



# Strategická priorita *Vládny Cloud*

(Verzia 1)



**VLÁDNY CLOUD**



## **Autori**

*Úrad podpredsedu vlády pre investície a informatizáciu*

Richard Hollý

*Ministerstvo financií Slovenskej republiky*

Martin Dobrucký

Andrej Hajdúch

*Ministerstvo vnútra Slovenskej republiky*

Pavol Maliarik

*ITAS*

Peter Weber

Gabriel Fedorko

Peter Wolek

Peter Dostál

Peter Kováč

*PPP*

Rastislav Neczli

## **PodĎakovanie**

Za hodnotné návrhy a pripomienky ďakujeme: ÚPPVII (Lucii Fábryovej, Andri Adámek, Petrovi Bírovi), slovensko.digital (Petrovi Mihálikovi) ITAS (Júlii Steinerovej), ISACA (Ivanovi Kopáčíkovi), DEUS (Jozefovi Jankovičovi)



1	Obsah	
1	Manažérske zhrnutie	6
2	Úvod	7
2.1	Účel dokumentu	7
3	Organizačné zabezpečenie	8
3.1	Základné rozdelenie činností	8
3.2	Role a procesy	10
4	Služby Vládneho cloudu	13
5	IaaS	14
5.1	Ciele	14
5.2	Aktuálny stav	14
5.3	Architektúra	16
5.4	Služby vládneho cloudu	24
5.5	Rozvoj IaaS služieb	25
6	PaaS	26
6.1	Ciele	26
6.2	Aktuálny stav	26
6.3	PaaS katalóg	28
6.4	PaaS automatizácia	31
6.5	SLA PaaS služieb	33
6.6	Spôsoby riešenia riadenia licencií SW	34
7	SaaS	37
7.1	Ciele	37
7.2	Aktuálny stav	37
7.3	Spôsoby riešenia	37
8	SLA služieb	40
8.1	Ciele	40
8.2	Štandardy	40
8.3	Terminológia	40
8.4	Aktuálny stav	40
8.5	Špecifiká cloud computingu ovplyvňujúce nastavenie SLA	41
8.6	SLA komponenty	41
8.7	Parametre SLA	41
9	Hybridný vládny cloud	44
9.1	Ciele	44
9.2	Typické situácie použitia služieb vládneho cloudu, kedy je možné očakávať lepšiu ekonomickú efektívnosť v prípade využitia hybridného vládneho cloudu	45
9.3	Spôsoby riešenia	46



10	Podpora „DR a BCP“ pomocou cloudových služieb	49
10.1	Cieľ	49
10.2	Business Continuity Planning alebo BCP	50
10.3	Disaster Recovery alebo DR	50
10.4	Aktuálny stav	51
10.5	Plánované využitie DR pre aplikácie	55
11	Migrácie do vládneho cloudu	56
11.1	Ciele	56
11.2	Aktuálny stav	57
11.3	Spôsob financovania migrácii	62
12	Bezpečnosť	63
12.1	Ciele	63
12.2	Štandardy	63
12.3	Legislatíva	63
12.4	Cloud špecifiká	64
12.5	Bezpečnostná politika	66
12.6	Organizácia informačnej bezpečnosti	66
12.7	Personálna bezpečnosť	67
12.8	Riadenie aktív	67
12.9	Riadenie a kontrola prístupov a identít	67
12.10	Šifrovanie	68
12.11	Fyzická bezpečnosť a bezpečnosť prostredia	68
12.12	Bezpečnosť prevádzky	69
12.13	Bezpečnosť komunikačnej infraštruktúry	69
12.14	Vývoj, zavádzanie a údržba systémov	69
12.15	Vzťahy s dodávateľmi	70
12.16	Riadenie incidentov	70
12.17	Havarijné plánovanie a BCP	71
12.18	Kontrola dodržovania bezpečnosti (compliance)	71
13	Certifikácia a akreditácia služieb	72
13.1	Ciele	72
13.2	Spôsoby riešenia	73
14	Model(y) spoplatnenia	75
14.1	Ciele	75
14.2	Pravidlá pre stanovovanie cien cloudových služieb	76
14.3	Procesy vysporiadania za spotrebované cloudové služby	79
15	Prevádzka	80
15.1	Ciele	80
15.2	Riadenie prevádzky	81
15.3	Štandardizácia procesov, prostredí a konsolidácia architektúry	81
15.4	Onboarding	81
16	Legislatívne požiadavky	82

16.1	Navrhované opatrenia	83
17	Plánovanie a migrácia	84
17.1	Akčný plán podľa NKIVS	84
17.2	Kľúčové strategické programy/projekty	85
18	Záver	94
19	Odkazy na externé zdroje	94
20	Slovník pojmov	96
21	Prílohy	99
21.1	Príloha č.1 - Popis biznis procesov	99
21.2	Príloha č.2 - Popis aplikačných funkcií	110
21.3	Príloha č.3 – Riadenie aktív	115
21.4	Príloha č.4 – Riadenie a kontrola prístupov a identít	117
21.5	Príloha č.5 – Bezpečnosť prevádzky	118
21.6	Príloha č.6 - Návrh komunikačnej infraštruktúry z pohľadu bezpečnosti	122
21.7	Príloha č.7 – Hybridný Cloud - Návrh užívateľských scenárov Pre Hybridný Vládny Cloud	124
21.8	Príloha č.8 – PaaS – Zdrojové dáta	128
21.9	Príloha č.9 – Ceny IaaS služieb vládneho cloudu - prepočet	128
21.10	Príloha č.10 – Ceny IaaS služieb vládneho cloudu	128
21.11	Príloha č.11 – Prehľad a popis modulov a služieb projektu DCOM	130

Obrázok 1	Sumárny pohľad na role a procesy – privátny vládny cloud	11
Obrázok 2	Sumárny pohľad na role a procesy – hybridný vládny cloud	13
Obrázok 3	Aktuálny stav nasadenia cloudových služieb vládneho cloudu	15
Obrázok 4	Úvodné hľadisko – role, prístupové kanály, služby, procesy	17
Obrázok 5	Úvodné hľadisko – aplikačné služby, aplikačné funkcie	18
Obrázok 6	Úvodné hľadisko – technologické služby, technologické komponenty, siete	19
Obrázok 7	Hľadisko biznis procesov	20
Obrázok 8	Aplikačné funkcie	21
Obrázok 9	Projektovo orientované prostredie vládneho cloudu	22
Obrázok 10	WAN a smerovanie do vnútra DC	22
Obrázok 11	Hierarchia projektovo orientovaných prostredí	23
Obrázok 12	Top 10 výrobcovia softvéru pre serverovú časť v prevádzke orgnizáciami štátnej správy	27
Obrázok 13	Typy platforiem	27
Obrázok 14	PaaS kategórie služieb	28
Obrázok 15	PaaS funkcionality	28
Obrázok 16	PaaS automatizácia a DEVOPS	31



Obrázok 17 Generický model PAAS služby - SLA 1 .....	33
Obrázok 18 Generický model PAAS služby - SLA 2 .....	34
Obrázok 19 Generický model PAAS služby - SLA 3 .....	34
Obrázok 20 Principiálna schéma prepojenia riadiacich komponentov. ....	52
Obrázok 21 Prístup klienta na DNS službu. ....	55
Obrázok 22 Podiel typov IS v rezorte - príklad .....	59
Obrázok 23 Jednotlivé schémy z hľadiska geografického pôsobenia a rozsahu .....	74
Obrázok 24 Príklad použitia cien cloudových služieb .....	77
Obrázok 25 Príklad zohľadnenia prínosov pri používaní cloudových služieb .....	77
Obrázok 26 Štruktúra výdavkov na IaaS služby vládneho cloudu počas 10 rokov .....	78
Obrázok 27 Predpokladaný nárast poskytovaných cloudových IaaS služieb riešením IaaS časť 1 .....	79
Obrázok 28 Dejová línia pre Efektivitu verejnej správy .....	84

# 1 Manažérske zhrnutie

Národná koncepcia informatizácie verejnej správy (ďalej len „NKIVS“) ustanovuje<sup>1</sup> 10 strategických priorít informatizácie verejnej správy:

- 1 Multikanálový prístup,
- 2 Interakcia s verejnou správou, životné situácie a výber služby navigáciou,
- 3 Integrácia a orchestrácia,
- 4 Rozvoj agendových informačných systémov,
- 5 Využívanie centrálnych spoločných blokov,
- 6 Riadenie údajov a Big data (Manažment údajov),
- 7 Otvorené údaje,
- 8 **Vládny cloud,**
- 9 Komunikačná infraštruktúra,
- 10 Kybernetická bezpečnosť.

NKIVS ku každej strategickej priorite informatizácie verejnej správy vysvetľuje jej cieľ, prístup k riešeniu a tiež rámcový architektonický model. Tento dokument ďalej nadväzuje na NKIVS a rozširuje kapitolu 6.2.8 Vládny cloud. Dokument je zároveň vstupom pre Detailný akčný plán informatizácie verejnej správy, pričom v rámci kapitoly 18 Plánovanie a migrácia definuje plán aktivít v oblasti rozvoja vládneho cloudu.

Zavedenie vládneho cloudu na Slovensku je zakotvené ako jedna z priorít a špecifických cieľov už viacerými strategickými dokumentami<sup>2</sup>, pričom viaceré aktivity prebiehajú už od roku 2013. Doterajšími investíciami do rozvoja hlavných dátových centier štátu boli implementované IaaS služby, ktoré sú už v súčasnosti poskytované organizáciám štátnej správy a samosprávy. Vzhľadom na to, že do roku 2013 neboli cloudové služby poskytované centralizovaným spôsobom, vznikajú špecifické prevádzkové a organizačné požiadavky. Tie sú bližšie popísané v kapitolách 4 Organizačné zabezpečenie a 16 Prevádzka. Vzhľadom na vyššie uvedené je značná časť kapitoly 6 IaaS venovaná popisu aktuálneho stavu. Kapitola 11 Podpora „DR a BCP“ pomocou cloudových služieb a kapitola 13 Bezpečnosť odrážajú koncepciu nastavovanú predovšetkým realizáciou IaaS služieb vládneho cloudu.

Dôležitou iniciatívou od roku 2014 je odštartovanie presunu jednotlivých ISVS do vládneho cloudu. Posúdenie aktuálneho stavu migrácie IKT jednotlivých rezortov a návrh ďalšieho postupu je uvedený v kapitole 12 Migrácie do vládneho cloudu. Vzhľadom na požiadavky rezortov, ktoré už vyplynuli z plánovania presunu ISVS do vládneho cloudu, je v dokumente venovaná značná pozornosť aj príprave platformových služieb vládneho cloudu (PaaS) v kapitole 7.

Úrovniam poskytovania služieb (SLA) cloudových služieb je venovaná kapitola 9 SLA služieb, ktorá je dôležitá aj preto, že sa problematika vládneho cloudu koncepčne posúva od realizácie privátneho vládneho cloudu k využívaniu služieb public cloudu. Typické prípady použitia a možné spôsoby riešenia sú uvedené v kapitole 10 Hybridný vládny cloud. V prostredí (nie len) hybridného cloudu je základným kameňom pre budovanie dôvery v cloudové služby nezávislé uistenie pre všetkých zúčastnených, že poskytované služby sú bezpečné a plne v súlade s očakávanými parametrami služieb. Zároveň všetci odberatelia potrebujú mať istotu, že kvalita služby je postavená na udržateľných základoch v súlade s legislatívou a best practice. Čo takéto uistenie predstavuje a aký je navrhovaný postup v tejto problematike je uvedené v kapitole 14 Certifikácia a akreditácia služieb.

V súčasnosti je téma spoplatnenia vládneho cloudu pre odberateľov nastavená jednoducho – je poskytovaný bezplatne. Aj vzhľadom na nové koncepty, ako je napr. postupný prechod do prostredia hybridného cloudu, nabera na dôležitosť problematika oceňovania a prípadného spoplatňovania služieb vládneho cloudu, ktorou sa zaoberá kapitola 15 Model(y) spoplatnenia.

Finálne kapitola 18 Plánovanie a migrácia obsahuje prehľad navrhovaných aktivít pre túto strategickú prioritu, ktoré budú súčasne zaradené v Detailnom akčnom pláne.

<sup>1</sup> Odkazy na externé zdroje - [6]

<sup>2</sup> Odkazy na externé zdroje - [2], [3], [4], [5]

## 2 Úvod

### 2.1 Účel dokumentu

Účelom tohto dokumentu je, v zmysle úlohy B.5. uznesenia vlády SR č. 437/2016, podrobne rozpracovať jednotlivé dokumenty NKIVS, ktoré sú uvedené v kapitole 9 Súvisiace dokumenty. V tomto prípade ide o dokument Strategická priorita: Vládny cloud.

Tento dokument v zmysle NKIVS obsahuje definíciu problematiky, ciele v danej oblasti, návrh organizačného zabezpečenia, výber strategického prístupu a použitých alternatív, návrh riešenia, posúdenie problémov a rizík, vyhodnotenie legislatívnych požiadaviek a plánovanie realizácie v podobe konkrétnych pracovných balíčkov. Dokument v rámci svojich výstupov v časti Plánovanie a migrácia poskytne vstupy pre Detailný akčný plán informatizácie verejnej správy 2016-2020. Zodpovednosť za detailné riešenie navrhovaných pracovných balíčkov, t.j. napr. príprava legislatívy, vypracovanie reformného zámeru, štúdie realizovateľnosti a následnú realizáciu formou zabezpečenia implementácie príslušného projektu, resp. projektov, má gestor podľa nemu prislúchajúcej kompetencie alebo objektívne určený gestor.

#### 2.1.1 Cieľová skupina

Dokument je určený pre OVM, a to pre riadiacich zamestnancov OVM, a najmä architektov na úrovni národnej (strategickej) a segmentovej architektúry a architektúry riešení konkrétnych informačných systémov verejnej správy.

##### 2.1.1.1 Úrad podpredsedu vlády Slovenskej republiky pre investície a informatizáciu ako ústredný orgán štátnej správy

Podľa § 4 zákona č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov má Úrad podpredsedu vlády Slovenskej republiky pre investície a informatizáciu (ďalej len „ÚPPVII“) centrálnu zodpovednosť za koordináciu budovania informačných systémov verejnej správy na národnej a medzinárodnej úrovni. Túto kompetenciu musí uplatňovať vo vzťahu k povinným osobám podľa § 3 ods. 3 citovaného zákona, ktorým úrad schvaľuje koncepcie rozvoja informačných systémov pre nimi spravované informačné systémy, vrátane ich architektúry, prípadne použitých technológií.

##### 2.1.1.2 Manažment orgánov verejnej moci

Aj v nasledujúcom období bude rozvoj nových, či modernizácia existujúcich informačných systémov v gescii jednotlivých povinných osôb<sup>3</sup>. Realizácia priorít vlády SR a rovnako aj naplnenie cieľov operačných programov Operačný program Integrovaná infraštruktúra a Operačný program Efektívna verejná správa si však vyžadujú zmenu prístupu k riadeniu IKT projektov na úrovni manažmentu odborných útvarov OVM, ktorých agendy majú novo budované alebo modernizované informačné systémy podporovať. Pre každý rozvojový program alebo projekt je potrebné, aby na úrovni vedenia OVM bola presadzovaná a následne monitorovaná požiadavka na dosiahnutie maximálnej efektívnosti z pohľadu realizácie programov a projektov, ale hlavne z pohľadu očakávaných výstupov pre používateľov. Špecifická situácia je v miestnej územnej samospráve, kde prípravu a realizáciu rozvojových projektov bude zabezpečovať aj Datacentrum elektronizácie územnej samosprávy Slovenska (ďalej len „DEUS“), napr. pre malé obce.

##### 2.1.1.3 Architekti na úrovni strategickej architektúry verejnej správy

Úrad podpredsedu vlády SR pre investície a informatizáciu, aj v úzkej spolupráci s Ministerstvom vnútra SR<sup>4</sup>, pre plnenie odborných úloh v oblasti informatizácie verejnej správy zastrešuje architektonickú

<sup>3</sup> V zmysle § 3 zákona č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

<sup>4</sup> V zmysle systému vzájomnej koordinácie medzi Operačným programom Integrovaná infraštruktúra a Operačným programom Efektívna verejná správa.



kanceláriu informačných systémov verejnej správy<sup>5</sup> (ďalej len „AKVS“), ktorá vykonáva na úrovni strategickej architektúry kľúčové úlohy v týchto základných oblastiach:

- v oblasti správy, riadenia a metodickej podpory architektúr verejnej správy SR,
- v oblasti dohľadu nad realizáciou architektúr verejnej správy SR,
- v oblasti zabezpečenia podpory programov a projektov povinných osôb.

AKVS je zodpovedná za schválenie referenčnej architektúry navrhutej napr. na základe architektúry konkrétnych riešení. Je nutné zabezpečiť, aby bol proces zavádzania a rozvoja architektúr metodicky a koncepcne riadený. Preto

je potrebné, aby boli z pozície AKVS pre celú verejnú správu navrhnuté také výstupy, ktoré tento proces plne podporia. Ide o rôzne architektonické štandardy, rámce, metodiky a iné prostriedky.

V oblasti budovania architektúry verejnej správy SR bude dôraz AKVS kladený najmä na správu a riadenie strategickej architektúry verejnej správy SR a v gescii architektov na úrovni segmentov verejnej správy aj na správu a riadenie jednotlivých segmentových architektúr a architektúr konkrétnych riešení.

Podpora projektov zabezpečí, popri vzdelávaní architektov jednotlivých povinných osôb, mechanizmus spolupráce a spoločnú platformu koordinácie a kooperácie jednotlivých architektov verejnej správy SR. Dohľad AKVS nebude zameraný len na kontrolné funkcie, ale v prvom rade bude slúžiť ako podpora a pomoc pre architektov jednotlivých inštitúcií verejnej správy práve pri správe a riadení ich segmentových architektúr v súlade s centrálnymi riadenými architektúrami verejnej správy SR.

#### 2.1.1.4 Architekti na úrovni segmentovej architektúry

Zodpovední za tvorbu, definovanie, udržiavanie a rozvoj segmentových architektúr jednotlivých rezortov, subjektov samosprávy alebo architektúr spoločných modulov, ako aj architektúr jednotlivých riešení sú architekti povinných osôb. Títo sú metodicky riadení AKVS, ako vlastníkom a gestorom strategickej architektúry verejnej správy.

Segmentoví architekti prostredníctvom vypracovania a pravidelnej aktualizácie segmentovej architektúry a z nej odvodené konceptie rozvoja informačných systémov (KRIS) ich rezortu zabezpečujú rozvoj svojho informačného prostredia v súlade so strategickou architektúrou verejnej správy a princípmi informatizácie uvedenými v tomto dokumente. Zároveň tak definujú a uskutočňujú všetky činnosti potrebné na ich realizáciu a zabezpečujú dohľad nad architektúrou jednotlivých riešení vo svojom segmente (v súlade s referenčnou architektúrou).

## 3 Organizačné zabezpečenie

### 3.1 Základné rozdelenie činností

Nasledujúce rozdelenie činností spresňuje úlohu B1. uznesenia vlády SR č. 247/2014 (ďalej len „uznesenie“) na základe kapitoly 6. Opatrenia na zabezpečenie centralizácie DC štátu predmetného materiálu Návrh centralizácie a rozvoja dátových centier v štátnej správe.

Navrhované rozdelenie činností zohľadňuje aktuálnu situáciu, ktorá nastala po vzniku Úradu podpredsedu vlády pre investície a informatizáciu a schválení NKIVS.

#### 3.1.1 Činnosti ÚPPVII

ÚPPVII ako nositeľ koordinačnej, riadiacej a kontrolnej kompetencie bude v úzkej spolupráci, a po prerokovaní s MV SR a MF SR, realizovať najmä nasledujúce opatrenia:

1. ustanoviť pravidlá poskytovania a využívania cloudových služieb a spôsob vymáhania práv a povinností,
2. riadenie zmluvných vzťahov pre zabezpečenie poskytovania cloudových služieb odberateľom,
3. zostaviť, riadiť, koordinovať a dohliadať na plán implementácie centralizácie a rozvoja DC,
4. vytvoriť a viesť katalóg cloudových služieb so zoznamom technických a funkčných parametrov o službe,

---

<sup>5</sup> V zmysle dokumentu Informácia o postupe zavedenia architektúry verejnej správy v SR.

5. vyhodnocovať spotrebu, požiadavky a stav služieb, poskytovať výstupy pre tvorbu rozpočtu a efektívne pridelovanie finančných prostriedkov na základe plánovanej a skutočnej spotreby cloudových služieb,
6. zabezpečovať koordináciu požiadaviek používateľov, dohliadať na kvalitu a vysporiadanie profesionálnych vzťahov (SLA),
7. rozhodovať v prípade sporu a nedodržovania SLA,
8. vykonávať audit plnenia kritérií ustanovených pre cloudové služby a súvisiace informačné systémy z hľadiska ich výkonnosti, zabezpečenia a iných parametrov dohodnutých v podmienkach používania,
9. štandardizovať kategorizáciu cloudových služieb podľa úrovne bezpečnosti v nadväznosti na kategorizáciu dát,
10. upraviť práva a povinnosti prevádzkovateľov a používateľov cloudových služieb štátu prostredníctvom pripravovaného zákona o ITVS<sup>6</sup>,
11. vykonávať akreditáciu Poskytovateľov cloudových služieb v SR a EU, ktorí môžu poskytovať služby v hybridnom cloude a audit služieb poskytovaných týmito Poskytovateľmi,
12. vykonávať funkciu Sprostredkovateľa cloudových služieb v hybridnom cloude vo fáze obstarávania služby i vo fáze poskytovania služby. Za týmto účelom vybudovať ISVS sprostredkovateľa cloudových služieb.

### 3.1.1 Činnosti MV SR

MV SR ako nositeľ kompetencie poskytovateľa a prevádzkovateľa IaaS a PaaS cloudových služieb bude vykonávať najmä tieto opatrenia:

13. poskytovať bezpečné cloudové služby a plniť záväzky SLA poskytovaných služieb,
14. starať sa o vývoj a správu služieb, systematický rozvoj zdrojov a dodávateľského reťazca pre jednotlivé poskytované cloudové služby,
15. dodržiavať architektúru cloudu ustanovenú prílohou č. 7 výnosu MF SR č. 55/2014 Z. z. o štandardoch pre ISVS (ďalej aj ako „výnos o štandardoch“),
16. optimalizovať poskytované zdroje,<sup>7</sup>
17. analyzovať a riešiť prevádzkové udalosti v súlade s dohodnutými podmienkami,
18. vykonávať nápravné opatrenia po zacytení definovanej prevádzkovej udalosti,
19. poskytovať informácie o stave poskytovaných cloudových služieb pre ÚPPVII,
20. oboznamovať určené osoby odberateľa o definovaných prevádzkových udalostiach,
21. generovať a poskytovať dohodnuté zostavy a štatistiky pre ÚPPVII a odberateľov,
22. vypracovať bezpečnostný projekt, zaviesť bezpečnostné procesy a implementovať bezpečnostné opatrenia,
23. poskytovať dohodnuté podklady pred umiestnením služby do katalógu cloudových služieb a pri vykonávaní auditu.

### 3.1.2 Činnosti DC MF SR a DC MV SR

MV SR a MF SR ako nositelia kompetencie riadenia a zabezpečovania prevádzky DC štátu budú vykonávať tieto opatrenia:

24. V spolupráci s ÚPPVII, participovať na:
  - a) plánovaní a príprave ponuky služieb housingu v DC,
  - b) zmenách existujúcich služieb housingu v DC,
  - c) rozvoji zdrojov potrebných pre prevádzku týchto služieb,
25. zabezpečovať a konsolidovať technické, organizačné a procesné podmienky fungovania DC,
26. analyzovať a riešiť prevádzkové udalosti v súlade s dohodnutými podmienkami,
27. vykonávať nápravné opatrenia po zacytení definovanej prevádzkovej udalosti,
28. poskytovať informácie o využívaní DC pre ÚPPVII.

---

<sup>6</sup> Návrh legislatívneho zámeru zákona o výkone správy v oblasti informačných technológií verejnej správy bol schválený 8.12.2015

<sup>7</sup> Predovšetkým z pohľadu možného zdieľania zdrojov, za dodržania uzatvorených SLA.

### 3.1.3 Činnosti DEUS<sup>8</sup>

29. poskytovať podporu migrácie do vládneho cloudu pre subjekty samosprávy,
30. poskytovať bezpečné cloudové služby a plniť záväzky SLA poskytovaných služieb pre subjekty samosprávy,
31. zabezpečovať koordinačné aktivity medzi subjektami samosprávy a prevádzkovateľmi vládneho cloudu,
32. poskytovať dohodnuté podklady pred umiestnením služby do katalógu cloudových služieb a pri vykonávaní auditu,
33. realizovať uplatňovanie cenových modelov využívania DCOM a DC ako súčastí vládneho cloudu smerom k subjektom samospráv.

### 3.1.4 Činnosti povinných osôb

Prostredníctvom správcov informačných systémov verejnej správy je potrebné vykonávať tieto opatrenia:

34. vypracovať a priebežne aktualizovať plán postupnej migrácie ISVS do vládneho cloudu,
35. zabezpečiť v spolupráci s ÚPPVII a prevádzkovateľmi DC štátu implementáciu plánu migrácie ISVS do vládneho cloudu,
36. postupovať v súlade s navrhnutými pravidlami pre využívanie cloudových služieb,
37. manažovať prechod na cloudové služby vo svojom rezorte.

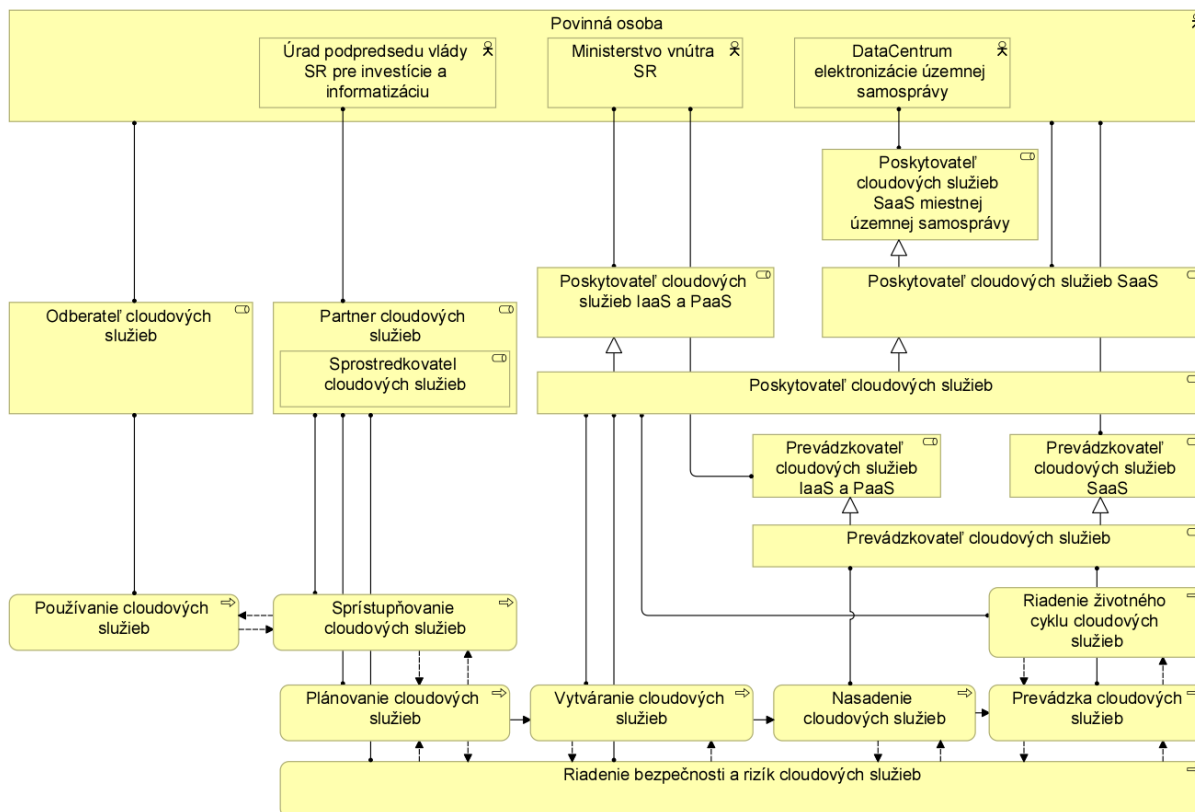
## 3.2 Role a procesy

Kapitola obsahuje detailnejšie popisy jednotlivých činností vykonávané príslušnými aktérmi.

---

<sup>8</sup> Ako špecifického poskytovateľa služieb pre samosprávu

### 3.2.1 Sumárny pohľad – privátny cloud



Obrázok 1 Sumárny pohľad na role a procesy – privátny vládny cloud

Uvedená schéma je univerzálna vo vzťahu k vytváraniu, poskytovaniu a odoberaniu IaaS, PaaS a SaaS služieb vo vládnom cloud.

*Odberateľ cloudových služieb je osoba, ktorá na základe dohody o poskytovanej úrovni cloudových služieb využíva cloudové služby poskytovateľa cloudových služieb.*

Na vyššie uvedenom obrázku sú ostatní aktéri (ÚPPVII, MV SR, DEUS) uvedení tak, aby bolo zrejmé, že sú súčasne aj povinnými osobami. Platí teda, že odberateľom služieb privátného vládneho cloudu, môže byť hociktorá organizácia VS.

Partnerom cloudovej služby je povinná osoba, ktorá sa zapája do podpory alebo pomoci činnostiam poskytovateľa cloudovej služby alebo odberateľa cloudovej služby, resp. oboch. Rola partnera cloudovej služby v sebe zahŕňa aj aktivity sprostredkovateľa cloudových služieb, ako:

*osoby, ktorá na základe zmluvného vzťahu s poskytovateľom cloudových služieb sprostredkuje využívanie, výkon a dodávku cloudových služieb.*

Túto úlohu zabezpečuje ÚPPVII. K základným aktivitám patria:

- proces sprístupňovania cloudových služieb, ktorý zahŕňa všetky kroky potrebné na začatie poskytovania cloudových služieb pre odberateľa cloudových služieb. Činnosť sprístupňovania služieb zahŕňa prijatie a spracovanie požiadavky na služby od používateľa s príslušným overením,
- proces plánovania cloudových služieb, ktorý zahŕňa aktivity potrebné na zabezpečenie efektívneho plánovania kapacít a služieb ktoré poskytuje vládny cloud.

V zmysle koordinačnej kompetencie ÚPPVII na zabezpečenie kvalitného plánovania a sprístupňovania bezpečných cloudových služieb zriadi Kanceláriu vládneho cloudu, ktorej prizvanými členmi budú aj zástupcovia jednotlivých poskytovateľov cloudových služieb, a ktorej úlohou bude pravidelné vyhodnocovanie:

- kapacity poskytovaných cloudových služieb,
- dodržiavania úrovni poskytovania cloudových služieb,
- požiadaviek na nové služby,
- požiadaviek na zmeny poskytovaných služieb,
- bezpečnosti poskytovaných cloudových služieb.

*Poskytovateľom cloudových služieb je osoba zodpovedná za správu cloud computingu a poskytovanie cloudových služieb, a to podľa podmienok dohodnutých v dohode o poskytovanej úrovni cloudových služieb.*

*Dohodou o poskytovanej úrovni cloudových služieb je zmluvný vzťah upravujúci parametre a kvalitu poskytovaných cloudových služieb, ktorá obsahuje úlohy a povinnosti zmluvných strán, pričom táto dohoda sa obvykle uzatvára medzi odberateľom cloudových služieb a poskytovateľom cloudových služieb alebo sprostredkovateľom cloudových služieb.*

Vo vyššie uvedenom obrázku je tiež uvedená špecializácia poskytovateľa cloudových služieb, pre poskytovanie služieb IaaS a PaaS vládneho cloudu, pričom túto úlohu zabezpečuje MV SR. Ďalej je uvedená špecializácia poskytovateľa cloudových služieb typu SaaS, pričom túto úlohu môže zabezpečovať hociktorá povinná osoba. Rolu poskytovateľa cloudových služieb SaaS miestnej územnej samosprávy zabezpečuje DataCentrum elektronizácie územnej samosprávy (ďalej aj ako „DEUS“).

K základným aktivitám poskytovateľa patrí:

- proces vytvárania cloudových služieb, ktorý je zameraný na tvorbu, vývoj, testovanie a údržbu implementácie cloudovej služby.

*Prevádzkovateľ cloudových služieb je osoba, ktorá na základe zmluvného vzťahu s poskytovateľom cloudových služieb zabezpečuje technické podmienky na prevádzkovanie, prepojenie a prenos cloudových služieb.*

Pre IaaS a PaaS služby vládneho cloudu je špecifickým prevádzkovateľom týchto služieb MV SR. Explicitne je tiež uvedená rola prevádzkovateľa cloudových služieb typu SaaS, aby bolo zrejmé, že povinné osoby, ktoré by sa stali poskytovateľmi SaaS služieb musia zabezpečovať aj ich prevádzku.

K základným aktivitám prevádzkovateľa patrí:

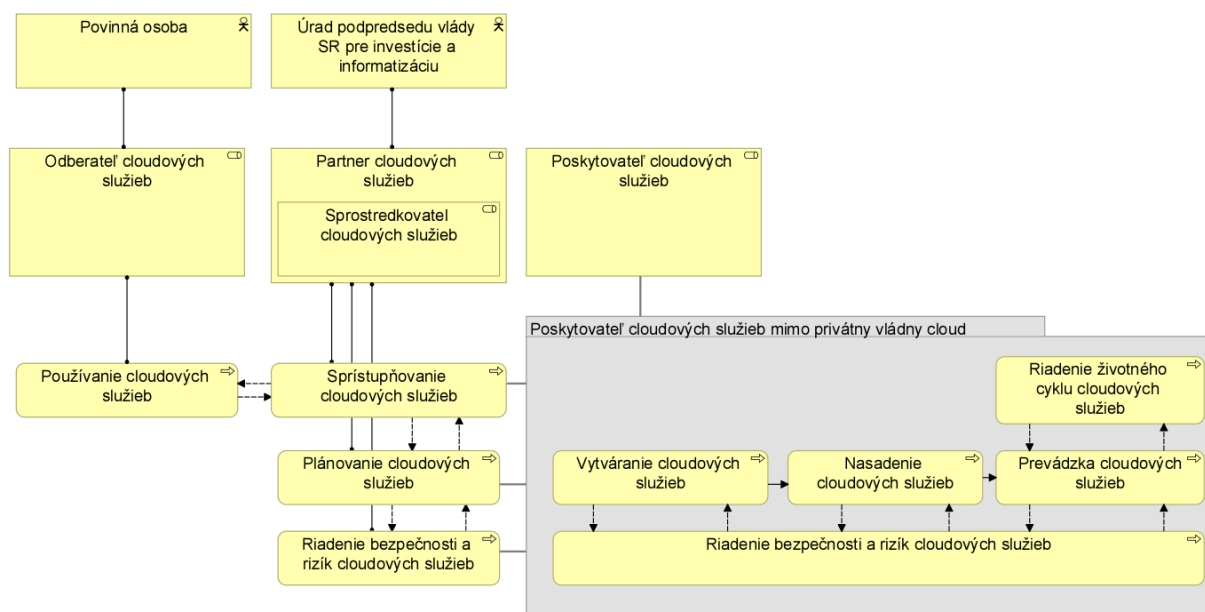
- proces nasadenia cloudových služieb, ktorý zahŕňa zabezpečenie fungovania implementácie služby a zabezpečenie jej dostupnosti v koncovom bode siete pre používateľov cloudových služieb a dosiahnutie toho, aby cloudová služba bola schopná vyriešiť požiadavky zo strany používateľov,
- proces prevádzky cloudových služieb, ktorý zahŕňa uskutočňovanie všetkých prevádzkových procesov a postupov a zabezpečenie toho, aby všetky služby a súvisiaca infraštruktúra spĺňala prevádzkové ciele.

Podrobnejšie vysvetlenie uvedených biznis procesov je v časti Príloha č.1 - Popis biznis procesov.

Prechodom inštitúcií na cloudové služby budú ministerstvá a ústredné orgány štátnej správy odbremenené od značnej časti agendy prevádzky IKT služieb. Časť osôb alokovaných v IT oddeleniach ministerstiev a ústredných orgánov štátnej správy zodpovedných za prevádzku IKT sa môžu v prípade potreby premiestniť k prevádzkovateľom cloudových služieb.

V špecifickom prostredí samosprávy dochádza pri využívaní cloudových služieb DCOM ku zvyšovaniu úrovne poskytovania IT služieb úradom a občanom a znižovaniu prevádzkových nákladov.

### 3.2.2 Sumárny pohľad – hybridný cloud



Obrázok 2 Sumárny pohľad na role a procesy – hybridný vládny cloud

Uvedená schéma je univerzálna vo vzťahu k vytváraniu a poskytovaniu IaaS, PaaS a aj SaaS služieb v hybridnom vládnom cloude, ktorý je charakteristický predovšetkým tým, že služby sú poskytované subjektami, ktoré nie sú súčasťou VS (vid. tiež kapitola 10 Hybridný vládny cloud). Dôležitú úlohu v tomto mechanizme poskytovania a odoberania cloudových služieb predstavuje Partner cloudových služieb, ktorý zabezpečuje:

- Plánovanie cloudových služieb, identifikáciu a zber požiadaviek na nové alebo zmenené cloudové služby.
- Akreditáciu existujúcich poskytovateľov cloudových služieb (prípadne môže touto aktivitou poveriť inú nezávislú organizáciu) – vid. tiež kapitola 13 Certifikácia a akreditácia služieb.
- Centralizované riešenie zmluvných vzťahov pri sprístupňovaní cloudových služieb (súčasť procesov sprístupňovania).
- Riadenie finančného spracovávaní (súčasť procesov sprístupňovania) – vid. tiež kapitola 14 Model(y) spoplatnenia.

## 4 Služby Vládneho cloudu

V zmysle súčasne platnej legislatívy<sup>9</sup> - § 54 ods. 1 rozlišujeme nasledujúce modely poskytovania cloudových služieb:

*Štandardom modelov poskytovania cloudových služieb je rozdelenie modelov poskytovania cloudových služieb najmä na model*

*a) infraštruktúra ako služba, označovaný aj ako IaaS, pri ktorom cloudová službu predstavuje poskytovanie virtualizovanej infraštruktúry ako serverov, úložísk údajov a sieťovej infraštruktúry,*

*b) platforma ako služba, označovaný aj ako PaaS, pri ktorom cloudová službu predstavuje poskytovanie hardvérovej a softvérovej platformy, potrebnej na vytvorenie a správu aplikácií, vrátane umožnenia ich navrhovania,*

<sup>9</sup> Výnos č. 55/2014 Z. z., Výnos Ministerstva financií Slovenskej republiky o štandardoch pre informačné systémy verejnej správy



vývoja, testovania a nasadzovania do produkčnej prevádzky, pričom tieto aplikácie ostávajú v správe odberateľa cloudových služieb,

c) softvér ako služba, označovaný aj ako SaaS, pri ktorom cloudovú službu predstavuje poskytovanie softvéru, vrátane aplikácií.

Pre vytváranie služieb vládneho cloudu je nevyhnutné:

1. byť v súlade s organizačným zabezpečením vládneho cloudu a dodržiavať stanovený rozsah činností (aj v prípade hybridného cloudu),
2. poskytované služby musia byť zaradené v katalógu služieb vládneho cloudu,
3. pre služby privátneho vládneho cloudu musí byť zabezpečený súlad s výnosom o štandardoch § 55 Správa cloud computingu, § 56 Vytváranie a rozvoj cloud computingu,
4. vyššie uvedené body je potrebné dodržiavať bez ohľadu na spôsob financovania.

Pre používanie služieb vládneho cloudu je nevyhnutné:

5. používané služby musia byť zaradené v katalógu služieb vládneho cloudu,
6. používanie cloudových služieb musí byť zabezpečené v súlade s výnosom o štandardoch § 57 Používanie cloudových služieb,
7. vyššie uvedené body je potrebné dodržiavať bez ohľadu na spôsob financovania.

Pre vytváranie a používanie služieb vládneho cloudu môžu byť ďalej nastavené špecifické podmienky individuálnymi operačnými programami, predovšetkým z titulu oprávnenosti výdavkov.

## 5 IaaS

### 5.1 Ciele

Vládny cloud na úrovni IaaS je budovaný od roku 2015. Cieľom tejto kapitoly je poskytnúť zhodnotenie stavu implementácie IaaS služieb a poskytnúť východisko na ďalšie rozširovanie a užitíciu poskytovaných IaaS služieb.

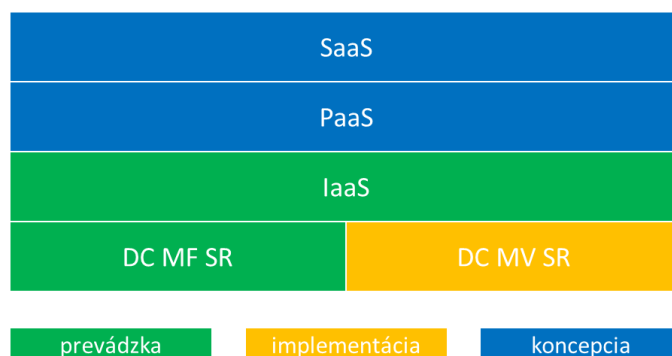
K najbližším cieľom IaaS služieb privátneho vládneho cloudu patrí:

- stabilizácia prevádzky už implementovaného riešenia iniciálnej sady IaaS služieb,
- doriešenie rozdelenia úloh a kompetencií, ktoré sú popísané v kapitole 4 Organizačné zabezpečenie,
- doriešenie disaster recovery (navrhovaným projektom IaaS časť. 2 bude realizované technologické zabezpečenie a prepojenie DC), viac popísané v kapitole 11 Podpora „DR a BCP“ pomocou cloudových služieb.

Aj napriek tomu, že boli realizované 2 projekty pre zavedenie IaaS služieb vládneho cloudu, prax a požiadavky odberateľov priniesli ďalšie konkrétne požiadavky na kvalitatívne rozšírenie služieb. Návrh rozšírenia je uvedený v kapitole 18 Plánovanie a migrácia.

### 5.2 Aktuálny stav

V súlade so schváleným strategickým materiálom „Návrh centralizácie a rozvoja dátových centier v štátnej správe“, ktorý bol vládou SR schválený dňa 21.5.2014 bola postupne od roku 2015 budovaná cloudová infraštruktúra poskytujúca služby odberateľom cloudových služieb. Na nižšie uvedenej schéme je zobrazený aktuálny stav nasadenia cloudových služieb vládneho cloudu.



Obrázok 3 Aktuálny stav nasadenia cloudových služieb vládneho cloudu

### 5.2.1 IKT infraštruktúra pre IaaS, časť 1

Projekt IKT infraštruktúra pre IaaS, časť 1, bol prvým projektom, ktorého cieľom bolo vybudovanie infraštruktúry a systémov umožňujúcich poskytovanie cloudových služieb na úrovni IaaS. Projekt bol realizovaný v rámci OPIS a bol odovzdaný do prevádzky k termínu 9/2015.

Implementáciou projektu bolo umožnené prostredníctvom samoobslužného portálu a orchestračného nástroja cSP (Cloud Service Provisioner) poskytovanie nasledovných skupín cloudových služieb:

- Virtuálny server
- Diskový priestor
- Pripojenie siete
- Sieťové služby

Minimálny rozsah nasadených IaaS služieb je na základe štúdie uskutočniteľnosti pre projekt IKT infraštruktúra IaaS, časť 1, nasledovný:

- Iniciálny počet nasadzovaných IS: 40.
- Priemerný počet prostredí per jeden IS projekt: 4.
- 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, Produkčné-2.
- Priemerný výkon jedného virtuálneho servera:
  - 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,
  - produkčné : 4 core, 128 GB RAM, 2 TB HDD.
- Na základe hore uvedených predpokladov bol implementovaný požadovaný rozsah IKT infraštruktúry pre IaaS časť 1 v nasledovnom rozsahu:
  - 2400 core,
  - 53 TB RAM,
  - 1 200 TB HDD.

#### 5.2.1.1 Aktuálna alokácia cloudových služieb – DC Kopčianska

Služba	Max	Aktuálna alokácia	jednotka	%
Virtuálny server x86	2 048	913	jadier	44,58%
Virtuálny server RISC	440	0	jadier	0,00%
Diskový priestor - "TIER 1"	18 500	3110	GB	16,81%
Diskový priestor - "TIER 2"	454 800	113153	GB	24,88%
Diskový priestor - "TIER 3"	697 400	56280	GB	8,07%



Pripojenie siete	100	15	ks	15,00%
Sieťové služby - Vytvorenie preddefinovaného sieťového modelu a základných FW pravidiel	200 000	3683	pravidiel	1,84%

### 5.2.2 IKT infraštruktúra pre IaaS, časť 2

Cieľom projektu IKT infraštruktúra pre IaaS, časť 2, bolo vybudovanie rovnakej infraštruktúry ako v rámci projektu IKT infraštruktúra pre IaaS, časť 1, a navyše implementácia technológií pre umožnenie poskytovania georedundantných služieb. Projekt bol realizovaný v rámci OPPII a bol odovzdaný do prevádzky k termínu 12/2016.

Z pohľadu kapacity IaaS služieb je možné poskytnúť rovnaký počet cloudových služieb ako pri projekte IKT infraštruktúra pre IaaS, časť 1.

### 5.2.1 IKT infraštruktúra DCOM pre prostredie samosprávy

Projekt DCOM bol prvým projektom v rámci špecifickej oblasti samosprávy, ktorého cieľom bolo vybudovanie infraštruktúry a systémov (aplikácií) umožňujúcich poskytovanie cloudových služieb na úrovni SaaS pre vybrané agendy samosprávy. Projekt bol realizovaný v rámci OPIS a bol odovzdaný do prevádzky k termínu 11/2015

## 5.3 Architektúra

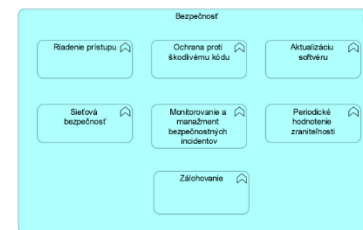
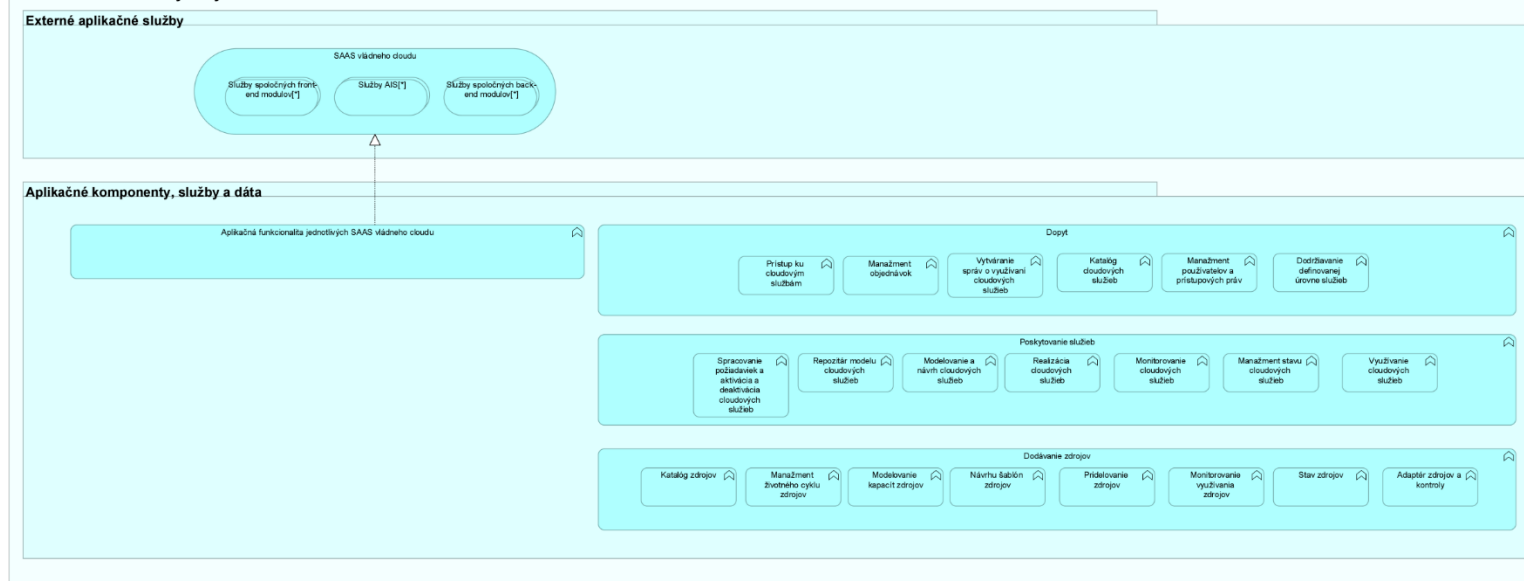
### 5.3.1 Úvodné hľadisko

Úvodné hľadisko predstavuje komplexný pohľad na všetky vrstvy architektúry. Účelom je poukázať na vzájomné vzťahy medzi jednotlivými vrstvami, pričom tieto sú ďalej detailnejšie popísané.

