-NÁVRH -

Koncepcia
rozvoja vládneho cloudu

pracovná verzia 009

Určené pre**:**	Orgány riadenia podľa § 5 ods. 2 zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení zákona č. 423/2020 Z. z.
Vydáva:	Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky, Sekcia informačných technológií verejnej správy
Záväznosť:	Tento dokument má záväzný charakter.
Počet príloh:	2
Dátum vydania:	...2024
Dátum účinnosti:	Dňom zverejnenia na webovom sídle Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky (link https://mirri.gov.sk/sekcie/informatizacia/vladny-cloud/)
Schválil:	**Martin Déneši,** generálny riaditeľ sekcie Sekcia informačných technológií verejnej správy Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky

Obsah

1. Úvod 2
2. Manažérske zhrnutie 3
   2.1. Základné piliere dlhodobej koncepcie rozvoja vládneho cloudu 4
   2.2. Rámcové kroky potrebné na dosiahnutie stanovených cieľov 5
   2.3. Odporúčania pre efektívne využívanie cloudových technológií vo verejnej správe 6
      2.3.1. Odporúčania pre efektívne využívanie cloudových technológií vo verejnej správe - MIRRI 6
      2.3.2. Odporúčania pre efektívne využívanie cloudových technológií vo verejnej správe - OR 6
3. Zhrnutie aktuálneho stavu 7
   3.1. Stav v krajinách EU 8
4. Cieľový stav 12
   4.1. Základné opatrenia pre zabezpečenie cieľového stavu 14
5. Pilier 1 - Maximalizácia využívania služieb verejného cloudu 15
   5.1. Prínosy 16
   5.2. Riziká 16
   5.3. Ošetrenie rizík 16
   5.4. Merateľné ukazovatele 16
   5.5. Plán realizácie 17
6. Pilier 2 - Modernizácia, spoplatnenie a rozšírenie privátnej časti vládneho cloudu 18
   6.1. Prínosy 19
   6.2. Riziká 19
   6.3. Ošetrenie rizík 19
   6.4. Merateľné ukazovatele 19
   6.5. Plán realizácie 20
      6.5.1. Rozšírenie privátnej časti Vládneho cloudu – „eSKa Cloud“ 21
7. Pilier 3 - Sanácia kľúčovej rezortnej infraštruktúry v opodstatnených prípadoch. 22
   7.1. Prínosy 23
   7.2. Riziká rezortných dátových centier 23
   7.3. Ošetrenie rizík 23
   7.4. Merateľné ukazovatele 24
   7.5. Plán realizácie 24
8. Záver 26

9. Skratky a definície 26
10. Príloha 1.: Klasifikácia cloudových služieb 28
10.1. Kategória U1 29
10.2. Kategória U2 29
10.3. Kategória U3 29
10.4. Kategória U4 29
10.5. Minimálne požiadavky na CSP a poskytované cloudové služby 32
10.6. Čo patrí do verejnej a čo do privátnej časti vládneho cloudu 33
10.6.1. ISVS, ktoré musia byť prevádzkované využitím služieb privátnej časti vládneho cloudu 33
10.6.2. ISVS, ktoré môžu byť prevádzkované využitím služieb verejnej časti vládneho cloudu 33
10.6.3. Postup pre získanie kategórie potrebných ISVS 34
11. Príloha 2.: Využitie vládneho cloudu 34

1. Úvod

V súčasnej dobe digitálnej transformácie sa stále viac verejných inštitúcií a organizácií obracia ku cloudovým technológiám, aby zlepšili svoju efektívnosť a škálovateľnosť služieb. Dlhodobá koncepcia rozvoja vládneho cloudu preto slúži ako základ pre budúce rozhodnutia týkajúce sa IT infraštruktúry a cloudových služieb na úrovni štátu.

Význam a potreba dlhodobej koncepcie rozvoja vládneho cloudu spočíva v jej schopnosti poskytnúť vládnym inštitúciám a organizáciám spoločný rámec a jasné usmernenie pre využívanie cloudových technológií. Týmto spôsobom sa zabezpečí súlad s reguláciou, interoperabilita a dosiahne lepšia koordinácia a efektívnosť pri vývoji, nasadzovaní a správe cloudových riešení. Zároveň tak vzniká podklad na vyhodnotenie opodstatnenosti a efektivity budúcich navrhovaných projektov v IT. Taktiež sa zaručí, že štátna IT infraštruktúra bude flexibilná, škálovateľná a udržateľná, a že sa zabezpečuje kontinuita a kvalita služieb poskytovaných občanom a podnikateľskému sektoru.

Tento dokument predstavuje základný rámec pre plánovanie, implementáciu a správu vládnych cloudových služieb, s cieľom dosiahnuť správne nasmerovanie dlhodobého rozvoja a so zameraním sa na udržateľnosť v tejto oblasti.

Koncepcia rozvoja vládneho cloudu je založená na troch základných pilieroch:

I. Maximalizácia využívania služieb verejného cloudu.
II. Modernizácia, spoplatnenie a rozšírenie privátnej časti vládneho cloudu.
III. Sanácia kľúčovej rezortnej infraštruktúry v opodstatnených prípadoch.

Nasleduje prehľad a analýza jednotlivých pilierov, ich prínosov, rizík a opatrení na zmiernenie týchto rizík. Ďalej koncepcia predstavuje plány realizácie a merateľné ukazovatele, ktoré umožňujú monitorovať a hodnotiť úspešnosť jej implementácie v praxi. Jej implementácia a úspešné dosiahnutie stanovených cieľov prispeje k vytvoreniu modernej, efektívnej a bezpečnej digitálnej infraštruktúry, ktorá bude slúžiť ako základ pre budúci rozvoj digitálnych služieb verejnej správy.

2. Manažérske zhrnutie

Táto časť dokumentu poskytuje stručný prehľad o hlavných cieľoch a prístupoch tejto koncepcie. Autori vyjadrujú presvedčenie, že táto koncepcia prispeje k úspešnej implementácií a efektívnemu riadeniu cludových služieb vo verejnom sektore.

2.1.Základné piliere dlhodobej koncepcie rozvoja vládneho cloudu

I. Maximalizácia využívania služieb verejného cloudu.

Prvým zo základných pilierov dlhodobej koncepcie je optimalizácia nákladov na cloudové služby formou využitia služieb verejného cloudu všade, kde je to možné. Tie sú totiž v porovnaní s budovaním kapacity privátnej časti technologicky aktuálnejšie, často cenovo výhodnejšie a jednoduchšie dostupné. Tým je možné poskytnúť verejnej správe veľkú škálu moderných služieb a možností. Využitie verejných cloudových služieb môže celkovo pomôcť štátu dosiahnuť väčšiu efektívnosť a flexibilitu pri napĺňaní svojich IT potrieb.

Pri obstaraní cloudových služieb má byť prvou voľbou organizácií verejného sektora využitie verejného cloudu. Iné riešenia by mali byť použité len, ak existujú objektívne prekážky, znemožňujúce tento postup.

Pre zabezpečenie vyššieho využívania služieb hybridného vládneho cloudu budú vykonávané aktivity, ktoré pomôžu zvýšiť osvetu a vzdelanosť v oblasti využívania cloudových služieb, zvýšiť vzdelanosť v oblasti architektúry budovania informačných systémov v cloude.

II. Modernizácia, spoplatnenie a rozšírenie privátnej časti vládneho cloudu.

Druhý pilier dlhodobej koncepcie zahŕňa budovanie a zabezpečenie nových cloudových služieb, v časti privátneho vládneho cloudu, ktorý bude naďalej slúžiť ako základňa pre tie informačné systémy verejnej správy, ktoré nie je možné prevádzkovať vo verejnej časti vládneho cloudu. Ďalší rozvoj privátnej časti vládneho cloudu musí byť navrhnutý tak, aby poskytoval vysokú úroveň bezpečnosti, súkromia a súladu s právnymi predpismi, ako aj efektívnosť a škálovateľnosť potrebnú pre dlhodobý rozvoj.

Tento pilier musí zahŕňať:

- Výber vhodných technologických riešení, ktoré budú zabezpečovať potrebnú infraštruktúru, platformy a služby pre verejnú správu.
- Zabezpečenie integrácie s existujúcimi systémami a procesmi v rámci verejnej správy, ako aj s verejnými cloudovými službami.
- Vytvorenie a implementácia pravidiel a postupov pre správu, monitorovanie a bezpečnosť privátneho vládneho cloudu.
- Poskytovanie vzdelávania a školení pre zamestnancov verejnej správy, ktorí budú zodpovední za správu a využívanie cloudových služieb.

V súčasnosti existujúca kapacita privátnej časti vládneho cloudu je technologicky zastaralá a ekonomicky nevýhodná. Toto riešenie je potrebné modernizovať s cieľom umožnenia jednoduchej migrácie k iným poskytovateľom služieb vládneho cloudu alebo medzi jednotlivými lokalitami súčasného riešenia. Po dosiahnutí možnosti jednoduchej migrácie a jej overenia úspešnou realizáciou niekoľkých migrácií projektov, je potrebné zvážiť optimalizáciu zoznamu prevádzkových lokalít a ukončenie prevádzky tých, ktoré sa ukážu ako nadbytočné a na konci svojej životnosti.

Nevyhnutným predpokladom zefektívnenia využívania kapacít privátnej časti vládneho cloudu je zároveň zavedenie spoplatnenia jeho služieb. Spoplatnenie zabezpečí ekonomický stimul na strane správcov informačných systémov zreálniť požadovanú kapacitu a hľadať najefektívnejšie riešenia na jej získanie. Na strane prevádzkovateľov kapacity privátnej časti vládneho cloudu zároveň zabezpečí stimul na efektívne plánovanie a alokáciu kapacít. Spoplatnenie musí byť zavedené transparentne a s ohľadom na potreby jednotlivých rezortov a inštitúcií.

III. Sanácia kľúčovej rezortnej infraštruktúry v opodstatnených prípadoch.

Tretí pilier dlhodobej koncepcie sa zameriava na riešenie súčasného stavu mnohých rezortných dátových centier, ktoré sú na hranici alebo za hranicou svojej životnosti a zároveň prevádzkujú služby, **ktorých migrácia do vládneho cloudu nie je prakticky realizovateľná, alebo zásadne nehospodárna.** Medzi možné prekážky znemožňujúce migráciu patrí napríklad zakúpené licencie špecificky viazane na určitý presne definovaný HW alebo aplikácia (ISVS) napísaná na špecifický HW (napríklad mainframe).

