Inkoop van cloud services in de publieke sector

Handboek - Inclusief RFP voorbeeldtekst voor een cloud raamovereenkomst

Versie 2: februari 2022

Kennisgeving

Dit document is uitsluitend bedoeld ter informatie. Het is niet ontwikkeld in overeenstemming met de wettelijke vereisten voor openbare aanbestedingen binnen een bepaalde regio. Cloud klanten zijn verantwoordelijk voor het maken van hun eigen onafhankelijke beoordeling van de informatie in dit document en het eventuele gebruik van de producten of diensten van een cloud aanbieder. Dit document geeft geen garanties, verklaringen, contractuele verplichtingen, voorwaarden of zekerheden.

Voorbeelddocumenten en -tekst mogen niet worden opgevat als juridisch advies, begeleiding of raadgeving. Cloud klanten dienen hun eigen juridische adviseurs te raadplegen over hun verantwoordelijkheden onder de toepasselijke wetgeving in hun eigen land. CISPE wijst uitdrukkelijk elke garantie of verantwoordelijkheid of schade af die verband houdt met of voortvloeit uit de informatie die in dit document wordt verstrekt.

Over CISPE

CISPE *(Cloud Infrastructure Services Providers in Europe*, https://cispe.cloud) is een onafhankelijke branche organisatie zonder winstoogmerk. Wij vertegenwoordigen dienstverleners op het gebied van cloud infrastructuur in Europa en werken samen met de sector en beleidsmakers aan begeleiding en voorlichting op het gebied van cloud services en hun rol in de sector, het openbare leven en de maatschappij in het algemeen.

Ons groeiend aantal leden omvat bedrijven die actief zijn in alle landen van de EU en die in 16 Europese landen hun wereldwijde hoofdkantoren hebben. De organisatie staat open voor bedrijven op voorwaarde dat zij verklaren dat ten minste één van hun diensten voldoet aan de vereisten van de CISPE gedragscode voor gegevensbescherming. Wij:

- Bepleiten de voordelen van het 'cloud first'-beleid inzake overheidsopdrachten binnen de EU en de EU-lidstaten
- Betrekken de cloud infrastructuursector bij het bereiken van klimaatneutraliteit in 2030
- Bevorderen samenhangende beveiligingseisen en technische normen voor de hele EU
- Ondersteunen uitgebreide privacyvereisten met een gedragscode voor gegevensbescherming
- Werken eraan om de EU-markt voor cloud infrastructuur open, concurrerend en vrij van afhankelijkheid te houden
- Voorkomen ongerechtvaardigde verplichtingen op het gebied van het toezicht op inhoud in het wettelijk kader van de EU

Onze leden leveren en onderhouden de essentiële 'bouwstenen voor IT' die het voor de overheid, openbare instanties en het bedrijfsleven mogelijk maken om hun eigen systemen te bouwen en essentiële diensten te leveren aan miljarden burgers. In deze rol helpen we de ontwikkeling van geavanceerde technologieën en diensten mogelijk te maken die kunstmatige intelligentie (KI), Connected Objects, autonome voertuigen en 5G, en de volgende generatie mobiele connectiviteitstechnologie gebruiken.

Gedragscode voor cloud-infrastructuurservices

De CISPE gedragscode voor gegevensbescherming, die in september 2016 werd gelanceerd, stamde al van voor de handhaving van de Europese Algemene Verordening Gegevensbescherming (AVG). Het sluit aan bij de strenge AVG eisen om cloud infrastructuuraanbieders te helpen voldoen aan de naleving van de gegevensbeveiliging en biedt een sterk kader om klanten te helpen bij het selecteren van cloud aanbieders en het vertrouwen in hun diensten. De CISPE gedragscode is in mei 2021 goedgekeurd door het Europees Comité voor gegevensbescherming (EDPB) en in juni 2021 door de Franse CNIL goedgekeurd, die optreedt als de bevoegde autoriteit. https://www.codeofconduct.cloud/

Climate Neutral Data Centre Pact

CISPE heeft eind 2019 samen met de Europese Commissie een reeks maatstaven en een zelfregulerend initiatief ontwikkeld om de klimaatneutraliteit van datacenters in 2030 te garanderen. Dit initiatief is ontwikkeld in samenwerking met de European Data Centre Association (EUDCA), samen met andere brancheorganisaties en marktpartijen op het gebied van datacenters - in januari 2021 geïntroduceerd als het 'Climate Neutral Data Centre Pact' https://www.climateneutraldatacenter.net/

Fair Software Initiative

Samen met de Franse CIO organisatie CIGREF, en met de steun van andere brancheorganisaties van CIO's en aanbieders in heel Europa, heeft CISPE 10 Principles of Fair Software Licensing for Cloud Customers geïntroduceerd, een reeks best practices voor bedrijven die groei-innovatie en flexibiliteit van de cloud verwachten, en die hun softwareleveranciers uitdagen om te zorgen dat er naar eerlijke licentievoorwaarden wordt verwezen.
https://www.fairsoftware.cloud/

GAIA-X

CISPE was een van de tweeëntwintig oprichters van GAIA-X – het Europese initiatief om een open, transparant en veilig digitaal ecosysteem te bieden. Als zodanig heeft CISPE zich vanaf het begin sterk gemaakt voor de visie en de principes van de GAIA-X organisatie en is de secretaris-generaal van CISPE in juni 2021 opnieuw gekozen om in de raad van bestuur te treden. Sommige tools waarnaar in het handboek wordt verwezen, zoals de CISPE gedragscode voor gegevensbescherming en de SWIPO IaaS gedragscode, zijn nuttig om de naleving van de GAIA-X-principes aan te tonen. https://www.gaia-x.eu

CISPE en de publieke sector

CISPE draagt bij aan het Europese publieke beleidsdebat en werkt aan een beter begrip van de rol, de bijdrage en het potentieel van de Europese branche op het gebied van cloud-infrastructuur.

Terwijl het openbare inkoopmodel de voorwaarde moet stellen voor het proces van het invoeren en gebruiken van cloud computing, verschilt de aanschaf van cloud services van de meeste traditionele technologie aankopen die bekend zijn in de publieke sector. Inkoopbenaderingen moeten worden heroverwogen: CISPE moedigt beleidsmakers in de EU aan om een ambitieuzere en meer toekomstgerichte aanpak op EU schaal te ontwikkelen op basis van 'cloud first'-beleidsinitiatieven, die de groei van de interne markt voor cloud infrastructuur in Europa helpen stimuleren en de groeidoelstellingen van de Digital Single Market (DSM) ondersteunen.

Dit handboek is gecreëerd om nuttige richtlijnen en ondersteuning te bieden aan publieke organisaties bij het aanschaffen van cloud services.

Meer informatie

CISPE leden: https://cispe.cloud/members
Raad van bestuur: https://cispe.cloud/board-of-directors
Cloud-computingservices verklaard onder de CISPE gedragscode:
https://www.codeofconduct.cloud/public-register/

Inhoudsopgave

versie 2, februari 2022

Samenvatting en doel van dit handboek

Het doel van dit **Handboek inkoop van cloud services** is om richtlijnen te bieden aan klanten die cloud services willen kopen via een inkoopproces op basis van concurrentie **(RFP voor cloud services)**, maar die niet over de expertise beschikken om een cloud-raamovereenkomst op te stellen.

Dit document is uitsluitend bedoeld ter informatie. Het is niet ontwikkeld in overeenstemming met de wettelijke vereisten voor openbare aanbestedingen binnen een bepaald land of een bepaalde regio.

In het handboek wordt ook gekeken naar extra selectiecriteria voor **Call-offs** of **Mini-competities** bij het kopen via een cloud-raamovereenkomst. De paragrafen van het handboek zijn zo onderverdeeld dat ze lijken op een algemene IT RFP. De voorbeeldtekst voor algemene RFP en selectiecriteria gaat gepaard met commentaar om te helpen begrijpen waarom een cloud RFP anders is dan een traditionele IT RFP.

Na de publicatie van de cloudstrategie van de Europese Commissie, die aangeeft hoe de Europese instellingen en diensten hun IT infrastructuur zullen moderniseren door middel van een cloud-first aanpak, heeft CISPE in juli 2019 het handboek aan de Europese Commissie overhandigd tijdens het evenement *'How to transform governments through a smart cloud policy'*.

Versie 2 van dit handboek bevat nieuwe richtlijnen met betrekking tot: gegevensbescherming (paragraaf 2.3.1.1), het wisselen van cloud-aanbieders en het overdragen van gegevens (paragraaf 2.3.1.2), softwarevoorwaarden (paragraaf 2.5.2), duurzaamheid in de cloud (paragraaf 3.6) en een vernieuwde bijlage B Live technische evaluatie.

> ***'Cloud services'*** *verwijst naar alle cloud technologieën en gerelateerde diensten waar een eindgebruiker mogelijk toegang toe nodig heeft. Het omvat consultancy, zakelijke dienstverlening of managed services die de migratie naar de cloud moeten ondersteunen en uitvoeren en die de workloads op de cloud moeten ondersteunen, naast de cloud infrastructuur zelf, en de diensten van de cloud marketplace zoals Software as a Service (SaaS)-producten.*

De opkomst van cloud computing als de standaardkeuze voor IT in de publieke sector biedt een kans om bestaande inkoopstrategieën te moderniseren. Cloud-gerichte inkoopprocessen kunnen organisaties in de publieke sector in staat stellen om de volledige voordelen van de cloud te benutten,

zoals toegang tot toonaangevende innovatie, verhoogde snelheid en wendbaarheid, verbeterde beveiligingshouding en compliance-governance, waardoor efficiëntie en kostenbesparingen kunnen worden bereikt.

Traditionele IT-inkoopmethoden voor de aanschaf van hardware, software en datacenters laten zich niet vertalen naar de aanschaf van cloud services. De benaderingen van prijsstelling, contractbeheer, algemene voorwaarden, beveiliging, technische eisen, SLA's en meer veranderen allemaal in een cloud model, en het gebruik van bestaande inkoopmethoden doet uiteindelijk de voordelen die de cloud biedt deels of geheel teniet.

Een van de beste manieren om cloud services effectief in de publieke sector aan te schaffen is via een **cloud raamovereenkomst** – een multi-organisatorische gunning van een menu van cloud services, van waaruit in aanmerking komende inkopers die zijn aangesloten bij de inkooporganisatie, de cloudtechnologieën en bijbehorende services kunnen aanschaffen die aan hun behoeften voldoen en deze kunnen afstemmen. Als middel voor cloud contracten maken dergelijke raamovereenkomsten het mogelijk om cloud services op een efficiënte en effectieve manier aan te kopen, zodat de aankopende organisaties en eindgebruikers toegang hebben tot een volledig scala aan cloud services en uiteindelijk ten volle kunnen profiteren van de voordelen van de cloud: flexibiliteit, enorme schaalvoordelen, schaalbaarheid om een betere beschikbaarheid te bereiken tegen lagere kosten, breedte van de functionaliteit, innovatiesnelheid, capaciteit om op te schalen naar nieuwe regio's.

Hou er rekening mee dat **dit document zich richt op de inkoop van Infrastructure as a Service (IaaS) en Platform as a Service (PaaS) cloud technologieën, zoals aangeboden door een *Cloud Infrastructure Service Provider (CISP)*.** Dergelijke cloud technologieën kunnen rechtstreeks bij een CISP worden gekocht, of via een CISP reseller. *Voor distributeurs van cloud marketplacediensten (PaaS en SaaS) en cloudconsulting-services zijn aanvullende RFP overwegingen vereist.*

Hou er ook rekening mee dat dit document niet elk aspect van het creëren van een end-to-end cloud-inkoopframework behandelt. Er zijn veel andere documenten van de branche en analisten die betrekking hebben op zaken als best practices voor cloud inkoop, hoe te budgetteren voor de cloud, cloud governance, enz., en we raden ten zeerste aan dergelijke adviezen en documenten in aanmerking te nemen bij de ontwikkeling van een algemene cloud inkoopstrategie. **Tabel 1** hieronder geeft een overzicht van het RFP voor cloud services handboek, met RFP voorbeeldtekst voor elke component van een RFP voor cloud services.

Tabel 1 – Samenvatting van de paragrafen van het handboek voor een cloud services-RFP

Paragraaf	Overzicht en RFP-voorbeeldtekst
0 **Overzicht van een cloud** raamovereenkomst	Een overkoepelende visie op het model van de raamovereenkomst voor de cloud (percelen, hoe te concurreren en te contracteren)
2.0 Overzicht RFP voor	Voorbeeld van een algemene RFP tekst die de onderstaande paragrafen omvat, samen met commentaar waarin de redenering achter de RFP structuur en de gebruikte taal van de cloud services worden uitgelegd.
2.1 Opzet RFP voor	2.1.1 Inleiding en strategische doelstellingen 2.1.2 Tijdlijn RFP beantwoording

Paragraaf	Overzicht en RFP-voorbeeldtekst
	2.1.3 Definities 2.1.4 Gedetailleerde beschrijving van het inkoopmodel en concurrentie binnen de raamovereenkomst 2.1.5 Minimumeisen voor de bieder - Administratief
2.2 Technisch	2.2.1 Minimumeisen 2.2.2 Vergelijking tussen leveranciers 2.2.3 Contracten
2.3 Beveiliging	2.3.1 Minimumeisen 2.3.1.1 Gegevensbescherming 2.3.1.2 Schakelen tussen cloud aanbieders en overdracht van gegevens 2.3.2 Vergelijking tussen leveranciers 2.3.3 Contracten
2.4 Prijzen	2.4.1 Minimumeisen 2.4.2 Vergelijking tussen leveranciers
2.5 Contract uitvoer opzetten/algemene voorwaarden	2.5.1 Algemene voorwaarden 2.5.2 Algemene voorwaarden software 2.5.3 Hoe te selecteren tussen de deelnemers aan een project 2.5.4 Onboarding en offboarding
3.0 Best practices/Lessons learned	3.1 Cloud Governance 3.2 Budgettering voor de cloud 3.3 Inzicht in het bedrijfsmodel van partners 3.4 Cloud 3.5 Pre-RFP sourcing/marktonderzoek 3.6 Duurzaamheid
Bijlage A - Technische eisen voor de vergelijking tussen bieders	Een lijst met algemene cloud technologievereisten voor call-off of mini-competities
Bijlage B – Live technische evaluatie	Een voorbeeldscript voor een product met cloud-technologie dat scores demonstreert (cloud demo's als onderdeel van een afroep of mini-competitie)

1.0 Overzicht van een cloud raamovereenkomst

Een goed ontworpen cloud raamovereenkomst kan de inkoop van cloud services mogelijk maken op een manier die zowel de deelnemende overheidsorganisaties als de cloud leveranciers ten goede komt. Voordelen van een goed ontworpen cloud raamovereenkomst zijn onder andere:

- Van nature coöperatief:
    - Meerdere organisaties die zich verenigen om orders te plaatsen voor vergelijkbare eisen betekent gemak, efficiëntie, lagere kosten en een vereenvoudigd bestelproces. Het stelt een effectieve manier vast om de vraag van meerdere overheidsorganisaties naar gemeenschappelijke cloud technologieën en bijbehorende cloud services, zoals marketplaceoplossingen en consultancy, te bundelen.
- Volledig aanbod aan cloud services:
    - Het kan alle consultancy, zakelijke dienstverlening of managed services omvatten die nodig zijn om de migratie naar de cloud volledig te ondersteunen en uit te voeren en om workloads in de cloud te ondersteunen, naast de door CISP geleverde cloud technologieën en marketplacediensten.
    - Cloud technologieën kunnen rechtstreeks bij een CISP of via een aangewezen reseller worden aangeschaft.
- Contractbeheer:
    - Dit brengt verschillende organisaties/kopers op één lijn rond een gemeenschappelijke reeks voorwaarden en één enkele hoofdgunning, in plaats van verschillende voor elke organisatie.
    - Het is ook van belang voor leveranciers omdat het een standaard aanschafproces, voorwaarden en bestelmechanisme biedt om te navigeren in plaats van verschillende voor elke organisatie in de publieke sector.
    - Het biedt flexibiliteit. Het creëren, goedkeuren en uitvoeren van een effectief cloud contract binnen het bestaande overheidsbeleid/regelgeving vereist experimenteren en het vermogen om zich snel aan te passen. Het is veel voordeliger om een raamovereenkomst te creëren die de publieke sector en cloud leveranciers in staat stelt om samen te werken om het contract contractueel, mechanisch en efficiënt te verbeteren. Een meerjarig contract dat niet werkt en niet kan worden aangepast, leidt tot een slechte ervaring voor eindgebruikers in de publieke sector, inkooporganisaties en cloud leveranciers.
- Keuze:
    - Het stelt kopers in staat om te kiezen tussen verschillende gekwalificeerde CISP's, en legt de lat hoog voor alle cloud services en bijbehorende services zoals een cloud PaaS/SaaS-markt, en cloud consulting.

- Het maakt het mogelijk controle te hebben over het aantal leveranciers binnen een raamovereenkomst door ervoor te zorgen dat de standaard van elke deelnemer op de juiste manier wordt onderzocht.

Een raamovereenkomst voor inkoop van cloud services werkt het beste wanneer deze de door CISP's geleverde IaaS/PaaS-technologieën omvat, samen met een PaaS/SaaS-marketplace en de consultancydiensten waartoe eindgebruikers uit de publieke sector toegang hebben, wanneer dat nodig is, om hen te helpen bij de planning, de transitie, het gebruik en het onderhoud van een workload die in de cloud wordt uitgevoerd. We stellen daarom voor om een cloud services RFP voor het opzetten van een cloud raamovereenkomst op te splitsen in 3 percelen zoals hieronder:

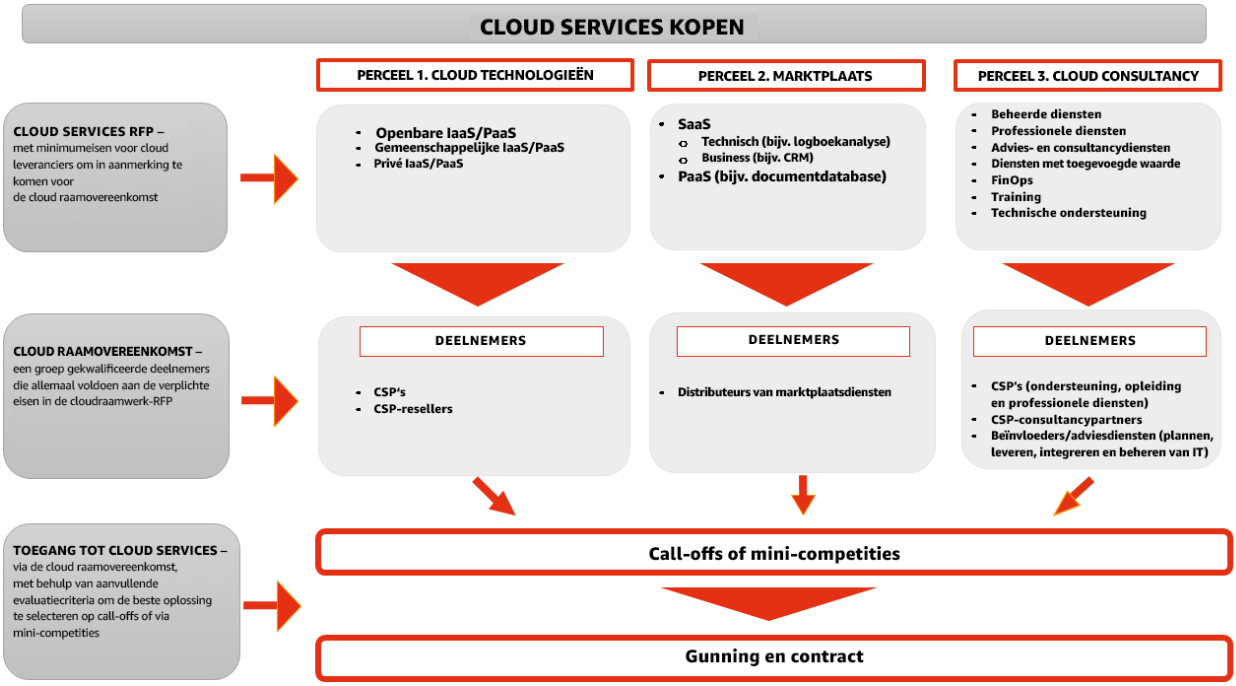
- PERCEEL 1 - CLOUD- TECHNOLOGIEËN
  Cloud technologieën die rechtstreeks bij een CISP of via een aangewezen CISP-reseller worden gekocht.

- PERCEEL 2 - MARKETPLACE
  Toegang tot een marketplace van PaaS- en SaaS diensten.

- PERCEEL 3 - CLOUD CONSULTANCY
  Cloud gerelateerde consultancy diensten (training, zakelijke dienstverlening, managed services, enz.) en technische ondersteuning.

*Zoals eerder opgemerkt, richt dit document zich op de inkoop van IaaS- en PaaS cloud technologieën (**PERCEEL 1**) zoals die door een CISP worden geleverd (rechtstreeks van een CISP gekocht, of via een CISP-reseller). Afzonderlijke kwalificatie eisen voor leveranciers zijn benodigd voor leveranciers in PERCEEL 2 en 3 van een cloud service RFP.*

Afbeelding 1 geeft een overkoepelend beeld van hoe een goed gestructureerde cloud service RFP, onderverdeeld in deze drie percelen, kan leiden tot een cloud raamovereenkomst die organisaties in de publieke sector voorziet van flexibiliteit (zowel technisch als contractueel), zichtbaarheid en controle van uitgaven en cloud gebruik, samen met de mogelijkheid om alle benodigde cloud services ter beschikking te hebben om oplossingen te bouwen en te onderhouden.



Afbeelding 1 - Een succesvolle RFP voor cloud services bestaat uit drie percelen. Elk perceel bevat categorieën of 'soorten aanbiedingen' onder het desbetreffende deel, om er zeker van te zijn dat deze technisch en contractueel geschikt zijn om te voldoen aan de eisen van de eindgebruiker bij de inkoop van de cloud raamovereenkomst.

