Nakupování cloudových služeb ve veřejném sektoru

Příručka – včetně vzoru Žádosti o podání nabídky (Request for Proposal – RFP) vedoucí k uzavření rámcové smlouvy o poskytování cloudových služeb

Verze 2: únor 2022

Poznámka

Tento dokument je poskytován pouze pro informativní účely. Nebyl vypracován v souladu s právními požadavky na zadávání veřejných zakázek v jakémkoli regionu. Za vlastní nezávislé posouzení informací uvedených v tomto dokumentu a za jakékoli použití produktů nebo služeb poskytovatele cloudových služeb nese odpovědnost zákazník. Tento dokument nevytváří žádné záruky, prohlášení, smluvní závazky, podmínky nebo přísliby.

Vzorové dokumenty a uvedené formulace nelze považovat za právní rady, pokyny ani formu poradenství. Zákazníci využívající cloudové služby se musí poradit s vlastními právními poradci ohledně povinností vyplývajících z platných zákonů v zemi, kde působí. Sdružení CISPE se výslovně zříká jakýchkoli záruk nebo odpovědnosti za škody související nebo přímo vyplývající z informací uvedených v tomto dokumentu.

O sdružení CISPE

CISPE (*Cloud Infrastructure Services Providers in Europe*, https://cispe.cloud) je neziskové a nezávislé oborové sdružení. Zastupujeme poskytovatele cloudových služeb v Evropě. Ve spolupráci s představiteli průmyslu a politickými zástupci jednotlivých zemí poskytujeme poradenství a vzdělávání v oblasti cloudových služeb. V neposlední řadě je naším cílem informovat společnost o roli cloudových služeb v současném průmyslu, veřejném životě a společnosti obecně.

Naše členská základna se neustále rozrůstá. Našimi členy jsou společnosti působící ve všech zemích EU a globální společnosti, jejichž sídlo se nachází v některé ze 16 evropských zemí. Do sdružení mohou vstoupit společnosti, které prohlásí, že alespoň jedna z jejich služeb splňuje požadavky Kodexu chování CISPE pro ochranu dat (dále jen Kodex). Naším cílem je:

- poukazovat na výhody systému zadávání veřejných zakázek prostřednictvím cloudové infrastruktury, a to v rámci EU a členských států EU,
- zapojit sektor cloudové infrastruktury do snahy o dosažení klimatické neutrality do roku 2030,
- propagovat a prosazovat technické standardy a požadavky na zabezpečení uplatňované Evropskou unií,
- podporovat komplexní požadavky na ochranu soukromí za pomoci Kodexu chování pro ochranu dat,
- usilovat o to, aby trh služeb cloudové infrastruktury v EU zůstal otevřený, konkurenceschopný a aby na něm nedocházelo k nekalým praktikám,
- v rámci právního prostoru EU bránit vzniku neodůvodněných povinností s ohledem na monitorování obsahu.

Členové našeho sdružení jsou staviteli a správci základních „stavebních kamenů IT“, které umožňují vládám, veřejným orgánům i firmám budovat vlastní systémy a poskytovat základní služby miliardám občanů. V rámci této role pomáháme rozvoji moderních technologií a služeb zahrnujících umělou inteligenci (AI), připojené objekty, autonomní vozidla, síť 5G a novou generaci technologie mobilního připojení.

Kodex chování pro poskytovatele služeb cloudové infrastruktury

Kodex, který byl veřejně představen v září 2016, vznikl ještě před zavedením obecného nařízení Evropské unie o ochraně osobních údajů (GDPR). Tento kodex je zcela v souladu s nařízením GDPR a pomáhá poskytovatelům cloudové infrastruktury dodržovat podmínky ochrany osobních údajů. Zároveň poskytuje bezpečný rámec, ve kterém mohou zákazníci vybírat poskytovatele cloudových služeb a důvěřovat jejich službám. Kodex chování CISPE byl ratifikován Evropským sborem pro ochranu osobních údajů (EDPB) v květnu 2021. Poté byl v červnu 2021 schválen francouzskou komisí CNIL v roli kompetentního orgánu. https://www.codeofconduct.cloud/

Pakt o klimaticky neutrálních datových centrech

Sdružení CISPE začalo na konci roku 2019 spolupracovat s Evropskou komisí s cílem vytvořit sadu metrik a samoregulační iniciativu, která by do roku 2030 pomohla zajistit klimatickou neutralitu datových center. Tato iniciativa byla vyvinuta společně s Evropskou asociací datových center (EUDCA) a dalšími obchodními sdruženími a subjekty na trhu datových center. Spuštěna pak byla v lednu 2021 s názvem „Pakt o klimaticky neutrálních datových centrech“. https://www.climateneutraldatacentre.net/

Iniciativa Fair Software

Společně s francouzským CIO sdružením CIGREF a s podporou dalších profesních CIO sdružení a poskytovatelů cloudové infrastruktury v Evropě vydalo sdružení CISPE 10 zásad spravedlivého licencování softwaru pro zákazníky cloudových služeb. Jde o soubor osvědčených postupů pro podniky, které chtějí

využít služeb cloudové infrastruktury pro růst v oblasti inovací a flexibility a které vyzývají dodavatele softwaru, aby zajistili spravedlivé licenční podmínky.
https://www.fairsoftware.cloud/

GAIA-X

CISPE je jedním z 22 zakládajících členů GAIA-X, evropské iniciativy usilující o vytvoření otevřeného, transparentního a bezpečného digitálního ekosystému. CISPE se od samého počátku hlásí k vizi a zásadám organizace GAIA-X. Důkazem toho je fakt, že generální tajemník sdružení byl v červnu 2021 znovu zvolen členem správní rady organizace GAIA-X. Tato příručka odkazuje na užitečné nástroje, kterými lze prokázat soulad se zásadami organizace GAIA-X. Jde například o Kodex chování CISPE týkající se ochrany dat a Kodex chování SWIPO IaaS. https://www.gaia-x.eu

CISPE a veřejný sektor

Sdružení CISPE přispívá k dialogu o evropské veřejné politice a usiluje o lepší pochopení přínosu, potenciálu a role, kterou hrají cloudové služby v rámci celé Evropy.

Modely řízení veřejných zakázek by měly být určujícím faktorem pro zavádění a používání cloud computingu (cloudových výpočetních operací). Pořizování cloudových služeb se totiž od většiny nákupů tradičních technologií, které veřejný sektor zná a používá, značně liší. Je třeba přehodnotit celkový přístup k zadávání veřejných zakázek: Sdružení CISPE proto vybízí politiky EU k vytvoření ambicióznějšího a perspektivnějšího přístupu, který podporuje iniciativy typu „cloud first“. Takový přístup pomůže růstu jednotného evropského trhu v cloudové infrastruktuře a podpoří ambici růstu jednotného digitálního trhu (DSM).

Cílem této příručky je poskytnout orgánům veřejné správy poradenství a podporu v oblasti nakupování cloudových služeb.

Další informace

Členové sdružení CISPE: https://cispe.cloud/members
Výkonná rada: https://cispe.cloud/board-of-directors
Služby v oblasti cloud computingu (cloudových výpočetních operací) deklarované v rámci Kodexu chování CISPE: https://www.codeofconduct.cloud/public-register/

Obsah

v2 2022 – únor

Shrnutí a účel této příručky

Účelem této **Příručky pro nakupování cloudových služeb** je poskytnout návod zákazníkům cloudových služeb, kteří chtějí nakupovat cloudové služby prostřednictvím výběrových řízení (vytvořením **Žádosti o podání nabídky na cloudové služby - Cloud Services Request for Proposal - dále jen RFP na cloudové služby**), ale nemají odborné znalosti pro vytvoření a uzavření Rámcové smlouvy o poskytování cloudových služeb (dále jen Rámcová smlouva).

Tento dokument je poskytován pouze pro informativní účely. Nebyl vypracován v souladu s právními požadavky na zadávání veřejných zakázek v dané zemi nebo oblasti.

Tato příručka zároveň slouží jako dodatečný zdroj výběrových kritérií pro **Objednávky** nebo **Výběrová řízení malého rozsahu** při nákupech vyplývajících z Rámcové smlouvy. Jednotlivé části příručky jsou uspořádány tak, aby byly v souladu s obecnými podmínkami RFP pro oblast IT. Vzory obecných RFP a znění výběrových kritérií jsou doplněny komentáři. Tyto komentáře pomáhají lépe pochopit rozdíly mezi tradičními IT technologiemi a cloudovými službami s ohledem na tvorbu RFP.

Strategie pro cloudové služby, kterou zveřejnila Evropská komise, popisuje způsob využití cloudových služeb pro modernizaci IT infrastruktury evropských institucí a agentur. Při příležitosti zveřejnění této strategie předali zástupci sdružení CISPE Evropské komisi tuto příručku. Stalo se tak v červenci roku 2019 během akce *„Jak transformovat státní správu prostřednictvím inteligentní cloudové politiky“*.

Verze 2 této příručky obsahuje nové pokyny týkající se ochrany dat (oddíl 2.3.1.1), změny poskytovatele cloudových služeb a přenosu dat (oddíl 2.3.1.2), podmínek používání softwaru (oddíl 2.5.2), udržitelnosti v oblasti cloudových služeb (oddíl 3.6) a aktualizovaný dodatek B Technické hodnocení „naživo“.

*Výraz **„Cloudové služby“** označuje všechny cloudové technologie a související služby, ke kterým může koncový uživatel potřebovat přístup. To zahrnuje konzultační nebo profesionální/spravované služby podpory a migrace do cloudu a podporu pro spouštění úloh v cloudu. Výraz také zahrnuje samotné cloudové infrastruktury a služby cloudového tržiště marketplace, jako jsou produkty typu Software jako služba (SaaS).*

Využití cloud computingu (cloudových výpočetních operací) jako výchozí volby řízení IT ve veřejném sektoru představuje příležitost k modernizaci stávajících strategií pro zadávání veřejných zakázek. Řízení nákupních procesů pomocí cloudových technologií umožní subjektům veřejného sektoru využívat všech výhod cloudu, mezi které patří přístup k nejmodernějším technologiím, vyšší rychlost a flexibilita, vyšší úroveň zabezpečení, efektivnější řízení souladu s předpisy, vyšší celková efektivita a úspora nákladů.

Tradiční postupy řízení oblasti IT pro nákup hardwaru, softwaru a datových center nejsou pro nákup cloudových služeb relevantní. Cenotvorba, řízení smluv a jejich podmínek, zabezpečení, technické požadavky, smlouvy SLA atd. – to vše se v modelu cloudových služeb mění. Použití stávajících metod zadávání zakázek tak v konečném důsledku snižuje nebo eliminuje výhody, které cloudová infrastruktura poskytuje.

Jedním z nejefektivnějších způsobů nakupování cloudových služeb ve veřejném sektoru je tzv. **Rámcová smlouva o poskytování cloudových služeb**. Jde o nabídku cloudových služeb více subjektů, ze které mohou oprávnění kupující přidružení k nakupující organizaci získat cloudové technologie a související služby, které vyhovují jejich potřebám. Tyto rámcové smlouvy umožňují nakupovat cloudové služby efektivním způsobem. Nakupující organizace a koncoví uživatelé tak mají přístup k celé škále cloudových služeb a v konečném důsledku využívají všech výhod cloudové infrastruktury, mezi které patří flexibilita, masivní úspory z rozsahu, škálovatelnost (díky které lze dosáhnout lepší dostupnosti při nižších nákladech), široké portfolio funkcí, rychlost inovací či schopnost škálovat na nové zeměpisné oblasti.

Vezměte prosím na vědomí, **že tento text se týká nákupu cloudových technologií v režimu Infrastruktura jako služba (IaaS) a Platforma jako služba (PaaS), které poskytuje *poskytovatel služeb cloudové infrastruktury (Cloud Infrastructure Services Provider - dále jen CISP)***. Tyto cloudové technologie lze zakoupit přímo od CISP nebo prostřednictvím jejich prodejců. *Pokud bychom uvažovali o distributorech služeb cloudového tržiště marketplace (PaaS a SaaS) a poradenských služeb v oblasti cloudových služeb, bylo by nutné při tvorbě RFP vzít do úvahy další aspekty, které zde nejsou popsány.*

Je třeba vzít také na vědomí, že tento dokument se nezabývá všemi aspekty tvorby komplexního rámce pro zadávání zakázek v cloudu. Pro tento účel existuje celá řada dalších dokumentů vytvořených odborníky a analytiky. Tyto dokumenty se zabývají otázkami, jako jsou osvědčené postupy pro nakupování cloudových služeb, způsoby jejich rozpočtování, správa cloudových služeb atd. Důrazně proto doporučujeme, abyste se při vytváření celkové strategie pořizování cloudových služeb řídili také těmito dalšími relevantními podklady. **Tabulka 1** níže uvádí přehled částí příručky, které se týkají tvorby RFP. Zároveň uvádí místa, kde se nacházejí znění RFP pro konkrétní komponenty cloudových služeb.

Tabulka 1 – Přehled částí příručky pro tvorbu RFP na cloudové služby

Část	Přehled a vzor znění RFP
1.0 Přehled Rámcové smlouvy	Souhrnný pohled na model rámcové smlouvy (TYPY SLUŽBY, způsoby soutěžení a uzavírání smluv).
2.0 Přehled RFP na cloudové služby	Vzorové obecné znění RFP pokrývající níže uvedené části. Obsahuje komentáře vysvětlující strukturu a formulace použité při tvorbě RFP na cloudové služby.
2.1 Nastavení RFP na cloudové služby	2.1.1 Úvod a strategické cíle 2.1.2 Časová osa odezvy na RFP 2.1.3 Definice 2.1.4 Podrobný popis nákupního modelu a soutěžení za podmínek Rámcové smlouvy 2.1.5 Minimální požadavky na uchazeče – administrativa
2.2 Technická specifikace	2.2.1 Minimální požadavky 2.2.2 Porovnání dodavatelů 2.2.3 Uzavírání smluv
2.3 Bezpečnost	2.3.1 Minimální požadavky 2.3.1.1 Ochrana dat 2.3.1.2 Změna poskytovatele cloudových služeb a přenos dat 2.3.2. Porovnání dodavatelů 2.3.3 Uzavírání smluv

Část	Přehled a vzor znění RFP
2.4 Ceny	2.4.1 Minimální požadavky 2.4.2 Porovnání dodavatelů
2.5 Uzavření smlouvy a smluvní podmínky	2.5.1 Smluvní podmínky 2.5.2 Podmínky použití softwaru 2.5.3 Postup výběru mezi vybranými dodavateli 2.5.4 Zahájení a ukončení spolupráce
3.0 Osvědčené postupy a získané zkušenosti	3.1 Řízení cloudových služeb 3.2 Sestavení rozpočtu 3.3 Porozumění obchodnímu modelu zahrnujícímu partnery 3.4 Zprostředkovatelé cloudových služeb 3.5 Příprava na žádost RFP a průzkum trhu 3.6 Udržitelnost
Dodatek A – Technické požadavky pro porovnání dodavatelů	Seznam obecných požadavků na cloudové technologie pro objednávky nebo výběrová řízení malého rozsahu.
Dodatek B – Technické hodnocení „Naživo“	Vzorový skript pro hodnocení ukázky cloudové technologie (cloudové demoverze poskytované v rámci objednávky nebo výběrových řízení malého rozsahu).

1.0 Přehled Rámcové smlouvy

Dobře navržená Rámcová smlouva může zajistit nakupování cloudových služeb způsobem, který je výhodný jak pro zúčastněné organizace veřejného sektoru, tak pro dodavatele cloudových technologií. Mezi výhody dobře navržené rámcové smlouvy patří:

- Přirozené prostředí pro spolupráci:
    - Spojení více organizací, které na základě podobných požadavků zadávají společně objednávky, znamená větší pohodlí, vyšší efektivitu, snížení nákladů a také zjednodušení procesu objednávání. Přináší to také možnost účinně agregovat poptávku více organizací z veřejného sektoru po společných cloudových technologiích a souvisejících službách, jako jsou řešení pro tržiště marketplace či poradenství.
- Kompletní nabídka cloudových služeb:
    - Kromě služeb tržiště marketplace a cloudových technologií dodaných ze strany CISP mohou do rozsahu služeb patřit i veškeré poradenské/profesionální/spravované služby potřebné pro podporu a realizaci migrace do cloudu a podporu úloh v cloudu.
    - Cloudové technologie lze zakoupit přímo od CISP nebo prostřednictvím jejich prodejců.
- Výhodný typ smluvní spolupráce:
    - Rámcová smlouva sjednocuje různé organizace/nákupčí, kteří hledají stejné obchodní podmínky, pod jednu hlavní smlouvu. Tím odpadá potřeba tvorby většího množství smluv a smluvních vztahů.
    - Tento typ spolupráce je přínosem také pro dodavatele, protože zaručuje standardní nákupní proces, jednotné podmínky a mechanismus objednávání. Dodavatelé tak nemusí u každé organizace veřejného sektoru vytvářet unikátní způsob nabízení svých služeb.
    - Tento smluvní vztah nabízí vysokou míru flexibility. Tvorba, schvalování a řízení efektivní smlouvy o poskytování cloudových služeb v souladu se stávajícími postupy/nařízeními jednotlivých vlád vyžaduje experimentování a schopnost rychlého přizpůsobení. Je proto mnohem výhodnější vytvořit rámcovou smlouvu, která umožní organizacím ve veřejném sektoru a dodavatelům cloudových služeb spolupracovat a řídit si smluvní podmínky podle potřeby – smluvně, mechanicky a efektivně. Smlouva na více let, která přestane být funkční a nelze ji upravit, se stane příčinou nespokojenosti koncových uživatelů ve veřejném sektoru, zadavatelů veřejných zakázek ale i samotných dodavatelů cloudových služeb.
- Volba:
    - Kupující si mohou vybrat mezi více kvalifikovanými CISP. Celý systém tak nastavuje vysokou laťku pro všechny cloudové a související služby, jako jsou například cloudová tržiště marketplace PaaS/SaaS a poradenské služby v oblasti cloudových služeb.
    - Tento typ smluvního vztahu umožňuje kontrolovat větší množství dodavatelů. Celý systém totiž umožňuje náležité prověření standardů každého vybraného dodavatele.

Rámcová smlouva nabízí největší přidanou hodnotu, pokud zahrnuje základní technologie typu IaaS/PaaS od CISP, řešení tržiště marketplace typu PaaS/SaaS, a také poradenské služby, které mohou koncoví

uživatelé z veřejného sektoru kdykoli využít a které jim pomohou s plánováním, přechodem, využíváním a údržbou úloh v cloudu. Z tohoto důvodu navrhujeme, aby byla RFP vedoucí k uzavření Rámcové smlouvy rozdělena na tři části, jak je uvedeno níže:

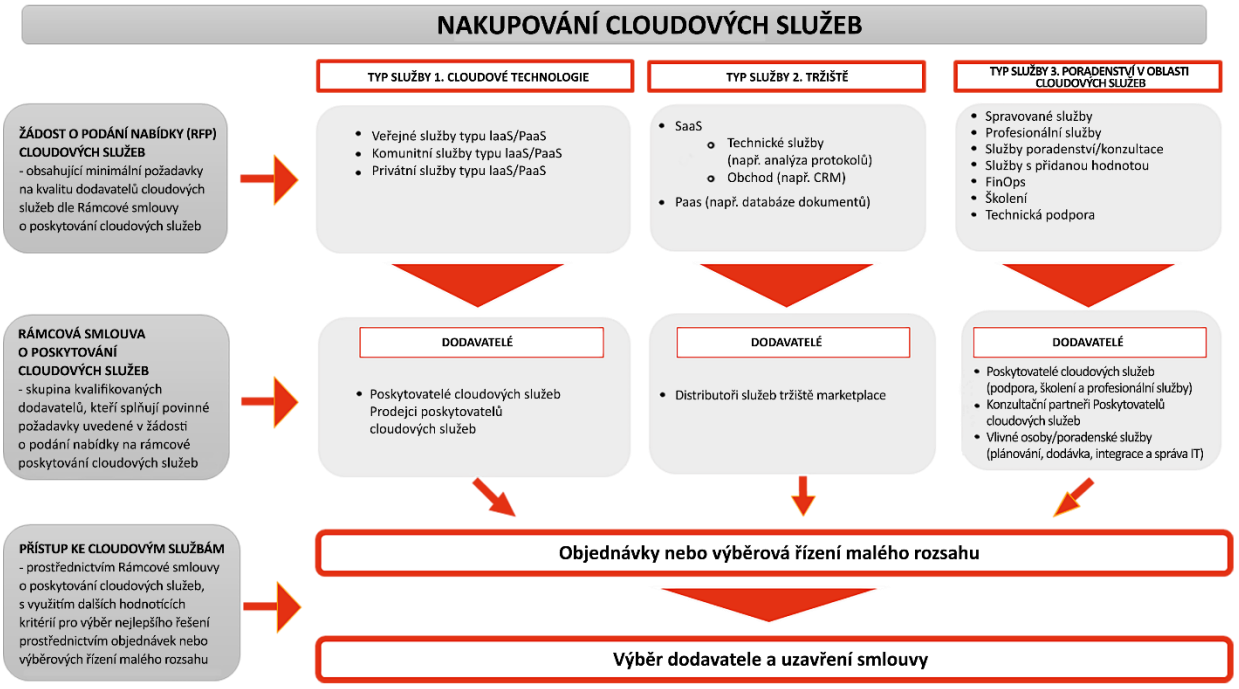
- TYP SLUŽBY 1 – CLOUDOVÉ TECHNOLOGIE
  Cloudové technologie lze nakupovat přímo od CISP nebo prostřednictvím určených prodejců CISP.

- TYP SLUŽBY 2 – TRŽIŠTĚ MARKETPLACE
  Přístup na tržiště marketplace se službami typu PaaS a SaaS.

- TYP SLUŽBY 3 – PORADENSKÉ SLUŽBY V OBLASTI CLOUDOVÝCH SLUŽEB
  Poradenské služby v oblasti cloudových služeb (školení, odborné služby, spravované služby atd.) a technická podpora.

*Jak již bylo uvedeno, tento dokument se zaměřuje na nákup cloudových technologií typu IaaS a PaaS (**TYP SLUŽBY 1**), které poskytují dodavatelé CISP (a které jsou zakoupené přímo od CISP nebo prostřednictvím prodejců CISP). Pro dodavatele u TYPŮ SLUŽBY 2 a 3 by v rámci RFP na cloudové služby bylo nutné stanovit samostatné kvalifikační požadavky.*

Obrázek 1 níže poskytuje celkový pohled na správnou strukturu RFP na cloudové služby. Žádost je rozdělena na tři typy služeb a vede k uzavření Rámcové smlouvy, která subjektům veřejného sektoru poskytne potřebnou flexibilitu (po technické i smluvní stránce), přehled a kontrolu nad výdaji a využíváním cloudu a navíc jim zpřístupní všechny cloudové služby potřebné k vytvoření a údržbě řešení, která potřebují.



Obrázek 1 – Dobře připravená a úspěšná RFP na cloudové služby je rozdělena na 3 části (typy služeb). Každý typ služby dále obsahuje kategorie neboli vlastní „typy nabídek" v rámci daného typu služby. Tyto kategorie slouží ke zpřesnění a zajištění technické a smluvní shody s požadavky koncových uživatelů při nákupu mimo Rámcovou smlouvu.

Vezměte prosím na vědomí, že:

- Každý typ služby podléhá výběru více dodavatelů.
- U TYPU SLUŽBY 3 lze výběr dodavatele a zadání zakázky provádět prostřednictvím jiných RFP nebo také prostřednictvím existující smlouvy na poradenské služby.

Kategorie TYPU SLUŽBY 1

U dobře připravené a úspěšné Rámcové smlouvy jsou CISP vyzváni k tomu, aby popsali model cloudu, který nabízejí, a rozdělili jej do kategorií v rámci každého typu služby. Doporučujeme používat průmyslový standard pro cloud computing (cloudové výpočetní operace) Základní charakteristiky cloudu Národního institutu standardů a technologie (NIST), a to zejména pro definování termínů **veřejný** cloud, **komunitní** cloud a **privátní** cloud. Takto strukturovaná rámcová smlouva poskytuje agenturám a veřejným subjektům, které v daném rámci nakupují, možnost výběru z různých modelů cloudu podle svých potřeb.

V části 2.1.3 Definice naleznete definice standardu NIST pro každý model cloudu u TYPU SLUŽBY 1 (veřejný IaaS/PaaS, komunitní IaaS/PaaS a privátní IaaS/PaaS).

Jak soutěžit – objednávky nebo výběrová řízení malého rozsahu?

Kvalifikační kritéria pro RFP na cloudové služby by měla zahrnovat kritické prvky a minimální standardy. Neměla by obsahovat standardy, které by „byly fajn, ale nejsou nezbytně nutné“. Přidání dodatečných standardů nad rámec těch potřebných a základních může vést k tomu, že někteří dodavatelé nebudou schopni podat nabídku. To v konečném důsledku povede ke zbytečnému snížení počtu dodavatelů a menšímu výběru pro kupující.

Na základě RFP a následného nastavení Rámcové smlouvy si mohou subjekty veřejného sektoru, které jsou součástí smluvního rámce, vyžádat nebo „objednat“ (call off) cloudové služby, které potřebují. Při vytvoření objednávky na základě rámcové smlouvy mohou kupující upřesnit své požadavky pomocí dodatečné funkční specifikace. Zároveň si však kupující zachovávají výhody nabízené v rámci Rámcové smlouvy.

Pokud to bude považováno za nutné, je možné uspořádat výběrové řízení malého rozsahu s cílem určit nejlepšího dodavatele pro určité aplikace nebo projekty. Výběrové řízení malého rozsahu je proces, při kterém zákazník realizuje další soutěž na základě Rámcové smlouvy. Tuto soutěž spouští tak, že vyzve všechny dodavatele v rámci jednoho typu služby, aby odpověděli na soubor požadavků. Zákazník vyzve všechny schopné dodavatele v rámci daného typu služby k podání nabídky. U daného typu služby hrají nyní důležitou roli minimální požadavky, které splňují dodavatelé vybraní v rámci RFP na cloudové služby. Tím je zajištěn vysoký standard všech nabízených variant pro každý typ služby.

*Vezměte prosím na vědomí, že je velice důležité, aby pro každý typ služby (jak je uvedeno na obrázku 1 výše) byly k dispozici **odlišné soubory smluvních podmínek**. Přístup typu „jedna smlouva na všechny typy služeb“ povede nutně k problémům s technickou proveditelností a kompatibilitou.*

2.0 Přehled RFP na cloudové služby

Tato část popisuje model a rozsah RFP na cloudové služby, včetně strategických cílů, účastníků, definic, časového harmonogramu a minimálních administrativních požadavků. Znovu upozorňujeme, že tato příručka se zaměřuje na TYP SLUŽBY 1 – CLOUDOVÉ TECHNOLOGIE.

2.1 Nastavení RFP na cloudové služby

Zástupcům subjektů veřejného sektoru důrazně doporučujeme, aby si již na počátku tvorby RFP na cloudové služby ujasnili své hlavní cíle a požadavky.

2.1.1 Úvod a strategické cíle

Aby bylo od samého počátku jasné, jakých strategických cílů chce zadavatel dosáhnout, je vhodné si na samotném počátku tvorby RFP na cloudové služby formulovat následující: **(1)** obchodní cíle a benefity, kterých chce organizace s využitím cloudových služeb dosáhnout; **(2)** strukturu rámcové smlouvy – tzn. kdo nakupuje, kdo provozuje, kdo sestavuje rozpočet atd.; **(3)** jak zadavatel chápe model sdílené odpovědnosti mezi veřejným sektorem a dodavateli cloudových služeb, protože právě dobře nastavený model je základem úspěšného nákupu a využívání cloudu, a **(4)** typ vztahu mezi CISP, distributory služeb tržiště marketplace, partnery v oblasti poradenství, státními subjekty/státními smluvními agenturami a koncovými uživateli ve veřejném sektoru. Pokud zadávající organizace dobře formuluje tyto čtyři body, může vytvořit RFP, která bude přesně odpovídat jejím potřebám. Navíc tím dává všem zúčastněným stranám jasně najevo, co od podání RFP očekává.

RFP na cloudové služby se podstatně liší od tradičních RFP na IT služby. Cloudová technologie není jen pouhou náhradou tradičních výpočetních metod, ale představuje zcela nový způsob využívání technologií. Dobře vytvořené RFP na cloudové služby mohou urychlit přechod na cloudové technologie. Díky tomu budou moci subjekty veřejného sektoru bez zbytečného odkladu užívat jejich výhod.

Pokud chceme porozumět všem aspektům nákupu cloudových služeb, je dobré znát všechny osvědčené postupy. A ze všech dostupných postupů správné praxe je nejlepší začít modelem sdílené odpovědnosti. Model sdílené odpovědnosti[1] je většinou zmiňován, když hovoříme o bezpečnosti a dodržování předpisů v prostředí cloudu. Tento model rozdělení odpovědností se však týká všech aspektů cloudových technologií. V RFP by mělo být jasně uvedeno, co má v cloudovém prostředí zůstat v kompetenci CISP a co je odpovědností zákazníka. CISP může například poskytovat funkce pro monitorování zdrojů a aplikací, které běží v cloudu, ***ale*** je jen na samotném zákazníkovi, aby tyto funkce, které CISP poskytuje, skutečně využíval. Není totiž v silách CISP, který funguje v masovém měřítku, aby tuto službu zajišťoval pro miliony zákazníků.

Zákazníci, kteří kupují cloudové služby, by také měli mít jasné povědomí o tom, jak jim může partnerská síť CISP pomoci s využíváním služeb cloudu a řízením jejich povinností. Poskytovatel cloudových spravovaných služeb (MSP) může například pomoci zákazníkovi nakonfigurovat a používat funkce monitorování od CISP tak, aby tyto funkce splňovaly jedinečné požadavky zákazníka na audit a shodu s předpisy.

[1] Viz část 5 Kodexu chování CISPE pro poskytovatele služeb cloudové infrastruktury: https://cispe.cloud/website_cispe/wp-content/uploads/2017/06/Code-of-Conduct-27-January-2017-corrected-march-20.pdf

Zjednodušeně řečeno jsou odpovědnosti v tomto modelu cloudu rozděleny takto:

CISP poskytuje cloudovou technologii.

Zákazník používá cloudovou technologii.

Poradenské firmy (pokud jsou jejich služby využívány) pomáhají zákazníkovi s přístupem a používáním cloudové technologie.

> ***„Poradenské firmy“*** *poskytují odborné a spravované služby, které pomáhají zákazníkům navrhovat, projektovat, sestavovat, migrovat a spravovat jejich úlohy a aplikace v cloudu. Mezi tyto firmy patří systémoví integrátoři, strategické poradenské společnosti, agentury, poskytovatelé spravovaných služeb a prodejci s přidanou hodnotou.*

Představte si „nakupování“ cloudových služeb jako obdobu nakupování ve velkém železářství. Máte k dispozici širokou nabídku materiálů a nástrojů pro stavbu čehokoli, co potřebujete. Můžete si postavit skříň, bazén nebo celý dům, je to jen a jen na vás. Jakmile si koupíte materiál a nářadí, zaměstnanci železářství vám mohou poskytnout poradenské služby a své odborné znalosti, nemohou ale přijít k vám domů a nic za vás nepostaví. Máte tedy několik možností, jak postupovat:

1. Můžete si koupit materiál a nářadí a postavit si sami, co potřebujete.
2. Nebo si koupíte materiál a nářadí a najmete si někoho, kdo za vás něco postaví a/nebo to bude provozovat.
3. Také můžete uzavřít smlouvu s někým, kdo pro vás něco postaví/bude provozovat, a zároveň se s ním domluvíte, že vám poskytne veškerý materiál a nástroje jako součást své komplexní nabídky.

Pokud má daná organizace vlastní lidi s potřebnými dovednostmi a dokáže vytvořit a spravovat své cloudové prostředí a řešení, pak skutečně potřebuje pouze přístup ke standardizovaným cloudovým technologiím a nástrojům. Ty získá přímo od CISP nebo prodejců zastupujících CISP – viz **TYP SLUŽBY 1**. Potřebný software typu SaaS a PaaS by měl být dostupný na cloudovém tržišti marketplace (**TYP SLUŽBY 2**). Pokud je zapotřebí následné poradenství, migrace, implementace a/nebo pomoc při správě, přichází na řadu partnerská síť CISP (**TYP SLUŽBY 3**).

Vzor znění RFP: Úvod a strategické cíle

Cloud computing (cloudové výpočetní operace) poskytuje subjektům z veřejného sektoru rychlý přístup k široké škále flexibilních a nízkonákladových IT zdrojů v modelu pay-as-you-use (placení podle spotřeby). Organizace si tak mohou zaplatit potřebný typ a objem prostředků, které potřebují k realizaci svých cílů nebo k provozu svých IT oddělení. Tento způsob nákupu eliminuje nutnost velkých investic do hardwaru a/nebo dlouhodobých licenčních smluv na software.

<ORGANIZACE> *formuluje požadavek na přístup k těmto typům komerčně dostupných cloudových technologií, aby dokázala uspokojit své obchodní potřeby v rámci širokého spektra přidružených organizací.*

Hlavním cílem této RFP je uzavření nevýhradní paralelní ***<RÁMCOVÉ SMLOUVY>*** *až s* ***<x>*** *poskytovateli různých cloudových technologií a souvisejících služeb.*

1. ***TYP SLUŽBY 1**. Poskytovatelé cloudových služeb (CISP) nebo jejich prodejci nabízejí cloudové technologie.*
2. ***TYP SLUŽBY 2.** Poskytovatelé služeb tržiště marketplace.*
3. ***TYP SLUŽBY 3.** Poskytovatelé poradenských služeb, kteří prodávají odborné znalosti potřebné pro migraci a používání služeb nabízených ze strany CISP.*

*V rámci **TYPU SLUŽBY 1** musí nabízející organizace (CISP nebo prodejci CISP) prokázat, jak a zda jejich nabídka splňuje následující cíle:*

- ***Flexibilita –** zpřístupnění zdrojů IT koncovým uživatelům v řádu minut namísto týdnů a měsíců.*
- ***Inovace –** okamžitý přístup k nejnovějším a nejinovativnějším technologiím na trhu.*
- ***Náklady –** výměna kapitálových výdajů za provozní náklady (např. CapEx za OpEx). Platí se pouze za to, kolik se spotřebuje.*
- ***Rozpočtování –** zobrazení informací o vyúčtování a využívání na detailní i souhrnné úrovni, vizualizace vzorců výdajů v průběhu času a předpověď budoucích výdajů.*
- ***Elasticita –** dosažení nižších variabilních nákladů díky úsporám z rozsahu, které cloud poskytuje.*
- ***Kapacita –** eliminace odhadů v oblasti kapacitních potřeb infrastruktury.*
- ***Konec spoléhání se na datová centra –** zaměření se na práci pro občany a ne na těžkou práci spojenou se stavbou a napájením serverů.*
- ***Zabezpečení –** formální navrhování účtů s větší mírou viditelnosti a auditovatelnosti zdrojů a eliminace nákladů na ochranu zařízení a fyzického hardwaru.*
- ***Sdílená odpovědnost –** CISP je schopný převzít náročný provoz, správu a řízení komponent infrastruktury od hostitelského operačního systému a virtualizační vrstvy až po fyzické zabezpečení zařízení, ve kterých služby fungují.*
- ***Automatizace –** CISP dokáže v rámci cloudové architektury automatizovat konkrétní procesy, které umožní rychlé, nákladově efektivnější a bezpečné škálování služeb.*
- ***Řízení cloudových služeb –** postup řízení by měl být následující: (1) úplný soupis všech IT prostředků; (2) centrální správa všech prostředků; (3) vytváření upozornění týkajících se používání/účtování/zabezpečení atd. – to vše s funkcemi pro sledování prostředků, správu inventáře, změn, protokolů, analýzu protokolů, celkový přehled a správu cloudu.*
- ***Kontrola –** získání úplného přehledu o tom, jak jsou služby IT využívány a kde je prostor pro jejich vyladění z hlediska bezpečnosti, spolehlivosti, výkonu a nákladů.*
- ***Reverzibilita –** nástroje a služby přenositelnosti, které usnadňují migraci do infrastruktury CISP a mimo ni, minimalizují riziko uzamčení dodavatele a respektují kodex(y) chování platné pro dané odvětví.*
- ***Ochrana dat –** schopnost prokázat soulad s obecným nařízením o ochraně osobních údajů (GDPR) prostřednictvím kodexu chování pro poskytování služeb cloudové infrastruktury: Kodex chování CISPE pro ochranu dat.*
- ***Transparentnost –** zákazníci by měli mít právo znát umístění infrastruktur používaných ke zpracování a ukládání svých dat (na úrovni městské oblasti).*
- ***Klimatická neutralita –** zákazníci by měli spolupracovat s CISP, kteří podnikají konkrétní kroky vedoucí k dosažení cílů klimatické neutrality do roku 2030 a kteří jsou signatáři Paktu o klimaticky neutrálních datových centrech. Takoví poskytovatelé pomohou zákazníkům při plnění jejich vlastních cílů klimatické neutrality.*

2.1.2 Časová osa odezvy na RFP

Při vytváření rámcové smlouvy a související RFP na cloudové služby je dobrou praxí pro uchazeče definovat časový plán předpokládaných činností. Čím více odborníků z odvětví cloudových služeb do tohoto procesu zapojíte, tím lepší bude výsledek. Pomůžete tak zajistit, aby všechny strany jasně chápaly všechny aspekty RFP a také způsob, jakým všechny služby dodavatele zapadají do modelu cloudových služeb.

