



Nákup cloudových služieb vo verejnom sektore

Príručka – vrátane vzorového znenia RFP pre
rámcovú dohodu o poskytovaní cloudových služieb

2. verzia: február 2022

Predbežné upozornenia

Tento dokument slúži len na informačné účely. Nebol vypracovaný v zmysle právnych požiadaviek na procesy verejného obstarávania v rámci žiadneho konkrétneho regiónu. Zákazníci, ktorí cloud využívajú, sú zodpovední za vlastné nezávislé posúdenie informácií uvedených v tomto dokumente a za akékoľvek použitie produktov alebo služieb poskytovateľa cloudu. Tento dokument nepredstavuje žiadne záruky, vyhlásenia, zmluvné záväzky, podmienky ani zaistenia.

Vzorové dokumenty a ich znenie by sa nemali chápať ako právne poradenstvo, usmernenia alebo rady. Zákazníci, ktorým je cloud poskytovaný, by sa mali poradiť s vlastnými právnymi poradcami o svojich povinnostiach vyplývajúcich z platných zákonov v krajine ich pôsobenia. CISPE sa výslovne zrieka akýchkoľvek záruk, zodpovednosti alebo škôd spojených alebo vyplývajúcich z informácií uvedených v tomto dokumente.

O CISPE

CISPE (*Cloud Infrastructure Services Providers in Europe* – Poskytovatelia služieb cloudovej infraštruktúry v Európe, <https://cispe.cloud>) je nezávislé neziskové združenie. Zastupujeme poskytovateľov služieb cloudovej infraštruktúry v Európe a spolupracujeme s partnermi v priemyselnom sektore a tvorcami politik pri poskytovaní poradenstva a vzdelávaní na tému cloudových služieb a ich úlohy v priemysle, verejnom živote a spoločnosti všeobecne.

Naša rastúca členská základňa zahŕňa spoločnosti pôsobiace vo všetkých krajinách EÚ, ktoré majú sídlo celkovo v 16 európskych krajinách. Združenie je spoločnostiam otvorené za predpokladu, že deklarujú, že aspoň jedna z ich služieb spĺňa požiadavky etického kódexu CISPE na ochranu údajov. Čo robíme:

- Obhajujeme výhody zásad verejného obstarávania podľa princípu „cloud first“ v rámci EÚ a členských štátov EÚ.
- Zapájame sektor cloudovej infraštruktúry, aby sme do roku 2030 dosiahli klimatickú neutralitu.
- Presadzujeme koherentné bezpečnostné požiadavky a technické normy v celej EÚ.
- Podporujeme komplexné požiadavky na ochranu osobných údajov prostredníctvom etického kódexu na ochranu údajov.
- Pracujeme na tom, aby bol trh EÚ s cloudovou infraštruktúrou otvorený, konkurencieschopný a bez uzamknutí.
- Predchádzame neodôvodneným povinnostiam monitorovania obsahu v právnom rámci EÚ.

Naši členovia dodávajú a udržiavajú základné „stavebné bloky pre IT“, ktoré vláde, verejným orgánom a podnikom umožňujú budovať vlastné systémy a poskytovať základné služby miliardám občanov. V tejto úlohe pomáhame pri podpore vývoja špičkových technológií a služieb zahŕňajúcich umelú inteligenciu (AI), prepojené objekty, autonómne vozidlá a 5G, ako aj ďalšiu generáciu technológie mobilného pripojenia.

Etický kódex v oblasti služieb cloudovej infraštruktúry

Etický kódex CISPE na ochranu údajov, ktorý bol prvýkrát zverejnený v septembri 2016, predchádzal platnosti všeobecného nariadenia Európskej únie o ochrane údajov (GDPR). Spĺňa prísne požiadavky nariadenia GDPR, aby pomohol poskytovateľom cloudovej infraštruktúry zaviesť povinnosť plnenia ochrany údajov do praxe a ponúknuť silný rámec, ktorý zákazníkom pomôže vybrať si poskytovateľov cloudu a dôverovať ich službám. Etický kódex CISPE [potvrdil v máji 2021 Európsky výbor pre ochranu údajov](#) (EDPB) a v júni 2021 ho [schválil francúzsky výbor CNIL](#) pôsobiaci ako príslušný orgán. <https://www.codeofconduct.cloud/>

Pakt o klimatickej neutralite dátových centier

Združenie CISPE sa koncom roka 2019 spojilo s Európskou komisiou pri vypracovaní súboru metrík a samoregulačnej iniciatívy na zabezpečenie klimatickej neutrality dátových centier do roku 2030. Táto iniciatíva bola vyvinutá v spolupráci s Európskou asociáciou dátových centier (EUDCA) a ďalšími obchodnými združeniami a hráčmi na trhu s dátovými centrami a v januári 2021 bola predstavená ako „pakt o klimatickej neutralite dátových centier“. <https://www.climateutraldatacentre.net/>

Iniciatíva za spravodlivý softvér

Spolu s CIGREF (francúzskou asociáciou CIO) a s podporou ďalších obchodných združení CIO a poskytovateľov cloudovej infraštruktúry v celej Európe predstavilo združenie CISPE [10 princípov spravodlivého licencovania softvéru pre cloudových zákazníkov](#). Ide o súbor osvedčených postupov pre podniky, ktoré v cloude vidia možnosti inovácie v oblasti rastu a flexibility a ktoré vyzývajú poskytovateľov svojho softvéru, aby zabezpečili plnenie spravodlivých podmienok pri udeľovaní licencií.

<https://www.fairsoftware.cloud/>

GAIA-X

Združenie CISPE bolo jedným z dvadsiatich dvoch zakladajúcich členov GAIA-X – európskej iniciatívy na poskytovanie otvoreného, transparentného a bezpečného digitálneho ekosystému. Združenie CISPE sa v rámci toho už od začiatku zaviazalo naplňať víziu a princípy organizácie GAIA-X a generálny tajomník CISPE bol v júni 2021 opätovne zvolený do správnej rady. Niektoré z nástrojov, na ktoré sa v tejto príručke odkazuje, napríklad [etický kódex na ochranu údajov CISPE](#) a [etický kódex SWIPO IaaS](#) sú užitočné na preukázanie plnenia princípov GAIA-X. <https://www.gaia-x.eu>

CISPE a verejný sektor

CISPE prispieva k diskusii o európskej verejnej politike a pracuje na zabezpečení lepšieho pochopenia úlohy, prínosu a potenciálu sektora cloudovej infraštruktúry v Európe.

Kým modely verejného obstarávania by mali podmieňovať proces prijatia a používania cloud computingu, akvizícia cloudových služieb sa líši od väčšiny tradičných technologických akvizícií, ktoré verejný sektor pozná. Prístupy k obstarávaniu treba prehodnotiť, a preto CISPE nabáda politikov v EÚ, aby na úrovni EÚ prijali ambicióznejší a prezieravejší prístup založený na politických iniciatívach „cloud first“, ktorý pomôže podporiť rast jednotného trhu s cloudovou infraštruktúrou v Európe a bude oporou pri dosahovaní cieľov rastu digitálneho jednotného trhu (Digital Single Market – DSM).

Táto príručka je navrhnutá tak, aby poskytla užitočné rady a podporu verejným orgánom pri obstarávaní cloudových služieb.

Viac informácií

Členovia CISPE: <https://cispe.cloud/members>

Predstavenstvo: <https://cispe.cloud/board-of-directors>

Služby cloud computingu deklarovane podľa etického kódexu CISPE:
<https://www.codeofconduct.cloud/public-register/>

Obsah

Predbežné upozornenia	2
O CISPE	3
Obsah	5
Zhrnutie a účel tejto príručky	1
1.0 Prehľad rámcovej dohody o poskytovaní cloudových služieb	4
2.0 Prehľad RFP na cloudové služby	7
2.1 Nastavenie RFP na cloudové služby	7
2.1.1 Úvod a strategické ciele	7
2.1.2 Časový harmonogram odpovede na RFP	10
2.1.3 Definície	10
2.1.4 Podrobný opis modelu obstarávania a súťaženia na základe rámcovej dohody	11
2.1.5 Minimálne požiadavky na uchádzača – administratívne	15
2.2 Technické požiadavky	17
2.2.1 Minimálne požiadavky	17
2.2.2 Porovnanie medzi dodávateľmi	20
2.2.3 Uzatváranie zmlúv	22
2.3 Bezpečnosť	24
2.3.1 Minimálne požiadavky	24
2.3.2 Porovnanie medzi dodávateľmi	29
2.3.3 Uzatváranie zmlúv	29
2.4 Stanovenie cien	30
2.4.1 Minimálne požiadavky	30
2.4.2 Porovnanie medzi dodávateľmi	32
2.5 Nastavenie plnenia zmluvy/zmluvné podmienky	34
2.5.1 Zmluvné podmienky	34
2.5.2 Podmienky používania softvéru	37
2.5.3 Ako si vybrať dodávateľa na projekt spomedzi ocenených	38
2.5.4 Vstup a odchod	38
3.0 Osvedčené postupy/získané skúsenosti	39
3.1 Riadenie cloudu	39
3.2 Tvorba rozpočtu na cloud	39
3.3 Oboznámte sa s obchodným modelom partnerov	41
3.4 Cloudoví makléri	42
3.5 Zabezpečovanie zdrojov/prieskum trhu pred vydaním RFP	42
3.6 Trvalá udržateľnosť	42
Príloha A – Technické požiadavky na porovnanie medzi účastníkmi výberového konania	44
1. Profil poskytovateľa cloudových služieb	44
2. Globálna infraštruktúra	44
3. Infraštruktúra	45
3.1 Výpočet	45

3.2 Vytváranie siete	48
3.3 Úložisko.....	52
4. Spravovanie	56
5. Bezpečnosť	57
6. Dodržiavanie predpisov	59
7. Migrácie	64
8. Fakturácia	66
9. Riadenie	67
10. Podpora	69
Príloha B – Technické hodnotenie naživo	71
Platforma – príklad technického hodnotenia naživo.....	72
Pracovné zaťaženie: webová aplikácia – príklad technického hodnotenia naživo	80

Zhrnutie a účel tejto príručky

Účelom tejto príručky o **nákup cloudových služieb** je poskytnúť poradenstvo tým zákazníkom cloudu, ktorí si chcú obstaráť cloudové služby prostredníctvom konkurenčného procesu obstarávania (**žiadost o ponuku na cloudové služby – RFP**), ale nemajú dostatok odborných znalostí na vypracovanie rámcovej dohody o poskytovaní cloudových služieb.

Tento dokument slúži len na informačné účely. Nebol vypracovaný v zmysle právnych požiadaviek na procesy verejného obstarávania v rámci žiadnej konkrétnej krajiny alebo regiónu.

Táto príručka zároveň slúži aj ako znenie dodatočných výberových kritérií pre objednávky vyplývajúce z rámcovej dohody (tzv. **call-offs**) alebo **minisúťaže** pri nakupovaní podľa rámcovej dohody o poskytovaní cloudových služieb. Časti tejto príručky sú usporiadané tak, aby pripomínali všeobecnú RFP v oblasti IT. Vzorová všeobecná RFP a znenie výberových kritérií sú doplnené komentárom, ktorý objasňuje, prečo sa RFP na cloud líši od tradičnej RFP v oblasti IT.

Po zverejnení cloudovej stratégie Komisie EÚ, ktorá usmerňuje to, ako budú európske inštitúcie a agentúry modernizovať svoju IT infraštruktúru prostredníctvom prístupu na základe pravidla „cloud first“, združenie CISPE v júli 2019 na podujatí s názvom „Ako transformovať vlády prostredníctvom politiky inteligentného cloudu“ odovzdalo Európskej komisii túto príručku.



2. verzia tejto príručky obsahuje nové usmernenia týkajúce sa nasledujúcich tém: ochrana údajov (časť 2.3.1.1), zmena poskytovateľov cloudu a prenos údajov (časť 2.3.1.2), zmluvné podmienky k poskytovaniu softvéru (časť 2.5.2), trvalá udržateľnosť v cloudu (časť 3.6) a aktualizovaná príloha B Technické hodnotenie naživo.

„Cloudové služby“ sú všetky cloudové technológie a súvisiace služby, ku ktorým môže koncový používateľ potrebovať prístup. Tento pojem popri samotnej cloudovej infraštruktúre zahŕňa konzultačné alebo odborné/spravované služby potrebné na podporu a realizáciu migrácie do cloudu a podporu pracovného zaťaženia v cloudu, ako aj služby cloudového trhoviska (tzv. marketplace), napr. produkty typu „softvér ako služba“ (SaaS).

Vznik cloud computingu ako štandardnej voľby pre IT verejného sektora predstavuje príležitosť na modernizáciu existujúcich stratégií obstarávania. Procesy akvizície zamerané na cloud môžu subjektom verejného sektora umožniť využívať všetky výhody cloudu, ako je prístup k špičkovým inováciám, zvýšená rýchlosť a agilita, zlepšený stav zabezpečenia a riadenie plnenia predpisov – a zároveň dosiahnuť efektívnosť a úsporu nákladov.

Tradičné metódy obstarávania v oblasti IT pri nákupe hardvéru, softvéru a dátových centier sa do nákupu cloudových služieb nepremietajú. V cloudovom modeli sa menia prístupy k cenám, správe zmlúv, zmluvným podmienkam, bezpečnosti, technickým požiadavkám, zmluvám o poskytovaní služieb a ďalším prvkom a používanie existujúcich metód obstarávania v konečnom dôsledku znižuje alebo eliminuje výhody, ktoré cloud prináša.

Jedným z najlepších spôsobov efektívneho nákupu cloudových služieb vo verejnom sektore je **rámcová dohoda o poskytovaní cloudových služieb**. Ide o multiorganizačné pridelenie ponuky cloudov, z ktorej môžu oprávnení nákupcovia pridružení k nákupnej organizácii kupovať cloudové technológie a súvisiace služby, ktoré spĺňajú ich potreby a vyhovujú im. Ako nástroj pre cloudové zákazky umožňujú takéto rámcové dohody nakupovať cloudové služby efektívnym a hospodárnym spôsobom, vďaka čomu majú nákupné organizácie a entity koncových používateľov prístup k celej škále cloudových služieb a v konečnom dôsledku využívajú všetky výhody cloudu: agilnosť, obrovské úspory z rozsahu, škálovateľnosť na dosiahnutie lepšej dostupnosti pri nižších nákladoch, široká paleta funkčnosti, tempo inovácií, schopnosť škálovať do nových geografických oblastí.

Upozorňujeme, že **táto príručka sa zameriava na nákup cloudových technológií typu „Infrastructure as a Service“ (IaaS – infraštruktúra ako služba) a „Platform as a Service“ (PaaS – platforma ako služba), ktoré poskytuje poskytovateľ cloudovej infraštruktúry (CISP)**. Takéto cloudové technológie sa dajú zakúpiť priamo od CISP alebo prostredníctvom sprostredkovateľa CISP. *U distribútorov služieb súvisiacich s cloudovým marketplace (PaaS a SaaS) a cloudových konzultačných služieb by sa v RFP vyžadovali ďalšie zohľadnenia.*

Rovnako upozorňujeme, že tento dokument nepokrýva všetky aspekty vytvárania komplexného rámca na obstarávanie cloudu. Existuje množstvo ďalších dokumentov od odborníkov a analytikov, ktoré pokrývajú otázky, ako sú osvedčené postupy cloudového obstarávania, ako vytvoriť rozpočet pre cloud, riadenie cloudu atď., a dôrazne odporúčame, aby sa takéto rady a dokumenty zohľadnili pri vývoji celkovej stratégie cloudového obstarávania. V **tabuľke 1** nižšie je uvedený prehľad príručky k RFP na cloudové služby aj to, kde sa nachádza vzorové znenie RFP pre každý jeden komponent RFP na cloudové služby.

Tabuľka 1 – Zhrnutie jednotlivých častí príručky k RFP na cloudové služby

Časť	Prehľad a znenie vzorovej RFP
1.0 Prehľad rámcovej dohody o poskytovaní cloudových služieb	Zobrazenie modelu rámcovej dohody o poskytovaní cloudových služieb na vysokej úrovni (skupiny, ako súťažiteľ a uzatváranie zmlúv).
2.0 Prehľad RFP na cloudové služby	Ukážka všeobecného znenia RFP, ktoré pokrýva nižšie uvedené časti, s komentárom vysvetľujúcim zdôvodnenie štruktúry RFP na cloudové služby a použitého jazyka.
2.1 Nastavenie RFP na cloudové služby	2.1.1 Úvod a strategické ciele 2.1.2 Časový harmonogram odpovede na RFP 2.1.3 Definície 2.1.4 Podrobný opis modelu obstarávania a súťaženia na základe rámcovej dohody 2.1.5 Minimálne požiadavky na uchádzača – administratívne
2.2 Technické požiadavky	2.2.1 Minimálne požiadavky 2.2.2 Porovnanie medzi dodávateľmi 2.2.3 Uzatváranie zmlúv
2.3 Bezpečnosť	2.3.1 Minimálne požiadavky 2.3.1.1 Ochrana údajov 2.3.1.2 Zmena poskytovateľov cloudu a prenos údajov 2.3.2. Porovnanie medzi dodávateľmi 2.3.3 Uzatváranie zmlúv

Časť	Prehľad a znenie vzorovej RFP
2.4 Stanovenie cien	2.4.1 Minimálne požiadavky 2.4.2 Porovnanie medzi dodávateľmi
2.5 Nastavenie plnenia zmluvy/zmluvné podmienky	2.5.1 Zmluvné podmienky 2.5.2 Podmienky používania softvéru 2.5.3 Ako si vybrať spomedzi víťazných poskytovateľov 2.5.4 Vstup a odchod
3.0 Osvedčené postupy/získané skúsenosti	3.1 Riadenie cloudu 3.2 Tvorba rozpočtu na cloud 3.3 Oboznámte sa s obchodným modelom partnerov 3.4 Cloudoví makléri 3.5 Zabezpečovanie zdrojov/prieskum trhu pred vydaním RFP 3.6 Trvalá udržateľnosť
Príloha A – Technické požiadavky na porovnanie medzi účastníkmi výberového konania	Zoznam všeobecných požiadaviek na cloudovú technológiu pri objednávkach vyplývajúcich z rámcovej dohody (call-offs) alebo minisúťažiach.
Príloha B – Technické hodnotenie naživo	Vzorový skript pre produkt cloudovej technológie so získanými bodmi (ukážky cloudu ako súčasť call-off alebo minisúťaže).

1.0 Prehľad rámcovej dohody o poskytovaní cloudových služieb

Dobre navrhnutá rámcová zmluva o poskytovaní cloudových služieb môže podporiť nákup cloudových služieb spôsobom, ktorý je prínosom pre zúčastnené organizácie verejného sektora aj pre dodávateľov cloudu. K výhodám dobre navrhutej rámcovej dohody o poskytovaní cloudových služieb patrí:

- **Je prirodzene kooperatívna:**
 - Ak sa pri zadávaní objednávok s podobnými požiadavkami spojí viacero organizácií, výsledkom je pohodlnosť, efektívnosť, zníženie nákladov, ako aj zjednodušený proces objednávaní. Je to efektívny spôsob, ako agregovať dopyt viacerých organizácií verejného sektora po spoločných cloudových technológiách a súvisiacich cloudových službách, ako sú riešenia marketplace a poradenstvo.
- **Kompletný rozsah cloudových služieb:**
 - Popri cloudových technológiách, ktoré poskytujú CISP, a službách súvisiacich s marketplace, môže zahŕňať všetky poradenské/odborné/spravované služby potrebné na plnú podporu a realizáciu migrácie do cloudu a podporu pracovných zaťažení v cloude.
 - Cloudové technológie sa dajú zakúpiť priamo od CISP alebo prostredníctvom určeného sprostredkovateľa.
- **Riadenie zadaní:**
 - Zoraduje rozdielne organizácie/nákupcov podľa spoločného súboru zmluvných podmienok a jedného hlavného zadania, a nie rôznych podmienok a zadaní pre každú organizáciu.
 - Navyše je prínosom pre dodávateľov, pretože zabezpečuje štandardný proces akvizície, zmluvné podmienky a mechanizmus objednávaní, podľa ktorých môžu postupovať, namiesto rozdielnych podmienok pre každú organizáciu verejného sektora.
 - Poskytuje flexibilitu. Vytvorenie, schválenie a plnenie efektívnej zmluvy o poskytovaní cloudových služieb v rámci existujúcich štátnych politík/predpisov si vyžaduje experimentovanie a schopnosť rýchlo sa prispôbiť. Oveľa výhodnejšie je vypracovať rámcovú dohodu, ktorá umožní verejnému sektoru a dodávateľom cloudu spolupracovať na vylepšovaní zmluvy – zmluvne, mechanicky a efektívne. Viacročná zmluva, ktorá nefunguje a nedá sa upraviť, má za následok zlé skúsenosti na strane koncových používateľov z verejného sektora, obstarávacích organizácií a dodávateľov cloudu.
- **Možnosť výberu:**
 - Umožňuje nákupcom vybrať si spomedzi niekoľkých kvalifikovaných CISP a nastavuje vysokú latku pre všetky cloudové služby a súvisiace služby, ako je cloudový marketplace s PaaS/SaaS a cloudové poradenstvo.
 - Umožňuje kontrolu nad počtom dodávateľov v konkrétnom rámci tak, že zabezpečuje, aby bol štandard každého víťaza súťaže primerane preverený.

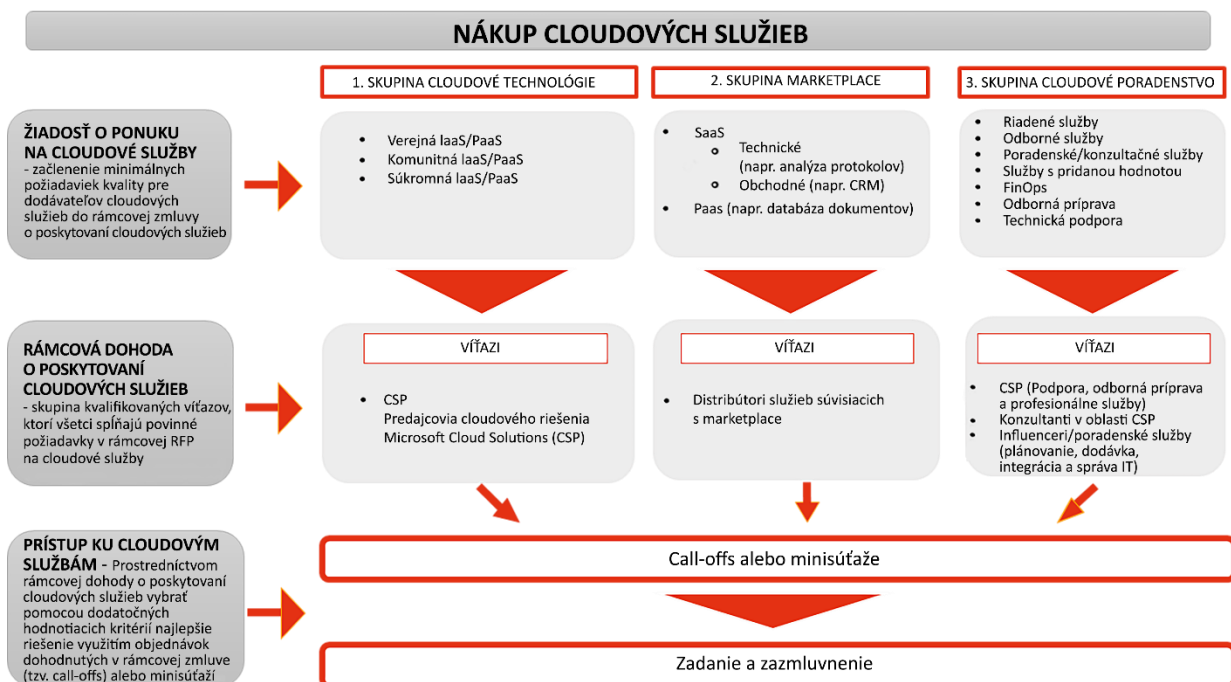
Rámcová dohoda o nákupe cloudových služieb funguje najlepšie, ak zahŕňa základné technológie IaaS/PaaS poskytované CISP s marketplace PaaS/SaaS a konzultačnými službami, ku ktorým môžu v prípade potreby pristupovať koncoví používatelia z verejného sektora, aby im pomohli pri plánovaní, prechode, využívaní a

udržiavaní pracovného zaťaženia realizovaného v cloude. Preto odporúčame, aby sa RFP na cloudové služby pri tvorbe rámcovej dohody o poskytovaní cloudových služieb rozdelila na 3 časti, ako je uvedené nižšie:

- **1. SKUPINA – CLOUDOVÉ TECHNOLOGIE**
Cloudové technológie zakúpené priamo od CISP alebo prostredníctvom určeného sprostredkovateľa CISP.
- **2. SKUPINA – MARKETPLACE**
Prístup na marketplace so službami typu PaaS a SaaS.
- **3. SKUPINA – CLOUDOVÉ PORADENSTVO**
Konzultačné služby súvisiace s cloudom (školenia, odborné služby, spravované služby atď.) a technická podpora.

Ako už bolo uvedené, tento dokument sa zameriava na nákup cloudových technológií typu IaaS a PaaS (1. SKUPINA), ktoré poskytuje CISP (sú zakúpené priamo od CISP alebo prostredníctvom sprostredkovateľa CISP). V prípade dodávateľov, ktorí spadajú do 2. a 3. SKUPINY z hľadiska RFP na cloudové služby, by boli potrebné samostatné kvalifikačné požiadavky na dodávateľa.

Na **obrázku 1** nižšie je na vysokej úrovni zobrazené to, ako môže dobre štruktúrovaná RFP na cloudové služby, rozdelená do týchto troch skupín, viesť k vypracovaniu rámcovej dohody o poskytovaní cloudových služieb, ktorá subjektom verejného sektora zabezpečuje agilitu (technicky aj zmluvne), viditeľnosť a kontrolu výdavkov a používanie cloudu aj s možnosťou prístupu k všetkým cloudovým službám potrebným na vybudovanie a údržbu požadovaných riešení.



Obrázok 1 – Úspešná RFP na cloudové služby je rozdelená do 3 skupín. Každá skupina obsahuje kategórie alebo „typy ponuky“, ktoré pod ňu spadajú, aby sa zabezpečila technická a zmluvná primeranosť na splnenie požiadaviek koncového používateľa pri nakupovaní podľa rámcovej dohody o poskytovaní cloudových služieb.

Upozorňujeme, že:

- Každá skupina má viacero víťazov súťaže.
- Tretia SKUPINA by mohla byť zadaná prostredníctvom inej RFP alebo prípadne prostredníctvom existujúcej zmluvy na poradenské služby.

Kategórie 1. SKUPINY

Úspešné rámcové dohody o poskytovaní cloudových služieb vyžadujú od CISP opis ponúkaného modelu cloudu, rozdelený do kategórií v rámci jednotlivých skupín. Na definície **verejného** cloudu, **komunitného** cloudu a **súkromného** cloudu odporúčame použiť zavedený štandard pre cloud computing ([základné charakteristiky cloudu podľa Národného inštitútu pre štandardy a technológie \(NIST\)](#)). Štruktúrovanie rámcovej dohody o poskytovaní cloudových služieb týmto spôsobom umožňuje obstarávajúcej agentúre a verejným orgánom, ktoré využívajú rámec, vybrať si z rôznych modelov cloudu, ktoré vyhovujú ich potrebám.

Definície každého cloudového modelu v rámci 1. SKUPINY (verejné IaaS/PaaS, komunitné IaaS/PaaS a súkromné IaaS/PaaS) podľa NIST nájdete v *časti 2.1.3 Definície*.

Ako súťažiť – objednávky vyplývajúce z rámcovej dohody alebo minisúťaže?

Kvalifikačné kritériá pre RFP na cloudové služby by mali pokrývať kritické prvky a minimálne štandardy a nemali by zahŕňať „doplňkové“ štandardy. Pridanie doplnkových štandardov, ktoré presahujú základnú úroveň, môže u dodávateľov spĺňajúcich požiadavky definovaného rámca viesť k tomu, že niektorí z nich nebudú môcť predkladať ponuky a v konečnom dôsledku budú mať nákupcovia menší výber.

Po RFP a následnom nastavení rámcovej dohody o poskytovaní cloudových služieb si môžu orgány verejného sektora, ktoré sú zmluvnými stranami príslušného rámca, objednať alebo „doobjednať“ požadované cloudové služby podľa potreby. Uzavretie zmluvy o doobjednaní na základe rámcovej dohody umožňuje kupujúcim spresniť požiadavky s dodatočnou funkčnou špecifikáciou pre konkrétnu objednávku, pričom si zachovávajú výhody vyplývajúce z rámcovej dohody.

V prípade potreby sa môže uskutočniť minisúťaž, v ktorej sa určí najlepší dodávateľ pre konkrétny pracovný rozsah alebo projekt. V minisúťaži prejde zákazník do ďalšej súťaže podľa rámcovej dohody s tým, že vyzve všetkých dodávateľov v rámci skupiny, aby reagovali na súbor požiadaviek. Zákazník vyzve všetkých kvalifikovaných dodávateľov v skupine, aby predložili ponuku, a preto je dôležité pre víťazov minisúťaže uviesť v RFP na cloudové služby minimálne požiadavky. Zabezpečí sa tak vysoký štandard možností v rámci každej skupiny.

*Upozorňujeme, že je dôležité, aby pre každú skupinu existovali **odlišné súbory zmluvných podmienok**, ako je uvedené vyššie na obrázku 1. „Univerzálny prístup“ k uzatváraniu zmlúv pre všetky skupiny bude mať za následok problémy týkajúce sa technickej realizovateľnosti a kompatibility.*

2.0 Prehľad RFP na cloudové služby

V tejto časti je opísaný model a rozsah RFP na cloudové služby vrátane: strategických cieľov, účastníkov, definícií, časovej osi a minimálnych administratívnych požiadaviek. Opäť pripomínáme, že táto príručka sa zameriava na **1. SKUPINU – CLOUDOVÉ TECHNOLOGIE**.

2.1 Nastavenie RFP na cloudové služby

Subjektom verejného sektora dôrazne odporúčame, aby pri nastavovaní RFP na cloudové služby jasne vyjadrili svoje ciele a požiadavky na vysokej úrovni.

2.1.1 Úvod a strategické ciele

V záujme dosiahnutia jasného vyjadrenia strategických cieľov sa osvedčilo formulovať ich hneď v úvode RFP na cloudové služby, a to nasledovne: **(1)** obchodné ciele a výhody, ktoré sa organizácia usiluje dosiahnuť používaním cloudu; **(2)** štruktúra rámcovej dohody – kto nakupuje, kto prevádzkuje, kto zostavuje rozpočet atď.; **(3)** jasné vyjadrenie modelu zdieľanej zodpovednosti medzi verejným sektorom a dodávateľmi cloudu, ktorý je základom úspešného nákupu a používania cloudu a **(4)** typ vzťahu vytvoreného medzi poskytovateľmi cloudových služieb (CISP), distribútormi služieb na marketplace, konzultantmi, štátnymi obstarávacími/zmluvnými agentúrami a štátnymi koncovými používateľmi. Vyjadrenie týchto štyroch bodov pomáha organizáciám vypracovať RFP, ktorá najlepšie vyhovuje ich potrebám a navyše bude zaistené, že zákazníci aj dodávatelia budú mať jasno v otázke výstupov RFP.

RFP na cloudové služby sa zámerne líši od tradičných RFP v oblasti IT. Cloudová technológia nie je jednoduchou náhradou tradičných výpočtových metód. Predstavuje úplne nový spôsob spotreby technológie. Dobre navrhnuté RFP na cloudové služby môžu pomôcť subjektom verejného sektora rýchlo reagovať a využívať výhody cloudu.

Zo všetkých aspektov nákupu cloudu, ktoré uvádzame ako osvedčený postup, je azda najlepším východiskovým bodom jasné vyjadrenie modelu zdieľanej zodpovednosti. Model zdieľanej zodpovednosti¹ sa väčšinou používa pri diskusiách o zabezpečení a dodržiavaní predpisov v cloude, ale toto vymedzenie zodpovedností sa vzťahuje na všetky aspekty cloudových technológií. V RFP na cloudové služby by malo byť jasné, čo je v kompetencii CISP v cloudovom prostredí a za čo zodpovedá zákazník. Napríklad CISP poskytuje možnosti na monitorovanie zdrojov a aplikácií, ktoré sa v cloude používajú, **ale** je na zákazníkovi, aby tieto možnosti, ktoré mu CISP poskytuje, skutočne využíval, pretože to CISP pri pôsobení vo veľkom rozsahu nedokáže robiť pre milióny zákazníkov.

Zákazníci cloudu by mali navyše vedieť, ako partnerská sieť CISP pomáha zákazníkovi využívať cloud a spravovať ich povinnosti. Napríklad poskytovateľ spravovaných služieb (MSP) cez cloud môže zákazníkovi pomôcť nakonfigurovať a používať monitorovacie funkcie poskytované CISP v záujme plnenia ich jedinečných požiadaviek na dodržiavanie predpisov a audit.

Jednoducho povedané, zodpovednosti v modeli cloudu sú nasledovné:

¹ Viac o poskytovateľoch služieb cloudovej infraštruktúry nájdete v 5. časti etického kódexu CISPE: https://cispe.cloud/website_cispe/wp-content/uploads/2017/06/Code-of-Conduct-27-January-2017-corrected-march-20.pdf

CISP poskytuje cloudovú technológiu

Zákazník využíva cloudovú technológiu

Poradenské firmy (ak sú) pomáhajú zákazníkovi pristupovať ku cloudovej technológii a využívať ju

„Poradenské firmy“ sú spoločnosti poskytujúce konzultačné a spravované/odborné služby, ktoré pomáhajú zákazníkovi navrhovať, stavať, vytvárať, migrovať a spravovať ich pracovný rozsah a aplikácie v cloude. Medzi takéto firmy patria integrátori systémov, strategickí konzultanti, agentúry, poskytovatelia spravovaných služieb a sprostredkovatelia s pridanou hodnotou.

Predstavte si „nakupovanie“ cloudových služieb ako analogické nakupovanie v železiarstve. V železiarstve je k dispozícii rozsiahly sortiment materiálov a nástrojov na zostavenie toho, čo potrebujete. Môžete si zložiť skrinku alebo postaviť bazén prípadne celý dom – je to na vás. Keď si kúpite materiály a nástroje, personál železiarstva vám môže ponúknuť poradenstvo a odborné znalosti, ale nepríde k vám domov, aby vám niečo postavil. Máte teda niekoľko možností:

1. Sami si kúpite materiály a nástroje a sami si postavíte, čo chcete.
2. Sami si kúpite materiály a nástroje a potom si najmete niekoho, kto vám postaví, čo chcete, a/alebo bude prevádzkovať, čo chcete.
3. Najmete si niekoho, kto vám postaví, čo chcete, a/alebo bude prevádzkovať, čo chcete, a zároveň ho požiadate, aby v rámci cenovej ponuky zabezpečil aj materiály a nástroje.

Ak má organizácia interné zručnosti na to, aby si sama vybudovala a spravovala svoje cloudové prostredie a riešenia, potom vlastne potrebuje len prístup k štandardizovaným cloudovým technológiám a nástrojom od CISP (priamo s CISP alebo prostredníctvom sprostredkovateľa CISP – pozri **1. SKUPINU**). Potrebný softvér s SaaS a PaaS by mal byť dostupný na cloudovom marketplace (**2. SKUPINA**). Ak sú potrebné ďalšie konzultácie, migrácia, implementácia a/alebo pomoc so správou, práve tu vstupuje do hry partnerská sieť CISP (**3. SKUPINA**).

Znenie vzorovej RFP: Úvod a strategické ciele

Cloud computing poskytuje organizáciám verejného sektora rýchly prístup k širokému spektru flexibilných a nízkonákladových IT zdrojov s platbou podľa používania. Organizácie môžu využiť správny typ a veľkosť zdrojov, ktoré potrebujú na podporu svojich najnovších nápadov alebo na prevádzku svojich IT oddelení, čím sa zbavia potreby veľkých investícií do hardvéru a/alebo dlhodobých licenčných zmlúv na softvér.

<ORGANIZÁCIA> má požiadavku na prístup k týmto typom komerčne dostupných cloudových technológií, aby uspokojila svoje obchodné potreby v rámci širokého spektra pridružených organizácií.

Hlavným cieľom tejto RFP je podpísanie nevýhradnej paralelnej <RÁMCOVEJ DOHODY> s maximálne <x> poskytovateľmi zastupujúcimi rôzne cloudové technológie a cloudové služby.

1. **1. SKUPINA** Poskytovatelia cloudových služieb (CISP) alebo sprostredkovatelia CISP na nákup cloudových technológií.
2. **2. SKUPINA** Poskytovatelia služieb marketplace.

3. **3. SKUPINA** Poskytovatelia poradenských služieb, ktorí poskytnú ďalšie odborné znalosti na migráciu a využitie týchto ponúk CISP.