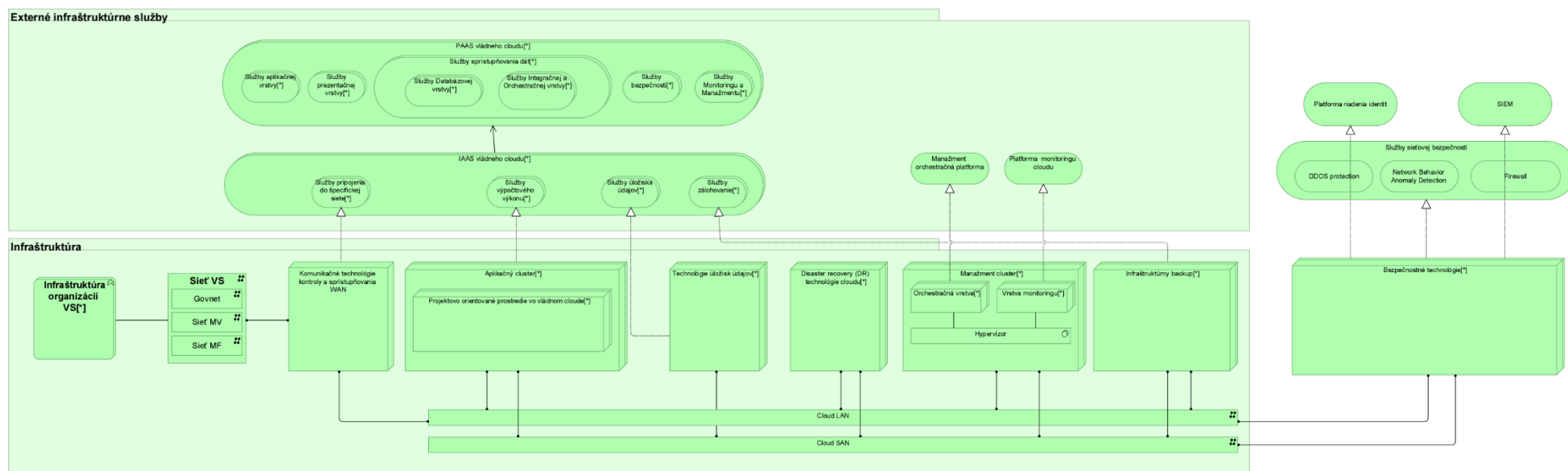




## Architektúra informačných systémov

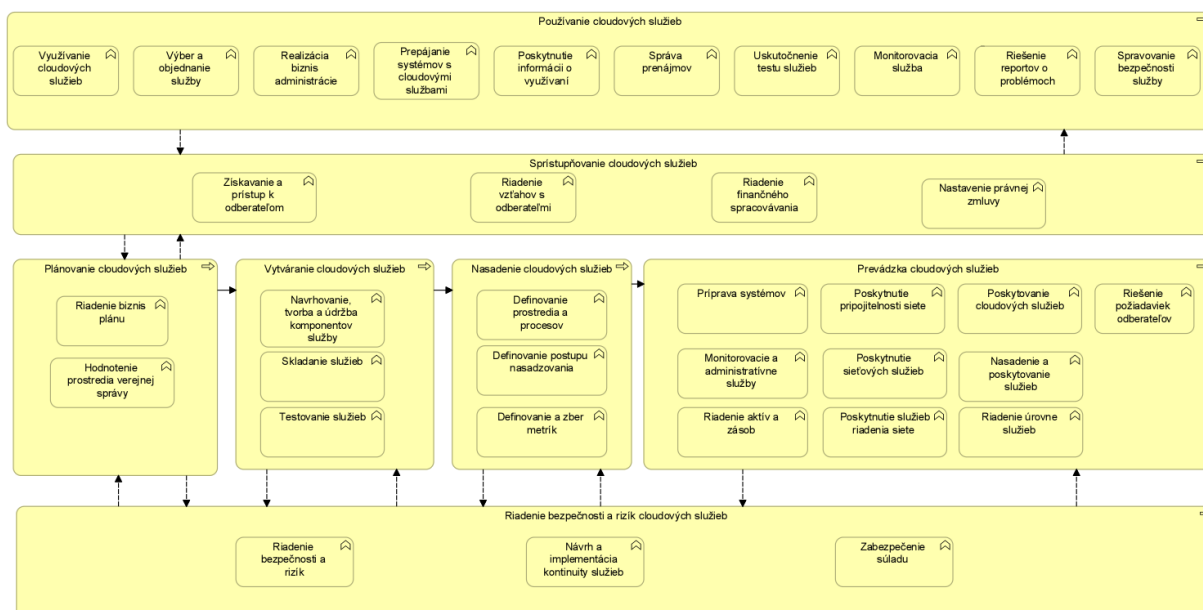


Obrázok 5 Úvodné hľadisko – aplikačné služby, aplikačné funkcie



Obrázok 6 Úvodné hľadisko – technologické služby, technologické komponenty, siete

### 5.3.2 Biznis vrstva



Obrázok 7 Hľadisko biznis procesov

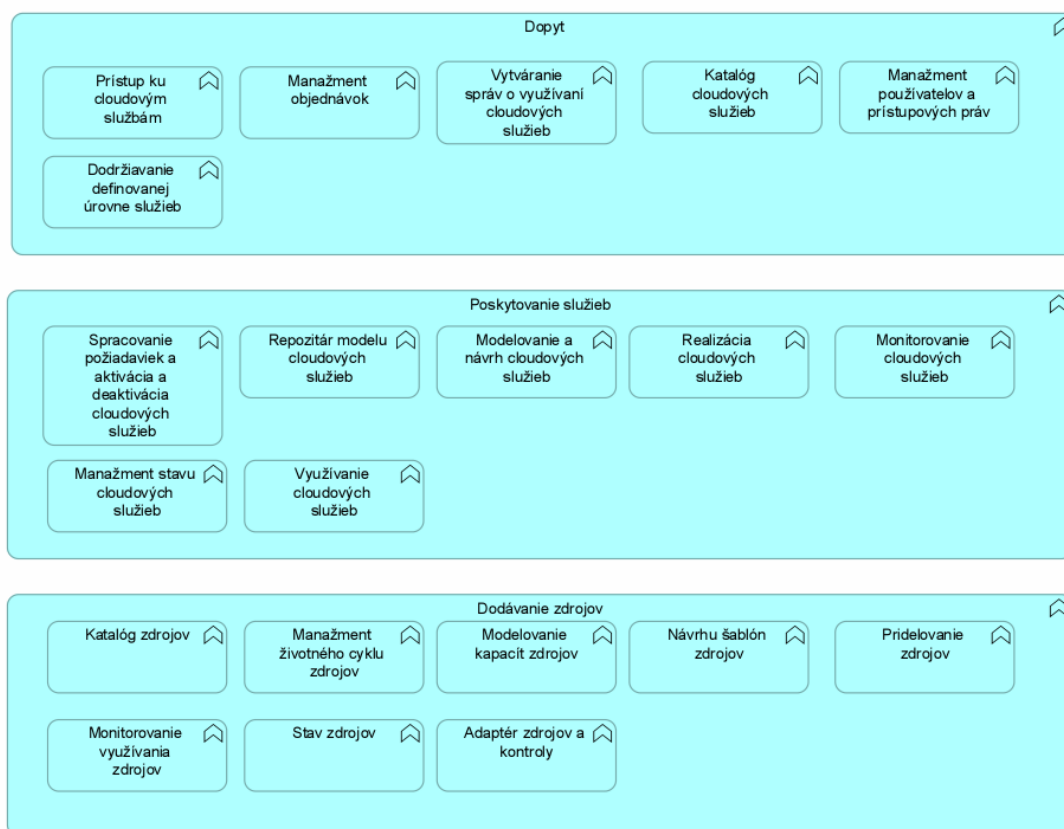
Podrobnejší popis biznis procesov je uvedený v časti Príloha č.1 - Popis biznis procesov.

### 5.3.3 Aplikačná vrstva

Požadovaná funkcionálna už pre iniciálnu verziu počíta s funkčnými komponentami, tak ako boli identifikované a sú popísané vo výnose MF SR č. 55/2014 o štandardoch pre ISVS.

Výsledná realizácia v závislosti od riešenia môže obsahovať rôznu kombináciu aplikácií, avšak musí byť dodržaná požadovaná funkčnosť a musí spĺňať najlepšie princípy (best practice) softvérového riešenia, ako napr. SOA, EDA – ako aj byť v súlade s relevantnými štandardami.

Vízia sa nevzťahuje na konkrétny technologický „stack“, a aj z pohľadu ďalšieho iteratívneho rozvoja cloudu, môže predstavovať predmet zmeny (optimalizácie v rámci úspor).



Obrázok 8 Aplikačné funkcie

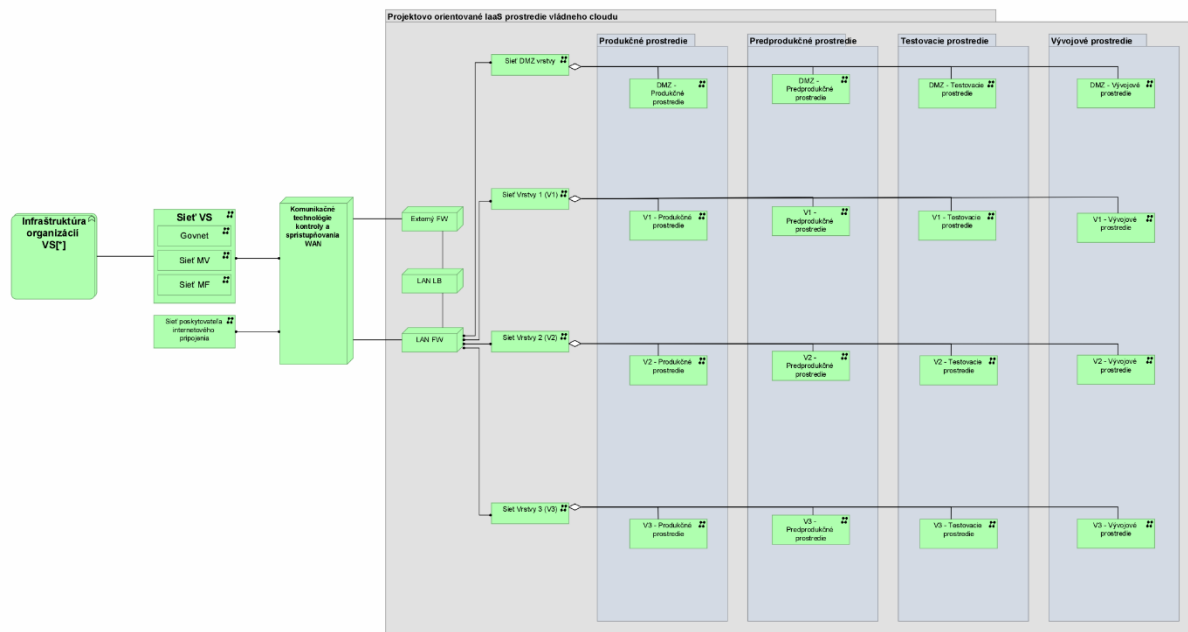
Popis	
Poskytovanie služieb	Vrstva poskytovania cloudových služieb riadi cloudové služby a ich kompozície na základe požiadaviek vrstvy dopytu a dostupnosti vrstvy dodávania cloudových služieb s cieľom zabezpečiť súlad s dohodou o poskytovanej úrovni cloudových služieb.
Dodávanie zdrojov	Vrstva dodávania zdrojov poskytuje jednotné rozhranie pre ľubovoľné hardvérové zdroje, zabezpečuje riadenie zdrojov, optimalizuje a monitoruje využitie prostriedkov z dispozičných zdrojov.
Dopyt	Vrstva dopytu riadi katalóg opisujúci cloudové služby dostupné pre odberateľov cloudových služieb a zabezpečuje validitu ich vzájomného mapovania podľa dohody o poskytovanej úrovni cloudových služieb.

Podrobný popis aplikačných funkcií je uvedený v časti Príloha č.2 - Popis aplikačných funkcií.

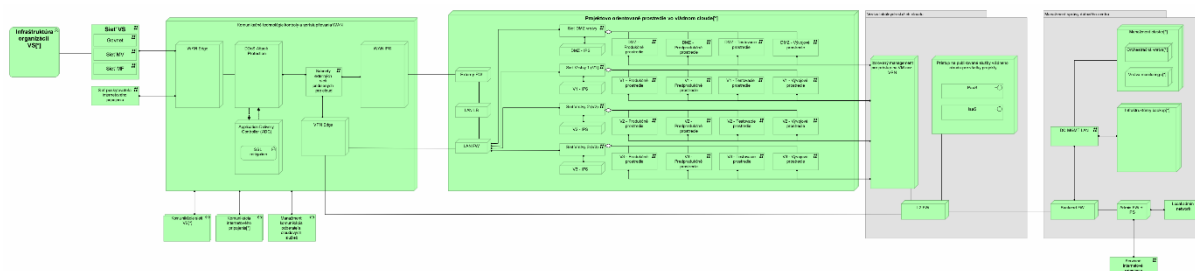
### 5.3.4 Technologická vrstva

Všeobecná technologická topológia ktorú znázorňuje „Obrázok 6 Úvodné hľadisko – technologické služby, technologické komponenty, siete“ je v nasledujúcich detailoch priblížená za účelom vysvetliť:

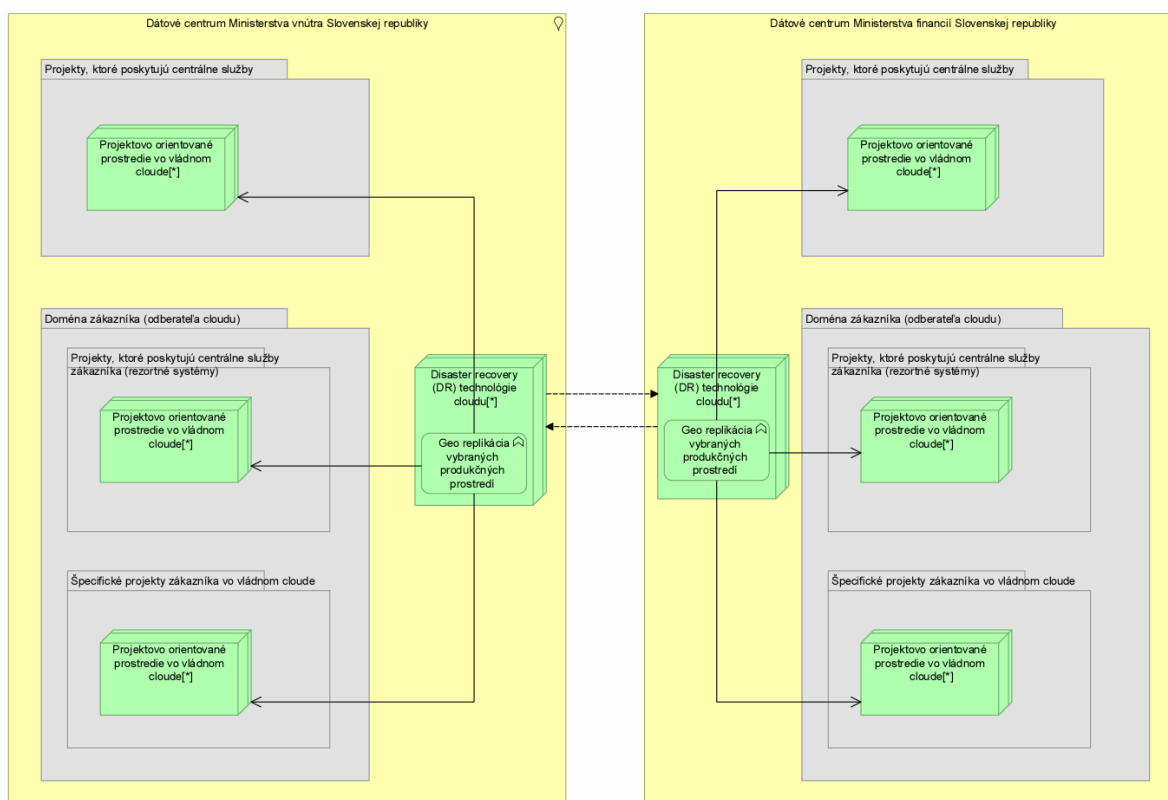
- tzv. projektovo orientované prostredie – predovšetkým sieťovú topológiu takýchto prostredí,
- kontext celkového prepojenia prostredí na WAN komunikáciu a interné komponenty vládneho cloudu,
- logickú hierarchiu, ktorú majú tieto jednotlivé prostredia v oboch lokalitách vládneho cloudu.



Obrázok 9 Projektovo orientované prostredie vládneho cloudu



Obrázok 10 WAN a smerovanie do vnútra DC



Obrázok 11 Hierarchia projektovo orientovaných prostredí

### 5.3.5 Hybridné IT

Cloud poskytuje prepojenie zákazníckeho „on-premise“ informačného systému a informačného systému v cloudu pomocou modulu na obrázku vyššie označeného ako „VPN edge“. Tento modul umožňuje vytvorenie zabezpečeného VPN spojenia organizácie do prezentačnej (V1) vrstvy konkrétného IS v cloudu.

Predpoklady:

Technologicky ide o vybudovanie permanentného „site-to-site“ tunela podľa cloudom definovanej šablóny a odberateľom definovaných komunikačných pravidiel medzi V1 a „on-premise“ IS. Odberateľ musí vo svojom DC disponovať kompatibilným VPN koncentrátorom. Na zriadenie prepojenia musí odberateľ využívať niektorú z cloudom poskytovaných externých sietí. Preklopenie VPN spojenia do záložnej lokality cloudu (DR) je možné zrealizovať zo strany odberateľa pomocou dvojice active/standby tunelov, sledovaním dostupnosti v primárnej lokalite a následne preklopením smerovania do standby VPN.

Obmedzenia:

Nie je možné zdieľanie adresného priestoru medzi prepojenými IS. Priame prepojenie, alebo smerovanie do inej ako prezentačnej (V1) vrstvy nie je z architektonického hľadiska umožnený. VPN prepojenie informačných systémov obchádza bezpečnostné komponenty (DDoS, ADC, WAN IPS) modulu na obrázku nazvaného ako „Komunikačné technológie kontroly a sprístupňovania WAN“.



## 5.4 Služby vládneho cloudu

Implementáciou projektu IKT infraštruktúra pre IaaS, časť 1 a časť 2, bolo umožnené poskytovanie nasledovných skupín cloudových služieb:

### **Voliteľné cloudové služby – služby ktorých parametre a počet definuje odberateľ cloudových služieb**

- vytvorenie preddefinované sieťového modelu,
- pripojenie do internetu/intranetu,
- poskytnutie „load balancing“ služieb,
- pridelenie virtuálnej IP,
- vytvorenie externých FW pravidiel,
- vytvorenie interných FW pravidiel,
- vytvorenie virtuálneho servera na technologickej platforme Intel a operačným systémom Windows, Red Hat alebo Centos,
- vytvorenie virtuálneho servera na technologickej platforme RISC a operačným systémom AIX,
- vytvorenie georedundantného virtuálneho servera na technologickej platforme Intel a operačným systémom Windows, Red Hat alebo Centos,
- vytvorenie georedundantného virtuálneho servera na technologickej platforme RISC a operačným systémom AIX,
- poskytovanie diskového priestoru (TIER I, TIER II a TIER III),
- poskytovanie sieťovej infraštruktúry (sieťový model, pripojenie do siete Internet, GOVNET, KTI, KTI2, MVNET).

### **Ďalšie služby – služby ktoré sú dostupné prevádzkovateľovi cloudových služieb**

- poskytovanie zálohovania snímky virtuálneho servera (zálohy sú vykonávané inkrementálne denne za posledných 6 dní v týždni a v siedmy deň celková záloha („full backup“), retenčná doba je 30 dní. Zálohy sa primárne ukládajú na virtuálnu knižnicu (disky), kópia z od zálohovaných dát sa robí na páskové médiá raz za týždeň),
- poskytovanie záloh replikovaných v záložnom dátovom centre,
- Intrusion Prevention System,
- Intrusion Detection System,
- DDos ochrana,
- Network Behavioral Analysis,
- Security Information & Event Management,
- Monitoring.

Podrobný katalóg služieb je uvedený na stránke <http://www.sk.cloud/>.

Všetky vyššie uvedené služby sú poskytované v režime HA (t.j. vo vysokej dostupnosti), pričom georedundantné/DR služby je po ukončení implementácie projektu možné poskytovať aj zo strany DC Ministerstva Financíí SR.

### 5.4.1 Elasticita vládneho cloudu

Elasticita cloudového prostredia predstavuje schopnosť pružne zdieľať fyzické zdroje pre poskytovanie cloudových služieb. To znamená, že fyzické zdroje sú zdieľané medzi viacerými projektami/zákazníkmi a sú dynamicky pridelované v závislosti od aktuálnych požiadaviek.

Úroveň a technologické riešenie elasticity je závislé od konkrétnych technológií. Výhodou cloudových prostredí s vysokou úrovňou elasticity je schopnosť v maximálnej miere utilizovať dostupné IKT zdroje.

Zo strany Poskytovateľa cloudových služieb je úroveň elasticity nastavená tak aby boli IKT zdroje čo v najväčšej miere utilizované a súčasne nedošlo k degradácii kvality cloudových služieb. V nasledujúcej tabuľke je uvedený súčasný stav elasticity cloudových služieb na úrovni IaaS.

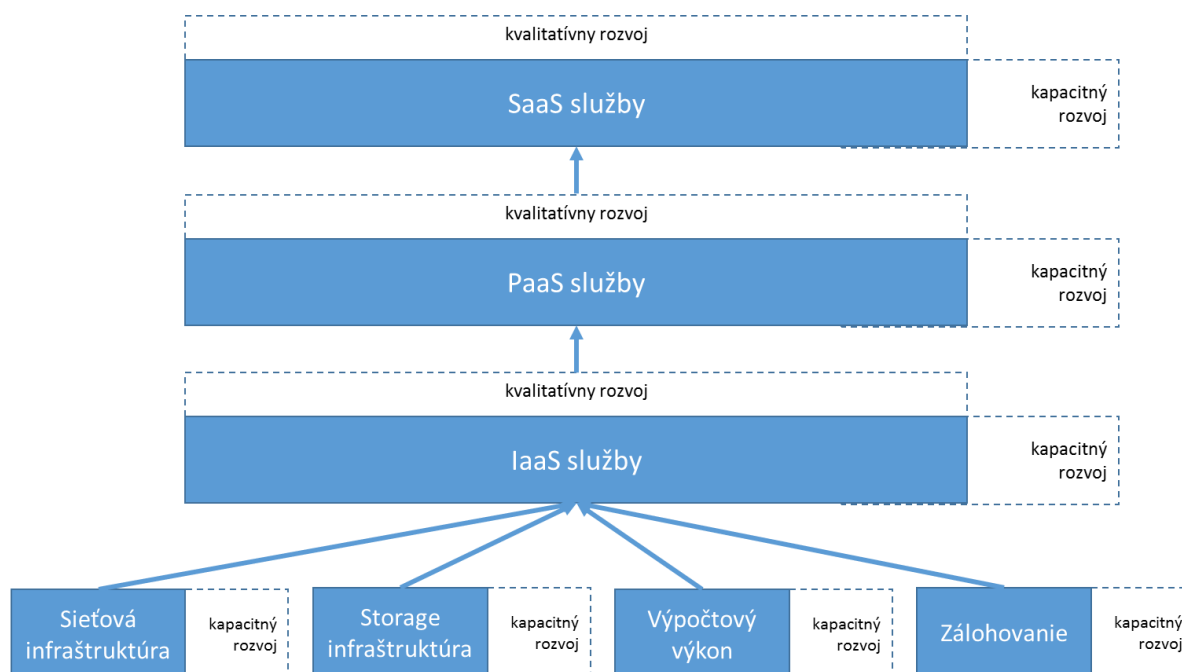
Kategória	Popis	Súčasný stav
Intel serverová platforma	Výpočtový výkon (CPU)	<b>1:5</b>
	Operačná pamäť (RAM)	<b>1:1</b>
RISC serverová platforma	Výpočtový výkon (CPU)	<b>1:2</b>
	Operačná pamäť (RAM)	<b>1:1</b>
Zdieľanie diskového priestoru (HDD)		„Thin provisioning“
Zdieľanie sieťovej infraštruktúry (NETWORK)		Aktivované zdieľanie sieťovej priepustnosti

## 5.5 Rozvoj IaaS služieb

Vládny cloud predstavuje dynamické prostredie, ktoré sa musí flexibilne prispôbovať požiadavkám odberateľov cloudových služieb. Rozvoj vládneho cloudu môže byť realizovaný v dvoch smeroch:

Kapacitný rozvoj – v prípade, že požiadavky odberateľov cloudových služieb prevyšujú kapacitu vládneho cloudu je potrebné zrealizovať kapacitný rozvoj za účelom doplnenia potrebných IKT zdrojov. Rozvoj je špecifický v závislosti od charakteru služieb a to nasledovne:

- IaaS služby – v prípade nedostatku zdrojov je doplnená IKT infraštruktúra, t.j. potrebný hardvér a softvérové licencie pre zvýšenie kapacity IaaS služieb.
- PaaS služby – nakoľko PaaS je poberateľom aj IaaS služieb je v závislosti od typu nedostatku služieb potrebné navýšiť kapacitu IaaS služieb a/alebo navýšiť softvérové licencie pre zvýšenie kapacity PaaS služieb.
- SaaS služby – nakoľko SaaS je poberateľom IaaS a/alebo PaaS služieb je v závislosti od typu nedostatku služieb potrebné navýšiť kapacitu IaaS a/alebo PaaS služieb a/alebo navýšiť softvérové licencie pre zvýšenie kapacity SaaS služieb.
- Navýšenie kapacity, môže byť realizované i formou služieb Hybridného vládneho cloudu, pokiaľ sa ukáže, že hybridné riešenie je vhodné a ekonomicky výhodnejšie.
- Kvalitatívny rozvoj – predstavuje rozvoj ktorý má dopad na kvalitu poskytovaných cloudových služieb (napr. dostupnosť) alebo rozvoj nových cloudových služieb na úrovni IaaS, PaaS a SaaS.



## 6 PaaS

### 6.1 Ciele

PaaS služby vládneho cloudu budú určené pre organizácie VS za účelom:

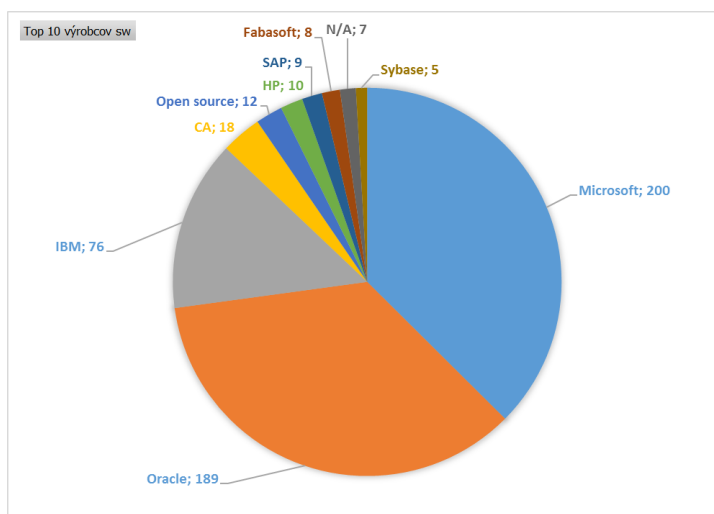
- 1 migrácie existujúcich ISVS do vládneho cloudu,
- 2 prípravy nových ISVS s využitím platformových služieb – predovšetkým v OPII.

PaaS služby vládneho cloudu musia umožniť:

- 1 zjednodušenie plánovania
  - 1.1 predpripravené služby s vopred známymi SLA a architektúrou ktoré redukujú komplexnosť prípravy architektúry a finančného plánovania.
- 2 zrýchlenie vývoja
  - 2.1 prostredia pre vývoj a testovania ktoré sú dostupné vo veľmi krátkom čase.
- 3 flexibilitu škálovania
  - 3.1 zdieľanie SW prostriedkov a ich pridelovanie podľa potreby ktoré rozširuje spôsoby úspor prostredníctvom cloudu.
- 4 stabilitu a zlacnenie prevádzky
  - 4.1 nové postupy ako DevOps s podporou PaaS automatizácie ktoré umožňujú rýchlejšie a bezpečnejšie riešenie zmenových požiadaviek a incidentov.

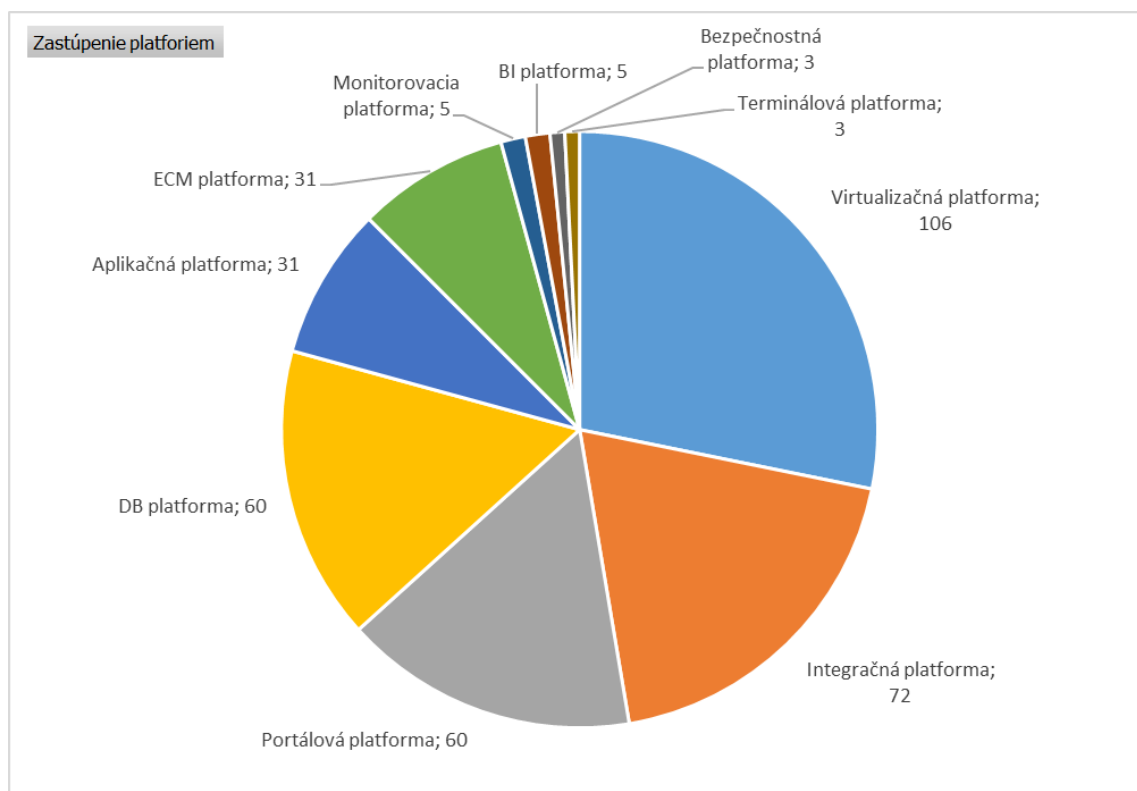
### 6.2 Aktuálny stav

Na základe Metodického usmernenia Ministerstva financií Slovenskej republiky č. MF/020304/2014 [5] a informácií zaslaných jednotlivými organizáciami je zastúpenie výrobcov softvéru pre serverovú časť v prevádzke organizáciami štátnej správy nasledovné.



Obrázok 12 Top 10 výrobcovia softvéru pre serverovú časť v prevádzke orgnizáciami štátnej správy

Taktiež súčasťou zberu údajov, bola požiadavka na určenie existujúcich platforiem, ktoré jednotlivé organizácie štátnej správy majú.



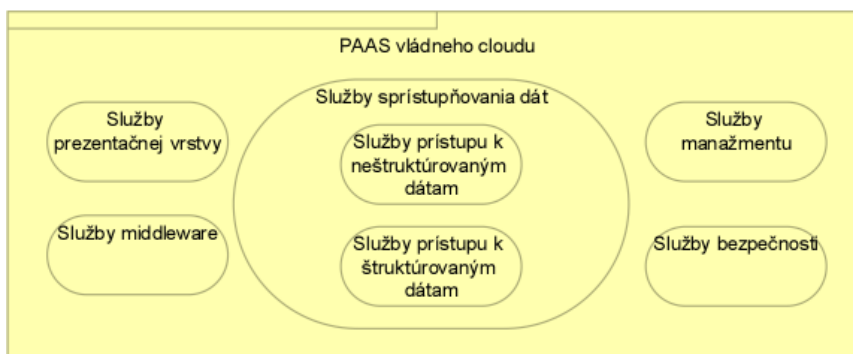
Obrázok 13 Typy platforiem

Na základe komunikácie s jednotlivými organizáciami sa dá konštatovať, že žiadna z vyššie uvedených platforiem nie je poskytovaná „ako služba“ medzirezortne. Sú však vybudované viaceré platformy, ktoré organizácie vyžívajú súčasne pre viacero ISVS. To tiež znamená, že určitá skúsenosť s prevádzkou (vlastnými zdrojmi, alebo formou „outsourcingu“) platforiem v zdieľanom režime na strane štátu je a musí byť pri návrhu riešenia zohľadnená.

Východiskové dáta sú uvedené v prílohe tohto dokumentu.

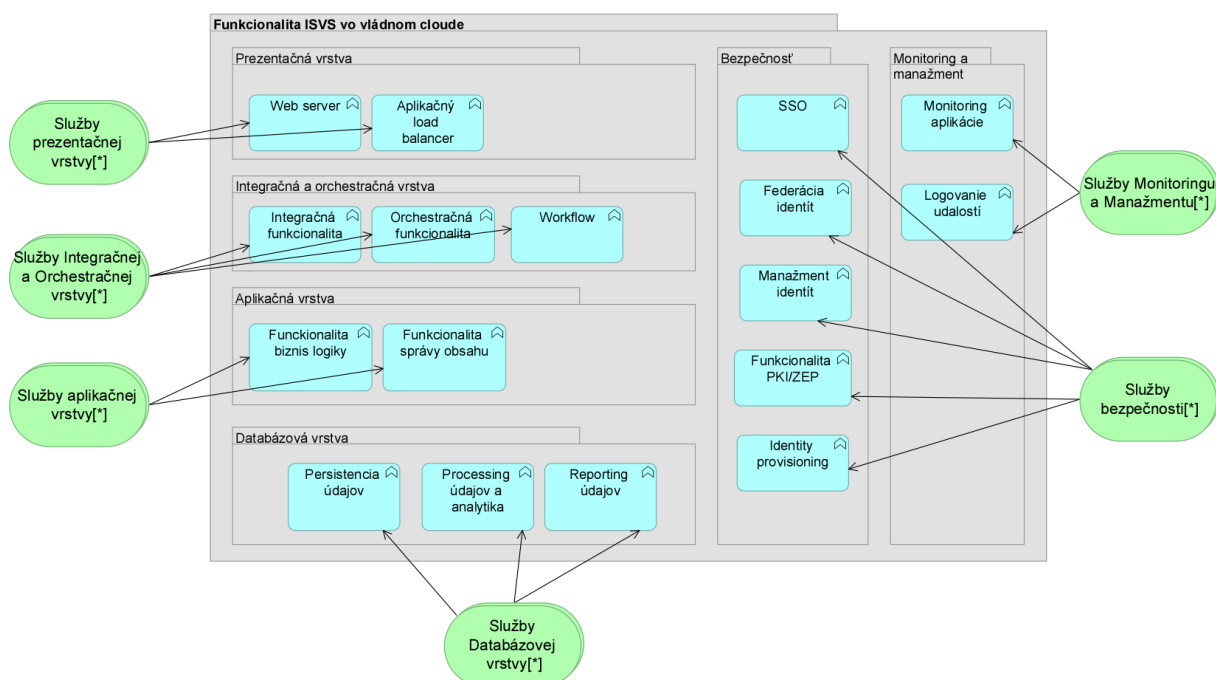
## 6.3 PaaS katalóg

V NKIVS 2016 je uvedené rámcové delenie PaaS služieb.



Obrázok 14 PaaS kategórie služieb

Takto nastavené rozdelenie je adresované aj ostatnými strategickými prioritami. Platformové služby musia poskytovať nasledujúcu funkcionality.



Obrázok 15 PaaS funkcionality

### 6.3.1 Služby Databázovej vrstvy

Poskytujú v prostredí cloudu priestor pre perzistenciu údajov. Tieto služby môžu byť vytvorené štandardnou databázou typu SQL, ale aj databázami typu NoSQL (dokumentové, kľúč-hodnota, grafové). Umiestnenie do cloudu zabezpečuje pre služby databázovej vrstvy elasticitu výkonu a kapacity. Popri službách ukladacieho priestoru sa medzi službami dátovej vrstvy nachádzajú aj súvisiace služby spracovania údajov a služby dátovej analýzy. Ďalšou typickou realizáciou služieb je napríklad analytická platforma typu BI a analytická platforma pre Hadoop. Rozšírením služieb databázovej vrstvy sú aj nadstavbové služby reportingu údajov a dátovej vizualizácie. Služby databázovej vrstvy disponujú súpravou nástrojov, ktorá je určená na návrh, rýchlu konfiguráciu, plnú alebo čiastočnú správu databáz (napr. zálohovanie, patching a upgrade). Služby databázovej vrstvy v režime on-demand budú prístupné cez užívateľskú samoobsluhu, zriaďované pružne, automatizovane,

flexibilne. Budú ľahko škálovateľné, vysoko dostupné s vysokým výkonom a budú podporovať merateľnosť svojho použitia. Služba databázovej vrstvy musí poskytnúť agilné plánovanie zdrojov na báze politik, podporiť aplikovanie merateľnosti a zavedenie pravidiel účtovania, ktoré sú dôležité pre zabezpečenie nákladovej zodpovednosti a väčšej kontroly nad prostredím služieb tejto vrstvy. Služby databázovej vrstvy musia poskytnúť proaktívny a prediktívny prístup pre svoju správu.

### 6.3.2 Služby Integračnej a Orchestračnej vrstvy

Integračná a orchestračná vrstva ako služba je určená pre vytváranie a zavádzanie integrácií a orchestrácií v rámci cloudu. Umožňuje však aj zavádzanie integrácie a orchestrácie medzi cloudom a miestnou aplikáciou. Umožní pripojenie cloudových aplikačných služieb a súčasne poskytne bezpečný prístup k rezortným aplikáciám, ktoré sú (alebo nie sú) prepojené rezortnou integračnou platformou. Integračná funkcionálna je typicky realizovaná cloudovou servisnou zbernicou, API bránou, spravovanou infraštruktúrou pre spracovanie veľkého množstva správ, ako aj podporou REST služieb. Navyše orchestračná funkcionálna a workflow rozširujú služby tejto vrstvy o podporu riadenia procesov a spracovanie komplexných udalostí. V rámci týchto služieb sú dostupné nástroje na vývoj, riadenie a beh integračných a orchestračných scenárov a integrácií v zmysle servisne orientovanej architektúry alebo architektúry orientovanej na mikroslužby. Služby tejto vrstvy podporujú návrh, vývoj, automatizáciu a správu procesov v cloud. Umožňujú v cloud vytvárať, meniť a upraviť a prevádzkovať všetky typy procesov v cloud. Používateľ riadi a navrhuje integračné scenáre, pričom služby integračnej a orchestračnej vrstvy poskytujú nástroje na vývoj a riadenie integrácií. Súčasťou tohto typu služieb sú aj nástroje pre dátovú integráciu, transformácie dát, zabezpečenie komunikácie a adaptéry pre podporované formáty dát. Služby integračnej a orchestračnej vrstvy musia disponovať podporou pre monitorovanie a správu spolu s možnosťou prehľadného zviditeľnenia integračných a procesných tokov, vyhľadávania integračných transakcií, detailnú analýzu, audit a diagnostiku pre integračné a orchestračné scenáre (aj v reálnom čase).

### 6.3.3 Služby Aplikačnej vrstvy

Poskytujú funkcionálnu pre umiestnenie tzv. biznis logiky. Typickou reprezentáciou je využitie služieb aplikačného servera. Aplikačný server, aplikačný kontajner prípadne aj manažment kontajner v tejto vrstve je špecializovaný pre prevádzkovanie zdieľaných aplikácií. Jedná sa o softvérovú platformu, ktorá zabezpečuje základné služby pre prevádzku samotných aplikácií. Ďalšou funkcionálnou, ktorú by mali služby aplikačnej vrstvy zabezpečiť je funkcionálna správy obsahu. V praxi sa jedná o počítačový systém, používaný pre sledovanie a ukladanie elektronických dokumentov alebo obrázkov z papierových dokumentov. Umiestnenie do cloudu zabezpečí elasticitu výkonu a kapacity a jednoduchšiu integráciu na služby orchestrácie dokumentov. Zároveň predpripravené štandardné prostredie DMS v rámci PaaS platformy zjednoduší implementáciu a zníži celkové náklady na udržiavanie systému. Služby aplikačnej vrstvy sú realizované kompletnou platformou v cloudovej infraštruktúre pre vytváranie, nasadzovanie a správu aplikácií, ktorá disponuje funkcionálnou rýchleho nastavovania aplikačného prostredia, aplikačných kontajnerov, load balancera, dátovej cache potrebnej pre rozdelenie zaťaženia. Prostredie služieb aplikačnej vrstvy by malo byť predinštalované a predkonfigurované a malo by podporovať aplikácie pre zabezpečenie maximálneho výkonu, škálovateľnosti a spoľahlivosti. Toto prostredie musí disponovať pružnou kapacitou výpočtového výkonu ako aj pružnou kapacitou dátového úložiska, tak aby bolo možné spustiť takmer ľubovoľnú záťaž.

### 6.3.4 Služby prezentačnej vrstvy

V nadväznosti na služby aplikačnej vrstvy je funkcionálna služieb prezentačnej vrstvy typicky zabezpečená službami web servera, aplikačného load balancera, službami API brány a prípadne aj službami mobilnej platformy. Služby prezentačnej vrstvy podporujú škálovateľnosť takmer akejkolvek aplikácie, s pomocou služieb vyrovnávania zaťaženia. Služby prezentačnej vrstvy majú funkcie vyššej úrovne ako je perzistencia session, kontrola funkcionality a rôzne typy load balancing algoritmov. Vyváženie zaťaženia je pre služby prezentačnej vrstvy je typicky k dispozícii pre HTTP a TCP protokoly. Služby prezentačnej vrstvy podporujú moderné webové aplikácie ako aj tak aj podnikové aplikácie. Pre optimalizáciu výkonu je k dispozícii služba vyrovnávacej pamäte, ktorá zlepšuje dobu načítania webových stránok a znižuje prevádzku smerom na backendové alebo integračné servre. Služby vyrovnávacej pamäte podporujú aj caching obsahu. Služby prezentačnej vrstvy ďalej zabezpečujú webové aplikácie nielen z pohľad dát, ale podporia behu web aplikácií v prípade obmedzenej prevádzky

súvisiacej s narušením bezpečnosti. Služby prezentačnej vrstvy môžu stanovovať limity na základe žiadostí, šírky pásma a pripojenia k spomaleniu alebo odkloneniu DDoS útokov. Služby prezentačnej vrstvy zaisťujú takto pre frontend aplikácie konzistentnosť, dobrú integrovanosť a hladkú prevádzku.

### 6.3.5 Služby bezpečnosti

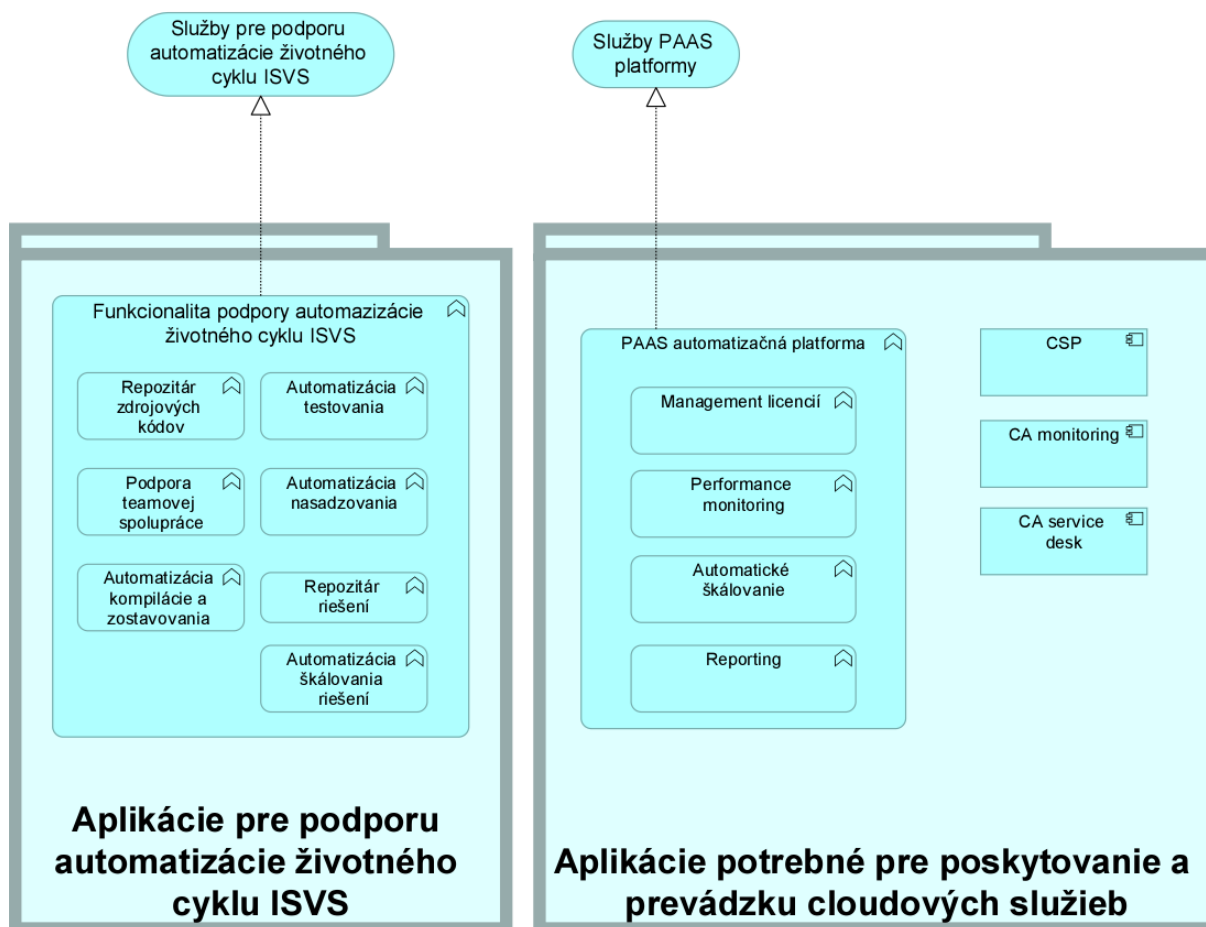
Služby bezpečnosti sú aj v prostredí PaaS prierezové a majú najvyššiu dôležitosť. Ich úlohou je zabezpečenie Cloud služieb. Služby bezpečnosti podporujú koncepciu zavedenia bezpečnosti ako služby (SecaaS), teda schopnosti rozvíjať opakovane použiteľné softvérové bezpečnostné služby, ktoré môžu byť zložené (spojené) so štandardnými cloud službami tak, aby im mohli poskytnúť vhodné bezpečnostné funkcie. V tejto súvislosti existuje silná potreba metód a nástrojov pre modelovanie bezpečnosti, ako aj pre hodnotiace techniky, pre podporu a porovnanie rôznych možností dizajnu a analýzy ich vplyvu na správanie nových služieb pred ich vlastnou realizáciou z pohľadu bezpečnosti. Typickou množinou funkcionalít služieb bezpečnosti je podpora pre SSO, federácia a manažment identít, ochrana koncových staníc, nastavovanie a správa práv a privilégiií a identít, úschova a správa PKI kľúčov (HSM), adresárové služby ako aj ďalšia funkcionalita služieb typu SIEM. Služby bezpečnosti využívané v cloude musia byť dobre integrovateľné s ostatnými službami PaaS a musia taktiež disponovať ucelenou súpravou podporných nástrojov pre prevádzku nasadzovania a monitorovanie tohto typu služieb.

### 6.3.6 Služby monitoringu a manažmentu

Služby monitoringu a manažmentu v sebe spájajú výhody technológie cloud computingu a tradičného riešenia sledovania a správy infraštruktúry on-premise. Tento typ služieb je zameraný na prierezové použitie s ostatnými cloudovými službami. Služby monitoringu a manažmentu sú typicky zamerané na monitorovanie aplikácie, logovanie udalostí a správu logov, monitoring chovania používateľov, konfiguračný manažment koncových staníc ako aj na správu mobilných zariadení. K službám monitoringu a manažmentu je možné pristupovať odkiaľkoľvek a kedykoľvek. Služby monitorovania môžu generovať upozornenia na základe špecifických obchodných podmienok, podporovať niekoľko úrovní eskalácii tak, že rôzne skupiny užívateľov môžu získať rôzne úrovne upozornení. Okrem služieb monitoringu a manažmentu služieb v cloude je možné využiť monitorovanie pre zmes cloud a on-premise infraštruktúry a služieb. Z tohto dôvodu v nasadeniach, kde je mix monitoringu on-premise a cloud tieto služby predstavujú výhodné možnosti monitorovania pre hybridného prostredia.



## 6.4 PaaS automatizácia



Obrázok 16 PaaS automatizácia a DEVOPS

### 6.4.1 Aplikácie potrebné pre poskytovanie a prevádzku PaaS služieb

Táto oblasť je tvorená aplikačnou funkcionalitou, ktorá má podporovať procesy poskytovania a prevádzky platformových služieb.

Za rozširujúcu funkcionalitu sa pokladá predovšetkým samoobslužná (konfiguračná) zóna PAAS automatizačnej platformy, ktorá má umožňovať odberateľovi nielen výber niektorej z ponúkaných služieb, ale musí zabezpečiť aj automatizáciu komplexnejších topológií a vzájomných závislostí jednotlivých platformových služieb. Takáto samoobslužná zóna je zvyčajne interaktívny portál, prostredníctvom ktorého môžu používatelia nasadiť, monitorovať a spravovať služby podľa požiadaviek

Poskytovateľ môže ponúkať niektoré zo služieb z katalógu v modeli podľa požiadaviek alebo samoobslužne. Bude to pravdepodobne podskupina katalógu, teda služieb, ktoré sú vhodnými kandidátmi pre plnú automatizáciu. Príkladom sú databázové služby pre testovanie a vývoj. Zložitejšie konfigurácie, ako napríklad tie, ktoré zohľadňujú špecifické požiadavky na dodržiavanie pravidiel alebo výkonových požiadaviek, nie sú zvyčajne ponúkané v samoobslužnom katalógu.

Nevyhnutnou požiadavkou PAAS automatizačnej platformy, je využívanie štandardného API, ktoré poskytuje automatizačná platforma IAAS.

### 6.4.2 Aplikácie pre podporu automatizácie životného cyklu ISVS

Jedným z dôležitých cieľov realizácie PaaS je umožnenie rýchleho návrhu, testov, nasadenia, používania a škálovania aplikácií (ISVS).



V tomto prípade sa jedná o podporné nástroje k PaaS službám, tak aby bolo možné počas výstavby, alebo migrácie ISVS čo najefektívnejšie podporiť proces využívania PaaS a prechod systémov do prevádzky. K takýmto aplikáciám môžeme zaradiť celú kategóriu tzv. DevOps nástrojov.

Pre vytvorenie vhodného prostredia na implementáciu aplikácií do PAAS vládneho cloudu je potrebné vytvoriť základné portfólio PAAS služieb. Otvorená platforma pre PAAS zabezpečuje, že vývojári a používatelia nebudú obmedzení pri výbere vhodných technológií, aplikačných služieb, alebo riešení pre cloud, ale bude možné na základe dopytu používateľov alebo ponuky dodávateľov služieb dobudovanie ďalších PAAS služieb. Pri vytvorení iniciálnej ponuky služieb je potrebné brať ohľad na rozsah služieb tak, aby pri spustení PAAS platformy boli dostupné najpoužívanejšie služby pre zabezpečenie štandardných funkcionalít tak ako sú uvedené pre oblasť „Špecializované aplikácie poskytovaných PAAS“. Tu je možné tiež uplatnenie open-source produktov, ak tieto spĺňajú požiadavky na požadované SLA. Celkovo je však potrebné minimalizovať počty dostupných služieb, pretože nepoužívané služby neefektívne zvyšujú náklady na prevádzku.

Pre implementáciu služieb je tiež nutné vyhodnotiť licenčné podmienky pre použitie v rámci vládneho cloudu, možnosti virtualizácie v rámci cloud prostredia a dostupnosť podpory pre dodávané riešenia služieb.

### 6.4.3 Špecializované rozhrania platformových služieb

Táto oblasť predstavuje funkčnú projekciu platformových služieb do aplikačnej architektúry, konkrétne do funkcionalít, ktorými chceme podporovať vlastnosti budúcich ISVS nachádzajúcich sa v cloudu.

Preferenciou je využívanie ucelenej skupiny služieb vo forme predkonfigurovanej výpočtovej platformy spolu so softvérovou súpravou vo forme služby. Takáto platforma (pozn. nie samotné služby ale takáto platforma má často pomenovanie PAAS) uľahčuje zavádzanie aplikácií bez vysokých nákladov, zložitosti nákupu a správy infraštruktúry, softvéru a ďalších prác súvisiacich s inštaláciou a konfiguráciou. Zvyčajne poskytuje všetko potrebné pre podporu celého životného cyklu budovania a poskytovania nie len webových aplikácií, príslušných API a súvisiacich služieb cez internet.

Každá platforma je vybavená zodpovedajúcim SDK a IDE, ktoré môže byť na zákazku upravené alebo rozšírené cez IDE plugíny dodaných poskytovateľom cloudu. IDE sada nástrojov by mala mať možnosť simulovať lokálny cloud runtime prostredia PAAS a zvyčajne zahŕňa aj spustiteľné aplikačné servery. Typické PaaS IDE môže ponúknuť širokú škálu nástrojov a programových zdrojov, ako sú softvérové knižnice, knižnice tried, rámce-frameworky, API integrácia a rôzne runtime možnosti, ktoré emulujú zamýšľané cloud prostredie určené pre implementáciu. Tieto funkcie umožňujú vývojárom vytvárať, testovať, a spustiť kód aplikácie v cloudu alebo lokálne (on-premise) a pri použití IDE ja emulovať cloud prostredie implementácie. Zostavené alebo dokončené aplikácie sú potom zbalené a nahraté do cloudu a nasadené pomocou predpripraveného prostredia. Tento proces nasadenia možno tiež ovládať vzdialene prostredníctvom IDE voči cloud PAAS prostrediu.