V týchto prípadoch sa urobí prieskum, či dané prekážky existujú aj na ostatných rezortoch a navrhne sa riešenie, ktoré dokáže vyriešiť problémy viacerých rezortov súčasne. Napríklad sa identifikuje nová služba, ktorú vládny cloud začne poskytovať. **Dané riešenia prejdú procesom zápisu cloudovej služby do katalógu služieb vládneho cloudu, pričom bude posúdená ich zhoda s požiadavkami kladenými na cloudové služby v zmysle zákona 95/2019, § 24a, odstavec 3 a metodického usmernenia pre zápis cloudových služieb do Katalógu služieb Vládneho cloudu.**

Rezortné dátové centrá **nebudú využívané pre poskytovanie infraštruktúry novým informačným systémom** – tie budú budované v súlade s NKIVS ako tzv. „cloud-ready“, teda pripravené na prevádzku prostredníctvom cloudových služieb.

Rezortné dátové centrá sa môžu modernizovať a rozširovať aj v prípade, ak v nich prevádzkované systémy **nie sú informačnými technológiami verejnej správy v zmysle zákona č. 95/2019 Z. z. o** informačných technológiách vo verejnej správe, a zároveň existujú prekážky pre využitie služieb vládneho cloudu. V takýchto prípadoch by sa mali budovať ako rezortný špecializovaný cloud, ktorý umožní verejným inštitúciám so spoločnými potrebami a záujmami zdieľať zdroje, znalosti a náklady na prevádzku a správu cloudových služieb. Tieto riešenia musia byť navrhnuté tak, aby zohľadňovali špecifické potreby a požiadavky daného rezortu, a zároveň aj zabezpečiť kompatibilitu a interoperabilitu v rámci celého štátneho cloudového ekosystému.

2.2. Rámcové kroky potrebné na dosiahnutie stanovených cieľov

- Kontinuálna analýza stavu a potrieb jednotlivých verejných inštitúcií s ohľadom na využitie cloudových služieb.
- Vytvorenie jasných pravidiel a postupov pre výber služieb vládneho cloudu, vrátane kategorizácie údajov a výberu vhodných riešení pre rôzne typy systémov a aplikácií.
- Zabezpečenie potrebných cloudových služieb v privátnej a verejnej časti v dostatočnom rozsahu a kapacite.
- Spolupráca medzi verejnými inštitúciami a prevádzkovateľmi cloudových služieb pri vývoji a implementácii lokálnych riešení v nevyhnutných prípadoch.
- Vytváranie a úprava informačných systémov s dôrazom na využívanie cloudových služieb v privátnej a verejnej časti vládneho cloudu, alebo v hybridnej forme.

- Monitorovanie a hodnotenie výsledkov a efektívnosti týchto riešení a pravidelná aktualizácia dlhodobej koncepcie rozvoja verejného cloudu.
- Zabezpečenie vykonávania vzdelávacích aktivít za účelom osvety, zvyšovania povedomia o cloudových technológiách, zvyšovania úrovne vzdelanosti v oblasti využívania cloudových technológií na všetkých úrovniach štátnej a verejnej správy.
    - Využívať vzdelávacie možnosti v spolupráci s veľkými poskytovateľmi cloudových služieb.

2.3. Odporúčania pre efektívne využívanie cloudových technológií vo verejnej správe

2.3.1. Odporúčania pre efektívne využívanie cloudových technológií vo verejnej správe - MIRRI

I) Podporovať ekonomickú motiváciu na strane správcov informačných systémov a správcov dátových centier pri hľadaní najefektívnejších alternatív pre získanie potrebnej kapacity.

II) Vypracovať jasné pravidlá a kategórie údajov, ktoré určia, aké systémy a informácie môžu byť prevádzkované v privátnom vládnom cloude a ktoré môžu využívať komerčný cloud.

III) Urýchlene zabezpečiť centrálny privátny vládny cloud, ktorý bude poskytovaný formou "Cloud as a Service" a jeho štruktúra a prevádzkový model budú podobné poskytovateľom verejného cloudu.

IV) Podporovať migráciu do vládneho cloudu, umožnite optimálne využitie existujúcich zdrojov a zabezpečiť efektívnejšiu prevádzku.

V) Podporovať sanáciu dátových centier v nevyhnutných prípadoch. Zabezpečte aby sa dátové centrá rozvíjali na základe vlastnej koncepcie s cieľom poskytovať moderné cloudové služby na nevyhnutnú dobu.

VI) Zabezpečiť centrálnu koordináciu a monitorovanie požiadaviek na IT infraštruktúru, aby ste eliminovali duplicitnú alokáciu kapacít a neefektívne riešenia.

VII) Vytvoriť jasné usmernenia a podporujte verejné inštitúcie a organizácie pri zavádzaní cloudových technológií, aby boli schopné identifikovať vhodné projekty a aplikácie pre migráciu do cloudu a využiť jeho výhody efektívne.

VIII) Dodržovať bezpečnostné a regulačné aspekty v súlade s požiadavkami štátu a medzinárodnými normami, aby boli cloudové služby spoľahlivé a dôveryhodné pre verejné inštitúcie a organizácie.

IX) Investovať do vzdelávania a zvyšovania povedomia o cloudových technológiách medzi zamestnancami verejných inštitúcií a organizácií, aby boli schopní efektívne využívať cloudové riešenia a adaptovať sa na nové technologické prístupy.

X) Nastaviť a sledovať merateľné ukazovatele pre každý z pilierov, aby ste mohli hodnotiť úspešnosť implementácie dlhodobej koncepcie a identifikovať potenciálne oblasti zlepšenia.

2.3.2. Odporúčania pre efektívne využívanie cloudových technológií vo verejnej správe - OR

I) Používať verejné cloudové služby pre projekty a aplikácie, ktoré nevyžadujú prísne bezpečnostné opatrenia alebo špeciálne regulačné požiadavky, čo umožní získať výhody z ekonomiky rozsahu a flexibilnosti týchto riešení.

II) Rozhodovať sa, na základe vyhodnotenia kategorizácie systémov, či je vhodnejšie prevádzkovať systémy a údaje v privátnej časti vládneho cloudu, alebo vo verejnej časti. Využívať metodiku klasifikácie informačných systémov a určenie rôznych variant TCO pre správne rozhodnutia kde prevádzkovať Váš ISVS.

III) Uprednostňovať PaaS a SaaS cloudové služby, ktoré urýchlia vývoj ISVS a zjednodušujú prevádzku.

IV) Preskúmať možnosti migrácie existujúcich systémov. Zvážiť možnosti optimalizácie a využitia moderných cloudových riešení. Využiť možnosti financovania z dopytových výziev. Identifikujte vhodné projekty a aplikácie na migráciu do cloudu.

V) Koordinovať svoje kapacitné požiadavky na cloudové služby s MIRRI. Zabezpečte, aby vaše alokácie kapacít boli efektívne a bez duplicít.

VI) Dodržiavať bezpečnostné požiadavky vyplývajúce z platnej legislatívy. Uistite sa, že cloudové a infraštruktúrne služby, ktoré využívate, sú spoľahlivé a dôveryhodné.

VII) Investovať do vzdelávania a tréningov pre vašich zamestnancov v oblasti cloudových technológií.

VIII) Nastaviť a sledovať merateľné ukazovatele pre každý z pilierov, aby ste mohli hodnotiť úspešnosť implementácie dlhodobej koncepcie a identifikovať potenciálne oblasti zlepšenia.

3. Zhrnutie aktuálneho stavu

Vládny cloud dlhodobo patrí medzi základné priority Národnej koncepcie informatizácie verejnej správy Slovenskej republiky (ďalej len "NKIVS"). Dôvod je hlavne zjednodušenie prevádzky systémov, finančná efektivita a vysoká pridaná hodnota pre orgány verejnej správy. Vládny cloud sa skladá zo služieb, ktoré sú zapísane v katalógu služieb Vládneho cloudu. Katalóg služieb Vládneho cloudu spravuje cloudová kancelária Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky (ďalej len "MIRRI"). Tieto služby sa nachádzajú:

- v privátnej časti – momentálne len Ministerstvo vnútra SR (Kopčianska a Tajov), v dohľadnom čase bude rozšírená o RPC (Ministerstvo financií SR) a eSKa Cloud (MIRRI),
- vo verejnej – poskytovatelia z komerčného sektora (Oracle, AWS, Azure, VNET, atď.).

Služba sa do katalógu pridá po kontrole splnenia a dodržania podmienok podľa § 24a zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len "akreditácia").

Elektronická forma katalógu s možnosťou vyhľadávania: **https://katalog.statneit.sk/**

Každá služba sa posudzuje na určitú bezpečnostnú úroveň U1 (otvorené dáta), U2 (regulované dáta), U3 (klasifikované dáta), U4 (špeciálne dáta, ktoré je potrebné spracovať a uchovať v privátnej časti vládneho cloudu).

Popis bezpečnostných úrovní je uvedený v prílohe: Klasifikácia cloudových služieb.

Výber cloudových služieb na prevádzku informačných systémov je podmienený bezpečnostnou úrovňou služby. Väčšina informačných systémov môže byť prevádzkovaná vo verejnej časti vládneho cloudu, ale existujú aj systémy, ktoré štát z bezpečnostných a strategických dôvodov potrebuje prevádzkovať vo svojich dátových centrách.

Súčasná privátna časť vládneho cloudu sa začala budovať v roku 2015 na základe návrhu, ktorý vznikol ešte pred samotnou realizáciou. V súčasnosti sú služby privátnej časti Vládneho cloudu zastarané, nedajú sa porovnávať s funkcionalitou, ktoré ponúkajú komerční poskytovatelia. Sú evidované viaceré problémy, či už výkonnostné, nedostupnosť PaaS, alebo nedostatky šifrovania dát, nedostupnosť automatizovaných činností, backup, resize, ktoré zamedzujú používaniu existujúcej privátnej časti. Lokality privátnej časti sú nejednotné a pristupuje sa k nim ako k dvom rozdielnym riešeniam. Privátna časť vládneho cloudu poskytuje iba služby Infraštruktúra ako služba (ďalej len "**IaaS"), t.j.** virtuálne stroje a diskový priestor. Aktuálne sa realizuje projekt na zavedenie platformových služieb "PaaS".