Pokiaľ ide o **1. SKUPINU**, zúčastnené organizácie (CISP alebo sprostredkovatelia CISP) musia preukázať, ako ich ponuka spĺňa tieto ciele:

- **Agilita** – Sprístupnenie IT zdrojov koncovým používateľom v priebehu niekoľkých minút namiesto tradičných týždňov a mesiacov.
- **Inovácie** – Okamžitý prístup k najnovším a najinovatívnejším technológiám na trhu.
- **Náklady** – Obchodné kapitálové náklady na variabilné náklady (napr. CapEx až OpEx). Platí sa len za to, koľko sa spotrebuje.
- **Rozpočtovanie** – Zobrazenie informácií o fakturácii a používaní na podrobnej aj súhrnnej úrovni, vizualizácia vzorov výdavkov v priebehu času, ako aj prognózy budúcich výdavkov.
- **Elasticita** – Dosiahnutie nižších variabilných nákladov vďaka vyšším úsporám z rozsahu, ktoré poskytuje cloud.
- **Kapacita** – Eliminácia odhadov, pokiaľ ide o kapacitné potreby infraštruktúry.
- **Koniec spoliehania sa na dátové centrá** – Zameranie sa skôr na záležitosti našich občanov než na ťažké zdvíhanie regálov, stohovanie a napájanie serverov.
- **Zabezpečenie** – Formalizácia návrhu účtu s lepšou viditeľnosťou a auditovateľnosťou zdrojov a elimináciou nákladov na ochranu zariadení a fyzického hardvéru.
- **Zdieľaná zodpovednosť** – Redukcia prevádzkovej záťaže, keďže CISP prevádzkuje, spravuje a kontroluje komponenty od hostiteľského operačného systému a virtualizačnej vrstvy až po fyzické zabezpečenie zariadení, v ktorých služba funguje.
- **Automatizácia** – Integrácia automatizácie do cloudovej architektúry na zlepšenie schopnosti bezpečnejšieho škálovania rýchlejšie a nákladovo efektívnejšie.
- **Riadenie cloudu** – (1) začať s kompletným inventárom všetkých IT aktív; (2) centrálné spravovať všetky tieto aktíva a (3) vytvoriť upozornenia týkajúce sa používania/fakturácie/zabezpečenia/atď. – to všetko s funkciami na sledovanie aktív, správu zásob, správu zmien, správu a analýzu protokolov a celkovú viditeľnosť a riadenie cloudu.
- **Kontrola** – Získanie úplného prehľadu o tom, ako sa využívajú IT služby a kde sa dajú doladiť z hľadiska zabezpečenia, spoľahlivosti, výkonu a nákladov.
- **Reverzibilita** – Nástroje a služby prenosnosti na pomoc pri migrácii do a z infraštruktúry CISP, čím sa minimalizuje uzamknutie zákazníka (tzv. vendor lock-in) a rešpektuje sa zaužívaný etický kódex
- **Ochrana údajov** – Schopnosť preukázať plnenie všeobecného nariadenia o ochrane údajov (GDPR) prostredníctvom špecializovaného etického kódexu v súvislosti so službami cloudovej infraštruktúry: etický kódex CISPE na ochranu údajov.
- **Transparentnosť** – Zákazníci by mali mať právo poznať polohu infraštruktúr používaných na spracovanie a ukladanie svojich údajov (mestská oblasť).
- **Klimatická neutralita** – Zákazníci by mali spolupracovať s CISP, ktorí prijímajú preukázané konkrétne opatrenia na splnenie cieľov klimatickej neutrality do roku 2030 a sú signatármi paktu o klimaticky neutrálnych dátových centrách. To pomôže zákazníkom splniť si vlastné ciele v oblasti klimatickej neutrality.

2.1.2 Časový harmonogram odpovede na RFP

Pri vytváraní rámcovej dohody o poskytovaní cloudových služieb a súvisiacej RFP na cloudové služby sa osvedčilo poskytnúť uchádzačom časový harmonogram s predpokladanými činnosťami pri predkladaní ponuky. Čím väčšia angažovanosť v odvetví, tým lepšie, pretože to pomôže zabezpečiť, aby všetky strany jasne rozumeli požiadavkám RFP a najmä tomu, ako všetky služby dodávateľov zapadajú do modelu cloudových služieb.

Upozorňujeme, že časový harmonogram uvedený v žiadosti o ponuku podlieha miestnym zákonom a právnym povinnostiam a zoznam uvedený nižšie slúži len ako príručka osvedčených postupov, nie ako predpisový zoznam činností a časových rámcov.

Znenie vzorovej RFP: Časový harmonogram odpovede

Pozrite si časový harmonogram RFP v prípade RFP na cloudové služby:

Časový harmonogram RFP na cloudové služby
• <i>Vydanie žiadosti o informácie (RFI):</i> • <i>Odpoveď na RFI:</i> • <i>Vydanie predbežnej žiadosti o ponuku (RFP):</i> • <i>Termín odpovede na predbežnú RFP:</i> • <i>Fáza odbornej konzultácie: <časové harmonogramy></i> • <i>Vydanie predkvalifikačnej RFP:</i> • <i>Odpoveď na predkvalifikačnú RFP:</i> • <i>Vydanie RFP:</i> • <i>Termín predloženia otázok v 1. kole:</i> • <i>1. kolo odpovedí:</i> • <i>Termín predloženia otázok v 2. kole:</i> • <i>2. kolo odpovedí:</i> • <i>Termín odpovede na RFP:</i> • <i>Obdobie objasnenia ponuky:</i> • <i>Obdobie rokovania:</i> • <i>Dátum plánovaného vyhlásenia víťaza:</i> • <i>Dátum podpísania zmluvy:</i> • <i>Platnosť zmluvy (možnosti predĺženia):</i>

2.1.3 Definície

RFP na cloudové služby má obsahovať podrobný zoznam definícií. V tomto zozname sú uvedené roly dodávateľov (napr. poskytovateľ cloudových služieb, sprostredkovateľ cloudu, partnerský dodávateľ), všeobecné technologické koncepty (výpočtová technika, úložisko, IaaS/PaaS, SaaS) a ďalšie kľúčové časti zmluvy. Toto je vzorový zoznam definícií:

Znenie vzorovej RFP: Vymedzenie pojmov

Nižšie uvedené pojmy sú definície, ktoré používa Národný inštitút pre štandardy a technológie (NIST) v oblasti cloud computingu.²

- **Infraštruktúra ako služba (IaaS).** Schopnosť poskytovaná spotrebiteľovi spočíva v zabezpečení spracovania, ukladania, sietí a iných základných výpočtových zdrojov, v ktorých je spotrebiteľ schopný nasaďovať a spustiť ľubovoľný softvér, čo môže zahŕňať operačné systémy a aplikácie. Spotrebiteľ nespravuje ani neriadi základnú cloudovú infraštruktúru, ale má kontrolu nad operačnými systémami, úložiskom a nasadenými aplikáciami a prípadne aj obmedzenú kontrolu nad vybranými sieťovými komponentmi (napr. hostiteľskými firewallmi).
- **Platforma ako služba (PaaS).** Spotrebiteľ získava schopnosť nasaďovať do cloudovej infraštruktúry ním vytvorené alebo obstarané aplikácie vytvorené pomocou programovacích jazykov, knižníc, služieb a nástrojov podporovaných poskytovateľom. Spotrebiteľ nespravuje ani nekontroluje základnú cloudovú infraštruktúru (vrátane siete, serverov, operačných systémov alebo úložiska), ale má kontrolu nad nasadenými aplikáciami a môže mať kontrolu aj nad konfiguračnými nastaveniami pre prostredie hostovania aplikácií.
- **Softvér ako služba (SaaS).** Spotrebiteľ získava schopnosť používať aplikácie poskytovateľa bežiacie na cloudovej infraštruktúre. Aplikácie sú prístupné z rôznych klientskych zariadení buď cez rozhranie tenkého klienta (tzv. thin client), ako je webový prehliadač (napr. webový e-mail), alebo cez programové rozhranie. Spotrebiteľ nespravuje ani nekontroluje základnú cloudovú infraštruktúru (vrátane siete, serverov, operačných systémov, úložiska a dokonca ani funkcie jednotlivých aplikácií), azda s výnimkou obmedzených nastavení konfigurácie aplikácií špecifických pre používateľa.
- **Verejný cloud.** Cloudová infraštruktúra je poskytovaná na otvorené používanie širokou verejnosťou. Môže ju vlastniť, riadiť a prevádzkovať obchodná, akademická alebo štátna organizácia alebo ich kombinácia. Existuje v lokálnom prostredí poskytovateľa cloudu.
- **Komunitný cloud.** Tento typ cloudovej infraštruktúry je poskytovaný špecifickej komunite spotrebiteľov z organizácií, ktoré majú spoločné záujmy (napr. poslanie, bezpečnostné požiadavky, zásady a pravidlá týkajúce sa plnenia zásad), na výhradné použitie. Môže ju vlastniť, riadiť a prevádzkovať jedna alebo viacero organizácií v komunite, tretia strana alebo ich kombinácia a môže existovať v lokálnom prostredí alebo mimo lokálneho prostredia.
- **Hybridný cloud.** Táto cloudová infraštruktúra je zložením dvoch alebo viacerých odlišných cloudových infraštruktúr (súkromných, komunitných alebo verejných), ktoré zostávajú jedinečnými entitami, ale sú spojené štandardizovanou alebo chránenou technológiou, ktorá umožňuje prenosnosť údajov a aplikácií (napr. metóda cloud bursting na vyrovnávanie zaťaženia medzi cloudmi).
- **Súkromný cloud.** Táto cloudová infraštruktúra je poskytovaná na výhradné použitie len jednej organizácii, ktorá zahŕňa viacerých spotrebiteľov (napr. obchodné útvary). Môže ju vlastniť, riadiť a prevádzkovať organizácia, tretia strana alebo ich kombinácia a môže existovať v lokálnom prostredí alebo mimo lokálneho prostredia.

2.1.4 Podrobný opis modelu obstarávania a súťaženia na základe rámcovej dohody

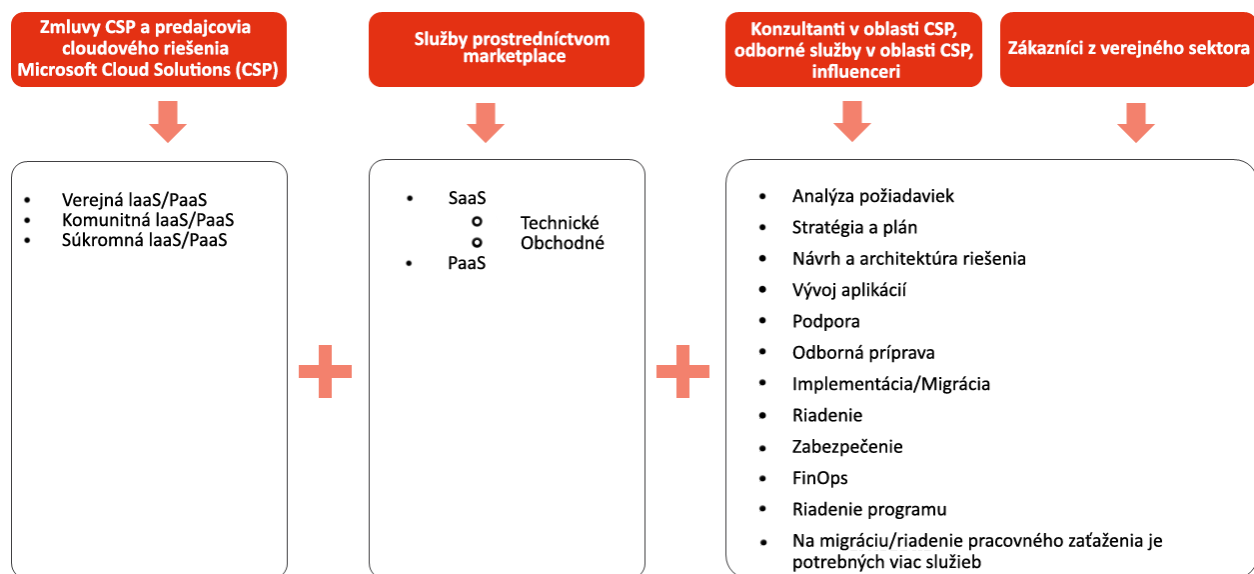
Ako je uvedené vyššie, organizácie verejného sektora by mali identifikovať model toho, ako bude rámcová dohoda fungovať ako nákupný mechanizmus pre cloudové technológie a súvisiace služby implementácie a správy. Práve to by malo byť v RFP na cloudové služby jasne uvedené, aby dodávatelia cloudových technológií, súvisiace organizácie poskytujúce poradenstvo, distribútori služieb marketplace a nakupujúce subjekty rozumeli svojim príslušným úlohám.

² <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>

Pokiaľ ide o rozsah rámcovej dohody a v nadväznosti na objednávky vyplývajúce z rámcovej dohody alebo minisúťaže, organizácie by mali zvážiť nasledovné:

- Kto bude zodpovedný za integráciu a spravované služby zahŕňajúce využívanie cloudových technológií na základe zmluvy.
- Existuje požiadavka, aby sprostredkovateľ CISP/partner poskytoval iné služby s pridanou hodnotou popri udržiavaní zmluvného vzťahu s CISP, poskytovaní konsolidovaných fakturačných služieb a včasného a priameho prístupu k údajom o používaní a fakturácii spojeným s používaním služieb poskytovateľa cloudu?
- Existuje nejaká požiadavka na sprostredkovateľa s pridanou hodnotou v plnom rozsahu, systémového integrátora alebo poskytovateľa spravovaných služieb alebo na akúkoľvek formu služieb zabezpečenia pracovnej sily v oblasti IT?

Je dôležité poznamenať, že CISP nie je systémový integrátor (SI) ani poskytovateľ spravovaných služieb (MSP). Mnoho zákazníkov z verejného sektora bude pre svoje IaaS/PaaS potrebovať CISP a služby poradenstva a odborného plánovania, migrácie a správy bude externe zadávať SI alebo MSP. Vykreslenie vymedzenia úloh a zodpovedností v modeli cloudových služieb nájdete nižšie na **obrázku 2**.



Obrázok 2 – RFP na cloudové služby by mala koncovým používateľom poskytnúť ponuku všetkých cloudových služieb, ktoré potrebujú. Zákazníci z verejného sektora budú pre cloudové technológie potrebovať CISP, v prípade potreby marketplace pre produkty PaaS a SaaS. Následne si zákazník môže určiť, akú veľkú rolu chce prevziať pri poskytovaní cloudových služieb a koľko úloh plánuje zadávať externe konzultačnej firme/systémovému integrátorovi/poskytovateľovi spravovaných služieb/atď.

Nižšie uvedené vzorové znenie formujú roly a povinnosti, ako je znázornené na obrázku 2 vyššie. Rámcová dohoda o poskytovaní cloudových služieb a súvisiaca RFP na cloudové služby by mali zabezpečiť, aby kupujúci mali možnosť primerane posúdiť ponuky každého dodávateľa, čo im umožní vybrať si zo služieb potrebných pre ich pracovný rozsah/projekt. Najlepšie sa to dosiahne rozdelením služieb do skupín (ako už bolo spomenuté) a objasnením spôsobu, akým sa podľa rámcovej dohody realizujú objednávky (call-offs) a minisúťaže.

Znenie vzorovej RFP: Model obstarávania

Táto zmluva bude slúžiť ako **rámcový** prostriedok pri obstarávaní. Táto rámcová dohoda o poskytovaní cloudových služieb bude pokrývať viacero skupín, ktoré definuje <ORGANIZÁCIA> a ktoré sa budú týkať cloudových technológií a súvisiacich služieb/produktov na marketplace, konzultačných služieb, odborných služieb/systémovej integrácie/spravovaných služieb/migrácie, odbornej prípravy a podpory podľa definície <ORGANIZÁCIE>, a bude ju používať viacero oprávnených nákupcov pridružených k <ORGANIZÁCIÍ>. Tým sa zjednoduší proces obstarávania a zároveň sa optimalizujú úspory z rozsahu.

Po ustanovení tejto rámcovej dohody môže organizácia nakupovať konkrétne cloudové technológie a služby súvisiace s cloudom, keď ich bude potrebovať – na rozdiel od nákupu prostredníctvom samostatných obstarávaní. Vďaka tomuto prístupu sa redukujú administratívne požiadavky a výrazne sa zjednoduší proces obstarávania aj doba cyklu.

Rámcová dohoda bude platná maximálne <X> roky/rokov vrátane jej prípadných predĺžení. Maximálna dĺžka platnosti zmluvnej objednávky vyplývajúcej z rámcovej dohody je zvyčajne <X> mesiace/mesiakov. Táto doba sa môže predĺžiť o <X> mesiace/mesiakov a potom o ďalšie <X> mesiace/mesiakov s príslušnými internými súhlasmi, ak je to potrebné na predĺženie platnosti zmluvnej objednávky. Táto skutočnosť bude špecifikovaná pri každej jednej **objednávke** vyplývajúcej z rámcovej dohody.

RÁMEC je rozdelený do 3 (troch) skupín.

1. **1. SKUPINA: CLOUDOVÉ TECHNOLOGIE** – kompletný rozsah technológií poskytovateľov cloudu (priamo od CISP, od sprostredkovateľa alebo od sprostredkovateľa so službami/podporou s pridanou hodnotou):
 - i. **Služby typu IaaS a PaaS** – ponuka cloudových technológií, napr. výpočtová technika, úložisko, sieť, databáza, analytika, aplikačné služby, nasadenie, správa, vývojár, internet vecí (IoT) atď.). Zahŕňa cloudové technologické riešenia v balíkoch, ako sú DR/COOP, Archív, Big Data a analýza, DevOps atď.
2. **2. SKUPINA: MARKETPLACE** – kompletný rozsah služieb/produktov typu PaaS a SaaS, ako je účtovníctvo, CRM, dizajn, HR, GIS a mapovanie, HPC, BI, správa obsahu, analýza protokolov atď.
3. **3. SKUPINA: CLOUDOVÉ PORADENSTVO** – kompletný rozsah konzultačných služieb (spravované služby, odborné služby, poradenské/konzultačné služby, služby s pridanou hodnotou, FinOps, technická podpora) súvisiacich s migráciou a používaním cloudu. Tieto služby môžu zahŕňať: plánovanie, návrh, migráciu, správu, podporu, kontrolu kvality, bezpečnosť, odbornú prípravu atď.

Dodávatelia môžu predkladať svoje ponuky viacerým skupinám.

Dodávatelia predložia svoje ponuky a súvisiace ceny vo formáte podľa vlastného výberu.

SÚŤAŽ PODĽA RÁMCOVEJ DOHODY A ZADÁVANIE ZÁKAZIEK**OBJEDNÁVKY VYPLÝVAJÚCE Z RÁMCOVEJ DOHODY**

Orgány verejného sektora, ktoré sú zmluvnými stranami rámcovej dohody, si môžu v prípade potreby objednať alebo „doobjednať“ služby, ktoré potrebujú. Uzavretie zmluvy o doobjednaní na základe rámcovej dohody umožňuje kupujúcim spresniť požiadavky s dodatočnou funkčnou špecifikáciou pre konkrétnu objednávku, pričom si zachovávajú výhody vyplývajúce z rámcovej dohody.

Zákazky zadane na základe rámcovej dohody budú môcť preukázať jasný kontrolný záznam z hľadiska požiadaviek použitých na výber dodávateľa v rámci každej skupiny. Koncoví obstarávatelia budú uchovávať záznamy o komunikácii s dodávateľmi, vrátane akéhokoľvek predbežného prieskumného kontaktu, otázok na objasnenie, e-mailov a osobných rozhovorov.

1. SPÍSANIE POŽIADAVIEK NA OBJEDNÁVKY VYPLÝVAJÚCE Z RÁMCOVEJ DOHODY A POŽIADANIE O INTERNÉ SCHVÁLENIE NÁKUPU

Všetci koncoví nákupcovia oprávnení používať rámcovú dohodu vytvoria spoločné tímy obchodných koncových používateľov, nákupných špecialistov a technických expertov, aby pripravili zoznam „nevyhnutných“ a „požadovaných“ položiek. Tieto požiadavky pomôžu rozhodnúť, ktorá skupina sa na dodávateľa vzťahuje a ktorý dodávateľ má najlepšiu kvalifikáciu na splnenie požiadaviek. Pri navrhovaní požiadaviek nákupcovia zvažia:

- dostupné finančné prostriedky na používanie služby
- technické požiadavky projektu a požiadavky týkajúce sa obstarávania
- kritériá, na základe ktorých sa bude vyberať

2. VYHĽADÁVANIE SLUŽIEB

Podľa rámcovej dohody budú nákupcovia na vyhľadávanie produktov/služieb, ktoré spĺňajú ich uvedené potreby, používať online rámcový katalóg (portál, na ktorom budú uvedení kvalifikovaní signatári rámcovej dohody a ich služby). Vyberú si aj primerané skupiny a potom vyhľadajú služby.

3. PRESKÚMANIE A VYHODNOTENIE SLUŽIEB

V zmysle rámcovej dohody nákupcovia preskúmajú opisy služieb, aby našli služby, ktoré najlepšie vyhovujú ich potrebám na základe požiadaviek a rozpočtu. Opis každej služby bude zahŕňať:

- Dokument s definíciou služby alebo odkazy na definície služby
- Dokument so zmluvnými podmienkami
- Dokument s uvedením cien (odkazy na verejné ceny sú prijateľné za predpokladu, že úplný cenník/dokument s cenami je k dispozícii na vyžiadanie)

Cenu budú predstavovať náklady na najbežnejšiu konfiguráciu služby. Stanovenie cien sa však zvyčajne zakladá na objeme, takže nákupcovia by si mali vždy pozrieť cenník dodávateľa alebo verejne stanovené ceny a nástroje cenovej kalkulačky, aby zistili skutočnú cenu toho, čo sa kupuje, a celkovú hodnotu poskytnutú nákupcovi (napr. služby na optimalizáciu a následné zníženie nákladov).

V zmysle rámcovej dohody môžu nákupcovia hovoriť s dodávateľmi a požiadať ich, aby vysvetlili svoj opis služby, zmluvné podmienky, dokumenty/model uvádzajúce ceny alebo definície služby. O akýchkoľvek rozhovoroch s dodávateľmi sa budú uchovávať záznamy.

4. VÝBER SLUŽBY A UZATVORENIE ZMLUVY

Jeden dodávateľ

Ak požiadavky spĺňa iba jeden dodávateľ, môže sa s ním uzavrieť zmluva.

Viacero dodávateľov

Ak je v užšom výbere viacero služieb, nákupca si vyberie službu s ekonomicky najvýhodnejšou ponukou (skr. MEAT, z angl. výrazu Most Economically Advantageous Tender). Kritériá hodnotenia na základe MEAT nájdete v nasledujúcej tabuľke. Nákupcovia sa môžu rozhodnúť, aké podrobné charakteristiky použijú a akú hodnotu im priradia.

Upozorňujeme, že nákupca môže potrebovať:

- pozrieť sa na kombinácie rôznych dodávateľov
- konkrétne informácie o objemových alebo podnikových zľavách a službách optimalizácie nákladov dodávateľa

Hodnotenie dodávateľov by malo byť vždy spravodlivé a transparentné. Výber bude vychádzať z najvhodnejšej ponuky a dodávateľa/služby nebudú vylúčení/vylúčené bez odvolania sa na požiadavky projektu.

Tabuľka 2 – Hodnotenie na základe MEAT

Kritériá na vyhodnotenie ponúk
Náklady na celú životnosť: efektívnosť nákladov, cena a prevádzkové náklady
Technická hodnota a funkčná primeranosť: pokrytie, kapacita siete a výkon, ako je uvedené v príslušných opisoch služieb
Riadenie popredajných služieb: helpdesk, dokumentácia, funkcia správy účtov a zabezpečenie dodávky celého radu služieb
Nefunkčné vlastnosti

MINISÚŤAŽE

V prípade potreby sa môže uskutočniť minisúťaž, v ktorej sa určí najlepší dodávateľ pre konkrétny pracovný rozsah alebo projekt. V minisúťaži prejde zákazník do ďalšej súťaže podľa rámcovej dohody s tým, že vyzve všetkých dodávateľov v rámci skupiny, aby reagovali na súbor požiadaviek. Zákazník vyzve všetkých kvalifikovaných dodávateľov v rámci skupiny, aby predložili ponuku. Ďalšie informácie na porovnanie nájdete nižšie v častiach týkajúcich sa technických, bezpečnostných aspektov a cien/hodnoty.

ZMLUVA

Kupujúci aj dodávateľ podpíšu vyhotovenie zmluvy predtým, ako bude možné službu využívať. Maximálna dĺžka platnosti rámcovej dohody je zvyčajne <x> mesiace/mesiakov. Táto doba sa môže predĺžiť o <x> mesiace/mesiakov a potom o ďalšie/ďalších <x> mesiace/mesiakov s príslušnými internými súhlasmi, ak je to potrebné na predĺženie platnosti zmluvy.

Kópiu zmluvy musia podpísať všetky zainteresované strany (kupujúci a dodávateľ) pred možnosťou použitia služby.

2.1.5 Minimálne požiadavky na uchádzača – administratívne

Vďaka jednoduchému a jasnému jazyku pri stanovení kvalifikačných kritérií rámcovej dohody nebudú ponuky predkladať bežné dátové centrá ani poskytovatelia hardvéru, ktorí ponúknu balík s tradičným riešením ako „cloud“. Uchádzači by mali preukázať, ako spĺňajú nižšie uvedené minimálne administratívne požiadavky.

Znovu pripomínáme, že tento dokument sa zameriava na **1. SKUPINU – CLOUDOVÉ TECHNOLOGIE**. V prípadoch, kedy je vhodné poskytnúť celkový kontext z hľadiska požiadaviek a rozsahu žiadosti o ponuku, sme však doplnili aj ďalšie informácie o **2. SKUPINE – MARKETPLACE** a **3. SKUPINE – CLOUDOVÉ PORADENSTVO**. Napríklad je dôležité uviesť v RFP minimálne kvalifikačné kritériá na sprostredkovateľa CISP/MSP/SI/poradenskú firmu/atď., ktoré pomôžu zabezpečiť, aby boli (1) priamo pridružení k CISP ako sprostredkovateľ alebo partner v rámci kanála, (2) mali certifikáciu od CISP na ďalší predaj priameho prístupu k ponukám CISP externým subjektom a (3) aby mali certifikácie od týchto CISP, v ktorých sa uvádzajú ich schopnosti a odbornosť.

Znenie vzorovej RFP: Minimálne požiadavky na uchádzača – administratívne

Podľa tejto rámcovej dohody sa budú zadávať zákazky viacerým dodávateľom v nasledujúcich kategóriách. Sprostredkovatelia musia byť komerčným CISP, externým sprostredkovateľom CISP, distribútorom služieb trhoviska a/alebo poskytovateľom služieb na využitie CISP (napr. konzultačné, migračné služby, riadené služby, FinOps atď.). Uveďte roly, o ktoré sa uchádzate:

1. SKUPINA

- _____ - Priamy poskytovateľ (CISP) verejnej cloudovej služby (IaaS A PaaS)
- _____ - Priamy poskytovateľ (CISP) komunitnej cloudovej služby (IaaS A PaaS)
- _____ - Priamy poskytovateľ (CISP) súkromnej cloudovej služby (IaaS A PaaS)
- _____ - Externý sprostredkovateľ CISP (schopnosť poskytovať priamy prístup k online cloudovým ponukám poskytovateľa internetových služieb).

- Uved'te ponuku CISP, ktorá potvrdzuje, že môžete predávať priamy prístup k ich službám: _____
- Predložte list od CISP potvrdzujúci, že ste autorizovaným sprostredkovateľom jeho ponuky: _____

2. SKUPINA

- _____ - Priamy poskytovateľ služieb marketplace, ktoré sa realizujú na CISP (PaaS a/alebo SaaS)
- _____ - Distribútor služieb marketplace, ktoré sa realizujú na (PaaS a/alebo SaaS)

3. SKUPINA

- _____ - CISP poskytujúci odborné služby
- _____ - Poskytovateľ technickej podpory CISP
- _____ - Partner CISP poskytujúci služby na použitie alebo prevádzku na CISP
- _____ - Influencer/Poradca poskytujúci služby na využitie alebo prevádzku na CISP

Identifikujte typ ponuky:

- Spravované služby pracovných zariadení na CISP (Á/N): _____
 - Identifikujte odbory, ak je to relevantné: _____
- Odborné služby: (Á/N): _____
- Poradenstvo – Odborná príprava (Á/N): _____
- Poradenstvo – Stratégia (Á/N): _____
- Poradenstvo – Migrácia (Á/N): _____
- Poradenstvo – Riadenie cloudu (Á/N): _____
- Poradenstvo – FinOps (Á/N): _____
- Poradenstvo – Iné (uved'te): _____

Identifikujte CISP, ktorým poskytujete služby: _____

Predložte list od CISP potvrdzujúci vaše označenie partnera podľa modelu CISP: _____

1. SKUPINA – MINIMÁLNE ADMINISTRATÍVNE POŽIADAVKY**Poskytovatelia cloudových služieb (CISP)**

V prípade kvalifikácie ako CISP je nutné preukázať splnenie nižšie uvedených požiadaviek.

Navrhované kvalifikačné kritériá pre CISP	Dôvod
Organizačné údaje napr. meno, právna štruktúra, registračné číslo/číslo DUNS, DPH atď.	
Veľkosť spoločnosti, ekonomická a finančná situácia ³	Zákazník môže určiť, že CISP bude schopný plniť zmluvu.
Dôvody vylúčenia napr. trestná/podvodná činnosť atď.	
Prípadové štúdie/referencie od zákazníkov (uvedte požadované číslo/typ)	Zákazník má možnosť zmerať skúsenosti CISP pri poskytovaní požadovaných služieb.
Spoločenská zodpovednosť spoločnosti	Malo by ísť o verejne prístupné verzie, ktoré poskytuje CISP.
Verejne dostupné záväzky a postupy v oblasti trvalej udržateľnosti.	Zákazník môže vidieť, že CISP je odhodlaný vykonávať svoju činnosť čo najekologickejšim spôsobom.
CISP musí poskytnúť preukázateľné výsledky v oblasti inovácií a predstavovaní nových užitočných služieb a funkcií za posledných 5 rokov, najmä v oblasti PAAS, strojového učenia a analýzy, Big Data, spravovaných služieb a funkcií optimalizácie využívania cloudu. Na potvrdenie tohto tvrdenia možno použiť verejne prístupné záznamy zmien alebo informačné kanály.	Ukazuje, že CISP pracuje na tom, aby sa nové produkty rýchlo dostali do rúk zákazníkov, následne rýchlo zavádza osvedčené procesy a produkty vylepšuje. Zákazníkom to pomáha udržiavať najmodernejšiu IT infraštruktúru bez toho, aby museli investovať do rekapitalizácie.

Vzťah sprostredkovateľa/partnera s CISP

<ORGANIZÁCIA> žiada, aby bol hlavný dodávateľ priamo spojený s CISP ako sprostredkovateľ alebo partner, aby mal od CISP certifikáciu na predaj priameho prístupu k ponukám CISP externým subjektom, pričom sa v takej certifikácii od týchto CISP uvádzajú schopnosti a odbornosť sprostredkovateľa/partnera. Tým sa eliminuje požiadavka, aby <ORGANIZÁCIA> preskúmala zmluvné podmienky a služby spojené s ďalšou vrstvou subdodávok medzi hlavným dodávateľom **rámцovej dohody** a CISP. Táto požiadavka navyše redukuje zložitnosť, ktorú vytvárajú ďalšie vrstvy sprostredkovateľov, keď (1) <ORGANIZÁCIA> vykonáva svoju náležitú starostlivosť, aby zabezpečila jasné pridelenie zodpovedností v súvislosti so službami, ktoré sa majú poskytovať, a keď (2) <ORGANIZÁCIA> vykonáva každodenné činnosti zahŕňajúce využívanie cloudových služieb.

2.2 Technické požiadavky

RFP na cloudové služby by mala zvýšiť latku pre CISP tak, že bude vyžadovať, aby poskytovali štandardizované cloudové technológie potrebné pre zákazníka na vytvorenie vlastného riešenia. Ako už bolo spomenuté, tento rozdiel medzi tým, čo je štandardizované a čo je prispôbené, je pri prístupe k RFP na cloudové služby veľmi dôležitý. CISP ponúkajú štandardizované služby miliónom zákazníkov, takže prispôbenia v RFP na cloudové služby sa zameriavajú na riešenia a výstupy na vyššej úrovni, na rozdiel od základných metód, infraštruktúry alebo hardvéru používaných v rámci ponuky cloudových služieb, ktoré slúžia na dosiahnutie výstupov riešenia.

2.2.1 Minimálne požiadavky

Tradičné obstarávanie v oblasti IT sa často spolieha na obchodné požiadavky vypracované v rámci série pracovných stretnutí, ktoré dokumentujú, ako organizácia v súčasnosti vykonáva svoju činnosť. Splniť tieto

³ Upozorňujeme, že RFP na cloudové služby sa zameriava na údaje o spoločnosti na vysokej úrovni, nie na počet zamestnancov v spoločnosti ani na internú štruktúru tímu zamestnancov. Pri cloudovej technológii nie je žiadna súvislosť medzi zárukou plnenia služby a počtom zamestnancov. Namiesto toho sa RFP na cloudové služby zameriavajú na celkovú veľkosť spoločnosti, aby spĺňali požiadavky (primeraný rozsah) a overené skúsenosti/výkon.

požiadavky úplne správne je aj za tých najlepších okolností náročný proces. Ak sú tieto stretnutia zamerané na určenie požiadaviek úspešné, dokumentujú pôvodný obchodný proces, ktorý môže byť sám osebe zastaraný a neefektívny. Ak sa potom tieto požiadavky stanú súčasťou RFP, ktoré má CISP replikovať, jediným riešením môže byť riešenie na mieru. Tento model nie je kompatibilný s obstarávaním v oblasti cloudu.

Organizácie verejného sektora by mali poznať svoje obchodné ciele a potreby plnenia, ale v RFP by nemali byť normatívne a diktovať prevedenie a funkčnosť systému. Namiesto toho by mala organizácia nakupovať to, čo najviac vyhovuje jej činnosti. Namiesto hodnotenia návrhov na základe stoviek alebo dokonca tisícok normatívnych požiadaviek, ktoré nemusia viesť k vyhovujúcim službám, by organizácie mali uviesť hodnotiace kritériá založené na tom, ako dobre technológia a súvisiace služby splnia alebo vylepšia podnikateľské ciele, či splnia ich výkonnostné potreby a mali by zahrnúť aj schopnosť doladiť obchodné pravidlá prostredníctvom konfigurácie.

*V RFP na cloudové služby by mali byť predložené správne otázky, ktoré zabezpečia najlepšie riešenia. Vzhľadom na to, že v modeli cloudu sa nenakupujú fyzické aktíva, mnohé tradičné požiadavky na obstarávanie adresované dátovým centrárami nie sú použiteľné. **Recyklácia otázok adresovaných dátovým centrárami bude nevyhnutne viesť k odpovediam dátových centier**, čo následne povedie k tomu, že CISP nebudú môcť predkladať svoje ponuky, alebo k zle navrhnutým zmluvám, ktoré bránia zákazníkom z verejného sektora využiť všetky možnosti a výhody cloudu.*

RFP na cloudové služby sa zameriava na kľúčové požiadavky kladené na CISP a cloudové služby, vďaka čomu dodávatelia, ktorí sa kvalifikujú pre 1. SKUPINU, spĺňajú skutočne vysokú úroveň. Požiadavky by však nemali byť príliš normatívne, aby neobmedzovali prístup verejného sektora k širokej škále kvalifikovaných poskytovateľov CISP.

Znenie vzorovej RFP: Schopnosti poskytovateľa cloudu

Pozrite si aj vyššie uvedené minimálne administratívne požiadavky na CISP v prípade 1. SKUPINY.

Navrhované kvalifikačné kritériá pre CISP	Dôvod
Infraštruktúra	
Infraštruktúra CISP by mala ponúkať aspoň 2 klastre dátových centier. Každý klastor sa musí skladať aspoň z 2 dátových centier prepojených linkou s nízkou latenciou, aby sa zabezpečilo vysokodostupné nasadenie v režime Active-Active a implementácia scenárov DR-BC. Dátové centrá tvoriace každý klastor musia byť fyzicky izolované a navzájom nezávislé v prípade zlyhania.	CISP musí vedieť ponúknuť infraštruktúru schopnú budovať vysokodostupné aplikácie, kde sa dá vyhnúť samostatným chybám.
CISP by mal zabezpečiť logicky a geograficky izolované regióny. Mimo týchto oblastí nesmie CISP replikovať údaje zákazníkov.	Z požiadaviek na rezidenciu údajov vyplýva, že zákazník musí mať úplnú kontrolu nad tým, kde sa jeho údaje nachádzajú.
CISP musí vedieť poskytnúť priamu, vyhradenú a súkromnú konektivitu medzi dátovými centrami CISP.	Súkromná konektivita je základnou požiadavkou na vybudovanie hybridnej, bezpečnej infraštruktúry.
CISP by mal poskytovať dostatočné mechanizmy, ktoré zahŕňajú šifrovanie údajov pri prenose.	Zákazník môže požadovať zaistenie toho, aby sa žiadne dáta nemohli prenášať nezašifrované.