Vezměte na vědomí, že časová osa procesu RFP podléhá také místním zákonům a právním závazkům. Níže uvedený seznam je proto zamýšlen jako vodítko obsahující osvědčené postupy, nikoli jako normativní seznam předepsaných aktivit a časových rámců.

Vzor znění RFP: Časová osa odezvy

Níže jsou uvedeny jednotlivé milníky časové osy pro RFP na cloudové služby:

Časová osa RFP na cloudové služby
• *Zveřejnění žádosti o informace (RFI):* • *Odezva na RFI:* • *Zveřejnění návrhu RFP:* • *Termín odezvy na návrh RFP:* • *Fáze odborných konzultací: <termíny>* • *Zveřejnění předkvalifikační RFP:* • *Odezva na předkvalifikační RFP:* • *Zveřejnění RFP:* • *Termín pro 1. kolo podání dotazů:* • *Odpovědi pro 1. kolo:* • *Termín pro 2. kolo podání dotazů:* • *Odpovědi pro 2. kolo:* • *Termín odezvy na RFP:* • *Období pro objasnění nejasností v nabídkách:* • *Období vyjednávání:* • *Datum zamýšleného výběru dodavatele:* • *Uzavření smlouvy:* • *Doba trvání smlouvy (možnost prodloužení):*

Vezměte na vědomí, že časová osa procesu RFP podléhá také místním zákonům a právním závazkům. Níže uvedený seznam je proto zamýšlen jako vodítko obsahující osvědčené postupy, nikoli jako normativní seznam předepsaných aktivit a časových rámců.

2.1.3 Definice

Žádost o podání RFP na cloudové služby by měla obsahovat podrobný seznam definic. Tento seznam by měl zahrnovat role dodavatele (např. poskytovatel cloudových služeb, prodejce cloudových služeb, partner dodavatele), obecné technologické koncepty (výpočetní prostředky, úložiště, IaaS/PaaS, SaaS) a další klíčové části smlouvy. Níže je uveden vzorový seznam definic:

Vzor znění RFP: Definice

Níže uvedené definice jsou definicemi platnými pro cloud computing (cloudové výpočetní operace) dle Národního institutu standardů a technologie (NIST).[2]

- ***Infrastruktura jako služba (IaaS).*** *Tato platforma poskytuje spotřebitelům výpočetní, úložné, síťové a další základní výpočetní zdroje, se kterými je spotřebitel schopen nasadit a provozovat libovolný software zahrnující operační systémy a aplikace. Spotřebitel neprovádí správu ani řízení základní cloudové infrastruktury, má však kontrolu nad operačními systémy, úložišti a nasazenými aplikacemi a případně také omezenou kontrolu nad vybranými síťovými komponentami (např. hostitelskými bránami firewall).*

- ***Platforma jako služba (PaaS).*** *V rámci této platformy má spotřebitel možnost nasadit na cloudovou infrastrukturu vlastní vytvořené nebo získané aplikace, které využívají programovací jazyky, knihovny, služby a nástroje podporované poskytovatelem. Spotřebitel neprovádí správu ani řízení základní cloudové infrastruktury, která zahrnuje sítě, servery, operační systémy nebo úložiště, má však kontrolu nad nasazenými aplikacemi a případně nad konfiguracemi a nastaveními prostředí pro hostování aplikací.*

- ***Software jako služba (SaaS).*** *V rámci této platformy spotřebitel používá aplikace poskytovatele, které jsou provozovány na cloudové infrastruktuře. Aplikace jsou přístupné z různých klientských zařízení buď prostřednictvím dynamického rozhraní klienta, jako je třeba webový prohlížeč (např. webový e-mail), nebo prostřednictvím programového rozhraní. Spotřebitel neprovádí správu ani řízení základní cloudové infrastruktury, která zahrnuje sítě, servery, operační systémy či úložiště. Dokonce neovládá ani možnosti jednotlivých aplikací. Výjimečně může provádět omezené konfigurace aplikací pro konkrétní uživatele.*

- ***Veřejný cloud.*** *V tomto režimu je cloudová infrastruktura určena pro volné použití široké veřejnosti. Může ji vlastnit, spravovat a provozovat podnik, akademická nebo vládní organizace nebo různé kombinace výše uvedeného. Infrastruktura se nachází v prostorách poskytovatele cloudu.*

- ***Komunitní cloud.*** *Zde je cloudová infrastruktura poskytována pro výhradní použití určitou komunitou uživatelů z organizace, kteří sdílejí společné charakteristiky (např. poslání, bezpečnostní požadavky, zásady a dodržování předpisů). Takovou infrastrukturu může vlastnit, řídit a provozovat jedna nebo více organizací v komunitě nebo jiná třetí strana či kombinace výše uvedeného. Infrastruktura může být umístěna v prostorách dané organizace nebo mimo ně.*

- ***Hybridní cloud.*** *Hybridní cloudová platforma se skládá ze dvou nebo více různých cloudových infrastruktur (privátních, komunitních nebo veřejných), které zůstávají jedinečnými entitami, ale jsou spojeny standardizovanou nebo proprietární technologií. Ta zajišťuje přenositelnost dat a aplikací (např. přetečení cloudu pro vyrovnávání zátěže mezi cloudy).*

- ***Privátní cloud.*** *V tomto režimu je cloudová infrastruktura poskytována výhradně jedné organizaci se zahrnutím více spotřebitelů (např. obchodních jednotek). Infrastrukturu může vlastnit, spravovat a provozovat organizace, třetí strana nebo kombinace výše uvedeného. Tato infrastruktura může být umístěna v prostorách organizace nebo mimo ně.*

2.1.4 Podrobný popis nákupního modelu a soutěžení za podmínek Rámcové smlouvy

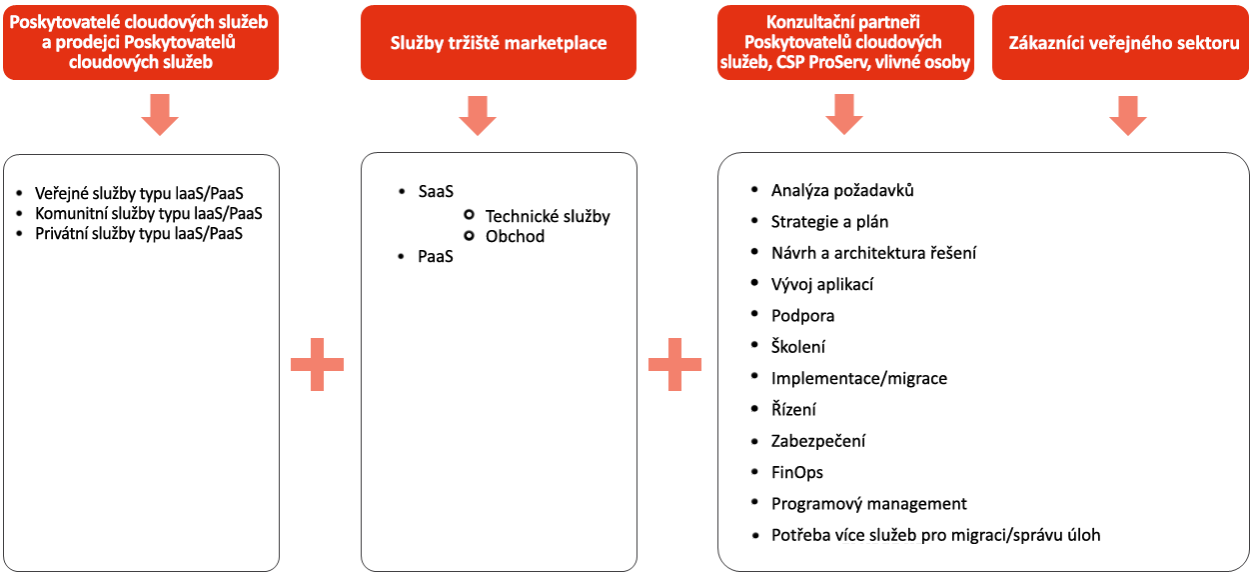
Jak již bylo výše uvedeno, zástupci veřejného sektoru by měli mít jasnou představu o tom, jaký model zvolí pro fungování rámcové smlouvy a následný mechanismus nákupu cloudových technologií a souvisejících služeb implementace a správy. Tato představa by měla být jasně definována v RFP na cloudové služby. Díky tomu budou moci všechny zúčastněné strany pochopit své role hned na počátku spolupráce, ať už jde o dodavatele cloudových technologií, související organizace poskytující poradenské služby, distributory na tržištích marketplace nebo samotné nakupující subjekty.

[2] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

S ohledem na rozsah rámcové smlouvy, následné objednávky a výběrová řízení malého rozsahu by měly organizace zvážit následující:

- Kdo bude odpovědný za integraci a spravované služby, které zahrnují využívání cloudových technologií v rámci smlouvy?
- Je potřeba, aby CISP nebo jeho prodejce poskytovali dodatečné služby přidané hodnoty nad rámec základních, mezi které patří služby nezbytné k udržení smluvního vztahu s CISP, poskytování konsolidovaných fakturačních služeb, zajištění včasného a přímého přístupu k údajům o využívání a fakturaci za používání cloudových služeb?
- Existuje požadavek na využití služeb prodejce s přidanou hodnotou, systémového integrátora, poskytovatele spravovaných služeb nebo jakoukoli formu práce v oblasti IT?

Je důležité si uvědomit, že CISP není systémový integrátor (SI) ani poskytovatel spravovaných služeb (MSP). Mnoho zákazníků z veřejného sektoru bude potřebovat CISP pro správu svých služeb IaaS/PaaS. Také budou muset outsourcovat na SI nebo MSP poradenské služby a služby plánování, migrace a správy. Vymezení rolí a odpovědností v modelu cloudových služeb je přehledně znázorněno níže na obrázku 2.



Obrázek 2 – RFP na cloudové služby by měla zahrnovat kompletní nabídku cloudových služeb, které koncoví uživatelé potřebují. Zákazníci z veřejného sektoru budou od CISP vyžadovat zajištění cloudové technologie, v případě potřeby také služby tržiště marketplace pro produkty PaaS a SaaS. Poté si zákazníci sami určí, jak velkou roli chtějí v rámci dodávek cloudových služeb převzít a do jaké míry hodlají outsourcovat služby poradenských firem, systémových integrátorů, poskytovatelů spravovaných služeb atd.

Níže uvedené vzorové znění bylo vytvořeno na základě modelu rolí a odpovědností, který je uveden znázorněn na obrázku 2 výše. Rámcová smlouva a související RFP na cloudové služby by měly být zárukou toho, že kupující dokážou adekvátně posoudit nabídky jednotlivých dodavatelů a vybrat si mezi různými službami tu, která odpovídá jejich potřebám pro úlohy/projektu. Takového stavu dosáhneme tím, že služby rozdělíme na tři typy, jak již bylo řečeno, a zároveň jasně definujeme způsob, jakým se uvnitř rámcové smlouvy budou realizovat objednávky nebo výběrová řízení malého rozsahu.

Vzor znění RFP: Nákupní model

*Tato smlouva slouží jako **Rámcový** nástroj pro realizaci nákupu. Tato Rámcová smlouva bude zahrnovat více **typů služeb** definovaných ze strany **<ORGANIZACE>**. Jde o cloudové technologie a související služby a produkty tržiště marketplace, poradenské služby, profesionální služby systémové integrace, spravovaných služeb, migrace služeb, školení a podpory, a to způsobem, který definuje **<ORGANIZACE>**. Smlouvu a s ní spojený rámec služeb bude využívat více oprávněných kupujících v rámci **<ORGANIZACE>**. Tento model zjednodušuje proces zadávání zakázek a zároveň optimalizuje úspory z rozsahu.*

Po uzavření této rámcové smlouvy může organizace nakupovat konkrétní cloudové technologie a služby, kdykoli je potřebuje – na rozdíl od modelu nakupování prostřednictvím samostatných veřejných zakázek. Tento přístup snižuje administrativní požadavky a významně snižuje složitost zadávání zakázek a délku cyklu.

*Doba trvání Rámcové smlouvy bude maximálně **<X>** let včetně případných prodloužení. Maximální délka smluvní objednávky z Rámcové smlouvy je obvykle **<x>** měsíců; tuto délku lze prodloužit o **<x>** měsíců a poté o dalších **<x>** měsíců, přičemž prodloužení smluvní objednávky musí být v případě potřeby schváleno příslušnými interními orgány. Takový případ bude uveden v každé konkrétní **Objednávce**.*

*RÁMEC spolupráce je rozdělen na **3 (tři) typy služeb**.*

1. ***TYP SLUŽBY 1: CLOUDOVÉ TECHNOLOGIE** – plný rozsah cloudových technologií poskytovatele (přímo od CISP, jeho prodejce nebo od prodejce služeb/podpory s přidanou hodnotou):*
    i. ***Služby typu IaaS a PaaS** – nabídka cloudových technologií, např. výpočetní* prostředky, *úložiště, sítě, databáze, analytika, aplikační služby, nasazení, správa, vývojáři, internet věcí (IoT) atd. Tato nabídka zahrnuje balíčky cloudových technologických řešení, jako jsou DR/COOP, Archive, Big Data & Analytics, DevOps atd.*
2. ***TYP SLUŽBY 2: TRŽIŠTĚ MARKETPLACE** – plný rozsah služeb/produktů typu PaaS a SaaS, jako je účetnictví, CRM,* design, *HR, GIS a mapování, HPC, BI, správa obsahu, analýza protokolů atd.*
3. ***TYP SLUŽBY 3: PORADENSKÉ SLUŽBY V OBLASTI CLOUDOVÝCH SLUŽEB** – plný rozsah poradenských služeb (spravované služby, odborné služby, poradenské/konzultační služby, služby s přidanou hodnotou, FinOps, technická podpora) souvisejících s migrací a využíváním cloudu. Tyto služby mohou zahrnovat: plánování,* design, *migraci, správu, podporu, řízení kvality, bezpečnost, školení atd.*

Dodavatelé mohou předložit své nabídky v rámci více typů služeb.

Dodavatelé předloží své nabídky a související ceny v libovolném formátu.

SOUTĚŽENÍ DLE PODMÍNEK RÁMCOVÉ SMLOUVY A ZADÁVÁNÍ SMLUVNÍCH ZAKÁZEK

OBJEDNÁVKY

Subjekty veřejného sektoru, které jsou smluvní stranou rámcové smlouvy, si mohou objednat resp. „vyžádat" služby, které potřebují. Při vytvoření objednávky na základě rámcové smlouvy mohou kupující upřesnit své požadavky pomocí dodatečné funkční specifikace. Zároveň si však kupující zachovávají výhody nabízené v rámci Rámcové smlouvy.

U smluvních zakázek zadaných dle podmínek rámcové smlouvy bude možno prokázat splnění podmínek auditu s ohledem na požadavky stanovené při výběru dodavatele v rámci každého typu služby. Koncoví kupující budou uchovávat záznamy o komunikaci s dodavateli, včetně veškeré tržní aktivity na počátku spolupráce, upřesňujících dotazů, e-mailů a osobních rozhovorů.

1. SOUPIS POŽADAVKŮ PRO TVORBU OBJEDNÁVKY A ZÍSKÁNÍ INTERNÍHO SOUHLASU S NÁKUPEM

Všichni koncoví kupující, kteří jsou způsobilí k využívání Rámcové smlouvy, vytvoří týmy podnikových koncových uživatelů, specialistů nákupu a technických odborníků. Ti poté společně připraví seznam nezbytných i vhodných položek. Tento seznam usnadní rozhodování o tom, které typy služeb se budou objednávat a kteří dodavatelé jsou nejvhodnější pro splnění daných požadavků. Při sestavování požadavků by měli kupující brát v úvahu:

- *finanční prostředky, které jsou k dispozici pro využívání služeb;*
- *technické požadavky a zadávací podmínky daného projektu;*
- *kritéria, na jejichž základě bude výběr proveden.*

2. VYHLEDÁVÁNÍ SLUŽEB

Na základě Rámcové smlouvy budou kupující pro nákup potřebných výrobků/služeb využívat Rámcový online katalog (portál, na kterém budou uvedeni kvalifikovaní dodavatelé a jejich služby dle Rámcové smlouvy). Kupující si zvolí odpovídající typy služby a poté vyhledají konkrétní služby.

3. PŘEZKOUMÁNÍ A VYHODNOCENÍ SLUŽEB

Kupující v režimu rámcové smlouvy přezkoumají popisy služeb a vyberou ty, které nejlépe odpovídají jejich požadavkům a rozpočtu. Každý popis služby bude obsahovat:

- *dokument s definicí služby nebo odkazy na definice služeb;*
- *dokument s obchodními podmínkami;*
- *cenový dokument (odkazy na veřejné informace o cenách jsou přijatelné za předpokladu, že je na vyžádání k dispozici úplný ceník/cenový dokument).*

Cena bude odpovídat ceně nejběžnější konfigurace dané služby. Ceny se obvykle odvíjejí od objemu odebíraných služeb. Proto by se kupující měli vždy podívat do cenového dokumentu dodavatele, veřejných ceníků nebo do nástrojů pro cenové kalkulace, aby zjistili skutečnou cenu nakupovaného zboží a celkovou hodnotu poskytovanou kupujícímu (například výsledné snížení celkových nákladů u služeb optimalizace).

Kupující v režimu Rámcové smlouvy mohou dodavatele oslovit a požádat je o dodatečné informace o popisech služby, obchodních podmínkách, cenách, definicích služby a modelech. O všech rozhovorech s dodavateli bude veden záznam.

4. VÝBĚR SLUŽBY A ZADÁNÍ SMLUVNÍ ZAKÁZKY

Jediný dodavatel

Pokud požadavky splňuje pouze jeden dodavatel, může být zakázka zadána jemu.

Více dodavatelů

Pokud je na užším seznamu více dodavatelů, vybere zadavatel ekonomicky nejvýhodnější nabídku (MEAT). Kritéria pro hodnocení založené na metodě MEAT naleznete v následující tabulce. Kupující se může rozhodnout, jaké podrobné charakteristiky použije a jakou váhu jim přiřadí.

Vezměte prosím na vědomí, že kupující možná bude muset:

- *porovnat kombinace různých dodavatelů;*
- *získat konkrétní informace o množstevních nebo podnikových slevách a službách, které prodejci nabízejí s ohledem na optimalizaci nákladů.*

Hodnocení dodavatelů by mělo být vždy spravedlivé a transparentní. Výběr by měl být založen na nejvhodnějším řešení a vyloučení dodavatelů/služeb by mělo proběhnout s uvedením důvodů a odkazem na konkrétní požadavky projektu.

Tabulka 2 – Hodnocení založené na ekonomicky nejvýhodnější nabídce (MEAT)

Kritéria udělení zakázky
Náklady po celou dobu životnosti: *nákladová efektivita, cena a provozní náklady*
Technické přednosti a funkční způsobilost: *pokrytí, kapacita sítě a výkonnost podle příslušných úrovní služeb*
Řízení poprodejních služeb: *helpdesk, dokumentace, funkce správy účtů a zajištění dodávek celé řady služeb*
Charakteristiky, které se netýkají funkčnosti

VÝBĚROVÁ ŘÍZENÍ MALÉHO ROZSAHU

Pokud to bude považováno za nutné, je možné uspořádat výběrové řízení malého rozsahu s cílem určit nejlepšího dodavatele pro určité aplikace nebo projekty. Výběrové řízení malého rozsahu je proces, při kterém zákazník realizuje další soutěž na základě Rámcové smlouvy. Tuto soutěž spouští tak, že vyzve všechny dodavatele v rámci jednoho typu služby, aby odpověděli na soubor požadavků. Zadavatel vyzve všechny schopné dodavatele v rámci daného typu služby, aby podali nabídku. Více informací o porovnávání dodavatelů naleznete v níže uvedených částech týkajících se technických aspektů, zabezpečení a ceny/hodnoty.

SMLUVNÍ OBJEDNÁVKA

*Než bude možné začít službu používat, kupující i prodávající podepíšou kopii smluvní objednávky. Maximální délka Rámcové smlouvy je obvykle **<x>** měsíců; tuto délku lze prodloužit o **<x>** měsíců a poté o dalších **<x>** měsíců, přičemž prodloužení smluvní objednávky musí být v případě potřeby schváleno příslušnými interními orgány.*

Před zahájením používání služby musí být kopie smluvní objednávky podepsána všemi zúčastněnými stranami (kupujícím a dodavatelem).

2.1.5 Minimální požadavky na uchazeče – administrativa

Při určování kvalifikačních kritérií dle podmínek rámcové smlouvy je vhodné používat jednoduché a jasné formulace. To pomůže eliminovat případy, kdy tradiční poskytovatelé datových center nebo hardwaru nabízejí tradiční řešení, která vydávají za „cloud“. Účastníci podávající RFP by měli prokázat, zda a jak splňují níže uvedené minimální administrativní požadavky na uchazeče.

Opět upozorňujeme na fakt, že tento dokument se zaměřuje na TYP SLUŽBY 1 – CLOUDOVÉ TECHNOLOGIE. Přesto jsme přidali také další informace týkající se TYPU SLUŽBY 2 – TRŽIŠTĚ MARKETPLACE a TYPU SLUŽBY 3 – PORADENSKÉ SLUŽBY V OBLASTI CLOUDOVÝCH SLUŽEB, které mohou poskytnout celkový kontext s ohledem na požadavky a rozsah RFP. Například je velice důležité, aby zadavatel zmínil minimální kvalifikační kritéria pro role CISP/MSP/SI/poradenských firem apod. a aby zajistil, že tyto subjekty budou (1) přímo spojeny s konkrétním CISP jako prodejci nebo distribuční partneři, (2) certifikovány ze strany CISP pro případný přeprodej přímého přístupu k nabídkám CISP ze strany subjektů třetích stran a (3) mít certifikaci od těchto CISP označující jejich schopnosti a odborné znalosti.

Vzor znění RFP: Minimální požadavky na uchazeče – administrativa

Na základě této rámcové smlouvy budou realizovány smluvní objednávky s více dodavateli v následujících kategoriích. Dodavatelé musí být komerční CISP, prodejci poskytovatelů CISP jako třetí strany, distributoři služeb tržiště marketplace a/nebo poskytovatelé služeb využívaných ve spojení s CISP (např. poradenství, migrační služby, spravované služby, FinOps atd.). Uveďte prosím role, které odpovídají vaší situaci:

TYP SLUŽBY 1

____ - Přímý CISP služeb veřejného cloudu (IaaS a PaaS)

____ - Přímý CISP služeb komunitního cloudu (IaaS a PaaS)

____ - Přímý CISP služeb privátního cloudu (IaaS a PaaS)

____ - CISP Prodejce třetí strany (možnost poskytovat přímý přístup k online cloudovým nabídkám CISP)

- *Identifikujte nabídku CISP, u které máte možnost působit jako prodejce přímého přístupu k dané službě: _____*
- *Předložte dopis od CISP, který potvrzuje, že jste autorizovaným prodejcem nabídek tohoto poskytovatele: _____*

TYP SLUŽBY 2

____ - Přímý poskytovatel služeb tržiště marketplace provozovaných na platformě CISP (PaaS a/nebo SaaS)

____ - Distributor služeb tržiště marketplace provozovaných na platformě CISP (PaaS a/nebo SaaS)

TYP SLUŽBY 3

____ - CISP nabízející odborné služby

____ - Poskytovatel technické podpory CISP

____ - Partner poskytovatele CISP poskytující služby pro používání nebo provoz na platformě CISP

____ - Vlivná osoba/poradce poskytující služby pro používání nebo provoz na platformě CISP

Identifikujte typ nabídky:

- *Spravované služby pro úlohy na platformě CISP (ANO/NE): _____*
  - *Uveďte případné specializace: _____*
- Profesionální služby*: (ANO/NE): _____*
- *Poradenství – školení (ANO/NE): _____*
- *Poradenství – strategie (ANO/NE): _____*
- *Poradenství – migrace (ANO/NE): _____*
- *Poradenství – řízení cloudových služeb (ANO/NE): _____*
- *Poradenství – FinOps (ANO/NE): _____*
- *Poradenství – jiné (uveďte): _____*

Identifikujte CISP, pro kterého/které poskytujete služby: _____
Předložte dopis od CISP, který potvrzuje váš statut partnera dle modelu CISP: _____

TYP SLUŽBY 1 MINIMÁLNÍ ADMINISTRATIVNÍ POŽADAVKY

Poskytovatelé cloudových služeb (CISP)
Aby mohl být poskytovatel kvalifikován jako CISP, musí splňovat níže uvedené požadavky.

Navrhovaná kvalifikační kritéria pro CISP	*Důvod*
Organizační údaje, např. název, právní struktura, registrační číslo/DUNS, DPH atd.	
Velikost, ekonomická a finanční situace společnosti[3]	*Zákazník může sám odhadnout a určit, zda je CISP schopen smlouvu splnit.*
Důvody pro vyloučení, např. trestná/podvodná činnost atd.	
Případové studie/reference zákazníků (uveďte požadovaný počet/typ)	*Zákazník má možnost prověřit zkušenosti CISP s výkonem požadovaných služeb.*
Společenská odpovědnost firem	*Mělo by se jednat o veřejně přístupné podklady, které poskytuje CISP.*
Veřejně viditelné závazky a postupy v oblasti udržitelnosti	*Zákazník vidí a může se snadno přesvědčit, že se CISP snaží provozovat svou činnost co nejšetrněji k životnímu prostředí.*
CISP musí mít za posledních 5 let prokazatelné výsledky v oblasti inovací a vydávání nových užitečných služeb a funkcí, zejména v oblasti PAAS, strojového učení a analytiky, Big Data, spravovaných služeb a funkcí pro optimalizaci využití cloudu. Jako důkaz lze použít veřejně přístupné protokoly změn nebo informační kanály aktualizací.	*Toto kritérium prokazuje, že CISP pracuje na tom, aby se nové produkty rychle dostaly do rukou zákazníků, a poté je rychle iteruje a vylepšuje. To pomáhá zákazníkům udržovat nejmodernější infrastrukturu IT, aniž by museli vynakládat nové investiční výdaje.*

Vztah prodejce/partnera s CISP

<ORGANIZACE> *požaduje, aby byl hlavní dodavatel přímo spojen s CISP jako prodejce nebo distribuční partner, aby byl certifikovaný ze strany CISP pro následný prodej přímého přístupu k nabídkám CISP určeným subjektům třetích stran, včetně certifikace tohoto CISP, která dostatečně prokazuje schopnosti a odborné znalosti daného prodejce nebo distribučního partnera. Díky tomuto postupu odpadá organizaci* ***<ORGANIZACE>*** *povinnost přezkoumat podmínky a služby spojené s procesem subdodávky mezi hlavním dodavatelem z* ***Rámcové smlouvy*** *a CISP. Tento požadavek rovněž eliminuje složitosti, které vznikají přidáváním dalších prodejců. Avšak to platí pouze za předpokladu, že (1)* ***<ORGANIZACE>*** *vynakládá náležitou péči, aby zajistila jasné přidělení odpovědností ve vztahu ke službám, které mají být poskytovány, a že (2)* ***<ORGANIZACE>*** *vykonává každodenní činnosti zahrnující využívání cloudových služeb.*

2.2 Technická specifikace

RFP na cloudové služby by měla zvýšit laťku pro CISP tím, že bude vyžadovat, aby tito poskytovali standardizované cloudové technologie, které zákazník potřebuje k vytvoření vlastního řešení. Jak již bylo zmíněno výše, v případě RFP na cloudové služby je velice důležité vnímat rozdíl mezi tím, co je standardizované, a tím, co je přizpůsobené. CISP nabízejí standardizované služby milionům zákazníků. Přizpůsobení služeb, popisované v RFP na cloudové služby, se proto musí zaměřit na řešení a výsledky na vyšších úrovních, nikoli na tyto standardizované základní metody, infrastruktury a hardware, používané pro dosažení standardních výsledků.

[3] RFP na cloudové služby se zaměřuje na informace vysoké úrovně, nikoli třeba na informace o počtu zaměstnanců ve společnosti nebo o struktuře interních týmů zaměstnanců. U cloudových technologií neexistuje skutečná souvislost mezi počtem zaměstnanců a zárukou výkonu služby. V RFP na cloudové služby se místo toho zohledňuje celková velikost společnosti, která musí odpovídat konkrétním požadavkům (s ohledem na rozsah), a prokázané zkušenosti/výkonnost.

2.2.1 Minimální požadavky

Tradiční způsoby nakupování IT se často řídí obchodními požadavky vyplývajícími z řady pracovních schůzek, které zachycují a dokumentují způsob fungování organizace. Správné stanovení těchto požadavků je i v těch nejlepších podmínkách velice obtížný proces. V lepším případě, pokud je tento proces správně realizován, účastníci těchto schůzek zachytí a zdokumentují historický obchodní model fungování organizace, který ovšem může být sám o sobě zastaralý a neefektivní. Pokud dále účastníci z tohoto modelu vyvodí požadavky a ty se stanou součástí RFP, kterou má CISP brát v úvahu, může být jediným východiskem vypracování řešení na míru. Tento model ovšem není kompatibilní s postupy nakupování cloudových služeb.

Subjekty ve veřejném sektoru by měly rozumět svým obchodním cílům a výkonnostním potřebám, ale neměly by v rámci RFP diktovat, jak má vypadat návrh a funkčnost systému. Místo toho by se dané subjekty měly zaměřit na nejvhodnější obchodní řešení. Místo hodnocení návrhů na základě stovek nebo dokonce tisíců normativních požadavků, které ani nemusí vést k tomu, že bude služba kvalitní, by subjekty veřejného sektoru měly brát v úvahu kritéria hodnocení založená na tom, jak dobře technologie a související služby splní nebo zvýší obchodní cíle, zda dosáhnou svých výkonnostních potřeb a zda je možné doladit obchodní pravidla úpravou konfigurace.

RFP na cloudové služby by měly klást správné otázky, které povedou k získání nejlepšího možného řešení. Vzhledem k tomu, že v modelu cloudu neprobíhá nakupování fyzického majetku, neplatí zde mnoho tradičních požadavků uplatňovaných při zadávání zakázek pro datová centra. ***Opakovaní otázek, které mají smysl v případě pořizování datového centra, nevyhnutelně povede k odpovědím relevantním pro datová centra****. Poté nebude moci CISP předložit vhodnou nabídku, nebo ještě hůře, povede to ke špatně navrženým smlouvám, které znemožní zákazníkům z veřejného sektoru využívat možnosti a výhody cloudu.*

RFP na cloudové služby musí obsahovat klíčové požadavky na CISP a cloudové služby. Jedině tak budou dodavatelé, kteří se kvalifikují do rámce TYPU SLUŽBY 1, splňovat vysoké nároky na kvalitní dodávku služeb. Požadavky by rovněž neměly být příliš normativní. Subjekty veřejného sektoru by měly mít možnost výběru ze široké škály kvalifikovaných CISP.

Vzor znění RFP: Možnosti poskytovatelů cloudových služeb

Podívejte se také na výše uvedené minimální administrativní požadavky na CISP pro TYP SLUŽBY 1.

Navrhovaná kvalifikační kritéria pro CISP	*Důvod*
Infrastruktura	
Infrastruktura CISP by měla nabízet alespoň 2 klastry datových center. Každý klastr musí být tvořen alespoň 2 datovými centry propojenými spojením s nízkou latencí, aby bylo možné použít vysoce dostupný model nasazení typu aktivní-aktivní a aby bylo možno implementovat scénáře DR-BC. Datová centra tvořící klastr musí být fyzicky izolovaná a vzájemně nezávislá s ohledem na případné poruchy.	*CISP musí být schopen nabídnout infrastrukturu vhodnou pro vytváření vysoce dostupných aplikací, kde není třeba navrhovat jediné body selhání.*
CISP by měl být schopen nabídnout logicky a geograficky oddělené oblasti. CISP nesmí replikovat data zákazníků mimo tyto oblasti.	*Požadavky na rezidenci dat mají být nastavené tak, aby měl zákazník plnou kontrolu nad tím, kde jsou jeho data umístěna.*

CISP musí být schopen poskytovat přímé, vyhrazené a privátní připojení mezi datovými centry CISP.	*Privátní konektivita je základním předpokladem pro vybudování bezpečné hybridní infrastruktury.*
CISP by měl disponovat odpovídajícími mechanismy, které zahrnují šifrování dat v tranzitu.	*Zákazník může požadovat možnost, aby nemohla být přenášena žádná data nešifrovaně.*
Minimální certifikace CISP	
CISP musí být certifikován dle ISO 27001	*Audity třetích stran, certifikace a akreditace jsou mimo jiné nástrojem pro to, aby zákazníci mohli porovnávat služby (a zejména platformy) z hlediska kvality, bezpečnosti a spolehlivosti. Je nezbytné, aby poskytovatelé splňovali alespoň dané certifikační minimum.*
CISP musí fungovat v souladu s Kodexem chování CISPE pro ochranu dat, aby byl schopen poskytovat funkce a služby v souladu s nařízením GDPR a aby tyto funkce a služby umožňovaly zákazníkům vytvářet aplikace v souladu s GDPR.	*Zákazník musí být schopen vytvářet nebo provozovat aplikace v souladu s nařízením GDPR.*
CISP musí zpřístupnit zprávy auditované třetí stranou, jde například o zprávy SOC 1 a 2 (se zahrnutím míst a služeb využívaných ze strany EC), aby byla zajištěna transparentnost kontrol a postupů CISP.	*CISP musí být zcela transparentní v tom, jak je aplikace provozována a spravována. Zprávy SOC mají zásadní význam pro zajištění důvěry a transparentnosti.*
CISP musí dodržovat Pakt o klimaticky neutrálních datových centrech.	*Pakt o klimaticky neutrálních datových centrech zavazuje CISP k tomu, aby směřovali k dosažení klimatické neutrality do roku 2030, a dává tak příležitost samotným uživatelům, aby také pracovali na svých cílech z hlediska udržitelnosti. Pro poskytovatele s více než 250 zaměstnanci na plný pracovní úvazek platí povinnost použití služeb auditora třetí strany (neplatí pro malé a střední podniky).*
CISP musí dodržovat Kodex chování pro přenos dat v rámci IaaS, vydaný skupinou SWIPO.	*Kodex chování pro přenos dat v rámci IaaS vydaný skupinou SWIPO je zárukou toho, že služba splňuje požadavky čl. 6 „Přenos" nařízení o volném pohybu neosobních údajů.*
Charakteristika služby	
Infrastruktura CISP musí být přístupná prostřednictvím programových rozhraní (API) a webové konzoly pro správu.	*Samoobslužný přístup a programová rozhraní jsou standardem požadovaným od CISP, který slouží k tomu, aby co nejvíce oddělil přístup uživatelů od přístupu samotného poskytovatele.*
CISP musí nabízet základní soubor služeb, který zahrnuje: objektové úložiště, spravovanou relační databázi, spravovanou nerelační databázi, spravované vyrovnávání zatížení, monitorování a integrované automatické škálování.	*Samotná nabídka virtuálních strojů nestačí k tomu, aby byl poskytovatel kvalifikován jako poskytovatel cloudu. Poskytovatelé cloudu by měli nabízet sadu služeb typu PAAS a IAAS, které urychlují a vylepšují aplikace zákazníků.*
CISP musí zajistit, aby zákazník mohl volně měnit používání a konfiguraci služeb nebo přesouvat data v rámci platformy CISP i mimo ni (samoobslužná nabídka).	*Samoobslužný přístup ke službám a datům je zásadním požadavkem, který umožňuje zákazníkovi fungovat zcela nezávisle.*
CISP musí umožnit účtování svých služeb v režimu „platby za použití".	*Platba za použití umožňuje zákazníkovi optimalizovat náklady s ohledem na zatížení, snížit rizika a využít platformu CISP pro krátkodobé aplikace a PoC.*

Zabezpečení dat a systémů	
CISP musí zajistit, aby si zákazník zachoval plnou kontrolu nad svými daty a aby měl možnost svobodně si zvolit, kde budou data uložena (na úrovni městské oblasti). Poskytovatel musí také zaručit, že žádná data zákazníka nebudou přesunuta, pokud k takovému přesunu nedá podnět sám zákazník.	*Zákazník musí mít kontrolu nad tím, kde jsou data uložena, dále nad správou přístupu k obsahu a přístupu uživatelů ke službám a zdrojům.*
Charakteristiky CISP musí zákazníkovi poskytnout plnou kontrolu nad jeho bezpečnostními zásadami, včetně důvěrnosti, integrity a dostupnosti dat a systémů zákazníka.	*Zákazník musí být schopen definovat a implementovat své bezpečnostní standardy pro všechny své úlohy. Nestačí jen důvěřovat poskytovateli, že bude s daty zákazníků „správně zacházet".*
Řízení nákladů	
CISP musí disponovat mechanismy a nástroji, které zákazníkovi umožní sledovat jeho výdaje v průběhu času. Tyto nástroje musí umožňovat základní segmentaci nákladů na základě zatížení, služeb a účtů.	
CISP musí nabízet nástroje, které zákazníka upozorní, kdykoli dojde k překročení stanoveného limitu nákladů.	
CISP musí dát zákazníkovi k dispozici podrobné vyúčtování. Vyúčtování musí být vypracováno tak, aby bylo možné rozdělit náklady podle zatížení, prostředí a účtů.	