Hou er rekening mee dat:

- Ieder perceel aan meerdere kandidaten gegund kan worden.
- PERCEEL 3 kan worden gegund via een andere RFP, of eventueel via een bestaand contract voor consultancydiensten.

PERCEEL 1 categorieën

Succesvolle cloud raamovereenkomsten vragen CISP's om het cloud model te beschrijven dat zij aanbieden, onderverdeeld in categorieën onder elk perceel. Wij raden u aan de branchestandaard voor cloud computing te gebruiken (de essentiële cloud kenmerken van het National Institute of Standards and Technology (NIST)) – voor de definities van **publieke-**, **gemeenschappelijke-** en **privé** cloud. Door op deze manier een cloud raamovereenkomst te structureren, kunnen de aanbestedende dienst en de overheidsinstellingen die het framework gebruiken, kiezen uit verschillende cloud modellen om aan hun behoeften te voldoen.

Bekijk *Paragraaf 2.1.3 Definities* voor de NIST-definitie van ieder cloudmodel in PERCEEL 1 (publieke IaaS/PaaS, gemeenschappelijke IaaS/PaaS, en privé IaaS/PaaS).

Hoe te concurreren - via call-off of mini-competities?

Kwalificatiecriteria voor een RFP voor cloud services moeten betrekking hebben op belangrijke elementen en minimumnormen, en mogen geen 'nice to have'-normen bevatten. Het toevoegen van aanvullende normen boven de basiseisen, om voor de raamovereenkomst in aanmerking

te komen, kan ertoe leiden dat sommige leveranciers niet in staat zijn om een bod uit te brengen, en uiteindelijk tot minder keuze voor de kopers.

Na de RFP en de daaropvolgende opzet van de cloud raamovereenkomst kunnen overheidsinstanties die partij zijn in het framework de benodigde cloud services bestellen of 'afroepen' wanneer dat nodig is. Door een call-off (afroep) contract onder een raamovereenkomst te plaatsen, kunnen kopers hun eisen verfijnen met aanvullende functionele specificaties voor een afroep, met behoud van de voordelen die de raamovereenkomst biedt.

Indien dit nodig wordt geacht, kan een mini-competitie worden gehouden om de beste leverancier voor een bepaalde workload of een bepaald project te identificeren. Bij een mini-competitie gaat een klant in het kader van de raamovereenkomst de concurrentie verder aan, door alle leveranciers binnen een perceel uit te nodigen om te reageren op een reeks van eisen. De klant zal alle bekwame leveranciers binnen het perceel uitnodigen om een bod uit te brengen, vandaar het belang van minimumeisen voor deelnemers bij een RFP voor cloud services - omdat het een hoge norm aan opties onder elk perceel garandeert.

Hou er rekening mee dat het belangrijk is dat er ***verschillende algemene voorwaarden*** *gelden voor elk van de percelen zoals vermeld in Afbeelding 1 hierboven. Een 'universele aanpak' voor het sluiten van contracten voor alle percelen zal leiden tot problemen met betrekking tot de technische haalbaarheid en compatibiliteit.*

2.0 Overzicht RFP voor cloud services

In dit gedeelte worden het model en -scope beschreven, waaronder: strategische doelstellingen, deelnemers, definities, tijdlijn, en administratieve minimumvereisten. Hou er nogmaals rekening mee dat de focus van dit handboek ligt op **PERCEEL 1 - CLOUD TECHNOLOGIEËN**.

2.1 Opzet RFP voor cloud services

We raden overheidsinstanties ten zeerste aan om duidelijk te zijn over hun doelstellingen en eisen op high-level bij de invoering van een RFP voor cloud services.

2.1.1 Inleiding en strategische doelstellingen

Om duidelijkheid te bereiken als het gaat om strategische doelstellingen, is het een goede praktijk om de volgende zaken te formuleren in de inleiding van een RFP voor cloud services: **(1)** de doelstellingen en voordelen die de organisatie wil bereiken door gebruik te maken van de cloud; **(2)** de structuur van de raamovereenkomst – wie koopt, wie uitvoert, wie budgetteert, enz.; **(3)** een duidelijk inzicht van het model van gedeelde verantwoordelijkheid tussen de publieke sector en cloud leveranciers, dat de kern vormt van succesvolle cloud inkoop en -gebruik, en **(4)** het type relatie dat tot stand komt tussen cloudaanbieders (CISP's), distributeurs van marketplacediensten, consultancy partners, overheidsinkoop/contracterende instanties en eindgebruikers bij de overheid. Het formuleren van deze vier punten helpt organisaties bij het ontwikkelen van een RFP die het beste aansluit bij hun behoeften, en zorgt er bovendien voor dat zowel klanten als leveranciers duidelijk zijn over de RFP producten.

Een cloud RFP is doelbewust anders dan traditionele IT RFP's. Cloud technologie is niet zomaar een soort vervanging voor traditionele computing methoden - het introduceert een compleet nieuwe manier om technologie af te nemen. Goed ontworpen RFP's voor cloud services kunnen organisaties in de publieke sector helpen snel te migreren om te profiteren van de cloud.

Van alle aspecten van het kopen van cloud die we noemen als een goede praktijk, is een duidelijk begrip van het model van gedeelde verantwoordelijkheid misschien wel het beste uitgangspunt. Het gedeelde verantwoordelijkheidsmodel[1] wordt vooral gebruikt in verband met beveiliging en compliance in de cloud, maar deze afbakening van verantwoordelijkheid is van toepassing op alle aspecten van cloud technologieën. Een cloud-eigen beleid kan u helpen bij het informeren over wat in een cloud omgeving bij de taak van een CSP hoort en wat de verantwoordelijkheid van de klant blijft. Zo biedt een CISP mogelijkheden om applicaties die in de cloud uitgevoerd worden te bewaken, ***maar*** het is de verantwoordelijkheid van de klant om daadwerkelijk gebruik te maken van dergelijke door CISP geboden mogelijkheden - aangezien een CISP die op grote schaal opereert, niet is ingericht om dit te doen voor miljoenen klanten.

Verder moeten cloud klanten begrijpen hoe een CISP partnernetwerk klanten helpt de cloud te gebruiken en te beheren. Zo kan een cloud managed service provider (MSP) een klant helpen bij

[1] Zie paragraaf 5 van de CISPE gedragscode voor dienstaanbieders voor cloudinfrastructuur: https://cispe.cloud/website_cispe/wp-content/uploads/2017/06/Code-of-Conduct-27-January-2017-corrected-march-20.pdf

het configureren en gebruiken van door CISP aangeboden beveiligingsopties, om te voldoen aan hun eigen unieke compliance- en auditvereisten.

Simpel gezegd zijn de verantwoordelijkheden in het cloudmodel als volgt:

Een CISP biedt cloud technologie

Een klant maakt gebruik van cloud technologie

Consultancybedrijven (indien van toepassing) helpen een klant bij de toegang tot en het gebruik van cloud technologie

'Consultancybedrijven' zijn bedrijven die consultancy, zakelijke dienstverlening of managed services leveren op het gebied van het ontwerpen, vormgeven, bouwen, migreren en beheren van hun workloads en applicaties in de cloud. Tot deze bedrijven behoren systeemintegratoren, strategische consultants, aanbieders van managed services en 'value added resellers'.

Het 'shoppen' voor cloud services is vergelijkbaar met het shoppen bij een bouwmarkt. Een uitgebreide keuze aan materialen en gereedschappen om te bouwen wat u nodig hebt, is beschikbaar in een bouwmarkt. Het is uw keuze of u een kast, een zwembad, of een heel huis bouwt. Wanneer u de materialen en gereedschappen koopt, kan het personeel van de bouwmarkt u adviseren en expertise bieden, maar ze komen niet thuis om iets voor u op te bouwen. Daarom hebt u een paar opties:

1. De materialen en het gereedschap zelf kopen en zelf iets bouwen.
2. De materialen en het gereedschap zelf kopen en iemand anders iets voor u laten bouwen en/of laten uitvoeren.
3. Iemand iets voor u laten bouwen/uitvoeren en hen de materialen en het gereedschap laten leveren als onderdeel van hun totale aanbod.

Als een organisatie de vaardigheden in huis heeft om zelf haar cloudomgeving en -oplossingen te bouwen en te beheren, dan hoeft ze alleen maar toegang te hebben tot de gestandaardiseerde cloud technologieën en -tools van de CISP (rechtstreeks met een CISP, of via een CISP-reseller – zie **PERCEEL 1**). De benodigde SaaS- en PaaS-software zou beschikbaar moeten zijn op een cloud marketplace **(PERCEEL 2)**. Als er extra hulp nodig is op het gebied van consulting, migratie, implementatie en/of beheer, is dit waar het partnernetwerk van een CISP ingezet kan worden **(PERCEEL 3)**.

RFP-voorbeeldtekst: Inleiding en strategische doelstellingen

Cloud computing biedt organisaties in de publieke sector snelle toegang tot een breed scala aan flexibele en goedkope pay-as-you-use IT-resources. Organisaties kunnen het juiste type en de juiste omvang aan resources leveren die ze nodig hebben om hun nieuwste slimme ideeën aan te sturen of hun IT-afdelingen te bedienen, waardoor grote investeringen in hardware en/of lange termijn softwarelicentiecontracten niet meer nodig zijn.

De <ORGANISATIE> heeft toegang tot dit soort commercieel beschikbare cloud technologieën nodig om te kunnen voldoen aan de bedrijfsbehoeften van een breed spectrum van aangesloten organisaties.

*Het belangrijkste doel van deze RFP is om een niet-exclusieve parallelle **<RAAMOVEREENKOMST>** te gunnen met maximaal **<x>** aanbieders die verschillende cloud technologieën en cloud gerelateerde diensten vertegenwoordigen.*

1. ***PERCEEL 1.** Cloud Service Providers (CISP's) of CISP-resellers voor de inkoop van cloud technologieën*
2. ***PERCEEL 2.** Leveranciers van marketplacediensten.*
3. ***PERCEEL 3.** Leveranciers van consultancydiensten om extra expertise te bieden om te migreren naar en gebruik te maken van dit CISP-aanbod*

*Met betrekking tot **PERCEEL 1** moeten biedende organisaties (CISP's of CISP-reseller) aantonen hoe hun aanbod aan deze doelstellingen voldoet:*

- ***Flexibiliteit** – Het beschikbaar maken van IT resources voor eindgebruikers binnen minuten in plaats van de traditionele weken en maanden.*
- ***Innovatie** – Toegang hebben tot de nieuwste en meest innovatieve technologie op de markt.*
- ***Kosten** – Handelskapitaalkosten voor variabele kosten (bijv. CapEx naar OpEx). Alleen betalen voor hoeveel er wordt verbruikt.*
- ***Budgettering** – Bekijken van factuur- en gebruiksinformatie op zowel gedetailleerd als samenvattend niveau, visualiseren van patronen in de uitgaven in de loop van de tijd, naast het voorspellen van toekomstige uitgaven.*
- ***Elasticiteit** – Lagere variabele kosten door de grotere schaalvoordelen die de cloud biedt.*
- ***Capaciteit** – Een einde aan het gissen als het gaat om de capaciteitsbehoeften van de infrastructuur.*
- ***Niet meer vertrouwen op datacenters** – Focus op burgerzaken, in plaats van op het zware werk van het plaatsen, stapelen en aansturen van servers.*
- ***Beveiliging** – Een geformaliseerd accountontwerp met meer zichtbaarheid en controleerbaarheid van de resources en geen kosten voor de bescherming van faciliteiten en fysieke hardware.*
- ***Gedeelde verantwoordelijkheid** – Lagere operationele lasten, want de CISP exploiteert, beheert en controleert de onderdelen van het host-besturingssysteem en de virtualisatielaag tot aan de fysieke beveiliging van de faciliteiten waarin de dienst draait.*
- ***Automatisering** – Ingebouwde automatisering in de cloud architectuur om de mogelijkheid te verbeteren om veilig te schalen sneller en kosteneffectiever te maken.*
- ***Cloud governance** – (1) beginnen met een volledige inventaris van alle IT assets; (2) al deze assets centraal beheren; en (3) waarschuwingen aanmaken met betrekking tot gebruik/facturatie/beveiliging/enz. – alles met mogelijkheden voor het volgen van assets, voorraadbeheer, wijzigingsbeheer, logboekbeheer en -analyse, en algemene zichtbaarheid en cloud governance.*
- ***Controle** – Volledig inzicht in hoe IT services worden gebruikt en waar ze kunnen worden afgestemd voor beveiliging, betrouwbaarheid, prestaties en kosten.*
- ***Omkeerbaarheid** – Portabiliteitstools en -services om te helpen bij de migratie naar en van de CISP infrastructuur, waardoor de leveranciersafhankelijkheid tot een minimum wordt beperkt en de gedragscode(s) in de branche gerespecteerd wordt.*

- *Gegevensbescherming – Mogelijkheid om de naleving van de algemene verordening inzake gegevensbescherming (AVG) aan te tonen door middel van een specifieke gedragscode voor de sector voor cloud infrastructuurservices: de CISPE gedragscode voor gegevensbescherming.*
- *Transparantie – Klanten moeten het recht hebben om de locatie te kennen van infrastructuur die wordt gebruikt om hun gegevens te verwerken en op te slaan (stadsgebied).*
- *Klimaatneutraliteit – Klanten moeten overeenkomsten aangaan met CISP's die bewezen specifieke stappen ondernemen om de klimaatneutrale doelstellingen tegen 2030 te bereiken, en die het Climate Neutral Data Centre Pact hebben ondertekend. Dit zal klanten helpen om hun eigen klimaatneutrale doelen te bereiken.*

2.1.2 Tijdlijn RFP beantwoording

Het is een goede gewoonte om deelnemende partijen een tijdlijn te verstrekken van verwachte offerteactiviteiten bij het tot stand komen van een cloud raamovereenkomst, en de bijbehorende RFP voor cloud services. Hoe meer betrokkenheid met de branche hoe beter, omdat het zal helpen om ervoor te zorgen dat alle partijen een duidelijk begrip hebben van de RFP vereisten, en zelfs van hoe alle leveranciersdiensten in het model passen.

Hou er rekening mee dat de RFP tijdlijn onderworpen is aan de lokale wetgeving en wettelijke verplichtingen, en dat de onderstaande lijst bedoeld is als een gids voor best practices, in tegenstelling tot een voorgeschreven lijst van activiteiten en termijnen.

RFP voorbeeldtekst: tijdlijn beantwoording

Zie de onderstaande tijdlijn voor de RFP voor cloud services:

RFP voor cloud services tijdlijn
• *Request for Information (RFI) publicatie:* • *RFI beantwoording:* • *Concept Request for Proposal (RFP) publicatie:* • *Uiterste datum indiening concept RFP:* • *Raadpleging branche: <tijdlijnen>* • *Pre-kwalificatie RFP publicatie:* • *Pre-kwalificatie RFP beantwoording:* • *RFP publicatie:* • *Ronde 1 Vragen:* • *Ronde 1 Antwoorden:* • *Ronde 2 Vragen:* • *Ronde 2 Antwoorden:* • *Uiterste datum RFP beantwoording:* • *Verduidelijkingstermijn offerte:* • *Onderhandelingsperiode:* • *Datum gunningsintentie:* • *Contractgunning:* • *Duur van het contract (met verlengingsopties):*

Hou er rekening mee dat de RFP tijdlijn onderworpen is aan de lokale wetgeving en wettelijke verplichtingen, en dat de onderstaande lijst bedoeld is als een gids voor best practices, in tegenstelling tot een voorgeschreven lijst van activiteiten en termijnen.

2.1.3 Definities

Een RFP voor cloud services moet een gedetailleerde lijst met definities bevatten. Deze lijst bevat leveranciersrollen (bijv. cCloud service aanbieder, cloud reseller, leverancierspartner), algemene technologieconcepten (computing, opslag, IaaS/PaaS, SaaS) en andere belangrijke onderdelen van de overeenkomst. Hieronder volgt een voorbeeld van een definitielijst:

RFP voorbeeldtekst: Definities

De onderstaande definities zijn de definities van cloud computing van het National Institute of Standards and Technology (NIST).[2]

- ***Infrastructure as a Service (IaaS).*** *De mogelijkheid die aan de consument wordt geboden is de levering van verwerkings-, opslag-, netwerk- en andere fundamentele computing resources waar de consument willekeurige software, zowel besturingssystemen als applicaties, kan implementeren en uitvoeren. De consument beheert of controleert de onderliggende cloud infrastructuur niet, maar heeft controle over besturingssystemen, opslag en ingezette applicaties; en mogelijk beperkte controle over geselecteerde netwerkcomponenten (bijv. host-firewalls).*

- ***Platform as a Service (PaaS).*** *De mogelijkheid die aan de consument wordt geboden, is het inzetten op de door de consument gecreëerde of aangeschafte applicaties in de cloud infrastructuur die zijn gemaakt met behulp van programmeertalen, bibliotheken, diensten en tools die door de aanbieder worden ondersteund. De consument beheert of controleert de onderliggende cloud infrastructuur niet, met inbegrip van netwerk, servers, besturingssystemen of opslag, maar heeft controle over de ingezette applicaties en mogelijk configuratie instellingen voor de applicatie-hosting omgeving.*

- ***Software as a Service (SaaS).*** *De mogelijkheid die aan de consument wordt geboden, is het gebruik van de applicaties van de aanbieder die op een cloud infrastructuur worden uitgevoerd. De applicaties zijn toegankelijk vanaf verschillende client apparaten via een thin client interface, zoals een webbrowser (bijv. webgebaseerde e-mail), of een programma interface. De consument beheert of controleert de onderliggende cloud infrastructuur niet, inclusief netwerk, servers, besturingssystemen, opslag, of zelfs individuele applicatiemogelijkheden, met de mogelijke uitzondering van beperkte gebruikersspecifieke applicatieconfiguratie instellingen.*

- ***Openbare cloud.*** *De cloud infrastructuur wordt beschikbaar gesteld voor open gebruik door particulieren. Het kan eigendom zijn van, beheerd en geëxploiteerd worden door een bedrijf, een academische of een overheidsorganisatie, of een combinatie daarvan. Het bestaat op de locatie van de cloud aanbieder.*

- ***Community cloud.*** *De cloudinfrastructuur is bestemd voor exclusief gebruik door een specifieke gemeenschap van consumenten van organisaties die gedeelde aandachtspunten hebben (bijvoorbeeld missie, beveiligingsvereisten, beleid en compliance overwegingen). Het kan eigendom zijn van, beheerd en geëxploiteerd worden door een of meer organisaties binnen deze gemeenschap, een externe partij of een combinatie daarvan, en ze kan bestaan op of buiten de bedrijfslocatie.*

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

- ***Hybride cloud.*** *De cloud infrastructuur is een samenstelling van twee of meer verschillende cloud infrastructuren (privé, gemeenschappelijk of openbaar) die uniek blijven, maar met elkaar verbonden zijn door gestandaardiseerde of gepatenteerde technologie die data- en applicatieportabiliteit mogelijk maakt (bijv. cloud bursting voor load balancing tussen clouds).*

- ***Privé cloud.*** *De cloud infrastructuur is voorzien voor exclusief gebruik door één enkele organisatie met meerdere consumenten (bijv. business units). Het kan eigendom zijn van, beheerd en geëxploiteerd worden door de organisatie, een externe partij of een combinatie daarvan, en kan bestaan op of buiten de locatie.*

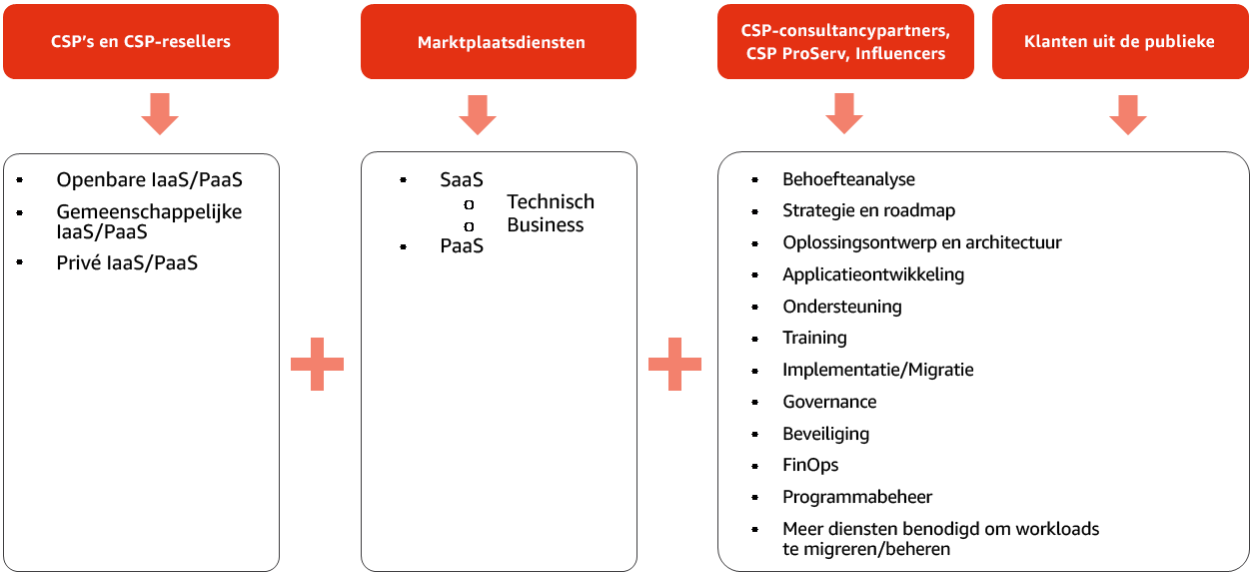
2.1.4 Gedetailleerde beschrijving van het inkoopmodel en concurrentie binnen de raamovereenkomst

Zoals hierboven opgemerkt, moeten publieke organisaties het model vaststellen hoe een raamovereenkomst zal functioneren als een inkoopmechanisme voor cloud technologieën, en de daarmee samenhangende implementatie- en beheersdiensten. Dit moet duidelijk worden gemaakt in de RFP voor cloud services, zodat leveranciers van cloudtechnologie, gerelateerde consultancybedrijven, marktdistributeurs en inkooporganisaties hun respectieve functies begrijpen.