Minimálne požiadavky na certifikácie CISP	
<i>CISP musí byť certifikovaný podľa ISO 27001</i>	<i>Vďaka externému auditu, certifikácii a akreditácii si môžu zákazníci porovnávať služby (a najmä platformu) z hľadiska kvality, bezpečnosti a spoľahlivosti. Minimálne požiadavky na certifikáciu musia byť splnené.</i>
<i>CISP musí spĺňať etický kód CISPE na ochranu údajov, aby mohol poskytovať funkcie a služby, ktoré možno používať v súlade s nariadením GDPR, vďaka čomu môžu zákazníci vytvárať aplikácie vyhovujúce ustanoveniam GDPR.</i>	<i>Zákazník musí byť schopný vytvárať alebo spúšťať aplikácie v súlade s nariadením GDPR.</i>
<i>CISP musí sprístupniť protokoly z externého auditu, ako sú správy SOC 1 a 2 (pokrývajúce prevádzku a služby použité EK) v záujme transparentnosti s ohľadom na kontroly a postupy CISP.</i>	<i>CISP musí byť transparentný, pokiaľ ide o spôsob, akým sa aplikácia prevádzkuje a riadi. Správy SOC slúžia na zabezpečenie dôvery a transparentnosti.</i>
<i>CISP musí dodržiavať pakt o klimaticky neutrálnom dátovom centre.</i>	<i>Pakt o klimaticky neutrálnom dátovom centre zaväzuje CISP dosiahnuť klimatickú neutralitu do roku 2030, vďaka čomu môže používateľ podporovať vlastné ciele v oblasti trvalej udržateľnosti. V prípade poskytovateľov > 250 FTE (nie MSP) sú externí audítori povinní.</i>
<i>CISP musí dodržiavať etický kódex SWIPO v oblasti IaaS v súvislosti s prenosnosťou</i>	<i>Etický kódex správania SWIPO v oblasti IaaS v súvislosti s prenosnosťou zabezpečuje, že služby spĺňajú požiadavky čl. 6 „Prenos neosobných údajov“ (tzv. data porting) nariadenia o voľnom toku neosobných údajov.</i>
Vlastnosti služby	
<i>Infraštruktúra CISP musí byť prístupná prostredníctvom programových rozhraní (API) a webovej konzoly na správu.</i>	<i>Požadovaným štandardom na strane poskytovateľov CISP je samoobslužný prístup a programové rozhrania, ktoré čo najviac sprostredkujú prístup používateľov a samotného poskytovateľa.</i>
<i>CISP musí ponúkať základný súbor služieb vrátane nasledovných: ukladanie objektov, spravovaná relačná databáza, spravovaná nerelačná databáza, spravované vyrovnávače zaťaženia, monitorovanie a integrované automatické škálovanie.</i>	<i>Samotná ponuka virtuálnych strojov na to, aby sa poskytovateľ kvalifikoval ako poskytovateľ cloudu, nestačí. Poskytovatelia cloudu by mali ponúkať súbor služieb typu PAAS a IAAS na zrýchlenie a zlepšenie zákaznických aplikácií.</i>
<i>CISP musí umožniť zákazníkovi voľne meniť používanie a konfiguráciu svojich služieb alebo presúvať dáta v rámci a mimo CISP (samoobslužná ponuka).</i>	<i>Samoobslužný prístup k službám a dátam je nemennou požiadavkou, ktorá zákazníkovi zaisťuje plnú nezávislosť.</i>
<i>CISP musí umožňovať fakturáciu svojich služieb podľa platobného modelu „pay per use“ (platba podľa spotreby).</i>	<i>Tento model zákazníkovi umožňuje nákladovo optimalizovať svoje pracovné zaťaženie, minimalizovať riziko a využiť CISP pre aplikácie a PoC s krátkou životnosťou.</i>
Zabezpečenie dát a systémov	
<i>CISP musí zákazníkovi umožniť zachovať si úplnú kontrolu nad svojimi údajmi, poskytnúť zákazníkovi slobodu pri výbere miesta uloženia údajov (mestská oblasť) a zaručiť, aby sa žiadne údaje zákazníka nepresúvali, pokiaľ takýto presun neinicuje samotný zákazník.</i>	<i>Zákazník musí mať kontrolu nad tým, kde sú dáta uložené, ako spravovať prístup k obsahu a nad užívateľským prístupom k službám a zdrojom.</i>

Vlastnosti CISP musia zákazníkovi poskytnúť plnú kontrolu nad jeho bezpečnostnými zásadami vrátane dôvernosti, integrity a dostupnosti údajov a systémov zákazníka.	Zákazník musí vedieť definovať a implementovať svoje bezpečnostné štandardy v rámci svojich pracovných zaťažení. Dôverovať poskytovateľovi, že s údajmi zákazníka „zaobchádza správne“, nestačí.
Kontrola nákladov	
CISP musí mať mechanizmy a nástroje, ktoré zákazníkovi umožnia sledovať výdavky v priebehu času. Nástroje musia zabezpečiť základnú segmentáciu nákladov na základe pracovného zaťaženia, služby a účtu.	
CISP musí ponúkať nástroje, ktoré zákazníka vždy upozornia na prekročenie prahovej hodnoty nákladov.	
CISP musí zákazníkovi dodať podrobné vyúčtovanie. Účet musí byť možné štruktúrovať tak, aby sa náklady rozdelili podľa pracovného zaťaženia, prostredia a účtu.	

CISP by navyše mali poskytnúť odpovede na nižšie uvedené technické požiadavky.

RIEŠENIA

CISP by mal ukázať, ako dokáže zabezpečiť vopred vytvorené šablóny a softvérové riešenia, ktoré sú buď hostované na CISP, alebo sú s CISP integrované, a to v prípade nasledujúcich riešení:

- Ukladanie
- DevOps
- Zabezpečenie/plnenie predpisov
- Big Data/Analytika
- Obchodné aplikácie
- Telekomunikácie a siete
- Geopriestorové údaje
- Internet vecí (IoT)
- [Iné]

Predložte prehľad o tom, ako sa CISP využíval pri nasledujúcich pracovných zaťaženiach:

- Obnova po havárii
- Vývoj a testovanie
- Archivácia
- Zálohovanie a obnova
- Big Data
- High Performance Computing (HPC)
- Internet vecí (IoT)
- Webové stránky
- Bezserverová výpočtová technika
- DevOps
- Doručovanie obsahu
- [Iné]

2.2.2 Porovnanie medzi dodávateľmi

Popri minimálnych požiadavkách v RFP na cloudové služby je dôležité uviesť kritériá, podľa ktorých možno technológie CISP porovnávať pri posudzovaní konkurencie.

V žiadostiach o predloženie ponuky na cloudové služby by mali byť požadované tie cloudové funkcie, ktoré organizácia potrebuje, pričom treba zohľadniť, že zákazník zodpovedá za použitie týchto možností na vytvorenie svojho riešenia. Nadštandardné funkcie, ktoré môže CISP poskytnúť (ako sú vopred vytvorené riešenia prostredníctvom CISP alebo automatizačné funkcie), možno použiť v RFP na cloudové služby na zmysluplnejšiu analýzu „možností s pridanou hodnotou“ alebo „najlepšieho pomeru ceny/kvality“.

Verejný sektor často v súťaži medzi uchádzačmi požaduje použitie hodnotiacich kritérií, ako je najlepší pomer ceny/kvality, ekonomicky najvýhodnejšia ponuka (MEAT) alebo najnižšia cena. Keďže subjekty verejného sektora rátajú s touto časťou RFP na cloudové služby, je dôležité vytvoriť prístup, ktorý zohľadní jedinečné vlastnosti cloudu. Napríklad, je dôležité vedieť, že jednoduché porovnávanie riadkových položiek medzi ponukami poskytovateľov cloudu (napr. výpočtová technika alebo úložisko) nie je efektívny spôsob porovnávania ponúk. Namiesto toho dôrazne odporúčame zamerať sa na riešenia vyššej úrovne, ako sú tie, ktoré sú uvedené vyššie v časti 2.2.1. Subjekty verejného sektora sa potom môžu pozrieť na požiadavky špecifické pre cloud, ako sú tie, ktoré sú uvedené v *Príloha A – Technické požiadavky na porovnanie medzi účastníkmi výberového konania*.

V RFP by sa mali uvádzať základné charakteristiky cloudu potrebné na vytvorenie cloudového riešenia. Organizácie verejného sektora môžu na tento účel popri správach od externých analytikov využiť aj základné charakteristiky cloudu podľa Národného inštitútu pre štandardy a technológie (NIST). Zabezpečia ich tak, že CISP predloží najvhodnejšiu ponuku „skutočného cloudu“, ktorý funguje vo veľkom meradle.

Znenie vzorovej RFP – Porovnanie medzi dodávateľmi

CISP by mali poskytnúť odpovede na VŠETKY otázky týkajúce sa technických požiadaviek uvedených v prílohe A.

Respondenti musia mať nasledujúce atribúty a musia opísať, ako ich ponuky cloudových služieb spĺňajú päť základných charakteristík pre cloud computing⁴.

- 1) **Samoobsluha na požiadanie:** Respondent musí poskytnúť možnosť jednostranného poskytovania výpočtových možností, ako je čas servera a sieťové úložisko, podľa potreby automaticky a bez nutnosti ľudskej interakcie s každým poskytovateľom služieb. Respondent poskytne v prípade činnosti objednávanie možnosť jednostranného poskytovania služieb (t. j. bez kontroly alebo schválenia dodávateľa). Vysvetlite, ako je táto požiadavka zohľadnená vo vašej ponuke alebo v ponuke, ktorú predkladáte.*
- 2) **Všadeprítomný prístup k sieti:** Respondent musí poskytovať viacero možností sieťového pripojenia, z ktorých jedna musí byť založená na internete. Vysvetlite, ako je táto požiadavka zohľadnená vo vašej ponuke alebo v ponuke, ktorú predkladáte.*
- 3) **Zoskupovanie zdrojov:** CISP respondenta musí poskytovať zoskupené výpočtové zdroje, ktoré slúžia viacerým spotrebiteľom pomocou modelu viacerých nájomníkov s rôznymi virtuálnymi zdrojmi dynamicky pridelovanými a opätovne pridelovanými podľa dopytu spotrebiteľov. Používateľ môže určiť polohu na vyššej úrovni abstrakcie (napr. krajina, región alebo umiestnenie dátového centra). Respondent podporí škálovanie týchto zdrojov do niekoľkých minút alebo hodín od prijatia žiadosti o také plnenie. Vysvetlite, ako je táto požiadavka zohľadnená vo vašej ponuke alebo v ponuke, ktorú predkladáte.*
- 4) **Rýchla pružnosť:** CISP respondenta musí podporovať možnosti poskytovania služieb a rušenia prístupu k službám (navyšovanie a znižovanie) tak, aby bola služba sprístupnená v minimálnej predpísanej dobe (maximálne „x“ hodín) od prijatia žiadosti o toto plnenie. Respondent podporuje úpravy pri fakturácii vyplývajúce zo žiadosti o toto plnenie na hodinovej alebo dennej báze.*

⁴ <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>

- 5) **Meraná služba:** Respondent ponúkne prehľad o používaní služby prostredníctvom online dashboardu alebo podobných elektronických prostriedkov.

CISP musí navyše:

- byť uznávaný líder v poskytovaní cloudových služieb podľa správ Gartner Magic Quadrant v prípade IaaS⁵,
- poskytnúť odborníkmi uznávané správy od externých analytikov, ktoré preukazujú osvedčené schopnosti a spoľahlivosť CISP.

Nakoniec budú CISP porovnaní pomocou scenárov uvedených v prílohe B.

2.2.2.1 Dohody o poskytovaní služieb

CISP poskytujú štandardizované komerčné dohody o poskytovaní služieb miliónom zákazníkov, a preto nie sú schopní ponúkať prispôbené dohody o poskytovaní služieb, ako je to v prípade modelu lokálneho dátového centra. Zákazníci CISP (často im pomáhajú partneri CISP) však môžu navrhnúť použitie svojho cloudu, aby využili komerčné dohody CISP o poskytovaní služieb pri plnení a presahovaní špecifických požiadaviek zákazníkov a jedinečných dohôd o poskytovaní služieb.

RFP na cloudové služby by mali zabezpečiť, aby CISP ponúkali schopnosti a usmernenia potrebné na využitie svojich služieb a komerčných dohôd o poskytovaní služieb, aby jednotliví koncoví používatelia mohli splniť požiadavky na výkon a dostupnosť.

Znenie vzorovej RFP: Dohody o poskytovaní služieb

Uvedte informácie a odkazy na prístup CISP k dohodám o poskytovaní služieb (SLA).

<ORGANIZÁCIA> bude udržiavať informovanosť o dohode CISP o poskytovaní služieb a použije dôležité pracovné zaťaženia a aplikácie takým spôsobom, aby fungovali aj v prípade neplnenia dohody o poskytovaní služieb.

<ORGANIZÁCIA> bude zodpovedná za udržiavanie príslušných dohôd o poskytovaní služieb spojených s akýmkoľvek zariadením vo vlastníctve <ORGANIZÁCIE> alebo službami prevádzkovanými <ORGANIZÁCIOU> používanými s CISP.

CISP by mal <ORGANIZÁCIU> poskytnúť možnosti zabezpečujúce nepretržitú viditeľnosť a vykazovanie v súvislosti s operatívnym plnením dohody o poskytovaní služieb a zdokumentované osvedčené postupy na využitie infraštruktúry CISP pri návrhu služieb z hľadiska výkonu, trvanlivosti a spoľahlivosti.

2.2.3 Uzatváranie zmlúv

Zmluvné podmienky CISP sú navrhnuté tak, aby odzrkadľovali, ako funguje model cloudových služieb (fyzické aktíva sa nenakupujú a CISP pôsobia vo veľkom rozsahu a ponúkajú štandardizované služby). Preto je dôležité, aby boli zmluvné podmienky CISP začlenené a využívané v maximálnej možnej miere. Viac informácií o zmluvných podmienkach a uzatváraní zmlúv nájdete nižšie v časti 2.5.

2.2.3.1 Nové a meniace sa služby

CISP zabezpečujú plnenie prostredníctvom služby. Na rozdiel od tradičných lokálnych riešení, ktoré si vyžadujú upgrady a zmluvy o údržbe služieb s konkrétnou dobou platnosti, poskytovatelia cloudu jednoducho poskytujú štandardizovanú službu. Ak má model cloudu viesť k úsporám z rozsahu, upgrady a zmeny základnej infraštruktúry sa sprístupňujú všetkým, nie jednotlivým používateľom, a zákazníci si potom vyberajú a volia

⁵ <https://www.gartner.com/doc/reprints?id=1-2G2O5FC&ct=150519&st=sb>

služby, ktoré používajú. Služba je plynulejšia než bývalé lokálne systémy a poskytovatelia cloudu neustále pridávajú nové a vylepšené služby, ktoré môžu zákazníci používať podľa vlastného uváženia.

Ak nové alebo vylepšené služby CISP nemožno pridať po termíne na predloženie RFP, organizácie verejného sektora si samy obmedzia možnosť využívať nové služby a vylepšené funkcie až do vydania ďalšej iterácie rámcovej zmluvy. Dôrazne preto odporúčame, aby bolo poskytovanie služieb opísaných v rámcovej zmluve všeobecné a umožňovalo pridávanie nových služieb CISP po termíne na predloženie. Právne predpisy EÚ v oblasti verejného obstarávania môžu obmedziť zavedenie podstatne odlišných nových služieb CISP, ktoré sa majú pridať do rámcovej zmluvy, ale aktualizácie a nové verzie služieb, ktoré sa nepovažujú za podstatné zmeny, by sa mohli pridať bez akýchkoľvek problémov s obstarávaním.

Znenie vzorovej RFP: Nové a meniace sa služby

CISP poskytne nákladovo efektívne riešenie, ktoré využíva osvedčené a stabilné virtualizačné technológie a neustále obnovované špičkové technológie. <ORGANIZÁCIA> potvrdzuje a súhlasí, že cloudové technológie môžu byť <ORGANIZÁCII> a iným klientom CISP poskytované na základe zdieľaných služieb zo spoločnej kódovej základne a/alebo spoločného prostredia a že CISP môže priebežne: meniť, pridávať alebo odstrániť funkcie, vlastnosti, výkon alebo iné charakteristiky cloudových služieb, a ak sa takáto zmena, prídanie alebo odstránenie uskutoční, špecifikácie cloudovej služby sa primerane upravujú.

Rozsah tejto objednávky zahŕňa všetky aktuálne existujúce a nové alebo vylepšené služby CISP **V ROZSAHU RÁMCOVEJ ZMLUVY**. Cloudové služby, ktoré CISP poskytuje a ktoré sú dostupné komerčným zákazníkom, budú sprístupnené <ORGANIZÁCII>.

2.2.3.2 Uzamknutie zákazníka (Vendor Lock-in)/Reverzibilita

Cloudová technológia redukuje uzamknutie zákazníka, keďže fyzické aktíva sa nenakupujú a zákazníci môžu kedykoľvek presunúť svoje údaje od jedného poskytovateľa cloudu k druhému.

Pri nákupe cloudových služieb je však nevyhnutná určitá miera viazanosti dodávateľov, pretože nie všetky cloudy sú rovnaké, a tak môže jeden CISP ponúkať služby a možnosti, ktoré iný jednoducho poskytnúť nevie. Tým sa znižuje možnosť využívať takéto služby u druhého poskytovateľa. Rozumným prístupom je vyžadovať, aby CISP poskytovali potrebné funkcie a služby na odchod z ich cloudu. Dokumentácia o tom, ako tieto služby používať, by v tomto prípade mohla slúžiť ako primeraná „stratégia odchodu“ – vzhľadom na to, že CISP nepozná jedinečnú konfiguráciu toho, ako zákazník využíva jeho štandardizované služby, a tak nemôže poskytnúť prispôbený plán odchodu.

Informácie o etických kódexoch v odvetví, ktoré sa týkajú „prenosu neosobných dát od jedného poskytovateľa k inému“ (tzv. data porting) a „zmeny poskytovateľov cloudu“ v záujme splnenia požiadaviek článku 6 „Nariadenia EÚ o voľnom toku iných ako osobných údajov“, nájdete v časti 2.3.1.2.

Znenie vzorovej RFP: Vstup a odchod

<ORGANIZÁCIA> hľadá návrhy, ktoré poskytujú primeranú stratégiu odchodu, aby predišla uzamknutiu (vendor lock-in). <ORGANIZÁCIA> nenakupuje fyzické aktíva a CISP poskytne možnosť posúvať sa v zásobníku IT nahor a nadol. CISP bude poskytovať nástroje a služby prenosnosti, ktoré pomôžu pri migrácii na platformu CISP a z nej, čím sa uzamknutie minimalizuje. Ako primeraný plán odchodu poslúži podrobná dokumentácia o tom, ako používať nástroje a služby prenosnosti, ktoré CISP poskytuje.

CISP by nemal vyžadovať **povinné** minimálne záväzky ani **povinné** dlhodobé zmluvy.

Údaje uložené u poskytovateľa služieb môže zákazník kedykoľvek exportovať. CISP umožní <ORGANIZÁCII> presúvať dáta podľa potreby medzi úložiskom CISP a mimo neho. CISP zároveň umožní sťahovanie obrazov virtuálnych strojov a ich prenos novému poskytovateľovi cloudu. <ORGANIZÁCIA> môže exportovať svoje virtuálne počítače (tzv. machine images) a používať ich v lokálnom prostredí alebo u iného poskytovateľa (v závislosti od licenčných obmedzení softvéru).

2.3 Bezpečnosť

Zodpovednosť za bezpečnosť a dodržiavanie predpisov sa medzi CISP a zákazníkmi cloudu zdieľa. V tomto modeli práve zákazníci cloudu riadia to, ako navrhujú a zabezpečujú svoje aplikácie a údaje vložené do infraštruktúry, zatiaľ čo CISP sú zodpovední za poskytovanie služieb na vysoko zabezpečenej a kontrolovanej platforme a za poskytovanie širokej škály ďalších bezpečnostných funkcií. Úroveň zodpovednosti CISP a zákazníka v tomto modeli závisí od modelu nasadenia cloudu (IaaS/PaaS/SaaS) a zákazníci by mali poznať svoje povinnosti v každom modeli.

Pochopenie tohto modelu zdieľanej zodpovednosti je kľúčové pre vytvorenie úspešnej RFP na cloudové služby. Organizácie verejného sektora by sa mali uistiť, že vedia, za čo zodpovedá CISP, za čo sú samy zodpovedné a kde môžu pomôcť konzultanti/ISV partneri a ich riešenia.

2.3.1 Minimálne požiadavky

Kľúčovým slovom, pokiaľ ide o bezpečnosť v cloude, je **schopnosť**. Organizácie verejného sektora by mali byť na CISP prísne a mali by od CISP vyžadovať poskytovanie bezpečnostných funkcií potrebných na to, aby si zákazníci mohli plniť svoje povinnosti v rámci modelu zdieľanej zodpovednosti. Ako vidieť z reprezentatívneho zoznamu požiadaviek, od CISP sa vyžaduje, aby poskytol štandardizovanú funkciu, ktorú môže zákazník využiť na zabezpečenie svojho jedinečného cloudového prostredia.

- **Zabezpečte možnosti** brán firewall na ochranu sietí a webových aplikácií v záujme vytvorenia súkromných sietí a riadenia prístupu k inštanciam a aplikáciám.
- **Zabezpečte možnosti** pripojenia, ktoré umožňujú súkromné alebo vyhradené pripojenia z vašich kancelárií alebo lokálneho prostredia.
- **Zabezpečte možnosť** implementovať hĺbkovú stratégiu obrany a zmariť útoky DDoS.
- **Možnosti** šifrovania údajov dostupné v úložných a databázových službách.
- **Zabezpečte flexibilné možnosti** správy kľúčov, ktoré vám umožnia vybrať si, či chcete, aby šifrovacie kľúče spravoval CISP, alebo aby si úplnú kontrolu nad kľúčmi mohol ponechať zákazník.
- **Poskytnite** zákazníkovi **rozhrania API** na integráciu šifrovania a ochrany údajov s akýmikoľvek službami vyvinutými alebo nasadenými v prostredí CISP.
- **Zabezpečte nástroje** nasadenia na správu tvorby a vyradovania zdrojov CISP podľa noriem organizácie.
- **Zabezpečte nástroje** na správu inventára a konfigurácie, ktoré identifikujú zdroje CISP a potom priebežne sledujú a riadia zmeny týchto zdrojov.
- **Zabezpečte nástroje a funkcie**, vďaka ktorým budú zákazníci presne vidieť, čo sa deje v prostredí ich CISP.
- **Umožnite** podrobný **prehľad** o volaniach API – vrátane toho, kto, čo a odkiaľ boli volania uskutočnené.
- **Zabezpečte možnosti** agregácie protokolov, zefektívnenia vyšetřovania a vykazovania zhody.
- **Poskytnite možnosť** konfigurovať upozornenia pri výskyte konkrétnych udalostí alebo prekročení prahových hodnôt.
- **Poskytnite možnosti** na definovanie, presadzovanie a správu zásad prístupu používateľov v rámci služieb CISP.
- **Poskytnite možnosť** definovať jednotlivé používateľské účty s povoleniami naprieč zdrojmi CISP.
- **Poskytnite možnosť** integrácie a spojenia s podnikovými adresármi v záujme redukcie administratívnej réžie a zlepšenia využitia pre koncových používateľov.

Viac o týchto požiadavkách nájdete v Príloha A – Technické požiadavky na porovnanie medzi účastníkmi výberového konania.

Funkcie nad rámec minimálneho štandardu zabezpečenia možno v RFP použiť na zmysluplnejšiu analýzu „možností s pridanou hodnotou“ alebo „najlepšieho pomeru ceny/kvality“. Pokiaľ ide o zabezpečenie, čím viac funkcií je integrovaných alebo automatizovaných, tým lepšie. Požiadavky na porovnanie medzi uchádzačmi nájdete opäť v Príloha A – *Technické požiadavky na porovnanie medzi účastníkmi výberového konania*.

Organizácie verejného sektora by sa mali pozrieť na certifikácie a hodnotenia cloudovej akreditácie, aby sa ubezpečili, že sú zavedené požadované bezpečnostné kontroly CISP. Napríklad: predstavte si CISP, ktorý má validáciu a certifikáciu od nezávislého audítora na potvrdenie plnenia certifikačnej normy ISO 27001. Príloha A normy ISO 27001 sa v doméne 14 zaoberá špecifickými kontrolami, ktoré CISP dodržiava podľa požiadaviek ISO v oblasti akvizície, vývoja a údržby systému. Je pravdepodobné, že tieto kontroly pokrývajú väčšinu, ak nie všetky kontroly týkajúce sa akvizície, vývoja a údržby systému, ktoré by zvyčajne požadovala organizácia v žiadosti o ponuku v súvislosti s IT. Dáva teda zmysel, že organizácia jednoducho vyžaduje, aby bol CISP certifikovaný podľa ISO 27001, namiesto duplikovania úsilia a zavádzania kontrolných požiadaviek týkajúcich sa akvizície, vývoja a údržby systému v RFP na cloudové služby.

Tento prístup využitia externých správ o zhode možno použiť na väčšinu kontrol zabezpečenia a zhody, napríklad: etický kódex CISPE na ochranu údajov v zmysle GDPR, ISO, SOC atď.

Znenie vzorovej RFP: Zabezpečenie

CISP poskytne svoje nechránené bezpečnostné procesy a technické obmedzenia <ORGANIZÁCII> tak, aby bolo možné dosiahnuť primeranú ochranu a flexibilitu medzi <ORGANIZÁCIU> a poskytovateľom služieb.

CISP uvedie svoje úlohy a povinnosti, pokiaľ ide o bezpečnosť a plnenie predpisov:

- V navrhovanej ponuke opíšte úlohy a povinnosti súvisiace s bezpečnosťou na strane CISP a <ORGANIZÁCIE>. Jednoznačne vymedzte povinnosti a opíšte služby CISP, ktoré pomôžu <ORGANIZÁCIU> pri budovaní a automatizácii bezpečnostných funkcií v jej cloudovom prostredí.*
- Odpovedzte na technické špecifikácie uvedené v PRÍLOHE A týkajúce sa bezpečnostných požiadaviek <ORGANIZÁCIE>.*

VLASTNÍCTVO A KONTROLA OBSAHU <ORGANIZÁCIE>

Opíšte spôsobilosť CISP ochrániť údaje <ORGANIZÁCIE> z hľadiska dôvernosti. Uvedte kontrolné prvky na riešenie ochrany obsahu <ORGANIZÁCIE>. CISP musí zabezpečiť silnú regionálnu izoláciu, aby objekty uložené v regióne nikdy región neopustili, pokiaľ ich do iného regiónu výslovne neprenesie <ORGANIZÁCIA>.

- Prístup k svojmu obsahu, službám a zdrojom bude spravovať <ORGANIZÁCIA>. CISP by mal poskytnúť pokročilý súbor funkcií prístupu, šifrovania a protokolovania, ktoré <ORGANIZÁCIU> pomôžu pri efektívnom spravovaní prístupu. CISP nebude pristupovať k obsahu <ORGANIZÁCIE> a nebude ho používať na žiadny iný účel, než sa uvádza v zákone, a na zachovanie služieb CISP a ich poskytovanie <ORGANIZÁCIU> a jej koncovým používateľom.*
- <ORGANIZÁCIA> vyberie región (regióny), v ktorom bude jej obsah uložený. CISP nebude presúvať ani replikovať obsah <ORGANIZÁCIE> mimo jej zvolených regiónov, s výnimkou prípadov, keď to vyžaduje zákon a je to nevyhnutné na zachovanie služieb CISP a ich poskytovanie <ORGANIZÁCIU> a jej koncovým používateľom.*
- <ORGANIZÁCIA> si vyberie, ako bude jej obsah zabezpečený. CISP musí zabezpečiť silné šifrovanie obsahu <ORGANIZÁCIE> pri prenose alebo v pokoji a rovnako musí <ORGANIZÁCIU> poskytnúť možnosť spravovať vlastné šifrovacie kľúče.*

- CISP musí mať program na zaistenie bezpečnosti využívajúci globálne osvedčené postupy na ochranu osobných údajov, aby <ORGANIZÁCIA> mohla vytvoriť, prevádzkovať a využívať prostredie kontroly zabezpečenia CISP. Bezpečnostné ochrany a kontrolné procesy musia byť nezávisle overené viacerými nezávislými externými hodnoteniami.

Certifikácie a hodnotenia na cloudovú akreditáciu poskytujú organizáciám verejného sektora istotu, že CISP majú zavedené účinné fyzické a logické bezpečnostné kontroly. Keď sa tieto akreditácie využívajú v RFP, zefektívňuje to proces obstarávania a pomáha predísť duplicitným, príliš zaťažujúcim procesom alebo schvaľovacím pracovným postupom, ktoré nemusia byť pre cloudové prostredie potrebné.

RFP na cloudové služby by mali dať CISP možnosť dokázať, že plnia požiadavky akreditácií a hodnotení v súvislosti s dodržiavaním pravidiel. Ako je uvedené vyššie, rizikové scenáre a postupy riadenia rizík sa v rámci týchto akreditačných schém značne prekrývajú, a keďže kontroly a požiadavky sú v takýchto akreditáciách zoskupené, požiadavka, aby CISP dodržiavali akreditácie, je rýchlejšim spôsobom, ako v RFP vyriešiť povinnosti plnenia, než duplikovanie úsilia pri uvádzaní takýchto individuálnych kontrol (**mnohé z nich môžu byť prevzaté z predchádzajúcich žiadostí o ponuku, ktoré sú priamo v lokálnych dátových centrách, a ako také sa nemusia vzťahovať na oblasť cloud computingu**).

POZNÁMKA: Rovnako je veľmi dôležité vedieť, ako možno získať prístup k nižšie uvedeným správam. Napríklad správy SOC 1 a SOC 2 sú zvyčajne citlivé dokumenty. Majte na pamäti, že prístup k takým dokumentom si vyžaduje konkrétne dohody (napr. dohoda o zachovaní mlčanlivosti), a nežiadajte ľahkovážne o ich predloženie ako súčasť odpovede na žiadosť o ponuku (tieto dokumenty môžu byť poskytnuté prostredníctvom zákonov o otvorených záznamoch alebo podobnej legislatívy, ktorá ohrozuje zabezpečenie cloudu).

Znenie vzorovej RFP: Plnenie predpisov

Používanie uznávaných noriem bezpečnosti, dodržiavania predpisov a prevádzkových noriem odvodených z osvedčených postupov pri prevádzke cloudových služieb (vrátane spracovania údajov, zabezpečenia údajov, dôvernosti, dostupnosti atď.) zjednodušuje proces obstarávania cloudovej technológie.

<ORGANIZÁCIA> vyhodnotí ponuky s jedinečnými návrhmi na základe akceptovaných noriem bezpečnosti, dodržiavania predpisov a prevádzkových noriem, ako je uvedené nižšie a v **prílohe A**. Ak sa bude <ORGANIZÁCIA> spoliehať na certifikáciu dodávateľa v oblasti dodržiavania predpisov podľa jednotlivých noriem, môže ako východisko pri hodnotení ponuky použiť minimálne plnenie v zmysle normy.

Požiadavka, aby CISP naďalej spĺňal minimálne požiadavky normy počas trvania zmluvy, poskytuje výhodu zachovania aktuálnosti pri plnení predpisov.

CISP, ktorý predkladá ponuku (priamo alebo prostredníctvom sprostredkovateľa), by mal vedieť preukázať svoju schopnosť splniť nasledujúce atestácie, správy a certifikácie nezávislých tretích strán (Poznámka: ak sa na niektoré z týchto atestácií, správ a certifikácií vzťahujú obmedzenia zverejnenia vzhľadom na otázky bezpečnosti, <Organizácia> bude s CISP spolupracovať na získaní spoločne dohodnutého prístupu).

Certifikácie/atestácie	Zákony, predpisy a ochrana údajov	Usmernenia/rámce
☐ C5 (Nemecko)		☐ CDSA
☐ Etický kódex CISPE na ochranu údajov (GDPR)		

☐ CNDP (Pakt o klimatickej neutralite dátových centier)		
☐ DIACAP	☐ Smernica EÚ o ochrane údajov	☐ CIS
☐ DoD SRG úrovně 2 a 4	☐ Modelové doložky EÚ	☐ Informačná služba o trestnom súdnictve (CJIS)
☐ HDS (Francúzsko, zdravotná starostlivosť)		
☐ FedRAMP	☐ FERPA	☐ CSA
☐ FIPS 140-2	☐ GDPR	☐ Štít na ochranu osobných údajov medzi EÚ a USA
☐ ISO 9001	☐ GLBA	☐ Bezpečný prístav EÚ
☐ ISO 27001	☐ HIPAA	☐ FISC
☐ ISO 27017	☐ HITECH	☐ FISMA
☐ ISO 27018	☐ IRS 1075	☐ G-Cloud [Spojené kráľovstvo]
☐ IRAP [Austrália]	☐ ITAR	☐ GxP (FDA CFR 21 časť 11)
☐ MTCS úroveň 3 [Singapur]	☐ PDPA – 2010 [Malajzia]	☐ ICREA
☐ PCI DSS úroveň 1	☐ PDPA – 2012 [Singapur]	☐ IT Grundschutz [Nemecko]
☐ SEC pravidlo 17-a-4(f)	☐ PIPEDA [Kanada]	☐ MARS – E
☐ SecNumCloud (Francúzsko)		
☐ SOC1 / ISAE 3402	☐ Zákon o ochrane súkromia [Austrália]	☐ MITA 3.0
☐ SOC2 / SOC3	☐ Zákon o ochrane súkromia [Nový Zéland]	☐ MPAA
☐ Kódex SWIPO v súvislosti s IaaS		
	☐ Autorizácia španielskeho úradu na ochranu údajov	☐ NIST
	☐ Úrad na ochranu údajov v Spojenom kráľovstve - 1988	☐ Úrovně inštitútu Uptime
	☐ VPAT/odsek 508	☐ Zásady cloudovej bezpečnosti v Spojenom kráľovstve

Nižšie uvedený zoznam slúži len na ilustračné účely a nemal by sa považovať za úplný zoznam certifikácií a noriem, ktoré možno uplatniť na cloudové služby.

2.3.1.1 Ochrana údajov

Kľúčovým bodom pri využívaní cloudových služieb je, aby sa osobné údaje spracúvali podľa platných právnych predpisov EÚ o ochrane údajov vrátane všeobecného nariadenia o ochrane údajov (GDPR). GDPR je nariadenie založené na zásadách, a preto neuvádza usmernenia pre konkrétne odvetvie, ktoré by pomohli zabezpečiť dodržiavanie predpisov. Nariadenie GDPR však podporuje prijatie nástrojov na dodržiavanie predpisov, ako sú etické kódexy, ktoré takéto usmernenia poskytujú. Združenie CISPE

vypracovalo v spolupráci s francúzskym úradom na ochranu údajov (CNIL) etický kódex zameraný na ochranu údajov (kódex združenia CISPE⁶), ktorý schválil Európsky výbor pre ochranu údajov so všeobecnou platnosťou v Európe. Účelom tohto kódexu je pomôcť CISP dodržiavať ustanovenia GDPR a usmerniť zákazníkov pri posudzovaní, či sú CISP vhodní na spracúvanie osobných údajov podľa žiadosti zákazníka.

- Kódex sa zameriava výlučne na sektor IaaS a rieši špecifické úlohy a povinnosti poskytovateľov IaaS.
- Pomáha objasniť aspekty spravodlivého a transparentného spracovania a primeraných bezpečnostných opatrení v kontexte služieb cloudovej infraštruktúry (GDPR, článok 40 ods. 2).
- Pomáha zákazníkovi pochopiť, ako si môžu zachovať suverenitu nad svojimi údajmi, ak zabezpečia, aby zostali v rámci EÚ.
- Propaguje osvedčené postupy ochrany údajov, ktoré podporujú iniciatívu EÚ GAIA-X na rozvoj európskych cloudových dátových služieb.

Ak sa CISP riadia etickým kódexom na ochranu údajov (ako je kódex združenia CISPE), ide o záruku, že osobné údaje budú spracované v prísnom súlade s nariadením GDPR.

Znenie vzorovej RFP: Ochrana údajov

CISP, ktorý podáva ponuku (priamo alebo prostredníctvom sprostredkovateľa), by mal vedieť preukázať svoju schopnosť dodržiavať požiadavky etického kódexu na ochranu údajov, akým je napríklad kódex združenia CISPE. Kódex na ochranu údajov musí spĺňať požiadavky stanovené v rámci GDPR. Kódex by mal obsahovať minimálne: (1) jasné vymedzenie úloh a povinností CISP, (2) požiadavku, že CISP nebude používať údaje zákazníkov na marketingové ani reklamné účely, a (3) možnosť zákazníkov vybrať si služby CISP, ktoré umožňujú spracúvanie údajov výlučne v rámci Európskeho hospodárskeho priestoru. Plnenie ustanovení kódexu musia overiť externí nezávislí audítori (monitorovacie orgány) a akreditovať nezávislí externí audítori akreditovaní Európskym úradom na ochranu údajov.

2.3.1.2 Zmena poskytovateľov cloudu a prenos údajov

Zákazníci by mali mať možnosť slobodne si vybrať cloudové služby, ktoré chcú používať, a nemali by byť „uzamknutí“ poskytovateľom CISP alebo poskytovateľom PaaS/SaaS.

Cloudové služby poskytované CISP sú štandardizované a ponúkané na báze vzťahu „one-to-many“, pričom služby konfiguruje, poskytuje a riadi zákazník. Výhodou cloud computingu je, že zákazníci majú možnosť vybrať si akékoľvek štandardizované služby, ktoré potrebujú na vývoj svojich jedinečných aplikácií a riešení. Táto výhoda navyše umožňuje prechod na nové alebo iné služby, ktoré najlepšie vyhovujú potrebám zákazníkov v akomkoľvek konkrétnom čase.

Rovnako ako v prípade ochrany údajov môžu etické kódexy zákazníkovi poskytnúť istotu a dôveru, pokiaľ ide o prechod na cloud z lokálnej infraštruktúry alebo pri zmene CISP. Združenie CISPE s EuroCIO (Európska asociácia CIO) spolupredsedalo pri vypracovaní etického kódexu zameraného na prenosnosť údajov a prechod cloudových služieb na cloudové služby typu IaaS (Kódex SWIPO v súvislosti s IaaS^{7,8}). Prvá verzia kódexu bola vypracovaná podľa nariadenia EÚ o voľnom toku údajov a v novembri 2019 počas fínskeho predsedníctva EÚ bola odovzdaná Európskej komisii. V máji 2020 ju zverejnila asociácia

⁶ <https://cispe.cloud/code-of-conduct/>

⁷ <https://ec.europa.eu/digital-single-market/en/news/cloud-stakeholder-working-groups-start-their-work-cloud-switching-and-cloud-security>

⁸ <https://swipo.eu/>

SWIPO AISBL. Prvé služby riadiace sa kódexom asociácie SWIPO AISBL boli deklarované v apríli 2021 a v máji 2021 boli rovnako deklarované prvé služby členov združenia CISPE.

Znenie vzorovej RFP: Zmena poskytovateľov cloudu a prenos údajov

CISP, ktorý predkladá ponuku (priamo alebo prostredníctvom sprostredkovateľa), by mal vedieť preukázať svoju schopnosť dodržiavať etický kódex týkajúci sa prechodu a prenosu neosobných údajov (tzv. data porting“), ako je kódex SWIPO v súvislosti s IaaS. V takomto kódexe sa musí podrobne uvádzať, ako CISP zákazníkom zaistí bezpečný prenos obchodných údajov, ak sa rozhodnú CISP zmeniť.

2.3.2 Porovnanie medzi dodávateľmi

Rovnako ako v prípade vyššie uvedených technických kritérií, je dôležité v RFP na cloudové služby popri minimálnych bezpečnostných požiadavkách uviesť aj kritériá, podľa ktorých možno pri hodnotení konkurencie porovnať možnosti zabezpečenia a služby CISP.

