž umožňuje monitorovat chování komponent informačního systému od hardware až po aplikace. Dává možnost, v co nejkratší době, detekovat reálné ale i potenciální problémy, které se mohou vyskytnout v každodenních činnostech IT systémů. Nonstop monitorování zajistí bezpečnost a efektivitu práce IT systémů – 7 dnů v týdnu, 365 dní v roce.

Hlavní vlastnosti řešení Spectator:

Dohled nad zařízeními a dostupností služeb v síťovém prostředí

Kontrola UPS, teploty v serverových místnostech, routerů

Aktivní i pasivní sběr informací

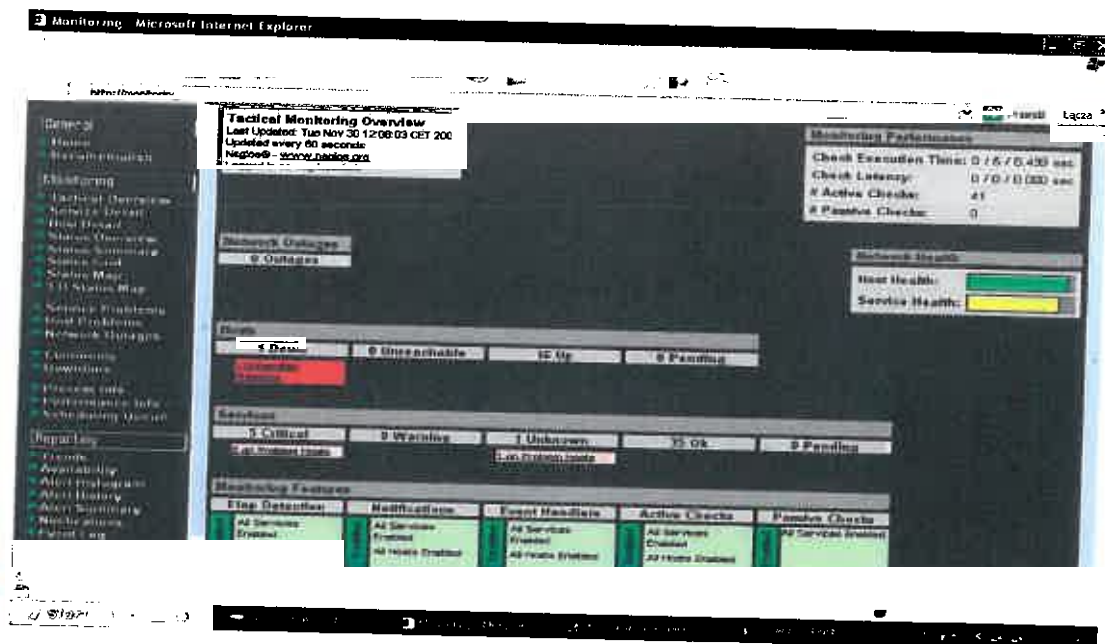
Použití vlastních agentů nebo SNMP protokolu

- Možnost vývoje agentů nových (pro zařízení i aplikace) Notifikace
- Notifikace
- Oznámí problém před tím, ještě než je uživateli vůbec zjištěn
 - Definice alertů (OK, WARNING, CRITICAL, UNKNOWN)
 - Různé způsoby oznámení (e-mail, SMS...) Webová konzole operátora

Webová konzole administrátora

Aktuální stav zařízení a služeb

- Historie všech záznamů
- Reporty o dostupnosti zařízení a služeb
- Reporty o závadách a problémech
- Reporty o oznámeních/notifikacích



Výhody platformy Nagios

Plně škálovatelná – systém roste s potřebami společnosti bez nutnosti vybavování novou technickou infrastrukturou či nákupem licencí

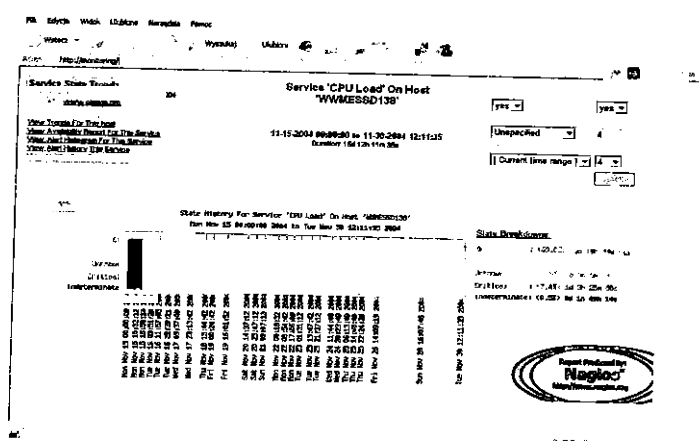
- Využívá současně infrastruktury k přenosu dat (vyžaduje IP síťové prostředí)
- Umožňuje rychlou implementaci s minimálním vlivem na monitorované systémy

Běží na Linuxu – operační systém s nízkým TCO

(m notifikacím apod.)

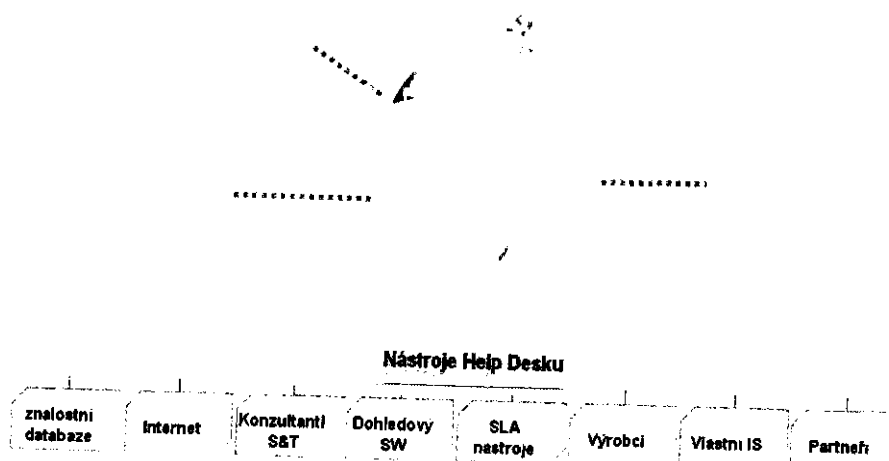
dohledový server je

jedné vývojářské



8.2.2. Servicedesk

S&T CZ provozuje ve vlastních prostorách ServiceDesk, který je rozdělen na několik virtuálních týmů dle klienta a typu práce (HelpDesk, Kvalifikace, Dispečink, Dohled). Všechny členy ServiceDesku spojuje jedna technologická základna telefonického CallCentra od společnosti Alcatel s nadstavbou pro profesionální CallCentra Genesys. ServiceDesk pracuje s vlastním IMS společnosti stejně jako s informačními systémy našich klientů. Plné služby ServiceDesku poskytujeme v době 8x10 a 24x7 v stand-by režimu s dohledem systémů našich klientů v nonstop režimu. Procesy ServiceDesku jsou standardizovány s tím, že pro každého klienta jsou upraveny v průběhu implementace služby tzv. "na míru" klienta a jeho požadavků.



ServiceDesk představuje provoz centrálního místa Dodavatele pro hlášení a evidenci požadavků Objednatele souvisejících s plněním Služby ve lhůtách uvedených v SLA. Součástí této Dílčí služby je zejména:

- Příjem požadavků na odstranění vad
- Evidence požadavků na straně S&T
- Evidence průběhu řešení a výsledného řešení požadavků na odstranění vad
- Technická podpora zaměstnanců odboru ICT Zadavatele
- Spolupráce s pracovníky odboru ICT Zadavatele a s dodavateli třetích stran při odstraňování problémů
- Poskytování informací o dodávaných službách pro odbor ICT Zadavatele
- Příprava podkladů pro reporting

Hlavními charakteristickými rysy služeb ServiceDesk jsou:

- Užívání metodických standardů a ověřené procesní metodologie ITSM
- Víceúrovňová struktura umožňující typovou segmentaci a vyšší efektivitu práce

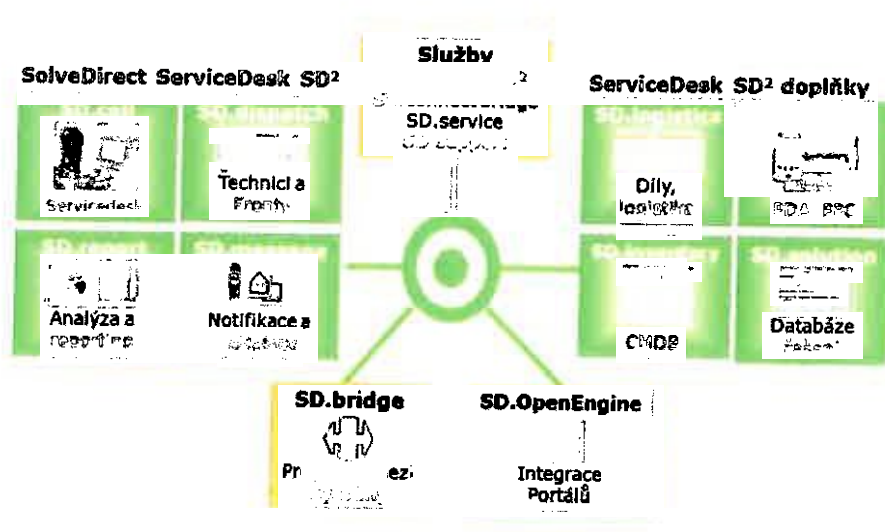
S&T poskytuje komplexní služby outsourcingu, které pokrývají celý životní cyklus od návrhu řešení a architektury, přes poskytování technologií formou služby, řízení změn v průběhu životního cyklu až po provozování a podporu infrastruktury. Funkce ServiceDesku je nedílnou součástí provozu a podpory a S&T takový IT ServiceDesk provozuje pro řadu významných klientů v České republice, srovnatelných co do velikosti se Zadavatelem.

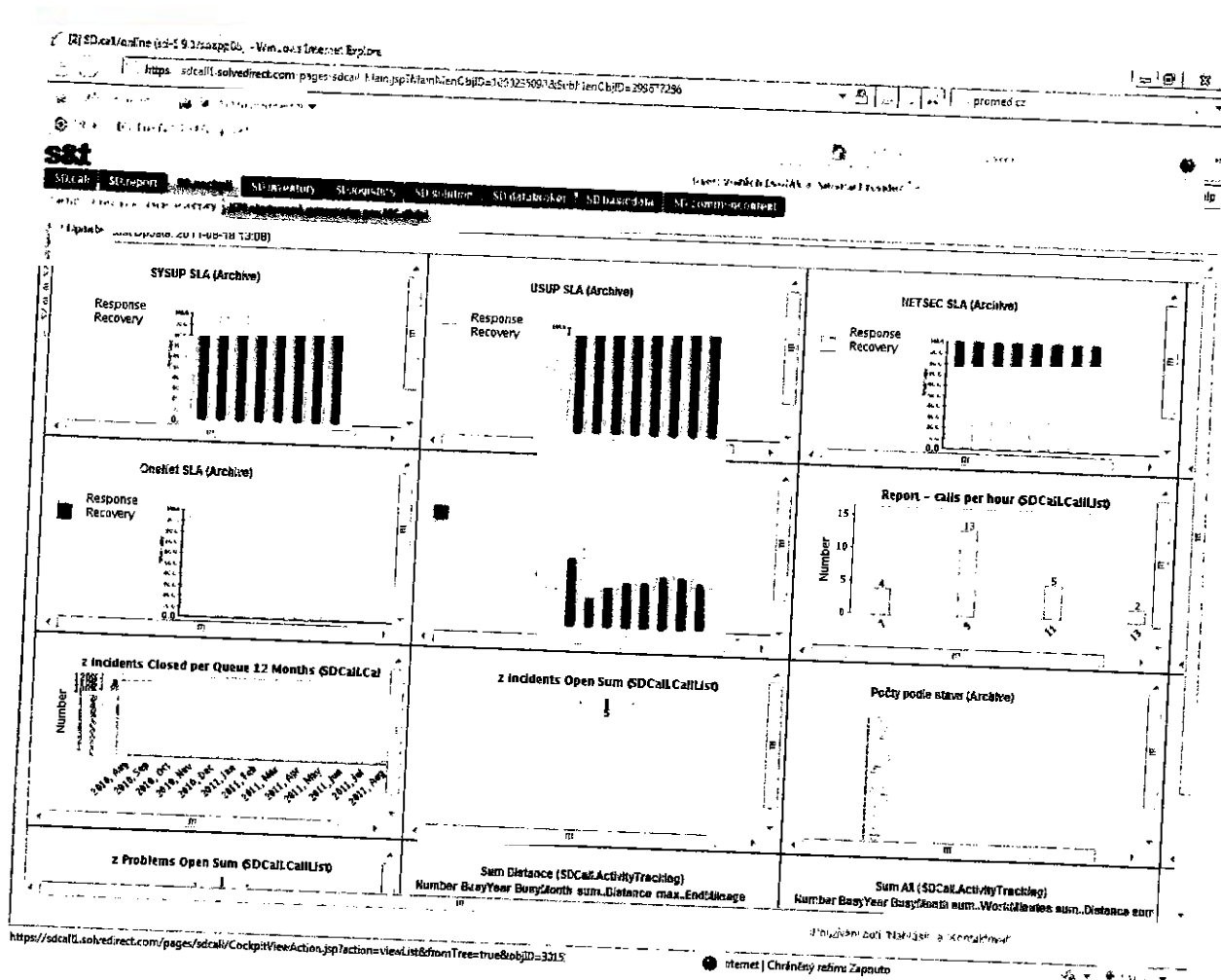
ServiceDesk S&T je jeden tým pracující ve sdíleném režimu pro více zákazníků, fyzicky umístěný v prostorách S&T. ServiceDesk je organizován do několika vrstev s rozdílnými rolmi v rámci procesů ITIL.

Název		
Level 1	Primární kontaktní místo pro uživatele IT	Incident Management, Request Fulfillment, Access Management
Level 2	Technické řízení	Incident Management, Problem Management, Release and Deployment, Operations Management (provozní činnosti)
Level 3	Technická autorita	Change Management, Design

8.2.2.1. Incident Management System SolveDirect

Solvedirect je plně webová online aplikace specificky vytvořená pro práci s požadavky. Je jedním z nejčastěji užívaných systémů outsourcingovými společnostmi a společnostmi poskytujícími servisní služby více zákazníkům z jednoho nástroje. Systém jako takový je provozován buď formou Cloudu (SaaS) nebo méně častou formou instalované vlastní instalované stand-alone aplikace.





Systém Solvedirect obsahuje všechny klíčové funkcionality pro management požadavků tedy:

- Databáze kontaktů, lokalit, zařízení, software, výrobců atd.
- Procesní workflow, které lze libovolně měnit a upravovat
- Eskalační a notifikační nástroje (SMS, mail atd.)
- Měření SLA (hodnoty odezva, oprava/náprava)
- Silný reporting všech hodnot souvisejících s požadavky (kvantitativní, kvalitativní)
- Webové rozhraní jak pro běžné prohlížeče, tak pro přístup z mobilních zařízení
- Znalostní databáze
- A mnoho dalších funkcí. Detaily lze nalézt na stránkách výrobce <http://www.solvedirect.com>

Reporting a evidence

Reporting a evidence zahrnuje vedení evidence Zařízení přenechaných kužívání Objednateli a vytvoření sady pravidelných reportů, které zahrnují informace a to zejména:

Reporting

- Počtu servisních požadavků a reklamací
 - Seznam s počty roztríděný po jednotlivých měsících a letech

- Pole detailního seznamu budou obsahovat všechna data relevantní k daným požadavkům a reklamám
- Řešeno on-line reportem z logického celku reportingu "Množství Volání" viz. metodika níže
- Plnění SLA parametrů u incidentů a reklamací
 - Seznam s procentem plnění SLA po jednotlivých měsících a letech
 - Pole detailního seznamu budou obsahovat časová razítka ze který je proveden výpočet procenta dosaženého SLA
 - Řešeno on-line reportem z logického celku reportingu "Úroveň Služby" viz. metodika níže
- Přehled obnovy techniky v případě havárie včetně plnění SLA
 - Seznam s počty a plněním SLA roztržiděný po jednotlivých měsících a letech
 - Řešeno on-line kombinací reportů z celků "Množství Volání" a "Úroveň Služby"
- Přehled plnění harmonogramu obnovy techniky
 - Report s plánem harmonogramu a časovými razítky finální realizace
 - Řešeno on-line reportem exportovaným z CMDB s časovými razítky
- Přehled instalací jednotlivých Image na zařízeních.
 - Seznam zařízení s detaily ze CMDB mezi které patří i verze image
 - Řešeno on-line reportem exportovaným z CMDB s detaily o verzích image
- Přehled dostupných opravných balíčků k centrální distribuci včetně údajů o případné distribuci
 - Seznam všech opravných balíčků s uvedeným stavem
 - Stav: žádost na balíček, v přípravě, testování, připraveno k distribuci, distribuováno
- Přehled dostupných opravných balíčků; které nelze distribuovat centrálně včetně údajů o případné distribuci
 - Rozšířený seznam viz. bod výše o stav nelze distribuovat s uvedením důvodu
 Jelikož se jedná o balíčky nedistribuované automaticky bude řešeno seznamem udržovaným Service Manažerem s využitím odpovídajícího SW nástroje
- Přehled využívání služeb dodavatele podle jednotlivých katalogových listů
 - Report s počty požadavků na každý katalogový list po jednotlivých měsících a letech – KL bude zaveden do systému jako PrvekSmlouvy viz. metodika níže
 - Řešeno on-line reportem z logického celku reportingu "Množství Volání" viz. metodika níže

Evidence SW

- Evidence SW instalovaného v místě odběratele
 - Podle druhů SW
 - Podle HW na kterém je instalován

Evidence SW bude realizována na vstupu typováním použité verze SW do CMDB. Změna zařízení, SW nebo reinstalace povede vždy k aktualizaci dat v CMDB. Každé HW má v CMDB vlastní sadu polí mezi které patří i pole pro uložení potřebných informací o SW.