Als het gaat om de scope van de raamovereenkomst, en na afroepen of mini-competities, moeten organisaties overwegen:

- Wie verantwoordelijk is voor integratie en managed services waarbij gebruik wordt gemaakt van de cloud technologieën die onder het contract vallen.
- Is er een vereiste voor een CISP-reseller/partner om andere diensten met toegevoegde waarde te leveren dan het onderhouden van een contractuele relatie met de CISP, het leveren van geconsolideerde factureringsdiensten, en tijdige en directe toegang tot gebruiks- en factureringsgegevens in verband met het gebruik van de diensten van de cloud aanbieder?
- Is er een vereiste voor een full-service value-added reseller, systeemintegrator, of leverancier van managed services, of enige vorm van IT-arbeidsdiensten?

Het is belangrijk op te merken dat een CISP geen systeemintegrator (SI) of managed service provider (MSP) is. Veel klanten uit de publieke sector zullen een CISP nodig hebben voor hun IaaS/PaaS, en zullen consultancy en planning, migratie en beheerswerkzaamheden uitbesteden aan een SI of MSP. Een afbeelding van de afbakening van de rollen en verantwoordelijkheden in een cloud servicemodel vindt u hieronder in Afbeelding 2.



Afbeelding 2 - Een RFP voor cloud services moet eindgebruikers een menu bieden van alle cloud services die ze nodig hebben. Klanten uit de publieke sector zullen een CISP voor cloud technologieën nodig hebben, een marketplace voor PaaS en SaaS-producten indien nodig, dan kan de klant bepalen hoe groot de rol is die hij wil spelen in het leveren van cloud services en hoeveel hij van plan is uit te besteden aan een consultancybedrijf/systeemintegrator/managed services provider/enz.

De onderstaande voorbeeldtekst wordt gevormd door de rollen en verantwoordelijkheden zoals weergegeven in Afbeelding 2 hierboven. Een cloud raamovereenkomst, en de bijbehorende RFP voor cloud services, moet ervoor zorgen dat inkopers de mogelijkheid hebben om het aanbod van elke leverancier adequaat te beoordelen, zodat ze kunnen kiezen tussen de diensten die nodig zijn voor de workload/project. Dit kan het beste worden gedaan door de diensten op te splitsen in percelen, zoals reeds is besproken, en door duidelijk te zijn over de wijze waarop afroep en mini-competities in het kader van de raamovereenkomst worden uitgevoerd.

RFP voorbeeldtekst: Inkoopmodel

*Dit contract zal dienen als een **framework** inkoopinstrument. Deze cloud raamovereenkomst zal meerdere **percelen** omvatten, zoals gedefinieerd door **<ORGANISATIE>**, voor cloud technologieën en gerelateerde marketplacediensten/producten, consultancydiensten, zakelijke dienstverlening/systeemintegratie/migratiediensten, training en ondersteuning zoals gedefinieerd door **<ORGANISATIE>**, en worden gebruikt door meerdere in aanmerking komende kopers die zijn aangesloten bij **<ORGANISATIE>**. Dit zal het inkoopproces vereenvoudigen en tegelijkertijd schaalvoordelen optimaliseren.*

Eenmaal tot stand gekomen stelt deze raamovereenkomst een organisatie in staat om de specifieke cloud technologieën en cloud gerelateerde diensten aan te schaffen die zij wenst, wanneer zij deze nodig hebben, in tegenstelling tot de aankoop via afzonderlijke aanbestedingen. Een dergelijke aanpak vermindert de administratieve vereisten en vermindert de complexiteit en de cyclustijd van de aanbestedingen aanzienlijk.

*De looptijd van de raamovereenkomst zal maximaal **<X>** jaar bedragen, inclusief eventuele verlengingen. De maximale duur van een raamovereenkomst voor diensten op afroep is normaal gesproken **<x>** maanden; dit kan worden verlengd met **<x>** maanden en vervolgens nog eens **<x>** maanden, met de juiste interne goedkeuringen als dat nodig is voor contractverlenging. Dit wordt gespecificeerd in elke specifieke **afroep**.*

*Dit FRAMEWORK is onderverdeeld in **3 (drie) percelen.***

1. *PERCEEL 1: CLOUDTECHNOLOGIEËN - volledige scope van cloudaanbieder technologieën (rechtstreeks van CISP, van reseller of van reseller met services/ondersteuning met toegevoegde waarde):*
    i. ***IaaS- en PaaS-diensten** - een menu van cloud technologieën, bijv. computing, opslag, netwerken, database, analyse, applicatiediensten, implementatie, beheer, ontwikkelaar, Internet of Things (IoT), enz. Omvat gebundelde cloud technologieoplossingen zoals DR/COOP, Archive, Big Data & Analytics, DevOps, enz.*
2. *PERCEEL 2: MARKETPLACE - volledige omvang van PaaS- en SaaS-diensten/producten zoals boekhouding, CRM, ontwerp, HR, GIS en Mapping, HPC, BI, content management, logboekanalyse, enz.*
3. *PERCEEL 3: CLOUD CONSULTANCY - volledige scope van adviesdiensten (managed services, zakelijke dienstverlening, advies-/consultancy diensten, diensten met toegevoegde waarde, FinOps, technische ondersteuning) met betrekking tot cloud migratie en -gebruik. Deze diensten omvatten: planning, ontwerp, migratie, beheer, ondersteuning, QA, beveiliging, training, enz.*

Leveranciers kunnen op meerdere percelen bieden.

Leveranciers zullen hun aanbod en de bijbehorende prijzen in het door hen gekozen formaat indienen.

HET CONCURREREN BINNEN HET FRAMEWORK EN HET GUNNEN VAN OPDRACHTEN

AFROEPEN

Openbare instanties die partij zijn in de raamovereenkomst kunnen de diensten die zij nodig hebben, bestellen of 'afroepen' wanneer dat nodig is. Door een afroepcontract onder een raamovereenkomst te plaatsen, kunnen kopers hun eisen verfijnen met aanvullende functionele specificaties voor een afroep, met behoud van de voordelen die de raamovereenkomst biedt.

Opdrachten die via de raamovereenkomst worden gegund, zullen een duidelijk controletraject kunnen laten zien met betrekking tot de eisen die worden gesteld aan de selectie van de leverancier binnen elk perceel. Eindkopers zullen de communicatie met de leveranciers bijhouden, met inbegrip van alle vroege marktbetrokkenheid, verduidelijkingsvragen, e-mails en face-to-face gesprekken die zij hebben gevoerd.

1. HET OPSTELLEN VAN AFROEPEISEN EN HET VRAGEN VAN INTERNE GOEDKEURING OM IN TE KOPEN

Alle eindkopers die in aanmerking komen voor het gebruik van de raamovereenkomst zullen gezamenlijke teams van interne eindgebruikers, inkoopspecialisten en technische deskundigen samenstellen om een lijst van 'must-haves' en 'wants' op te stellen. Deze eisen zullen helpen beslissen welke percelen van toepassing zijn, en welke leverancier het best gekwalificeerd is om aan de eisen te voldoen. Bij het opstellen van de eisen zullen de kopers rekening houden met:

- *middelen die beschikbaar zijn om gebruik te maken van de dienst*
- *technische en aanbestedingsvoorschriften van het project*
- *criteria waarop de keuze wordt gebaseerd*

2. DIENSTEN ZOEKEN

Kopers in het kader van de raamovereenkomst zullen een online frameworkcatalogus (een portaal waarop de leveranciers die een plek gegund is onder de raamovereenkomst en hun diensten zullen worden vermeld) gebruiken om producten/diensten te vinden die aan hun geïdentificeerde behoeften voldoen. Zij kiezen de juiste percelen en zoeken dan naar diensten.

3. DIENSTEN BEOORDELEN EN EVALUEREN

Kopers onder de raamovereenkomst zullen de servicebeschrijvingen herzien om de diensten te vinden die het best voldoen aan de behoeften op basis van zowel de eisen als het budget. Elke dienstbeschrijving bevat een:

- *Definitiedocument of links naar definities*
- *Voorwaardendocument*
- *Prijsdocument (links naar openbare prijzen zijn aanvaardbaar in de veronderstelling dat een volledige prijslijst/prijsdocument op verzoek beschikbaar is)*

De getoonde prijs is die van de meest voorkomende configuratie van de dienst. De prijsstelling is echter normaal gesproken gebaseerd op het volume, dus kopers moeten altijd kijken naar het prijsdocument van de leverancier of de openbare prijsstelling, en de prijscalculatie instrumenten om de werkelijke prijs van wat wordt gekocht uit te rekenen, en de totale waarde die aan de koper wordt geleverd (bijvoorbeeld diensten voor optimalisatie en de daaruit voortvloeiende kostenverlaging).

Kopers onder de raamovereenkomst kunnen met leveranciers spreken om hen te vragen hun dienstbeschrijving, voorwaarden, prijsstelling of definitiedocumenten/model toe te lichten. Er wordt een register bijgehouden van eventuele gesprekken met leveranciers.

4. EEN DIENST KIEZEN EN EEN CONTRACT GUNNEN

Enkele leverancier

Als slechts één leverancier aan de eisen voldoet, kan er een contract aan deze worden gegund.

Meerdere leveranciers

Als er een aantal diensten op een shortlist staan, kiest de koper de dienst met de economische meest voordelige inschrijving (EMVI). Zie de criteria in de volgende tabel voor de beoordeling op basis van EMVI. Kopers kunnen zelf bepalen welke gedetailleerde kenmerken ze gebruiken en hoe ze die wegen.

Hou er rekening mee dat de koper wellicht:

- *moet kijken naar combinaties van verschillende leveranciers*
- *specifieke informatie moet krijgen over volume- of organisatiekortingen, en de kostenoptimalisatiediensten van de leverancier*

De beoordeling van leveranciers moet altijd eerlijk en transparant zijn. De keuze wordt gemaakt op basis van geschiktheid, en leveranciers/diensten worden niet uitgesloten zonder terug te verwijzen naar de eisen van het project.

Tabel 2 – Op EMVI gebaseerde beoordeling

Toekenningscriteria
Kosten gehele levensduur: kosteneffectiviteit, prijs en exploitatiekosten
Technische verdienste en functionele geschiktheid: dekking, netwerkcapaciteit en prestaties zoals gespecificeerd in de relevante service levels
After-sales service: helpdesk, documentatie, accountmanagementfunctie en waarborging van de levering van een reeks diensten
Niet-functionele kenmerken

MINI-COMPETITIES

Indien dit nodig wordt geacht, kan een mini-competitie worden gehouden om de beste leverancier voor een bepaalde workload of een bepaald project te identificeren. Bij een mini-competitie gaat een klant in het kader van de raamovereenkomst de concurrentie verder aan, door alle leveranciers binnen een perceel uit te nodigen om te reageren op een reeks van eisen. De klant zal alle capabele leveranciers binnen het perceel uitnodigen om een bod uit te brengen. Zie de aanvullende vergelijkingsinformatie in de onderstaande paragrafen over technische aspecten, beveiliging en prijzen/waarde.

CONTRACT

*De koper en de leverancier zullen beiden een kopie van het contract ondertekenen voordat de dienst kan worden gebruikt. De maximale duur van een raamovereenkomst is normaal gesproken **<x>** maanden; dit kan worden verlengd met **<x>** maanden en vervolgens nog eens **<x>** maanden, met de juiste interne goedkeuringen als dat nodig is voor contractverlenging.*

Een kopie van het contract moet door alle betrokken partijen (de koper en de leverancier) worden ondertekend voordat de dienst kan worden gebruikt.

2.1.5 Minimumeisen voor de bieder - Administratief

Eenvoudige en duidelijke taal om kwalificatiecriteria voor raamovereenkomsten vast te stellen, zal ervoor zorgen dat er geen inzendingen zijn van traditionele datacenters of hardwareleveranciers die een traditionele oplossing als 'cloud' verpakken. RFP deelnemers moeten aantonen hoe zij voldoen aan de onderstaande minimale administratieve vereisten voor bieders.

Hou er opnieuw rekening mee dat dit document zich richt op PERCEEL 1 - CLOUD TECHNOLOGIEËN. We hebben echter aanvullende informatie toegevoegd over PERCEEL 2 - MARKETPLACE en PERCEEL 3 - CLOUD CONSULTANCY wanneer het helpt om de algemene context te bieden in voorwaarden van vereisten en RFP scope. Het is bijvoorbeeld belangrijk om minimale kwalificatiecriteria op te nemen voor een CISP-reseller/MSP/SI/consultancy bedrijf/enz., en het helpt om ervoor te zorgen dat zij (1) rechtstreeks verbonden zijn met de CISP als reseller of kanaalpartner, (2) gecertificeerd zijn door een CISP om directe toegang tot het CISP-aanbod door te verkopen aan externe partijen, en (3) gecertificeerd zijn door die CISP's voor wat betreft hun deskundigheid

RFP-voorbeeldtekst: Minimumvereisten bieder – Administratief

Deze raamovereenkomst zal contracten gunnen aan meerdere leveranciers in de volgende categorieën. Leveranciers moeten een commerciële CISP, een derde reseller van een CISP, een distributeur van marketplacediensten en/of een aanbieder van diensten voor het gebruik van een CISP zijn (bijvoorbeeld; consultancy, migratiediensten, managed services, FinOps, enz.). Geef de rollen aan die u biedt:

PERCEEL 1

____ - Directe aanbieder (CISP) van openbare cloud service (IaaS EN PaaS)

____ - Directe aanbieder (CISP) van gemeenschappelijke cloud service (IaaS EN PaaS)

____ - Directe aanbieder van (CISP) privé cloud service (IaaS EN PaaS)

____ - CISP derde reseller (mogelijkheid om directe toegang te bieden tot het online cloud aanbod van een CISP).

- *Geef het aanbod van CISP aan waarvoor u in staat bent om directe toegang tot hun dienst door te verkopen: _____*
- *Verstrek een brief van de CISP dat u een geautoriseerde reseller bent van hun aanbod: _____*

PERCEEL 2

____ - Rechtstreekse aanbieder van marketplacediensten uitgevoerd op een CISP (PaaS en/of SaaS)

____ - Distributeur van marketplacediensten uitgevoerd op een CISP (PaaS en/of SaaS)

PERCEEL 3

____ - CISP die zakelijke dienstverlening biedt

____ - Aanbieder van technische ondersteuning van CISP

____ - CISP partner die diensten verleent voor het gebruik of de werking van een CISP

____ - CISP partner die diensten verleent voor het gebruik of de werking van een CISP

Geef het type aanbod aan:

- *Beheerde dienst van workload op een CISP (J/N): _____*
  - *Benoem bijzonderheden indien van toepassing: _____*
- *Professionele diensten: (J/N): _____*
- *Consultancy – Training (J/N): _____*
- *Consultancy – Strategie (J/N): _____*
- *Consultancy – Migratie (J/N): _____*
- *Consultancy – Cloud governance (J/N): _____*
- *Consultancy – FinOps (J/N): _____*
- *Consultancy – Andere (gelieve te benoemen): _____*

Noem de CISP/CISP's waarvoor u diensten verleent: _____
Verstrek een brief van de CISP ter bevestiging van uw partneraanduiding onder het CISP-model: _____

PERCEEL 1 MINIMALE ADMINISTRATIEVE VEREISTEN

Cloud Service Providers (CISP's)
Om in aanmerking te komen als CISP moet deze voldoen aan de onderstaande vereisten.

Voorgestelde kwalificatiecriteria voor CISP	*Reden*
Organisatorische gegevens zoals naam, juridische structuur, registratie/DUNS-nummer, BTW, enz.	
Bedrijfsgrootte, economische en financiële draagkracht[3]	*De klant kan bepalen dat de CISP in staat is om het contract uit te voeren.*
Redenen voor uitsluiting, bijv. criminele/frauduleuze activiteiten, enz.	
Casestudy's/klantreferenties (geef het vereiste aantal/type op)	*De klant heeft de mogelijkheid om CISP-ervaring te meten om de vereiste diensten te kunnen leveren.*
Maatschappelijk verantwoord ondernemen	*Dit moeten openbaar toegankelijke versies zijn die de CISP aanbiedt.*
Openbaar beschikbare duurzaamheidsverbintenissen en -praktijken.	*De klant kan zien dat een CISP zich inzet voor een zo milieuvriendelijk mogelijke bedrijfsvoering*
De CISP moet de afgelopen 5 jaar een bewezen staat van dienst hebben bij het innoveren en vrijgeven van nieuwe nuttige diensten en functies, vooral op het gebied van PAAS, machine learning en analyse, big data, managed services en optimalisatiefuncties voor cloudgebruik. Openbaar toegankelijke changelogs of update feeds kunnen worden gebruikt om het punt te bewijzen.	*Toont dat de CISP werkt om nieuwe producten snel in de handen van klanten te krijgen, en vervolgens snel te itereren en te verbeteren. Dit helpt klanten continu de stand der techniek te volgen op het gebied van IT infrastructuur zonder dat ze hoeven te investeren in herkapitalisatie*

Relatie reseller/partner met CISP

***<ORGANISATIE>** vereist dat de hoofdaannemer rechtstreeks verbonden is met de CISP als reseller of channel partner, gecertificeerd door een CISP om rechtstreekse toegang tot het CISP-aanbod door te verkopen aan derde partijen, met certificeringen van deze CISP's die hun capaciteiten en expertise aanduiden. Dit neemt het vereiste voor **<ORGANISATIE>** weg om de voorwaarden en diensten te herzien die verbonden zijn aan een extra laag van onderaanneming tussen de **raamovereenkomst** van de hoofdaannemer en CISP. Deze eis vermindert ook de complexiteit die extra reseller-lagen genereren wanneer (1) **<ORGANISATIE>** haar due diligence uitvoert om te zorgen voor een duidelijke toewijzing van verantwoordelijkheden met betrekking tot de te leveren diensten, en (2) **<ORGANISATIE>** dagelijkse activiteiten uitvoert met betrekking tot het gebruik van de cloud services.*

2.2 Technisch

Een RFP voor cloud services zou de lat voor CISP's hoger moeten leggen door te eisen dat ze de gestandaardiseerde cloud technologieën leveren die een klant nodig heeft om zijn oplossing op maat te bouwen. Zoals eerder vermeld, is dit verschil tussen wat gestandaardiseerd is en wat maatwerk is erg belangrijk bij het benaderen van een RFP voor cloud services. CISP's bieden gestandaardiseerde diensten aan miljoenen klanten, dus aanpassingen in een RFP voor cloud services richten zich op oplossingen en resultaten van hogere kwaliteit, in tegenstelling tot de onderliggende methoden, infrastructuur of hardware die worden gebruikt om de cloud services aan te bieden die worden gebruikt om de resultaten van de oplossing te bereiken.

[3] Hou er rekening mee dat een RFP voor cloud services kijkt naar bedrijfsinformatie op hoog niveau, in tegenstelling tot het aantal werknemers in de bedrijfs- en interne personeelsstructuur. Bij cloud technologie is er geen correlatie tussen de garantie van de serviceprestaties en het aantal medewerkers. In plaats daarvan kijken cloud RFP's naar de totale bedrijfsgrootte om te voldoen aan vereisten (voldoende schaal) en bewezen ervaring/prestaties.

2.2.1 Minimumeisen

Traditionele IT aankopen zijn vaak gebaseerd op eisen vanuit de business die zijn ontwikkeld door middel van een reeks werksessies die documenteren hoe de organisatie op dit moment haar activiteiten uitvoert. Het is zelfs in de beste omstandigheden een moeilijk proces om deze eisen perfect op elkaar af te stemmen. Als deze sessies succesvol zijn, documenteren ze het historische bedrijfsproces dat op zich al verouderd en inefficiënt kan zijn. Als deze vereisten vervolgens deel uitmaken van de RFP die door de CISP moet worden gerepliceerd, kan de enige oplossing een maatwerkoplossing zijn. Dit model is niet verenigbaar met cloud aanbestedingen.

Overheidsorganisaties moeten hun bedrijfsdoelstellingen en prestatiebehoeften begrijpen, maar mogen in een RFP niet voorschrijvend optreden door het systeemontwerp en de functionaliteit te dicteren. In plaats daarvan zou de organisatie moeten inkopen op basis van de beste geschiktheid. In plaats van offertes te evalueren op honderden of zelfs duizenden normatieve eisen die mogelijk niet leiden tot succesvolle diensten, zouden organisaties evaluatiecriteria moeten opnemen op basis van hoe goed de technologie en de bijbehorende diensten aan de organisatiedoelstellingen voldoen of deze verbeteren, of het nu gaat om het bereiken van prestatiebehoeften of de mogelijkheid om business rules te fine-tunen door middel van configuratie.

Cloud RFP's moeten de juiste vragen stellen om de beste oplossingen te verkrijgen. Aangezien in een cloud model geen fysieke assets worden aangeschaft, zijn veel traditionele eisen voor de aanschaf van datacenters niet van toepassing. ***Het hergebruiken van vragen over datacenters zal onvermijdelijk leiden tot antwoorden op datacentervragen,*** *wat ertoe leidt dat CISP's niet in staat zijn te bieden, of tot slecht ontworpen contracten die klanten uit de publieke sector ervan weerhouden om de volledige mogelijkheden en voordelen van de cloud te benutten.*

Een RFP voor cloud services richt zich op de belangrijkste eisen die worden gesteld aan een CISP en cloud services, en zorgt ervoor dat leveranciers die in aanmerking komen voor PERCEEL 1 een hoog niveau hebben. De eisen moeten ook voorkomen dat ze te voorschrijvend zijn, zodat de toegang van de publieke sector tot gekwalificeerde CISP's niet wordt beperkt.