Príklad požiadaviek pre CISP na zabezpečenie nájdete v *Príloha A – Technické požiadavky na porovnanie medzi účastníkmi* výberového konania. Dôrazne odporúčame, aby boli pre subjekty verejného sektora, ktoré CISP posudzujú, kľúčovými bezpečnostnými faktormi nižšie uvedené možnosti:

Znenie vzorovej RFP: Kľúčové faktory zabezpečenia

- *CISP je oboznámený s modelom zdieľanej zodpovednosti a zákazník má k dispozícii dokumentáciu, vďaka ktorej pozná vymedzenie povinností v oblasti zabezpečenia v súvislosti s funkciami a službami CISP (napríklad v kontexte GDPR)*
- *Preukázateľná história zabezpečenia infraštruktúry CISP s verejne dostupnou nechránenou dokumentáciou o bezpečnostnej pozícii CISP a fyzických/logických kontrolách*
- *Podpora CISP špecifická pre zabezpečenie cloudu*
- *Služby, ktoré umožňujú zákazníkovi formalizovať návrh účtu, automatizovať kontroly zabezpečenia a riadenia cloudu a zefektívniť audit*
- *Schopnosť vytvárať, poskytovať a spravovať zbierku zdrojov spôsobom podobným šablóne (vrátane šablón zabezpečenia zlatého štandardu, ktoré vypracoval CISP/partner CISP)*
- *Schopnosť zaviesť spoľahlivú a opakovateľnú prevádzku kontrol*
- *Funkcie na nepretržitý audit v reálnom čase*
- *Možnosť technického skriptovania zásad riadenia cloudu*
- *Schopnosť vytvárať vynútené funkcie, ktoré nemôžu byť prepísané používateľmi bez povolenia upravovať tieto funkcie*
- *Schopnosť spoľahlivo implementovať to, čo bolo predtým napísané v zásadách, štandardoch a nariadeniach, popri tvorbe vymáhateľného zabezpečenia a plnenia predpisov, čo následne vytvára funkčný spoľahlivý model riadenia cloudu pre IT prostredia*
- *Služby, ktoré chránia pred bežnými, najčastejšími sa vyskytujúcimi útokmi na distribuované odmietnutia služby (DDoS) na sieťovej a transportnej vrstve, s možnosťou písania prispôbených pravidiel na zmiernenie sofistikovaných útokov na aplikačnú vrstvu*
- *Služba spravovanej detekcie hrozieb*

2.3.3 Uzatváranie zmlúv

Ako je uvedené vyššie, zmluvné podmienky CISP sú navrhnuté tak, aby odzrkadľovali, ako funguje model cloudových služieb (fyzické aktíva sa nenakupujú a CISP pôsobia vo veľkom rozsahu a ponúkajú štandardizované služby). Preto je dôležité, aby boli zmluvné podmienky CISP začlenené a využívané v maximálnej možnej miere. Viac informácií o zmluvných podmienkach a uzatváraní zmlúv nájdete nižšie v časti 2.5.

Pokiaľ ide o bezpečnosť, opäť dôrazne odporúčame umožniť CISP neustále aktualizovať ponuky alebo umožniť dodávateľom pridávať produkty aj po termíne predkladania, pokiaľ budú zodpovedať pôvodným parametrom RFP. Súvisí to so skutočnosťou, že bezpečnostné funkcie a služby sa rýchlo vyvíjajú a CISP často predstavujú služby zamerané na bezpečnosť, ktoré sú v mnohých prípadoch voľne použiteľné. Upozorňujeme, že je dôležité mať aspoň základnú úroveň zabezpečenia (pozri minimálne požiadavky vyššie), ktorá zaručí, aby zmeny v ponukách zabezpečenia neboli škodlivé.

Je samozrejmé, že v RFP na cloudové služby je jadrom bezpečnosti model zdieľanej zodpovednosti. Každá strana musí mať jasno v tom, aké sú jej povinnosti v oblasti zabezpečenia, a CISP by mali mať povinnosť zdokumentovať bezpečnostné povinnosti CISP/zákazníkov v súvislosti s cloudovými technológiami, ktoré CISP poskytujú. Rovnako by mali zákazníkom sprístupniť dokumentáciu, ktorá im pomôže zaviesť a automatizovať osvedčené bezpečnostné postupy.

Rámcová dohoda o poskytovaní cloudových služieb by mala zabezpečiť flexibilitu pri vyradovaní dodávateľa, ktorý už nespĺňa minimálne požiadavky na bezpečnosť a plnenie predpisov uvedené v RFP na cloudové služby.

2.4 Stanovenie cien

Ak chcú organizácie verejného sektora uzavrieť zmluvu na cloudovú technológiu spôsobom, ktorý zodpovedá kolísavému dopytu, potrebujú zmluvu, ktorá im umožní platiť za služby podľa spotreby – s požadovaným riadením cloudu a prehľadom o spotrebe a výdavkoch.

Dôležité je, aby sa RFP na cloudové služby zamerali na hodnotu a celkové náklady na vlastníctvo (TCO z angl. „total cost of ownership“), nielen na jednoduché porovnanie jednotkových cien rovnakých položiek. Táto zaužívaná prax hľadania najnižšej jednotkovej ceny sa nepremieta do modelu cloudu a ako taká nemá tendenciu viesť k ekonomicky najvýhodnejšej ponuke alebo celkovo najnižšej cene.

*Ako pomôcka pri hodnotení cien CISP je užitočné mať najprv predbežnú kvalifikáciu alebo užší zoznam CISP s **minimálnymi požiadavkami týkajúcimi sa cien**, aby sa pre rámcovú zmluvu mohli kvalifikovať CISP s podobnými schopnosťami. Následne sa proces hodnotenia objednávok vyplývajúcich z rámcovej zmluvy a minisúťaž môže zamerať na výber typických príkladov cloudových architektúr a **cenových scenárov**, ktoré zodpovedajú niektorým typickým pracovným zaťaženiam verejného sektora, so žiadosťou o ich ocenenie zo strany CISP. Odporúčajú sa aj ukážky testov naživo, ktoré umožnia porovnanie výkonu a elasticity služieb cloudových technológií, ktoré CISP poskytujú. Vzorový ukázkový testovací skript pre cloudové technológie nájdete v prílohe B.*

2.4.1 Minimálne požiadavky

Časť v RFP na cloudové služby venovaná cenám má štyri kľúčové prvky:

1. **Ceny za spotrebu:** Zákazníci cloudu zapracujú spotrebný model s priebežnými platbami, v rámci ktorého na konci každého mesiaca jednoducho zaplatia za využitie, čo je optimálne pre metriky spotreby a zdrojov.
2. **Transparentné stanovovanie cien:** Ceny CISP by mali byť verejne dostupné a transparentné.
3. **Dynamické stanovovanie cien:** Zahŕňa flexibilitu, ktorá umožňuje kolísanie cien cloudu na základe trhových cien. Tento prístup využíva dynamickú a konkurenčnú povahu cloudových cien a podporuje inovácie a znižovanie cien.

4. **Kontrolované výdavky:** CISP by mali poskytovať nástroje na vykazovanie, monitorovanie a predpovedanie, ktoré zákazníkom umožňujú (1) monitorovať spotrebu a výdavky na súhrnnej aj podrobnej úrovni, (2) prijímať upozornenia, keď spotreba a výdavky dosiahnu určené prahové hodnoty a (3) odhadnúť spotrebu a výdavky s cieľom plánovať rozpočet na cloud v budúcnosti.

Znenie vzorovej RFP: Stanovenie cien

<ORGANIZÁCIA> žiada, aby odpovedajúci CISP uviedli navrhovanú metódu a cenový model v súvislosti s poskytovaním každej svojej služby koncovým používateľom ako možnosť komerčného cloudu.

CISP poskytne:

- Dokument s definíciou služby alebo odkazy na definície služby
- Dokument so zmluvnými podmienkami
- Dokument s uvedením cien (odkazy na verejné ceny sú prijateľné za predpokladu, že úplný cenník/dokument s cenami je k dispozícii na vyžiadanie)

Cenu budú predstavovať náklady na najbežnejšiu konfiguráciu služby. CISP by mali poskytovať možnosti objemových zliav a nástroje na výpočet cien na zistenie skutočnej ceny toho, čo sa kupuje, a celkovej hodnoty poskytnutej kupujúcemu (napr. služby na optimalizáciu a následné zníženie nákladov).

V zmysle rámcovej dohody môžu nákupcovia hovoriť s dodávateľmi a požiadať ich, aby vysvetlili svoj opis služby, zmluvné podmienky, dokumenty/model uvádzajúce ceny alebo definície služby. O akýchkoľvek rozhovoroch s dodávateľmi sa budú uchovávať záznamy.

Dodatočné cenové požiadavky

- Poskytovanie cloudových technológií s dynamickým cenovým modelom, ktorý zabezpečuje maximálnu flexibilitu podnikania a umožňuje škálovateľnosť a rast.
- Atribúty cien musia zahŕňať nasledujúce:
 - Sú ceny uvedené vo formáte služby na požiadanie, podľa spotreby a priebežne? Vysvetlite svoj model cenotvorby.
 - Viete poskytnúť ďalšie zľavy v prípade viazanej spotreby a/alebo objemového nákupu? Uveďte podrobnosti.
 - Sú ceny verejne dostupné a transparentné? Uveďte odkazy na verejne dostupné ceny.
 - Je cenotvorba dynamická a rýchlo a efektívne reaguje na konkurenciu na trhu?
 - Zabezpečujete osvedčené postupy a zdroje na sledovanie výdavkov?
 - Zabezpečujete osvedčené postupy a zdroje na optimalizáciu nákladov?

Cenová transparentnosť

Vzhľadom na neustály trend poklesu cien v oblasti komerčných cloudových technológií poháňaný inováciami a konkurenciou, merané jednotkové náklady na službu CISP, ktoré hradí <ORGANIZÁCIA> podľa rámcovej zmluvy, nikdy nepresiahnu jednotkovú cenu poskytovateľa cloudu zverejnenú na webovej stránke poskytovateľa cloudu, ktorá je účinná v čase využitia služby zákazníkom.

Upozornenia na rozpočet a fakturáciu/výkazy

Na preukázanie poskytovania a využívania cloudových technológií by CISP mali <ORGANIZÁCII> poskytnúť nástroje na generovanie podrobných výkazov o fakturácii s rozpisom nákladov na hodiny, dni alebo mesiace, podľa jednotlivých účtov v organizácii, podľa produktu alebo zdroja produktu, alebo podľa označení, ktoré určí zákazník. <ORGANIZÁCIA> potvrdzuje, že v rámci modelu zdieľanej zodpovednosti v súvislosti s cloudom bude <ORGANIZÁCIA> zodpovedná za používanie funkcií a nástrojov na rozpočtovanie a fakturáciu, ktoré jej CISP poskytuje na splnenie jedinečných požiadaviek na prognózovanie a vykazovanie.

- Uved'te, ako si môže <ORGANIZÁCIA> prezerať informácie o fakturácii na podrobnej aj súhrnnej úrovni, vizualizovať vzory výdavkov na zdroje CISP v priebehu času a predpovedať budúce výdavky.
- Uved'te, ako si môže <ORGANIZÁCIA> filtrovať zobrazenie spotreby/fakturácie podľa služby, podľa prepojeného účtu alebo podľa vlastných označení použitých na zdroje a ako môže vytvárať upozornenia týkajúce sa fakturácie, ktoré pošlú oznámenie, keď sa spotreba priblíži k prahovým hodnotám/rozpočtu <ORGANIZÁCIE> alebo ich prekročí.
- Uved'te, ako môže <ORGANIZÁCIA> predpovedať, koľko cloudových služieb využije v definovanom predpovedanom časovom období na základe predchádzajúcej spotreby. CISP by mal ponúknuť **odhad** toho, aké vyúčtovanie CISP <ORGANIZÁCII> vystaví, a umožní <ORGANIZÁCII> používať upozornenia a rozpočty na sumy, ktoré sa podľa predpovede použijú, aby mala väčšiu kontrolu nad nákladmi a výdavkami.

2.4.2 Porovnanie medzi dodávateľmi

Organizácie verejného sektora často v súťaži medzi uchádzačmi požadujú použitie hodnotiacich kritérií, ako je najlepší pomer ceny/kvality, ekonomicky najvýhodnejšia ponuka (MEAT) alebo najnižšia cena. Pri plánovaní ocenenia objednávok vyplývajúcich z rámcovej dohody (tzv. call-offs) alebo minisúťaží je dôležité vypracovať prístup, ktorý zohľadňuje jedinečné vlastnosti cloudu. Treba napríklad vedieť, že jednoduché porovnávanie riadkových položiek medzi ponukami poskytovateľov cloudu (napr. výpočty alebo úložisko) nie je efektívny spôsob porovnávania, pretože nezohľadňuje funkcie, ako je výkon, optimalizácia nákladov pomocou cloudových natívnych služieb a monitorovacích nástrojov CISP ani odlišné služby, ktoré môžu CISP ponúkať zadarmo. Katalógová cena CISP môže navyše predstavovať desiatky tisíc riadkových položiek a modely cenotvorby sa líšia od jednej služby k druhej a od jedného poskytovateľa k druhému.

Analýza TCO

Odporúčame zamerať sa na celkové náklady na vlastníctvo (TCO z angl. „total cost of ownership“) vymedzených prípadov použitia, ktoré zohľadňujú všetky aspekty cloudového riešenia (vrátane partnerských služieb, štandardizovaných zliav CISP, technických funkcií, ktoré môžu zvýšiť výkon a znížiť/optimalizovať náklady, atď.).

Porovnanie podľa scenárov

Hodnotiaci proces môže brať do úvahy aj typické scenáre, ktoré zodpovedajú bežným systémom alebo aplikáciám. Takéto scenáre (napr. webhosting alebo implementácia systému ľudských zdrojov s x počtom používateľov atď.) môžu zahŕňať premenné, ako je rýchlosť a rozsah zdrojov, výkon aplikácie alebo riešenia, časy prístupu k úložisku, nízkoobjemové komplexné dáta v porovnaní s jednoduchými výpočtovými úlohami s veľkým objemom atď. Typické scenáre môžu mať aj aplikácie alebo systémy. Napríklad spracovanie veľkého objemu pri daňovom priznaní, núdzové upozornenia v prípade varovania pred povodňami. Tieto scenáre by mali byť komplexné, aby zahŕňali rozsah technológií a služieb, ktoré môže zákazník počas projektu využívať. Zákazník si tak môže porovnať odhadované celkové náklady na projekt.

Finančné a technické porovnanie scenárov

Pri porovnávaní cien medzi ponukami CISP je tiež dôležité vziať do úvahy technické výhody. Napríklad, jeden z CISP môže vďaka svojmu modelu s dátovými centrami v klastroch v rámci geografického regiónu zákazníkom umožniť vybudovať topológiu obnovy po havárii (DR z angl. „Disaster Recovery“) v režime „active-active“. CISP, ktorý nemá tento druh redundancie a konfigurácie dátového centra, môže byť o x % drahší vzhľadom na náklady na zohľadnenie potrieb obnovy po havárii. Ako príklad toho, prečo je holistický prístup k cenotvorbe, ktorý zahŕňa ďalšie technické vlastnosti, rozhodujúci pri hodnotení CISP, posúďte nižšie uvedenú alternatívu priameho porovnania rovnakých položiek.

Príklad: Zákazník chce porovnať cenu objektového úložiska, ktoré poskytujú kvalifikovaní CISP v rámci dohody. Cena položky úložnej „jednotky“ u CISP 1 je 0,023 €/GB. Cena tej istej „jednotky“ u CISP 2 je 0,01 GB. Pri jednoduchom porovnaní jednotiek by zákazník nekládol kritické otázky ako:

1. Koľko redundantných kópií objektu je k dispozícii v prípade zlyhania? Vo vyššie uvedenom príklade je CISP 1 pripravený utrieť súbežnú stratu údajov v dvoch rôznych zariadeniach a zachovať viaceré kópie údajov. V prípade CISP 2 sa nadbytočné kópie nevytvárajú.
2. Aká je úroveň udržateľnosti uložených objektov? U CISP 1 je to 99,99999999 %, kým u CISP 2 je 99 %.
3. Berte do úvahy náklady na vlastníctvo celého projektu alebo pracovného zaťaženia počas životnosti a ako môžu funkcie optimalizácie nákladov znížiť náklady, pokiaľ ide o spôsob ukladania a používania údajov (napríklad zvýšenie používania bezserverových funkcií CISP môže znížiť náklady o x %).

Toto sú len niektoré z mnohých iných technických aspektov, ktoré sa zohľadňujú pri cenotvorbe, najmä pokiaľ ide o bezpečnosť a dodržiavanie predpisov.

Faktory, ktoré treba zohľadniť pri cenových scenároch

Základné sadzby – ide v podstate o verejné ceny CISP. CISP by mali tieto ceny uvádzať verejne, avšak (ako je uvedené vyššie) v záujme efektívneho porovnania CISP môžu zákazníci požiadať o 3 až 5 konkrétnych scenárov (alebo podľa toho, koľko z nich zákazník považuje za primerané), ktoré budú oceňovať všetci dodávatelia. Scenáre by mali byť komplexné, aby zahŕňali širokú škálu služieb a technológií, ktoré zákazník pravdepodobne využije v priebehu projektu. Zákazník tak môže porovnať celkové odhadované náklady na projekt. Porovnania na úrovni riadkovej položky/SKU bývajú pre zákazníkov a dodávateľov skôr problematické než užitočné (zákazníci by museli porovnávať desiatky tisíc riadkových položiek u všetkých CISP a dodávatelia by museli zabezpečiť túto úroveň podrobností a spravovať ju, hoci sa skutočná cena určuje len na základe spotreby služby).

Pre zákazníkov cloudu, ktorí chcú získať najlepší pomer hodnoty a kvality, je hodnotenie obsahovej množiny schopností CISP nevyhnutnosťou. CISP môžu mať, napríklad, množstvo služieb, ktoré sú buď bezplatné, alebo takmer bezplatné, pričom cenové hodnotenie by malo zohľadňovať takéto služby aj skutočnosť, že ostatní CISP môžu za podobné funkcie účtovať poplatky.

Hodnotiace kritériá môžu byť napísané takým spôsobom, ktorý CISP umožní poukázať na svoje „zahrnuté x predvolené“ funkcie a na to, aký majú tieto služby celkový dopad na náklady. Hodnotiace kritériá sa môžu zamerať aj na ceny CISP podľa objemu/úrovne a komerčne dostupných zliav, ako sú rezervované inštancie/spotové inštancie. Napríklad:

- úspora x %, ak si zákazníci zakúpia rezervovanú výpočtovú kapacitu (1 rok, 3 roky atď.)
- zľava x % pri viacúrovňovej/množstevnej cenotvorbe
- úspora x % na základe preskúmania architektúry a optimalizácie infraštruktúry, ako je prechod na vhodnejšiu výpočtovú možnosť
- Ako je uvedené vyššie, vezmite do úvahy náklady na celú životnosť a ako môžu funkcie optimalizácie nákladov znížiť náklady.

CENOVÝ SCENÁR

Uchádzači musia poskytnúť ceny v prípade nižšie uvedeného scenáru len na účely hodnotenia. Skutočná cena bude vychádzať zo spotreby služieb podľa modelu platby za použitie a na požiadanie.

Nižšie sú uvedené reprezentatívne požiadavky na účely zisťovania cien. Uvádzajú sa s výslovným porozumením, že počas trvania zmluvy sa tieto nominálne požiadavky zmenia. Uveďte ceny za kapacitu na požiadanie na 12 a 36 mesiacov a za rezervovanú kapacitu na 12 a 36 mesiacov.

Uveďte:

- *Názov navrhovaného riešenia (riešeni):*
- *Najlepšia cena uchádzača:*
- *Prevádzkové hodiny: 24 x 7 x 365*
- *Dostupnosť služby: 99,95 %*

Cenové scenáre môžu zahŕňať aj príklady od existujúcich zákazníkov s podobným pracovným zaťažením, ktorí optimalizovali svoje výdavky počas 1/2/3 rokov – pomocou monitorovacích a optimalizačných nástrojov CISP, prijatím optimalizovaných cloudových natívnych riešení a znížením cien CISP.

2.5 Nastavenie plnenia zmluvy/zmluvné podmienky

Cloudové technológie a operácie, ktoré CISP poskytujú, sú štandardizované už pri návrhu, preto sú štandardizované aj zmluvné podmienky. Existuje však možnosť okrajovo tieto zmluvy upraviť tak, aby sa prispôbili miestnym legislatívnym a regulačným kontextom.

Tradičné metódy obstarávania IT často zahŕňajú prísne pravidlá, ktoré od uchádzačov vyžadujú splnenie mnohých alebo všetkých požiadaviek obstarávania, inak sú ich ponuky zamietnuté. Prípadne môžu obsahovať prísnu podskupinu povinných požiadaviek. Keď sa tento spôsob získavania zdrojov použije v prípade cloudových technológií, ktoré sú v skutočnosti súborom štandardizovaných komponentov a nástrojov určených na pomoc pri návrhu vlastných riešení, obstarávania zvyčajne zlyhávajú.

2.5.1 Zmluvné podmienky

Pri uzatváraní zmlúv v rámci RFP na cloudové služby je prvým krokom preskúmanie a pochopenie existujúcich obchodných podmienok CISP, ktoré možno v mnohých prípadoch verejne nájsť na webových stránkach CISP. Subjekty verejného sektora čoraz častejšie prijímajú obchodné podmienky predložené zo strany CISP. Súčasťou tohto úsilia o oboznámenie sa s podmienkami je stretnúť sa s CISP a ich partnermi, aby sa podrobne prediskutovali ich prístupy. Kľúčovou otázkou, ktorú si treba položiť, je „prečo“ CISP pracujú s konkrétnymi podmienkami. Niektoré z týchto podmienok sa môžu zdanlivo líšiť od bežných podmienok v oblasti IT, no existujú veľmi špecifické dôvody, „prečo“ sú súčasťou zmluvy o cloude. Ak verejne dostupné podmienky nie sú prijateľné, CISP majú často mierne upravitel'né dohody pre podnikových zákazníkov, ktoré možno preskúmať.

Spolu s preskúmaním zmluvných podmienok CISP je dôležité porozumieť aj existujúcim zásadám, nariadeniam a/alebo zákonom (napr. tým, ktoré sa týkajú technológie, klasifikácie údajov, ochrany údajov, personálu atď.). Zásady/predpisy/zákony, ktoré upravujú nákup a využívanie tradičných IT ponúk, môžu byť v rozpore s modelom CISP. Napríklad možnosť používať len tie cloudové technológie, ktoré boli zahrnuté v pôvodnej ponuke rámcovej dohody prostredníctvom RFP na cloudové služby. CISP neustále pridávajú nové služby a nové funkcie. Obmedzenie prístupu k týmto novým službám len preto, že sa riadite tradičným prístupom obnovy IT produktov, nemá pre koncového zákazníka zmysel. Ak je to tak, je dôležité podrobne s CISP tieto zásady/predpisy a/alebo zákony prediskutovať a preskúmať.

Využite diskusie pred vypracovaním RFP

Ako je uvedené vyššie, pred vypracovaním RFP si nájdite čas na stretnutie s CISP a súvisiacimi dodávateľmi, aby ste sa oboznámili s ich zmluvnými podmienkami a poučili ich o prístupe, zásadách, nariadeniach a zákonoch vášho subjektu. Najdôležitejšou súčasťou týchto diskusií je, aby sa obe strany dozvedeli, „prečo“ príslušné podmienky fungujú tak, ako fungujú. Napríklad zmluvné podmienky cloudu sa líšia od podmienok tradičného dátového centra, spravovaných služieb, použitia hardvéru, použitia softvéru a systémovej integrácie. Keďže ide o samostatné modely, ktoré zahŕňajú neustále inovácie, ich obchodné modely si vyžadujú, aby bol proces vypracovania RFP dostatočne flexibilný a umožnil rokovania alebo diskusie na objasnenie konkrétnych bodov.

Ak organizácie verejného sektora umožnia objasnenie podmienok počas diskusií alebo rokovaní, lepšie porozumejú cloudovým modelom a predídu problémom so zamietnutím poskytovateľov, ktorí by v skutočnosti mohli uspokojiť potreby organizácie. Organizácia zvyčajne vopred identifikuje určité podmienky, o ktorých je ochotná diskutovať a rokovať pred zadaním. Predbežným vyjednaním prijateľných podmienok s uchádzačom organizácia zaistí, že sa pre zadanie najlepšie hodí, a vyrieši rozdiely, ktoré by inak mohli viesť k zamietnutiu účinnej ponuky. Subjekty verejného sektora môžu zároveň preskúmať svoje zásady, nariadenia a zákony a obe strany môžu zistiť, ako používanie cloudu zapadne do týchto modelov. Často sa dá pracovať s už existujúcimi ustanoveniami. V prípade problematickej oblasti môžu obe strany spolupracovať pri hľadaní riešenia (ideálne je diskutovať o tom v dostatočnom predstihu pred predložením RFP a následným zmluvným rokaním).

Flexibilita pri rokovaní

Aby mohli byť zmluvy podpísané podľa miestnej legislatívy a bolo zároveň možné spoliehať sa na štandardizované zmluvné podmienky CISP, odporúča sa (1) požiadať uchádzačov o ich štandardnú zmluvu, (2) neprijíť neprimerané zmluvné podmienky pri vypracúvaní rámcovej zmluvy na účely RFP na cloudové služby a (3) zabezpečiť možnosť rokovania o všetkých ustanoveniach týkajúcich sa konzultácie a návrhov, ktoré vyúsťia do rámcovej zmluvy (samozrejme okrem povinných ustanovení stanovených zákonom).

Poznámka: Rozsah zdieľanej zodpovednosti je súčasťou modelu cloudu a mal by sa odraziť v podmienkach zmluvy (napr. CISP potvrdzuje, že zákazníci vlastnia svoje údaje tam, kde sa nachádzajú, a poskytuje nástroje na zabezpečenie toho, aby bol výber umiestnenia údajov obmedzený, **ALE** za používanie týchto nástrojov je zodpovedný zákazník alebo partner).

*Upozorňujeme, že je dôležité, aby pre každú skupinu existovali v rámcovej dohode o poskytovaní cloudových služieb **odlišné súbory zmluvných podmienok**. „Univerzálny prístup“ k uzatváraniu zmlúv pre všetky skupiny bude mať za následok problémy týkajúce sa technickej realizovateľnosti a kompatibility.*

Ako už bolo uvedené, RFP s povinnými podmienkami, o ktorých sa nedá rokovať, sú pre poskytovateľov v podstate nekompromisným návrhom, ktorý môže viesť k odmietnutiu inak prijateľnej ponuky. Organizácie verejného sektora by mali dôkladne zvážiť dôsledky používania povinných podmienok, **pokiaľ, samozrejme, nevyplývajú zo zákona**. Organizácie by si mali byť isté potrebou povinnej požiadavky alebo podmienky, pretože v ďalších rokovaniach budú klasifikované ako povinné. Používanie povinných požiadaviek alebo podmienok by sa malo obmedziť na absolútne minimum, aby mala organizácii flexibilitu potrebnú na získanie najlepšej technológie a riešenia.

Majte na pamäti, že cloudové technológie, ktoré CISP ponúkajú, sú v plnej miere štandardizované a dodávané plne automatizovaným spôsobom. CISP teda nie je schopný prijať zmenu podmienok, ktorá by si vyžadovala úpravu základnej služby. Ceny služieb sú navyše zvyčajne verejné a štandardizované pre všetkých používateľov, čo znamená, že CISP nemôže upravovať ceny, aby absorboval väčšie riziko v mene konkrétneho zákazníka.

Nepriame obstarávanie

Alternatívnou možnosťou nákupu cloudových technológií priamo od CISP je ich nákup od sprostredkovateľa CISP. Viac informácií o sprostredkovateľoch CISP nájdete vyššie v časti 2.1.3.

Znenie vzorovej RFP: Zmluvné podmienky

CISP alebo zastupujúci dodávatelia musia poskytnúť svoje verejne dostupné všeobecné podmienky a poskytnúť spätnú väzbu ku kľúčovým všeobecným podmienkam poskytnutým <ORGANIZÁCIOU>.

<ORGANIZÁCIA> má v úmysle uzavrieť s úspešným uchádzačom písomnú zmluvu na základe zmluvných podmienok uchádzača. Uchádzač by mal <ORGANIZÁCIU> na preskúmanie poskytnúť súbor navrhovaných zmluvných podmienok, ktoré predstavujú jeho najlepší obchodný a právny návrh. Navrhovatelia a <ORGANIZÁCIA> môžu diskutovať o oboch súboroch zmluvných podmienok počas fázy <DISKUSIA/ROKOVANIE>.

- *Rámcové hlavné podmienky na vysokej úrovni by tvorili nanajvýš tieto komponenty:*
 - *Trvanie rámcovej zmluvy*
 - *Riadenie rámcovej zmluvy*
 - *Plnenie rámcovej zmluvy*
 - *Ukončenie rámcovej zmluvy*
 - *Rozsah rámcovej zmluvy*
 - *Proces objednávaní*
 - *Ustanovenia o zachovaní mlčanlivosti*
 - *IP špecifická pre kategóriu a informácie*
 - *Minimálne technické požiadavky, ktoré musia CISP spĺňať – napr. štandardy kvality, akreditácia, bezpečnosť a ochrana údajov*
- ***Pre každú skupinu v rámcovej dohode budú platiť odlišné podmienky***
- *Špecifiká služby CISP sa môžu zväčšiť a budú sa riešiť pri konkrétnych objednávkach vyplývajúcich z rámcovej dohody*
- *Možnosť zmien zmluvy – podmienky by nemali obmedzovať zákazníkov ani dodávateľov pri dohode na zmenách zmluvy alebo integrácii nových služieb alebo vylepšení. Vyvíjajúca sa povaha cloudových služieb predpokladá, že priebežne budú k dispozícii všetky vylepšenia služieb, ktoré môžu pomôcť zákazníkovi zvýšiť efektívnosť.*
- *Zákazník by nemal špecifikovať zmluvy o poskytovaní služieb. Podmienky zákazníka by nemali definovať zmluvy o poskytovaní služieb na mieru s konkrétnou províziou, ktoré sa líšia od štandardných modelov poskytovania služieb, ktoré CISP používajú. Ak budú pre CISP povolené štandardné zmluvy o poskytovaní služieb, CISP budú môcť zachovať nízke náklady a preniesť ich na zákazníkov, pričom zákazníci budú mať istotu, že CISP dokáže zmluvy o poskytovaní služieb splniť.*
- *Limity zodpovednosti by mali byť primerané. Zodpovednosť by mala byť úmerná obstarávaným službám a horné limity zodpovednosti by nemali byť neúmerne vysoké. Neúmerne vysoké limity by odrádzali CISP od prijímania projektov s nízkou hodnotou. Tieto projekty zákazníkom často slúžia ako praktický úvod a „skúšobný“ prípad, aby mohli zistiť, či sú určité cloudové riešenia pre ich organizáciu efektívne.*
- *Zákazníci by mali vlastniť svoje údaje. Zákazníci by mali kontrolovať a vlastniť svoje údaje a mali by mať možnosť určiť geografickú polohu, v ktorej sa uchovávajú. Zákazníci vďaka tomu predídu uzamknutiu zo strany dodávateľa (tzv. vendor lock-in) a budú môcť voľne prenášať údaje k novým poskytovateľom.*

2.5.2 Podmienky používania softvéru

Hoci sa táto príručka zameriava na nákup cloudových technológií typu IaaS a PaaS, ktoré poskytujú CISP, je dôležité zdôrazniť aj podmienky používania softvéru, ktoré môžu organizácie verejného sektora zvážiť pri nákupe softvéru od dodávateľov. Na obrázku 1 (strana 5) si môžete pozrieť, ako sa nakupuje softvér v rámci dobre štruktúrovanej RFP na cloudové služby.

Softvér zohráva kľúčovú úlohu takmer v každom podnikaní, vrátane verejného sektora. Zahrnutie povinností, ako sú zmluvné podmienky licencovania softvéru, do RFP na cloudové služby, pomôže subjektom verejného sektora získať najlepší pomer ceny/kvality a zabezpečiť im slobodu pri výbere dodávateľov pri nákupe softvéru.

Ďalšie informácie nájdete v časti Desť princípov spravodlivého licencovania softvéru pre cloudových zákazníkov⁹. Zásady vypracovalo združenie Cigref¹⁰ združujúce veľké francúzske spoločnosti a orgány verejnej správy, ktoré zastupujú používateľov digitálnych technológií, v spolupráci so združením CISPE a s podporou ďalších európskych obchodných združení CIO a poskytovateľov s cieľom riešenia postupov, ktoré obe združenia považujú za škodlivé pre digitálnu transformáciu organizácií všetkých veľkostí pri ich prechode do cloudu.

Znenie vzorovej RFP: Softvér

<ORGANIZÁCIA> má v úmysle uzavrieť s úspešným uchádzačom písomnú zmluvu na základe zmluvných podmienok uchádzača. Uchádzač by mal <ORGANIZÁCIU> na preskúmanie poskytnúť súbor navrhovaných zmluvných podmienok, ktoré predstavujú jeho najlepší obchodný a právny návrh. Dodávatelia softvéru a <ORGANIZÁCIA> môžu diskutovať o oboch súboroch zmluvných podmienok počas fázy <DISKUSIA/ROKOVANIE>.

Požiadavka 1.0. Dodávatelia softvéru musia uviesť jasné licenčné podmienky vrátane rozpisu nákladov na súhrnnej a podrobnej úrovni.

Požiadavka 1.1. Všetky poplatky súvisiace s nedodržaním licenčných podmienok musia byť uvedené na súhrnnej a podrobnej úrovni.

Požiadavka 2.0. Softvérové licencie musia <Organizácii> poskytovať možnosť migrovať licencovaný softvér z lokálneho prostredia do cloudu podľa vlastného výberu bez toho, aby sa vyžadovalo zakúpenie samostatných duplicitných licencií pre rovnaký softvér.

Požiadavka 2.1. Softvérové licencie nesmú obsahovať licenčné obmedzenia a zvýšené náklady, ktoré obmedzujú schopnosť <Organizácie> používať licencovaný softvér v cloude podľa vlastného výberu.

Požiadavka 3.0. Softvérové licencie musia <Organizácii> povoľovať spúšťať licencovaný softvér na ich vlastnom hardvéri (zvyčajne označovanom ako „on-premises“ softvér), ako aj na cloude podľa vlastného výberu.

Požiadavka 4.0. Softvérové licencie nesmú vyžadovať, aby licencovaný softvér bežal iba na hardvéri určenom výhradne pre <Organizáciu>.

Požiadavka 5.0. Dodávatelia softvéru nesmú penalizovať <Organizáciu>, ak sa ich licencovaný softvér používa v cloudovej ponuke iného dodávateľa, napríklad zahrnutím práv na vykonávanie prísnejších alebo rušivých softvérových auditov alebo ukladaním vyšších licenčných poplatkov za softvér.

⁹ <https://www.fairsoftware.cloud/principles/>

¹⁰ <https://www.cigref.fr/>

Požiadavka 6.0. Adresárový softvér musí podporovať otvorené štandardy na synchronizáciu a autentifikáciu identít používateľov nediskriminačným spôsobom s inými službami identity.

Požiadavka 7.0. Dodávatelia softvéru nesmú účtovať rozdielne ceny za rovnaký softvér výlučne na základe toho, kto vlastní hardvér, na ktorom je nainštalovaný.

Požiadavka 7.1. Ceny za softvér nesmú rozlišovať medzi softvérom nainštalovaným vo vlastnom dátovom centre <Organizácie>, externe spravovanom dátovom centre, na počítačoch prenajatých od tretej strany alebo u poskytovateľa cloudu podľa preferencií <Organizácie>.

Požiadavka 8.0. Počas platnosti zmluvy nesmú dodávatelia softvéru zásadne meniť licenčné podmienky, aby <Organizáciu> neobmedzili v už povolenom používaní, pokiaľ to nevyplýva zo zákona alebo z bezpečnostných dôvodov.

Požiadavka 9.0. Dodávatelia softvéru nesmú <Organizáciu> zavádzať ručením, že softvérové licencie budú pokrývať jej zamýšľané použitie softvéru, ako je uvedené v <požiadavkách Organizácie>, ak by si také použitie mohlo vyžadovať zakúpenie dodatočných licencií.

Požiadavka 10.0. Ak má <Organizácia> právo predávať a prenášať softvérové licencie, dodávatelia softvéru musia <Organizácii>, ktorá zákonne získala licenciu na ďalší predaj, naďalej ponúkať podporu a opravy za spravodlivých podmienok.

2.5.3 Ako si vybrať dodávateľa na projekt spomedzi ocenených

Orgány verejného sektora, ktoré sú zmluvnou stranou rámcovej zmluvy, si môžu v prípade potreby objednať alebo „doobjednať“ služby, ktoré potrebujú. Uzavretie zmluvy o doobjednaní na základe rámcovej dohody umožňuje kupujúcim spresniť požiadavky s dodatočnou funkčnou špecifikáciou pre konkrétnu objednávku, pričom si zachovávajú výhody vyplývajúce z rámcovej dohody.

V prípade potreby sa môže uskutočniť minisúťaž, v ktorej sa určí najlepší dodávateľ pre konkrétny pracovný rozsah alebo projekt. V minisúťaži postupuje zákazník do ďalšej súťaže v zmysle rámcovej zmluvy tým, že vyzve všetkých dodávateľov v konkrétnej skupine, aby odpovedali na súbor požiadaviek. Zákazník vyzve všetkých kvalifikovaných dodávateľov v skupine, aby predložili ponuku, a preto je dôležité pre víťazov minisúťaže uviesť v RFP na cloudové služby minimálne požiadavky. Zabezpečí sa tak vysoký štandard možností v rámci každej skupiny.

Znova upozorňujeme, že je dôležité, aby mala každá kategória skupín odlišné súbory zmluvných podmienok (napr. verejná IaaS/PaaS, komunitná IaaS/PaaS, súkromná IaaS/PaaS), pretože „univerzálny prístup“ pri uzatváraní zmlúv pre každú skupinu bude mať za následok problémy týkajúce sa technickej realizovateľnosti a kompatibility.

Vzorové znenie RFP v prípade výberu spomedzi ocenených nájdete v časti 2.1.4.

2.5.4 Vstup a odchod

Pri vypracúvaní rámcovej dohody o poskytovaní cloudových služieb treba mať na pamäti možnosť dynamického systému obstarávania (DPS z angl. „Dynamic Purchasing System“). S modelom DPS budú do rámcovej dohody prijatí všetci dodávatelia, ktorí spĺňajú minimálne požiadavky rámcovej dohody. Počet dodávateľov, ktorí sa môžu zapojiť do rámcovej dohody, nie je pevne obmedzený a na rozdiel od tradičného rámcového modelu môžu dodávatelia požiadať o zapojenie sa do rámcového DPS kedykoľvek počas platnosti rámcovej dohody.