Seznam bude obsahovat detaily o HW i SW (výrobní číslo, typ, verze atd.) s uvedením verze image/SW.

- Řešeno on-line reportem ze CMDB

Evidence HW

Evidence HW instalovaného v místě odběratele, která bude obsahovat minimálně tyto povinná pole:

- Konfigurace
- TypUmístění
- Výměna
- Vyřazení
- Servis

Stejně jako evidence SW je detailní evidence všech atributů HW výše uvedených, součástí CMDB. Mimo výše uvedená datové pole bude seznam rozšířen o další důležité informace např.: Inventární číslo, model/typ, odpovídající servisní SLA, datum a jméno k poslední editaci záznamu v CMDB.

- Řešeno on-line reportem ze CMDB

8.2.2.2. Metodika poskytování a příklady reportů

Vytváření reportů je v kompetenci role Service Manažera. Jedná se o klíčovou službu pro měření kvalitativních a kvantitativních parametrů dodávaných služeb.

Vstupy do procesu měření a reportingu kvalitativních a kvantitativních parametrů jsou především:

- SLA – tedy klientem smluvně definované parametry, jež služba musí dlouhodobě splňovat
- OLA – interní mimo smlouvu definované parametry, které slouží k měření návazných služeb
CSI – subjektivní hodnocení spokojenosti zákazníka nebo uživatelů s poskytovanými službami
- CMDB – databáze obsahující veškerá a detailní data o HW, SW a všech realizovaných službách a aktivitách

Výstupy z procesu měření a reportingu kvalitativních a kvantitativních parametrů se předkládají ve dvou informačních vrstvách. První je tzv. souhrnný jednostránkový DashBoard, jež slouží, k rychlému shrnutí celkové kvality všech poskytovaných dílčích služeb a je využíván především managementem zákazníka a dodavatele. Druhá informační vrstva je mnohem detailnější (až na úroveň dat z CMDB). Tuto vrstvu reportů a detailů využívají především nominovaní Service Manažeři k detailní analýze trendů, problémů, návrhů na zlepšení atd.

Základem druhé vrstvy nebo také úrovně reportingu jsou on-line generované reporty u kterých jsou k dispozici následující funkcionality:

- Jedním klikem export do Excelu, CSV a XML souborů

- Jedním klikem export do PDF
- Drill-Down funkcionalita
- Seznam instalované báze HW/SW

Drill-Down umožňuje z každého on-line reportu proklikáváním vstupovat do dat ze kterých je report složen nebo vypočítán. Tedy lze jedním klikem z přehledové tabulky např. s počty instalací/oprav v jednotlivých měsících vstoupit do detailního seznamu s popisy jednotlivých instalací/oprav, a dalším klikem zobrazit úplný detail jedné jediné instalace nebo opravy včetně všech příloh, časů a komentářů techniků i uživatelů.

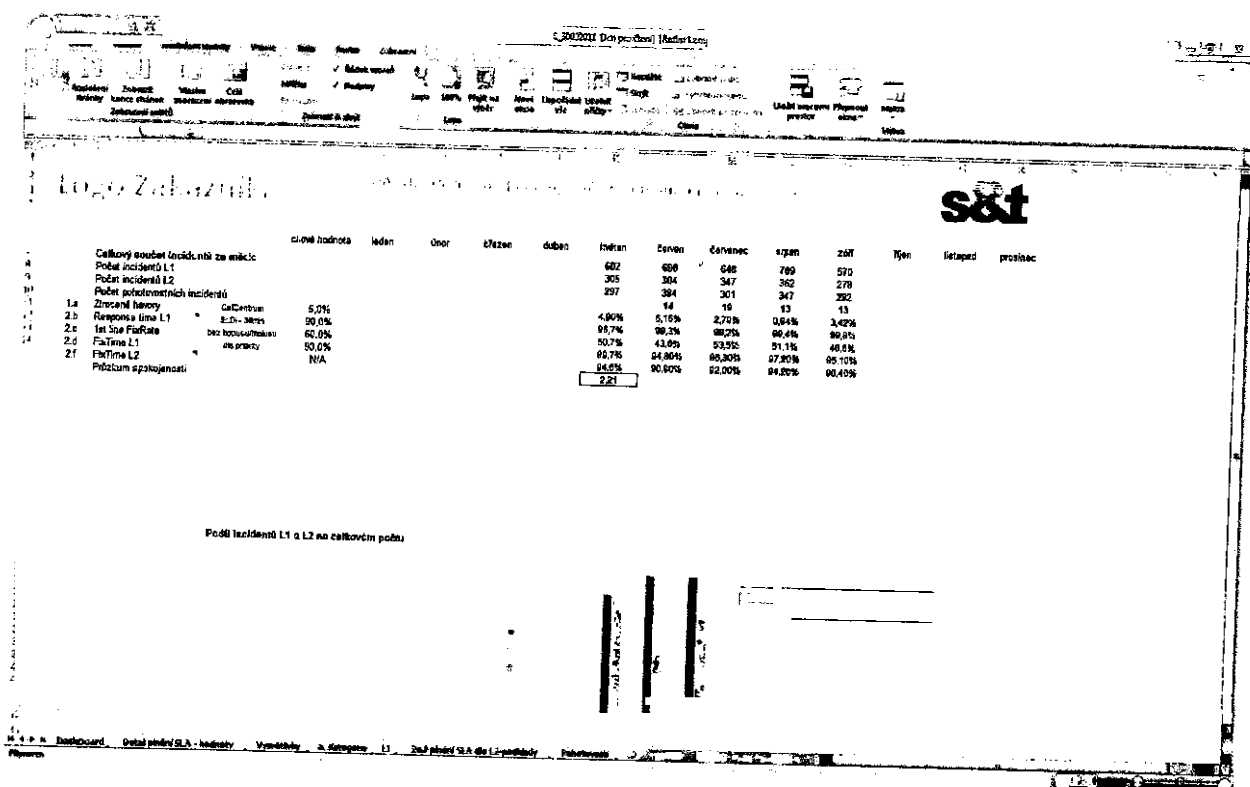
První úroveň reportingu – Dashboard

V první vrstvě (tzv. Dashboard) jsou prezentována především tyto data:

Percentuální plnění SLA

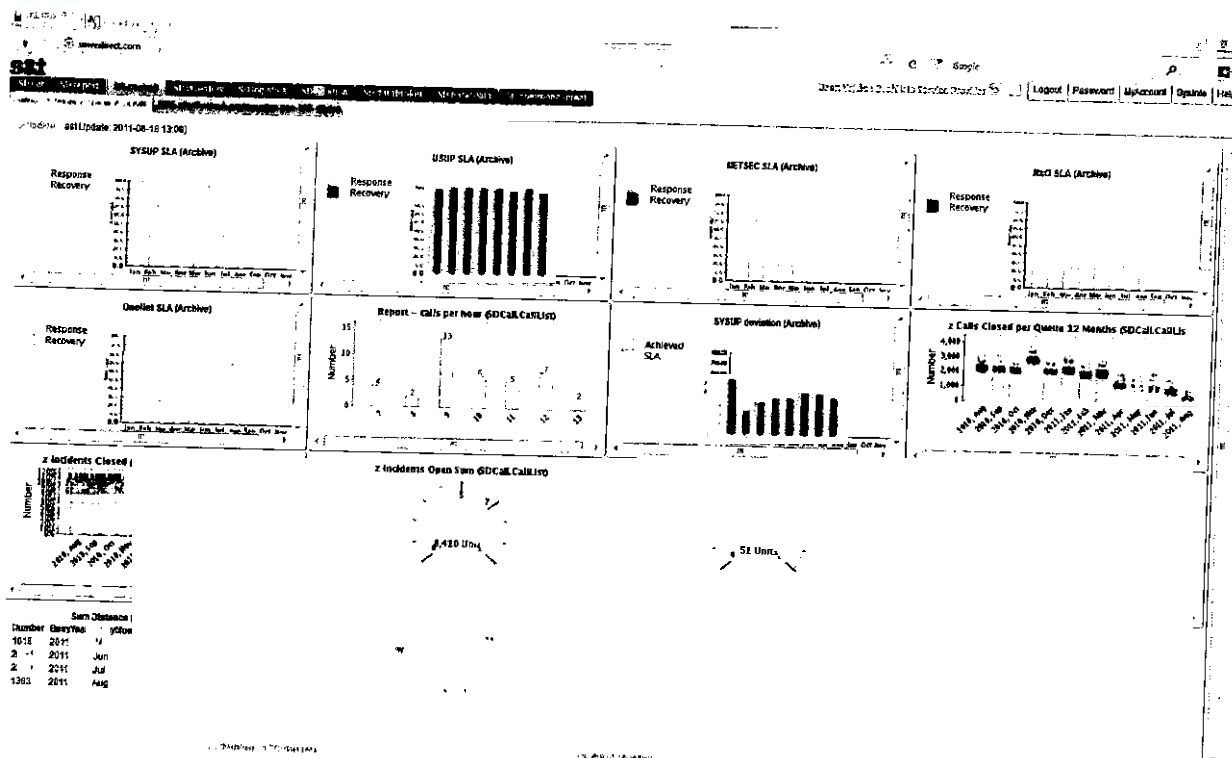
- Index hodnocení zákazníka a uživatelů

Součástí bývá souhrn finanční kalkulace/podklad pro fakturaci



DashBoard je generován na konci každého kalendářního měsíce a je podkladem pro pravidelné měsíční vyhodnocování poskytovaných služeb smluvními stranami včetně odsouhlasení souvisejících finančních podkladů.

DashBoard může být se základními parametry poskytovaných služeb generován kdykoli v průběhu i on-line. Tento on-line náhled může být zobrazen na dohledovém displeji nebo mobilním zařízení Service Manažera dodavatele pro aktuální přehled stavu všech klíčových parametrů poskytovaných služeb.



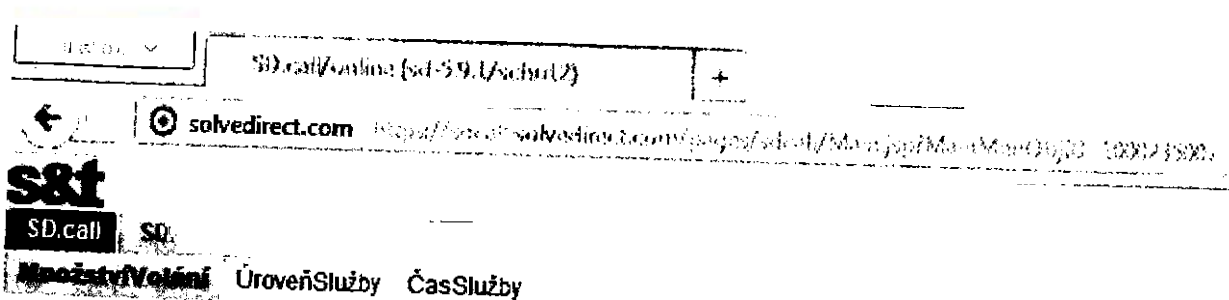
Screenshot on-line pohledu na webový DashBoard

Ve druhé vrstvě jsou prezentována především detailní přehledové reporty ze CMDB obsahující počty incidentů, kategorie, aktivity, lokality atd. Všechny reporty z této vrstvy jsou k dispozici vždy (24x7) on-line Service Manažerovi zákazníka i odběratele.

V této úrovni reportingu je rozsah možností pro generování různých reportů natolik rozsáhlá, že umožňuje on-line přístup k více jak 200 kusům reportů. Tuto rozmanitost a hloubku získá i neškolený Service Manažer zákazníka přes intuitivní on-line webové rozhraní které je zdarma bez limitu počtu Service Manažerů nebo jiných uživatelů ze strany zákazníka.

Webové rozhraní obsahuje desítky parametrů, kterými lze výsledný report ovlivňovat (filtrovat, omezovat, třídit, zobrazovat). Sady reportů jsou zde rozděleny do tří logických celků:

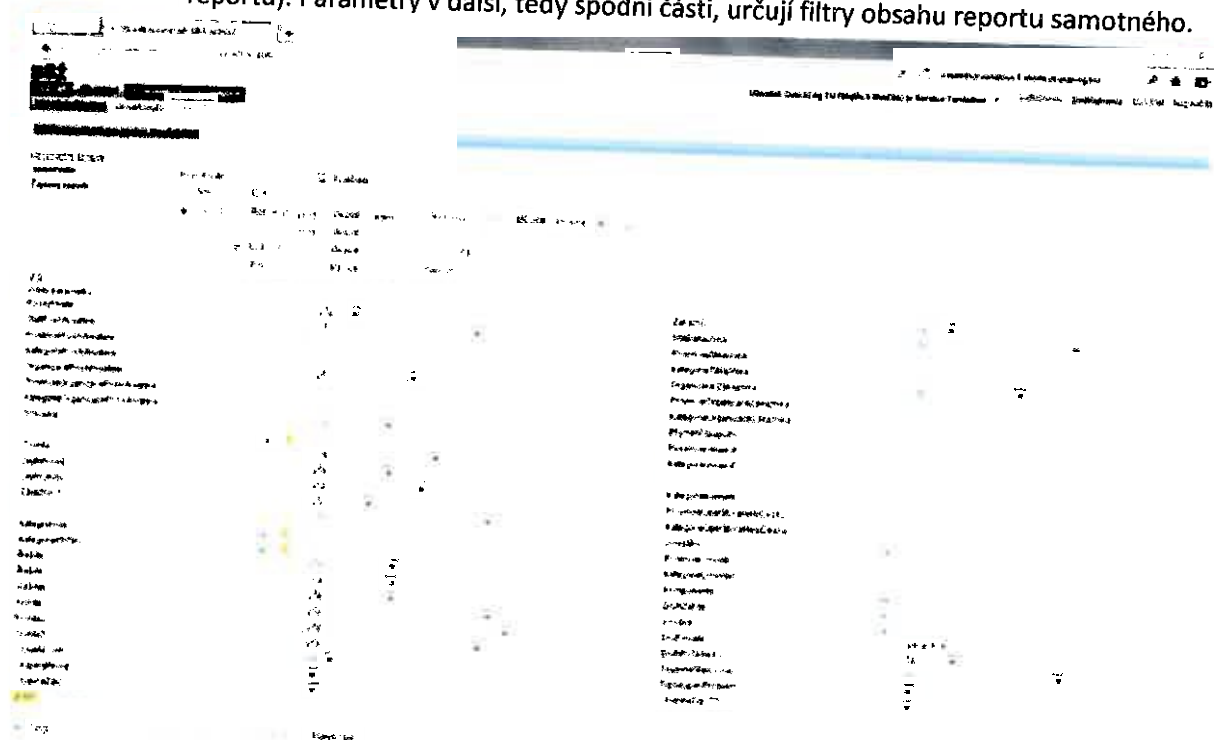
7. Množství Volání – výstupem této skupiny reportů jsou vždy počty (součty incidentů, změn apod.)
8. Úroveň Služby – výstupem této skupiny jsou procenty vyjádřené hodnoty proti nastaveným SLA
9. Čas Služby – výstupy z této skupiny jsou časové hodnoty v minutách a hodinách (např. délka trvání oprav atd.)



