

# Cloud Ministerstva vnútra SR

## *Typ 3 štúdie uskutočniteľnosti.*

*Štúdia zameraná na cloudové služby typu IaaS.*

## Obsah

1	Základné informácie	1
1.1	Prehľad	1
1.2	Dôvod	2
1.3	Rozsah	2
1.4	Použité skratky a značky	2
2	Manažérske zhrnutie	5
2.1	Motivácia	7
2.2	Popis aktuálneho stavu	8
2.2.1	Legislatíva	8
2.2.2	Architektúra	9
2.2.3	Prevádzka	12
2.3	Alternatívne riešenia	14
2.3.1	Alternatíva A – „Konzervatívna“	14
2.3.2	Alternatíva B – „Hybridné riešenie“	14
2.3.3	Alternatíva C – „Cloud riešenie“	15
2.4	Popis budúceho stavu	16
2.4.1	Legislatíva	16
2.4.2	Architektúra	16
2.4.3	Prevádzka	26
2.4.4	Ekonomická analýza	27

## Zoznam obrázkov

No table of figures entries found.

## Zoznam tabuliek

Tabuľka 1 Základné informácie - zhrnutie .....	1
Tabuľka 2 Skratky a značky .....	2
Tabuľka 3 Motivácia – budúci stav .....	7
Tabuľka 4 Legislatíva – aktuálny stav .....	8
Tabuľka 5 Biznis architektúra - aktuálny stav .....	9
Tabuľka 6 Architektúra informačných systémov - aktuálny stav .....	9
Tabuľka 7 Technologická architektúra - aktuálny stav .....	10
Tabuľka 8 Bezpečnostná architektúra - aktuálny stav .....	11
Tabuľka 9 Prevádzka - aktuálny stav .....	12
Tabuľka 10 Legislatíva - budúci stav .....	16
Tabuľka 11 Biznis architektúra – budúci stav .....	16
Tabuľka 12 Architektúra informačných systémov - budúci stav .....	18
Tabuľka 13 Technologická architektúra - budúci stav .....	19
Tabuľka 14 Implementácia a migrácia .....	21
Tabuľka 15 Bezpečnostná architektúra - budúci stav .....	23
Tabuľka 16 Prevádzka - budúci stav .....	26
Tabuľka 17 Ekonomická analýza - budúci stav .....	27
Tabuľka 18: Prehľad ukazovateľov efektivity .....	27
Tabuľka 19: Prehľad nákladov a prínosov .....	28

# 1 Základné informácie

## 1.1 Prehľad

Tabuľka 1 Základné informácie - zhrnutie

Zdôvodnenie využitia národného projektu a vylúčenia výberu projektu prostredníctvom výzvy	
<p>Predkladaná štúdia je štúdiou uskutočniteľnosti pre nové programové obdobie 2014 až 2020 pre Operačný program Integrovaná infraštruktúra, Prioritná os číslo 7 Informačná spoločnosť.</p> <p>Dokument vychádza z materiálu „Návrh centralizácie a rozvoja dátových centier v štátnej správe“, číslo materiálu: UV-21676/2014, schválený vládou SR uznesením číslo 247/2014, ktorý bol spracovaný na základe úlohy B.1 uznesenia vlády SR č. 680 z 27.11.2013, ktorým vláda SR schválila správu zo zasadnutia Európskej rady konanej v Bruseli 24. - 25. októbra 2013 a nadväzuje na štúdiu „IKT infraštruktúra pre IaaS časť 1.“ vypracovanej pre Ministerstvo financií SR, ktorej primárnym cieľom bolo posúdenie uskutočniteľnosti vybudovania riešenia poskytujúceho úvodné portfólio cloudových služieb nadrezortných dátových centier.</p> <p>Uvedená štúdia špecifikovala riešenie Dátového centra v pôsobnosti dvoch organizácií – DataCentrum a Ministerstvo vnútra SR.</p> <p>V rámci projektu na ktorý sa vzťahuje táto štúdia budú realizované aktivity, ktoré sú nevyhnutné na dosiahnutie cieľa, pričom tieto vychádzajú z metodiky riadenia projektov pre implementáciu infraštruktúrnych riešení (analýza a dizajn, implementácia, testovanie a nasadenie, dodávka HW a SW) a podporných aktivít nevyhnutných pre riadenie projektu a PR súvisiace s realizáciou projektov financovaných z prostriedkov ŠF.</p>	
Prijímateľ/partner národného projektu a dôvod jeho určenia	
<p>Predmetom štúdie Cloud ministerstva vnútra je projekt „IKT pre IaaS, 2.časť“ ktorý má zabezpečiť druhú časť informačnej a komunikačnej infraštruktúry pre rozšírenie cloudových služieb resp. služieb Infrastructure as a Service (IaaS), ktoré budú tvoriť portfólio cloudových služieb nadrezortných dátových centier.</p> <p>V zmysle vyššie uvedenej schválenej štúdie Dátové centrum pre eGovernment (13.5.2013) je prijímateľom navrhovaného národného projektu IKT pre IaaS, 2.časť Ministerstvo vnútra SR a partnerom Ministerstvo financií SR. Tu pomenované partnerstvo vyplýva z celkovej koncepcie riešenia Dátového centra pre eGovernment, realizačne však MF SR zabezpečuje relevantnú časť riešenia samostatným projektom (IKT pre IaaS, 1.časť). Implementácia národného projektu IKT pre IaaS, 2.časť bude len u prijímateľa Ministerstvo vnútra SR v lokalite mimo BSK.</p>	
Kritéria kvality	Spresnenie kritérií kvality: Odkazy na relevantné identifikátory kritérií kvality v prílohe Kritéria kvality.
Q01 - Kvalita vstupných informácií Q02 - Komplexnosť spracovania Q03 - Zohľadnenie rizikových faktorov Q04 - Vecnosť Q05 - Súlad s požadovanými štandardmi pre tvorbu štúdií uskutočniteľnosti Q06 - Dôraz na kvalitatívne kritéria Q07 - Dôsledné spracovanie príloh Q08 - Relevantnosť spracovaných príloh Q09 - Komplexnosť spracovania	
Príslušnosť národného projektu k relevantnej časti PO7 OPII	<p>Národný projekt „Cloud Ministerstva vnútra SR patrí do Prioritnej osi 7 Informačná spoločnosť,</p> <p>INVESTIČNÁ PRIORITA 2c): Posilnenie aplikácií IKT v rámci elektronickej štátnej správy, elektronickeho vzdelávania, elektronickej inklúzie, elektronickej kultúry a elektronickeho zdravotníctva</p>

	ŠPECIFICKÝ CIEL 7.8: Racionalizácia prevádzky informačných systémov pomocou eGovernment cloudu
Indikatívna výška finančných prostriedkov určených na realizáciu národného projektu	44 402 288,40 Eur s DPH <sup>1</sup>

<sup>1</sup> Na prepočet bol použitý kurz USD k 30.6.2015 zo stránky [www.nbs.sk](http://www.nbs.sk) – 1,1189

## 1.2 Dôvod

Cieľom štúdie je posúdenie uskutočniteľnosti projektu „Cloud Ministerstva vnútra SR.“ Predmetom tohto projektu je zabezpečiť **druhú časť** informačnej a komunikačnej infraštruktúry pre vybudovanie cloudovej služby resp. služieb Infrastructure as a Service (IaaS), ktoré budú tvoriť portfólio cloudových služieb nadrezortných dátových centier. Prvá časť (IKT infraštruktúra pre IaaS časť 1) bola realizovaná v novovybudovanom nadrezortnom dátovom centre Ministerstva financií SR. Dátové centrum MV SR a MF SR si budú vzájomne poskytovať geograficky oddelenú záložnú lokalitu, kde bude možné v krátkom čase obnoviť požadovanú prevádzku.

Projekt vytvorí podmienky a predpoklady na znižovanie nákladov na verejnú správu, nakoľko zabezpečí unifikáciu prostredia pre prevádzku informačných systémov poskytujúcich eGovernment služby, optimalizuje využitie zdrojov, zníži obstarávacie a prevádzkové náklady a zvýši efektivitu manažmentu na všetkých úrovniach od prevádzky infraštruktúry až po manažment vzťahov.

## 1.3 Rozsah

Predmetom „Cloud Ministerstva vnútra SR.“, bude vybudovanie riešenia poskytujúceho IaaS služby. Budovanie cloudových služieb prevádzkovaných v nadrezortných dátových centrách je komplexná a časovo náročná úloha a preto sú budované v iteráciách.

Prvá časť riešenia IaaS vytvorila iniciálne prostredie umiestnené v novovybudovanom nadrezortnom dátovom centre Ministerstva financií SR, ktoré je primárne určené pre nové projekty informačných systémov prevádzkované vo vládnom cloude. Iniciálne prostredie umožnilo „proof of concept (PoC)“ pre nadrezortný cloud, definovanie technologických štandardov a prevádzkových procesov, poskytujúce vysoko dostupné škálovateľné a bezpečné IaaS služby pre vývojové, testovacie, predprodukčné a produkčné prostredia nových informačných systémov.

Krok popísaný v tejto štúdii predstavuje implementáciu IKT infraštruktúry pre poskytovanie IaaS služieb v datacentre MV SR, ktoré predstavuje druhú časť riešenia „IKT infraštruktúry pre IaaS“, ktoré je rozšírené o funkcionality replikácie medzi datacentrom MV SR a datacentrom MF SR.

Navrhované riešenie umožní jednoduchý prístup k IaaS službám na vyžiadanie vo virtuálnom prostredí. Tieto služby môžu byť pridelované alebo uvoľňované s flexibilným časovým obmedzením a to na základe voliteľného škálovania, nezávisle od lokality zdrojov, prístupu k nim a bez nutnosti osobného kontaktu s poskytovateľom IaaS služby.