Popis cloudových služieb je uvedený v prílohe: Využitie vládneho cloudu

Mnoho organizácií verí, že ich citlivé údaje sú bezpečnejšie v privátnom cloude, alebo v dátovom centre. Realita je však taká, že verejné cloudy sú tradične bezpečnejšie, pretože sú spravované tisíckami odborníkmi na bezpečnosť, ktorí rozumejú potrebám v oblasti cloudovej bezpečnosti a ako ich dosiahnuť. Zároveň verejné cloudy prechádzajú pravidelnými certifikáciami a auditmi, ktoré reflektujú rôzne potreby z pohľadu prenosu a zabezpečenia údajov všeobecne, osobných údajov, zdravotníckych údajov, bankových údajov, alebo dát patriacich verejnej správe. Auditné správy je možné získať a nezávisle overiť.

3.1.Stav v krajinách EU

Na základe prieskumu „Vypracovanie panorámy národných cloudových politík v EÚ“[1)] vykonaného v nasledujúcich krajinách EU (BE, BU, CY, CZ, DE, DK, EL, FI, FR, IE, IT, LT, LV, MT, NL, PL, PT, SE, SK, + DG-DIGIT) formou dotazníka, boli spracované nasledujúce zistenia.

ROZSAH A VÝHODY

1.1 Aké sú stávky formálne spojené s vašou cloudovou politikou?	váha kritéria	%
Modernizácia a transformácia verejnej činnosti	1	90%
Suverenita	1	30%
Kyber ochrana	1	80%
Agility	1	65%
Zníženie nákladov	1	70%
Zneužívanie údajov	1	35%
Atraktivita podania	1	30%
Prijatie posunu umelej inteligencie	1	30%
Iné špecifikuj)	1	5%
Žiadna odpoveď		

1.2 Aký je rozsah vašich zásad pre cloud? *(možných viac odpovedí)*	váha kritéria	%
Centrálna správa	1	90%
Verejné spoločnosti delegované centrálnym štátom	1	40%
Miestna vláda	1	50%
Všetky štátne firmy	1	30%
Iné (uveďte)		
Žiadna odpoveď		

PRIORITA DANÁ CLOUDU

2.1 Akú prioritu má cloud – verejný vs. súkromný?	váha kritéria	%
Najprv verejný cloud	1	10%

[1)] Drawing up a panorama of national cloud policies in the EU 3rd meeting of the informal member state cloud cooperation group.

Najprv dôveryhodný verejný cloud (napríklad vyhradený cloud alebo virtuálny súkromný cloud)	1	10%
Najprv súkromný cloud (on-premises).	0.5	5%
Cloud first – nie je uvedený jasný cieľ, ale súbor pravidiel	1	60%
Cloud nemá žiadnu prioritu – konvenčný hosting je stále možnosťou	0	15%
Iné (uveďte)		
2.2 Akú prioritu má cloud – politika SaaS?	váha kritéria	%
Najprv SaaS	1	30%
SaaS sa neuprednostňuje	0	70%
Žiadna odpoveď		

STRATÉGIA PRIJÍMANIA CLOUDU

3.1 Aký je váš prístup z hľadiska plánovania prijatia cloudu?*(možných viac odpovedí)*	váha kritéria	%
Plánuje sa hromadný tréning a zmena operačného modelu	1	20%
Pre existujúce aktíva sa plánuje migrácia do cloudu	1	45%
Cloud Policy neobsahuje plánovanie	0	35%
Iné (uveďte)		30%
Žiadna odpoveď		
3.2 Čo sa týka prijatia cloudu, aké dodatočné zdroje poskytujete administratíve?*(možných viac odpovedí)*	váha kritéria	%
Sprievodca vyhodnocovaním cloudových príležitostí pre nové projekty	1	60%
Štandardy a odporúčané modely architektúry	1	65%
Prevádzkové osvedčené postupy	1	55%
Cloudové centrum excelentnosti podporujúce projekty	1	30%
Tréningové centrum	1	15%
Iné (uveďte)	1	25%
Žiadna odpoveď		

OBSTARÁVANIE

4.1 Poskytujete verejným obstarávateľom „katalóg“ dostupných ponúk na trhu?	váha kritéria	%
Áno	1	65%
Nie	0	35%

4.2 Poskytujete centrálny digitálny trh, ktorý spája všetky alebo hlavné časti zdrojov spojených s cloudom?*(možných viac odpovedí)*	váha kritéria	%
Infraštruktúrne a platformové služby	1	60%
SaaS	0.5	40%
Poradenstvo a odborné znalosti (Cloud stratégia, FinOps atď.)	1	40%
Opakujúce sa činnosti (migrácia, outsourcing atď.)	1	35%
Iné špecifikuj)		30%
Žiadna odpoveď		25%

BEZPEČNOSŤ

5.1 Aké nástroje a opatrenia majú administratívy k dispozícii z hľadiska bezpečnosti a nezávisle od regulovaných činností týkajúcich sa národnej bezpečnosti?*(možných viac odpovedí)*	váha kritéria	%
Rámec osvedčených postupov	1	40%
Odporúčanie na používanie kvalifikácií pre kybernetickú bezpečnosť (ISO 27001, C5, SecNumCloud,...)	1	75%
Opatrenia súvisiace s umiestnením operácií alebo údajov (miestne/EÚ/iné)	1	85%
Opatrenia, ktorých cieľom je zabezpečiť, aby bol hospodársky subjekt prísne nezávislý od jurisdikcií mimo EÚ	1	25%
Opatrenia súvisiace so spracovaním žiadostí vydaných jurisdikciami mimo EÚ	1	25%
Iné (uveďte)	1	20%
Žiadna odpoveď		5%

ĽUDSKÉ ZDROJE

6.1 Aká je vaša politika ľudských zdrojov súvisiaca s vašou cloudovou stratégiou?*(možných viac odpovedí)*	váha kritéria	%
Popis cloudových úloh	1	25%

Strategické plánovanie pracovnej sily	1	20%
Tréningové programy	1	25%
Komunikácia	1	45%
Náborové opatrenia	1	30%
Iné (uveďte)	1	15%
Žiadna odpoveď		

RIADENIE

7.1 Máte vyhradenú správu cloudovej politiky na kontrolu okrem iného nasledujúcich aspektov?*(možných viac odpovedí)*	váha kritéria	%	
Štandardizácia	1		0
Súlad s cloudovými vzormi	1		0
Súlad s pravidlami cloudu	1		1
Správa údajov	1		0
Nákupy	1		0
Bezpečnosť	1		1
Prechod prevádzkových modelov	1		0
Komunity odborníkov	1		0
Iné (uveďte)	1		0
Žiadna odpoveď			

Záver: Z prieskumu vyplýva, že Cloud First s dôrazom na verejný cloud je najčastejšie aplikovaná politika v rámci krajín EU. Pri výbere cloudových služieb sa uprednostňujú IaaS, PaaS a čoraz častejšie SaaS. Umiestnenie dát a posúdenie bezpečnosti cloudových služieb je kľúčový aspekt. Na národnej úrovni je potrebné zabezpečiť školiace a konzultačné aktivity pre osvojenie cloudu.

4. Cieľový stav

Efektívny, bezpečný a inovatívny vládny cloud pre digitalizovanú verejnú správu.

Naša vízia je zabezpečiť a udržiavať cloudové služby vo vládnom cloude, ktorý plne podporuje digitalizáciu verejnej správy, znižuje náklady, zvyšuje efektívnosť, zabezpečuje bezpečnosť a umožňuje rýchlu adaptáciu na technologické inovácie. Vládny cloud bude predstavovať základný stavebný kameň pri transformácii verejných služieb a zlepšovaní životov občanov.

Kľúčové ciele tejto vízie:

1. **Flexibilita a Škálovateľnosť:** Vládny cloud bude poskytovať flexibilné a škálovateľné služby, aby dokázal rýchlo reagovať na zmeny potrieb a požiadaviek verejných inštitúcií a občanov. Jeho architektúra umožní jednoduché prispôsobenie a rozširovanie služieb podľa potreby.
   Cieľ plánujeme dosiahnuť:
   - Podporou využívania bezpečných existujúcich cloudových služieb verejných poskytovateľov, všade tam kde je to možné a adekvátne.
   - Podporou rozširovania a rozvoja privátnej časti vládneho cloudu zavedením služieb a procesov vedúcich k optimalizácii využívania a kapacitného plánovania.
   - Skrátením procesu zabezpečenia nových a rozšírenia existujúcich cloudových služieb.

2. **Bezpečnosť a súkromie**: Bezpečnosť údajov a súkromie občanov budú na prvom mieste. Vládny cloud bude poskytovať zabezpečené služby v súlade s najvyššími štandardmi a pravidlami, aby chránil citlivé informácie a zabezpečil dôveru v digitálne služby.
   Cieľ plánujeme dosiahnuť:
   - Podporou rozvoja privátnej časti vládneho cloudu v oblasti služieb, ktoré zabezpečia autonómnosť a bezpečnosť pre kritické systémy štátu.
   - Certifikáciou a autorizáciou jednotlivých poskytovaných služieb zapísaných v katalógu služieb vládneho cloudu.
   - Zavedením služieb a procesov vedúcich k monitorovaniu a pravidelnej kontrole bezpečnostných procesov prevádzkovateľov cloudových služieb.

3. **Inovácie a spolupráca**: Vládny cloud bude podporovať inovácie a spoluprácu medzi verejnými inštitúciami, občanmi a súkromným sektorom v rámci SR ako aj v rámci EÚ. Umožní vývoj a implementáciu nových služieb, technológií a riešení, ktoré zlepšia kvalitu života a prispievajú k hospodárskemu rastu.
   Cieľ plánujeme dosiahnuť:
   - Rozširovaním a adopciou verejnej časti vládneho cloudu
   - Podporou rozvoja privátnej časti vládneho cloudu, umožnením hybridných riešení

4. **Účinnosť a efektívnosť:** Vládny cloud bude využívať najlepšie dostupné technológie a postupy na znižovanie prevádzkových nákladov, optimalizáciu využitia zdrojov a zlepšenie efektívnosti služieb poskytovaných verejným inštitúciám a občanom.
   Cieľ plánujeme dosiahnuť:

- Podporou rozvoja privátnej časti vládneho cloudu zavedením cloudových služieb IaaS, PaaS, SaaS na základe reálnych potrieb používateľov služieb.
- Uplatňovaním minimálnych požiadaviek na vývoj a prevádzku „Cloud native“ informačných systémov.
- Spoplatnením privátnej časti vládneho cloudu, motiváciou prevádzkovateľov cloudových služieb v privátnej časti poskytovať nákladovo efektívne riešenia.