RFP voorbeeldtekst: Mogelijkheden van de cloud aanbieder

Zie ook de bovenstaande minimale administratieve vereisten voor een CISP voor PERCEEL 1

Voorgestelde kwalificatiecriteria voor CISP	*Reden*
Infrastructuur	
De CISP infrastructuur moet ten minste 2 clusters van datacenters bieden. Elk cluster moet bestaan uit ten minste 2 datacenters die zijn verbonden met een lage latency link om zeer beschikbare actief-actief implementaties van DR-BC-scenario's mogelijk te maken. De datacenters waaruit elk cluster bestaat, moeten fysiek geïsoleerd en uitvalonafhankelijk van elkaar zijn.	*De CISP moet in staat zijn een infrastructuur te bieden die geschikt is voor het bouwen van hoogbeschikbare applicaties waar storingspunten kunnen worden vermeden.*

De CISP moet logisch en geografisch geïsoleerde regio's bieden. Klantgegevens mogen niet buiten deze regio's worden gerepliceerd door de CISP.	*De eis geldt dat de klant de volledige controle heeft over de plaats waar zijn gegevens zich bevinden.*
De CISP moet de mogelijkheid hebben om directe, speciale en privé verbindingen tussen de CISP datacenters te leveren.	*Privé connectiviteit is een fundamentele vereiste om een hybride, veilige infrastructuur te kunnen bouwen.*
CISP moet voldoende mechanismen bieden, waaronder encryptie voor gegevens in overdracht.	*De klant kan eisen dat er een mogelijkheid is dat er geen gegevens ongecodeerd kunnen worden doorgegeven.*
Minimum CISP certificaten	
De CISP moet gecertificeerd zijn volgens ISO 27001	*Audits door derden, certificering en accreditatie zorgen ervoor dat klanten diensten (en in het bijzonder het platform) kunnen benchmarken op kwaliteit, beveiliging en betrouwbaarheid. Het is van essentieel belang dat aan een minimum aan certificeringen wordt voldaan.*
De CISP moet voldoen aan de Gedragscode voor gegevensbescherming van CISPE, om functies en diensten te kunnen bieden die kunnen worden gebruikt in overeenstemming met de AVG, waardoor klanten applicaties kunnen bouwen die voldoen aan de AVG.	*De klant moet in staat zijn om applicaties te bouwen of uit te voeren in overeenstemming met de AVG.*
De CISP moet door derden ge-audite verslagen zoals SOC 1- en SOC 2-verslagen (over de door de EC gebruikte locaties en diensten) ter beschikking stellen om de transparantie met betrekking tot de CISP controles en -procedures mogelijk te maken.	*De CISP moet transparant zijn over de manier waarop de applicatie wordt gebruikt en beheerd. SOC-verslagen zijn van groot belang voor het vertrouwen en de transparantie*
De CISP moet zich houden aan het Climate Neutral Data Centre Pact.	*Het Climate Neutral Data Centre Pact vraagt de CISP in 2030 klimaatneutraliteit te bereiken, en stelt de gebruiker in staat zijn eigen duurzaamheidsdoelstellingen te ondersteunen. Externe accountants zijn verplicht voor aanbieders met meer dan 250 FTE (niet-KMO's)*
De CISP moet zich houden aan de SWIPO IaaS gedragsnormen voor overdraagbaarheid	*De SWIPO IaaS gedragsnormen voor overdraagbaarheid zorgen ervoor dat de diensten in overeenstemming zijn met art. 6 'Data Porting' van de regelgeving inzake het vrije verkeer van niet-persoonsgegevens.*
Dienstkenmerken	
De CISP infrastructuur moet toegankelijk zijn via programmatische interfaces (API's) en een beheerconsole op web-basis.	*Self-servicetoegang en programmatische interfaces zijn een vereiste standaard van CISP aanbieders om de gebruikerstoegang en de aanbieder zelf zo veel mogelijk te ontkoppelen.*
De CISP moet een basispakket van diensten aanbieden, waaronder objectopslag, beheerde relationele database, beheerde niet-relationele database, beheerde load-balancers, bewaking en geïntegreerd autoschalen.	*Het aanbod van virtuele machines alleen is niet voldoende om een aanbieder als cloud aanbieder te kwalificeren. Cloud aanbieders moeten een reeks PaaS- en IaaS diensten aanbieden om de applicaties van klanten te versnellen en te verbeteren.*
De CISP moet de klant toestaan om het gebruik en de configuratie van zijn diensten vrij te wijzigen, of om gegevens binnen en buiten de CISP (selfservice aanbod) te verplaatsen.	*Self-service toegang tot diensten en gegevens is een harde eis die de klant in staat stelt om volledig onafhankelijk te zijn.*

De CISP moet bij de facturering van de diensten prijzen op verbruiksbasis mogelijk maken.	*Met een prijs op verbruiksbasis kan de klant zijn workload kostenbesparend maken, risico's minimaliseren en de CISP gebruiken voor kortstondige applicaties en POC's.*
Beveiliging van gegevens en systemen	
De CISP moet de klant in staat stellen de volledige controle te houden over zijn gegevens, de klant de vrijheid geven te kiezen waar gegevens worden opgeslagen (stadsgebied), en garanderen dat er geen klantgegevens zullen worden verplaatst tenzij een dergelijke verhuizing door de klant zelf wordt geïnitieerd.	*De klant moet controle hebben over waar de gegevens worden opgeslagen, over hoe de toegang tot de content wordt beheerd, en gebruikerstoegang hebben tot de diensten en resources*
De CISP kenmerken moeten de klant volledige controle geven over zijn beveiligingsbeleid, met inbegrip van de vertrouwelijkheid, integriteit en beschikbaarheid van de gegevens en systemen van de klant.	*De klant moet in staat zijn om zijn beveiligingsnormen te definiëren en te implementeren in zijn hele workload. Erop vertrouwen dat de aanbieder 'het juiste doet' met de gegevens van de klant is niet voldoende.*
Kostenbeheersing	
De CISP moet over mechanismen en tools beschikken om de klant in staat te stellen de uitgaven in de loop van de tijd te controleren. De tools moeten een basissegmentatie van de kosten mogelijk maken op basis van de workload, de service en het account.	
De CISP moet tools bieden om de klant te waarschuwen wanneer een kostendrempel wordt overschreden.	
De CISP moet gedetailleerde facturen aan de klant leveren. Het moet mogelijk zijn om de factuur te structureren om de kosten uit te splitsen naar workload, omgeving en account.	

De CISP's moeten ook antwoorden geven op de vragen over de technische vereisten die hieronder worden gesteld.

OPLOSSINGEN

De CISP moet laten zien hoe het kan voorzien in kant-en-klare templates en softwareoplossingen die worden gehost op of geïntegreerd met de CISP, voor de volgende oplossingen:

- *Opslag*
- *DevOps*
- *Beveiliging/compliance*
- *Big data/Analyse*
- *Bedrijfsapplicaties*
- *Telecommunicatie en netwerken*
- *Geospatiaal*
- *IoT*
- *[Overige]*

Een overzicht geven van de manier waarop de CISP is ingezet voor de volgende workload:

- *Noodherstel*
- *Ontwikkeling en testen*
- *Archivering*
- *Backup en herstel*
- *Big data*

- *High performance computing (HPC)*
- *Internet of Things (IoT)*
- *Websites*
- *Serverless computing*
- *DevOps*
- *Content delivery*
- *[Overige]*

2.2.2 Vergelijking tussen leveranciers

Naast de minimumeisen in een RFP voor cloud services is het belangrijk om criteria te geven waarmee CISP technologieën kunnen worden vergeleken tijdens een competitieve evaluatie.

RFP's voor cloud services moeten vragen om die cloud capaciteiten die een organisatie nodig heeft om hun oplossing te bouwen. Functionaliteit die verder gaat dan de standaard die een CISP kan bieden (zoals vooraf gebouwde oplossingen via de CISP, of automatiseringsfuncties) - kan worden gebruikt voor een meer zinvolle analyse van 'waardetoevoegende opties' of 'beste waarde' in een RFP voor cloud services.

De publieke sector vereist vaak concurrentie tussen inschrijvers met behulp van evaluatiecriteria zoals de beste waarde, de economisch meest voordelige inschrijving (EMVI) of de laagste prijs. Voor dit onderdeel van een cloud services RFP, is het belangrijk om een evaluatie model te ontwerpen dat rekening houdt met de unieke kenmerken van de cloud. Het is belangrijk te begrijpen dat het eenvoudigweg vergelijken van individuele items (bijvoorbeeld; computing of opslag) geen effectieve manier is om aanbiedingen te vergelijken. In plaats daarvan raden we sterk aan om de aandacht te richten op oplossingen op een hoger niveau, zoals die hierboven in paragraaf *2.2.1* zijn genoemd. Publieke organisaties kunnen dan kijken naar cloud specifieke vereisten, zoals die vermeld in *Bijlage A - Technische eisen voor de vergelijking tussen* bieders.

RFP's moeten de essentiële cloud kenmerken vermelden die nodig zijn om de gewenste cloud oplossing te bouwen. Om dit te doen, kunnen organisaties in de publieke sector gebruik maken van het National Institute of Standards and Technology (NIST) Essential Cloud Characteristics, naast het gebruik van rapporten van externe analisten om ervoor te zorgen dat de CISP het best passende 'echte cloud'-aanbod heeft, dat op grote schaal opereert.

RFP voorbeeldtekst – Vergelijking tussen leveranciers

CISP's moeten antwoorden geven op ALLE vragen over technische vereisten in ***Bijlage A****.*

Respondenten moeten de volgende kenmerken hebben en moeten beschrijven hoe hun aanbod van cloud services voldoet aan de vijf essentiële kenmerken van cloud computing[4].

1) ***Zelfbediening op afroep:*** *De respondent moet de mogelijkheid bieden om eenzijdig computingcapaciteiten, zoals servertijd en netwerkopslag, naar behoefte automatisch te leveren zonder dat er menselijke interactie met elke serviceprovider nodig is. De respondent moet de mogelijkheid bieden om de bestelactiviteit eenzijdig (d.w.z. zonder beoordeling of goedkeuring door de leverancier) te leveren. Leg uit hoe dit werkt met uw aanbod of het aanbod dat u vertegenwoordigt.*

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

2) ***Overal aanwezige netwerktoegang:*** *De respondent moet meerdere netwerkverbindingsopties bieden, waarvan één op het internet gebaseerd moet zijn. Leg uit hoe dit werkt met uw aanbod of het aanbod dat u vertegenwoordigt.*

3) ***Resource pooling:*** *De CISP van de respondent moet gepoolde computingresources bieden die meerdere consumenten bedienen met behulp van een multi-tenant model met verschillende virtuele resources die dynamisch worden toegewezen en opnieuw toegewezen volgens de vraag van de consument. De gebruiker kan een locatie opgeven op een hoger abstractieniveau (bijv. land, regio of datacenterlocatie). De respondent ondersteunt het schalen van deze resources binnen enkele minuten of uren na een leveringsvraag. Leg uit hoe dit werkt met uw aanbod of het aanbod dat u vertegenwoordigt.*

4) ***Snelle elasticiteit:*** *De CISP van de respondent moet de dienstverlening ondersteunen en de mogelijkheden om de dienstverlening te onderbreken (op en neer schalen), waarbij de dienstverlening beschikbaar wordt gesteld binnen de minimaal voorgeschreven tijden (maximaal 'x' uur) van de leveringsvraag. De respondent moet het mogelijk maken om op dag- of uurbasis de facturen die voortvloeien uit deze aanvragen aan te passen.*

5) ***Gemeten dienst:*** *De respondent biedt zicht op het gebruik van de dienst via een online dashboard of soortgelijke elektronische resources.*

Daarnaast moet de CISP:

- *Een erkend leider zijn in het leveren van cloud services, zoals blijkt uit het Gartner Magic Quadrant voor IaaS*[5]
- *Door de branche erkende rapporten leveren van externe analisten die de bewezen capaciteiten en betrouwbaarheid van CISP's aantonen.*

Tot slot zullen de CISP's worden vergeleken aan de hand van de scenario's in bijlage B.

2.2.2.1 Service Level Agreements (SLA's)

CISP's leveren gestandaardiseerde commerciële SLA's aan miljoenen klanten en kunnen daarom geen persoonlijke SLA's aanbieden, zoals het geval is bij een datacentermodel op locatie. Echter kunnen CISP klanten (vaak bijgestaan door CISP partners) hun cloudgebruik zo ontwerpen, dat ze de commerciële SLA's van een CISP kunnen gebruiken om te voldoen aan klantspecifieke eisen en unieke SLA's en deze zelfs te overtreffen.

RFP's voor cloud services moeten ervoor zorgen dat CISP's de mogelijkheden en begeleiding bieden die nodig zijn om hun diensten en commerciële SLA's te benutten, zodat individuele eindgebruikers kunnen voldoen aan de eisen op het gebied van prestaties en beschikbaarheid.

RFP voorbeeldtekst: Service Level Agreements

Informatie verstrekken over, en linken naar de CISP benadering van de Service Level Agreements (SLA's).

<ORGANISATIE> dient zich steeds bewust te zijn van de SLA's van CISP en belangrijke workloads en applicaties zodanig implementeren dat deze blijven werken als niet aan een SLA wordt voldaan.

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

<ORGANISATIE> is verantwoordelijk voor het naleven van de juiste SLA's in verband met <ORGANISATIE> bedrijfsgebonden apparaten of door <ORGANISATIE> gerunde diensten die gebruikt worden met de CISP.

De CISP zou <ORGANISATIE> de mogelijkheden moeten bieden om doorlopende zichtbaarheid en rapportage van de operationele SLA-prestaties te hebben, en gedocumenteerde best practices om de CISP-infrastructuur te gebruiken om services te ontwerpen voor prestaties, duurzaamheid en betrouwbaarheid.

2.2.3 Contracten

De voorwaarden van CISP's zijn ontworpen om weer te geven hoe een model voor cloud services functioneert (fysieke assets worden niet gekocht, en CISP's werken op grote schaal en bieden gestandaardiseerde diensten aan); het is dus van cruciaal belang dat de voorwaarden van een CISP zo volledig mogelijk worden opgenomen en gebruikt. Zie paragraaf *2.5* hieronder voor meer informatie over de voorwaarden en contracten.

2.2.3.1 Nieuwe en veranderende diensten

CISP's leveren prestaties door middel van een dienst. In tegenstelling tot traditionele oplossingen op locatie die upgrades en servicecontracten vereisen die aflopen, bieden cloud aanbieders eenvoudigweg de gestandaardiseerde dienst aan. Om het cloud model schaalvoordelen te laten opleveren, worden upgrades en veranderingen in de onderliggende infrastructuur doorgevoerd naar iedereen, niet naar individuele gebruikers, en klanten kiezen vervolgens de diensten die ze gebruiken. De dienst is naadlozer dan de on-premise systemen op locatie uit het verleden, en cloud aanbieders voegen voortdurend nieuwe en verbeterde services toe die klanten naar wens kunnen gebruiken.

Als nieuwe of verbeterde CISP services niet kunnen worden toegevoegd na een uiterste datum voor indiening van een RFP, beperkt dit overheidsorganisaties om gebruik te maken van nieuwe diensten en verbeterde functies tot de volgende iteratie van een raamovereenkomst. Wij raden daarom ten zeerste aan de te leveren diensten ruim te beschrijven, zodat er na de indieningstermijn nieuwe CISP diensten kunnen worden toegevoegd. De EU-wetgeving inzake overheidsopdrachten kan de invoering beperking van wezenlijk verschillende nieuwe CISP diensten die aan de raamovereenkomst moeten worden toegevoegd, maar updates en nieuwe versies van diensten die niet als wezenlijke wijzigingen worden beschouwd, kunnen zonder enige aanbestedingsuitdaging worden toegevoegd.

RFP voorbeeldtekst: Nieuwe en veranderende diensten

De CISP biedt een kosteneffectieve oplossing aan die gebruik maakt van zowel beproefde als stabiele virtualisatietechnologieën en geavanceerde technologieën die voortdurend worden geupdate. De <ORGANISATIE> erkent en stemt ermee in dat de cloudtechnologieën op basis van een gedeelde service kunnen worden geleverd aan de <ORGANISATIE> en andere klanten van de CISP vanuit een gemeenschappelijke codebasis en/of gemeenschappelijke omgeving, en dat de CISP van tijd tot tijd: de functies, eigenschappen, prestaties of andere kenmerken van de cloud services wijzigen of verwijderen, en als een dergelijke wijziging, toevoeging of verwijdering wordt aangebracht, de specificaties van de cloud service overeenkomstig zullen worden aangepast.

*De omvang van deze leveringsopdracht omvat alle momenteel bestaande en, nieuwe of verbeterde CISP diensten **BINNEN DE SCOPE VAN DE RAAMOVEREENKOMST.** De door de CISP geleverde cloud services die beschikbaar zijn voor commerciële klanten worden beschikbaar gesteld aan <ORGANISATIE>.*

2.2.3.2 Leveranciersafhankelijkheid/Omkeerbaarheid

Cloud technologie vermindert de afhankelijkheid van leveranciers omdat er geen fysieke assets worden gekocht en klanten hun gegevens op elk moment van de ene naar de andere cloud aanbieder kunnen verplaatsen.

Een zekere mate van leveranciersafhankelijkheid is echter onvermijdelijk bij de inkoop van cloud services - omdat niet alle clouds gelijk zijn en de ene CISP dus diensten en mogelijkheden kan bieden die een andere aanbieder niet kan bieden – waardoor de mogelijkheid om dergelijke diensten bij een andere aanbieder te gebruiken, wordt beperkt. Een voorzichtige benadering is om te eisen dat CISP's de vereiste functies en diensten leveren om hun cloud te verlaten, met documentatie over hoe deze diensten te gebruiken als een redelijke 'exit-strategie' – gezien het feit dat het onmogelijk is voor een CISP om de unieke configuratie van het gebruik van een klant van hun gestandaardiseerde diensten te kennen, en als zodanig een op maat gemaakt exit-plan te leveren.

Zie paragraaf 2.3.1.2 voor informatie over de gedragscodes uit te branche om 'Data Porting' en 'Switching Cloud Providers' aan te pakken om te voldoen aan de vereisten van artikel 6 van de EU 'regelgeving inzake het vrije verkeer van niet-persoonsgegevens'.

RFP voorbeeldtekst: Onboarding en offboarding

*De **<ORGANISATIE>** is op zoek naar voorstellen die een redelijke exitstrategie bieden om afhankelijkheid te voorkomen. De **<ORGANISATIE>** koopt geen fysieke assets, en de CISP biedt de mogelijkheid om omhoog en omlaag te klimmen langs de IT stack. De CISP biedt portabiliteitstools en -services om te helpen bij de migratie naar en van het CISP platform, waardoor de afhankelijkheid tot een minimum wordt beperkt. Gedetailleerde documentatie over het gebruik van door CISP geboden portabiliteitstools en -diensten zal dienen als een redelijk exitplan.*

*De CISP zou geen **verplichte** minimale verplichtingen of **verplichte** lange-termijncontracten moeten hebben.*

*Gegevens die bij een serviceprovider zijn opgeslagen, kunnen op elk moment door de klant worden geëxporteerd. De CISP staat de **<ORGANISATIE>** toe om gegevens als dat nodig is in en uit de CISP opslag te verplaatsen. De CISP maakt het ook mogelijk om beelden van virtuele machines te downloaden en over te brengen naar een nieuwe cloud aanbieder. De **<ORGANISATIE>** kan zijn machine images exporteren en deze op locatie of bij een andere aanbieder gebruiken (met inachtneming van de beperkingen van de softwarelicenties).*

2.3 Beveiliging

Beveiliging en compliance zijn gedeelde verantwoordelijkheden van de CISP en cloud klanten. In dit 'shared responsibility' model hebben cloud klanten de controle over de manier waarop zij hun applicaties en gegevens op de infrastructuur ontwerpen en beveiligen, terwijl CISP's verantwoordelijk zijn voor het leveren van diensten op een zeer veilig en gecontroleerd platform, en voor het leveren van een breed scala aan extra beveiligingsfuncties. Het niveau van CISP en klantverantwoordelijkheden in dit model is afhankelijk van het cloud implementatiemodel (IaaS/PaaS/SaaS) en klanten moeten duidelijk begrijpen wat hun verantwoordelijkheden zijn in elk model.

Het begrijpen van dit 'shared responsibility' model is cruciaal voor het ontwerpen van een succesvolle RFP voor cloud services. Overheidsorganisaties moeten ervoor zorgen dat ze weten waarvoor een CISP verantwoordelijk is, waar ze zelf verantwoordelijk voor zijn, en waar consultancy/ISV's partners en hun oplossingen passen om te helpen.

2.3.1 Minimumeisen

Het sleutelwoord als het gaat om beveiliging in de cloud is **'Capability'**. Overheidsorganisaties zouden van CISP's moeten eisen dat deze de beveiligingsmogelijkheden bieden die nodig zijn om ervoor te zorgen dat klanten hun verantwoordelijkheden in het 'shared responsibility' model kunnen nakomen. Zoals blijkt uit de lijst met representatieve vereisten hieronder, wordt de CISP gevraagd om een gestandaardiseerde tools en services te bieden, zodat de klant deze kan gebruiken om zijn unieke cloud omgeving te beveiligen.

- ***Bieden van*** *netwerk firewalls en webapplicatie firewall* ***mogelijkheden*** *om privé netwerken te creëren, en de toegang tot instances en applicaties controleren.*
- ***Bieden van*** *connectiviteits****opties*** *die persoonlijke of speciale verbindingen mogelijk maken vanuit uw kantoor of lokale omgeving.*
- ***Bieden van*** *de* ***mogelijkheid*** *om een verdedigingsstrategie te implementeren en DDoS-aanvallen te dwarsbomen.*
- *Gegevensencryptie****mogelijkheden*** *beschikbaar in opslag- en databaseservices.*
- ***Bieden van*** *flexibele codebeheer****opties****, zodat u kunt kiezen of u de CISP de encryptiecodes laat beheren of de klant de volledige controle over de codes laat behouden.*
- ***Bieden van API's v****oor klanten om codering en gegevensbescherming te integreren met alle diensten die zijn ontwikkeld of geïmplementeerd in een CISP omgeving.*
- ***Bieden van*** *implementatie****tools*** *voor het beheren van het maken en stopzetten van CISP resources volgens de normen van de organisatie.*
- ***Bieden van tools*** *voor inventaris- en configuratiebeheer die CISP- resources identificeren en vervolgens wijzigingen in deze resources in de loop der tijd bijhouden en beheren.*
- ***Bieden van tools en functies*** *die klanten in staat stellen om precies te zien wat er in hun CISP omgeving gebeurt.*
- ***Diep inzicht*** *in API oproepen* ***mogelijk maken****, inclusief wie, wat, en waar oproepen zijn gedaan.*
- ***Bieden van opties*** *voor het samenvoegen van logboeken, waardoor onderzoeken en complianceverslagen worden gestroomlijnd.*
- *De mogelijkheid bieden om waarschuwingsberichten te configureren wanneer zich specifieke gebeurtenissen voordoen of wanneer drempels worden overschreden.*
- ***Bieden van mogelijkheden*** *om het toegangsbeleid voor gebruikers te definiëren, af te dwingen en te beheren voor alle CISP diensten.*
- ***Bieden van de mogelijkheid*** *om individuele gebruikersaccounts te definiëren met machtigingen voor CISP resources.*
- ***Bieden van de mogelijkheid*** *om te integreren en samen te werken met corporate directories om de administratieve overhead te verminderen en de ervaring van de eindgebruiker te verbeteren.*

Meer van deze vereisten zijn te vinden in *Bijlage A - Technische eisen voor de vergelijking tussen* bieders.