V ďalších častiach bude riešenie postupne sprístupňovať služby IaaS, neskôr PaaS a následne SaaS jednotlivým inštitúciám štátnej správy v požadovanom rozsahu a prevezme zodpovednosť za starostlivosť o ich IT zdroje. Finálny stav vyústi do optimalizácie a zefektívnenia využívania zariadení a prostriedkov a do potenciálu na zníženie nákladov na informačné a komunikačné technológie.

## 1.4 Použité skratky a značky

Tabuľka 2 Skratky a značky

Skratka / Značka	Vysvetlenie
DataCentrum	Organizácia v zriaďovateľskej pôsobnosti Ministerstva financií SR
DC	Dátové centrum

DNS	Domain name system/server
HW	Hardware
IaaS	Infrastructure as a Service
IISVS	Integrovaný informačný systém verejnej správy
IKT	Informačné a komunikačné technológie
ISVS	Informačný systém verejnej správy
IT	Informačné technológie
LAN	Local area network
MF SR	Ministerstvo financií Slovenskej republiky
MV SR	Ministerstvo vnútra Slovenskej republiky
NKIVS	Národná koncepcia informatizácie verejnej správy
OPIS	Operačný program Informatizácia spoločnosti
PaaS	Platform as a Service
PDC	Primárne dátové centrum
PO1	Prioritná os 1
Podporná infraštruktúra	technologické zariadenia DC zaisťujúce prevádzkové podmienky IKT s definovanou dostupnosťou (elektrické napájanie, chladenie), fyzickú bezpečnosť a požiaru ochranu
SaaS	Software as a Service
SAN	Storage area network
SDN	Software Defined Networking
SLA	Service level agreement, zmluva o úrovni poskytovaného servisu
SW	Software
TCO	Total cost of ownership
UPS	Uninterruptible Power Supply - záložný zdroj
VPN	Virtual private network
WAN	Wide area network

DR	Disaster Recovery
TIER 1	Podľa definície Uptime Institute. Základná infraštruktúra, vybavenie garantuje dostupnosť 99,671 %
TIER 2	Podľa definície Uptime Institute. Redundantné prvky infraštruktúry garantujú dostupnosť 99,741 %
TIER 3	Podľa definície Uptime Institute. Servisovateľné za prevádzky s garantovanou dostupnosťou 99,982 %
TIER 4	Podľa definície Uptime Institute. Bezvýpadková redundantná elektrická sieť so záložnými zdrojmi a distribučnými cestami zaručujúcimi dostupnosť 99,995 %

## 2 Manažérske zhrnutie

Štúdia nadväzuje na Strategický dokument pre oblasť rastu digitálnych služieb a oblasť infraštruktúry prístupovej siete novej generácie (2014 – 2020), ktorý bol prerokovaný 8. januára 2014 vládou SR. V strategickom dokumente je problematika zavádzania eGovernment cloudu rozpracovaná ako špecifický cieľ pre nové programové obdobie, ktorý bude následne podporený Operačným programom Integrovaná infraštruktúra.

Z neho vychádza aj materiál „Návrh centralizácie a rozvoja dátových centier v štátnej správe“, číslo materiálu: UV-21676/2014, schváleným vládou SR uznesením číslo 247/2014, ktorý bol spracovaný na základe úlohy B.1 uznesenia vlády SR č. 680 z 27.11.2013, ktorým vláda SR schválila správu zo zasadnutia Európskej rady konanej v Bruseli 24. - 25. októbra 2013.

Cieľová architektúra riešenia vychádza z konceptu architektonickej vízie cloudového riešenia MF SR v rámci programu eGovernmentu. Riešenie predpokladá vybudovanie konsolidovanej technologickej platformy, ktorá umožní poskytovať skupinu služieb s rôznou úrovňou presunu kompetencií na centrálnu DC a to počnúc v prvej fáze službami IaaS a postupným rozširovaním záberu až po služby SaaS a poskytovanie centralizovaných riešení bez potreby správy na zákazníckej strane.

Prvá časť riešenia IKT infraštruktúry pre IaaS v datacentre MF bola predmetom samostatnej štúdie v súčasnosti je už aj riešenie v realizácii.

Štúdia „Cloud Ministerstva vnútra SR.“, popisuje druhú časť riešenia eGovernment cloudu, ktoré zabezpečí IaaS služby v datacentre MV SR. Realizáciou projektu sa dosiahne požadovaná dostupnosť a možnosti realizácie disaster recovery scenárov vybraných IS. Nasadenie služieb IaaS sa tak implementuje v dvoch lokalitách, ktoré budú dostatočne geograficky vzdialené, aby najmä živelná udalosť v jednej lokalite neovplyvnila prevádzku v druhej.

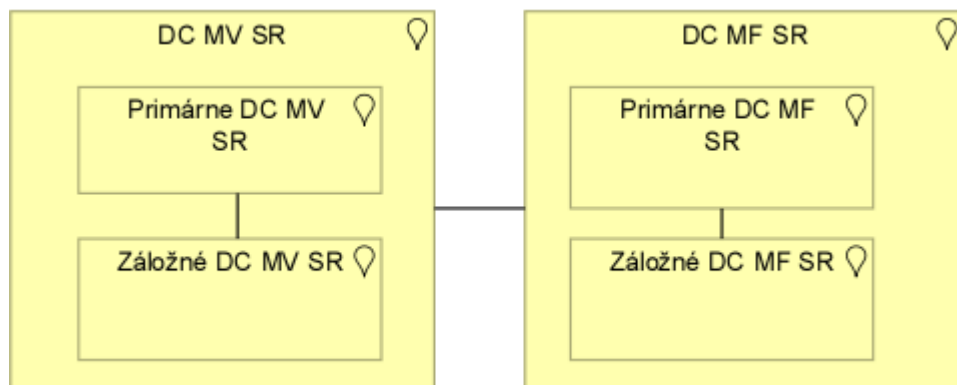
Vo finálnom stave bude vládny Cloud poskytovať služby vo forme IaaS, PaaS a SaaS jednotlivým inštitúciám štátnej správy v požadovanom rozsahu a prevezme zodpovednosť za starostlivosť o ich IT zdroje. Inštitúciám štátnej správy tak odpadnú činnosti, akými sú nákup potrebných infraštruktúrnych zariadení, pravidelné aktualizovanie vydaného softvéru, ktorý sa viaže na infraštruktúru, údržba infraštruktúry a celková podpora prostredí. Prevádzkovateľ zaručí a zabezpečí požadovanú bezpečnosť a dostupnosť infraštruktúry. Cieľový stav vyústi do optimalizácie a zefektívnenia využívania zariadení a prostriedkov a do potenciálu na zníženie nákladov na informačné a komunikačné technológie.

Účelom tejto štúdie je popísať hlavné požiadavky, parametre, charakteristiky a návrh základnej technologickej infraštruktúry, ktoré budú reflektovať požiadavky zainteresovaných strán, a ktoré sú predpokladom na prevádzkovanie služby IaaS. V rámci štúdie sú analyzované 3 alternatívy, pričom na základe zistených výhod/nevýhod bola za odporúčanú zvolená alternatíva C – „Cloud riešenie“. Cloud riešenie predpokladá vybudovanie eGovernment cloudu, poskytujúceho IaaS služby v datacentre MV SR, pričom Datové centrá MV SR a MF SR si budú vzájomne poskytovať geograficky oddelenú záložnú lokalitu, kde je možné obnoviť požadovanú prevádzku v krátkom čase (Disaster Recovery - DR).

Štúdia predpokladá, že v novom programovom období 2014 - 2020 nebude možné z prostriedkov OPII nakupovať HW a SW infraštruktúru individuálne jednotlivými rezortami, ale iba centrálnu a to do dátových centier MFSR a MVS SR.



Obrázok 1 Cieľová architektúra logického dátového centra štátu



## 2.1 Motivácia

Tabuľka 3 Motivácia – budúci stav

Súhrnný popis	
<p>Potreby v oblasti základnej IKT infraštruktúry typicky nie sú priamymi potrebami, ale potrebami vyvolanými z vyšších úrovní, t.j. v hierarchii od efektívnej správy vecí verejných a potreby efektívnej interakcie verejnosti s verejnou správou, cez elektronické služby, informačné systémy a následne HW a SW platformy, na ktorých sa prevádzkujú ide o potreby na najnižšom stupni.</p> <p>Je zjavné, že úspory z realizácie projektu sa prejavujú v rámci štátnej správy, ktorá môže finančné zdroje vytvorené úsporou na IKT technológiách použiť na iné účely. Dominantne je preto projekt IKT infraštruktúra pre laaS časť 2 pre štátnu správu projektom prierezovým.</p> <p>Zároveň ale ide o priestor, kde je možné najviac a relatívne najjednoduchšie optimalizovať využitie zdrojov či už koncentráciou do väčších a efektívnejších dátových sál, zdieľaním IKT infraštruktúry, príslušného technického vybavenia a v neposlednom rade aj obsluhu personálu, až po virtualizáciu serverov a zdieľanie zdrojov na čo najvyššej úrovni.</p> <p>Potreba zavedenia cloudu verejnej správy a centralizácie DC štátu je v základnej štúdii Dátové centrum pre eGovernment podrobne zdôvodnená a uznesenie vlády 247/2014 Návrh centralizácie a rozvoja dátových centier v štátnej správe ju potvrdzuje.</p> <p>Zúčastnené strany sú uvedené v prílohe č.1 tabuľka 5 Zoznam zainteresovaných.</p>	
<p>Všeobecne je možné konštatovať že prostredie eGov disponuje značným množstvom zdrojov na IKT infraštruktúru avšak v rámci súčasne plánovaného priebehu projektov ich nedokáže spoločne využiť. Každý projekt predpokladá vlastnú, redundantnú a vysoko dostupnú infraštruktúru v mnohých prípadoch s umiestnením v dvoch a niekedy až v troch geograficky oddelených lokalitách. Na túto infraštruktúru sú v rámci projektov dedikované nie malé finančné zdroje, pričom je potrebné zabezpečiť finančné zdroje aj na následnú prevádzku a podporu tejto infraštruktúry a v neposlednom rade aj na podporu používateľov eGov služieb. Súčasný stav zabezpečenia IKT infraštruktúry, jej prevádzky a podpory v prostredí projektov OPIS (predovšetkým mimo rezortov MVSR a MFSR) sa preto javí ako neoptimálny z hľadiska využitia plánovaných technických prostriedkov IKT.</p> <p>Vývoj v oblasti poskytovania IT služieb vo forme "Cloud Computing" otvára nové pole možností tým, že umožňuje jednoduchý prístup k dynamicky konfigurovateľným službám. Cloud predstavuje nový spôsob šetrenia IT nákladov formami, ktoré propagujú štandardné formy optimalizácie a zdieľania infraštruktúry, ako aj poskytovania unifikovaných služieb. Pre súčasný stav prevádzky a podpory v prostredí projektov OPIS je poskytovanie služieb formou Government Private Cloud-u spôsobom, ktorým sa eliminujú hlavné problémové faktory často uvádzané pre Verejné Cloud-y (často iba Cloud-y) akými sú bezpečnosť, neznáma spoľahlivosť infraštruktúry a vlastníctvo dát.</p>	
Kritéria kvality	<b>Spresnenie kritérií kvality:</b> Odkazy na relevantné identifikátory kritérií kvality v prílohe Kritéria kvality.
Q10 - Naplnenie cieľov Q11 - Naplnenie prínosov	
Riziká	<b>Spresnenie identifikovaných rizík:</b> Odkazy na relevantné identifikátory rizík v prílohe Riziká.
Stručná charakteristika identifikovaných rizík (Max. 400 znakov) R 01 - Dátové centrum MF SR nebude pripravené na synchronizáciu R 02 - MV nebude mať potrebné priestory na nové IKT technológie pre cloudové služby R 03 - Jednotlivé povinné osoby nebudú mať záujem o služby laaS	
Prílohy	Diagramy, modely, obrázky v plnom rozlíšení
Tabuľka 2 Riziká Tabuľka 5 Zoznam zainteresovaných Tabuľka 6 Zoznam cieľov Tabuľka 7 Princípy a požiadavky	Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