4.1.Základné opatrenia pre zabezpečenie cieľového stavu

Zoznam opatrení plánovaných pre zabezpečenie úspešného dosiahnutia cieľového stavu:

1. pripraviť metodické usmernenie pre klasifikáciu ISVS podľa údajov s ktorými systémy pracujú a ukladajú,
2. pripraviť metodické usmernenie pre určenie cenotvorby cloudových služieb v privátnej časti vládneho cloudu,
3. pripraviť metodické usmernenie pre postup určenia miesta produktívnej prevádzky ISVS (prevádzka v cloude - verejná časť alebo privátna časť),
    - pre zabezpečenie čo najoptimálnejšie prevádzky s pohľadu ekonomického, ale aj s pohľadu použitých technológií v cloude,
4. pripraviť a presadiť formu platieb za služby privátnej časti vládneho cloudu,
5. zabezpečiť optimalizáciu využívania kapacít privátnej časti vládneho cloudu,
6. pripraviť a presadiť metodické usmernenie pre architektúru ISVS v cloude, ako vytvárať ISVS so zachovaním a dodržiavaním princípov Cloud Native/Ready, doporučené DevOps procesy a postupy, využívanie IaC,
    - je potrebné zaviesť zoznam cloudových služieb jednotlivých poskytovateľov služieb, ktoré je možné používať, aby sa zamedzilo problémom pri Cloud-EXIT procese.
7. vytvoriť skúsený tím, ktorý bude koordinovať a riadiť vzdelávacie aktivity pre štátnych zamestnancov,
    - **Formovanie tímu:** Identifikovať a najať expertov v rôznych oblastiach na vytvorenie špecializovaného tímu pre vzdelávanie a rozvoj. Zabezpečiť, aby členovia tímu boli dobre oboznámení so svojimi odbormi, čo im umožní nezávislé vykonávanie vzdelávacích programov.
    - **Hodnotenie potrieb:** Uskutočniť dôkladné hodnotenie vzdelávacích potrieb našej organizácie. Identifikovať kľúčové oblasti, ktoré vyžadujú rozvoj zručností, s dôrazom na role ako softvéroví architekti, cloud architekti, administrátori ISVS a v oblasti DevOps.
    - **Prispôsobené vzdelávacie plány:** Vytvoriť prispôsobené vzdelávacie plány pre rôzne úrovne zamestnancov na základe ich pracovných zodpovedností. To zahŕňa navrhovanie vzdelávacích ciest pre softvérových a cloud architektov, administrátorov v oblasti DevOps, s dôrazom na ich konkrétne pracovné úlohy.
    - **Spolupráca s poskytovateľmi cloudových služieb:** Naviazať partnerstvá s poprednými poskytovateľmi cloudových služieb s cieľom využiť ich vzdelávacie zdroje. Využiť vzdelávacie iniciatívy týchto poskytovateľov na zdokonaľovanie zručností štátnych zamestnancov, najmä v oblasti cloudových technológií.
    - **Autonómne učenie:** Umožniť členom tímu autonómne viesť a riadiť vzdelávacie aktivity. Podporovať kultúru samostatného učenia, čím umožniť členom tímu prevziať zodpovednosť za konkrétne vzdelávacie programy a iniciatívy.

- **Kontinuálne hodnotenie:** Implementovať robustný systém pre kontinuálne hodnotenie účinnosti vzdelávacích programov. Pravidelne hodnotiť zručnosti a kompetencie zamestnancov po absolvovaní školení (matica zručností), aby sa zabezpečilo dosiahnutie vzdelávacích cieľov.
- **Prispôsobivý kurikulum:** Zachovať flexibilitu v kurikule pre prispôsobenie sa vývoju a potrebám štátu. Zabezpečiť, aby vzdelávací obsah ostal relevantný a aktuálny s ohľadom na dynamiku v technológií.
- **Zapojenie zainteresovaných strán:** Zapojiť sa s príslušnými orgánmi riadenia na získanie názorov a spätnej väzby o účinnosti vzdelávacích programov. To umožní neustále zdokonaľovanie a zaradenie vzdelávania do cieľov.
- **Transparentná komunikácia:** Zaviesť transparentné komunikačné kanály týkajúce sa vzdelávacích iniciatív, pokroku a dostupných zdrojov. Informovať zamestnancov o nadchádzajúcich školeniach a príležitostiach na rozvoj zručností.
- **Metriky Výkonu:** Definovať jasné metriky výkonu na meranie vplyvu školení na individuálny a organizačný výkon. Využívať kľúčové ukazovatele výkonu (KPI) na hodnotenie návratnosti investícií do vzdelávania zamestnancov.

8. vzdelávanie zabezpečovať aj za pomoci služieb od veľkých poskytovateľov cloudových služieb s využívaním ich vzdelávacích akcií,
9. zabezpečenie technologickej udržateľnosti prevádzkovaných cloudových riešení v privátnej časti vládneho cloudu,
    - zmenami v riešeniach súčasne prevádzkovaných privátnych cloudoch,
    - zriadenie nového privátneho cloudu formou Cloud as a service, s platbou len za využité služby, čo odbremení štát od údržby a správy HW komponentov,
10. pri každom ISVS a potrebe jeho migrácie je potrebné vykonať komplexnú analýzu migrovateľnosti s analýzou rizík pre všetky variantné situácie a scenáre, ktoré môžu vzniknúť pri prevádzke ISVS prípadne jeho migrácii.

5. Pilier 1 - Maximalizácia využívania služieb verejného cloudu

5.1. Prínosy

- Finančná úspora: Využitie verejných (komerčných) cloudových služieb umožňuje štátu platbu len za skutočne využité zdroje, čo vedie k úspore nákladov na IT infraštruktúru a prevádzku.
- Flexibilita: Verejné (komerčné) cloudové služby poskytujú štátu flexibilitu pri škálovaní zdrojov v závislosti od aktuálnych potrieb.
- Dostupnosť: Verejné (komerčné) cloudové služby sú dostupné hneď, v prakticky neobmedzenom rozsahu.
- Inovácia: Verejné (komerčné) cloudové služby sú často na čele technologických inovácií, čo umožňuje štátu využívať najmodernejšie riešenia a služby.

5.2. Riziká

- Bezpečnosť a súkromie: Pri využití verejných cloudových služieb je potrebné zabezpečiť ochranu citlivých údajov a systémov pred neoprávneným prístupom a únikom informácií.
- Závislosť na externých poskytovateľoch: Využitie verejných cloudových služieb môže vytvoriť závislosť na externých dodávateľoch, čo by mohlo v prípade problémov s týmito poskytovateľmi ohroziť kontinuitu služieb verejnej správy.
- Právne a regulačné otázky: Využitie verejných cloudových služieb môže byť obmedzené právnymi a regulačnými požiadavkami štátu, napríklad v oblasti ochrany osobných údajov alebo bezpečnosti informácií.
- Nevhodná architektúra : architektúra ITVS, ktorá neumožňuje plné využitie škálovania v cloude.
- Nízka vzdelanosť v oblasti využívania cloudových služieb: z dôvodu nižšej vzdelanosti môže vzniknúť neochota využívať cloudové služby.

5.3. Ošetrenie rizík

- Zabezpečenie: Štát by mal pri výbere verejných cloudových služieb dbať na ich bezpečnostné normy a certifikácie, ako aj na dodržiavanie súkromia a ochrany údajov.
- Diverzifikácia poskytovateľov: Pre znižovanie závislosti na jednom poskytovateľovi by mal štát zvažovať diverzifikáciu cloudových služieb medzi viacerými dodávateľmi a informačné systémy vyvíjať s dôrazom na prenositeľnosť.
- Jasné právne a regulačné usmernenia: Štát by mal vypracovať jasné právne a regulačné usmernenia pre využívanie verejných cloudových služieb, vrátane pravidiel pre spracovanie a uchovávanie údajov, aby sa zaistila ich zhoda s vnútroštátnymi požiadavkami.
- Finančné prostriedky: Štát zabezpečí finančné prostriedky na úpravu ISVS, na ich migráciu do verejných cloudov a zabezpečiť cloudové služby vo verejnej časti.
- Zabezpečenie zvýšenia povedomia o využívaní cloudových služieb, ich prínosov. Zvýšenie vzdelanosti formou kurzov a školení.
- Vytvorenie plánu školení na dlhšie obdobie vopred, aby bola dobrá informovanosť o školeniach.
- Zabezpečenie plánovaných školení v súčinnosti s najväčšími dodávateľmi cloudových služieb.

5.4.Merateľné ukazovatele

Úspory nákladov:

- Celková suma úspor nákladov dosiahnutých vďaka optimalizácii využitia cloudových služieb.

Efektívnosť využívania zdrojov:

- Percentuálny pokles nevyužitých alebo nadmerných IT zdrojov, ako sú kapacita úložiska, výpočtový výkon a pamäť.
- Percentuálny nárast využitia existujúcich IT zdrojov v dôsledku prechodu na verejné cloudové služby.

Počet migrácií systémov a aplikácií:

- Počet úspešne migrovaných systémov a aplikácií do verejných cloudov alebo na optimálne riešenia v rámci privátneho cloudu.

Zlepšenie časových rámcov implementácie:

- Skrátenie časových rámcov pre implementáciu nových IT projektov a služieb vďaka zlepšenej efektívnosti a flexibilite cloudových služieb.
- Percentuálny pokles doby potrebnej na spustenie nových IT projektov a služieb.

Spokojnosť zákazníkov:

- Percentuálny nárast spokojnosti zákazníkov (inštitúcií verejnej správy) s cloudovými službami, ktorý je merateľný prostredníctvom prieskumov spokojnosti alebo hodnotenia služieb.

Tieto merateľné ukazovatele umožňujú hodnotiť úspešnosť prvého piliera koncepcie rozvoja vládneho cloudu, ako aj monitorovať pokrok a identifikovať oblasti, ktoré si vyžadujú zlepšenie alebo úpravy stratégie.