Subjektom verejného sektora dôrazne odporúčame, aby nastavili vysoké štandardy na zabezpečenie kvality a zaistenia služieb od kvalifikovaných dodávateľov, ale aby zároveň neboli príliš špecifickí a nediskvalifikovali CISP spôsobom, ktorý nezabezpečuje spravodlivú hospodársku súťaž. V konečnom dôsledku je cieľom predísť tomu, aby bol koncový používateľ zahľtený veľkým počtom možností, a zachovať vysoký štandard dostupných cloudových technológií.

3.0 Osvedčené postupy/získané skúsenosti

Nižšie uvádzame niekoľko poznatkov o tom, ako realizovať úspešnú rámcovú dohodu o poskytovaní cloudových služieb s dobre vypracovanou RFP na cloudové služby.

3.1 Riadenie cloudu

Riadenie v cloude spočíva v spoločnej zodpovednosti. CISP poskytujú funkcie a služby na integráciu riadenia cloudu do každého aspektu cloudového prostredia, zatiaľ čo zákazníci prinášajú svoje existujúce štandardy riadenia cloudu a zisťujú, ako riadenie cloudu podporuje samotný cloud.

Zákazníci majú v cloude možnosť vybudovať si IT prostredie, aké chcú, a nemusia len spravovať to, čo majú. Cloud umožňuje zákazníkom: (1) začať s kompletným inventárom všetkých aktív IT; (2) centrálnie spravovať všetky tieto aktíva a (3) vytvárať upozornenia týkajúce sa používania/fakturácie/zabezpečenia/atď. Všetky tieto mimoriadne dôležité výhody cloudu pomáhajú zákazníkovi získať optimalizovanú – a v čo najväčšom možnom rozsahu automatizovanú – architektúru bez potreby neustáleho obstarávania a inštalácie nového hardvéru. O to sa starajú CISP, ktorí zákazníkovi pomáhajú presunúť orientáciu zo správy nediferencovanej infraštruktúry na nevyhnutnú prevádzkovú úroveň.

Odporúčame pozrieť sa na cloud CISP ako na veľmi veľké rozhranie API. Či už spúšťate nový server, alebo meníte nastavenie zabezpečenia, v podstate iba realizujete volania API. Každá zmena prostredia sa zachytáva a zaznamenáva (kto zmenu zaznamenáva, čo, kde a kedy). Tým je zabezpečené riadenie cloudu, kontrola a viditeľnosť, čo je možné len v cloudovom prostredí. Zákazníci tak môžu prehodnotiť svoje existujúce modely riadenia IT a určiť, ako ich možno zefektívniť a zlepšiť vzhľadom na výhody, ktoré cloud prináša.

Riadenie cloudu môže predstavovať aj komunikáciu a začlenenie pozitívnych zmien procesov a nových zručností, ktoré s cloudom prichádzajú. Napríklad projektoví manažéri majú skúsenosti s mesiacmi čakania na vybudovanie IT prostredia, a preto môžu výrazne nadhodnotiť plány na vytvorenie vývojového alebo testovacieho prostredia v cloude (čo môže v cloude trvať len minúty). Prispôbenie sa tejto novoobjavenej agilite bude evolučným procesom a deje sa priebežne program po programe. Takéto získané skúsenosti by sa mali zdieľať, aby sa rámcová dohoda o poskytovaní cloudových služieb mohla naďalej vyvíjať takým spôsobom, aby boli požiadavky nastavené na nové procesy a agilitu.

3.2 Tvorba rozpočtu na cloud

Pokiaľ ide o to, ako štruktúrovať cenotvorbu pri cloude v režime platby podľa spotreby tak, aby vyhovovala požiadavkám verejného sektora na akvizíciu a rozpočtovanie, zistili sme, že pomáha zahrnúť služby CISP do jednej riadkovej položky (výpočet, úložisko, sieť, databáza, IoT atď.) – všetko pod riadkovou položkou „cloudové technológie“. Tento prístup zabezpečuje flexibilitu pri ponuke všetkých súčasných a nových technológií CISP používateľom v reálnom čase a poskytuje používateľom rýchly prístup k potrebným zdrojom práve vtedy, keď ich potrebujú. Zároveň zohľadňuje kolísanie dopytu, čo vedie k optimalizovanému využitiu a nízkym nákladom.

Organizácie verejného sektora môžu pridávať ďalšie riadkové položky pri objednávkach z iných skupín v zmysle rámcovej dohody, ak potrebujú konzultačné/odborné alebo spravované služby, softvér z marketplace, služby cloudovej podpory a školenia o ponukách CISP.

Ďalšiu flexibilitu pri uzatváraní zmlúv možno zabezpečiť využívaním doplnkových zmluvných riadkových položiek v rámci primeraných kategórií zdrojov na zohľadnenie budúceho rastu. Prípadne, ak by organizácia chcela spojiť cloudové technológie s konzultačnými/odbornými/spravovanými službami do jednej riadkovej položky, môže to urobiť pomocou riadkovej položky, ako je „Cloudové technológie a pomocná práca“.

Príklad takéhoto prístupu je znázornený nižšie. V tomto príklade sa každá jednotka riadkovej položky „#1001 – Cloudové technológie“ rovná 1,00 EUR použitých „cloudových technológií“. Každý mesiac je možné financovať prírastky objednávok na základe aktuálnych a predpokladaných prognóz používania.

Tabuľka 3 – Príklad cenovej štruktúry jednej riadkovej položky.

Č. POLOŽKY	DODÁVKY/SLUŽBY	MNOŽSTVO	JEDNOTKA	JEDNOTKOVÁ CENA	SUMA
1001	Cloudové technológie	1 000	Kus	1 EUR	1 000 EUR
1002	Poradenské služby	1	Za týždeň	3 000 EUR	3 000 EUR
1003	Podpora cloudu	1	Za mesiac	1 000 EUR	1 000 EUR
1004	Školenie o cloude	1	Za deň	3,00 EUR	3 000 EUR
1005	Cloudový marketplace	10	Kus	10 EUR	100 EUR

Príklad toho, ako môže táto štruktúra fungovať: Organizácia verejného sektora spolupracuje s CISP pri odhade, koľko cloudových technologických služieb bude organizácia využívať. Organizácia sa dohodne s dodávateľom na podmienkach – napr. 10 miliónov EUR na 5 rokov, čo predstavuje 2 milióny EUR ročne. Organizácia vyčlení počiatočnú sumu 2 milióny EUR za rok. Každý mesiac dostane vyúčtovanie a z fondu sa vyberú peniaze na zaplatenie. Čerpá sa z príslušného účtu. Zvyšné prostriedky sa monitorujú z hľadiska „burn rate“ (t. j. množstvo peňazí, ktoré sa utratia za mesiac) pomocou nástrojov CISP na monitorovanie a predpovedanie. Ak zostávajúce prostriedky klesnú, organizácia požiada finančného riaditeľa o dodatočné prostriedky, ktoré sa môžu vyčleniť na zachovanie poskytovania služieb.

Znenie vzorovej RFP: Cenotvorba – Uzatváranie zmlúv

PLATOBNÉ PODMIENKY

Platobné podmienky musia byť primerane štruktúrované tak, aby sa platilo iba za zdroje, ktoré <ORGANIZÁCIA> použije, ako je uvedené nižšie:

1. Mesačná platba bude vychádzať zo skutočného využitia/spotreby služieb a z verejne dostupných cien CISP.

MINIMÁLNA ZÁRUKA A MAXIMÁLNE VÝDAVKY

Pretože pre <ORGANIZÁCIU> nebude možné presne určiť, aký objem zdrojov konkrétneho poskytovateľa cloudových služieb bude spotrebovaný v konkrétnom časovom období, v objednávke budú špecifikované pevné cenové jednotkové množstvá jednej objednávkovej riadkovej položky pre „cloudové technológie“.

Každá objednaná jednotka riadkovej položky bude zodpovedať hodnote <1,00 EUR> objednaných cloudových technológií. Prírastkové objednávky budú pravidelne zadávané modifikáciou tejto objednávky v rôznych množstvách, aby bola <ORGANIZÁCIA> flexibilná a mohla si predobjednať rôzne cloudové technológie v „množstve eur“ na základe svojho odhadovaného využitia pre potreby rôzneho trvania. <ORGANIZÁCIA> bude pravidelne predobjednávať množstvá dostatočné na pokrytie odhadovaných nákladov na cloudové technológie, ktoré sa použijú na splnenie rôznych požiadaviek.

Č. položky	Opis	Množstvo	Jednotka	Cena
01	Cloudové technológie CISP	1 000	kus	1 000,00 EUR

MINIMÁLNA OBJEDNÁVKA /PRÍRASTKOVÁ OBJEDNÁVKA

Objednávky budú pravidelne zadávané na rôzne množstvá <10 000> jednotiek riadkových položiek na základe odhadovanej spotreby cloudových technológií zo strany <ORGANIZÁCIE>. Toto usporiadanie poskytne <ORGANIZÁCI> flexibilitu na predobjednanie <10 000> jednotiek „cloudových technológií“, ak je to potrebné na podporu činnosti a na zachovanie konzistentnosti s obchodnými postupmi v oblasti cloud computingu v režime platby poľa spotreby.

Po zadaní prvej objednávky podľa rámcovej dohody bude objednaný počiatočný prírastok <100 000> jednotiek v cene <100,000 EUR>. Minimálny počet celkových jednotiek riadkovej položky, ktoré možno zadať do jednej prírastkovej objednávky s použitím jednej alebo viacerých riadkových položiek, je <x>. Maximálny počet jednotiek, ktoré je možné objednať v rámci objednávky na dodávku, nesmie prekročiť <x>, ale v kombinácii so všetkými predchádzajúcimi objednanými jednotkami nesmie nikdy prekročiť hodnotu objednávky podľa rámcovej dohody. <ORGANIZÁCIA> bude zodpovedná za to, aby boli všetky objednávky v rámci limitov špecifikovaných v tejto časti.

MAXIMÁLNA OBJEDNÁVKA

Celková maximálna hodnota objednávky je <x> pozostávajúca z maximálne <x> jednotiek jednej riadkovej položky s cenou <x> za jednotku. Táto hodnota je založená na odhade požiadaviek <ORGANIZÁCIE> počas obdobia plnenia, ale nie je zaručená.

3.3 Oboznámte sa s obchodným modelom partnerov

Subjekty verejného sektora by sa mali usilovať porozumieť modelom, podľa ktorých CISP poskytujú svoje ponuky, a mali by si uvedomiť, že partneri poskytujúci poradenstvo, spravované služby, ďalší predaj a mnohé ďalšie služby sú pre tento proces rozhodujúci. Mnoho zákazníkov potrebuje pre svoju infraštruktúru poskytovateľa cloudu, pričom na odborné plánovanie, migráciu a správu si externe najímajú systémového integrátora (SI) alebo poskytovateľa spravovaných služieb. Z tejto kombinácie „služieb“ môžu vyplývať požiadavky, ktoré sa nevzťahujú na poskytovateľov cloudu, napríklad ustanovenia o postúpení smerom k subdodávateľom.

Vezmime si takéto ustanovenia o postúpení na ilustráciu toho, prečo je dôležité pochopiť, ako partneri a sprostredkovatelia fungujú vo vzťahu k CISP. V niektorých typoch obstarávania existujú doložky, ktoré od hlavného dodávateľa vyžadujú, aby k určitým povinným ustanoveniam zaviazal všetkých svojich partnerov/subdodávateľov. CISP zvyčajne nebudú poskytovať ani ponúkať návrhy ako formálni subdodávatelia, pretože ponúkajú štandardizovanú službu v obrovskom rozsahu, ktorá nie je prispôbená jedinečným požiadavkám konkrétneho koncového zákazníka (vrátane potrieb zákazníka z verejného sektora na základe zmluvy o verejnom sektore). V modeli nepriameho obstarávania (obstarávanie cloudových služieb prostredníctvom predajcu CISP) môže CISP tieto ustanovenia od svojho sprostredkovateľa odmietnuť, pretože sa nevzťahujú na dodávateľa komerčných služieb „2. úrovne“. V takom prípade CISP sám neplní rozsah práce podľa zmluvy. Plní ju skôr partner CISP, ktorý na to používa infraštruktúru CISP. CISP je teda komerčným dodávateľom (nie subdodávateľom) operácií partnera. V modeli priameho obstarávania (nákup cloudových služieb priamo od CISP) by CISP zvyčajne tieto „povinné“ ustanovenia vhodné pre bežného subdodávateľa komodít odmietol z dôvodu komerčnej povahy zmluvných služieb a skutočnosti, že väčšina CISP nepotrebuje subdodávateľov na poskytovanie svojich obchodných služieb.

3.4 Cloudoví makléri

Koncept cloudového makléra ako prostriedku na obmedzenie potenciálneho uzamknutia dodávateľa (vendor lock-in) môže byť problematický. Hoci cloudový maklére môže byť teoreticky dobrý nápad, v praxi by pravdepodobne veci viac skomplikoval a zamotal, než by priniesol skutočnú hodnotu.

Úsilie navrhnuť aplikácie tak, aby fungovali vo viacerých cloudoch súčasne alebo zameniteľne, nevyhnutne vedie ku kompromisom v schopnostiach (**cloud nemá žiadnu Rosettskú dosku**). Tento prístup môže v konečnom dôsledku pridať len zbytočnú vrstvu zložitosti medzi zákazníkov z verejného sektora a ich cloudové služby, čo môže ohroziť efektívnosť a výhody v oblasti bezpečnosti, ktoré sa snaží dosiahnuť – čo následne vedie k obmedzenej možnosti škálovateľnosti a agility, zvýšeným nákladom a spomaleniu inovácií.

3.5 Zabezpečovanie zdrojov/prieskum trhu pred vydaním RFP

Počas toho, ako subjekt verejného sektora plánuje RFP na cloudové služby, mal by do procesu od samého začiatku zapojiť zainteresované strany zo všetkých aspektov organizácie, t. j. vrcholové vedenie, obchodných partnerov, technické oddelenie, finančné oddelenie, obstarávanie, právne oddelenie a tím zodpovedný za zmluvy. Vďaka tomuto prístupu budú všetky zainteresované strany rozumieť cloudovému modelu a následne budú informovane pristupovať k prehodnocovaniu tradičných metód obstarávania IT.

Pokiaľ ide o dialóg s partnermi v odvetví, dôrazne odporúčame subjektom verejného sektora, aby si našli čas na podrobný dialóg s cieľom získať spätnú väzbu – od CISP, partnerov CISP, dodávateľov na marketplace s PaaS/SaaS a odborníkov. Takýto dialóg môže mať, napríklad, formu odborných dní alebo workshopov o bezpečnosti a obstarávaní. Ďalším efektívnym spôsobom, ako podrobne pochopiť proces obstarávania cloudu, je vydať RFI prípadne ideálne návrh dokumentu RFP. Často sa potom odhalia potenciálne problémy, ktoré možno identifikovať, prediskutovať a upraviť pred vydaním konečnej RFP na cloudové služby.

3.6 Trvalá udržateľnosť

Trvalá udržateľnosť je súčasťou cloud computingu a prechod na cloud zvyšuje energetickú účinnosť v porovnaní s lokálnymi servermi alebo podnikovými dátovými centrami. Identifikácia CISP, ktorý uprednostňuje trvalú udržateľnosť a prijal verejné záväzky na dosiahnutie cieľov udržateľnosti, je ďalšou zárukou toho, že je cloud udržateľný. Európski CISP a prevádzkovatelia dátových centier (s podporou Európskej komisie) vypracovali pakt o klimaticky neutrálnych dátových centrách¹¹, samoregulačnú iniciatívu, ktorá stanovuje jasné, jednoduché a ďalekosiahle kritériá udržateľnosti pre odvetvie dátových centier. Cieľom je zabezpečiť, aby boli prevádzkovatelia dátových centier a poskytovatelia cloudových služieb klimaticky neutrálni do roku 2030. Táto samoregulačná iniciatíva uvádza jasné ciele v oblasti energetickej účinnosti dátových centier, úspory vody, opätovného použitia a opravy serverov a využívania bezuhlíkovej energie na napájanie dátových centier. CISP, ktorí sa zapoja do samoregulačnej iniciatívy, súhlasia so splnením týchto cieľov a zaväzujú sa dodržiavať stanovené kritériá, aby mohli byť považovaní za klimaticky neutrálnych prevádzkovateľov.

V RFP na cloudové služby by mala byť otázka, či sa CISP zaviazali dodržiavať takéto kritériá, a konkrétne, či sa zapojili do samoregulácie a kedy takýto záväzok prijali.

¹¹ <https://www.climateutraldatacentre.net/self-regulatory-initiative/>

Vzorové znenie RFP: Trvalá udržateľnosť

Zaviazali ste sa prevádzkovať klimaticky neutrálne dátové centrá podpísaním iniciatívy Climate Neutral Data Center Self-Regulatory Initiative? Ak áno, kedy ste ju podpísali?

Môžete poskytnúť dôkaz o tom, že máte oprávnenie používať znak signatára paktu o klimaticky neutrálnych dátových centrách?

Príloha A – Technické požiadavky na porovnanie medzi účastníkmi výberového konania

Nižšie uvádzame niektoré požiadavky na generické cloudové technológie, ktoré by sa mohli použiť na porovnávanie CISP počas objednávok dohodnutých v rámcovej dohode alebo minisúťaží podľa rámcovej dohody o poskytovaní cloudových služieb.

1. Profil poskytovateľa cloudových služieb

	Požiadavka
1.	TRHOVÉ SKÚSENOSTI: <i>Koľko rokov pôsobí poskytovateľ cloudových služieb v cloudovom trhovom segmente?</i>
2.	OTVORENOSŤ A OCHRANA ÚDAJOV: <i>Dodržiava poskytovateľ cloudových služieb ochranu údajov alebo obojstranných priemyselných kódexov správania?</i> <i>Dodržiava poskytovateľ cloudových služieb zásady vývoja open source a open API?</i>

2. Globálna infraštruktúra

	Požiadavka
1.	GLOBÁLNY DOSAH: <i>Ponúka poskytovateľ cloudových služieb globálnu infraštruktúru, aby pomohol používateľom dosiahnuť nízke oneskorenie a vysokú priepustnosť?</i>
2.	REGIÓNŮ: <i>Je poskytovateľ cloudových služieb regionálne prítomný v požadovaných geografických oblastiach?</i>
3.	DOMÉNY/ZÓNY: <i>Realizuje poskytovateľ cloudových služieb koncepciu domén alebo zón, v ktorých sú zoskupené dátové centrá prostredníctvom siete s nízkym oneskorením, aby sa poskytol vyšší stupeň vysokej dostupnosti a tolerance chýb?</i> • Ak áno, uveďte počet domén alebo zón a počet dátových centier v rámci požadovanej geografickej oblasti.
4.	VZDIALENOSŤ DOMÉN/ZÓN: <i>Vytvára poskytovateľ cloudových služieb svoje domény alebo zóny s dátovými centrami, ktoré sa fyzicky nachádzajú oddelene na podporu zálohovania, vysokej dostupnosti a nízkeho oneskorenia?</i>
5.	VYBUDOVANÉ DÁTOVÉ CENTRÁ: <i>Ponúka poskytovateľ cloudových služieb dátové centrá navrhnuté tak, aby boli izolované od zlyhaní v iných dátových centrách so záložným napájaním, chladením a prepojením do siete?</i>
6.	REPLIKÁCIA DÁTOVÉHO CENTRA: <i>Ponúka poskytovateľ cloudových služieb replikáciu údajov naprieč dátovými centrami v rámci domény alebo zóny s automatickým zabezpečením pred zlyhaním?</i>
7.	REPLIKÁCIA DOMÉNY/ZÓNY: <i>Ponúka poskytovateľ cloudových služieb replikáciu údajov naprieč doménami alebo zónami v rámci regiónu?</i>

3. Infraštruktúra

3.1 Výpočet

	Požiadavka
1.	POČÍTAČ – PRAVIDELNÁ INŠTANCIA – VŠEOBECNÝ ÚČEL: Ponúka poskytovateľ cloudových služieb tieto typy inštancií? - Všeobecný účel – optimalizovaný pre generické aplikácie a poskytuje vyváženosť výpočtu, pamäti a zdrojov siete. - Ak áno, aká je najväčšia inštancia?
2.	POČÍTAČ – PRAVIDELNÁ INŠTANCIA – PAMÄŤOVO OPTIMALIZOVANÝ: Ponúka poskytovateľ cloudových služieb tieto typy inštancií? - Pamäťovo optimalizované – optimalizované pre aplikácie náročné na pamäť - Ak áno, aká je najväčšia inštancia?
3.	POČÍTAČ – PRAVIDELNÁ INŠTANCIA – VÝPOČTOVO OPTIMALIZOVANÝ: Ponúka poskytovateľ cloudových služieb tieto typy inštancií? - Výpočtovo optimalizované – optimalizované pre aplikácie náročné na výpočet - Ak áno, aká je najväčšia inštancia?
4.	POČÍTAČ – PRAVIDELNÁ INŠTANCIA – OPTIMALIZOVANÁ NA UCHOVÁVANIE V PAMÄTI: Ponúka poskytovateľ cloudových služieb tieto typy inštancií? - Optimalizované na uchovávanie v pamäti – ponúka veľké množstvo lokálnej úložnej kapacity. - Ak áno, aká je maximálna úložná kapacita (napr. 5, 10, 20, 50 TB) a maximálny počet diskov (HDD/SSD), ktoré môžu byť poskytnuté a pripojené k inštancii?
5.	POČÍTAČ – PRAVIDELNÁ INŠTANCIA – GRAFICKY OPTIMALIZOVANÁ: Ponúka poskytovateľ cloudových služieb tieto typy inštancií? - Nízkonákladová grafika – ponúka zrýchlenie nízkonákladovej grafiky na výpočet inštancií? - Ak áno, aká je najväčšia inštancia?
6.	POČÍTAČ – PRAVIDELNÁ INŠTANCIA – GPU OPTIMALIZOVANÁ: Ponúka poskytovateľ cloudových služieb tieto typy inštancií? - GPU – ponúka hardvérové jednotky grafického spracovania (GPU) pre graficky náročné aplikácie. - Ak áno, koľko GPU a aké modely GPU je poskytovateľ cloudových služieb schopný ponúkať na inštanciu?
7.	POČÍTAČ – PRAVIDELNÁ INŠTANCIA – FPGA OPTIMALIZOVANÝ: Ponúka poskytovateľ cloudových služieb tieto typy inštancií? - FPGA – ponúka polia logických členov programovateľné užívateľom (FPGA) na vývoj a využívanie zrýchlenia špeciálneho hardvéru pre aplikácie. - Ak áno, koľko FPGA je poskytovateľ cloudových služieb schopný ponúkať na inštanciu?
8.	POČÍTAČ – PREKONATELNÁ INŠTANCIA: Ponúka poskytovateľ cloudových služieb prekonateľné inštalácie, ktoré poskytujú základnú úroveň výkonu centrálnej procesorovej jednotky (CPU) so schopnosťou prekonať základnú hodnotu? Ak áno, aká je najväčšia prekonateľná inštancia?

9.	POČÍTAČ – IO NÁROČNÁ INŠTANCIA: Ponúka poskytovateľ cloudových služieb inštalácie ktoré používajú mechaniky s nepohyblivým médiom (SSD) energeticky nezávislej pamäti (NVMe) optimalizované pre nízke oneskorenie, veľmi vysoký náhodný I/O výkon a vysokú sekvenčnú priepustnosť čítania? • Ak áno, aká je maximálna kapacita vstupných/výstupných operácií za sekundu najväčšej inštalácie?
10.	POČÍTAČ – DOČASNÉ MIESTNE ÚLOŽISKO: Podporuje poskytovateľ cloudových služieb lokálne úložisko výpočtových inšancií, aby sa použili na dočasné uloženie informácií, ktoré sa často menia?
11.	POČÍTAČ – PODPORA VIACNÁSOBNÝCH SIEŤOVÝCH KARIET (NIC): Podporuje poskytovateľ cloudových služieb viacnásobné (primárne a doplnkové) karty sieťových rozhraní (NIC), ktoré majú byť pridelené pre danú inštaláciu? • Ak áno, aký je maximálny počet NIC na inštaláciu?
12.	POČÍTAČ – AFINITA INŠTANCIÍ: Ponúka poskytovateľ cloudových služieb používateľom schopnosť logicky zoskupiť inštalácie dohromady v rámci toho istého dátového centra?
13.	POČÍTAČ – ANTIAFINITA INŠTANCIÍ: Ponúka poskytovateľ cloudových služieb používateľom schopnosť logicky zoskupiť inštalácie a umiestniť ich v rôznych dátových centrách v rámci regiónu?
14.	POČÍTAČ – SAMOOSLUŽNÉ POSKYTOVANIE: Ponúka poskytovateľ cloudových služieb samoobslužné poskytovanie viacerých inšancií súčasne cez programové rozhranie, riadiacu konzolu alebo webový portál?
15.	POČÍTAČ – PRISPÔSOBENIE POTREBÁM POUŽÍVATEĽA: Ponúka poskytovateľ cloudových služieb inštalácie prispôsobiteľné potrebám používateľa, t. j. schopnosť meniť konfiguráciu nastavení, napríklad virtuálne centrálné procesorové jednotky (vCPU) a pamäť s priamym prístupom (RAM)?
16.	POČÍTAČ – NÁJOM: Ponúka poskytovateľ cloudových služieb inštalácie jedného nájomníka, ktoré bežia na hardvéri vyhradenom pre jedného používateľa? • Ak áno, aká je najväčšia dostupná inštalácia jedného nájomníka?
17.	POČÍTAČ – PODOBNOSŤ HOSTITEĽA: Ponúka poskytovateľ cloudových služieb schopnosť spustiť inštaláciu a špecifikovať, že táto inštalácia sa vždy reštartuje na tom istom fyzickom hostiteľovi?
18.	POČÍTAČ – ANTIAFINITA HOSTITEĽA: Ponúka poskytovateľ cloudových služieb schopnosť rozdelenia a hostovania pre konkrétne inštalácie v rámci rôznych fyzických hostiteľov?
19.	POČÍTAČ – AUTOMATICKÉ ŠKÁLOVANIE: Ponúka poskytovateľ cloudových služieb schopnosť automaticky zvyšovať počet inšancií počas nárastov dopytu, aby sa udržiaval výkon (t. j. „škálovanie“)?
20.	POČÍTAČ – MECHANIZMUS IMPORTOVANIA OBRÁZKOV: Ponúka poskytovateľ cloudových služieb používateľom schopnosť importovať ich existujúce obrázky a uložiť ich ako nové, súkromne dostupné obrázky, ktoré sa potom môžu použiť na poskytovanie inšancií v budúcnosti? • Ak áno, aké formáty sú podporované?

21.	POČÍTAČ – MECHANIZMUS EXPORTOVANIA OBRÁZKOV: Podporuje poskytovateľ cloudových služieb schopnosť vziať existujúcu bežiacu inštanciu alebo kópiu inštancie a exportovať inštanciu do virtuálneho strojového formátu? • Ak áno, aké formáty sú podporované?
22.	POČÍTAČ – PRERUŠENIE SLUŽBY: Ponúka poskytovateľ cloudových služieb mechanizmy na zabránenie výpadkom alebo odstávkam inštancií, keď poskytovateľ vykonáva akýkoľvek druh údržby hardvéru alebo služby na úrovni hostiteľa?
23.	POČÍTAČ – REŠTARTOVANIE INŠTANCIÍ: Ponúka poskytovateľ cloudových služieb mechanizmy na automatické reštartovanie inštancií na zdravom hostiteľskom počítači, ak pôvodný fyzický hostiteľský počítač zlyhá?
24.	POČÍTAČ – OZNÁMENIA: V prípade udalosti týkajúcej sa odolnosti počítača, má poskytovateľ cloudových služieb schopnosť oznámiť používateľovi, že takáto udalosť nastala, a je používateľ schopný prijať alebo neprijať túto komunikáciu cez samoobslužné prostriedky?
25.	POČÍTAČ – NAPLÁNOVANIE UDALOSTI: Ponúka poskytovateľ cloudových služieb schopnosť naplánovať udalosti pre inštancie používateľa, napríklad naštartovanie, zastavenie, spustenie alebo vyradenie inštancie?
26.	POČÍTAČ – MECHANIZMUS ZÁLOHOVANIA A OBNOVY: Ponúka poskytovateľ cloudových služieb integrovaný mechanizmus zálohovania a obnovenia?
27.	POČÍTAČ – MECHANIZMUS SNÍMKY OBRAZOVKY: Ponúka poskytovateľ cloudových služieb návod pre mechanizmus snímky obrazovky na požiadanie?
28.	POČÍTAČ – METADÁTA: Ponúka poskytovateľ cloudových služieb službu metadát inštancie, ktorá používateľom umožňuje ľubovoľne nastaviť páry kľúčových hodnôt pre inštanciu?
29.	POČÍTAČ – VYVOLANIE METADÁT: Ponúka poskytovateľ cloudových služieb službu metadát inštancie, ktorá poskytuje aplikačné programovacie rozhranie (API), ktoré môže inštancia vyvolať, aby sa našli informácie o nej samotnej?
30.	POČÍTAČ – MECHANIZMUS PONÚKANIA: Ponúka poskytovateľ cloudových služieb mechanizmus na ponúkание nízkonákladových inštancií, ktoré môžu byť okamžite konkretizované, aby hostili kritické pracovné zaťaženia bez úloh?
31.	POČÍTAČ – MECHANIZMUS PLÁNOVANIA: Ponúka poskytovateľ cloudových služieb spôsob plánovania a rezervovania dodatočnej počítačovej kapacity na opakujúcom sa základe, t. j. denný, týždenný, mesačný harmonogram?
32.	POČÍTAČ – MECHANIZMUS REZERVÁCIE: Ponúka poskytovateľ cloudových služieb spôsob rezervovania dodatočnej počítačovej kapacity pre budúcnosť (t. j. 1 rok, 2 roky, 3 roky atď.)?
33.	POČÍTAČ – OPERAČNÝ SYSTÉM LINUX: Podporuje poskytovateľ cloudových služieb posledné dve dlhodobé podporované verzie aspoň jednej distribučnej spoločnosti Linux (napríklad Red Hat, SUSE) a jednej bežne používanej distribúcie (napríklad Ubuntu, CentOS a Debian)?
34.	POČÍTAČ – OPERAČNÝ SYSTÉM WINDOWS: Podporuje poskytovateľ cloudových služieb posledné dve hlavné verzie servera Windows (Windows Server 2017 a Windows Server 2016)?

35.	POČÍTAČ – PRENOSNOSŤ LICENCOVANIA: Ponúka poskytovateľ cloudových služieb prenosnosť a podporu licencie? • Ak áno, uveďte dodávateľa softvéru, názvy softvéru, vydania a ich verzie.
36.	POČÍTAČ – LIMITY SLUŽBY: Má poskytovateľ cloudových služieb nejaké obmedzenia (t. j. limity služby) s ohľadom na vyššie uvedenú počítačovú sekciu? Príklad: Maximálny počet inštancií na účet Maximálny počet vyhradených hostiteľských počítačov na účet Maximálny počet vyhradených adries internetových protokolov (IP)

3.2 Vytváranie siete

	Požiadavka
1.	VYTVÁRANIE SIETE – VIRTUÁLNE SIETE: Podporuje poskytovateľ cloudových služieb schopnosť vytvárať logickú, izolovanú virtuálnu sieť, ktorá reprezentuje vlastnú sieť spoločnosti v cloude?
2.	VYTVÁRANIE SIETE – PREPOJENOSŤ ROVNAKÝCH REGIÓNOV: Podporuje poskytovateľ cloudových služieb prepojenie dvoch virtuálnych sietí v rámci toho istého regiónu, aby sa nasmerovala prevádzka medzi nimi pomocou súkromných adries internetového protokolu (IP)?
3.	VYTVÁRANIE SIETE – PREPOJENOSŤ RÔZNYCH SIETÍ: Podporuje poskytovateľ cloudových služieb prepojenie dvoch virtuálnych sietí medzi rôznymi regiónmi, aby sa nasmerovala prevádzka medzi nimi pomocou súkromných adries internetového protokolu (IP)?
4.	VYTVÁRANIE SIETE – SÚKROMNÁ PODSIEŤ: Ponúka poskytovateľ cloudových služieb schopnosť vytvárať úplne izolované (súkromné) virtuálne siete a podsiete, kde sa môžu inštancie obstarávať bez adresy verejného internetového protokolu (IP) alebo smerovania internetu?
5.	VYTVÁRANIE SIETE – ROZSAH ADRIES VIRTUÁLNEJ SIETE: Podporuje poskytovateľ cloudových služieb rozsahy adries internetového protokolu (IP) špecifikované v žiadosti a komentáre (RFC) 1918, ako aj bloky verejne smerovateľného beztriedneho interdoménového smerovania (CIDR)?
6.	VYTVÁRANIE SIETE – VIACNÁSOBNÉ PROTOKOLY: Podporuje poskytovateľ cloudových služieb viacnásobné protokoly vrátane protokolu riadenia prenosu (TCP), používateľského datagramového protokolu (UDP) a protokolu (CMP)?
7.	VYTVÁRANIE SIETE – AUTOMATICKÉ PRIRAĐOVANIE PRE IP ADRESY: Podporuje poskytovateľ cloudových služieb schopnosť automaticky priraďovať verejné adresy internetového protokolu (IP) k inštanciám?
8.	VYTVÁRANIE SIETE – REZERVOVANÉ STATICKÉ IP ADRESY: Podporuje poskytovateľ cloudových služieb adresy internetových protokolov (IP) s účtom používateľa, nie konkrétnu inštanciu? IP adresa musí zostať združená s účtom, pokiaľ nie je výslovne uvoľnená.
9.	VYTVÁRANIE SIETE – PODPORA IPV6: Podporuje poskytovateľ cloudových služieb internetový protokol verziu 6 (IPv6) buď na vstupnej bráne alebo na úrovni inštancie a umožnenie tejto funkčnosti používateľom?