CISP by měli být rovněž schopni odpovědět na níže uvedené dotazy k technickým požadavkům.

ŘEŠENÍ

CISP by měl být schopen prokázat způsob, jakým poskytuje předem připravené šablony a softwarová řešení, které jsou buď hostované na platformě CISP, nebo jsou s ní integrované, a to pro následující řešení:

- *Úložiště*
- *DevOps*
- *Zabezpečení/dodržování předpisů*
- *Big Data/analytika*
- *Podnikové aplikace*
- *Telekomunikace a sítě*
- *Geoprostorové funkce*
- *IoT*
- *[Ostatní]*

Poskytněte přehled o tom, jak byl systém CISP používán pro následující úlohy:

- *Obnovení po katastrofě*
- *Vývoj a testování*
- *Archivace*
- *Zálohování a obnovení*
- *Big Data*
- *Vysoce výkonné výpočetní prostředky (HPC)*
- *Internet věcí (IoT)*
- *Webové stránky*
- *Výpočetní řešení bez serveru*
- *DevOps*
- *Doručování obsahu*
- *[Ostatní]*

2.2.2 Porovnání dodavatelů

Kromě minimálních požadavků v RFP na cloudové služby je důležité stanovit kritéria, podle kterých bude možné srovnat technologie CISP při posuzování konkurence.

V RFP na cloudové služby by měly být požadovány pouze cloudové funkce, které organizace potřebuje. Ze žádosti by mělo dále vyplývat, že zákazník je vlastníkem těchto funkcí a bude je používat pro vytvoření svého řešení. Funkce, které přesahují standard požadovaný od CISP (například předem připravená řešení ze strany CISP nebo funkce automatizace), lze v rámci RFP na cloudové služby využít jako nástroj pro zjištění „možností s přidanou hodnotou" nebo „nejlepší hodnoty".

Ve veřejném sektoru se při výběrových řízeních jako hodnotící kritérium často používá nejlepší hodnota, ekonomicky nejvýhodnější nabídka (MEAT) nebo nejnižší cena. Výše uvedený přístup subjektů veřejného sektoru má vliv na plánování RFP na cloudové služby, je proto důležité vytvořit přístup, který bude brát v úvahu unikátní vlastnosti cloudu. Je důležité si uvědomit, že prosté porovnávání položek mezi nabídkami poskytovatelů cloudových služeb (např. výpočetní prostředky nebo velikost úložiště) není efektivním způsobem porovnávání nabídek. Důrazně proto doporučujeme zaměřit se na charakteristiky vyšší úrovně, jako jsou položky uvedené výše v oddíle *2.2.1*. Poté se subjekty veřejného sektoru mohou zaměřit na specifické požadavky na cloud, viz požadavky uvedené v oddíle *Dodatek A – Technické požadavky pro porovnání dodavatelů*.

V RFP by měly být uvedeny základní charakteristiky cloudu potřebné pro vytvoření cloudového řešení. Za tímto účelem mohou organizace veřejného sektoru použít základní charakteristiky cloudu dle institutu National Institute of Standards and Technology (NIST). Organizace mohou také spolupracovat s analytiky třetích stran a z jejich zpráv si ověřit, že daný CISP nabízí tu nejlepší nabídku skutečného cloudového řešení, které bude fungovat i v masivním měřítku.

Vzor znění RFP – Porovnání dodavatelů

CISP by měli být schopni odpovědět na VŠECHNY dotazy k technickým požadavkům dle ***Dodatku A****.*

Respondenti musí splňovat následující atributy a musí být schopni popsat, zda a jak jejich nabídky cloudových služeb splňují pět základních charakteristik pro cloud computing (cloudové výpočetní operace)[4]*.*

1) ***Samoobslužné služby na vyžádání:*** *Respondent musí být schopen jednostranně poskytovat výpočetní kapacity, jako je serverový čas nebo síťové úložiště, v případě potřeby automaticky bez nutnosti lidské interakce s jednotlivými poskytovateli služeb. Respondent musí zajistit, aby zadavatel mohl jednostranně (tj. bez kontroly nebo schválení ze strany dodavatele) objednávat služby. Vysvětlete, jak v rámci své nabídky zajišťujete výše uvedené služby.*

2) ***Všudypřítomný přístup k síti:*** *Respondent musí poskytovat více možností připojení k síti, z nichž jedna musí být s podporou internetu. Vysvětlete, jak v rámci své nabídky zajišťujete výše uvedené služby.*

3) ***Sdružování zdrojů:*** *CISP musí nabízet sdružené výpočetní zdroje, které slouží více spotřebitelům, a to pomocí modelu více tenantů s různými virtuálními zdroji, které jsou dynamicky přidělovány a přerozdělovány podle poptávky spotřebitelů. Uživatel musí mít možnost zadat umístění na vyšší úrovni abstrakce (např. země, oblast nebo umístění datového centra). Zároveň musí respondent poskytovat podporu škálování těchto zdrojů, a to v řádu minut nebo hodin od zadání požadavku. Vysvětlete, jak v rámci své nabídky zajišťujete výše uvedené služby.*

[4] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

4) ***Rychlá elasticita:*** *CISP musí podporovat funkce poskytování a rušení služeb (škálování nahoru a dolů), aby byla služba dostupná v minimálním předepsaném čase (maximálně „x" hodin) od zadání požadavku na poskytnutí. Respondent musí nabízet úpravy vyúčtování s ohledem na výše uvedené změny v poskytování služeb. Úpravy vyúčtování musí evidovat na denní bázi s rozdělením na hodinové nebo denní účtované jednotky.*

5) ***Měřená služba:*** *Respondent musí zpřístupnit přehled o využívání služby pomocí řídicího online panelu nebo podobného elektronického nástroje.*

CISP také musí:

- *být uznávaným předním dodavatelem v oblasti cloudových služeb v souladu s hodnocením dle magického kvadrantu společnosti Gartner pro služby typu IaaS,*[5]
- *poskytovat oborově uznávané zprávy analytiků třetích stran, které prokazují schopnosti a spolehlivost CISP.*

Jako poslední krok doporučujeme porovnat CISP pomocí scénářů uvedených v dodatku B.

2.2.2.1 Smlouvy o úrovni služeb (SLA)

CISP uzavírají standardizované komerční smlouvy SLA s miliony zákazníků, a proto nemohou nabízet smlouvy SLA na míru, jako je tomu v případě modelu místního datového centra. Zákazníci však mohou (často s pomocí partnerů CISP) naplánovat a zavést své využívání cloudových služeb tak, aby dokázali plně pokrýt, anebo překonat své potřeby a požadavky v rámci své komerční smlouvy SLA.

RFP na cloudové služby by měla obsahovat potřebné zadání a vést CISP k tomu, aby v rámci své nabídky poskytl a popsal možnost maximálního využití svých služeb a komerční smlouvy SLA. Cílem poptávky je služba, která dokáže plnit požadavky na výkon a dostupnost všech jednotlivých koncových uživatelů.

Vzor znění RFP: Smlouvy o úrovni služeb

Poskytněte všechny nezbytné informace a odkazy na způsob, jakým budou CISP ve svých nabídkách zpracovávat téma smluv o úrovni služeb (SLA).

<ORGANIZACE> *bere na vědomí ujednání smluv SLA s CISP, nasadí důležitou pracovní zátěž a aplikace tak, aby fungovaly i v případě, že nebudou splněny podmínky smlouvy SLA.*

<ORGANIZACE> *odpovídá za dodržování příslušných smluv SLA spojených s jakýmkoli vybavením ve vlastnictví organizace* ***<ORGANIZACE>*** *nebo službami provozovanými ze strany* ***<ORGANIZACE>*** *a používanými ve spolupráci s CISP.*

CISP by měl zajistit, aby ***<ORGANIZACE>*** *měla průběžný přehled a dostávala zprávy o provozní výkonnosti v rámci smlouvy SLA. Organizace by také měla mít přístup ke zdokumentovaným osvědčeným postupům vedoucím k maximalizaci využití infrastruktury poskytovatele, aby tak organizace mohla vytvářet a nastavovat služby s ohledem na výkonnost, životnost a spolehlivost.*

2.2.3 Uzavírání smluv

Smluvní podmínky CISP jsou sestaveny tak, aby odrážely fungování modelu cloudových služeb (nekupují se fyzické položky a CISP nabízejí standardizované služby v obrovském měřítku). Je proto velmi důležité, aby smluvní podmínky CISP byly začleněny a používány v maximálním realizovatelném rozsahu. Další informace o smluvních podmínkách a uzavírání smluv najdete níže v oddíle *2.5*.

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

2.2.3.1 Nové a měnící se služby

CISP zajišťují výkonnost prostřednictvím služby. Oproti tradičním řešením umístěným na pracovišti, která vyžadují upgrady a časově omezené smlouvy o údržbě služeb, poskytovatelé cloudu jednoduše poskytují standardizovanou službu. Aby byl cloudový model schopen zajistit úspory z rozsahu, upgrady a změny hlavní infrastruktury se zpřístupňují všem uživatelům, nikoli jednotlivcům, a zákazníci si pak zvolí služby, které používají. Fungování služby je lepší než u dřívějších místních systémů a poskytovatelé cloudu neustále přidávají nové vylepšené služby, které zákazníci můžou podle potřeby používat.

Pokud po vypršení termínu k podání RFP nelze přidat nové nebo vylepšené služby CISP, organizace veřejného sektoru se odřezávají od výhod nových služeb a vylepšených funkcí až do vydání příští iterace Rámcové smlouvy. Proto důrazně doporučujeme, aby zajišťování služeb popsané v rámcové smlouvě bylo široké a umožňovalo přidání nových služeb CISP po vypršení termínu k podání žádosti. Právní předpisy EU týkající se zadávání zakázek můžou omezit přidávání podstatně odlišných nových služeb CISP do rámcové smlouvy, ale aktualizace a nové verze služeb, které nejsou považované za podstatné změny, by bylo možné přidávat, aniž by vznikl problém ohledně zadávání zakázek.

Vzor znění RFP: Nové a měnící se služby

CISP bude zajišťovat cenově efektivní řešení využívající jak osvědčené a stabilní virtualizační technologie, tak průběžně aktualizované nejnovější technologie. ***<ORGANIZACE>*** *bere na vědomí a souhlasí s tím, že cloudové technologie můžou být poskytovány na sdílené bázi organizaci* ***<ORGANIZACE>*** *a dalším klientům daného poskytovatele CISP ze stejného základu kódu, případně společného prostředí, a daný CISP může čas od času změnit, přidat nebo odebrat funkce, prvky, výkonnost nebo jiné charakteristiky cloudových služeb. Pokud provede takovou změnu, přidání nebo odebrání, příslušným způsobem budou upraveny specifikace cloudové služby.*

Rozsah této dodací objednávky zahrnuje veškeré stávající a nové či vylepšené služby CISP ***V ROZSAHU URČENÉHO RÁMCE****. Cloudové služby poskytované ze strany CISP a dostupné pro komerční uživatele budou zpřístupněny organizaci* ***<ORGANIZACE>****.*

2.2.3.2 Uzamčení zákazníka a reverzibilita

Cloudová technologie snižuje míru uzamčení zákazníků, protože nekupují fyzické položky a můžou kdykoli přesunout svá data od jednoho poskytovatele cloudu k druhému.

Určitý stupeň uzamčení je však při nákupu cloudových služeb nevyhnutelný. Každý cloud je jiný a jeden CISP může nabízet konkrétní služby a možnosti, které jiný poskytovatel není schopen zajistit. Snižuje se tak možnost používat takové služby u jiných poskytovatelů. Rozumný přístup spočívá v tom, že CISP zajistí nezbytné funkce a služby k opuštění jejich cloudu, včetně dokumentace s postupy, jak používat tyto služby umožňující přiměřenou „únikovou cestu“ – s ohledem na to, že CISP nemůže znát jedinečnou konfiguraci, v jaké daný zákazník používá jeho standardizované služby, a není tedy schopen poskytnout na míru šitý plán odchodu.

V oddíle 2.3.1.2 najdete informace o oborových kodexech chování, které pojednávají o „Přenosu dat“ a „Změně poskytovatelů cloudu“, jak to vyžaduje článek 6 směrnice EU „o rámci pro volný tok neosobních údajů“.

Vzor znění RFP: Zahájení a ukončení spolupráce

<ORGANIZACE> požaduje návrhy, jak zajistit přiměřenou strategii odchodu, aby se vyhnula uzamčení. <ORGANIZACE> nekupuje fyzické položky a CISP zajistí možnost přecházet nahoru a zpátky dolů v hodnotovém řetězci IT. CISP poskytne nástroje a služby pro přenos, umožňující migrovat na jeho platformu a pryč z této platformy, aby byla míra uzamčení minimální. Podrobná dokumentace, jak používat nástroje a služby pro přenos od CISP, bude sloužit jako přiměřený plán odchodu.

*CISP by neměl **vyžadovat** minimální povinné závazky nebo **vyžadovat** dlouhodobé smlouvy.*

*Data uložená u poskytovatele služeb může zákazník kdykoli exportovat. CISP umožní organizaci **<ORGANIZACE>** přesunovat podle potřeby data do úložiště CISP a mimo něj. CISP také umožní stahování a přesun virtuálních bitových kopií k novému poskytovateli cloudu. **<ORGANIZACE>** může exportovat své bitové kopie a použít je na pracovišti nebo u jiného poskytovatele (v rámci omezení daných softwarovými licencemi).*

2.3 Bezpečnost

O odpovědnost za bezpečnost a splnění předpisů se dělí CISP a zákazníci využívající cloud. V tomto modelu zákazníci využívající cloud řídí způsob, jak vybudují a zabezpečí své aplikace a data vložená do infrastruktury, zatímco CISP odpovídají za poskytování služeb na vysoce zabezpečené a řízené platformě a poskytují širokou škálu dalších funkcí zabezpečení. Rozsah odpovědnosti na straně CISP a zákazníka v tomto modelu závisí na modelu nasazení cloudu (IaaS/PaaS/SaaS). Zákazník by měl mít jasno o tom, za co u jednotlivých modelů odpovídá.

Porozumění tomuto modelu sdílené odpovědnosti je klíčové pro sestavení úspěšné RFP na cloudové služby. Organizace ve veřejném sektoru by měly mít přehled o tom, za co odpovídá CISP, za co odpovídají oni sami a pro které oblasti je dostupná pomoc poradenských partnerů a nezávislých dodavatelů softwaru a jejich řešení.

2.3.1 Minimální požadavky

Co se týče zabezpečení cloudu, klíčový termín je **Funkce**. Organizace ve veřejném sektoru by měly od CISP požadovat, aby zajistili funkce zabezpečení potřebné k tomu, aby zákazníci byli schopní převzít odpovídající díl odpovědnosti v modelu sdílené odpovědnosti. Jak je vidět z reprezentativního seznamu požadavků uvedeného níže, od CISP je vyžadováno zajištění standardizované funkce, aby ji zákazník mohl využít k zabezpečení svého jedinečného cloudového prostředí.

- ***Zajistěte funkce** pro brány firewall pro sítě a webové aplikace, aby bylo možné vytvářet privátní sítě a řídit přístup k instancím a aplikacím.*
- ***Zajistěte možnosti** pro konektivitu umožňující privátní nebo vyhrazená připojení z prostředí vaší kanceláře nebo pracoviště.*
- ***Zajistěte funkce** pro implementaci strategie hloubkové ochrany a maření útoků DDoS.*
- ***Funkce** pro šifrování dat dostupné ve službách úložiště a databáze.*
- ***Zajistěte** flexibilní klíčové **funkce** pro správu umožňující zvolit, zda nechat CISP spravovat šifrovací klíče, anebo dát kompletní kontrolu nad klíči zákazníkovi.*
- ***Zajistěte API**, aby si zákazníci mohli integrovat šifrování a ochranu dat s kteroukoli ze služeb vyvinutých nebo nasazených v prostředí CISP.*
- ***Zajistěte nástroje** pro nasazení, které slouží ke správě vytváření a vyřazení prostředků CISP podle standardů organizace.*
- ***Zajistěte nástroje** pro správu inventáře a konfigurace, které slouží k identifikaci prostředků CISP a průběžně sledujte a spravujte změny těchto prostředků.*
- ***Zajistěte nástroje a funkce** umožňující zákazníkům vidět, co přesně se děje v jejich prostředí CISP.*

- ***Zajistěte** hloubkovou **viditelnost** volání API, například od koho a z čeho volání pochází, komu a odkud byla provedena.*
- ***Zajistěte možnosti** pro agregaci protokolů, které zjednoduší vyšetřování a reportování ohledně plnění předpisů.*
- *Zajistěte funkci ke konfiguraci výstražných upozornění pro případ, že dojde ke konkrétním událostem nebo při překročení prahových hodnot.*
- ***Zajistěte funkce** sloužící k definování, vynucování a správě zásad pro přístup uživatelů pro všechny služby CISP.*
- ***Zajistěte funkci** pro definování jednotlivých uživatelských účtů s oprávněními napříč prostředky CISP.*
- ***Zajistěte funkci** pro integraci a federování s firemními adresáři, aby se omezila administrativní režie a zlepšilo uživatelské prostředí.*

Většinu z těchto požadavků uvádí *Dodatek A – Technické požadavky pro porovnání dodavatelů*.

Funkce přesahující minimální standard zabezpečení lze použít kvůli smysluplnější analýze „možností pro přidanou hodnotu“ nebo „nejlepší hodnoty“ v RFP. Čím více funkcí v oblasti zabezpečení je integrovaných nebo automatizovaných, tím lépe. Požadavky na srovnání mezi nabídkami jsou uvedeny v části *Dodatek A – Technické požadavky pro porovnání dodavatelů*.

Organizace ve veřejném sektoru by si měly v akreditačních certifikacích a hodnoceních cloudu ověřit, že CISP má zavedeny požadované kontrolní mechanismy zabezpečení. Například: Dejme tomu, že CISP byl ověřen a certifikován nezávislým auditorem, který potvrdil soulad s certifikační normou ISO 27001. Příloha A, kapitola 14 normy ISO 27001 se zabývá konkrétními opatřeními, kterým CISP musí vyhovět podle požadavků ISO a které se týkají akvizice, vývoje a údržby systému. Tato opatření pravděpodobně pokrývají většinu, pokud ne všechna, opatření týkajících se akvizice, vývoje a údržby systému, která by obvykle požadovala organizace v RFP pro oblast IT. Proto dává smysl, když organizace jednoduše požaduje, aby měl CISP certifikaci ISO 27001, namísto vynakládání zbytečné energie na vypisování požadavků na opatření týkající se akvizice, vývoje a údržby systému v RFP.

Tento přístup využívající zprávy o dodržení předpisů od třetích stran lze aplikovat na většinu opatření v oblasti zabezpečení a dodržování předpisů, například: Kodex chování CISPE GDPR, ISO, SOC aj.

Vzor znění RFP: Zabezpečení

*CISP bude organizaci **<ORGANIZACE>** informovat o bezpečnostních procesech, na které se nevztahuje jeho vlastnické právo, a technických omezeních, aby bylo možné dosáhnout adekvátní ochrany a flexibility mezi organizací **<ORGANIZACE>** a poskytovatelem služeb.*

CISP uvede své role a odpovědnosti týkající se zabezpečení a souladu s předpisy:

- *V navrhované nabídce popište role a odpovědnosti týkající se zabezpečení na straně CISP a **<ORGANIZACE>**. Jasně vysvětlete rozdělení odpovědnosti a uveďte služby CISP, které pomůžou organizaci **<ORGANIZACI>** při sestavování a automatizaci bezpečnostních funkcí v cloudovém prostředí.*
- *Uveďte odpovědi na technické specifikace v **DODATKU A** ohledně požadavků **<ORGANIZACE>** na zabezpečení.*

VLASTNICTVÍ OBSAHU <ORGANIZACE> A KONTROLA NAD NÍM

*Popište, jak funkce CISP můžou ochránit soukromí dat **<ORGANIZACE>**. Uveďte také opatření, která jsou zavedená s cílem chránit obsah **<ORGANIZACE>**. CISP musí zajistit silnou izolaci oblastí, aby objekty uložené v určité oblasti tuto oblast nikdy neopouštěly kromě případů, kdy je **<ORGANIZACE>** výslovně přesune do jiné oblasti.*

- *<ORGANIZACE> bude spravovat přístup ke svému obsahu, službám a prostředkům. CISP by měl poskytnout pokročilou sadu funkcí pro přístup, šifrování a přihlašování, které organizaci **<ORGANIZACE>** usnadní jejich*

efektivní využívání. CISP nebude přistupovat k obsahu organizace **<ORGANIZACE>** *ani jej nebude využívat k žádnému jinému účelu, než je zákonně vyžadováno pro údržbu služeb CISP a jejich poskytování organizaci* **<ORGANIZACE>** *a jejím koncovým uživatelům.*

- **<ORGANIZACE>** *zvolí oblast či oblasti, ve kterých bude uložen její obsah. CISP nebude přesouvat nebo replikovat obsah* **<ORGANIZACE>** *mimo zvolenou oblast či oblasti, s výjimkou případů, kdy je to vyžadováno zákonem a pokud je to nezbytné pro údržbu služeb CISP a jejich poskytování organizaci* **<ORGANIZACE>** *a jejím koncovým uživatelům.*

- **<ORGANIZACE>** *si zvolí způsob, jakým bude zabezpečen její obsah. CISP musí zajistit silné šifrování obsahu* **<ORGANIZACE>** *při přenosu nebo na úrovni úložiště (at rest) a možnost, aby* **<ORGANIZACE>** *mohla spravovat své vlastní šifrovací klíče.*

- *CISP musí disponovat programem záruky bezpečnosti, který využívá globální osvědčené postupy ochrany osobních údajů a dat, aby* **<ORGANIZACE>** *mohla vytvořit, provozovat a využívat prostředí CISP pro kontrolu zabezpečení. Bezpečnostní opatření a řídicí procesy musí být nezávisle ověřeny několika nezávislými hodnoceními třetích stran.*

Akreditační certifikace a hodnocení cloudu poskytují organizacím ve veřejném sektoru jistotu, že CISP mají zavedené účinné fyzické a logické kontroly zabezpečení. Když RFP využívají tyto akreditace, zjednoduší se proces zadávání zakázek a zamezí se duplicitním a nadměrně zatěžujícím procesům nebo schvalovacím postupům, které pro cloudové prostředí nemusí být nezbytné.

V RFP na cloudové služby by CISP měl mít příležitost doložit svůj soulad s akreditacemi a hodnoceními ohledně splnění předpisů. Jak je zmíněno výše, tyto akreditační systémy se ve velkém rozsahu překrývají ohledně rizikových scénářů a postupů řízení rizika. Protože jsou v takových akreditacích kontroly a požadavky seskupené dohromady, požadavek na soulad CISP s akreditacemi je rychlejší způsob, jak v RFP řešit splnění předpisů. Vypisování jednotlivých takových kontrol by znamenalo zbytečné vynakládání energie (mnoho z těchto kontrol lze převzít z předchozích žádostí, umístěných přímo v lokálních datových centrech, které se jako takové nemusí vztahovat ke cloudovým výpočetním produktům).

POZNÁMKA: Velmi důležité je také vědět, jak se k uvedeným zprávám dostat. Zprávy SOC 1 a SOC 2 například zpravidla představují citlivé dokumenty. Udělejte si přehled o dohodách, které jsou potřebné, abyste měli k těmto dokumentům přístup (například dohoda o zachování důvěrnosti – NDA), a nepožadujte jednoduše předložení těchto dokumentů v rámci odpovědi na RFP (tyto dokumenty by mohly být zpřístupněné veřejnosti na základě právních předpisů typu Open Records, což by mohlo ohrozit zabezpečení cloudu).

Vzor znění RFP: Soulad s předpisy

Vyřizování zakázek na cloudovou technologii lze zjednodušit používáním uznávaných standardů v oblasti zabezpečení, splnění předpisů a provozu, odvozených z doporučených postupů ohledně provozu cloudových služeb, včetně manipulace s daty, zabezpečení, důvěrnosti a dostupnosti dat apod.

<ORGANIZACE> *posoudí jedinečnou nabídku s ohledem na přijaté standardy zabezpečení, souladu s předpisy a provozu, jak jsou uvedeny níže a v* **Dodatku A**. *Když* **<ORGANIZACE>** *přihlédne k certifikaci souladu s každou normou, může návrh posoudit na základě minimálního souladu s normou.*

Když budete požadovat, aby CISP nadále zajišťoval soulad s minimálními standardy po celou dobu platnosti smlouvy, zajistíte si trvale aktuální soulad služby s předpisy.

CISP předkládající nabídku (přímo nebo prostřednictvím zprostředkovatele) by měl být schopen doložit svoji schopnost splnit následující atestace, zprávy nebo certifikace nezávislých třetích stran (poznámka: pokud se na poskytnutí některé z těchto atestací, zpráv nebo certifikací vztahují bezpečnostní omezení, bude <ORGANIZACE> spolupracovat s CISP na získání společného přístupu):

Certifikace a atestace	*Zákony, předpisy a ochrana soukromí*	*Harmonizace a právní rámce*
☐ *C5 (Německo)*		☐ *CDSA*
☐ *Kodex chování CISPE týkající se ochrany dat (GDPR)*		
☐ *CNDCP (Pakt o klimaticky neutrálních datových centrech)*		
☐ *DIACAP*	☐ *Směrnice EU o ochraně údajů*	☐ *CIS*
☐ *DoD SRG úroveň 2 a 4*	☐ *Standardní doložky EU*	☐ *Informační služby trestního soudnictví (CJIS)*
☐ *HDS (Francie, zdravotní péče)*		
☐ *FedRAMP*	☐ *FERPA*	☐ *CSA*
☐ *FIPS 140-2*	☐ *GDPR*	☐ *Štít soukromí EU-USA*
☐ *ISO 9001*	☐ *GLBA*	☐ *Zásady „bezpečného přístavu" EU*
☐ *ISO 27001*	☐ *HIPAA*	☐ *FISC*
☐ *ISO 27017*	☐ *HITECH*	☐ *FISMA*
☐ *ISO 27018*	☐ *IRS 1075*	☐ *G-Cloud [Spojené království]*
☐ *IRAP [Austrálie]*	☐ *ITAR*	☐ *GxP (FDA CFR 21 část 11)*
☐ *MTCS stupeň 3 [Singapur]*	☐ *PDPA – 2010 [Malajsie]*	☐ *ICREA*
☐ *PCI DSS úroveň 1*	☐ *PDPA – 2012 [Singapur]*	☐ *IT Grundschutz [Německo]*
☐ *SEC pravidlo 17-a-4(f)*	☐ *PIPEDA [Kanada]*	☐ *MARS – E*
☐ *SecNumCloud (Francie)*		
☐ *SOC1/ISAE 3402*	☐ *Zákon o ochraně soukromí [Austrálie]*	☐ *MITA 3.0*
☐ *SOC2/SOC3*	☐ *Zákon o ochraně soukromí [Nový Zéland]*	☐ *MPAA*
☐ *Kodex SWIPO IaaS*		
	☐ *Španělské schválení zákona o ochraně dat*	☐ *NIST*
	☐ *Britský zákon DPA o ochraně osobních údajů – 1988*	☐ *Úrovně organizace Uptime Institute*
	☐ *VPAT/oddíl 508*	☐ *Britské zásady cloudového zabezpečení*

Uvedený seznam slouží pouze k ilustračním účelům a neměl by být považován za vyčerpávající přehled veškerých certifikací a standardů, které se můžou na cloudové služby vztahovat.

2.3.1.1 Ochrana dat

Při používání cloudových služeb je klíčové, aby zpracování osobních údajů probíhalo v souladu s platnými právními předpisy EU ohledně dat, tj. obecného nařízení o ochraně údajů (GDPR). GDPR je regulace založená na všeobecných principech, a neobsahuje proto pro konkrétní sektory pokyny, jak zajistit plnění požadavků. Doporučuje však přijmout nástroje pro splnění předpisů, které takové pokyny budou obsahovat, například kodexy chování. Sdružení CISPE ve spolupráci s francouzským úřadem pro ochranu dat CNIL sestavilo kodex chování zaměřený na ochranu dat (Kodex CISPE[6]), schválený Evropským sborem pro osobních ochranu údajů a obecně použitelný v Evropě. Kodex má CISP pomoci dodržovat požadavky GDPR a zákazníky provést posuzováním, zda je poskytovatel CISP vhodný pro zpracovávání osobních údajů, které chce zákazník provádět.

- Kodex je zaměřen výhradně na sektor IaaS a pojednává o konkrétních rolích a odpovědnostech poskytovatelů IaaS.
- Pomáhá vyjasnit aspekty spravedlivého a transparentního zpracování a odpovídající bezpečnostní opatření v kontextu služeb cloudové infrastruktury (GDPR, článek 40 [2]).
- Zákazníkům pomáhá porozumět, jak si zachovat svrchovanost nad vlastními daty a zajistit, že jejich data zůstanou v EU.
- Propaguje doporučené postupy ohledně ochrany dat, které podporují iniciativu GAIA-X EU zaměřenou na vývoj evropských cloudových datových služeb.

Když CISP dodržuje kodexy chování ohledně ochrany dat, jako je Kodex CISPE, znamená to, že osobní údaje budou zpracovávány v přísném souladu s nařízením GDPR.

Vzor znění RFP: Ochrana dat

CISP předkládající nabídku (přímo nebo prostřednictvím zprostředkovatele) by měl být schopen doložit svoji schopnost splnit požadavky kodexu chování zaměřeného na ochranu dat. Takovým kodexem je například Kodex CISPE. Kodex musí být v souladu s požadavky uvedenými v rámcovém nařízení GDPR. Kodex by měl minimálně zahrnovat (1) jasnou definici rolí a odpovědností poskytovatele CISP, (2) požadavek, aby CISP nevyužíval data zákazníka k marketingovým nebo reklamním účelům, a (3) požadavek, aby zákazník měl možnost vybrat si služby CISP umožňující zpracování dat výhradně v Evropském hospodářském prostoru. Soulad s kodexem musí ověřit nezávislí externí auditoři (dozorové orgány) akreditovaní nezávislými externími auditory, kteří jsou akreditovaní evropským orgánem pro ochranu dat.

2.3.1.2 Změna poskytovatele cloudových služeb a přenos dat

Zákazníci by měli mít svobodu zvolit cloudové služby, které chtějí používat, namísto uzamčení ze strany poskytovatele nebo přímo v rámci služeb (PaaS/SaaS).

Cloudové služby zajišťované ze strany CISP jsou standardizované a nabízené na základě principu „jedna služba mnoha zákazníkům“, přičemž služby konfiguruje, zřizuje a kontroluje zákazník. Výhodou využívání cloudu je, že zákazník si může zvolit, které standardizované služby potřebuje, aby si mohl vytvořit jedinečné

[6] https://cispe.cloud/code-of-conduct/

aplikace a řešení. Výhoda se týká také možnosti přejít na nové nebo jiné služby, které v daný okamžik vyhovují zákazníkovým potřebám.

Podobně jako u ochrany dat, kodexy chování mohou zákazníkům garantovat možnost přejít do cloudu z místní infrastruktury nebo si zvolit jiného CISP. Společně se sdružením EuroCIO (evropské sdružení vedoucích pracovníků IT) se sdružení CISPE podílelo na sestavování kodexu chování zaměřeného na přenositelnost dat a možnost přechodu mezi cloudovými službami v rámci služeb IaaS (Kodex SWIPO IaaS[7,8]). První verze Kodexu byla sestavena v souladu s nařízením EU o volném pohybu údajů, které bylo Evropské komisi předáno v listopadu 2019 v období finského předsednictví a zveřejněno asociací SWIPO AISBL v květnu 2020. V dubnu 2021 organizace SWIPO AISBL potvrdila splnění kodexu prvními službami a v květnu 2021 bylo potvrzeno u prvních členských služeb sdružení CISPE.

Vzor znění RFP: Změna poskytovatele cloudových služeb a přenos dat

CISP předkládající nabídku (přímo nebo prostřednictvím zprostředkovatele) by měl být schopen doložit svoji schopnost splnit kodex chování zaměřený na přechod mezi poskytovateli a přenos dat. Takovým kodexem je například Kodex SWIPO IaaS. V kodexu musí být podrobně vysvětleno, jak CISP nabízí zákazníkům bezpečný přenos firemních dat, pokud se rozhodnou přejít k jinému poskytovateli.

2.3.2 Porovnání dodavatelů

Podobně jako u technických kritérií popsaných v předchozích sekcích, kromě minimálních požadavků na zabezpečení je důležité v RFP na cloudové služby uvést kritéria, podle kterých lze srovnat funkce a služby CISP při posuzování konkurence.