5.5.Plán realizácie

- Analýza súčasného stavu: Identifikácia a zhodnotenie súčasných IT systémov, ktoré sú kandidátmi na migráciu do verejného cloudu. Identifikácia oblasti, kde by mohol byť výhodne využitý spoločný tenant na zdieľanie zdrojov medzi rôznymi inštitúciami štátu, so zameraním na bezpečnostné charakteristiky, Identity and Access Management (IAM), prepojenie do privátnych sieti (Govnet) a ďalšie.
- Výber vhodných verejných cloudových služieb: Porovnanie dostupných verejných cloudových služieb na trhu a výber tých, ktoré najlepšie vyhovujú potrebám štátu z hľadiska nákladov, bezpečnosti a spĺňania právnych a regulačných požiadaviek zameriavajúc sa na PaaS a SaaS.
- Zabezpečenie cloudových služieb: Zaistiť financovanie cloudových služieb vo verejnej časti, nastavenie schvaľovacieho procesu pre umiestnenie ISVS a obstaranie potrebných cloudových služieb.
- Migrácia a integrácia systémov: Plánovanie a realizácia migrácie ISVS do verejného cloudu, vrátane integrácie s existujúcimi privátnymi vládnymi cloudovými službami a inými IT systémami štátu.
- Monitorovanie a optimalizácia: Sledovanie výkonu a nákladov na cloudové služby po migrácii, a pravidelná optimalizácia využívania zdrojov v súlade s potrebami štátu.
- Vzdelávanie a podpora: Zabezpečenie dostatočnej odbornej prípravy a podpory pre zamestnancov verejnej správy zodpovedných za správu a využitie verejných cloudových služieb.

Poskytovanie odborníkov na cloudové služby vo verejnej časti vládneho cloudu, ktorí zastrešia konzultačné práce a usmernia OVM pri používaní cloudu. Vytvorenie plánu vzdelávania na dlhšie obdobie vopred. Plánované vzdelávacie aktivity rozšíriť aj o vzdelávanie zabezpečené v súčinnosti s najväčšími dodávateľmi cloudových služieb.

- Bezpečnosť a rýchla adopcia: zabezpečenie znovu použiteľných šablón pre urýchlené vytvárania prostredia vo verejnom cloude. Vytvorenie sady bezpečnostných pravidiel, po aplikovaní ktorých, nebude existovať pochybnosť o dostatočnej bezpečnosti cloudového prostredia.
- Sieťové prepojenie: Realizovať prepojenie privátnej siete Govnet s vybranými cloudovými poskytovateľmi. Aktualizácia štandardov pre doménu gov.sk a domény pre sieť Govnet.

6. Pilier 2 - Modernizácia, spoplatnenie a rozšírenie privátnej časti vládneho cloudu

6.1. Prínosy

- Kontrola a bezpečnosť: Vlastný privátny vládny cloud poskytuje verejnej správe väčšiu kontrolu nad svojimi dátami a IT infraštruktúrou, čo zlepšuje bezpečnosť a ochranu citlivých údajov. Privátny cloud môže fungovať aj pri odpojení od verejnej siete internet.
- Prispôsobivosť: Privátny vládny cloud môže byť navrhnutý tak, aby vyhovoval špecifickým potrebám a požiadavkám verejnej správy.
- Integrácia služieb: Privátny vládny cloud umožňuje jednoduchšiu integráciu rôznych kritických IT systémov a služieb verejnej správy.
- Zlepšenie využitia zdrojov: Centrálny privátny cloud môže zvýšiť efektivitu využívania zdrojov a znížiť prevádzkové náklady.
- Spoplatnenie vládneho cloudu: Zavedenie poplatkov za služby privátneho vládneho cloudu motivuje správcov informačných systémov k efektívnejšiemu využitiu zdrojov a optimalizácii nákladov.

6.2. Riziká

- Náklady na implementáciu a prevádzku: Vybudovanie a udržiavanie privátneho vládneho cloudu môže byť finančne náročné, najmä pokiaľ ide o investície do infraštruktúry a personálu.
- Zastaranie technológií: Technológie a riešenia v privátnom vládnom cloude môžu rýchlo zastarávať v porovnaní s rýchlym vývojom v oblasti komerčných cloudových služieb.
- Správa zdrojov: Správa zdrojov v privátnom vládnom cloude môže byť náročná, najmä pokiaľ ide o pridelenie a účinné využitie kapacít.

6.3. Ošetrenie rizík

- Kombinácia privátneho a verejného cloudu: Využitie hybridného cloudového riešenia, ktoré kombinuje privátny vládny cloud s verejnými (komerčnými) cloudovými službami, umožňuje optimalizovať náklady a zdroje.
- Pravidelná aktualizácia technológií: Implementácia plánu pravidelnej aktualizácie technológií a riešení v privátnom vládnom cloudu, aby bol v súlade s najnovšími trendmi a inováciami.
- Efektívna správa zdrojov: Zabezpečenie dostatočných kapacít na úrovni personálu a zlepšenie procesov správy zdrojov v privátnom vládnom cloude.
- Obstarať “eSKa Cloud" ako ”Cloud as a Service! , službu vďaka ktorej sa rôzne cloudové služby, ako infraštruktúra, platformy a softvér, poskytujú používateľom na vyžiadanie a na základe predplatného. Táto služba eliminuje potrebu organizácií investovať do vlastnej fyzickej infraštruktúry a umožňuje im využívať výhody cloudu bez nutnosti nakupovať hardvér a softvér na sklad. Tato služba je dostupná aj na území Slovenskej republiky, pretože je možné ju implementovať v nami zvolenom dátovom centre. Tento typ služby poskytuje škálovateľnosť, flexibilitu, nákladovú efektívnosť a exkluzivitu na území Slovenskej republiky.

6.4.Merateľné ukazovatele

Merateľné ukazovatele druhého piliera, ktorý sa zameriava na základnú koncepciu budovania privátnej časti vládneho cloudu zabezpečením centrálneho privátneho cloudového riešenia, by mali zahŕňať:

Dostupnosť a spoľahlivosť infraštruktúry:

- Percentuálny nárast úrovne dostupnosti centrálneho vládneho privátneho cloudu.
- Počet úspešne riešených incidentov týkajúcich sa infraštruktúry a služieb centrálneho privátneho cloudu.

Čas nasadenia a integrácie systémov:

- Skrátenie časových rámcov pre nasadenie a integráciu nových systémov a služieb v rámci centrálneho vládneho privátneho cloudu.
- Percentuálny pokles doby potrebnej na integráciu nových systémov a služieb do existujúceho prostredia.

Zabezpečenie a zhoda s regulačnými požiadavkami:

- Percentuálny nárast počtu systémov a služieb, ktoré sú v súlade so zákonnými a regulačnými požiadavkami.
- Počet úspešne identifikovaných a riešených bezpečnostných hrozieb a zraniteľností v rámci centrálneho vládneho privátneho cloudu.

Optimalizácia výkonu a zdrojov:

- Percentuálny pokles celkových nákladov na IT infraštruktúru a služby v dôsledku zavedenia spoplatnenia privátneho vládneho cloudu a väčšieho využitia verejných cloudov.
- Percentuálny pokles nevyužitých alebo nadmerných IT zdrojov, ako sú kapacita úložiska, výpočtový výkon a pamäť, v rámci centrálneho vládneho privátneho cloudu.
- Percentuálny nárast efektívnosti využitia existujúcich IT zdrojov v centrálnej vládnej privátnej cloudovej infraštruktúre.

Spokojnosť zákazníkov a účastníkov:

- Percentuálny nárast spokojnosti zákazníkov (verejných inštitúcií) s infraštruktúrou a službami vládneho privátneho cloudu, merateľný prostredníctvom prieskumov spokojnosti alebo hodnotenia služieb.

6.5.Plán realizácie

- Realizácia projektu "eSKa Cloud": Zabezpečenie rýchlej implementácie projektu formou "Cloud as a Service", ktorý bude disponovať štruktúrou a prevádzkovým modelom veľmi podobným verejným cloudovým poskytovateľom.
- Nastavenie poplatkov za privátne vládne cloudové služby: Vývoj a implementácia modelu spoplatnenia služieb privátneho vládneho cloudu, ktorý zohľadňuje náklady na infraštruktúru, prevádzku a správu.
- Zjednodušenie migrácie zo súčasného vládneho cloudu: Zabezpečenie funkcionality pre jednoduchú migráciu v rámci privátneho cloudu prevádzkovaného MV SR, alebo k iným poskytovateľom služieb vládneho cloudu. Jednoduchú migráciu je možné dosiahnuť napríklad zjednotením platformy a zavedením funkcionality jednoduchého importu/exportu, ktorý zohľadní

požiadavky vybraných poskytovateľov služieb vládneho cloudu. Po dosiahnutí nastavenia poplatkov, možnosti jednoduchej migrácie a migrácií prvých projektov, je potrebné zvážiť obnovu, rozšírenie, alebo ukončenie prevádzky lokality Tajov, ktorá je v súčasnosti na konci svojej životnosti.

- Nové služby, redundancia a dostupnosť: Realizácia projektu pre rozšírenie privátnej časti “eSKa Cloud” o druhú lokalitu a pre zabezpečenie financovania služieb vo verejnej časti vládneho cloudu.
- Orientácia na bežne dostupné krabicové riešenia: Pri nákupe uprednostňovať riešenia, ktoré sú bežne dostupné a nie je ich potrebné prispôsobovať a dopĺňať o bežne dostupné funkcionality. Zamerať sa na riešenia, ktoré umožňujú postupné prírastky, nenakupovať na sklad a vytvárať nákupné kanály, ktoré umožnia rýchle obstarávanie.
- Monitorovanie a správa: Zavedenie systému monitorovania výkonu, utilizácie a bezpečnosti pre všetky služby v privátnej časti vládneho cloudu.
- Vzdelávanie a podpora: Poskytovanie odbornej prípravy a podpory pre zamestnancov verejnej správy.
- Rozšírenie privátnej časti vládneho cloudu: Zabezpečenie akreditácie s cieľom zápisu nových cloudových služieb v privátnej časti vládneho cloudu, prevádzkovaných MV SR, MF SR a MIRRI.
- Pravidlá pre redundanciu: Vytvoriť metodické usmernenie, na základe ktorého bude možné určiť, aká redundancia je potrebná pre ISVS (lokálna, geo redundancia). Zabezpečiť cloudové služby, ktoré budú podporovať potrebné spôsoby redundancie.