10.	VYTVÁRANIE SIETE – VIACNÁSOBNÉ IP ADRESY NA JEDNU NIC: <i>Podporuje poskytovateľ cloudových služieb schopnosť priradiť primárnu a sekundárnu adresu internetového protokolu (IP) karte sieťového rozhrania (NIC), ktorá je pripojená k danej inštancii?</i>
11.	VYTVÁRANIE SIETE – VIACNÁSOBNÉ NIC: <i>Podporuje poskytovateľ cloudových služieb schopnosť priradiť viacnásobné karty sieťového rozhrania (NIC) k danej inštancii?</i>
12.	VYTVÁRANIE SIETE – NIC A IP MOBILITA: <i>Podporuje poskytovateľ cloudových služieb schopnosť presúvať karty sieťového rozhrania (NIC), ako aj adresy internetových protokolov (IP) medzi inštanciami?</i>
13.	VYTVÁRANIE SIETE – PODPORA SR-IOV: <i>Podporuje poskytovateľ také schopnosti, ako virtualizácia vstupu/výstupu s jedným koreňom (SR-IOV) pre vyšší výkon (t. j. pakety za sekundu - PPS), menšie oneskorenie a nižšiu časovú nestabilitu?</i>
14.	VYTVÁRANIE SIETE – FILTROVANIE VSTUPU: <i>Podporuje poskytovateľ cloudových služieb pridávanie alebo odoberanie pravidiel uplatniteľných na prichádzajúcu prevádzku (vstup) pre inštancie?</i>
15.	VYTVÁRANIE SIETE – FILTROVANIE VÝSTUPU: <i>Podporuje poskytovateľ cloudových služieb pridávanie alebo odoberanie pravidiel uplatniteľných na odchádzajúcu prevádzku (výstup) pochádzajúcu z inštancii?</i>
16.	VYTVÁRANIE SIETE – ACL: <i>Ponúka poskytovateľ cloudových služieb kontrolné zoznamy prístupu (ACL) na kontrolu prichádzajúcej a odchádzajúcej prevádzky do podsietí?</i>
17.	VYTVÁRANIE SIETE – PODPORA ZÁZNAMU TOKU: <i>Ponúka poskytovateľ cloudových služieb schopnosť zachytenia záznamov prevádzkového toku siete?</i>
18.	VYTVÁRANIE SIETE – NAT: <i>Poskytuje poskytovateľ cloudových služieb službu prekladu sieťovej adresy riadenú vstupnou bránou (NAT), aby umožnil inštanciam v súkromnej sieti pripojiť sa k internetu alebo k iným cloudovým službám, ale zabránil, aby internet inicializoval pripojenie k týmto inštanciam?</i>
19.	VYTVÁRANIE SIETE – KONTROLA ZDROJA/MIESTA URČENIA: <i>Má poskytovateľ cloudových služieb schopnosť vypnúť kontrolu zdroja/miesta určenia na kartách sieťového rozhrania (NIC)?</i>
20.	VYTVÁRANIE SIETE – PODPORA VPN: <i>Podporuje poskytovateľ cloudových služieb prepojenie virtuálnej súkromnej siete (VPN) medzi poskytovateľom cloudových služieb a dátovým centrom používateľa?</i>
21.	VYTVÁRANIE SIETE – TUNELY VPN: <i>Podporuje poskytovateľ cloudových služieb viacnásobné pripojenia virtuálnej súkromnej siete (VPN) na virtuálnu sieť?</i>
22.	VYTVÁRANIE SIETE – PODPORA IPSEC VPN: <i>Umožňuje poskytovateľ cloudových služieb používateľom prístup ku cloudovým službám buď cez tunel virtuálnej súkromnej siete (VPN) zabezpečený internetovým protokolom (IPsec), alebo vrstvou zabezpečených socketov (SSL) tunela virtuálnej súkromnej siete (VPN) cez verejný internet?</i>
23.	VYTVÁRANIE SIETE – PODPORA BGP: <i>Využíva poskytovateľ cloudových služieb protokol hraničnej vstupnej brány (BGP) na zlepšenie zabezpečenia pred zlyhaním cez internetový bezpečnostný protokol (IPsec) tunelov virtuálnej súkromnej siete (VPN)?</i>

24.	VYTVÁRANIE SIETE – SÚKROMNÉ VYHRADENÉ PREPOJENIE: <i>Ponúka poskytovateľ cloudových služieb službu priameho súkromného prepojenia medzi lokalitami poskytovateľa cloudových služieb a dátovým centrom používateľa, kanceláriou alebo spoločným umiestnením, ktoré umožňuje veľké a rýchle prenosy údajov?</i>
25.	VYTVÁRANIE SIETE – KLIENTSKY VYROVNÁVAČ ZAŤAŽENIA: <i>Ponúka poskytovateľ cloudových služieb službu klientskeho vyrovnávania zaťaženia (smerom k internetu), ktorá preberá žiadosti od klientov cez internet a rozdeľuje tieto žiadosti medzi inštancie, ktoré sú zaregistrované vyrovnávačom zaťaženia?</i>
26.	VYTVÁRANIE SIETE – SERVEROVÝ VYROVNÁVAČ ZAŤAŽENIA: <i>Ponúka poskytovateľ cloudových služieb službu serverového vyrovnávania zaťaženia (súkromného), ktorá smeruje prevádzku k inštanciám nachádzajúcim sa na súkromnej podsieti?</i>
27.	VYTVÁRANIE SIETE – VYROVNÁVAČ ZAŤAŽENIA VRSTVY 7: <i>Ponúka poskytovateľ cloudových služieb službu vyrovnávača zaťaženia vrstvy 7 (hypertextový protokol prenosu - HTTP) schopný vyrovnávať záťaž prevádzky siete pre viacero inšancií?</i>
28.	VYTVÁRANIE SIETE – VYROVNÁVAČ ZAŤAŽENIA VRSTVY 4: <i>Ponúka poskytovateľ cloudových služieb službu vyrovnávača zaťaženia vrstvy 4 (protokol riadenia prenosu - TCP) schopnú vyrovnávať záťaž prevádzky siete pre viacero inšancií?</i>
29.	VYTVÁRANIE SIETE – AFINITA RELÁCIE PRE VYROVNÁVAČE ZAŤAŽENIA: <i>Ponúka poskytovateľ cloudových služieb službu vyrovnávania zaťaženia, ktorá podporuje afinitu relácie?</i>
30.	VYTVÁRANIE SIETE – VYROVNÁVANIE ZAŤAŽENIA ZALOŽENÉ NA DNS: <i>Ponúka poskytovateľ cloudových služieb službu vyrovnávania zaťaženia schopnej vyrovnávať záťaž prevádzky pre inštancie hostené vo viacerých hostiteľských počítačoch, ktoré patria jednej doméne?</i>
31.	VYTVÁRANIE SIETE – ZÁZNAMY VYROVNÁVAČA ZAŤAŽENIA: <i>Poskytuje poskytovateľ cloudových služieb záznamy, ktoré zachytávajú podrobné informácie o všetkých žiadostiach zaslaných do vyrovnávača zaťaženia?</i>
32.	VYTVÁRANIE SIETE – DNS: <i>Ponúka poskytovateľ cloudových služieb službu vysoko dostupného a škálovateľného systému názvov domén (DNS)?</i>
33.	VYTVÁRANIE SIETE – SMEROVANIE DNS ZALOŽENÉ NA ONESKORENÍ: <i>Ponúka poskytovateľ cloudových služieb službu systému názvov domén (DNS), ktorá podporuje smerovanie založené na oneskorení (t. j. služba DNS odpovedá na otázky DNS so zdrojmi, ktoré poskytujú najlepšie oneskorenie)?</i>
34.	VYTVÁRANIE SIETE – SMEROVANIE DNS ZALOŽENÉ NA GEOGRAFIU: <i>Ponúka poskytovateľ cloudových služieb službu systému názvov domén (DNS), ktorá podporuje smerovanie založené na geografii (t. j. služba DNS odpovedá na otázky DNS založené na geografickom umiestnení používateľov)?</i>
35.	VYTVÁRANIE SIETE – SMEROVANIE DNS ZALOŽENÉ NA ZABEZPEČENÍ PRED ZLYHANÍM: <i>Ponúka poskytovateľ cloudových služieb službu systému názvov domén (DNS), ktorá podporuje smerovanie založené na zabezpečení pred zlyhaním (t. j. služba DNS nasmeruje otázky DNS na zdroj, ktorý je aktuálne aktívny, zatiaľ čo druhý zdroj čaká a stane sa aktívnym v prípade zlyhania primárneho zdroja)?</i>
36.	VYTVÁRANIE SIETE – SLUŽBA REGISTRÁCIE DOMÉNY: <i>Ponúka poskytovateľ cloudových služieb služby registrácie názvov domén (t. j. používatelia môžu vyhľadávať a zaregistrovať dostupné názvy domén)?</i>
37.	VYTVÁRANIE SIETE – KONTROLY STAVU DNS: <i>Ponúka poskytovateľ cloudových služieb službu systému názvov domén (DNS), ktorá používa kontroly stavu na monitorovanie stavu a výkonu zdrojov?</i>

38.	VYTVÁRANIE SIETE – INTEGROVANIE DNS A VYROVNÁVAČA ZAŤAŽENIA: <i>Ponúka poskytovateľ cloudových služieb službu systému názvov domén (DNS), ktorá integruje vyrovnávače zaťaženia poskytovateľa cloudových služieb?</i>
39.	VYTVÁRANIE SIETE – VIZUÁLNY EDITOR: <i>Ponúka poskytovateľ cloudových služieb nástroj, ktorý umožňuje používateľom vytvoriť postupy pre manažment aktivity?</i>
40.	SIEŤ NA DORUČOVANIE OBSAHU (CDN): <i>Ponúka poskytovateľ cloudových služieb službu siete na doručovanie obsahu (CDN) na distribúciu obsahu s malým oneskorením a vysokými rýchlosťami prenosu údajov?</i>
41.	VYTVÁRANIE SIETE – ZÁNÍK VYROVNÁVACEJ PAMÄTE CDN: <i>Ponúka poskytovateľ cloudových služieb službu siete na sprístupňovanie obsahu (CDN), ktorá umožňuje odstrániť objekt z vyrovnávacej pamäti pred jej zánikom vrátane takých vlastností ako je zrušenie platnosti objektov a vyhotovenie ich verzií?</i>
42.	VYTVÁRANIE SIETE – EXTERNÝ PÔVOD CDN: <i>Ponúka poskytovateľ cloudových služieb službu siete na sprístupňovanie obsahu (CDN), ktorá podporuje zákaznícky pôvod, t. j. hypertextový prenosový protokol (HTTP) servera?</i>
43.	VYTVÁRANIE SIETE – OPTIMALIZÁCIA CDN: <i>Ponúka poskytovateľ cloudových služieb službu siete na doručovanie obsahu (CDN) s podrobnou kontrolou pre konfiguráciu serverov rôzneho pôvodu a pamäťové vlastnosti pre rôzne jednotné vyhľadávače zdrojov (URL)?</i>
44.	VYTVÁRANIE SIETE – GEOGRAFICKY OBMEDZENÁ CDN: <i>Ponúka poskytovateľ cloudových služieb službu siete na sprístupňovanie obsahu (CDN), ktorá podporuje geografické obmedzenie, t. j. znemožňuje používateľom prístup k obsahu v konkrétnych geografických oblastiach?</i>
45.	VYTVÁRANIE SIETE – TOKENY CDN: <i>Ponúka poskytovateľ cloudových služieb službu siete na doručovanie obsahu (CDN), ktorá podporuje označené jednotné vyhľadávače zdrojov (URL), ktoré obvykle obsahujú doplnkové informácie, napríklad dátum/čas uplynutia, aby používatelia získali väčšiu kontrolu nad prístupom k ich obsahu?</i>
46.	VYTVÁRANIE SIETE – CERTIFIKÁTY CDN: <i>Ponúka poskytovateľ cloudových služieb službu siete na doručenie obsahu (CDN), ktorá podporuje certifikáty vrstvy zabezpečených socketov (SSL), aby sa obsah bezpečne sprístupnil cez zabezpečený hypertextový prenosový protokol (HTTPS) z okrajových lokalít?</i>
47.	VYTVÁRANIE SIETE – VIACVRSTVOVÁ VYROVNÁVACIA PAMÄŤ: <i>Ponúka poskytovateľ cloudových služieb službu siete na doručenie obsahu (CDN), ktorá využíva prístup viacvrstvovej vyrovnávacej pamäti s použitím regionálnych vyrovnávacích pamätí, aby sa znížilo oneskorenie?</i>
48.	VYTVÁRANIE SIETE – KOMPRESIA CDN: <i>Ponúka poskytovateľ cloudových služieb službu siete na doručenie obsahu (CDN), ktorá podporuje kompresiu súborov?</i>
49.	VYTVÁRANIE SIETE – ZAŠIFROVANÉ NAHRATIA ÚDAJOV CDN: <i>Ponúka poskytovateľ cloudových služieb sieť na doručenie obsahu (CDN), ktorá umožňuje používateľom nahrávať ich citlivé údaje spôsobom, aby takéto informácie mohli byť prezerané iba určitými komponentmi a službami v pôvodnej infraštruktúre používateľa?</i>
50.	VYTVÁRANIE SIETE – KONCOVÉ BODY: <i>Ponúka služba vytvárania siete poskytovateľa cloudových služieb používateľom s koncovými bodmi schopnými nasmerovať prevádzku cez prepojenosť internej siete (t. j. súkromnú prepojenosť), aby sa znížili náklady na komunikáciu a zlepšila sa bezpečnosť prevádzky?</i>

51.	VYTVÁRANIE SIETE – LIMITY SLUŽBY: Má poskytovateľ cloudových služieb nejaké obmedzenia (t. j. limity služby) s ohľadom na vyššie uvedenú sekciu vytvárania siete? Príklad: Maximálny počet virtuálnych sietí na účet Maximálna veľkosť virtuálnej siete Maximálny počet podsietí na účet Maximálny počet vyrovnávačov zaťaženia na účet Maximálny počet zápisov do kontrolného zoznamu prístupov (ACL) Maximálny počet tunelov virtuálnej súkromnej siete (VPN) Maximálny počet originálov na distribúciu Maximálny počet certifikátov na vyrovnávač zaťaženia
-----	--

3.3 Úložisko

	Požiadavka
1.	SLUŽBA BLOKOVÉHO ÚLOŽISKA: Ponúka poskytovateľ cloudových služieb objemy ukladania na úrovni bloku, aby sa použili s počítačovými inštanciami?
2.	BLOKOVÉ ÚLOŽISKO – IOPS: Ponúka poskytovateľ cloudových služieb možnosť zakúpenia výkonu s jasným cieľom alebo úrovne výkonu s objemami blokového úložiska, napríklad určitý počet vstupných/výstupných operácií za sekundu (IOPS) alebo megabytov za sekundu (MB/s) priepustnosti?
3.	BLOKOVÉ ÚLOŽISKO – MECHANIKY S NEPOHYBLIVÝM MÉDIOM: Podporuje poskytovateľ cloudovej služby mechaniky s nepohyblivým médiom (SSD) média záložného ukladania, ktoré ponúka jednočíslkové milisekundové oneskorenie? Ak áno, aký je maximálny počet SSD, ktorý môže byť pripojený k inštancii?
4.	BLOKOVÉ ÚLOŽISKO – ŠKÁLOVANIE: Ponúka poskytovateľ cloudových služieb používateľom schopnosť zväčšovať veľkosť objemu existujúceho blokového úložiska bez poskytnutia nového objemu a kopírovania/presúvania údajov?
5.	BLOKOVÉ ÚLOŽISKO – SNÍMKY OBRAZOVKY: Má poskytovateľ cloudových služieb schopnosť robiť snímky obrazovky pre službu blokového úložiska?
6.	BLOKOVÉ ÚLOŽISKO – VYMAZANIE ÚDAJOV: Podporuje poskytovateľ cloudových služieb úplné vymazanie údajov, aby takéto údaje neboli čitateľné alebo prístupné pre neoprávnených používateľov a/alebo pre tretie strany?
7.	BLOKOVÉ ÚLOŽISKO – ŠIFROVANIE ULOŽENÝCH ÚDAJOV: Ponúka poskytovateľ cloudových služieb šifrovanie uložených údajov na strane servera pre údaje uložené v objemoch a snímkach? Ak áno, aký šifrovací algoritmus sa používa?

8.	SLUŽBA ULOŽENIA OBJEKTU: <i>Ponúka poskytovateľ cloudových služieb bezpečné, trvanlivé, vysoko škálovateľné uloženie objektov pre ukladanie a vyhľadávanie akéhokoľvek množstva údajov z webu?</i>
9.	ULOŽENIE OBJEKTU – ZRIEDKAVÝ PRÍSTUP: <i>Ponúka poskytovateľ cloudových služieb službu nízkonákladového uloženia zameranú na ukladanie menej navštevovaných objektov a súborov?</i>
10.	ULOŽENIE OBJEKTU – NIŽŠIA TRVANLIVOSŤ: <i>Ponúka poskytovateľ cloudových služieb zníženú úroveň zálohovania, kde používateľ môže ukladať menej významné, ľahko reprodukovateľné objekty za nižšiu cenu?</i>
11.	ULOŽENIE OBJEKTU – MENEJ ČASTÝ PRÍSTUP: <i>Ponúka poskytovateľ cloudových služieb úroveň pre menej časté navštevovanie údajov, ktoré si však ešte stále vyžaduje rýchly prístup?</i>
12.	ULOŽENIE OBJEKTU – OBJEKT USPORIADANÝ V ÚROVNIACH: <i>Ponúka poskytovateľ cloudových služieb schopnosť rozvrstvenia uloženia objektu, t. j. schopnosť odporúčať prechod objektu medzi triedami alebo úrovňami uloženia objektu na základe frekvencie prístupu?</i>
13.	ULOŽENIE OBJEKTU – RIADENIE ŽIVOTNÉHO CYKLU: <i>Podporuje poskytovateľ cloudových služieb riadenie životného cyklu objektu pomocou konfigurácie životného cyklu, ktorá definuje, ako sú objekty riadené počas životného cyklu, od vytvorenia po vymazanie?</i>
14.	ULOŽENIE OBJEKTU – RIADENIE USMERŇOVANÉ POSTUPOM: <i>Ponúka poskytovateľ cloudových služieb schopnosť vytvárať a používať postupy na riadenie uložených údajov, ich životného cyklu a nastavení ich rozvrstvenia?</i>
15.	ULOŽENIE OBJEKTU – UMIESTNENIE A POSTUPY ZALOŽENÉ NA ČASE: <i>Ponúka poskytovateľ cloudových služieb schopnosť vytvárať postupy, ktoré môžu obmedziť prístup k údajom na základe umiestnenia používateľa a času žiadosti?</i>
16.	ULOŽENIE OBJEKTU – HOSŤOVANIE WEBOVEJ STRÁNKY: <i>Podporuje poskytovateľ cloudových služieb hostenie statických webových sídiel mimo služby uloženia objektu?</i>
17.	ULOŽENIE OBJEKTU – ŠIFROVANIE ULOŽENÝCH ÚDAJOV: <i>Podporuje poskytovateľ cloudových služieb šifrovanie uložených údajov v pokoji na strane servera (SSE), keď poskytovateľ cloudových služieb spravuje šifrovacie kľúče?</i> • Ak áno, aký šifrovací algoritmus sa používa?
18.	ULOŽENIE OBJEKTU – ŠIFROVANIE S KĹÚČMI POUŽÍVATEĽA: <i>Ponúka poskytovateľ cloudových služieb schopnosť šifrovania na strane servera (SSE) pomocou šifrovacích kľúčov poskytnutých zákazníkom?</i>
19.	ULOŽENIE OBJEKTU – SLUŽBA RIADENÁ KĹÚČOM: <i>Podporuje poskytovateľ cloudových služieb šifrovanie na strane servera (SSE) pomocou služby riadenia kľúča, ktorá vytvára šifrovacie kľúče, definuje postupy, ktoré kontrolujú, ako sa kľúče môžu používať, a audituje používanie kľúčov, aby preukázala, že sa správne používajú?</i>
20.	ULOŽENIE OBJEKTU – HLAVNÝ KĹÚČ NA STRANE KLIENTA: <i>Ponúka poskytovateľ cloudových služieb používateľom možnosť ponechania kontroly nad šifrovacími kľúčmi a dokončenia šifrovania/rozšifrovania objektov na strane klienta?</i>
21.	ULOŽENIE OBJEKTU – SILNÁ KONZISTENCIA: <i>Podporuje poskytovateľ cloudových služieb konzistenciu čítania po zápise pre operácie PUT pre nové objekty?</i>

22.	ULOŽENIE OBJEKTU – UMIESTNENIE ÚDAJOV: <i>Ponúka poskytovateľ cloudových služieb silnú regionálnu izoláciu takže objekty uložené v regióne nikdy región neopustia, pokiaľ ich používateľ výslovne neprenesie do iného regiónu?</i>
23.	ULOŽENIE OBJEKTU – KOPÍROVANIE: <i>Ponúka poskytovateľ cloudových služieb funkciu kopírovania medzi regiónmi, ktorá bude automaticky kopírovať objekty medzi regiónmi vybranými používateľom?</i>
24.	ULOŽENIE OBJEKTU – UVÁDZANIE VERZIÍ: <i>Podporuje poskytovateľ cloudových služieb uvádzanie verzií, t. j. schopnosť ukladať a uchovávať viacero verzií objektu?</i>
25.	ULOŽENIE OBJEKTU – OZNAČENIE NEVYMAZÁVANIA: <i>Umožňuje poskytovateľ cloudových služieb používateľovi označiť nejakú položku ako nevymazateľnú?</i>
26.	ULOŽENIE OBJEKTU – VYMAZANIE MFA: <i>Podporuje poskytovateľ cloudových služieb overovanie viacerých faktorov pre postupy vymazania (MFA) ako doplnkovú bezpečnostnú možnosť?</i>
27.	ULOŽENIE OBJEKTU – ODOSIELANIE VO VIACERÝCH ČASTIACH: <i>Umožňuje poskytovateľ cloudových služieb nahratie objektu ako súboru častí, kde každá časť je súvislou časťou údajov objektu a tieto časti objektov môžu byť nahraté nezávisle a v akomkoľvek poradí?</i>
28.	ULOŽENIE OBJEKTU – TAGY: <i>Ponúka poskytovateľ cloudových služieb schopnosť vytvoriť a združiť premenlivé, dynamické tagy na úrovni objektu?</i>
29.	ULOŽENIE OBJEKTU – OZNÁMENIA: <i>Ponúka poskytovateľ cloudových služieb schopnosť posilať oznámenia, keď nastanú určité udalosti na úrovni objektu (t. j. postupy pridávania/vymazania)?</i>
30.	ULOŽENIE OBJEKTU – ZÁZNAMY: <i>Ponúka poskytovateľ cloudových služieb schopnosť vytvárať záznamy z auditov, ktoré zahŕňajú podrobnosti o jednej žiadosti o prístup, napríklad žiadateľa, čas žiadosti, požadovaný zásah, stav odpovede a kód chýb?</i>
31.	ULOŽENIE OBJEKTU – INVENTÁR OBJEKTOV: <i>Ponúka poskytovateľ cloudových služieb schopnosť inventára objektov, aby sa používateľom poskytla možnosť rýchlo vizualizovať objekty a ich stav, čo umožní používateľom rýchlo identifikovať objekty s prístupom verejnosti?</i>
32.	ULOŽENIE OBJEKTU – ZOZNAM METADÁT: <i>Ponúka poskytovateľ cloudových služieb schopnosť inventára objektov, aby sa používateľom poskytla možnosť rýchlo vizualizovať metadáta objektov?</i>
33.	ULOŽENIE OBJEKTU – OPTIMALIZÁCIA ODOSIELANÍ: <i>Má poskytovateľ cloudových služieb schopnosť nasmerovať údaje z okrajových lokalít do služby ukladania pomocou optimalizovanej dráhy siete?</i>
34.	ULOŽENIE OBJEKTU – SCHOPNOSŤ DOPYTU: <i>Ponúka poskytovateľ cloudových služieb schopnosť dopytu týkajúceho sa jeho služby ukladania objektov pomocou vyhlásení štruktúrovaného dopytového jazyka (SQL)?</i>
35.	ULOŽENIE OBJEKTU – VYHLÁDÁVANIE PODSKUPÍN: <i>Ponúka poskytovateľ cloudových služieb schopnosť vyhľadávať časti údajov o objekte pomocou jednoduchých výrazov štruktúrovaného dopytového jazyka (SQL)?</i>

36.	SLUŽBA UKLADANIA SÚBOROV: <i>Ponúka poskytovateľ cloudových služieb jednoduchú a škálovateľnú službu ukladania súborov na použitie s počítačovými inštanciami v cloude?</i>
37.	UKLADANIE SÚBOROV – ZÁLOHOVANIE: <i>Zálohuje poskytovateľ cloudových služieb objekty systému súborov (t. j. adresár, súbor a link) vo viacerých dátových centrách alebo zariadeniach, aby sa dosiahli vyššie úrovne dostupnosti a trvanlivosti?</i>
38.	UKLADANIE SÚBOROV – VYMAZANIE ÚDAJOV: <i>Podporuje poskytovateľ cloudových služieb úplné vymazanie údajov uložených súborov, aby už neboli čitateľné alebo prístupné pre neoprávnených užívateľov alebo pre tretie strany?</i>
39.	UKLADANIE SÚBOROV – VYSOKÁ DOSTUPNOSŤ: <i>Poskytuje systém súborov riadený poskytovateľom cloudových služieb vysoký stupeň dostupnosti?</i>
40.	UKLADANIE SÚBOROV – NFS: <i>Podporuje poskytovateľ cloudových služieb protokol systému sieťového súboru (NFS)?</i>
41.	UKLADANIE SÚBOROV – SMB: <i>Podporuje poskytovateľ cloudových služieb protokol bloku hlásení servera (SMB)?</i>
42.	UKLADANIE SÚBOROV – ŠIFROVANIE ULOŽENÝCH SÚBOROV: <i>Podporuje služba ukladanie súboru poskytovateľa cloudových služieb šifrovanie uložených údajov?</i>
43.	UKLADANIE SÚBOROV – ŠIFROVANIE PRENÁŠANÝCH ÚDAJOV: <i>Podporuje služba ukladanie súboru poskytovateľa cloudových služieb šifrovanie prenášaných údajov?</i>
44.	UKLADANIE SÚBOROV – NÁSTROJ NA MIGRÁCIU ÚDAJOV: <i>Ponúka poskytovateľ cloudových údajov nástroj na migráciu údajov, aby sa umožnilo používateľom presúvať údaje zo systémov v priestoroch do cloudových súborových systémov?</i>
45.	SLUŽBA ARCHIVAČNÉHO UKLADANIA: <i>Ponúka poskytovateľ cloudových služieb službu nízkonákladového uloženia zameranú na archivovanie objektov a súborov s menej častým prístupom a takmer nemeniteľných?</i>
46.	ARCHIVAČNÉ UKLADANIE – TOLERANCIA CHÝB: <i>Poskytuje architektúra poskytovateľa cloudových služieb toleranciu chýb pre jeho službu archivačného ukladania?</i>
47.	ARCHIVAČNÉ UKLADANIE – NEMENITEĽNOSŤ: <i>Podporuje poskytovateľ cloudových služieb nemeniteľnosť archivovaných objektov a súborov?</i>
48.	ARCHIVAČNÉ UKLADANIE – WORM: <i>Ponúka poskytovateľ cloudových služieb schopnosť zapísať raz, čítať mnohokrát (WORM)?</i>
49.	ARCHIVAČNÉ UKLADANIE – VYHLÁDÁVANIE PODSKUPÍN: <i>Ponúka poskytovateľ cloudových služieb používateľom schopnosť vyhľadávať iba podskupinu údajov v archivovanom objekte pomocou jednoduchých výrazov štruktúrovaného dopytového jazyka (SQL)?</i>
50.	ARCHIVAČNÉ UKLADANIE – RÝCHLOSŤ VYHLÁDÁVANIA: <i>Ponúka poskytovateľ cloudových služieb používateľom viacero možností vyhľadávania údajov s rôznymi nákladmi a časmi vyhľadávania?</i>
51.	ARCHIVAČNÉ UKLADANIE – ŠIFROVANIE ULOŽENÝCH ÚDAJOV: <i>Podporuje služba archivačného ukladania poskytovateľa cloudových služieb šifrovanie uložených údajov?</i>

52.	UKLADANIE – LIMITY SLUŽBY: Má poskytovateľ cloudových služieb nejaké obmedzenia (t. j. limity služby) ohľadom na vyššie uvedenú sekciu ukladania? Príklad: Maximálna veľkosť objemu Maximálny počet mechaník pripojených k inštancii Maximálny počet vstupných/výstupných operácií za sekundu (IOPS) Maximálna veľkosť objektu Maximálny počet objektov na účet úložiska Maximálny počet snímok obrazovky
-----	---

4. Spravovanie

	Požiadavka
1.	SPRAVOVANIE – POUŽÍVATELIA A SKUPINY: Ponúka poskytovateľ cloudových služieb službu na vytvorenie a spravovanie používateľov a skupín používateľov v rámci svojej infraštruktúry a prostriedkov?
2.	SPRAVOVANIE – RESETOVANIE HESLA: Umožňuje poskytovateľ cloudových služieb používateľom resetovať ich vlastné heslo samoobslužným spôsobom?
3.	SPRAVOVANIE – POVOLENIA: Ponúka poskytovateľ cloudových služieb schopnosť pridávať povolenia používateľom a skupinám na úrovni zdroja?
4.	SPRAVOVANIE – DOČASNÉ POVOLENIA: Ponúka poskytovateľ cloudových služieb schopnosť vytvárať povolenia, ktoré platia pre konkrétny časový interval?
5.	SPRAVOVANIE – DOČASNÉ PRIHLASOVACIE ÚDAJE: Ponúka poskytovateľ cloudových služieb používateľom schopnosť vytvárať a poskytovať dočasné bezpečnostné potvrdenia dôveryhodným používateľom, ktoré budú trvať od niekoľko minút do niekoľko hodín?
6.	SPRAVOVANIE – RIADENIE PRÍSTUPU: Ponúka poskytovateľ cloudových služieb jemne štruktúrované riadenie prístupu k svojim prostriedkom infraštruktúry? Ak áno, aké podmienky môžu byť použité týmito kontrolami (t. j. čas dňa, pôvodná IP adresa atď.)?
7.	SPRAVOVANIE – INTEGROVANÉ SÚBORY PRAVIDIEL: Obsahuje infraštruktúra poskytovateľa cloudových služieb integrované súbory pravidiel riadenia prístupu, ktoré môžu byť pripojené k používateľom a skupinám?
8.	SPRAVOVANIE – VLASTNÉ POSTUPY: Umožňuje infraštruktúra poskytovateľa cloudových služieb vytvoriť a prispôsobiť potrebám zákazníka postupy riadenia prístupu, ktoré môžu byť pripojené k používateľom a skupinám?
9.	SPRAVOVANIE – SIMULÁCIA SÚBORU PRAVIDIEL Ponúka poskytovateľ cloudových služieb mechanizmus na testovanie účinkov súborov pravidiel riadenia prístupu pred praktickým zavedením takýchto súborov pravidiel?

10.	SPRAVOVANIE – VIACFAKTOROVÉ OVEROVANIE V CLOUDE: Podporuje poskytovateľ cloudových služieb používanie viacfaktorového overovania (MFA) ako doplnkovú úroveň riadenia prístupu a overovania svojej infraštruktúry?
11.	SPRAVOVANIE – LIMITY SLUŽBY: Má poskytovateľ cloudových služieb nejaké obmedzenia (t. j. limity služby) s ohľadom na vyššie uvedenú sekciu spravovania? Príklad: Maximálny počet používateľov Maximálny počet skupín Maximálny počet spravovaných pravidiel

5. Bezpečnosť

	Požiadavka
1.	BEZPEČNOSŤ – BEZPEČNOSTNÉ KONTROLY: Podliehajú všetci pracovníci poskytovateľa cloudových služieb, ktorí majú prístup k infraštruktúre služby (fyzický alebo nefyzický), bezpečnostným kontrolám?
2.	BEZPEČNOSŤ – FYZICKÝ PRÍSTUP: Obmedzuje poskytovateľ cloudových služieb prístup pracovníkov k infraštruktúre služby, pokiaľ neexistuje oznámenie porúch, žiadosť o zmenu alebo podobné formálne oprávnenie?
3.	BEZPEČNOSŤ – ZÁZNAMY PRÍSTUPU: Zaznamenáva poskytovateľ cloudových služieb prístup pracovníkov k svojej infraštruktúre, keď je takýto prístup vždy zaznamenávaný a záznamy sú uchovávané minimálne 90 dní?
4.	BEZPEČNOSŤ – PRIHLÁSENIA HOSTITEĽA: Obmedzuje poskytovateľ cloudových služieb svojich pracovníkov pri prihlasovaní do hostiteľských počítačov namiesto automatizovania všetkých úloh vykonávaných na hostiteľských počítačoch, kde je zaznamenávaný obsah týchto automatizovaných prác so záznamami uchovávanými minimálne 90 dní?
5.	BEZPEČNOSŤ – ŠIFROVACIE KĹÚČE: Ponúka poskytovateľ cloudových služieb službu na vytváranie a kontrolu šifrovacích kľúčov používaných na šifrovanie užívateľských údajov?
6.	BEZPEČNOSŤ – SPRÁVA PRÍSTUPOVÝCH KĹÚČOV: Ponúka poskytovateľ cloudových služieb schopnosť identifikovať, kedy bol naposledy použitý prístupový kľúč, striedať staré kľúče a odstrániť neaktívnych používateľov?
7.	BEZPEČNOSŤ – KĹÚČE, KTORÉ POSKYTUJE ZÁKAZNÍK: Umožňuje poskytovateľ cloudových služieb používateľom importovať kľúče z ich vlastnej infraštruktúry spravovania kľúčov do služby spravovania kľúčov poskytovateľa cloudových služieb?
8.	BEZPEČNOSŤ – INTEGRÁCIA SLUŽBY ŠIFROVACÍCH KĹÚČOV: Integruje sa služba spravovania kľúčov poskytovateľa cloudových služieb s inými cloudovými službami na poskytovanie údajov so schopnosťou šifrovania uložených údajov?

9.	BEZPEČNOSŤ – HSM: <i>Ponúka poskytovateľ cloudových služieb hardvérové bezpečnostné moduly bezpečnosti vyhradeného softvéru (HSM), t. j. hardvérové zariadenia, ktoré poskytujú bezpečné uloženie kľúčov a šifrovacie postupy v rámci hardvérového modulu odolného proti nedovolenému zasahovaniu?</i>
10.	BEZPEČNOSŤ – TRVANLIVOSŤ ŠIFROVACÍCH KĹÚČOV: <i>Podporuje poskytovateľ cloudových služieb trvanlivosť kľúčov vrátane uloženia viacerých kópií, takže kľúče sú k dispozícii, keď sú potrebné?</i>
11.	BEZPEČNOSŤ – SSO: <i>Ponúka poskytovateľ cloudových služieb riadenú službu jediného prihlásenia (SSO), ktorá používateľom umožňuje centrálnu riadiť prístup k viacerým účtom a obchodným aplikáciám?</i>
12.	BEZPEČNOSŤ – CERTIFIKÁTY: <i>Ponúka poskytovateľ cloudových služieb riadenú službu na poskytovanie, spravovanie a rozmiestnenie certifikátov vrstvy zabezpečených socketov (SSL)/bezpečnostnej prenosovej vrstvy (TLS)?</i>
13.	BEZPEČNOSŤ – OBNOVA CERTIFIKÁTOV: <i>Uľahčuje certifikát riadenia služby poskytovateľa cloudových služieb obnovu certifikátov?</i>
14.	BEZPEČNOSŤ – CERTIFIKÁTY SO ZÁSTUPNÝMI ZNAKMÍ: <i>Podporuje certifikát riadenia služby poskytovateľa cloudových služieb používanie certifikátov so zástupnými znakmi?</i>
15.	BEZPEČNOSŤ – CERTIFIKAČNÝ ORGÁN: <i>Pôsobí sekcia riadenia certifikátov poskytovateľa cloudových služieb aj ako certifikačný orgán (CA)?</i>
16.	BEZPEČNOSŤ – AKTÍVNY ADRESÁR: <i>Ponúka poskytovateľ cloudových služieb službu riadeného aktívneho adresára (AD) Microsoftu v cloude?</i>
17.	BEZPEČNOSŤ – AKTÍVNY ADRESÁR V PREVÁDZKACH: <i>Podporuje služba riadenia aktívneho adresára Microsoftu (AD) poskytovateľa cloudových služieb integráciu aktívneho adresára Microsoftu (AD) v prevádzkach?</i>
18.	BEZPEČNOSŤ – LDAP: <i>Podporuje riadený aktívny adresár Microsoftu (AD) poskytovateľa cloudových služieb protokol ľahkého prístupu k adresáru (LDAP)?</i>
19.	BEZPEČNOSŤ – AKTÍVNY ADRESÁR: <i>Podporuje služba riadený aktívny adresár Microsoftu (AD) poskytovateľa cloudových služieb protokol (SAML)?</i>
20.	BEZPEČNOSŤ – RIADENIE DOKUMENTOV PRIHLASOVACÍCH ÚDAJOV: <i>Ponúka poskytovateľ cloudových služieb riadenú službu, ktorá pomáha používateľom ľahko stridať, riadiť a vyhľadávať potvrdenia, napríklad kľúče aplikačného programovacieho rozhrania (API), dokumenty databázy a iné tajomstvá?</i>
21.	BEZPEČNOSŤ – WAF: <i>Ponúka poskytovateľ cloudových služieb webový aplikačný firewall (WAF), ktorý pomáha chrániť webové aplikácie pred bežnými webovými zneužitiami, ktoré môžu ovplyvniť dostupnosť aplikácií, poškodiť bezpečnosť alebo nadmerne spotrebúvať zdroje?</i>
22.	BEZPEČNOSŤ – DDOS: <i>Ponúka poskytovateľ cloudových služieb službu, ktorá chráni pred najčastejšie sa vyskytujúcimi distribuovanými útokmi odmietnutia služby (DDoS) na sieť a transportnú vrstvu spolu so schopnosťou napísať pravidlá prispôbené potrebám zákazníka na zmiernenie sofistikovaných útokov na aplikačnú vrstvu?</i>

23.	BEZPEČNOSŤ – BEZPEČNOSTNÉ ODPORÚČANIA: Ponúka poskytovateľ cloudových služieb službu na automatické posúdenia potenciálnej zraniteľnosti aplikácií a zdrojov?
24.	BEZPEČNOSŤ – DETEKCIA HROZBY: Ponúka poskytovateľ cloudových služieb riadenú službu detekcie hrozby?
25.	BEZPEČNOSŤ – LIMITY SLUŽBY: Má poskytovateľ cloudových služieb nejaké obmedzenia (t. j. limity služby) s ohľadom na vyššie uvedenú sekciu bezpečnosti? Príklad: Maximálny počet zákazníckych hlavných kľúčov Maximálny počet bezpečnostných modulov hardvéru (HSM)

6. Dodržiavanie predpisov

Nižšie uvedený zoznam bol poskytnutý iba na ilustračné účely, nemal by sa považovať za úplný a uvádza certifikácie a normy, ktoré možno uplatniť na cloudové služby.

Uvedte, ktorý súbor medzinárodných a priemyselných noriem poskytovateľ cloudových služieb dodržal.

Certifikácie/atestácie	Zákony, predpisy a ochrana údajov	Usmernenia/rámce
☐ C5 [Nemecko]	☐ Smernica EÚ o ochrane údajov	☐ CDSA
☐ Etický kódex CISPE na ochranu údajov	☐ Modelové doložky EÚ	
☐ CNDP (Pakt o klimatickej neutralite dátových centier)		
☐ DIACAP	☐ FERPA	☐ CIS
☐ DoD SRG úrovne 2 a 4	☐ GDPR	☐ Informačná služba o trestnom súdnictve (CIJS)
☐ FedRAMP	☐ GLBA	☐ CSA
☐ FIPS 140-2	☐ HIPAA	☐ Štít na ochranu osobných údajov medzi EÚ a USA
☐ HDS (Francúzsko, zdravotná starostlivosť)	☐ HITECH	☐ Bezpečný prístav EÚ
☐ ISO 9001	☐ IRS 1075	☐ FISC
☐ ISO 27001	☐ ITAR	☐ FISMA
☐ ISO 27017	☐ PDPA – 2010 [Malajzia]	☐ G-Cloud [Spojené kráľovstvo]
☐ ISO 27018	☐ PDPA – 2012 [Singapur]	☐ GxP (FDA CFR 21 časť 11)
☐ IRAP [Austrália]	☐ PIPEDA [Kanada]	☐ ICREA

☐ MTCS úroveň 3 [Singapur]	☐ Zákon o ochrane súkromia [Austrália]	☐ IT Grundschutz [Nemecko]
☐ PCI DSS úroveň 1	☐ Zákon o ochrane súkromia [Nový Zéland]	☐ MARS – E
☐ SEC pravidlo 17-a-4(f)	☐ Autorizácia španielskeho úradu na ochranu údajov	☐ MITA 3.0
☐ SOC1 / ISAE 3402	☐ Úrad na ochranu údajov v Spojenom kráľovstve - 1988	☐ MPAA
☐ SOC2 / SOC3	☐ VPAT/odsek 508	☐ NIST
☐ Kódex SWIPO v súvislosti s IaaS		
		☐ Úrovne inštitútu Uptime
		☐ Zásady cloudovej bezpečnosti v Spojenom kráľovstve

Využívanie vyššie uvedených správ o dodržiavaní predpisov umožňuje organizáciám verejného sektora vyhodnotiť jedinečné ponuky oproti akceptovanej bezpečnosti, dodržiavania a prevádzkového štandardu. Takéto správy môžu uvádzať, že CISP, prostredníctvom ich dodržiavania, splňa nižšie uvedené kontroly prevádzky dátových centier, ktoré sa požadujú pre verejného poskytovateľa cloudových služieb. Požadovanie zhody s takýmito správami pomáha subjektom verejného sektora nadobudnúť uistenie, že nižšie uvedené kontroly sú zavedené.