## 2.2 Popis aktuálneho stavu

### 2.2.1 Legislatíva

Tabuľka 4 Legislatíva – aktuálny stav

Súhrnný popis	
Relevantná legislatíva je uvedená v prílohe č.1 tabuľka 4 Legislatíva.	
Riziká	<b>Spresnenie identifikovaných rizík:</b> Odkazy na relevantné identifikátory rizík v prílohe Riziká.
Prílohy	Diagramy, modely, obrázky v plnom rozlíšení
Tabuľka 2 Riziká Tabuľka 4 Legislatíva	Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

## 2.2.2 Architektúra

### 2.2.2.1 Biznis architektúra

Tabuľka 5 Biznis architektúra - aktuálny stav

Súhrnný popis	
Kapitola nie je relevantná nakoľko MV SR nie je v súčasnosti poskytovateľom IaaS služieb.	
Riziká	<b>Spresnenie identifikovaných rizík:</b> Odkazy na relevantné identifikátory rizík v prílohe Riziká.
Prílohy	Diagramy, modely, obrázky v plnom rozlíšení
	Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

### 2.2.2.2 Architektúra informačných systémov

Tabuľka 6 Architektúra informačných systémov - aktuálny stav

Súhrnný popis	
Kapitola nie je relevantná nakoľko MV SR nie je v súčasnosti poskytovateľom IaaS služieb..	
Riziká	<b>Spresnenie identifikovaných rizík:</b> Odkazy na relevantné identifikátory rizík v prílohe Riziká.

Prílohy	Diagramy, modely, obrázky v plnom rozlíšení
Tabuľka 2 Riziká	Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

### 2.2.2.3 Technologická architektúra

Tabuľka 7 Technologická architektúra - aktuálny stav

Súhrnný popis
<p>Produkčná a testovacia prevádzka informačných systémov MV SR je prevádzkovaná v dvoch dátových centrách MV SR:</p> <ul style="list-style-type: none"> <li>• DCA Timravy,</li> <li>• DCB Tajov.</li> </ul> <p>Architektúra a implementácia IT infraštruktúry umožňuje efektívne využitie zdrojov oboch Dátových centier (režim Aktívny/Aktívny) a schopnosť rýchlej obnovy po havarijnej situácii v jednom z dátových centier (HA&amp;DR, High Availability, Disaster recovery).</p> <p>Na zabezpečenie HA a DR riešenia je v geograficky vzdialenom dátovom centre DCB Tajov umiestnená výkonovo a architektonicky rovnocenná HW infraštruktúra, ktorá je schopná prevádzkovať produkčné systémy MV SR v plnej funkcii.</p>
<p>A) Dátová sála – primárne</p> <p><u>DCA - Timravy</u></p> <p>DC Timravy obsahuje dve IT sály. IT sála 1 bola vybudovaná v roku 2004 pri vybudovaní dátového centra. Od tohto času boli do sály postupne pridávané ďalšie systémy, kapacita sály je na hranici. Pridanie ďalších systémov už nie je možné.</p> <p>Rozloha IT sály je cca 130m<sup>2</sup> a max. záťaž je dimenzovaná na cca 120kW. Súčasná obsadenosť a záťaž dosahuje kapacitné limity. Dátové centrum je dizajnované v štandarde Tier II s jednou vetvou napájania a priemernou štatistickou dostupnosťou 99,749%. Infraštruktúra kritických systémov neumožňuje odstávku alebo servis za prevádzky.</p> <p>Pre účely ďalšieho rozvoja bola v roku 2014 vybudovaná druhá IT sála o rozlohe 70 m<sup>2</sup> a max príkon IKT je dimenzovaný na 60 kW. Spolu s druhou IT sálou bola vybudovaná podporná infraštruktúra elektrického napájania, chladenia, rozšírené bezpečnostné a požiarne systémy a doplnený ďalší motor generátor. DC Timravy sa v aktuálnom čase vzhľadom na intenzívny rozvoj IKT v rezorte MV SR ukazuje ako kapacitne nedostatočné pre najkritickejšie systémy zo strednodobého a dlhodobého pohľadu z nasledovných dôvodov</p> <p><u>DCB – Tajov</u></p> <p>DC Tajov bolo pôvodne budované ako záložné stredisko. V súčasnosti je toto dátové centrum využívané v produkčnom režime.</p> <p>B) Napájanie</p> <p>Zálohované napájanie je na úrovni Tier II s jednou vetvou napájania. Zálohovanie je riešené s použitím UPS v redundancii N+1 a motor-generátora. Infraštruktúra napájania neumožňuje zásah / odstavenie alebo servisovanie za prevádzky bez výpadku IT systémov.</p> <p>C) Klimatizácia</p> <p>Klimatizácia je riešená v 5 split systémami v redundancii N+1 rozmiestnenými v 2 technologických miestnostiach.</p>

Riziká	<b>Spresnenie identifikovaných rizík:</b> Odkazy na relevantné identifikátory rizík v prílohe Riziká.
R 04 - Nebude možné dosiahnuť ďalšie zvyšovanie efektivity vďaka úsporám z rozsahu, centralizácie a automatizácie R 05 - Nebude možné migrovať niektoré IS povinných osôb kvôli odlišnej technológii	
Prílohy	Diagramy, modely, obrázky v plnom rozlíšení
Tabuľka 2 Riziká Tabuľka 13 Komunikačná infraštruktúra	Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

### 2.2.2.4 Bezpečnostná architektúra

Tabuľka 8 Bezpečnostná architektúra - aktuálny stav

Súhrnný popis
<p>Aj napriek tomu, že MV SR nie je v súčasnosti poskytovateľom IaaS služieb na nižšie uvedenom obrázku sú znázornené rámcové oblasti bezpečnosti, ktoré má MV SR už zavedené, nakoľko je prevádzkovateľom množstva dôležitých ISVS. Kľúčové funkcie bezpečnostnej architektúry sú:</p> <ul style="list-style-type: none"> <li>- riadenie prístupu - Zabezpečenie jednotnej služby pre účely identifikácie, autentifikácie a autorizácie systémových správcov a odberateľov cloudových služieb</li> <li>- Ochrana proti škodlivému kódu - zabezpečuje detekciu útokov na prostredie cloud computingu a to vrátane komponent určených na manažment cloud computingu a zaisťuje aj podporu zabezpečenia dôverylosti, autenticity a integrity prenášaných dát pomocou kryptografických opatrení</li> <li>- Aktualizáciu softvéru - Aktualizácia softvéru, pričom sa zabezpečuje aj testovanie aktualizácie virtualizačného prostredia a softvéru pre správu cloudu v testovacom prostredí</li> <li>- Sieťová bezpečnosť - virtualizáciu firewallov a iných prvkov siete, segmentácie siete napr. vo forme VLAN a detekciu škodlivého kódu a jeho odstraňovanie na sieťovej bezpečnosti</li> </ul>

Riziká	<b>Spresnenie identifikovaných rizík:</b> Odkazy na relevantné identifikátory rizík v prílohe Riziká.
R 06 - Nové datacenterum nebude spĺňať všetky bezpečnostné požiadavky ISVS povinných osôb R 07 - Súčasný ISVS, ktoré sa majú migrovať, nebudú z pohľadu riešenia bezpečnosti kompatibilné s architektúrou DC MV.	
Prílohy	Diagramy, modely, obrázky v plnom rozlíšení
Tabuľka 2 Riziká	Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

### 2.2.3 Prevádzka

Tabuľka 9 Prevádzka - aktuálny stav

Súhrnný popis
<p>V súčasnosti je prevádzka IS v prostredí MV SR riešená čiastočne z vlastných zdrojov a čiastočne dodávateľsky. MV SR disponuje skúsenosťami z oboch modelov.</p> <p>V súčasnosti na prevádzku dátových centier Timravy a Tajov je dedikovaných 65 interných zamestnancov MV SR z čoho:</p> <ul style="list-style-type: none"> <li>• L1 podporu zabezpečujú interní zamestnanci call centra (15 ľudí) a centrá podpory</li> <li>• L2 podporu zabezpečujú dodávateľia a interní zamestnanci MV SR</li> <li>• L3 podporu zabezpečujú dodávateľia a interní zamestnanci MV SR (v prípade IS, ktoré si MV vyvíjalo vo vlastnej réžii.)</li> </ul>

Riziká	<b>Spresnenie identifikovaných rizík:</b> Odkazy na relevantné identifikátory rizík v prílohe Riziká.
R 08 - Nie je možné zabezpečiť efektívne a včasné zavádzanie a udržiavanie zmien	
Prílohy	Diagramy, modely, obrázky v plnom rozlíšení
Tabuľka 2 Riziká	Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.