6.5.1. Rozšírenie privátnej časti Vládneho cloudu – „eSKa Cloud“

Prínosy

- Zlepšená efektívnosť prostriedkov: centrálne cloudové riešenia umožňujú lepšie využitie existujúcich zdrojov a znižujú potrebu investovať do nových, potenciálne neefektívnych riešení.
- Spolupráca medzi inštitúciami: centrálne riešenie cloudu posilňuje spoluprácu medzi rôznymi verejnými inštitúciami a umožňujú zdieľanie zdrojov, znalostí a best practices.
- Flexibilita: "eSKa Cloud" poskytne najväčšiu mieru flexibilitu v rámci verejnej správy, keďže umožňujú rýchlejšie prispôsobenie sa meniacim potrebám a požiadavkám.
- Vyššia bezpečnosť a dostupnosť centrálneho riešenia: Tretí pilier zabezpečuje najvyššiu mieru bezpečnosti a dostupnosti pri prevádzke ISVS vo verejnej správe.
- Zabezpečenie nových cloudových služieb: “eSKa Cloud“ ponúkne nové podporované IaaS, PaaS, SaaS služby v privátnej a verejnej časti. Zabezpečí sa prepojenie s najčastejšie používanými verejnými cloudmi a umožní sa hybridný model prevádzky informačných systémov.

Riziká

- Analýza migrovateľnosti: nedostatočne dôsledne vykonaná analýza migrovateľnosti
- Neochota: vykonávať migrácie
- Nedostatok finančných prostriedkov: na migrácie.

Ošetrovanie rizík

- Obstaranie „krabicového“ riešenia, ktoré bude poskytovať služby podobné ako verejné cloudy
- Vytvorenie štandardov a pravidiel: Zavedenie jasných štandardov a pravidiel pre migrácie.
- Koordinácia a spolupráca medzi inštitúciami: Podpora spolupráce a koordinácie medzi rôznymi verejnými inštitúciami, aby sa podporila migrácia ISVS.
- Zabezpečenie dostatku financií na migračné projekty.

- Zjednodušenie procesu podávania žiadostí o prostriedky na migráciu ISVS

7. Pilier 3 - Sanácia kľúčovej rezortnej infraštruktúry v opodstatnených prípadoch.

7.1. Prínosy

- Spolupráca medzi inštitúciami: Lepšie využitie existujúcich zdrojov, posilnenie spolupráce medzi rezortnými organizáciami čím sa umožní zdieľanie zdrojov, znalostí a best practices.
- Dostupnosť: Lokálne a rezortné cloudové riešenia poskytnú dostupnosť pre systémy, ktoré nie je možné prevádzkovať v inej časti vládneho cloudu.
- Flexibilita: Poskytnutie špecifických služieb, ktoré nedokážu alebo nechcú poskytnúť iní prevádzkovatelia vo vládnom cloude.
- Zníženie závislosti na centrálne riešenia: Tretí pilier znižuje závislosť verejnej správy na veľkých, centralizovaných riešeniach a podporuje diverzifikáciu riešení, čo vedie k vyššej odolnosti voči výpadkom a technickým problémom.

7.2. Riziká rezortných dátových centier

- Náklady na implementáciu a prevádzku: Vybudovanie a udržiavanie rezortného dátového centra môže byť finančne náročné, najmä pokiaľ ide o investície do infraštruktúry-nakupovanie na sklad.
- Zastaranie technológií: Technológie a riešenia v rezortnom dátovom centre môžu rýchlo zastarávať v porovnaní s rýchlym vývojom v oblasti verejných (komerčných) cloudových služieb.
- Správa zdrojov: Správa zdrojov v rezortnom dátovom centre môže byť náročná, najmä pokiaľ ide o pridelenie a účinné využitie kapacít.
- Nedostatočné využívanie zdrojov
- Fragmentácia zdrojov a služieb: Lokálne a riešenia môžu viesť k väčšej fragmentácii IT zdrojov a služieb, čo môže spôsobiť problémy s interoperabilitou a kompatibilitou medzi rôznymi systémami.
- Nedostatočná alebo žiadna štandardizácia: Absencia jasných štandardov a pravidiel pre riešenia v rezortných dátových centrách môže viesť k rôznym prístupom k bezpečnosti, správe a prevádzke týchto riešení, čo môže spôsobiť problémy s udržateľnosťou a škálovateľnosťou.
- Nízka úroveň bezpečnosti: Rezortné dátové centrá môžu byť náchylnejšie na bezpečnostné hrozby, ak nie sú správne zabezpečené a riadené, čo by mohlo viesť k úniku dát alebo zneužitiu zdrojov.
- Duplicita nákladov: Bez koordinácie a zdieľania zdrojov medzi inštitúciami môžu vzniknúť duplicitné náklady na riešenia a infraštruktúru, čo môže viesť k neefektívnym investíciám
- Personálne problémy: nedostatok kvalitného obslužného personálu

7.3. Ošetrenie rizík

- Zavedenie pravidiel pre financovanie: Vytvorenie pravidiel na základe ktorých bude zreteľne, že je vhodné financovať sanáciu a rozvoj lokálneho dátového centra, čím sa zrýchli rozhodovanie a schvaľovanie projektov.
- Vytvorenie štandardov a pravidiel: Zavedenie jasných štandardov a pravidiel pre rezortné dátové centrá, ktoré zabezpečia bezpečnosť a možnosti postupného využívania cloudových služieb.

- Lokálne koncepcie: Vyžadovať vytvorenie koncepcie pre rezortné dátové centrum, ktorá bude jednoznačne definovať cieľový stav a stratégiu pre postupné využívanie služieb vládneho cloudu pokiaľ je to možné.
- Koordinácia a spolupráca medzi inštitúciami: Podpora spolupráce a koordinácie medzi rôznymi verejnými inštitúciami, aby sa zabránilo fragmentácii zdrojov a služieb, ako aj zbytočným nákladom.
- Zabezpečenie a monitorovanie: Implementácia robustných bezpečnostných opatrení a monitorovania v rezortných dátových centrách, aby sa minimalizovalo riziko úniku dát alebo zneužitia zdrojov.
- Konsolidácia a optimalizácia zdrojov: Vykonávanie pravidelných analýz zdrojov a služieb s cieľom identifikovať a eliminovať duplicitné alebo neefektívne riešenia, a optimalizovať využitie existujúcich zdrojov.
- Posúdenie bezpečnosti, dostupnosti a integrity: Zapísať služby rezortných dátových centier a rezortných špecializovaných cloudov do katalógu služieb vládneho cloudu s cieľom posúdiť bezpečnosť a dostupnosť služieb.

7.4. Merateľné ukazovatele

Merateľné ukazovatele tretieho piliera, ktorý sa zameriava na sanáciu infraštruktúry existujúcich rezortných dátových centrách, by mali zahŕňať:

Zabezpečenie dostupnosti informačných systémov:

- Percentuálny pokles nedostupnosti systémov v dôsledku sanácie v existujúcich dátových centrách.

Zníženie duplicity a redundancie systémov:

- Počet úspešne zlučovaných a racionalizovaných systémov, ktoré boli predtým duplicitné alebo redundantné.
- Percentuálny pokles počtu duplicitných a redundantných systémov v rámci štátnej IT infraštruktúry.

Flexibilita a škálovateľnosť riešení:

- Počet úspešne implementovaných a nasadených flexibilných a škálovateľných riešení v rámci rezortných špecializovaných cloudov.
- Percentuálny nárast výkonu a kapacity IT infraštruktúry v dôsledku nasadenia flexibilných a škálovateľných riešení.

Spokojnosť zákazníkov a účastníkov:

- Percentuálny nárast spokojnosti zákazníkov (verejných inštitúcií) s rezortnými špecializovanými cloudovými riešeniami, merateľný prostredníctvom prieskumov spokojnosti alebo hodnotenia služieb.

7.5.Plán realizácie

- Analýza súčasného stavu: Identifikácia a zhodnotenie súčasných IT systémov, ktoré sú kandidátmi na migráciu do vládneho cloudu a ktoré je potrebné prevádzkovať v rezortnom dátovom centre. Aktualizácia evidencie v Centrálnom meta informačnom systéme verejnej správy (MetaIS).
- Monitorovanie a optimalizácia: Sledovanie výkonu, využitia a nákladov na cloudové služby Pravidelná optimalizácia využívania zdrojov v súlade s potrebami štátu.
- Sieťové prepojenie: Realizovať dostatočne robustné prepojenie rezortných dátových centier do privátnej siete GOVNET.
- Orientácia na bežne dostupné krabicové riešenia: Pri nákupe uprednostňovať riešenia, ktoré sú bežne dostupné a nie je ich potrebné prispôsobovať a dopĺňať o bežne dostupné funkcionality. Zamerať sa na riešenia, ktoré umožňujú postupné prírastky, nenakupovať na sklad a vytvárať nákupné kanály, ktoré umožnia rýchle obstarávanie.
- Pravidlá pre redundanciu: Vytvoriť metodické usmernenie, na základe ktorého bude možné určiť aká redundancia je potrebná pre ISVS (lokálna, geo-redundancia). Zabezpečiť cloudové služby, ktoré budú podporovať potrebné spôsoby redundancie.
- Audit a kontrola: Zabezpečenie akreditácie služieb rezortného dátového centra s cieľom zápisu do katalógu služieb vládneho cloudu na dosiahnutej úrovni.

8. Záver

Koncepcia rozvoja vládneho cloudu prináša strategický rámec pre využitie cloudových služieb v prospech štátu a občanov. Tento rámec je založený na troch základných pilieroch: Využívanie služieb verejného cloudu, Modernizácia, spoplatnenie a rozšírenie privátnej časti vládneho cloudu a Sanácia infraštruktúry v rezortných dátových centrách.

Implementácia tejto koncepcie umožní štátu dosiahnuť väčšiu efektívnosť, flexibilitu a transparentnosť pri poskytovaní služieb občanom, pričom zároveň zabezpečí vysokú úroveň bezpečnosti a súkromia pre citlivé údaje a ISVS. Koncepcia rozvoja služieb vládneho cloudu tiež podporuje spoluprácu medzi verejnými inštitúciami a komerčnými poskytovateľmi cloudových služieb, čo vedie k inovácii a zlepšeniu kvality služieb.