Z pohľadu prevádzky hlavne pre komplexnejšie systémy je emulácia prostredí nedostatočná a za účelom eliminácie chybovosti a komplikácií pri nasadzovaní je nevyhnutné plné budovanie prostredí Vývojové/Testovacie/Predprodukčné/Produkčné identickou architektúrou, technológiou a zdrojmi ( OS, HW ) zohľadňujúcu len počet užívateľov. Zapojenie pracovníkov prevádzky do testovania a automatizovaného nasadzovania musí byť umožnené už na predprodukčnom prostredí.

Žiada tiež vyššiu úroveň servisného managementu – nastavenie servisných okien a synchronizácia s business potrebami tenantov, riadenie testovania pri patchovaní s rôznymi nastaveniami a ďalšie špecifické úlohy. Z praktického hľadiska odporúčame dôslednú analýzu nákladov a prínosov

V prostredí PAAS prichádza do úvahy nový spôsob využitia zdieľaného modelu aplikácie a platformových zdrojov, ktorý sa označuje ako multitenantnosť. Pri multitenantnom návrhu aplikácie sa počíta s umožnením viac odberateľom (tenantom) prístupu k rovnakej aplikačnej logike súčasne. Každý tenant má svoj vlastný pohľad na aplikáciu, ktorú používa, spravuje ju a prispôsobuje ako vyhradenú inštanciu softvéru, zatiaľ čo je izolovaných od ďalších tenantov, ktorý používajú rovnakú aplikáciu alebo technológiu.

Je nevyhnutné zabezpečiť vyššiu úroveň servisného managementu – nastavenie servisných okien a synchronizácia s business potrebami tenantov, riadenie testovania pri patchovaní s rôznymi

nastaveniami a ďalšie špecifické úlohy. Z praktického hľadiska je potrebné doplniť dôslednú analýzu nákladov a prínosov.

Multitenantné aplikácie (technológie), zabezpečujú, že tenanti nemajú prístup k dátam a konfiguračným informáciám, ktoré nie sú ich vlastné. Multitenantná aplikačná architektúra je často výrazne zložitejšia ako u aplikácii určených pre jedného tenanta.

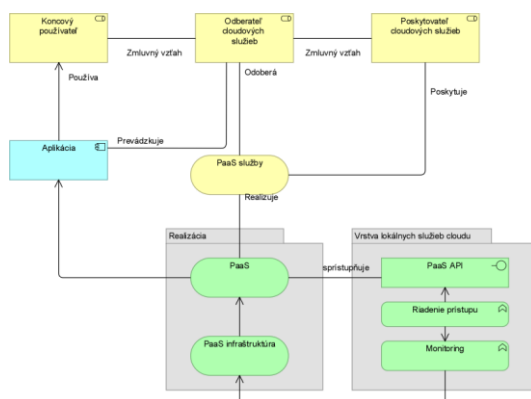
Multitenantná aplikácia potrebuje podporu zdieľania rôznych artefaktov zo strany viacerých používateľov vrátane portálov, dátových schém, middleware a databáz, pri zachovaní úrovne zabezpečenia a oddelení prostredí jednotlivých tenantov.

## 6.5 SLA PaaS služieb

Pre služby PaaS sú navrhované 3 úrovne SLA, a týmto spôsobom budú služby zaradené v katalógu služieb, pričom jednotlivé úrovne SLA by mali mať nasledovné charakteristiky:

### 6.5.1 I. úroveň SLA PaaS služieb

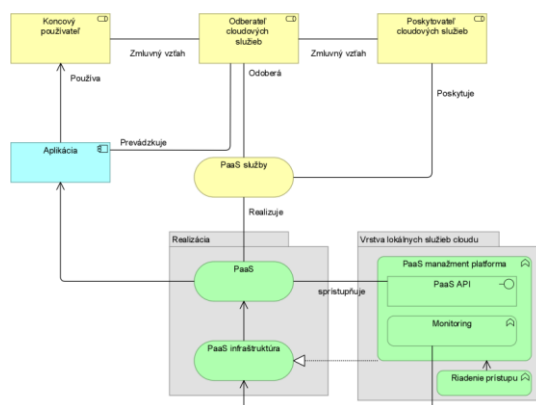
Najnižšia úroveň – „single node“ služby, s výraznou podporou predovšetkým pre open source produkty.



Obrázok 17 Generický model PAAS služby - SLA 1

### 6.5.2 II. úroveň SLA PaaS služieb

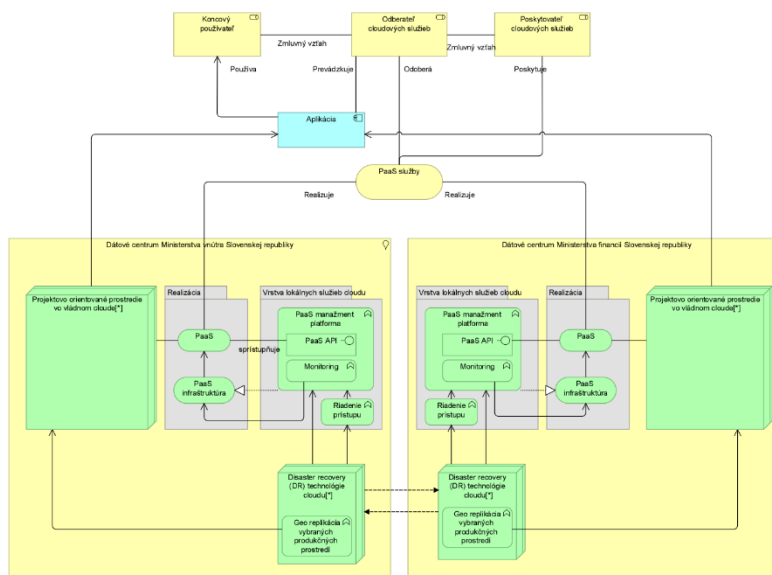
Úroveň s plnou podporou automatizácie (PAAS manažment platformy) – služby na tejto úrovni musia v plnej miere podporovať automatizáciu PAAS platformy.



Obrázok 18 Generický model PAAS služby - SLA 2

### 6.5.3 III. úroveň SLA PaaS služieb

Služby s najvyššou úrovňou podpory – služby s vysokou dostupnosťou, DR riešením v oboch lokalitách vládneho cloudu a využitím predovšetkým licencovaných produktov.



Obrázok 19 Generický model PAAS služby - SLA 3

## 6.6 Spôsob riešenia riadenia licencií SW

### 6.6.1 Alternatíva 1 – Poskytovanie iba centrálne manažovaných licencií SW produktov

#### 6.6.1.1 Súhrnný popis

Táto alternatíva predstavuje spôsob, pri ktorom sú centrálne (riadené) poskytované iba licencie SW produktov. V takomto prípade je platforma pripravená pre konkrétne použitie odberateľovi s použitím týchto licencií, pričom odberateľ si musí ďalej zabezpečiť prevádzkovú podporu takto nasadenej platformy.

### 6.6.1.2 SWOT analýza

#### 6.6.1.2.1 Silné stránky

- Rozdistribúovanie zodpovednosti a participácie, a tým eliminovanie „SPoF“.
- Precíznejšie prispôsobovanie sa potrebám projektov.

#### 6.6.1.2.2 Slabé stránky

- Nie všetky organizácie VS majú dostatočné IT na zabezpečenie takéhoto typu podpory.
- Ďalšie opakované aktivity, ktoré je potrebné uskutočňovať pri realizácii projektov
- Obmedzené možnosti licenčnej konsolidácie resp. technologických zmien

#### 6.6.1.2.3 Príležitosti

- Využitie existujúcich skúseností, ktoré časom získali jednotlivé organizácie
- Priestor na lepšie dohodnutie podmienok, podľa konkrétnych požiadaviek

#### 6.6.1.2.4 Hrozby

- Nedostatočné pre-používanie licencií – smerovania viac-menej ku kumulatívne systému, kde sa licencie iba dokupujú
- Opakovanie aktivít, ktoré by mohli byť priestorom na ďalšie šetrenie

### 6.6.1.3 Odporúčanie

Pre značnú časť sw. licencií, ktoré má štát vo vlastníctve bude potrebná ešte určitá doba, počas ktorej je potrebné aktívnejšie centrálné manažovať licencie SW produktov. Je však nevyhnutné priebežne konsolidovať toto portfólio, a tam kde sa dá prejsť na model platby za skutočne spotrebúvané licencie.

## 6.6.2 Alternatíva 2 - Riešenie privátnej PaaS platformy s predplatenými licenciami SW produktov

### 6.6.2.1 Súhrnný popis

Vybudovanie privátnej PaaS platformy s portfóliom služieb založenom na SW produktoch od výrobcov, ktoré budú k dispozícii pre používateľov týchto služieb s využitím SW licencií ktoré sú vopred nakúpené (nakupované). Na základe dopytu a ponuky jednotlivých služieb je možné PaaS platformu tiež rozšíriť o ďalšie služby – zmenovou požiadavkou. Služby budú k dispozícii okamžite po akceptácii do prevádzky a licenčné krytie týchto služieb bude riešené formou predplatených licencií. Licencie zakúpi poskytovateľ PaaS platformy resp. budú súčasťou projektu vybudovania takýchto služieb. Táto alternatíva predpokladá, že PaaS platforma sa bude budovať na existujúcom IaaS vládneho cloudu. Jedná o vybudovanie PaaS služieb s využitím vlastných best-practice a preferencií.

### 6.6.2.2 SWOT analýza

#### 6.6.2.2.1 Silné stránky

- Ľahšie spočítateľné TCO (celkové náklady na IT)
- Licencie sú k dispozícii okamžite
- Technická podpora a SLA, ktorá sa dá výhodnejšie zjednať pri nákupoch väčších celkov

#### 6.6.2.2.2 Slabé stránky

- Licencie sú nakúpené v celom požadovanom objeme resp. prikupované vo väčších celkoch

- TCO v horizonte 10 rokov
- Flexibilita takéhoto zoznamu licencií
- Flexibilita celkového financovania

#### 6.6.2.2.3 Príležitosti

- Migrácie existujúcich licencií do spoločných „poolov“

#### 6.6.2.2.4 Hrozby

- Závislosť na výrobcovi („vendor-lock-in“)
- Permanentný problém vyvažovania potreby a spotreby

### 6.6.2.3 Odporúčanie

Táto alternatíva je výhodná vtedy, ak máme vopred jasne stanovené technologické požiadavky a vieme aj kvantitatívne určiť rozsah týchto požiadaviek. Nie je tiež vylúčené kombinovať túto alternatívu s modelom „Pay-per-use“.

## 6.6.3 Alternatíva 3 - Riešenie privátnej PaaS platformy s licenčným modelom „Pay- per-Use“

### 6.6.3.1 Súhrnný popis

Vybudovanie privátnej PaaS platformy s portfóliom služieb založenom na SW produktoch od výrobcov, ktoré budú k dispozícii pre používateľov týchto služieb s využitím SW licencií ktoré sú uhrádzané podľa skutočne spotrebovaného množstva.

Aby mohla táto alternatíva v privátnom cloud-e pracovať čo najefektívnejšie je nevyhnutné aplikovať model „pay-per-use“ v čo najrozvinutejšej forme aj smerom na zriadenie a poskytovanie služby prevádzkovateľom, tiež vrátane služieb IaaS. To znamená aby SW licencie boli riešené touto formou, a podpora týchto služieb bola tiež spoplatňovaná podľa skutočne spotrebovávaných služieb. Na základe dopytu a ponuky jednotlivých služieb by bolo možné PaaS platformu rozšíriť o ďalšie služby. Dôležitým faktorom tejto alternatívy je určenie mechanizmu na priebežné uhrádzanie SW licencií – ak by bol projekt realizovaný z EŠIF. Táto alternatíva predpokladá, že PaaS platforma sa bude budovať na existujúcom IaaS vládneho cloudu.

### 6.6.3.2 SWOT analýza

#### 6.6.3.2.1 Silné stránky

- Ľahšie spočítateľné TCO (celkové náklady na IT)
- Licencie sú k dispozícii okamžite
- Technická podpora a SLA, ktorá sa dá výhodnejšie zjednať pri nákupoch väčších celkov

#### 6.6.3.2.2 Slabé stránky

- Licencie sú nakúpené v celom požadovanom objeme resp. prikupované vo väčších celkoch
- TCO v horizonte 10 rokov
- Flexibilita takéhoto zoznamu licencií
- Flexibilita celkového financovania

#### 6.6.3.2.3 Príležitosti

- Migrácie existujúcich licencií do spoločných „poolov“

## 6.6.3.2.4 Hrozby

- Závislosť na výrobcovi („vendor-lock-in“)
- Permanentný problém vyvažovania potreby a spotreby

## 7 SaaS

### 7.1 Ciele

Softvér ako služba, označovaný aj ako SaaS (Software as a Service), pri ktorom cloudovú službu predstavuje poskytovanie softvéru, vrátane aplikácií, t.j. používatelia využívajú aplikačnú funkcionálnu (odberateľ získava prístup k aplikácii, nie samotnú aplikáciu).

Postupným rozširovaním a želaným cieľovým stavom bude poskytovať komplexnejší softvér formou služieb SaaS. Najmä štandardizované podporné procesy vnútornej správy budú realizované centrálnymi podpornými a administratívnymi informačnými systémami vnútornej správy nasadenými v cloude, čím sa podporí centralizácia operácií a tým sa zjednodušia a zjednotia procesy naprieč organizáciami.

Spoločným merateľným ukazovateľom, ktorý je uvádzaný v materiáloch (Odkazy na externé zdroje [2], [3], [6] ) je Počet centrálne využitých podporných systémov vnútornej správy v rámci ISVS (ako služieb v cloude SaaS) s cieľovou hodnotou 7.

Cieľom však bude túto hodnotu nie len dosiahnuť, ale prekročiť pretože:

- v konečnom dôsledku do tohto ukazovateľa musíme zahrnúť systémy dodávané formou služieb pre samosprávy (ako súčasť VS) v prevádzke a ďalšom rozvoji DCOM (predovšetkým užšej integrácii na vládny cloud),
- celkový koncept hybridizácie (vid. kapitola Hybridný vládny cloud) vytvára predpoklady na využívanie existujúcich akreditovaných (vid. kapitola Certifikácia a akreditácia služieb) riešení.

### 7.2 Aktuálny stav

V súčasnosti nie sú žiadne SaaS služby uvádzané v katalógu služieb, avšak z technického hľadiska existuje viacero implementácií riešení vo VS, ktoré majú charakter SaaS. Jedným z nich je aj DCOM.

IS DCOM bol vybudovaný s cieľom presunu a centralizácie administratívnych a podporných systémov vnútornej správy. Tieto systémy sú v DCOM prevádzkované za použitia virtualizačných technológií vo forme cloudu. Pre každú obec je vytvorený virtuálny priestor na prevádzku týchto aplikácií. Cloud technológia a virtualizácia umožňuje samosprávam namiesto lokálnej správy tisícov počítačov (v kombinácii s desiatkami aplikácií a jednotkami konkrétnych verzií operačných systémov) spravovať jedno virtuálne prostredie, v ktorom je možné efektívnejšie dosiahnuť plnenie podmienok prevádzky a bezpečnosti informačných systémov.

Kľúčové SaaS služby poskytované v rámci projektu DCOM sú: 138 elektronických služieb samosprávy vrátane integrácii na ÚPVS, elektronická schránka, elektronická podateľňa, IAM (zabezpečenie identifikačného procesu), modul elektronických platieb, Integrácia na IS VS (Register fyzických osôb, Register právnických osôb, Kataster nehnuteľností, Register adries, IS Sociálnej poisťovne, IS Finančná správa, IS MPSVaR a IS Nár. evidencia vozidiel) a modul daní a poplatkov. Z hľadiska funkčnosti sa jedná o SaaS služby ktoré prostredníctvom vytvorených modulov umožnia mestám a obciam poskytovať občanom a podnikateľom elektronické služby.

### 7.3 Spôsoby riešenia

Principiálne sú nastavované 2 základné spôsoby riešenia:

1. príprava SaaS služby formou projektu v privátnom vládnom cloude (napr. pre projekty OPII bola pre SaaS pripravená samostatná forma štúdie uskutočniteľnosti),

2. akreditáciou existujúcej SaaS služby. Tento spôsob bude k dispozícii po realizácii aktivít nevyhnutných na zavedenie tejto metódy. Vid. tiež kapitoly Vytvorenie dôveryhodného prostredia, Realizácii funkcií Sprostredkovateľa Hybridného cloudu.

### 7.3.1 Príprava SaaS služby formou projektu v privátnom vládnom cloud

Často kladenou otázkou v prípade realizácie ISVS je, či je takto pripravovaný IS systémom, ktorý poskytuje svoje služby (čo je drvivá väčšina) alebo sa jedna o IS, ktorý je poskytnutý formou služby SaaS.

Pri rozhodovaní by mala pomôcť nasledujúca tabuľka, pričom SaaS riešenie musí splniť všetky kritéria.

Kritérium	ISVS ako SaaS	ISVS ako riešenie, ktoré poskytuje el. služby
Odoberá služby IaaS a PaaS vládneho cloudu	Áno	Nie je podmienkou
Ponúkané riešenie je súčasťou katalógu služieb vládneho cloudu	Áno	Nie
Riešenie spĺňa podmienky z. 275 o ISVS	Áno	Áno
Poskytovateľ služby spĺňa podmienky Výnosu 55 o štandardoch, §55 Správa cloud computingu	Áno	Nie
Dynamický model subskripcie <sup>10</sup>	Áno	Nie
Podpora riešenia až na úroveň L1	Áno	Nie je podmienkou <sup>11</sup>
Riešenie je prístupné cez web	Áno	Nie je podmienkou
Zákazník ma možnosť samoobslužnej konfigurácie cez web	Áno	Nie je podmienkou
Kompetencia výkonu agendy, ktorú systém podporuje	Na strane odberateľa	Na strane poskytovateľa

Z organizačného pohľadu, sa aj na tento prípad vzťahuje schéma uvedená v kapitole 3.2.1 Sumárny pohľad – privátny cloud, pričom dôležitými aspektami sú:

- Určenie role Gestora pripravovanej SaaS služby (poskytovateľa a prevádzkovateľa).
- Kooperácia s ÚPPVII pri plánovaní a príprave služby (projektu).

<sup>10</sup> Je stanovený tzv. tenant (odberateľ), pričom poskytovaná služba logicky ohraničuje údaje jednotlivých tenantov, tak aby tieto údaje neboli vzájomne viditeľné. Zároveň riešenie umožňuje dynamicky pridávať a odoberať jednotlivých tenantov.

<sup>11</sup> Zabezpečí IT organizácie odberateľa



- Kooperácia s prevádzkou vládneho cloudu pri realizácii, nasadzovaní a prechode do prevádzky.
- Určenie rozdelenia kompetencií podpory (za čo je zodpovedný Gestor služby, a za čo sú zodpovední gestori služieb, ktoré SaaS služba potrebuje pre svoj beh).

### 7.3.2 Oblasť riešenia

**Detailnejšou stratégiou v oblasti agend VS a ich realizácie formou SaaS sa zaoberá strategická priorita Digitalizácia agend VS.**

Rámčovo je však možné konštatovať, že aj v prípade komplexnejších informačných systémov sú tieto rozčlenené na moduly, ktoré je možné v prípade potreby realizovať samostatne, resp. nahradiť identifikované spoločné funkcionality SaaS službami. Vládny cloud bude poskytovať SaaS predovšetkým v nasledujúcich oblastiach (uvedené tiež v prílohe dokumentu Odkazy na externé zdroje [3]):

- služby ERP (Enterprise resource planning) – predstavujú základ pre riešenie administratívnych činností subjektu (inštitúcie verejnej správy - povinnej osoby),
- zmluvný účet – rozšírenie účtovníctva o vedľajšiu knihu, systém sledujúci záväzky a pohľadávky subjektov (fyzických a právnických osôb),
- správa nehnuteľností – systém umožní evidenciu nehnuteľností (katalóg nehnuteľností a ich pasportizácia) a riadenie ich používania: prenájom, predaj, zmluvy súvisiace s nehnuteľnosťami (zúčtovanie nákladov) a procesy súvisiace s údržbou nehnuteľností,
- manažment vozového parku (AVL) – sústava aplikácií pre komplexný manažment vozového parku, plánovanie kontrol a údržby, sledovanie pohybu, priradzovanie na úlohy a podobne
- riadenie ľudských zdrojov - sústava aplikácií, ktoré zabezpečia komplexné riadenie a rozvoj ľudského kapitálu v inštitúciách verejnej správy, ktoré budú integrované s ERP,
- manažment zamestnancov v teréne – služby pre inštitúcie, ktorých zamestnanci riešia úlohy v teréne,
- EDMS (Electronic document management system) a workflow je sústava aplikácií pre evidenciu, sledovanie a tvorbu dokumentov v procesoch inštitúcie,
- centrálny email – emailový server pre pracovníkov štátnej správy,
- elektronické úložisko záznamov (alebo aj ERMS - Electronic Record Management System) služby pre ukladanie elektronických záznamov a následné sprístupňovanie prostredníctvom vyhľadávania,
- kolaboračná platforma - súbor aplikácií umožní jednoduchú výmenu informácií, skúseností, úloh a zjednoduší tak najmä odbornú prácu a tvorbu politik,
- analytické nástroje – sústava aplikácií, ktoré podporia procesy prostredníctvom štatistických metód a metód dátovej analýzy,
- centrálny eLearning – služba zabezpečí komplexné vzdelávanie zamestnancov verejnej správy formou eLearningu, tvorbu kurzov a tém, diskusie, testovanie, návštevu kurzov,
- manažment projektov – služba bude poskytovať nástroje pre projektový manažment podľa nastavených metodík (PRINCE2, PMI), plánovanie zdrojov, rozpočtu, aktivít, harmonogram a následné vykonávanie, kontrolu a manažment kvality výstupov,
- podpora verejného obstarávania – služba podporí verejného obstarávateľa vo všetkých krokoch životného cyklu obstarávania,
- manažment kvality – výstupov a výsledkov verejnej správy,
- nástroje pre Opendata – sústava nástrojov pre spracovanie dát (čistenie, spájanie, prepájanie) do podoby vhodnej na publikovanie v otvorenom formáte linked-data,



- geografický informačný systém – informačný systém, ktorý umožní vytvárať a používať špecifické vrstvy nad sústavou priestorových informácií a mapových podkladov,

## 8 SLA služieb

### 8.1 Ciele

V podmienkach cloud computingu existuje obchodný vzťah medzi odberateľom cloudových služieb a poskytovateľom cloudových služieb. Podmienky, práva a povinnosti jednotlivých subjektov v rámci tohto obchodného vzťahu sú predmetom zmluvy o poskytovaní cloudových služieb. Je v kompetencii poskytovateľa cloudových služieb zvoliť spôsob a rozsah presunu SLA podmienok na prevádzkovateľa cloudových služieb. Nevyhnutnou súčasťou zmluvy o poskytovaní cloudových služieb sú SLA podmienky objednaných cloudových služieb. Cieľom tejto kapitoly je popísať súčasný stav, základnú terminológiu a navrhnúť SLA rámec na strategickú úroveň pre služby poskytované vládny cloudom.

Informačné systémy odberateľov poskytované z Vládneho cloudu majú vlastné SLA zmluvy na konkrétne aplikačné služby nimi poskytované. Časti týchto SLA sú naviazané na SLA služieb Vládneho cloudu avšak vo väčšine prípadov sem vstupujú aj SLA externých entít, napr. SLA privátneho sieťového pripojenia odberateľa do Vládneho cloudu. Aby vedeli relevantné časti SLA informačných systémov byť jednoznačne mapované na celú infraštruktúru je potrebné aby sa definovala minimálna podmnožina SLA parametrov aj pre komponenty mimo Vládneho cloudu. Túto problematiku skúsime rozviesť a zadefinovať v samostatnej podkapitole.

Role a zodpovednosti účastníkov zmluvného vzťahu sú predmetom inej kapitoly tohto dokumentu.

### 8.2 Štandardy

Na medzinárodnej úrovni sa špecificky problematikou SLA v podmienkach cloud computingu okrem iných štandardov zaoberá ISO/IEC 19086-1:2016. Pri písaní tejto časti dokumentu sa vychádzalo práve z tohto štandardu. Ďalšie dôležité štandardy v oblasti cloud computingu:

- ISO/IEC CD 19086-2 - Cloud computing - Service level agreement (SLA) framework -- Part 2: Metric Model.
- ISO/IEC DIS 19086-3 - Cloud computing - Service level agreement (SLA) framework -- Part 3: Core conformance requirements.

### 8.3 Terminológia

Je dôležité aby všetky zúčastnené strany („stakeholderi“), mali relevantné znalosti terminológie používanej pri definovaní jednotlivých parametrov SLA.

SLO – Service level objective – predstavuje kvantifikovateľný parameter cloudovej služby. Napríklad pri SLA v oblasti dostupnosti, môže byť SLO definované ako konkrétne percento.

SQO – Service qualitative objective – predstavuje kvalitatívny parameter cloudovej služby. Napríklad pri SLA bezpečnostnej certifikácie, môže byť SQO definované ako konkrétny ISO certifikát.

### 8.4 Aktuálny stav

Implementáciou projektov IKT infraštruktúra pre IaaS, časť 1, a IKT infraštruktúra pre IaaS, časť 2, bola vybudovaná technologická infraštruktúra umožňujúca poskytovanie SLA s nasledovnými parametrami:

- Dostupnosť – pre IaaS služby je dostupnosť pre všetky prostredia (vývojové, testovacie, integračné a produkčné) na minimálnej úrovni 99.9268%.
- Disaster recovery – podrobný popis koncepcie DR riešenia je predmetom kapitoly DR.
- Výkonnosť – na úrovni IaaS obsahujú služby aj výkonnostné parametre jednotlivých služieb (napr. diskový priestor TIER II ma výkonnosť min. 0.15 IOPS per GB a max. 150 IOPS), je na rozhodnutí odberateľa cloudových služieb si zvoliť výkonnosť služieb adekvátnu požiadavkám.

Pridaním ďalších IaaS služieb alebo vybudovaním vyšších vrstiev cloudových služieb (PaaS a SaaS) je možné optimalizovať úroveň SLA parametrov.

## 8.5 Špecifiká cloud computingu ovplyvňujúce nastavenie SLA

Pre zadefinovanie efektívnych parametrov SLA pre cloudové služby je nevyhnutné zohľadniť kľúčové charakteristiky cloudového prostredia. V nasledovnej časti sú uvedené najvýznamnejšie charakteristiky cloudového prostredia, ktoré majú dopad na SLA:

- „Self-service“ nástroje – prístup ku cloudovým službám môže byť realizovaný cez automatizované softvérové nástroje. V prípade použitia takýchto nástrojov je potrebné v SLA podmienkach špecifikovať tieto softvérové nástroje.
- Zdieľanie zdrojov a multi-tenantnosť – cloudové prostredie využíva virtualizačné technológie pre umožnenie virtualizácie serverov, diskových úložísk, sietí a pod. Multi-tenantnosť umožňuje zdieľanie fyzických zdrojov takým spôsobom, že odberatelia cloudových služieb sú navzájom izolovaní.
- Elasticita a škálovateľnosť – v cloudovom prostredí môže byť rozsah fyzických alebo virtuálnych zdrojov zvýšený alebo znížený dynamicky a v niektorých prípadoch automatizovaným spôsobom.
- Kompromis medzi cenou a kontrolou – pre zabezpečenie efektívnej prevádzky cloudového prostredia obsahuje cloudové prostredie štandardizované služby. V prípade požiadaviek na úpravu alebo väčšiu kontrolu zo strany odberateľa cloudových služieb je na rozhodnutí poskytovateľa cloudových služieb, či umožní za dodatočné náklady realizovať požadované zmeny.
- Merateľnosť – poskytované cloudové služby sú voči odberateľom cloudových služieb vyúčtované na základe dohodnutej časovej lehoty. Pre umožnenie vyúčtovania je nevyhnutné zabezpečiť merateľnosť poskytovaných cloudových služieb.

## 8.6 SLA komponenty

V nasledovnej časti sú definované relevantné komponenty SLA. Zo strany odberateľa cloudových služieb ako aj poskytovateľa cloudových služieb je potrebné disponovať dôkladnou znalosťou týchto komponentov. Problematika SLA komponentov je uvedená aj v štandarde ISO/IEC 19086-1:2016, kapitola 9.

Poskytované služby – definícia na ktoré služby sa vzťahuje SLA zmluva. V prípade že SLA pokrýva viacero služieb, tak je odporúčané definovať všetky služby a uviesť separátne SLO a SQO pre jednotlivé služby

SLA definície – definícia podmienok SLA zmluvy, ktoré sú špecifické pre daný SLA kontrakt. Je dôležité aby odberateľ cloudových služieb rozumel všetkým podmienkam uvedených v SLA.

Monitoring služieb – parametre SLA, ktoré sú zo strany poskytovateľa cloudových služieb monitorované a reporty, ktoré sú poskytované odberateľom cloudových služieb. Súčasťou môže byť popis podmienok, ktorými sa riadi dostupnosť nástrojov pre umožnenie monitoringu služieb.

Role a zodpovednosti – popis rolí a zodpovedností za odberateľa cloudových služieb a poskytovateľa cloudových služieb.

## 8.7 Parametre SLA

V nasledovnej časti sú uvedené návrhy SLA parametrov pre cloudové služby. Výber konkrétnych SLA, SLO a SQO parametrov je v zodpovednosti poskytovateľa cloudových služieb. Problematika SLA parametrov je uvedená aj v štandarde ISO/IEC 19086-1:2016, kapitola 10.

### 8.7.1 Asistenčná podpora

Poskytovateľ cloudových služieb by mal brať do úvahy aj skutočnosť, že ku službám môže byť požadovaný prístup odberateľmi s obmedzeniami, ktoré im bránia plne využívať cloudové služby. V súčasnosti existujú technológie (čítačky obrazovky, alternatívne vstupné zariadenia a pod.) a štandardy poskytujúce relevantné informácie v oblasti asistenčnej podpory, napr.:

- W3C Web Content Accessibility Guidelines (WCAG) 2.0,
- ISO/IEC 40500:2012,
- ISO/IEC TR 29138 (all parts),
- ISO/IEC Guide 71.

V rámci SLA je potrebné uviesť, či cloudové služby poskytujú asistenčnú podporu a ak áno, tak definovať akými nástrojmi a v akom rozsahu.

### 8.7.2 Dostupnosť

Dostupnosť je definovaná ako vlastnosť, kedy je služba použiteľná oprávnenou osobou. Doba, kedy služba nie je k dispozícii je označovaná ako „nedostupná“ („downtime“). V prípade pravidelných servisných updatov, upgradov a podobne môže nastať „plánovaná nedostupnosť“ („scheduled downtime“). Pri plánovanej nedostupnosti je potrebné informovať odberateľa cloudových služieb v dostatočnom časovom predstihu. Doba, kedy služba nie je k dispozícii, ale nie je to považované za nedostupnosť je označovaná ako „povolená nedostupnosť“ („allowable downtime“).

Dostupnosť je vyjadrená ako celkový čas v definovanom intervale mínus čas kedy je služba nedostupná. Dostupnosť nie je redukovaná o dobu povolenej nedostupnosti. V SLA zmluve sa dostupnosť vyjadruje ako percentuálna hodnota za daný časový interval, pričom percento vyjadruje hodnotu dostupnosti služby.

### 8.7.3 Výkonnostné parametre cloudových služieb

Ďalším parametrom SLA sú výkonnostné parametre cloudových služieb, ktoré je možné individuálne definovať pre jednotlivé cloudové služby. Príklady výkonnostných parametrov:

- doba odozvy – odozva cloudovej služby môže byť nadefinovaná rôznymi spôsobmi. Napríklad maximálna odozva od momentu zadania vstupu až do momentu odozvy, alebo priemerná odozva od momentu zadania vstupu až do momentu odozvy. Taktiež je možné rozlíšiť či je odozva meraná pri vysokej záťaži systému alebo minimálnej záťaži systému.
- kapacita služby – súčasťou SLA môžu byť kapacitné parametre ako napr. objem RAM pamäte, počet CPU, priepustnosť siete a pod. elasticita služby – elasticita je schopnosť cloudovej služby dynamicky upraviť objem IKT zdrojov pridelených k inštanciám služby.
- elasticita môže byť riešená automatizovane, kedy ku zmene dochádza bez interakcie. Zmena IKT zdrojov môže nastať v reaktívnom spôsobe, kedy na základe sledovania skutočného vyťaženia služby sa v prípade nedostatku/prebytku IKT zdroje navýšia alebo redukujú. Opačný prípad je aktívny prístup, kedy za použitia algoritmov sa predvída budúce zaťaženie služby a tomu adekvátne sa upravujú IKT zdroje.

### 8.7.4 Ochrana osobných údajov

V rámci SLA je potrebné zohľadniť aj ochranu osobných údajov, ktorá z pohľadu legislatívy je predmetom zákona č. 122/2013 Z. z. - Zákon o ochrane osobných údajov.

### 8.7.5 Bezpečnosť

Bezpečnosť cloudových služieb sa dotýka mnohých SLA komponentov a SLO a SQO parametrov. Zo strany poskytovateľa cloudových služieb je potrebné zadať úroveň bezpečnosti cloudových služieb.

### 8.7.6 Zrušenie služieb

V prípade zrušenia služieb alebo aj celkovo zrušenia odberateľa cloudových služieb je potrebné mať poskytovateľom cloudových služieb zadefinovaný „exit“ proces, ktorý definuje:

- výpovednú lehotu,
- spôsob vysporiadania s platbami,
- spôsob navrátenia dát a/alebo aplikačných artefaktov odberateľovi cloudových služieb,
- spôsob vymazania dát,
- ustanovenia ohľadne doby medzi pozastavením služby a vymazaním údajov,
- a ďalšie relevantné aspekty pri zrušení služby.

Predmetom SLA zmluvy je uvedenie podmienok zrušenia služieb alebo zrušenia odberateľa cloudových služieb.

### 8.7.7 Servisná podpora

Súčasťou SLA sú aj podmienky servisnej podpory vrátane SLO a SQO pre poskytované cloudové služby. Servisná podpora by mala obsahovať 1st level podporu zabezpečujúcu podporu pre bežné administratívne úlohy (reset hesiel, fakturácia, zadávanie incidentov a pod.) a taktiež 2nd level podporu pre riešenie závažných incidentov.

SLO môžu byť rôzne kategorizované podľa kritickosti incidentu, služby a podobne a je možné ich definovať ako:

- servisné časy – doba počas ktorej je poskytovaná servisná podpora,
- reakčná doba – doba do ktorej poskytovateľ cloudovej služby poskytne spätnú väzbu odberateľovi cloudových služieb,
- doba vyriešenia incidentu – doba do ktorej musí byť incident vyriešený.

SQO môžu byť definované spôsobom komunikácie servisnej podpory, reportingovými nástrojmi, servisnými plánmi a pod.

### 8.7.8 Štandardy, certifikácia a audit (governance)

V rámci SLA je potrebné definovať legislatívu, štandardy, normy, audity alebo ďalšie relevantné dokumenty na základe ktorých sú riadené cloudové služby.

### 8.7.9 Zmenové požiadavky

V prípade zmeny služieb je potrebné mať poskytovateľom cloudových služieb zadefinovaný proces zmenových požiadaviek (change management). V podmienkach vládneho cloudu môže byť pri zmenách povinná autorizácia zo strany poskytovateľa cloudových služieb.

### 8.7.10 Spoľahlivosť služieb (reliability)

Spoľahlivosť služieb je dôležitou charakteristikou cloudových služieb. V rámci SLA môžu byť zohľadnené nasledovné aspekty spoľahlivosti služby:

- Tolerancia voči výpadkom (Fault tolerance) – schopnosť plynulej prevádzky služby v prípade výpadku jedného alebo viacerých komponentov.
- Doba obnovy (Resilience) – schopnosť služby navrátenia do pôvodného stavu v prípade významnej poruchy.
- Zálohovanie a obnova dát – SLA môže obsahovať parametre a doby zálohovania a obnovy
- Disaster recovery – SLA môže obsahovať disaster recovery plán a údaje ohľadne RTO (recovery time objective) a RPO (recovery point objective).

### 8.7.11 Manažment dát

V rámci SLA je odporúčané uviesť špecifiká ohľadne prístupu k dôvernosti informácií, prenositeľnosti, vymazania, retencie, legislatívnej regulácie a geografickej polohy umiestnenia dát.

### 8.7.12 Ochrana duševného vlastníctva

V rámci SLA je odporúčané zdefinovať prístup poskytovateľa cloudových služieb k ochrane duševného vlastníctva odberateľa cloudových služieb.

### 8.7.13 Dáta poskytovateľa cloudových služieb

Dáta potrebné k prevádzke cloudového prostredia sú pod kontrolou a vlastníctvom poskytovateľa cloudových služieb, okrem prípadov kedy sa odberateľ a poskytovateľ cloudových služieb špecificky dohodnú na inom prístupe k vymedzeným dátam.

## 9 Hybridný vládny cloud

### 9.1 Ciele

NKVIS v kapitole 6.2.8 hovorí, že budú preskúmané možnosti postupnej hybridizácie vládneho cloudu, ktorý je v prvej fáze budovaný ako privátny cloud predovšetkým z hľadiska bezpečnosti a ochrany osobných údajov. Sprostredkovateľ cloudových služieb (Government Cloud Broker - GCB), ktorým je ÚPPVII, alebo ním poverená organizácia, bude na základe kritérií ekonomickej výhodnosti rozhodovať, či nová cloudová služba požadovaná užívateľom z verejnej správy, bude vyvíjaná a prevádzkovaná výhradne v prostredí vládneho cloudu, alebo bude využitá hybridná schéma. Tzn., že zhodnotí, či nie je možné a ekonomicky výhodnejšie použiť cloudovú službu od poskytovateľa cloudových služieb (Cloud Service Provider - CSP) mimo vládny (privátny) cloud v rámci SR, alebo EU alebo či takáto hybridná schéma neprináša iné výhody ako väčšiu pružnosť, agilnosť alebo kratší čas zavedenia služby (time-to-value). Tento proces bude s postupným nárastom realizovaný automatizovaným-samoobslužným spôsobom (Cloud Management Platformy a ďalšie nástroje).

V súlade so stratégiou EU v oblasti rozvoja cloudových služieb NKIVS zdôrazňuje, že prioritne by v hybridnom vládnom cloude mali byť využívané služby vládnych cloudov ostatných členských štátov EU, keďže existuje silný predpoklad, že cloudové služby vyvíjané a prevádzkované jednotlivými členskými štátmi EU budú do značnej miery podobné a budú spĺňať prísne kritériá nielen na bezpečnosť, ale i na špecifické požiadavky verejnej správy. Pred vybudovaním plnej funkcie cloud brokera (2018) je vhodné realizovať pilotné projekty využitia hybridného vládneho cloudu. Práve využitie hybridného cloudu dáva možnosť pre organizácie verejnej správy efektívne preklenúť obdobie, kým budú všetky príslušné služby sprístupnené v rámci štátneho cloudu.

V nasledujúcich kapitolách sú popísané:

- Typické situácie, v ktorých je možné predpokladať pre používateľa cloudovej služby ekonomickú výhodu použitia hybridnej schémy vládneho cloudu (Use Cases).
- Odporúčané štandardy pre komunikáciu a výmenu dát v hybridnom vládnom cloude.
- Procesy a základné funkcie, ktoré bude plniť sprostredkovateľ služieb vo vládnom cloude, predovšetkým certifikácia poskytovateľov a ich služieb, udržiavanie a monitorovanie certifikovaných služieb, obstarávanie nových cloudových služieb u certifikovaných poskytovateľov.



## 9.2 Typické situácie použitia služieb vládneho cloudu, kedy je možné očakávať lepšiu ekonomickú efektívnosť v prípade využitia hybridného vládneho cloudu

### 9.2.1 Prípad použitia 1 – Uskladnenie otvorených dát

Používateľ vládneho cloudu má veľké objemy otvorených dát, ktoré sú pseudonymizované, relatívne statické a ktoré si nevyžadujú najvyššiu úroveň bezpečnosti. Pokiaľ certifikovaný public CSP splňuje požadovanú SLA a jeho služba je lacnejšia v porovnaní s vládny cloudom, bude táto služba hybridná.

### 9.2.2 Prípad použitia 2 – Úložisko pre Big Dáta

Používateľ prevádzkuje agendový systém vo vládnom cloud, ktorý pracuje s Big dátami, ktoré pochádzajú zo zdrojov mimo VS a ktoré nie sú citlivé. Uchovávanie takýchto dát vo vládnom cloud by zaberalo pamäťový priestor, potrebný pre agendy s vyššou citlivosťou. Pokiaľ certifikovaný public cloud CSP splňuje SLA a jeho služba je lacnejšia, bude použitý takýto hybridný vládny cloud.

### 9.2.3 Prípad použitia 3 – Cloudbursting

V prípade krátkodobého nedostatku výpočtového výkonu alebo pamäťovej kapacity (cloud outbursting) u CSP vládneho cloudu (DC MF, DC MV) budú menej citlivé dáta, služby alebo agendové systémy vo vopred definovanom poradí presúvané k certifikovanému CSP, prednostne do vládneho cloudu iného ČS EU, ktorý je schopný splniť požadované SLA. Súčasťou SLA bude povinnosť vymazať všetky dáta, ktoré boli dočasne presunuté do tohto cloudu po ukončení služieb outburstingu.

### 9.2.4 Prípad použitia 4 – Využitie SaaS služieb

Odberateľ vládneho cloudu žiada o zavedenie novej služby SaaS alebo SaaS ktorý využije ako riešenie agendového systému, ktorý si nevyžaduje nový vývoj a nejedná sa o citlivú službu, ktorá a priori musí byť prevádzkovaná vo vládnom cloud. Sprostredkovateľ (CSB) preverí v zoznamoch služieb certifikovaných CSP v EU, či požadovaná SaaS alebo agenda nie je k dispozícii u niektorého z týchto CSP. Pokiaľ takto definovaná služba existuje u niektorého CSP vládneho cloudu iného ČS EU bude odberateľovi sprostredkovaná cestou CSB táto služba. Pokiaľ nie je, vyhlási CSB obstarávanie, ktorého sa okrem CSP vládneho cloudu môžu prihlásiť i certifikovaní CSP v SR alebo EU. Pokiaľ je víťazom tendra CSP mimo vládneho cloudu SR, bude SaaS alebo agendový systém prevádzkovaný v tomto príslušnom cloud.

Pozn.: Je potrebné zdôrazniť, že bez ohľadu na to, či bude odberateľovi poskytovaná služba vládneho cloudu SR, alebo služba bude poskytovaná hybridne niektorým certifikovaným CSP v SR alebo EU, bude z pohľadu používateľa poskytovaná transparentne ako služba vládneho cloudu.

### 9.2.5 Prípad použitia 5 – Najlepšie miesto pre prevádzku

Pokiaľ sa nejedná sa o citlivú službu, ktorá a priori musí byť prevádzkovaná vo vládnom cloudu, môže byť umiestnená a prevádzkovaná u iného certifikovaného CSP na základe svojich špecifických požiadaviek.

### 9.2.6 Prípad použitia 6 – Hybridný model riadenia procesov SW inžinierstva

Aplikácie a služby vo vývojových a testovacích fázach sú umiestnené a prevádzkované u certifikovaného CSP, zatiaľ čo prevádzka týchto aplikácií a služieb je zabezpečená vládny cloudom.

### 9.2.7 Prípad použitia 7 – Architektúra rozdelenia vrstiev

Architektúra rozdelenia vrstiev môže umožniť realizovať aplikácie s požiadavkami na sofistikovanú databázu prevádzkovanú vo vládnom cloud, zatiaľ čo vrstvy front-endu budú nasadené hybridne niektorým certifikovaným CSP.

### 9.2.8 Prípad použitia 8 – Disaster Recovery

Architektúra disaster recovery umožňujúca prevádzku v systémov vo vládnom cloude, ale pre potreby BCP sa využívajú podľa potreby služby certifikovaného CSP.

### 9.2.9 Prípad použitia 9 – Zálohy a archivácia

Archivácia a záloha nekritických dát môže byť realizovaná mimo základných služieb vládneho cloudu, ak sú podmienky vhodné a výhodnejšie, avšak vždy v súlade s bezpečnostným projektom daného ISVS.

### 9.2.10 Prípad použitia 10 – Federácia Identít

Systém federácie identít umožní podporu jednotlivých cloudových služieb od rôznych CSP a synchronizáciu identít od odoberajúcich organizácií. Zároveň umožní kontrolovanú a bezpečnú spoluprácu s externými subjektami, používajúcimi cloudové služby.

## 9.3 Spôsoby riešenia

### 9.3.1 Odporúčané štandardy pre komunikáciu a výmenu dát v hybridnom vládnom cloude

Komunikačné mechanizmy Hybridného Cloudu je možné rozdeliť podľa povahy služby prevádzkovej v hybridnom scenári a požiadaviek, ktoré sú kladené na dostupnosť a spoľahlivosť komunikačného kanála:

1. Zabezpečené aplikačné volania cez dostupnú Internet infraštruktúru.
2. Bezpečné prepojenie pomocou kryptovaného kanála – VPN.
3. Bezpečné a spoľahlivé priame pripojenie na úrovni dátového/telekomunikačného operátora.

### 9.3.2 Zabezpečené aplikačné volania cez dostupnú Internet infraštruktúru

Tento spôsob komunikácie je vhodný pre jednoduché služby typu bezpečný web portál alebo web sídlo. Prístup ku službe je realizovaný dostupnou Internet infraštruktúrou, komunikácia však musí byť však kryptovaná a zabezpečená aspoň na úrovni certifikátov, prípadne asymetrických kľúčov.

Príklady použitia:

- https volania služby,
- zabezpečené JSON volania cez https na konfiguráciu služby,
- bezpečné RDP/RDS alebo SSH volania.

### 9.3.3 Bezpečné prepojenie pomocou šifrovaného kanála – VPN

Tento spôsob komunikácie je najčastejšie používanou metódou komunikácie, kde sa medzi odoberateľom služby a poskytovateľom zabezpečenou šifrovanou linkou, ktorá je postavená na internet komunikačnej infraštruktúre.

Tento variant umožňuje vytvorenie hybridnej infraštruktúry, nad ktorou bude mať organizácia kontrolu. Požaduje však nasledovné:

- Dodanie vlastnej IP adresy a serverov DNS.
- Zabezpečenie pripojenia pomocou IPSec VPN.

Medzi prínosy tejto variant patrí:

- Získanie detailnej kontroly prevádzky medzi podsietami.
- Vytvorenie prepracovaných sieťových topológií pomocou virtuálnych prostriedkov.

- Získanie izolovaného a zabezpečeného prostredia pre služby a aplikácie, kde sa služba vyskytuje transparentne a homogénne k privátnemu cloudu.

#### 9.3.4 Bezpečné a spoľahlivé priame pripojenie na úrovni dátového/telekomunikačného operátora.

Tento komunikačný spôsob využíva koncept vyhradenej privátnej linky mimo internet. Priame pripojenie umožňuje vytvoriť privátne pripojenie medzi dátovým centrom hybridných služieb a infraštruktúrou v privátnom cloudu alebo v okolitom prostredí. Ponúka spoľahlivejšie, rýchlejšie a bezpečnejšie spojenie s nižšou latenciou ako typické pripojenia cez internet.

Typickým spôsobom priameho pripojenia je spojenie zo súčasnej siete – určený bod v sieti WAN prepojený pomocou VPN s technológiou MPLS, od poskytovateľa sieťových služieb, ku komunikačnému bodu v dátovom centre hybridných cloudových služieb.

#### 9.3.5 Funkcie Sprostredkovateľa v Hybridnom vládnom cloudu (Government Cloud Broker- GCB)

Funkcie GCB budú vytvárať platformu pre zabezpečenie všetkých scenárov využitia Hybridného vládneho cloudu uvedených v čl. 5.2 pri zohľadnení špecifických požiadaviek VS na cloudové služby, predovšetkým z hľadiska bezpečnosti, ochrany osobných údajov, ďalších legislatívnych požiadaviek, interoperability, platformovej neutrality a prenositeľnosti cloudových služieb (vylúčenie vendor-lock). Riešenie GCB sa bude opierať o štandardy resp. odporúčania ENISA a ETSI (REST, CIMI, JSON, výstupy Cloud for Europe,...). GCB bude udržiavať zoznam akreditovaných Poskytovateľov cloudových služieb (CSP) a certifikovaných služieb od týchto CSP. (Procesy akreditácie CSP a certifikácie cloudových služieb sú uvedené v kap. 11). V prípade požiadaviek užívateľov na nové cloudové služby sa bude GCB podieľať na ich obstaraní v prípade, že služby odpovedajú niektorému zo scenárov vhodných pre Hybridný vládny cloud tak, že GCB bude štandardným spôsobom komunikovať s akreditovanými CSP s cieľom vybrať najvhodnejšieho dodávateľa služby v rámci SR alebo vládnych cloudov ČS EU. GCB bude schopný v prípade komplexných cloudových služieb vytvárať kombinované služby CSP Vládneho cloudu a externých CSP (napr. Big Data sú uložené u externého CSP ale sú spracovávané vo Vládnom cloudu).

#### 9.3.6 Základné funkcie GCB

- Atribúty cloudových služieb

Atribút popisuje charakteristiku cloudovej služby, ktorá môže byť posúdená kvantitatívne resp. kvalitatívne ľudskými alebo automatizovanými prostriedkami (ISO 27000:2014).

- Ponuka služby

Súbor vymedzení atribútov (napr. up-time > 99,99) popisujúci SLA úrovne poskytovania, model spoplatnenia a ďalšie podmienky používania služby CSP.

službu CSP

- Požiadavka na služby

Špecifický súbor vymedzení na atribúty popisujúce požiadavky užívateľa na aplikáciu (alebo jej časť) v strojovo čitateľnej forme. Tento dokument umožňuje výber certifikovanej služby od akreditovaných CSP (alebo vyhodnotenie miery splnenia požiadaviek na službu) a spustenie vybranej služby.

- Potvrdenie služby

Potvrdenie parametrov služby ponúkanej konkrétnym CSP, ktorá bola verifikovaná podľa štandardnej metodiky (audítorom alebo potvrdeným sebahodnotením CSP).

- Kontrakt



Digitálnym kľúčom podpísaný formálny záznam potvrdzujúci dohodnuté atribúty služby (SLA, model spoplatnenia, a pod.) spolu so všetkými súvisiacimi obchodnými podmienkami kontraktu – zaručujúci nezmeniteľnosť dohodnutých podmienok (princíp elektronického podpisu).

- Priebežné monitorovanie cloudových služieb

Monitorovanie atribútov cloudových služieb spojených s bezpečnosťou a plnením legislatívnych požiadaviek.

- Bezpečnostná služba

Služba poskytujúca informáciu o úrovni bezpečnosti cloudovej služby.

- Finálne zúčtovanie služieb

Vytvorenie a prevádzkovanie služieb v zmysle ekonomicky najvýhodnejšieho prevádzkovania poskytovaných služieb v rátane finálneho zúčtovania s medzi poskytovateľmi. Podrobne finančný model rozoberá samostatná kapitola 14 Model(y) spoplatnenia.

### 9.3.6.1 Funkčné komponenty GCB

#### A. Repozitár atribútov

Repozitár poskytuje definície všetkých atribútov, ktoré môžu použiť v Ponuke cloudových služieb, v Popise požiadaviek na službu a Potvrdení služby. Umožňuje vyhľadávať Atribúty a podporuje vývoj Atribútov a celkovú ontológiu. Každý Atribút je identifikovaný unikátnym URI. Repozitár riadi každý Atribút ako samostatný REST zdroj umožňujúci štandardné CRUD akcie pomocou API na báze CIMI štandardu. Každý Atribút má svoj zoznam prístupových práv určujúci kto môže vidieť alebo modifikovať tento Atribút.