## 2.3 Alternatívne riešenia

### 2.3.1 Alternatíva A – „Konzervatívna“

Súhrnný popis
<p>Alternatívou A je konzervatívny prístup zachovania súčasného stavu. Správa IKT pre verejnú správu je riadená v rámci kompetencií jednotlivých rezortov, resp. subjektov. Rozvoj IKT infraštruktúry je realizovaný samostatnými projektami týchto subjektov, pričom sa nepožaduje vzájomné zdieľanie alebo konsolidácia HW a SW infraštruktúry.</p> <p>Jednotliví prevádzkovatelia IKT a teda aj žiadatelia o NFP, disponujú rôznou úrovňou IKT infraštruktúry v rozsahu od komplexných dátových centier so zabezpečením disaster recovery (Tier 3) až po jednoduché serverovne spĺňajúce len najzkladanejšie požiadavky na dostupnosť (Tier 1, resp. Tier 2.)</p> <p>Dosiahnutie úrovne Tier 3 pre všetky subjekty vrátane vlastných záložných lokalít znamená pre tieto subjekty rozsiahle projekty vyžadujúce investície aj ľudské zdroje, často krát kompilované hlavne nutnosťou budovania vzdialeného záložného centra, pre ktoré nie sú k dispozícii v jednotlivých rezortoch vhodné objekty.</p>
<p>V máji 2013 uskutočnilo MF SR prieskum medzi jednotlivými organizáciami štátnej správy, z ktorého vyplýva, že klasifikácii Tier 3 zodpovedajú DataCentrum, DC MV SR a ŠÚ SR. V zmysle koncepcie budovania ISVS podľa NKIVS a aj charakteru poskytovaných eGov služieb, sa požaduje dostupnosť informačných systémov verejnej správy v rozsahu 24 hodín denne 7 dní v týždni úroveň Tier 3. Aktuálna naplnenosť DataCentra MF SR a DC Ministerstva vnútra SR je vyše 80% (64% MF SR a 100% v MV SR).</p>
<p>Dôvod zamietnutia.</p> <p>Posilnenie všetkých priestorov štátnej správy na kvalifikovateľný štandard (Tier 3) by si vyžiadalo nadmerné úsilie a veľa finančných prostriedkov s negarantovaným výsledkom, nakoľko veľká väčšina dátových centier je v priestoroch, kde nie je technicky a/alebo priestorovo možné vykonať posilnenie na akceptovateľný štandard.</p>

### 2.3.2 Alternatíva B – „Hybridné riešenie“

Súhrnný popis
<p>Alternatívou B je hybridné riešenie, ktoré by rešpektovalo súčasný stav IKT infraštruktúry jednotlivých subjektov štátnej správy, ale by sa vybudovalo spoločné záložné dátové centrum vo vzdialenej lokalite. Takéto riešenie by vytvorilo predpoklady na to aby všetky ISVS dosiahli úroveň Tier 3.</p> <p>Toto riešenie predpokladá koncepčné riešenie záložného centra, ktoré by využívali všetky subjekty štátnej správy. Ak má byť takéto riešenie efektívne, malo by umožňovať dynamické pridelovanie výkonu a kapacity pre všetky subjekty. Prakticky to znamená vybudovať datacentrum (cloud) ponúkajúci služby IaaS v rozsahu funkcionalít záložného dátového centra. Tieto služby by potom umožnili každému subjektu štátnej správy realizáciu ISVS s úrovňou Tier 3.</p>
<p>Na prvý pohľad sa zdá takýto kompromis ideálnym riešením. Pri jeho realizácii však treba očakávať značné problémy, pretože súčasné riešenia IS týchto subjektov nie sú na takúto hybridnú architektúru pripravené a jej implementácia by vyžadovala aj investície do IKT na strane každého z týchto subjektov. Predovšetkým ide o to, že hoci poskytovaný výkon sa špecifikuje počtom a výkonom CPU, prakticky sa implementácia odlišuje podľa konkrétnych technológií. Keďže primárne riešenia nie sú budované na unifikovanom prostredí, adaptácia by vyžadovala ďalšie úpravy a testovanie.</p> <p>Realizácia alternatívy B vyžaduje technicky a technologicky rovnaké riešenie ako je pri navrhovanom projekte: centrálné riešenie obsahujúce primárne aj záložné dátové centrum poskytujúce infraštruktúru formou IaaS. Existujúce súčasné IKT jednotlivých subjektov by sa však museli na hybridnú architektúru adaptovať.</p>
<p>Dôvod zamietnutia.</p> <p>Takáto hybridná architektúra je komplikovaná a z dlhodobého hľadiska neperspektívna, preto je potrebné vnímať ju iba ako núdzovú na čas, kým sa dosiahne cieľový stav. Prechodné obdobie by predstavovalo niekoľko rokov a následne by vynaložené</p>

investície na úpravy neboli ďalej využívané. Takéto riešenie, hoci je technicky realizovateľné, nepredstavuje najlepšiu ekonomickú alternatívu. Prechodné obdobie je dočasné a nemalo by vyžadovať neperspektívne investície.

### 2.3.3 Alternatíva C – „Cloud riešenie“

#### Súhrnný popis

##### Súhrnný popis

Alternatívou C je cloudové riešenie, ktoré predpokladá vybudovanie eGovernment cloudu, poskytujúceho IaaS služby v datacentre MV SR. Datové centrá MV SR a MF SR si budú vzájomne poskytovať geograficky oddelenú záložnú lokalitu, kde je možné obnoviť požadovanú prevádzku v krátkom čase (Disaster Recovery - DR).

Alternatíva C vyžaduje technicky a technologicky podobné riešenie ako pri projekte „IKT infraštruktúra pre IaaS časť 1.“ vrátane zabezpečenie technológií na realizáciu replikácii medzi dátovým centrom MV SR a MF SR.

## 2.4 Popis budúceho stavu

Z vyššie uvedených alternatív je odporúčaná alternatíva C – „Cloud riešenie“. Odporúčané riešenie je predmetom tejto kapitoly.

### 2.4.1 Legislatíva

Tabuľka 10 Legislatíva - budúci stav

Súhrnný popis	
Relevantná legislatíva je uvedená v prílohe č.1 tabuľka 4 Legislatíva.	
<p>Nové požiadavky na legislatívne zmeny môžu vyplývať v procese migrácie pri príprave prevádzky špecifických systémov rezortov v dátovom centre, pri ktorých je nakladanie s údajmi resp. informačnými systémami upravené špecifickou legislatívou. Tieto nie je možné v súčasnosti identifikovať, nakoľko plán využívania DC jednotlivými subjektami s konkretizovaním jednotlivých IS a aplikácii nie je spracovaný. Hoci projekt umožňuje migrácie súčasných IS jednotlivých subjektov, je nutné predpokladať, že tieto IS boli z veľkej miery realizované v ostatnom čase a teda z dôvodu ochrany investícií sa musia najskôr amortizovať.</p> <p>Projekty budovania dátových centier a ich spoločného využívania viacerými organizáciami verejnej správy už sú realizované a funkčné, čo poukazuje na priaznivý stav legislatívy v tejto oblasti. Nepredpokladáme nutnosť legislatívnych zmien ako predpokladu pre realizáciu a prevádzku projektu.</p>	
Riziká	<b>Spresnenie identifikovaných rizík:</b> Odkazy na relevantné identifikátory rizík v prílohe Riziká.
Prílohy	Diagramy, modely, obrázky v plnom rozlíšení
Tabuľka 2 Riziká Tabuľka 4 Legislatíva	Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