Na úspešnú realizáciu tejto koncepcie je potrebné zabezpečiť:

- revíziu a aktualizáciu koncepcie, aby odrážala zmeny v technologických trendoch, potrebách verejnej správy a očakávaniach,
- koordináciu medzi rôznymi úseky verejnej správy a komerčnými poskytovateľmi cloudových služieb pri vývoji a implementácii riešení,
- monitorovanie a hodnotenie výsledkov a efektívnosti implementácie koncepcie, vrátane analýzy nákladov a prínosov,
- podporu vzdelávania a odbornej prípravy pre zamestnancov verejnej správy zodpovedných za správu a využitie cloudových služieb.

Dlhodobá koncepcia rozvoja vládneho cloudu predstavuje dôležitý krok v transformácii verejnej správy pri poskytovaní elektronických služieb občanom. Vytvára rámec pre efektívne využitie cloudových technológií, optimalizáciu nákladov a zabezpečenie vysokého stupňa bezpečnosti, súkromia a spolupráce medzi štátnymi inštitúciami a komerčnými partnermi. Implementácia tejto koncepcie prispeje k modernizácii verejnej správy a zlepšeniu kvality služieb poskytovaných občanom.

9. Skratky a definície

Skratka	Popis
DataCentrum	Organizácia v zriaďovateľskej pôsobnosti Ministerstva financií SR
DC	Dátové centrum
DNS	Domain name system/server
HW	Hardware
IaaS	Infrastructure as a Service
IKT	Informačné a komunikačné technológie
ISVS	Informačný systém verejnej správy
IT	Informačné technológie
LAN	Local Area Network
MIRRI	Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky
MF SR	Ministerstvo financií Slovenskej republiky
MV SR	Ministerstvo vnútra Slovenskej republiky
NKIVS	Národná koncepcia informatizácie verejnej správy
OPIS	Operačný program Informatizácia spoločnosti
PaaS	Platform as a Service
PDC	Primárne dátové centrum
Podporná infraštruktúra	Technologické zariadenia DC zaisťujúce prevádzkové podmienky IKT s definovanou dostupnosťou (elektrické napájanie, chladenie), fyzickú bezpečnosť a požiarnu ochranu
SaaS	Software as a Service
SAN	Storage Area Network
SDN	Software Defined Networking
SLA	Service Level Agreement, zmluva o úrovni poskytovaniaslužby
SW	Software
TCO	Total Cost of Ownership
UPS	Uninterruptible Power Supply - záložný zdroj
VPN	Virtual Private Network
WAN	Wide Area Network

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

10. Príloha 1.: Klasifikácia cloudových služieb

Ponúkané cloudové služby sa podľa obsahu a úrovne parametrov (C, I ,A) spracovávaných údajov, delia na nasledovné kategórie U1,U2,U3,U4.

10.1. Kategória U1

Najmenej citlivou a najmenej kritickou je **kategória U1**, tzv. Open Data (Základná úroveň zabezpečenia). Ponúkaná cloudová služba spracováva údaje, ktoré sú verejne dostupné a použiteľné. Za „Open data“ podľa vyššie uvedených bezpečnostných požiadaviek sa považujú uchovávané a spracovávané údaje úrovne C0I0A0 a C0I1A1. Pre účely posudzovania kvality a vyspelosti cloudovej služby považujeme vývojové a testovacie prostredie za prostredie kategórie U1 za predpokladu, že nebude obsahovať produkčné údaje a nebude na ňom služba produkčne prevádzkovaná.

10.2. Kategória U2

Spracovávané údaje so **Strednou mierou citlivosti** sú zaradené do **kategórie U2 (Stredná úroveň zabezpečenia)** - údaje potrebné pre fungovanie ISVS (napr. neštruktúrované informácie potrebné k vyriešeniu životnej situácie občana, štruktúrované informácie potrebné k vyriešeniu životnej situácie občana). Za údaje, ktoré sú s vyššou mierou citlivosti zaradené do kategórie U2, podľa vyššie uvedených bezpečnostných požiadaviek sa považujú uchovávané a spracovávané údaje úrovne C1I2A2 až C2I2A2.

10.3. Kategória U3

Vysoko citlivé údaje a ich spracovávanie formou ponúkanej cloudovej služby sú zaradené do **kategórie U3 (Vysoká úroveň zabezpečenia)**. Sú to údaje, s ktorými nakladenie je upravené osobitnými právnymi predpismi. Za Regulované údaje podľa vyššie uvedených bezpečnostných požiadaviek sa považujú uchovávané a spracovávané údaje úrovne C3I3A3.

10.4. Kategória U4

Kritické údaje a ich spracovávanie formou ponúkanej cloudovej služby sú zaradené do **kategórie U4 (Kritická úroveň zabezpečenia)**. Sú to údaje, s ktorými nakladenie je upravené osobitnými právnymi predpismi a zároveň vyžadujú uchovávanie a spracovávanie v privátnej časti vládneho cloudu. Za Kritické údaje podľa vyššie uvedených bezpečnostných požiadaviek sa považujú uchovávané a spracovávané údaje úrovne C3I3A3 a zároveň existuje oprávnený záujem, aby pôsobnosť nad týmito údajmi mala výhradne Slovenská republika.

Požiadavky na bezpečnostnú úroveň sú uvedené v nasledujúcej tabuľke. Všeobecné vyjadrenie bezpečnostnej úrovne informácie má tvar C (0, 1, 2, 3), I (0, 1, 2, 3), A (0 ,1, 2, 3).

Bezpečnostná	Žiadna (0)	Nízka (1)	Stredná (2)	Vysoká (3)

požiadavka				
Dôvernosť (C)	Neexistuje požiadavka na dôvernosť informácie.	Neautorizované zverejnenie informácie môže mať obmedzený vplyv na procesy, služby, aktíva a osoby.	Neautorizované zverejnenie informácie môže mať závažný vplyv na procesy, služby, aktíva a osoby.	Neautorizované zverejnenie informácie môže mať obzvlášť závažný vplyv na procesy, služby, aktíva a osoby.
Integrita (I)	Neexistuje požiadavka na integritu informácie.	Neautorizované modifikácia alebo zničenie informácie môže mať obmedzený vplyv na procesy, služby, aktíva a osoby.	Neautorizované modifikácia alebo zničenie informácie môže mať závažný vplyv na procesy, služby, aktíva a osoby.	Neautorizované modifikácia alebo zničenie informácie môže mať obzvlášť závažný vplyv na procesy, služby, aktíva a osoby.
Dostupnosť (A)	Neexistuje požiadavka na dostupnosť informácie.	Nedostupnosť informácie môže mať obmedzený vplyv na procesy, služby, aktíva a osoby.	Nedostupnosť informácie môže mať závažný vplyv na procesy, služby, aktíva a osoby.	Nedostupnosť informácie môže mať obzvlášť závažný vplyv na procesy, služby, aktíva a osoby.

U1	U2	U3	U4

Parametre C, I, A z pohľadu ISVS - informačného aktíva

	C	I	A
0	**verejné** informačné aktíva určené pre verejnosť, ktoré sú získateľné z verejných zdrojov alebo z informácií, ktoré sú pripravené na tento účel alebo sú preklasifikované z inej úrovne prostredníctvom vlastníka a zahŕňajú napríklad informácie z médií, povinne publikované informácie alebo všeobecne dostupné informácie,		
1	**interné**(default) informačné aktíva, ktoré sú používané a prístupné pre všetkých používateľov v rámci organizácie prevádzkovateľa základnej služby bez ohľadu na ich pracovnú rolu; na sprístupnenie týchto aktív tretím stranám je potrebné schválenie zo strany vlastníka informácie,	**nízka** zahŕňa informačné aktíva, ktorých chyba alebo nepresnosť výrazne neohrozí poskytovanú základnú službu,	**nízka** zahŕňa informačné aktíva prevádzkovateľa základnej služby, ktorých výpadok výrazne neohrozí poskytovanú službu alebo pre ktoré existujú alternatívne postupy,
2	**chránené** informačné aktíva, ktoré sú používané a prístupné len určeným skupinám oprávnených osôb a ktorých neautorizované odhalenie, prezradenie alebo zničenie môže mať pre prevádzkovateľa základnej služby negatívny vplyv na poskytovanie služby; prístup k údajom klasifikovaným ako „Chránené“ je riadený pomocou zásady „potreby vedieť“ a zásady „najnižších privilégií“ a je vymedzený výhradne vopred definovaným a schváleným útvarom alebo iným jasne vymedzeným skupinám osôb; tretie strany majú k týmto údajom prístup len v nevyhnutných a jednoznačne definovaných prípadoch schválených vlastníkom,	**stredná** zahŕňa informačné aktíva, ktoré sú dôležité pre činnosť prevádzkovateľa základnej služby a ktorých chyba alebo nepresnosť môže spôsobiť dopad na kontinuitu poskytovanej základnej služby, strategickú oblasť, trhové a operačné riziká,	**stredná** zahŕňa informačné aktíva, ktoré sú dôležité pre činnosť prevádzkovateľa základnej služby a ktorých zlyhanie môže mať dopad na kontinuitu poskytovanej základnej služby, strategickú oblasť, trhové a operačné riziká,

3	**prísne-chránené** informačné aktíva, ktoré sú používané a prístupné len jednotlivým vybraným používateľom prevádzkovateľa základnej služby a ktorých neautorizované odhalenie, prezradenie alebo zničenie môže mať s vysokou pravdepodobnosťou negatívny vplyv na poskytovanie základnej služby; prístup k údajom klasifikovaným ako „Prísne chránené“ je riadený pomocou zásady „potreby vedieť“ a zásady „najnižších privilégií“ a výhradne konkrétnym, vopred definovaným a schváleným osobám; tretie strany majú k týmto údajom prístup len vo výnimočných a jednoznačne definovaných prípadoch schválených vlastníkom alebo na základe ustanovení osobitných predpisov	**vysoká** zahŕňa vybrané kľúčové informačné aktíva, ktoré sú kritické pre činnosť prevádzkovateľa základnej služby a ktorých chyba, nepresnosť bezprostredne ohrozuje poskytovanú základnú službu, s ňou spojené aktivity a reputáciu prevádzkovateľa základnej služby.	**vysoká** zahŕňa vybrané kľúčové informačné aktíva, ktoré sú kritické pre činnosť prevádzkovateľa základnej služby a ktorých zlyhanie bezprostredne ohrozuje poskytovanú základnú službu, s ňou spojené aktivity a dobrú povesť prevádzkovateľa základnej služby.