- **Preskúmaný prístup:** CISP by mal obmedziť fyzický prístup na tých ľudí, ktorí potrebujú byť na mieste z oprávneného pracovného dôvodu. Ak je prístup poskytnutý, musí byť odvolaný bezprostredne po dokončení potrebnej práce.
- **Kontrolovaný a monitorovaný vstup:** Vstupovanie do perimetra vrstvy dátového centra musí byť kontrolovaný proces. CISP musí zabezpečiť, aby pri vstupných bránach boli bezpečnostní pracovníci a zamestnať kontrolórov, ktorí budú monitorovať pracovníkov a návštevníkov bezpečnostnými kamerami. Keď sú schválené osoby na mieste, musia dostať menovku, ktorá vyžaduje viacfaktorové overenie a obmedzuje prístup do vopred schválených priestorov.
- **Pracovníci dátového centra CISP:** Zamestnanci CISP, ktorí bežne potrebujú prístup do dátového centra, musia dostať povolenia pre príslušné oblasti zariadenia na základe pracovnej funkcie, pričom prístup je pravidelne skúmaný. Zoznam pracovníkov musí vedúci prístupu do priestoru pravidelne skúmať, aby sa zabezpečilo, že každé oprávnenie zamestnanca je ešte stále potrebné. Ak zamestnanec nemá pretrvávajúci dôvod na svoju prítomnosť v dátovom centre, musí byť požiadaný, aby prešiel procesom pre návštevníkov.
- **Monitorovanie neoprávneného vstupu:** CISP musia neustále monitorovať neoprávnený vstup do priestorov dátového centra s pomocou video dohľadu, detekcie vniknutia a systémami monitorovania záznamov vstupu. Vchody musia byť zabezpečené zariadeniami, ktoré spustia alarmy, ak sú dvere násilne otvorené alebo držané otvorené.
- **Centrá bezpečnostných operácií CISP monitorujú globálnu bezpečnosť:** Centrá bezpečnostných operácií CISP musia byť rozmiestnené po celom svete a zodpovedné za monitorovanie, triedenie a vykonávanie bezpečnostných programov pre dátové centrá CISP. Musia dohliadať na riadenie fyzického prístupu a reakciu na detekciu vniknutia, a zároveň poskytovať globálnu nepretržitú podporu 24 hodín denne počas celého týždňa pre bezpečnostné tímy dátových centier na mieste; poskytujú nepretržité monitorovacie činnosti, napríklad činnosti sledovania prístupu, odvolanie povolení na vstup a sú k dispozícii na reagovanie na a analyzovanie možného bezpečnostného incidentu.
- **Preskúmanie prístupu po vrstvách:** Prístup k vrstve infraštruktúry musí byť obmedzený na základe prevádzkovej potreby. Zavedením preskúmania prístupu po vrstvách sa právo prístupu do každej vrstvy neposkytuje štandardne. Prístup ku konkrétnej vrstve by sa mal poskytnúť iba vtedy, ak existuje špecifická potreba prístupu k tejto špecifickej vrstve.

- **Udržiavanie zariadenia ako súčasti pravidelných postupov:** Tímy CISP by mali vykonávať diagnostiku na strojoch, sieťach a záložných zariadeniach, aby zabezpečili, že sú v prevádzkovom stave a v pohotovosti. Bežné kontroly údržby na zariadeniach a vybavení dátového centra by mali byť súčasťou pravidelných postupov dátového centra CISP.
- **Záložné zariadenia v pohotovosti:** Voda, elektrina, telekomunikácie a pripojenie k internetu by mali byť navrhnuté so zálohovaním, takže CISP môže udržiavať nepretržitú prevádzku aj v prípade núdze. Elektrické napájacie systémy by mali byť navrhnuté tak, aby boli úplne zálohované, takže v prípade prerušenia sa môžu pre niektoré funkcie použiť zdroje neprerušiteľného napájania, zatiaľ čo generátory môžu poskytovať záložné napájanie pre celé zariadenie. Ľudia a systémy by mali monitorovať a kontrolovať teplotu a vlhkosť, aby sa zabránilo prehriatiu, čím sa ďalej znížia výpadky služby.
- **Technológia a ľudia spolupracujú na pridanej bezpečnosti:** Mali by existovať povinné postupy na získanie oprávnenia na vstup do dátovej vrstvy. Zahŕňa to preskúmanie a schválenie žiadosti osoby o prístup oprávnenými pracovníkmi. Medzitým by elektronické systémy detekcie ohrozenia a vniknutia mali monitorovať a automaticky spustiť poplachy v prípade identifikovaných hrozieb a podozrivej činnosti. Napríklad ak sú dvere držané otvorené alebo sú otvorené násilím, spustí sa alarm. CISP by mal využívať bezpečnostné kamery a uchovávať metráž v súlade s požiadavkami dodržiavania predpisov.
- **Prevenca fyzických a technologických vniknutí:** Prístupové miesta do serverovni by mali byť chránené elektronickými kontrolnými zariadeniami, ktoré si vyžadujú viacfaktorové schválenie. CISP by mal byť tiež pripravený zabrániť technologickému vniknutiu. Servery CISP by mali byť schopné varovať zamestnancov pred akýmkoľvek pokusom odstrániť údaje. V nepravdepodobnom prípade porušenia by mal byť server automaticky vypnutý.
- **Serverom a médiám sa venuje zvýšená pozornosť:** Zariadenia na ukladanie médií používané na uloženie zákaznických údajov by mali byť klasifikované CISP ako kritické, a počas celej ich životnosti by sa s nimi malo zaobchádzať ako s vysoko rizikovými. CISP by mal mať prísne štandardy pre inštaláciu, servis a prípadné vyradenie zariadení, keď už nie sú využívané. Keď zariadenie na ukladanie dosiahlo koniec svojej životnosti, CISP vyradí médiá pomocou postupov podrobne uvedených v NIST 800-88. Média, v ktorých sú uložené zákaznické údaje sa nevyjmú spod kontroly CISP, pokiaľ nebudú bezpečne vyradené.
- **Audítori tretej strany overujú postupy a systémy CISP:** CISP by mal byť auditovaný externými audítormi, ktorí skontrolujú dátové centrá vykonaním hĺbkovej kontroly s cieľom potvrdiť, že CISP dodržiava zavedené pravidlá na získanie bezpečnostných certifikátov. V závislosti od programu dodržiavania a jeho požiadaviek môžu mať externí audítori pohovory so zamestnancami CISP o tom, ako zaobchádzajú s médiami a vyradujú ich. Audítori môžu tiež sledovať obsah bezpečnostných kamier a pozorovať vstupy a haly dátového centra. A môžu preskúmať také zariadenia CISP, ako sú elektronické zariadenia na kontrolu prístupu a bezpečnostné kamery.
- **Pripravenosť na neočakávané udalosti:** CISP by sa mal aktívne pripravovať na možné environmentálne hrozby, ako sú prírodné katastrofy a požiar. Inštalácia automatických senzorov a citlivo reagujúce zariadenie sú dva spôsoby, ako bude CISP chrániť dátové centrá. Mali by sa inštalovať zariadenia na detekciu vody, aby upozornili zamestnancov na problémy, keď automatické čerpadlá pracujú na odstránení kvapaliny a zabránení škode. Podobne automatické hlásiče požiaru a hasiace zariadenia znižujú riziko a môžu oznámiť problém zamestnancom CISP a hasičom.
- **Vysoká dostupnosť prostredníctvom viacnásobných zón dostupnosti:** CISP by mal poskytnúť viacnásobné zóny dostupnosti pre väčšiu toleranciu chýb. Každá zóna dostupnosti by mala pozostávať z jedného alebo viacerých dátových centier fyzicky od seba oddelených a mala by mať záložné napájanie a vytváranie siete. Zóny dostupnosti by mali byť navzájom prepojené rýchlou súkromnou optickou sieťou, aby sa vytvorili aplikácie, ktoré automaticky prechádzajú medzi zónami dostupnosti bez prerušenia.
- **Simulovanie prerušení a meranie našej reakcie:** CISP by mal mať plán na zabezpečenie kontinuity činnosti ako návod na prevádzkové postupy, ktorý uvádza, ako zabrániť a znížiť prerušenia spôsobené prírodnými katastrofami s podrobnými krokmi, ktoré sa majú vykonať pred, počas a po udalosti. Aby sa CISP zmiernil a pripravil sa na neočakávané udalosti, musí pravidelne testovať plán na zabezpečenie kontinuity činnosti s nácvikmi, ktoré simulujú rôzne scenáre. CISP by mal dokumentovať, ako konajú jeho ľudia a procesy, potom opísať ponaučenia a nápravné opatrenia, ktoré môžu byť potrebné na zlepšenie rýchlosti reakcie. Pracovníci CISP by mali byť vyškolení a pripravení rýchlo reagovať na prerušenia s metodickým postupom obnovy, aby sa minimalizovali ďalšie odstávky spôsobené chybami.
- **Pomoc spĺňa ciele účinnosti:** Okrem riešenia environmentálnych rizík by CISP mal zahrnúť do návrhu dátových centier aj úvahy o udržateľnosti. CISP by mal poskytnúť podrobnosti o svojom záväzku využívať obnoviteľnú energiu pre svoje dátové centrá a poskytnúť informácie ako jej zákazníci môžu znížiť emisie uhlíka oproti vlastným dátovým centrom.
- **Výber miesta:** Pred výberom miesta by CISP mala vykonať počiatočné environmentálne a geografické posúdenia. Umiestnenia dátových centier by sa mali dôkladne vybrať, aby sa zmiernili environmentálne riziká, napríklad zaplavenie,

extrémne počasie a seizmickú činnosť. Zóny dostupnosti CISP by mali byť vybudované tak, aby boli nezávislé a fyzicky oddelené jedna od druhej.

- **Zálohovanie:** Dátové centrá by mali byť navrhnuté tak, aby predpokladali a tolerovali zlyhanie počas údržby úrovni služby. V prípade zlyhania by mali automatizované procesy odsunúť prevádzku z postihnutej oblasti. Hlavné aplikácie by mali byť zavedené podľa štandardu N+1, takže v prípade zlyhania dátového centra existuje dostatočná kapacita, ktorá umožní, aby zaťaženie prevádzky bolo rovnomerne rozdelené na zostávajúce miesta.
- **Dostupnosť:** CISP by mal identifikovať kritické komponenty systému požadované na udržiavanie dostupnosti jeho systému a obnoviť službu v prípade výpadku. Kritické komponenty systému by mali byť zálohované na viacerých, izolovaných lokalitách. Každá lokalita alebo zóna dostupnosti by mala byť navrhnutá tak, aby pôsobila nezávisle s vysokou spoľahlivosťou. Zóny dostupnosti by mali byť prepojené, aby umožnili aplikáciám automaticky prechod medzi zónami dostupnosti bez prerušenia. Vysoko odolné systémy a dostupnosť služby by mali byť funkciou návrhu systému. Návrh dátového centra so zónami dostupnosti a kopírovanie údajov by mali umožniť zákazníkovi CISP dosiahnuť extrémne krátky čas obnovy a cieľe miesta obnovy, ako aj najvyššie úrovne dostupnosti služieb.
- **Plánovanie kapacity:** CISP by mal nepretržite monitorovať využívanie služieb, aby rozmiestnila infraštruktúru na podporu záväzkov a požiadaviek týkajúcich sa dostupnosti. CISP by mal udržiavať model plánovania kapacity, ktorý posudzuje využívanie infraštruktúry a požiadavky CISP aspoň raz za mesiac. Tento model by mal podporovať plánovanie budúcich požiadaviek a zahŕňať také faktory ako sú spracúvanie informácií, telekomunikácie a uchovávanie záznamov z auditov.

KONTINUITA ČINNOSTI a OBNOVA PO KATASTROFE

- **Plán kontinuity činnosti:** Plán kontinuity činnosti CISP by mal uvádzať opatrenia na zabránenie a zmenšenie environmentálnych prerušení. Mal by zahŕňať prevádzkové podrobnosti o krokoch, ktoré sa majú vykonať pred udalosťou a po nej. Plán kontinuity činnosti by mal byť podporený testovaním, ktoré zahŕňa simulácie rôznych scenárov. Počas testovania a po ňom by mala CISP dokumentovať výkon ľudí a procesu, nápravné opatrenia a poučenia s cieľom nepretržitého zlepšovania.
- **Reakcia na pandémie:** CISP by mal zahrnúť metódy a postupy reakcie na pandémiu do svojho plánovania obnovy po katastrofe, aby sa pripravil na rýchlu reakciu na hrozby vypuknutia infekčnej choroby. Stratégie zmierňovania zahŕňajú alternatívne modely personálneho zabezpečenia na presun kritických procesov na zdroje mimo regiónu a aktiváciu plánu krízového riadenia na podporu kritických obchodných činností. Pandemické plány by mali odkazovať na medzinárodné zdravotné agentúry a predpisy vrátane kontaktných miest pre medzinárodné agentúry.

MONITOROVANIE a PROTOKOLOVANIE

- **Preskúmanie prístupu do dátových centier:** Prístup k dátovým centráм sa má pravidelne skúmať. Prístup by mal byť automaticky zrušený, keď sa v systéme ľudských zdrojov CISP ukončí evidencia o zamestnancovi. Okrem toho, keď uplynie prístup zamestnanca alebo zhotoviteľa v súlade so schváleným trvaním žiadosti, jeho alebo jej prístup bude zrušený, dokonca aj keď zostáva zamestnancom CISP.
- **Záznamy o prístupe do dátového centra:** Fyzický prístup má byť zaznamenaný, monitorovaný a uchovaný v dátovom centre CISP. CISP má korelovať informácie získané z logických a fyzických monitorovacích systémov, aby zvýšila bezpečnosť podľa potreby.
- **Monitorovanie prístupu do dátového centra:** CISP má monitorovať dátové centrá pomocou globálnych centier bezpečnostných operácií, ktoré zodpovedajú za monitorovanie, triedenie a vykonávanie bezpečnostných programov. Budú poskytovať globálnu podporu 24 hodín denne počas celého týždňa riadením a monitorovaním činností prístupu do dátových centier, vybavením miestnych tímov a iných podporných tímov na reagovanie na bezpečnostné incidenty triedením, konzultovaním, analyzovaním a odosielaním odpovedí.

DOHĽAD a DETEKCIA

- **CCTV:** Miesta fyzického prístupu do serverovni by mali byť zaznamenávané priemyselnou televíziou (CCTV). Obrázky by mali byť uchovávané podľa zákonných požiadaviek a požiadaviek na dodržiavanie predpisov.
- **Miesta vstupu do dátového centra:** Fyzický prístup by mal byť kontrolovaný na miestach vstupu do budovy profesionálnymi bezpečnostnými pracovníkmi využívajúcimi dohľad, detekčné systémy a iné elektronické prostriedky. Oprávnení pracovníci by mali využívať mechanizmy viacfaktorového overovania prístupu do dátových centier. Vstupy do serverovni by mali byť chránené zariadeniami, ktoré spustia alarm na iniciovanie reakcie na incident, ak sa dvere otvoria násilím alebo sa držia otvorené.

- **Detekcia vniknutia:** Systémy elektronickej detekcie vniknutia by mali byť inštalované v dátovej vrstve, aby monitorovali, detegovali a automaticky upozornili príslušných pracovníkov na bezpečnostné incidenty. Miesta vstupu a výstupu zo serverovni by mali byť chránené zariadeniami, ktoré požadujú od každej osoby, aby pred umožnením vstupu alebo výstupu poskytla viac faktorové overenie. Tieto zariadenia spustia alarm, keď sa dvere násilne otvoria alebo držia otvorené bez oprávnenia. Poplachové zariadenia dverí budú tiež konfigurované na detekciu prípadov, kde osoba vychádza alebo vchádza do dátovej vrstvy bez poskytnutia viacfaktorového overenia. Alarmy musia byť okamžite odoslané do centier bezpečnostných operácií CISP fungujúcich 24 hodín počas celého týždňa na okamžité zaregistrovanie, analýzu a reakciu.

SPRÁVA ZARIADENÍ

- **Správa aktív:** Aktíva CISP by mali byť centrálné manažované cez inventarizačný systém, ktorý ukladá a sleduje vlastníka, miesto, stav, udržiavanie a opisné informácie pre aktíva vlastnené CISP. Po obstaraní budú aktíva snímané a sledované a aktíva, na ktorých sa vykonáva údržba, budú monitorované v súvislosti s vlastníctvom, stavom a rozlišovaním.
- **Zničenie médií:** Zariadenia na ukladanie médií používané na uloženie zákazníckych údajov by mali byť klasifikované CISP ako kritické, a počas celej ich životnosti by sa s nimi malo zaobchádzať ako s vysoko rizikovými. CISP by mal požadovať prísne normy o tom, ako inštalovať, obsluhovať a prípadne vyradiť zariadenia, ak už nie sú užitočné. Keď zariadenie na ukladanie dosiahlo koniec svojej životnosti, CISP vyradí médiá pomocou postupov podrobne uvedených v NIST 800-88. Média, v ktorých sú uložené zákaznícke údaje, sa nevyčlenia spod kontroly CISP, pokiaľ nebudú bezpečne vyradené.

SYSTÉMY PREVÁDZKOVEJ PODPORY

- **Elektrina:** Systémy napájania dátových centier CISP by mali byť navrhnuté tak, aby boli úplne zálohované a udržiavateľné bez vplyvu na operácie, 24 hodín denne. CISP má zabezpečiť, aby boli dátové centrá vybavené záložným napájaním, aby sa zabezpečilo, že elektrina je k dispozícii na udržiavanie operácií v prípade zlyhania dodávky elektriny pre kritické podstatné záťaže v zariadení.
- **Klíma a teplota:** Dátové centrá CISP by mali používať mechanizmy na regulovanie klímy a udržiavanie vhodnej prevádzkovej teploty pre servery a iný hardvér, aby sa zabránilo prehriatiu a znížila sa možnosť výpadkov služby. Pracovníci a systémy by mali monitorovať a regulovať teplotu a vlhkosť na príslušných úrovniach.
- **Zisťovanie a hasenie požiarov:** Dátové centrá CISP by mali byť vybavené automatickým systémom hlásenia požiaru a hasiacim zariadením. Systémy hlásenia požiaru by mali využívať senzory dymu v rámci sieťových, mechanických a infraštruktúrnych priestorov. Tieto oblasti by mali byť tiež chránené hasiacimi systémami.
- **Detekcia unikania:** Aby sa zistila prítomnosť únikov vody, CISP by mala vybaviť dátové centrá s funkčnosťou na zisťovanie prítomnosti vody. Ak sa voda zistí, mali by byť zavedené mechanizmy na odstránenie vody s cieľom zabrániť ďalšiemu poškodeniu vodou.

ÚDRŽBA INFRAŠTRUKTÚRY

- **Údržba zariadení:** CISP by mal monitorovať a vykonávať preventívnu údržbu elektrických a mechanických zariadení s cieľom udržiavať pokračujúcu prevádzkyschopnosť systémov v rámci dátových centier CISP. Postupy údržby zariadení by mali vykonávať kvalifikované osoby a mali by byť dokončené podľa zdokumentovaného harmonogramu údržby.
- **Environmentálny manažment:** CISP by mal monitorovať elektrické a mechanické systémy a zariadenia s cieľom umožniť okamžitú identifikáciu problémov. Toto by sa malo vykonávať využívaním kontinuálnych auditových nástrojov a informácií poskytovaných stavebnou správou a elektrickými monitorovacími systémami CISP. Preventívna údržba by sa mala vykonať na udržiavanie pokračujúcej prevádzkyschopnosti zariadenia.

RIADENIE A RIZIKÁ

- **Pokračujúce riadenie rizík dátového centra:** Centrum bezpečnosti operácií CISP by malo vykonávať pravidelné preskúmania hrozieb a zraniteľnosti dátových centier. Pokračujúce posudzovanie a zmierňovanie možných zraniteľností by sa malo vykonávať prostredníctvom činností posudzovania rizík dátových centier. Toto posudzovanie by malo byť vykonávané navyše k procesu posudzovania rizík na úrovni podniku používaného na identifikáciu a zvládnutie rizík pre podnik ako celok. Tento proces by mal brať do úvahy aj regionálne regulačné a environmentálne riziká.

- **Atestácia bezpečnosti treťou stranou:** Testovanie dátových centier CISP treťou stranou dokumentované v správach tretích strán by malo zabezpečiť, aby CISP vhodne realizovala bezpečnostné opatrenia zladené so zavedenými pravidlami potrebnými na získanie bezpečnostných certifikátov. V závislosti od programu dodržiavania predpisov a jeho požiadaviek môžu externí auditori vykonávať testovanie vyradovania médií, preskúmanie metráže bezpečnostných kamier, pozorovanie vstupov a hál v dátovom centre, testovanie elektronických prístrojov na kontrolu prístupu a preskúmanie vybavenia dátových centier.

7. Migrácie

	Požiadavka
1.	SLUŽBA MIGRÁCIÍ: Koľko rozdielnych služieb migrácií údajov ponúka poskytovateľ cloudových služieb?
2.	MIGRÁCIE – CENTRALIZOVANÉ MONITOROVANIE: Ponúka poskytovateľ cloudových služieb organizáciám centralizovanú službu (t. j. ucelené zobrazenie), kde môžu sledovať a monitorovať stav svojho servera a migrácie aplikácií?
3.	MIGRÁCIE – OVLÁDACÍ PANEL: Ponúka migračný nástroj poskytovateľa cloudových služieb ovládací panel na rýchlu vizualizáciu stavu migrácie, súvisiacu metriku a históriu migrácie?
4.	MIGRÁCIE – NÁSTROJE POSKYTOVATEĽA CLOUDOVÝCH SLUŽIEB: Ponúka migračný nástroj poskytovateľa cloudových služieb integráciu s inými migračnými nástrojmi od poskytovateľa cloudových služieb, ktoré môžu vykonávať migrácie servera a aplikácií?
5.	MIGRÁCIE – NÁSTROJE TRETEJ STRANY: Umožňuje migračný nástroj poskytovateľa cloudových služieb zahrnúť migračné nástroje tretej strany? • Ak áno, aké sú podporované migračné nástroje tretej strany?
6.	MIGRÁCIE – MIGRÁCIE DO VIACERÝCH REGIÓNOV: Ponúka migračný nástroj poskytovateľa cloudových služieb schopnosť sledovania a monitorovania migrácií servera a aplikácií, ktoré sa konajú v rôznych regiónoch?
7.	MIGRÁCIE – MIGRÁCIA SERVERA: Ponúka migračný nástroj poskytovateľa cloudových služieb spôsob, ako vykonať migráciu virtualizovaného servera v prevádzkach do cloudu? • Ak áno, ktoré virtualizované prostredia sú momentálne podporované?
8.	MIGRÁCIE – ZISŤOVANIE SERVERA: Má migračný nástroj poskytovateľa cloudových služieb schopnosť zisťovania, aby automaticky našiel virtuálne servery v prevádzkach, ktoré majú byť migrované do cloudu?
9.	MIGRÁCIE – ÚDAJE O VÝKONE SERVERA: Má migračný nástroj poskytovateľa cloudových služieb schopnosť zhromažďovať a zobrazovať výkon servera a/alebo virtuálneho stroja ako je centrálna procesorová jednotka (CPU) a využívanie pamäte s náhodným prístupom (RAM)?
10.	MIGRÁCIE – DATABÁZA ZISŤOVANIA: Má migračný nástroj poskytovateľa cloudových služieb schopnosť ukladať všetky zhromaždené údaje v centralizovanej databáze? • Ak áno, majú organizácie schopnosť tieto údaje exportovať? Do akých formátov?
11.	MIGRÁCIE – ŠIFROVANIE NA ÚLOŽISKU: Šifruje poskytovateľ cloudových služieb na úložisku všetky informácie zhromaždené a uložené v databáze zisťovania?

12.	MIGRÁCIE – REPLIKÁCIA PRÍRASTKOVÉHO SERVERA: Ponúka migračný nástroj poskytovateľa cloudových služieb automatizovanú, živú replikáciu prírastkového servera počas migrácie servera alebo virtuálneho stroja ako spôsob podpory zahrnutia všetkých zmien vykonaných na serveri alebo virtuálnom stroji do konečného migrovaného obrazu? • Ak áno, ako dlho môže táto služba bežať?
13.	MIGRÁCIE – VMWARE: Podporuje migračný nástroj poskytovateľa cloudových služieb VMWare migrácie virtuálneho stroja z prevádzok do cloudu?
14.	MIGRÁCIE – HYPER-V: Podporuje migračný nástroj poskytovateľa cloudových služieb Hyper-V migrácie virtuálneho stroja z prevádzok do cloudu?
15.	MIGRÁCIE – ZISŤOVANIE APLIKÁCIÍ: Má migračný nástroj poskytovateľa cloudových služieb schopnosť zisťovať a zoskupovať aplikácie pred ich migrovaním?
16.	MIGRÁCIE – MAPOVANIE ZÁVISLOSTI: Má migračný nástroj poskytovateľa cloudových služieb schopnosť zisťovať závislosti medzi servermi a aplikáciami pred ich migrovaním?
17.	MIGRÁCIE – MIGRÁCIA DATABÁZY: Má migračný nástroj poskytovateľa cloudových služieb schopnosť migrovať databázy prevádzok do cloudu?
18.	MIGRÁCIE – ODSŤÁVKA MIGRÁCIE DATABÁZY: Má migračný nástroj poskytovateľa cloudových služieb schopnosť vykonávať migráciu databázy do cloudu s minimálnou odstávkou, t. j. zdrojová databáza zostane úplne prevádzkyschopná počas procesu migrácie?
19.	MIGRÁCIE – ZDROJOVÁ DATABÁZA: Podporuje migračný nástroj poskytovateľa cloudových služieb migrovanie rôznych databázových zdrojov ako sú Oracle, SQL Server atď.? • Ak áno, uveďte všetky podporované zdrojové databázy, ktoré môžu byť migrované do cloudu.
20.	MIGRÁCIE – HETEROGÉNNE MIGRÁCIE: Má migračný nástroj poskytovateľa cloudových služieb schopnosť vykonávať migrácie heterogénnych databáz, t. j. Z jednej zdrojovej databázy do odlišnej cieľovej databázy, napríklad z Oracle do SQL Server? • Ak áno, uveďte všetky možné kombinácie migrácie heterogénnych databáz.
21.	MIGRÁCIE – MIGRÁCIA ÚDAJOV VO VEĽKOSTI PETABAJTOV: Ponúka poskytovateľ cloudových služieb riešenie transportu údajov vo veľkosti petabajtov, ktoré používa bezpečné prostriedky na prenos veľkých množstiev údajov do cloudu a z neho?
22.	MIGRÁCIE – MIGRÁCIA ÚDAJOV VO VEĽKOSTI EXABAJTOV: Ponúka poskytovateľ cloudových služieb riešenie transportu údajov vo veľkosti exabajtov na presun extrémne veľkých množstiev údajov do cloudu?
23.	MIGRÁCIE – PODNIKOVÉ ZÁLOHOVANIE: Ponúka poskytovateľ cloudových služieb službu hladkého integrovania dátového centra zákazníka so službami ukladania cloudu, ktoré umožnia prenos a ukladanie údajov do služby ukladania údajov poskytovateľa cloudových služieb?
24.	MIGRÁCIE – PODNIKOVÉ ZÁLOHOVANIE – UKLADANIE OBJEKTOV: Ponúka služba podnikového zálohovania poskytovateľa cloudových služieb integráciu so službou ukladania objektov poskytovateľa cloudových služieb?

25.	MIGRÁCIE – PODNIKOVÉ ZÁLOHOVANIE – PRÍSTUP K SÚBOROM: <i>Umožňuje služba podnikového zálohovania poskytovateľa cloudových služieb používateľom ukladať a vyhľadávať objekty pomocou protokolov súborov, ako je protokol systému súborov siete (NFS)?</i>
26.	MIGRÁCIE – PODNIKOVÉ ZÁLOHOVANIE – PRÍSTUP K BLOKOM: <i>Umožňuje služba podnikového zálohovania poskytovateľa cloudových služieb používateľom ukladať a vyhľadávať objekty pomocou protokolov blokov, ako je protokol rozhrania internetových malých počítačových systémov (iSCSI)?</i>
27.	MIGRÁCIE – PODNIKOVÉ ZÁLOHOVANIE – PRÍSTUP K PÁSKE: <i>Umožňuje služba podnikového zálohovania poskytovateľa cloudových služieb používateľom zálohovať svoje údaje prostredníctvom knižnice virtuálnych magnetických pásk a uložiť tieto zálohovania na páskach do cloudu poskytovateľa?</i>
28.	MIGRÁCIE – PODNIKOVÉ ZÁLOHOVANIE – ŠIFROVANIE: <i>Ponúka služba podnikového zálohovania poskytovateľa cloudových služieb šifrovanie údajov v pokoji alebo na ceste?</i>
29.	MIGRÁCIE – PODNIKOVÉ ZÁLOHOVANIE – INTEGRÁCIA SOFTVÉRU TRETEJ STRANY: <i>Integruje sa služba podnikového zálohovania poskytovateľa cloudových služieb s bežne používaným záložným softvérom tretej strany?</i>
30.	MIGRÁCIE – LIMITY SLUŽBY: <i>Má poskytovateľ cloudových služieb nejaké obmedzenia (t. j. limity služby) s ohľadom na vyššie uvedenú sekciu migrácií?</i> <i>Príklad:</i> <i>Maximálny počet súbežných migrácií virtuálneho stroja</i> <i>Maximálny usporiadateľný počet riešení transportu údajov</i>

8. Fakturácia

	Požiadavka
1.	FAKTURÁCIA – SLEDOVANIE A NAHLASOVANIE: <i>Ponúka poskytovateľ cloudových služieb sledovanie a nahlasovanie fakturačnej služby, aby pomohol používateľom riadiť a monitorovať využívanie cloudových ponúk?</i>
2.	FAKTURÁCIA – ALARM A OZNÁMENIA: <i>Ponúka poskytovateľ cloudových služieb používateľom mechanizmus nastavovania alarmov s oznámeniami, aby upozornil používateľov, keď ich výdavky prekročili konkrétny prah?</i>
3.	FAKTURÁCIA – RIADENIE NÁKLADOV: <i>Ponúka poskytovateľ cloudových služieb mechanizmus na vytváranie a zobrazovanie grafov, ktoré sumarizujú náklady a výdavky?</i>
4.	FAKTURÁCIA – ROZPOČTY: <i>Ponúka poskytovateľ cloudových služieb mechanizmus na zobrazovanie a riadenie rozpočtu a predvídané odhadované náklady?</i>
5.	FAKTURÁCIA – KONSOLIDOVANÝ POHĽAD: <i>Ponúka poskytovateľ cloudových služieb mechanizmus na konsolidovanie fakturovania z viacerých účtov pod jedným, primárne platiacim účtom?</i>

6.	FAKTURÁCIA – LIMITY SLUŽBY: Má poskytovateľ cloudových služieb nejaké obmedzenia (t. j. limity služby) s ohľadom na vyššie uvedenú sekciu fakturovania? Príklad: Maximálny počet účtov, ktoré môžu byť zoskupené Maximálny počet alarmov, ktoré môžu byť vytvorené Maximálny počet rozpočtov, ktoré môžu byť riadené
----	---

9. Riadenie

	Požiadavka
1.	RIADENIE – MONITOROVACIA SLUŽBA: Ponúka poskytovateľ cloudových služieb monitorovaciu službu pre riadenie cloudových zdrojov a aplikácií, ktorá zberá, monitoruje a nahlásuje pomocou vopred definovaných metrík?
2.	RIADENIE – ALARMY: Umožňuje monitorovacia služba poskytovateľa cloudových služieb používateľom nastaviť alarmy?
3.	RIADENIE – ZÁKAZNÍCKA METRIKA: Umožňuje monitorovacia služba poskytovateľa cloudových služieb používateľom vytvoriť a monitorovať zákaznícke metriky?
4.	RIADENIE – MONITOROVANIE PODROBNOSTÍ: Poskytuje monitorovacia služba poskytovateľa cloudových služieb rôzne úrovne monitorovania podrobností až na 1-minútovú úroveň?
5.	RIADENIE – SLEDOVACIA SLUŽBA API: Ponúka poskytovateľ cloudových služieb službu, ktorá zaznamenáva, monitoruje a ukladá činnosť týkajúcu sa cloudových zdrojov na úrovni konzoly a aplikačného programovacieho rozhrania (API) na zlepšenie viditeľnosti? Ak áno, aké sú služby poskytovateľa cloudových služieb, ktoré sa integrujú s touto sledovacou službou?
6.	RIADENIE – OZNÁMENIE: Umožňuje poskytovateľ cloudových služieb schopnosť posielat' oznámenia založené na úrovniach činnosti aplikačného programovacieho rozhrania (API)?
7.	RIADENIE – KOMPRESIA: Ponúka poskytovateľ cloudových služieb mechanizmus na kompresiu záznamov vytváraných systémom sledovania aplikačného programovacieho rozhrania (API), aby pomohol používateľom znížiť náklady na ukladanie súvisiace s touto službou?
8.	RIADENIE – SPÁJANIE REGIÓNOV: Ponúka poskytovateľ cloudových služieb schopnosť zaznamenávať činnosť účtu aplikačného programovacieho rozhrania (API) vo všetkých regiónoch a poskytuje tieto informácie súhrnným spôsobom pre uľahčenie používania?
9.	RIADENIE – INVENTARIZÁCIA ZDROJOV: Ponúka poskytovateľ cloudových služieb službu na posúdenie, audit a vyhodnotenie konfigurácií zdrojov zavedených používateľom?
10.	RIADENIE – ZMENY KONFIGURÁCIE: Zaznamenáva poskytovateľ cloudových služieb automaticky zmenu konfigurácie zdrojov, keď táto nastane?

11.	RIADENIE – HISTÓRIA KONFIGURÁCIE: <i>Ponúka poskytovateľ cloudových služieb schopnosť preskúmať konfiguráciu zdrojov v každom jednom bode v minulosti?</i>
12.	RIADENIE – PRAVIDLÁ KONFIGURÁCIE: <i>Ponúka poskytovateľ cloudových služieb usmernenia a odporúčania pre zaistovanie, konfigurovanie a nepretržité monitorovanie dodržiavania predpisov?</i>
13.	RIADENIE – ŠABLÓNY ZDROJOV: <i>Ponúka poskytovateľ cloudových služieb používateľom schopnosť vytvárania, zaistovania a riadenia zhromažďovania zdrojov spôsobom podobným šablóne?</i>
14.	RIADENIE – REPLIKÁCIA ŠABLÓN ZDROJOV: <i>Ponúka poskytovateľ cloudových služieb rýchle replikovanie týchto šablón zdrojov v rôznych regiónoch, ktoré sa potenciálne použijú v situáciách obnovy po katastrofe (DR)?</i>
15.	RIADENIE – DIZAJNÉR ŠABLÓNY: <i>Ponúka poskytovateľ cloudových služieb ľahko použiteľný grafický nástroj s funkčnosťou potiahnuť a pustiť, ktorá urýchľuje proces vytvárania takýchto šablón zdrojov?</i>
16.	RIADENIE – KATALÓG SLUŽIEB: <i>Ponúka poskytovateľ cloudových služieb službu na vytváranie a spravovanie katalógu služieb, t. j. serverov, virtuálnych strojov, softvéru, databáz atď.?</i>
17.	RIADENIE – PRÍSTUP KU KONZOLE: <i>Ponúka poskytovateľ cloudových služieb užívateľské rozhranie založené na webe na uľahčenie riadenia a monitorovania cloudových služieb?</i>
18.	RIADENIE – PRÍSTUP K CLI: <i>Ponúka poskytovateľ cloudových služieb jednotný nástroj na riadenie a konfigurovanie viacnásobných cloudových služieb z rozhrania príkazového riadku (CLI) a umožňuje zautomatizovať úlohy riadenia prostredníctvom používania prihlasovacích súborov?</i>
19.	RIADENIE – MOBILNÝ PRÍSTUP: <i>Ponúka poskytovateľ cloudových služieb smartfónovú aplikáciu, aby používateľom umožnil pripojiť sa ku cloudovej službe a riadiť ich zdroje?</i> • Ak áno, je táto aplikácia dostupná pre iOS a Android?
20.	RIADENIE – NAJLEPŠIE POSTUPY: <i>Má poskytovateľ cloudových služieb službu, ktorá pomáha používateľom porovnávať ich využitie cloudov s najlepšimi postupmi?</i>
21.	RIADENIE – LIMIT SLUŽBY: <i>Má poskytovateľ cloudových služieb nejaké obmedzenia (t. j. limity služby) s ohľadom na vyššie uvedenú sekciu riadenia?</i> <i>Príklad:</i> <i>Maximálny počet konfiguračných pravidiel na účet</i> <i>Maximálny počet alarmov, ktoré môžu byť vytvorené</i> <i>Maximálny počet záznamov, ktoré môžu byť uložené</i>

10. Podpora

	Požiadavka
1.	PODPORA – SLUŽBA: <i>Ponúka poskytovateľ cloudových služieb podporu kedykoľvek, 24 hodín denne, 7 dní v týždni, 365 dní v roku cez telefón, chat a email?</i>
2.	PODPORA – ÚROVNE PODPORY: <i>Ponúka poskytovateľ cloudových služieb rôzne úrovne podpory?</i>
3.	PODPORA – PRIDELENIE VRSTVY: <i>Umožňuje poskytovateľ cloudových služieb používateľom, aby sami priradili spotrebované zdroje/služby rôznym úrovniam podpory na základe podrobnej klasifikácie a nie nútením používateľov udržiavať oddelené cloudové účty na dosiahnutie a prijatie rôznych úrovni podpory?</i>
4.	PODPORA – FÓRA: <i>Ponúka poskytovateľ cloudových služieb verejné fóra pre zákazníkov, aby prediskutovali svoje problémy?</i>
5.	PODPORA – PANEL STAVU SLUŽBY: <i>Ponúka poskytovateľ cloudových služieb panel stavu služby, ktorý zobrazuje do minúty informácie o dostupnosti služby vo viacerých regiónoch?</i>
6.	PODPORA – PERSONALIZOVANÝ PANEL: <i>Ponúka poskytovateľ cloudových služieb panel, ktorý zobrazuje personalizovaný pohľad na výkon a dostupnosť služieb zdôrazňujúci špecifické zdroje používateľa?</i>
7.	PODPORA – HISTÓRIA PANELA: <i>Ponúka poskytovateľ cloudových služieb históriu panela stavu služby počas 365 dní?</i>
8.	PODPORA – CLOUDOVÝ PORADCA: <i>Ponúka poskytovateľ cloudových služieb službu, ktorá pôsobí ako cloudový expert pre potreby zákazníka a pomáha porovnávať využitie zdrojov s najlepšími postupmi?</i>
9.	PODPORA – TAM: <i>Ponúka poskytovateľ cloudových služieb technického manažera účtov (TAM), ktorý poskytuje technické odborné znalosti pre celý rozsah cloudových služieb?</i>
10.	PODPORA – PODPORA APLIKÁCIE TRETEJ STRANY: <i>Ponúka poskytovateľ cloudových služieb podporu pre spoločné operačné systémy a spoločné komponenty aplikačného zásobníka?</i>
11.	PODPORA – VEREJNÉ API: <i>Ponúka poskytovateľ cloudových služieb verejné aplikačné programovacie rozhranie (API), ktoré programovo spolupôsobí s prípadmi podpory pri vytváraní, editovaní a uzatváraní takýchto prípadov?</i>
12.	PODPORA – DOKUMENTÁCIA SLUŽBY: <i>Ponúka poskytovateľ cloudových služieb dobrú kvalitu, verejne prezerateľné technické dokumentácie pre všetky svoje služby vrátane, okrem iného, návodov, konzultačných hodín, často kladených otázok (FAQ) a poznámok k vydaniu?</i>
13.	PODPORA – DOKUMENTÁCIA CLI: <i>Ponúka poskytovateľ cloudových služieb dobrú kvalitu, verejne prezerateľnú technickú dokumentáciu pre svoje rozhranie príkazového riadku (CLI)?</i>

14.	PODPORA – REFERENČNÉ ARCHITEKTÚRY: <i>Ponúka poskytovateľ cloudových služieb voľnú on-line kolekciu referenčných architektonických dokumentov, aby pomohol zákazníkom pripraviť špecifické riešenia v kombinácii s mnohými cloudovými službami poskytovateľa cloudových služieb?</i>
15.	PODPORA – REFERENČNÉ ROZMIESTNENIA: <i>Ponúka poskytovateľ cloudových služieb voľnú on-line kolekciu dokumentov, ktorá obsahuje podrobné, testované a schválené postupy krok za krokom vrátane najlepšieho postupu, aby sa realizovali spoločné riešenia (t. j. DevOps, Big Data, Data Warehouse, Microsoft workloads, SAP workloads, atď.) v jeho cloudových ponukách?</i>

Príloha B – Technické hodnotenie naživo

Pri výbere CISP je dôležité posúdiť schopnosti cloudovej platformy „naživo“ pomocou verejne dostupných služieb a infraštruktúry CISP. Odporúčame aspoň 1 celý deň pre technické hodnotenie CISP z užišieho zoznamu. Počas hodnotenia môžete: 1) vykonať hĺbkové hodnotenie, aby sa posúdilo, či preukázané schopnosti spĺňajú vaše požiadavky RFP a písomné odpovede CISP, 2) poskytnúť platformu pre svojich expertov, aby preskúmali, či CISP zabezpečuje zladenie s vašimi technickými a organizačnými potrebami a 3) získať dôveru v služby CISP a schopnosť CISP škálovať, bezpečne pracovať, pracovať odolne a pokračovať v inováciách, aby sa splnili budúce potreby.