#### B. Katalóg cloudových služieb

Katalóg riadi Ponuku služieb a Potvrdenie služieb v rámci Hybridného cloudu. Ponuka služieb a Potvrdenie služieb obsahujú hodnoty asociované s Atribútmi konkrétnej služby. Ponuka služby zahŕňa i všeobecnú informáciu o CSP a cenové informácie. Potvrdenie služby je poskytované samotným CSP, poskytovateľom bezpečnostnej informácie alebo audítorom.

#### C. Katalóg požiadaviek na cloudové služby

Katalóg obsahuje popis Požiadaviek na služby, ktoré sú asociované s komponentami aplikácií užívateľa. Popis Požiadaviek na služby môže byť špecifický pre konkrétnu aplikáciu alebo pre spoločné politiky zdieľané viacerými užívateľmi. V Katalógu sú vykonávané dopyty na základe ktorých je vybraný konkrétny CSP a sú vyhodnotené výsledky vzhľadom na Požiadavky.

Popis služby obsahuje:

- Referenciu na žiadateľa, ktorý vytvoril Požiadavku
- Súbor popisov vymedzení Atribútov alebo referenciu na existujúci popis Požiadavky na službu
- Vytvorenie časovej pečiatky

#### D. Sprostredkovateľ služieb CSP pre užívateľov

Sprostredkovateľ použije popis Požiadavky na službu a Potvrdenie služby aby vybral z Katalógu služieb požadovanú službu. Sprostredkovateľ bude volaný „Deployment Enginom“ pri každom spustení služby počas jej životného cyklu, vrátane iníciačného alokovania zdrojov a následného škálovania. „Deployment Engine“ bude využívať RESTful API Sprostredkovateľa.

#### E. Katalóg kontraktov

Katalóg obsahuje zoznam aktívnych, ale i historických kontraktov, medzi užívateľmi a CSP, zabezpečuje ich integritu ako aj celkový manažment životného cyklu dlhodobého úložiska elektronicky podpísaných dokumentov.

#### F. Manažment životného cyklu služieb

Generická platforma pre komplexné riadenie životného cyklu cloudových služieb rôznych CSPs. Táto platforma bude používať katalóg cloudových služieb, katalóg kontraktov, a podporované integračne rozhrania pre sprostredkovanie aktivácie, deaktivácie služby a manažmentu zmien konfigurácií služieb. Platforma bude podporovať kompozitné multi-cloudové schémy, kde jednotlivé cloud služby môžu byť aktivované na rôznych cloudových infraštruktúrach Hybridného vládneho cloudu.

#### G. Poskytovateľ bezpečnostných informácií

Poskytovateľ bezpečnostných informácií zabezpečuje, aby aktuálna informácia o bezpečnosti služby bola súčasťou Katalógu služieb vo forme Potvrdenia služby.

Poskytovateľ bezpečnostných informácií vykonáva:

- Extrakt informácií z Bezpečnostného servisu týkajúceho sa daného CSP,
- Upravuje túto informáciu s použitím definovaných Atribútov a schém,
- Vkladá túto informáciu formou Potvrdenia služby do Katalógu služieb,
- Premieta zmeny bezpečnostnej informácie keď sa objavia v Bezpečnostnom servise.

#### H. Pribežné monitorovanie

CSP ktorí budú participovať v Hybridnom vládnom cloudu a ktorí chcú poskytovať služby s vysokou garanciou bezpečnosti budú musieť implementovať monitorovací API, ktorý umožní užívateľovi získavať informáciu o úrovni bezpečnosti poskytovaného servisu takmer v reálnom čase.

#### I. Notifikácie

Riešenie GCB bude obsahovať notifikačný rámec, ktorý bude zabezpečovať:

- oznam pre CSP, že Požiadavka na novú cloudovú službu bola publikovaná po tom ako žiadna existujúca služba v Katalógu služieb nevyhovela Požiadavke na službu,
- oznam pre užívateľa, že CSP má novú ponuku, ktorá splňuje atribúty skôr vydannej Požiadavky na novú cloudovú službu,
- oznam pre užívateľov, že nový Atribút bol navrhnutý vytvoriť alebo upraviť v Repozitári Atribútov,
- oznam užívateľovi, že zmena v obstaranej službe môže znehodnotiť niektoré požiadavky pôvodne uvedené v popise Požiadavky na službu.

## 10 Podpora „DR a BCP“ pomocou cloudových služieb

### 10.1 Cieľ

Cieľom tejto kapitoly je definovanie stratégie pre implementáciu BCP vrátane DR pre služby poskytované vládny cloudom. Oba tieto parametre by mali byť súčasťou SLA pre jednotlivé služby. Preto je nutné ich adresovať po vrstvách: IaaS, PaaS a SaaS. SLA je definované vždy medzi odberateľom a dodávateľom služby. Dodávateľ služby je zodpovedný za návrh, implementáciu a prevádzku technologického riešenia zabezpečujúceho tieto parametre.

Vládny cloud je centrálnym poskytovateľom vládnych IT služieb a preto akékoľvek neplánované prerušenie služieb môže mať závažný dopad na fungovanie štátu. Pre zabezpečenie plynulej prevádzky je nevyhnutné zabezpečiť:

- Business Impact analýzu (identifikácia a analýza potencionálnych hrozieb).
- Vypracovanie BCP stratégie vrátane DR plánov, procedúr a pod.
- Realizácia pravidelných DR testov.

Po organizačnej stránke musia byť jasne definované role a zodpovednosti za plánovanie, manažment a realizáciu BDP a DR.

## 10.2 Business Continuity Planning alebo BCP

Z hľadiska zaistenia Business Continuity Planning (BCP) služieb vládneho cloudu sú dôležité nasledujúce aspekty:

- vysoká dostupnosť (high availability / HA),
- nepretržité operácie (continuous operations),
- zotavenie z havárie (disaster recovery /DR).

„High availability“ (HA) je súhrn technických riešení pre nepretržitú dostupnosť výpočtových služieb a zdrojov tak, že vzniknutý výpadok systému bude mať na užívateľov minimálny dopad. V IT infraštruktúre sa HA dosahuje elimináciou kritických bodov zlyhania (SPOF-single point of failure). Využívané sú technologické prístupy ako redundantná stavba komponent, kontrola chýb a samo opravné mechanizmy, alternatívne či redundantné cesty pre I/O požiadavky, ale aj transparentne zrkadlené dáta na oddelených úložných zariadeniach. Systém sa po výpadku zotaví automaticky takže vlastný výpadok užívateľ takmer alebo vôbec nezaregistruje.

Pojem „continuous operations“ (CO) predstavuje schopnosť minimalizácie výpadkov systému počas rutinných operácií nad IT infraštruktúrou. Rutinné operácie zahŕňujú zálohovanie, údržbu systémov, upgrady, rekonfigurácie a iné.

Zotavenie z havárie „disaster recovery“ (DR) je dopredu definovaný proces reakcie na vzniknutú haváriu, prípadne živelnú pohromu, ktorého cieľom je opätovne poskytnúť služby výpočtového výkonu zo záložnej lokality. V prípade takejto situácie si musia byť užívatelia vedomí, že výpadok zasiahol primárne dátové centrum a doba výpadku je priamo závislá od riešenia procesu obnovy DR.

HA je predmetom technickej a CO predmetom prevádzkovej dokumentácie. Požaduje sa HA infraštruktúra bez SPOF pomocou implementácie minimálne princípu N+1. Kde v prípade zlyhania jedného komponentu je tento nahradený automaticky a v čo najkratšom čase iným rovnakého typu.

Princípom DR sa budeme venovať v nasledujúcich kapitolách tejto časti dokumentu.

## 10.3 Disaster Recovery alebo DR

Spôsob riešenia procesu obnovy DR je závislý od nasledujúcich parametrov:

- Recovery Time Objective (RTO) vyjadruje časový úsek, počas ktorého je nevyhnutné obnovu po havárii dokončiť, inými slovami aký dlhý výpadok služby je akceptovateľný.
- Recovery Point Objective (RPO) definuje časový bod pred haváriou do ktorého je možné obnovu previesť, čo v podstate znamená aká veľká strata dát z doby pred haváriou je akceptovateľná.

V závislosti od požadovaných hodnôt RTO a RPO sa bude líšiť konkrétne riešenie DR. Jednotlivé úrovne DR boli definované skupinou s názvom SHARE ako „7-úrovňový model Disaster Recovery“ (Seven tiers of Disaster Recovery)

Prehľad jednotlivých úrovní modelu SHARE:

Úroveň modelu SHARE pre Disaster Recovery
<b>0 – No off-site data</b>
<b>1 – Data backup with no hot site</b>
<b>2 – Data backup with a hot site</b>
<b>3 – Electronic vaulting</b>

**4 – Point-in-time copies****5 – Transaction integrity****6 – Zero or near-Zero data loss****7 – Highly automated, business integrated solution***Tabuľka 1 Prehľad jednotlivých úrovní modelu SHARE*

Bližší popis jednotlivých úrovní DR sa nachádza na nasledujúcom odkaze:  
<http://recoveryspecialties.com/7-tiers.html>

Voľba správneho DR riešenia vyžaduje zvoliť rozumný kompromis medzi finančnými nákladmi na technické riešenie a nákladmi spojenými s prestojmi a stratou dát. Napr. môže byť prijateľná strata určitého množstva dát v prípade, že tieto dáta môžu byť obnovené z iných zdrojov alebo nanovo vygenerované.

## 10.4 Aktuálny stav

V roku 2015 bol zrealizovaný projekt IaaS časť 1. v DK1 Kopčianska v gescii MF SR. Koncom roku 2016 bude dokončená realizácia projektu IaaS časť 2 DT1 Tajov v gescii MV SR. Súčasťou druhého menovaného projektu je aj infraštruktúra potrebná na zabezpečenie DR pre IaaS služby medzi oboma časťami. Nasledujúca tabuľka mapuje technologické riešenie a možnosti pre odberateľov služby.

Úroveň modelu SHARE pre Disaster Recovery	Podpora zo strany Cloud platformy IaaS
<b>0 – No off-site data</b>	Áno (dostupné odberateľom)
<b>1 – Data backup with no hot site</b>	Áno (dostupné odberateľom)
<b>2 – Data backup with a hot site</b>	Áno (nedostupné odberateľom)
<b>3 – Electronic vaulting</b>	Áno (nedostupné odberateľom)
<b>4 – Point-in-time copies</b>	Áno (dostupné odberateľom)
<b>5 – Transaction integrity</b>	Nie (podpora od úrovne Cloud platformy PaaS)
<b>6 – Zero or near-Zero data loss</b>	Nie (podpora od úrovne Cloud platformy PaaS)
<b>7 – Highly automated, business integrated solution</b>	Nie (podpora od úrovne Cloud platformy SaaS)

*Tabuľka 2 Prehľad jednotlivých úrovní modelu SHARE a ich podpora zo strany Cloud platformy IaaS.*

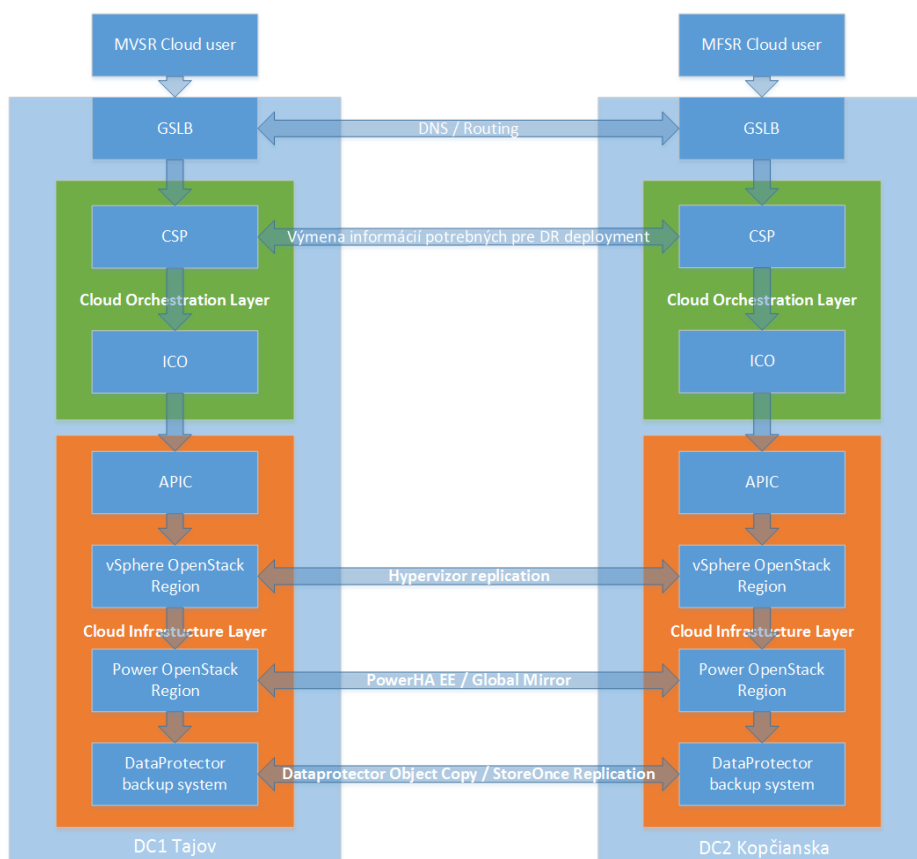
To znamená, že odberateľom IaaS služieb cloudu sú dostupné úrovne 1 a 4. Z dôvodu úspory aktív IaaS je DR úroveň 4 dostupná iba pre produkčné prostredia. Úroveň 0 si nevyžaduje žiadne navýšenie aktív IaaS, ale neposkytuje ani žiadne DR nástroje, čo nie je v súlade s výnosom č. 55/2014 Z. z. ministerstva financií Slovenskej republiky o štandardoch pre informačné systémy verejnej správy.

Úroveň 1 poskytuje možnosť „offsite backup“ (záloha systémov mimo lokalitu datacentra, z ktorého sú prevádzkované) a vyžaduje zvýšené náklady na úložisko. V prípade aplikovania DR bude nutné vybudovanie novej IaaS infraštruktúry a obnova systémov z týchto záloh.

Úroveň 4. poskytuje vybudovanie identického prostredia v datacentre v inej lokalite. Toto prostredie (DR) je pasívne a pravidelne sa synchronizuje s primárnym prostredím, tak aby vytváralo jeho zrkadlový obraz. V prípade rozhodnutia o aktivácii DR pre dané prostredie:

1. prevádzkový personál IaaS zruší sieťový prístup k primárnemu prostrediu a zabezpečí aktiváciu DR prostredia. Čas potrebný na aktiváciu DR prostredia by nemal prekročiť 12 hodín.
2. Odberatelia IaaS služieb zabezpečia správne fungovanie svojich systémov v DR prostredí .
3. Odberatelia IaaS služieb požiadajú prevádzkový personál IaaS o sieťové sprístupnenie DR prostredia a presmerovanie koncových užívateľov na DR prostredie. Tento proces by nemal prekročiť dobu 1 hodiny.
4. Po odstránení príčiny, ktorá vyvolala DR je nutné v prvom rade vytvoriť na primárnom prostredí zrkadlový obraz DR prostredia a následne aplikovať kroky 1 až 3 s tým, že sa vymení rola DR a primárneho prostredia.

Pre zabezpečenie uvedených mechanizmov DR IaaS je nutné vytvoriť vzájomné prepojenia riadiacich systémov IaaS. Princiálna schéma prepojenia je v nasledujúcom obrázku:



Obrázok 20 Princiálna schéma prepojenia riadiacich komponentov.

#### 10.4.1 Prepojenie orchestračných platforiem/nástrojov (cSP)

Celá konfigurácia aplikačného prostredia je realizovaná cez samoobslužný portál a orchestračný nástroj cSP. Táto zabezpečuje konfiguráciu jednotlivých komponentov aplikačného prostredia ako sú virtuálne servery, diskové úložiská, firewall a loadbalancer inštancie a podobne.

Aby bolo požadované aplikačné prostredie vytvorené aj v sekundárnom dátovom centre je nutné vytvoriť synchronizačné prepojenie medzi orchestračnými platformami jednotlivých DC.

### 10.4.2 Koncept DR pre serverové platformy.

V rámci projektov IaaS časť 1. a 2. boli vybudované dve serverové platformy: Intel a RISC

Pre replikáciu dát na serverovej platforme Intel je využívaná technológia na báze replikácie zápisov na úrovni virtualizačnej platformy (hypervisor-based replication). Pre replikáciu dát na serverovej platforme RISC je využívaná technológia klastrovania. Topológia klastra bude definovaná pre DR jedným uzlom klastra v dvoch geograficky oddelených lokalitách (DT1, DK1) s definovanou primárnou a záložnou lokalitou, celkovo dva uzly na jeden klastrový systém.

### 10.4.3 Asynchrónna replikácia diskových polí

Použitie replikačnej technológie determinuje kompatibilita s použitou DR serverovou platformou a geografická vzdialenosť cca. 200km medzi lokalitami DT1 a DK1.

	Synchronná replikácia	Asynchrónna replikácia
<b>Failover</b>	Manuálny	Manuálny
<b>Prerušenie služby</b>	Áno	Áno
<b>Resynchronizácia</b>	Manuálna	Manuálna
<b>RPO</b>	Nula	Blízke nule
<b>RTO</b>	Minúty/hodiny	Minúty/hodiny
<b>Host I/O výkonnosť</b>	Latencia diskov + RTT linky	Latencia diskov
<b>Použitie prenosových protokolov</b>	FCP, FCoE	FCP, FCoE, FCIP
<b>Latencia (maximálna)</b>	20ms	80ms
<b>Vzdialenosť (maximálna)</b>	300 km	8000 km
<b>Konfigurácia SAN Fabrikov</b>	Štandard	Štandard

Tabuľka 3 Charakteristiky replikačných módov diskového poľa.

S pohľadu integrity replikovaných dát je preferovaným riešením využitie synchronnej replikácie, ktorá zabezpečuje nulovú stratu dát tzn. RPO=0, čo je zabezpečené potvrdením zápisu na systémovej úrovni až v momente keď sú dáta zapísané na diskoch diskových polí v oboch lokalitách. Synchronná replikácia dát má však s rastúcou vzdialenosťou zásadný vplyv na výkonnosť I/O keďže zápis dát je závislý od latencie disku na diskovom poli a latencii prenosovej linky RTT medzi diskovými poľami.

Pokiaľ budeme uvažovať vzdialenosť medzi dátovými centrami DT1 a DK1 cca. 200km bude teoretická latencia podľa dokumentácie:

**RTT=2ms (200km) + 3ms (dodatočná latencia z dôvodu sieťovej infraštruktúry) = 5ms**

Čo by znamenalo pri synchronnej replikácii, že každý zápis dát je závislý od latencie disku na diskovom poli a na latencii prenosovej linky RTT medzi diskovými poľami tzn. každé potvrdenie zápisu na disk by trvalo viac ako **5ms**.

Z dôvodu veľkej výkonovej degradácie pri použití synchronnej replikácie **uvažujeme iba s využitím asynchrónnej replikácie dát**, ktorá zabezpečuje nízku stratu dát s vysokým výkonom I/O operácií.



**Pri asynchrónnej replikácii dát** pri zápise na disk je zabezpečené potvrdenie zápisu na systémovej úrovni už v momente keď sú dáta zapísané na disku v primárnej lokalite čím sa eliminuje latencia zápisu, ktorá je závislá iba od typu disku a jeho aktuálneho vyťaženia viď nižšie uvedený obrázok. **Pri využití asynchrónnej replikácie dát je strata dát vyjadrená parametrom RPO závislá od konkrétnej aplikácie.**

#### 10.4.4 Prepojenie dátových centier

Pre potreby realizácie prepojenia riadiacich komponentov dátových centier je nutné vytvoriť fyzické prepojenie dátových centier ako takých. Z povahy požadovaných prepojení je nutné realizovať prepojenie pre IP/ethernet ako aj pre synchronizáciu dátových úložísk v SAN sieti.

Potrebné prepojenia sú definované nasledovne:

- 2x 10Gbps ethernet
- 2x 8Gbps FC
- Je požadované prepojenie po dvoch nezávislých trasách

Fyzické prepojovacie trasy sú vytvorené ako prenajaté okruhy cez DWDM.

#### 10.4.5 Prístup používateľa na aplikácie resp. IS v DR režime

Používateľské požiadavky na služby prevádzkované v geograficky rozdielnych lokalitách (cloud DC) je najefektívnejšie smerovať pomocou DNS záznamov. Samotné služby v rôznych DC budú prevádzkované na nezávislých verejných IPv4 adresách (v budúcnosti je možný prechod/kombinácia IPv6). Tieto DNS záznamy však nebudú statické ale budú dynamicky riadené na základe rôzneho množstva parametrov.

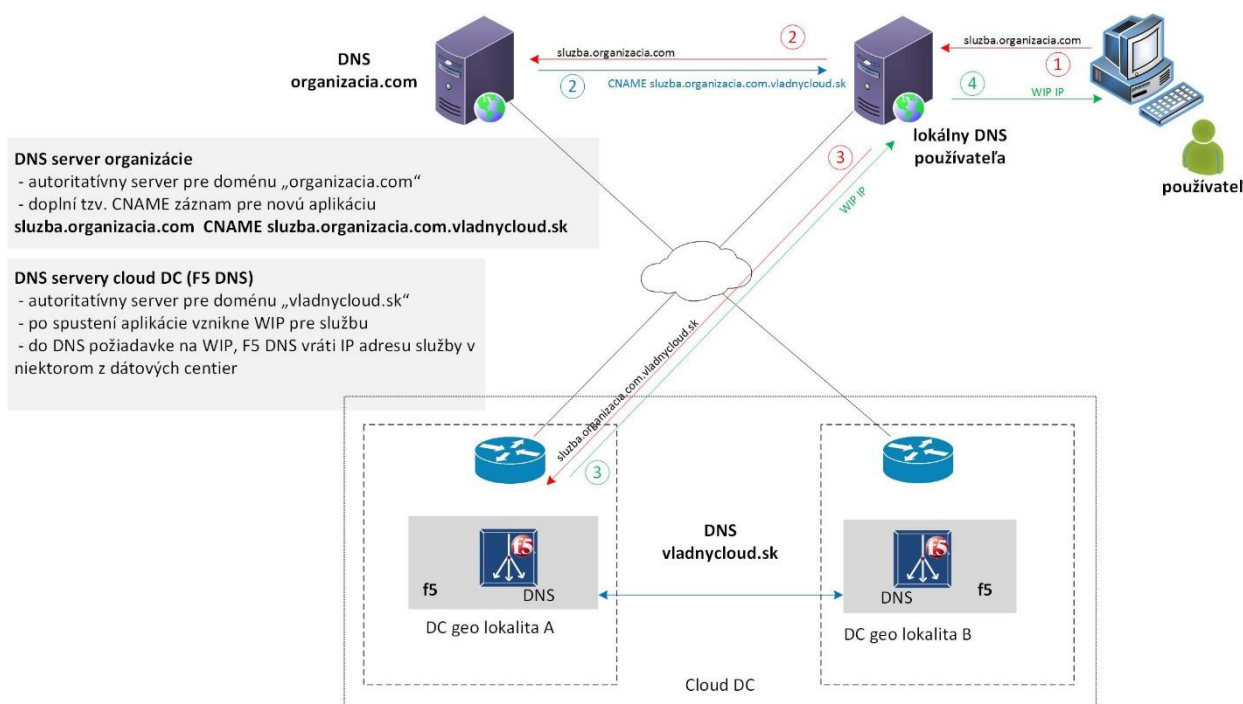
#### 10.4.6 Väzba na DNS systémy správcov aplikácií

Najčastejší prípad je že správca aplikácie prevádzkuje službu v rámci už existujúcej DNS domény. Z možností ako nasmerovať takýto záznam na tzv. WIP adresu (Wide IP pre geo redundanciu) bol zvolený model definície jednotlivých DNS záznamov (nie celej alebo časti DNS domény) s využitím DNS záznamu typu CNAME.

Výhodou tohto modelu je že na strane prevádzkovateľa domény (služby) si to vyžiada iba minimálny zásah a zároveň prevádzkovateľovi naďalej zostáva plná kontrola nad svojim DNS záznamom. Postup prechodu na geo redundanciu je nasledovný:

1. Správca služby pozná DNS meno svojej existujúcej alebo novo definovanej služby (napríklad: sluzba.organizacia.com).
2. Prevádzkovateľ služby v cloud DC oznámi správcovi aplikácie DNS meno pre WIP (napríklad: sluzba.organizacia.com.vladnyccloud.sk, pričom držiteľom DNS domény „vladnyccloud.sk“ bude prevádzkovateľ cloud DC).
3. Správca aplikácie zadefinuje (zmení) DNS záznam „sluzba.organizacia.com“ na záznam typu CNAME pričom ako parameter uvedie WIP DNS meno „sluzba.organizacia.com.vladnyccloud.sk“. Príklad:

sluzba.organizacia.com	CNAME	sluzba.organizacia.com.vladnyccloud.sk
------------------------	-------	--



Obrázok 21 Prístup klienta na DNS službu.

Prístup klienta na službu prevádzkovanú pod menom „sluzba.organizacia.com“:

1. Klient si vyžiada službu zadáním DNS mena „sluzba.organizacia.com“.
2. DNS požiadavka je zaslaná postupne až na autoritatívny DNS server pre doménu „organizacia.com“. Ten vráti DNS záznam typu CNAME „sluzba.organizacia.com.vladnyccloud.sk“.
3. DNS odpoveď musí byť preložená, takže prebehne ďalší proces DNS prekladu ktorý postupne skončí na autoritatívnom DNS serveri pre doménu „vladnyccloud.sk“ (v tomto prípade to bude jeden zo štvorice f5 BIGIP DNS). Práve tu bude zadefinovaná WIP adresa „sluzba.organizacia.com.vladnyccloud.sk“ s logikou geo redundancie.
4. Klient dostane odpoveď v podobe IP adresy služby v konkrétnom cloud DC.

## 10.5 Plánované využitie DR pre aplikácie

Všetky technické špecifikácie realizované pre DR IaaS vychádzajú z potrieb DR pre aplikačné prostredia (alebo vyššie vrstvy cloudu). Preto je nutné definovať režimy DR pre aplikačné prostredia, ktoré sú z pohľadu implementácie do IaaS prostredia podporované.

Charakteristiku DR pre aplikačné prostredia si definuje odberateľ IaaS služieb pri vytváraní aplikačného prostredia.

V tejto dokumentácii sú uvedené definované mechanizmy DR, nie postup ich konfigurácie. Tento bude obsahom prevádzkovej dokumentácie.

### 10.5.1 Aplikácia v DR režime „off-site backup“

Ide o aplikáciu, ktorá je realizovaná len v jednom z cloud dátových centier. Redundancia takejto aplikácie je riešená len redundanciou zariadení v jednotlivých dátových centrách, ktorých záloha sa ukladá na zálohovacích zariadeniach v inom dátovom centre.

Nie sú implementované žiadne konfiguračné rozšírenia z primárneho do sekundárneho dátového centra.



### 10.5.2 Aplikácia v DR režime „Active/Standby“

Aplikácia v tomto režime DR je aktívna a beží v jednom z cloud dátových centier (pre danú aplikáciu **primárne DC**). V tomto primárnom dátovom centre táto aplikácia beží za bežných podmienok.

V druhom z dátových centier (pre danú aplikáciu **sekundárne DC**) sú alokované zdroje a sú vytvorené všetky prvky (diskový priestor, siete atď.), aby v prípade úplného výpadku primárneho DC aplikácia mohla naštartovať a poskytovať danú službu.

Pre tento model DR je realizovaná replikácia dát z primárneho do sekundárneho dátového centra. Ide o asynchrónnu a jednosmernú replikáciu dát. Z dôvodov vzdialenosti dátových centier a s ohľadom na výkonnosť aplikačného prostredia nie je uvažované nad synchrónnymi replikáciami.

### 10.5.3 Aplikácia v DR režime „Active/Active“

Aplikácia v tomto režime DR beží v oboch cloud dátových centrách súčasne a na oboch lokalitách aktívne poskytuje služby pre koncových používateľov. Pri tomto modeli neexistuje pojem primárneho a sekundárneho dátového centra.

Tento druh DR režimu nie je nijak aktívne podporovaný IaaS infraštruktúrou cloud dátových centier. Pri tomto režime ide z pohľadu poskytovateľa IaaS služieb o 2 nezávislé inštancie danej aplikácie bežiace v dvoch lokalitách. Všetky synchronizačné mechanizmy pre správne fungovanie aplikácie v tomto režime sú plne v zodpovednosti administrátorov danej aplikácie a aplikačného prostredia.

Pre tento druh DR nie sú aktivované z pohľadu IaaS infraštruktúry žiadne replikačné mechanizmy ani synchronizácia prostredí (virtuálne servery, diskové priestory).

### 10.5.4 Nepodporované režimy

Iné režimy pre redundanciu jednotlivých aplikačných prostredí nie sú podporované.

V tejto fáze implementácie cloud dátových centier nie sú podporované žiadne priame prepojenia aplikačných prostredí ako takých. Všetky komunikácie medzi aplikačnými prostrediami je nutné z pohľadu administrátora aplikačného prostredia realizovať cez externé siete.

## 11 Migrácie do vládneho cloudu

### 11.1 Ciele

V roku 2014 bol na zasadnutí vlády SR schválený materiál „*Návrh centralizácie a rozvoja dátových centier v štátnej správe*“ spolu s prijatým Uznesením č. 247. Úloha B5 uložila ministrom, predsedom ostatných ústredných orgánov štátnej správy a správcom ďalších kapitol štátneho rozpočtu zabezpečiť do 31. decembra 2020 migráciu informačno-komunikačných technológií príslušného rezortu do dátového centra štátu. Táto úloha sa netýka informačno-komunikačných technológií týkajúcich sa zabezpečenia obrany Slovenskej republiky, bezpečnosti Slovenskej republiky, ochrany utajovaných skutočností a citlivých informácií.

Pre zjednotenie metodológie migrácií bola prijatá úloha B2, ktorá zaväzovala ministerstvo financií vypracovať „*Metodické usmernenie Ministerstva financií Slovenskej republiky č. MF/020304/2014-1721 na spracovanie analýzy stavu a potrieb informačno-komunikačných technológií a na spracovanie harmonogramu migrácie informačno-komunikačných technológií jednotlivých rezortov do dátového centra štátu*“. To bolo vypracované, schválené a publikované na jeseň 2014 a definovalo procesný rámec pre migrácie IS do VC.

Úloha B3 zaväzuje ministerstvo financií každý rok k 30.9. až do roku 2020 publikovať a aktualizovať katalóg služieb poskytovaných dátovými centrami štátu. Následne úloha B6 ukladá ministrom, predsedom ostatných ústredných orgánov štátnej správy, správcom ďalších kapitol štátneho rozpočtu predkladať každý rok k 31.12. až do roku 2020 podpredsedovi vlády a ministrovi financií odpočet plnenia harmonogramu migrácie informačno-komunikačných technológií príslušného rezortu za kalendárny rok a aktualizovaný harmonogram migrácie informačno-komunikačných technológií príslušného rezortu do

dátového centra štátu na ďalšie obdobie. Inakšie povedané, v logike uznesenia majú povinné osoby po publikovaní aktualizovanej verzie Katalógu služieb poskytovaných VC aktualizovať svoje analýzy a plány migrácií.

V zmysle vyššie uvedeného, stručne povedané, je cieľom uznesenia je centralizácia dátových centier v štátnej správe. Postupne sa neskôr vyšpecifikovalo, že všetky IKT okrem IKT zabezpečenia obrany Slovenskej republiky, bezpečnosti Slovenskej republiky, ochrany utajovaných skutočností a citlivých informácií, budú umiestnené v dvoch dátových centrách štátu. Tieto poskytujú aj priestor dátového centra, jeho kapacity sú však limitované. Primárne poskytujú cloudové služby. Tým sa celá centralizácia dátových centier posúva do roviny migrácie IS do VC.

Metodické usmernenie obsahuje 39 súborov potrebných na zmapovanie celého všetkých fáz migrácie dátových centier. Jasne nepomenúva, a nemá ani takú ambíciu, registre, resp. nástroj, v ktorom by mali byť získavané informácie evidované a udržiavané. Spustením produkčnej prevádzky MetaIS a vydaním Metodického pokynu č. MF/011247/2016-1721 z 4.3.2016 na aktualizáciu obsahu Centrálneho metainformačného systému verejnej správy (ďalej aj ako „MetaIS“) povinnými osobami je takýto nástroj k dispozícii. Výstupy úlohy B3 realizované v rokoch 2014 a 2015 povinnými osobami, ktoré získalo Ministerstvo financií SR, boli transformované do MetaIS údajov. V tomto momente sa 17 súborov požadovaných v Metodickom usmernení kryje s informáciami udržiavanými v MetaIS. Odporúčame aktualizovať Metodické usmernenie o migrácií tak, aby technické informácie boli zhromažďované a aktualizované v MetaIS a procesné a finančné údaje týkajúce sa samotnej migrácie konkrétneho IS boli vo forme aktualizovaných súčasných súborov.

## 11.2 Aktuálny stav

Od publikovania prvého Katalógu služieb 30.9.2014 mali byť zrealizované a odovzdané 2 komplexné analýzy migrácií IS v štátnej správe. Ako však vidno z nasledovnej tabuľky, odovzdané podklady však tomu nenasvedčujú:

	V roku 2014	V roku 2015
Počet organizácií ktoré odovzdalo podklady	34	12 <sup>12</sup>
Počet analyzovaných IS	1541	1566

Celkovo sa dá povedať, že kvalita a rozsah odovzdaných podkladov zaostáva za očakávaniami. Príkladom z tohto roku je rezort, ktorý v roku 2014 do analýz zahrnul 97 IS, o rok neskôr 108 IS, ale až hĺbkový audit realizovaný v tomto roku reálne zmapoval stav a identifikoval a analyzoval 257 IS.

Tento stav má niekoľko príčin:

- Nevynútiteľnosť vykonania – za nesplnenie úlohy nie je definovaný postih. Pomocným riešením tohto problému bolo nedovolenie čerpania prostriedkov na nové projekty bez zavedenia súčasného stavu do MetaIS. Toto riešenie však nemôže zabezpečiť analýzy nad IS, ktoré sa zásadnejšie nemenia.
- Nekontrolovateľnosť údajov – nakoľko doteraz neexistoval register IS, MetaIS v jeho súčasnej podobe je v prevádzke od 4.3.2016, nie je možné odovzdané údaje overiť.
- Podcenenie prácnosti – dobré zmapovanie rezortu, vyplnenie všetkých potrebných dokumentov a následná aktualizácia informácií v MetaIS je práca v rozsahu stoviek človeko-dní. A na túto prácnosť je bol vyhradený reálny čas 2 mesiacov (od termínu publikovania katalógu po termín odovzdanie analýz).
- Nekvalitnosť vypracovania prvej analýzy – s ohľadom na podcenenie prácnosti, od publikovania prvého Katalógu služieb (30.9.2014) do odovzdania prvej komplexnej analýzy za

<sup>12</sup> Zaslané aktualizované údaje

rezort (31.12.2014) bol veľmi krátky čas na naozajstné vypracovanie hĺbkovej analýzy. Takto vytvorený rozpor s realitou sa dedí a nezmenšuje.

- Nepripravenosť dostatočnej priority, dôležitosti – neuvedenie si prácnosti, komplexnosti informácií a aj projektového rozsahu, málokto si uvedomil, že vypracovanie dôkladnej prvej analýzy musí byť profesionálne projektovo riadené, za účasti špecialistov zo strany rezortu ale aj dodávateľov jednotlivých IS, resp. servisných organizácií. S dostatočnou finančnou alokáciou v rozpočte príslušnej organizácie.
- Nedostatočnosť zdrojov na vypracovanie dôkladnej analýzy – i keď na prvotnú analýzu v roku 2014 bolo málo času, teoreticky bolo možné ju dorobiť v roku 2015. V tomto roku však finišovala väčšina projektov z programového obdobia 2010-2015, ktorá blokovala špecialistov potrebných na analýzu migrácií.
- Nesúlad medzi potrebami zadávateľa a organizácie – zadávateľ, Ministerstvo financií SR rozmýšľa v úrovni povinnej osoby, resp. organizácie, a tak aj pripravilo podporné dokumenty. Naopak, organizácia rozmýšľa na úrovni IS a podporné dokumenty takúto granularitu nie celkom reflektujú.

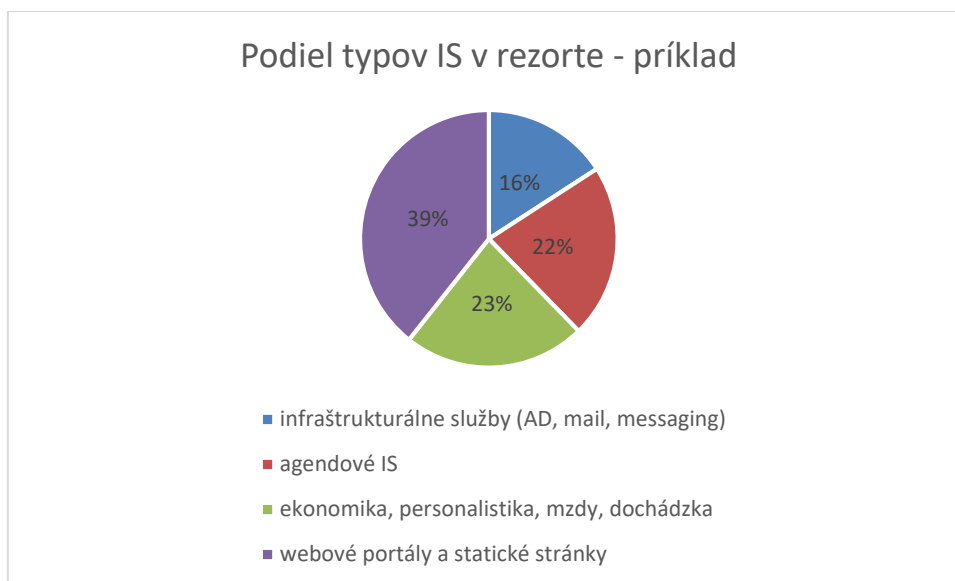
Za 2 roky od publikovania prvej verzie Katalógu služieb tvorili majoritu IS umiestňovaných do VC nové projekty. Len minimum bolo reálne migrovaných existujúcich IS. Je predpoklad, že tento trend sa začne otáčať v prospech migrácií existujúcich IS. Treba si však veľmi dobre uvedomiť, koľko paralelných migrácií IS je schopná organizácia popri nových rozvojových projektoch v jednom roku realizovať. Z praxe sa dá odvodzovať, že v najbližších 4 rokoch, organizácia stihne v prvom roku migrovať 40-50% IS, jednoduchších na ktorých si overí fungovanie VC. V nasledujúcich 2 rokoch potom migrovať 30-40% zložitejších IS a v poslednom roku musí migrovať zvyšok. Pokiaľ kvôli nedostatku záujmu, zdrojov, prostriedkov alebo informácií mešká rok, môže sa dostať do časového sklzu plnenia úlohy, ktorého náprava odčerpá zdroje potrebné v rokoch 2019/20 na finišovanie projektov z dôvodu ukončovania rozpočtovacieho obdobia 2016-20. Je nutné začať čo najskôr.

Materiál „*Návrh centralizácie a rozvoja dátových centier v štátnej správe*“ obsahoval aj kalkuláciu výhodnosti takejto centralizácie. Z pohľadu investícií štátu do IKT vyšlo centralizované riešenie najvýhodnejšie. Akákoľvek kalkulácia výhodnosti migrácie jedného alebo viacerých IS do VC, voči zachovaniu alebo rozvoju existujúceho stavu lokálnej prevádzky tohto, resp. týchto IS preto nie je relevantná a nemá zmysel ju vypracovávať. Energiu je potrebné venovať migráciám IS do VC.

Na migráciu IS do VC je možné nazerať z rôznych strán a zvažovať rôzne kritériá a postupy. Všetky tieto prístupy budú odvodené od typu a rozsahu IS. Našťastie je možné si pomôcť výstupom z analýzy 180 IS zahrnutých do migrácie do VC. Zistené IS bolo možné si klasifikovať do 4 skupín:

- agendové informačné systémy – vyznačovali sa najkomplexnejšou architektúrou,
- webové a portálové stránky – ktorých väčšina vznikla v rámci projektov,
- erp aplikácie – ktoré v nejakej obmene obsahujú účtovníctvo, personalistiku, mzdy, dochádzku, prípadne sklad a ktoré až na 1-2 výnimky boli postavené na komerčných softvéroch s jednoduchou architektúrou,
- podporné aplikácie – typu email, AD, Lync a pod.

Pomerové zastúpenie jednotlivých typov je na nasledovnom obrázku:



Obrázok 22 Podiel typov IS v rezorte - príklad

Je z neho jasné, že IS s komplexnejšou architektúrou, ktorých migrácia môže byť komplikovaná je menej ako 22% zo všetkých IS.

Vo Fáze Plánovania na úrovni organizácie je nutné vytvoriť si prioritizáciu migrácie jednotlivých IS. Na jej vytvorenie stačí posúdenie niekoľko základných kritérií:

1. pre ktoré IS je plánovaná ich aplikačná aktualizácia,
2. ktoré IS nespĺňajú v súčasnosti výkonnostné alebo štandardizačné požiadavky,
3. ktoré IS majú komponenty vhodné na migráciu do PaaS služby.

IS, ktoré sa kvalifikujú na kritérium 1 musia byť migrované v rámci ich aplikačnej aktualizácie. IS, ktoré sa kvalifikujú na kritérium 2 musia byť migrované na začiatku, resp. čo najskôr. Všetky IS, ktoré sa kvalifikuje na kritérium 3, musia ísť až po sprístupnení PaaS služieb. Popísané a od nich odvodené kritéria majú samozrejme v praktickom svete viacero ďalších aspektov vyhodnotenia. Sú uvedené samostatne aj s podrobnejším popisom v ďalšom texte.

### 11.2.1 Migrácia IS s plánovanou aplikačnou aktualizáciou

IS, pre ktoré je plánovaná obnova sa odporúča migrovať v rámci obnovy. Tzn. v rámci obnovy IS je potrebné si dohodnúť alebo zazmluvniť, že nová verzia IS už bude nasadená do VC. Najlepšie je už v rámci projektu aplikačnej aktualizácie použiť testovacie prostredia z VC.

Najkomplexnejšiu architektúru majú agendové systémy. Zvyknú však, či už z legislatívnych alebo funkčných zmien, mať aplikačnú obnovu minimálne každých 3-4 roky. Z dôvodu konca podpory operačných systémov to býva najneskôr do 6-7 rokov. Väčšina zo súčasných agendových systémov išla do produkčnej prevádzky najneskôr koncom roka 2015, často krát po 1-2 rokoch realizácie projektov. Štandardne sa verzie operačných systémov používajú také, aké sú dostupné pri rozbehu projektu. Je preto možné odvodzovať a predpokladať, že na väčšine agendových IS bude do roku 2020 naplánovaná aplikačná aktualizácia a tým aj migrácia do VC.

Doteraz bola zaznamenaná jediná výnimka, a to v prípade, že aplikácia je umiestnená v iného zazmluvneného partnera, za toto umiestnenie sa platí, a aplikačná aktualizácia je naplánovaná až po dlhšom období. Odporúčame, vždy keď je IS umiestnený v externom komerčnom „hostingovom“ centre vykonať TCO analýzu výhodnosti samostatnej migrácie.

#### 11.2.1.1 SWOT analýza

##### 11.2.1.1.1 Silné stránky

- Ekonomicky výhodnejšie je v rámci aplikačnej aktualizácie naplánovať umiestnenie jej novej verzie priamo do VC, než robiť samostatnú migráciu.
- Pri agendových systémoch odporúčané riešenie.

##### 11.2.1.1.2 Slabé stránky

- V niektorých prípadoch, ak je IS hostované u externej firmy a aplikačná aktualizácia je plánovaná až o niekoľko rokov, nemusí byť takéto riešenie ekonomicky výhodné.

##### 11.2.1.1.3 Príležitosti

- V rámci spojenia s aplikačnou aktualizáciou je väčšia šanca zmeniť deployment model IS tak, aby lepšie pasoval na požiadavky VC. V prípade nového deploymentu je možné dodržať členenie IS do 4 vrstiev tak, ako to IaaS služba VC požaduje.

##### 11.2.1.1.4 Hrozby

- Prípadná zmena deployment modelu pri nasadení novej verzie aplikácie do VC môže mať dopad na dĺžku termínu nasadenia IS. V prípade viacvrstvovej architektúry podporovanej a vynucovanej zo strany VC je prácnejšie nasadenie IS a nadefinovanie korektných, minimálne nutných prestupov medzi vrstvami. Takáto architektúra je však v súlade s Výnosom o štandardoch a preto sa jej musí IS prispôbiť.

#### 11.2.2 IS aktuálne nespĺňajúce výnos o štandardoch

Nesúlad medzi Výnos č. 55/2014 Z. z Ministerstva financií Slovenskej republiky o štandardoch pre informačné systémy verejnej správy a realitou býva napr. v zabezpečení pravidelného vytvárania a odkladania archivačnej kópie IS do externej lokality.

#### 11.2.2.1 SWOT analýza

##### 11.2.2.1.1 Silné stránky

- Splnenie litery zákona.

##### 11.2.2.1.2 Slabé stránky

- Môže byť ekonomicky neefektívne. Tradične v prostredí jedného lokálneho dátového centra, kde by bolo možné pri malých investíciách dosiahnuť naplnenie štandardov.

##### 11.2.2.1.3 Príležitosti

- V prípade nového deploymentu je možné dodržať členenie IS do 4 vrstiev tak, ako to IaaS služba VC požaduje.

##### 11.2.2.1.4 Hrozby

- Nie sú.

#### 11.2.3 IS prevádzkované na IKT za hranicou životnosti

Súhrnný popis

### 11.2.3.1 SWOT analýza

#### 11.2.3.1.1 Silné stránky

- VC je v tomto ideálny prípad nakoľko vytvorenie a sprístupnenie prostredia je počítané v dňoch. Pri výkonnostných problémoch alebo problémoch so spoľahlivosťou zastaraného IKT je možné, v rámci možností podporných aplikačných tímov organizácie, presunúť IS do VC.

#### 11.2.3.1.2 Slabé stránky

- Riziko neúspechu migrácie do VC je z dôvodov nevyhnutného zabezpečenia konektivity na VC a prestupmi medzi vrstvami vyššie než pri jednoduchej hardvérovej obnove serverov, kde sa často krát dajú použiť pôvodné disky a migrácia je bezriziková.

#### 11.2.3.1.3 Príležitosti

- V prípade nového deploymentu je možné dodržať členenie IS do 4 vrstiev tak, ako to IaaS služba VC požaduje.

#### 11.2.3.1.4 Hrozby

- Nie sú.

### 11.2.4 IS kompletne hostované u externej firmy

IS, ktorú sú hostované u externej firmy majú jednu záludnosť. Vo väčšine prípadov sú spojené so službami, ktoré VC v dobe písania tohto dokumentu neposkytuje. Najbežnejším príkladom je prevádzka webových stránok v hostingových centrách, ktorú reálne môžeme pomenovať ako Webserver as a Service. Organizácia sa nestará o prevádzku operačného systému a ani webového servera, dokonca ani o redakčný systém. Stará sa len o napĺňanie obsahu a jeho vizualizáciu.

Kým nebude vo VC poskytovaný PaaS Webserver as a Service je nutné spolu s migráciou takýchto IS zabezpečiť aj štandardné činnosti poskytované hostingovým partnerom. Nakoľko ide z našej skúsenosti o nie ojedinelý prípad, odporúčame zastrešiť tieto servisné práce príslušným ministerstvom.

### 11.2.4.1 SWOT analýza

#### 11.2.4.1.1 Silné stránky

- Ušetrenie financií za hosting.

#### 11.2.4.1.2 Slabé stránky

- Náklady na prevádzku operačných systémov a webových serverov môžu byť niekedy vyššie než ušetrené prostriedky.

#### 11.2.4.1.3 Príležitosti

- V prípade nového deploymentu je možné dodržať členenie IS do 4 vrstiev tak, ako to IaaS služba VC požaduje.

#### 11.2.4.1.4 Hrozby

- Zníženie plnenia SLA pri nedodržaní zazmluvnenia servisu operačného systému a webového servera, prípadne iných komponentov.

### 11.2.5 Infraštruktúrne služby

Medzi infraštruktúrne služby zaradíme napr. emailový systém, kolaboračný systém, Active Directory, súborový server a pod. Sú v tomto texte uvedené samostatne nakoľko majú jedno nie nepodstatné špecifikum. Ich migrácia je postupná a počas migrácií sú prevádzkované paralelne v pôvodnom DC aj vo VC.

Dôvodom je, že vo väčších organizáciách sú agendové systémy úzko naviazané na email, AD a súborový server. Pri postupnej migrácii, aká bude vo väčšine organizácií musí dôjsť v úvode migrácií



k rozšíreniu týchto entít do VC, počas migrácií musia bežať paralelne a integrovane a až po migrácií je možné niektoré z pôvodného DC zrušiť. V niektorých prípadoch, napr. pri väčšom počte pracovných miest užívateľov v okolí DC bude pravdepodobne AD a súborový server.

### 11.2.5.1 SWOT analýza

#### 11.2.5.1.1 Silné stránky

- Migrácia neovplyvní užívateľský komfort.

#### 11.2.5.1.2 Slabé stránky

- Počas migrácií, môže trvať formálne až 4 roky, bude potrebné administrovať viac komponentov.

#### 11.2.5.1.3 Príležitosti

- Nie sú.

#### 11.2.5.1.4 Hrozby

- Nie sú.

## 11.2.6 IS samospráv

V roku 2014 bol na zasadnutí vlády SR schválený materiál „Návrh centralizácie a rozvoja dátových centier v štátnej správe“ spolu s prijatým Uznesením č. 247. Úloha B5 uložila ministrom, predsedom ostatných ústredných orgánov štátnej správy a správcom ďalších kapitol štátneho rozpočtu zabezpečiť do 31. decembra 2020 migráciu informačno-komunikačných technológií príslušného rezortu do dátového centra štátu. Táto úloha sa však nevzťahuje na subjekty samospráv, avšak špecificky najmä pre túto oblasť sú k dispozícii pre vybrané agendy na platforme DCOM aplikácie poskytované formou SaaS.

Všeobecné východiská a prínosy (zastarávajúci HW, snaha o ušetrenie prostriedkov na prevádzke, zabezpečenie dostatočnej kvality a bezpečnosti poskytovaných služieb) sú však veľmi podobné ako pri organizáciách štátnej správy. Je teda možné konštatovať, že aj pre samosprávu existuje záujem o zvyšovanie efektivity pre prevádzku ISVS s využívaním vybraných služieb vládneho cloudu. Cieľom tejto kategórie migrácií je zvýšenie využívania už existujúcich SaaS bežiacich vo vládnom cloude alebo jeho častiach

## 11.3 Spôsob financovania migrácií

V čase písania tohto dokumentu boli identifikované nasledovné spôsoby financovania migrácií IS do VC:

1. Migrácia v rámci aplikačnej aktualizácie – tento spôsob je závislý od spôsobu financovania aplikačnej aktualizácie.
2. Pri presune IS od externého poskytovateľa DC do VC a ušetrení finančných prostriedkov za toto poskytovanie je financovanie z rozpočtu organizácie v rámci optimalizácie nákladov.
3. Financovanie z rozpočtu organizácie, v prípade že je nutné riešiť haváriu na súčasnom IKT.
4. Financovanie z rozpočtu ministerstva, či už priamo alebo alokáciou prostriedkov na organizáciu.
5. Financovanie z EŠIF

Keďže najnáročnejšie migrácie bolo odporúčané realizovať v rámci aplikačnej aktualizácie, a migrácie sú v čase písania tohto dokumentu rozložené do 4 rokov, dopad na financovanie zo štátneho rozpočtu ministerstva / organizácie by mohol byť v medziach bežných výdavkov.