### 2.4.2 Architektúra

#### 2.4.2.1 Biznis architektúra

Tabuľka 11 Biznis architektúra – budúci stav

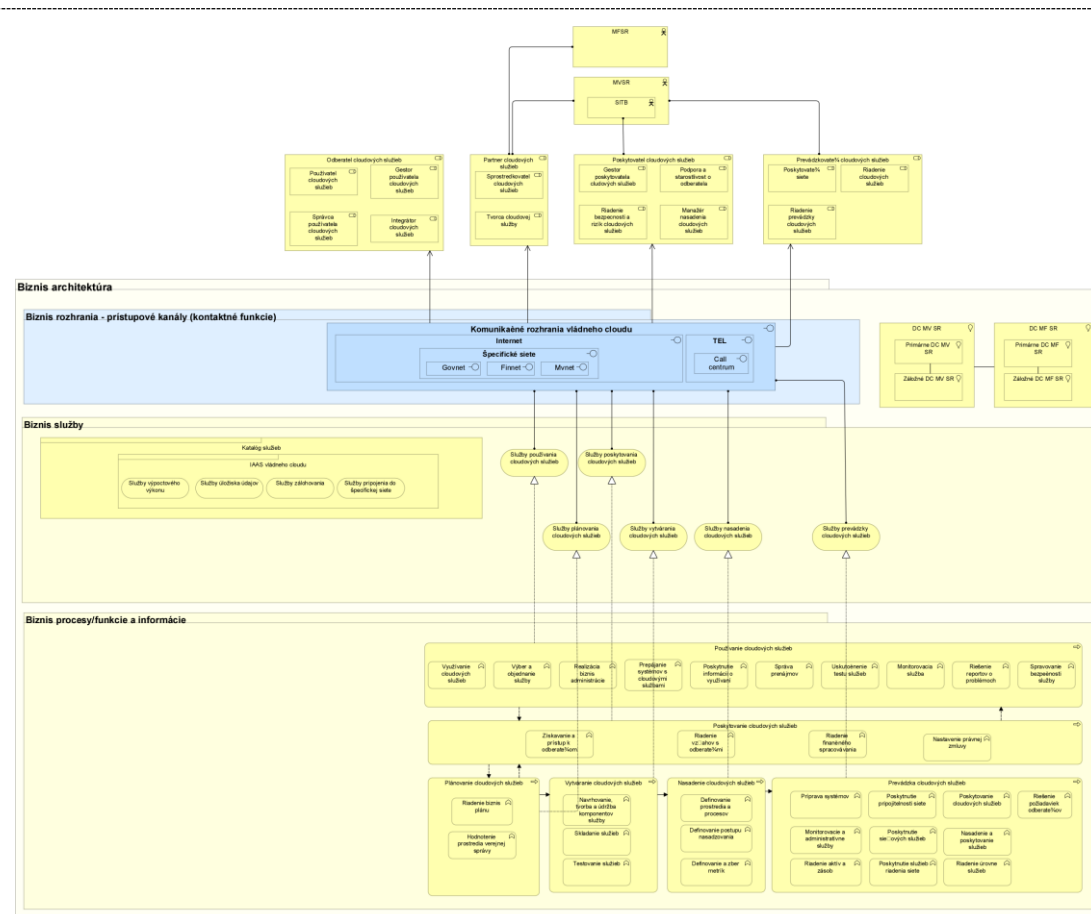
Súhrnný popis
---------------

V rámci biznis architektúry zohrávajú kľúčovú rolu MV SR, MF SR a povinné osoby, resp. konzumenti IaaS služieb. Jednotlivé subjekty reprezentujú v rámci biznis architektúry nasledovné role:

- Odberteľ cloudových služieb - Konzumenti IaaS služieb/používatelia z rôznych rezortov, inštitúcií a organizácií verejnej správy, ktorí budú k službám pristupovať prostredníctvom rozhrania pre zákazníka
- Partner cloudových služieb – MV SR/MF SR v roli sprostredkovateľa cloudových služieb a tvorca cloudových služieb
- Poskytovateľ cloudových služieb – MV SR, zodpovedný za manažérske schvaľovanie požiadaviek, riešenie zmenových požiadaviek, kapacitné plánovanie a pod.
- Prevádzkovateľ cloudových služieb – MV SR, zodpovedný za technické schvaľovanie požiadaviek, poskytovanie cloudových služieb a prevádzku IKT infraštruktúry

Biznis architektúra modelu poskytovania IaaS služieb, sa skladá z logických vrstiev, ktorými sú biznis rozhrania, biznis služby a biznis procesy/funkcie/informácie.

- biznis rozhrania – podrobný popis je uvedený v prílohe č.1 tabuľka 9
- biznis služby – podrobný popis je uvedený v prílohe č.1 tabuľka 12
- biznis procesy/funkcie/informácie – podrobný popis je uvedený v prílohe č.1 tabuľka 10, 11 a 13



Kritéria kvality	<b>Spresnenie kritérií kvality:</b> Odkazy na relevantné identifikátory kritérií kvality v prílohe Kritéria kvality.
Q12 - Súlad s architektonickým rámcom	

Riziká	Spresnenie identifikovaných rizík: Odkazy na relevantné identifikátory rizík v prílohe Riziká.
R 09 - Nepodariť sa presadiť dostatočne radikálnu optimalizáciu procesov, s reálnym dopadom na efektivitu a výrazným inovačným potenciálom. R 10 - Nespokojnosť povinných osôb s centrálnym riešením. R 11 - Neochota poskytovať služby DC iným rezortom R 12 - Neochota umiestniť IT zdroje do dátových centier v správe iných subjektov R 13 - Nebudú vytvorené organizačné a personálne predpoklady na fungovanie dátového centra MV SR	
Prílohy	Diagramy, modely, obrázky v plnom rozlíšení
Tabuľka 2 Riziká Tabuľka 3 Kritéria kvality Tabuľka 9 Biznis rozhrania Tabuľka 10 Biznis procesy Tabuľka 11 Biznis funkcie Tabuľka 12 Biznis služby Tabuľka 13 Biznis informácie	Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

## 2.4.2.2 Architektúra informačných systémov

Tabuľka 12 Architektúra informačných systémov - budúci stav

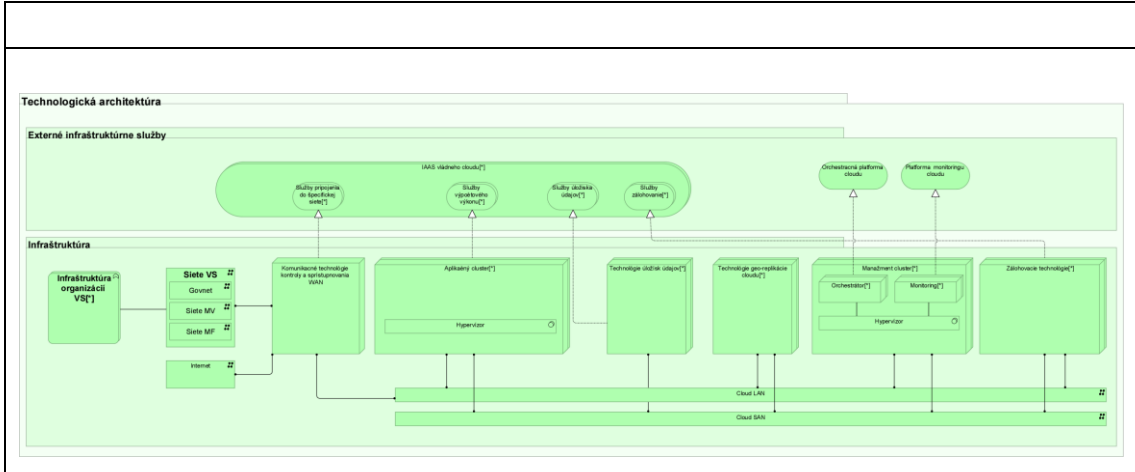
Súhrnný popis
<p>Architektúra modelu poskytovania IaaS služieb, sa skladá z funkcionálnych vrstiev, ktorými sú vrstva dopytu, vrstva poskytovania cloudových služieb a vrstva dodávania zdrojov.</p> <ul style="list-style-type: none"> <li>Vrstva dopytu riadi katalóg opisujúci IaaS služby dostupné pre odberateľov IaaS služieb a zabezpečuje validitu ich vzájomného mapovania podľa dohody o poskytovanej úrovni IaaS služieb.</li> <li>Vrstva poskytovania IaaS služieb riadi IaaS služby a ich kompozície na základe požiadaviek vrstvy dopytu a dostupnosti vrstvy dodávania IaaS služieb s cieľom zabezpečiť súlad s dohodou o poskytovanej úrovni IaaS služieb.</li> <li>Vrstva dodávania zdrojov poskytuje hardvérové zdroje, zabezpečuje riadenie zdrojov, optimalizuje a monitoruje využitie prostriedkov z dispozičných zdrojov.</li> </ul>

<div> <div>Dopyt</div> <div> <div>Pristup ku cloudovým službám</div> <div>Manažment objednávok</div> <div>Vytváranie správ o využívaní cloudových služieb</div> <div>Katalóg cloudových služieb</div> <div>Manažment používateľov a prístupových práv</div> <div>Dodržiavanie definovanej úrovne služieb</div> </div> </div> <div> <div>Poskytovanie služieb</div> <div> <div>Spracovanie požiadaviek a aktivácia a deaktivácia cloudových služieb</div> <div>Repozitár modelu cloudových služieb</div> <div>Modelovanie a návrh cloudových služieb</div> <div>Realizácia cloudových služieb</div> <div>Monitorovanie cloudových služieb</div> <div>Manažment stavu cloudových služieb</div> <div>Využívanie cloudových služieb</div> </div> </div> <div> <div>Dodávanie zdrojov</div> <div> <div>Katalóg zdrojov</div> <div>Manažment životného cyklu zdrojov</div> <div>Modelovanie kapacít zdrojov</div> <div>Návrhu šablón zdrojov</div> <div>Pridelovanie zdrojov</div> <div>Monitorovanie využívania zdrojov</div> <div>Stav zdrojov</div> <div>Adaptér zdrojov a kontroly</div> </div> </div>	
Kritéria kvality	<b>Spresnenie kritérií kvality:</b> Odkazy na relevantné identifikátory kritérií kvality v prílohe Kritéria kvality.
Q13 - Využitie cloudových služieb	
Riziká	<b>Spresnenie identifikovaných rizík:</b> Odkazy na relevantné identifikátory rizík v prílohe Riziká.
R 14 - Problémy pri migrácii údajov v celom rozsahu z distribuovaných systémov povinných osôb do nového riešenia R 15 - Zložitosť a časová náročnosť riešenia SaaS s využitím len existujúcich IaaS služieb (PaaS sa môžu výrazne oneskoriť) R 16 - Neuspokojivá škálovateľnosť riešenia R 17 - Vymáhanie dohodnutej SLA bude problematické.	
Prílohy	Diagramy, modely, obrázky v plnom rozlíšení
Tabuľka 2 Riziká Tabuľka 3 Kritéria kvality Tabuľka 14 Zoznam informačných systémov Tabuľka 15 Aplikačné moduly Tabuľka 16 Poskytované služby IS	Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