Keď CISP odpovedajú na požiadavky RFP na cloudové služby, môžu nastať komplikácie založené na vysokej úrovni interpretácie požiadaviek, ktorým chýba úplný kontext pracovného prostredia/aplikačných potrieb organizácie. Odporúčame vybrať členov komisie na technické hodnotenie naživo tak, aby zahŕňala vedúcich technických, prevádzkových, bezpečnostných a aplikačných odborníkov. Hodnotitelia by mali posudzovať CISP prostredníctvom hodnotenia a ako najlepší postup by ma hodnotiť CISP nezávisle, s hodnotiacimi scenármi na stupnici 0-4 (0 = neakceptovateľné, 1 = okrajové, 2 = akceptovateľné, 3 = dobré, 4 = vynikajúce). Potom sa môžu ukážkové hodnotenia konsolidovať s priemerným skóre pre každý hodnotiaci scenár rozšírený na celkové hodnotenie CISP. Scenáre s veľkou štandardnou odchýlkou by mali byť prediskutované hodnotiacim tímom pred konečným rozhodnutím. Po skonsolidovaní skóre sa môže použiť váženie založené na kritičnosti scenárov.

Z hľadiska rozsahu ukážok odporúčame holistický pohľad na platformu CISP a potom, po hlbšom preskúmaní, vyhodnotiť špecifické zaťaženia prebiehajúce na platforme. Nižšie je uvedený príklad hodnotenia platformy a záťaže. Organizácie môžu stavať na tomto základnom scenári alebo prispôbiť ho potrebám zákazníka, aby zabezpečili, že vybraná CISP spĺňa špecifické funkčné a nefunkčné požiadavky. Ako najlepší postup môžu dodávatelia, ktorí predložili zoznam scenárov a požiadaviek, navrhnuť program pre vyhodnotenie naživo, ktorý maximalizuje pokrytie a zahŕňa 20 % času otázok a odpovedí.

Hodnotenie platformy: Viaceré CISP prijali výraz „dobre navrhnutý“ vzťahujúci sa na prístup ku cloudu, ktorý poskytuje optimálnu hodnotu a minimálne riziko. Dobre navrhnuté scenáre v technickej ukážke naživo môžu zahŕňať:

1. **Bezpečnosť:** Identita, centralizovaná správa, automatická detekcia hrozieb, ochrana údajov, pripravenosť udalosti
2. **Účinnosť výkonu:** Správne dimenzovanie, škálovateľnosť/pružnosť, bez serveru
3. **Spôľahlivosť:** Vysoká dostupnosť (odolnosť proti poruchám), zníženie rizika zmeny, obnovenie po katastrofe, zálohovanie
4. **Riadenie nákladov:** Finančné operácie, komerčná optimalizácia, rozpočty a rozloženie nákladov
5. **Prevádzková excelentnosť:** Automatizácia, monitorovanie, podpora, riadenie a schopnosti požadované na migrovanie do cloudu a prevádzka v ňom

Hodnotenie pracovného zaťaženia: Spoločný súbor typov aplikácií, ktorý môže byť preukázaný zahŕňa:

- **Webová aplikácia:** Verejný hosting dynamických webových stránok vrátane backendovej databázy a ukladania statických objektov.
- **Analýza údajov:** Architektúra Data Lake alebo Lake House, ktoré umožňujú konsolidáciu údajov od poskytovateľov rozdielnych údajov a schopnosť zaobchádzať s vysokým objemom údajov (TB/PB údajov) a rýchlosť (rýchlosť generovania údajov, zmena a vzory kladenia otázok).
- **Platforma dátovej vedy:** Platforma, ktorá umožňuje vývoj, rozmiestnenie a používanie schopností založených na AI/ML vo vašej organizácii.
- **Aplikácia IoT:** Platforma/schopnosť, ktorá spája cloud, sieťovú schopnosť a zariadenia.

Pre každé reprezentatívne pracovné zaťaženie, dôležité pre vašu organizáciu, môžete definovať scenáre, ktoré majú byť predvedené CISP. Scenáre by mali preukázať celkové schopnosti, ktoré umožňujú rozmiestnenie pracovného zaťaženia dobre vytvoreným spôsobom. Ďalšie stránky obsahujú príklad kritérií technického hodnotenia naživo pre; 1) platformu CISP a 2) príklad pracovného zaťaženia webovej aplikácie.

Platforma – príklad technického hodnotenia naživo

ID scenára	Názov scenára	Kritičnosť (1 = nízka, 4 = kritická)	Požiadavky na preukazovanie	Pokyny pre hodnotenie
Bezp. platf. 1	Spojenie identít	4	Preukážte schopnosť federovania z existujúceho ukladacieho priestoru identít do cloudovej služby.	• Podpora pre štandardné protokoly, napríklad SAML. • Podpora pre replikáciu identity založenú na SCIM. • Schopnosť definovať rôzne úrovne prístupu v rámci podnikového ukladacieho priestoru identít a ich aplikácia v rámci poskytovateľa cloudových služieb. • Schopnosť obmedziť špecifické tímy/jednotlivcov iba na niektoré účty/projekty/pracovné zaťaženia. • Schopnosť podporovať kontrolu prístupu založenú na atribútoch (ABAC) a používať tieto atribúty v rámci identity poskytovateľa cloudových služieb a systému riadenia prístupu (IAM) na kontrolu prístupu do cloudových zdrojov.
Bezp. platf. 2	Centrálna správa	4	Preukážte schopnosť definovať postup a požiadavky centrálné, na úrovni organizácie (globálne postupy) a tiež na úrovni organizačného útvaru a projektu.	• Postup by mal zahŕňať: aktivovanie/deaktivovanie služieb, aplikovanie geografických obmedzení (limitované regióny). • Postupy by mali tiež obmedziť používateľov, vrátane správcov, pri blokovaní auditov/kontrol spravovania.
Bezp. platf. 3	Obmedzenie povolenia používateľa	3	Preukážte automatické odporúčania pre zúženie povolení používateľa.	• Schopnosť porovnávať existujúce povolenia s požadovanými povoleniami. • Automatické generovanie postupov na podporu minimálneho privilégia.
Bezp. platf. 4	Vedenie záznamov z auditu	4	Preukážte vedenie záznamov z auditu týkajúcich sa cloudovej činnosti vrátane povolených a nepovolených činností.	• Centralizované záznamy pre celú organizáciu. • Špecifické záznamy účtov/projektov na podporu nízkej úrovne sledovania a zodpovednosti. • Nástroje na umožnenie skúmania záznamov. • Nástroje, ktoré umožňujú spustiť činnosti založené na špecifických udalostiach/položkách záznamov. • Schopnosť prezerať podpornú činnosť dodávateľa. • Schopnosť zabrániť vymazaniu záznamov, dokonca aj správcami.
Bezp. platf. 5	Izolácia siete	4	Preukážte a doložte, ak je to možné, izoláciu nájomníkov v rámci cloudu. Preukážte konfiguráciu izolovaných	• Oddelenie nájomníkov vrátane VPN a prepojených sietí. • Schopnosť kontrolovať prevádzku zvonku cloudovej infraštruktúry (v prevádzkach), v rámci nej a na internete.

ID scenára	Názov scenára	Kritičnosť (1 = nízka, 4 = kritická)	Požiadavky na preukazovanie	Pokyny pre hodnotenie
			(bez prepojenia), súkromných (bez internetu) a verejných podsietí (s prístupom na internet).	Ako funguje oddelenie, keď sa používajú zdieľané služby, napríklad kontajnerové hostiteľské služby alebo funkcia ako služba.
Bezpečnosť. platf. 6	Šifrovanie na úložisku	4	Preukážte schopnosť šifrovania uložených údajov vrátane možnosti BYOK a šifrovania na strane klienta.	- Schopnosť požadovať šifrovanie citlivých údajov. - Schopnosť používať buď kľúče spravované poskytovateľom alebo kľúče spravované zákazníkom. - Dodržiavanie FIPS 140-2. - Schopnosť upozorniť na a zaznamenať nedodržanie požiadaviek šifrovania. - Vplyv dodatočných nákladov. - Vplyv výkonu. - Podpora algoritmov na preukázanie množstva a veľkosti kľúčov.
Bezpečnosť. platf. 7	Šifrovanie na ceste	4	Preukážte schopnosť šifrovať údaje na ceste.	- Štandardné šifrovanie pre službu API. - Schopnosť umožniť šifrovanie na ceste (TLS) na vyrovnávačoch zaťaženia a riadených API. - Podpora vzájomného overovania (klient a server).
Bezpečnosť. platf. 8	Správa kľúčov	4	Preukážte svoju schopnosť spravovať kľúče. Zahrňte celý životný cyklus kľúčov. Zahrňte integráciu s cloudovými službami.	Vytvorenie záznamu, používanie, striedanie a zničenie kľúčov.
Bezpečnosť. platf. 9	Riadenie konfigurácie	3	Preukážte svoje schopnosti riadenia konfigurácie cloudovej platformy.	- Udržiavajte presné CMDB. - Skontrolujte dodržiavanie. - Automaticky spustite činnosti založené na nedodržaní. - Schopnosť vyhodnotiť zmeny konfigurácie v porovnaní s najlepšimi postupmi alebo zákaznickými pravidlami.
Bezpečnosť. platf. 10	Bezpečnosť siete	3	Preukážte firewall webovej aplikácie a schopnosť firewallu vrátane integrácie s pravidlami tretej strany/firewallmi a ochranou proti masívnym útokom.	- Schopnosti WAF (firewall webovej aplikácie): škálovateľnosť. - Podpora súkromnej ako aj verejnej siete. - Schopnosť objednať si priemyselné/dodávateľské dodávky pre súbory pravidiel. - Automatické spustenie činností v rámci infraštruktúry založené na udalostiach z WAF. - Schopnosti firewallu, škálovateľnosť. - Firewall založený na hostiteľovi a sieti. - Schopnosť odvolávať sa na logické skupiny alebo objekty okrem schopnosti špecifikovať bloky CIDR IP.

ID scenára	Názov scenára	Kritičnosť (1 = nízka, 4 = kritická)	Požiadavky na preukazovanie	Pokyny pre hodnotenie
				- Počet pravidiel podporovaných na každej úrovni/komponente. - Schopnosť podporovať distribuovaný prevádzkový model (tím siete + tím zariadení) prostredníctvom postupu a konfigurácie siete.
Bezp. platf. 11	Prepojenosť siete	3	Preukážte schopnosť pripojiť sa k sieťam v prevádzkach, ako aj ku koncovým bodom/klientom súkromných sietí v rámci cloudu.	- Súkromná prepojenosť (veľmi široké pásmo > 10 GB). - Schopnosť podporovať vedenie a postupy firewallu v organizácii. - VPN prepojenosť (z miesta na miesto a s klientom). - Podpora IPV6.
Bezp. platf. 12	Riadenie inštancií	3	Preukážte schopnosti riadenia inštancií.	- Schopnosť monitorovať a riadiť stav dočasnej opravy veľkého objemu inštancií. - Podpora riadenia dočasnej opravy operačných systémov Linux a Windows. - Schopnosť vykonávať príkazy v skupine serverov bez potreby SSH. - Schopnosť centrálnne kontrolovať a vykonávať audit diaľkového prístupu k virtuálnym strojom. - Schopnosť meniť veľkosť inštancie, pripájať ďalšie objemy, meniť konfiguráciu siete atď. cez konzolu, CLI a API.
Bezp. platf. 13	Aplikácia postupu	3	Preukážte schopnosť konfigurovať služby, aby sa zabránilo prístupu z verejného internetu.	- Automatizované smerovanie prevádzky do zdravých hostiteľov. - Schopnosť definovať postupy, ktoré kontrolujú prístup k údajom, na základe zdrojovej siete. - Aplikácia týchto obmedzení prístupu na všetkých používateľov vrátane používateľov s vysokým stupňom poverení.
Bezp. platf. 14	Snímanie zraniteľnosti	2	Preukážte schopnosť snímať obrázky (kontajner VM) pre zraniteľnosti.	- Schopnosť automaticky snímať kontajnery v registri. - Schopnosť snímať virtuálne stroje pre známe zraniteľnosti. - Schopnosť vykonávať snímanie siete.
Bezp. platf. 15	Kontrola siete	2	Preukážte schopnosť zachytávať/odzrkadľovať prevádzku siete	Schopnosť odzrkadľovať časť/celú prevádzku v rámci infraštruktúry poskytovateľa cloudových služieb (z hľadiska nájomníka zákazníka) vrátane zachytenia celého paketu.

ID scenára	Názov scenára	Kritičnosť (1 = nízka, 4 = kritická)	Požiadavky na preukazovanie	Pokyny pre hodnotenie
			(NetFlow a plný paket) zo zákazníckeho prostredia.	- Schopnosť jednoducho vybrať, ktorú prevádzku chcete zachytiť. - Schopnosť škálovať veľmi veľké objem prevádzky (> 50 GBps).
Bezp. platf. 16	Definícia hrozby	3	Preukážte, že vaša platforma je schopná detekcie vniknutia, vrátane hrozieb zo siete, použitia poverení a využitia obrazovej analýzy ako príklad.	- Schopnosť zistiť podozrivé činnosti ako je „mínovanie“. - Schopnosť zistiť brutálne útoky na overovanie ako sú prihlásenia SSH. - Schopnosť zistiť únik alebo zneužitie poverení. - Aplikácia ML, analyzovanie veľkého počtu udalostí a surfovanie cez prioritizované udalosti. - Snaha umožniť/konfigurovať (jednoduché je lepšie). - Schopnosť integrovať sa s externými službami a spustiť oznámenia. - Schopnosť konfigurovať IDS na globálnej úrovni pre všetky projekt/účty.
Výk. platf. 1	Optimalizácia počítača	2	Preukážte automatické odporúčania pre optimalizáciu virtuálneho stroja a funkcie ako náklad na službu.	- Odporúčania založené na skutočnom využití a vzoroch pracovného zaťaženia. - Odporúčania zahŕňajú odhadované úspory a nahliadnutia do očakávanej úrovne zaťaženia/technických dôsledkov. - Optimalizácia by mala zahŕňať úspory a „výkonové riziko“, kde virtuálne stroje môžu napríklad byť poddimenzované.
Výk. platf. 2	Optimalizácia prostredia	2	Preukážte automatické odporúčania pre iné cloudové komponenty, ako sú vyrovnávače zaťaženia, zosieťovanie, databázy, ukladanie atď.	Odporúčania identifikujú úspory a možné príležitosti na účinnosť výkonu v iných komponentoch mimo hlavného počítača.
Výk. platf. 3	Automatické škálovanie počítača	4	Preukážte schopnosti automatického škálovania aplikácie používanej mimo vyrovnávača zaťaženia vo virtuálnom výpočtovom prostredí. Preukážte dostupné odlišné možnosti/prístupy a schopnosť spustiť iné (voliteľné) činnosti pred/po postupoch škálovania, ako je oznamovanie.	- Odlišné možnosti pre škálovanie, založené na spúšťaní, na čase, ručné alebo inteligentnejšie prístupy, ktoré používajú strojové učenie na predpovedanie požadovanej kapacity. - Plne automatizované škálovanie vrátane registrácie s vyrovnávačom zaťaženia a kontrolami dobrého stavu. - Schopnosť používať ľubovoľný kód na špecifických miestach životného cyklu škálovania.

ID scenára	Názov scenára	Kritičnosť (1 = nízka, 4 = kritická)	Požiadavky na preukazovanie	Pokyny pre hodnotenie
Výk. platf. 4	On-line škálovanie pre ukladanie	3	Preukážte schopnosť škálovať kapacitu a priepustnosť ukladania bloku bez prerušenia pracovnej záťaže.	- Schopnosť ukladania prechodného bloku medzi rôznymi typmi ukladania bez potreby úplne prebudovať služby. - Schopnosť zväčšiť veľkosť objemov predstavovaných VM.
Výk. platf. 5	Automatické škálovanie pre spravované služby	3	Preukážte schopnosť škálovania pre ukladanie objektov, sieťový priechod API, platformu FaaS a databázu NoSQL od niekoľkých (10) po veľké množstvo (1 000) súbežných používateľov.	- Hladké automatické škálovanie bez zásahu administrátora. - Konzistentný výkon počas rampového škálovania až do doby, keď sa vyrovná s požiadavkami na škálovanie produkcie. - Pre niektoré komponenty, napríklad FaaS, si všimnite možnosti predhrievania a riadenia limitov súbežného vykonávania, ak sú tiež potrebné.
Výk. platf. 6	Pracovné záťaž založené na kontajneri	3	Preukážte schopnosť hostiť pracovné záťaž založené na kontajneri.	- Možnosti pre platformy kontajnerových hostiteľských služieb. - Integrácia s inými komponentmi IaaS, napríklad s vyrovnávačmi zaťaženia. - Dostupnosť sieťového riešenia služby. - Nemajetkové možnosti pre kontajnerové hostiteľské služby, napríklad Kubernetes. - Prírodná podpora vysokej dostupnosti v rámci kontajnerovej kontrolnej hladiny. - Schopnosť riadiť kontajnerových hostiteľov.
Rel. platf. 1	Regionálna odolnosť	4	Preukážte automatizované zabezpečenie pred zlyhaním inštancie relačnej databázy v rámci regiónu, keď sa simuluje geograficky lokalizované zlyhanie (napríklad výpadok prúdu).	- Automatizované zabezpečenie pred zlyhaním. - Izolované poruchové zóny v rámci cloudového regiónu. - Jasne vymedzené a jednoducho navrhované pre vysokú dostupnosť.
Rel. platf. 2	Automatická obnova inštancie	2	Preukážte automatickú obnovu inštancie/súboru inštancií po zlyhanej kontrole stavu.	- Kontroly konfigurovateľného stavu. - Úplne automatizovaná obnova inštancií.
Rel. platf. 3	Povedomie stavu vyrovnávača zaťaženia	3	Preukážte, ako vyrovnávač zaťaženia automaticky zisťuje chybnú inštanciu a presmeruje prevádzku do iných zdravých hostiteľov.	- Kontroly konfigurovateľného stavu. - Automatizované vedenie prevádzky do zdravých hostiteľov.

ID scenára	Názov scenára	Kritičnosť (1 = nízka, 4 = kritická)	Požiadavky na preukazovanie	Pokyny pre hodnotenie
Rel. platf. 4	Zabezpečenie pred zlyhaním regiónu	3	Preukážte architektúru pre viac regiónov vrátane automatizovaného presmerovania prevádzky do druhého regiónu.	• Globálne povedomie o kontrolách stavu. • Možnosti automatického smerovania: oneskorenie, vážené a zabezpečenie pred zlyhaním. • Podpora pre pracovné zaťaženie virtuálneho stroja, ako aj spravované služby ako sú ukladanie objektov/služba databázy NoSQL.
Rel. platf. 5	Zálohovanie a obnova	4	Preukážte možnosti zálohovania a obnovy pre: virtuálny stroj, databázy, spravované služby.	• Úroveň automatizácie. • Možnosť obnoviť rovnaký/iný cloudový región. • Schopnosť kopírovania záloh do iného cloudového regiónu.
Nákl. platf. 1	Rozpočty	3	Preukážte schopnosť riadenia rozpočtu vrátane jeho štruktúrovania pre podúčty a projekty.	• Vezmite do úvahy schopnosť aplikovania rozpočtových kontrol a monitorovania na rôznych úrovniach vašej organizácie. • Skontrolujte flexibilitu, napríklad schopnosť zoskupiť komponenty (cez označovanie), nastavenie rozpočtov pre špecifické cloudové služby a konfigurovanie prahov pre upozornenia/monitorovanie.
Nákl. platf. 2	Pridelenie rozpočtu	1	Preukážte poskytnutie nového prostredia projektu (účet) vrátane postupu prideľovania rozpočtu pre projekt. Poskytovanie by malo zahŕňať krok ručného schvaľovania pre 1) technické preskúmanie/IT, 2) obchodné preskúmanie/financie.	• Schopnosť samofinancovania s príslušnými schváleniami. • Automatizácia konfigurácie s príslušným nastavením rozpočtu, oznámeniami alebo rozpočtovými postupmi vhodnými pre vašu organizáciu.
Nákl. platf. 3	Podávanie správ o rozpočte	2	Preukážte schopnosť podávať správy o rozpočte v organizácii. Podávanie správ pre konkrétne oddelenie v porovnaní s celou organizáciou (potreba poznať). Podávanie správ by malo zahŕňať „aktuálne“, ako aj predpovedané/odhadované hodnoty spotreby.	• Schopnosť poskytovať viditeľnosť na rôznych úrovniach organizácie, vytváranie povedomia a transparentnosti, ale na základe zásady potreby poznania. • Predpovedanie by malo byť založené na existujúcich a minulých trendoch spotreby a poskytovať včasné varovanie o možných prekročeníach rozpočtu.
Nákl. platf. 4	Kontroly rozpočtu	1	Preukážte schopnosť prijať opatrenia, keď sa dosiahne limit rozpočtu. Opatrenia by mali zahŕňať oznámenia,	• Schopnosť jednoducho definovať opatrenia na rôzne projekty.

ID scenára	Názov scenára	Kritičnosť (1 = nízka, 4 = kritická)	Požiadavky na preukazovanie	Pokyny pre hodnotenie
			aplikovaní obmedzení alebo aktívny zásah na zabránenie prekročenia rozpočtu.	- Schopnosť prijať opatrenia, ktoré sa líšia v závislosti od projektu, napríklad zohľadnenie rozvojových dôsledkov v porovnaní s výrobnými dôsledkami. - Schopnosť definovať viaceré opatrenia alebo prahy pre ten istý rozpočet/projekt. - Schopnosť definovať zákaznícke opatrenia ako doplnok štandardných schopností.
Nákl. platf. 5	Periodicita rozpočtu	1	Preukážte schopnosť aplikovať rozpočty na rôzne časové obdobia, denne/mesačne/ročne atď. Pre ročné rozpočty preukážte schopnosť aplikovať variabilnú distribúciu očakávaných výdavkov počas roka.	- Schopnosť definovať rozpočty pre rôzne časové obdobia. - Schopnosť konfigurovať distribúciu výdavkov počas roka pre ročné rozpočty, čo je dôležité najmä pre sezónne/veľmi pružné pracovné záťaž, napríklad ročné daňové priznanie.
Nákl. platf. 6	Marketplace tretej strany	3	Preukážte schopnosť kupovať a rozmiestňovať výrobky tretej strany. Preukážte, ako nastaviť rozpočet pre skupinu výrobkov tretej strany dostupných cez marketplace a tiež schopnosť obmedziť dostupné výrobky.	- Schopnosť nastaviť rozpočet pre konkrétny výrobok; globálny rozpočet, rozpočet pre skupinu projektov/účtov. - Schopnosť predložiť podskupinu širšieho marketplace cloudovým používateľom.
Nákl. platf. 7	Počítačové modely oceňovania	3	Preukážte rôzne modely oceňovania/komerčné modely, ktoré sa môžu aplikovať na virtuálne stroje.	- Schopnosti by mali zahŕňať nacenenie na vyžiadanie, bez povinnosti dlhodobého záväzku a podrobné ocenenie (za minútu/hodinu). - Voliteľné dlhodobé záväzky ako protihodnota za zľavu. - Schopnosť kupovať inštancie s ochotou akceptovať prerušenie ako protihodnotu za zľavu. - Je dôležité, aby bolo možné kombinovať tieto modely v rámci toho istého projektu/účtov a zdieľať aj výhody v rôznych účtoch.
Nákl. platf. 8	Odporúčania pre komerčnú optimalizáciu	3	Preukážte schopnosť prijímať odporúčania pre komerčnú optimalizáciu, aby ste optimalizovali výdavky (bez vykonania technických zmien).	- Holistické odporúčania pre viacnásobné služby, napríklad vrátane virtuálnych strojov a riadených databáz. - Schopnosť vykonať odporúčania jednoducho a pochopiť očakávané úspory/výhody.

ID scenára	Názov scenára	Kritičnosť (1 = nízka, 4 = kritická)	Požiadavky na preukazovanie	Pokyny pre hodnotenie
Nákl. platf. 9	Vyhradení hostiteľa	4	Preukážte schopnosť poskytnúť vyhradeného hostiteľa s cieľom umožniť používanie licencovania prevádzok, ktoré sú naviazané na konkrétneho hostiteľa.	• Uľahčenie poskytovania. • Schopnosť riadiť využívanie hostiteľa. • Schopnosť zdieľať hostiteľa v rôznych projektoch/vlastníctvach.
Op. platf. 1	Migrácia virtuálneho stroja	3	Preukážte import virtuálneho stroja z prevádzok do služby VM založenej na cloude.	• Schopnosť importovať operačné systémy Windows a Linux. • Schopnosť importovať viacero strojov naraz. • Schopnosť udržiavať replikačné relácie s cieľom umožniť rýchle „zabezpečenie pred zlyhaním“ do cloudu.
Op. platf. 2	Operácie zariadení (DevOps) a automatizované schopnosti	4	Preukážte svoje operácie zariadení/automatizované schopnosti vrátane definícií takých prostredí, ako sú kódy, podpora od plne automatizovaných nasadení, automatizované testovanie a odstránenia.	• Schopnosť definovať všetky komponenty systémov, ako sú kódy, vrátane siete, virtuálnych strojov, ukladania, databázy. • Schopnosť vytvoriť dátovod. • Schopnosť vytvoriť schránku kódov. • Schopnosť automatizovať vývoje. • Schopnosť vykonávať modré/zelené nasadenia. • Schopnosť vytvárať viaceré prostredia a mať viacero etáp nasadení. • Automatizované zrušenie zlyhaných nasadení
Op. platf. 3	Hostingové služby aplikácie	2	Preukážte hosting pre jednoduchú 2-vrstvovú aplikáciu v strojovom kóde/službe platformy. Vráťane relačnej databázy a automatického škálovania pre aplikáciu/webovú vrstvu.	• Jednoduchá konfigurácia cez UI. • Zahrnutie kontrol stavu, škálovania, vysokej dostupnosti. Podpora platformy, Windows, Linux.
Op. platf. 4	Integrácia bezpečnosti	2	Preukážte integračné schopnosti vašej platformy z hľadiska bezpečnostného incidentu a riadenia udalosti.	• Schopnosť ľahko integrovať a spotrebovať záznamy súvisiace s bezpečnosťou od poskytovateľa cloudových služieb + API pre integráciu.
Op. platf. 5	Integrácia ITSM	3	Preukážte integračné schopnosti vašej platformy z hľadiska ITSM (riadenie IT služieb).	• Schopnosť podporovať, monitorovať a aktualizovať podporu prípadu prostredníctvom API. • Schopnosť poskytovať služby alebo skupiny služieb ako „produkty“ prostredníctvom API.
Op. platf. 6	Podpora	4	Preukážte svoju ponuku podpory.	• Rôzne úrovne podpory pre rôzne typy pracovného zaťaženia. • Schopnosť podporovať operačný systém/databázový stroj atď. primerane pre danú službu.

ID scenára	Názov scenára	Kritičnosť (1 = nízka, 4 = kritická)	Požiadavky na preukazovanie	Pokyny pre hodnotenie
				- Schopnosť ponúkať jedinečnosť s menovitou podporou pre kritické pracovné zataženia. - Schopnosť ponúkať štruktúrovanú pripravenosť na udalosti a proces preskúmania architektúry. - Pohľad na cestnú mapu poskytovateľa.
Op. platf. 7	Schopnosť vykonávať audit	4	Preukážte nástroje, ktoré máte na podporu auditov zhody.	- Schopnosť získať podrobnosti o auditoch zhody cez konzolu. - Schopnosť riadiť a automatizovať audity prostredia.
Op. platf. 8	VM do kontajnera	1	Preukážte konverziu aplikácie na virtuálnom stroji na kontajner a obsluhu pomocou kontajnerovej platformy poskytovateľa cloudových služieb.	- Uľahčíte používanie konverzie. - Čas na konvertovanie. - Podpora platformy, .Net a Java.

Pracovné zataženie: webová aplikácia – príklad technického hodnotenia naživo

Nasledujúca sekcia poskytuje príklad hodnotiaceho záznamu pre konkrétne pracovné zataženie „webovej aplikácie“. Pri vypracúvaní hodnotiaceho záznamu pre danú aplikáciu sa dôrazne odporúča zapojiť používateľov aplikácie, vývojárov a administrátorov, pretože pravdepodobne najlepšie chápu požiadavky, aktuálne výzvy a obmedzenia.

ID scenára	Názov scenára	Kritickosť (1 = nízka, 4 = kritická)	Požiadavky na preukazovanie	Pokyny pre hodnotenie
Bezp.web. 1	Bezpečnosť - ochrana aplikácie	3	Preukážte svoju schopnosť blokovat' zlomyseľné pokusy využiť aplikáciu cez SQL Injection, útok XSS Scripting a iné útoky.	- Schopnosť chrániť proti bežným útokom „na bezprostredné použitie“ (out of the box) so štandardnými pravidlami/schopnosťami. - Schopnosť vytvoriť zákaznícke kontroly/pravidlá/funkcie.
Bezp.web. 2	Bezpečnosť - ochrana založená na rýchlosti	3	Preukážte svoju schopnosť blokovania/ochrany proti útokom zahŕňajúcim žiadosti o veľké rýchlosti alebo objemy údajov smerujúce k aplikácii.	Schopnosť konfigurovať limity a obmedzovať miery žiadostí z danej IP adresy alebo zoznamu adries.

ID scenára	Názov scenára	Kritickosť (1 = nízka, 4 = kritická)	Požiadavky na preukazovanie	Pokyny pre hodnotenie
Bezp.web. 3	Bezpečnosť - ochrana založená na zdroji	3	Preukážte schopnosť obmedziť prístup založený na sieti/geografickom zdroji.	- Schopnosť obmedziť sieťový blok alebo zoznam sieťových blokov. - Schopnosť obmedziť krajinu pôvodu (bez potreby riadiť IP zoznamy).
Bezp.web. 4	Bezpečnosť - segmentácia siete	4	Preukážte schopnosť izolovať/chrániť komponenty/webový server, aplikačný server/DB server na ochranu proti propagácii sever-juh a východ-západ cez infraštruktúru.	- Schopnosť umiestniť rôzne podsiete a kontrolovať prevádzkový tok medzi rôznymi podsietami. - Schopnosť kontrolovať prevádzkový tok na úrovni sieťového rozhrania. - Schopnosť odkazovania na logické skupiny, ako aj bloky CIDR.
Bezp.web. 5	Bezpečnosť - podpora TLS a riadenie certifikácie	4	Preukážte schopnosť dodávať koncový bod zabezpečený TLS a automaticky riadiť podporné komponenty, ktoré sú dodávané vrátane príkladu pre automatickú rotáciu certifikátov.	- Podpora pre najnovšie protokoly TLS a schopnosť vyradiť zdedené verzie, ak sa to požaduje. - Jednoduché vytváranie certifikátov, riadenie a rotácia (v ideálnom prípade plne automatizované).
Výk. web. 1	Výkon - škálovateľnosť	4	Preukážte svoju schopnosť škálovať od 10 do 100 000 súčasných používateľov webovej aplikácie prostredníctvom dynamického automatického škálovania.	- Schopnosť definovať pravidlá škálovania založené na čase a spúšťaní. - Hladké škálovanie pre koncových používateľov a administrátora. Automatické škálovanie smerom hore, keď sa záťaž zvyšuje a škálovanie smerom dolu, keď sa záťaž znižuje. - Zabezpečte, aby škálovanie existovalo v každej vrstve webovej aplikácie (vyrovnávač zaťaženia, webová vrstva, dátová vrstva atď.). - Dostupnosť služby ukladania do vyrovnávacej pamäte v rôznych vrstvách aplikácie v primeranej miere.
Výk. web. 2	Výkon - globálna dodávka	3	Preukážte svoju schopnosť CDN vrátane preukázania latentnosti z rôznych miest po celom svete vrátane Austrálie, Ázie, Afriky, Stredného Východu, Severnej Ameriky, Južnej Ameriky a Európy.	- Schopnosť vytvoriť a konfigurovať CDN prostredníctvom konzoly CISP/API. - Konfigurovateľné distribučné pravidlá pre rôzne geografie. - Konfigurovateľné ukladanie do vyrovnávacej pamäte pre rôzne prípady používania.
Spol. web. 1	Spoľahlivosť - odolnosť jedného regiónu	4	Preukážte schopnosť tolerovať a lokalizovať udalosť ako je napríklad strata pripojenia siete k dátovému centru CISP.	Automatizované zabezpečenie pred zlyhaním a vysoká dostupnosť v rámci cloudového regiónu (mesta).

ID scenára	Názov scenára	Kritickosť (1 = nízka, 4 = kritická)	Požiadavky na preukazovanie	Pokyny pre hodnotenie
Spol. web. 2	Spôľahlivosť - rozmiestnenie vo viacerých regiónoch	3	Preukážte rozmiestnenie webovej aplikácie vo viacerých regiónoch vrátane globálne replikovanej databázy.	- Schopnosť programovo rozmiestniť aplikáciu vo viacerých regiónoch. - Replikácia medzi regiónmi pre ukladanie údajov. - Automatizované nasmerovanie používateľov do ich optimálneho regiónu.
Spol. web. 3	Spôľahlivosť - zabezpečenie pred zlyhaním vo viacerých regiónoch	3	Preukážte automatizované zabezpečenie pred zlyhaním webovej aplikácie v prípade problému so službou s regionálnym dopadom.	Automatizované zabezpečenie pred zlyhaním a vysoká dostupnosť vo viacerých cloudových regiónoch.
Nákl. web. 1	Náklady - viditeľnosť	2	Preukážte schopnosť sledovať náklady na aplikáciu	Schopnosť prezerať históriu nákladov na konkrétnu aplikáciu, keď sa škáluje hore/dolu.
Nákl. web. 2	Náklady - rozpočet	2	Preukážte schopnosť nastaviť rozpočty a súvisiace upozornenia na aplikáciu.	Rozpočty konfigurované na aplikáciu a schopnosť spustiť akcie/upozornenia založené na konfigurovaných prahoch.
Op. web. 1	Operácie - okná údržby	3	Preukážte schopnosť konfigurovať údržby, aby ste sa vyrovnali s obchodnou požiadavkou, najmä keď môže mať údržba vplyv na dostupnosť aplikácie.	Konfigurovateľné okná údržby pre komponenty, ako je služba relačnej databázy.
Op. web. 2	Operácie - protokolovanie	3	Preukážte schopnosť centralizovať zaznamenávanie pre aplikáciu s viacerými komponentmi vrátane pretrvávania záznamov po ukončení/zlyhaní virtuálnych strojov.	- Schopnosť konfigurovať službu centralizovaného zaznamenávania, ktorá môže byť škálovaná s požiadavkami aplikácie. - Schopnosť definovať pravidlá/filtre na spustenie upozornení alebo opatrení založených na konkrétnych udalostiach záznamov.
Op. web. 3	Operácie - monitorovanie	3	Preukážte monitorovanie aplikácie vrátane výkonu, dostupnosti, časov reakcie, počtov chýb atď. a funkčnosti, aby sa vykonali oznámenia o krokoch/spustení založené na rôznych prahoch metrík.	- Dostupná zbierka štandardných metrík, napríklad disk IO, CPU, metriky databáz, sieť, vyrovnávač zaťaženia atď. - Schopnosť definovať špeciálne metriky, prahy. - Schopnosť vytvoriť špeciálny panel na reprezentovanie najdôležitejších metrík a zdieľanie týchto panelov s relevantnými používateľmi.