Screenshot třech základních kategorií on-line reportingu

Množství Volání

Základní logika reportů je postavena na dvou částech. První část, první třetina níže uvedeného screenshotu určuje, jaký typ reportu bude vygenerován (seskupení reportu). Parametry v další, tedy spodní části, určují filtry obsahu reportu samotného.



Hlavní pohled na tvorbu reportů ze skupiny Množství Volání

Níže uvádíme kompletní seznam možných reportů (tedy seskupení podle pole) v celku Množství Volání:

- | | | |
|------------------------------------|----------------------|-------------------------------|
| • Poskytovatel | Umístění | • ProvincieKontaktu |
| • ProvinciePoskytovatele | • ProvincieUmístění | • KategorieKontaktu |
| • KategoriePoskytovatele | • KategorieUmístění | • ProvincieOperátoraHelpDesku |
| • StátPoskytovatele | Komponenta | • KategorieOperátoraHelpDesku |
| • OrganizacePoskytovatele | • DruhZařízení | • Fronta |
| • KategorieOrganizacePoskytovatele | • Výrobce | • Fronta2 |
| • ProvincieOrganizacePoskytovatele | • KategorieVolání | • Fronta3 |
| | • KategorieVolání1+2 | • ÚroveňFronty |
| | KategorieVolání1–3 | • Řešitel |

• Zákazník	KategorieVolání1–4	Řešitel2
• KategorieZákazníka	KategorieVolání1–5	Řešitel3
• ProvincieZákazníka	KategoriePříčiny	DruDodavateležadavku
• StátZákazníka	KategoriePříčiny1+2	SkupinaStavůVolání
• Organizace Zákazníka	KategoriePříčiny1–3	SkupinaPriorit
• KategorieOrganizaceZákazníka	KategoriePříčiny1–4	TypSkupinyProblému
• ProvincieOrganizaceZákazníka	KategoriePříčiny1–5	SkupinaTypůChyb
• Smlouva	PříjmeníVolajícího	SkupinaZávažnosti
• PrvekSmlouvy	PoskincieVolajícího	
• Priorita	KategorieVolajícího	
• DruDodavatelroblému		
• DruhChyby		
• Závažnost		
• StavVolání		

Základní filtry pro reporty (seskupení podle) v této skupině jsou:

Otevřená Volání – do reportu jsou zahrnuty všechna vytvořená volání

Uzavřená Volání – do reportu jsou zahrnuty již jen ukončená volání

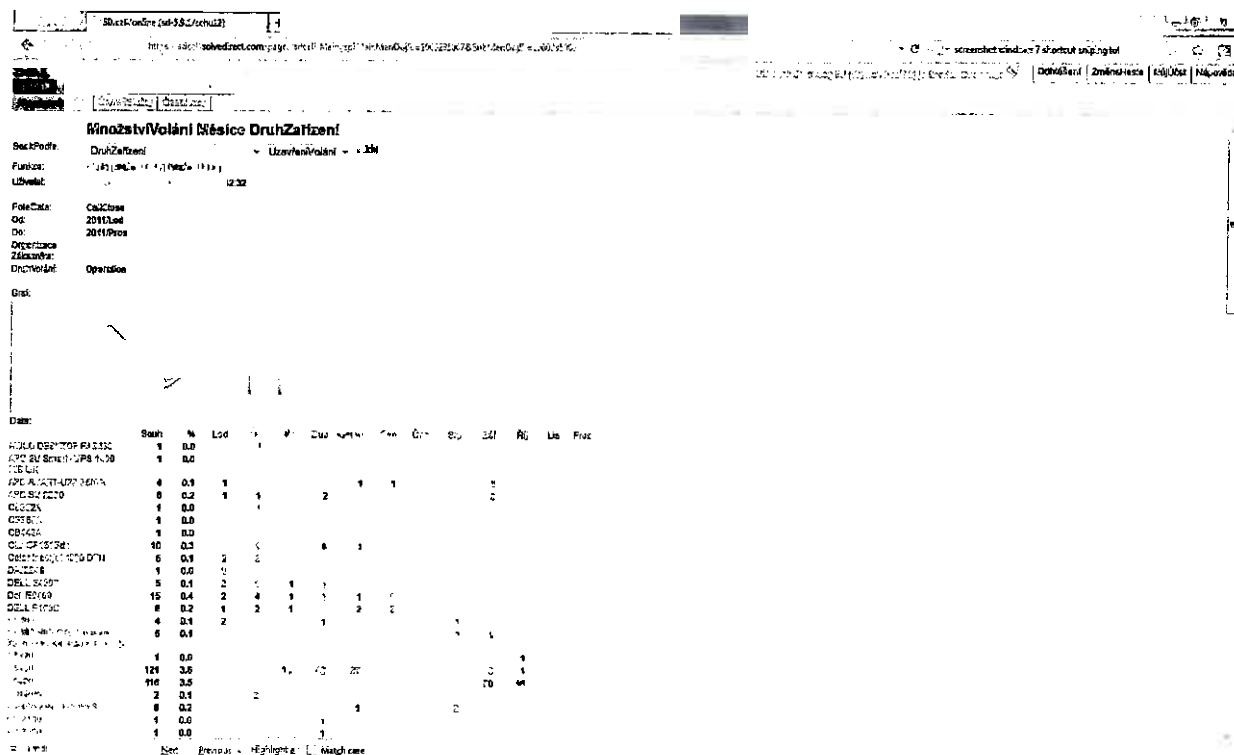
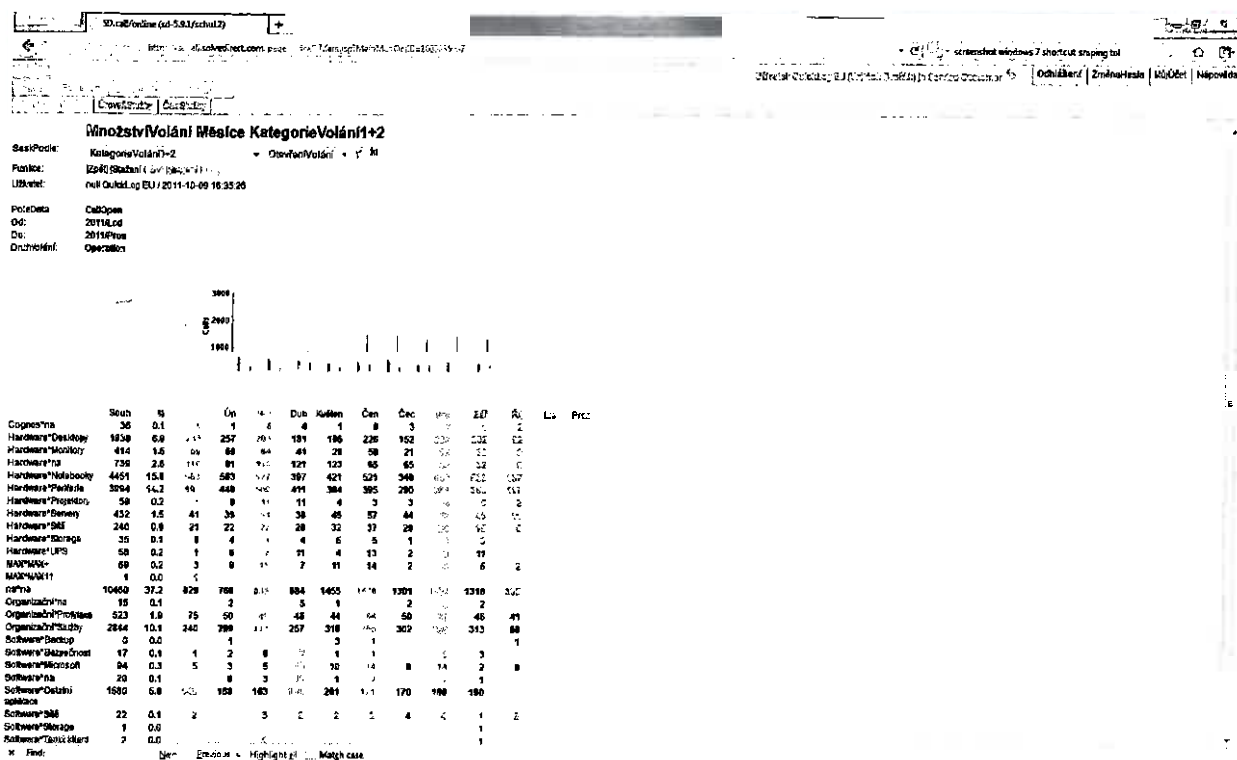
Časové hodnoty – vymezení hodnot od kdy, do kdy má report být vygenerován

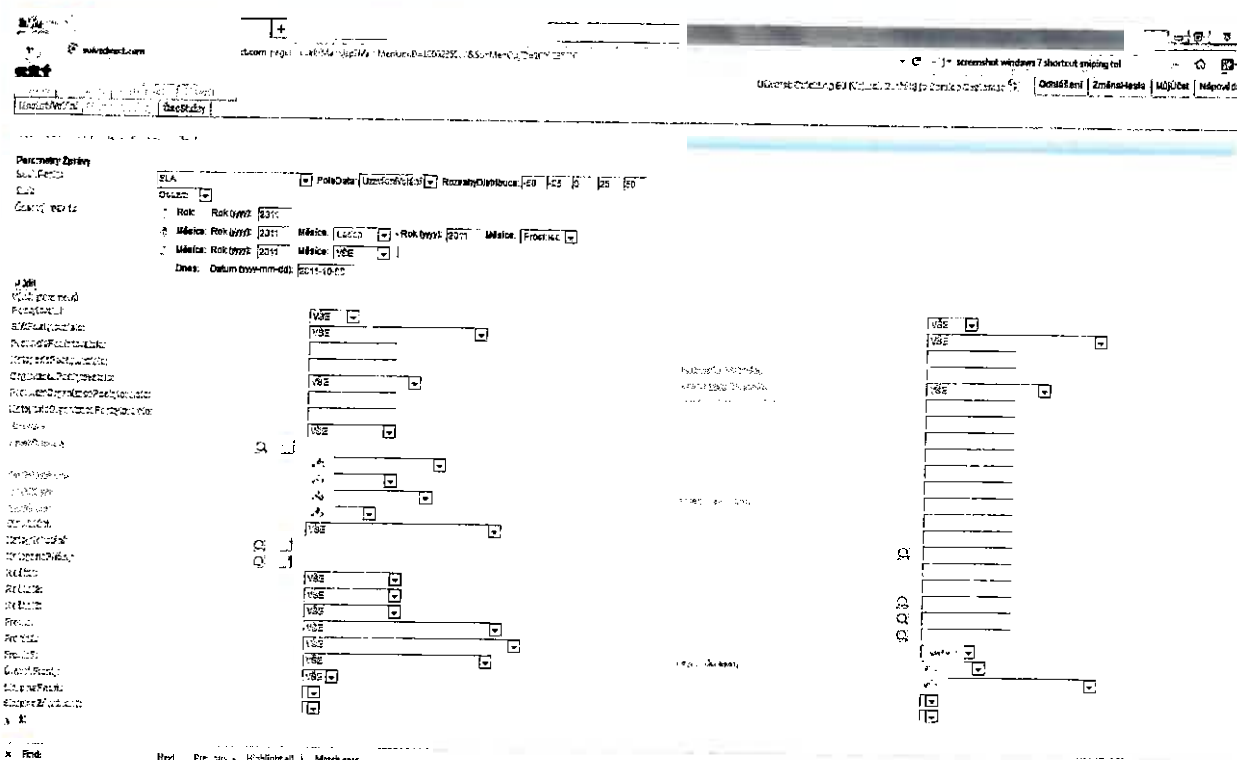
Časová granularita – vymezení detailu

- na rok
- na měsíce a roky
- na pracovní dny v měsíci a roce
- na dny

V této sadě reportů "Množství Volání" jsou položky typu reportu (seskupení reportu) a parametry pro kompletní seznam filtrů obsahu reportu shodné.

Níže uvádíme nejčastěji využívané reporty ze sady Množství Volání:





Hlavní pohled na tvorbu reportů ze skupiny Úroveň Služby

Níže uvádíme kompletní seznam možných reportů (tedy seskupení podle pole) v skupině Úroveň Služby:

- SLA
- Poskytovatel
- OrganizacePoskytovatele
- KategorieOrganizacePoskytovatele
- Zákazník
- Organizace Zákazníka
- KategorieOrganizaceZákazníka
- Smlouva
- PrvekSmlouvy
- Naplnění
- Odchylná
- Distribuce

Základní filtry pro reporty (seskupení podle) v této skupině jsou:

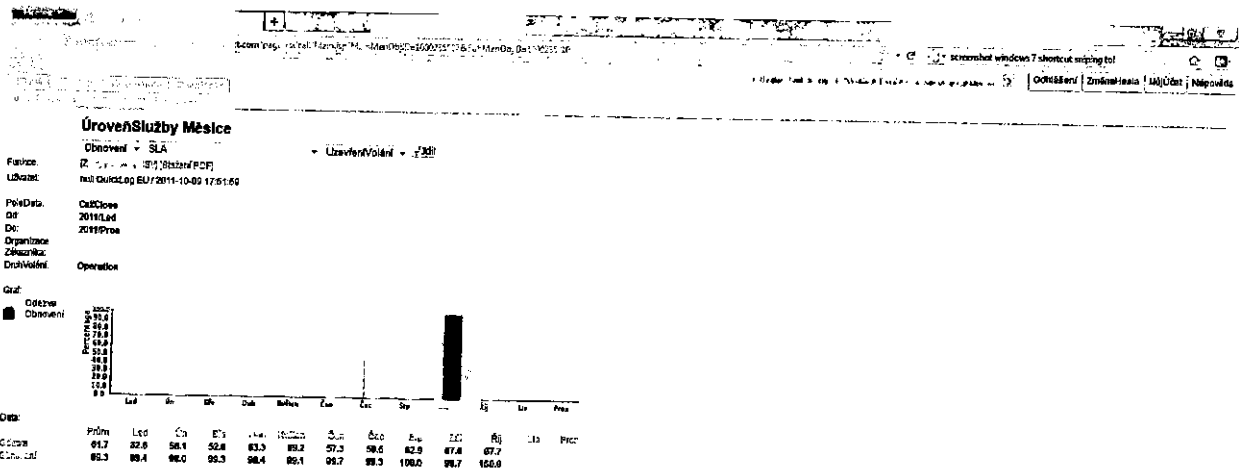
- Otevřená Volání – do reportu jsou zahrnuta všechna vytvořená volání
- Uzavřená Volání – do reportu jsou zahrnuta již jen ukončená volání
- Rozsah Distribuce – v procentech, nastavení pro vyobrazení jak daleko od předepsaného SLA se nachází reálně dosažená hodnota kvality služby
- Typ SLA – zda bude generován report nad parametrem Odezva (Response Time) nebo Obnovení (oprava, Fix Time)
- Časové hodnoty – vymezení hodnot od kdy, do kdy má report být vygenerován
- Časová granularita – vymezení detailu
 - na rok