### 2.4.2.3 Technologická architektúra

Tabuľka 13 Technologická architektúra - budúci stav

Súhrnný popis
<p>Základné komponenty technologickej architektúry sú uvedené na obrázku dolu, podrobnejší popis je uvedený v Prílohe č. 1 kapitola 1.6.1.</p> <p>Okrem uvedených komponentov je dôležitým technologickým prvkom riešenie DR medzi DC MV SR a DC MF SR. Vzhľadom na vzdialenosť medzi jednotlivými DC, ktorá je cca. 150km je možné uvažovať iba nad asynchrónnou replikáciou dát. Serverová infraštruktúra v DR lokalite môže byť primerane výkonovo redukovaná. V prípade potreby DR bude prechod služieb IKT systémov z jedného dátového centra do druhého zabezpečený manuálne riadeným procesom. Priebežný prenos dát medzi dátovými úložiskami v oboch lokalitách bude zabezpečený asynchrónnou replikáciou na úrovni FC alebo LAN prepojenia prostredníctvom softvérovej replikácie. S takýmto riešením bude musieť uvažovať aplikačná vrstva, ktorá zabezpečí odolnosť voči nekonzistencii dátovej kópie v DR dátovom centre.</p>



Pri definovaní požiadaviek na výkon a iné parametre riešenia sa vychádza z rovnakých požiadaviek definovaných v štúdiu uskutočniteľnosti „IKT infraštruktúra pre IaaS časť 1“ (Tabuľka 3 Predpokladaný minimálny rozsah IKT infraštruktúry), ktorá je rozšírená o požiadavky na zabezpečenie DR spôsobilostí. Tieto požiadavky zabezpečia iniciálne prostredie umiestnené v novovybudovanom nadrezortnom dátovom centre Ministerstva vnútra SR, ktoré bude primárne určené pre nové projekty informačných systémov prevádzkované vo vládnom cloude. Navrhované riešenie musí umožňovať škálovanie v závislosti od aktuálnych požiadaviek realizovaných projektov.

Predpokladaný minimálny rozsah IKT infraštruktúry zo štúdie uskutočniteľnosti IKT infraštruktúra pre IaaS časť 1.

Predpoklad	Hodnota
Iniciálny počet nasadzovaných IS projektov	40
Priemerný počet prostredí pre jeden IS projekt	4 (kombinácia nasledovných prostredí: vývojové, integračné, testovacie, predprodukčné, školiace, produkčné)
Priemerný počet vrstiev logickej architektúry pre jedno prostredie	3
Minimálny počet virtuálnych serverov na každej jednej vrstve pre jednotlivé prostredia	Vývojové : 1 Integračné : 1 Testovanie : 2 (Pred)produkčné/školiace: 2
Priemerný výkon jedného virtuálneho servera (cores, RAM, HDD)	Vývojové : 2 core, 32 GB RAM, 1 TB HDD Integračné : 2 core, 32 GB RAM, 1 TB HDD Testovanie : 4 core, 64 GB RAM, 2 TB HDD (Pred)produkčné/školiace: 4 core, 128 GB RAM, 2 TB HDD

Na základe predpokladov uvedených vo vyššie uvedenej tabuľke je požadovaný rozsah IKT infraštruktúry pre IaaS časť 1 minimálne v nasledovnom rozsahu:

- 2400 core
- 53 TB RAM
- 1 200 TB HDD.

<p>Z pohľadu pridelovania zdrojov poskytuje navrhované riešenie výraznú flexibilitu. V prípade že reálne požiadavky na počty vrstiev, prostredí, serverov, služieb a pod. budú vyššie / nižšie oproti predpokladom, navrhované riešenie umožní dynamicky zmeniť jednotlivé počty v závislosti od aktuálnych systémových požiadaviek pre jednotlivé prostredia a aj preto je potrebné chápať túto konfiguráciu ako minimálnu.</p>	
Kritéria kvality	<b>Spresnenie kritérií kvality:</b> Odkazy na relevantné identifikátory kritérií kvality v prílohe Kritéria kvality.
Riziká	<b>Spresnenie identifikovaných rizik:</b> Odkazy na relevantné identifikátory rizik v prílohe Riziká.
<p>R 18 - Riešenie nebude dostatočne flexibilné. R 19 - Integrácia s externým prostredím bude komplikovaná.</p>	
Prílohy	Diagramy, modely, obrázky v plnom rozlíšení
<p>Tabuľka 2 Rizika</p> <p>Tabuľka 3 Kritéria kvality</p> <p>Technická špecifikácia ktorá obsahuje:</p> <p>Tabuľka 19 Platforma</p> <p>Tabuľka 21 Platformový softvér</p> <p>Tabuľka 22 Výpočtové zdroje</p> <p>Tabuľka 23 Úložiská údajov</p> <p>Tabuľka 24 Zálohovanie</p> <p>Tabuľka 25 Komunikačná infraštruktúra</p> <p>Tabuľka 26 Špeciálne technológie</p> <p>Tabuľka 27 Dátové centrum - sála</p>	Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

#### 2.4.2.4 Implementácia a migrácia

Tabuľka 14 Implementácia a migrácia

	Súhrnný popis
	<p>Nasadenie riešenia bude vykonané podľa detailného plánu inštalácie softvéru a hardvéru, ktorý bude výstupom inicializačnej fázy ako výsledok Analýzy a návrhu riešenia.</p> <p>Celkové trvanie projektu je nastavené na 10 mesiacov. Nasledujúca tabuľka obsahuje rámcový plán projektových aktivít. Stĺpce označené ako „M“ a číslo označujú mesiac od zahájenie projektových aktivít. Harmonogram počítá s paralelizáciou niektorých aktivít a relatívne bezproblémovým priebehom.</p> <p>Špecifikom tohto projektu je, že vytvára platformu pre ostatné projekty a samotná migrácia iných riešení nie je súčasťou tohto projektu.</p>



Aktivity projektu	Fázy projektu	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10
Podporná aktivita	Prípravná fáza										
Podporná aktivita	Analýza potrieb a požiadaviek										
Podporná aktivita	Inicializačná fáza										
Hlavná aktivita	Analýza a návrh riešenia										
Hlavná aktivita	Implementácia organizačných a procesných zmien										
Hlavná aktivita	Realizačná fáza										
Hlavná aktivita	Implementácia na úrovni dátovej a aplikačnej vrstvy										
Hlavná aktivita	Inštalácia infraštruktúry										
Hlavná aktivita	Nasadenie a integrácia										
Hlavná aktivita	Implementácia organizačných a procesných zmien										
Podporná aktivita	Dokončovacia fáza										
Podporná aktivita	Akceptácia										
	<p>Predmetný projekt nie je priamo cieleň na široké skupiny používateľov – občanov a podnikateľov – a teda preň nie sú relevantné typické KPI projektu OPII zamerané na služby verejnosti.</p> <p>Významné znásobenie prevádzkovej infraštruktúry a inštalácia kritických systémov, ktoré si budú vyžadovať nepretržitú podporu, môže priniesť so sebou nároky na zvýšenie počtu zamestnancov, ktorí budú túto infraštruktúru prevádzkovať, a následne aj proporčné navýšenie ostatného personálu. Zvýšenie počtu zamestnancov bude takisto čiastočne spôsobené zavedením ďalšej fyzickej lokality do celkovej architektúry za účelom dosiahnutia vysokej dostupnosti a odolnosti voči výpadkom. Ako je však spomínané vyššie, vo finále sa predpokladá úspora pracovnej sily práve z dôvodu centralizácie, automatizácie a poskytovania služieb s vyššou pridanou hodnotou. Z dôvodu</p>										

	<p>prevádzkovaní služieb s požadovanou dostupnosťou 24x7, ktoré budú poskytovať implementované informačné systémy, sa v úvodnej fáze predpokladajú zvýšené finančné nároky zabezpečenie technickej podpory systémov. Konsolidácia a centralizácia infraštruktúry a existujúcich platforiem však umožní optimálne využívanie zdrojov, úsporu nákladov na nákup a správu softvérových licencií, úsporu nákladov na energie, a v neposlednom rade aj už spomínané úspory nákladov na pracovnú silu.</p> <p>V prostredí IKT služieb IaaS bude potrebné vykonať analýzu rizík každej požiadavky na službu IaaS a navrhnuť technologicky nezávislé bezpečnostné mechanizmy a funkcie. Na základe tejto analýzy bude možné rozhodnúť o spôsobe implementácii na technológii nezávislé bezpečnostné postupy tak, aby výsledná úroveň bezpečnosti z hľadiska integrity, dostupnosti a dôverylosti bola pre všetky komponenty IKT infraštruktúry konzistentná a zároveň aby sa dosiahla výrazne lepšia kvalita bezpečnostných opatrení. Keďže všetky bezpečnostné opatrenia budú implementovať centrálné, je dôvodné predpokladať, že pri rovnakej výške investícií do bezpečnosti, aké sa vynakladajú dnes, bude možné zaručiť lepšiu ochranu a bezpečnosť dát a osobných údajov spracovávaných v systémoch ISVS.</p>	
	Kritéria kvality	<b>Spresnenie kritérií kvality:</b> Odkazy na relevantné identifikátory kritérií kvality v prílohe Kritéria kvality.
	Riziká	<b>Spresnenie identifikovaných rizík:</b> Odkazy na relevantné identifikátory rizík v prílohe Riziká.
	<p>R 20 - Implementačný tím nebude mať dostatočnú kapacitu, vedomosti a schopnosti.</p> <p>R 21 - Závislosť na dostupnosti vhodných priestorov s technologickou infraštruktúrou</p> <p>R 22 - Spolupráca povinných osôb nebude dostatočná z rozličných dôvodov</p> <p>R 23 - Nedostačujúci počet zamestnancov na prevádzku IaaS služieb</p>	
	Prílohy	Diagramy, modely, obrázky v plnom rozlíšení
	<p>Tabuľka 2 Riziká</p> <p>Tabuľka 3 Kritéria kvality</p> <p>Tabuľka 23 Dodávateľská podpora</p> <p>Tabuľka 24 Podpora vlastnými zdrojmi</p> <p>Tabuľka 25 Prostriedky v prenájme</p>	Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