## 12 Bezpečnosť

### 12.1 Ciele

Ambíciou tejto časti dokumentu nie je navrhnuť bezpečnostnú politiku ani technický návrh bezpečnosti vládneho cloudu. Účelom tejto kapitoly je adresovať bezpečnosť vládneho cloudu na strategickej úrovni.

Vládny cloud sa buduje postupne po vrstvách (vertikálne): IaaS, PaaS a SaaS. Pre každú vrstvu je potrebné adresovať bezpečnosť individuálne. Každá vrstva by mala byť navrhnutá tak, aby škálovala a bolo možné zvyšovať kapacitu poskytovaných služieb (horizontálne). Pri plánovaní bezpečnosti je nutné zvážiť toto postupné rozširovanie vládneho cloudu vertikálne aj horizontálne a zvážiť aj následné rozširovanie portfólia poskytovaných služieb a použitých technológií.

Vychádzajúc z aktuálne schválenej NKIVS je nutné zvážiť aj rozšírenie vládneho cloudu o služby verejného cloudu čím sa z vládneho cloudu stane hybridný cloud.

Bezpečnosť cloudu by mala adresovať minimálne nasledovné ciele:

1. Zaisťovať poskytovanie cloudových služieb v dohodnutom rozsahu a kvalite.
2. Zaisťovať bezpečnosť spracúvaných dát a poskytovaných služieb.
3. Dosiahnuť a udržiavať súlad s aplikovateľnou legislatívou.

### 12.2 Štandardy

Na medzinárodnej úrovni sa špecificky problematikou bezpečnosti cloudu zaoberá ISO/IEC 27017:2015, ktorý vychádza zo všeobecnejších štandardov ISO/IEC 27001 a 27002, ktoré adresujú otázky riadenia IT bezpečnosti resp. ich implementáciou. Pri písaní tejto časti dokumentu sa vychádzalo práve z tohto štandardu. V budúcnosti, pri podrobnejšom adresovaní požiadaviek na bezpečnosť cloudu a ich implementácii je vhodné uplatniť ďalšie špecializované rámce (frameworky) v závislosti od príslušnej oblasti bezpečnosti. SABSA (Sherwood Applied Business Security Architecture) obsahuje viacero komponentov, ktoré môžu byť použité separátne alebo spoločne (napr. rámec pre riadenie rizík a príležitostí, rámec bezpečnostných domén a ďalšie). Jericho forum (časť Open Group Security Forum) disponuje tzv. Cloud Cube modelom, ktorý stanovuje kľúčové princípy EA (enterprise architecture) priamo pre bezpečnosť cloudu. Dôležitým základným rámcom pre cloudové bezpečnostné opatrenia je CSA CCM (Cloud Security Alliance Cloud Control Matrix). CCM poskytuje syntézu a krížové mapovanie viacerých bezpečnostných štandardov a rámcov (napr. ISO 27001/27002/27017/27018, COBIT, PCI DSS). CCM sa aktualizuje podľa aktuálnych poznatkov, skúseností a trendov. Pre účely výberu a implementácie bezpečnostných opatrení špecificky v kontexte cloudu a jeho služieb je preto kľúčovým metodickým východiskom.

### 12.3 Legislatíva

Pri tvorbe tejto časti dokumentu sa vychádzalo aj z legislatívnych usmernení výnosu č. 55/2014 Z. z. ministerstva financií Slovenskej republiky o štandardoch pre informačné systémy verejnej správy (ďalej len výnos MF SR) v kontexte ďalšej platnej legislatívy, ktorý nadobudol účinnosť 1.7.2016. Výnos sa v paragrafe č.55 venuje problematike správy cloud computingu v rozsahu:

- riadenie informačnej bezpečnosti podľa § 29,
- personálna bezpečnosť podľa § 30,
- manažment rizík pre oblasť informačnej bezpečnosti podľa § 31,
- kontrolný mechanizmus riadenia informačnej bezpečnosti podľa § 32,
- ochrana proti škodlivému kódu podľa § 33,
- sieťová bezpečnosť podľa § 34,
- fyzická bezpečnosť a bezpečnosť prostredia podľa § 35,
- aktualizácia softvéru podľa § 36,
- monitorovanie a manažment bezpečnostných incidentov podľa § 36,
- periodické hodnotenie zraniteľnosti podľa § 38,
- zálohovanie podľa § 39,



- fyzické ukladanie záloh podľa § 40,
- riadenie prístupu podľa § 41,

Súčasťou štandardu pre správu cloud computingu v správe povinnej osoby je aj bezpečnosť zdieľaného prostredia, pričom sa

- pri výpadku cloudových služieb v súlade s podmienkami a garantovanými parametrami dostupnosti zabezpečuje migrácia do záložného prostredia podľa vopred určeného scenára tak, aby dodávka cloudových služieb nebola dlhodobo ohrozená,
- umožňuje oddeliť údaje jednotlivých odberateľov cloudových služieb, pričom spôsob oddelenia je obsiahnutý v dohode o poskytovanej úrovni cloudových služieb,
- virtuálne komponenty oddeľujú do bezpečnostných zón podľa typu použitia s cieľom zníženia rizika neautorizovaného prístupu alebo zmien.

Súčasťou štandardu pre správu cloud computingu v správe povinnej osoby je aj správa cloud computingu zabezpečovaná tak, aby:

- boli v dohode o poskytovanej úrovni cloudových služieb obsiahnuté aj podmienky a garantované parametre dostupnosti cloudových služieb a spracúvaných údajov,
- bolo odberateľovi cloudových služieb na základe žiadosti umožnené úplné skopírovanie jeho údajov na ďalšie použitie, pričom podmienky, lehoty a výstupné formáty údajov sú obsahom dohody o poskytovanej úrovni cloudových služieb, pričom lehota na skopírovanie údajov sa v dohode nedohodne na dlhšie ako tri mesiace; takými údajmi sa rozumejú údaje, ktoré do cloud computingu vložil alebo si nastavil odberateľ cloudových služieb na základe dohody o poskytovanej úrovni cloudových služieb,
- bolo odberateľovi cloudových služieb umožnené úplné vymazanie jeho údajov, a to vrátane všetkých kópií a záloh v cloud computingu, pričom pri ukončení zmluvného vzťahu s odberateľom cloudových služieb sa takéto vymazanie zabezpečuje bezodkladne bez nutnosti osobitnej žiadosti odberateľa cloudových služieb; takéto vymazanie sa netýka údajov, pri ktorých to podmienky podľa osobitného predpisu neumožňujú alebo pre ktoré je to v príslušnej dohode o poskytovanej úrovni cloudových služieb dohodnuté inak, pričom lehota pre úplné vymazanie údajov sa v dohode o poskytovanej úrovni cloudových služieb nedohodne na dlhšie ako tri mesiace, a
- bolo súčasťou dohody o poskytovanej úrovni cloudových služieb vyhlásenie poskytovateľa cloudových služieb o súlade s príslušnými štandardmi podľa tohto výnosu, a to v rozpise podľa jednotlivých štandardov.

Za účelom zosúladenia stratégie rozvoja vládneho cloudu a aktuálneho znenia výnosu č. 55/2014 Z. z. je potrebné uvedený výnos doplniť o nasledovnú požiadavku:

- odberateľ cloudových služieb registráciou do prostredia vládneho cloudu záväzne akceptuje dodržiavanie bezpečnostných politík a pravidiel vládneho cloudu.

## 12.4 Cloud špecifiká

Vyššie spomenutý výnos MF SR definuje modely poskytovania cloudových služieb v paragrafe 54 nasledovne:

*Štandardom modelov poskytovania cloudových služieb je rozdelenie modelov poskytovania cloudových služieb najmä na model*

*a) infraštruktúra ako služba, označovaný aj ako IaaS, pri ktorom cloudovú službu predstavuje poskytovanie virtualizovanej infraštruktúry ako serverov, úložísk údajov a sieťovej infraštruktúry,*

*b) platforma ako služba, označovaný aj ako PaaS, pri ktorom cloudovú službu predstavuje poskytovanie hardvérovej a softvérovej platformy, potrebnej na vytvorenie a správu aplikácií, vrátane umožnenia ich navrhovania, vývoja, testovania a nasadzovania do produkčnej prevádzky, pričom tieto aplikácie ostávajú v správe odberateľa cloudových služieb,*

*c) softvér ako služba, označovaný aj ako SaaS, pri ktorom cloudovú službu predstavuje poskytovanie softvéru, vrátane aplikácií.*

*Štandardom pre typy cloud computingu je rozdelenie typov cloud computingu najmä na*

a) *privátny cloud, pri ktorom je cloud computing alokovaný výhradne pre potreby jednej organizácie, pričom poskytovateľom cloudových služieb, prevádzkovateľom cloudových služieb ani sprostredkovateľom cloudových služieb nemusí byť táto organizácia,*

b) *komunitný cloud, pri ktorom cloud computing využíva niekoľko organizácií, ktoré tvoria jednu komunitu, zdieľajúcu podobné záujmy, napríklad ciele, požiadavky na bezpečnosť, politiku a dodržiavanie záujmov, pričom poskytovateľom cloudových služieb, prevádzkovateľom cloudových služieb ani sprostredkovateľom cloudových služieb nemusí byť ani jedna z týchto organizácií,*

c) *verejný cloud, pri ktorom je cloud computing zdieľaný ľubovoľnými odberateľmi cloudových služieb, pričom ani jeden z nich nemusí byť poskytovateľom cloudových služieb alebo prevádzkovateľom cloudových služieb,*

d) *hybridný cloud, ktorý predstavuje kompozitné využitie cloudových služieb dvoch alebo viacerých typov cloud computingu, pričom využívané cloudové služby sú naďalej podporované jednotlivými infraštruktúrnymi prostriedkami daných typov cloud computingu, ale ako také sú vzájomne spojené štandardizovanými alebo proprietárnymi technológiami, ktoré umožňujú prenositeľnosť údajov a aplikácií.*

### 12.4.1 Zúčastnené strany a ich vzťahy

Z pohľadu prevádzky cloudových služieb je možné definovať tri hlavné strany:

1. poskytovateľ cloudových služieb - sprístupňuje cloudové služby odberateľom cloudovej služby. Táto rola sa zameriava na činnosti cloud computingu potrebné na poskytovanie cloudovej služby a činnosti cloud computingu potrebné na zabezpečenie plnenia voči odberateľovi cloudovej služby.
2. prevádzkovateľ cloudových služieb - zabezpečuje všetky činnosti potrebné na nasadenie cloudových služieb odberateľom cloudových služieb, riadenie prevádzky cloudových služieb, monitorovacie a administratívne služby.
3. odberateľ cloudových služieb - povinná osoba ktorá je v obchodnom vzťahu s Poskytovateľom cloudových služieb pre účely využívania cloudových služieb.

Role a zodpovednosti pri návrhu, budovaní a prevádzke cloudu definuje kapitola 4 tohto dokumentu.

### 12.4.2 Riadenie rizík

Vyššie menovaný výnos MF SR definuje štandard pre manažment rizík pre oblasť informačnej bezpečnosti v paragrafe 31 nasledovne:

a) *implementácia systému riadenia a monitorovania rizík v súvislosti s informačnými systémami verejnej správy, a to najmä podľa relevantných technických noriem a pravidelné zbieranie relevantných údajov súvisiacich s rizikami,*

b) *používanie systému riadenia a monitorovania rizík pri všetkých procesoch riadenia informačnej bezpečnosti,*

c) *identifikácia, analýza a hodnotenie rizík spojených s využívaním aktív a informačných systémov verejnej správy mimo priestorov povinnej osoby a zavedenie primeraných postupov a opatrení na redukciiu týchto rizík,*

d) *analyzovanie procesov povinnej osoby, ktoré sú podstatné pre plnenie činnosti povinnej osoby z hľadiska ich závislosti na informačných systémoch verejnej správy a určenie procesov, ktoré nemôžu prebiehať v prípade výpadku alebo obmedzenia funkčnosti príslušných informačných systémov verejnej správy; tieto procesy sú kritickými procesmi,*

e) *analyzovanie rizík, vyplývajúcich z hrozieb pre informačné systémy verejnej správy, od ktorých závisia kritické procesy; tieto informačné systémy sú kritickými informačnými systémami verejnej správy,*

f) *vypracovanie plánov na obnovu činnosti nefunkčných, poškodených alebo zničených kritických informačných systémov verejnej správy.*

Na základe vyššie spomenutého je nutné vybudovať a prevádzkovať systém na riadenie a monitorovanie rizík (alebo využiť existujúci) a zapracovať vyššie spomenuté požiadavky do prevádzkovej dokumentácie a bezpečnostnej politiky.

## 12.5 Bezpečnostná politika

Požiadavky na bezpečnostnú politiku definuje vyššie spomenutý výnos v paragrafe 29 v nasledujúcom rozsahu:

- *určenie bezpečnostných cieľov povinnej osoby z hľadiska informačnej bezpečnosti,*
- *určenie spôsobov vyhodnocovania bezpečnostných cieľov, kritérií vyhodnocovania ich dosahovania, spôsobov priebežného hodnotenia ich adekvátnosti a spôsobov kontroly postupov využívaných na ich dosahovanie,*
- *určenie úlohy vedenia povinnej osoby pri zaistovaní informačnej bezpečnosti a uvedenie vyhlásenia vedenia povinnej osoby o podpore bezpečnostnej politiky povinnej osoby,*
- *určenie všeobecných a špecifických zodpovedností a povinností v oblasti informačnej bezpečnosti a stanovenie potrebných pozícií pre manažment informačnej bezpečnosti,*
- *určenie povinnosti pre zaistenie nenarušenia informačnej bezpečnosti povinnej osoby,*
- *zhodnotenie súladu bezpečnostnej politiky povinnej osoby so všeobecne záväznými právnymi predpismi, vnútornými predpismi povinnej osoby a jej zmluvnými záväzkami,*
- *určenie požiadaviek na informačné systémy verejnej správy, vyplývajúce zo všeobecne záväzných právnych predpisov, vnútorných predpisov povinnej osoby a jej zmluvných záväzkov a určenie spôsobu vedenia a aktualizácie dokumentácie o informačných systémoch verejnej správy,*
- *určenie rozsahu a úrovne ochrany všetkých informačných systémov verejnej správy vrátane hodnotenia slabých miest a ohrození,*
- *určenie rámca pre manažment rizík u povinnej osoby v súvislosti s aktívami, od ktorých závisí činnosť informačných systémov verejnej správy, alebo ktoré závisia od činnosti informačných systémov verejnej správy; rámec určí, najmä ktoré aktíva sú pre povinnú osobu kritické, čo ich ohrozuje a zásady ich ochrany,*
- *určenie rozsahu a periodicity auditu informačnej bezpečnosti u povinnej osoby a zároveň určenie udalostí v informačných systémoch verejnej správy, o ktorých sa vytvára záznam auditu,*
- *určenie operačných smerníc pre zálohovanie a určenie ktoré skupiny údajov, v akom rozsahu, akým spôsobom a s akou periodicitou sa zálohujú v prevádzkovej zálohe a archivačnej zálohe,*
- *určenie periodicity monitorovania bezpečnosti a aktualizácie softvéru,*
- *určenie dokumentov, ktoré povinná osoba na zaistenie informačnej bezpečnosti vypracuje a uvedie ich zoznam,*
- *určenie postupu pri revízii bezpečnostnej politiky povinnej osoby vrátane periodicity pravidelných a dôvodov mimoriadnych revízií bezpečnostnej politiky povinnej osoby,*

Účelom tohto dokumentu nie je definovať bezpečnostnú politiku vládneho cloudu. Táto by mala byť spracovaná samostatne alebo ako súčasť bezpečnostného projektu v čo najkratšom čase tak, aby boli naplnené vyššie citované požiadavky.

## 12.6 Organizácia informačnej bezpečnosti

Interná organizačná štruktúra, dodávateľské aktivity vo vzťahu k informačnej bezpečnosti, definovanie rolí a zodpovedností vo vzťahu k informačnej bezpečnosti by mali byť predmetom bezpečnostnej politiky, ktorá by mala byť spracovaná ako súčasť bezpečnostného projektu pre vládny cloud buď ako celok, ktorý sa pravidelne aktualizuje alebo pre každú vrstvu IaaS, PaaS a SaaS samostatne. Pri jej tvorbe je nutné brať do úvahy existujúcu organizačnú štruktúru poskytovateľov a prevádzkovateľov vládneho cloudu.

Očakáva sa definícia rolí na strane poskytovateľov cloudových služieb ako aj na strane prevádzkovateľov cloudových služieb. Pre zabezpečenie objektivity pri posudzovaní úrovne a kvality implementácie bezpečnostných opatrení, sa neodporúča, aby audit bezpečnosti vykonávali osoby (audítori cloudu) zodpovedné za implementáciu a dodržovanie bezpečnostnej politiky.

## 12.7 Personálna bezpečnosť

Požiadavku na personálnu bezpečnosť podrobne špecifikuje vyššie spomenutý výnos MF SR v paragrafe 31 v nasledovnom rozsahu:

- a) zabezpečenie, aby boli všetci zamestnanci povinnej osoby a osoby, ktoré vykonávajú činnosti pre povinnú osobu vyplývajúce zo zmluvných záväzkov (ďalej len „tretia strana“) poučení o schválenej bezpečnostnej politike povinnej osoby a o povinnostiach z nej vyplývajúcich,
- b) zabezpečenie, aby boli zamestnanci povinnej osoby a tretia strana poučení o svojich právach a povinnostiach predtým, ako získajú prístup k informačnému systému verejnej správy; v prípade rozdielných práv a povinností pre rôzne informačné systémy verejnej správy sa poučenie zopakuje a jeho obsah sa primerane upraví,
- c) zabezpečenie, aby povinnosti vyplývajúce z bezpečnostnej politiky povinnej osoby a z pracovného zaradenia zamestnanca boli uvedené v jeho pracovnej zmluve alebo inom dokumente týkajúcom sa jeho právneho vzťahu s povinnou osobou,
- d) vypracovanie postupu pre disciplinárne konanie vo vzťahu k zamestnancovi alebo vo vzťahu k tretej strane, ktorí porušia bezpečnostnú politiku povinnej osoby alebo niektorý zo súvisiacich predpisov,
- e) zabezpečenie povinnosti zamestnancov oznamovať bezpečnostné incidenty v súlade s postupmi podľa § 37,
- f) vypracovanie postupu pri ukončení pracovného pomeru vlastného zamestnanca a pri ukončení spolupráce s externým pracovníkom alebo tretou stranou, ktorým sa zabezpečí
1. prípadné obmedzenie vo vzťahu k bývalému zamestnancovi, ktorým je najmä mlčanlivosť a obmedzenie na výkon činností po istú dobu po ukončení zamestnania,
  2. navrátenie pridelených zariadení, ktorými sú najmä počítače, pamäťové médiá, čipové karty a navrátenie informačných aktív, ktorými sú najmä programy, dokumenty a údaje,
  3. odstránenie informácií povinnej osoby zo zariadení pridelených zamestnancovi, ktorými sú najmä počítače, notebooky, pamäťové médiá a ďalšie mobilné elektronické zariadenia,
  4. zrušenie prístupových práv v informačných systémoch verejnej správy,
  5. odovzdanie výsledkov práce v súvislosti s informačnými systémami verejnej správy, ktorými sú najmä programy vrátane dokumentácie a vlastné elektronické dokumenty.

Vyššie spomenutú požiadavku je nutné premietnuť do prevádzkovej dokumentácie vládneho cloudu a poskytnúť technické prostriedky pre ich naplnenie.

## 12.8 Riadenie aktív

Na dosiahnutie ochrany informačného systému pred jeho ohrozením je potrebné zabezpečiť technické, organizačné a personálne opatrenia pre všetky vrstvy IaaS, PaaS, SaaS. Tieto opatrenia je povinný prevádzkovateľ každej vrstvy služieb zabezpečiť v takej miere, aby sa zabránilo neoprávnenému prístupu k informáciám, narušeniu ich dôveryhodnosti a dostupnosti. Podrobne sa problematike riadenia aktív venuje príloha č.3.

## 12.9 Riadenie a kontrola prístupov a identít

Požiadavky na riadenie prístupov podrobne špecifikuje vyššie spomenutý výnos MF SR v paragrafe 41 v nasledovnom rozsahu:

- a) zavedenie identifikácie používateľa a následnej autentizácie pri vstupe do informačného systému verejnej správy,
- b) vypracovanie interného aktu riadenia prístupu k údajom a funkciám informačného systému verejnej správy založenej na zásade, že používateľ má prístup iba k tým údajom a funkciám, ktoré sú potrebné na vykonávanie jeho úloh,
- c) určenie postupu a zodpovednosti v súvislosti s pridelením prístupových práv používateľom,
- d) určenie požiadaviek, ktoré majú používatelia v súlade s bezpečnostnou politikou povinnej osoby dodržiavať pri používaní informačného systému verejnej správy,

e) automatické zaznamenávanie zmien v pridelenom prístupe a ich archivácia počas celej doby činnosti informačného systému verejnej správy,

f) určenie bezpečnostných zásad pre mobilné pripojenie do informačného systému verejnej správy a pre prácu na diaľku; mobilným pripojením je najmä prenosný počítač a personal digital assistant (PDA),

g) zabezpečenie, aby používatelia nepoužívali informačné systémy verejnej správy na nelegálne účely,

h) umožniť fyzickým osobám zodpovedným za správu a prevádzku informačných systémov verejnej správy prístup iba k takým údajom a funkciám v týchto informačných systémoch verejnej správy, ktoré nevyhnutne potrebujú na vykonávanie pridelených úloh,

i) automatické zaznamenávanie každého prístupu každého používateľa vrátane administrátora do informačného systému verejnej správy, zamedzenie možnosti zmeny týchto záznamov a zamedzenie možnosti vymazania týchto záznamov bez schválenia zodpovednou osobou určenou podľa § 29 písm. c),

j) vedenie formalizovanej dokumentácie prístupových práv všetkých používateľov informačného systému verejnej správy.

Architektonický rámec a referenčná architektúra je definovaná v nasledovných ISO štandardoch:

- ISO/IEC 24760-1:2011
- ISO/IEC 24760-2:2015
- ISO/IEC 24760-3:2016

Podrobnejšie sa venujeme problematike kontroly a riadenia prístupov a identít v prílohe č.4.

## 12.10 Šifrovanie

Šifrovanie ako jeden z nástrojov bezpečnosti zabezpečuje prístup k šifrovaným dátam výhradne autentifikovaným a autorizovaným osobám alebo systémom. V rámci návrhu a implementácie bezpečnostnej politiky a implementácie bezpečnostného projektu je potrebné zvážiť čo bude šifrované, akým mechanizmom a aký bude mechanizmus na zabezpečenie autentifikácie a autorizácie užívateľov a systémov, ktorí majú mať prístup k šifrovaným dátam.

## 12.11 Fyzická bezpečnosť a bezpečnosť prostredia

Tejto problematike sa venuje vyššie spomenutý výnos MF SR vo svojom paragrafe 35 v nasledovnom rozsahu:

a) umiestnenie informačného systému verejnej správy v takom priestore, aby informačný systém verejnej správy alebo aspoň jeho najdôležitejšie komponenty boli chránené pred nepriaznivými prírodnými vplyvmi a vplyvmi prostredia, možnými dôsledkami havárií technickej infraštruktúry a fyzickým prístupom nepovolanych osôb (ďalej len „zabezpečený priestor“),

b) oddelenie zabezpečeného priestoru od ostatných priestorov fyzickými prostriedkami najmä stenami a zábranami,

c) zabezpečenie, aby sa v okolí zabezpečeného priestoru nevyskytovali zariadenia, ktorými sú najmä kanalizácia a vodovod alebo materiály, ktorými sú najmä horľaviny, ktoré by mohli ohroziť informačný systém verejnej správy umiestnený v tomto zabezpečenom priestore,

d) vypracovanie a implementácia pravidiel pre prácu v zabezpečenom priestore,

e) zabezpečenie ochrany pred výpadkom zdroja elektrickej energie pre tie časti informačného systému verejnej správy, ktoré vyžadujú nepretržitú prevádzku a zabezpečenie, aby takýto výpadok nenastal,

f) zabezpečenie, aby boli existujúce záložné kapacity informačného systému verejnej správy, zabezpečujúce funkčnosť alebo náhradu informačného systému verejnej správy, umiestnené v sekundárnom zabezpečenom priestore, dostatočne vzdialenom od zabezpečeného priestoru,

g) zabezpečenie, aby bola prevádzka, používanie a manažment informačného systému verejnej správy v súlade s osobitnými predpismi, vnútornými predpismi povinnej osoby a jej zmluvnými záväzkami,

h) vypracovanie, zavedenie a kontrola dodržiavania pravidiel pre

1. údržbu, uchovávanie a evidenciu technických komponentov informačného systému verejnej správy a zariadení informačného systému verejnej správy,



2. používanie zariadení informačného systému verejnej správy na iné účely, na aké boli pôvodne určené,
  3. používanie zariadení informačného systému verejnej správy mimo určených priestorov,
  4. vymazávanie, vyradovanie a likvidovanie zariadení informačného systému verejnej správy a všetkých typov relevantných záloh,
  5. prenos technických komponentov informačného systému verejnej správy alebo zariadení informačného systému verejnej správy mimo priestorov povinnej osoby,
  6. narábanie s elektronickými dokumentmi, dokumentáciou systému, pamäťovými médiami, vstupnými a výstupnými údajmi informačného systému verejnej správy tak, aby sa zabránilo ich neoprávnenému zverejneniu, odstráneniu, poškodeniu alebo modifikácii,
- i) stanovenie parametrov pre informačné systémy verejnej správy, ktoré definujú maximálnu prípustnú dobu výpadku informačného systému verejnej správy a vytvorenie a zavedenie opatrení, ktoré sú zamerané na riešenie obnovy prevádzky v prípade výpadku informačného systému verejnej správy.

V roku 2015 bol zrealizovaný projekt IaaS časť 1. v DK1 Kopčianska v gescii MF SR. Koncom roku 2016 bude dokončená realizácia projektu IaaS časť 2 DT1 Tajov v gescii MV SR. Obe dátové centrá poskytujú služby minimálne v štandarde Tier III podľa definície Uptime Institute. Vychádzajúc z tohto faktu autor predpokladá, že došlo k naplneniu vyššie definovaných požiadaviek na fyzickú bezpečnosť a bezpečnosť prostredia v plnom rozsahu.

## 12.12 Bezpečnosť prevádzky

Pre zabezpečenie efektívnej prevádzky bezpečnosti cloudového prostredia je nutné aplikovať procesný prístup manažmentu informačnej bezpečnosti. Medzinárodná norma STN ISO/IEC 27001 si v oblasti procesného riadenia osvojila model PDCA ("Plánuj-Urob-Overuj-Konaj"). Model PDCA je možné aplikovať na všetky procesy manažmentu informačnej bezpečnosti. Problematiku auditu bezpečnosti prevádzky adresuje ISO/IEC 27002 bod 12.7. Podrobne sa bezpečnosti prevádzky venujeme v prílohe č. 5.

## 12.13 Bezpečnosť komunikačnej infraštruktúry

Komunikačná infraštruktúra cloudu zabezpečuje integritu a ochranu cloudového prostredia a chráni aktíva cloudu pred hrozbami zvonku. Okrem toho zabezpečuje izoláciu jednotlivých prostredí cloudu v prostredí zdieľanej IKT infraštruktúry a umožňuje výhradne kontrolovaný spôsob komunikácie medzi nimi.

Na elimináciu bezpečnostných rizík je použitá architektúra oddeľujúca jednotlivé prostredia (tenantov) do logických izolovaných celkov, takzvaných kontextov. Každé projektové zákaznícke prostredie je ďalej delené až na štyri horizontálne vrstvy (napr. DMZ, prezentačná, aplikačná, DB) a vertikálne izolované až na štyri prostredia (napr. Dev, Test, Staging a Prod). Štruktúru projektovo orientovaného prostredia je znázorňuje Obrázok 9 Projektovo orientované prostredie vládneho cloudu

Návrh komunikačnej infraštruktúry je uvedený v časti Príloha č.6 - Návrh komunikačnej infraštruktúry z pohľadu bezpečnosti.

## 12.14 Vývoj, zavádzanie a údržba systémov

Problematike aktualizácie IKT (zavádzania a údržby) sa podrobnejšie venuje paragraf 42 vyššie spomenutého výnosu MF SR v nasledovnom rozsahu:

a) zavedenie postupov s počiatočným stanovením a zahrnutím bezpečnostných požiadaviek a schvaľovacieho procesu pre

1. zmenu konfigurácie, zavádzanie nových alebo aktualizáciu a rozširovanie funkcionality existujúcich informačných systémov verejnej správy alebo ich častí; v prípade automatizovanej on-line aktualizácie sa schvaľovanie zavádza iba, ak si vyžaduje finančné zdroje alebo je aktualizácia príliš rozsiahla,

2. zavádzanie nových informačno-komunikačných technológií u povinnej osoby najmä s ohľadom na zaistenie kompatibility a zachovanie potrebnej úrovne bezpečnosti,

b) vymenovanie zástupcu správcu alebo prevádzkovateľa informačného systému verejnej správy, zodpovedného za informačnú bezpečnosť a činnosti podľa písmena a),

c) vymenovanie zástupcu dodávateľa, ak je dodávateľom činnosti podľa písmena a) tretia strana, zodpovedného za informačnú bezpečnosť,

d) vykonanie testovania pre činnosti podľa písmena a) a vytvorenie dokumentácie o spôsobe testovania a o dosiahnutých výsledkoch, a to najmenej vykonanie interného používateľského testovania v rozsahu najmenej jedného týždňa pred odovzdaním informačného systému verejnej správy, jeho časti alebo súvisiacej aplikácie dodávateľom a zahrnutie jeho výstupov do dokumentácie o spôsobe testovania a o dosiahnutých výsledkoch,

e) uchovávanie a aktualizácia dokumentácie o informačných systémoch verejnej správy alebo ich častiach, ktorá obsahuje

1. používateľskú dokumentáciu, ktorou je návod na používanie informačného systému verejnej správy,
2. administrátorskú dokumentáciu, ktorou je návod na správu a prevádzku informačného systému verejnej správy,
3. prevádzkovú dokumentáciu, ktorou je dokumentácia o architektúre informačného systému verejnej správy alebo jeho časti, jeho konfigurácii a väzbách na existujúce informačné systémy verejnej správy.

Na základe vyššie uvedeného je potrebné zapracovať tieto požiadavky do prevádzkovej dokumentácie s dôrazom na bezpečnosť a minimálny dopad na prevádzku. Ďalšie budovanie vládneho cloudu je potrebné realizovať v súlade s prílohou č. 7 vyššie spomenutého výnosu MF SR: Štandard pre architektúru cloud computingu.

## 12.15 Vzťahy s dodávateľmi

Vzťahy s dodávateľmi definuje vyššie spomenutý výnos MF SR vo svojom paragrafe v nasledovnom rozsahu:

*Štandardom pre účasť tretej strany je*

a) analýza rizík v súvislosti s informačnými systémami verejnej správy podľa § 31, vyplývajúcej z činnosti tretích strán v týchto informačných systémoch, najmä dodávateľov, externých spolupracovníkov, orgánov verejnej správy, fyzických osôb a zaistenie takých technických, organizačných a právnych podmienok pre činnosť tretích strán v informačných systémoch verejnej správy, aby nebola narušená bezpečnosť informačného systému verejnej správy a bezpečnostná politika povinnej osoby,

b) zabezpečenie, aby boli v zmluvách s treťou stranou o poskytovaní služieb súvisiacich s informačným systémom verejnej správy uvedené bezpečnostné požiadavky na tieto služby,

c) zamedzenie prístupu tretích strán ku všetkým údajom v informačnom systéme verejnej správy, ktoré sa považujú za aktíva, alebo umožnenie prístupu tretích strán k takýmto údajom na základe zmluvy tak, aby nebola narušená bezpečnosť informačného systému verejnej správy a bezpečnostná politika povinnej osoby,

d) zabezpečenie kontroly plnenia bezpečnostných požiadaviek podľa písmena b),

e) zabezpečenie, aby nesplnenie bezpečnostných požiadaviek podľa písmen b) a c) alebo podľa § 42 písm. a), c) a d) bolo dôvodom na neukončenie príslušnej etapy projektu alebo neschválenie prevzatia vykonávanej činnosti.

Dodávatelia (tretia strana) sú predovšetkým dodávatelia, ktorí sa podieľajú na

- návrhu a architektúre vládneho cloudu
- budovaní a rozvoji vládneho cloudu
- podpore prevádzky vládneho cloudu

Za dodávateľov sa v tomto kontexte nepovažujú výrobcovia technológií používaných vo vládnom cloudu s výnimkou aktivít podpory týchto zariadení. Z vyššie uvedeného vyplývajú požiadavky, ktoré je nutné implementovať do zmluvných vzťahov s dodávateľmi a prevádzkovej dokumentácie.

## 12.16 Riadenie incidentov

Problematike riadenia incidentov sa podrobnejšie venuje paragraf 37 vyššie spomenutého výnosu MF SR v nasledovnom rozsahu:

a) vypracovanie interného aktu obsahujúceho

1. postup pri ohlasovaní bezpečnostných incidentov a odhalených slabých miest informačných systémov verejnej správy, najmä za účelom včasného prijatia preventívnych a nápravných opatrení,

2. postup pri riešení jednotlivých typov bezpečnostných incidentov a spôsob ich vyhodnocovania,

3. spôsob evidencie bezpečnostných incidentov a použitých riešení,

b) zabezpečenie, aby o postupoch podľa písmena a) boli primeraným spôsobom informovaní všetci používatelia informačného systému verejnej správy, a aby boli tieto postupy dodržiavané,

c) zavedenie evidencie každého výpadku informačného systému verejnej správy a spôsobu jeho riešenia,

d) pre povinné osoby podľa § 3 ods. 3 písm. a) zákona používanie systému na detekciu prienikov, ktorý monitoruje bezpečnosť najmenej v rozsahu Intrusion Detection System (IDS),

e) vytvorenie a prevádzka kontaktného miesta povinnej osoby pre ohlasovanie bezpečnostných incidentov a odhalených slabých miest informačných systémov verejnej správy v správe povinnej osoby.

Problematicku riadenia bezpečnostných incidentov adresujú aj nasledovné štandardy:

- ISO/IEC 27017 – bod 16.
- ISO/IEC 27002 – bod 16.1.
- ISO/IEC 27035-1.
- ISO/IEC 27035-2.

## 12.17 Havarijné plánovanie a BCP

Požiadavky na túto oblasť definuje predovšetkým paragraf 55 a 35 vyššie spomenutého výnosu MF SR. Havarijné plánovanie adresuje špecificky iná časť tohto dokumentu následne by problematiku BCP resp. BCM mal podrobnejšie adresovať bezpečnostný projekt.

## 12.18 Kontrola dodržiavania bezpečnosti (compliance)

Problematicku kontroly dodržiavania bezpečnosti rieši vyššie menovaný výnos MF SR v paragrafe 55 kde špecificky definuje vykonať raz ročne:

1. audit informačnej bezpečnosti auditorom cloudu

2. umožňuje odberateľovi cloudových služieb vykonať prostredníctvom audítora cloudu alebo po dohode s poskytovateľom cloudových služieb inou osobou audit informačnej bezpečnosti všetkých zdrojov, ktoré využívajú jemu poskytované cloudové služby alebo sa týkajú jemu poskytovaných cloudových služieb, a to podľa podmienok upravených v dohode o poskytovanej úrovni cloudových služieb, pričom ak nastane bezpečnostný incident týkajúci sa týchto zdrojov, ktorý ovplyvní kvalitu príslušných poskytovaných cloudových služieb, umožňuje sa vykonať takýto audit bezodkladne po tomto incidente nezávisle od počtu auditov vykonávaných ročne podľa tohto bodu

3. umožňuje odberateľovi cloudových služieb vykonať prostredníctvom audítora cloudu alebo po dohode s poskytovateľom cloudových služieb inou osobou penetračný test týkajúci sa cloudových služieb poskytovaných tomuto odberateľovi cloudových služieb, pričom takýto test je pripravený podľa podmienok dohodnutých v dohode o poskytovanej úrovni cloudových služieb a tak, aby neovplyvnil kvalitu poskytovaných cloudových služieb alebo ju ovplyvnil v rozsahu dohodnutom medzi odberateľom cloudových služieb a poskytovateľom cloudových služieb

Problematicky kontroly dodržiavania bezpečnosti sa vyššie menovaný výnos MF SR okrajovo dotýka aj v nasledovných ustanoveniach:

§ 38 - Periodické hodnotenie zraniteľnosti

Štandardom pre periodické hodnotenie zraniteľnosti je pravidelné hodnotenie slabých miest a ohrození informačného systému verejnej správy identifikovaných podľa bezpečnostnej politiky povinnej osoby s periodicitou najmenej raz ročne.

§ 32 - Kontrolný mechanizmus riadenia informačnej bezpečnosti

Štandardom pre kontrolný mechanizmus riadenia informačnej bezpečnosti je

a) dodržiavanie bezpečnostnej politiky povinnej osoby a zabezpečenie a vykonávanie vnútornej kontroly alebo auditu informačnej bezpečnosti, ktorého periodicita sa určuje v bezpečnostnej politike povinnej osoby,

b) zabezpečenie archivácie, ochrany a vyhodnocovania auditných správ.



## § 29 - Riadenie informačnej bezpečnosti

*Štandardom pre riadenie informačnej bezpečnosti je*

- a) vypracovanie a schválenie bezpečnostnej politiky povinnej osoby,*
- b) zabezpečenie realizácie a dodržiavania schválenej bezpečnostnej politiky povinnej osoby,*
- c) určenie osoby alebo osôb zodpovedných za informačnú bezpečnosť povinnej osoby vrátane zodpovednosti za bezpečnosť všetkých informačných systémov verejnej správy,*
- d) určenie jednotlivých úloh osoby alebo osôb zodpovedných za informačnú bezpečnosť v súlade s bezpečnostnou politikou povinnej osoby,*
- e) zabezpečenie koordinácie aktivít organizačných zložiek povinnej osoby pri riešení informačnej bezpečnosti,*
- f) určenie konkrétnej zodpovednosti za jednotlivé aktíva povinnej osoby,*
- g) určenie privilegovaných používateľských rolí v informačných systémoch verejnej správy, určenie bezpečnostných požiadaviek na jednotlivé privilegované používateľské roly a určenie, ktoré používateľské roly nie je možné navzájom zlúčiť; privilegovanými používateľskými rolami sú najmä správca systému, operátor, používateľ, audítor a programátor.*

Z vyššie spomenutého je zrejmé, že je nutné zapracovať požiadavky paragrafov 55, 38, 32 a 29 do prevádzkovej dokumentácie vládneho cloudu a zmluvných vzťahov medzi poskytovateľom a odberateľom cloudových služieb minimálne v rozsahu definovanom týmto výnosom. Je nutné si uvedomiť, že minimálne raz ročne je nutné vykonať nezávislý audit informačnej bezpečnosti audítorom cloudu a o jeho výsledkoch informovať zúčastnené strany. Na základe prípadných zistení auditu je potrebné implementovať nápravné opatrenia v čo najkratšom čase. Rovnako raz ročne je potrebné umožniť odberateľovi cloudových služieb vykonať audit cloudových služieb, ktoré sú mu poskytované a nad nimi vykonať aj penetračný test.

# 13 Certifikácia a akreditácia služieb

## 13.1 Ciele

Pre prevádzkovateľa cloudových služieb bude potrebné, aby jeho služby boli maximálne dôveryhodné, aby každý, kto do nich zverí svoje dáta nemohol mať pochybnosti o zabezpečení dát a prevádzky (dostupnosť, rýchlosť odozvy, atď.). Zamerať sa iba na bezpečnosť dnes už nestačí.

Proces certifikácie ukončený príslušným certifikátom bude dávať jasnú a transparentnú správu o tom, že daná služba spĺňa náročné kritériá. Súčasťou kvalitnej certifikácie sú aj otázky o ochrane dát, interoperability a prenositeľnosti, dodržiavaní právnych predpisov, férovosti SLA, ochrane životného prostredia, ako je zamedzené tzv. Vendor lock-in, apod.

Kladný výrok audítora znamená, že daná služby prešla cez tzv. „sito neoddiskutovateľných otázok“ (non-negotiable scope).

Základným kameňom certifikácie je v zmysle hore uvedeného dosiahnuť, aby sa budovaný vládny cloud stal dostatočne dôveryhodným pre využívanie eGov služieb a vytvoril de-facto štandard pre poskytovanie cloudových služieb aj komerčnej sfére. Prechod bude pozostávať z 3 samostatných aktivít.

1. Dôveryhodný vládny cloud.
2. Kvalitný a vzdelaný personál.
3. Systém obstarávania cloudových služieb.

Tieto aktivity je potrebné v budúcnosti koordinovať s momentálne bežiacimi projektami, ktoré sa snažia eGov služby na úrovni európskej únie prepojiť na báze certifikovaných služieb ako sú Cloud for Europe (MFSR je členom konzorcia), EU Cert (MFSR je členom konzorcia), NG Cert. A v maximálnej možnej miere využiť výsledky pre rozvoj dôveryhodného cloudu.

## 13.2 Spôsoby riešenia

### 13.2.1 Dôveryhodnosť v prvom rade

Základným kameňom pre budovanie dôvery v cloudové služby je nezávislé uistenie pre všetkých zúčastnených, že poskytované služby sú bezpečné a plne v súlade s očakávanými parametrami služieb. Zároveň všetci odberatelia potrebujú mať istotu, že kvalita služby je postavená na udržateľných základoch v súlade s legislatívou a best-practice. Zároveň je potrebné uistenie, že aj podmienky poskytovania služby budú dodržiavané v čase a v prípade, že sa budú meniť tak zákazník bude mať možnosť presunúť svoje dáta do bezpečnejšieho cloudu.

### 13.2.2 Vzdelávanie

Vzdelávanie v oblasti certifikácie a štandardizácie pre rôzne dôvody.

Očakávaným výsledkom zavedenia systematického vzdelávania v oblasti cloudových služieb je príprava všetkých zúčastnených (prevádzkovateľov cloudových služieb ako aj prijímateľov prostriedkov pre rôzne projekty), aby už v úvodných fázach požiadavky kladené na nové služby už zohľadňovali okrem legislatívneho prostredia aj požiadavky na následnú certifikáciu služieb v záujme zvýšenia dôveryhodnosti.

### 13.2.3 Obstarávanie cloudových služieb

Pri budovaní vládneho cloudu je potrebné zvažovať aj skutočnosť, že vládny cloud bude rozšírený aj o verejnú časť, ktorá bude spracovávať dáta, ktoré sú menej kritické z pohľadu ochrany údajov. Ďalšie informácie sa nachádzajú v kapitole Hybridný vládny cloud.

Za týmto účelom bude potrebné vytvoriť samostatný systém obstarávania cloudových služieb. Vzhľadom na skutočnosť, že nákup cloudových služieb je pomerne rýchly proces medzi požiadavkou a samotnou realizáciou je potrebné zabezpečiť prostredie, kde by sa dalo pomerne efektívne nakupovať služby bez nutnosti pri každej požiadavke iniciovať celý proces verejného obstarávania.

Výsledkom bude prostredie, ktoré umožní efektívne pokrývať požiadavky organizácií na rôzne druhy cloudových služieb (PaaS, IaaS, XaaS,...).

### 13.2.4 Iba certifikované služby

Vzhľadom na fakt, že vládny cloud bude poskytovať certifikované služby tak požiadavka na certifikované služby na strane nákupu je nevyhnutná. Uľahčí sa týmto spôsobom aj budúcej certifikácii služieb vládneho cloudu.

V rámci certifikácie služieb je vhodné definovať, ktoré schémy sú vhodnými pre potreby cloudových služieb. ENISA uvádza približne 15 schém, z ktorých každá je zameraná na inú oblasť ICT. Pre potreby vládneho cloudu budú stanovené schémy, ktoré pokrývajú cloudové služby komplexne.

Jednotlivé schémy z hľadiska geografického pôsobenia a rozsahu sú uvedené v nasledovnej tabuľke:

	General	Cloud Computing	ICT, miscellaneous
Europe			
International		   	      
USA			

Obrázok 23 Jednotlivé schémy z hľadiska geografického pôsobenia a rozsahu

Najrozšírenejšie z týchto certifikačných schém aj s uvedením pokrytia dôležitých aspektov cloud computingu:

	Certifikácia				
Najdôležitejšie aspekty	ISO 27001	CSA	ISAE3402	TUV	ECSA
Cloud špecifické hodnotenie	☆☆☆	☆☆☆	☆☆☆	☆☆☆	☆☆☆
Hodnotenie bezpečnosti	☆☆☆	☆☆☆	☆☆☆	☆☆☆	☆☆☆
Hodnotenie súladu s legislatívou	☆☆☆	☆☆☆	☆☆☆	☆☆☆	☆☆☆
Hodnotenie súkromia údajov	☆☆☆	☆☆☆	☆☆☆	☆☆☆	☆☆☆
Spoločný rozsah - bez rokovaní	☆☆☆	☆☆☆	☆☆☆	☆☆☆	☆☆☆
Pokrytý celý dodávateľský reťazec cloudu	☆☆☆	☆☆☆	☆☆☆	☆☆☆	☆☆☆
Verejne dostupné hodnotiace kritériá	☆☆☆	☆☆☆	☆☆☆	nie	☆☆☆

★ = obsahuje

☆ = neobsahuje

Zdroj: CLOUD SERVICE CERTIFICATIONS: MEASURING CONSUMERS' PREFERENCES FOR ASSURANCES; Authors: Lansing Jens, Schneider Stephan; Sunyaev Ali

V súlade so zoznamom cloudových certifikačných schém publikovaných organizáciou ENISA – CCSL (Cloud Certification Schemes List) odporúčame pre certifikáciu poskytovateľov cloudových služieb vládneho cloudu nasledovné schémy (v abecednom poradí):

- Certified Cloud Service - TÜV Rheinland
- CSA Certification - OCF Level 2
- EuroCloud Star Audit Certification
- ISO/IEC 27001 Certification

Okrem definovania okruhu vhodných certifikačných schém je potrebné definovať aj minimálnu úroveň dosiahnutej certifikácie. Pre CSA sa odporúča dosiahnutie CSA Certification – OCF Level 2, pre ECSA Star Audit Certification na úrovni troch hviezd je odporúčané.

### 13.2.5 Vytvorenie katalógu služieb, ktoré budú nakupované

V zmysle vyššie uvedeného pri vytváraní systému na obstarávanie bude potrebné vytvoriť katalóg služieb, ktoré môžu byť nakupované pre rôzne účely na strane vládneho cloudu. Tento katalóg okrem špecifikácie služby bude obsahovať aj parametre potrebné na prevádzkovanie a integráciu služieb ako aj zoznam relevantných dodávateľov služby, ktorí prešli akreditáciou a môžu byť využití na dodávanie služby a integráciu do vládneho cloudu.

### 13.2.6 Akreditácia služieb

Vzhľadom na rýchly vývoj v oblasti ICT bude potrebné vytvoriť systém akreditácie služieb so vzájomným prepojením na postupy verejného obstarávania.

Zaradenie služby do katalógu bude prebiehať 2 možnými spôsobmi:

1. akceptácia certifikácie nezávislou inštitúciou (podľa zvolených schém),
2. samostatné preverenie procesov vyškolenými pracovníkmi prevádzkovateľa vládneho cloudu, tak aby dodávaná služba zodpovedala zvoleným pravidlám certifikácie.

Takýto postup bude treba kontinuálne zabezpečovať vzhľadom na to, že technológie a legislatívne požiadavky sa menia veľmi rýchlym tempom. Minimálny interval prehodnotenia konkrétnej služby a jej akreditácia je 1x za rok.

## 14 Model(y) spoplatnenia

### 14.1 Ciele

Súčasný stav budovania vládneho cloudu z pohľadu financovania (a finančných tokov) je podmienený využívaním prostriedkov EŠIF. Doterajšie investície smerovali (v súlade s koncepciou stanovenou v „centralizácii DC“) do rozvoja 2 dátových centier a zavedenia IaaS služieb. Tieto služby boli pripravené ako služby privátneho vládneho cloudu pričom jednou zo základných podmienok ich poskytovania bol, fakt že boli (a stále sú) určené výhradne pre organizácie verejnej správy. Súčasný stav je však taký, že primárnymi odberateľmi sú organizácie ŠS, pretože pre samosprávu bol budovaný DCOM a k implementačným požiadavkám na služby vládneho cloudu na konci programového obdobia OPIS z väčších miest (neboli súčasťou DCOM) nedošlo. Aj vzhľadom na požiadavky stanovené v NKIVS 2016, kde by samospráva mala využívať služby DCOM, dochádza k posunu pohľadu na to ako je potrebné pristupovať k plánovaniu, vyhodnocovaniu ale aj spoplatňovaniu služieb vládneho cloudu. Ešte väčší posun nastáva v prípade hybridného modelu, využívania služieb public cloudu, pri ktorom je zavedeným štandardom spoplatnenie na báze skutočne spotrebovaných zdrojov, pričom dochádza k priebežnému vyhodnocovaniu a vypradávaní (napr. fakturácii na mesačnej báze).

Ako bolo vyššie uvedené, tak IaaS služby vládneho cloudu sú financované z prostriedkov EŠIF, s podmienkou, že projekt mohol dostať pomoc zo štrukturálnych fondov ak táto investícia nebude prinášať priamy finančný príjem. Na základe toho v súčasnosti poskytované služby nie sú spoplatnené.

Z dôvodov:

- dlhodobejšej vízie poskytovania cloudových služieb (ako doba udržateľnosti OPIS/OPII projektov),
- poskytovania cloudových služieb aj pre samosprávu,
- využívania vybraných cloudových služieb od komerčných poskytovateľov (tzv. hybridný cloud),
- transparentného (na báze spoločných pravidiel) vyčíslňovania úspor pri migráciách ISVS do vládneho cloudu,

je nevyhnutné čo najskôr zaviesť:

- pravidlá pre stanovovanie cien cloudových služieb,
- procesov vysporiadania za spotrebované cloudové služby.

## 14.2 Pravidlá pre stanovovanie cien cloudových služieb

Na problematiku ohodnotenia cloudových služieb sa v prípade vládneho cloudu dá pozeráť z viacerých strán:

- verejná správa buduje vlastné cloudové služby a je potrebné sa zaoberať tým, čo všetko tvorí cenu takýchto služieb (TCO – celkové náklady na vlastníctvo),
- v prípade hybridného cloudu, môže mať VS záujem o komerčne poskytované cloudové služby, pričom v tomto prípade je tiež nevyhnutné poznať, čo všetko tvoria celkové náklady na vlastníctvo.

V neposlednom rade, dochádza a bude neustále dochádzať k porovnávaniu celkových nákladov na vlastníctvo budovaných privátnych a verejných cloudových služieb rovnakého typu. Aby bolo takéto porovnanie objektívne a mohli byť vyčísľované skutočné úspory alebo straty, je nevyhnutné aby vo všetkých prípadoch boli uplatňované rovnaké metódy výpočtu. Je tiež potrebné podotknúť, že služby rovnakého typu môžu byť zásadne cenovo rozdielne aj na základe rôznych úrovni poskytovania (SLA). Pre normalizáciu rôznych úrovni SLA je nevyhnutné zobrať do úvahy rovnaké kritéria. Tie sú uvedené v kapitole SLA.

Nasledujúca kapitola detailnejšie poukazuje na to akým spôsobom sa narába s cenami cloudových služieb v OPII projektoch. Zámerom je aby rovnaký (alebo veľmi podobný) koncept, platil nie len pre OPII projekty.

### 14.2.1 Ceny cloudových služieb v OPII projektoch

V prípade OPII projektov je metóda uvádzania celkových nákladov na vlastníctvo už súčasťou finančných analýz projektov (CBA). Pričom bola rozšírená aj o časť, ktorá zahŕňa výdavky za spotrebúvané cloudové služby.