Příklady požadavků na CISP týkajících se zabezpečení uvádí *Dodatek A – Technické požadavky pro porovnání dodavatelů*. Důrazně doporučujeme subjektům ve veřejném sektoru posuzujícím CISP zohlednit v oblasti zabezpečení především následující funkce:

Vzor znění RFP: Co je třeba zohlednit v otázce zabezpečení

- *Zda CISP chápe model sdílené odpovědnosti a jakou dokumentaci k oddělení odpovědnosti za zabezpečení u funkcí a služeb CISP (například v kontextu GDPR) poskytuje zákazníkům*
- *Zda má CISP doloženou historii zabezpečení infrastruktury, včetně veřejně dostupné dokumentace nechráněné vlastnickými právy, s ohledem na jeho stav zabezpečení a fyzické či logické ochranné prvky*
- *Podpora CISP konkrétně zaměřená na zabezpečení cloudu*
- *Služby, které zákazníkům umožňují formalizovat návrhy účtů, automatizovat kontroly zabezpečení a správy cloudu a zefektivnit audit*
- *Možnosti vytvářet, zřizovat a spravovat sadu prostředků na základě šablon (včetně šablon zlatého standardu zabezpečení sestavených CISP nebo jeho partnery)*
- *Možnost zavést spolehlivé a opakovatelné fungování kontrolních prvků*
- *Funkce pro průběžné auditování v reálném čase*
- *Funkce pro technické skriptování zásad pro řízení cloudu*
- *Možnost vytvářet vynucovací funkce, které nemohou potlačit uživatelé bez povolení k úpravám*

[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/

- *Možnost realizovat spolehlivou implementaci toho, co bylo dříve sepsáno v zásadách, standardech či regulacích, spolu s vytvořením vynutitelného zabezpečení a souladu s předpisy, aby byl zajištěn funkční a spolehlivý model řízení cloudu pro prostředí IT*
- *Služby chránící před běžnými, nejčastěji prováděnými distribuovanými útoky typu odepření služby (DDoS) v síti a na transportní vrstvě, možnost vytvářet přizpůsobená pravidla ke zmírnění rizik spojených se sofistikovanými útoky na aplikační vrstvu*
- *Spravovaná služba detekce hrozeb*

2.3.3 Uzavírání smluv

Jak je uvedeno výše, smluvní podmínky CISP jsou sestaveny tak, aby odpovídaly fungování modelu cloudových služeb (nekupují se fyzické položky a CISP nabízejí standardizované služby v masivním měřítku). Je proto velmi důležité, aby smluvní podmínky CISP byly začleněny a používány v maximálním realizovatelném rozsahu. Další informace o smluvních podmínkách a uzavírání smluv najdete níže v oddíle *2.5*.

Co se týče zabezpečení, opět důrazně doporučujeme CISP, aby svoji nabídku průběžně aktualizovali, a dodavatelům, aby přidávali produkty po termínu předložení nabídky, pokud odpovídají původním parametrům v RFP. Důvodem je fakt, že funkce a služby v oblasti zabezpečení se rychle vyvíjejí a CISP často vydávají služby zaměřené na zabezpečení, které jsou často volně k použití. Upozorňujeme, že je důležité mít základní úroveň zabezpečení (viz minimální požadavky uvedené výše), aby bylo zajištěno, že změny v nabídce řešení pro zabezpečení nebudou mít negativní dopad.

Klíčovým prvkem zabezpečení v RFP na cloudové služby je samozřejmě model sdílené odpovědnosti. Každá smluvní strana musí mít jasnou představu o své odpovědnosti v oblasti zabezpečení. Je tedy třeba požadovat, aby CISP zdokumentoval povinnosti týkající se cloudových technologií, a to jak na straně CISP, tak na straně zákazníka. Také je požadováno, aby CSIP poskytli dokumentaci, která zákazníkům pomůže vytvořit a automatizovat doporučené postupy v oblasti zabezpečení.

Rámcová smlouva by měla zajistit flexibilitu k odchodu od dodavatele, pokud přestane plnit minimální požadavky na zabezpečení a pokud dojde k nesouladu s předpisy dle RFP na cloudové služby.

2.4 Ceny

Organizace z veřejného sektoru, které chtějí ve smlouvě na cloudové služby zohlednit kolísající poptávku, by měly požadovat smluvní garanci pro možnost placení za služby, které právě využívají. Poskytovatel by měl zajistit odpovídající systém řízení a viditelnost informací o využití a výdajích.

Je důležité, aby RFP na cloudové služby řešily hodnotu a celkové náklady na vlastnictví (TCO) oproti jednoduchému srovnání jednotkových cen jednotlivých položek. Tradiční přístup zaměřený na nejnižší jednotkovou cenu u cloudového modelu nefunguje a sám o sobě nezajistí ekonomicky nejvýhodnější tendr ani celkově nejnižší cenu.

Při výběru CISP se proto doporučuje nejdříve provést předběžný výběr kandidátů, který obsahuje jen ***minimální množství požadavků týkajících se cen****. Takto získáme skupinu CISP, jejíž členové disponují podobnými schopnostmi a možnostmi a se kterými lze uzavřít rámcovou smlouvu. V rámci objednávek a výběrových řízení malého rozsahu lze následně specifikovat typický příklad cloudové architektury a* ***cenového scénáře****, který odpovídá použití ve veřejném sektoru, a vyžádat si od CISP jejich cenové nabídky. Zadavatelé si také mohou nechat předvést testovací demoverze a porovnat fungování a elasticitu cloudových technologií nabízených jednotlivými CISP. Vzorový testovací scénář pro cloudové technologie najdete v dodatku B.*

2.4.1 Minimální požadavky

Část RFP na cloudové služby, která se týká cen, obsahuje čtyři hlavní prvky:

1. **Model placení podle spotřeby:** Zákazníci využívající cloud přijímají model průběžného placení za služby, kdy na konci každého měsíce jednoduše uhradí svoji spotřebu. Jedná se o optimální model vzhledem ke skutečnému využívání služeb a zdrojů.
2. **Transparentní ceny:** Ceny nabízené ze strany CISP by měly být veřejně dostupné a transparentní.
3. **Dynamický cenový model:** Tento flexibilní model umožňuje kolísání cen cloudových služeb podle aktuálních cen na trhu. Tento přístup představuje dynamickou a konkurenční metodu určování cen za cloudové služby a podporuje inovace a snižování cen.
4. **Kontrola nad výdaji:** CISP by měli zajistit nástroje pro reportování, monitorování a předpovídání, které zákazníkům poslouží (1) ke sledování využití a výdajů jak na souhrnné, tak na podrobné úrovni, (2) k zasílání výstrah v případě, že využití a výdaje překročí vlastní prahové hodnoty, a (3) k odhadování využití a výdajů kvůli plánování budoucích rozpočtů na cloud.

Vzor znění RFP: Ceny

<ORGANIZACE> požaduje, aby zúčastnění CISP uvedli navrhovaný způsob a cenový model pro každou službu poskytovanou koncovým uživatelům ve formě komerčního cloudu.

CISP dodá:

- *dokument s definicí služby nebo odkazy na definice služeb;*
- *dokument s obchodními podmínkami;*
- *Cenový dokument (odkazy na veřejné informace o cenách jsou přijatelné za předpokladu, že je na vyžádání k dispozici úplný ceník/cenový dokument).*

Cena bude odpovídat ceně nejběžnější konfigurace dané služby. CISP by měli poskytnout slevy za objem a nástroje pro cenové kalkulace, aby bylo možné zjistit skutečnou cenu nakupovaných položek a celkovou hodnotu poskytovanou kupujícímu (například vyčíslení úspory celkových nákladů u služby optimalizace).

Kupující v režimu Rámcové smlouvy mohou dodavatele oslovit a požádat je o dodatečné informace o popisech služby, obchodních podmínkách, cenách, definicích služby a modelech. O všech rozhovorech s dodavateli bude veden záznam.

Další požadavky pro stanovení cen

- *Poskytovatel musí nabízet cloudové technologie s dynamickým cenovým modelem, který zajišťuje maximální firemní flexibilitu a umožňuje škálovatelnost a růst.*
- *Cenová nabídka musí splňovat následující podmínky:*
  - *Jsou ceny stanoveny pomocí modelu „utility-style“, „pay-as-you-go“, tedy v modelu placení podle spotřeby? Popište a vysvětlete svůj cenový model.*
  - *Lze dosáhnout dalších slev, pokud se klient zaváže k určitému objemu nebo využívání služeb? Uveďte podrobnosti.*
  - *Je výše cen veřejně dostupná a transparentní? Uveďte odkazy na veřejně dostupné informace o cenách.*
  - *Je určování cen dynamické a reaguje rychle a efektivně na konkurenci na trhu?*
  - *Poskytujete doporučené postupy a zdroje ke sledování výdajů?*
  - *Poskytujete doporučené postupy a zdroje k optimalizaci nákladů?*

Transparentnost cen
*Protože ceny v oblasti komerčních cloudových technologií trvale klesají díky inovaci a konkurenci, sledované náklady na jednotku služeb CISP hrazené organizací **<ORGANIZACE>** podle rámcové smlouvy nikdy nepřekročí jednotkové ceny poskytovatele cloudu zveřejněné na jeho webu, které jsou platné v době, kdy službu využívá zákazník.*

Upozornění a sestavy týkající se rozpočtu a fakturace
*Aby CISP doložili dodávky a používání cloudových technologií, měli by organizaci **<ORGANIZACE>** poskytnout nástroje ke generování podrobných fakturačních zpráv, ve kterých jsou náklady rozepsané podle hodin, dní nebo měsíců, podle každého účtu v organizaci, podle produktů nebo produktových zdrojů nebo podle tagů definovaných zákazníkem. **<ORGANIZACE>** bere na vědomí, že v rámci modelu sdílené odpovědnosti za cloud bude **<ORGANIZACE>** odpovídat za využívání fakturačních funkcí a nástrojů, které CISP poskytuje a které umožňují tvorbu sestav a předpovědí.*

- *Vysvětlete, jak si **<ORGANIZACE>** může zobrazit informace o fakturaci na podrobné i souhrnné úrovni, vzorce výdajů na CISP v průběhu času a předpovědi budoucích výdajů.*
- *Vysvětlete, jak může **<ORGANIZACE>** filtrovat zobrazení využívání nebo fakturace podle služby, propojeného účtu nebo podle vlastních tagů aplikovaných na zdroje a jak může vytvářet výstrahy ohledně fakturace, když se využití služeb přiblíží nebo překročí limity nebo rozpočty definované organizací **<ORGANIZACE>**.*
- *Vysvětlete, jak může **<ORGANIZACE> na základě předchozího využívání** předpovídat, jak hodně bude cloudové služby využívat za určenou dobu. CISP by měl předložit **odhad** částky, kterou bude **<ORGANIZACI>** účtovat, a dát **<ORGANIZACI>** možnost používat výstrahy a rozpočty ohledně částek, které podle předpovědi vynaloží. To umožní organizaci větší kontrolu nad náklady a výdaji.*

2.4.2 Porovnání dodavatelů

Organizace ve veřejném sektoru při výběrových řízeních jako hodnotící kritérium často používají nejvyšší hodnotu, ekonomicky nejvýhodnější nabídku (MEAT) nebo nejnižší cenu. Při plánování cen v rámci objednávky nebo výběrového řízení malého rozsahu s cílem uzavřít rámcovou smlouvu je důležité zohlednit jedinečné charakteristiky cloudu. Je třeba chápat například fakt, že prosté srovnání řádkových položek v nabídkách různých poskytovatelů cloudu (například výpočetní prostředky nebo velikost úložiště) nepředstavuje efektivní způsob porovnání, protože nebere ohled na funkce, jako je výkonnost, optimalizace nákladů pomocí cloud-nativních služeb a monitorovacích nástrojů CISP, případně na služby, které poskytovatel na rozdíl od jiných nabízí zdarma. Kromě toho může katalogová cena CISP zahrnovat desítky tisíc řádkových položek a také cenové modely se mohou u jednotlivých služeb a poskytovatelů lišit.

Analýza celkových nákladů na vlastnictví (TCO)

U definovaných případů použití doporučujeme, aby se zákazník zaměřil na celkové náklady na vlastnictví (TCO). Ty totiž zohledňují veškeré aspekty cloudového řešení (včetně služeb partnerů, standardizovaných slev CISP, technických funkcí zvyšujících efektivitu a nákladů na redukci či optimalizaci apod.).

Srovnání podle scénářů

Při posuzování lze zvážit typické scénáře, které odpovídají běžným systémům nebo aplikacím. Takové scénáře (například hostování webu nebo implementace systému lidských zdrojů s x uživateli apod.) můžou zahrnovat proměnné jako rychlost a měřítko prostředků, výkon aplikace nebo řešení, přístupové doby úložiště, úlohy s komplexními daty a nízkým objemem oproti jednoduchým úlohám s vysokým objemem apod. Typické scénáře se mohou týkat také aplikací nebo systémů, například zpracování velkého objemu při podání daňových přiznání nebo nouzová upozornění jako varování před povodní. Scénáře by měly pokrývat kompletní rozsah technologií a služeb, které zákazník může během projektu použít. Zákazník díky tomu dokáže srovnat odhadované celkové náklady na projekt.

Finanční a technické srovnání scénářů

Při srovnávání různých nabídek CISP je důležité zohlednit také technické výhody. Určitý CISP například může dávat zákazníkům možnost sestavit topologii zotavení po havárii (DR) typu aktivní/aktivní, protože má datová centra v určité geografické oblasti v clusterech. CISP, který nemá takovou redundanci a konfiguraci datových center, by mohl být dražší o x % kvůli nákladům spojeným se zajištěním služby zotavení po havárii. Jako příklad, proč je při posuzování CISP holistický přístup k cenám se zahrnutím dodatečných technických funkcí klíčový, může posloužit níže uvedený příklad.

Příklad: Zákazník chce porovnat cenu na úložiště objektů u několika CISP splňujících podmínky Rámcové smlouvy. Položková cena za „jednotku" úložiště u CISP č. 1 je 0,023 EUR za GB. Cena stejné „jednotky" u CISP č. 2 je 0,01 EUR za GB. Při prostém srovnání jednotek by si zákazník nepoložil klíčové otázky, například:

1. Kolik redundantních kopií objektu je dostupných v případě selhání? V uvedeném případě je CISP č. 1 nastaven tak, aby vydržel současnou ztrátu dat ve dvou různých zařízeních, a uchovává víc kopií dat. U CISP č. 2 se redundantní kopie nevytvářejí.
2. Jaká je úroveň udržitelnosti uložených objektů? U CISP č. 1 je to 99,999999999 %, u CISP č. 2 99 %.
3. Zaměřte se na náklady po celou dobu vlastnictví celkového projektu nebo úlohy a na to, jak funkce pro optimalizaci nákladů mohou snížit náklady spojené s uložením a používáním dat (například zvýšením používání funkcí Serverless lze u CISP snížit náklady o x %).

Toto jsou pouze některé z mnoha dalších technických aspektů, které mají návaznost na cenu a které se týkají zabezpečení a souladu s předpisy.

Jaké by měly být cenové scénáře

Základní sazby – jedná se v podstatě o veřejné ceny CISP. CISP by měli tyto ceny uvádět veřejně. Jak jsme ale uvedli výše, k efektivnímu srovnání poskytovatelů mohou zákazníci všechny dodavatele požádat o nacenění 3 až 5 konkrétních scénářů (případně tolika, kolik jich je pro zákazníka smysluplných). Scénáře by měly být vyčerpávající, aby pokryly šíři služeb a technologií, které bude zákazník v průběhu projektu pravděpodobně využívat. Zákazník díky tomu dokáže srovnat odhadované celkové náklady na projekt. Srovnání na úrovni řádkových položek nebo skladových jednotek bývá pro zákazníky i dodavatele spíše problematické než užitečné (zákazníci by museli srovnávat desítky tisíc řádkových položek u všech CISP a dodavatelé by museli předkládat a spravovat takto podrobné informace, ačkoli skutečná cena je určena až na základě spotřeby služeb).

Zákazníci, kteří chtějí z cloudu získat nejvyšší hodnotu, musí posoudit celkovou sadu možností každého CISP. CISP například mohou nabízet řadu služeb, které jsou buď zdarma, nebo v podstatě zdarma, a posouzení cen by mělo takové služby zohlednit, protože jiní poskytovatelé mohou za podobné funkce účtovat poplatky.

Hodnotící kritéria mohou být navržena tak, aby měli CISP možnost uvést funkce, které jsou již zahrnuté a výchozí, a jaký je jejich dopad na celkové náklady. Hodnotící kritéria mohou přihlížet také k určování cen podle objemu nebo úrovně a ke komerčně dostupným slevám, jako jsou rezervované instance nebo spotové instance. Příklad:

- úspora x %, pokud si zákazníci zakoupí rezervovanou výpočetní kapacitu (1 rok, 3 roky apod.)
- sleva x % při vázaných cenách nebo při určitém objemu

- úspora x % na základě revizí a optimalizace infrastruktury, například přechod na lépe vyhovující výpočetní modul
- Jak bylo uvedeno výše, zaměřte se na náklady za celou životnost a na to, jak mohou funkce pro optimalizaci nákladů snížit vaše výdaje.

CENOVÉ SCÉNÁŘE

Uchazeči musí uvést ceny pro následující scénář, a to pouze pro hodnotící účely. Skutečná cena bude vycházet ze spotřeby služeb v modelu placení za spotřebované služby (pay-per-use).

Níže jsou uvedeny požadavky, které poslouží k účelům zjišťování cen. Jsou uvedeny s vědomím, že během trvání smlouvy se tyto nominální požadavky změní. Uveďte prosím výši cen při platbě za použití (on-demand) na 12 a 36 měsíců a za 12 a 36 měsíců s rezervovanou kapacitou.

Uveďte:

- *Název navrhovaného řešení:*
- *Nejvýhodnější cena uchazeče:*
- *Provozní doba: 24x7x365*
- *Dostupnost služeb: 99,95 %*

Scénáře týkající se služeb mohou zahrnovat také příklady od stávajících zákazníků s podobnými úlohami, kteří si optimalizovali náklady na dobu jednoho, dvou nebo tří let, a to využíváním monitorovacích a optimalizačních nástrojů od CISP, přijetím optimalizovaných řešení nativních pro cloud a také snížením cen ze strany CISP.

2.5 Uzavření smlouvy a smluvní podmínky

Cloudové technologie a operace zajišťované ze strany CISP jsou od základu standardizované, a proto jsou standardizované také smluvní podmínky. Existuje však možnost tyto smlouvy mírně upravit kvůli místní legislativě a regulačnímu kontextu.

Standardní způsoby zadávání zakázek v oblasti IT často zahrnují přísná pravidla, podle kterých uchazeč musí vyhovět mnoha nebo všem požadavkům, pokud nechce být vyřazen. Případně mohou požadavky zahrnovat přísnou dílčí sadu povinných položek. Když se tento způsob obstarávání zdrojů použije u cloudových technologií, které ve skutečnosti představují sadu standardizovaných součástí a nástrojů sloužících k vybudování vlastního řešení, zadávání zakázky bývá neúspěšné.

2.5.1 Smluvní podmínky

S ohledem na uzavření smlouvy a vytvoření RFP na cloudové služby je nutné si nejprve projít a pochopit stávající obchodní podmínky CISP, které lze v mnoha případech najít na jejich veřejných webech. Organizace ve veřejném sektoru stále ochotněji přijímají komerční podmínky CISP. Součástí tohoto úsilí o porozumění podmínkám je setkat se s CISP a jejich partnery a udělat si lepší představu o jejich přístupu. Klíčová otázka je, „proč“ CISP stanovují konkrétní podmínky. Některé z podmínek se zdají být odlišné od tradičních podmínek v oblasti IT, pro to ale existují velmi specifické důvody. Pokud veřejně dostupné podmínky nejsou přijatelné, CISP je pro podnikové zákazníky často mohou mírně upravit.

Kromě seznámení s podmínkami CISP je důležité porozumět stávajícím zásadám, regulacím a právním předpisům (těm, které se týkají technologie, klasifikace dat, soukromí, zaměstnanců apod.). Často jsou k dispozici stávající zásady, regulace nebo právní předpisy upravující nákup a využití tradičních nabídek IT, které nemusí vyhovovat modelu CISP. Příkladem je povolení používat pouze cloudové technologie, které byly uvedené v RFP

na cloudové služby. CISP průběžně přidávají nové služby a funkce. Zablokování přístupu k těmto novým službám jen proto, že používáte tradiční přístup k obnovování IT produktů, pro koncového zákazníka nedává smysl. V takovém případě je nutné s CISP tyto zásady, regulace a právní předpisy podrobně probrat.

Jakou výhodu mají diskuze před sestavením RFP

Jak je uvedeno výše, před sepsáním RFP věnujte čas na setkání s CISP a souvisejícími dodavateli, abyste porozuměli jejich smluvním podmínkám a seznámili je s přístupem vašeho subjektu a souvisejícími zásadami, regulacemi a právními předpisy. Nejdůležitější součástí těchto diskuzí pro obě strany je zjistit, „proč" příslušné podmínky fungují tak, jak fungují. Smluvní podmínky týkající se cloudu se například liší od tradičních podmínek spojených s datovým centrem, spravovanou službou, hardwarem, krabicovým softwarem a systémovou integrací. Protože jde o jediný model, který zahrnuje průběžné inovace, obchodní modely vyžadují, aby proces RFP byl dostatečně flexibilní a dával prostor na vyjednávání či diskuze k vyjasnění otázek.

Když si organizace ve veřejném sektoru ponechají možnost vyjasnit si smluvní podmínky v diskuzích a vyjednáváních, lépe porozumí cloudovým modelům a vyhnou se tomu, že by odmítly poskytovatele, kteří jsou ve skutečnosti schopní splnit jejich potřeby. Typicky to probíhá například tak, že organizace předem stanoví určité podmínky, o kterých je ochotná před volbou dodavatele diskutovat a vyjednávat. Když s uchazeči předem jedná o přijatelných podmínkách, získává organizace jistotu, že zvolí toho nejlepšího a vyřeší rozdíly, které by jinak mohly vést k odmítnutí přijatelného návrhu. Subjekty ve veřejném sektoru také mohou projít své zásady, regulace a právní předpisy a obě strany pak spolu mohou porozumět tomu, jak těmto modelům přizpůsobit používání cloudu. Často je nejlepší možností úprava stávajících ustanovení. Pokud je však nějaká oblast problematická, mohou oba týmy spolupracovat na hledání řešení (je lepší tyto diskuze realizovat v dostatečném předstihu před vyjednáváním o RFP a následným vyjednáváním o smlouvě).

Flexibilita při vyjednávání

Aby bylo možné podepisovat smlouvy v souladu s místní legislativou a současně se opírat o standardizované smluvní podmínky CISP, doporučuje se (1) vyžádat si od uchazečů jejich standardní smlouvu, (2) nezavádět při vytváření rámcové smlouvy k RFP na cloudové služby nevhodné smluvní podmínky a (3) ponechat možnost vyjednávání o všech ustanoveních o konzultacích a návrzích, ze kterých vzejde rámcová smlouva (samozřejmě s výjimkou povinných ustanovení vyžadovaných právními předpisy).

Upozornění: Smluvní podmínky by měly odrážet rozsah sdílené odpovědnosti, který je s cloudovým modelem nezbytně spojený (například CISP potvrdí, že zákazníci vlastní svá data tam, kde jsou uložena, a poskytne nástroje omezující volbu ohledně umístění dat – ALE – odpovědnost používat tyto nástroje je na straně zákazníka nebo partnera).

Vezměte prosím na vědomí, že je důležité, aby pro každý typ služby byly k dispozici ***odlišné soubory smluvních podmínek****. Přístup typu „jedna smlouva na všechny typy služeb" povede nutně k problémům s technickou proveditelností a kompatibilitou.*

Jak už jsme uvedli, RFP zahrnující povinné podmínky, o kterých nelze jednat, pro poskytovatele v podstatě představují návrh „ber, nebo nech být", kvůli kterému mohou odmítnout jinak přijatelné návrhy. Organizace ve veřejném sektoru by měly pečlivě zvážit, jaké následky bude mít použití povinných podmínek, pokud je nevyžadují právní předpisy. Organizace by měly mít jistotu, zda je povinný požadavek nebo podmínka opravdu potřeba, protože jejich označením za povinné se vylučuje další vyjednávání. Povinné požadavky

nebo podmínky by se měly využívat v absolutně minimální míře, aby si organizace udržely flexibilitu pro získání nejlepší technologie a řešení.

Nezapomínejte, že cloudové technologie CISP jsou kompletně standardizované a dodávají se plně automatizovaným způsobem. CISP proto není schopen provádět takové změny smluvních podmínek, které by vyžadovaly přizpůsobení základových služeb. Kromě toho jsou ceny služeb zpravidla veřejné a standardizované pro všechny uživatele, a CISP proto nemůže upravovat ceny tak, aby na sebe vzal větší část rizika u konkrétního zákazníka.

Nepřímé nákupy

Další možnost vedle zakoupení cloudových technologií přímo od CISP je zakoupit je od prodejce CISP. Další informace o CISP najdete výše v oddíle *2.1.3*.

Vzor znění RFP: Smluvní podmínky

*CISP nebo reprezentativní dodavatelé musí předložit své veřejně dostupné smluvní podmínky a vyjádřit se k hlavním podmínkám předloženým <**ORGANIZACÍ**>.*

*Záměrem **<ORGANIZACE>** je uzavřít písemnou smlouvu s úspěšným uchazečem na základě jeho smluvních podmínek. Uchazeč by měl **<ORGANIZACI>** předložit k prostudování navrhované smluvní podmínky, které představují jeho nejlepší návrh z komerčního i právního hlediska. Předkladatelé nabídky a **<ORGANIZACE>** mohou ve fázi **<DISKUZÍ/VYJEDNÁVÁNÍ>** probrat oboje smluvní podmínky.*

- *Klíčová témata obecné rámcové smlouvy by měla být tato:*
  - *Trvání rámce*
  - *Řízení rámce*
  - *Fungování rámce*
  - *Ukončení rámce*
  - *Rozsah rámce*
  - *Proces zadávání objednávky*
  - *Ustanovení o důvěrnosti*
  - *Práva na duševní vlastnictví a informace podle kategorie*
  - *Jaké minimální technické požadavky musí CISP splnit, například standardy kvality, akreditace, zabezpečení a ochrana dat*
- ***Podmínky se budou lišit pro každou dávku v rámci rámcové smlouvy.***
- *Specifika ohledně služeb CISP, která lze posoudit, budou vyřešena během dílčí objednávky.*
- *Prostor pro změny ve smlouvě – podmínky by neměly omezovat zákazníky a dodavatele v případech změn smlouvy, které jsou nutné pro přidání nových služeb nebo vylepšení. Cloudové služby se velice rychle vyvíjí, a budou průběžně zpřístupňována vylepšení služeb, která mohou zákazníkům zvýšit efektivitu.*
- *Zákazník by neměl určovat smlouvy o úrovni služeb (SLA). Smluvní podmínky zákazníka by neměly vymezovat smlouvy o úrovni služeb (SLA) přizpůsobené jednotlivé zakázce, které se liší od standardních modelů dodávání služeb CISP. Když zákazník akceptuje standardní smlouvy o úrovni služeb (SLA), budou CISP schopní udržet nízké ceny a zajistit je zákazníkům, kteří navíc získají jistotu, že poskytovatel vyhoví podmínkám těchto smluv.*
- *Limity odpovědnosti by měly být přiměřené. Odpovědnost by měla odpovídat kupovaným službám a limity odpovědnosti by neměly být nepřiměřeně vysoké. Pokud budou limity odpovědnosti nepřiměřeně vysoké, CISP nebudou motivováni k přijímání projektů s nízkou hodnotou. Tyto projekty jsou často „testovací“ a slouží pro zahájení spolupráce. Zákazníci dle nich mohou posoudit, zda jsou určitá cloudová řešení vhodná pro jejich organizaci.*

- *Zákazníci by měli být vlastníky svých dat. Měli by proto mít nad svými vlastními daty kontrolu a také by měli určovat, ve které geografické lokalitě budou data uložena. Zákazníci se tak vyhnou uzamčení a budou mít možnost svobodně přesunout data k novým poskytovatelům.*

2.5.2 Smluvní podmínky na software

Ačkoli se tato příručka soustředí na nákup cloudových technologií IaaS a PaaS poskytovaných ze strany CISP, je důležité zaměřit pozornost také na smluvní podmínky k softwaru, které mohou pomoci organizacím z veřejného sektoru při nákupu softwaru od dodavatelů. Obrázek 1 (str. 5) ukazuje nákup softwaru v rámci kvalitně sestavené RFP na cloudové služby.

Software hraje klíčovou roli téměř v každé firmě, veřejný sektor nevyjímaje. Pokud subjekty veřejného sektoru do RFP na cloudové služby zahrnou také např. licenční podmínky na software, zajistí si nejvyšší možnou hodnotu a svobodu zvolit si dodavatele i při nákupu softwaru.

Dále uvádíme Deset zásad spravedlivého licencování softwaru pro zákazníky cloudových služeb[9]. Tyto zásady sestavila organizace Cigref[10], sdružující významné francouzské společnosti a orgány veřejné správy zastupující uživatele digitální technologie, ve spolupráci se sdružením CISPE a za podpory dalších evropských oborových sdružení vedoucích pracovníků a poskytovatelů IT, a to v reakci na praktiky, které obě sdružení považují za škodlivé vůči digitální transformaci organizací nejrůznějších velikostí, které přecházejí do cloudu.

Vzor znění RFP: Software

*Záměrem **<ORGANIZACE>** je uzavřít písemnou smlouvu s úspěšným uchazečem na základě jeho smluvních podmínek. Uchazeč by měl **<ORGANIZACI>** předložit k prostudování navrhované smluvní podmínky, které představují jeho nejlepší návrh z komerčního i právního hlediska. Dodavatelé softwaru a **<ORGANIZACE>** mohou ve fázi **<DISKUZÍ/VYJEDNÁVÁNÍ>** probrat smluvní podmínky pro obě oblasti.*

***Požadavek 1.0.** Dodavatelé softwaru musí uvádět jasné licenční podmínky, včetně rozdělení nákladů na souhrnné a podrobné úrovni.* ***Požadavek 1.1.** Veškeré poplatky spojené s nedodržením licenčních podmínek musí být uvedeny na souhrnné a podrobné úrovni.*
***Požadavek 2.0.** Licence na software musí organizaci **<ORGANIZACE>** dávat možnost přesunout licencovaný software z místního umístění do zvoleného cloudu, aniž by si ke stejnému softwaru musela kupovat samostatnou, duplicitní licenci.* ***Požadavek 2.1.** Licence na software nesmí zahrnovat licenční omezení a zvýšené náklady, které by omezily možnost **<ORGANIZACE>** používat licencovaný software ve zvoleném cloudu.*
***Požadavek 3.0.** Licence na software musí organizaci **<ORGANIZACE>** povolovat provozování licencovaného softwaru na vlastním hardwaru (zpravidla označováno jako „místní" software) a také ve zvoleném cloudu.*
***Požadavek 4.0.** Licence na software nesmí vyžadovat, aby byl licencovaný software provozován pouze na hardwaru určeném výhradně pro **<ORGANIZACI>**.*

[9] https://www.fairsoftware.cloud/principles/
[10] https://www.cigref.fr/

Požadavek 5.0. *Dodavatelé softwaru nesmí* ***<ORGANIZACI>*** *penalizovat v případě, že se jejich licencovaný software používá v cloudové nabídce jiného dodavatele, například tak, že by si vyhrazovali právo provádět pokročilé nebo hloubkové audity softwaru nebo stanovili vyšší licenční poplatky za software.*
Požadavek 6.0. *Adresářový software musí podporovat otevřené standardy pro synchronizaci a ověřování identit uživatelů. Musí tak činit nediskriminačním způsobem vzhledem k jiným službám pro zajištění identity.*
Požadavek 7.0. *Dodavatelé softwaru nesmí účtovat různou cenu za stejný software pouze na základě toho, kdo vlastní hardware, na kterém je software instalován.* ***Požadavek 7.1.*** *Ceny za software nesmí rozlišovat mezi softwarem nainstalovaným ve vlastním datovém centru* ***<ORGANIZACE>****, v datovém centru spravovaném třetí stranou, na počítačích pronajatých od třetí strany nebo od poskytovatele cloudu zvoleného organizací* ***<ORGANIZACE>****.*
Požadavek 8.0. *Během trvání smlouvy nesmí dodavatelé softwaru provádět podstatné změny licenčních podmínek, které by organizaci* ***<ORGANIZACE>*** *zakazovaly dříve povolená použití, kromě případů, kdy to vyžadují právní předpisy nebo v případě vzniku bezpečnostních rizik.*
Požadavek 9.0. *Dodavatelé softwaru nesmí* ***<ORGANIZACI>*** *uvádět v omyl prohlášeními, že licence na software pokrývají potřeby používání softwaru podle záměrů* ***<ORGANIZACE>****, jak jsou uvedené v části* ***<POŽADAVKY ORGANIZACE>****, pokud takové používání může vyžadovat nákup dalších licencí.*
Požadavek 10.0. *Pokud* ***<ORGANIZACE>*** *mají právo licence na software dále prodávat a převádět, musí dodavatelé softwaru dál za férových podmínek poskytovat podporu a aktualizace organizaci* ***<ORGANIZACE>****, která legálně získala přeprodanou licenci.*

2.5.3 Jak u konkrétního projektu vybrat mezi dodavateli

Subjekty veřejného sektoru, které jsou smluvní stranou rámcové dohody, si mohou vyžádat resp. „objednat“ služby, které potřebují. Při vytvoření objednávky na základě rámcové smlouvy mohou kupující upřesnit své požadavky pomocí dodatečné funkční specifikace. Zároveň si však kupující zachovávají výhody nabízené v rámci Rámcové smlouvy.

Pokud to bude považováno za nutné, je možné uspořádat výběrové řízení malého rozsahu s cílem určit nejlepšího dodavatele pro určité aplikace nebo projekty. Výběrové řízení malého rozsahu je proces, při kterém zákazník realizuje další soutěž na základě Rámcové smlouvy. Tuto soutěž spouští tak, že vyzve všechny dodavatele v rámci jednoho typu služby, aby odpověděli na soubor požadavků. Zákazník vyzve všechny schopné dodavatele v rámci daného typu služby k podání nabídky. U daného typu služby hrají nyní důležitou roli minimální požadavky, které splňují dodavatelé vybraní v rámci RFP na cloudové služby. Tím je zajištěn vysoký standard všech nabízených variant pro každý typ služby.

Znovu upozorňujeme, že je důležité mít samostatné smluvní podmínky pro každou kategorii uvedenou pro Typ nabídky (například veřejná infrastruktura IaaS/PaaS, komunitní infrastruktura IaaS/PaaS, privátní infrastruktura IaaS/PaaS), protože přístup „jedna smlouva na všechno“ povede nutně k potížím s technickou proveditelností a kompatibilitou.

Vzory znění RFP týkající se výběru mezi dodavateli najdete v části *2.1.4*.

2.5.4 Zahájení a ukončení spolupráce

Při vytváření rámcové smlouvy je třeba využít Dynamický nákupní systém (DNS). Při použití modelu DNS budou mít do rámce přístup všichni dodavatelé, kteří splňují požadavky Rámcové smlouvy. Na to, kolik dodavatelů se může do rámce zapojit, není stanoven pevný limit. Navíc, na rozdíl od běžných rámcových modelů, mohou dodavatelé zažádat o vstup do „rámce DNS" kdykoli během jeho trvání.

Subjektům ve veřejném sektoru důrazně doporučujeme, aby stanovily standardy k zajištění kvality a zajištění služby od způsobilých dodavatelů, avšak nikoli takovým způsobem, že by předem vyřazovaly konkrétní CISP a bránily spravedlivé konkurenci. Konečným cílem je zabránit tomu, aby byl koncový uživatel přehlcen obrovským množstvím možností, a současně udržet vysoký standard dostupných cloudových technologií.

3.0 Osvědčené postupy a získané zkušenosti

Níže uvádíme některé poznatky k uzavírání Rámcové smlouvy s pomocí kvalitně sestavené RFP na cloudové služby.