- na měsíce a roky
- na měsíc
- na dny

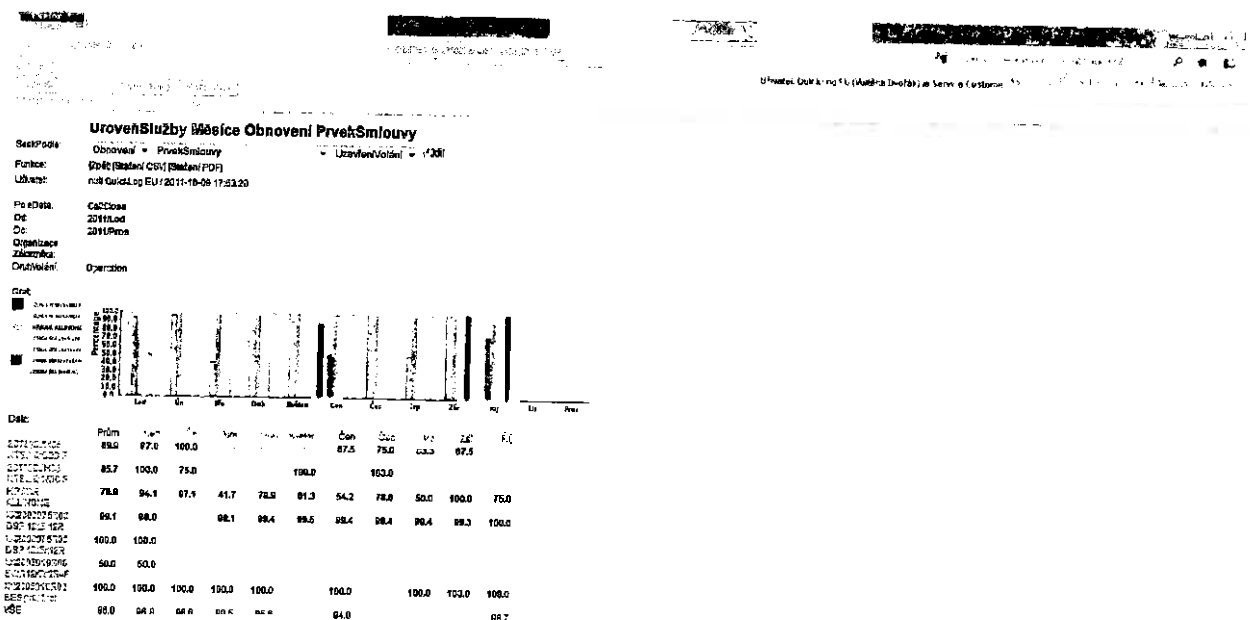
V této sadě reportů "Úroveň Služby" jsou k dispozici tyto parametry pro tvoření filtrů obsahu reportu:

• Poskytovatel	Umístění	ProvincieKontaktu
• ProvinciePoskytovatele	ProvincieUmístění	KategorieKontaktu
• KategoriePoskytovatele	KategorieUmístění	ProvincieOperátoraHelpDesku
• StátPoskytovatele	Komponenta	KategorieOperátoraHelpDesku
• OrganizacePoskytovatele	DruhZařízení	Fronta
• KategorieOrganizacePoskytovatele	Výrobce	Fronta2
• ProvincieOrganizacePoskytovatele	KategorieVolání	Fronta3
• Zákazník	KategorieVolání1+2	ÚroveňFronty
• KategorieZákazníka	KategorieVolání1–3	Řešitel
• ProvincieZákazníka	KategorieVolání1–4	Řešitel2
• StátZákazníka	KategorieVolání1–5	Řešitel3
• Organizace Zákazníka	KategoriePříčiny	DruDodavateložadavku
KategorieOrganizaceZákazníka	KategoriePříčiny1+2	SkupinaStavůVolání
• ProvincieOrganizaceZákazníka	KategoriePříčiny1–3	SkupinaPriorit
• Smlouva	KategoriePříčiny1–4	TypSkupinyProblému
• PrvekSmlouvy	KategoriePříčiny1–5	SkupinaTypůChyb
• Priorita	PříjmeníVolajícího	SkupinaZávažnosti
• DruDodavatelroblému	PoskincieVolajícího	
• DruhChyby	KategorieVolajícího	
• Závažnost		
• StavVolání		

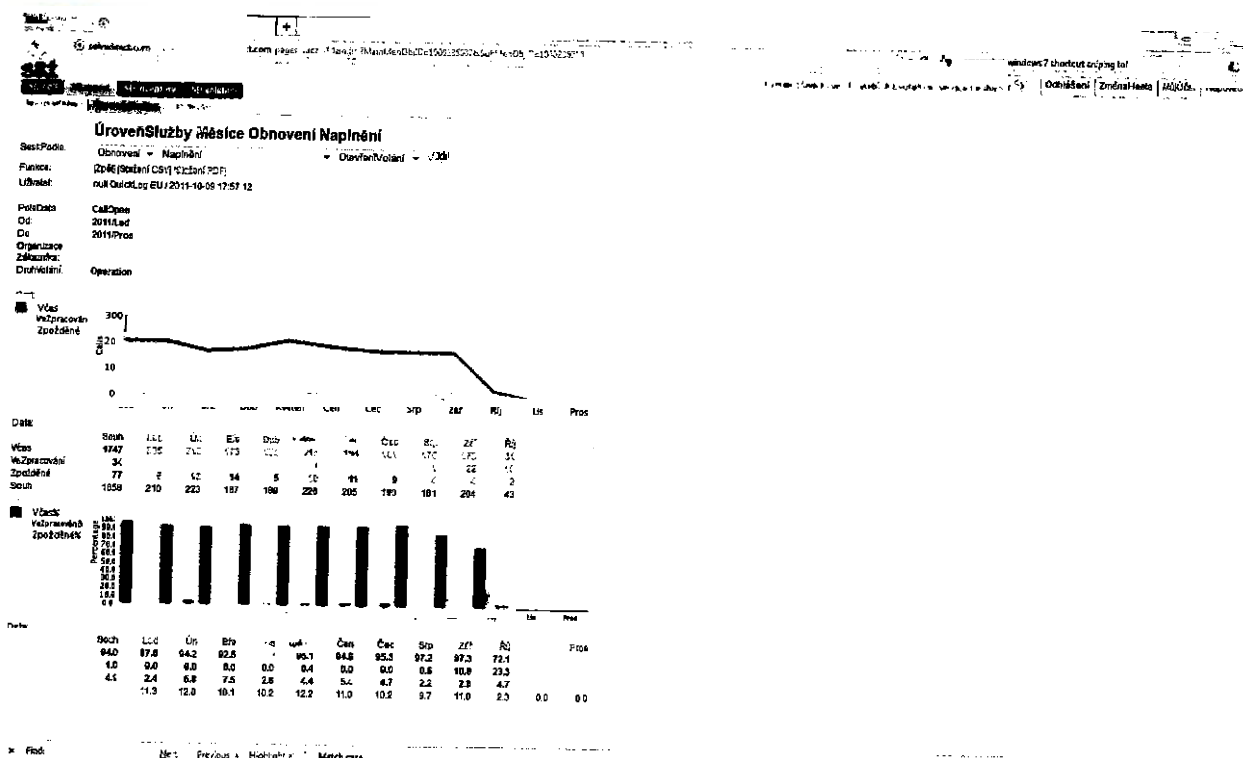
Níže uvádíme nejčastěji využívané reporty ze sady Množství Volání:



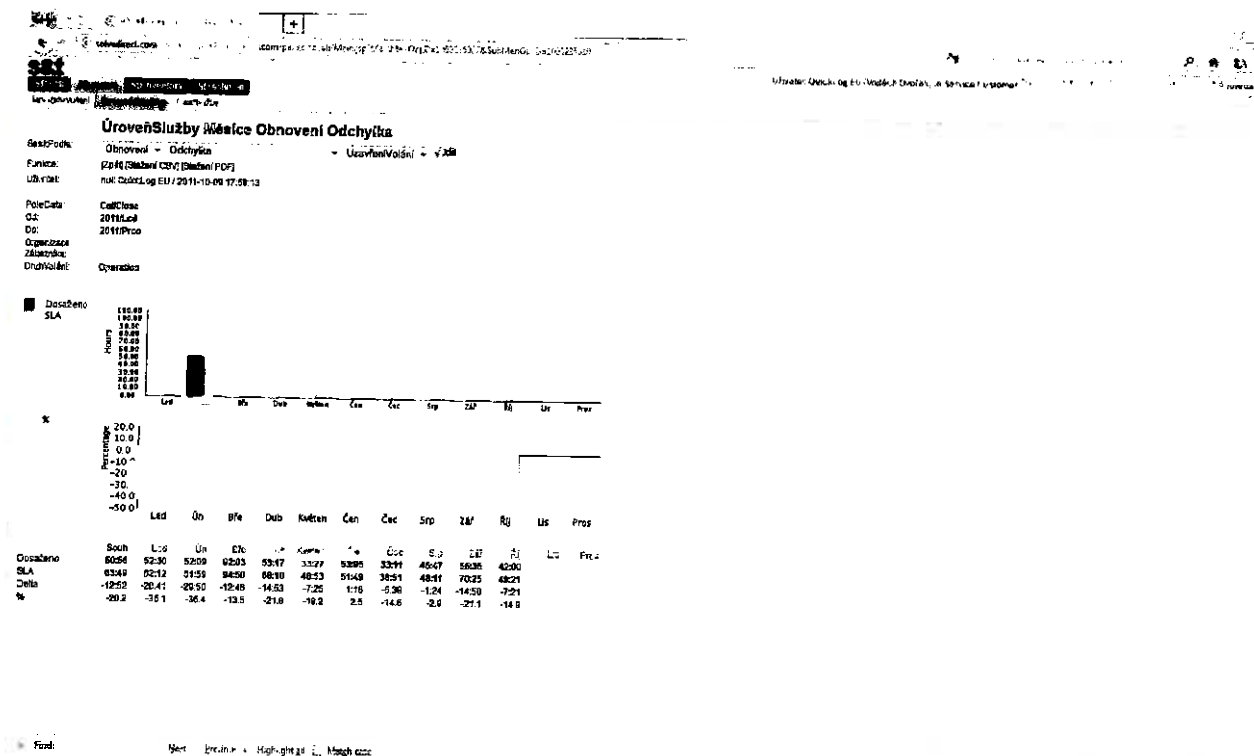
Celkový pohled na percentuální plnění SLA parametrů Odezva a Obnova



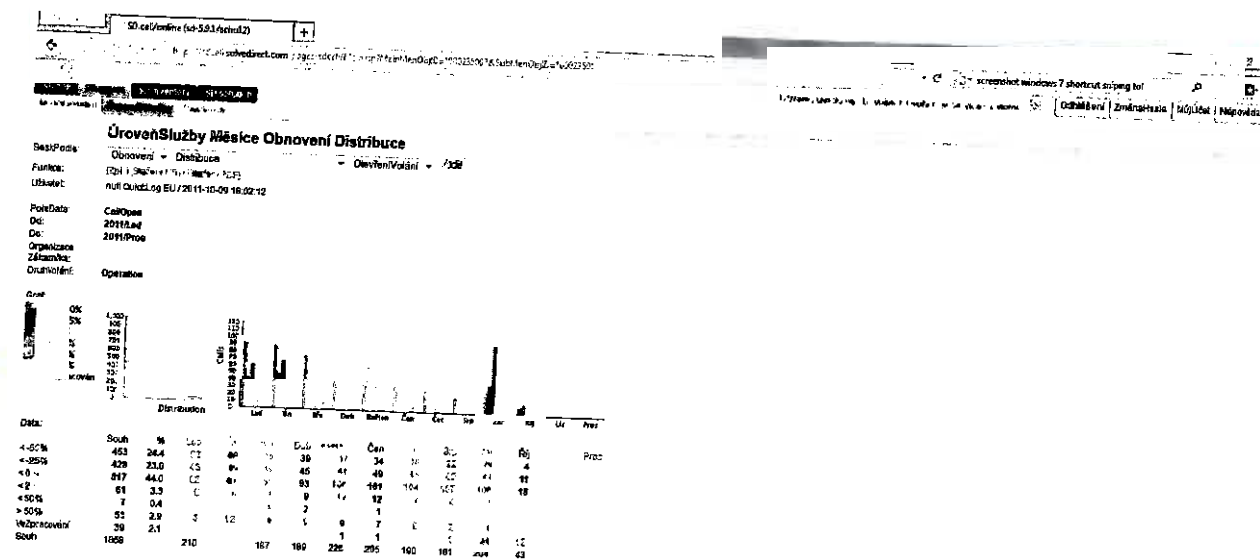
Screenshot zachycující percentuální plnění SLA po jednotlivých měsících s rozdělením na jednotlivé poskytované služby



Percentuální přehled plnění SLA za jednotlivé měsíce včetně procenta ještě rozpracovaných požadavků



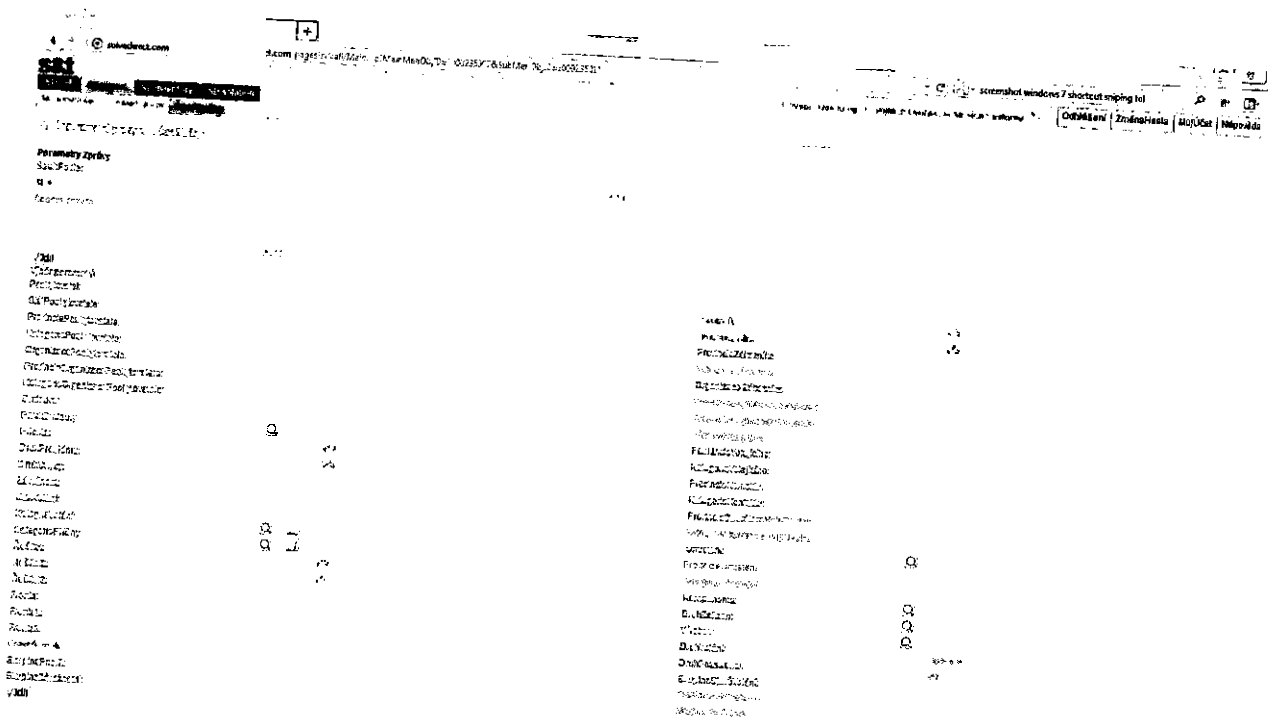
Odchytky od definovaného SLA v hodinách – slouží k analýze trendu kvality služby



Report distribuce plnění definovaných SLA – jak procentuálně je rychlé plnění SLA v rozsahu –50% až +50% (volitelné)

Čas služby

Základní logika reportů této skupiny je postavena stejně jako ta předchozí na dvou částech. První část, první třetina níže uvedeného screenshotu určuje, jaký typ reportu bude vygenerován (seskupení reportu). Parametry v další, tedy spodní části, určují filtry obsahu reportu samotného.