Veľkou výhodou, takto vopred prepočítaných cien je z pohľadu odberateľa zjednodušený pohľad na problematiku IKT, pretože v cene poskytovanej služby sú už započítané všetky výdavky (vid. kapitola 14.2.1.2 Pohľad poskytovateľa) a tiež sa tým eliminuje disproporcia v podobe rozdielného započítavania výdavkov jednotlivými projektami.

#### 14.2.1.1 Pohľad odberateľa služieb vládneho cloudu

Z pohľadu odberateľa cloudových služieb, ktorý ide realizovať projekt OPII a spracováva finančnú analýzu projektu, je situácia jednoduchá.

Stačí použiť príslušnú „CBA excel“ prílohu s dynamicky prepojeným cenníkom<sup>13</sup>. A v záložke „spotrebúvané cloudové služby“ najskôr aktualizovať cenník, následne si vybrať typy služieb a ich množstvo, tak ako je znázornené na nasledujúcom príklade.

---

<sup>13</sup> Cenník je publikovaný na metais a pre správnu funkciu je potrebné mať povolené makrá.

*Obrázok 24 Príklad použitia cien cloudových služieb*

- služby 1 virtuálneho servera
- diskového priestoru TIER 2 s kapacitou 500 GB

<b>Nepriame prínosy</b>						<b>Prínosy spolu</b>						
<b>Úspora z prevádzky pri využívaní cloudových služieb</b>			<b>Kvalitatívne prínosy vo finančnom vyjadrení</b>			<b>Finančné prínosy</b>			<b>Ekonómické prínosy</b>			
<b>TCO AS-IS</b>	<b>Cloudové služby spolu</b>	<b>rozdiel</b>	<b>Alternat. A</b>	<b>Alternat. B</b>	<b>rozdiel</b>	<b>Alternat. A</b>	<b>Alternat. B</b>	<b>rozdiel</b>	<b>Alternat. A</b>	<b>Alternat. B</b>	<b>rozdiel</b>	
0,00	6 598,44	-6 598,44	0,00	0,00	0,00	0,00	6 598,44	6 598,44	0,00	0,00	0,00	
0,00	6 598,44	-6 598,44	0,00	0,00	0,00	0,00	6 598,44	6 598,44	0,00	0,00	0,00	
0,00	6 598,44	-6 598,44	0,00	0,00	0,00	0,00	6 598,44	6 598,44	0,00	0,00	0,00	
0,00	6 598,44	-6 598,44	0,00	0,00	0,00	0,00	6 598,44	6 598,44	0,00	0,00	0,00	
0,00	6 598,44	-6 598,44	0,00	0,00	0,00	0,00	6 598,44	6 598,44	0,00	0,00	0,00	
0,00	6 598,44	-6 598,44	0,00	0,00	0,00	0,00	6 598,44	6 598,44	0,00	0,00	0,00	
0,00	6 598,44	-6 598,44	0,00	0,00	0,00	0,00	6 598,44	6 598,44	0,00	0,00	0,00	
0,00	6 598,44	-6 598,44	0,00	0,00	0,00	0,00	6 598,44	6 598,44	0,00	0,00	0,00	
0,00	6 598,44	-6 598,44	0,00	0,00	0,00	0,00	6 598,44	6 598,44	0,00	0,00	0,00	
0,00	6 598,44	-6 598,44	0,00	0,00	0,00	0,00	6 598,44	6 598,44	0,00	0,00	0,00	
0,00	6 598,44	-6 598,44	0,00	0,00	0,00	0,00	6 598,44	6 598,44	0,00	0,00	0,00	
0,00	6 598,44	-6 598,44	0,00	0,00	0,00	0,00	6 598,44	6 598,44	0,00	0,00	0,00	
0,00	6 598,44	-6 598,44	0,00	0,00	0,00	0,00	6 598,44	6 598,44	0,00	0,00	0,00	
<b>SPOLU</b>						0,00	65 984,40	65 984,40	0,00	0,00	0,00	

*Obrázok 25 Príklad zohľadnenia prínosov pri používaní cloudových služieb*

Táto CBA kalkulačka je pripravená tak, aby umožňovala:

- kombinovať vlastné výdavky projektu na IKT so spotrebovanými službami vládneho cloudu (tzv. hybridné IT),
- dynamicky meniť a aktualizovať ponuku cloudových služieb, prostredníctvom centrálného distribučného bodu umiestneného na metais.

V prípade poskytovateľa služieb vládneho cloudu sa ako najvhodnejší spôsob určenia ceny javí metóda, ktorá vychádza z pomeru celkovej kapacity riešenia ku celkovým nákladom na vlastníctvo. V prípade komerčného poskytovateľa cloudových služieb (hybridný cloud) je cenotvorba plne na poskytovateľovi



služieb, avšak strategicky by mali byť tiež vyčíslované a porovnávané celkové náklady na vlastníctvo pri využívaní služieb vo väčšom časovom horizonte, aby sa eliminovalo skreslenie spôsobné krátkodobým dotovaním/cenovým dumpingom.

Ďalej uvádzaný postup bol aplikovaný na IaaS služby vládneho cloudu na základe nasledujúcich podmienok:

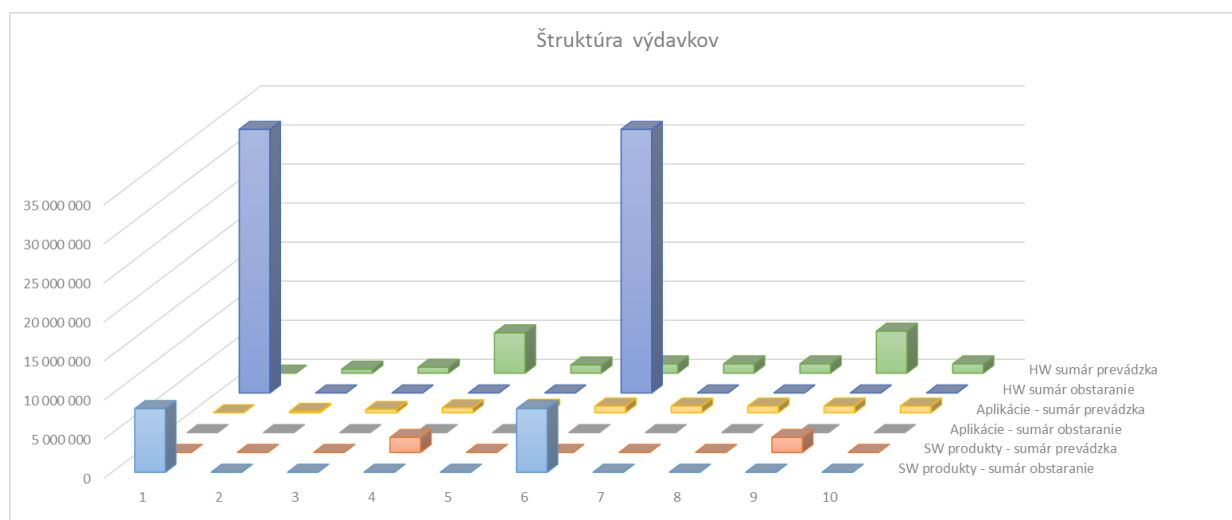
- uvedený prepočet bol vykonaný pre lokalitu DC Kopčianska (projekt IaaS časť 1)<sup>14</sup>
- vstupné hodnoty z OPIS projektu boli aplikované do OPII šablóny pre vykonanie CBA a hodnoty boli ďalej spresnené
- CBA šablóna predstavuje kontrolu vzájomného pomeru celkových nákladov na vlastníctvo v období 10 rokov ku celkovej kapacite prevádzkovej infraštruktúry násobenej stanovenými cenami za jednotlivé služby tak aby výsledok v 10 roku (ENPV) bol 0.

Katalóg služieb s cenami za mesiac, určenými na základe uvedeného postupu je uvedený v kapitole Príloha č.10 – Ceny IaaS služieb vládneho cloudu, kompletný prepočet je uvedený v kapitole Príloha č.9 – Ceny IaaS služieb vládneho cloudu - prepočet, a pre zabezpečenie automatizovanej distribúcie cenníka sú tieto hodnoty uvedené pre jednotlivé služby v lokalite<sup>15</sup>

<https://metais-test.finance.gov.sk/cilist/InfraSluzbaCennikovyZaznam>

Uvedené ceny nie sú tzv. predajné ceny, ale úlohou týchto cien je čo najpresnejšie odzrkadliť celkové náklady na vlastníctvo v horizonte 10 rokov na kapacitu ktoré uvedené riešenie ponúka. Na základe tohto pomeru (TCO/kapacita riešenia) sú stanovené adekvátne pomerné ceny, ktoré obsahujú:

- investičné výdavky v prvom roku,
- investičné výdavky v 6 roku na obnovenie HW infraštruktúry,



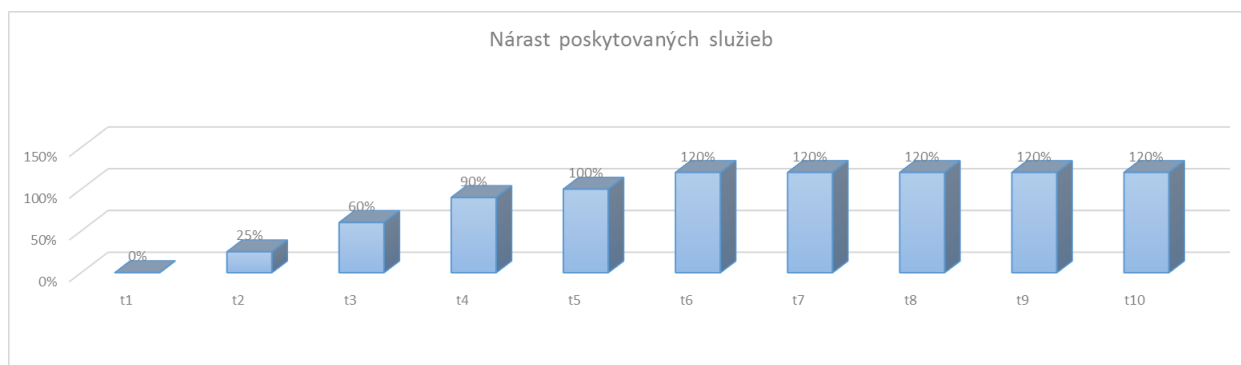
Obrázok 26 Štruktúra výdavkov na IaaS služby vládneho cloudu počas 10 rokov

- utilizáciu s postupným zaplnením po jednotlivých rokoch nasledovne,

<sup>14</sup> Projekt IaaS časť 2 je budovaný ako kapacitne identický projekt

<sup>15</sup> Zatiaľ v testovacej verzii





Obrázok 27 Predpokladaný nárast poskytovaných cloudových IaaS služieb riešením IaaS časť 1

- ceny za energie a celkovú spotrebu na základe aktuálnych meraní v DC,
- kompletnú prevádzkovú podporu 24x7
- poskytnutie x86 ako aj RISC virtualizácie
- komplexné riešenie sieťovej bezpečnosti (sieťové modely – zonácia na prostredia a vrstvy, IDS, IPS, SIEM, DDOS protection, HW load balancing)

Výdavky na všetky tieto služby/technológie sú zahrnuté v cene jednotlivých služieb. Zahrnutie všetkých položiek do ceny následne predstavuje základ pre dobrý prepočet nákladov na vlastníctvo a udržiavateľnosť ISVS prevádzkovaných vo vládnom cloude a istotu, že nebola opomenutá žiadna zásadná IKT funkcionálna pri navrhovaní nových projektov. To znamená, že riešitelia projektov sa nemusia vyššie uvedenými oblasťami zaoberať, ale služby majú požiadanie k dispozícii.

Uvedená metóda sa dá analogicky aplikovať aj pre určovanie cien PaaS a SaaS služieb vládneho cloudu, pričom:

- do ceny PaaS služieb sa budú započítavať ceny za spotrebúvané IaaS služby (tak ako je uvedené v kapitole Pohľad odberateľa služieb vládneho cloudu.
- do ceny SaaS služieb sa budú započítavať ceny za spotrebúvané IaaS a PaaS služby.

#### 14.2.2 Pohľad na financovanie cloudových služieb z pohľadu riadenia rozpočtu

V súčasnosti prostriedky na prevádzku a rozvoj informačných prostriedkov pochádzajú z dvoch zdrojov

1. EŠIF,
2. rozpočtové zdroje.

V rámci zákona o štátnom rozpočte 411/2015 Z.z. – zákon o štátnom rozpočte bol definovaný program pre Vládny cloud - 074040T. Ktorý bude obsahovať výdavky spojené s prevádzkou a ďalším budovaním vládneho cloudu. Keďže tento program sa dá chápať ako nadrezortný program je potrebné v najbližšej dobe metodicky doriešiť spôsoby zainteresovania organizácií, ktoré využívajú zdroje vládneho cloudu pre potreby budovaných rezortných IS. Cieľom tohto zainteresovania je v čo najväčšej miere využiť dostupné kapacity, ktoré sú zdieľané všetkými zainteresovanými stranami. Základnými pravidlami by malo byť optimálne odhadovanie potrieb konkrétnych systémov tak aby v prípade nadhodnotenia a dlhodobého nevyužívania kapacity rezortným systémom bolo možné nevyužívané zdroje okamžite použiť inou organizáciou. Na druhej strane je potrebné v súčinnosti ÚPPVII vytvoriť ucelenú metodiku stanovovania ceny migrácie IS do vládneho cloudu, aby jednotlivé rezortné systémy boli schopné v rámci prípravy rozpočtu odhadnúť dostatočné prostriedky.

### 14.3 Procesy vysporiadania za spotrebované cloudové služby

ÚPPVII ako cloud broker, ktorého úlohu je zabezpečovať okrem prevádzky vládneho cloudu aj zúčtovanie s externými poskytovateľmi služieb (vid. kapitola 9), potrebuje vytvoriť samostatné procesy pre

zúčtovanie nakupovaných služieb ako aj spotrebu vlastných zdrojov. Tento proces je komplikovaný vzhľadom na rozpočtové pravidlá ako aj pravidlá pre poskytovanie prostriedkov EŠIF. Pre tento účel by bolo vhodné budúcnosti uvažovať s vytvorením vnútorného zúčtovania pomocou pravidiel definovaných na základe spotreby zdrojov vládneho cloudu vrátane nakupovaných služieb. Ako prvý krok pre je vhodným riešením pravidelné reportovanie ÚPPVII ostatným rezortom o spotrebúvaní zdrojov prostredníctvom výkonových parametrov služieb vládneho cloudu a nakupovaných služieb.

## 15 Prevádzka

### 15.1 Ciele

Implementáciou projektu vládneho cloudového datacentra vzniká špecifické IT prostredie s novým typom požiadaviek na prevádzku. Jeho hlavné charakteristické znaky sú:

- Zabezpečenie prevádzky cloudového prostredia so zreteľom na zdieľanú zodpovednosť centrálnych a klientskych prevádzkových tímov, vyplývajúca z implementácie klientsky spravovaných aplikačných komponentov na centrálnej infraštruktúrnej platforme.
- Heterogénne postupy a procesy prevádzky jednotlivých klientov sú synchronizované a komunikačne prepojené so štandardizovanými postupmi prevádzky cloudového riešenia.
- Implementovať prevádzkové nástroje a procesy, ktoré umožnia prevádzkovať cloudové prostredie s požadovanými kvalitatívnymi parametrami a nárokmi na vyššiu dynamiku zmien v porovnaní s klasickým datacentrom.
- Cieľom prevádzky cloudového riešenia je optimalizácia využitia HW zdrojov a nákladovosti prevádzky pri udržaní parametrov služieb definovaných v SLA.
- Prevádzkové prostredie predpokladá metodiku, procesný model, integračný model, definíciu infraštruktúry a prevádzkových tímov tak aby bolo cloudové prostredie schopné udržať definované SLA aj s nárastom počtu klientov a používaných služieb.
- Zabezpečiť finančné a personálne opatrenia na doplnenie personálnych zdrojov, predovšetkým špecialistov IT a IT bezpečnostných pracovníkov prevádzkovateľa vládneho cloudu v počte 26 zodpovedajúcich tabuliek.

Pre procesný model prevádzky bude vyžadované vypracovanie a implementácia procesov:

- Service desk - bude potrebné zabezpečiť obsluhu rutinných požiadaviek na bežné (štandardizované) prevádzkové zmeny čo najviac automatizovaným spôsobom. To žiadateľovi zaručí predovšetkým plynulé vybavenie požiadaviek. Pre žiadateľa bude k dispozícii samoobslužné rozhranie, ktoré mu umožní jednoduchý výber z možností, zadávanie a sledovanie stavu požiadaviek. Podľa potreby môže byť zaradené schvaľovanie, prípadne notifikácie účastníkov procesu.
- Správa incidentov - bezprostredným cieľom procesu bude zabezpečiť predídanie hroziacemu výpadku ako aj najskoršie možné odstránenie výpadku služby či obnovenie požadovanej úrovne služby. V záujme efektívneho riešenia incidentov bude definovaná klasifikácia a bude potrebné definovať scenáre a zodpovednosti za riešenie
- Problém Management - cieľom procesu bude identifikovať príčinu (root cause) a navrhnúť najvhodnejšie riešenie a ďalej odovzdať riešenie príslušnému procesu alebo tímu.
- Správa SLA - Na prevádzkovej úrovni bude cieľom správy SLA zabezpečiť kontrolu a dodržiavanie definovaných SLA pre služby z katalógu služieb prípadne tiež definované požiadavky na podporné služby resp. procesy. Bude potrebné vykonať analýzu nadväzných akcií pre prípad nedodržania SLA. Bez príslušnej reakcie a relevantnej definície parametrov SLA nie je prevádzka reálne vyhodnocovateľná
- Monitoring a meranie spotreby - meranie prevádzkových parametrov prostredia a využívanie zdrojov a licencií. Bude potrebné vytvoriť model spolplatnenia využitia služieb "Pay as you Go" a naviazať spotrebu na rozpočtové zdroje odberateľov cloudových služieb
- Riadenie zmien - proces bude mať zastrešovať plánovanie, koordináciu a zaznamenávanie zmien vrátane aktualizácie konfiguračnej databázy. Súčasťou procesu bude aj vyhodnocovanie zmien a prispôsobovanie samotného procesu meniacim sa potrebám a rozširovaniu o služby z vyššou pridanou hodnotou. Plánované zmeny bude potrebné vyhodnotiť aj z pohľadu dopadu na existujúci stav a riziká pre prevádzku cloudu.

- Release and Deployment Management
- Správa licencií a konfigurácií - kontrola efektivity alokovaných licencií a infraštruktúrnych a platformových konfigurácií
- Riadenie prístupov - na všetkých úrovniach (Service portal, VM, Cloud platforma, monitoring nástroje) bude založená na centrálnom IAM riešení s modelom RBAC. Funkcie sú bližšie popísané v kapitole "Radenie bezpečnosti".
- Riadenie kapacít cloudu - vyhodnocovanie využitia existujúcich kapacít, trendov a predpokladaného nárastu požiadaviek bude potrebné vyhodnocovať na základe vstupov a pripomienkovania prevádzky ako kľúčového stakeholdera pre odhad kapacít.
- Riadenie dostupnosti - požiadavky na dostupnosť služieb budú dané definovanými SLA pre služby z katalógu služieb. Požiadavky na dostupnosť budú premietnuté do režimu prevádzky cloudového riešenia a tiež do požiadaviek na monitorovacie riešenie.

## 15.2 Riadenie prevádzky

Na zabezpečenie efektívneho riadenia prevádzky musí vzniknúť riadiaci výbor, ktorý bude kontrolovať technickú infraštruktúru a konzistentnosť riešenia vládneho cloudu, ktorý bude jednotný a platný v oboch lokalitách vládneho cloudu ( oboch dátových centrách ). Riadiaci výbor prevádzky bude rozhodovať ohľadne plánovania a všetkých zmenách, ktoré budú mať dopad na kvalitu a udržateľnosť prevádzky.

## 15.3 Štandardizácia procesov, prostredí a konsolidácia architektúry

Efektivita prevádzky bude výrazne ovplyvnená dosiahnutou štandardizáciou prevádzkových procesov pre všetkých odberateľov cloudových služieb. Prevádzka bude tiež vyžadovať konsolidáciu architektúry riešení, tak aby bolo možné prevádzkovať centrálné platformové služby typu centrálny monitoring, centrálny IAM, tak aby sa vylúčila opakovaná implementácia tých istých služieb v rôznych obmenách.

Bude tiež potrebné vyhodnotiť dopad množstva prevádzkovaných typov prostredí na efektivitu a udržateľnosť prevádzky. V rámci schvaľovania aplikačných architektúr nových projektov vyžadovať maximálnu možnú štandardizáciu prevádzkovaných platforiem a prostredí s ohľadom na efektivitu nákladov a udržateľnosť prevádzky.

Zvýšenie efektivity rutinných operácií prevádzky v nadväznosti na aktivity vývojových tímov bude potrebné podporiť zavedením nástrojov automatizácie činnosti pre správu konfigurácií a artefaktov, provisioning prostredí, nasadzovanie riešení a monitoring - DevOps platforma, časť prevádzky. Bude potrebné vykonať analýzu možných realistických scenárov s ohľadom na predpokladané spúšťanie projektov OPII.

Nástroje a technologické prvky cloudovej platformy sú charakteristické intenzívnym vývojom a častými zmenami verzií a technológie komponentov. Toto prináša na jednej strane mimoriadne rýchly posun v oblasti, na druhej strane kladie zvýšené nároky na zmenové konania a incident management pre prevádzku platformy. Pre udržanie aktuálnej verzie implementovanej OpenStack platformy bude potrebné zo strany prevádzky kontinuálne vyhodnocovanie a monitorovanie implementovaných zmien. Aktivita zmenového konania bude potrebné zosúladiť s vopred ohlásenými major releasmi OpenStack platformy ( predpoklad je 2 x ročne). Okrem toho môže vzniknúť potreba implementácie zmeny pre rôzne verzie a fix packy, ktoré budú postupne uvoľňované. SLA prevádzkovaného prostredia bude rámcom pre postupy release a change managementu cloud platformy.

Okrem základnej technologickej platformy bude potrebné pripraviť a priebežne aktualizovať plán zmenových konaní aj pre ďalšie technologické prvky zabezpečujúce fungovanie platformy - Servisný orchestrátor, SIEM nástroje, komponenty pre monitoring platformy a aplikácii, servisný katalóg a pod.

## 15.4 Onboarding

Onboarding klientov do prevádzky bude charakteristický preberaním implementovaných štruktúr nových prostredí z implementačného projektu a zároveň prepájaním klientskeho a centrálného prevádzkového tímu na úrovni nástrojov a procesov podpory prevádzky.

Základné aktivity onboarding procesu budú pokrývať:

- Review kompatibility štandardov klientskeho a centrálného prostredia.
- Validácia a review návrhu riešenia (nasadzované a prevádzkované aplikácie, integračné väzby na iné aplikácie a klientske prostredie, definované závislosti...).
- Validácia a review sieťového dizajnu virtualizovanej klientskej infraštruktúry.
- Validácia a kontrola nastavenia sieťových protokolov aplikačnej vrstvy.
- Validácia a zosúladenie bezpečnostných a eskalačných postupov.
- Validácia a otestovanie plánov zabezpečenia kontinuity prevádzky - úplný test nástrojov a postupov obnovy prevádzky v záložnom prostredí by mal prebehnúť na produkčnej a záložnej infraštruktúre pred nábehom prevádzky.
- Validácia a otestovanie plánov zálohovania a obnovy prostredí – úplný test nástrojov a postupov zálohovania a obnovy dát by mal prebehnúť na produkčnej infraštruktúre pred nábehom prevádzky.
- Validácia postupov riadenia prístupov a požiadaviek na autentifikáciu – v prvej fáze sa bude jednať o autentifikáciu a autorizáciu skupiny administrátorov zodpovedných za prevádzku riešenia a pracovníkov technickej podpory.
- Príprava klientskeho prevádzkového tímu na prechod do cloudového prostredia – školenia. Prevádzkový tím klienta musí byť oboznámený so základnou technickou koncepciou, postupmi a možnosťami cloudového riešenia.
- Príprava komunikačných kanálov pre riadenie služieb so zdieľanou zodpovednosťou
  - Prepojenie ITSM nástrojov,
  - Priradenie prístupov na service desk,
  - Validácia a schválenie zoznamu samoobslužných služieb rutínnej prevádzky zo servisného katalógu a oprávnení k ich využívaniu.
- Iniciálne nastavenie prístupových oprávnení pre nábeh prevádzky.
- Príprava monitoringu a zdieľania informácií pre prevádzkový tím.
- Kontrola nástrojov, dát a informačných tokov reportingu parametrov prevádzky služieb.
- Validácia bill of material pre zdroje datacentra a MF SR, pridelené klientovi, kontrola iniciálneho stavu CMDB.

Preberanie nových systémov do prevádzky bude tiež vyžadovať preverenie a otestovanie všetkých obstaraných a nakonfigurovaných služieb pre odberateľa cloudových služieb - prevádzkové testy pre priepustnosť sieťovej infraštruktúry, clustrové a ďalšie sieťové služby, disaster recovery a ďalšie. Preberacie testy budú súčasťou procesu uvádzania do prevádzky.

Pre nemanážené serverové platformy bude tiež potrebné vykonať analýzu možných vulnerabilit v priradenej zodpovednosti tímov za jednotlivé kroky disaster recovery procesu.

## 16 Legislatívne požiadavky

Na medzinárodnej úrovni je problematike cloud computingu v oblasti ISO/IEC venovaných viacero štandardov:

*ISO/IEC 17789:2014 - Cloud computing - Reference architecture*

*ISO/IEC 19086-1:2016 - Cloud computing - Service level agreement (SLA) framework -- Part 1: Overview and concepts*

*ISO/IEC CD 19086-2 - Cloud computing - Service level agreement (SLA) framework -- Part 2: Metric Model*

*ISO/IEC DIS 19086-3 - Cloud computing - Service level agreement (SLA) framework -- Part 3: Core conformance requirements*

*ISO/IEC CD 19941 - Cloud computing - Interoperability and portability*

*ISO/IEC DIS 19944 - Cloud computing - Cloud services and devices: data flow, data categories and data use*

ktoré boli východiskové aj pri príprave tohto dokumentu.

Na úrovni VS SR je problematika cloud computingu uvedená vo **výnose č. 55/2014 Z. z. ministerstva financií Slovenskej republiky o štandardoch pre informačné systémy verejnej správy** (ďalej len

výnos MF SR) v kontexte ďalšej platnej legislatívy, ktorý nadobudol účinnosť 1.7.2016. Výnos sa v paragrafe č.55 venuje problematike cloud computingu, v rozsahu:

- Modely poskytovania cloudových služieb a typy cloud computingu podľa § 54
- Správa cloud computingu podľa § 55
- Vytváranie a rozvoj cloud computingu podľa § 56
- Používanie cloudových služieb podľa § 57

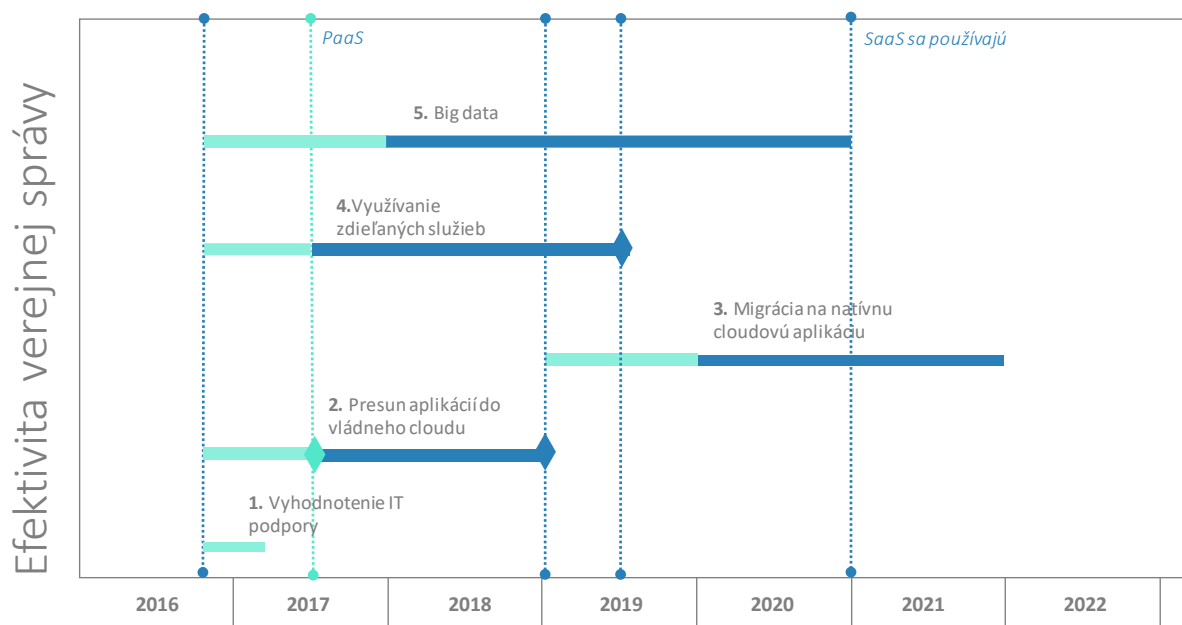
V časti Navrhované opatrenia sú uvedené oblasti, ktoré je potrebné zapracovať do existujúcich legislatívnych predpisov.

## 16.1 Navrhované opatrenia

Legislatívny predpis	Navrhované opatrenie	Predpokladaný termín
Úprava organizačného poriadku dotknutých OVM.	Založenie „Kancelárie vládneho cloudu“ na ÚPPVII	Apríl 2017
Novelizácia zákona č.275/2006 Z.z. o Informačných systémoch verejnej správy.  Príprava zákona o ITVS.	Zavedenie komplexných povinností v oblasti výkonu správy IT so zohľadnením medzinárodných štandardov v oblasti cloud computingu.	Koniec roka 2017
Výnos MF SR č. 55/2014 o štandardoch pre ISVS.	Doplnenie kritérií akreditácie a certifikácie služieb.	Koniec roka 2017
Novelizácia zákona o kritickej infraštruktúre (zákon č. 45/2011 Z. z. o kritickej infraštruktúre)	Optimalizácia rozsahu kritickej infraštruktúry;  Stanovenie pravidiel pre zabezpečenie kritickej infraštruktúry.	Koniec roka 2017
Metodický pokyn Ministerstva financií SR na usmernenie rozpočtovania IT výdavkov financovaných zo štátneho rozpočtu	Doplnenie typov výdavkov na cloudové služby	Koniec roka 2017

## 17 Plánovanie a migrácia

### 17.1 Akčný plán podľa NKIVS



Obrázok 28 Dejová línia pre Efektivitu verejnej správy

#### Kľúčové míľniky

- Vyhodnotenie stavu IT riešení (do konca marca 2017).
- Presun aplikácií do vládneho cloudu (do konca roka 2019).
- Migračný plán do vládneho cloudu (do mája 2017).
- Nasadenie služieb „Infraštruktúra ako služba“ (k dispozícii už teraz).
- Definovanie filozofie postupného rozširovania služieb PaaS a nastavenie pravidiel prevádzky služieb PaaS (do decembra 2016) a nasadenie základného súboru služieb „Platforma ako služba“ (do decembra 2017).
- Postupné sprístupňovanie ďalších služieb PaaS podľa vopred vypracovaného harmonogramu (do júna 2020).
- Realizácia migrácie (do konca roka 2019).

## 17.2 Kľúčové strategické programy/projekty

Vysvetlenie komplexity

- **B** – biznis komplexita (**Nízka** – metodiky, štúdie; **Stredná** – realizácia, alebo úprava procesov a služieb na úrovni organizácie, **Vysoká** – realizácia, alebo úprava procesov a služieb s nadrezortným rozsahom resp. dopadom na veľkú skupinu občanov, alebo podnikateľov)
- **A** – aplikačná komplexita (**Nízka** – konfiguračné zmeny ISVS, použitie SaaS, alebo COTS; **Stredná** – vývoj nového ISVS; **Vysoká** – príprava nadrezortných služieb s integráciou množstva IS, migrácie množstva ISVS do vládneho cloudu)
- **T** – technologická komplexita (**Nízka** – konfiguračné zmeny, použitie IaaS; **Stredná** – technologické zmeny IS veľkého rozsahu s použitím PaaS; **Vysoká** – technologické zmeny veľkého rozsahu – viacerých IS, príprava technológií pre využitie na medzirezortnej úrovni)





## 17.2.1IaaS vládneho cloudu

Aktivita		Merateľný ukazovateľ	Závislosť na inej aktivite	Začiatok Koniec	Komplexita	Zodpovednosť	
1	<p>Príprava štúdie uskutočniteľnosti pre ďalší rozvoj IaaS služieb v nasledovných oblastiach:</p> <ul style="list-style-type: none"> <li>1) Sieťové služby <ul style="list-style-type: none"> <li>- DNS – poskytnutie centralizovaných a automatizovaných DNS služieb pre projekty vo vládnom cloud</li> <li>- NTP – sprístupnenie centrálného NPT v sieti "shared services" pre IS vo vládnom cloud</li> <li>- Automatizované VPN – poskytnutie automatizovaných VPN profilov na zabezpečené prepojenie prezentačnej vrstvy projektov nasadených vo vládnom cloud s privátnymi dátovými centrami, alebo organizáciami za účelom bezpečného využívania služieb medzi projektami v cloud a služieb privátnych DC</li> </ul> </li> <li>2) Metering &amp; Billing - Pre všetky cloudové služby poskytované vládny cloudom je potrebné zabezpečiť jednotný systém, ktorý bude poskytovať nasledovné služby: <ul style="list-style-type: none"> <li>- Kvantitatívne meranie poskytovaných cloudových služieb, t.j. meranie výkonnostných a/alebo kapacitných parametrov cloudových služieb za definované obdobie.</li> <li>- Meranie úrovni poskytovaných SLA, t.j. meranie poskytujúce informácie či zazmluvnené SLA parametre a podmienky medzi Poskytovateľom a Odberateľom sú dodržané.</li> </ul> </li> </ul>			K:6/2017	B:Nizka	ÚPPVII spolupráci MVSR	v s



	<p>3) HSM – služba zariadenia Hardware Security Modulu do topológie informačného systému prevádzkovaného vo vládnom cloude.</p> <p>4) Zálohovanie ako služba (Backup as a service). Doplnenie služby k existujúcim službám infraštruktúry, tak aby nebol zabezpečovaný iba backup virtálnych strojov bežiacich vo vládnom cloude, ale aby odberatelia dostali k dispozícii plnohodnotnú „multi-tenant“ službu, ktorá dokáže zabezpečiť zálohovanie podľa konfiguračných požiadaviek odberateľa v rámci vládneho cloudu, alebo mimo vládny cloud. Resp. do prostredia vládneho cloudu z IT odberateľa, ako spôsob riešenia DR s BCP pre hybridné IT scenáre.</p> <p>5) Integrácia PaaS a hybridný cloud - rozšírenie samoobslužného portálu a orchestračného nástroja cSP (Cloud Service Provisioner) pre umožnenie zadania požiadaviek na PaaS a služby hybridného cloudu, automatizovaný provisioning IaaS služieb pre potreby PaaS a hybridného cloudu.</p>					
2	Bezpečnostný projekt – vypracovanie bezpečnostného projektu na posúdenie, eliminovanie a minimalizovanie hrozieb a rizík pôsobiacich na informačné systémy prevádzkované vo vládnom cloude, z hľadiska narušenia jeho bezpečnosti, spoľahlivosti a funkčnosti.			K:12/2017	B: Nízka	
3	Realizácia kvalitatívneho rozšírenia IaaS služieb v rozsahu bodu 1.	Počet využívaných IaaS služieb vládneho cloudu	1	K:6/2018	A: Nízka T: Vysoká	MVSR
4	Realizácia kvantitatívneho rozšírenia IaaS služieb podľa potreby.	Počet využívaných IaaS služieb vládneho cloudu		K:6/2018		MVSR
5	Realizácia prepojenia DCOM do infraštruktúry vládneho cloudu s cieľom zdieľaného využívania vybraných služieb.	Počet využívaných PaaS služieb vládneho cloudu z DCOM			T: Nízka	MVSR, DEUS



6	<p>Integrácia oboch inštancií cSP a rozšírenie cSP o služby DR IaaS.</p> <p>1) Automatizovaný záznam dátovej komunikácie v okamžiku detekcie kritickej bezpečnostnej anomálie.</p> <p>2) Globálny monitoring dostupnosti aplikácií zo sieťovej prevádzky.</p>	Počet ISVS s využívaním DR IaaS		K:12/2017	T:Nízka	MVSR
---	---	------------------------------------	--	-----------	---------	------



## 17.2.2 Vytvorenie dôveryhodného prostredia

Aktivita		Merateľný ukazovateľ	Závislosť na inej aktivite	Začiatok Koniec	Komplexita	Zodpovednosť
7	Na základe požiadaviek a posúdenia relevantných certifikačných schém definovať, ktoré budú pre oblasť vládneho cloudu považované za hodnoverné.	Definované minimálne 2 schémy na základe štúdie a vytvorenie spoločného katalógu certifikačných kontrol		Z: 3.2017 K: 6.2017	B: Nízka	ÚPPVII
8	Etablovanie pravidiel hodnotenia služieb pre Úrad podpredsedu vlády ako súčasť národného cloud brokera.		7	Z: 7.2017 K: 12.2017	B: Nízka	ÚPPVII
9	Vytvorenie kontinuálneho vzdelávacieho systému pre pracovníkov úradu ako aj pre prijímateľov z jednotlivých organizácií, aby všetky projekty už o počiatku zodpovedali riešeniam cloudových služieb v zmysle štandardov definovaných pre vládny cloud ako aj „best practice“ v iných oblastiach IT.		7, 8	Z: 7.2017	B: Stredná A: Nízka	ÚPPVII
10	Certifikácia vybraných služieb nezávislou inštitúciou.	Certifikácia aspoň 30% poskytovaných služieb	7	Z: 7.2017	B: Nízka	
11	Rozšírenie existujúceho katalógu služieb o služby budované pomocou hybridného cloudu a sprístupnenie public cloud services najmä pre oblasť vývoja nových služieb alebo prevádzku služieb, ktoré nevyžadujú veľmi vysokú mieru zabezpečenia a ochrany (napr. Open data). Pre potreby nákupu a zaradenia služieb je potrebné vytvoriť systém akým národný cloud broker bude schopný rýchlym spôsobom obstarávať služby.		13,14	Z: 12.2017	B: Nízka	ÚPPVII v spolupráci s MVSR

### 17.2.3 Realizácia funkcií Sprostredkovateľa Hybridného vládneho cloudu

Všetky funkcie Sprostredkovateľa Hybridného vládneho cloudu podľa čl.5.4. musia byť automatizované s výnimkou akreditácie CSP pre Hybridný vládny cloud. V iniciálnej fáze implementácie tejto organizačnej zložky je však možné implementovať semi-automatický prístup, ktorý bude založený na schválenej procesnej a metodologickej báze, tak, aby jeho implementácia korelovala s ďalšími aktivitami v rámci Vládneho Cloudu (napr. PaaS).

(Pri vývoji Sprostredkovateľa Hybridného vládneho cloudu môžu byť využité i IPR, ktoré MF SR získava ako výsledok projektu „Cloud for Europe“).

Akreditáciu CSP bude zabezpečovaná ÚPP II na základe metodiky, ktorá bude zohľadňovať komplexne systémové, bezpečnostné a komerčné aspekty spojené s poskytovaním služieb daného CSP. V prípade CSP, ktoré sú súčasťou vládneho cloudu iného ČŠ EU, bude metodika zohľadňovať i bilaterálne dohody alebo iné strategické aspekty.

Funkciu Sprostredkovateľa služieb Vládneho Cloudu tak privátneho ako aj v budúcnosti hybridného zabezpečuje ÚPP II. Hybridný vládny cloud ako nástroj rozšírenia funkcionality a zlepšenia ekonomickej efektívnosti prevádzky by mal byť uvedený do prevádzky v r. 2019.

Aktivita		Merateľný ukazovateľ	Závislosť na inej aktivite	Začiatok Koniec	Komplexita	Zodpovednosť
12	Spracovať Štúdiu uskutočniteľnosti Sprostredkovateľa Hybridného vládneho cloudu a pripraviť súťaž na jeho dodávku.			K: 6.2017	B:Nízka	ÚPPVII
13	Realizovať dodávku Sprostredkovateľa Hybridného vládneho cloudu.		12	K: 6.2018	B: Stredná A: Stredná T: Nízka	ÚPPVII
14	Pripraviť Metodiku akreditácie CSP zo SR a ČŠ EU pre zapojenie do Hybridného vládneho cloudu a Metodiku sprostredkovania služieb Hybridného vládneho cloudu.		8,12	K: 9.2017	B:Nízka	ÚPPVII

### 17.2.4 Migrácie do vládneho cloudu



Aktivita	Merateľný ukazovateľ	Závislosť na inej aktivite	Začiatok Koniec	Komplexita	Zodpovednosť
15 Aktualizovať Metodické usmernenie Ministerstva financií SR č. MF/020304/2014-1721 s ohľadom na Metodický pokyn Ministerstva financií SR č. MF/011247/2016-1721 tak, aby relevantné údaje, ktoré poskytuje alebo môže poskytovať MetaIS aktualizovali priamo v MetaIS a príslušné súbory z Metodického usmernenia vypustiť.				<b>B:</b> Nizka	ÚPPVII
16 Prepracovať Fázu Plánovanie Metodického usmernenia aby reflektovala pohľad per IS.				<b>B:</b> Nizka	ÚPPVII
17 Tam kde nie je, vypracovať hĺbkový audit IS s cieľom zmapovať reálny počet a stav IS a zaviesť, aktualizovať informácie o nich, v MetaIS.	Počet auditovaných IS			<b>B:</b> Nizka	ÚPPVII v spolupráci s organizáciami VS
18 Realizovať migrácie komplexných agendových IS v rámci projektu aplikačnej aktualizácie týchto IS.	Počet migrovaných komplexných agendových IS			<b>B:</b> Vysoká <b>T:</b> Stredná	Organizácie VS
19 Realizovať migráciu subjektov samosprávy s cieľom zvýšenia využívania SaaS aplikácií.	Počet subjektov samosprávy využívajúcich SaaS služby vládneho cloudu			<b>A:</b> Vysoká	DEUS



### 17.2.5 Model spoplatnenia cloudových služieb

Aktivita		Merateľný ukazovateľ	Závislosť na inej aktivite	Začiatok Koniec	Komplexita	Zodpovednosť
20	Pripraviť metodické usmernenie pre zavedenie pravidiel jednotného stanovovania celkových nákladov na vlastníctvo ISVS a stanovovania cien služieb vládneho cloudu. Vráťane stanovenia výdavkov na výstavbu a migrácie ISVS s využitím služieb hybridného vládneho cloudu.	- Počet ISVS s určeným TCO  - Počet služieb cloudu so stanovenými cenami		K: 12.2017	B:Nízka	ÚPPVII v s a spolupráci MVSR DEUS
21	Rozšíriť funkcionality Sprostredkovateľa o „Rozúčtovávanie výdavkov za spotrebované cloudové služby“ aplikovateľnú na celú VS a pre služby Hybridného vládneho cloudu.		20		B:Stredná A: Nízka	ÚPPVII





## 17.2.6PaaS

Aktivita	Merateľný ukazovateľ	Závislosť na inej aktivite	Začiatok Koniec	Komplexita	Zodpovednosť
22 Príprava štúdie uskutočniteľnosti pre prípravu PaaS služieb v nasledovných oblastiach: 3) PaaS automatizácia, 4) PaaS DevOps, 5) PaaS služby: - Služby databázovej vrstvy, - Služby Integračnej a orchestračnej vrstva, - Služby aplikačnej vrstvy, - Služby prezentačnej vrstvy, - Služby bezpečnosti, - Služby monitoringu a manažmentu.			K: 3.2017	B:Nízka	MVSR
23 Realizácia PaaS služieb vládneho cloudu.	Počet využívaných PaaS služieb vládneho cloudu	22	K: 12.2017	B: Stredná A: Nízka T: Vysoká	MVSR
24 Riadenie licencií SW poskytovaných PaaS služieb.	Objem finančných prostriedkov určených na SW licencie poskytovaných PaaS služieb	23	Z: 12.2017	B: stredná	ÚPPVII

## 18 Záver

Tento dokument vznikol v otvorenom a participantovom procese odborníkov z verejnej správy a komerčného sektora. Dokument bude schválený v Rade vlády SR pre digitalizáciu verejnej správy a jednotný digitálny trh.

Rozsahom sa dokument zameriaval na detailnejšie rozpracovanie principiálnych tém v oblasti cloud computingu vo VS SR, ktoré boli uvedené v NKIVS. V stanovenom čase potrebnom na prípravu tohto dokumentu nebolo možné viaceré z oblastí rozpracovať ešte do väčšieho detailu (návodov a metodických pokynov). Takže pre praktickú aplikáciu tvorí toto rozpracovanie skupinu ďalších nadväzujúcich aktivít, uvedených v kapitole Plánovanie a migrácia.

Vzhľadom na to, že strategická priorita Vládny cloud je len jednou z 10 strategických priorít (určené v NKIVS) a problematika IT VS sa v mnohých oblastiach prekrýva, taktiež z dôvodu postupného rozpracovávaní jednotlivých priorít je ďalej nevyhnutné zosúladiť SP predovšetkým v oblastiach:

- SP kybernetická bezpečnosť – s bezpečnostnými konceptami tejto SP.
- SP rozvoj agendových IS a SP využívanie centrálnych spoločných blokov – s časťou SaaS.
- Strategická architektúra a referenčná architektúra konkrétnych riešení – s modelom architektúry vládneho cloudu v centrálnom repozitári. Vzory, spôsoby a prípady používania cloudových služieb musia byť pripravené pre referenčnú architektúru konkrétnych riešení.
- Governance (prístup k procesu informatizácie) – zosúladenie povinností v oblasti organizačného zabezpečenia a prevádzky.

Plánovaný zoznam aktivít, bude ďalej vstup pre prípravu Detailného akčného plánu (rozpracovanie NKIVS kapitoly Návrh realizácie).

## 19 Odkazy na externé zdroje

#	Názov	Verzia	Stručný popis
[1]	Výnos ministerstva financií Slovenskej republiky zo 4.3.2014 o štandardoch pre informačné systémy verejnej správy.	2014/55	Výnos o štandardoch pre ISVS [č. 55/2014 Z. z.] - v účinnosti od 15. marca 2014 - vydaný v Zbierke zákonov
[2]	Strategický dokument pre oblasť rastu digitálnych služieb a oblasť infraštruktúry prístupovej siete novej generácie (2014 – 2020)		Strategický dokument pre oblasť rastu digitálnych služieb a oblasť infraštruktúry prístupovej siete novej generácie (2014 – 2020) vypracovalo Ministerstvo financií SR za účelom splnenia ex ante kondicionálít definovaných v rámci tematického cieľa 2 „Zlepšenie prístupu k informačným a komunikačným technológiám a zlepšenie ich využívania a kvality“, prostredníctvom ktorých Európska únia posudzuje pripravenosť členských štátov realizovať zvolené investičné priority v programovom období 2014 – 2020.  Dňa 08.01.2014 vzala vláda SR Strategický dokument na vedomie.
[3]	Návrh centralizácie a rozvoja dátových centier v štátnej správe	MF_014451_2 014-1721	21.5.2014 vládou schválený materiál, ktorý bol predložený Ministerstvom

			financií SR s cieľom zlepšovať služby a zvyšovať produktivitu verejnej správy.
[4]	Koncepcia eGovernmentu (2014 – 2020)	2.0	Dokument Koncepcia eGovernmentu 2014 až 2020 navrhuje implementáciu stratégie rozvoja eGovernmentu stanovenú v Strategickom dokumente pre oblasť rastu digitálnych služieb a oblasť infraštruktúry prístupovej siete novej generácie. Predstavuje tak východisko a katalóg možných projektov pre prioritnú os 7 Operačného programu Integrovaná infraštruktúra.
[5]	Metodické usmernenie Ministerstva financií Slovenskej republiky č. MF/020304/2014		Metodické usmernenie Ministerstva financií Slovenskej republiky č. MF/020304/2014-1721 na spracovanie analýzy stavu a potrieb informačno-komunikačných technológií a na spracovanie harmonogramu migrácie informačno-komunikačných technológií jednotlivých rezortov do dátového centra štátu
[6]	Národná koncepcia informatizácie verejnej správy Slovenskej republiky	2016	Materiál Národná koncepcia informatizácie verejnej správy Slovenskej republiky (ďalej len „NKIVS“) sa predkladá vláde SR na schválenie v zmysle § 4 ods. 1 písm. a) zákona č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov v znení neskorších predpisov. NKIVS navrhovaná na indikatívne obdobie do roku 2020 nadväzuje na pôvodné princípy informatizácie definované v NKIVS schválenej v roku 2008, aktuálny stav architektúry integrovaného informačného systému verejnej správy, zrealizované rozvojové projekty a uskutočnené aktivity, ktoré rozširuje o nové princípy vyplývajúce zo súčasných trendov a získaných skúseností, ako aj z možností poskytovaných rozvojom informačno-komunikačných technológií.