3.1 Řízení cloudových služeb

Řízení cloudu představuje sdílenou odpovědnost. CISP dávají k dispozici funkce a služby, se kterými lze řízení cloudových služeb integrovat do každého aspektu cloudového prostředí. Zákazníci si současně přinášejí vlastní standardy ohledně řízení cloudových služeb a zjišťují možnosti pro řízení cloudu.

Díky cloudu získají zákazníci možnost vytvořit si vlastní IT prostředí dle svých požadavků. Nejde tedy pouze o změnu ve správě stejného prostředí. Cloud umožňuje zákazníkům: (1) začít s úplným inventářem všech IT prostředků; (2) spravovat všechna tato aktiva centrálně a (3) vytvářet výstrahy týkající se používání/fakturace/zabezpečení/atd. Všechny tyto důležité výhody cloudu pomáhají zákazníkům mít optimalizovanou – a v plném rozsahu automatizovanou – architekturu bez nutnosti neustále obstarávat a instalovat nový hardware. Tyto činnosti realizuje CISP, který tak zákazníkům umožňuje přesunout pozornost od řízení infrastruktury a zaměřit se na klíčové provozní činnosti.

Jedním z užitečných způsobů, jak se dívat na cloudové prostředí CISP je, že se jedná o velmi velké rozhraní API. Ať už spouštíte nový server, nebo měníte nastavení zabezpečení, dochází k volání systémového rozhraní API. Každá změna prostředí je zaprotokolována a zaznamenána (u každé změny je zaznamenáno kdo, co, kde a kdy). Probíhá tak automaticky správa, kontrola a zajištění viditelnosti, které lze zajistit pouze v prostředí cloudu. Zákazníci zde mají možnost zamyslet se nad stávajícím modelem řízení IT a určit, jak jej s pomocí cloudu zjednodušit a zlepšit.

Řízení cloudových služeb může také zahrnovat informace o pozitivních změnách procesů nebo o nových sadách dovedností získaných díky cloudu. Projektoví manažeři znají situace, kdy čekají několik měsíců na vybudování nového IT prostředí. S využitím cloudu lze vytvořit vývojové nebo testovací prostředí během několika minut. Adaptace na tento nový způsob fungování bude probíhat postupně po jednotlivých programech. Doporučujeme, aby odpovědné osoby předávaly získané zkušenosti ostatním. Rámcová smlouva a její požadavky se tak budou moci dále vyvíjet s ohledem na nové procesy a schopnosti.

3.2 Sestavení rozpočtu

Placení cloudových služeb podle využití (pay-as-you-use) má ve veřejném sektoru svá specifika spojená s akvizicí a rozpočtem. Podle našich zkušeností je výhodné spojit všechny služby CISP do jediné rozpočtové položky. Výpočetní služby, úložiště, sítě, databáze, IoT apod., to vše lze zahrnout do jediné položky s názvem

Cloudové technologie. Tento přístup zajišťuje flexibilitu a nabízí uživatelům všechny aktuální a nové technologie CISP v reálném čase. Zároveň tento způsob dává uživatelům rychlý přístup k nezbytným zdrojům v okamžiku, kdy je potřebují. Kromě toho zohledňuje kolísající poptávku a napomáhá tak optimalizovat využití a náklady.

Organizace ve veřejném sektoru si mohou přidat další položky z jiných typů služeb dle Rámcové smlouvy. Může jít o konzultační, odborné či spravované služby, software z tržiště marketplace, služby technické cloudové podpory nebo školení týkající se produktů CISP.

Ještě flexibilnější smluvní model lze navrhnout s využitím doplňkových řádkových položek, které mohou v rámci daných kategorií zohledňovat budoucí růst. Pokud by organizace chtěla spojit cloudové technologie a konzultační, odborné či spravované služby, je možné tak učinit a řádkovou položku nazvat „cloudové technologie a pomocné práce".

Níže je uvedena ukázka takového přístupu. V následujícím příkladu má každá řádková položka „č. 1001 – cloudové technologie" hodnotu 1,00 EUR. Každý měsíc lze pak hradit objednávky podle aktuálního a předpovídaného využití.

Tabulka 3 – Příklad cenové struktury jednořádkových položek.

Č. POLOŽKY	DODÁVKA/SLUŽBY	MNOŽSTVÍ	JEDNOTKA	JEDNOTKOVÁ CENA	ČÁSTKA
1001	Cloudové technologie	1 000	ks	1 EUR	1 000 EUR
1002	Poradenské služby	1	za týden	3 000 EUR	3 000 EUR
1003	Podpora cloudu	1	za měsíc	1 000 EUR	1 000 EUR
1004	Školení na cloud	1	za den	3 EUR	3 000 EUR
1005	Cloudové tržiště marketplace	10	ks	10 EUR	100 EUR

Příklad, jak tato struktura může fungovat: Organizace z veřejného sektoru se obrátí na CISP, aby odhadl, jaký objem služeb cloudové technologie organizace využije. Organizace souhlasí s podmínkami dodavatele, například 10 milionů EUR za 5 let, tj. 2 miliony EUR za rok. Organizace se zaváže k úvodní částce 2 milionů EUR za rok. Každý měsíc přijde faktura a částka se uhradí z dostupných finančních prostředků. Částka se strhne z příslušného účtu. U zbývajících prostředků se pomocí monitorovacích a prognostických nástrojů CISP sleduje jejich vynakládání. Pokud bude množství zbývajících financí nízké, organizace si vyžádá další prostředky od finančního ředitele, který má na starosti správu služeb.

Vzor znění RFP: Uzavírání smluv

PLATEBNÍ PODMÍNKY

*Platební podmínky musí být sestavené tak, aby byly hrazeny pouze prostředky, které **<ORGANIZACE>** využije, jak je popsáno níže:*

1. *Měsíční platba bude vycházet ze skutečného využití či spotřeby služeb podle veřejně dostupné výše cen CISP.*

MINIMÁLNÍ ZÁRUKA A MAXIMÁLNÍ VÝDAJE

*Protože **<ORGANIZACE>** není schopná určit, jak velký objem prostředků od poskytovatele cloudových služeb přesně spotřebuje za určitou dobu, objednávky budou uvádět množství jednotek s pevnou cenou u jednořádkové položky „cloudových technologií".*

*Každá jednotka objednané řádkové položky bude odpovídat ceně **<1,00 EUR>** objednaných cloudových technologií. Formou úpravy této objednávky budou pravidelně zasílány doplňkové objednávky na různá množství tak, aby **<ORGANIZACE>** mohla flexibilně předobjednávat různá „množství v eurech" cloudových technologií CISP na základě odhadovaného využití a s ohledem na potřeby, které trvají různou dobu. **<ORGANIZACE>** bude pravidelně předobjednávat množství dostatečné k pokrytí odhadovaných nákladů na cloudové technologie, které budou využity ke splnění různých požadavků.*

Č. položky	Popis	Množství	Jednotka	Cena
01	Cloudové technologie CISP	1 000	EA	1 000,00 EUR

MINIMÁLNÍ OBJEDNÁVKA A DOPLŇKOVÁ OBJEDNÁVKA

*Objednávky budou podávané pravidelně na různé množství z **<10 000>** jednotek řádkových položek podle odhadovaného využití cloudových technologií ze strany **<ORGANIZACE>**. Toto nastavení zajistí organizaci **<ORGANIZACE>** flexibilní možnost objednat předběžně **<10 000>** jednotek „cloudových technologií" pro pokrytí provozních potřeb a dál u cloudových technologií používat režim „pay as you go (placení podle spotřeby)".*

*Při podávání objednávky podle rámcové smlouvy bude objednáno úvodní dodatečné množství **<100 000>** jednotek za cenu **<100 000 EUR>**. Minimální počet celkových jednotek řádkových položek, které lze zahrnout do jedné doplňkové objednávky s jednou nebo více řádkovými položkami, je **<x>**. Maximální počet jednotek, které lze objednat v rámci dodací objednávky, nesmí překročit **<x>**, ale při kombinaci se všemi předchozími objednanými jednotkami nesmí překročit hodnotu objednávky podle Rámcové smlouvy. **<ORGANIZACE>** bude odpovídat za to, aby žádné objednávky nepřesahovaly limity stanovené v tomto oddíle.*

MAXIMÁLNÍ OBJEDNÁVKA

*Celková maximální hodnota objednávky je **<x>** a může zahrnovat maximálně **<x>** jednotek jednořádkových položek s cenou **<x>** za jednotku. Hodnota vychází z odhadovaných požadavků **<ORGANIZACE>** za období plnění, ale není zaručena.*

3.3 Porozumění obchodnímu modelu zahrnujícímu partnery

Subjekty ve veřejném sektoru by se měly pokusit porozumět modelům, podle kterých CISP poskytují své nabídky, a uvědomit si, že kritické místo v tomto procesu zaujímají partneři zajišťující konzultační služby, spravované služby, následný prodej a další služby. Mnozí zákazníci požadují poskytovatele cloudových služeb pro svoji infrastrukturu a outsourcují „administrativní" úlohy plánování, migrace a správy systémovému integrátorovi (SI) nebo poskytovateli spravovaných služeb. Při tomto mixu „služeb" se můžou vyskytnout požadavky, které se poskytovatelů cloudových služeb netýkají, například ustanovení týkající se subdodavatelů.

Příklad ustanovení týkajících se dodavatelů ukazuje, proč je důležité chápat, jak partneři a druhotní prodejci působí ve vztahu k CISP. Některé typy zprostředkování zakázek zahrnují ustanovení vyžadující, aby hlavní dodavatel přenesl některá povinná ustanovení na všechny své partnery nebo subdodavatele. CISP zpravidla neposkytují a nenabízejí služby jako formální partneři v roli subdodavatelů, protože poskytují standardizovanou službu v obrovském měřítku, přičemž tato služba není přizpůsobená podle jedinečných požadavků konkrétního koncového zákazníka (včetně potřeb zákazníka z veřejného sektoru v rámci veřejné zakázky). V modelu nepřímého zadávání zakázky (zajišťování cloudových služeb prostřednictvím druhotného prodejce CISP) může CISP tato ustanovení od svého prodejce odmítnout s odůvodněním, že se nevztahují na dodavatele komerčních služeb na druhém stupni. V takovém případě samotný CISP nerealizuje rozsah práce sjednaný ve smlouvě; dělá to jeho partner, který k tomu využívá jeho infrastrukturu. Co se týče operací partnera, CISP proto představuje komerčního dodavatele

(ne subdodavatele). V modelu přímého zadávání zakázky (nákup cloudových služeb přímo od CISP) by CISP tato „povinná“ ustanovení zpravidla zamítl, protože se vztahují na dodavatele typických komodit, a to svou komerční povahou nasmlouvaných služeb, a také kvůli tomu, že většina CISP nevyžaduje, aby jejich komerční služby zajišťovali subdodavatelé.

3.4 Zprostředkovatelé cloudových služeb

Snaha vyhnout se uzamčení u dodavatele s pomocí zprostředkovatele cloudových služeb může být problematická. I když zprostředkovatel cloudových služeb může teoreticky vypadat jako dobrý nápad, v praxi by pravděpodobně do procesu vnesl spíš složitost a zmatek než skutečnou hodnotu.

Snaha o takovou architekturu aplikací, která by fungovala současně nebo zaměnitelně mezi více cloudy, nevyhnutelně vede k negativním dopadům na funkce (neexistuje Rosettská deska pro cloud). Tento přístup může nakonec vnést další úroveň složitosti mezi zákazníky ve veřejném sektoru a jejich cloudovými službami. To může narušit efektivitu a zabezpečení, kterého se mělo dosáhnout, a výsledkem může být menší škálovatelnost a agilita, zvýšené náklady a zpomalení inovací.

3.5 Příprava na žádost RFP a průzkum trhu

Když se subjekt ve veřejném sektoru připravuje na vytvoření RFP na cloudové služby, měl by hned od začátku procesu zapojit představitele všech aspektů organizace – vyššího vedení, technologií, financí, zadávání zakázek, právního oddělení a oddělení pro uzavírání smluv. Bude tak zajištěno, že všechny zainteresované strany chápou model cloudu a následně zaujmou poučený přístup k přehodnocení tradičních metod zadávání zakázek v oblasti IT.

Co se týče dialogu s hráči v oboru, subjektům ve veřejném sektoru velmi doporučujeme, aby vynaložily čas na podrobné rozhovory a získaly zpětnou vazbu od společností působících v příslušném odvětví – od CISP, jejich partnerů, dodavatelů tržišť marketplace PaaS/SaaS a odborníků zaměřených na daný obor. Takový dialog může probíhat například v rámci oborových dnů nebo seminářů zaměřených na zabezpečení a zadávání zakázek. Další efektivní způsob, jak dobře porozumět zadávání zakázek na cloudové služby, je vydat žádost o informace (RFI), v ideálním případě sestavit dokument RFP. Tyto dokumenty často uvádějí potenciální problémy, které lze identifikovat, prodiskutovat a zmírnit ještě před vydáním finální RFP na cloudové služby.

3.6 Udržitelnost

Cloudové výpočetní operace jsou ze své povahy spojené s udržitelností. Přechod na cloud znamená nárůst energetické efektivity ve srovnání s místními servery nebo podnikovými datovými centry. Další záruku, že je daný cloud udržitelný, poskytuje takový CISP, který upřednostňuje udržitelnost a veřejně se zavázal k dosahování cílů udržitelnosti. Evropští CISP a provozovatelé datových center (s podporou Evropské komise) vytvořili Pakt o klimaticky neutrálních datových centrech[11], samoregulační iniciativu s cílem sestavit jasná, jednoduchá a dalekosáhlá kritéria udržitelnosti pro odvětví datových center a zajistit, aby provozovatelé datových center a poskytovatelé cloudových služeb dosáhli do roku 2030 klimatické neutrality. Samoregulační iniciativa uvádí jasné cíle ohledně energetické účinnosti datových center, šetření vodou, opětovného používání a oprav serverů a napájení datových center pomocí bezuhlíkové energie. CISP, kteří se k Samoregulační iniciativě přihlásí, souhlasí se splněním těchto cílů a splňují kritéria pro označení „klimaticky neutrální provozovatel“.

[11] https://www.climateneutraldatacentre.net/self-regulatory-initiative/

V RFP na cloudové služby by měla být otázka, zda se CISP zavázali splnit taková kritéria, konkrétně zda a kdy přijali závazek samoregulace.

Vzor znění RFP: Udržitelnost

Zavázali jste se provozovat klimaticky neutrální datová centra podpisem Samoregulační iniciativy ohledně klimaticky neutrálních datových center (Climate Neutral Data Centre Self-Regulatory Initiative)? Pokud ano, kdy jste ji podepsali?

Můžete doložit, že vám byla udělena pečeť Paktu o klimaticky neutrálních datových centrech?

Dodatek A – Technické požadavky pro porovnání dodavatelů

Níže uvádíme několik obecných požadavků na cloudové technologie. Tento seznam požadavků lze použít jako nástroj pro porovnání CISP při vystavování smluvní objednávky nebo během výběrových řízení malého rozsahu v rámci Rámcové smlouvy.

1. Profil poskytovatele cloudových služeb

	Požadavek
1.	***ZKUŠENOSTI NA TRHU:*** *Kolik let působí poskytovatel v segmentu cloudových služeb?*
2.	***OTEVŘENOST A OCHRANA DAT:*** *Dodržuje poskytovatel cloudových služeb kodexy chování v oblasti ochrany dat či reverzibility? Dodržuje poskytovatel cloudu zásady pro vývoj open source a otevřených rozhraní API?*

2. Globální infrastruktura

	Požadavek
1.	***GLOBÁLNÍ DOSAH:*** *Nabízí poskytovatel cloudu globální infrastrukturu, která uživatelům pomáhá dosahovat nízké latence a vysoké propustnosti?*
2.	***OBLASTI:*** *Má poskytovatel cloudu oblastní zastoupení v potřebných zeměpisných oblastech?*
3.	***DOMÉNY/ZÓNY:*** *Zavádí poskytovatel cloudu koncept domén nebo zón, kde je více datových center seskupeno prostřednictvím sítě s nízkou latencí, aby byl zajištěn vyšší stupeň vysoké dostupnosti a odolnosti proti chybám?* • *Pokud ano, uveďte prosím počet domén nebo zón a počet datových center v rámci potřebného zeměpisného prostoru.*
4.	***VZDÁLENOST DOMÉN/ZÓN:*** *Vytváří poskytovatel cloudových služeb své domény či zóny prostřednictvím datových center, která jsou od sebe vzdálená, za účelem redundance, vysoké dostupnosti a nízké latence?*
5.	***ZPŮSOB BUDOVÁNÍ DATOVÝCH CENTER:*** *Navrhuje poskytovatel cloudových služeb svá datová centra tak, aby byla izolovaná od poruch v jiných datových centrech, měla záložní napájení, chlazení a sítě?*
6.	***REPLIKACE DATOVÉHO CENTRA:*** *Nabízí poskytovatel cloudu replikaci dat mezi datovými centry v rámci domény nebo zóny s automatickým převzetím služeb při selhání?*
7.	***REPLIKACE DOMÉNY/ZÓNY:*** *Nabízí poskytovatel cloudu replikaci dat mezi doménami nebo zónami v rámci dané oblasti?*

3. Infrastruktura

3.1 Výpočetní prostředky

	Požadavek
1.	***VÝPOČETNÍ PROSTŘEDKY – BĚŽNÁ INSTANCE – OBECNÝ ÚČEL:*** *Nabízí poskytovatel cloudu následující typy instancí?* • *Obecný účel – typ optimalizovaný pro obecné aplikace. Poskytuje vyváženou kapacitu výpočetních, paměťových a síťových zdrojů.* ○ *Pokud ano, jakou největší instanci poskytovatel nabízí?*
2.	***VÝPOČETNÍ PROSTŘEDKY – BĚŽNÁ INSTANCE – OPTIMALIZOVANÁ PRO PAMĚŤ:*** *Nabízí poskytovatel cloudu následující typy instancí?* • *Optimalizovaná pro paměť – optimalizace pro paměťově náročné aplikace* ○ *Pokud ano, jakou největší instanci poskytovatel nabízí?*
3.	***VÝPOČETNÍ PROSTŘEDKY – BĚŽNÁ INSTANCE – OPTIMALIZOVANÁ PRO VÝPOČETNÍ VÝKON:*** *Nabízí poskytovatel cloudu následující typy instancí?* • *Optimalizovaná pro výpočetní výkon – optimalizace pro aplikace náročné na výpočetní výkon* ○ *Pokud ano, jakou největší instanci poskytovatel nabízí?*
4.	***VÝPOČETNÍ PROSTŘEDKY – BĚŽNÁ INSTANCE – OPTIMALIZOVANÁ PRO ÚLOŽIŠTĚ:*** *Nabízí poskytovatel cloudu následující typy instancí?* • *Optimalizovaná pro úložiště – nabízí velkou kapacitu místního úložiště* ○ *Pokud ano, jaká je maximální kapacita úložiště (tj. 5, 10, 20, 50 TB) a maximální počet disků (HDD/SSD), které lze k instanci připojit?*
5.	***VÝPOČETNÍ PROSTŘEDKY – BĚŽNÁ INSTANCE – OPTIMALIZOVANÁ PRO GRAFICKÝ VÝKON:*** *Nabízí poskytovatel cloudu následující typy instancí?* • *Nízkonákladová grafika – nabízí poskytovatel nízkonákladovou grafickou akceleraci pro výpočetní výkon instancí?* ○ *Pokud ano, jakou největší instanci poskytovatel nabízí?*
6.	***VÝPOČETNÍ PROSTŘEDKY – BĚŽNÁ INSTANCE – OPTIMALIZOVANÁ PRO GPU:*** *Nabízí poskytovatel cloudu následující typy instancí?* • *GPU – hardwarové grafické procesory (GPU) pro graficky náročné aplikace* ○ *Pokud ano, kolik GPU a jaké modely GPU je poskytovatel cloudu schopen nabídnout pro každou instanci?*
7.	***VÝPOČETNÍ PROSTŘEDKY – BĚŽNÁ INSTANCE – OPTIMALIZOVANÁ PRO FPGA:*** *Nabízí poskytovatel cloudu následující typy instancí?* • *FPGA – programovatelná hradlová pole (FPGA) pro vývoj a nasazení vlastní hardwarové akcelerace aplikací.* ○ *Pokud ano, kolik FPGA a jaké modely FPGA je poskytovatel cloudu schopen nabídnout pro každou instanci?*
8.	***VÝPOČETNÍ PROSTŘEDKY – NÁRAZOVÁ INSTANCE:*** *Nabízí poskytovatel cloudu nárazové instance, které poskytují základní úroveň výkonu centrálních procesorových jednotek (CPU) s možností nárazového navýšení nad základní úroveň?* • *Pokud ano, jakou největší nárazovou instanci poskytovatel nabízí?*

9.	***VÝPOČETNÍ PROSTŘEDKY – INSTANCE S INTENZIVNÍM PROVOZEM V/V:*** *Nabízí poskytovatel cloudu instance, které používají energeticky nezávislé (NVMe) paměťové disky SSD optimalizované pro nízkou latenci, velmi vysoký výkon s náhodným vstupem/výstupem a vysokou propustnost sekvenčního čtení?* • *Pokud ano, jaká je maximální kapacita pro vstupní/výstupní operace za sekundu (IOPS) u největší dostupné instance?*
10.	***VÝPOČETNÍ PROSTŘEDKY – DOČASNÉ MÍSTNÍ ÚLOŽIŠTĚ:*** *Podporuje poskytovatel cloudu místní úložiště pro výpočetní instance, které lze použít pro dočasné ukládání často se měnících informací?*
11.	***VÝPOČETNÍ PROSTŘEDKY – PODPORA VÍCE KARET NIC:*** *Podporuje poskytovatel cloudu přidělení více (primárních a dalších) karet síťového rozhraní (NIC) pro danou instanci?* • *Pokud ano, jaký je maximální počet karet NIC na instanci?*
12.	***VÝPOČETNÍ PROSTŘEDKY – AFINITA INSTANCE:*** *Nabízí poskytovatel cloudu uživatelům možnost logicky seskupovat instance v rámci jednoho datového centra?*
13.	***VÝPOČETNÍ PROSTŘEDKY – ANTI-AFINITA INSTANCE:*** *Nabízí poskytovatel cloudu uživatelům možnost logicky seskupovat instance a umisťovat je do různých datových center v rámci dané oblasti?*
14.	***VÝPOČETNÍ PROSTŘEDKY – POSKYTOVÁNÍ SAMOOBSLUŽNÝCH SLUŽEB:*** *Nabízí dodavatel cloudu poskytování samoobslužných služeb pro více instancí najednou prostřednictvím programového rozhraní, konzoly pro správu nebo webového portálu?*
15.	***VÝPOČETNÍ PROSTŘEDKY – PŘIZPŮSOBENÍ:*** *Nabízí poskytovatel cloudu přizpůsobitelné instance, tj. možnost úpravy konfigurací, jako jsou virtuální centrální procesorové jednotky (vCPU) a paměť RAM?*
16.	***VÝPOČETNÍ PROSTŘEDKY – OBSAZENÍ:*** *Nabízí poskytovatel cloudu instance pro jednoho tenanta, které běží na hardwaru vyhrazeném pro jednoho uživatele?* • *Pokud ano, jaká je největší dostupná instance pro jednoho tenanta?*
17.	***VÝPOČETNÍ PROSTŘEDKY – AFINITA HOSTITELE:*** *Nabízí poskytovatel cloudu možnost spustit instanci a určit, aby se tato instance vždy restartovala na stejném fyzickém hostitelském zařízení?*
18.	***VÝPOČETNÍ PROSTŘEDKY – ANTI-AFINITA HOSTITELE:*** *Nabízí poskytovatel cloudu možnost rozdělení a hostování konkrétních instancí na různých fyzických hostitelích?*
19.	***VÝPOČETNÍ PROSTŘEDKY – AUTOMATICKÉ ŠKÁLOVÁNÍ:*** *Nabízí poskytovatel cloudu možnost automatického navýšení počtu instancí pro zajištění výkonu v případě nárůstu poptávky (tzv. „scale-out“)?*
20.	***VÝPOČETNÍ PROSTŘEDKY – MECHANISMUS IMPORTU BITOVÝCH KOPIÍ:*** *Nabízí poskytovatel cloudu uživatelům možnost importovat své stávající bitové kopie a uložit je jako nové, soukromě dostupné bitové kopie, které lze pak v budoucnu použít k poskytování instancí?* • *Pokud ano, jaké formáty jsou podporovány?*
21.	***VÝPOČETNÍ PROSTŘEDKY – MECHANISMUS EXPORTU BITOVÝCH KOPIÍ:*** *Podporuje poskytovatel cloudu možnost vzít stávající běžící instanci nebo její kopii a exportovat ji do formátu virtuálního stroje?* • *Pokud ano, jaké formáty jsou podporovány?*

22.	***VÝPOČETNÍ PROSTŘEDKY – VÝPADKY SLUŽEB:*** *Nabízí poskytovatel cloudu mechanismy, které zabrání výpadkům nebo odstávkám instancí v případě, že poskytovatel provádí jakoukoli údržbu hardwaru nebo služeb na úrovni hostitele?*
23.	***VÝPOČETNÍ PROSTŘEDKY – RESTARTOVÁNÍ INSTANCE:*** *Nabízí poskytovatel cloudu mechanismy pro automatický restart instancí na jiném serveru, který je v dobrém stavu, pokud dojde k selhání původního fyzického umístění?*
24.	***VÝPOČETNÍ PROSTŘEDKY – OZNÁMENÍ:*** *Je poskytovatel cloudu v případě nenadále události schopen informovat uživatele o tom, že k takové události došlo, a má uživatel možnost se k takové komunikaci přihlásit nebo se z ní odhlásit prostřednictvím samoobslužných prostředků?*
25.	***VÝPOČETNÍ PROSTŘEDKY – PLÁNOVÁNÍ UDÁLOSTÍ:*** *Nabízí poskytovatel cloudu uživatelům instance možnost plánovat události, jako je restartování, zastavení, spuštění nebo vyřazení instance?*
26.	***VÝPOČETNÍ PROSTŘEDKY – MECHANISMUS ZÁLOHOVÁNÍ A OBNOVY:*** *Nabízí poskytovatel cloudu integrovaný mechanismus zálohování a obnovy?*
27.	***VÝPOČETNÍ PROSTŘEDKY – MECHANISMUS SNÍMKU:*** *Nabízí poskytovatel cloudu manuální mechanismus pořízení snímku na vyžádání?*
28.	***VÝPOČETNÍ PROSTŘEDKY – METADATA:*** *Nabízí poskytovatel cloudu službu metadat instance, která umožňuje uživatelům nastavit libovolné páry klíč-hodnota pro instanci?*
29.	***VÝPOČETNÍ PROSTŘEDKY – VOLÁNÍ METADAT:*** *Nabízí poskytovatel cloudu službu metadat instance poskytující aplikační programovací rozhraní (API), které může instance volat, aby o sobě zjistila informace?*
30.	***VÝPOČETNÍ PROSTŘEDKY – MECHANISMUS NABÍDKY LEVNĚJŠÍ INSTANCE:*** *Nabízí poskytovatel cloudu mechanismus pro nabídku levnější instance, kterou lze okamžitě instalovat pro hostování úloh, které nejsou kritické?*
31.	***VÝPOČETNÍ PROSTŘEDKY – MECHANISMUS PLÁNOVÁNÍ:*** *Nabízí poskytovatel cloudu nějaký způsob, jak naplánovat a rezervovat další výpočetní kapacitu na pravidelné bázi, tj. denní, týdenní nebo měsíční plán?*
32.	***VÝPOČETNÍ PROSTŘEDKY – MECHANISMUS REZERVACÍ:*** *Nabízí poskytovatel cloudu nějaký způsob rezervování další výpočetní kapacity do budoucna (tj. na 1 rok, 2 roky, 3 roky atd.)?*
33.	***VÝPOČETNÍ PROSTŘEDKY – OPERAČNÍ SYSTÉM LINUX:*** *Podporuje poskytovatel cloudu poslední dvě dlouhodobě podporované verze alespoň jedné podnikové distribuce Linuxu (například Red Hat, SUSE) a jedné běžně používané svobodné distribuce Linuxu (například Ubuntu, CentOS a Debian)?*
34.	***VÝPOČETNÍ PROSTŘEDKY – OPERAČNÍ SYSTÉM WINDOWS:*** *Podporuje poskytovatel cloudu poslední dvě hlavní verze systému Windows Server (Windows Server 2017 a Windows Server 2016)?*
35.	***VÝPOČETNÍ PROSTŘEDKY – PŘENOSITELNOST LICENCÍ:*** *Nabízí poskytovatel cloudu možnost přenositelnosti licence a podporu?* • *Pokud ano, uveďte dodavatele softwaru, názvy softwaru, jejich vydání a verze.*

36.	***VÝPOČETNÍ PROSTŘEDKY – LIMITY SLUŽBY:*** *Má poskytovatel cloudu nějaká omezení (tj. limity služeb), pokud jde o výše uvedenou část týkající se výpočetních prostředků?* *Příklad:* *Maximální počet instancí na účet* *Maximální počet vyhrazených hostitelů na účet* *Maximální počet rezervovaných adres internetového protokolu (IP)*

3.2 Sítě

	Požadavek
1.	***SÍTĚ – VIRTUÁLNÍ SÍTĚ:*** *Podporuje poskytovatel cloudu možnost vytvořit logickou, izolovanou virtuální síť, která představuje vlastní síť společnosti v cloudu?*
2.	***SÍTĚ – MOŽNOSTI PŘIPOJENÍ VE STEJNÉ OBLASTI:*** *Podporuje poskytovatel cloudu možnost propojení dvou virtuálních sítí ve stejné oblasti a směrování provozu mezi nimi pomocí privátních adres internetového protokolu (IP)?*
3.	***SÍTĚ – MOŽNOSTI PŘIPOJENÍ V RŮZNÝCH OBLASTECH:*** *Podporuje poskytovatel cloudu možnost propojení dvou virtuálních sítí mezi různými oblastmi a směrování provozu mezi nimi pomocí privátních adres internetového protokolu (IP)?*
4.	***SÍTĚ – PRIVÁTNÍ PODSÍŤ:*** *Nabízí poskytovatel cloudu možnost vytvoření plně izolovaných (privátních) virtuálních sítí a podsítí, v nichž lze zřizovat instance bez jakékoli veřejné adresy internetového protokolu (IP) nebo internetového směrování?*
5.	***SÍTĚ – ROZSAH ADRES VIRTUÁLNÍ SÍTĚ:*** *Podporuje poskytovatel cloudu rozsahy adres internetového protokolu (IP) uvedené v žádosti o komentáře (RFC) 1918 a veřejně směrovatelné bloky CIDR?*
6.	***SÍTĚ – VÍCE PROTOKOLŮ:*** *Podporuje poskytovatel cloudu více protokolů včetně protokolů TCP (transmission control protocol), UDP (user datagram protocol) a ICMP (Internet control message protocol)?*
7.	***SÍTĚ – AUTOMATICKÉ PŘIDĚLOVÁNÍ IP ADRES:*** *Podporuje poskytovatel cloudu možnost automatického přidělování veřejných adres internetového protokolu (IP) instancím?*
8.	***SÍTĚ – REZERVOVANÉ STATICKÉ IP ADRESY:*** *Podporuje poskytovatel cloudu adresy internetového protokolu (IP) spojené s uživatelským účtem, nikoli s konkrétní instancí? IP adresa by měla zůstat spojena s účtem, dokud nebude výslovně uvolněna.*
9.	***SÍTĚ – PODPORA PROTOKOLU IPV6:*** *Podporuje poskytovatel cloudu internetový protokol verze 6 (IPv6) na úrovni brány nebo instance a zpřístupňuje tuto funkci uživatelům?*
10.	***SÍTĚ – VÍCE IP ADRES NA JEDNU KARTU NIC:*** *Podporuje poskytovatel cloudu možnost přiřadit primární a sekundární adresu internetového protokolu (IP) kartě síťového rozhraní (NIC), která je připojena k dané instanci?*

11.	***SÍTĚ – VÍCE KARET NIC:*** *Podporuje poskytovatel cloudu možnost přiřadit dané instanci více karet síťového rozhraní (NIC)?*
12.	***SÍTĚ – MOBILITA karet NIC a adres IP:*** *Podporuje poskytovatel cloudu možnost přesouvat karty síťového rozhraní (NIC) a adresy internetového protokolu (IP) mezi instancemi?*
13.	***SÍTĚ – PODPORA SR-IOV:*** *Podporuje poskytovatel cloudu funkce, jako je virtualizace single root input/output (SR-IOV) pro vyšší výkon (tj. pakety za sekundu – PPS), nižší latenci a nižší kolísání?*
14.	***SÍTĚ – FILTROVÁNÍ PŘÍCHOZÍHO PŘENOSU:*** *Podporuje poskytovatel cloudu přidávání nebo odebírání pravidel platných pro příchozí provoz (příchozí přenos) do instancí?*
15.	***SÍTĚ – FILTROVÁNÍ VÝCHOZÍHO PŘENOSU:*** *Podporuje poskytovatel cloudu přidávání nebo odebírání pravidel platných pro odchozí provoz (výchozí přenos) z instancí?*
16.	***SÍTĚ – ACL:*** *Nabízí poskytovatel cloudu seznamy řízení přístupu (ACL) pro řízení příchozího a odchozího provozu do podsítí?*
17.	**SÍTĚ** – ***PODPORA PROTOKOLU TOKU:*** *Nabízí poskytovatel cloudu možnost zaznamenávat protokoly toku síťového provozu?*
18.	***SÍTĚ – NAT:*** *Nabízí poskytovatel cloudu spravovanou službu překladu síťové adresy (NAT), která umožňuje instancím v privátní síti připojit se k internetu nebo jiným cloudovým službám, ale brání internetu v navázání spojení s těmito instancemi?*
19.	***SÍTĚ – KONTROLA ZDROJE/CÍLE:*** *Má poskytovatel cloudu možnost zakázat kontrolu zdroje/cíle na kartách síťového rozhraní (NIC)?*
20.	***SÍTĚ – PODPORA SÍTĚ VPN:*** *Podporuje poskytovatel cloudu připojení k virtuální privátní síti (VPN) mezi poskytovatelem cloudu a datovým centrem uživatele?*
21.	***SÍTĚ – PODPORA TUNELU VPN:*** *Podporuje poskytovatel cloudu více připojení k virtuální privátní síti (VPN) pro jednu virtuální síť?*
22.	***SÍTĚ – PODPORA TUNELU IPSEC VPN:*** *Umožňuje poskytovatel cloudu uživatelům přístup ke cloudovým službám prostřednictvím tunelu virtuální privátní sítě (VPN) se zabezpečením internetového protokolu (IPsec) nebo tunelu virtuální privátní sítě (VPN) s vrstvou zabezpečených soketů (SSL) přes veřejný internet?*
23.	***SÍTĚ – PODPORA BGP:*** *Používá poskytovatel cloudu border gateway protocol (BGP) ke zlepšení převzetí služeb při selhání v rámci tunelů VPN (virtual private network) se zabezpečením internetového protokolu (IPsec)?*
24.	***SÍTĚ – SOUKROMÉ VYHRAZENÉ PŘIPOJENÍ:*** *Nabízí poskytovatel cloudu přímou, privátní službu připojení mezi lokalitami poskytovatele cloudu a datovým centrem, kanceláří nebo kolokačním prostředím uživatele, která umožňuje velké a rychlé přenosy dat?*
25.	***SÍTĚ – FRONT-END NÁSTROJ PRO VYROVNÁVÁNÍ ZATÍŽENÍ:*** *Nabízí poskytovatel cloudu front-end službu vyrovnávání zatížení (internetové nasazení), která přijímá přes internet požadavky od klientů a rozděluje je mezi instance s registrací pro vyrovnávání zatížení?*