Hlavní pohled na tvorbu reportů ze skupiny Úroveň Služby

Níže uvádíme kompletní seznam možných reportů (tedy seskupení podle pole) ve skupině Úroveň Služby:

- Poskytovatel
- OrganizacePoskytovatele
- KategorieOrganizacePoskytovatele
- Zákazník
- Organizace Zákazníka
- KategorieOrganizaceZákazníka
- Smlouva
- PrvekSmlouvy
- Distribuce

Základní filtry pro reporty (seskupení podle) v této skupině jsou:

- Otevřená Volání – do reportu jsou zahrnuta všechna vytvořená volání
- Uzavřená Volání – do reportu jsou zahrnuta již jen ukončená volání
- Rozsah Distribuce – v hodinách, nastavení pro vyobrazení jak dlouho od předepsaného SLA se nachází reálně dosažený čas
- Typ SLA – zda bude generován report nad parametrem Odezva (Response Time) nebo Obnovení (oprava, Fix Time)
- Časové hodnoty – vymezení hodnot od kdy, do kdy má report být vygenerován
- Časová granularita – vymezení detailu
 - na rok
 - na měsíce a roky
 - na měsíc

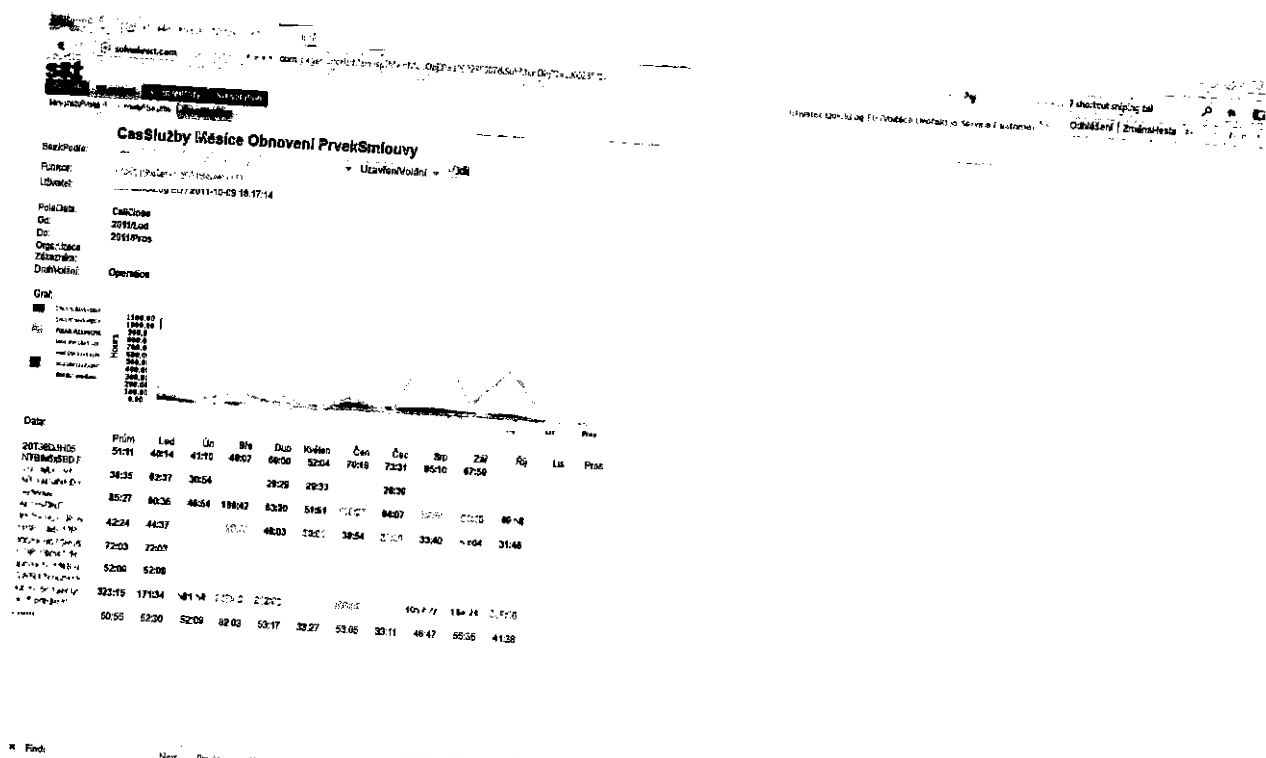
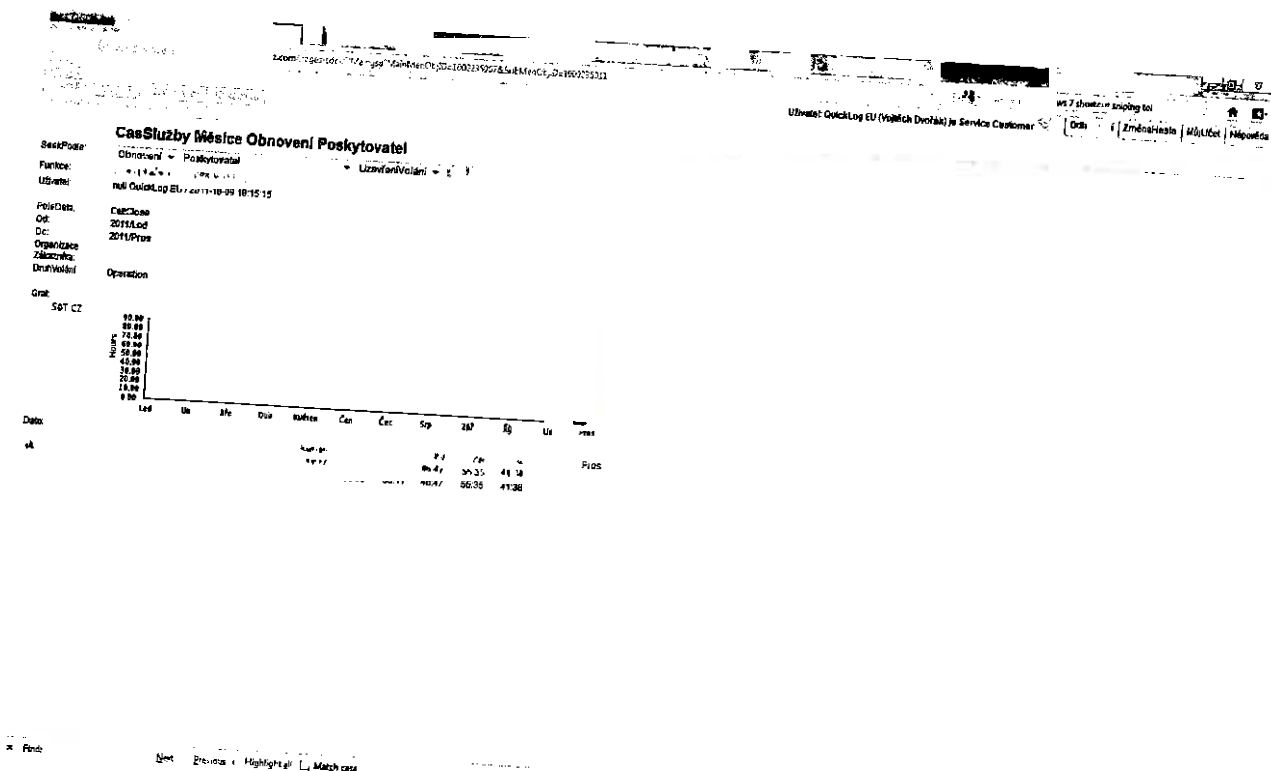
V této sadě reportů "Úroveň Služby" jsou k dispozici tyto parametry pro tvoření filtrů obsahu reportu:

Poskytovatel
 ProvinciePoskytovatele
 KategoriePoskytovatele
 StátPoskytovatele
 OrganizacePoskytovatele
 KategorieOrganizacePoskytovat
 ele
 • ProvincieOrganizacePoskytovat
 ele
 Zákazník
 KategorieZákazníka
 ProvincieZákazníka
 StátZákazníka
 Organizace Zákazníka
 • KategorieOrganizaceZákazníka
 • ProvincieOrganizaceZákazníka
 • Smlouva
 • PrvekSmlouvy
 • Priorita
 • DruDodavatelroblému
 DruhChyby
 • Závažnost
 • StavVolání

Umístění
 ProvincieUmístění
 KategorieUmístění
 Komponenta
 DruhZařízení
 Výrobce
 KategorieVolání
 KategorieVolání1+2
 KategorieVolání1–3
 KategorieVolání1–4
 KategorieVolání1–5
 KategoriePříčiny
 KategoriePříčiny1+2
 KategoriePříčiny1–3
 KategoriePříčiny1–4
 KategoriePříčiny1–5
 PříjmeníVolajícího
 PoskincieVolajícího
 KategorieVolajícího

ProcincieKontaktu
 KategorieKontaktu
 ProvincieOperátoraHelpDesku
 KategorieOperátoraHelpDesku
 Fronta
 Fronta2
 Fronta3
 ÚroveňFronty
 Řešitel
 Řešitel2
 Řešitel3
 DruDodavateložadavku
 SkupinaStavůVolání
 SkupinaPriorit
 TypSkupinyProblému
 SkupinaTypůChyb
 SkupinaZávažnosti

Níže uvádíme nejčastěji využívané reporty ze sady Množství Volání:



V hodinách vyjádřená doba potřebná k vyřešení požadavků v jednotlivých měsících v detailu podle SLA

- HlavníDatum
- MěsíceÚdržby
- PlánovanýPočetÚdržby
- OtevřenýPočetÚdržby
- ÚdržbaJeAktivní

Seznam informací které lze na požádání a zdarma do reportů pro Service Manažery přidat je velmi rozsáhlý a obsahuje přes 50 dalších polí z databáze CMDB. Pole, jež budou využita pro poskytování služby odpovídají požadavkům na informační hodnotu reportů a jsou součástí dohodv na počátku poskytování služeb.

Přehled nad celou instalovanou bází			
Id	Model / Info	Platnost / Provoz	Stav / Vlastník
1	HP LJ1300HP LJ1300	ONC0000000	HP
2	HP LJ1300HP LJ1300	ONC0000000	HP
3	HP LJ1300HP LJ1300	ONC0000000	HP
4	HP LJ1300HP LJ1300	ONC0000000	HP
5	HP LJ1300HP LJ1300	ONC0000000	HP
6	HP LJ1300HP LJ1300	ONC0000000	HP
7	HP LJ1300HP LJ1300	ONC0000000	HP
8	HP LJ1300HP LJ1300	ONC0000000	HP
9	HP LJ1300HP LJ1300	ONC0000000	HP
10	HP LJ1300HP LJ1300	ONC0000000	HP
11	HP LJ1300HP LJ1300	ONC0000000	HP
12	HP LJ1300HP LJ1300	ONC0000000	HP
13	HP LJ1300HP LJ1300	ONC0000000	HP
14	HP LJ1300HP LJ1300	ONC0000000	HP
15	HP LJ1300HP LJ1300	ONC0000000	HP
16	HP LJ1300HP LJ1300	ONC0000000	HP
17	HP LJ1300HP LJ1300	ONC0000000	HP
18	HP LJ1300HP LJ1300	ONC0000000	HP
19	HP LJ1300HP LJ1300	ONC0000000	HP
20	HP LJ1300HP LJ1300	ONC0000000	HP
21	HP LJ1300HP LJ1300	ONC0000000	HP
22	HP LJ1300HP LJ1300	ONC0000000	HP
23	HP LJ1300HP LJ1300	ONC0000000	HP
24	HP LJ1300HP LJ1300	ONC0000000	HP
25	HP LJ1300HP LJ1300	ONC0000000	HP
26	HP LJ1300HP LJ1300	ONC0000000	HP
27	HP LJ1300HP LJ1300	ONC0000000	HP
28	HP LJ1300HP LJ1300	ONC0000000	HP
29	HP LJ1300HP LJ1300	ONC0000000	HP
30	HP LJ1300HP LJ1300	ONC0000000	HP
31	HP LJ1300HP LJ1300	ONC0000000	HP
32	HP LJ1300HP LJ1300	ONC0000000	HP
33	HP LJ1300HP LJ1300	ONC0000000	HP
34	HP LJ1300HP LJ1300	ONC0000000	HP
35	HP LJ1300HP LJ1300	ONC0000000	HP
36	HP LJ1300HP LJ1300	ONC0000000	HP
37	HP LJ1300HP LJ1300	ONC0000000	HP
38	HP LJ1300HP LJ1300	ONC0000000	HP
39	HP LJ1300HP LJ1300	ONC0000000	HP
40	HP LJ1300HP LJ1300	ONC0000000	HP
41	HP LJ1300HP LJ1300	ONC0000000	HP
42	HP LJ1300HP LJ1300	ONC0000000	HP
43	HP LJ1300HP LJ1300	ONC0000000	HP
44	HP LJ1300HP LJ1300	ONC0000000	HP
45	HP LJ1300HP LJ1300	ONC0000000	HP
46	HP LJ1300HP LJ1300	ONC0000000	HP
47	HP LJ1300HP LJ1300	ONC0000000	HP
48	HP LJ1300HP LJ1300	ONC0000000	HP
49	HP LJ1300HP LJ1300	ONC0000000	HP
50	HP LJ1300HP LJ1300	ONC0000000	HP

Přehled nad celou instalovanou bází

8.3.1.3. Strategie zvládnutí rizik

Jedná se o určení způsobu, jak se s daným rizikem vypořádáme, jak ovlivníme jeho dopad a pravděpodobnost – zda se ho raději vyvarujeme, akceptujeme ho, minimalizujeme ho či ho přeneseme.

Výsledek identifikace, vyhodnocení a strategie zvládnutí rizik je zaznamenán do tzv. registru rizik, který je veden v elektronické formě.

Kromě klasifikace rizik obsahuje i nápravná opatření a sledování jejich úspěšné aplikace. Důležité je také určit odpovědnou osobu spojenou s provedením preventivního opatření.

8.3.1.4. Monitorování, vykazování a reportování

Pravidelná aktualizace registru rizik je potřebná pro včasnou identifikaci případných nových rizik, přehodnocování dříve identifikovaných rizik, posuzování opatření na jeho zvládnutí (původní strategie funguje, není potřeba nějaká změna?), aktualizace dokumentace, komunikace.

Během jakéhokoli projektu se mohou objevit další rizikové události, a proto musejí být rizika stále monitorována.

Registr rizik bude mít minimálně tyto položky (příklad v tabulce níže).

Riziko	Popis Rizika	Dopad	Váha Rizika	Řešení	Vlastník
Riziko 1	Dostupnost všech potřebných SW nástrojů a přístupů k potřebným aplikacím	Vysoký: 3	X	Zajištění že veškeré potřebné SW a přístupy jsou všem k dispozici	Projektový Manažer
Riziko 2	Popis Rizika	Dopad	Váha Rizika	Řešení	Vlastník
Riziko 2	příteln inform gem ent procesu	Vysoký: 3		Včasná definice pravidel a procesů s následnými testy a odsouhlasením uživatelů	Projektový Manažer a Manažer ServiceDesku
		Nízký: 1			

Registr rizik připraví a bude aktualizovat pracovní tým projektu. ŘV bude registr rizik schvalovat, tzn. schvalovat identifikovaná rizika, jejich klasifikaci a přijatá opatření.

8.4. Postup zajištění procesu změnových řízení

Tento proces řídí veškeré změny oproti stávajícímu stavu IT, které nějakým způsobem mohou nebo zasáhnou do činností Zadavatele. Změnová řízení platí pro změny v IT službách, software, hardware, síti. S&T zajistí co nejmenší dopad změn za využití standardních procesů jak komunikovat a implementovat takové změny.

		<i>dl na podnikání</i>	Komunikace a schvalování Zadavatelem	Příklad
Plánované	Standardní	Velmi malé nebo se opakující změny, jenž jsou běžného provozního charakteru, <i>bez jakéhokoli dopadu</i> na podnikání.	Není třeba.	Vytvoření účtu novému zaměstnanci.
	Malé	Malé změny, které mají dokumentovaný a vyzkoušený postup implementace s <i>velmi malým</i> dopadem na podnikání.	S&T upozorní Zadavatele <i>pět dní před</i> provedením změny. Postačuje zpráva Zadavatele bez potvrzení o jejím přijetí.	Instalování nového service packu na server.
	Střední	Změny, které mohou ohrozit vícero aplikací a mají <i>širší</i> dopad na podnikání.	S&T upozorní Zadavatele <i>pět dní před</i> provedením změny. Zadavatel <i>musí</i> potvrdit přijetí zprávy.	Instalace nebo reinstalace serveru, změny v LAN.
		Změny, které mohou ohrozit vícero aplikací skrze celou společnost a mají <i>signifikantní dopad</i> na podnikání.	S&T upozorní Zadavatele <i>deset dní před</i> provedením změny. Zadavatel <i>musí</i> potvrdit přijetí zprávy.	Spuštění nového antiviru, změna IS. Komplexní výměna HW včetně SW.
Neplánované	Kritické (mimo prac. dobu)	Změny, které musí být provedeny za účelem zprovoznění havarované IT služby s <i>nějakým dopadem</i> na podnikání.	S&T <i>co nejdříve</i> po zjištění nutnosti takové změny informuje Zadavatele. Potvrzení takové zprávy od Zadavatele je preferováno.	"Zatuhlá" služba na serveru – musí být opraveno ještě před začátkem zálohování.

		Změny, které musí být	S&T informuje Zadavatele	Útok viru.