## 20 Slovník pojmov

Pojem	Definícia
<b>ACL</b>	Access Control List
<b>ADC</b>	Application Delivery Control
<b>API</b>	Application programming interface - rozhranie pre programovanie aplikácií
<b>BCP</b>	Business Continuity Planning
<b>CNAME</b>	CNAME záznam, alebo „záznam kanonické meno“ spôsobuje, že jeden názov domény je aliasom pre iný. Takáto doména má platné všetky subdomény a DNS záznamy originálu.
<b>CO</b>	Continuous operations
<b>cSP</b>	Cloud Service Provisioner
<b>CSP</b>	Cloud Service Provider
<b>DataCentrum</b>	Organizácia v zriaďovateľskej pôsobnosti Ministerstva financií SR
<b>DC</b>	Dátové centrum
<b>DCOM</b>	Dátové centrum miest a obcí
<b>DDOS</b>	Distributed denial-of-service
<b>DMZ</b>	Demilitarizovaná zóna alebo demilitarizované pásmo, počítačová sieť s kontrolovanými možnosťami prístupu na servery, ktoré sú na sieť pripojené
<b>DNS</b>	Domain name system/server
<b>DWDN</b>	Dense Wavelength Division Multiplexing
<b>DR</b>	Disaster Recovery
<b>EA</b>	Enterprise architecture
<b>EDA</b>	Event-driven Architecture
<b>ECSA</b>	EuroCloud Star Audit
<b>ENISA</b>	European Network and Information Security Agency (v skratke ENISA) je Európska agentúra pre bezpečnosť sietí a informácií
<b>EŠIF</b>	Európske štrukturálne a investičné fondy (EŠIF) sú s rozpočtom 454 miliárd EUR na roky 2014 – 20 hlavným nástrojom investičnej politiky Európskej únie
<b>FC</b>	Fiber Channel
<b>FCP</b>	Fiber Channel Protocol



<b>FCoE</b>	Fiber Channel over Ethernet
<b>FCIP</b>	Fiber Channel Internet Protocol
<b>FW</b>	Firewall
<b>GCB</b>	Sprostredkovateľ cloudových služieb (Government Cloud Broker)
<b>GEO</b>	Geografický
<b>HA</b>	High availability
<b>HSM</b>	Hardware Security Module
<b>HTTPS</b>	Zabezpečený hypertextový prenosový protokol (angl. hypertext transfer protocol secure), skr. HTTPS, je zabezpečená verzia HTTP, komunikačného protokolu World Wide Web.
<b>HW</b>	Hardware
<b>IaaS</b>	Infrastructure as a Service, Infraštruktúra ako služba
<b>IAM</b>	Identity and access management
<b>ICMP</b>	Internet Control Message Protocol
<b>ICT</b>	Informačné a komunikačné technológie alebo menej často informačná a komunikačná technológia, skr. IKT (angl. information and communication(s) technology alebo menej často information and communication(s) technologies, ICT)
<b>IDS</b>	Intrusion Detection System
<b>IISVS</b>	Integrovaný informačný systém verejnej správy
<b>IKT</b>	Informačné a komunikačné technológie
<b>IP</b>	Internet Protocol
<b>IPS</b>	Intrusion Prevention System
<b>IS</b>	Information System
<b>ISVS</b>	Informačný systém verejnej správy
<b>IT</b>	Informačné technológie
<b>ITSM</b>	Manažment služieb IT alebo ITSM alebo (Information Technology Service Management) znamená riadenie služieb informačných technológií.
<b>LAN</b>	Local area network
<b>LAN LB</b>	Local Area Network Load Balancing
<b>LAN FW</b>	Local Area Network Firewall



<b>MF SR</b>	Ministerstvo financií Slovenskej republiky
<b>MPLS</b>	Multiprotocol Label Switching
<b>MV SR</b>	Ministerstvo vnútra Slovenskej republiky
<b>NKIVS</b>	Národná koncepcia informatizácie verejnej správy
<b>NTP</b>	Network Time Protocol
<b>OPII</b>	Operačný program Integrovaná infraštruktúra
<b>OPIS</b>	Operačný program Informatizácia spoločnosti
<b>PaaS</b>	Platform as a Service
<b>PDC</b>	Primárne dátové centrum
<b>PDCA</b>	Plánuj-Urob-Overuj-Konaj (plan–do–check–act or plan–do–check–adjust)
<b>PKI</b>	Public key infrastructure – infraštruktúra verejných kľúčov
<b>PO1</b>	Prioritná os 1
<b>RBAC</b>	Role-based access control
<b>RFC</b>	Request for Comments
<b>RISC</b>	Reduced instruction set computer, skratene RISC (doslova počítač s obmedzenou sadou inštrukcií) je architektúra procesorov s priamočiarym vykonávaním pomerne jednoduchých inštrukcií.
<b>RPO</b>	Recovery point objective
<b>RTO</b>	Recovery time objective
<b>RTT</b>	Round-trip time
<b>SaaS</b>	Software as a Service
<b>SABSA</b>	Sherwood Applied Business Security Architecture
<b>SAN</b>	Storage area network
<b>SDN</b>	Software Defined Networking
<b>SHARE</b>	SHARE je nezávislá dobrovoľná IT asociácia
<b>SLA</b>	Service level agreement, zmluva o úrovni poskytovaného servisu
<b>SLO</b>	Service level objective
<b>SOA</b>	Service Oriented Architecture
<b>SPOF</b>	Single Point of Failure

<b>SR</b>	Slovenská republika
<b>SSH</b>	Zabezpečený prístup k príkazovému interpretovaču (angl. secure shell), skr. SSH, je v informatike počítačový program ako aj súvisiaci sieťový protokol určený na prihlasovanie a vykonávanie príkazov na vzdialenom počítači v počítačovej sieti.
<b>SQO</b>	Service Qualitative Objective
<b>SW</b>	Software
<b>TCO</b>	Total cost of ownership
<b>TIER 1</b>	Podľa definície Uptime Institute. Základná infraštruktúra, vybavenie garantuje dostupnosť 99,671 %
<b>TIER 2</b>	Podľa definície Uptime Institute. Redundantné prvky infraštruktúry garantujú dostupnosť 99,741 %
<b>TIER 3</b>	Podľa definície Uptime Institute. Servisovateľné za prevádzky s garantovanou dostupnosťou 99,982 %
<b>TIER 4</b>	Podľa definície Uptime Institute. Bezvýpadková redundantná elektrická sieť so záložnými zdrojmi a distribučnými cestami zaručujúcimi dostupnosť 99,995 %
<b>UPS</b>	Uninterruptible Power Supply - záložný zdroj
<b>ÚPPVII</b>	Úrad podpredsedu vlády pre investície a informatizáciu
<b>URI</b>	Jednotný identifikátor prostriedku (iné názvy: jednotný identifikátor zdroja, jednotný identifikátor zdrojov, angl. Uniform Resource Identifier, skratka URI) je kompaktný reťazec znakov používaný na identifikáciu alebo pomenovanie zdroja
<b>VPN</b>	Virtual private network
<b>VS</b>	Verejná správa
<b>WAN</b>	Wide area network
<b>WIP</b>	Wide Internet Protocol

## 21 Prílohy

### 21.1 Príloha č.1 - Popis biznis procesov

#### 21.1.1 Používanie cloudových služieb

Popis		
Využívanie služieb	cloudových	Využívanie činnosti cloudových služieb zahŕňa využívanie služieb poskytovateľa cloudových služieb s cieľom splniť niektoré úlohy. Využívanie činnosti cloudových služieb spravidla zahŕňa:



		<ul style="list-style-type: none"><li>• poskytovanie záruk poskytovateľovi cloudových služieb za účelom udelenia prístupu ku cloudovým službám,</li><li>• využívanie cloudových služieb, ktoré smeruje k dosiahnutiu konkrétnych výsledkov.</li></ul>
Výber a objednanie služby		<p>Činnosť výberu a objednania služby zahŕňa:</p> <ul style="list-style-type: none"><li>• skúmanie ponuky cloudových služieb a určenie, či ponúkaná služba spĺňa obchodné a technické požiadavky odberateľa cloudovej služby. Toto spravidla zahŕňa čítanie katalógu služieb a dokumentácie ku každej službe, ktorá môže zahŕňať technické informácie o službe a jej SLA, spolu s obchodnými informáciami vrátane cien,</li><li>• vyjednávanie podmienok cloudovej služby (ak poskytovateľ cloudovej služby umožní variabilné podmienky služby),</li><li>• prijatie zmluvy na cloudové služby a uskutočnenie registrácie u poskytovateľa cloudovej služby.</li></ul>
Realizácia administrácie	biznis	<p>Činnosť uskutočňovania biznis administrácie zahŕňa riadenie obchodných aspektov využívania cloudových služieb, vrátane rozpočtovania. Táto činnosť zahŕňa:</p> <ul style="list-style-type: none"><li>• prispôbenie plánu na využívanie cloudových služieb,</li><li>• sledovanie využívania služieb a riešenia riadenia rozpočtu,</li><li>• zabezpečenie toho, aby požiadavky zodpovedali skutočnému využívaniu cloudových služieb zo strany odberateľa cloudových služieb,</li></ul>
Prepájanie systémov s cloudovými službami	s	<p>Činnosť prepájania systémov s cloudovými službami zahŕňa integráciu existujúcich systémov a cloudových služieb a obsahuje prepojenie existujúcich zložiek a aplikácií s cieľovou cloudovou službou (službami), ako aj prepojenie zákazníckeho monitorovania a riadiacich systémov s monitoringom poskytovateľa cloudovej služby a riadením cloudových služieb.</p> <p>Prepojenie existujúcich zložiek a aplikácií s cieľovou cloudovou službou (službami) zahŕňa:</p> <ul style="list-style-type: none"><li>• hodnotenie dopadu cloudovej služby (služieb) na existujúce procesy, systémy a služby,</li><li>• mapovanie obchodných údajov medzi existujúcimi systémami zákazníka cloudovej služby a cloudovými službami,</li><li>• volanie cloudových služieb z existujúcich aplikácií,</li><li>• poskytovanie prístupových práv pre používateľov cloudových služieb,</li><li>• definovanie a implementovanie požiadaviek súvisiacich s bezpečnosťou, vrátane dôvernosti a integrity tokov údajov,</li><li>• integrovanie zákazníckych zariadení pre správu používateľských kont, bezpečnostných úloh, identít a povolení s ekvivalentnými zariadeniami pre cloudové služby,</li></ul>

	<ul style="list-style-type: none"><li>• tvorba a monitorovanie konkrétnych používateľských kont a identít na využívanie manažérskych rozhraní pre cloudové služby,</li></ul> integrovanie prihlasovania a riadenie bezpečnostných incidentov medzi cloudovými službami a monitoringom odberateľa cloudových služieb
Poskytnutie informácií o využívaní	Činnosť poskytovania informácií o využívaní zahŕňa prípravu správ o využívaní cloudových služieb zákazníkymi organizáciami a pridružené správy týkajúce sa tohto využívania. Tieto správy sa poskytujú gestorovi používateľa cloudových služieb.
Správa prenájmov	Činnosť správy prenájmov zahŕňa správu prenájmov odberateľa cloudových služieb s poskytovateľom cloudových služieb. Táto činnosť zahŕňa: <ul style="list-style-type: none"><li>• konfiguráciu a kontrolu bezpečnostných aspektov, vrátane používateľských kont, bezpečnostných úloh, identít a povolení,</li><li>• identifikáciu a riadiace údaje zdieľané dvoma používateľmi v rámci prenájmu,</li><li>• tvorbu a odstraňovanie prenajímateľov,</li><li>• riadenie používateľov a alokovaných zdrojov prenajímateľov.</li></ul>
Uskutočnenie testu služieb	Uskutočnenie testu služieb zahŕňa služby poskytovateľa cloudových služieb s cieľom zabezpečiť, aby boli cloudové služby v súlade s obchodnými potrebami odberateľa cloudových služieb. Cloudové služby sa používajú na základe testu, podľa vzájomnej dohody a chápania medzi poskytovateľom cloudovej služby a odberateľom cloudovej služby.  Uskutočnenie testovacej činnosti služieb zahŕňa: <ul style="list-style-type: none"><li>• poskytnutie používateľského oprávnenia s cieľom umožniť poskytovateľovi cloudovej služby overiť identitu používateľa a povoliť prístup do „testovacej“ cloudovej služby,</li><li>• sprístupnenie „testovacej“ cloudovej služby, ktorá môže byť overená odberateľom cloudovej služby.</li></ul>
Monitorovacia služba	Aktivita monitorovacej služby monitoruje kvalitu poskytnutých služieb s ohľadom na úroveň služieb definovanú v zmluve o úrovni služieb (SLA) medzi odberateľom cloudovej služby a poskytovateľom cloudovej služby. Táto činnosť využíva vnútorné monitorovacie funkcie cloudového systému. Táto činnosť zahŕňa: <ul style="list-style-type: none"><li>• sledovanie, do akej miery a ktorými používateľmi sa cloudová služba využíva</li><li>• monitorovanie integrácie cloudových služieb a existujúcich systémov IKT odberateľa</li><li>• definovanie meracích bodov a indikátorov výkonu súvisiacich s danou službou (napr. dostupnosť služby, frekvencia výpadku služby,</li></ul>

		<p>priemerný čas opravy, reakcie schopnosť kontaktného miesta poskytovateľa a pod.).</p> <ul style="list-style-type: none"><li>• monitorovanie, analýza a archivácia týchto údajov o indikátoroch.</li><li>• porovnanie kvality skutočne poskytnutej služby s dohodnutou kvalitou služieb.</li></ul>
Riešenie problémov	reportov o	<p>Činnosť riešenia reportov o problémoch zahŕňa riešenie hlásených problémov na strane odberateľa cloudových služieb poskytovateľovi cloudových služieb. Táto činnosť zahŕňa:</p> <ul style="list-style-type: none"><li>• hodnotenie dopadu každého problému,</li><li>• riešenie problému s cieľom určiť príčinu (príčiny) problému,</li><li>• otvorenie problémovej správy (správ) u poskytovateľa cloudovej služby a hľadanie riešenia,</li><li>• tvorba spôsobov riešenia problému,</li><li>• eskalácia problémov, ktoré nie sú pevne stanovené v dohodnutých časových harmonogramoch alebo ktoré majú vážny dopad.</li></ul>
Spravovanie služby	bezpečnosti	<p>Činnosť spravovania bezpečnosti služieb zahŕňa (z pohľadu odberateľa cloudových služieb):</p> <ul style="list-style-type: none"><li>• zaistenie primeranej bezpečnosti údajov odberateľa cloudovej služby, ktoré sú vložené do prostredia cloud computingu,</li><li>• zavedenie plánov zálohovania a obnovy údajov, potenciálne aj duplikácie a zabezpečenie pred zlyhaním,</li><li>• správu bezpečnostných politík,</li><li>• definíciu šifrovania a technológií integrity vo vzťahu k údajom odberateľa cloudových služieb,</li><li>• definíciu riešenia osobných údajov.</li></ul>

### 21.1.2 Sprístupňovanie cloudových služieb

Popis	
Získavanie a prístup k odberateľom	<p>Činnosť získavania a prístupu k odberateľom zahŕňa aktivity požadované na marketing a ponuku cloudových služieb po bod, kedy odberateľ cloudovej služby súhlasí so zmluvou o využívaní jednej alebo viacerých služieb. Táto činnosť cloud computingu zahŕňa:</p> <ul style="list-style-type: none"><li>• poskytovanie informácií potenciálnym odberateľom o dostupných službách a súvisiacich SLA a zmluvných podmienkach,</li><li>• vyjednávanie podmienok s odberateľmi,</li></ul>

	<ul style="list-style-type: none"><li>• hodnotenie potrieb a požiadaviek odberateľa na cloudové služby.</li></ul>
Riadenie vzťahov s odberateľmi	<p>Činnosť riadenia vzťahov s odberateľmi zahŕňa riadenie obchodných vzťahov poskytovateľa cloudovej služby s odberateľom cloudovej služby, vrátane:</p> <ul style="list-style-type: none"><li>• tvorby a údržby obsahu katalógu služieb,</li><li>• získavania odberateľov,</li><li>• poskytovanie kontaktného bodu pre odberateľa pre všetky obchodné záležitosti,</li><li>• diskutovanie a riešenie otázok alebo problémov odberateľov,</li><li>• riešenie žiadostí o zmenu (napr. zmeny nárokovateľných požiadaviek).</li></ul>
Riadenie finančného spracovávaní	<p>Činnosť riadenia finančného spracovávaní zahŕňa:</p> <ul style="list-style-type: none"><li>• riešenie rozpočtovania a výdavkov na zabezpečenie poskytovania cloudových služieb (celkové výdavky na vlastníctvo služby - TCO na poskytovanie cloudovej služby),</li><li>• výdavky súvisiace s využívaním cloudových služieb,</li><li>• riešenie prijatia finančných prostriedkov na zabezpečenie poskytovania cloudových služieb.</li></ul>
Nastavenie právnej zmluvy	<p>Činnosť nastavenia právnej zmluvy sa týka zmluvy o poskytnutí služby medzi odberateľom cloudovej služby a vybraným poskytovateľom (poskytovateľmi) cloudovej služby. Toto zahŕňa vyjednávanie zmluvy o poskytnutí služby medzi odberateľom cloudovej služby a vybraným poskytovateľom (poskytovateľmi) cloudovej služby s cieľom splniť potreby odberateľa.</p>

### 21.1.3 Plánovanie cloudových služieb

Popis	
Hodnotenie prostredia verejnej správy	Činnosť hodnotenia prostredia verejnej správy sa zameriava na hodnotenie aktuálnych služieb v prostredí verejnej správy s cieľom nájsť cloudovú službu (cloudové služby), ktoré spĺňajú požiadavky odberateľa. Táto činnosť cloud computingu zahŕňa:

	<ul style="list-style-type: none"><li>• hodnotenie ponuky produktov poskytovateľov cloudových služieb na základe technických a iných informácií,</li><li>• objednanie si a doručovanie upozornení o zmenách v katalógu služieb poskytovateľov cloudových služieb,</li><li>• spájanie ponuky produktov s potrebami a požiadavkami odberateľa, vrátane technických, obchodných a regulačných podmienok.</li></ul>
Riadenie biznis plánu	<p>Činnosť riadenia biznis plánu zahŕňa:</p> <ul style="list-style-type: none"><li>• definovanie ponuky služby, opis technických aspektov ponuky (funkčné rozhrania, SLA ...) a obchodné hľadisko ponuky,</li><li>• tvorba obchodného plánu, čo zahŕňa ponuku jednej alebo viacerých cloudových služieb pre odberateľa, riešenie finančných a technických podmienok služieb, cieľových zostáv odberateľa, zmlúv a SLA,</li><li>• sledovanie využívania služby v porovnaní s plánom s cieľom zabezpečiť, aby boli splnené ciele pre poskytovateľa cloudovej služby,</li><li>• príprava obchodného plánu a prispôsobenie obchodného plánu k poskytovaniu cloudových služieb.</li></ul>

#### 21.1.4 Riadenie bezpečnosti a rizík cloudových služieb

Popis	
Riadenie bezpečnosti a rizík	<p>Činnosť riadenia bezpečnosti a rizík sa zameriava na riadenie bezpečnosti a rizík súvisiacich s tvorbou, poskytovaním, využívaním a podporou cloudových služieb. Táto činnosť zahŕňa:</p> <ul style="list-style-type: none"><li>• definovanie politiky informačnej bezpečnosti - s prihliadnutím na požiadavky služieb, zákonné a regulačné požiadavky a zmluvné povinnosti a povinnosti SLA,</li><li>• definovanie rizík informačnej bezpečnosti v súvislosti s cloudovými službami a prístupu k týmto rizikám v súlade s obchodnými cieľmi poskytovateľa cloudových služieb. Významným bodom v tejto oblasti je, že riadenie rizík informačnej bezpečnosti je spojené s nákladmi a že poskytovateľ môže zaujať obchodnú pozíciu neriešenia niektorých rizík a namiesto toho preniesť zodpovednosť za tieto riziká na odberateľa cloudových služieb prostredníctvom zmluvy o poskytovaní služieb,</li><li>• kontroly informačnej bezpečnosti s ohľadom na riešenie rizík spojených so službou. Kontroly spravidla pokrývajú skupinu kategórií, ako sú:<ul style="list-style-type: none"><li>– riadenie identity a prístupu,</li></ul></li></ul>

	<ul style="list-style-type: none"><li>– objavovanie, kategorizácia, ochrana údajov a informačných aktív,</li><li>– nákup, vývoj a údržba informačných systémov,</li><li>– bezpečná infraštruktúra z hľadiska hrozieb a zraniteľnosti,</li><li>– riadenie problémov a incidentov informačnej bezpečnosti,</li><li>– riadenie bezpečnosti a súlad,</li><li>– fyzická a personálna bezpečnosť,</li><li>– bezpečnosť sietí a komunikácií,</li><li>– izolácia (medzi nájomcami pri riešení situácie kde je viacej nájomcov - tenants),</li><li>• zabezpečenie, aby boli kontroly zavedené pri nasadzovaní služby a súvisiacej infraštruktúry,</li><li>• systém návrhu, implementácie a hodnotenia a aplikačná bezpečnosť,</li><li>• riadenie, návrh, implementácia a hodnotenie bezpečnosti cloudových služieb poskytovateľov,</li><li>• hodnotenie účinnosti implementovaných kontrol a uskutočnenie zmien na základe skúseností,</li><li>• zabezpečenie, aby systémy prevádzkovej a obchodnej podpory poskytovali prístup k údajom zamestnancom poskytovateľa cloudových služieb na základe konkrétnych nájomcov odberateľa cloudových služieb, ktorým poskytujú služby.</li></ul>
Návrh a implementácia kontinuity služieb	<p>Činnosť navrhovania a implementácie kontinuity služieb zahŕňa:</p> <ul style="list-style-type: none"><li>• zvažovanie potenciálnych spôsobov zlyhania cloudovej služby a podporu infraštruktúry, zavedenie procesov obnovy, ktoré umožnia dostupnosť cloudovej služby v súlade s podmienkami SLA prostredníctvom techník, ako je load-balancing a replikácia.</li></ul>
Zabezpečenie súladu	<p>Činnosť zabezpečenia súladu sa sústreďí na implementáciu regulačného súladu a súladu s normami. Táto činnosť zahŕňa:</p> <ul style="list-style-type: none"><li>• zabezpečenie, aby implementácia cloudovej služby a jej podpornej infraštruktúry spĺňala požiadavky noriem, napríklad môžu byť normy požadované skupinou cieľových odberateľov alebo môžu byť vyžadované schémou certifikácie, ktorú si poskytovateľ zvolil na zabezpečenie služby,</li><li>• zabezpečenie, aby implementácia cloudovej služby a jej podpornej infraštruktúry (vrátane práce s údajmi) spĺňala regulačné požiadavky, ktoré môžu existovať pre služby alebo pre údaje uložené alebo spracovávané službou.</li></ul>

## 21.1.5 Vytváranie cloudových služieb

Popis	
Navrhovanie, tvorba a údržba komponentov služby	<p>Činnosť navrhovania, tvorby a údržby komponentov služby zahŕňa:</p> <ul style="list-style-type: none"><li>• navrhovanie a tvorbu softvérových komponentov, ktoré sú súčasťou implementácie služby,</li><li>• tvorbu funkcií, ktoré sú ponúkané používateľom služby, ktoré tiež zahŕňajú pripojenie komponentov služieb k systémom prevádzkovej podpory poskytovateľa, aby mohla byť implementácia služby monitorovaná a riadená,</li><li>• spracovávanie správ o problémoch týkajúcich sa prevádzky implementácie služby,</li><li>• poskytovanie fixných implementácií služieb,</li><li>• poskytovanie rozšírenia implementácií služieb.</li></ul>
Skladanie služieb	<p>Činnosť zloženia služieb sa zameriava na zloženie služieb pomocou aktuálnych služieb. Táto činnosť zahŕňa:</p> <ul style="list-style-type: none"><li>• tvorbu služieb formou zloženia jednej alebo viacerých existujúcich služieb poskytovaných inde,</li><li>• opis technických aspektov služby (funkčné rozhrania, SLA...),</li><li>• navrhovanie rozhrania odberateľa cloudovej služby predstavujúce zložené služby z viacerých ponúk poskytovateľa cloudových služieb,</li><li>• uskutočnenie skladania, ktoré môže zahŕňať sprostredkovanie, agregáciu alebo rozhodovanie o existujúcich službách.</li></ul>
Testovanie služieb	<p>Činnosť testovania služieb sa zameriava na testovanie zložiek a služieb vytvorených tvorcom cloudovej služby. Táto činnosť zahŕňa:</p> <ul style="list-style-type: none"><li>• uskutočňovanie testovania komponentov, ktoré tvoria implementáciu služby s cieľom zabezpečiť, aby tieto služby uskutočňovali funkcie úplne a správne,</li><li>• zabezpečenie interoperability cloudových služieb poskytovaných poskytovateľom cloudovej služby,</li><li>• testovanie, ktoré by malo zahŕňať kontrolu toho, či sú prevádzkové systémy podpory poskytovateľa cloudovej služby prevádzkované správne - preto je spravidla potrebné uskutočniť nejaké testovanie testovacej oblasti dátového centra poskytovateľa cloudových služieb.</li></ul>



### 21.1.6 Nasadenie cloudových služieb

Popis	
Definovanie prostredia a procesov	<p>Činnosť definovania prostredia a procesov sa zameriava na definovanie požadovaného technického prostredia a prevádzkových procesov využívaných v čase prevádzkovania služby. Táto činnosť zahŕňa:</p> <ul style="list-style-type: none"><li>• definovanie požadovaného technického prostredia z hľadiska počítačových, úložných a sieťových zdrojov, softvérových závislostí, vrátane konfigurácie,</li><li>• definovanie politík a procesov zvýšenia a zníženia využívania zdrojov ako reakcia na zmenu požiadavky na využívanie,</li><li>• zabezpečenie toho, aby cloudové služby spĺňali príslušné normy súvisiace s bezpečnosťou a obchodným súladom,</li><li>• definovanie procesov sledovania počas prevádzkovania služby, vrátane plánov na opravy, inovácie a migráciu.</li></ul>
Definovanie postupu nasadzovania	<p>Činnosť definovania postupu nasadzovania sa zameriava na definovanie krokov nasadenia služieb. Táto činnosť zahŕňa opis každého kroku potrebného na strane prevádzky a podporných tímov s cieľom nasadiť a pripraviť implementáciu služieb na využitie odberateľmi cloudových služieb.</p>
Definovanie a zber metrík	<p>Činnosť definovania a zberu meraní sa zameriava na definovanie meraní úrovne služieb a manažment. Táto činnosť zahŕňa:</p> <ul style="list-style-type: none"><li>• definovanie meraní, ktoré sú používané v súvislosti s prevádzkou cloudových služieb a ktoré sú spravidla zohľadnené v SLA súvisiacej s týmito službami,</li><li>• nastavenie merania pre každú cloudovú službu,</li><li>• definovanie spôsobu hlásenia a riadenia merania, najmä zabezpečenie toho, aby boli splnené ciele SLA.</li></ul>

### 21.1.7 Prevádzka cloudových služieb

Popis	
Príprava systémov	<p>Činnosť prípravy systémov sa zameriava na prípravu systémov prostredia poskytovateľa pre nasadenie a implementáciu nových cloudových služieb.</p> <p>Táto činnosť zahŕňa:</p>

	<ul style="list-style-type: none"><li>• zhodnotenie dopadu nasadenia a implementácie nových služieb alebo zvýšenia používania existujúcich služieb,</li><li>• úpravu alebo rozšírenie zdrojov v dátovom centre s cieľom splniť nové požiadavky.</li></ul>
Monitorovacie a administratívne služby	<p>Činnosť služieb monitorovania a administratívy sa zameriavajú na služby monitorovania a spravovania prislúchajúcej infraštruktúry, ktorá zahŕňa aj používateľské a systémové oprávnenia. Táto činnosť zahŕňa:</p> <ul style="list-style-type: none"><li>• monitorovanie služieb a infraštruktúry poskytovateľa cloudovej služby,</li><li>• zachytávanie udalostí a údajov, ktoré sú významné z hľadiska poskytovateľa a prezentovanie týchto údajov vo forme, ktorá je potrebná pre gestora cloudových služieb. Takéto informácie zahŕňajú položky, ako je využívanie cloudových služieb odberateľmi cloudových služieb a výdavky na poskytnutie týchto služieb,</li><li>• správa sieťovej infraštruktúry, vrátane routerov, serverov názvu domény, IP adries, virtuálnych súkromných sietí (VPN), firewallov a filtrovania obsahu,</li><li>• umiestňovanie a správa ukladania údajov,</li><li>• správa používateľských a systémových oprávnení,</li><li>• konfigurácia a údržba prevádzkových systémov a hypervízorov,</li><li>• správa virtualizačného prostredia,</li><li>• monitorovanie prostredia IKT poskytovateľa cloudových služieb s cieľom zabezpečiť, že funguje správne a že poskytnuté cloudové služby spĺňajú podmienky SLA,</li><li>• zaznamenávanie problémov, hlásenie problémov (čo môže zahŕňať správu zaslanú jednému alebo viacerým odberateľom) a sledovanie procesov riešenia problému až kým nie je problém vyriešený.</li></ul>
Riadenie aktív a zásob	<p>Činnosť riadenia aktív a zásob zahŕňa:</p> <ul style="list-style-type: none"><li>• sledovanie všetkých počítačových, úložných, sieťových a softvérových aktív a vzťahu medzi nimi. Toto zahŕňa sledovanie aspektov ako sú verzie a opravy, ako aj konfiguračné informácie, ak je to relevantné,</li><li>• vznik nových aktív a likvidácia starých aktív. Toto môže znamenať zabezpečenie, aby boli nové aktíva vhodné z hľadiska účelu a boli náležite skontrolované z hľadiska bezpečnosti a riadenia a môže to zahŕňať aj likvidáciu aktív, ktoré už nie sú potrebné. Môže to tiež zahŕňať vhodnú a bezpečnú likvidáciu akýchkoľvek aktív s údajmi.</li></ul>
Poskytnutie prepojitelnosti siete	<p>Činnosť poskytovania sieťovej konektivity zahŕňa nastavenie požadovaných sieťových pripojení a súvisiacich parametrov, vrátane pripojení medzi odberateľmi cloudovej služby a systémom poskytovateľa cloudovej služby a medzi jedným systémom poskytovateľa cloudovej služby a iným systémom poskytovateľa cloudovej služby. Toto môže</p>

	<p>zahŕňať zapojenie zariadení, ako je VPN alebo dedikovanie šírky pásma pripojenia.</p> <p>Sieťové možnosti zahŕňajú možnosť poskytovať primerane obmedzenú latenciu, šírku pásma, kvalitu služby a spoľahlivosť všetkých kategórií cloudovej služby a pre cloudové a nie cloudové účely v prípade NaaS.</p>
Poskytnutie sieťových služieb	Činnosť poskytovania sieťových služieb zahŕňa poskytovanie služieb súvisiacich so sieťou, ako je firewall alebo vyrovňovanie zaťaženia.
Poskytnutie služieb riadenia siete	<p>Činnosť poskytovania služieb riadenia siete sa zameriava na riadenie sieťovej infraštruktúry využívanej na poskytovanie cloudových služieb. Táto činnosť poskytuje metódy, nástroje a postupy umožňujúce prevádzku, správu, údržbu a poskytovanie infraštruktúry cloudovej siete. Zahŕňa tiež úlohy pre:</p> <ul style="list-style-type: none"><li>• zabezpečenie plnej funkčnosti siete,</li><li>• sledovanie zdrojov v sieti a ich umiestnenia,</li><li>• uskutočňovanie opráv a inovácií, napríklad, ak musí byť zariadenie vymenené alebo inovované s novými funkciami,</li><li>• konfigurovanie zdrojov v sieti na podporu cloudových služieb.</li></ul>
Poskytovanie cloudových služieb	<p>Činnosť poskytovania cloudových služieb zahŕňa všetky kroky potrebné na poskytovanie cloudových služieb odberateľom cloudových služieb. Činnosť poskytovania služieb zahŕňa prijatie a spracovanie vyvolania služby od používateľa s príslušným overením a overením totožnosti používateľa.</p> <p>Činnosť poskytovania služieb tiež zahŕňa nasledovné:</p> <ul style="list-style-type: none"><li>• riadenie procesu riešenia chyby služby,</li><li>• riadenie systému obchodnej podpory a systému prevádzkovej podpory,</li><li>• údržba služby a súvisiacej infraštruktúry,</li><li>• procesy automatizácie systému,</li><li>• riadenie dlhodobej kapacity a výkonu,</li><li>• inštalácia, konfigurácia a vykonávanie aktualizácie údržby na požadovanom hardvéri pre počítačové, úložné a sieťové kapacity pre dátové centrum poskytovateľa cloudových služieb,</li><li>• inštalácia a konfigurácia softvéru požadovaného na prevádzku dátového centra poskytovateľa cloudu a podpora implementácií cloudových služieb. Toto zahŕňa podľa potreby aplikáciu aktualizácií a inovácií, opráv pre tento softvér.</li></ul>
Nasadenie a poskytovanie služieb	Činnosť nasadenia a poskytovania služieb zahŕňa dosiahnutie fungovania implementácie služby a zabezpečenie jej dostupnosti v koncovom bode siete pre

	<p>používateľov cloudových služieb a dosiahnutie toho, aby bola schopná vyriešiť požiadavky na služby zo strany používateľov. Táto činnosť zahŕňa:</p> <ul style="list-style-type: none"><li>• sledovanie procesov nasadenia určeného pre túto službu.</li></ul> <p>POZNÁMKA - Táto činnosť tiež pokrýva procesy požadované pre zrušenie nasadenia a zrušenie poskytovania cloudovej služby.</p>
Riadenie úrovne služieb	<p>Činnosť riadenia úrovne služby sa zameriava na riadenie súladu s cieľmi SLA. Táto činnosť zahŕňa:</p> <ul style="list-style-type: none"><li>• monitorovanie meraní pre každú službu a ich porovnanie s cieľmi služby požadovanými v SLA,</li><li>• konanie, ak meranie nespĺňa hodnoty požadované SLA, ktorého cieľom je dosiahnuť, aby služba bola opäť v súlade so SLA, napríklad, sledovaním postupov stanovených manažérom nasadenia cloudovej služby,</li><li>• hlásenie problému, ak nie je možné udržať plnenie SLA.</li></ul>
Riešenie požiadaviek odberateľov	<p>Činnosť riešenia požiadaviek odberateľa zahŕňa:</p> <ul style="list-style-type: none"><li>• riešenie žiadostí o podporu, správ a incidentov odberateľa cloudových služieb, bez ohľadu na spôsob doručenia. Odberatelia môžu využívať rôzne spôsoby komunikácie, od fór cez emaily, systémy podpory odberateľa alebo webové portály až po komunikáciu s podpornými pracovníkmi poskytovateľa v reálnom čase.</li></ul>

## 21.2 Príloha č.2 - Popis aplikačných funkcií

### 21.2.1 Poskytovanie služieb

Popis	
Spracovanie požiadaviek a aktivácia a deaktivácia cloudových služieb	<p>Funkcionalita spracovania požiadaviek a aktivácie a deaktivácie cloudových služieb</p> <p>a) spracováva požiadavky z modulu manažmentu objednávok na základe dohody o poskytovanej úrovni cloudových služieb, dostupnosti zdrojov a konfiguračného modelu cloudových služieb,</p> <p>b) vytvára požiadavky pre vrstvu dodávania zdrojov ohľadom aktivácie a deaktivácie cloudových služieb,</p> <p>c) rozhoduje na základe príslušných politík o zvolení adekvátnej vrstvy, ak viaceré vrstvy dodávania zdrojov spĺňajú kritériá na vybavenie požiadavky,</p> <p>d) riadi aktiváciu a deaktiváciu cloudových služieb na základe príslušných pracovných postupov, ktoré synchronizujú nasadzovanie všetkých komponentov cloudovej služby s transakčnou konzistenciou,</p>

	<p>e) zapisuje stav cloudovej služby do modulu repozitára modelu cloudových služieb,</p> <p>f) iniciuje nápravné kompenzácie pri zlyhaní spracovania požiadaviek.</p>
Manažment stavu cloudových služieb	<p>Manažmentu stavu cloudových služieb</p> <p>a) spravuje monitorovanie cloudových služieb a prezentuje jeho výstupy vo forme prehľadov o stave cloudovej služby,</p> <p>b) ukladá a koreluje udalosti na úrovni cloudových služieb a podľa potreby ich eskaluje do obslužných procesov.</p>
Repozitár modelu cloudových služieb	<p>Repozitár modelu cloudových služieb</p> <p>a) definuje konfiguračné šablóny a atribúty cloudovej služby, pracovné postupy pre aktiváciu a deaktiváciu cloudovej služby,</p> <p>b) definuje hierarchiu cloudových služieb, zachytáva stavy cloudových služieb v reálnom čase a zabezpečuje mapovanie medzi cloudovými službami a potrebnými zdrojmi.</p>
Využívanie cloudových služieb	<p>Funkcionalita využívania cloudových služieb zbiera informácie o využívaní a meraní realizácie cloudovej služby a spracováva ich dávkovo alebo v reálnom čase pre každého odberateľa cloudovej služby.</p>
Modelovanie a návrh cloudových služieb	<p>Modelovanie a návrh cloudových služieb</p> <p>a) špecifikuje cloudové služby z pohľadu implementačných detailov a definuje informácie potrebné pre modul repozitár modelu cloudových služieb,</p> <p>b) navrhuje vhodné šablóny cloudových služieb a pracovných postupov s cieľom automatizácie riadenia životného cyklu cloudových služieb.</p>
Realizácia cloudových služieb	<p>Realizácia cloudových služieb</p> <p>a) konfiguruje virtuálnu infraštruktúru pre realizáciu cloudovej služby na základe informácií z modulu repozitára modelu cloudových služieb,</p> <p>b) realizuje cloudovú službu,</p> <p>c) implementuje možnosť zmeny realizácie cloudovej služby bez nutnosti jej opätovnej aktivácie,</p> <p>d) komunikuje s vrstvou dodávania zdrojov s cieľom využitia špecifických atribútov zdrojov pri realizácii cloudovej služby,</p> <p>e) overuje a pripravuje všetky parametre aktivácie a realizuje cloudovú službu.</p>
Monitorovanie cloudových služieb	Monitorovanie cloudových služieb

- a) konfiguruje monitorovanie cloudových služieb, ktoré nasledujú po aktivácii cloudovej služby,
- b) zhromažďuje udalosti a informácie o výkone v reálnom čase pre modul manažmentu stavu cloudových služieb.

### 21.2.2 Dodávanie zdrojov

Popis	
Katalóg zdrojov	<p>Katalóg zdrojov</p> <ul style="list-style-type: none"><li>a) poskytuje unifikované informácie o zdrojoch, obsahujúce typy ich kompozícií,</li><li>b) v reálnom čase poskytuje informácie zachytené modulmi pre modelovanie kapacít a stavov zdrojov,</li><li>c) v reálnom čase riadi vyváženie zaťaženia zdrojov na základe stavu zdrojov,</li><li>d) zabezpečuje mapovanie modelov poskytovania služieb na zdroje,</li><li>e) poskytuje funkciu riadenia životného cyklu využívaných softvérových licencií.</li></ul>
Monitorovanie využívania zdrojov	<p>Monitorovania využívania zdrojov</p> <ul style="list-style-type: none"><li>a) monitoruje zmeny spotreby a využívania zdrojov, špecifických pre konkrétnu službu alebo odberateľa cloudových služieb, s využitím modulu manažmentu životného cyklu zdrojov,</li><li>b) monitoruje dostupnosť a úroveň využívania zdrojov a informuje modul manažmentu životného cyklu zdrojov o ich skutočnom alebo predpokladanom preťažení.</li></ul>
Manažment životného cyklu zdrojov	<p>Manažment životného cyklu zdrojov</p> <ul style="list-style-type: none"><li>a) prijíma požiadavky z vrstvy poskytovania cloudových služieb a alokuje potrebné zdroje,</li><li>b) prijíma požiadavky na kapacity a výkon z modulu modelovania kapacít zdrojov a modulu návrhu šablón zdrojov,</li><li>c) prijíma informácie dostupnosti nových zdrojov a odosiela ich do vrstvy poskytovania cloudových služieb,</li><li>d) určuje potrebný počet a typy zdrojov na základe požiadavky na kapacitu cloudovej služby,</li><li>e) riadi spotrebu zdrojov a modul monitorovania využívania zdrojov,</li></ul>

	f) riadi zdroje s ohľadom na záťaž cloudovej služby a manažuje rozdeľovanie záťaže v reálnom čase s preddefinovanou logikou.
Stav zdrojov	<p>Stav zdrojov</p> <p>a) poskytuje modulu manažmentu stavu cloudových služieb informácie o zlyhaniach a chybách zdrojov, ktoré môžu potenciálne ovplyvniť kvalitu poskytovania cloudových služieb,</p> <p>b) sleduje a spracováva chybové stavy zdrojov a pri výskyte chyby iniciuje proces nápravy,</p> <p>c) udržiava v reálnom čase dostupné agregované správy riadenia udalostí ohľadom dostupnosti zdrojov a ich zlyhaní.</p>
Modelovanie kapacít zdrojov	<p>Modelovanie kapacít zdrojov</p> <p>a) slúži na prognózovanie využívania zdrojov a poskytuje informácie o kapacitách a výkonnosti zdrojov, a to v reálnom čase a v historickom spracovaní,</p> <p>b) zabezpečuje koordináciu modulov vrstvy dodávania zdrojov s ohľadom na pridelenie zdrojov, manažment záťaže a monitorovanie pre modelovanie požiadaviek na dodávku,</p> <p>c) zabezpečuje priradovanie požiadaviek na zdroje s dostupnými zdrojmi v module katalógu zdrojov a podľa potreby vytvára informácie pre obstarávanie dodatočných prostriedkov.</p>
Adaptér zdrojov a kontroly	<p>Adaptér zdrojov a kontroly</p> <p>a) poskytuje funkciu inteligentného virtualizačného prostredia, ktoré na základe typu hardvéru prekladá abstraktné výkonné operácie do konkrétnych inštrukcií,</p> <p>ktoré daný hardvér dokáže spracovať,</p> <p>b) transformuje požiadavky na pridelenie zdrojov na skutočné zdroje,</p> <p>c) v reálnom čase poskytuje aktualizovaný stav a informácie o využívaní konkrétneho hardvéru a softvéru pre modul katalógu zdrojov, modul monitorovania využívania zdrojov a modul stavu zdrojov.</p>
Návrhu šablón zdrojov	<p>Funkcionalita návrhu šablón zdrojov</p> <p>a) je zodpovedná za návrh zdrojov infraštruktúry a modifikácie špecifických typov zdrojov na základe využívaných cloudových služieb,</p> <p>b) je zodpovedný za návrh pracovných postupov pre modul manažmentu životného cyklu zdrojov, vrátane návrhu konfigurácie zdrojov, ich nasadzovania,</p>



	<p>manažmentu zaťaženia a automatizácie špecifických alebo všeobecných cloudových služieb,</p> <p>c) poskytuje návrhy pre modul katalóg zdrojov,</p> <p>d) navrhuje metriky pre modul manažmentu životného cyklu zdrojov na monitorovanie stavu prostriedkov.</p>
Pridelovanie zdrojov	<p>Funkcionalita realizácie pridelovania zdrojov</p> <p>a) prijíma informácie o kapacitných konfiguráciách zdrojov z modulu manažmentu životného cyklu prostriedkov,</p> <p>b) zabezpečuje mapovanie informácií o konfiguráciách zdrojov pre modul katalógu zdrojov,</p> <p>c) riadi alokáciu a konfiguráciu zdrojov pomocou modulu adaptéra zdrojov a kontroly.</p>

### 21.2.3Dopyt

Popis	
Prístup ku cloudovým službám	<p>Jedná sa unifikované webové používateľské rozhranie, poskytujúce prezentačnú funkciu najmä katalógu</p> <p>cloudových služieb podľa jednotlivých rolí používateľov tejto funkcionality.</p>
Dodržiavanie definovanej úrovne služieb	<p>Dodržiavanie definovanej úrovne služieb zabezpečuje správu požiadaviek pre vytváranie dohody o poskytovaní cloudových služieb.</p>
Manažment objednávok	<p>Manažment objednávok</p> <p>a) prijíma objednávky na operácie spojené s cloudovými službami,</p> <p>b) potvrdzuje správnosť objednávky v súlade s dohodou o poskytovanej úrovni cloudových služieb,</p> <p>c) rozkladá objednávku do adekvátnych služieb a ich atribútov na základe katalógu cloudových služieb,</p> <p>d) rozhoduje, ktoré cloudové služby sú poskytované tou-ktorou konkrétnou vrstvou, ak existujú viaceré vrstvy poskytovania cloudových služieb,</p> <p>e) preposiela požiadavky na služby do vrstvy poskytovania cloudových služieb,</p> <p>f) poskytuje informácie o stave objednávky a iniciuje nápravu v prípade zlyhania realizácie objednávky,</p>

	g) využíva katalóg cloudových služieb pre rozhodnutia, ktoré cloudové služby môžu byť ponúkané jednotlivému používateľovi.
Vytváranie správ o využívaní cloudových služieb	Transformuje interné informácie o využití služieb do zákaznických informácií. Zachováva históriu využívania. Môže vyvolať zmeny v kontrakte alebo upozornenia a proaktívne notifikácie.
Katalóg cloudových služieb	Funkcionalita katalógu cloudových služieb a) spravuje katalóg cloudových služieb, ktorý obsahuje informácie najmä o ponúkaných cloudových službách a ich možných kompozíciách, o dohodnutých podmienkach ako napríklad cene, špecifických atribútoch cloudových služieb, ktoré zabezpečujú dohodnuté podmienky, o mapovaní oprávnení používateľov k objednávaní konkrétnych cloudových služieb a o objednaných cloudových službách, b) priradzuje konkrétne charakteristiky z dohody o poskytovanej úrovni cloudových služieb ku konkrétnym cloudovým službám a obsahuje opis objednávkových a eskalačných procedúr, podmienok technickej podpory, špecifických zvýhodnení a podobne.
Manažment používateľov a prístupových práv	Manažment používateľov a prístupových práv a) zabezpečuje riadenie prístupu jednotlivých používateľov, vrátane administrátorov, a to najmä ich identifikáciu, autentifikáciu a autorizáciu, b) spravuje riadenie životného cyklu používateľských účtov, najmä ich vytváranie, modifikovanie a zrušenie.

## 21.3 Príloha č.3 – Riadenie aktív

### 21.3.1Zodpovednosť za aktíva

#### Prevádzkovateľ zabezpečí najmä:

- oboznámenie všetkých pracovníkov o právach a povinnostiach vyplývajúcich z prijatých bezpečnostných opatrení,
- vyhlásenie o mlčanlivosti všetkými osobami oprávnenými spracovávať údaje,
- fyzický prístup k prostriedkom informačného systému iba oprávneným osobám,
- elimináciu škodlivých vstupov z okolia informačného systému do informačného systému,
- odovzdávanie produktov informačných systémov, ktoré obsahujú osobitné osobné údaje externým organizáciám na ďalšie spracovanie tak, aby nemohlo dôjsť k úniku informácií,
- likvidovanie produktov informačného systému spôsobom zamedzujúcim úniku informácií,
- zamedzenie prístupu tretích strán ku všetkým údajom v informačnom systéme verejnej správy, ktoré sa považujú za aktíva, alebo umožnenie prístupu tretích strán k takýmto údajom

na základe zmluvy tak, aby nebola narušená bezpečnosť informačného systému verejnej správy a bezpečnostná politika povinnej osoby.

### 21.3.2 Klasifikácia informácií a dát

Aktívom vládneho cloudu je všetko, čo má pre prevádzkovateľa hodnotu v súvislosti so spracovávaním a uchovávaním informácií. Vlastníkom aktíva je prevádzkovateľ, respektíve vedúci organizačnej zložky, zodpovedný za aktívum v rámci svojej pôsobnosti. Vlastníctvo aktív nezahŕňa dáta, ktoré si odberateľ cloudových služieb umiestni na prevádzkované aktíva.

Z pohľadu architektúry je vládny cloud tvorený prvkami vo vrstvách:

- Backend a OOB vrstva  
Je rozhranie pre prevádzku, správcov a administrátorov cloudovej infraštruktúry v každom dátovom centre.
- Shared services vrstva  
Slúži na správu integrácii medzi IS a službami nasadenými v vládny cloud navzájom.
- Vrstva poskytovania IaaS, PaaS a SaaS služieb  
Logická vrstva pre prevádzkovanie služieb poskytovaných cloudom
- Vrstva publikovania služieb do externých sietí  
Predstavuje prístupový bod pre volania externých systémov na publikované služby

Nižšie sú uvedené aktíva podľa delenia:

1. Generické aktíva:
  - dátový nosič obsahujúci dáta v elektronickej forme
  - informácie a dokumenty v elektronickej podobe
  - výstupy dát a dokumentov v papierovej podobe
  - iné vstupno - výstupné zariadenia
  - e-mailová komunikácia
2. Systémové aktíva:
  - databázy a middleware
  - servery s určenými funkciami
  - veľkokapacitné pamäťové zariadenia (dátové polia, páskové knižnice)
3. Infraštruktúrne aktíva:
  - inštalčné médiá, aplikácií a softvéru
  - zálohy
  - kľúče priestorov a ochranných objektov využívaných v súvislosti s cloudom
  - IT špecialisti
4. Sieťové aktíva:
  - smerovače, prepínače
  - manažment siete
  - firewaly, IPS, dDoS ochrany
  - servery pre vzdialený prístup
  - sieťové rozhrania, interné alebo externé sieťové služby
5. Lokality:
  - Datacentrum Tajov
  - Datacentrum Kopčianska
  - jednotlivé pracoviská s prístupom na IS

### 21.3.3 Narábanie s nosičmi dát

Bezpečnostné požiadavky pre ochranu a narábanie s nosičmi dát:

- Všetky dáta musia byť zmazané pokiaľ prestala existovať odôvodnená potreba ich používania.
- Mazanie dát z dátových nosičov a prenosných dátových nosičov sa vykonáva bezpečným spôsobom s vopred zvolenou periodicitou, respektíve ich likvidácie v zariadeniach na to určených.
- Vyradené pevné disky a iné dátové nosiče musia mať zabezpečenú likvidáciu v príslušnom dátovom centre pomocou zariadení na to určených.
- Prenosné dátové nosiče ako CD, DVD, USB, Memory Keys, Cards, Sticks, ZIP disks a pod., ktoré obsahujú citlivé informácie, musia byť skladované na bezpečnom mieste.
- Prenosné dátové nosiče musia byť primerane označené, aby sa predišlo náhodnému odovzdaniu nepovolánym osobám. Označenie média nesmie identifikovať senzitívne informácie uložené na médiu.

## 21.4 Príloha č.4 – Riadenie a kontrola prístupov a identít

### 21.4.1 Biznis požiadavky na riadenie prístupov a identít

V súčasnosti je problematika správy prístupov a identít dôležitou témou v oblasti cloud computingu. V distribuovaných prostrediach je nevyhnutné zabezpečiť efektívnu autentifikáciu a autorizáciu pre zamedzenie prístupu neoprávnených používateľov k informáciám a tým zaistiť dôvernosť, integritu a dostupnosť informácií v prostredí cloudu. V rámci ďalšieho rozvoja vládneho cloudu je potrebné adresovať témy ako životný cyklus identít v cloud prostredí, identita ako služba a riadenie prístupov a identít v prostredí hybridného cloudu.

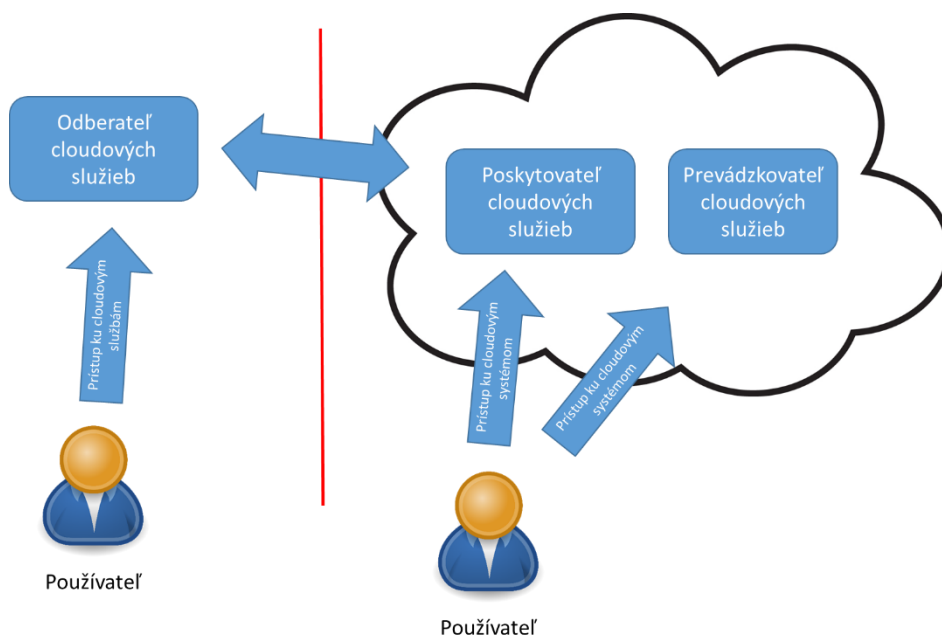
Biznis požiadavky riadenia prístupov a identít v cloud prostredí:

- Nasadenie používateľských, administrátorských a ďalších účtov pre cloudové aplikácie/služby.
- Riadenie oprávnenia identít (t.j. kto má prístup k čomu).
- Podpora single-sign on na základe štandardov.
- Podpora bezpečnostných smerníc a politík.
- Monitorovanie aktivít používateľov, logovanie a hlásenie na základe definovaných politík a štandardov.

### 21.4.2 Zodpovednosť a riadenie prístupov a identít pre jednotlivé role

V rámci prostredia vládneho cloudu sú zodpovednosti za riadenie prístupov a identít rozdelené nasledovne:

- Odberateľ cloudových služieb – zodpovedný za riadenie prístupov a identít používateľov cloudových služieb. Na úrovni IaaS má odberateľ cloudových služieb plnú zodpovednosť za definovanie a implementáciu politík, procesov, nástrojov a pod. v oblasti riadenia prístupov a identít. Na úrovni PaaS a SaaS je možný presun niektorých kompetencií na Poskytovateľa/Prevádzkovateľa cloudových služieb v závislosti od úrovni poskytovaných cloudových služieb.
- Poskytovateľ/Prevádzkovateľ cloudových služieb - zodpovedný za riadenie prístupov a identít používateľov cloudových systémov.