26.	***SÍTĚ – BACK-END NÁSTROJ PRO VYROVNÁVÁNÍ ZATÍŽENÍ:*** *Nabízí poskytovatel cloudu back-end (privátní) službu vyrovnávání zatížení, která směruje provoz na instance hostované v privátních podsítích?*
27.	***SÍTĚ – VYROVNÁVÁNÍ ZATÍŽENÍ VRSTVY 7:*** *Nabízí poskytovatel cloudu službu vyrovnávání zatížení na vrstvě 7 (protokol HTTP), která dokáže vyrovnávat zatížení distribucí síťového provozu mezi více instancí?*
28.	***SÍTĚ – VYROVNÁVÁNÍ ZATÍŽENÍ VRSTVY 4:*** *Nabízí poskytovatel cloudu službu vyrovnávání zatížení na vrstvě 4 (protokol TCP), která dokáže vyrovnávat zatížení distribucí síťového provozu mezi více instancí?*
29.	***SÍTĚ – AFINITA RELACÍ PRO VYROVNÁVÁNÍ ZATÍŽENÍ:*** *Nabízí poskytovatel cloudu službu vyrovnávání zatížení, která podporuje afinitu relací?*
30.	***SÍTĚ – VYROVNÁVÁNÍ ZATÍŽENÍ ZALOŽENÉ NA SLUŽBĚ DNS:*** *Nabízí poskytovatel cloudu službu vyrovnávání zatížení, která dokáže rozložit provoz na instance hostované na více hostitelích patřících do jedné domény?*
31.	***SÍTĚ – PROTOKOLY VYROVNÁVÁNÍ ZATÍŽENÍ:*** *Nabízí poskytovatel cloudu protokoly, které zachycují podrobné informace o všech požadavcích odeslaných na vyrovnávání zatížení?*
32.	***SÍTĚ – DNS:*** *Nabízí poskytovatel cloudu vysoce dostupnou a škálovatelnou službu systému doménových názvů (DNS)?*
33.	***SÍTĚ – SMĚROVÁNÍ DNS ZALOŽENÉ NA LATENCI:*** *Nabízí poskytovatel cloudu službu systému doménových názvů (DNS), která podporuje směrování založené na latenci (t.j. služba DNS odpovídá na dotazy DNS prostředky, které poskytují nejlepší latenci)?*
34.	***SÍTĚ – GEOGRAFICKÉ DNS SMĚROVÁNÍ:*** *Nabízí poskytovatel cloudu službu systému doménových názvů (DNS), která podporuje geografické dns směrování (t.j. služba DNS odpovídá na dotazy DNS na základě geografické polohy uživatelů)?*
35.	***SÍTĚ – SMĚROVÁNÍ DNS V RÁMCI PŘEVZETÍ SLUŽEB PŘI SELHÁNÍ:*** *Nabízí poskytovatel cloudu službu systému doménových názvů (DNS), která podporuje směrování v rámci převzetí služeb při selhání (tj. služba DNS směruje dotazy DNS na aktuálně aktivní prostředek, zatímco druhý prostředek čeká a aktivuje se pouze v případě selhání primárního prostředku)?*
36.	***SÍTĚ – SLUŽBA REGISTRACE DOMÉN:*** *Nabízí poskytovatel cloudu služby registrace doménových názvů (tj. uživatelé mohou vyhledávat a registrovat dostupné doménové názvy)?*
37.	***SÍTĚ – KONTROLY STAVU DNS:*** *Nabízí poskytovatel cloudu službu systému doménových názvů (DNS), která využívá kontroly stavu ke sledování stavu a výkonu prostředků?*
38.	***SÍTĚ – INTEGRACE DNS A VYROVNÁVÁNÍ ZATÍŽENÍ:*** *Nabízí poskytovatel cloudu službu systému doménových názvů (DNS), která je integrována s vyrovnáváním zatížení poskytovatele cloudu?*
39.	***SÍTĚ – VIZUÁLNÍ EDITOR:*** *Nabízí poskytovatel cloudu nástroj, který umožňuje uživatelům vytvářet zásady pro řízení provozu?*

40.	***SÍŤ PRO DORUČOVÁNÍ OBSAHU (CDN):*** *Nabízí poskytovatel cloudu službu sítě pro doručování obsahu (CDN) za účelem distribuce obsahu při nízké latenci a vysoké rychlosti přenosu dat?*
41.	***SÍTĚ – ČAS VYPRŠENÍ PLATNOSTI MEZIPAMĚTI CDN:*** *Nabízí poskytovatel cloudu službu sítě pro doručování obsahu (CDN), která umožňuje odstranit objekt z okrajových mezipamětí před vypršením jeho platnosti, včetně funkcí, jako je zneplatnění objektů a určování verze objektů?*
42.	***SÍTĚ – EXTERNÍ PŮVOD CDN:*** *Nabízí poskytovatel cloudu službu sítě pro doručování obsahu (CDN), která podporuje vlastní původ, tj. server protokolu HTTP?*
43.	***SÍTĚ – OPTIMALIZACE CDN:*** *Nabízí poskytovatel cloudu službu sítě pro doručování obsahu (CDN) s granulární kontrolou pro konfiguraci více serverů původu a vlastností ukládání do mezipaměti pro různé jednotné lokátory zdrojů (URL)?*
44.	***SÍTĚ – GEOGRAFICKY OMEZENÁ SÍŤ CDN:*** *Nabízí poskytovatel cloudu službu sítě pro doručování obsahu (CDN), která podporuje geografické omezení, tj. zabraňuje uživatelům v určitých zeměpisných oblastech v přístupu k obsahu?*
45.	***SÍTĚ – TOKENY CDN:*** *Nabízí poskytovatel cloudu službu sítě pro doručování obsahu (CDN) podporující podepsané jednotné lokátory zdrojů (URL), které obvykle obsahují další informace, jako je datum/čas vypršení platnosti, za účelem větší kontroly nad přístupem k obsahu ze strany uživatelů?*
46.	***SÍTĚ – CERTIFIKÁTY CDN:*** *Nabízí poskytovatel cloudu službu sítě pro doručování obsahu (CDN), která podporuje vlastní certifikáty vrstvy zabezpečených konektorů (certifikáty SSL) pro bezpečné doručování obsahu prostřednictvím protokolu HTTPS (Hypertext Transfer Protocol Secure) z okrajových umístění?*
47.	***SÍTĚ – VÍCEÚROVŇOVÁ MEZIPAMĚŤ CDN:*** *Nabízí poskytovatel cloudu službu sítě pro doručování obsahu (CDN), která používá víceúrovňovou mezipaměť s využitím oblastních okrajových mezipamětí za účelem snížení latence?*
48.	***SÍTĚ – KOMPRESE CDN:*** *Nabízí poskytovatel cloudu službu sítě pro doručování obsahu (CDN), která podporuje kompresi souborů?*
49.	***SÍTĚ – ŠIFROVANÉ ODESÍLÁNÍ V SÍTI CDN:*** *Nabízí poskytovatel cloudu síť pro doručování obsahu (CDN), která umožňuje uživatelům bezpečně nahrávat citlivá data tak, aby se tyto informace zobrazovaly pouze v určitých komponentách a službách v původní infrastruktuře uživatele?*
50.	***SÍTĚ – KONCOVÉ BODY:*** *Nabízí síťová služba poskytovatele cloudu uživatelům koncové body schopné směrovat provoz prostřednictvím interního síťového připojení poskytovatele (tj. privátního připojení), které umožňuje snížení nákladů na komunikaci a zvýšení bezpečnosti provozu?*
51.	***SÍTĚ – LIMITY SLUŽBY:*** *Má poskytovatel cloudu nějaká omezení (tj. limity služeb), pokud jde o výše uvedenou část týkající se sítí?* *Příklad:* *Maximální počet virtuálních sítí na účet* *Maximální velikost virtuální sítě* *Maximální počet podsítí na účet* *Maximální počet nástrojů na vyrovnávání zatížení na účet*

	Maximální počet položek seznamu řízení přístupu (ACL) *Maximální počet tunelů virtuální privátní sítě (VPN)* *Maximální počet původů v jedné distribuci* *Maximální počet certifikátů na jeden nástroj vyrovnávání zatížení*

3.3 Úložiště

	Požadavek
1.	***SLUŽBA BLOKOVÉHO ÚLOŽIŠTĚ:*** *Nabízí poskytovatel cloudu svazky úložiště na úrovni bloků pro použití s výpočetními instancemi?*
2.	***BLOKOVÉ ÚLOŽIŠTĚ – IOPS:*** *Nabízí poskytovatel cloudu možnost nakupovat na základě explicitního cíle výkonnosti nebo výkonnostní úrovně pro svazky blokového úložiště? Může jít například o určitý počet vstupních/výstupních operací za sekundu (IOPS) nebo megabajtů za sekundu (MB/S) propustnosti.*
3.	***BLOKOVÉ ÚLOŽIŠTĚ – DISKY SSD:*** *Podporuje poskytovatel cloudu úložná média s pevným diskem (SSD), která nabízejí latenci v řádu jednotek milisekund?* • *Pokud ano, jaký je maximální počet disků SSD, které lze připojit k jedné instanci?*
4.	***BLOKOVÉ ÚLOŽIŠTĚ – ŠKÁLOVÁNÍ:*** *Nabízí poskytovatel cloudu uživatelům možnost zvětšit velikost stávajícího svazku blokového úložiště, aniž by museli vytvářet nový svazek a kopírovat/přesouvat data?*
5.	***BLOKOVÉ ÚLOŽIŠTĚ – SNÍMKY:*** *Má poskytovatel cloudových služeb možnost vytvářet snímky v rámci své služby blokového úložiště?*
6.	***BLOKOVÉ ÚLOŽIŠTĚ – VYMAZÁNÍ DAT:*** *Podporuje poskytovatel cloudu možnost úplného vymazání dat tak, aby data již nebyla čitelná nebo přístupná neoprávněným uživatelům a/nebo třetím stranám?*
7.	***BLOKOVÉ ÚLOŽIŠTĚ – ŠIFROVÁNÍ DAT NA ÚROVNI ÚLOŽIŠTĚ (AT-REST):*** *Nabízí poskytovatel cloudu neaktivní šifrování dat na straně serveru pro data uložená na svazcích a pro jejich snímky?* • *Pokud ano, jaký je použitý kryptografický algoritmus?*
8.	***SLUŽBA ÚLOŽIŠTĚ OBJEKTŮ:*** *Nabízí poskytovatel cloudu bezpečné, trvalé a vysoce škálovatelné úložiště objektů pro ukládání a načítání libovolného množství dat z webu?*
9.	***ÚLOŽIŠTĚ OBJEKTŮ – OBČASNÝ PŘÍSTUP:*** *Nabízí poskytovatel cloudu levnější úroveň úložných služeb, která je určena pro ukládání objektů a souborů s méně častým přístupem?*
10.	***ÚLOŽIŠTĚ OBJEKTŮ – NIŽŠÍ ŽIVOTNOST:*** *Nabízí poskytovatel cloudu nižší úroveň redundance, kde může uživatel ukládat nekritické, snadno reprodukovatelné objekty za nižší cenu?*
11.	***ÚLOŽIŠTĚ OBJEKTŮ – MÉNĚ ČASTÝ PŘÍSTUP:*** *Nabízí poskytovatel cloudu úroveň pro data, ke kterým je přistupováno méně často, avšak stále vyžadují rychlý přístup?*

12.	***ÚLOŽIŠTĚ OBJEKTŮ – VRSTVENÍ OBJEKTŮ:*** *Nabízí poskytovatel cloudového úložiště možnost vrstvení objektového úložiště, tj. schopnost doporučení přechodu objektu mezi třídami nebo úrovněmi objektového úložiště na základě četnosti přístupu k němu?*
13.	***ÚLOŽIŠTĚ OBJEKTŮ – SPRÁVA ŽIVOTNÍHO CYKLU:*** *Podporuje poskytovatel cloudu správu životního cyklu objektu pomocí konfigurace životního cyklu, která definuje, jak jsou objekty spravovány během své životnosti od vytvoření až po odstranění?*
14.	***ÚLOŽIŠTĚ OBJEKTŮ – SPRÁVA ŘÍZENÁ ZÁSADAMI:*** *Nabízí poskytovatel cloudu možnost vytvářet a používat zásady pro správu uložených dat, jejich životního cyklu a nastavení úrovní?*
15.	***ÚLOŽIŠTĚ OBJEKTŮ – ZÁSADY TÝKAJÍCÍ SE UMÍSTĚNÍ A ČASU:*** *Nabízí poskytovatel cloudu uživatelům možnost vytvářet zásady, které mohou omezit přístup k datům na základě polohy uživatele a času požadavku?*
16.	***ÚLOŽIŠTĚ OBJEKTŮ – HOSTOVÁNÍ WEBOVÝCH STRÁNEK:*** *Podporuje poskytovatel cloudu hostování statických webových stránek ze své služby úložiště objektů?*
17.	***ÚLOŽIŠTĚ OBJEKTŮ – ŠIFROVÁNÍ DAT NA ÚROVNI ÚLOŽIŠTĚ (AT-REST):*** *Podporuje poskytovatel cloudu šifrování dat na úrovni úložiště na straně serveru (SSE), v rámci kterého jsou šifrovací klíče spravovány poskytovatelem cloudu?* • *Pokud ano, jaký je použitý kryptografický algoritmus?*
18.	***ÚLOŽIŠTĚ OBJEKTŮ – ŠIFROVÁNÍ POMOCÍ UŽIVATELSKÝCH KLÍČŮ:*** *Nabízí poskytovatel cloudu možnost šifrování na straně serveru (SSE) pomocí kryptografických klíčů poskytnutých zákazníkem?*
19.	***ÚLOŽIŠTĚ OBJEKTŮ – SLUŽBA SPRÁVY KLÍČŮ:*** *Podporuje poskytovatel cloudu šifrování na straně serveru (SSE) pomocí služby správy klíčů, která vytváří šifrovací klíče, definuje zásady kontrolující způsob jejich používání a toto používání kontroluje za účelem prověření, zda jsou používány správně?*
20.	***ÚLOŽIŠTĚ OBJEKTŮ – HLAVNÍ KLÍČ NA STRANĚ KLIENTA:*** *Nabízí poskytovatel cloudu uživatelům možnost ponechat si kontrolu nad šifrovacími klíči a dokončit šifrování/dešifrování objektů na straně klienta?*
21.	***ÚLOŽIŠTĚ OBJEKTŮ – SILNÁ KONZISTENCE:*** *Podporuje poskytovatel cloudu konzistenci čtení po zápisu u operací PUT pro nové objekty?*
22.	***ÚLOŽIŠTĚ OBJEKTŮ – LOKALITA DAT:*** *Nabízí CISP dostatečně silnou izolaci oblastí, aby objekty uložené v určité oblasti tuto oblast nikdy neopouštěly kromě případů, kdy tak učiní sám uživatel?*
23.	***ÚLOŽIŠTĚ OBJEKTŮ – REPLIKACE:*** *Nabízí poskytovatel cloudu funkci meziregionální replikace, která automaticky replikuje objekty mezi uživatelem zvolenými oblastmi?*
24.	***ÚLOŽIŠTĚ OBJEKTŮ – URČOVÁNÍ VERZE:*** *Podporuje poskytovatel cloudu službu určování verze, tj. možnost ukládat a udržovat více verzí objektu?*
25.	***ÚLOŽIŠTĚ OBJEKTŮ – OZNAČENÍ NESMAZATELNÉ POLOŽKY:*** *Umožňuje poskytovatel cloudu uživateli označit položku jako nesmazatelnou?*

26.	***ÚLOŽIŠTĚ OBJEKTŮ – VÍCEFAKTOROVÉ OVĚŘOVÁNÍ OPERACÍ MAZÁNÍ:*** *Podporuje poskytovatel cloudu vícefaktorové ověřování (MFA) jako další možnost zabezpečení pro operace mazání?*
27.	***ÚLOŽIŠTĚ OBJEKTŮ – NAHRÁVÁNÍ NA VÍCE ČÁSTÍ:*** *Umožňuje poskytovatel cloudu nahrát objekt jako sadu částí, kde každá část je souvislou částí dat objektu a tyto části objektu lze nahrát nezávisle a v libovolném pořadí?*
28.	***ÚLOŽIŠTĚ OBJEKTŮ – ZNAČKY:*** *Nabízí poskytovatel cloudu možnost vytvářet a přiřazovat proměnlivé dynamické značky na úrovni objektu?*
29.	***ÚLOŽIŠTĚ OBJEKTŮ – OZNÁMENÍ:*** *Nabízí poskytovatel cloudu možnost zasílání oznámení, pokud dojde k určitým událostem na úrovni objektu (např. operace přidání/odstranění)?*
30.	***ÚLOŽIŠTĚ OBJEKTŮ – PROTOKOLY:*** *Nabízí poskytovatel cloudu možnost generování protokolů z auditu, které obsahují podrobnosti o jednotlivých požadavcích na přístup, jako je žadatel, čas požadavku, akce požadavku, stav odpovědi a chybový kód?*
31.	***ÚLOŽIŠTĚ OBJEKTŮ – INVENTARIZACE OBJEKTŮ:*** *Nabízí poskytovatel cloudu možnost inventarizace objektů, díky níž mají uživatelé možnost rychle vizualizovat objekty a jejich stav a mohou rychle odhalit objekty s veřejným přístupem?*
32.	***ÚLOŽIŠTĚ OBJEKTŮ – INVENTARIZACE METADAT:*** *Nabízí poskytovatel cloudu možnost inventarizace objektů, díky níž mohou uživatelé rychle vizualizovat metadata objektů?*
33.	***ÚLOŽIŠTĚ OBJEKTŮ – OPTIMALIZACE ODESÍLÁNÍ DAT:*** *Má poskytovatel cloudu možnost směrovat data z okrajových lokalit do služby úložiště pomocí optimalizované síťové cesty?*
34.	***ÚLOŽIŠTĚ OBJEKTŮ – MOŽNOST DOTAZOVÁNÍ:*** *Nabízí poskytovatel cloudu uživatelům možnost dotazovat se na jeho službu objektového úložiště pomocí příkazů strukturovaného dotazovacího jazyka (SQL)?*
35.	***ÚLOŽIŠTĚ OBJEKTŮ – NAČTENÍ PODMNOŽINY DAT:*** *Nabízí poskytovatel cloudu uživatelům možnost načíst z objektu pouze podmnožinu dat pomocí jednoduchých výrazů strukturovaného dotazovacího jazyka (SQL)?*
36.	***SLUŽBA ÚLOŽIŠTĚ SOUBORŮ:*** *Nabízí poskytovatel cloudu jednoduchou a škálovatelnou službu úložiště souborů pro použití s výpočetními instancemi v cloudu?*
37.	***ÚLOŽIŠTĚ SOUBORŮ – REDUNDANCE:*** *Ukládá poskytovatel cloudu objekty souborového systému (tzn. adresáře, soubory a odkazy) redundantně ve více datových centrech nebo zařízeních za účelem dosažení vyšší úrovně dostupnosti a trvanlivosti?*
38.	***ÚLOŽIŠTĚ SOUBORŮ – VYMAZÁNÍ DAT:*** *Podporuje poskytovatel cloudu možnost úplného vymazání dat z úložiště souborů tak, aby data již nebyla čitelná nebo přístupná neoprávněným uživatelům nebo třetím stranám?*
39.	***ÚLOŽIŠTĚ SOUBORŮ – VYSOKÁ DOSTUPNOST:*** *Vykazuje spravovaný systém souborů poskytovatele cloudu vysoký stupeň vysoké dostupnosti?*
40.	***ÚLOŽIŠTĚ SOUBORŮ – NFS:*** *Podporuje poskytovatel cloudu protokol systému souborů NFS (Network File System)?*

41.	***ÚLOŽIŠTĚ SOUBORŮ – SMB:*** *Podporuje poskytovatel cloudu protokol SMB (Server Message Block)?*
42.	***ÚLOŽIŠTĚ SOUBORŮ – ŠIFROVÁNÍ DAT ÚROVNI ÚLOŽIŠTĚ (AT-REST):*** *Podporuje služba úložiště souborů poskytovatele cloudu šifrování dat na úrovni úložiště?*
43.	***ÚLOŽIŠTĚ SOUBORŮ – ŠIFROVÁNÍ V TRANZITU:*** *Podporuje služba úložiště souborů poskytovatele cloudu šifrování dat během jejich tranzitu?*
44.	***ÚLOŽIŠTĚ SOUBORŮ – NÁSTROJ PRO MIGRACI DAT:*** *Nabízí poskytovatel cloudu nějaký nástroj pro migraci dat, který umožňuje uživatelům přesouvat data ze systémů v místě do systému souborů v cloudu?*
45.	***SLUŽBA ÚLOŽIŠTĚ ARCHIVU:*** *Nabízí poskytovatel cloudu nějakou velmi nízkonákladovou službu úložiště, která je určena pro ukládání objektů a souborů s méně častým přístupem a téměř neměnných objektů a souborů?*
46.	***ÚLOŽIŠTĚ ARCHIVU – ODOLNOST PROTI CHYBÁM:*** *Zajišťuje architektura poskytovatele cloudu odolnost proti výpadkům u služby úložiště archivu?*
47.	***ÚLOŽIŠTĚ ARCHIVU – NEMĚNNOST:*** *Podporuje poskytovatel cloudu neměnnost archivovaných objektů a souborů?*
48.	***ÚLOŽIŠTĚ ARCHIVU – WORM:*** *Nabízí poskytovatel cloudu možnost jednorázového zápisu a opakovaného čtení (WORM)?*
49.	***ÚLOŽIŠTĚ ARCHIVU – NAČTENÍ PODMNOŽINY DAT:*** *Nabízí poskytovatel cloudu uživatelům možnost získat z archivovaného objektu pouze podmnožinu dat pomocí jednoduchých výrazů strukturovaného dotazovacího jazyka (SQL)?*
50.	***ÚLOŽIŠTĚ ARCHIVU – RYCHLOST NAČÍTÁNÍ:*** *Nabízí poskytovatel cloudu uživatelům více možností načítání dat s různými náklady a časy načítání?*
51.	***ÚLOŽIŠTĚ ARCHIVU – ŠIFROVÁNÍ DAT ÚROVNI ÚLOŽIŠTĚ (AT-REST):*** *Podporuje služba úložiště archivu poskytovatele cloudu šifrování dat na úrovni úložiště?*
52.	***ÚLOŽIŠTĚ ARCHIVU – LIMITY SLUŽBY:*** *Má poskytovatel cloudu nějaká omezení (tj. limity služeb), pokud jde o výše uvedenou část týkající se úložiště?* *Příklad:* *Maximální velikost svazku* *Maximální počet jednotek připojených k instanci* *Maximální vstupní/výstupní operace za sekundu (IOPS)* *Maximální velikost objektu* *Maximální počet objektů na jeden účet úložiště* *Maximální počet snímků*

4. Správa

	Požadavek
1.	***SPRÁVA – UŽIVATELÉ A SKUPINY:*** *Nabízí poskytovatel cloudu službu pro vytváření a správu uživatelů a skupin uživatelů v rámci své infrastruktury a prostředků?*
2.	***SPRÁVA – RESETOVÁNÍ HESLA:*** *Umožňuje poskytovatel cloudu uživatelům resetovat vlastní heslo v rámci samoobslužného procesu?*
3.	***SPRÁVA – OPRÁVNĚNÍ:*** *Nabízí poskytovatel cloudu možnost přidávat oprávnění uživatelům a skupinám na úrovni prostředků?*
4.	***SPRÁVA – DOČASNÁ OPRÁVNĚNÍ:*** *Nabízí poskytovatel cloudu možnost vytvářet oprávnění platná po určitý časový interval?*
5.	***SPRÁVA – DOČASNÉ POVĚŘENÍ:*** *Nabízí poskytovatel cloudu uživatelům možnost vytvářet a poskytovat dočasné bezpečnostní pověření důvěryhodným uživatelům, které může být nakonfigurované na dobu od několika minut do několika hodin?*
6.	***SPRÁVA – ŘÍZENÍ PŘÍSTUPU:*** *Nabízí poskytovatel cloudu jemně odstupňované řízení přístupu ke svým prostředkům infrastruktury?* • *Pokud ano, za jakých podmínek lze toto řízení použít (např. denní doba, zdrojová IP adresa atd.)?*
7.	***SPRÁVA – INTEGROVANÉ SOUBORY PRAVIDEL:*** *Obsahuje infrastruktura poskytovatele cloudu integrované soubory pravidel řízení přístupu, které lze přiřadit uživatelům a skupinám?*
8.	***SPRÁVA – VLASTNÍ SOUBORY PRAVIDEL:*** *Umožňuje infrastruktura poskytovatele cloudu vytvoření a přizpůsobení souboru pravidel pro řízení přístupu, které lze přiřadit uživatelům a skupinám?*
9.	***SPRÁVA – SIMULACE SOUBORU PRAVIDEL:*** *Nabízí poskytovatel cloudu mechanismus pro testování účinků souboru pravidel pro řízení přístupu před jejich zavedením do provozu?*
10.	***SPRÁVA – VÍCEFAKTOROVÉ OVĚŘOVÁNÍ (MFA) V CLOUDU:*** *Podporuje poskytovatel cloudu používání vícefaktorového ověřování (MFA) jako dodatečné úrovně řízení přístupu a autentizace v rámci své infrastruktury?*
11.	***SPRÁVA – LIMITY SLUŽBY:*** *Má poskytovatel cloudu nějaká omezení (tj. limity služeb), pokud jde o výše uvedenou část týkající se správy?* *Příklad:* *Maximální počet uživatelů* *Maximální počet skupin* *Maximální počet spravovaných souborů pravidel*

5. Bezpečnost

	Požadavek
1.	***BEZPEČNOST – PROVĚRKY ZAMĚSTNANCŮ:*** *Podléhají všichni zaměstnanci poskytovatele cloudu, kteří mají přístup k infrastruktuře služby (ať už fyzické nebo nefyzické), prověrkám?*
2.	***BEZPEČNOST – FYZICKÝ PŘÍSTUP:*** *Omezuje poskytovatel cloudu pracovníkům přístup k infrastruktuře služby, pokud nemají k dispozici konkrétní záznam řešení problému, žádost o změnu nebo podobné formální oprávnění?*
3.	***BEZPEČNOST – PROTOKOLY PŘÍSTUPU:*** *Eviduje poskytovatel cloudu přístup zaměstnanců a dalších pracovníků ke své infrastruktuře, zpracovává k přístupu protokoly a tyto uchovává minimálně po dobu 90 dnů?*
4.	***BEZPEČNOST – PŘIHLÁŠENÍ DO SERVERŮ ZAJIŠTUJÍCÍCH SLUŽBU:*** *Omezuje poskytovatel cloudu přihlašování svých pracovníků k serverům, které využívají zákazníci, a místo toho automatizuje všechny úlohy prováděné na těchto serverech, přičemž obsah těchto automatizovaných úloh je zaznamenáván a protokoly jsou uchovávány po dobu minimálně 90 dnů?*
5.	***BEZPEČNOST – KRYPTOGRAFICKÉ KLÍČE:*** *Nabízí poskytovatel cloudu službu vytváření a kontroly kryptografických klíčů používaných k šifrování uživatelských dat?*
6.	***BEZPEČNOST – SPRÁVA PŘÍSTUPOVÝCH KLÍČŮ:*** *Nabízí poskytovatel cloudu možnost zjistit, kdy byl přístupový klíč naposledy použit, obměňovat staré klíče a odstraňovat neaktivní uživatele?*
7.	***BEZPEČNOST – KLÍČE POSKYTNUTÉ ZÁKAZNÍKEM:*** *Umožňuje poskytovatel cloudových služeb uživatelům importovat klíče ze své vlastní infrastruktury pro správu klíčů do služby správy klíčů poskytovatele cloudových služeb?*
8.	***BEZPEČNOST – INTEGRACE SLUŽBY KRYPTOGRAFICKÝCH KLÍČŮ:*** *Je služba správy klíčů poskytovatele cloudu integrována s ostatními cloudovými službami a umožňuje šifrování dat na úrovni úložiště?*
9.	***BEZPEČNOST – HSM:*** *Nabízí poskytovatel cloudu vyhrazené hardwarové bezpečnostní moduly (HSM), tj. hardwarová zařízení, která zajišťují bezpečné ukládání klíčů a kryptografické operace v rámci hardwarového modulu odolného proti úmyslnému poškození?*
10.	***BEZPEČNOST – ŽIVOTNOST KRYPTOGRAFICKÝCH KLÍČŮ:*** *Podporuje poskytovatel cloudu stálost klíčů, včetně ukládání více kopií, aby byly klíče v případě potřeby k dispozici?*
11.	***BEZPEČNOST – SSO:*** *Nabízí poskytovatel cloudu spravovanou službu jednotného přihlášení (SSO), která umožňuje uživatelům centrálně spravovat přístup k více účtům a podnikovým aplikacím?*
12.	***BEZPEČNOST – CERTIFIKÁTY:*** *Nabízí poskytovatel cloudu spravovanou službu pro zajištění, správu a nasazení certifikátů Secure Sockets Layer (SSL)/ Zabezpečení transportní vrstvy (TLS)?*
13.	***BEZPEČNOST – OBNOVENÍ CERTIFIKÁTŮ:*** *Umožňuje služba správy certifikátů poskytovatele cloudu obnovu certifikátů?*

14.	***BEZPEČNOST – CERTIFIKÁTY WILDCARD:*** *Podporuje služba správy certifikátů poskytovatele cloudu používání certifikátů wildcard?*
15.	***BEZPEČNOST – CERTIFIKAČNÍ AUTORITA:*** *Funguje služba správy certifikátů poskytovatele cloudu také jako certifikační autorita (CA)?*
16.	***BEZPEČNOST – ACTIVE DIRECTORY:*** *Nabízí poskytovatel cloudu spravovanou službu Microsoft Active Directory (AD) v cloudu?*
17.	***BEZPEČNOST – MÍSTNÍ ACTIVE DIRECTORY:*** *Podporuje spravovaná služba Microsoft Active Directory (AD) poskytovatele cloudu integraci se službou Microsoft Active Directory (AD) v lokalitě zákazníka?*
18.	***BEZPEČNOST – LDAP:*** *Podporuje spravovaná služba Microsoft Active Directory (AD) poskytovatele cloudu protokol LDAP (Lightweight Directory Access Protocol)?*
19.	***BEZPEČNOST – ACTIVE DIRECTORY:*** *Podporuje spravovaná služba Microsoft Active Directory (AD) poskytovatele cloudu jazyk SAML (security assertion markup language)?*
20.	***BEZPEČNOST – SPRÁVA POVĚŘENÍ:*** *Nabízí poskytovatel cloudu spravovanou službu, která pomáhá uživatelům snadno střídat, spravovat a načítat pověření, jako jsou klíče aplikačního programovacího rozhraní (API), pověření k databázím a další tajemství?*
21.	***BEZPEČNOST – WAF:*** *Nabízí poskytovatel cloudu bránu firewall webových aplikací (WAF), která pomáhá chránit webové aplikace před běžnými webovými zranitelnostmi, jež by mohly ovlivnit dostupnost aplikací, ohrozit zabezpečení nebo spotřebovávat nadměrné prostředky?*
22.	***BEZPEČNOST – DDOS:*** *Nabízí poskytovatel cloudu služby chránící před běžnými, nejčastěji prováděnými distribuovanými útoky typu odepření služby (DDoS) v síti a na transportní vrstvě a také možnost vytvářet přizpůsobená pravidla ke zmírnění rizik spojených se sofistikovanými útoky na aplikační vrstvu?*
23.	***BEZPEČNOST – BEZPEČNOSTNÍ DOPORUČENÍ:*** *Nabízí poskytovatel cloudu službu automatického vyhodnocování potenciálních zranitelností aplikací a zdrojů?*
24.	***BEZPEČNOST – DETEKCE HROZEB:*** *Nabízí poskytovatel cloudu spravovanou službu detekce hrozeb?*
25.	***BEZPEČNOST – LIMITY SLUŽBY:*** *Má poskytovatel cloudu nějaká omezení (tj. limity služeb), pokud jde o výše uvedenou část týkající se zabezpečení?* *Příklad:* *Maximální počet hlavních klíčů zákazníka* *Maximální počet hardwarových bezpečnostních modulů (HSM)*

6. Dodržování předpisů

Níže uvedený seznam slouží pouze k ilustračním účelům a neobsahuje tedy kompletní a detailní seznam veškerých certifikací a standardů, které se mohou na cloudové služby vztahovat.

Uveďte, který soubor mezinárodních a oborových norem poskytovatel cloudu splnil:

Certifikace a atestace	***Zákony, předpisy a ochrana soukromí***	***Harmonizace a právní rámce***
☐ *C5 [Německo]*	☐ *Směrnice EU o ochraně údajů*	☐ *CDSA*
☐ *Kodex chování CISPE týkající se ochrany dat*	☐ *Standardní doložky EU*	
☐ *CNDCP (Pakt o klimaticky neutrálních datových centrech)*		
☐ *DIACAP*	☐ *FERPA*	☐ *CIS*
☐ *DoD SRG úroveň 2 a 4*	☐ *GDPR*	☐ *Informační služby trestního soudnictví (CJIS)*
☐ *FedRAMP*	☐ *GLBA*	☐ *CSA*
☐ *FIPS 140-2*	☐ *HIPAA*	☐ *Štít soukromí EU-USA*
☐ *HDS (Francie, zdravotní péče)*	☐ *HITECH*	☐ *Zásady „bezpečného přístavu" EU*
☐ *ISO 9001*	☐ *IRS 1075*	☐ *FISC*
☐ *ISO 27001*	☐ *ITAR*	☐ *FISMA*
☐ *ISO 27017*	☐ *PDPA – 2010 [Malajsie]*	☐ *G-Cloud [Spojené království]*
☐ *ISO 27018*	☐ *PDPA – 2012 [Singapur]*	☐ *GxP (FDA CFR 21 část 11)*
☐ *IRAP [Austrálie]*	☐ *PIPEDA [Kanada]*	☐ *ICREA*
☐ *MTCS stupeň 3 [Singapur]*	☐ *Zákon o ochraně soukromí [Austrálie]*	☐ *IT Grundschutz [Německo]*
☐ *PCI DSS úroveň 1*	☐ *Zákon o ochraně soukromí [Nový Zéland]*	☐ *MARS – E*
☐ *SEC pravidlo 17-a-4(f)*	☐ *Španělské schválení zákona o ochraně dat*	☐ *MITA 3.0*
☐ *SOC1/ISAE 3402*	☐ *Britský zákon DPA o ochraně osobních údajů – 1988*	☐ *MPAA*
☐ *SOC2/SOC3*	☐ *VPAT/oddíl 508*	☐ *NIST*
☐ *Kodex SWIPO IaaS*		
		☐ *Úrovně organizace Uptime Institute*
		☐ *Britské zásady cloudového zabezpečení*

Využití výše uvedených zpráv o dodržování předpisů umožňuje organizacím veřejného sektoru vyhodnocovat jednotlivé nabídky z hlediska přijatých standardů bezpečnosti, souladu s předpisy a provozu. Tyto zprávy mohou ukázat, zda CISP díky dodržování standardů splňuje kritéria níže uvedených prvků kontroly provozu datového centra, která jsou vyžadována od poskytovatele služeb veřejného cloudu. Požadavek na dodržování těchto zpráv pomáhá subjektům veřejného sektoru získat jistotu, že jsou zavedeny níže uvedené kontrolní mechanismy.