### 2.4.2.5 Bezpečnostná architektúra

Tabuľka 15 Bezpečnostná architektúra - budúci stav

Súhrnný popis
<p>Dátové centrum bude obsahovať zariadenia a systém schopný poskytovať ochranu, ktorá prestupuje celou sieťovou infraštruktúrou až po koncové virtuálne zariadenia. Všetky časti siete pritom spolupracujú pri ochrane dostupnosti, integrity a bezpečnosti komunikácie, sieťových služieb a koncových zariadení. Bezpečnostné zariadenia budú schopné reagovať automaticky na v súčasnosti známe útoky a pomôcť pri identifikácii neznámych útokov. Bezpečnostný systém je viacstupňový, vyžadujúci si kontinuálnu starostlivosť bezpečnostných expertov. Napriek tomu, že je využitá viacstupňová obrana, je potrebné rešpektovať bezpečnostnú politiku datacentra a neustále sledovať a dodržiavať aj nové bezpečnostné trendy. K predchádzaniu útokom patrí aj zaškolená a neprestajne z hľadiska bezpečnosti školená obsluha. Kontrolu dodržiavania pravidiel je potrebné kontrolovať nezávislými bezpečnostnými auditmi spolu s penetračnými testami. Hlavné oblasti riešenia bezpečnosti sú:</p> <ul style="list-style-type: none"> <li>- Riadenie prístupu</li> <li>- Ochrana proti škodlivému kódu</li> </ul>

- Aktualizácia softvéru
- Sieťová bezpečnosť
- Monitorovanie a manažment bezpečnostných incidentov
- Periodické hodnotenie zraniteľnosti
- Zálohovanie

Komponenty bezpečnostnej infraštruktúry:

#### Platforma riadenia identít

Na zabezpečenie správy zariadení datacentra s riadeným prístupom je požadovaný centrálny autentifikačný, autorizačný a zúčtovací systém (ďalej označovaný ako AAA). AAA systém bude zabezpečovať centrálny prvok pre overovanie používateľov a zariadení pripájajúcich sa do infraštruktúry. Pre samotnú realizáciu AAA služieb bude vytvorené redundantné riešenie s možnosťou lokálnej autentifikácie. Systém riadenia prístupov bude možné prepojiť aj s externým zdrojom identít. Monitorovanie bezpečnostných incidentov

#### SIEM (Security Information and Event Management)

Systém pre monitorovanie biznis kritických systémov a sieťovej infraštruktúry z pohľadu bezpečnostných udalostí. Veľké dátové prostredia musia spracovávať v reálnom čase množstvo dát s čím súvisia monitorovacie aktivity. Bezpečnostné incidenty sú vyhodnocované zo zberu údajov.

#### Firewall

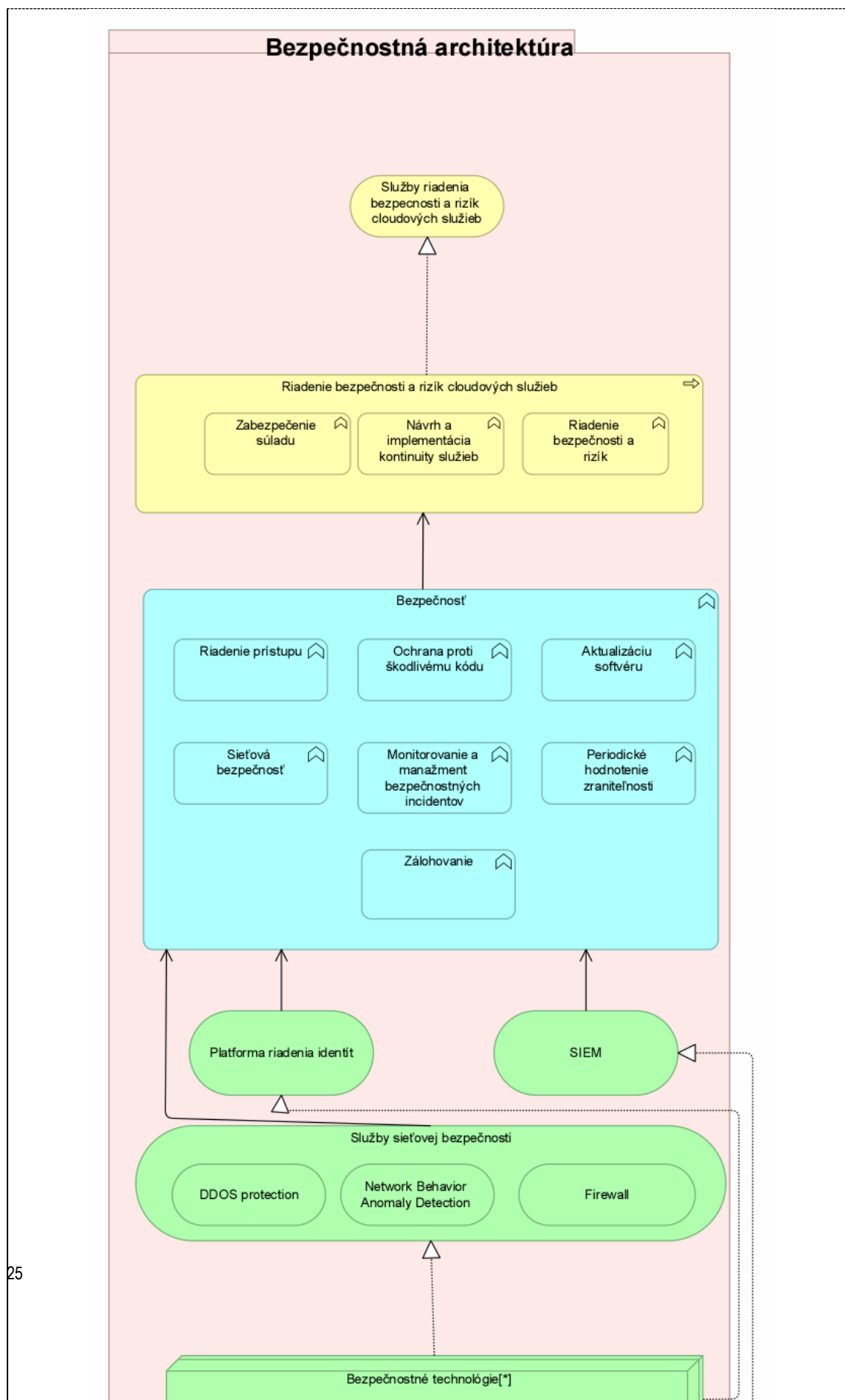
Firewall poskytuje stavovú inšpekciu a kontrolu sieťovej prevádzky, vrátane aplikačnej kontroly, ako aj možnosť kontroly na L2 a L3, vrátane tradičného blokovania portov. Je tiež schopný kontrolovať aplikácie meniace porty a proaktívne zabráňovať sieťovým hrozbám. Tiež poskytuje možnosť kontroly na základe rôznych politík, na základe používateľov, zariadení, rolí, typov aplikácií a profil hrozieb, pričom na perimetri dátového centra sú umiestnené fyzické verzie zariadenia.

#### Network behavior Anomaly Detection (NBAD)

Systém poskytujúci viditeľnosť do dátových tokov a sleduje anomálie. Je schopný snímať dátové toky zo zariadení na to určených. Následkom sledovania dátového toku je možné detekovať aj tzv. "day-zero" útoky, APT (advanced persistent threat – pokročilé ohrozenie), vnútorné hrozby a ostatné problémy prekračujúce perimetrovú obranu. Systém spolupracuje a je vyhodnocovaný do systému SIEM.

#### DDOS protection

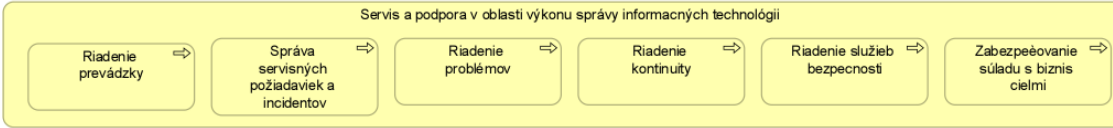
Systém poskytujúci viditeľnosť do dátových tokov určený na ochranu pred DDOS (distribúovaný útok zahltením)



Kritéria kvality	<b>Spresnenie kritérií kvality:</b> Odkazy na relevantné identifikátory kritérií kvality v prílohe Kritéria kvality.
Q14 - Komplexnosť spracovania	
Riziká	<b>Spresnenie identifikovaných rizík:</b> Odkazy na relevantné identifikátory rizík v prílohe Riziká.
R 24 - Nedostatočné vybudovanie bezpečnostných technológií a komponentov pre špecifické ISVS	
Prílohy	Diagramy, modely, obrázky v plnom rozlíšení
Tabuľka 2 Riziká Tabuľka 3 Kritéria kvality	Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

### 2.4.3 Prevádzka

Tabuľka 16 Prevádzka - budúci stav

Súhrnný popis	
<p>Pre zabezpečenie prevádzky IKT infraštruktúry pre cloudové služby je možné použiť rovnaký model ako je používaný na MV SR v súčasnosti, t.j.</p> <ul style="list-style-type: none"> <li>• L1 podporu zabezpečujú interní zamestnanci call centra a centrá podpory</li> <li>• L2 podporu zabezpečujú dodávatelia a interní zamestnanci MV SR</li> <li>• L3 podporu zabezpečujú dodávatelia a interní zamestnanci MV SR (v prípade IS, ktoré si MV vyvíjalo vo vlastnej réžii.)</li> </ul> <p>Kapacitne bude potrebné na strane MV SR zabezpečiť dostatok interných zdrojov pre zabezpečenie prevádzky IKT infraštruktúry pre cloudové služby ako aj SLA zmluvy s budúcimi dodávateľmi riešenia.</p> <p>Procesy riešené v rámci prevádzky sú zobrazené na nižšie uvedenej schéme.</p>	
	
Kritéria kvality	<b>Spresnenie kritérií kvality:</b> Odkazy na relevantné identifikátory kritérií kvality v prílohe Kritéria kvality.
Q15 - Plnenie požiadaviek na prevádzku	
Riziká	<b>Spresnenie identifikovaných rizík:</b> Odkazy na relevantné identifikátory rizík v prílohe Riziká.
<p>R 25 - Služby IaaS nebudú poskytované v dostatočnej kvalite (vyskytne sa veľké množstvo chýb, dlhé doby odozvy a podobne).</p> <p>R 26 - Organizačné zabezpečenie podpory nedokáže včas vybudovať štruktúru s dostatočnými skúsenosťami a kvalifikáciou.</p> <p>R 27 - Reakcia na vyriešenie metodicko-procesnej požiadavky bude príliš dlhá.</p>	

Prílohy	Diagramy, modely, obrázky v plnom rozlíšení
Tabuľka 2 Rizika Tabuľka 3 Kritéria kvality Tabuľka 31 Dodávateľská podpora Tabuľka 32 Podpora vlastnými zdrojmi Tabuľka 33 Prostriedky v prenájme	Odkazy na relevantné súbory. Prílohy obsahujú informácie vo forme modelov.