9. Projektové řízení, organizace a harmonogram projektu

Uchazečem navrhované řešení bude respektovat požadavky zadavatele a to zejména s ohledem na co nejvyšší kvalitu a propracovanost metodiky projektového řízení a organizace projektu včetně účinné kontroly a navržených opatření k zajištění cílů projektu, dále na komplexnost a propracovanost navrženého harmonogramu a přístupů pro zajištění realizovatelnosti projektu.

Zhotovitel bude celý projekt implementovat a řídit primárně dle mezinárodně uznávané metodiky IPMA, a dále dle dalších specifických metodik a standardů zohledňující dlouholeté působení uchazeče ve státní správě, které jsou nejvhodnější pro specifické dílčí části plnění tohoto projektu.

9.1. Popis způsobu a metodiky projektového řízení, organizace účastníků projektu

9.1.1. Organizace

Řízení projektu bude založeno na tříúrovňové hierarchii, bude tedy zabezpečeno prostřednictvím tří základních řídicích úrovní.

Nejnižší úrovní řízení jsou **pracovní týmy (PT)**, které jsou ustaveny k plnění konkrétního rozsahu úkolů v předem určených dílčích oblastech. Úkolem pracovních týmů je řešení běžných operativních, výrobních, logistických a dalších záležitostí, kontrola plnění dílčích úkolů dle harmonogramu a vytváření případných zadání požadavků na změnu na základě předložených návrhů. Výstupy z pracovních týmů a záležitosti, které potřebují rozhodnutí vyšší úrovně řízení, včetně požadavků na změnu, se ke schválení předávají na vyšší úroveň řízení a to na **Hlavní tým projektu (HTP)**.

Hlavní tým projektu (HTP) je základní řídicí platformou projektu, která má za úkol zajistit soulad postupu prací na projektu se schváleným věcným a časovým plánem. Hlavní tým projektu zároveň schvaluje všechny požadavky na změnu, financované z prostředků příslušné smlouvy. Nejvyšší strategickou úroveň řízení projektu pak zajišťuje **Řídicí výbor projektu (ŘV)**.

Řídicí výbor projektu (ŘV) řeší na nejvyšší řídicí úrovni zásadní otázky týkající se plnění či neplnění hlavních záměrů projektu jako celku. Zároveň přijímá opatření a definuje další postup v případě krizových stavů v rámci projektu.

Ze všech jednání týmů na všech úrovních jsou odpovědnými osobami dodavatele pořizovány zápisy, které jsou distribuovány k oponentuře všem členům příslušného týmu. Po zapracování připomínek je zápis schválen a uložen.

9.1.2. Struktura a kompetence orgánů řízení projektu

9.1.2.1. Řídící výbor projektu (ŘV)

Nejvyšší strategická úroveň řízení projektu, na které se řeší zásadní otázky týkající se plnění či neplnění hlavních záměrů projektu jako celku, rozhoduje o případech eskalovaných z úrovně HTP, které se nepodařilo vyřešit na nižších úrovních a přijímá opatření a definuje další postup v případě krizových stavů. ŘV zpravidla rozhoduje na základě připravených podkladů vypracovaných hlavním týmem projektu nebo pro tyto účely ustavenými poradními či pracovními skupinami.

ŘV se bude scházet pravidelně nejméně 1x za čtvrtletí. V případě potřeby může podat návrh na svolání mimořádné schůzky ŘV vedoucí projektu objednatele nebo vedoucí projektu dodavatele s uvedením důvodů pro mimořádnou schůzku. Uskutečnění mimořádné schůzky a její termín schvaluje vedoucí projektu objednatele.

Dodavatel navrhuje následující minimální složení ŘV:

- Zástupci objednatele
 - Zástupce vrcholového vedení Objednatele
 - Vedoucí projektu Objednatele
- Zástupci dodavatele
 - Vedoucí projektu dodavatele (Řídící manažer ŘV)
 - Zástupce vedoucího projektu dodavatele
 - Zástupce vrcholového managementu dodavatele

Na jednání ŘV mohou být fakultativně přizváni i další zástupci objednatele a dodavatele dle projednávané problematiky (zástupci odborných útvarů objednatele, garant infrastruktury dodavatele apod.).

9.1.2.2. Hlavní tým projektu (HTP)

Základní řídicí platforma projektu, na které jsou projednávány výstupy z pracovních týmů a záležitosti, které potřebují rozhodnutí vyšší úrovně řízení. Hlavní tým projektu zároveň schvaluje všechny požadavky na změnu, financované z prostředků příslušné smlouvy.

Dodavatel navrhuje následující složení HTP:

- Zástupci objednatele
 - Vedoucí projektu objednatele
 - Zástupci zainteresovaných odborů poskytovatele (vedoucí nebo jimi delegovaní zástupci)
- Odborní garanti odběratele:
 - Garant IS (osoba odpovědná za provoz ICT objednatele)

Garant provozu aplikační vrstvy
Garant bezpečnosti objednatele
atd.

- Zástupci dodavatele
 - Zástupce vedoucího projektu dodavatele (řídící manažer HTP)
 - Vedoucí projektu dodavatele
 - Odborní garanti dodavatele dle časových etap a věcné problematiky:
 - Garant IS
 - Garant provozu
 - Garant bezpečnosti
 - atd.

Jednání HTP se mohou účastnit podle potřeby další zástupci objednatele, a to pravidelně či pouze pro potřeby projednání specifického tématu, avšak vždy se souhlasem vedoucího projektu objednatele. Obdobně se jednání HTP mohou účastnit podle potřeby i další zástupci dodavatele, a to pravidelně či pouze pro potřeby projednání specifického tématu, avšak vždy se souhlasem vedoucího projektu dodavatele nebo zástupce vedoucího projektu poskytovatele.

Jednání HTP se koná pravidelně nejméně 1x za dva týdny.

Pro každé jednání HTP bude připravena ze strany dodavatele agenda; z každého jednání dodavatel zpracuje zápis, který bude po kontrole vedoucím projektu objednatele za obě strany podepsán. Výstupy z jednání budou promítány do další projektové dokumentace.

HTP využívá pro svou práci výstupů činnosti z úrovně pracovních či poradních týmů (PT) nebo jednotlivců.

Minimální agenda pravidelného jednání HTP o stavu projektu bude v rozsahu:

- Projednání a schválení zdroje financování předložených požadavků na změnu (jsou-li předloženy).
- Projednání a odsouhlasení dokumentů/návrhů připravených pracovními týmy.
- Kontrola plnění úkolů – za období od předchozího jednání.

Pokud mají projednávání skutečnosti dopad na celkový časový, finanční nebo věcný rozsah plnění dle smlouvy, je nutné jejich projednání a schválení na ŘV.

9.1.2.3. Pracovní týmy

Pracovní týmy představují nejnížší úroveň řízení a jsou ustaveny k plnění konkrétního rozsahu úkolů v předem určených dílčích oblastech. Úkolem pracovních týmů je řešení běžných provozních záležitostí, kontrola plnění dílčích úkolů dle harmonogramu a vytváření zadání požadavků na změnu na základě předložených návrhů.

Úkolem pracovního týmu je především:

kontrola plnění dílčích úkolů,
řešení běžných provozních problémů,
vytváření a připomínkování dílčích výstupů projektu,
eskalace nestandardních/neplánovaných situací a zjištěných rizik, které vznikly nebo byly identifikovány v průběhu realizace projektu,
vytváření zadání požadavků na změnu, schvalování požadavků na změnu z věcného hlediska, návrh způsobu financování pro požadavky na změnu k předložení na jednání HTP,

- příprava podkladů pro Hlavní tým projektu.

Schůzky pracovního týmu navrhujeme v týdenních intervalech, pokud nebude dohodnuto jinak. Z jednání pracovních týmů bude vždy pořízen zápis, který bude distribuován k připomínkám všem zúčastněným osobám a jiným zainteresovaným stranám.

Dodavatel navrhuje následující složení PT:

Vedoucí pracovního týmu dodavatele

Zástupce vedoucího projektu dodavatele

Dle konkrétní situace delegovaní pracovníci Zadavatele

Na jednání jednotlivých pracovních týmů mohou být fakultativně přizváni další zástupci objednatele a dodavatele dle projednávané problematiky.

9.1.3. Hlavní role projektu

9.1.3.1. Vedoucí projektu objednatele

Vedoucí projektu objednatele je zástupce objednatele, odpovědný za koordinaci činností, spojených s realizací projektu na straně objednatele na úrovni Hlavního týmu projektu.

Zejména se jedná o:

- určení a koordinaci jednotlivých odborných garantů relevantních systémů na straně objednatele,
zajištění součinností na straně objednatele,
- kontrolu přidělených úkolů a odpovědnost za splnění těchto úkolů vůči HTP,
koordinaci časových možností na straně objednatele (řešení časových kolizí s jinými pracovními úkoly),
- koordinaci oponentury jednotlivých výstupů odbornými guaranty na straně objednatele.

Vedoucí projektu objednatele je členem Řídícího výboru a Hlavního týmu projektu. Do pracovního týmu jmenuje svého odpovědného zástupce, odpovědného na úrovni pracovního týmu za koordinaci činností spojených s realizací projektu.

9.1.3.2. Vedoucí projektu dodavatele

Zástupce dodavatele, odpovědný za koordinaci činností spojených s realizací projektu.

Především jde o:

- koordinaci aktivit celého realizačního týmu, včetně podřízených dodavatelů,
- kontrolu přidělených úkolů a odpovědnost za splnění těchto úkolů vůči HTP,
- koordinaci přípravy výstupů k oponentuře.

Vedoucí projektu dodavatele je řídícím manažerem Řídícího výboru a členem Hlavního týmu projektu.

9.1.3.3. Odborný garant IS objednatele

Zástupce objednatele, jmenovaný pro každý podporovaný či implementovaný systém.

V rámci jemu svěřenému systému odpovídá zejména za:

- definici funkčních požadavků,
- posouzení návrhů na změnu systému,
- spolupráci při zpracování zadání požadavku na změnu,
- v rámci pracovního týmu je odpovědný za schválení požadavků na změnu z věcného hlediska,
- přípravu potřebných podkladů a znalostí na schůzku (tj. přípravu na jednání dle avizované agendy schůzky pracovního týmu),
- přípravu a provedení funkčních a následně akceptačních testů dle dodavatelem zpracovaných a objednatelem schválených testovacích scénářů,
- splnění úkolů definovaných na schůzce pracovního týmu v dohodnutém rozsahu a čase.

Účastní se schůzek pracovního týmu, ve výjimečných případech písemně jmenuje svého zástupce na konkrétní schůzku, které se nemůže zúčastnit. Na schůzku si může přizvat potřebný počet spolupracovníků v dané oblasti. Stále je ale jedinou odpovědnou osobou za dohodnuté závěry v rámci jemu svěřené oblasti.

9.1.3.4. Systémový a aplikační architekt

Zástupce dodavatele, který podléhá řízení Vedoucího projektu dodavatele a odpovídá za odborné činnosti a návrh i implementaci řešení v oblasti síťové a aplikační infrastruktury, databází, konsolidace datových zdrojů, serverových farem, operačních systémů, uživatelských rozhraní atd.

9.1.3.5. Garant bezpečnosti dodavatele

Pracovník na této pozici je odpovědný za zajištění procesu řízení bezpečnosti, včetně kontrol, zpracování pravidelných reportů, nezbytné dokumentace apod. V rámci své činnosti spolupracuje s garantem bezpečnosti objednatele, se kterým projednává návrhy na bezpečnostní opatření a spolupracuje při zpracování bezpečnostních auditů. Garant bezpečnosti je dále odpovědný za posuzování aktivit jednotlivých procesů řízení služeb provozu ICT z hlediska jejich vlivu na

bezpečnost, tzn. za identifikaci bezpečnostních rizik, která včas eskaluje na příslušné orgány řízení projektu.

9.1.3.6. Technický specialista dodavatele

Technický specialista je odborným pracovníkem v jednotlivých oblastech realizace projektu (administrátor, analytik, architekt, operátor, konzultant) na straně dodavatele a jeho subdodavatelů. Techničtí specialisté zároveň zastávají role specialistů v jednotlivých procesech implementace a řízení služeb.

9.1.4. Projektová jednání

Rozlišují se následující dva základní typy jednání:

- kontrolní a řídicí jednání (jednání ŘV a HTP),
- pracovní schůzka – jednání pracovního týmu.

Příprava podkladů (rozbor, vypracování návrhu atd.) probíhá výhradně mimo jednání. Zajištění podkladů je vždy povinností toho, kdo jednání vede (v případě HTP je to zpravidla vedoucí projektu dodavatele), aby nedocházelo k prolínání kontrolní a řídicí činnosti s řešením konkrétních pracovních podkladů. U ad-hoc svolaných jednání zajišťuje podklady vždy ten pracovník, který jednání inicioval.

9.1.4.1. Příprava na projektová jednání

Každé jednání musí být připraveno a realizováno minimálně v následujícím rozsahu:

Činnost	Odpovědnosti – ŘV	Odpovědnosti – HTP	Odpovědnosti – PT
Návrh termínu a délky schůzky	Vedoucí projektu objednatele	Vedoucí projektu objednatele	Odborný garant, Vedoucí pracovního týmu (řídicí manažer)
Příprava agendy	Vedoucí projektu dodavatele	Vedoucí projektu dodavatele	Vedoucí pracovního týmu (řídicí manažer)
Zajištění jednací místnosti	Vedoucí projektu objednatele	Vedoucí projektu objednatele	Odborný garant
Osobní příprava na schůzku dle agendy	Vedoucí projektu a přizvání členové	Vedoucí projektu a přizvání členové	Odborný garant, Vedoucí pracovního týmu, členové týmu dle pokynů garanta
Provedení jednání	Vedoucí projektu objednatele, Vedoucí projektu dodavatele a přizvání členové	Vedoucí projektu objednatele, Vedoucí projektu dodavatele a přizvání členové	Odborný garant, Vedoucí pracovního týmu a přizvání členové
Zpracování návrhu zápisu	Vedoucí projektu objednatele	Vedoucí projektu objednatele	Vedoucí pracovního týmu (řídicí manažer)
Oponentura a	Vedoucí projektu objednatele, Vedoucí	Vedoucí projektu objednatele, Vedoucí	Odborný garant, Vedoucí

Činnost	Odpovědnosti – ŘV	Odpovědnosti – HTP	Odpovědnosti – PT
odsouhlasení zápisu	projektu dodavatele	projektu dodavatele	pracovního týmu

9.1.4.2. Oponentura a schvalování zápisů

Z každého jednání připravuje příslušná odpovědná osoba ze strany dodavatele zápis.

V případě Řídícího výboru nebo Pracovního týmu je návrh zápisu zaslán e-mailem odpovědné osobě za stranu objednatele elektronickou poštou k oponentuře a je vyžádáno potvrzení o přečtení této zprávy (případně je u odpovědné osoby ověřeno, že tento zápis obdržela). Objednatel je povinen v dohodnutém termínu se k zápisu vyjádřit nebo jej odsouhlasit zpět e-mailem odesílateli zápisu, který potvrzuje vypořádání připomínek.

Zápis z pracovního týmu se stává platným a závazným již po tomto e-mailovém odsouhlasení nebo po uplynutí lhůty 3 pracovních dnů po odeslání zápisu, pokud nepřišla od odpovědné osoby objednatele zpět žádná reakce (kromě potvrzení přijetí e-mailu). Finální schválení zápisu z Řídícího výboru se provádí podpisem zápisu odpovědnými zástupci za stranu dodavatele objednatele.

V případě možnosti budou zápisy zpracovávány s využitím dataprojektoru tak, že mají možnost se k zápisu v aktuálním čase vyjádřit všechny zúčastněné strany. Zápis je pak podepisován na místě.

Zápisy jsou po schválení uloženy jako součást dokumentace projektu na dokumentačním úložišti zřízeném pro účel centrální evidence dokumentace projektu. Za ukládání a správu zápisů z jednání odpovídá až do aktivace Projektové kanceláře pracovní tým PT ADMIN.

9.2. Šablony projektových dokumentů

Uchazeč bude v rámci plnění předmětu smlouvy po celou dobu trvání projektu aplikovat metodiky a best practices projektového řízení dle standardů IPMA a ISO10.006.

Administraci projektu bude zajišťovat projektová kancelář prostřednictvím projektového manažera. Projektová kancelář umožní přístup oprávněných subjektů řízení projektu k potřebným uloženým informacím o projektu, jako jsou zejména:

- Harmonogram projektu (vzor viz kap.8.8),

- Projektová dokumentace - Analýza, Funkční specifikace, Technická specifikace, Uživatelská, Školící, Administrátorská dokumentace, apod. (dokumenty poskytnuté Zadavatele),

- Projektové výkazy činností,

- Komunikační matice,
Zápisy z jednání projektových týmů (na úrovni řídicího výboru a pracovních skupin),
Zpráva o stavu projektu,
Předávací protokoly,
Akceptační protokoly,
Změnové požadavky,
Testovací protokoly,
- Zpráva o ukončení projektu (předání do provozu).