Functionaliteit die verder gaat dan de minimumnorm voor beveiliging kan worden gebruikt voor een meer zinvolle analyse van 'opties met toegevoegde waarde' of 'beste waarde' in een RFP. En hoe meer functionaliteit er is ingebouwd of geautomatiseerd als het gaat om beveiliging, hoe beter. Bekijk nogmaals *Bijlage A - Technische eisen voor de vergelijking tussen* bieders voor de technische eisen voor de vergelijking tussen bieders.

Overheidsorganisaties zouden moeten kijken naar cloud accreditatiecertificeringen en evaluaties om er zeker van te zijn dat de vereiste CISP beveiligingscontroles aanwezig zijn. Denk bijvoorbeeld aan een CISP die is gevalideerd en gecertificeerd door een onafhankelijke auditor

omovereenstemming met de ISO 27001-certificeringsnorm te bevestigen. ISO 27001 Annex A, domein 14 ziet op de specifieke besturingselementen waaraan een CISP zich houdt volgens de ISO-vereisten rond systeemverwerving, -ontwikkeling en -onderhoud. Het is waarschijnlijk dat deze controles het merendeel, zo niet alle, controles rond systeem aankoop, -ontwikkeling en -onderhoud omvatten die gewoonlijk door een organisatie in een IT-gerelateerde RFP worden gevraagd. Daarom is het logisch dat een organisatie simpelweg eist dat een CISP ISO 27001 gecertificeerd is, in plaats van de inspanningen te dupliceren en de controlevereisten op het gebied van systeemacquisitie, ontwikkeling en onderhoud in een RFP voor cloud services op te nemen.

Deze benadering, waarbij gebruik wordt gemaakt van compliancerapporten van derden, kan bijvoorbeeld worden toegepast op de meeste beveiligings- en compliancecontroles: CISPE AVG-gedragscode, ISO, SOC enz.

RFP voorbeeldtekst: Beveiliging

De CISP maakt zijn niet-bedrijfseigen beveiligingsprocessen en technische beperkingen bekend aan de <ORGANISATIE> zodat adequate bescherming en flexibiliteit kan worden bereikt tussen de <ORGANISATIE> en de serviceprovider.

De CISP geeft aan wat zijn taken en verantwoordelijkheden zijn op het gebied van beveiliging en compliance:

- *Beschrijven van de beveiligingsgerelateerde functies en verantwoordelijkheden van de CISP en <ORGANISATIE> in het voorgestelde aanbod. Duidelijk zijn over de afbakening van verantwoordelijkheden, en CISP diensten schetsen om de <ORGANISATIE> te helpen bij het bouwen en automatiseren van beveiligingsfuncties in de cloud omgeving.*
- *Reageren op de technische specificaties in BIJLAGE A met betrekking tot de beveiligingseisen van de <ORGANISATIE>.*

EIGENDOM EN CONTROLE VAN DE INHOUD VAN DE <ORGANISATIE>

Beschrijf hoe CISP mogelijkheden de gegevensprivacy van de <ORGANISATIE> kunnen beschermen. De aanwezige controles voor de bescherming van de content van de <ORGANISATIE> meenemen. De CISP moet zorgen voor een sterke regionale isolatie, zodat objecten die in een regio zijn opgeslagen nooit de regio verlaten, tenzij de <ORGANISATIE> ze expliciet naar een andere regio overbrengt

- *De <ORGANISATIE> beheert de toegang tot de content, services en resources. De CISP moet een geavanceerde set toegangs-, versleutelings- en logboekfuncties bieden om de <ORGANISATIE> te helpen dit effectief te doen. De CISP mag de content van <ORGANISATIE> niet openen of gebruiken voor enig ander doel dan wettelijk vereist is en voor het onderhouden van de CISP diensten en het leveren ervan aan <ORGANISATIE> en haar eindgebruikers.*

- *De <ORGANISATIE> kiest de regio('s) waarin de content wordt opgeslagen. CISP verplaatst noch repliceert de content van de <ORGANISATIE> buiten de gekozen regio('s), behalve als dit wettelijk vereist is en als het nodig is om de CISP diensten te onderhouden en aan de <ORGANISATIE> en haar eindgebruikers te leveren.*

- *De <ORGANISATIE> kiest hoe de content wordt beveiligd. CISP moet krachtige encryptie bieden voor de content van de <ORGANISATIE> in overdracht of in ruststand, en de optie bieden voor de <ORGANISATIE> om haar eigen encryptiecodes te beheren.*

- *CISP moet een beveiligingsgarantieprogramma hebben dat gebruik maakt van wereldwijde best practices op het gebied van privacy en gegevensbescherming om de <ORGANISATIE> de beveiligingscontroleomgeving van de CISP op te laten zetten, te exploiteren en te gebruiken. Beveiligings- en controleprocessen moeten onafhankelijk worden gevalideerd door meerdere onafhankelijke beoordelingen door derden*

Cloud certificeringen en evaluaties bieden organisaties uit de publieke sector de zekerheid dat CISP's beschikken over effectieve fysieke en logische beveiligingscontroles. Wanneer deze accreditaties in RFP's worden gebruikt, wordt het procurement proces gestroomlijnd en worden dubbele processen of goedkeuring workflows , die voor een cloud omgeving misschien niet nodig zijn, vermeden.

Cloud RFP's moeten CISP's de mogelijkheid bieden om te bewijzen dat zij voldoen aan compliance accreditaties en -evaluaties. Zoals hierboven vermeld, is er een aanzienlijke overlap in de risicoscenario's en risicobeheerpraktijken van deze accreditaties. En aangezien de controles en eisen in dergelijke accreditaties worden gebundeld, is het sneller om naleving van accreditaties te eisen in een RFP, in plaats van het opstellen van een lijst van individuele controles (waarvan vele mogelijk afkomstig zijn uit eerdere RFP's die gericht zijn op on-premises datacenters, en als zodanig mogelijk niet van toepassing zijn op cloud computing).

NB: het is ook belangrijk om te begrijpen hoe toegang kan worden verkregen tot de onderstaande rapporten. Zo zijn bijvoorbeeld de SOC 1 en SOC 2 rapporten doorgaans gevoelige documenten. Begrijp de overeenkomsten die nodig zijn om toegang te krijgen tot deze documenten (bijv. geheimhoudingsovereenkomst – NDA) en vraag niet eenvoudigweg om deze documenten in te dienen als onderdeel van het antwoord van de RFP (deze documenten zouden openbaar kunnen worden gemaakt door middel van een wet op Openbaarheid van bestuur of soortgelijke wetgeving die de beveiliging van de cloud in het gedrang brengt).

RFP voorbeeldtekst: Compliance

Het gebruik van erkende beveiligings-, compliance- en operationele normen, afgeleid van best practices in cloud service activiteiten - waaronder gegevensverwerking, gegevensbeveiliging, vertrouwelijkheid, beschikbaarheid, enz. - stroomlijnen de aanschaf van cloud technologie.

De <ORGANISATIE> evalueert het unieke offerteaanbod aan de hand van aanvaarde beveiligings-, compliance- en operationele normen zoals hieronder en in Bijlage A wordt beschreven. Door te vertrouwen op de certificering van de leverancier van de naleving van elke norm, kan de <ORGANISATIE> minimale naleving van de norm gebruiken als basis voor de evaluatie van het voorstel.

De eis dat de CISP gedurende de looptijd van het contract aan de minimumnorm moet blijven voldoen, biedt het voordeel dat de dienstverlening actueel blijft.

De CISP waarmee wordt geboden (direct of via een reseller) moet kunnen aantonen dat hij in staat is te voldoen aan de volgende onafhankelijke attesten, rapporten en certificeringen van derden (NB: als sommige van deze attesten, rapporten en certificeringen onder openbaarmakingsbeperkingen vallen als gevolg van beveiligingskwesties, zal de <Organisatie> samenwerken met de CISP om gezamenlijk overeengekomen toegang te verkrijgen):

Certificeringen/Attesten	*Wet- en regelgeving en privacy*	*Afstemming/Frameworken*
☐ *C5 (Duitsland)*		☐ *CDSA*
☐ *CISPE gedragscode voor gegevensbescherming (AVG)*		
☐ *CNDCP (Climate Neutral Data Centre Pact)*		
☐ *DIACAP*	☐ *EU gegevensbeschermingsrichtlijn*	☐ *CIS*
☐ *DoD SRG niveaus 2 en 4*	☐ *EU-modelbepalingen*	☐ *Criminal Justice Info. Service (CJIS)*
☐ *HDS (Frankrijk, Gezondheidszorg)*		
☐ *FedRAMP*	☐ *FERPA*	☐ *CSA*
☐ *FIPS 140-2*	☐ *AVG*	☐ *EU-VS Privacy Schild*
☐ *ISO 9001*	☐ *GLBA*	☐ *EU Safe Harbor*
☐ *ISO 27001*	☐ *HIPAA*	☐ *FISC*
☐ *ISO 27017*	☐ *HITECH*	☐ *FISMA*
☐ *ISO 27018*	☐ *IRS 1075*	☐ *G-Cloud [VK]*
☐ *IRAP [Australië]*	☐ *ITAR*	☐ *GxP (FDA CFR 21 Deel 11)*
☐ *MTCS Tier 3 [Singapore]*	☐ *PDPA - 2010 [Maleisië]*	☐ *ICREA*
☐ *PCI DSS Level 1*	☐ *PDPA– 2012 [Singapore]*	☐ *IT Grundschutz (Duitsland)*
☐ *SEC-regel 17-a-4(f)*	☐ *PIPEDA [Canada]*	☐ *MARS – E*
☐ *SecNumCloud (Frankrijk)*		
☐ *SOC1/ISAE 3402*	☐ *Privacy Act [Australië]*	☐ *MITA 3.0*
☐ *SOC2/SOC3*	☐ *Privacy Act [Nieuw-Zeeland]*	☐ *MPAA*
☐ *SWIPO IaaS Code*		
	☐ *Spaanse DPA-autorisatie*	☐ *NIST*
	☐ *U.K. DPA - 1988*	☐ *Uptime Institute Tiers*
	☐ *VPAT/Section 508*	☐ *VK Cloud Security Principles*

Bovenstaande lijst is slechts ter illustratie en moet niet worden beschouwd als een uitputtende opsomming van de certificeringen en normen die van toepassing zouden kunnen zijn op cloud services.

2.3.1.1 Gegevensbescherming

Een belangrijke overweging bij het gebruik van cloud services is dat de verwerking van persoonlijke gegevens wordt uitgevoerd in overeenstemming met de toepasselijke EU-wetgeving inzake gegevensbescherming, waaronder de Algemene Verordening Gegevensbescherming (AVG). AVG is een op principes gebaseerde regelgeving en biedt daarom geen sectorspecifieke richtlijnen om naleving te helpen garanderen. AVG moedigt echter de invoering aan van compliancetools zoals gedragscodes om dergelijke richtlijnen te kunnen bieden. CISPE heeft in samenwerking met de Franse autoriteit voor gegevensbescherming (CNIL) een gedragscode voor gegevensbescherming (CISPE code[6]) ontwikkeld die is goedgekeurd door de Europese Raad voor gegevensbescherming en die algemeen toepasbaar is in Europa. Het doel van de gedragscode is om CISP's te helpen zich aan de AVG te houden en klanten te begeleiden bij het beoordelen of CISP's geschikt zijn voor de verwerking van persoonlijke gegevens die de klant wil uitvoeren.

- De code richt zich uitsluitend op de IaaS sector en richt zich op de specifieke functies en verantwoordelijkheden van IaaS leveranciers.
- Het helpt de aspecten van eerlijke en transparante verwerking en passende beveiligingsmaatregelen in de context van cloud infrastructuurservices te verduidelijken (AVG, artikel 40 [2]).
- Het helpt klanten te begrijpen hoe ze de onafhankelijkheid over hun gegevens kunnen behouden door ervoor te zorgen dat deze binnen de EU blijven.
- Het bevordert best practices voor gegevensbescherming die het GAIA-X-initiatief van de EU ondersteunen om Europese dataservices in de cloud te ontwikkelen.

De naleving door de CISP van gedragscodes voor gegevensbescherming zoals de CISPE code garandeert dat persoonsgegevens strikt in overeenstemming met de AVG worden verwerkt.

Voorbeeld RFP taal: Gegevensbescherming

De CISP die wordt geboden (rechtstreeks of via een reseller) moet kunnen aantonen dat hij in staat is te voldoen aan een gedragscode voor gegevensbescherming, zoals de CISPE code. De gegevensbeschermingscode moet in overeenstemming zijn met de eisen die in het AVG kader zijn vastgelegd. De code moet minimaal het volgende bevatten; (1) een duidelijke definitie van de functies en verantwoordelijkheden van de CISP, (2) de eis dat de CISP geen klantgegevens zal gebruiken voor marketing- of reclamedoeleinden, en (3) de mogelijkheid voor klanten om CISP diensten te selecteren die het mogelijk maken gegevens volledig binnen de Europese Economische Ruimte te verwerken. De naleving van de code moet worden geverifieerd door externe onafhankelijke auditors (toezichthoudende instanties) die zijn geaccrediteerd door onafhankelijke, externe accountants die zijn geaccrediteerd door de Europese Autoriteit voor Gegevensbescherming.

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

2.3.1.2 Wisselen tussen cloud aanbieders en overdracht van gegevens

Klanten moeten de vrijheid hebben om de cloud services te kiezen die ze willen gebruiken, en niet afhankelijk worden van een CISP of PaaS/SaaS-provider.

Door CISP geleverde cloud services worden gestandaardiseerd en aangeboden op een 'one–to-many'-basis, waarbij diensten worden geconfigureerd, geleverd en beheerd door de klant. Een voordeel van cloud computing is dat klanten de mogelijkheid hebben om te kiezen welke gestandaardiseerde diensten ze nodig hebben om hun unieke applicaties en oplossingen te ontwikkelen. Dit voordeel strekt zich uit tot de mogelijkheid om over te stappen op nieuwe of andere diensten die het beste voldoen aan de behoeften van de klant op een bepaald moment.

Net als bij gegevensbescherming kunnen gedragscodes klanten zekerheid en vertrouwen bieden als het gaat om het overschakelen naar de cloud vanuit een infrastructuur op locatie of bij het schakelen tussen CISP's. Samen met EuroCIO (de Europese organisatie van CIO's) was CISPE medevoorzitter van de ontwikkeling van de gedragscode voor gegevensoverdraagbaarheid en cloud service switching voor IaaS-cloud services (SWIPO IaaS Code[7,8]). De eerste versie van de code werd ontwikkeld in overeenstemming met de EU-verordening inzake de vrije gegevensstroom, die in november 2019 onder het Finse voorzitterschap van de EU aan de Europese Commissie werd overhandigd en in mei 2020 door de organisatie SWIPO AISBL werd gepubliceerd. In april 2021 werden de eerste diensten door SWIPO AISBL conform de code verklaard, en in mei 2021 werden de eerste diensten van CISPE leden verklaard zich aan de code te houden.

Voorbeeld RFP taal: Schakelen tussen cloud aanbieders en overdracht van gegevens

De CISP die biedt (rechtstreeks of via een reseller) moet kunnen aantonen dat het in staat is om te voldoen aan een gedragscode voor 'switching en gegevensoverdracht', zoals de SWIPO IaaS Code. De code moet aangeven hoe een CISP klanten veilige overdracht van bedrijfsgegevens biedt, indien deze besluiten over te stappen van een CISP.

2.3.2 Vergelijking tussen leveranciers

Net als bij de technische criteria in de bovenstaande paragrafen is het belangrijk om, naast de minimale beveiligingseisen in een RFP voor cloud services, criteria aan te reiken waarmee CISP beveiligingscapaciteiten en -diensten kunnen worden vergeleken tijdens een competitieve evaluatie.

Zie *Bijlage A - Technische eisen voor de vergelijking tussen bieders* voor voorbeelden van CISP beveiligingsvereisten. Wij bevelen ten zeerste aan dat de onderstaande mogelijkheden de belangrijkste beveiligingsoverwegingen zijn voor overheidsinstellingen die CISP's evalueren:

Voorbeeld RFP taal: belangrijke beveiligingsoverwegingen

- *CISP begrijpt het model van gedeelde verantwoordelijkheid, en documentatie om klanten te helpen de afbakening van beveiligingsverantwoordelijkheden voor CISP functies en service te begrijpen (bijvoorbeeld in de context van AVG)*

[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/

- *Bewezen geschiedenis van CISP infrastructuurbeveiliging, met openbaar beschikbare niet-eigen documentatie van de CISP beveiligingshouding en de fysieke/logische controles*
- *CISP ondersteuning specifiek voor cloud beveiliging*
- *Diensten die klanten in staat stellen om het accountontwerp te formaliseren, beveiligings- en cloudgovernancecontroles te automatiseren en audits te stroomlijnen*
- *De mogelijkheid om een verzameling van resources te creëren, aan te bieden en te beheren op een template-achtige manier (inclusief door CISP/CISP-Partner gebouwde gouden-standaardtemplates voor beveiliging)*
- *De mogelijkheid om een betrouwbare en herhaalbare werking van de controles in te stellen*
- *Functies voor continue en realtime auditing*
- *De mogelijkheid om het beleid inzake cloud governance technisch te scripten*
- *De mogelijkheid om dwingende functies te maken die niet kunnen worden genegeerd door gebruikers die deze functies niet mogen wijzigen*
- *De mogelijkheid om een betrouwbare implementatie uit te voeren van wat eerder in beleid, standaarden en regelgeving is geschreven, samen met het creëren van afdwingbare beveiliging en naleving, wat op zijn beurt een functioneel betrouwbaar cloud governancemodel voor IT-omgevingen creëert*
- *Diensten ter bescherming tegen veelvoorkomende DDoS-aanvallen (Distributed Denial of Service) op het netwerk en de transportlaag, en de mogelijkheid om aangepaste regels te schrijven om geavanceerde aanvallen op de applicatielaag te beperken*
- *Beheerde dienst voor bedreigingsdetectie*

2.3.3 Contracten

Zoals hierboven vermeld zijn de voorwaarden van CISP's ontworpen om te reflecteren hoe een model voor cloud services functioneert (fysieke assets worden niet gekocht, en CISP's werken op grote schaal en bieden gestandaardiseerde diensten aan); het is dus van cruciaal belang dat de voorwaarden van een CISP zo volledig mogelijk worden opgenomen en gebruikt. Zie paragraaf *2.5* hieronder voor meer informatie over de voorwaarden en contracten.

Als het gaat om de beveiliging, raden we nogmaals sterk aan om CISP's toe te staan om voortdurend aanbiedingen bij te werken, of om leveranciers toe te staan om producten toe te voegen na de indieningsdeadline, zolang ze voldoen aan de oorspronkelijke parameters van de RFP. Dit weerspiegelt het feit dat beveiligingsfuncties en -diensten zich snel ontwikkelen en dat CISP's vaak beveiligingsgerichte diensten vrijgeven, die in veel gevallen vrij te gebruiken zijn. Hou er rekening mee dat het belangrijk is om een basisbeveiligingsniveau te hebben (zie de minimumvereisten hierboven) om te garanderen dat wijzigingen in het beveiligingsaanbod niet nadelig zijn.

Het 'shared responsibility' model is natuurlijk de kern van de beveiliging in een RFP voor cloud services. Elke partij moet duidelijk zijn over zijn beveiligingsverantwoordelijkheden, en CISP's moeten worden verplicht om CISP/klant- beveiligingsverantwoordelijkheden te documenteren voor door CISP geleverde cloud technologieën, samen met documentatie om klanten te helpen bij het inbouwen en automatiseren van best practices op het gebied van beveiliging.

Een cloud raamovereenkomst moet de flexibiliteit bieden om een leverancier te verwijderen indien deze niet langer voldoet aan de minimale beveiligings- en compliance eisen zoals beschreven in de RFP voor cloud services.

2.4 Prijzen

Om de cloud technologie te contracteren op een manier die rekening houdt met de fluctuerende vraag, hebben overheidsorganisaties een contract nodig dat hen laat betalen voor diensten zoals ze worden geconsumeerd – met het vereiste cloud beheer en de zichtbaarheid rond gebruik en uitgaven.

Belangrijk is dat RFP's voor cloud services moeten kijken naar de waarde en de totale eigendomskosten (TCO), in tegenstelling tot een eenvoudige 'appels-met-appels'-vergelijking van de eenheidsprijzen. Deze traditionele praktijk van het kijken naar de laagste eenheidsprijs vertaalt zich niet naar het cloud model, en leidt als zodanig niet tot de meest economische voordelige inschrijving, of de algemene laagste prijs.