- ***Kontrolovaný přístup:*** *CISP by měl omezit fyzický přístup pouze na osoby, které mají pro svou přítomnost oprávněný důvod. Pokud je jim přístup udělen, měl by být po dokončení potřebných prací zase zrušen.*
- ***Kontrolovaný a monitorovaný vstup:*** *Vstup do oblasti obvodu/perimetru datového centra by měl být kontrolovaný. CISP by měl zajistit, aby u vstupních bran byli přítomni pracovníci ostrahy. Další pracovníci by měli monitorovat zaměstnance a návštěvníky prostřednictvím bezpečnostních kamer. Schválené osoby by pro přítomnost v kontrolovaném prostoru měly obdržet průkaz, který vyžaduje vícefaktorové ověření a omezuje přístup na předem schválené oblasti.*
- ***Pracovníci datového centra CISP:*** *Pracovníci CISP, kteří běžně potřebují přístup do datového centra, by měli mít pro vstup do příslušné oblasti oprávnění, a to na základě své pracovní funkce. Jejich přístup by měl být také pravidelně kontrolován. Správce přístupu by měl pravidelně kontrolovat seznamy zaměstnanců s oprávněním, aby se ujistil, že je oprávnění každé osoby stále nezbytné. Pokud již daná osoba nemá pravidelnou pracovní potřebu pro pobyt v datovém centru, měla by povinně přejít do režimu návštěvy.*
- ***Monitorování neoprávněného vstupu:*** *CISP by měl nepřetržitě monitorovat neoprávněné vstupy do oblasti datového centra, a to pomocí kamerových systémů, systémů pro odhalování vniknutí a systémů monitorování protokolů přístupu. Vstupy do oblasti by měly být zabezpečeny zařízením, které spustí alarm v případě násilného otevření dveří nebo jejich přidržení.*
- ***Monitorování globální bezpečnosti ze strany bezpečnostních operačních středisek CISP:*** *Bezpečnostní operační střediska CISP by měla být rozmístěna po celém světě a měla by odpovídat za monitorování, třídění a realizaci programů zabezpečení datových center CISP. Střediska by měla dohlížet na správu fyzického přístupu a reakci v případě odhalení vniknutí. Zároveň by měla poskytovat globální nepřetržitou podporu bezpečnostním týmům datových center na místě a zajišťovat nepřetržité monitorovací činnosti, jako je sledování přístupových aktivit nebo rušení přístupových oprávnění. Také by tato centra měla být schopna reagovat a analyzovat potenciální bezpečnostní incidenty.*
- ***Kontrola přístupu v jednotlivých vrstvách:*** *Přístup k jednotlivým vrstvám infrastruktury by měl být omezen a měl by se řídit konkrétními oprávněnými potřebami. Zavedením kontroly přístupu po jednotlivých vrstvách se ve výchozím nastavení neuděluje právo přístupu do každé vrstvy. Přístup do každé konkrétní vrstvy by měl být povolen pouze v případě, že existuje konkrétní potřeba takového přístupu.*
- ***Údržba zařízení jako součást běžného provozu:*** *Týmy CISP by měly provádět diagnostiku strojů, sítí a záložních zařízení, aby zajistily jejich funkčnost v aktuálním běžném provozu i v případě nouze. Součástí pravidelného provozu datového centra CISP by měly být běžné kontroly údržby zařízení a inženýrských sítí.*
- ***Záložní zařízení pro případy nouzových situací:*** *U dodávek vody, elektřiny, telekomunikačních zařízení a připojení k internetu je nutno počítat s určitou rezervou, aby byl CISP schopen v případě nouze zajistit nepřetržitý provoz. Systémy elektrického napájení by měly být navrženy jako plně redundantní, aby v případě výpadku mohly být pro potřebné funkce zapojeny jednotky nepřerušitelného napájení. Zároveň je nezbytné, aby generátory byly schopné zajistit záložní napájení celého objektu. Je nutné zajistit odpovědné osoby a systémy, které budou monitorovat a kontrolovat teplotu a vlhkost. Cílem je zajistit, aby nedocházelo k přehřátí a aby se minimalizovalo riziko možných výpadků služeb.*
- ***Technologie a lidé spolupracující na zvýšení bezpečnosti:*** *Je nutné zavést povinné postupy pro získání oprávnění ke vstupu do datové vrstvy. To zahrnuje také postup, v rámci kterého oprávněné osoby přezkoumávají a schvalují jednotlivé žádosti o přístup. Současně by měly fungovat elektronické systémy pro odhalení vniknutí a tyto by měly automaticky spouštět upozornění na identifikované hrozby nebo podezřelé aktivity. Pokud například dojde k přidržení dveří nebo jejich násilnému otevření, spustí se alarm. CISP by měl používat systémy bezpečnostních kamer a měl by uchovávat záznamy, to vše v souladu s právními požadavky a požadavky na dodržování předpisů.*
- ***Zabránění fyzickému a technologickému vniknutí:*** *Přístupové body do serveroven by měly být zabezpečeny elektronickými kontrolními zařízeními, která vyžadují vícefaktorovou autorizaci. CISP by měl být také dobře připraven zabránit neoprávněnému vniknutí. Servery CISP by měly být schopny upozornit zaměstnance na pokusy o odstranění dat. V nepravděpodobném případě narušení by měl být server automaticky deaktivován.*

- ***Serverům a médiím je věnována pečlivá pozornost:*** *Zařízení pro ukládání zákaznických dat by měla být ze strany CISP klasifikována jako kritická a mělo by s nimi být zacházeno jako s vysoce rizikovými. To by mělo platit po celou dobu jejich životního cyklu. CISP by měl mít a dodržovat přísné standardy s ohledem na instalaci, servis a případnou likvidaci zařízení, která již přestanou být využívaná. Po skončení životnosti paměťového zařízení vyřazuje CISP média z provozu prostřednictvím technik popsaných v dokumentu NIST 800-88. Média, na kterých jsou uloženy údaje zákazníků, jsou vyřazena ze správy CISP až po bezpečném vyřazení těchto médií z provozu.*

- ***Systémy a postupy CISP jsou ověřovány auditory třetích stran:*** *CISP by měl být auditován externími auditory, kteří provedou hloubkovou kontrolu datových center a ujistí se, že CISP dodržuje stanovená pravidla potřebná k získání bezpečnostních certifikátů. V závislosti na systému souladu s předpisy a jeho požadavcích mohou externí auditoři vést rozhovory se zaměstnanci CISP o tom, jak tito nakládají s médii a jak je likvidují. Auditoři mohou také sledovat záznamy z bezpečnostních kamer a sledovat vstupy a chodby v celém datovém centru. Mohou také prověřovat různé vybavení, jako jsou zařízení elektronické kontroly přístupu a bezpečnostní kamery CISP.*

- ***Připravenost na neočekávané události:*** *CISP by se měl aktivně připravovat na potenciální hrozby s ohledem na okolní prostředí, jako jsou přírodní katastrofy a požáry. CISP může zvýšit zabezpečení svých datových center instalací automatických senzorů a responzivních zařízení. Doporučuje se instalace zařízení detekujících vodu, která upozorní zaměstnance. Následně dojde ke spuštění automatických čerpadel, která odčerpají kapalinu a zabrání vzniku škod. Podobným způsobem snižují riziko škod automatická zařízení pro detekci a hašení požáru, která zároveň upozorní zaměstnance CISP a hasiče.*

- ***Vysoká dostupnost díky většímu množství zón dostupnosti:*** *CISP by měl nabízet více zón dostupnosti a zajistit tak větší odolnost proti chybám. Každá zóna dostupnosti by se měla skládat z jednoho nebo více datových center, zóny by měly být od sebe fyzicky oddělené a měly by mít redundantní napájení a síť. Zóny dostupnosti by měly být vzájemně propojeny rychlou privátní optickou sítí umožňující navrhování aplikací, které mezi zónami dostupnosti automaticky a bez přerušení přebírají služby při selhání.*

- ***Simulace výpadků a měření reakce:*** *CISP by měl mít Plán kontinuity provozu v podobě průvodce operačními postupy, který popisuje, jak se vyhnout a zmírnit následky narušení v důsledku přírodních katastrof, včetně podrobných kroků, které je třeba učinit před událostí, během ní a po ní. Za účelem zmírnění dopadů a přípravy na neočekávané události by měl CISP pravidelně testovat Plán kontinuity provozu pomocí cvičení, která simulují různé scénáře. CISP by měl dokumentovat, jak jeho lidé a procesy fungují. Měl by být schopen poskytovat hlášení o získaných zkušenostech a případných nápravných opatřeních, která mohou být nezbytná pro zlepšení míry odezvy. Zaměstnanci CISP by měli být vyškoleni a připraveni na rychlou obnovu po výpadku či katastrofě. Měli by znát odpovídající metodický proces obnovy a minimalizovat tak další prostoje způsobené chybami.*

- ***Pomoc při plnění cílů v oblasti hospodárnosti:*** *Kromě řešení environmentálních rizik by měl CISP do návrhu datového centra zahrnout také hledisko udržitelnosti. CISP by měl dát k dispozici podrobné informace o plnění svého závazku využívání obnovitelné energie ve svých datových centrech. Také by měl poskytovat informace o tom, jak mohou jeho zákazníci snížit uhlíkové emise ve svých datových centrech.*

- ***Výběr místa:*** *Před výběrem lokality by měl CISP provést úvodní environmentální a geografické posouzení. Umístění datových center by mělo být pečlivě vybíráno tak, aby se zmírnila environmentální rizika, jako jsou záplavy, extrémní počasí a seismická aktivita. Zóny dostupnosti CISP by měly být budovány jako nezávislé a vzájemně fyzicky oddělené jednotky.*

- ***Redundance:*** *Datová centra by měla být navržena tak, aby předvídala a tolerovala výpadky a aby byla schopná zachovat stávající úroveň služeb. V případě poruchy by měly automatizované procesy přesunout provoz mimo postiženou oblast. Klíčové aplikace by měly být nasazeny ve standardu N+1, aby v případě výpadku datového centra byla k dispozici dostatečná kapacita, která umožní rozložit provoz na zbývající lokality.*

- ***Dostupnost:*** *CISP by měl být schopen identifikovat kritické součásti systému, které jsou nezbytné pro udržení jeho dostupnosti a obnovení služeb v případě výpadku. Kritické součásti systému by měly být zálohovány na několika izolovaných místech. Každá lokalita nebo zóna dostupnosti by měla být navržena tak, aby fungovala nezávisle a s vysokou spolehlivostí. Zóny dostupnosti by měly být propojeny, aby aplikace mohly mezi zónami dostupnosti automaticky a bez přerušení přebírat služby při selhání. V rámci navrhování systému a jeho funkcí by mělo být počítáno s vysoce odolnými systémy a vysokou dostupností služeb. Návrh datového centra se zónami dostupnosti a replikací dat by měl zákazníkům CISP pomoci dosahovat extrémně krátkých časů obnovy, cílů bodu obnovení a nejvyšší úrovně dostupnosti služeb.*

- ***Plánování kapacity:*** *CISP by měl průběžně sledovat využívání služeb. Jedině tak může správně řídit nasazení infrastruktury a plnit své závazky s ohledem na dostupnost a požadavky zákazníků. Zároveň by měl CISP mít a udržovat model plánování svých kapacit, který alespoň jednou měsíčně vyhodnocuje využití infrastruktury a požadavky na ni. Při práci s modelem plánování by měl poskytovatel brát v úvahu budoucí požadavky a další kritéria, k nimž se řadí například zpracování informací, telekomunikace a ukládání protokolů z auditu.*

KONTINUITA PROVOZU a OBNOVENÍ PO KATASTROFĚ

- ***Plán kontinuity provozu:*** *Plán kontinuity provozu CISP by měl obsahovat opatření, která pomohou zamezit nebo alespoň zmírnit dopady výpadků, které způsobují vnější vlivy. Opatření by měla podrobně popisovat kroky, které je třeba realizovat před událostí, během ní a po ní. Plán kontinuity provozu by měl být doplněn testováním se zahrnutím simulací různých scénářů. Během testování a po něm by měl CISP dokumentovat výkonnost lidí a procesů, nápravná opatření a získané zkušenosti. Tento postup by měl vést k neustálému zlepšování.*

- ***Reakce na pandemii:*** *CISP by měl do svého plánování obnovení po katastrofě začlenit zásady a postupy pro reakci na pandemii, aby byl připraven rychle reagovat na hrozby spojené s šířením infekčních nemocí. Strategie zmírnění rizik zahrnují alternativní personální modely převodu kritických procesů na zdroje mimo danou oblast a také aktivaci plánu krizového řízení na podporu kritických operací. Pandemické plány by měly odkazovat na mezinárodní zdravotnické agentury a předpisy. Měly by také obsahovat informace o kontaktních místech těchto mezinárodních agentur.*

MONITOROVÁNÍ a PROTOKOLOVÁNÍ

- ***Kontrola přístupu do datového centra:*** *Přístup do datových center by měl být pravidelně přezkoumáván. Oprávnění k přístupu by mělo být automaticky zrušeno, jakmile dojde k ukončení pracovního poměru (a vymazání záznamu ze systému oddělení lidských zdrojů) daného zaměstnance CISP. Oprávnění přístupu zaměstnance nebo dodavatele by mělo být také zrušeno v případě, kdy vyprší platnost jeho povolení k přístupu, a to i v případě, že daná osoba nadále zůstává zaměstnancem CISP.*

- ***Protokoly přístupu do datového centra:*** *Fyzický přístup do datových center CISP by měl být zaznamenáván, monitorován a záznamy by měly být uchovávány. CISP by měl být schopen dávat informace získané z logických i fyzických monitorovacích systémů do souvislostí. Tomu by se měl věnovat tak často, jak je potřeba pro zvýšení úrovně bezpečnosti.*

- ***Monitorování přístupu do datového centra:*** *CISP by měl monitorovat datová centra pomocí globálních bezpečnostních operačních středisek, která jsou zodpovědná za monitorování, třídění a realizaci bezpečnostních programů. Tato střediska by měla poskytovat nepřetržitou globální podporu, měla by řídit a monitorovat přístupové aktivity datových center, vybavovat místní týmy a další podpůrné týmy tak, aby mohly reagovat na bezpečnostní incidenty prostřednictvím prioritizace, konzultací, analýz a odesíláním reakcí.*

SYSTÉMY DOHLEDU a DETEKCE

- ***KAMEROVÝ SYSTÉM:*** *Všechny fyzické přístupové body do serveroven by měly být monitorovány kamerovým systémem (CCTV). Záznamy je třeba uchovávat v souladu s právními předpisy a požadavky na dodržování předpisů.*

- ***Přístupové body datového centra:*** *Na všech vstupních bodech do budovy by měli být fyzicky přítomni profesionální bezpečnostní pracovníci, kteří s pomocí kamerových, detekčních a dalších elektronických systémů provádějí kontrolu osob vstupujících do objektu. Oprávnění zaměstnanci by měli pro přístup do datových center používat vícefaktorové ověřovací mechanismy. Vstupy do serveroven by měly být zabezpečeny zařízeními, která spustí alarm a zahájí reakci na událost, jakmile jsou dveře násilně otevřeny nebo drženy v otevřené pozici.*

- ***Odhalení vniknutí:*** *V rámci datové vrstvy by měly být instalovány elektronické systémy pro odhalení vniknutí, které monitorují, detekují a automaticky upozorňují příslušné pracovníky na bezpečnostní incidenty. Vstupní a výstupní body do serveroven by měly být zabezpečeny zařízeními, která vyžadují, aby každá osoba před povolením vstupu nebo výstupu absolvovala proces vícefaktorového ověření. Tato zařízení spustí alarm, pokud jsou dveře bez ověření násilně otevřeny nebo jsou drženy otevřené. Poplašná zařízení na dveřích by měla být konfigurována tak, aby detekovala všechny případy, kdy osoba opouští nebo vstupuje do datové oblasti bez poskytnutí vícefaktorového ověření. Údaje o poplachu by měly být okamžitě odesílány do bezpečnostních operačních středisek CISP s nepřetržitým provozem. Zde by mělo okamžitě dojít k záznamu události, analýze a následné reakci.*

SPRÁVA ZAŘÍZENÍ

- ***Správa majetku:*** *Majetek CISP by měl být centrálně spravován prostřednictvím systému správy inventáře, který uchovává a sleduje informace o vlastníkovi, umístění, stavu, údržbě a další popisné informace o majetku ve vlastnictví CISP. Po pořízení by měl být majetek zaevidován (naskenován) a sledován. U majetku, který prochází údržbou, by mělo být kontrolováno a sledováno jeho vlastnictví, stav a případná navržená řešení.*

- ***Likvidace médií:*** *Zařízení pro ukládání dat zákazníků by měla být ze strany CISP klasifikována jako kritická a mělo by s nimi být zacházeno jako s vysoce rizikovými. To by mělo platit po celou dobu jejich životního cyklu. CISP by měl používat přísné normy pro instalaci, servis a případnou likvidaci zařízení, pokud již nejsou využívána. Po skončení životnosti paměťového zařízení by měl vyřazovat CISP média z provozu prostřednictvím technik popsaných v dokumentu NIST 800-88. Média, na kterých jsou uloženy údaje zákazníků, by měla být vyřazena ze správy CISP až po bezpečném vyřazení těchto médií z provozu.*

SYSTÉMY PRO PODPORU PROVOZU

- ***Napájení:*** *Systémy elektrického napájení datového centra CISP by měly být navrženy tak, aby byly plně redundantní a udržovatelné bez narušení provozu. CISP by měl zajistit, aby byla datová centra vybavena záložním zdrojem napájení, který zajistí dostupnost energie a zachování provozu v případě výpadku elektrické energie pro kritické a nezbytné systémy.*

- ***Prostředí a teplota:*** *Datová centra CISP by měla používat mechanismy pro kontrolu klimatu a udržování vhodné provozní teploty serverů a dalšího hardwaru. Cílem je minimalizovat riziko přehřátí a výpadků služeb. Personál by měl s pomocí odpovídajících systémů monitorovat a kontrolovat teplotu a vlhkost.*

- ***Detekce a hašení požáru:*** *Datová centra CISP by měla být vybavena automatickým zařízením pro detekci a hašení požáru. Systémy detekce požáru by měly využívat kouřová čidla v síťových, mechanických a infrastrukturních prostorách. Tyto oblasti by měly být rovněž chráněny hasicími systémy.*

- ***Detekce úniku vody:*** *Datová centra CISP by měla být vybavena funkcemi detekce vody pro případ jejího úniku. Pokud je zjištěna přítomnost vody, je nutné použít zavedené mechanismy vedoucí k odstranění úniku a zabránění dalším škodám způsobeným vodou.*

ÚDRŽBA INFRASTRUKTURY

- ***Údržba zařízení:*** *CISP by měl sledovat a provádět preventivní údržbu elektrických a mechanických zařízení, aby byla zachována trvalá funkčnost systémů v jeho datových centrech. Údržbu zařízení by měly provádět kvalifikované osoby v souladu se zdokumentovaným plánem údržby.*

- ***Správa prostředí:*** *CISP by měl monitorovat elektrické a mechanické systémy a zařízení, aby byl schopen okamžitě identifikovat případné problémy. Měl by tak činit s využitím nástrojů permanentní kontroly a informací, které získává ze svého systému pro správu budov a monitorování elektrických zařízení. Preventivní údržba by měla být prováděna tak, aby byla zachována trvalá provozuschopnost zařízení.*

ŘÍZENÍ A KONTROLA RIZIK

- ***Průběžné řízení rizik datového centra:*** *Bezpečnostní operační středisko CISP by mělo provádět pravidelné kontroly hrozeb a zranitelností datových center. Průběžné hodnocení a eliminování potenciálních zranitelností by mělo probíhat na základě hodnocení rizik datového centra. Toto hodnocení by mělo být prováděno jako doplněk k procesu hodnocení rizik na úrovni podniku, který je používán k identifikaci a řízení rizik pro podnik jako celek. Tento proces by měl rovněž zohlednit rizika spojená s místními regulačními a environmentálními předpisy.*

- ***Bezpečnostní atestace třetích stran:*** *Testování datových center CISP třetími stranami, dokumentované zprávami těchto třetích stran, by mělo prověřit a potvrdit, že CISP vhodně zavedl bezpečnostní opatření v souladu se stanovenými pravidly pro získávání bezpečnostních certifikátů. V závislosti na programu pro soulad s předpisy a na jeho požadavcích mohou externí auditoři provádět kontrolu způsobu likvidace médií, dále mohou prohlížet záznamy z bezpečnostních kamer, pozorovat vstupy a chodby v celém datovém centru, testovat elektronická zařízení s ohledem na kontrolu přístupu a zkoumat vybavení datového centra.*

7. Migrace

	Požadavek
1.	***SLUŽBY MIGRACE:*** *Kolik různých služeb migrace dat poskytovatel cloudu nabízí?*
2.	***MIGRACE – CENTRALIZOVANÉ MONITOROVÁNÍ:*** *Nabízí poskytovatel cloudu organizacím centralizovanou službu (ucelené zobrazení), v rámci které mohou monitorovat stav migrace svých serverů a aplikací?*
3.	***MIGRACE – ŘÍDICÍ PANEL:*** *Nabízí poskytovatel cloudu v rámci nástroje pro migraci řídicí panel pro rychlou vizualizaci stavu migrace, souvisejících metrik a historie migrace?*
4.	***MIGRACE – NÁSTROJE POSKYTOVATELE CLOUDU:*** *Nabízí poskytovatel cloudu v rámci nástroje pro migraci možnost integrování s dalšími migračními nástroji poskytovatele cloudu, které mohou provádět migraci serverů a aplikací?*
5.	***MIGRACE – NÁSTROJE TŘETÍCH STRAN:*** *Nabízí poskytovatel cloudu v rámci nástroje pro migraci možnost začlenění nástrojů pro migraci třetích stran?* • *Pokud ano, jaké nástroje pro migraci třetích stran jsou podporovány?*
6.	***MIGRACE – MIGRACE V RÁMCI VÍCE OBLASTÍ:*** *Nabízí poskytovatel cloudu v rámci nástroje pro migraci možnost sledování a monitorování migrace serverů a aplikací v různých oblastech?*
7.	***MIGRACE – MIGRACE SERVERŮ:*** *Nabízí poskytovatel cloudu v rámci nástroje pro migraci možnost migrace lokálních virtualizovaných serverů do cloudu?* • *Pokud ano, jaká virtualizovaná prostředí jsou v současné době podporována?*
8.	***MIGRACE – ZJIŠŤOVÁNÍ SERVERŮ:*** *Má nástroj pro migraci, nabízený poskytovatelem cloudu, schopnost automaticky vyhledat místní virtuální servery, které mají být migrovány do cloudu?*
9.	***MIGRACE – DATA O VÝKONU SERVERU:*** *Má nástroj pro migraci nabízený poskytovatelem cloudu možnost shromažďovat a zobrazovat data o výkonu serveru a/nebo virtuálního stroje, jako jsou například data o využití centrální procesorové jednotky (CPU) a paměti RAM?*
10.	***MIGRACE – DISCOVERY DATABASE:*** *Má nástroj pro migraci, nabízený poskytovatelem cloudu, možnost ukládat všechna shromážděná data do centralizované databáze?* • *Pokud ano, mají organizace možnost tyto údaje exportovat? A do jakých formátů?*
11.	***MIGRACE – ŠIFROVÁNÍ NA ÚROVNI ÚLOŽIŠTĚ (AT-REST):*** *Šifruje poskytovatel cloudu za provozu všechny informace shromážděné a uložené v migrační databázi?*
12.	***MIGRACE – REPLIKACE SERVERU PO PŘÍRŮSTCÍCH:*** *Poskytuje nástroj pro migraci, nabízený poskytovatelem cloudu, automatickou, nepřetržitou replikaci serveru po přírůstcích během migrace serveru nebo virtuálního stroje (pro zajištění stavu, kdy jsou všechny změny provedené na serveru nebo virtuálním stroji zahrnuty do konečného migrovaného snímku)?* • *Pokud ano, jak dlouho může tato služba fungovat?*

13.	***MIGRACE – VMWARE:*** *Poskytuje nástroj pro migraci nabízený poskytovatelem cloudu migraci virtuálních strojů VMWare z místního prostředí do cloudu?*
14.	***MIGRACE – HYPER-V:*** *Poskytuje nástroj pro migraci nabízený poskytovatelem cloudu migraci virtuálních strojů Hyper-V z místního prostředí do cloudu?*
15.	***MIGRACE – ZJIŠŤOVÁNÍ APLIKACÍ:*** *Poskytuje nástroj pro migraci, nabízený poskytovatelem cloudu, možnost zjišťovat a seskupovat aplikace před jejich migrací?*
16.	***MIGRACE – MAPOVÁNÍ ZÁVISLOSTI:*** *Poskytuje nástroj pro migraci, nabízený poskytovatelem cloudu, možnost zjistit závislosti mezi servery a aplikacemi před jejich migrací?*
17.	***MIGRACE – MIGRACE DATABÁZE:*** *Poskytuje nástroj pro migraci, nabízený poskytovatelem cloudu, možnost migrace lokálních databází do cloudu?*
18.	***MIGRACE – VÝPADKY PŘI MIGRACI DATABÁZE:*** *Je nástroj pro migraci nabízený poskytovatelem cloudu schopen provést migraci databáze do cloudu s minimálními odstávkami, tj. tak, aby zdrojová databáze zůstala během procesu migrace plně funkční?*
19.	***MIGRACE – ZDROJOVÁ DATABÁZE:*** *Podporuje nástroj pro migraci nabízený poskytovatelem cloudu migraci různých databázových zdrojů, jako je Oracle, SQL Server atd...?* • *Pokud ano, uveďte prosím seznam všech podporovaných zdrojových databází, které lze migrovat do cloudu.*
20.	***MIGRACE – HETEROGENNÍ MIGRACE:*** *Má nástroj pro migraci nabízený poskytovatelem cloudu možnost provádět heterogenní migrace databází, tj. migrace z jedné zdrojové databáze do jiné cílové databáze, například z Oracle do SQL Serveru?* • *Pokud ano, uveďte všechny možné kombinace migrace heterogenních databází.*
21.	***MIGRACE – MIGRACE DAT V ŘÁDU PETABAJTŮ:*** *Nabízí poskytovatel cloudu petabajtové řešení, které využívá zabezpečená zařízení k přenosu velkého množství dat do cloudu a z něj?*
22.	***MIGRACE – MIGRACE DAT V ŘÁDU EXABAJTŮ:*** *Nabízí poskytovatel cloudu řešení pro přenos dat v řádu exabajtů, které umožňuje přesunout do cloudu extrémně velké objemy dat?*
23.	***MIGRACE – PODNIKOVÉ ZÁLOHOVÁNÍ:*** *Nabízí poskytovatel cloudu službu pro bezproblémovou integraci datového centra zákazníka se službami cloudového úložiště, která umožní přenášet a ukládat data do služby cloudového úložiště poskytovatele?*
24.	***MIGRACE – PODNIKOVÉ ZÁLOHOVÁNÍ – ÚLOŽIŠTĚ OBJEKTŮ:*** *Nabízí služba podnikového zálohování integraci se službou cloudového úložiště objektů poskytovatele?*
25.	***MIGRACE – PODNIKOVÉ ZÁLOHOVÁNÍ – PŘÍSTUP K SOUBORŮM:*** *Umožňuje služba podnikového zálohování, kterou dodává poskytovatel cloudu, uživatelům ukládat a načítat objekty pomocí souborových protokolů, jako je protokol systému souborů NFS?*
26.	***MIGRACE – PODNIKOVÉ ZÁLOHOVÁNÍ – PŘÍSTUP K BLOKŮM:*** *Umožňuje služba podnikového zálohování, kterou dodává poskytovatel cloudu, uživatelům ukládat a načítat objekty pomocí blokových protokolů, jako je protokol standardu iSCSI (Internet small computer systems interface)?*

27.	***MIGRACE – PODNIKOVÉ ZÁLOHOVÁNÍ – PŘÍSTUP K ZÁLOZE NA PÁSCE:*** *Umožňuje služba podnikového zálohování, kterou dodává poskytovatel cloudu, uživatelům zálohovat data prostřednictvím virtuální páskové knihovny a ukládat tyto zálohy na pásce do cloudu poskytovatele?*
28.	***MIGRACE – PODNIKOVÉ ZÁLOHOVÁNÍ – ŠIFROVÁNÍ:*** *Nabízí služba podnikového zálohování, kterou dodává poskytovatel cloudu, šifrování dat na úložišti (at-rest) i dat v tranzitu?*
29.	***MIGRACE – PODNIKOVÉ ZÁLOHOVÁNÍ – INTEGRACE SOFTWARU TŘETÍCH STRAN:*** *Je služba podnikového zálohování, kterou dodává poskytovatel cloudu, schopná integrace s běžně používanými zálohovacími softwary třetích stran?*
30.	***MIGRACE – LIMITY SLUŽBY:*** *Má poskytovatel cloudu nějaká omezení (tj. limity služeb), pokud jde o výše uvedenou část týkající se migrace?* *Příklad:* *Maximální počet souběžných migrací virtuálních strojů* *Maximální objednatelný počet řešení pro přenos dat*

8. Fakturace

	Požadavek
1.	***FAKTURACE – EVIDENCE A VYKAZOVÁNÍ:*** *Nabízí poskytovatel cloudu nějakou službu evidence a vykazování pro účely fakturace, která pomáhá uživatelům spravovat a sledovat stav využívání cloudových služeb?*
2.	***FAKTURACE – UPOZORNĚNÍ A OZNÁMENÍ:*** *Nabízí poskytovatel cloudu uživatelům možnost nastavení upozornění s oznámením, které uživatele informuje o tom, že jeho výdaje překračují určitou hranici?*
3.	***FAKTURACE – ŘÍZENÍ NÁKLADŮ:*** *Nabízí poskytovatel cloudu mechanismus pro tvorbu a vizualizaci grafů, které shrnují náklady a výdaje?*
4.	***FAKTURACE – ROZPOČTY:*** *Nabízí poskytovatel cloudu mechanismus pro zobrazení a správu rozpočtů včetně prognózy odhadovaných nákladů?*
5.	***FAKTURACE – KONSOLIDOVANÉ ZOBRAZENÍ:*** *Nabízí poskytovatel cloudu mechanismus pro konsolidaci fakturace z více účtů pod jeden primární platební účet?*
6.	***FAKTURACE – LIMITY SLUŽBY:*** *Má poskytovatel cloudu nějaká omezení (tj. limity služeb), pokud jde o výše uvedenou část týkající se fakturace?* *Příklad:* *Maximální počet účtů, které lze seskupit dohromady* *Maximální počet upozornění, která lze vytvořit* *Maximální počet rozpočtů, které lze spravovat*

9. Řízení

	Požadavek
1.	***ŘÍZENÍ – SLUŽBA PRO MONITOROVÁNÍ:*** *Nabízí poskytovatel cloudu monitorovací službu pro správu cloudových prostředků a aplikací, která shromažďuje, monitoruje a podává zprávy pomocí předem definovaných metrik?*
2.	***ŘÍZENÍ – ALARMY:*** *Umožňuje služba monitorování, kterou nabízí poskytovatel cloudu, uživatelům nastavit alarmy?*
3.	***ŘÍZENÍ – VLASTNÍ METRIKY:*** *Umožňuje služba monitorování, kterou nabízí poskytovatel cloudu, uživatelům vytvářet a nastavovat vlastní metriky?*
4.	***ŘÍZENÍ – GRANULARITA MONITOROVÁNÍ:*** *Poskytuje monitorovací služba, kterou nabízí poskytovatel cloudu, různé úrovně granularity monitorování až na úroveň 1 minuty?*
5.	***ŘÍZENÍ – SLUŽBA SLEDOVÁNÍ ROZHRANÍ API:*** *Nabízí poskytovatel cloudu službu, která pro lepší přehled zaznamenává, monitoruje a ukládá aktivity vzhledem ke cloudovým prostředkům jak na úrovni konzoly, tak na úrovni aplikačního programovacího rozhraní (API)?* • *Pokud ano, jaké služby poskytovatele cloudu jsou s touto službou sledování integrovány?*
6.	***ŘÍZENÍ – UPOZORNĚNÍ:*** *Umožňuje poskytovatel cloudu zasílání oznámení na základě úrovně aktivity aplikačního programovacího rozhraní (API)?*
7.	***ŘÍZENÍ – KOMPRESE:*** *Nabízí poskytovatel cloudu mechanismus komprese protokolů generovaných systémem sledování aplikačního programovacího rozhraní (API), který pomáhá uživatelům snížit náklady na ukládání dat spojené s touto službou?*
8.	***ŘÍZENÍ – AGREGACE DAT Z VÍCE OBLASTÍ:*** *Nabízí poskytovatel cloudu možnost zaznamenávat aktivity aplikačního programovacího rozhraní (API) účtu ve všech oblastech a poskytovat tyto informace souhrnně za účelem usnadnění používání?*
9.	***ŘÍZENÍ – INVENTARIZACE PROSTŘEDKŮ:*** *Nabízí poskytovatel cloudu službu pro posouzení, audit a vyhodnocení konfigurací prostředků nasazených uživatelem?*
10.	***ŘÍZENÍ – ZMĚNY KONFIGURACÍ:*** *Zaznamená poskytovatel cloudu automaticky změnu konfigurace prostředků, když k ní dojde?*
11.	***ŘÍZENÍ – HISTORIE KONFIGURACÍ:*** *Nabízí poskytovatel cloudu možnost prověřit konfiguraci prostředků v kterémkoli časovém okamžiku v minulosti?*
12.	***ŘÍZENÍ – PRAVIDLA PRO KONFIGURACE:*** *Nabízí poskytovatel cloudu pokyny a doporučení pro zajištění, konfiguraci a průběžné sledování souladu s předpisy?*
13.	***ŘÍZENÍ – ŠABLONY PROSTŘEDKŮ:*** *Nabízí poskytovatel cloudu uživatelům možnost vytvářet, poskytovat a spravovat kolekce prostředků ve formě šablon?*
14.	***ŘÍZENÍ – REPLIKACE ŠABLON PROSTŘEDKŮ:*** *Nabízí poskytovatel cloudu možnost rychlé replikace šablon prostředků v různých oblastech, aby je bylo možné použít v případě obnovení po katastrofě?*

15.	***ŘÍZENÍ – DESIGNER ŠABLON:*** *Nabízí poskytovatel cloudu snadno použitelný grafický nástroj s funkcí podpory přetahování objektů, který urychluje proces tvorby šablon prostředků?*
16.	***ŘÍZENÍ – KATALOG SLUŽEB:*** *Nabízí poskytovatel cloudu službu vytváření a správy katalogu služeb, tj. serverů, virtuálních strojů, softwaru, databází atd.?*
17.	***ŘÍZENÍ – PŘÍSTUP PŘES KONZOLI:*** *Nabízí poskytovatel cloudu webové uživatelské rozhraní, které usnadňuje správu a monitorování cloudových služeb?*
18.	***ŘÍZENÍ – PŘÍSTUP PŘES ROZHRANÍ CLI:*** *Nabízí poskytovatel cloudu jednotný nástroj pro správu a konfiguraci více cloudových služeb z rozhraní příkazového řádku (CLI) a umožňuje automatizovat úlohy správy pomocí skriptů?*
19.	***ŘÍZENÍ – MOBILNÍ PŘÍSTUP:*** *Nabízí poskytovatel cloudu aplikaci pro chytré telefony, se kterou se uživatelé mohou připojit ke cloudové službě a spravovat své prostředky?* • *Pokud ano, je tato aplikace dostupná pro iOS i Android?*
20.	***ŘÍZENÍ – OSVĚDČENÉ POSTUPY:*** *Nabízí poskytovatel cloudu službu, ve které mohou uživatelé porovnávat své používání cloudových služeb s osvědčenými postupy?*
21.	***ŘÍZENÍ – LIMITY SLUŽBY:*** *Má poskytovatel cloudu nějaká omezení (tj. limity služeb), pokud jde o výše uvedenou část týkající se řízení?* *Příklad:* *Maximální počet konfiguračních pravidel na účet* *Maximální počet upozornění, která lze vytvořit* *Maximální počet protokolů, které lze uložit*

10. Podpora

	Požadavek
1.	***PODPORA – SLUŽBA:*** *Nabízí poskytovatel cloudu podporu v jakoukoli dobu 24 hodin denně, 7 dní v týdnu a 365 dní v roce prostřednictvím telefonu, chatu a e-mailu?*
2.	***PODPORA – ÚROVNĚ PODPORY:*** *Nabízí poskytovatel cloudu různé úrovně podpory?*
3.	***PODPORA – ALOKACE ÚROVNÍ PODPORY:*** *Umožňuje poskytovatel cloudu uživatelům, aby sami přiřadili využívané zdroje/služby k různým úrovním podpory na základě jejich vlastní podrobné analýzy potřeb, a nenutí uživatele, aby si pro získání potřebných úrovní podpory zakládali samostatné cloudové účty?*
4.	***PODPORA – FÓRA:*** *Nabízí poskytovatel cloudu veřejná fóra podpory, kde mohou zákazníci diskutovat o svých problémech?*

5.	***PODPORA – ŘÍDICÍ PANEL STAVU SLUŽEB:*** *Nabízí poskytovatel cloudu řídicí panel, který poskytuje přehled o stavu služeb a zobrazuje aktuální informace o dostupnosti služeb v různých oblastech?*
6.	***PODPORA – PERSONALIZOVANÝ ŘÍDICÍ PANEL:*** *Nabízí poskytovatel cloudu řídicí panel, který umožňuje vytvoření personalizovaného přehledu výkonu a dostupnosti služeb s ohledem na konkrétní prostředky uživatele?*
7.	***PODPORA – ŘÍDICÍ PANEL A ZOBRAZENÍ HISTORIE:*** *Nabízí řídicí panel poskytovatele cloudu možnost zobrazení 365denní historie stavu služeb?*
8.	***PODPORA – PORADCE CLOUDOVÝCH SLUŽEB:*** *Nabízí poskytovatel cloudu službu, která funguje jako poradce cloudových služeb na míru a umožňuje porovnávat způsoby využití prostředků s doporučenými postupy?*
9.	***PODPORA – TAM:*** *Nabízí poskytovatel roli technického konzultanta přiděleného zákazníkovi TAM (technical account manager), který poskytuje technické znalosti pro celou škálu cloudových služeb?*
10.	***PODPORA – PODPORA APLIKACÍ TŘETÍCH STRAN:*** *Nabízí poskytovatel cloudu podporu pro běžné operační systémy a komponenty běžné aplikační architektury?*
11.	***PODPORA – VEŘEJNÉ ROZHRANÍ API:*** *Nabízí poskytovatel cloudu veřejné aplikační programovací rozhraní (API), které umožňuje programovou interakci s podporou nad žádostmi, tzn. nabízí možnost vytvářet, upravovat a uzavírat tyto žádosti?*
12.	***PODPORA – DOKUMENTACE SLUŽBY:*** *Nabízí poskytovatel cloudu kvalitní a veřejně přístupnou technickou dokumentaci ke všem svým službám, včetně uživatelských příruček, návodů, často kladených otázek (FAQ), poznámek k verzím apod.?*
13.	***PODPORA – DOKUMENTACE CLI:*** *Nabízí poskytovatel cloudu kvalitní a veřejně přístupnou technickou dokumentaci ke svému rozhraní příkazového řádku (CLI)?*
14.	***PODPORA – REFERENČNÍ ARCHITEKTURY:*** *Nabízí poskytovatel cloudu bezplatnou online kolekci dokumentů referenční architektury, která zákazníkům pomůže vytvářet konkrétní řešení kombinující velké množství cloudových služeb poskytovatele cloudu?*
15.	***PODPORA – REFERENČNÍ NASAZENÍ:*** *Nabízí poskytovatel cloudu bezplatnou online kolekci dokumentů, která obsahuje podrobné, otestované a ověřené postupy krok za krokem, včetně osvědčených postupů, pro implementaci běžných řešení (např. DevOps, Big Data, Data Warehouse, Microsoft workloads, SAP workloads atd.) ve svých cloudových nabídkách?*

Dodatek B – Technické hodnocení „Naživo“

Při výběru CISP je důležité posoudit schopnosti cloudové platformy „naživo“ pomocí veřejně dostupných služeb a infrastruktury CISP. Doporučujeme věnovat každému CISP z užšího výběru alespoň 1 celý den na technické hodnocení. Během hodnocení můžete: 1) provést důkladné hodnocení, abyste posoudili, zda prokázané schopnosti odpovídají požadavkům vaší RFP a písemným odpovědím CISP, 2) poskytnout vašim odborníkům platformu pro zkoumání CISP, abyste se ujistili, že odpovídá vašim specifickým technickým a organizačním potřebám, a 3) získat důvěru ve služby CISP a jeho schopnost škálovat, bezpečně a odolně fungovat a pokračovat v inovacích, které mu umožní vyhovět i budoucím potřebám.