9.3. Analýza rizik

Riziko je nejistá událost nebo podmínka, která když nastane, ovlivní nepříznivě projekt z pohledu naplnění jeho cílů. Řízení rizik je soubor postupů a nástrojů sloužících k identifikaci rizik, jejich vyhodnocení a přijetí opatření k jejich omezení z pohledu vyhodnocení událostí, které mohou mít nepříznivý vliv na jakékoli události, které jsou předmětem řízení projektu.

Cílem řízení rizik je identifikace a specifikace jednotlivých rizik projektu včetně posouzení jejich dopadů a celkové závažnosti a vymezení vhodných opatření na prevenci daného rizika nebo omezení následků při reálném uplatnění daného rizika. Na základě identifikace a specifikace jsou následně vybraná opatření plánována v rámci projektu.

Některá identifikovaná rizika mohou být záměrně akceptována bez jakýchkoli opatření (nebo jen s omezenými opatřeními) s ohledem na přílišnou (danému riziku neadekvátní) náročnost některých opatření (zejména nároky na časové, finanční a lidské zdroje).

Řízení rizik projektu bude provádět průběžně Vedení projektových týmů a jejich zjištění bude konsolidováno Vedením projektu. Tuto činnost koordinuje Projektový manažer tak, aby se plně prošetřila možná rizika. Zjištěná závažná rizika, jejich dopady a návrhy na jejich řešení či omezení jsou neprodleně předkládány k posouzení a případnému rozhodnutí Řídicímu výboru projektu.

Každý projekt, bez ohledu na velikost, vždy přináší rizika a problémy spojené s jeho realizací. Je nezbytné je rozpoznat a zvládat tak, aby se minimalizovaly škody a maximalizovaly šance na úspěch.

Rizika se hodnotí podle dvou faktorů:

- Pravděpodobnosti, že se něco stane
- Důsledku, jaký bude na projekt mít to, že se to stane

9.3.1. Identifikace rizik

Metodika rozlišuje pro účely řízení rizik dvě základní skupiny:

- **Externí rizika:** rizika působící na projekt z vnějšího prostředí, které je nezávislé na bezprostředních smluvních závazcích, které spolu smluvní strany uzavřely, jejich splnitelnost však může podmiňovat. Možnost ovlivňovat výskyt externích rizik (prevence) je (s ohledem na jejich charakter) velmi omezená. V případě externích rizik jsou dominantní opatření na omezení jejich dopadů.

Interní rizika: rizika projektu mající rámec ve smluvních vztazích mezi smluvními stranami. Výskyt interních rizik je možno do značné míry ovlivnit vzhledem k tomu že přímo souvisí s průběhem a vývojem projektu. V případě interních rizik jsou kombinována opatření na omezení výskytu rizik a opatření na omezení jejich dopadů.

Každé jednotlivé identifikované riziko musí být specifikováno v následujícím rozsahu:

- **Vymezení:** popis rizika a jeho projevů, na jehož základě lze riziko identifikovat,
Dopady: popis možných dopadů rizika na projekt,
Opatření: návrh opatření, která mohou riziko vyloučit nebo podstatně omezit jeho působení a dopady,
Závažnost: určení aktuální míry ohrožení projektu daným rizikem, která je posouzena a stanovena na základě aktuální pravděpodobnosti výskytu rizika a na základě aktuální závažnosti potenciálních dopadů rizika do projektu. Zejména závažnost rizik ve škále Nízká / Střední / Vysoká je nutné přehodnocovat průběžně.

Analýza rizik bude dále prováděna na úrovni vedení projektových týmů a koordinována na úrovni vedení projektu průběžně vzhledem k tomu, že rizika projektu se mohou měnit jak co do struktury (vznik a zánik rizik), tak do povahy existujících rizik (změna specifikace rizik a to zejména aktuální závažnosti).

V průběhu projektu bude nutné rizika přehodnocovat zejména v případech přechodu mezi jednotlivými fázemi realizace projektu.

Každý člen projektového týmu je povinen neprodleně informovat nadřízeného vedoucího projektového týmu o skutečnostech, které mohou reálně negativně ovlivnit projekt. Každý vedoucí projektového týmu je povinen neprodleně zvážit informace o skutečnostech, které mohou reálně negativně ovlivnit projekt a vyhodnotí-li je jako riziko projektu, pak o tomto riziku neprodleně informovat vedoucí projektového týmu. Vedení projektu je povinno zvážit dané riziko a informovat o něm Řídící výbor projektu.

Každé jednotlivé identifikované riziko musí být vedením projektu specifikováno ve výše uvedeném rozsahu. V případě závažných rizik projektu ovlivňujících rámec projektu daný smluvní dokumentací nebo zásadně ovlivňující organizaci Zadavatele musí být Řídící výbor projektu informován neprodleně.

Za výkon identifikace rizik odpovídají všechny zainteresované strany v projektu, tj. včetně všech členů projektového týmu Dodavatele a Zadavatele. Projektový manažer udržuje celkový "Registr rizik" projektu.

9.3.2. Hodnocení rizik

Hodnocení rizik rozdělujeme následujícím způsobem na:

- Kvantitativní

- Určíme pravděpodobnost a hodnotu ztráty, vytvoříme součin jehož hodnota je vyjádřena v peněžních jednotkách.
- Kvalitativní
 - Dopad a pravděpodobnost se určí verbálně (velký, malý apod.) nebo s pomocí bodovací stupnice bez peněžního významu. Tato metoda slouží k určení priority rizik.

Tato tabulka je finálním produktem identifikační části analýzy a následuje finální analytická činnost představující zatřídění rizik do jednotlivých tříd.

V praxi vypadá hodnocení rizik ze strany uchazeče následujícím způsobem. Tato tabulka je také součástí registru rizik:

Riziko	Garant	Pravděpodobnost [%]	Potenciál poškození	Důležitost	Pořadí	Opatření proti riziku
Riziko1	Garant1	10	10	100	3.	Opatření1
Riziko2	Garant2	30	5	150	1.	Opatření2
Riziko3	Garant3	15	8	120	2.	Opatření3
Riziko4	Garant3	5	2	10	4.	Opatření4
...						

Ve výše uvedené tabulce si pro každý faktor rizika (riziko) určíme:

- Pravděpodobnost výskytu rizika (Pravděpodobnost) a to v hodnotách od 0 až do 100%
- Potenciál poškození a to například v hodnotách od 1 (nejmenší) až 10 (největší)
- Míru důležitosti (Důležitost) poté vypočítáme jako součin hodnot Pravděpodobnost krát (*) Potenciál poškození

Následně z těchto hodnot určíme pořadí rizik podle důležitosti a vybereme rizika, která zařadíme do plánu rizik

9.3.3. Opatření na eliminaci rizik

V rámci opatření rizik bude uchazeč používat dále současně preventivní (proaktivní) následný (reaktivní) přístup k odezvě na riziko:

- **Proaktivní přístup** (prevence vzniku této situace)
 - Identifikace, eliminace a řízení rizik
 - Identifikace rizik
 - Vytvoření rizikové analýzy
 - Vytvoření mechanismu hodnocení rizik
 - Určení výše dopadu a pravděpodobnosti vzniku rizik
 - Eliminace rizik
 - Vyloučení rizika – zákaz vybraných rizikových aktivit a procesů
 - Snížení rizika – snížení velikosti dopadu např. pojištěním rizika

- Přenos rizika – redukce rizika snížením pravděpodobnosti nežádoucích událostí
- Přijetí rizika – akceptace rizika na stávající úrovni bez dalších aktivit
- Uplatňování zásad projektové řízení, správné nastavení úrovně řízení projektu, pravidelný Řídící výbor projektu, ustanovení sponzora projektu
 - Kontrolní den na měsíční bázi
 - Pravidelný reporting a průběžné sledování požadavků uživatelů v HelpDeskovém systému zadavatele
 - Využití projektových a procesních manažerů uchazeče disponujících mezinárodně uznávanými certifikacemi ITILv3, ISO 10.006 a IPMA
- Uplatňování zásad procesního řízení (ITIL)
- Řízení subdodavatelů a řízení kvality
- Pojištění – tento nástroj řešení rizik v sobě zahrnuje aktivní složku prevence, tj. minimalizace ztrát v případě výskytu rizika
- **Reaktivní přístup** (řešení situace až v případě vzniku rizika s cílem minimalizovat dopady). Uchazeč bude reagovat průběžně s ohledem na aktuální vývoj výskytu vybraných rizik v rámci projektu, které nelze řešit proaktivně a to např. z důvodu neekonomičnosti (tj. neúměrně vysokých nákladů na eliminaci těchto rizik), atd.

Když byla vyhodnocena pravděpodobnost a dopady každého rizika, je potřeba konkrétně naplánovat, jak se na dané riziko bude reagovat. Reakce na rizika má buď snížit jejich pravděpodobnost nebo omezit jejich nepříznivé důsledky, ev. oboje. Reakce na rizika v projektu mohou být následující:

- Akceptace – nebude se dělat nic. Znamená to, že projekt dané riziko toleruje, s tím, že pokud by se naplnilo, zvládnou se případné důsledky pomocí zavedených postupů.
- Ošetření rizika – naplánují se a provedou opatření snižující pravděpodobnost naplnění daného rizika. Například se naplánuje nějaká rezerva nebo dodatečné zdroje.
Přenesení rizika – speciální forma snížení rizika, při níž se důsledky daného rizika převedou na nějakou třetí stranu. Například se použije penále vůči dodavateli.
- Ukončení činnosti, z níž dané riziko vyplývá. Jinými slovy taková změna rozsahu projektu, že se možnost naplnění rizika vyloučí.

Vedle zřejmých negativních efektů rizik mohou někdy z nejistoty vyplývat i pozitivní příležitosti. Hledání příležitostí vyžaduje uvažovat i o věcech, u kterých nebyla zjištěna žádná rizika.

Řízení rizik tedy znamená:

Přidělení rizika konkrétní osobě (vlastníkovi), zodpovídající pak za schválené (re)akce

Hodnocení výsledků, které provedené akce přinesly

Opakované vyhodnocování rizik a rozhodování o případných dalších opatřeních

Kontrola toho, jestli neexistují ještě další, zatím neidentifikovaná rizika (příležitosti)

Veškeré informace o rizicích a plánovaných i provedených opatřeních se zaznamenávají do Evidence rizik.

1

- Specifikace rozsahu integrace se spisovou službou v kontextu jednotlivých funkčních akcí jednotlivých systémů (IPPD, číselníky, Evidence případů, Kontroly+ Stížnosti petice podněty, Exekuce insolvence, Evidence soudních sporů, Správa pohledávek, Evidence smluv) které požadavky POD001-015 budou uvažovány, není-li to nějakým požadavkem u některého ISu explicitně uvedeno a dalších obdobných obecných požadavků pro svázání s konkrétními systémy.

Specifikace a určení (pracovním příkazem) konkrétních osob (garantů, klíčových uživatelů, administrátorů – obecně řešitelského týmu ze strany Objednatele) a jejich termínových dispozic (zejména pro Návrh realizace a prototyp a všechna akceptační řízení) v souladu s harmonogramem projektu tak, aby jejich termíny dostupnosti (minimálně v rozsahu garantovaném v ZD bez ohledu na jiné smluvní závazky Objednavatele) neohrožovaly realizaci dle závazného harmonogramu i při vynaložení veškeré námahy, kterou lze po Poskytovateli spravedlivě požadovat, na minimalizaci následných prací na práci těchto konkrétních osob navazující; tyto osoby musejí být schopny pokrýt ať už svojí rolí či znalostmi všechny řešené scénáře a reprezentovat (lze i znalostí a časovými možnostmi např. pro akceptační testování) všechny uživatelské role identifikovatelné v systému.

- Během analýzy dostatečné množství prostor pro jednotlivá jednání s garanty/klíčovými osobami/administrátory, kde lze i v jednotlivých kancelářích, kuloárních místech atp., kde jediným požadavkem pro takové prostory je k dispozici přiměřené pracovní prostředí vyhovující přiměřeně účelu (např. vybavené přiměřeným nábytkem a přístupnými zásuvkami 230V), délce a rozsahu jednání v souladu zejména s předpisy zák. č. 309/2006 Sb., 258/2000 Sb., NV č. 148/2006 Sb., NV č. 361/2007 Sb. a navazujících v platném znění.

10.2. Analýza a návrh – SAN002 Model

- Specifikace a určení (pracovním příkazem) konkrétních osob (garantů, klíčových uživatelů, administrátorů – obecně řešitelského týmu ze strany Objednatele) a jejich termínových dispozic (zejména pro Návrh realizace a prototyp a všechna akceptační řízení) v souladu s harmonogramem projektu tak, aby jejich termíny dostupnosti (minimálně v rozsahu garantovaném v ZD bez ohledu na jiné smluvní závazky Objednavatele) neohrožovaly realizaci dle závazného harmonogramu i při vynaložení veškeré námahy, kterou lze po Poskytovateli spravedlivě požadovat, na minimalizaci následných prací na práci těchto

konkrétních osob navazujících; tyto osoby musejí být schopny pokrýt ať už svojí rolí či znalostmi všechny řešené scénáře a reprezentovat (lze i znalostí a časovými možnostmi např. pro akceptační testování) všechny uživatelské role identifikovatelné v systému a schopné zpracovávat analytické výstupy projektu v rozsahu definovaném v požadavcích DOC005 a DOC006 a v rozsahu logických propojů a návazností mezi jednotlivými součástmi řešení (po věcné stránce jejich odbornosti, netýká se technických záležitostí, pokud takové znalosti nejsou očekávatelné z hlediska jejich pracovních rolí, náplně práce či určení v projektu a to podle § 5 zák. č. 89/2012 Občanský zákoník).

10.3. Testování – SST001 Akceptační testy

- Specifikace věcných případů jednotlivých případů užití akceptačních testů jako podkladu pro TES001 nejpozději v průběhu analytických prací.
- Provedení akceptačních testů v souladu s TES002 a harmonogramem projektu.
- Vyhotovení protokolu o výsledcích s specifikací:
 - Identifikace selhalých testů
 - Dokumentace zadaných dat (bylo-li to možností skriptu) a postupu tak, aby byla chyba replikovatelná
 - Identifikace a dokumentace ostatních rozhodných skutečností (např.: logy komunikace prohlížeče, výstupy z konzole atp.)
- Zajištění dostupnosti a přístupu do všech produkčních či testovacích prostředí (dle relevantnosti a realizovatelnosti testů nad tím či oním prostředím) integrovaných systémů jménem OVM Objednatele.
- Zajištění již produkční verze související infrastruktury i pro nasazení prototypů.

10.4. Testování – SST002 Zátěžové testy

- Součinnost z pozice zákazníka třetí strany provádějící bezpečnostní testy.
- Zajištění již produkční verze související infrastruktury

10.5. Testování – SST003 Bezpečnostní testy

- Specifikace všech přístupových oprávnění dle charakteru všech takto řízených entit/položek pro všechny skupiny/role bezpečnostního modelu.
- Zajištění již produkční verze související infrastruktury (Active directory, použité certifikáty atp.)
- Součinnost z pozice zákazníka třetí strany provádějící bezpečnostní testy.

10.6. Migrace – SIG001 Struktura dat

- Validace Návrhu realizace – datové struktury proti stávající datové struktuře, řešení nesrovnalostí (v souladu s požadavky na migraci dat, tj. evaluace zda ta či ona entita/atribut může a za jakých podmínek splnit problematiku zkreslení, ztráty či duplikace).
- Určení osob vyhovujícím SAN001-SAN002 v rozsahu přiměřeném danému účelu pro poskytnutí té součinnosti, která je pro migraci nezbytná.

10.7. Migrace – SIG002 Forma dat

- Předání dat v takové formě, aby její zpracování neohrozilo harmonogram projektu dle Smlouvy a jejích Příloh.

10.8. Migrace – SIG003 Datový vzorek

- Předání datového vzorku nejpozději v termínu specifikovaném v harmonogramu pro iniciální migraci, včetně jeho dokumentace, konzultace

při nejasnostech stran této specifikace a dokumentace, zejména s ohledem na význam hodnot a designu a volby řešení jednotlivých tříd (druhů) neintegrit a chyb v datech.