*Ter ondersteuning van de CISP prijsevaluatie helpt het om eerst een CISP prekwalificatie of een shortlist te hebben, met **minimale prijsgerelateerde vereisten**, zodat CISP's met vergelijkbare capaciteiten in aanmerking kunnen komen voor de raamovereenkomst. Het evaluatieproces voor afroepen en mini-competities kan dan kijken naar een selectie van typische voorbeeld cloud architecturen en **prijsscenario's** die overeenkomen met een aantal typische workloads in de publieke sector, en deze door CISP's laten prijzen. Live testdemo's worden ook aanbevolen om de prestaties en elasticiteit van cloudtechnologieën die door CISP's worden geleverd te kunnen vergelijken. Zie bijlage B voor een voorbeeld van een demonstratietestscript voor cloud technologieën.*

2.4.1 Minimumeisen

Het gedeelte inzake prijzen in een RFP voor cloud services heeft vier belangrijke elementen:

1. **Prijs naar gebruik:** Cloud klanten nemen een pay-as-you-go gebruiksmodel op, waarbij ze aan het eind van elke maand gewoon betalen voor hun gebruik, wat optimaal is voor het gebruik en de resource cijfers.
2. **Transparante prijzen:** CISP prijsstelling moet openbaar beschikbaar en transparant zijn.
3. **Dynamische prijzen:** Biedt de flexibiliteit om cloud prijzen te laten schommelen op basis van marktprijzen. Deze aanpak maakt gebruik van het dynamische en concurrerende karakter van cloudprijzen en ondersteunt innovatie en prijsverlagingen.
4. **Gecontroleerde uitgaven:** CISP's moeten rapportage-, bewakings- en prognose-instrumenten bieden waarmee klanten (1) het gebruik en de uitgaven op zowel overkoepelend als gedetailleerd niveau kunnen bewaken, (2) waarschuwingen krijgen over wanneer het gebruik en de uitgaven op aangepaste drempels komen, en (3) het gebruik en de uitgaven kunnen inschatten om toekomstige cloud budgetten te kunnen plannen.

RFP voorbeeldtekst: Prijzen

*De **<ORGANISATIE>** vraagt dat reagerende CISP's hun voorgestelde methode en prijsmodel voor het leveren van elk van hun diensten aan eindgebruikers als een commerciële cloud capaciteit toevoegen.*

De CISP verstrekt:

- *Definitiedocument of links naar definities*
- *Voorwaardendocument*
- *Prijsdocument (links naar openbare prijzen zijn aanvaardbaar in de veronderstelling dat een volledige prijslijst/prijsdocument op verzoek beschikbaar is)*

De getoonde prijs is die van de meest voorkomende configuratie van de dienst. CISP's moeten opties bieden voor volumekortingen en prijscalculatietools om de werkelijke prijs van wat wordt gekocht uit te rekenen, en de totale waarde die aan de koper wordt geleverd (bijvoorbeeld diensten voor optimalisatie en de daaruit voortvloeiende kostenverlaging).

Kopers onder de raamovereenkomst kunnen met leveranciers spreken om hen te vragen hun dienstbeschrijving, voorwaarden, prijsstelling of definitiedocumenten/model toe te lichten. Er wordt een register bijgehouden van eventuele gesprekken met leveranciers.

Aanvullende eisen ten aanzien van de prijsstelling

- *Leveren van cloud technologieën met een dynamisch prijsmodel dat maximale bedrijfsflexibiliteit biedt en schaalbaarheid en groei mogelijk maakt.*

- *De prijskenmerken moeten het volgende omvatten:*
  - *Wordt de prijsstelling verzorgd in een on-demand, op basis van gebruik, pay-as-you-go service? Leg uw prijsmodel uit.*
  - *Kunt u nog meer kortingen krijgen als u zich vastlegt op het gebruik en/of bij een bulkaankoop? Geef details over hoe.*
  - *Is de prijsstelling openbaar en transparant? Voeg links toe naar algemeen beschikbare prijzen.*
  - *Is de prijsstelling dynamisch en reageert deze snel en efficiënt op de concurrentie op de markt?*
  - *Biedt u best practices en resources om de uitgaven te volgen?*
  - *Biedt u best practices en resources voor kostenoptimalisatie?*

Prijstransparantie

*Als gevolg van de voortdurend dalende trend in de prijzen van commerciële cloud technologieën, gedreven door innovatie en concurrentie, zullen de gemeten kosten per eenheid van de CISP service die door de **<ORGANISATIE>** in het kader van de raamovereenkomst worden betaald, nooit hoger zijn dan de prijs per eenheid van de cloud aanbieder die op de website van de cloud aanbieder wordt gepubliceerd en die van kracht is op het moment dat de eenheid van de dienst door de klant wordt verbruikt.*

Budgettering en factureringswaarschuwingen/rapporten

*Om de levering en het gebruik van cloud technologieën aan te tonen, moeten CISP's **<ORGANISATIE>** de tools bieden om gedetailleerde factureringsrapporten te genereren die de kosten per uur, dag of maand, per account in een organisatie, per product of productbron of per door de klant gedefinieerde tag verdelen. **<ORGANISATIE>** erkent dat **<ORGANISATIE>** als onderdeel van het model voor gedeelde verantwoordelijkheid in de cloud verantwoordelijk is voor het gebruik van door CISP verstrekte budgetterings- en factureringsfuncties en -tools om te voldoen aan unieke vereisten voor prognoses en rapportage.*

- *Geef informatie over hoe **<ORGANISATIE>** de factureringsinformatie op zowel gedetailleerd als samenvattend niveau kan bekijken, waarbij patronen in de uitgaven aan CISP resources in de loop van de tijd worden gevisualiseerd, in aanvulling op het voorspellen van toekomstige uitgaven.*

- *Geef informatie over hoe **<ORGANISATIE>** gebruik/factureringsweergave kan filteren op service, op gekoppelde account of op aangepaste tags die worden toegepast op resources, en maak factureringswaarschuwingen aan die meldingen versturen wanneer het gebruik van diensten de door de **<ORGANISATIE>**-gedefinieerde drempels/budgetten nadert of overschrijdt.*

- *Geef informatie over hoe **<ORGANISATIE>** kan voorspellen hoeveel cloud services worden gebruikt over een bepaalde voorspellingsperiode, gebaseerd op het gebruik in het verleden. CISP zou een **schatting** moeten geven van wat de CISP factuur voor de**<ORGANISATIE>** zal zijn, en de **<ORGANISATIE>** in staat moeten stellen om alarmen en budgetten te gebruiken voor bedragen waarvan wordt voorspeld dat ze zullen worden gebruikt, om zo meer grip te krijgen op de kosten en uitgaven.*

2.4.2 Vergelijking tussen leveranciers

Overheidsorganisaties vereisen vaak concurrentie tussen bieders met behulp van evaluatiecriteria zoals de beste waarde, de economisch meest voordelige inschrijving (EMVI) of de laagste prijs. Bij het plannen van de prijsstelling van raamovereenkomst afroepen of mini-competities is het belangrijk een aanpak te ontwikkelen die rekening houdt met de unieke kenmerken van de cloud. Begrijp bijvoorbeeld dat het eenvoudigweg vergelijken van individuele onderdelen van het aanbod van cloud aanbieders (bijv. computing of opslag) geen effectieve manier is om te vergelijken, omdat het geen rekening houdt met functies zoals prestaties, kostenoptimalisatie met behulp van cloud-eigen diensten en CISP bewakingstools, of onderscheidende diensten die CISP's gratis kunnen aanbieden. Bovendien kan de catalogusprijs van een CISP tienduizenden artikelen bevatten, de prijsmodellen verschillen van de ene dienst tot de andere en van de ene aanbieder tot de andere.

TCO analyseren

We adviseren te kijken naar de totale eigendomskosten (TCO) van gedefinieerde gebruiksscenario's, waarbij rekening wordt gehouden met alle aspecten van een cloudoplossing (inclusief partnerdiensten, gestandaardiseerde CISP kortingen, technische functies die de prestaties kunnen verbeteren, en kosten kunnen verlagen/optimaliseren, enz.).

Vergelijking per scenario

Bij het evaluatieproces kan ook rekening worden gehouden met de gebruikelijke scenario's die overeenkomen met gangbare systemen of applicaties. Dergelijke scenario's (zaken als webhosting, of de implementatie van een human resources systeem met x aantal gebruikers, enz.) kunnen variabelen bevatten zoals de snelheid en schaal van de resources, de prestaties van de applicatie of oplossing, toegangstijden voor opslag, laag-volume complexe gegevens in vergelijking met eenvoudige computing taken met een hoog volume enz. De applicaties of systemen kunnen ook gebruikelijke scenario's hebben zoals de verwerking van hoge volumes bij de belastingaangifte ofnoodmeldingen zoals hoogwaterwaarschuwingen. De scenario's moeten uitgebreid zijn om de scope van de technologie en diensten die de klant tijdens het project kan gebruiken, te omvatten. Op deze manier kan de klant de geschatte totale kosten van het project vergelijken.

Scenario's financieel en technisch vergelijken

Het is ook belangrijk om rekening te houden met de technische voordelen bij het vergelijken van de prijzen tussen de CISP aanbiedingen. Zo kunnen sommige CISP's klanten in staat stellen een active-activedisaster recovery-topologie op te bouwen dankzij het model van datacenters in clusters binnen een geografische regio. Een CISP die niet over dit soort redundantie en datacenterconfiguratie beschikt, zou x% duurder kunnen zijn gezien de kosten van meegerekende noodherstelbehoeften. Als voorbeeld waarom een holistische benadering van de prijsstelling met aanvullende technische kenmerken van cruciaal belang is voor de evaluatie van CISP's, kan het onderstaande alternatief voor een eenvoudige 'appels-met-appels'-vergelijking in overweging worden genomen.

Voorbeeld: Een klant wil de prijs van objectopslag door gekwalificeerde CISP's vergelijken op basis van een raamovereenkomst. De prijs van het item van de opslag 'eenheid' van CISP 1 is € 0,023/GB. De prijs van dezelfde 'eenheid' CISP 2 is € 0,01/GB. In een eenvoudige eenheid-tot-eenheid-vergelijking zou de klant geen belangrijke vragen stellen zoals:

1. Hoeveel overbodige exemplaren van het object zijn er beschikbaar in geval van een storing? In het bovenstaande voorbeeld is CISP 1 ontworpen om het gelijktijdige verlies van gegevens in twee verschillende faciliteiten te ondersteunen en meerdere kopieën van gegevens bij te houden. In het geval van CISP 2 worden geen overbodige kopieën gemaakt.
2. Wat is de mate van duurzaamheid van opgeslagen objecten? CISP 1 is 99,999999999%, CISP 2 is 99%.
3. Hou rekening met de kosten gedurende de levensduur van het totale project of de totale workload, en hoe functies voor kostenoptimalisatie de kosten kunnen verlagen als het gaat om de manier waarop gegevens worden opgeslagen en gebruikt (door bijvoorbeeld het gebruik van serverloze functies van een CISP te vergroten, kunnen de kosten met x% worden verlaagd.

Dit zijn slechts enkele van de vele andere technische overwegingen die een rol spelen bij de prijsstelling, met name op het gebied van beveiliging en compliance.

Overwegingen voor prijsscenario's omvatten onder meer

Basistarieven – dit zijn in wezen openbare prijzen van CISP's. CISP's moeten deze prijzen openbaar maken. Zoals hierboven opgemerkt kunnen klanten, om CISP's effectief te kunnen vergelijken, vragen om wellicht 3-5 specifieke scenario's (of hoeveel er ook zin hebben voor de klant) door alle leveranciers geprijsd te krijgen. Scenario's moeten alomvattend zijn om de breedte van de diensten en technologieën te omvatten die de klant waarschijnlijk tijdens het project zal gebruiken. Op deze manier kan de klant de geschatte totale kosten van het project vergelijken. Vergelijkingen op het niveau van individuele catalogusitems zijn meestal problematischer dan nuttig voor klanten en leveranciers. Klantenzouden namelijk tienduizenden items van CISP's moeten vergelijken, en leveranciers zouden dit niveau van detail moeten verstrekken en beheren wanneer de werkelijke prijs alleen wordt bepaald op basis van het dienstenverbruik.

Het evalueren van de overkoepelende capaciteiten van een CISP is een must voor cloud klanten die op zoek zijn naar de beste waarde. Zo kunnen CISP's bijvoorbeeld een aantal diensten hebben die ofwel gratis ofwel in wezen gratis zijn, en bij een prijsevaluatie moet rekening worden gehouden met dergelijke diensten, en dat andere CISP's voor soortgelijke functionaliteit kosten in rekening kunnen brengen.

De evaluatiecriteria kunnen zo worden opgesteld dat de CISP's hun 'inbegrepen x standaard' kenmerken kunnen oproepen, en hoe dergelijke diensten de totale kosten beïnvloeden. Evaluatiecriteria kunnen ook kijken naar CISP volumegebaseerde/gedifferentieerde prijsstelling en commercieel beschikbare kortingen zoals Reserved Instances/Spot Instances. Bijvoorbeeld:

- x% besparing als klanten gereserveerde compute capaciteit kopen (1 jr, 3 jr enz.)
- x% korting op gebonden/volumeprijzen

- x% besparing op basis van architectuuroverzichten en optimalisatie van de infrastructuur, zoals het overstappen op de beter passende computingoptie
- Zoals hierboven vermeld, houdt u rekening met de kosten van de hele levensduur en hoe functies voor kostenoptimalisatie de kosten kunnen verlagen

PRIJSSCENARIO
De bieders moeten de prijzen voor het onderstaande scenario alleen voor evaluatiedoeleinden opgeven. De werkelijke prijs zal gebaseerd zijn op het verbruik van diensten op basis van een on-demand pay-per-use model.

Hieronder staan representatieve eisen ten behoeve van de prijsvorming, met dien verstande dat deze nominale eisen gedurende de looptijd van het contract zullen veranderen. Geef de prijzen voor zowel 12 en 36 maanden on-demand als 12 en 36 maanden gereserveerde capaciteit.

Verstrek:

- *Naam van de voorgestelde oplossing(en):*
- *Beste prijs van de bieder:*

- *Diensturen: 24x7x365*
- *Dienstbeschikbaarheid: 99,95%*

Prijsscenario's kunnen ook voorbeelden bevatten van bestaande klanten met een vergelijkbare workload die hun uitgaven in 1/2/3 jaar hebben geoptimaliseerd - door gebruik te maken van CISP bewakings- en optimalisatietools, geoptimaliseerde cloud-eigen oplossingen te gebruiken en door CISP prijsverlagingen.

2.5 Contract uitvoer opzetten/algemene voorwaarden

Door een CISP verstrekte cloud technologieën en -uitvoeringen zijn gestandaardiseerd op basis van ontwerp, daarom zijn de contractuele voorwaarden ook gestandaardiseerd. Er is echter een mogelijkheid om deze contracten marginaal aan te passen aan de lokale wetgeving en regelgeving.

Vaak bevatten de traditionele IT-aanbestedingsmethoden strenge regels die vereisen dat de aanvragers aan veel of alle eisen van de aanbesteding moeten voldoen of afgewezen moeten worden. Of ze bevatten misschien een stricte subsetvan verplichte eisen. Wanneer deze inkoopmethode wordt gebruikt met cloud technologieën, die een set gestandaardiseerde onderdelen en tools zijn die u helpen bij het ontwerpen van een oplossing op maat, hebben aanbestedingen de neiging om te mislukken.

2.5.1 Algemene voorwaarden

De eerste stap als het gaat om het contracteren in een RFP voor cloud services is het beoordelen en begrijpen van bestaande CISP commerciële voorwaarden die in veel gevallen publiekelijk te vinden zijn op CISP websites. Overheidsinstellingen accepteren steeds gemakkelijker commerciële voorwaarden van CISP's. Een deel van deze inspanning om de voorwaarden te begrijpen, is het ontmoeten van CISP's en hun partners om hun aanpak te begrijpen. De belangrijkste vraag die moet worden gesteld is 'waarom' werken CISP's met specifieke voorwaarden. Sommige van deze voorwaarden lijken misschien anders te zijn dan traditionele IT-voorwaarden, maar er zijn zeer specifieke redenen waarom ze deel uitmaken van een cloud contract. Als de algemeen beschikbare voorwaarden niet acceptabel zijn, hebben CISP's vaak enigszins aanpasbare overeenkomsten voor zakelijke klanten die kunnen worden onderzocht.

Naast het beoordelen van de voorwaarden van de CISP is het belangrijk om inzicht te hebben in bestaand beleid, regelgeving en/of wetten (bijv. met betrekking tot technologie, dataclassificatie, privacy, personeel enz.). Vaak zijn er bestaande beleidslijnen/regelgeving/wetten die ontworpen zijn voor het kopen en gebruiken van traditionele IT-aanbiedingen, en deze kunnen op gespannen voet staan met het model van een CISP. Bijvoorbeeld alleen het gebruik toestaan van cloud technologieën die zijn opgenomen in het oorspronkelijke bod van de raamovereenkomst via de RFP voor cloud services. CISP's voegen voortdurend nieuwe diensten en functies toe. Het verstikken van de toegang tot die nieuwe diensten, simpelweg omdat u een traditionele IT-productvernieuwingsaanpak volgt, heeft voor de eindklant geen zin. Als dit het geval is, is het belangrijk om diepgaande discussies te voeren met de CISP's, waarbij onder meer wordt gekeken naar deze beleidslijnen/regelgeving en/of wetten.

Profiteer van pre RFP gesprekken

Zoals hierboven vermeld, moet u, voordat u een RFP opstelt, de tijd nemen om CISP's en aanverwante leveranciers te ontmoeten om hun voorwaarden te begrijpen en hen te informeren over de aanpak, het beleid, de regelgeving en de wetten van uw organisatie. Het belangrijkste onderdeel van deze besprekingen is dat beide partijen leren 'waarom' de relevante voorwaarden werken zoals ze werken. Zo zijn de voorwaarden in de cloud anders dan die voor traditionele datacenters, beheerde dienst, hardware, kant-en-klare software en systeemintegratie. Omdat het om één enkel model gaat en er voortdurend wordt geïnnoveerd, moet het RFP proces voldoende flexibel zijn om onderhandelingen of besprekingen mogelijk te maken om verduidelijking te verkrijgen.

Door de mogelijkheid om de voorwaarden te verduidelijken tijdens de besprekingen of onderhandelingen, krijgen overheidsorganisaties meer inzicht in de cloud modellen en vermijden ze het probleem van het afwijzen van aanbieders die eigenlijk wel in staat zijn om aan de behoeften van de organisatie te voldoen. Een gebruikelijk proces is dat de organisatie vooraf bepaalde voorwaarden vaststelt die ze bereid is te bespreken en over te onderhandelen voorafgaand aan de toekenning. Door vooraf met de bieder(s) over aanvaardbare voorwaarden te onderhandelen, zorgt de aanbestedende organisatie ervoor dat ze de beste kandidaat voor de gunning krijgt en lost ze verschillen of misinterpretaties op die anders zouden kunnen leiden tot de afwijzing van een effectief voorstel. Overheidsinstellingen kunnen ook hun beleid, regelgeving en wetten herzien, en beide partijen kunnen inzicht krijgen in hoe het gebruik van de cloud in die modellen zal passen. Vaak zijn er manieren om met de bestaande clausules te werken. Als er echter een probleemgebied is, kunnen beide teams samenwerken om een oplossing te vinden.Het is beter om deze besprekingen ruim voor elke RFP en de daaropvolgende contractuele onderhandelingen te voeren.

Onderhandelflexibiliteit

Om contracten te kunnen ondertekenen in overeenstemming met de lokale wetgeving, met een beroep op gestandaardiseerde contractuele voorwaarden van CISP, wordt aanbevolen (1) van de aanvragers hun standaardcontract op te vragen, (2) geen ongeschikte contractuele voorwaarden vast te stellen bij het opstellen van de raamovereenkomst voor de RFP voor cloud services, en (3) te voorzien in een onderhandelingsoptie over alle bepalingen van de aanbesteding en de voorstellen die zullen resulteren in de raamovereenkomst (met uitzondering natuurlijk van de verplichte clausules die door de wet worden opgelegd).

NB: de scope van de 'shared responsibility' is inherent aan het cloud model en moet worden weerspiegeld in de voorwaarden van het contract (zo bevestigt de CISP dat klanten eigenaar zijn van hun gegevens, waar deze zich bevinden, en worden tools geboden om ervoor te zorgen dat de keuze van de gegevenslocaties beperkt is - MAAR - het is de verantwoordelijkheid van de klant of partner om deze tools te gebruiken.

*Merk op dat het belangrijk is dat er **verschillende algemene voorwaarden** zijn voor elk perceel in een cloud raamovereenkomst. Een 'universele aanpak' voor het sluiten van contracten voor alle percelen zal leiden tot problemen met betrekking tot de technische haalbaarheid en compatibiliteit.*

Zoals reeds is opgemerkt, zijn RFP's die verplichte voorwaarden bevatten waarover niet kan worden onderhandeld, in wezen een 'take it or leave it'-voorstel voor aanbieders die ertoe kunnen leiden dat een anders aanvaardbaar voorstel wordt verworpen. Overheidsorganisaties moeten zorgvuldig nadenken over de gevolgen van het gebruik van verplichte voorwaarden tenzij dit een wettelijke verplichting is. Organisaties moeten zeker zijn van de noodzaak van een verplichte eis of voorwaarden, omdat toekomstige onderhandelingen worden voorkomen door hun classificatie als verplicht. Het gebruik van verplichte eisen of voorwaarden moet tot een absoluut minimum worden beperkt, om de organisatie de flexibiliteit te bieden die nodig is om de beste technologie en oplossing te verkrijgen.

Hou er rekening mee dat CISP cloud technologieën volledig gestandaardiseerd zijn en op een volledig geautomatiseerde manier worden geleverd. Daarom is een CISP niet in staat om enige wijziging aan te brengen in de voorwaarden en bepalingen die enige onderliggende aanpassing van de service zouden vereisen. Bovendien zijn de prijzen van de diensten doorgaans openbaar en gestandaardiseerd voor alle gebruikers, wat betekent dat een CISP de prijzen niet kan aanpassen om meer risico's voor een bepaalde klant te absorberen.

Indirecte aankopen

Een alternatieve optie voor de inkoop van cloud technologieën rechtstreeks van een CISP is om ze in plaats daarvan te kopen van een CISP reseller. Meer informatie over CISP resellers vindt u in paragraaf *2.1.3* hierboven.