## 2.4.4 Ekonomická analýza

Tabuľka 17 Ekonomická analýza - budúci stav

Súhrnný popis

Výdavky na vybudovanie „Cloud Ministerstva vnútra SR“ budú vykompenzované pozitívnym dopadom na výdavky vynakladané na správu a prevádzku individuálnych systémov jednotlivých rezortov.

**Všetky sumy uvedené v tejto ekonomickej analýze sú bez DPH.**

**Kvantifikované prínosy**

- Zefektívnenie verejnej správy:
  - Zvýšenie produktivity práce (ušetrenie času pracovníkov) vďaka prerozdeleniu úloh a štandardizácií,
  - Efektívnejšie využívanie a zdieľanie zdrojov IKT,
- Lepšia prevádzka informačných systémov (zníženie TCO):
  - Odborné kapacity IKT budú koncentrované,
  - Zníženie celkového počtu komponentov DC v rámci štátnej správy a ich unifikácia

**Kvalitatívne prínosy**

- Zlepšenie kvality riešenia:
  - Súlad s národnými štandardami pre ISVS, ako aj medzinárodnými normami a štandardami,
  - Implementácia centralizovanej, zdieľanej, škálovateľnej a stabilnej hardvérovej infraštruktúry pre IaaS
- Zlepšenie riadenia ľudských zdrojov:
  - Rast kvality ľudských zdrojov.
- Naplnenie dopytu po inovatívnych riešeniach.

Čistá súčasná ekonomická hodnota (ENPV) = 6 421 240,84 EUR

Rok návratu investície (PBP) = 8.

Tabuľka 18: Prehľad ukazovateľov efektivity

Ukazovateľ efektivity	Hodnota	Požadovaná hodnota	Vyhovuje
Čistá súčasná hodnota projektu	6 421 240,84 €	> 0	Áno
Rok návratu investície	8. rok	< 10 rokov	Áno

Tabuľka 19: Prehľad nákladov a prínosov

Obdobie	Cashflow projektu						Čistá súčasná hodnota z projektu		
	Finančný cashflow			Ekonomický cashflow			koeficient obdobia	Finančná (FNPV)	Ekonomická (ENPV)
	Alternat. A	Alternat. B	rozdiel	Alternat. A	Alternat. B	rozdiel			
t1	-11 068 072,32	-37 001 907,00	-25 933 834,68	-11 068 072,32	-36 929 907,00	-25 861 834,68	0	-25 933 834,68	-25 861 834,68
t2	-19 180 568,60	-1 222 969,00	17 957 599,60	-19 180 568,60	-838 969,00	18 341 599,60	1	17 266 922,69	17 468 190,10
t3	-9 335 465,28	-1 222 969,00	8 112 496,28	-9 335 465,28	-286 969,00	9 048 496,28	2	7 500 458,84	8 207 252,86
t4	-2 445 938,00	-7 490 932,00	-5 044 994,00	-2 445 938,00	-5 852 932,00	-3 406 994,00	3	-4 484 981,30	-2 943 089,52
t5	-4 191 230,80	-7 490 932,00	-3 299 701,20	-4 191 230,80	-5 430 932,00	-1 239 701,20	4	-2 820 598,41	-1 019 905,25
t6	-7 100 052,13	-9 490 932,00	-2 390 879,87	-7 100 052,13	-7 008 932,00	91 120,13	5	-1 965 128,97	71 395,01
t7	-8 263 580,67	-7 490 932,00	772 648,67	-8 263 580,67	-4 706 932,00	3 556 648,67	6	610 635,46	2 654 026,00
t8	-8 263 580,67	-7 490 932,00	772 648,67	-8 263 580,67	-4 404 932,00	3 858 648,67	7	587 149,49	2 742 269,57
t9	-8 263 580,67	-7 490 932,00	772 648,67	-8 263 580,67	-4 402 932,00	3 860 648,67	8	564 566,81	2 613 038,98
t10	-8 263 580,67	-7 490 932,00	772 648,67	-8 263 580,67	-4 400 932,00	3 862 648,67	9	542 852,70	2 489 897,77
SPOLU	-86 375 649,80	-93 884 369,00	-7 508 719,20	-86 375 649,80	-74 264 369,00	12 111 280,80	SPOLU	-8 131 957,36	6 421 240,84

Poznámka: Uvedené ceny sú bez DPH

CAPEX: Výdavky potrebné pre vybudovanie IKT infraštruktúry :

- ■ Návrh, dodávka a implementácia IKT infraštruktúry pre laaS

OPEX: Výdavky potrebné pre prevádzku

- Náklady na HW maintenance,
- Náklady na Maintenance SW licencií (obnova),
- Technická asistencia pre riešenie incidentov
- Mzdové náklady pracovníkov DC,
- Spotrebný materiál
- Réžia DC (priestory, energie, technologická infraštruktúra, ....).

Celkové náklady na projekt sú zložené z hodnoty projektu CAPEX a z nákladov na prevádzku OPEX, a to samostatne pre HW a samostatne pre SW. Služby sú implementačné práce a SLA pri prevádzke.

Tabuľka 20: TCO projektu

	t1	t2	t3	t4	t5
SW produkty - sumár obstaranie	10 425 211	0	0	0	0
SW produkty - sumár prevádzka	0,00	0	0	1 792 860	1 792 860
Aplikácie - sumár obstaranie	0,00	0	0	0	0
Aplikácie - sumár prevádzka	0,00	0	0	0	0
HW sumár obstaranie	26 576 696	0	0	0	0
HW sumár prevádzka	0,00	1 222 969	1 222 969	5 698 072	5 698 072
	37 001 907	1 222 969	1 222 969	7 490 932	7 490 932

Prínosy je pre tento projekt možné vyčíslit' jednak ušetrenými investíciami do budovania samostatných DC jednotlivých rezortov podľa štandardov ISVS a jednak ušetreným časom zamestnancov používateľa. Primárnym nepriamym prínosom je umožnenie zamestnancom organizácií verejnej správy, ktorých IKT budú prevádzkované v DataCentre, venovať sa už iným činnostiam, keďže ich popis pracovných činností nebude zahrňovať manažment IKT, ktorý bude prevádzkovaný v DataCentre. Tento benefit bol vyčíslený odhadnutým počtom až 18 zamestnancov (po 2 zamestnancov ročne počas 10 rokov) s postupným nábehom.

Dominantná úspora je však v nákupe externých odborných služieb SLA, kde sme uvažovali 200% v alternatíve 1, a pri alternatíve 2 sme uvažovali nákup 100% .

Ako predpoklad sme uvažovali v alternatíve 1 individuálny nákup HW, SW a služieb rozložený v troch rokoch 30% - 50% - 20% a v alternatíve 2 sme uvažovali nákup tovarov a služieb v objeme 100% už v prvom roku. Aj pri tomto predpoklade je projekt efektívny už len z titulu centralizovaného riešenia. Ďalšia efektívnosť sa prejaví na základe CBA jednotlivých projektov IS VS, ktoré budú na DC MV prevádzkované. Úspory z VO sme neuvažovali nakoľko existuje Rámcová zmluva pre Government.

Tabuľka 21: Alternatíva "AS-IS"

P.E.	Spolu	t1	t2	t3	t4	t5	t6	t7	t8	t9	t10
1. Náklady na dodávateľa spojené s prevádzkou SW	16 169 332	2 796 714	4 661 189	1 864 476	0	402 762	1 074 032	1 342 540	1 342 540	1 342 540	1 342 540
2. Náklady na dodávateľa spojené s prevádzkou HW	45 135 220	6 693 659	11 156 098	4 462 439	0	1 342 531	3 580 082	4 475 103	4 475 103	4 475 103	4 475 103
3. Personálne náklady*	0	0	0	0	0	0	0	0	0	0	0
4. Náklady na priestory a energie	25 071 098	1 577 700	3 363 281	3 008 550	2 445 938	2 445 938	2 445 938	2 445 938	2 445 938	2 445 938	2 445 938
Spolu**	86 375 649	11 068 072	19 180 569	9 335 465	2 445 938	4 191 231	7 100 052	8 263 581	8 263 581	8 263 581	8 263 581

Kritéria kvality	<b>Spresnenie kritérií kvality:</b> Odkazy na relevantné identifikátory kritérií kvality v prílohe Kritéria kvality.
Q16 - Overiteľnosť údajov	
Riziká	<b>Spresnenie identifikovaných rizík:</b> Odkazy na relevantné identifikátory rizík v prílohe Riziká.
R 28 - Nepodariť sa dosiahnuť preukázateľné úspory podľa predpokladu. R 29 - Náklady na vybudovanie DC presiahnu rozpočet. R 30 - Náklady na prevádzku DC presiahnu rozpočet.	
Prílohy	
Tabuľka 2 Riziká Samostatná príloha č.1 – Technická špecifikácia Samostatná príloha č.2 CBA Samostatná príloha č.3 TCO HW Samostatná príloha č.4 TCO SW	