- Předání základní přehledové dokumentace (entity, atributy, počty záznamů) pro získání přehledu strukturní a obsahové mohutnosti dat.

10.9. Migrace - SIG004 Produkční data

Specifikace technologického způsobu předání produkčních dat již v době analýzy.

10.10. Nasazení – SAS001 Výpočetní platforma

Náš návrh vychází z předpokladu, že prostředí bude provozováno ve virtuálním prostředí, kdy pro každou roli systému bude separátní sada VMs – Databázové servery a aplikační servery v jednotlivých clusterech, tak jak naznačuje náčrt jednotlivých prostředí. Dále se předpokládá, že pro management Hyper-V prostředí Objednatel využívá Microsoft Systém Center Virtual Machine Manager (SC VMM), pomocí kterého bude možné provádět management a některé speciální úkony, jako je klonování VMs, snapshoting, ... Detailní rozpad/náčrt potřeby konfigurací jednotlivých prostředí, včetně síťové infrastruktury bude součástí předimplementační studie.

10.11. Nasazení - SAS002 Konfigurace

Každé z prostředí v našem návrhu bude vyžadovat následující konfigurace = přidělené zdroje, na každé z lokalit, tak jak je definováno níže:

Produkční prostředí + záložní produkční prostředí

Role	Počet vCPU 2,4GHz	RAM	HDD OS GB	HDD Data GB	HDD Archiv TB	Licenc e OS	Licence SQL Core	poznámka	umístění
SQL 1	16	96	60	1024	8	1	16	Aktivní instance pro produkce	produkční lokalita
SQL 2	16	96	60	1024	8	1	16	Aktivní instance pro záložní produkce	záložní lokalita
APP IPPD 1	16	32	60	100	0	1	0	Aktivní instance pro produkce	produkční lokalita
APP IPPD 2	16	32	60	100	0	1	0	Aktivní instance pro záložní produkce	záložní lokalita
APP XML 1	12	32	60	100	0	1	0	Aktivní instance pro produkce	produkční lokalita
APP XML 2	12	32	60	100	0	1	0	Aktivní instance pro záložní produkce	záložní lokalita

APP Právní Agendy 1	12	32	60	100	0	1	Aktivní instance pro 0 produkce	produkční lokalita
APP Právní Agendy 2	12	32	60	100	0	1	Aktivní instance pro 0 záložní produkce	záložní lokalita

Testovací prostředí

Role	Počet vCPU 2,4GHz	RA M	HDD OS GB	HDD Data GB	HDD Archiv TB	Licence OS	Licence SQL Core	pozná mka	umístění
SQL 1		8 96	60	1024	8	1	8	Aktivní	produkční lokalita
SQL 2		8 96	60			1		Pasivní	produkční lokalita
APP IPPD 1	4	8	60	100	0	1	0	Aktivní	produkční lokalita
APP IPPD 2	4	8	60		0	1	0	Pasivní	produkční lokalita
APP XML 1	4	8	60	100	0	1	0	Aktivní	produkční lokalita
APP XML 2	4	8	60		0	1	0	Pasivní	produkční lokalita
APP Právní Agendy 1	4	8	60	100	0	1	0	Aktivní	produkční lokalita
APP Právní Agendy 2	4	8	60		0	1	0	Pasivní	produkční lokalita

Pomocné testovací prostředí

Role	Počet vCPU 2,4GHz	RA M	HDD OS GB	HDD Data GB	HDD Archiv TB	Licence OS	Licence SQL Core	pozná mka	umístění
SQL 1		8 96	60	1024	8	1	8	Aktivní	záložní lokalita
SQL 2		8 96	60			1		Pasivní	záložní lokalita

APP IPPD 1	4	8	60	100	0	1	0	Aktivní	záložní lokalita
APP IPPD 2	4	8	60		0	1	0	Pasivní	záložní lokalita
APP XML 1	4	8	60		0	1	0	Aktivní	záložní lokalita
APP XML 2	4	8	60		0	1	0	Pasivní	záložní lokalita
APP Právní Agendy 1	4	8	60		0	1	0	Aktivní	záložní lokalita
APP Právní Agendy 2	4	8	60		0	1	0	Pasivní	záložní lokalita

Vývojové prostředí

Role	Počet vCPU 2,4GHz	RAM	HDD OS GB	HDD Data GB	HDD Archiv TB	Licence OS	Licence SQL Core	poznámka	umístění
SQL 1	4	96	60	1024	4	1	4	Aktivní	záložní lokalita
SQL 2	4	96	60			1		Pasivní	záložní lokalita
APP IPPD 1	4	8	60	100	0	1	0	Aktivní	záložní lokalita
APP IPPD 2	4	8	60		0	1	0	Pasivní	záložní lokalita
APP XML 1	4	8	60		0	1	0	Aktivní	záložní lokalita
APP XML 2	4	8	60		0	1	0	Pasivní	záložní lokalita
APP Právní Agendy 1	4	8	60		0	1	0	Aktivní	záložní lokalita
APP Právní Agendy 2	4	8	60		0	1	0	Pasivní	záložní lokalita

Předpokládáme vytvoření jedné standardizované image OS Windows Server, dle potřeb vyvíjené aplikace a dle standardů Objednatele. Ta bude následně klonována pomocí SC VMM, z důvodu maximálního ušetření času během nasazení/implementace a zároveň dosažení minimálního roztržštění výsledného prostředí.

10.12. Nasazení SAS003 Prostředí

Za produkční prostředí považujeme:

- Primární produkční prostředí (v primární lokalitě)

Za testovací prostředí považujeme

- Testovací prostředí
- Pomocné testovací prostředí
- Vývojové prostředí

Za dočasné prostředí pro provádění integračních a zátěžových testů považujeme:

- Záložní produkční prostředí (v sekundární lokalitě), které pak bude sloužit jako DR prostředí pro Primární produkční prostředí
- Dále za něj lze považovat dočasně i Vývojové + Testovací + Pomocné testovací prostředí

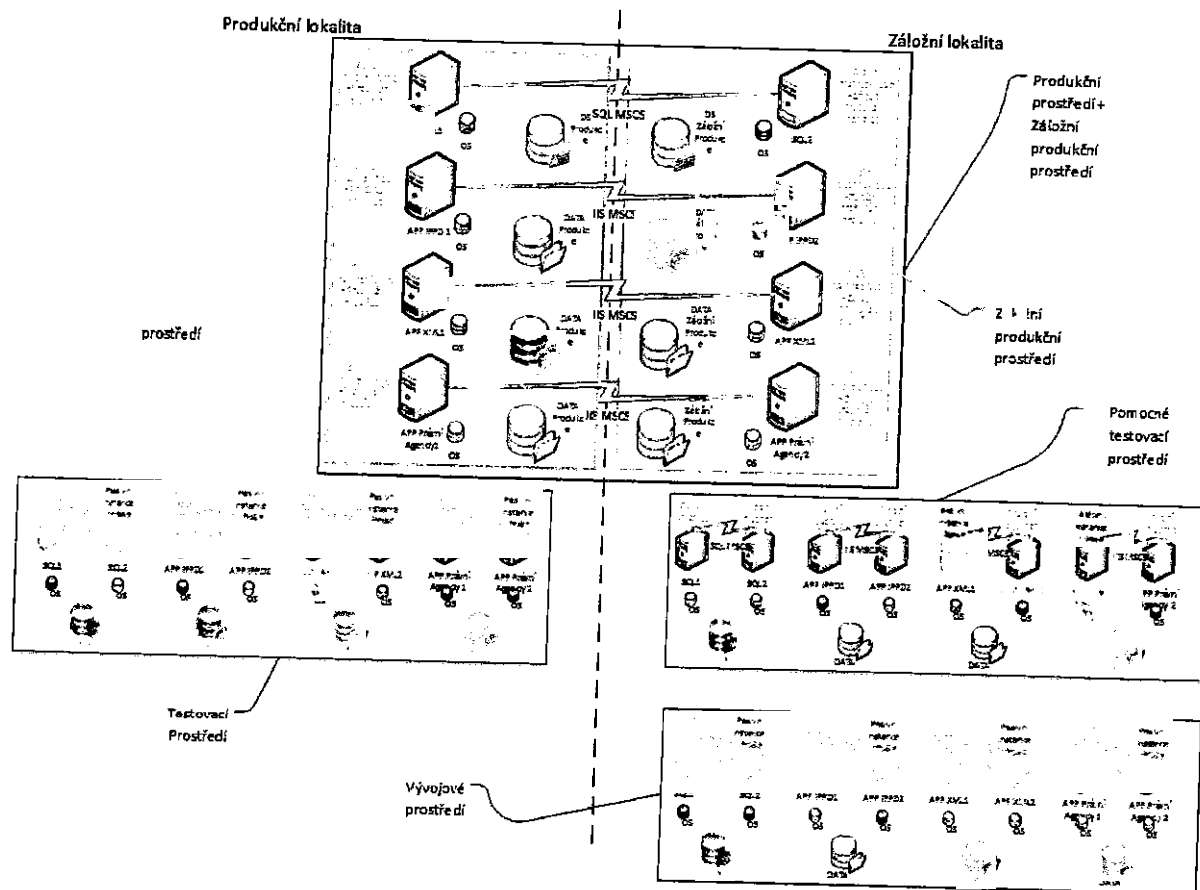
10.13. Nasazení – SAS004 Sítě a komunikace

Předpokládáme využití LAN a WAN Objednatele pro využití připojení systémů směrem k konzumentům služeb – tedy kontaktním pracovištím a krajským pobočkám. Detailní rozpad/nákres potřeby konfigurací jednotlivých prostředí, včetně síťové infrastruktury, v návaznosti na konzumenty služeb, bude součástí předimplementační studie.

10.14. Nasazení – SAS005 Redundance

Redundanci, v rámci našeho návrhu, předpokládáme zajistit pomocí aplikačních a databázových clusterů, které budou umístěny v obou lokalitách, tzn. jak v primární, tak záložní lokalitě. Z nákresu našeho návrhu je patrné, jak budou jednotlivé systémy rozmístěny přes obě lokality.

Nákres umístění systémů vůči lokalitám



10.15. Školení - SSK001 Školící prostory

- Disponuje-li Objednatel školícími prostorami vhodnými pro jím požadované či v Návrhu realizace projektu naplánované školení, včetně odpovídajícího vybavení, je požadováno jejich poskytnutí (je-li to s ohledem na jiné účely použití Objednatelem a harmonogram obsazenosti daných prostor možné). Takové poskytnutí prostor nezakládá ani v případě bezplatného poskytnutí nárok na slevu z těch částí plnění, týkajících se školení či ve kterých by bylo lze očekávat náklady nutné k vynaložení zajištění takových prostor mimo kooperaci s Objednatelem.

10.16. Školení – SSK002 Velikost a vybavení

- Je pokryto otázkou vhodnosti dle SSK001

10.17. Školení – SSK003 Termíny

- Nařízení zaměstnancům dostavit se k závazným termínům, řešení náhradních termínů s Poskytovatelem
- Maximalizace efektivity při konsolidaci harmonogramů školení pro minimalizaci cestovních nákladů Zhotovitele (maximalizace počtů školených osob geografické lokalitě a daného tématu k danému termínu)
- Aktivní spolupráci při následném řešení absencí.

10.18. Projektové řízení – SPR001 Kanceláře

- Kancelářské prostory pro nejméně 1/2 (poloviční) množství osob, které odpovídají počtu pracovních rolí požadovaných Objednatelem a počtu osob na ně Poskytovatelem dle závazných dokumentů alokovaných. Údaj o polovičním

množství neplatí v průběhu fází analýzy a návrhu prototypu. Není ani požadována alokace na jednom fyzickém místě, kapacity jednotlivých místností jsou naopak ponechány v kompetenci Objednatele v souladu s dislokací na úrovni krajských jednotek pracovišť jednotlivých osob určených dle SAN001 a SAN002.

- Kancelářské prostory musí poskytovat přiměřené pracovní prostředí vyhovující přiměřeně účelu (např. vybavené přiměřeným nábytkem a přístupnými zásuvkami 230V), zejména s předpisy zák. č. 309/2006 Sb., 258/2000 Sb., NV č. 148/2006 Sb., NV č. 361/2007 Sb. a navazujících v platném znění.
- Nezávislý přístup Poskytovatele do těchto prostor (pouze v souladu s bezpečnostní politikou a pravidly ostrahy objektu, ovšem tak, aby nebyl přístup závislý na konkrétních pracovnících pracovních týmů Objednatele, je samozřejmě přípustná „závislost“ na pracovnících ostrahy) v režimu nejméně 24x7 během fází dodání díla a nejméně 16x5 v průběhu poskytování služeb podpory provozu, kde v průběhu poskytování služeb podpory provozu musí být možný (v takovém případě i závislý) přístup – bude-li to charakter technické intervence vyžadovat – v souladu s režimy jednotlivých katalogových listů služeb podpory provozu.

10.19. Projektové řízení – SPR002 Připojení k síti Internet

- Jedná se o požadavek na připojení k Internetu pouze pro kancelářské prostory trvalého charakteru, zpravidla v sídle Objednatele nebo tam, kde bude objednatel vyžadovat dlouhodobější pravidelnou přítomnost Poskytovatele. Připojením se rozumí nejméně jedno spojení UTP s RJ45 (zásuvka či kabel) s veřejně přidělenou IP adresou bez omezení firewallem. Není-li to možné (veřejná IP, bez omezení firewallem), je pak požadována alokace a součinnost osob za toto spojení odpovědných pro libovolné požadavky Poskytovatele v průběhu celé doby využití kanceláři pro provedení nastavení nebo řešení požadavku Poskytovatele tak, aby byly realizovány (samozřejmě je jejich realizace v souladu s bezpečnostní politikou Objednatele). Je požadováno, aby takové řešení vždy umožnilo připojení vlastních prostředků (routery/WiFi access pointy/Switche). Pokud by bezpečnostní politika Objednatele nedovolovala připojení bezdrátovými technologiemi v daném místě, jsou požadovány zásuvkové nebo kabelové přípoje s koncovkami RJ45 v minimálním počtu ½ kapacity dané místnosti.

10.20. Projektové řízení – SPR003 Zasedací místnost

Kancelářské prostory pro nejméně ½ (poloviční) množství osob, které odpovídají počtu pracovních rolí požadovaných Objednatelem a počtu osob na ně Poskytovatelem dle závazných dokumentů alokovaných. Údaj o polovičním množství neplatí v průběhu fází analýzy a návrhu prototypu. Není ani požadována alokace na jednom fyzickém místě, kapacity jednotlivých místností jsou naopak ponechány v kompetenci Objednatele v souladu s dislokací na úrovni krajských jednotek pracovišť jednotlivých osob určených dle SAN001 a SAN002.

Kancelářské prostory musí poskytovat přiměřené pracovní prostředí vyhovující přiměřeně účelu (např. vybavené přiměřeným nábytkem a přístupnými

zásuvkami 230V) a charakteru délce jednání, zejména s předpisy zák. č. 309/2006 Sb., 258/2000 Sb., NV č. 148/2006 Sb., NV č. 361/2007 Sb. a navazujících v platném znění a poskytovat internetovou konektivitu dle SPRO02.

11. Poznámky:

Uvádí-li Poskytovatel kdekoli v jakémkoliv dokumentu souvisejícím s tímto výběrovým řízením či Smlouvou v nějaké konkrétní technické věci alternativní možnosti řešení, jedná se vždy o takové alternativy, které v dané věci Poskytovatel jako kvalifikovaný uchazeč ze svých zkušeností a pro splnění požadavku postupování s maximální odbornou péčí, kterou po něm lze požadovat, musí uvažovat a Objednateli v návaznosti na charakter specifikace jeho požadavků v té věci nabídnout (či byly dokonce Objednatel přímo vyžadovány), a které, s ohledem na svůj charakter nemají vliv na cenu či kvalifikaci nabídky ani jinak neovlivňují validitu plnění předmětu zakázky dle této Smlouvy a to bez ohledu na konečnou volbu jejich konkrétního provedení, a tedy NEpředstavují varianty ve smyslu § 70 a souvisejících zákona č. 137/2006 Sb. o veřejných zakázkách v platném znění a jsou tak plně v souladu s požadavkem kapitoly „4. POŽADAVKY NA VARIANTY NABÍDKY“ Zadávací dokumentace, která variantní řešení nabídky nepřipouští.