RFP voorbeeldtekst; Algemene voorwaarden

*CISP's of representatieve leveranciers moeten hun openbaar beschikbare algemene voorwaarden verstrekken en feedback geven over de belangrijkste algemene voorwaarden die door de **<ORGANISATIE>** worden verstrekt.*

***<ORGANISATIE>** is van plan een schriftelijk contract te sluiten met de succesvolle bieder op basis van de contractuele voorwaarden van de bieder. De bieder dient een reeks voorgestelde contractuele voorwaarden voor de **<ORGANISATIE>** ter beoordeling voor te leggen, die zijn beste commerciële en juridische voorstel vertegenwoordigt. Aanbieders en de <ORGANISATIE> kunnen beide sets van voorwaarden bespreken tijdens de fase van <BESPREKING/ONDERHANDELING>.*

- *De belangrijkste voorwaarden van de raamovereenkomst zouden op hoog niveau de meeste van de volgende onderdelen omvatten:*
  - *Duur van de raamovereenkomst*
  - *Governance van de raamovereenkomst*

- *Prestaties van de raamovereenkomst*
- *Beëindiging van de raamovereenkomst*
- *Scope van het framework*
- *Bestelprocedure*
- *Vertrouwelijkheidsbepalingen*
- *Categoriespecifieke IP en informatie*
- *Minimale technische vereisten waaraan CISP's moeten voldoen – bijv. kwaliteitsnormen, accreditatie, beveiliging en gegevensbescherming*

- *Voor elke raamovereenkomst gelden andere voorwaarden*
- *Specifieke CISP diensten kunnen worden overwogen en zullen worden behandeld bij de afroep.*
- *Laat contractwijzigingen toe – de voorwaarden mogen klanten en leveranciers er niet van weerhouden om contractwijzigingen overeen te komen, om nieuwe diensten of verbeteringen aan te brengen. Het evoluerende karakter van cloud services is van dien aard dat er voortdurend serviceverbeteringen beschikbaar zullen komen, die allemaal kunnen bijdragen aan het leveren van efficiëntieverbeteringen aan klanten.*
- *Service Level Agreements (SLA's) moeten niet door de klant worden gespecificeerd. Klantenvoorwaarden moeten geen commissie-specifieke, op maat gemaakte SLA's definiëren die verschillen van de standaard servicemodellen van CISP's. Door CISP's standaard SLA's toe te staan, zullen CISP's in staat zijn om de kosten laag te houden en deze door te rekenen aan klanten, terwijl de klanten erop kunnen vertrouwen dat de CISP kan voldoen aan de SLA.*
- *Aansprakelijkheidslimieten moeten proportioneel zijn. Aansprakelijkheid moet evenredig zijn met de diensten die worden gekocht en er mogen geen onevenredig hoge aansprakelijkheidslimieten zijn. Als de limieten onevenredig hoog zijn, zou dit de CISP's ontmoedigen om laagwaardige projecten te accepteren. Deze projecten fungeren vaak als een nuttig introductie- en testcase voor klanten om te bepalen of bepaalde cloudoplossingen effectief zijn voor hun organisatie.*
- *Klanten moeten hun eigen gegevens bezitten. Klanten moeten hun gegevens controleren en bezitten en de mogelijkheid hebben om de geografische locatie te bepalen waar ze worden bewaard. Dit zal klanten in staat stellen om leveranciersafhankelijkheid te vermijden en gegevens vrij te verplaatsen naar nieuwe aanbieders.*

2.5.2 Algemene voorwaarden software

Hoewel dit handboek zich richt op de inkoop van IaaS- en PaaS-cloudtechnologieën zoals geleverd door een CISP, is het belangrijk om de softwarevoorwaarden te benadrukken die organisaties in de publieke sector kunnen overwegen bij het aanschaffen van software van leveranciers. Raadpleeg Afbeelding 1 (pagina 6) om te bekijken hoe software wordt aangeschaft als onderdeel van een goed gestructureerde RFP voor cloud services.

Software speelt een cruciale rol in vrijwel elk bedrijf, inclusief de publieke sector. Het opnemen van verplichtingen zoals voorwaarden voor softwarelicenties in een RFP voor cloud services helpt te garanderen dat organisaties uit de publieke sector de beste waarde krijgen en de vrijheid hebben om leveranciers te kiezen bij de aanschaf van software.

Bekijk de Tien principes van eerlijke softwarelicenties voor Cloud klanten[9] voor meer informatie. De principes zijn ontwikkeld door Cigref[10], een organisatie die bestaat uit grote Franse bedrijven en

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

overheidsdiensten die de gebruikers van digitale technologie vertegenwoordigen, in samenwerking met CISPE, en de steun van andere Europese brancheorganisaties van CIO's en aanbieders, om praktijken aan te pakken die beide organisaties beschouwen als het schaden van de digitale transformatie van organisaties van elke omvang als ze naar de cloud verhuizen.

RFP voorbeeldtekst: Software

<ORGANISATIE> is van plan een schriftelijk contract te sluiten met de succesvolle bieder op basis van de contractuele voorwaarden van de bieder. De bieder dient een reeks voorgestelde contractuele voorwaarden voor de <ORGANISATIE> ter beoordeling voor te leggen, die zijn beste commerciële en juridische voorstel vertegenwoordigt. Softwareleveranciers en de <ORGANISATIE> kunnen beide sets voorwaarden en bepalingen bespreken tijdens de fase <BESPREKING/ONDERHANDELING>.

Vereiste 1.0. Softwareleveranciers moeten duidelijke licentievoorwaarden bieden, waaronder een specificatie van de kosten op samenvattend en gedetailleerd niveau. *Vereiste 1.1. Alle kosten die verband houden met het niet naleven van licentievoorwaarden moeten worden verstrekt op samenvattende en gedetailleerde niveaus.*
Vereiste 2.0. Softwarelicenties moeten <Organisatie> de mogelijkheid bieden om de gelicentieerde software te migreren van lokaal naar de cloud van hun keuze, zonder dat de aankoop van afzonderlijke, duplicatieve licenties voor dezelfde software vereist is. *Vereiste 2.1. Softwarelicenties moeten vrij zijn van licentiebeperkingen en hogere kosten die de mogelijkheid van <Organisatie> beperken om de gelicentieerde software in de cloud van hun keuze uit te voeren.*
Vereiste 3.0. Softwarelicenties moeten <Organisatie> het mogelijk maken de gelicentieerde software op hun eigen hardware (gewoonlijk 'lokale' software genoemd) en in de cloud van hun keuze uit te voeren.
Vereiste 4.0. Softwarelicenties mogen niet vereisen dat de gelicentieerde software alleen wordt uitgevoerd op hardware die uitsluitend is bestemd voor <Organisatie>.
Vereiste 5.0. Softwareleveranciers mogen <Organisatie> niet bestraffen als de gelicentieerde software van de leverancier wordt gebruikt op het cloudaanbod van een andere leverancier, bijvoorbeeld door het opnemen van rechten om meer of opdringerige software-audits uit te voeren, of door hogere kosten voor softwarelicenties op te leggen.
Vereiste 6.0. Directorysoftware moet open standaarden ondersteunen voor het synchroniseren en verifiëren van gebruikersidentiteiten op een niet-discriminerende manier met andere identiteitsservices.
Vereiste 7.0. Softwareleveranciers mogen geen verschillende prijzen in rekening brengen voor dezelfde software die uitsluitend is gebaseerd op de eigenaar van de hardware waarop deze is geïnstalleerd. *Vereiste 7.1. De prijzen voor software mogen geen onderscheid maken tussen software die is geïnstalleerd in het eigen datacenter van <Organisatie>, een datacenter dat wordt beheerd door een derde partij, op computers die zijn geleased van een derde partij of in de cloudaanbieder naar keuze van <Organisatie>.*
Vereiste 8.0. Gedurende de looptijd van het contract mogen softwareleveranciers geen belangrijke wijzigingen aanbrengen in licentievoorwaarden die <Organisatie> beperken tot eerder toegestaan gebruik, tenzij dit wettelijk is vereist of vanwege beveiligingsproblemen.

Vereiste 9.0. *Softwareleveranciers mogen <Organisatie> niet misleiden door te zeggen dat softwarelicenties bedoeld softwaregebruik van <Organisatie> zullen dekken, zoals beschreven in de vereisten van de <Organisatie>. Voor het dekken van dergelijk gebruik kan de aanschaf van extra licenties nodig zijn.*
Vereiste 10.0. *Als <Organisatie> het recht heeft om softwarelicenties door te verkopen en over te dragen, moeten softwareleveranciers onder eerlijke voorwaarden ondersteuning en patches blijven bieden aan <Organisatie>, die op legale wijze een opnieuw gekochte licentie heeft verkregen.*

2.5.3 Hoe per project te selecteren tussen de deelnemers aan een project

Publieke organisaties die partij zijn in een framework contract kunnen de diensten die zij nodig hebben, bestellen of 'afroepen' wanneer dat nodig is. Door een afroepcontract onder een raamovereenkomst te plaatsen, kunnen kopers hun eisen verfijnen met aanvullende functionele specificaties voor een afroep, met behoud van de voordelen die de raamovereenkomst biedt.

Indien dit nodig wordt geacht, kan een mini-competitie worden gehouden om de beste leverancier voor een bepaalde workload of een bepaald project te identificeren. Bij een mini-competitie gaat een klant in het kader van de raamovereenkomst de concurrentie verder aan, door alle leveranciers binnen een partij uit te nodigen om te reageren op een reeks van eisen. De klant zal alle bekwame leveranciers binnen het perceel uitnodigen om een bod uit te brengen, vandaar het belang van minimumeisen voor deelnemers op een RFP voor cloud services - omdat het een hoge norm aan opties onder elk perceel garandeert.

Nogmaals: het is belangrijk dat er verschillende reeksen algemene voorwaarden zijn voor elk van de partijcategorieën van het type aanbod (bijv. openbare IaaS/PaaS, gemeenschappelijke IaaS/PaaS, privé IaaS/PaaS), aangezien een standaard aanpak voor het sluiten van contracten voor elke partij zal leiden tot problemen in verband met de technische haalbaarheid en compatibiliteit.

Zie paragraaf *2.1.4* voor een RFP voorbeeldtekst als het gaat om het selecteren tussen deelnemers.

2.5.4 Onboarding en offboarding

Een van de overwegingen waarmee rekening moet worden gehouden bij het opstellen van een cloud raamovereenkomst is de optie voor een *dynamic purchasing system* (DPS). Met een DPS-model worden alle leveranciers die aan de minimumeisen van de raamovereenkomst voldoen, toegelaten tot het framework. Er is geen harde limiet voor het aantal leveranciers dat zich bij het framework mag aansluiten, en in tegenstelling tot het traditionele frameworkmodel kunnen leveranciers ook een aanvraag indienen om zich bij het 'DPS Framework' aan te sluiten op elk moment van de levensduur.

Wij raden overheidsinstellingen ten zeerste aan om hoge standaarden te hanteren om de kwaliteit en de zekerheid van de dienstverlening van gekwalificeerde leveranciers te garanderen, maar om niet te specifiek te zijn om CISP's te diskwalificeren op een manier die geen eerlijke concurrentie garandeert. Uiteindelijk is het doel om de eindgebruiker niet te verzadigen met een groot aantal opties, terwijl de standaard van de beschikbare cloud technologieën hoog blijft.

3.0 Best practices/lessons learned

Hieronder belichten we enkele lessen die we hebben geleerd hoe een succesvolle cloud raamovereenkomst te realiseren met een goed geschreven RFP voor cloud services.

3.1 Cloud governance

Governance in de cloud is een gedeelde verantwoordelijkheid. CISP's bieden functies en diensten om cloud governance in elk aspect van een cloud omgeving in te bouwen, terwijl klanten hun bestaande cloud governance standaarden meenemen en leren hoe de cloud een cloud governance mogelijk maakt.

In de cloud krijgen klanten de kans om de IT-omgeving te bouwen die ze willen, en niet alleen om de bestaande omgeving te beheren. De cloud stelt klanten in staat om: (1) te starten met een volledige inventaris van alle IT-assets; (2) al deze assets centraal te beheren; en (3) waarschuwingen in te stellen met betrekking tot gebruik/facturatie/beveiliging/enz. Al deze essentiële voordelen van de cloud helpen klanten om een geoptimaliseerde en volledig geautomatiseerde architectuur te hebben, zonder dat ze voortdurend nieuwe hardware hoeven aan te schaffen en te installeren. Dit wordt gedaan door de CISP, waardoor klanten de focus kunnen verschuiven van ongedifferentieerd infrastructuurbeheer naar het bedrijfskritische operationele niveau.

Een handige manier om een CISP cloud te bekijken is te beseffen dat het in feite een zeer grote API is. Of nu een nieuwe server gelanceerd wordt of een beveiligingsinstelling gewijzigd, u voert alleen API oproepen uit. Elke verandering in de omgeving wordt gelogd en geregistreerd (het wie, wat, waar en wanneer van elke verandering wordt geregistreerd). Dit zorgt voor cloud governance, controle en zichtbaarheid die alleen mogelijk is in een cloud omgeving. Het stelt klanten in staat om hun bestaande IT-governancemodellen te heroverwegen en te bepalen hoe ze gestroomlijnd en verbeterd kunnen worden, gezien de voordelen die de cloud met zich meebrengt.

Cloud governance kan ook betekenen dat de positieve procesveranderingen en nieuwe vaardigheden die bij de cloud horen, worden gecommuniceerd en geïntegreerd. Projectmanagers zijn bijvoorbeeld gewend maandenlang te wachten op een nieuwe IT-omgeving en kunnen daardoor de planning voor het creëren van een ontwikkel- of testomgeving in de cloud (die met de cloud slechts enkele minuten kan duren) aanzienlijk overschatten. De gewenning aan deze nieuwe wendbaarheid zal een evolutionair proces zijn en gebeurt programma per programma. Dergelijke lessen moeten worden gedeeld, zodat een cloud raamovereenkomst zich kan blijven ontwikkelen en vereisten geschikt zijn voor de cloud.

3.2 Budgettering voor de cloud

Als het gaat om het structureren van pay-as-you-use cloud prijzen om te voldoen aan de aankoop- en budgetvereisten van de publieke sector, hebben we ontdekt dat het helpt om CISP services te bundelen in één enkele categorie: cloud technologieën (computing, opslag, netwerken, database, IvD enz.). Deze aanpak biedt flexibiliteit om alle huidige en nieuwe CISP technologieën in real time aan gebruikers aan te bieden en biedt gebruikers snelle toegang tot de resources die ze nodig hebben. . Op deze manier wordt er ook rekening gehouden met de fluctuerende vraag, wat leidt tot een optimaal gebruik en lage kosten.

Overheidsorganisaties kunnen extra categorieën toevoegen voor bestellingen vanuit andere percelen van een cloud framework, als zij behoefte zouden hebben aan consultancy, managed services, software via een marketplace, cloud ondersteunende diensten, en training in CISP services.

Er kan extra flexibiliteit in contracten worden ingebouwd, door optionele items of services toe te voegen aan passende resource categorieën, om de toekomstige groei te kunnen opvangen. Als een organisatie cloud technologieën met consultancy, zakelijke dienstverlening of managed services wil bundelen onder één categorie, kan dat ook met een categorie als 'Cloud technologieën en nevenwerkzaamheden'

Hieronder staat een representatief voorbeeld van deze aanpak. In het onderstaande voorbeeld komt elke eenheid van het item '#1001 - Cloud Technologieën', overeen met € 1,00 van de gebruikte 'Cloud Technologieën'. Elke maand kunnen de orderverhogingen worden gefinancierd op basis van de huidige en verwachte gebruiksprognoses.

Tabel 3 - Voorbeeld van de prijsstructuur van een enkele rubriek.

ITEM NR.	LEVERINGEN/DIENSTEN	HOEVEELHEID	EENHEID	EENHEIDSPRIJS	BEDRAG
1001	Cloud technologieën	1.000	Elk	€ 1	€ 1.000
1002	Consultancy diensten	1	per week	€ 3.000	€ 3.000
1003	Cloud ondersteuning	1	Per maand	€ 1.000	€ 1.000
1004	Cloud training	1	Per dag	€ 3,00	€ 3.000
1005	Cloud marketplace	10	Elk	€ 10	€ 100

Als voorbeeld van hoe deze structuur kan werken: een overheidsorganisatie werkt met een CISP om in te schatten hoeveel cloud technologiediensten de organisatie gaat gebruiken. De organisatie komt een gebruik overeen met de leverancier van € 10 miljoen over 5 jaar, wat neerkomt op € 2 miljoen per jaar. De organisatie committeert zich aan het aanvankelijke bedrag van € 2 miljoen per jaar. Elke maand is er een factuur en het geld wordt uit gereserveerd budget betaald. Het resterende budget wordt gemonitord met behulp van CISP monitoring- en prognosetools. Als het resterende budget te laag wordt, vraagt de organisatie de financieel directeur om extra resources, die kunnen worden ingezet voor het behoud van de diensten.

RFP voorbeeldtekst: Prijzen - Contract

BETAALTERMIJNEN
*De betalingsvoorwaarden moeten zodoende worden gestructureerd om alleen te betalen voor de resources die door de **<ORGANISATIE>** worden gebruikt, zoals hieronder aangegeven:*

1. *Maandelijkse betaling op basis van het werkelijke gebruik/verbruik van de diensten en volgens de openbare beschikbare prijzen van de CISP's.*

MINIMALE GARANTIE EN MAXIMALE UITGAVEN
Omdat het voor de <ORGANISATIE> onmogelijk zal zijn om precies te bepalen welk volume van de resources van een specifieke Cloud Service Provider over een bepaalde periode zal worden verbruikt, zullen orders worden gespecificeerd als hoeveelheden per eenheid met een vaste prijs van één enkel besteld item voor cloud technologieën.

Elke eenheid van het bestelde item komt overeen met de waarde van <€1,00> aan bestelde cloud technologieën. Stapsgewijze bestellingen zullen periodiek worden geplaatst via een wijziging van deze bestelling in verschillende hoeveelheden om <ORGANISATIE> met de flexibiliteit om verschillende 'eurobedrag'-hoeveelheden van CISP Cloud technologieën vooraf te bestellen, op basis van het geschatte gebruik ervan, voor behoeften van verschillende duur. De hoeveelheden worden periodiek vooraf besteld door <ORGANISATIE> in hoeveelheden die voldoende zijn om de geschatte kosten te dekken voor cloud technologieën die zullen worden gebruikt om te voldoen aan een verscheidenheid van eisen.

Item nr.	Omschrijving	Hoeveelheid	Eenheid	Prijs
01	CISP cloud technologieën	1.000	EA	€1.000,00

MINIMUMBESTELLING/STAPSGEWIJZE BESTELLING
De bestellingen worden periodiek geplaatst voor verschillende hoeveelheden van <10.000> eenheden op basis van de geschatte inzet van cloud technologieën door de <ORGANISATIE>. Deze regeling biedt de <ORGANISATIE> de flexibiliteit om vooraf <10.000> eenheden van 'Cloud technologieën' te bestellen als dat nodig is om activiteiten te ondersteunen en om consistent te blijven met de commerciële praktijken van 'pay-as-you-go' op het gebied van cloud computing.

Een eerste verhoging van <100.000> eenheden ten koste van <€100.000> zal worden besteld wanneer de afroep wordt geplaatst. Het minimum aantal totale rubrieken dat op een enkele stapsgewijze bestelling kan worden geplaatst met één of meer items is <x>. Het maximum aantal eenheden dat kan worden besteld onder de leveringsbestelling mag niet hoger zijn dan <x>, maar het is niet toegestaan om de afroepwaarde te overschrijden in combinatie met alle eerder bestelde eenheden. <ORGANISATIE> is ervoor verantwoordelijk dat alle bestellingen binnen de in deze paragraaf aangegeven grenzen blijven.

MAXIMUM BESTELLING
De totale maximale orderwaarde is maximaal <x>, bestaande uit maximaal <x> eenheden van een enkel item dat <x> per eenheid kost. De waarde is gebaseerd op een schatting van de vereisten van <ORGANISATIE> gedurende de prestatieperiode, maar wordt niet gegarandeerd.

3.3 Inzicht in het bedrijfsmodel van partners

Organisaties uit de publieke sector moeten proberen de modellen te begrijpen waaronder CISP's hun services aanbieden en inzien dat partners die consultancy, managed services, resell en nog veel meer leveren, van cruciaal belang zijn voor het proces. Veel klanten hebben een cloud aanbieder nodig voor hun infrastructuur en besteden 'hands on keyboard' planning, migratie en beheer uit aan een systeemintegrator (SI) of een managed services provider. Gezien deze mix van 'diensten' kunnen er eisen zijn die niet van toepassing zijn op cloud aanbieders, zoals een flow-down clausule voor onderaannemers.

Dergelijke flow-down-clausules tonen aan waarom het belangrijk is te begrijpen hoe partners en resellers met CISP's werken. Zo zijn er bij sommige aanbestedingen clausules die de hoofdaanbieder verplichten bepaalde clausules door te voeren naar al zijn partners/onderaannemers. Gewoonlijk zullen CISP's niet als formele onderaannemingspartner optreden, aangezien zij een gestandaardiseerde dienst op grote schaal aanbieden die niet is afgestemd op de unieke behoeften van een bepaalde eindklant (met inbegrip van de behoeften van een klant uit de publieke sector in het kader van een overheidscontract). In een indirect inkoopmodel (het inkopen van cloud services via een CISP reseller) kan een CISP deze clausules van zijn reseller afwijzen als niet van toepassing op een '2e niveau' leverancier van commerciële diensten. In een dergelijk geval voert de CISP niet zelf de werkzaamheden uit die onder het contract vallen, maar maakt een CISP partner gebruik van de CISP infrastructuur om dit te doen. CISP is dus een commerciële leverancier (geen onderaannemer) van de activiteiten van een partner. In een rechtstreeks inkoopmodel (waarbij de cloud services rechtstreeks van een CISP worden gekocht) zou een CISP deze 'verplichte' clausules, die geschikt zijn voor een gewone grondstoffenleverancier, doorgaans afwijzen vanwege het commerciële karakter van de gecontracteerde diensten en het feit dat de meeste CISP's geen onderaannemers nodig hebben om hun commerciële diensten te leveren.