10.5. Minimálne požiadavky na CSP a poskytované cloudové služby

Pri posudzovaní zhody sa bude klásť dôraz na nasledujúce požiadavky.

Požiadavky	**Povinné**				**Doporučené**			
	U1	**U2**	**U3**	**U4**	**U1**	**U2**	**U3**	**U4**
Certifikát ISO 270001	Nie	Áno	Áno	Áno	Áno	---	---	---
Súlad s ISO 27017	Nie	Áno	Áno	Áno	Áno	---	---	---
Súlad s ISO 27018	Nie	Áno	Áno	Áno	Áno	---		---
Certifikát CSP podľa ENISA *	Nie	Áno Stredná úroveň *	Áno Vysoká úroveň *	Áno Vysoká úroveň *	Áno Základná úroveň *	---	---	---
Audit KB podľa zákona 69/2018	Nie	Nie	Nie	Áno zhoda 90%	Nie	Áno zhoda 80%	Áno zhoda 80%	---
Šifrovanie údajov – BYOK ** minimálne požiadavky	Nie	zdieľané HSM min. FIPS 2	dedikované HSM min. FIPS 2 level 3	dedikované HSM min. FIPS 2 level 3	Áno natívne od CSP	---	---	---

		level 2						
Auditné správy k certifikátom	Nie	Áno	Áno	Áno	Áno	---	---	---
Pre služby SaaS – Penetračné testy	Nie	Áno	Áno	Áno	Áno	---	---	---
Vyplnenie dokumentu „1F_Mapovanie_Pracovna_Príloha “ najme pre lokálnych CSP	Nie	Áno	Áno	Áno	Áno	---	---	---

** Šifrovanie vlastnými kľúčmi zákazník (BYOK)
zdieľané HSM = multi tenant, dedikované HSM = single tenant

* Rozdelenie bezpečnostných úrovní podľa Certifikačnej schémy pre **certifikáciu CSP podľa ENISA**

- Základná úroveň
- Stredná úroveň
- Vysoká úroveň

Tento certifikát sa bude vyžadovať len za predpokladu, že ho bude možne získať na Slovensku alebo v členskom štáte EU.

10.6. Čo patrí do verejnej a čo do privátnej časti vládneho cloudu

Pri rozhodovaní, kde sa má prevádzkovať ISVS, je potrebné vychádzať metodiky pre zaradenie cloudových služieb do katalógu vládnych cloudových služieb a z ohodnotenia konkrétneho ISVS parametrami C-dôvernosť, I-integrita. A-dostupnosť, podľa z pripravovanej **metodiky klasifikácie ISVS podľa údajov s ktorými ISVS pracujú a ktoré uchovávajú**.

10.6.1. ISVS, ktoré musia byť prevádzkované využitím služieb privátnej časti vládneho cloudu

A - ISVS s požiadavkou na U4 / C3, I3, A3

- ISVS, ktoré tvoria základné registre štátu ako - Register právnických osôb, register fyzických osôb, atď.
- ISVS, ktoré sú prvkami kritickej infraštruktúry. Tomu zodpovedá klasifikácia C3, I3, A3 a vyžadujú klasifikáciu cloudových služieb na úrovni U3
- Prípadne iné ISVS podľa rozhodnutia NBÚ

10.6.2. ISVS, ktoré môžu byť prevádzkované využitím služieb verejnej časti vládneho cloudu

Za podmienky zabezpečenia potrebných parametrov dôvernosti, integrity a dostupnosti, pričom potrebné parametre sú rovnaké alebo väčšie ako požadované parametre konkrétneho ISVS.

B - ISVS, ktoré môžu byť v oboch verziách cloudov (A,C)

- Štátne web stránky, portálové riešenia úradov, ISVS agendové, ISVS výkon verejnej moci, atď.
- Preferujeme umiestnenie do verejného cloudu.

C - ISVS s požiadavkou na U1 / C0, I0=1, A0-1

- Open data projekty, informačné portálové riešenia, rôzne ISVS zabezpečujúce dennú agendu úradov, ktoré majú údaje charakterizované ako OpenData, atď.

Využívanie cloudových služieb a umiestnenie ISVS sa musí riadiť podľa kategorizácie Ux{CxIxAx}. Pri umiestnení ISVS a výbere úrovne použitých cloudových služieb Uy{ CyIyAy}, sa postupuje tak aby platilo že X<= Y.

Zoznam ISVS patriacich do kategórie **A** je nutné presne identifikovať podľa **metodiky klasifikácie ISVS podľa údajov s ktorými ISVS pracujú a ktoré ukladajú**. MIRRI bude iniciovať vytvorenie zoznamu ISVS za pomoci CSIRT a NBÚ , ktoré je možné prevádzkovať len z privátnej časti Vládneho cloudu (U4).

10.6.3. Postup pre získanie kategórie potrebných ISVS

- Pre nové systémy: Klasifikácia systému a evidencia v MetaIS sa bude kontrolovať pri schvaľovaní projektovej dokumentácie a následne sa aktualizuje počas realizácie projektu.
- Pre existujúce systémy táto povinnosť vyplýva zo zákona 69/2018 a vyhlášky 362/2018.

11. Príloha 2.: Využitie privátnej časti vládneho cloudu

V súčasnosti privátna časť vládneho cloudu prevádzkovaného na MVSR pozostáva z 2 datacentier (Kopčianska a Tajov), ktorých kapacity sa delia na 2 časti:

- Virtualizované serverové platformy x86 (Windows alebo Linux) - generické využitie
- RISC (Unix) – primárne určené pre databázy

Vládny cloud ponúka virtualizované servery (VM) a diskové kapacity. Preto pri určovaní kapacity pracujeme s jednotkami:

- počet vCPU (virtuálnych jadier, pomer 1:5 s fyzickými jadrami),
- kapacita RAM
- kapacita T1 úložiska - 1280 IOPS
- kapacita T2 úložiska - 150 IOPS
- kapacita T3 úložiska – 100 IOPS

Celková kapacita privátnej časti vládneho cloudu je v súčasnosti nasledovná:

Maximálne použiteľná kapacita					
DC	vCPU	RAM GB	TIER1 GB	TIER2 GB	TIER3 GB
Kopčianska - x86	10240	32768	18573	367922	522382
Kopčianska - RISC	880	22528	1268	103080	141720
Tajov - x86	10240	32768	32547	382820	501217
Tajov - RISC	880	22528	7600	102180	141700
spolu	11120	55296	40147	485000	642917

Z pôvodnej kapacity polovica z celkovej diskovej kapacity RISC priradená pre x86 platformu. Dôvodom je, že RISC časť sa takmer vôbec nepoužíva.

Alokovaná kapacita k 01.06.2024 rozdelená medzi jednotlivé projekty je nasledovná:

Alokovaná kapacita + réžia					
DC	vCPU	RAM GB	TIER1 GB	TIER2 GB	TIER3 GB
Kopčianska - x86	11238	43983	25903,6	551572,4	673633,4
Kopčianska - RISC	69	464	1268,0	34950,0	63900,0
Tajov - x86	7490	32807	22137,4	419916,8	493192,4
Tajov - RISC	168	1198	1764,0	36302,0	12150,0
spolu	7658	34005	23901,4	456218,8	505342,4

K 01.06.2024 maximálne utilizovaná kapacita vyzerá nasledovne:

Max. Utilizovaná kapacita (pre RISC Štatistiky nemáme)					
DC	vCPU	RAM GB	TIER1 GB	TIER2 GB	TIER3 GB
Kopčianska - x86	4897	18712	36834,00	736819,00	830614,00
Tajov - x86	3759	21961	31256,00	674520,00	763214,00

Z reportov vyplýva, že VC je predimenzovaný. Projekty majú požiadavky, ktoré reálne nevyužívajú. Kapacity fyzicky dostupné sú, ale sú zle prerozdelené. Nepoužívajú sa funkcionality virtualizačnej platformy v dostatočnej miere tak, aby sa zabezpečila celá dostupná fyzická kapacita pre projekty.

Ak by sme sa na Štatistiky o utilizácií pozreli cez **priemerné** hodnoty, k 01.06.2024 by Štatistiky vyzerali nasledovne:

Priemer Utilizovaná kapacita (pre RISC Štatistiky nemáme)					
DC	vCPU	RAM GB	TIER1 GB	TIER2 GB	TIER3 GB
Kopčianska - x86	433	2 304	5 606	169 256	25 194
Tajov - x86	262	1 480	4 465	162 401	21 202

Priemerná utilizácia jasne ukazuje, že aktuálne fyzické kapacity vládneho cloudu nie sú dostatočne využívané. Tento problém bude aj naďalej pokračovať, ak nevytvoríme alternatívu k súčasnému vládnemu cloudu, ktorá umožní flexibilnejšie využívanie zdrojov vládneho privátneho cloudu a ak nezačneme motivovať OVM k racionalizácii pridelených zdrojov cez spoplatnenie.

	DC	vCPU	RAM GB	TIER1 GB	TIER2 GB	TIER3 GB
Alokovaná	Kopčianska - x86	109,75%	134,23%	139,47%	149,92%	128,95%
	Kopčianska - RISC	7,84%	2,06%	100,00%	33,91%	45,09%
	Tajov - x86	73,14%	100,12%	68,02%	109,69%	98,40%
	Tajov - RISC	19,09%	5,32%	23,21%	35,53%	8,57%
Max. utilizovaná	Kopčianska - x86	47,82%	57,10%	198,32%	200,27%	159,01%
	Tajov - x86	36,71%	67,02%	96,03%	176,20%	152,27%
Priemerne utilizovaná	Kopčianska - x86	4,23%	7,03%	30,18%	46,00%	4,82%
	Tajov - x86	2,56%	4,52%	13,72%	42,42%	4,23%

Reporty využitia vládneho cloudu sú bežne dostupné na adrese https://www.sk.cloud/data/report.xlsx. Od konca roku 2021 ich MIRRI dostáva na mesačnej báze.