Když CISP odpovídají na požadavky v RFP na cloudové služby, mohou uvádět svou shodu s požadavky vysoce interpretativním způsobem, který neposkytuje úplný kontext pro provozní prostředí organizace a potřeby aplikace. Doporučujeme proto sestavit technickou hodnotící komisi z předních technických, provozních, bezpečnostních a aplikačních odborníků. Hodnotitelé by měli v průběhu hodnocení CISP konfrontovat a v rámci osvědčeného postupu by měli CISP hodnotit nezávisle. Scénáře by měli hodnotit na stanovené stupnici, např. 0–4 (0=nepřijatelné, 1=hraniční, 2=přijatelné, 3=dobré, 4=vynikající). Poté lze výsledky ukázek konsolidovat a průměrné skóre za každý scénář zahrnout do celkového hodnocení CISP. Scénáře s vysokou směrodatnou odchylkou by měly být před finalizací projednány v týmu hodnotitelů. Po konsolidaci skóre lze použít váhu založenou na klíčovém významu scénářů.

Pokud jde o rozsah prokazování schopností, doporučujeme vytvořit ucelený pohled na platformu CISP a poté detailně vyhodnotit konkrétní úlohy, které na platformě běží. Níže naleznete vzorovou osnovu pro hodnocení platformy a úloh. Organizace mohou na této základní verzi stavět nebo si ji přizpůsobit tak, aby vybraný CISP musel splňovat specifické funkční požadavky i požadavky netýkající se funkcí. Osvědčeným postupem je, že dodavatelé, kterým je předložen seznam scénářů a požadavků, mohou navrhnout program hodnocení naživo, který nabízí maximální míru pokrytí potřeb a zahrnuje 20 % času na otázky a odpovědi.

Hodnocení platformy: Pro přístup ke cloudu, který přináší optimální hodnotu a minimalizuje rizika, se u různých CISP vžil termín „Well Architected“ (dobře navržená architektura). Well architected scénáře v aktivní technické ukázce mohou zahrnovat tyto charakteristiky:

1. **Zabezpečení:** identita, centralizovaná správa, automatizovaná detekce hrozeb, ochrana dat, připravenost na události
2. **Hospodárnost s ohledem na výkon:** správné dimenzování, škálovatelnost/elasticita, serverless
3. **Spolehlivost:** vysoká dostupnost (odolnost vůči poruchám), snížení rizika změn, obnovení po katastrofě, zálohování
4. **Řízení nákladů:** finanční operace, obchodní optimalizace, rozpočty a alokace nákladů
5. **Efektivnost provozu (Excellence):** automatizace, monitorování, podpora, správa a schopnosti potřebné pro přechod na cloud a jeho provozování

Hodnocení úloh: Mezi běžné typy aplikací, které lze testovat, patří:

- **Webová aplikace:** Veřejné hostování dynamických webových stránek, včetně backendové databáze a statického úložiště objektů.
- **Analýza dat:** Datové jezero (Data Lake) nebo architektura Lake House, která umožňuje konsolidaci dat od různých poskytovatelů dat a schopnost vypořádat se s vysokým objemem (TB/PB), různorodostí (strukturovaná, nestrukturovaná, různé formáty atd.) a rychlostí (rychlost generování dat, změny a vzory dotazů).
- **Platforma pro datové vědy:** Platforma, která umožňuje vývoj, nasazení a využití schopností založených na AI/ML v rámci celé organizace.
- **Aplikace IoT:** Platforma/schopnost IoT, která zahrnuje cloud, síťové schopnosti a zařízení.

Pro každou reprezentativní úlohu, která je pro vaši organizaci důležitá, můžete definovat scénáře, které má CISP představit. Scénáře by měly důvěryhodně prokázat schopnost nasazení úloh s dodržením standardu „well architected“. Následující stránky obsahují vzorová kritéria technického hodnocení za provozu pro: 1) platformu CISP a 2) vzorovou webovou aplikaci.

Platforma – Ukázka technického hodnocení „Naživo“

ID scénáře	Název scénáře	Klíčovost (1=nízká, 4=kritická)	Požadavky ukázky	Parametry hodnocení
Zabezp. plat.1	Federace identit	4	Prokázat schopnost federace ze stávajícího úložiště identit do cloudové služby.	• Podpora standardních protokolů, například SAML. • Podpora replikace identit na základě SCIM. • Možnost definovat různé úrovně přístupu v rámci úložiště podnikových identit a jejich aplikace v rámci poskytovatele cloudu. • Možnost omezit konkrétní týmy/jednotlivce pouze na určité účty/projekty/úlohy. • Schopnost podporovat řízení přístupu na základě atributů (ABAC) a používat tyto atributy v rámci systému správy identit a přístupu (IAM) poskytovatele cloudu k řízení přístupu ke cloudovým prostředkům.
Zabezp. plat.2	Centrální řízení	4	Prokázat schopnost definovat zásady a požadavky centrálně, na úrovni organizace (globální zásady) a také na úrovni podnikových jednotek a projektů.	• Zásady by měly zahrnovat: povolení/zakázání služeb, použití geografických omezení (omezení oblastí). • Zásady by také měly uživatelům, včetně správců, omezit možnost zakázat jakékoli kontroly auditu/správy.
Zabezp. plat.3	Omezení oprávnění uživatele	3	Prokázat automatická doporučení pro zpřísnění uživatelských oprávnění.	• Možnost porovnat aktuální oprávnění s požadovanými oprávněními. • Automatické generování zásad pro podporu nejmenších privilegií.
Zabezp. plat.4	Zaznamenávání protokolů pro činnost auditu	4	Prokázat zaznamenávání protokolů pro auditní činnosti v cloudu, včetně povolených a zakázaných akcí.	• Centralizované protokoly pro celou organizaci. • Protokoly pro konkrétní účet/projekt na podporu sledování a odpovědnosti na nízké úrovni. • Nástroje umožňující dotazování na protokoly. • Nástroje umožňující spouštění akcí na základě konkrétních událostí/záznamů v protokolu. • Možnost zobrazit aktivity podpory dodavatele. • Možnost zabránit mazání protokolů, a to i správcům.
Zabezp. plat.5	Izolace sítě	4	Prokázat a doložit izolaci různých tenantů v rámci cloudu, pokud je to možné. Prokázat konfiguraci izolované (bez připojení), privátní (bez přístupu k internetu) a veřejné (s přístupem k internetu) podsítě.	• Oddělení tenantů, včetně služeb VPN a křížového propojení. • Možnost řídit tok provozu mimo cloudovou infrastrukturu (lokálně), uvnitř ní a do internetu. • Jak se separace uplatňuje při používání sdílených služeb, jako je hostování kontejnerů nebo funkce jako služba.

ID scénáře	Název scénáře	Klíčovost (1=nízká, 4=kritická)	Požadavky ukázky	Parametry hodnocení
Zabezp. plat.6	Šifrování na úrovni úložiště (at-rest)	4	Prokázat schopnost šifrovat data na úrovni úložiště (at-rest), včetně možností šifrování BYOK a šifrování na straně klienta.	• Možnost vyžadovat šifrování citlivých dat. • Možnost používat klíče spravované poskytovatelem nebo klíče spravované zákazníkem. • Dodržování FIPS 140-2. • Schopnost upozorňovat na nedodržování požadavků na šifrování a zaznamenávat je do protokolů. • Vícenáklady. • Vliv na výkon. • Podpora kvantových důkazových algoritmů a velikostí klíčů.
Zabezp. plat.7	Šifrování při přenosu	4	Prokázat schopnost šifrovat data při přenosu.	• Šifrování ve výchozím nastavení pro rozhraní API služeb. • Možnost povolit šifrování při přenosu (TLS) u nástrojů pro vyrovnávání zátěže a spravovaných rozhraní API. • Podpora vzájemného ověřování (klienta a serveru).
Zabezp. plat.8	Správa klíčů	4	Prokázat schopnost správy klíčů. Zahrnout celý životní cyklus klíče. Zahrnout integraci s cloudovými službami.	• Zaznamenávání vytváření, používání, rotace a likvidace klíčů.
Zabezp. plat.9	Správa konfigurace	3	Prokázat schopnosti správy konfigurace cloudové platformy.	• Udržování přesné CMBD. • Kontrola souladu s požadavky. • Automatické spouštění akcí na základě nesouladu s předpisy. • Schopnost vyhodnocovat změny konfigurace na základě osvědčených postupů nebo vlastních pravidel.
Zabezp. plat.10	Zabezpečení sítě	3	Prokázat funkčnost a schopnosti webově aplikačního firewallu (WAF) a brány firewall, včetně integrace se sadami pravidel/firewally třetích stran a ochrany před volumetrickými útoky.	• Funkce WAF (Web Application Firewall): škálovatelnost. • Podpora privátních i veřejných sítí. • Možnost přihlásit se k odběru oborových kanálů/kanálů výrobců zařízení pro sady pravidel. • Automatické spouštění akcí v rámci infrastruktury na základě událostí z WAF. • Funkce brány firewall, škálovatelnost. • Brány firewall na úrovni serveru (host) a na úrovni sítě. • Možnost odkazovat na logické skupiny nebo objekty kromě možnosti zadávat IP bloky CIDR. • Počet pravidel podporovaných na každé úrovni/složce.

ID scénáře	Název scénáře	Klíčovost (1=nízká, 4=kritická)	Požadavky ukázky	Parametry hodnocení
				• Schopnost podporovat distribuovaný provozní model (síťový tým + tým vývojářů) prostřednictvím zásad a konfigurace sítě.
Zabezp. plat.11	Síťová konektivita	3	Prokázat schopnost připojit se k lokálním sítím, koncovým bodům/klientům, privátním sítím v cloudu.	• Privátní připojení (vysoká šířka pásma > 10 GBs). • Možnost řídit směrování (routing) a brány firewall v celé organizaci. • Připojení VPN (site-to-site a klientské). • Podpora IPV6.
Zabezp. plat.12	Správa instancí	3	Prokázat možnosti správy instancí.	• Schopnost monitorovat a spravovat stav aktualizací velkého množství instancí. • Podpora správy aktualizací operačních systémů Linux a Windows. • Možnost spouštět příkazy na celé flotile serverů bez nutnosti použití SSH. • Možnost centrálního řízení a auditu vzdáleného přístupu k virtuálním strojům. • Možnost měnit velikost instance, připojovat další svazky, měnit konfiguraci sítě atd. prostřednictvím konzoly, CLI a API.
Zabezp. plat.13	Aplikace zásad	3	Prokázat schopnost konfigurovat služby tak, aby se zabránilo přístupu z veřejného internetu.	• Možnost izolovat provoz do soukromé sítě pro služby, které mohou obsahovat kritická/důvěrná data. • Možnost definovat pravidla, která řídí přístup k datům na základě zdrojové sítě. • Uplatnění těchto omezení přístupu na všechny uživatele, včetně uživatelů s pověřeními vyšší úrovně.
Zabezp. plat.14	Kontrola zranitelností	2	Prokázat schopnost skenovat snímky (images) (kontejner a virtuální stroj) se zaměřením na zranitelnosti.	• Možnost automatického skenování kontejnerů v registru. • Možnost skenovat virtuální stroje na známé zranitelnosti. • Možnost provádět skenování sítě.
Zabezp. plat.15	Kontrola sítě	2	Prokázat schopnost zachytávat/zrcadlit síťový provoz (NetFlow a full packet) z prostředí zákazníka.	• Možnost zrcadlení části/celého provozu v infrastruktuře poskytovatele cloudu (z pohledu prostředí zákazníka – tenant), včetně úplného zachycení paketů. • Možnost jednoduše vybrat provoz, který chcete zachytit. • Schopnost škálovat na velmi velké objemy provozu (> 50 GB/s).

ID scénáře	Název scénáře	Klíčovost (1=nízká, 4=kritická)	Požadavky ukázky	Parametry hodnocení
Zabezp. plat.16	Detekce hrozeb	3	Prokázat schopnost detekce narušení vaší platformy, včetně hrozeb ze sítě, použití pověření a analýzy vzorů použití (usage pattern).	• Schopnost odhalit podezřelé činnosti, jako je „těžba“. • Schopnost detekovat útoky hrubou silou na autentizaci, například přihlášení SSH. • Schopnost odhalit únik nebo zneužití pověření (přihlašovacích údajů). • Použití strojového učení (ML) pro analýzu velkého množství událostí a vyhledávání těch prioritních. • Náročnost na aktivaci/konfiguraci (čím jednodušší, tím lepší). • Možnost integrace s externími službami a spouštění oznámení. • Možnost konfigurovat IDS na globální úrovni pro všechny projekty/účty.
Výk.plat.1	Optimalizace výpočetních prostředků/výkonu	2	Prokázat automatická doporučení pro optimalizaci nákladů na virtuální stroj a funkci jako službu.	• Doporučení na základě skutečného využití a dle vzorců využití. • Doporučení zahrnují odhadované úspory a informace o očekávané úrovni zatížení/technických důsledcích. • Optimalizace by měla zahrnovat jak úspory, tak „výkonnostní rizika“, kdy mohou být virtuální stroje například poddimenzované.
Výk.plat.2	Optimalizace prostředí	2	Prokázat automatická doporučení pro další cloudové komponenty, jako jsou nástroje pro vyrovnávání zátěže (load balancing), sítě, databáze, úložiště atd.	• Doporučení poukazují na úspory a potenciální příležitosti ke zvýšení efektivity v dalších komponentách mimo výpočetní prostředky.
Výk.plat.3	Automatické škálování výpočetního výkonu	4	Prokázat možnosti automatického škálování aplikace nasazené za nástrojem pro vyrovnávání zátěže ve virtuálním výpočetním prostředí. Prokázat různé možnosti/přístupy a možnost spouštět další (volitelné) akce před/po událostech škálování, například oznámení.	• Různé možnosti škálování založené na událostech, na čase, manuálních nebo pokročilejších přístupech, které používají strojové učení k předvídání požadované kapacity. • Plně automatizované škálování integrované s nástrojem pro vyrovnávání zátěže a kontrolami stavu. • Schopnost spustit libovolný kus kódu v určitých bodech životního cyklu škálování.
Výk.plat.4	Škálování v reálném čase pro úložiště	3	Prokázat schopnost škálovat kapacitu i propustnost blokového úložiště bez přerušení úloh.	• Možnost přechodu mezi různými typy blokových úložišť bez nutnosti kompletní přestavby služeb. • Možnost zvětšit velikost svazků pro virtuální stroje.

ID scénáře	Název scénáře	Klíčovost (1=nízká, 4=kritická)	Požadavky ukázky	Parametry hodnocení
Výk.plat.5	Automatické škálování pro spravované služby	3	Prokázat schopnosti úložiště objektů, brány API, platformy FaaS a databáze NoSQL škálovat od několika současně pracujících uživatelů až po tisíce.	• Plynulé automatické škálování, v ideálním případě bez zásahu správce. • Konzistentní výkon během celého průběhu škálování, které je v souladu s požadavky produkčního systému. • Možnosti procesu „pre-warming“ a nastavení limitů pro souběžné spouštění některých komponent (jako je FaaS), pokud to bude potřeba.
Výk.plat.6	Spouštění a řízení úloh pomocí kontejnerů	3	Prokázat schopnost spouštět a řídit úlohy pomocí kontejnerů.	• Druhy platforem pro hostování kontejnerů. • Integrace s dalšími komponentami IaaS, například s nástrojem pro vyrovnávání zatížení. • Dostupnost řešení service mesh. • Open-source možnosti hostování kontejnerů, například Kubernetes. • Nativní podpora vysoké dostupnosti v rámci řídicí roviny (control plane) kontejnerů. • Možnost spravovat hostitele kontejnerů v místě.
Spol.plat.1	Regionální odolnost	4	Prokázat automatizované převzetí služeb při selhání instance relační databáze v dané oblasti. Lze realizovat pomocí simulace geograficky lokalizovaného selhání (například výpadku proudu).	• Automatické převzetí služeb při selhání. • Izolování chybových zón v oblasti cloudu. • Jasně vymezený proces s jednoduchou architekturou umožňující vysokou dostupnost.
Spol.plat.2	Automatické obnovení instance	2	Prokázat automatické zotavení instance/skupiny instancí po neúspěšné kontrole stavu.	• Konfigurovatelné kontroly stavu. • Plně automatizované obnovení/opětovné zřízení instancí.
Spol.plat.3	Sledování zdraví pro nástroj vyrovnávání zátěže	3	Prokázat, jak nástroj pro vyrovnávání zátěže automaticky detekuje vadnou instanci a přesměruje provoz na jiné zdravé hostitele.	• Konfigurovatelné kontroly stavu. • Automatické směrování provozu na zdravé hostitele.
Spol.plat.4	Převzetí oblasti při selhání	3	Prokázat architekturu pro více oblastí, včetně automatizovaného převedení provozu do sekundární oblasti.	• Kontroly stavu v globálním kontextu. • Možnosti automatizovaného směrování: latence, vážení a převzetí služeb při selhání. • Podpora úloh virtuálních strojů a spravovaných služeb, jako je služba Object Store/databáze NoSQL.

ID scénáře	Název scénáře	Klíčovost (1=nízká, 4=kritická)	Požadavky ukázky	Parametry hodnocení
Spol.plat.5	Zálohování a obnovení	4	Prokázat možnosti zálohování a obnovení pro: virtuální stroje, databáze, spravované služby.	• Úroveň automatizace. • Možnost obnovení do stejného/jiného regionu cloudu. • Možnost kopírovat zálohy do jiného regionu cloudu.
Nákl.plat.1	Rozpočty	3	Prokázat schopnost řídit rozpočet, včetně jeho struktury pro podúčty a projekty.	• Zvažte možnost uplatnění rozpočtových kontrol a monitorování na různých úrovních organizace. • Zkontrolujte flexibilitu, například možnost seskupovat komponenty (pomocí tagů), nastavovat rozpočty pro konkrétní cloudové služby a konfigurovat prahové hodnoty pro upozornění/monitorování.
Nákl.plat.2	Přidělování rozpočtu	1	Prokázat zřízení nového projektového prostředí (účtu), včetně procesu přidělování rozpočtu na projekt. Zřizování by mělo zahrnovat manuální schvalovací kroky pro 1) technickou kontrolu/IT, 2) obchodní kontrolu/finance.	• Možnost vlastního zřizování s příslušnými povoleními. • Automatizace konfigurace příslušného nastavení rozpočtu, oznámení nebo rozpočtových zásad podle potřeby vaší organizace.
Nákl.plat.3	Vykazování rozpočtu	2	Prokázat schopnost podávat zprávy o rozpočtech v rámci celé organizace. Vykazování pro konkrétní oddělení vs. celou organizaci (need to know). Vykazování by mělo zahrnovat „skutečné“ i předpokládané/odhadované hodnoty výdajů.	• Schopnost zajistit viditelnost na různých úrovních organizace, vytvářet povědomí o rozpočtech a transparentnost, ale jen na základě oprávnění. • Prognózy by měly vycházet ze současných a minulých trendů spotřeby a měly by včas varovat před možným překročením rozpočtu.
Nákl.plat.4	Řízení rozpočtu	1	Prokázat schopnost přijmout opatření při dosažení určené hodnoty rozpočtu. Opatření mohou zahrnovat oznámení, uplatnění omezení nebo aktivní zásah s cílem zabránit nadměrnému čerpání rozpočtu.	• Možnost jednoduše definovat akce pro různé projekty. • Možnost, aby se akce v jednotlivých projektech lišily, například s ohledem na odlišnosti vývojových a produkčních prostředí. • Možnost definovat více akcí a hlídaných hodnot pro stejný rozpočet/projekt. • Možnost definovat vlastní akce jako doplněk ke standardním funkcím.
Nákl.plat.5	Periodicita rozpočtu	1	Prokázat schopnost používat rozpočty pro různá časová období, denní/měsíční/roční atd. U ročních rozpočtů prokažte schopnost použít proměnlivé rozložení očekávaných výdajů v průběhu roku.	• Možnost definovat rozpočty pro různá časová období. • Možnost konfigurovat rozložení výdajů v průběhu roku pro roční rozpočty, což je důležité zejména pro sezónní/vysoce elastické užití, jako je například roční daňové přiznání.

ID scénáře	Název scénáře	Klíčovost (1=nízká, 4=kritická)	Požadavky ukázky	Parametry hodnocení
Nákl.plat.6	Tržiště marketplace třetích stran	3	Prokázat možnost nakupovat a nasazovat produkty třetích stran. Prokázat nastavení rozpočtu pro sadu produktů třetích stran dostupných prostřednictvím tržiště marketplace, a také možnost omezit dostupné produkty.	• Možnost nastavit rozpočet pro konkrétní produkt, globální rozpočet, rozpočet pro sadu projektů/účtů. • Možnost prezentovat uživatelům cloudu pouze dílčí část širšího tržiště marketplace.
Nákl.plat.7	Cenové modely pro výpočetní výkon	3	Prokázat různé cenové/komerční modely, které lze použít pro virtuální stroje.	• Možnosti by měly zahrnovat služby na vyžádání bez nutnosti dlouhodobého závazku a jednotkové ceny (za minutu/hodinu). • Nepovinné dlouhodobé závazky za nižší cenu. • Schopnost nakupovat instance za nižší cenu s rizikem přerušení. • Důležité je, že by mělo být možné kombinovat tyto modely v rámci jednoho projektu/účtu a také sdílet výhody mezi různými účty.
Nákl.plat.8	Obchodní doporučení	3	Prokázat možnost získávat obchodní doporučení k optimalizaci výdajů (bez nutnosti provádění technických změn).	• Ucelená doporučení pro více služeb, včetně virtuálních strojů a spravovaných databází. • Schopnost jednoduše přijímat doporučení a chápat očekávané úspory/přínosy.
Nákl.plat.9	Vyhrazení hostitelé	4	Prokázat možnost zajistit službu vyhrazeného hostitele, na kterou jsou vázány místní licence, a možnost využití těchto licencí.	• Jednoduché nastavení. • Možnost řízení využití. • Možnost sdílet hostitele v rámci různých projektů/klientských architektur.
Op.plat.1	Migrace virtuálního stroje	3	Prokázat import virtuálního stroje z lokálního prostředí do cloudové služby virtuálního stroje.	• Možnost importu operačních systémů Windows i Linux. • Možnost importovat více strojů najednou. • Možnost udržovat relaci replikace, která umožňuje rychlé „převzetí služeb při selhání“ do cloudu.
Op.plat.2	Možnosti DevOps a automatizace	4	Prokázat schopnosti v oblasti DevOps/automatizace, včetně toho, jak jsou prostředí definována jako kód, podpory plně automatizovaného nasazení, automatizovaného testování a vracení zpět.	• Možnost definovat všechny součásti systému jako kód, včetně sítě, virtuálních strojů, úložišť a databází. • Schopnost vytvářet pipeline. • Možnost vytvořit repozitář kódu. • Možnost automatizace sestavení. • Schopnost provádět nasazení typu blue/green. • Možnost vytvářet více prostředí a mít více fází nasazení. • Automatické vracení neúspěšných nasazení.

ID scénáře	Název scénáře	Klíčovost (1=nízká, 4=kritická)	Požadavky ukázky	Parametry hodnocení
Op.plat.3	Hostování aplikací	2	Demonstrace hostování jednoduché dvouúrovňové aplikace v nízkokódové/platformní službě. Včetně relační databáze a automatického škálování pro aplikační/webovou vrstvu.	• Jednoduchá konfigurace prostřednictvím uživatelského rozhraní. • Zahrnutí kontrol stavu, škálování, vysoké dostupnosti. Podpora platforem, Windows a Linux.
Op.plat.4	Integrace zabezpečení	2	Prokázání možností integrace vaší platformy z hlediska správy bezpečnostních incidentů a událostí.	• Možnost snadno integrovat a využívat bezpečnostní protokoly/záznamy od poskytovatele cloudu + rozhraní API pro integraci.
Op.plat.5	Integrace ITSM	3	Prokázání integračních schopností vaší platformy z pohledu ITSM (IT Service Management).	• Možnost vyvolat, sledovat a aktualizovat případ podpory prostřednictvím rozhraní API. • Možnost poskytovat služby nebo sady služeb jako „produkty“ prostřednictvím rozhraní API.
Op.plat.6	Podpora	4	Prokázání nabízené podpory.	• Různé úrovně podpory pro různé typy zatížení. • Možnost zahrnout do podpory také operační systém/databázový stroj atd. podle potřeby pro danou službu. • Možnost nabídnout nadstandardní péči („white glove“) s přiřazením vedoucích pracovníků podpory pro kritické systémy. • Možnost přípravy na strukturovanou událost a přezkoumání architektury. • Nahlédnutí do road mapy poskytovatele.
Op.plat.7	Auditovatelnost	4	Prokázání nástrojů, které máte k dispozici pro podporu auditů shody.	• Možnost získat podrobnosti o auditu shody s pravidly prostřednictvím konzole. • Schopnost spravovat a automatizovat audity dopadu na životní prostředí.
Op.plat.8	Převedení virtuálního stroje na kontejner	1	Prokázání převodu aplikace ve virtuálním stroji do kontejneru a její obsluha pomocí kontejnerové platformy poskytovatele cloudu.	• Snadnost použití konverze. • Doba konverze. • Podpora platforem .Net a Java.

Zatížení: Webová aplikace – Technické hodnocení ukázky „Naživo“

V následující části je uveden vzorový list pro vyhodnocení zatížení pro konkrétní úlohu „Webová aplikace“. Při vytváření hodnotícího listu pro danou aplikaci se důrazně doporučuje zapojit uživatele, vývojáře a správce aplikace, protože ti pravděpodobně nejlépe znají požadavky, aktuální problémy a omezení.

ID scénáře	Název scénáře	Klíčovost (1=nízká, 4=kritická)	Požadavky ukázky	Parametry hodnocení
Zab.web.1	Zabezpečení – ochrana aplikace	3	Prokázat schopnost blokovat pokusy o zneužití aplikace prostřednictvím SQL Injection, XSS Scripting a dalších útoků.	• Schopnost chránit před běžnými útoky typu „out of the box“ pomocí standardních pravidel/možností. • Možnost vytvářet vlastní kontroly/pravidla/funkce.
Zab.web.2	Zabezpečení – ochrana na základě množství dotazů/dat	3	Prokázání schopnosti blokovat/chránit před útoky zahrnujícími velké množství požadavků nebo datových objemů směřujících na aplikaci.	• Možnost konfigurace limitů a omezení počtu požadavků z dané IP adresy nebo seznamu adres.
Zab.web.3	Zabezpečení – ochrana na základě zdroje	3	Prokázat schopnost omezit přístup na základě síťového/geografického zdroje.	• Možnost omezení podle síťového bloku nebo seznamu síťových bloků. • Možnost omezení podle země původu (bez nutnosti spravovat seznamy IP adres).
Zab.web.4	Zabezpečení – segmentace sítě	4	Prokázat schopnost izolovat komponenty (webový server, aplikační server/DB server) a chránit je před šířením tzv. sever-jih (North-South) i tzv. východ-západ (East-West) prostřednictvím infrastruktury.	• Možnost umístit komponenty do různých podsítí a řídit tok provozu mezi různými podsítěmi. • Možnost řídit tok provozu na úrovni síťového rozhraní. • Možnost odkazovat na logické skupiny i bloky CIDR.
Zab.web.5	Zabezpečení – podpora TLS a správa certifikátů	4	Prokázat schopnost poskytovat koncový bod zabezpečený protokolem TLS a automaticky spravovat podpůrné součásti pro jeho poskytování, včetně automatické rotace certifikátů.	• Podpora nejnovějších protokolů TLS a možnost v případě potřeby vypnout starší verze. • Jednoduché generování, správa a rotace certifikátů (ideálně plně automatizované).
Výk.web.1	Výkon – škálovatelnost	4	Prokázat schopnost škálovat webovou aplikaci od 10 do 100 000 souběžných uživatelů pomocí dynamického automatického škálování.	• Možnost definovat pravidla škálování na základě času i spouštěcí události. • Bezproblémové škálování pro koncového uživatele a správce. Automatické zvětšování při zvýšení zatížení a zmenšování při snížení jeho zatížení. • Zajistit škálovatelnost na každé vrstvě webové aplikace (Load Balancer, webová vrstva, datová vrstva atd.).

ID scénáře	Název scénáře	Klíčovost (1=nízká, 4=kritická)	Požadavky ukázky	Parametry hodnocení
				• Dostupnost služeb mezipaměti na různých vrstvách aplikace podle potřeby.
Výk.web.2	Výkonnost – globální dodávky	3	Prokázat schopnosti CDN včetně demonstrace latence z různých míst po celém světě, včetně: Austrálie, Asie, Afriky, Středního východu, Severní Ameriky, Jižní Ameriky a Evropy.	• Možnost vytvoření a konfigurace CDN prostřednictvím konzole/API poskytovatele. • Konfigurovatelná pravidla distribuce pro různé geografické oblasti. • Konfigurovatelné ukládání do mezipaměti pro různé případy použití/aplikace.
Spol.web.1	Spolehlivost – odolnost v rámci jedné oblasti	4	Prokázat schopnost tolerovat lokální událost, jako je ztráta síťového připojení k datovému centru CISP.	• Automatické převzetí služeb při selhání a vysoká dostupnost v rámci regionu cloudu (město).
Spol.web.2	Spolehlivost – nasazení ve více oblastech	3	Prokázat nasazení webové aplikace ve více oblastech včetně globálně replikované databáze.	• Možnost programového nasazení aplikace ve více oblastech. • Replikace datového úložiště mezi oblastmi. • Automatické směrování uživatelů do jejich optimální oblasti.
Spol.web.3	Spolehlivost – převzetí služeb při selhání ve více oblastech	3	Prokázat automatické převzetí služeb při selhání webové aplikace v případě problému se službou s dopadem na danou oblast.	• Automatizované převzetí služeb při selhání a vysoká dostupnost ve více regionech cloudu.
Nákl.web.1	Náklady – přehled	2	Prokázat schopnost sledovat náklady na aplikaci.	• Možnost zobrazit historické náklady pro konkrétní aplikaci, včetně případů, kdy se škáluje nahoru/dolů.
Nákl.web.2	Náklady – rozpočty	2	Prokázat schopnost nastavit rozpočty a související výstrahy pro jednotlivé aplikace.	• Rozpočty nakonfigurované pro jednotlivé aplikace a možnost spouštět akce/upozornění na základě nakonfigurovaných zvolených hodnot.
Op.web.1	Operace – termíny údržby	3	Prokázat schopnost konfigurovat termíny údržby v souladu s podnikovými požadavky, zejména v případech, kdy údržba může ovlivnit dostupnost aplikace.	• Konfigurovatelné termíny údržby pro komponenty, jako je služba relační databáze.
Op.web.2	Operace – protokolování	3	Prokázání schopnosti centralizovat protokolování pro aplikaci s více součástmi, včetně jejich zachování při ukončení nebo poruše virtuálních strojů.	• Možnost konfigurovat centralizovanou službu protokolování, kterou lze škálovat spolu s požadavky aplikace. • Možnost definovat pravidla/filtry pro spouštění výstrah nebo akcí na základě konkrétních událostí protokolu.

ID scénáře	Název scénáře	Klíčovost (1=nízká, 4=kritická)	Požadavky ukázky	Parametry hodnocení
Op.web.3	Operace – monitorování	3	Prokázat monitorování aplikace, včetně výkonu, dostupnosti, doby odezvy, počtu chyb atd., a funkcí pro provádění akcí nebo spouštění oznámení na základě zvolených hodnot různých metrik.	• K dispozici je sbírka standardních metrik, jako jsou diskové IO, CPU, databázové metriky, síť, vyrovnávání zatížení atd. • Možnost definovat vlastní metriky, limity. • Možnost vytvořit vlastní přehledový panel, který bude ukazovat nejdůležitější metriky, a sdílet tyto panely s příslušnými uživateli.