### 21.4.3 Riadenie prístupov k systémom a aplikáciám

Pre zachovanie dôvernosti, integrity a dostupnosti dát uložených v prostredí vládneho cloudu je nutné definovať mechanizmus riadenia prístupu z každej nasledovných vrstiev:

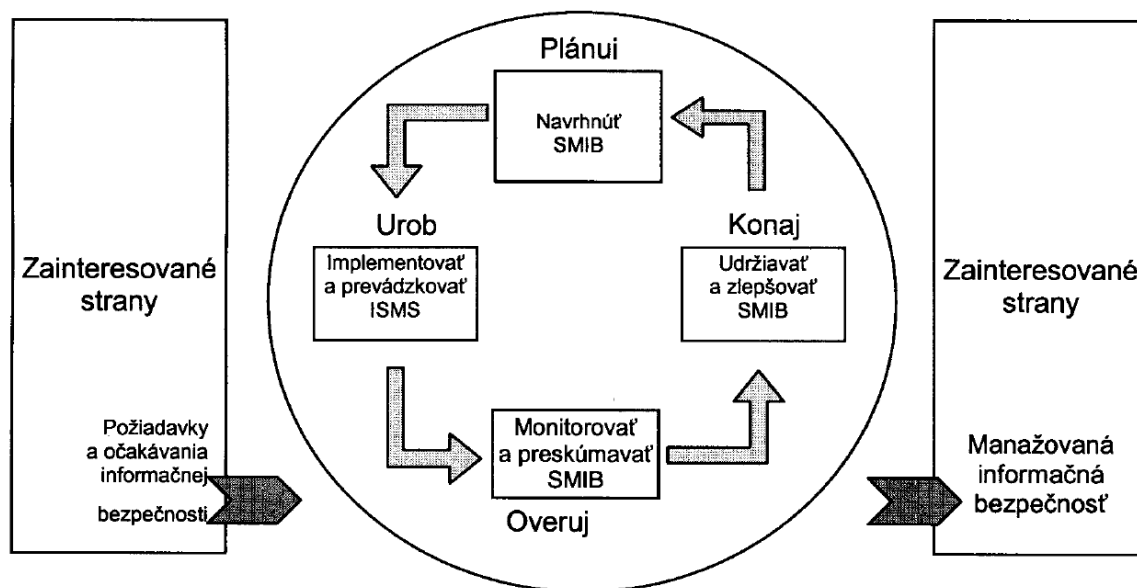
- Sieťová vrstva – na sieťovej úrovni nesmie mať používateľ cloudových služieb prístup k žiadnemu systému alebo časti siete bez toho že by mu to prístupové politiky umožnili
- Systémová vrstva – používateľ cloudových služieb nesmie mať prístup k systémom cloudu bez toho, že by mu to prístupové politiky umožnili
- Aplikačná vrstva – prístup ku cloudovým aplikáciám alebo službám je možný len na základe definovaných prístupových pravidiel
- Procesná vrstva – politiky riadenia prístupov a identít musia byť efektívne definované a aplikované pre umožnenie prístupu používateľom len k oprávneným procesom a funkciám
- Dátová vrstva – nutné je použitie politik riadenia prístupov a identít pre riadenie prístupov používateľov k dátam a súborovým systémom<sup>16</sup>.

## 21.5 Príloha č.5 – Bezpečnosť prevádzky

### 21.5.1 Prevádzkové procesy a zodpovednosť

Pre zabezpečenie efektívnej prevádzky bezpečnosti cloudového prostredia je nutné aplikovať procesný prístup manažmentu informačnej bezpečnosti. Medzinárodná norma STN ISO/IEC 27001 si v oblasti procesného riadenia osvojila model PDCA ("Plánuj-Urob-Overuj-Konaj"). Model PDCA je možné aplikovať na všetky procesy manažmentu informačnej bezpečnosti.

<sup>16</sup> Zdroj: Developing Interoperable and Federated Cloud Architecture: Manoj V. Thomas and K. Chandrasekaran



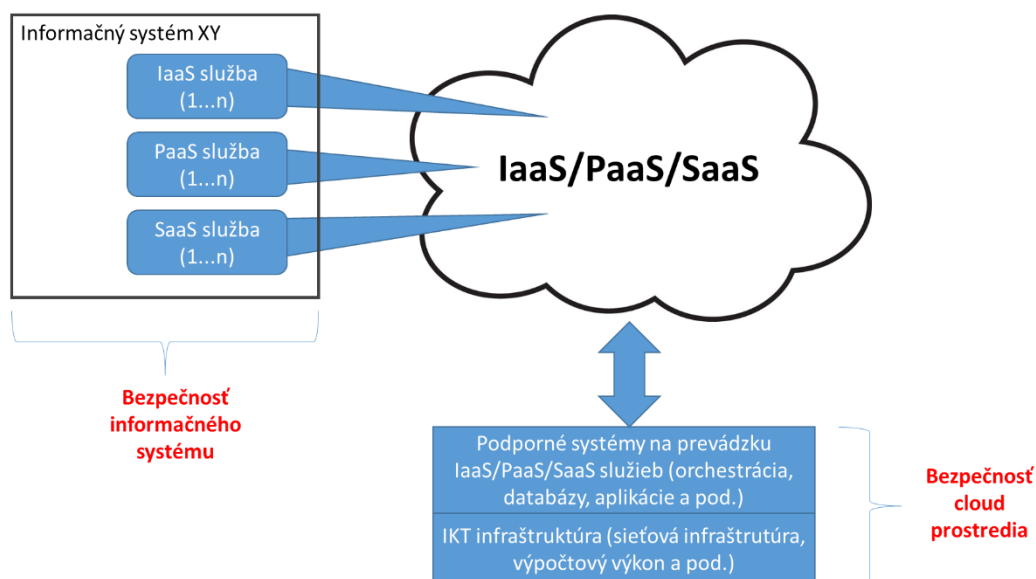
17

Problematickou oblasťou v cloud prostredí je rozdelenie kompetencií, resp. zodpovednosti za riešenie prevádzky bezpečnosti. Na dolu zobrazenom obrázku je uvedená koncepcia rozdelenia zodpovednosti za definovanie, implementáciu a správu bezpečnosti. Bezpečnosť je možné rozdeliť na 2 oblasti:

**Bezpečnosť informačného systému** – Odberateľ cloudových služieb si z katalógu služieb vládneho cloudu zvolí podľa svojich požiadaviek jednotlivé cloudové služby na základe ktorých implementuje/prevádzkuje informačný systém poskytujúci služby koncovým používateľom. Je v zodpovednosti Odberateľa definovať, implementovať a spravovať bezpečnosť na úrovni informačného systému.

**Bezpečnosť cloud prostredia** – Prevádzkovateľ cloudových služieb pri budovaní a správe cloudových služieb musí zabezpečiť definovanie, implementáciu a správu bezpečnosti na úrovni cloudových služieb, resp. cloudového prostredia.

<sup>17</sup> Zdroj: STN ISO/IEC 27001



Dôležitým aspektom pri prevádzke bezpečnosti cloudového prostredia je change management. Podľa ISO/IEC 27017 je odporúčané aby odberateľ cloudových služieb v rámci change management procesu zohľadnil zmeny vykonané na úrovni používaných cloudových služieb. Na druhej strane Poskytovateľ cloudových služieb by mal informovať odberateľa cloudových služieb o zmenách, ktoré by mohli mať nepriaznivý vplyv na cloudové služby.

### 21.5.2 Ochrana proti malwar-u

Narastajúcim problémom v cloudovom prostredí je nárast malware útokov. Na úrovni IaaS je zodpovednosť za ochranu proti malware útokom na strane Odberateľ cloudových služieb. Odberateľ je povinný implementovať a spravovať ochranu voči malware útokom. Na úrovni PaaS a SaaS prechádza táto zodpovednosť na prevádzkovateľa cloudových služieb.

Problematike ochrane proti malwaru adresuje ISO/IEC 27002 bod 12.4

### 21.5.3 Zálohovanie

Problematiku zálohovania adresuje ISO/IEC 27002 bod 12.3 a paragraf 39 vyššie spomenutého výnosu MF SR v nasledovnom rozsahu:

- a) zabezpečenie vytvorenia archivačnej zálohy a prevádzkovej zálohy podľa periodicity určenej v bezpečnostnej politike povinnej osoby, najmenej raz za týždeň, ak ide o prevádzkovú zálohu a najmenej raz za dva mesiace, ak ide o archivačnú zálohu,
- b) vyhotovenie archivačnej zálohy v dvoch kópiách,
- c) zabezpečenie vykonania testu funkcionality dátového nosiča archivačnej zálohy a prevádzkovej zálohy a v prípade nefunkčnosti, najmä pri nečitateľnosti alebo chybách pri čítaní, opätovné vytvorenie zálohy na inom dátovom nosiči,
- d) zabezpečenie vykonania testu obnovy informačného systému verejnej správy a údajov z prevádzkovej zálohy najmenej raz za jeden rok.



#### 21.5.4 Monitoring a logovanie

Zodpovednosť odberateľa cloudových služieb a poskytovateľa/prevádzkovateľa cloudových služieb za monitoring a logovanie je závislá od typu používanej cloudovej služby. Napríklad na úrovni IaaS je poskytovateľ/prevádzkovateľ zodpovedný za logovanie a monitoring na úrovni infraštruktúrnych komponentov a odberateľ za logovanie a monitoring virtuálnych serverov a aplikácií.

Problematiku monitoringu a logovania adresuje ISO/IEC 27002 bod 12.4.

#### 21.5.5 Riadenie prevádzkového softvéru

Riadenie prevádzkového softvéru cloud infraštruktúry je v zodpovednosti prevádzkovateľa cloudovej infraštruktúry. Zo strany prevádzkovateľa cloudovej infraštruktúry je potrebné vytvoriť a udržiavať zdokumentované postupy pre správu inštalácie a aktualizácie prevádzkovaného softvéru. Riadenie prevádzkového softvéru inštalovaného zo strany Odberateľa cloudových služieb prostredníctvom IaaS služieb je v zodpovednosti odberateľa cloudových služieb.

Problematiku riadenia prevádzkového softvéru adresuje ISO/IEC 27002 bod 12.5.

#### 21.5.6 Riadenie technických zraniteľností

Riadenie technických zraniteľností cloud infraštruktúry je v zodpovednosti prevádzkovateľa cloudovej infraštruktúry. Zo strany prevádzkovateľa cloudovej infraštruktúry je potrebné zabezpečiť:

- pravidelnú aktualizáciu inventáru prevádzkovaných aktív
- zavedenú a pravidelne aktualizovanú politiku obsahujúcu rozdelenie zodpovedností za riešenie riadenia technických zraniteľností,
- pravidelný monitoring zverejnených zraniteľností
- zavedený a pravidelne aktualizovaný proces na manažment rizík technických zraniteľností

Riadenie technických zraniteľností systémov využívajúcich cloudové služby je v zodpovednosti odberateľov cloudovej infraštruktúry.

Problematiku technických zraniteľností adresuje ISO/IEC 27002 bod 12.6.

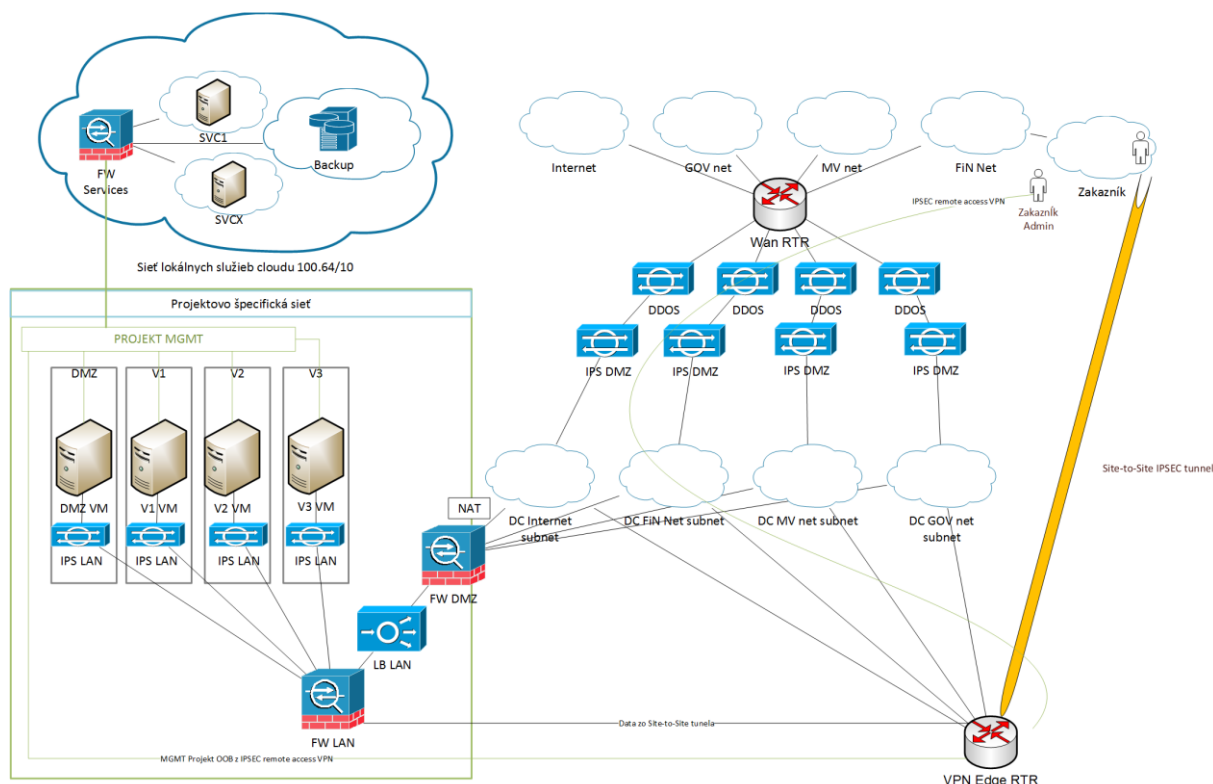
#### 21.5.7 Audit

Zo strany prevádzkovateľa cloudových služieb je potrebné zabezpečiť realizáciu pravidelných auditov cloud infraštruktúry. V prípade že audit si vyžaduje aktivity, ktoré môžu mať negatívny vplyv na kvalitatívne parametre cloudových služieb tak je v zodpovednosti prevádzkovateľa cloudových služieb informovať odberateľov cloudových služieb.

Problematiku auditu bezpečnosti prevádzky adresuje ISO/IEC 27002 bod 12.7.

## 21.6 Príloha č.6 - Návrh komunikačnej infraštruktúry z pohľadu bezpečnosti

Komplexný prehľad o bezpečnostných prvkoch a zónach ukáže logická schéma sieťovej topológie projektu poskytovaná ako infraštruktúrna služba. Použité sú kombinácie rôznych bezpečnostných prvkov (firawally, IPS, DDoS), rôznych vendorov a na rôznych vrstvách ochrany (interné, perimetrové).



Požiadavky na bezpečnosť komunikačnej infraštruktúry sú popísané v dokumente čiastkovej štúdie uskutočniteľnosti „IKT infraštruktúra pre IaaS“ nasledovne:

*Cloudové dátové centrum musí obsahovať zariadenia a systémy schopné poskytovať ochranu, ktorá prestupuje celou sieťovou infraštruktúrou až po koncové virtuálne zariadenia. Všetky časti pritom musia spolupracovať pri ochrane dostupnosti, integrity a bezpečnosti komunikácie, sieťových služieb a koncových zariadení. Bezpečnostné komponenty musia byť schopné reagovať automaticky na v súčasnosti známe útoky a pomôcť pri identifikácii neznámych útokov. Bezpečnostný systém musí byť viacstupňový, vyžadujúci si kontinuálnu a permanentnú starostlivosť bezpečnostných expertov. Napriek tomu, že je využitá viacstupňová obrana, je potrebné rešpektovať bezpečnostnú politiku a neustále sledovať a dodržiavať aj nové bezpečnostné trendy. K predchádzaniu útokov patrí aj zaškolená a neprestajne z hľadiska bezpečnosti školená obsluha. Kontrolu dodržiavania pravidiel je potrebné kontrolovať nezávislými bezpečnostnými auditmi spolu s penetračnými testami.*

Z pohľadu bezpečnosti komunikačnej infraštruktúry je nutné využívať bezpečnostné komponenty:

### *21.6.1 Intrusion Prevention System (IPS)*

Cloud obsahuje zariadenia schopné aktívnej reakcie pri narušení bezpečnosti – IPS, ktoré má možnosť monitorovať a aktívne prerušiť prebiehajúci útok alebo zabrániť bezpečnostnej hrozbe.

IPS deteguje a blokuje spojenia útočníka, je schopné zabrániť záškodnej sieťovej činnosti, detegovať a zabrániť DOS útokom, ale aj hrozbám ako sú botnety, malware, zero-day útoky, takisto je schopné vytvárať reputáciu hrozieb.

Systém prevencie pred prienikom do siete (IPS), ponúka presné detegovanie škodlivých dátových prenosov s možnosťou zastavenia útokov na 3 až 7 vrstve, vrátane detekcie anomálií, korelovania udalostí a rýchlej analýzy rizík na senzore. Sleduje tiež aplikácie, používateľov, zariadenia, operačné systémy, služby, procesy, sieťové správanie a ostatné hrozby.

Identifikácia hrozieb IPS systému uskutočňuje hĺbkovú kontrolu a analýzu prenosu na 3 až 7 vrstve:

- stavové rozpoznávanie vzoriek identifikujúce útoky založené na zraniteľnosti stavovov rekonštrukciou prenosu cez viac paketov pre všetky protokoly,
- analýza a detekcia hostov, operačných systémov, aplikácií, sieťových zariadení, potenciálnych zraniteľností, sieťových anomálií, typy súborov a protokolov,
- detekcia anomálií sieťových prenosov (ICMP a UDP flood, TCP SYN flood),
- detekcia anomálií protokolov (napr. HTTP odpoveď bez dotazu, kontrola súladu s RFC pre HTTP metódy),

### *21.6.2 Firewall*

Firewall poskytuje stavovú inšpekciu a kontrolu sieťovej prevádzky, ako aj možnosť kontroly na L2 a L3, vrátane tradičného blokovania portov.

### *21.6.3 Bezpečnosť virtuálnych strojov*

Prehľadný a robustný systém bezpečnosti zahŕňa nasadenie kontroly vnútornej prevádzky medzi virtuálnymi zariadeniami. Kontrola vnútornej sieťovej prevádzky prebieha na vnútorných FW a IPS. Hĺbková kontrola sieťovej prevádzky tak prebieha priamo z cloudovej infraštruktúry. Minimalizuje sa riziko šírenia útokov medzi virtuálnymi zariadeniami a šírenie útoku z virtuálneho zariadenia k hostom infekcie a nákazy.

### *21.6.4 Systém riadenia prístupov*

Na zabezpečenie správy zariadení s riadeným prístupom je implementovaný autentifikačný, autorizačný a účtovací systém (ďalej označovaný ako AAA). AAA systém zabezpečuje centrálny prvok pre overovanie správcov a zariadení pripájajúcich sa do infraštruktúry.

### *21.6.5 Monitorovanie bezpečnostných incidentov*

SIEM (Security Information and Event Management), aplikácia pre monitorovanie systémov a infraštruktúry z pohľadu bezpečnostných udalostí. Bezpečnostné incidenty sú vyhodnocované zo zberu údajov.

Komplexné riešenie zahŕňa tieto aspekty:

- hĺbková analýza dátových tokov,
- jednotné rozhranie pre všetky monitorované aktivity (konsolidácia) a komplexný pohľad na bezpečnosť cloudu,

- schopnosť ohlasovania alarmov,
- schopnosť definovania a ladenia sledovaných aktivít,
- korelácia dát,
- integrácia aktivít pre audit a dosiahnutie zhody s medzinárodnými bezpečnostnými štandardmi,
- uchovanie logov, bezpečnostné logy, logy bezpečnostných brán, záloha logov.

### 21.6.6 Network behaviour anomaly detection

NBAD (Network behaviour anomaly detection), systém poskytuje viditeľnosť do dátových tokov a sleduje anomálie. Je schopný snímať dátové toky zo zariadení na to určených. Následkom sledovania dátového toku je možné detegovať aj tzv. "day-zero" útoky, APT (advanced persistent threat – pokročilé ohrozenia), DDoS (distribúované útoky zahltením), vnútorné hrozby a ostatné problémy prekračujúce perimetrovú obranu. Systém spolupracuje a je vyhodnocovaný do systému SIEM.

## 21.7 Príloha č.7 – Hybridný Cloud - Návrh užívateľských scenárov Pre Hybridný Vládny Cloud

### 21.7.1 Všeobecne k navrhovaným scenárom

Navrhované scenáre predstavujú minimálnu množinu služieb potrebných pre realizáciu koncepcie NKIVS a jej strategického zámeru rozšírením o koncept Hybridného vládneho cloudu.

Popis služieb je len schematický, pre definíciu jednotlivých parametrov služieb bude potrebné definovať metriky služieb a parametre, ktoré budú voliteľnou zložkou služieb.

Zoznam služieb je rozdelený do základných kategórií:

- A. Služby v oblasti rozšírenia výpočtového výkonu
- B. Služby v oblasti diskového priestoru, ukladania dát, zálohovania a archivácie
- C. Služby v oblasti PaaS
- D. Služby v oblasti SaaS
- E. Služby v oblasti poskytovania služieb autentifikácie a bezpečnosti
- F. Služby pre DEV/TEST prostredie
- G. Služby v oblasti „Big Data“ a „Open Data“

### 21.7.2 Služby v oblasti rozšírenia výpočtového výkonu

V tejto kategórii uvádzame príklady služieb, ktoré umožňujú preklenúť požiadavky na zvýšenú výpočtovú kapacitu pre potreby organizácie. Môže sa jednať o vytvorenie jednoduchého virtuálneho stroja, ale aj o komplexnejšiu farmu alebo množinu zdrojov, ktorá poskytne vyššiu a škálovateľnejšiu výpočtovú kapacitu.

Č.	Názov	Popis
1	Virtuálny server – vytvorenie a prevádzka	Vytvorenie konfiguráciou nového alebo z obrazu
2	Virtuálny server – riadenie výkonnosti	Zmena počtu CPU / cores; zmena dostupnej RAM
3	Virtuálny server – vytvorenie a uloženie obrazu	Vytvorenie obrazu (snapshot) a jeho uloženie

4	Farma virtuálnych serverov (scale sets)	Vytvorenie konfiguráciou nového alebo z obrazu (template)
---	---	---

#### 21.7.2.1 Služby v oblasti diskového priestoru, ukladania dát, zálohovania a archivácie

Obdobne, ako služby na rozšírenie výpočtového výkonu, sú koncipované aj služby na rozšírenie diskového priestoru. Tieto služby sú špecificky rozšírené o možnosti archivácie, zálohovania údajov a zároveň aj o HSM. Pri definícii špecifikácie služby sa dá zväžiť lokálna alebo GEO redundancia údajov.

Č.	Názov	Popis
1	Virtuálny disk – spustenie a prevádzka	Služba pre vytvorenie diskového priestoru konfiguráciou alebo z obrazu pripojiteľného napr. k virtuálnemu serveru
2	Virtuálny disk – vytvorenie a uloženie obrazu	Vytvorenie obrazu a jeho dočasné uloženie (pozastavenie dostupnosti)
3	Archivácia dát a dokumentov	Služba pre dlhodobé uloženie dát a dokumentov, napr. pre spisovú službu, prípadne záznam log súborov.
4	Zálohovanie údajov	Zálohovanie dát umožňujúci využitie zálohovacích nástrojov z jednotlivých infraštruktúrnych zdrojov.
5	Hierarchický Manažment Dát	Kombinácia tzv. rýchlych údajov s údajmi, ktoré sú používané menej často a s údajmi určeným na archiváciu a zálohovanie (náhrada páskových knižníc).

#### 21.7.2.2 Služby pre oblasť PaaS

Služby pre oblasť PaaS dopĺňajú základnú množinu PaaS služieb a umožňujú ekonomicky efektívne a časovo dostupne splniť potreby organizácie v jednotlivých typologických „platformách“, nad ktorými si organizácia dokáže pripraviť vlastný informačný systém alebo služby v prostredí Gov Cloudu. Dôležité je citlivo posúdiť charakter údajov, ktoré môže takto koncipovaná služba spracovať.

Č.	Názov	Popis
1	Prezentačná vrstva	Vytvorenie bezpečnej prezentačnej platformy (typicky „front-end“, web sídlo, bezpečný portál), ktorá umožní bezpečne prezentovať výstupy ďalších služieb.
2	Load Balancer	Platformová služba na rozdelenie záťaže, prípadne požiadaviek na obsluhu medzi ďalšie služby.
3	Aplikačná vrstva	Platformová služba, ktorá umožňuje implementovať aplikačnú logiku pre špecifický informačný systém.
4	Integračná a Orchestračná vrstva	Platformová služba pre integráciu a riadenie výmeny údajov medzi ďalšími službami.

5	Databázová Vrstva	Služba na správu dát, ktorá môže byť koncipovaná ako jednoduchá databáza, alebo komplexnejší dátový sklad, prípadne farma.
6	Analytika a Reporting	Analytické spracovanie údajov a pripravenie špecifických výstupov – dátové skupiny, dashboardy.
7	Monitoring Aplikácií, Správa Udalostí a Log Súborov, Správa Mobilných Zariadení	Monitoring aplikácií a infraštruktúrnych zdrojov v hybridnom prostredí. Správa a konfigurácia prístupu mobilných zariadení (MDM). Možnosti správy udalostí a vyhodnocovanie / analytika obsahu log súborov.

#### 21.7.2.3 Služby pre oblasť SaaS

SaaS služby budú dopĺňať SaaS aplikácie poskytované ako základná množina. Podmienkou poskytovania týchto služieb je súlad s legislatívou SR a EU a zároveň natívna podpora Slovenského Jazyka (lokalizácia). Nižšie uvádzame len niektoré príklady služieb.

Č.	Názov	Popis
1	Kolaboračné systémy	Služba na spoluprácu medzi pracovníkmi organizácie štátnej správy.
2	Registratúra	Služba umožňujúca jednoducho implementovať systém podaní a riadiť životný cyklus podaní.
3	Spisová služba	Správa dokumentov a spisov, distribúcia na spracovanie a archivácia dokumentov.
4	Elektronické Aukcie	Služby na implementáciu elektronických aukcií.
5	Správa Vzťahov S Dodávateľmi (CRM)	Služby umožňujúce implementovať systémy na správu vzťahov s dodávateľmi.

#### 21.7.2.4 Služby v oblasti poskytovania služieb autentifikácie a bezpečnosti

Služby v tejto kategórii umožňujú implementovať základné bezpečnostné mechanizmy, ktoré sú často používané ďalšími službami pre koncepty interoperability a takisto môžu byť používané medzi viacerými organizáciami.

Ďalší platný scenár je spolupráca a ochrana „assets“ pri práci s externými subjektami.

Č.	Názov	Popis
1	IAM	Služba správy identít a prístupov, federačné mechanizmy.
2	Adresárová služba - SSO	Jednotný prístup k službám, aplikáciám a zdrojom na základe adresárových informácií.
3	Manažment kľúčov	Služba pre riadenie životného cyklu kľúčov (prístupové, šifrovacie) a ich ochrana – HSM
4	Ochrana	Antivírusová ochrana, ochrana pred malware

#### 21.7.2.5 Služby pre DEV/TEST prostredie

Služby pre DEV/TEST prostredie môžu byť komponované z už uvedených služieb v predchádzajúcich kapitolách, cieľom je však vývoj novej služby, čiže údaje a dátové vzorky použité pri takomto vývoji musia byť pripravené – anonymizované, očistené od prípadných citlivých častí a minimalizované pre vývoj a prípadné testovanie.

#### 21.7.2.6 Služby v oblasti „Big Data“ a „Open Data“

V tejto oblasti uvádzame príklady služieb v oblasti spracovania a analýzy Big Data a zároveň aj služby pre Open Data, ktoré sú štandardne dostupné pre občanov a externé subjekty. Táto oblasť pokrýva otvorené dáta, ktoré nepodliehajú špeciálnemu režimu spracovania a prístupu.

Č.	Názov	Popis
1	Hadoop Big Data	Služba na správu a analýzu vzoriek údajov, s mechanizmami škálovateľnosti typicky pomocou ETL.
2	Elastické Databázové Služby	Služba na správu a analýzu vzoriek údajov, s mechanizmami škálovateľnosti typicky pomocou ETL.
3	CKAN Plaforma pre Open Data	Štandardizovaná platforma pre implementáciu Open Data konceptu.
4	Socrata Dashboard pre Open Data	Štandardizovaná platforma pre implementáciu Open Data konceptu.
5	Aplikácie Pre Aktívnych Občanov	Služby, ktoré používajú koncept „Open Data“ pre občanov a umožňujú ich aktívnu angažovanosť vo verejnej správe.
6	GIS a Portálové aplikácie pre Občanov	Služby pre GIS systémy a portálové systémy pre občanov, kde môžu participovať jednotliví občania – fotky, komentáre, postrehy, môžu byť spojená aj s aplikáciami pre mobilné zariadenia.
7	Správa a Riadenie Spotreby Energii	Služby na implementáciu Smart Cities, Smart Buildings, riadenie spotreby energie a úspor.

#### 21.7.3 Návrh komunikačných mechanizmov Pre Hybridný Government Cloud

Každý z potenciálnych poskytovateľov cloudových služieb musí spĺňať princípy bezpečného pripojenia cloudu a samozrejme naplnenie týchto princípov bude predmetom certifikácie daného poskytovateľa pre možnosť poskytnutia služieb pre hybridný vládny cloud.

Medzi základné princípy platí ochrana verejne prístupných zdrojov a to hlavne z dvoch pohľadov:

- Prevencia a ochrana proti DDoS - poskytovateľ cloudových služieb musí implementovať distribuovanú fyzickú vrstvu ochrany „vstupných bodov“ do cloudu priestoru. DDOS útok je typicky vedený z viacerých uzlov za účelom znefunkčnenia určitej služby. Okrem štandardne poskytnutej ochrany a prevencie proti DDoS, musí mať zákazník aj možnosť konfigurácie dodatočných vrstiev a mechanizmov ochrany, ktoré mu umožňujú zabezpečiť dostupnosť jeho služieb.
- Ochrana a zabezpečenie koncových bodov jednotlivých cloudových služieb – takéto body umožňujú použitie mechanizmu verejných IP adries a prípadne portov, ktoré sú vystavené do verejného priestoru. Tieto body umožňujú preklad adries a vstup do interného priestoru cloudu. Ochranné mechanizmy musia zabezpečovať jednoznačný preklad vonkajších zdrojov na vnútorné zdroje, kontrolu a obmedzenie komunikácie a prípadne nastavenia postupu, ako je komunikácia prekladaná na vnútorné zdroje.



Akonáhle sa komunikácia dostane do vnútorného priestoru (virtuálne siete – privátne zákaznícke siete) poskytovateľa cloudových služieb, zákazník musí mať možnosť opäť implementovať viacero vrstiev na ochranu služieb – kontrola a izolácia komunikácie, bezpečné možnosti komunikácie a pripojenia, obmedzenia vo forme ACL, firewally atď.

Samotný poskytovateľ cloudových služieb musí zároveň poskytovať rozhranie na správu jednotlivých služieb – cez samoobslužný portál a prípadne API s možnosťami kontroly spotreby jednotlivých služieb, prehľadu prípadného účtovania a prostriedky na prípadný audit používania služieb.

## 21.8 Príloha č.8 – PaaS – Zdrojové dáta

IKT - platformy.xlsx<sup>18</sup>

IKT - server sw.xlsx<sup>19</sup>

## 21.9 Príloha č.9 – Ceny IaaS služieb vládneho cloudu - prepočet

Cenník - prepocet podla - OPII Usmernenie k CBA - Cloud.optimizer.xlsx<sup>20</sup>

### 21.10 Príloha č.10 – Ceny IaaS služieb vládneho cloudu

Skupina služieb	Názov služby	Cena/mesiac s DPH
<b>Virtuálny server</b>		
	Virtuálny server - "x86,WINDOWS,xSmall" - 1xVCPU; 2GB RAM; 32GB system disk TIER 2	67,10 €
	Virtuálny server - "x86,WINDOWS,Small" - 1xVCPU; 4GB RAM; 40GB system disk TIER 2	98,37 €
	Virtuálny server - "x86,WINDOWS,Medium" - 2xVCPU; 8GB RAM; 80GB system disk TIER 2	138,77 €
	Virtuálny server - "x86,WINDOWS,Large" - 4xVCPU; 16GB RAM; 100GB system disk TIER 2	260,43 €
	Virtuálny server - "x86,WINDOWS,xLarge" - 8xVCPU; 32GB RAM; 128GB system disk TIER 2	500,34 €
	Virtuálny server - "x86,WINDOWS,xxLarge" - 8xVCPU; 64GB RAM; 128GB system disk TIER 2	616,30 €
	Virtuálny server - "x86,Red Hat Linux,xSmall" - 1xVCPU; 1GB RAM; 20GB system disk TIER 2	60,49 €

<sup>18</sup> Dostupné tiež online <https://1drv.ms/x/s!Aog1mU4LEkSLgXbGwo7KHq0YYivv>

<sup>19</sup> Dostupné tiež online <https://1drv.ms/x/s!Aog1mU4LEkSLgXeHW6OnKUYWboio>

<sup>20</sup> Dostupné tiež online <https://1drv.ms/x/s!Aog1mU4LEkSLgljGL5Mz0JngoiMj>



Virtuálny server - "x86,Red Hat Linux,Small" - 1xVCPU; 4GB RAM; 40GB system disk TIER 2	93,59 €
Virtuálny server - "x86,Red Hat Linux,Medium" - 2xVCPU; 8GB RAM; 60GB system disk TIER 2	126,68 €
Virtuálny server - "x86,Red Hat Linux,Large" - 4xVCPU; 16GB RAM; 80GB system disk TIER 2	241,97 €
Virtuálny server - "x86,Red Hat Linux,xLarge" - 8xVCPU; 32GB RAM; 100GB system disk TIER 2	466,83 €
Virtuálny server - "RISC,AIX,xSmall" - 1xVCPU; 2GB RAM; 20GB system disk TIER 2	188,09 €
Virtuálny server - "RISC,AIX,Small" - 1xVCPU; 4GB RAM; 40GB system disk TIER 2	284,99 €
Virtuálny server - "RISC,AIX,Medium" - 2xVCPU; 8GB RAM; 80GB system disk TIER 2	387,58 €
Virtuálny server - "RISC,AIX,Large" - 4xVCPU; 16GB RAM; 100GB system disk TIER 2	758,06 €
Virtuálny server - "RISC,AIX,xLarge" - 8xVCPU; 32GB RAM; 128GB system disk TIER 2	1 495,60 €
Virtuálny server - "RISC,CentOS,xSmall" - 1xVCPU; 2GB RAM; 20GB system disk TIER 2	188,09 €
Virtuálny server - "RISC,CentOS,Small" - 1xVCPU; 4GB RAM; 40GB system disk TIER 2	284,99 €
Virtuálny server - "RISC,CentOS,Medium" - 2xVCPU; 8GB RAM; 80GB system disk TIER 2	387,58 €
Virtuálny server - "RISC,CentOS,Large" - 4xVCPU; 16GB RAM; 100GB system disk TIER 2	758,06 €
Virtuálny server - "RISC,CentOS,xLarge" - 8xVCPU; 32GB RAM; 128GB system disk TIER 2	1 495,60 €
<b>Diskový priestor</b>	
Diskový priestor - "TIER 1" - min. 1 GB, max. 256 GB, max 1280 IOPS	0,64 €
Diskový priestor - "TIER 2" - min. 1 GB, max. 1000 GB, max 150 IOPS	0,29 €
Diskový priestor - "TIER 3" - min. 1 GB, max. 2000 GB, max 100 IOPS	0,16 €
<b>Služba pripojenia do špecifickej siete</b>	

Poskytovanie sieťového pripojenia - Internet	
Poskytovanie sieťového pripojenia - GOVNET	75,91 €
Poskytovanie sieťového pripojenia - KTI,KTI2	75,91 €
Poskytovanie sieťového pripojenia - MVNET	75,91 €
<b>Sieťové služby</b>	
Sieťové služby - Poskytovanie preddefinovaného sieťového modelu a bezpečnostných pravidiel	1,29 €
Sieťové služby - Vytvorenie FW pravidiel	- €
Sieťové služby - Pridelenie virtuálnej IP	- €
Sieťové služby - Poskytovanie služby load balancingu	0,23 €
<b>Zálohovanie</b>	
Zálohovanie virtuálneho servera	11,36 €

## 21.11 Príloha č.11 – Prehľad a popis modulov a služieb projektu DCOM

Podstatou črtou všetkých SaaS služieb poskytovaných v rámci projektu DCOM je integrácie na referenčné registre je zabezpečenie aktuálnych údajov v riešení IS DCOM. Existujúce dátové integrácie na ostatné IS VS podstatným spôsobom zvyšujú pridanú hodnotu eSlužieb DCOM, pretože pre pracovníka obce, ako aj pre občana, uľahčujú a skracujú čas potrebný na zadanie podania, resp. na vytvorenie rozhodnutia. K dispozícii sú integrácie na Register fyzických osôb, Register adries, Evidenciu vozidiel, Kataster nehnuteľností, Register právnických osôb, Sociálnu poisťovňu, Finančnú správu a Ministerstvo práce sociálnych vecí a rodiny.

### 21.11.1 Modul Dane a poplatky

Rieši problematiku výberu a správy miestnych daní a poplatkov podľa Zákona č. 563/2009 Z. z. o správe daní (daňový poriadok) a o zmene a doplnení niektorých zákonov) a Zákona č. 582/2004 Z. z. o miestnych daniach a miestnom poplatku za komunálne odpady a drobné stavebné odpady v znení neskorších predpisov.

### 21.11.2 Modul Evidencie

Patria sem služby, ktoré riešia rôzne oblasti verejného života. Služby spravidla čítajú zdrojové dáta z back-office-ového systému (evidencia obyvateľov...). Nad týmito údajmi je následne vybudovaná nadstavba pre elektronizáciu a zefektívnenie pôvodného procesu. V rámci generického procesu je súčasťou dotknutých služieb aj platba.

### 21.11.3 Modul Majetok a prenajímanie

Modul poskytuje podporu pre predaj a prenájom nehnuteľného a hnutel'ného majetku obce, ktoré sa riadia zákonmi „Zákon č. 138/1991 Zb. o majetku obcí“ a „Zákon č. 182/1993 Z. z. o vlastníctve bytov a nebytových priestorov“.

### 21.11.4 Modul Obstarávanie

Modul obsahuje evidencie o verejnom obstarávaní (VO) obce/mesta a logiku pre spracovanie dát a zabezpečenie ich integrity. Zabezpečí tiež informovanie o VO, možnosť elektronického predloženia ponuky a všetkých sprievodných podkladov a dokumentov vyžadovaných súťažnými podmienkami konkrétneho VO.

### 21.11.5 Modul Platby

Tento modul je integrálnou súčasťou iných modulov IS DCOM, ktoré vyžadujú od občanov zaplatenie dane, poplatku, sankcie, penále, pokuty. Jednou skupinou platieb sú dane, druhou skupinou sú správne poplatky.

### 21.11.6 Modul Sociálne služby

Zabezpečuje spracovanie sociálnej agendy obcou. Poskytuje prehľad o osobách, ktoré rieši odbor sociálnych vecí obce a zároveň prehľad všetkých dôležitých informácií pre podporu rozhodovania v týchto záležitostiach.

### 21.11.7 Modul eDemokracia

Tento modul zabezpečuje elektronickú komunikáciu úradu a zastupiteľstva obce s občanmi v oblastiach, ktoré podporujú demokratické zapájanie obyvateľov do riadenia obce. Služby by mali zvyšovať povedomie a participovanie občanov na správe vecí verejných ako napr. vybavovanie petícií, rôzne pripomienky a informačné služby, návrhy a pripomienky verejnosti, návrhy a pripomienky na mestské/obecné zastupiteľstvo.

### 21.11.8 Modul ePodateľňa IS DCOM

Zabezpečuje procesy vybraných eGOV služieb v rozsahu od kontroly prijatého podania, cez vytvorenie konania, zaevidovanie dokumentu konaniu a zaslanie autorizácie (ÚPVS)

### 21.11.9 Modul Informovanie a poradenstvo

Modul podporuje zvyšovanie transparentnosti obce voči občanom. Služi na správu a zverejňovanie údajov vyplývajúcich zo zákona a informácií súvisiacich s poskytovanými službami. Všeobecne platí, že modul slúži iba na zverejňovanie informácií bez vyžiadania. Služby, ktoré sa týkajú zverejnenia informácií na požiadanie, sú zaradené v module eDemokracia.

### 21.11.10 Modul Licencovanie a povoľovanie

Modul zabezpečuje poskytovanie elektronických služieb mesta z pohľadu evidencie a správy žiadaných, schvaľovaných, schválených alebo zamietnutých licencií a povolení žiadateľov v oblastiach predaja, poskytovania služieb, dopravy, prevádzok, pozemných komunikácií a pod. Elektronizácia týchto služieb bude znamenať pre žiadateľov značnú úsporu nákladov a zníženie administratívnej záťaže. Modul umožní tiež minimalizovať potrebu elektronických príloh, keďže niektoré z nich bude možné získať z integrovaných systémov.

### 21.11.11 Modul Notifikácie a sťažností

Tento modul sa rieši oblasť oznámenia udalosti, ohlásenia skutočnosti alebo sťažnosti občanom prípadne podnikateľom, pričom je vyžadovaná spätná väzba. Služby je možné volať aj anonymne, avšak bez možnosti získať spätnú väzbu. Anonymný občan má možnosť sa dozvedieť o naložení s jeho

podaním iba prostredníctvom Info modulu. Služby modulu sú špecifické tiež tým, že môžu presahovať rámec legislatívnych požiadaviek na obec, keďže v niektorých prípadoch občan nemusí žiadať o konkrétnu službu, avšak chce upozorniť samosprávu na isté okolnosti, o ktorých je presvedčený, že by mala o nich vedieť. Služby zaradené do modulu sú bezplatné.

#### 21.11.12 Modul Podanie

Modul automatizuje procesy súvisiace s evidenciou nových konaní podávajúcim a jeho odoslaním miestnej príslušnej inštitúcii (správneho orgánu). Podanie sa vytvára na portáli. Tu vytvorené podanie predstavuje pre systém základný spôsob tvorby podaní do budúcnosti. Pre ostatné typy podaní (ústne podanie do zápisnice, písomné podanie do zápisnice, telegrafické a telefaxové) sa predpokladá postupná minimalizácia.

#### 21.11.13 Modul Knowledge base

Jedná sa o modul určený na zostavenie a prístup k znalostnej báze. Zabezpečuje a vytvára podmienky pre zdieľanie vedomostí. Systém v plnom rozsahu vytvára podmienky pre správu a tvorbu aktuálnych a konzistentných znalostí. Podporuje procesy zostavenia diela vo všetkých jeho fázach s cieľom minimalizovať náklady prevádzky a tak podporiť dlhodobé udržanie systému IS DCOM.

#### 21.11.14 Modul eLearning

Nosným prvkom aspektu kvality je kvalitná dokumentácia podporená výukovými materiálmi, návodmi, postupmi a systémom pomoci používateľovi. Systém eLearning primárne zastrešuje všetky aktivity samovzdelávania používateľov projektu DCOM.

#### 21.11.15 Verejný webový portál IS DCOM a Intranetový portál obce.

Verejný webový portál reprezentuje verejný prístupový bod IS DCOM a poskytuje webové riešenie pre stránky Používateľa.

#### 21.11.16 E-mailové služby

Služby elektronickej pošty poskytované všetkým používateľom obecných/mestských úradov s dôrazom na kvalitu, efektivitu, pohodlie a bezpečnosť.

#### 21.11.17 Zoznam poskytovaných elektronických služieb

1. Diskusné fórum
2. Elektronická úradná tabuľa
3. Elektronické verejné obstarávanie
4. Informovanie o centrách voľného času
5. Informovanie o cestovnom ruchu
6. Informovanie o cintorínoch obce
7. Informovanie o činnosti obce
8. Informovanie o dani z nehnuteľností
9. Informovanie o dani za jadrové zariadenie
10. Informovanie o dani za nevýherné hracie prístroje
11. Informovanie o dani za predajné automaty
12. Informovanie o dani za psa
13. Informovanie o dani za ubytovanie
14. Informovanie o dani za užívanie verejného priestranstva
15. Informovanie o dani za vjazd a zotrvanie motorového vozidla v historickej časti mesta
16. Informovanie o jazykových školách
17. Informovanie o komunitnom pláne sociálnych služieb obce
18. Informovanie o materských školách
19. Informovanie o mestskej autobusovej doprave
20. Informovanie o mestskej polícii



21. Informovanie o miestnom poplatku za komunálne odpady a drobné stavebné odpady
22. Informovanie o náboženských inštitúciách obce
23. Informovanie o odpadovom hospodárstve
24. Informovanie o pamätihodnostiach obce
25. Informovanie o pamiatkovom fonde na území obce
26. Informovanie o požiarnej ochrane obce
27. Informovanie o regionálnom rozvoji a jeho podpore
28. Informovanie o sociálnych službách v obci
29. Informovanie o sociálnych zariadeniach v obci
30. Informovanie o školských obvodoch
31. Informovanie o špeciálnych triedach
32. Informovanie o útulkoch a karanténach pre zvieratá
33. Informovanie o uzávierke miestnych komunikácií
34. Informovanie o územnom pláne
35. Informovanie o verejnom obstarávaní
36. Informovanie o základných školách
37. Informovanie o základných umeleckých školách
38. Informovanie o zariadeniach školského stravovania
39. Informovanie o životnom prostredí
40. Informovanie verejnosti o civilnej ochrane
41. Licencovanie mestskej autobusovej dopravy
42. Ohlasovanie porúch verejného osvetlenia a cestnej svetelnej signalizácie
43. Ohlasovanie vzniku, zániku alebo zmeny poplatkovej povinnosti za komunálne odpady a drobné stavebné odpady
44. Ohlasovanie závad na chodníkoch a priechodoch pre chodcov
45. Ohlasovanie závad zjazdovosti komunikácií
46. Organizovanie občianskeho svadobného obradu
47. Organizovanie občianskej rozlúčky so zosnulým
48. Oznamovanie malého zdroja znečisťovania ovzdušia
49. Oznamovanie o konaní dražby
50. Oznamovanie o konaní verejného kultúrneho podujatia
51. Oznamovanie o konaní verejných telovýchovných, športových a turistických podujatí
52. Oznamovanie o odstrele
53. Oznamovanie o vzniku, zániku alebo zmene daňovej povinnosti k dani z nehnuteľností
54. Oznamovanie o vzniku, zániku alebo zmene daňovej povinnosti k dani za jadrové zariadenie
55. Oznamovanie o vzniku, zániku alebo zmene daňovej povinnosti k dani za nevýherné hracie prístroje
56. Oznamovanie o vzniku, zániku alebo zmene daňovej povinnosti k dani za predajné automaty
57. Oznamovanie o vzniku, zániku alebo zmene daňovej povinnosti k dani za psa
58. Oznamovanie o vzniku, zániku alebo zmene daňovej povinnosti k dani za ubytovanie
59. Oznamovanie o vzniku, zániku alebo zmene daňovej povinnosti k dani za užívanie verejného priestranstva
60. Oznamovanie o vzniku, zániku alebo zmene daňovej povinnosti k dani za vjazd a zotrvanie motorového vozidla v historickej časti mesta
61. Oznamovanie o zvolaní zhromaždenia občanov
62. Oznamovanie otváracích hodín prevádzkarne alebo ich zmeny
63. Oznamovanie strát a nálezov
64. Oznamovanie zrušenia prevádzkovej jednotky
65. Platenie miestneho poplatku za komunálne odpady a drobné stavebné odpady
66. Platenie miestnych daní
67. Platenie ostatných poplatkov
68. Platenie pokút, úrokov a sankčných úrokov
69. Podávanie daňového priznania k dani z nehnuteľností
70. Poskytovanie finančného príspevku na prevádzku sociálnej služby
71. Poskytovanie finančného príspevku na sociálnu oblasť
72. Poskytovanie informácií podľa zákona o slobodnom prístupe k informáciám
73. Poskytovanie jednorazovej dávky v hmotnej núdzi
74. Poskytovanie návravných dotácií
75. Poskytovanie nenávratných dotácií
76. Poskytovanie odľahčovacej služby
77. Poskytovanie opatrovateľskej služby
78. Poskytovanie prepravných služieb





79. Poskytovanie sociálnej služby monitorovania a signalizácie potreby pomoci
80. Poskytovanie sociálnej služby v dennom stacionári
81. Poskytovanie sociálnej služby v ostatných zariadeniach sociálnej služby
82. Poskytovanie sociálnej služby v zariadení opatrovateľskej služby
83. Poskytovanie sociálnej služby v zariadení pre seniorov
84. Poskytovanie stravovania v jedálni
85. Poskytovanie súťažných podkladov pre verejné obstarávanie
86. Poskytovanie úľav alebo odpustenie daňového nedoplatku
87. Poskytovanie úľavy zo sankcií alebo odpustenie sankcií pre daňový subjekt
88. Poskytovanie základného sociálneho poradenstva
89. Potvrdzovanie výšky pohľadávok voči obci
90. Povoľovanie ambulantného predaja
91. Povoľovanie odkladu platenia dane a povoľovanie splátok
92. Povoľovanie ohňostrojových prác
93. Povoľovanie osobitných prevádzkových hodín
94. Povoľovanie používania symbolov obce
95. Povoľovanie predaja výrobkov a poskytovania služieb na trhovom mieste
96. Povoľovanie prístupu k archívnym dokumentom a registratúrnym záznamom
97. Povoľovanie realizácie podnikateľského plánu na území obce
98. Povoľovanie umiestnenia informačného, reklamného alebo propagačného zariadenia
99. Povoľovanie užívania a zabratia verejného priestranstva
100. Povoľovanie vjazdu do historickej časti mesta alebo pešej zóny
101. Povoľovanie zriadenia a posunu autobusových zastávok
102. Povoľovanie zriadenia vjazdu z miestnej komunikácie na susedné nehnuteľnosti
103. Požičiavanie zdravotných pomôcok
104. Predaj bytových priestorov obce
105. Predaj hnuteľného majetku obce
106. Predaj nebytových priestorov obce
107. Predaj ostatného nehnuteľného majetku obce
108. Prenájom bytových priestorov obce
109. Prenájom hnuteľného majetku obce
110. Prenájom hrobového miesta
111. Prenájom nebytových priestorov obce
112. Prenájom ostatného nehnuteľného majetku obce
113. Pridelovanie bytu osobitného určenia alebo bytu v dome osobitného určenia
114. Pridelovanie zberných nádob pre odpad a separovaný zber
115. Prípomienkovanie cestovného poriadku mestskej autobusovej dopravy
116. Prípomienkovanie návrhov nariadení
117. Prípomienkovanie návrhu komunitného plánu soc. služieb obce
118. Prípomienkovanie návrhu rozpočtu obce
119. Prípomienkovanie návrhu záverečného účtu obce
120. Prípomienkovanie plánu ochrany obyvateľstva a havarijných plánov podnikov a prevádzok na území obce
121. Prípomienkovanie územného plánu obce
122. Registrovanie psa
123. Schvaľovanie cestovného poriadku mestskej autobusovej dopravy
124. Udeľovanie individuálnej licencie na prevádzkovanie hazardných hier prostredníctvom výherných prístrojov
125. Určovanie, zmena alebo zrušenie súpisného a orientačného čísla
126. Uvítanie detí do života
127. Vrátanie pomernej časti dane
128. Vybavovanie petícií
129. Vybavovanie sťažností a podnetov
130. Vydávanie parkovacej karty
131. Vydávanie rybárskeho lístku
132. Vydávanie voličského preukazu
133. Vyhlasovanie v obecnom rozhlase alebo televízii
134. Vyhradzovanie parkovacieho miesta za poplatok
135. Zisťovanie základnej ceny pozemku podľa cenovej mapy
136. Zriaďovanie vecného bremena na majetok obce
137. Zverejňovanie aktualít a informačný servis
138. Zverejňovanie zmlúv ktoré sa týkajú nakladania s verejnými prostriedkami