3.4 Cloud brokers

Het concept van een cloud broker als middel om leveranciersafhankelijkheid te verminderen kan problematisch zijn. Hoewel een cloud broker in theorie een goed idee kan zijn, zalhet in de praktijk waarschijnlijk meer complexiteit en verwarring introduceren dan gerealiseerde waarde.

Het is onvermijdelijk dat het ontwerpen van applicaties om in meerdere clouds tegelijk of onderling te werken leidt tot concessies qua capaciteiten (er is geen Rosetta Stone voor de cloud). Deze aanpak kan uiteindelijk een onnodige laag van complexiteit toevoegen tussen klanten in de publieke sector en hun cloud services, wat de efficiëntie en beveiligingswinst die wordt nagestreefd in gevaar kan brengen, en wat leidt tot verminderde schaalbaarheid en wendbaarheid, hogere kosten en het vertragen van innovatie.

3.5 Pre-RFP sourcing/marktonderzoek

Als een overheidsinstantie plannen maakt voor een RFP voor cloud services, moeten stakeholders uit alle delen van de organisatie betrokken worden – senior management, business, IT, finance, procurement, legal, en contracts – vanaf het allereerste begin van het proces. Deze aanpak zorgt ervoor dat alle belanghebbenden het cloudmodel begrijpen, en daarmee een goed geïnformeerde aanpak kunnen toepassen voor het beoordelen en aanpassen van traditionele IT-inkoopmethoden.

Als het gaat om de dialoog met de sector, raden we overheids organisaties aan om de tijd te nemen om diepgaande gesprekken te voeren om feedback te verzamelen van de sector - CISP's, CISP Partners, PaaS/SaaS Marketplace leveranciers, en industrie experts. Een dergelijke dialoog kan bijvoorbeeld de vorm aannemen van branchedagen of workshops over beveiliging en inkoop. Een andere effectieve manier om een diepgaand inzicht te krijgen in cloud inkoop is het uitbrengen van een RFI, of idealiter een concept RFP document. Vaak bevatten deze potentiële problemen die kunnen worden geïdentificeerd, besproken en aangepast voordat de definitieve RFP voor cloud services wordt uitgebracht.

3.6 Duurzaamheid

Duurzaamheid is inherent aan cloud computing en de overstap naar de cloud biedt een energie en efficientie winst in vergelijking met lokale servers of datacenters van bedrijven. Het identificeren van een CISP die prioriteit geeft aan duurzaamheid en openbare toezeggingen heeft gedaan om duurzaamheidsdoelen te bereiken, biedt verdere zekerheid dat de cloud duurzaam is. Europese CISP's en exploitanten van datacenters (met de steun van de Europese Commissie) hebben het Climate Neutral Data Centre Pact[11] opgericht, een zelfregulerend initiatief om duidelijke, eenvoudige en verreikende duurzaamheidscriteria vast te stellen voor de datacenterbranche en ervoor te zorgen dat datacenteroperators en cloud service aanbieders in 2030 klimaatneutraal zijn. Dit zelfregulerend initiatief bevat duidelijke doelstellingen voor de energie efficiëntie van datacenters, waterbesparing, hergebruik en reparatie van servers, en het gebruik van koolstofvrije energie om datacenters van stroom te voorzien. CISP's die zich aanmelden voor dit initiatief spreken af de doelstellingen te halen en zich te certificeren aan de hand van deze criteria, om te mogen worden beschouwd als een klimaatneutrale exploitant.

Een RFP voor cloud services moet CISP's vragen of ze zich aan dergelijke criteria hebben gehouden, en specifiek vragen of ze zich hebben aangemeld voor zelfregulering en wanneer ze zo'n toezegging hebben gedaan.

Voorbeeld RFP taal: Duurzaamheid

Hebt u toegezegd klimaatneutrale datacenters te zullen exploiteren door u aan te melden bij het Climate Neutral Data Centre Self-Regulatory Initiative? Zo ja, wanneer heeft u dit ondertekend?

Kunt u bewijzen dat u het Climate Neutral Data Centre Pact-zegel voor gebruik hebt gekregen?

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

Bijlage A - Technische eisen voor de vergelijking tussen bieders

Hieronder geven we een overzicht van een aantal algemene cloud technologie eisen die kunnen worden gebruikt om CISP's te vergelijken tijdens afroepen of mini-competities in een cloud raamovereenkomst.

1. Profiel cloud aanbieder

	Vereiste
1.	*MARKTERVARING:* *Hoeveel jaar is de cloud aanbieder al actief in het marktsegment van de cloud?*
2.	*OPENHEID EN GEGEVENSBESCHERMING:* *Houdt de cloud aanbieder zich aan de gegevensbescherming of de omkeerbaarheid van de gedragscodes van de branche? Houdt de cloud aanbieder zich aan open source en open API ontwikkelingsprincipes?*

2. Wereldwijde infrastructuur

	Vereiste
1.	*WERELDWIJD BEREIK:* *Biedt de cloud aanbieder een wereldwijde infrastructuur om gebruikers te helpen een lage latency en hoge doorvoersnelheid te bereiken?*
2.	*REGIO'S:* *Heeft de cloud aanbieder een regionale aanwezigheid in de benodigde geografische gebieden?*
3.	*DOMEINEN/ZONES:* *Implementeert de cloud aanbieder het concept van domeinen of zones, waarbij meerdere datacenters worden gegroepeerd via een netwerk met een lage latency om een hogere mate van hoge beschikbaarheid en fouttolerantie te bieden?* • *Zo ja, vermeld het aantal domeinen of zones en het aantal datacenters binnen het benodigde geografisch gebied*
4.	*AFSTAND DOMEINEN/ZONES:* *Bouwt de cloud aanbieder zijn domeinen of zones met datacenters die fysiek uit elkaar liggen om redundantie, hoge beschikbaarheid en lage latency te ondersteunen?*
5.	*GEBOUWDE DATACENTERS:* *Biedt de cloud aanbieder datacenters die zijn ontworpen om te worden geïsoleerd van storingen in andere datacenters, met redundante stroomvoorziening, koeling en netwerken?*
6.	*DATACENTER REPLICATIE:* *Biedt de cloud aanbieder datareplicatie over datacenters binnen een domein of zone met automatische failover?*
7.	*REPLICATIE DOMEINEN/ZONE:* *Biedt de cloud aanbieder datareplicatie tussen domeinen of zones binnen een regio?*

3. Infrastructuur

3.1 Compute

	Vereiste
1.	*COMPUTE – REGULIERE INSTANCE – ALGEMEEN DOEL:* *Biedt de cloud aanbieder de volgende instancetypen aan?* • *Algemeen doel – geoptimaliseerd voor algemene applicaties en biedt een balans tussen computing, geheugen en netwerkresources.* ○ *Zo ja, wat is de grootste instance?*
2.	*COMPUTE – REGULIERE INSTANCE – GEHEUGEN GEOPTIMALISEERD:* *Biedt de cloud aanbieder de volgende instancetypen aan?* • *Geheugen geoptimaliseerd – geoptimaliseerd voor geheugenintensieve applicaties* ○ *Zo ja, wat is de grootste instance?*
3.	*COMPUTE – REGULIERE INSTANCE – COMPUTE GEOPTIMALISEERD:* *Biedt de cloud aanbieder de volgende instancetypen aan?* • *Compute geoptimaliseerd – geoptimaliseerd voor compute-intensieve applicaties* ○ *Zo ja, wat is de grootste instance?*
4.	*COMPUTE – REGULIERE INSTANCE – OPSLAG GEOPTIMALISEERD:* *Biedt de cloud aanbieder de volgende instancetypen aan?* • *Opslag geoptimaliseerd – biedt een grote hoeveelheid lokale opslagcapaciteit* ○ *Zo ja, wat is de maximale opslagcapaciteit (d.w.z. 5,10,20,50 TB) en het maximale aantal schijven (HDD's/SSD's) dat aan een instance kan worden geleverd en bevestigd?*
5.	*COMPUTE – REGULIERE INSTANCE – GRAPHICS GEOPTIMALISEERD:* *Biedt de cloud aanbieder de volgende instancetypen aan?* • *Goedkope grafische oplossingen – biedt betaalbare grafische versnelling voor compute instances?* ○ *Zo ja, wat is de grootste instance?*
6.	*COMPUTE – REGULIERE INSTANCE – GPU GEOPTIMALISEERD:* *Biedt de cloud aanbieder de volgende instancetypen aan?* • *GPU – biedt hardware grafische verwerkingseenheden (GPU's) voor grafisch-intensieve applicaties* ○ *Zo ja, hoeveel GPU's en welke GPU-modellen kan de cloud aanbieder per instance aanbieden?*
7.	*COMPUTE – REGULIERE INSTANCE – FPGA GEOPTIMALISEERD:* *Biedt de cloud aanbieder de volgende instancetypen aan?* • *FPGA – biedt in het veld programmeerbare gate arrays (FPGA) voor het ontwikkelen en inzetten van aangepaste hardwareversnelling voor applicaties.* ○ *Zo ja, hoeveel FPGA's kan de cloud aanbieder per instance aanbieden?*
8.	*COMPUTE – BURSTABLE INSTANCE:* *Biedt de cloud aanbieder burstable instances die een basisniveau van centrale verwerkingseenheid (CPU)-prestaties leveren met de mogelijkheid om boven de basislijn uit te komen?* • *Zo ja, wat is dan de grootste burstable instances?*

9.	*COMPUTE – IO-INTENSIEVE INSTANCE:* *Biedt de cloud aanbieder instances die gebruik maken van non-volatile memory express (NVMe) solid state drives (SSD's) die zijn geoptimaliseerd voor lage latency, zeer hoge random I/O-prestaties en hoge sequentiële leesdoorvoer?* • *Zo ja, wat is de maximale in- en uitvoercapaciteit per seconde (IOPS) van de grootste instance?*
10.	*COMPUTE – TIJDELIJKE LOKALE OPSLAG:* *Ondersteunt de cloud aanbieder lokale opslag voor compute_instances die worden gebruikt voor de tijdelijke opslag van informatie die regelmatig verandert?*
11.	*COMPUTE – ONDERSTEUNING VOOR MEERDERE NIC'S:* *Ondersteunt de cloud aanbieder meerdere (primaire en extra) netwerkkaarten (NIC's) die voor een bepaalde instance moeten worden toegewezen?* • *Zo ja, wat is het maximum aantal NIC's per instance?*
12.	*COMPUTE – INSTANCE AFFINITEIT:* *Biedt de cloud aanbieder gebruikers de mogelijkheid om instances binnen hetzelfde datacenter logisch te groeperen?*
13.	*COMPUTE – INSTANCE ANTI-AFFINITEIT:* *Biedt de cloud aanbieder gebruikers de mogelijkheid om instances logisch te groeperen en ze in verschillende datacenters binnen een regio te plaatsen?*
14.	*COMPUTE – SELF-SERVICE INRICHTING:* *Biedt de cloud aanbieder self-service inrichting van meerdere instances tegelijk aan via een programmatische interface, een beheerconsole of een webportaal?*
15.	*COMPUTE – AANPASSING:* *Biedt de cloud aanbieder aanpasbare instances, d.w.z. de mogelijkheid om configuratie-instellingen zoals virtuele centrale verwerkingseenheden (vCPU's) en random access memory (RAM) te wijzigen?*
16.	*COMPUTE – TENANCY:* *Biedt de cloud aanbieder enkele tenant instances die worden uitgevoerd op hardware die aan één gebruiker is toegewezen?* *Zo ja, wat is dan de grootste beschikbare instance voor een enkele tenant?*
17.	*COMPUTE – HOST AFFINITEIT:* *Biedt de cloud aanbieder de mogelijkheid om een instance te starten en te specificeren dat deze instance altijd herstart op dezelfde fysieke host?*
18.	*COMPUTE – HOST ANTI-AFFINITEIT:* *Biedt de cloud aanbieder de mogelijkheid om specifieke instances te splitsen en te hosten over verschillende fysieke hosts?*
19.	*COMPUTE – AUTOMATISCH SCHALEN* *Biedt de cloud aanbieder de mogelijkheid om tijdens vraagpieken automatisch het aantal instances te verhogen om de prestaties te behouden (d.w.z. 'uitschalen')?*
20.	*COMPUTE – MECHANISME VOOR HET IMPORTEREN VAN IMAGES:* *Biedt de cloud aanbieder gebruikers de mogelijkheid om hun bestaande images te importeren en op te slaan als nieuwe, privé beschikbare images die vervolgens in de toekomst worden gebruikt om instances te leveren?* • *Zo ja, welke indelingen worden ondersteund?*

21.	*COMPUTE – MECHANISME VOOR HET EXPORTEREN VAN IMAGES:* *Ondersteunt de cloud aanbieder de mogelijkheid om een bestaande lopende instance of een kopie van een instance te nemen en de instance te exporteren naar een virtuele machine indeling?* • *Zo ja, welke indelingen worden ondersteund?*
22.	*COMPUTE – DIENSTONDERBREKING:* *Biedt de cloud aanbieder manieren om uitval of downtime van instances te voorkomen wanneer de aanbieder enige vorm van hardware- of serviceonderhoud op hostniveau uitvoert?*
23.	*COMPUTE – INSTANCE HERSTARTEN:* *Biedt de cloud aanbieder manieren om instances op een gezonde host automatisch te herstarten als de oorspronkelijke fysieke host faalt?*
24.	*COMPUTE – KENNISGEVINGEN:* *Heeft de cloud aanbieder in het geval van een rekenbestendige gebeurtenis de mogelijkheid om de gebruiker op de hoogte te brengen van een dergelijke gebeurtenis en kan de gebruiker zich via zelfbedieningsmiddelen aanmelden of afmelden voor deze communicatie?*
25.	*COMPUTE – GEBEURTENISPLANNING:* *Biedt de cloud aanbieder de mogelijkheid om gebeurtenissen te plannen voor de instances van de gebruiker, zoals het opnieuw opstarten, stoppen, starten of buiten gebruik stellen van de instance?*
26.	*COMPUTE – BACK-UP- EN HERSTELMECHANISME:* *Biedt de cloud aanbieder een geïntegreerd back-up- en herstelmechanisme?*
27.	*COMPUTE – SNAPSHOTMECHANISME:* *Biedt de cloud aanbieder een handmatig, on-demand snapshotmechanisme?*
28.	*COMPUTE – METAGEGEVENS:* *Biedt de cloud aanbieder een metagegevensdienst voor de instance die gebruikers in staat stelt om willekeurige codewaardeparen voor de instance in te stellen?*
29.	*COMPUTE – METAGEGEVENS OPROEP:* *Biedt de cloud aanbieder een instance-metagegevensdienst die een applicatieprogrammeringsinterface (API) biedt die de instance kan oproepen om informatie over zichzelf te achterhalen?*
30.	*COMPUTE – BIEDINGSMECHANISME:* *Biedt de cloud aanbieder een biedingsmechanisme om te bieden voor goedkopere instances die onmiddellijk kunnen worden gestart om niet-bedrijfskritische workloads te hosten?*
31.	*COMPUTE – PLANNINGSMECHANISME:* *Biedt de cloud aanbieder een manier om extra rekencapaciteit op een terugkerende basis te plannen en te reserveren, bijvoorbeeld een dagelijkse, wekelijkse, maandelijkse planning?*
32.	*COMPUTE – RESERVERINGSMECHANISME:* *Biedt de cloud aanbieder enige mogelijkheid om extra computing capaciteit te reserveren voor de toekomst (d.w.z. 1 jr, 2 jr, 3 jr, enz.)?*
33.	*COMPUTE – LINUX-BESTURINGSSYSTEEM:* *Ondersteunt de cloud aanbieder de laatste twee langetermijnondersteunde versies van ten minste één Enterprise Linux distributie (zoals Red Hat, SUSE) en één veelgebruikte gratis Linux distributie (zoals Ubuntu, CentOS en Debian)?*
34.	*COMPUTE – WINDOWS-BESTURINGSSYSTEEM:* *Ondersteunt de cloud aanbieder de laatste twee grote Windows Server versies (Windows Server 2017 en Windows Server 2016)?*

35.	*COMPUTE – LICENTIEOVERDRAAGBAARHEID:* *Biedt de cloud aanbieder draagbaarheid en ondersteuning voor licenties?* • *Zo ja, vermeld dan de softwareleverancier, de namen van de software, de uitgaven en de versies.*
36.	*COMPUTE – SERVICELIMIETEN:* *Heeft de cloud aanbieder beperkingen (d.w.z. servicelimieten) ten aanzien van het bovenstaande compute gedeelte?* *Voorbeeld:* *Maximaal aantal instances per account* *Maximaal aantal specifieke hosts per account* *Maximaal aantal gereserveerde internetprotocol (IP)-adressen*

3.2 Netwerken

	Vereiste
1.	*NETWERKEN – VIRTUELE NETWERKEN:* *Ondersteunt de cloud aanbieder de mogelijkheid om een logisch, geïsoleerd virtueel netwerk te creëren dat het eigen netwerk van een bedrijf in de cloud vertegenwoordigt?*
2.	*NETWERKEN – CONNECTIVITEIT VOOR DEZELFDE REGIO:* *Ondersteunt de cloud aanbieder het verbinden van twee virtuele netwerken binnen dezelfde regio om verkeer tussen deze netwerken te routeren met behulp van privé internetprotocol (IP)-adressen?*
3.	*NETWERKEN – CONNECTIVITEIT MET ANDERE REGIO'S:* *Ondersteunt de cloud aanbieder het verbinden van twee virtuele netwerken tussen verschillende regio's om verkeer tussen deze netwerken te routeren met behulp van privé internetprotocol (IP)-adressen?*
4.	*NETWERKEN – PRIVÉ-SUBNET:* *Biedt de cloud aanbieder de mogelijkheid om volledig geïsoleerde (privé) virtuele netwerken en subnetten te creëren waar instances zonder openbaar internetprotocol (IP)-adres of internetrouting kunnen worden aangeboden?*
5.	*NETWERKEN – ADRESBEREIK VIRTUEEL NETWERK:* *Ondersteunt de cloud aanbieder internetprotocol (IP)-adresbereiken die in het verzoek om commentaar (RFC) 1918 zijn gespecificeerd, alsook openbaar te routeren klassenloze interdomein routering (CIDR) blokken?*
6.	*NETWERKEN – MEERDERE PROTOCOLLEN:* *Ondersteunt de cloud aanbieder meerdere protocollen, waaronder transmissiecontroleprotocol (TCP), gebruikersdatagramprotocol (UDP) en internetcontroleberichtprotocol (ICMP)?*
7.	*NETWERKEN – AUTOMATISCHE TOEWIJZING VOOR IP-ADRESSEN:* *Ondersteunt de cloud aanbieder de mogelijkheid om automatisch openbare internetprotocollen (IP-adressen) toe te wijzen aan instances?*
8.	*NETWERKEN – GERESERVEERDE STATISCH IP-ADRESSEN:* *Ondersteunt de cloud aanbieder IP-adressen (Internet Protocol) die zijn gekoppeld aan een gebruikersaccount, en niet aan een bepaalde instance? Het IP-adres moet aan het account verbonden blijven totdat het expliciet wordt vrijgegeven.*

9.	*NETWERK – IPV6 ONDERSTEUNING:* *Ondersteunt de cloud aanbieder Internetprotocol versie 6 (IPv6) op gateway- of instance niveau en wordt deze functionaliteit blootgesteld aan gebruikers?*
10.	*NETWERKEN – MEERDERE IP-ADRESSEN PER NIC:* *Ondersteunt de cloud aanbieder de mogelijkheid om een primair en een secundair internetprotocol (IP)-adres toe te wijzen aan een netwerkinterfacekaart (NIC) die aan een bepaalde instance is gekoppeld?*
11.	*NETWERKEN – MEERDERE NIC'S:* *Ondersteunt de cloud aanbieder de mogelijkheid om meerdere netwerkinterfacekaarten (NIC's) toe te wijzen aan een bepaalde instance?*
12.	*NETWERKEN – NIC EN IP MOBILITEIT:* *Ondersteunt de cloud aanbieder de mogelijkheid om netwerk-interfacekaarten (NIC's) en internetprotocol (IP)-adressen tussen instances te verplaatsen?*
13.	*NETWERKEN – SR-IOV ONDERSTEUNING:* *Ondersteunt de cloud aanbieder mogelijkheden zoals single root input/output virtualisatie (SR-IOV) voor hogere prestaties (d.w.z. pakketten per seconde - PPS), lagere latency en lagere interferentie?*
14.	*NETWERKEN – FILTEREN INKOMEND VERKEER:* *Ondersteunt de cloud aanbieder het toevoegen of verwijderen van regels die van toepassing zijn op inkomend verkeer (ingress) in instances?*
15.	*NETWERKEN – FILTEREN UITGAAND VERKEER:* *Ondersteunt de cloud aanbieder het toevoegen of verwijderen van regels die van toepassing zijn op uitgaand verkeer (egress) dat afkomstig is van instances?*
16.	*NETWERKEN – ACL:* *Biedt de cloud aanbieder toegangscontrolelijsten (ACL'en) aan om inkomend en uitgaand verkeer naar subnetten te controleren?*
17.	*NETWERKEN – STROOMLOGBOEKONDERSTEUNING* *Biedt de cloud aanbieder de mogelijkheid om netwerkverkeerstroomlogboeken vast te leggen?*
18.	*NETWERKEN – NAT:* *Biedt de cloud aanbieder een netwerk-adresvertaling (NAT) beheerde gateway dienst om instances in een privénetwerk in staat te stellen verbinding te maken met internet of andere cloud services, maar dat voorkomt dat internet verbinding met die instances tot stand brengt?*
19.	*NETWERKEN – BRON/BESTEMMINGSCONTROLE:* *Biedt de cloud aanbieder de mogelijkheid om de bron/bestemmingscontrole op de netwerkinterfacekaarten (NIC's) uit te schakelen?*
20.	*NETWERKEN – VPN-ONDERSTEUNING:* *Ondersteunt de cloud aanbieder een VPN connectiviteit (Virtual Private Network) tussen de cloud aanbieder en het datacenter van de gebruiker?*
21.	*NETWERKEN – VPN-TUNNELS:* *Ondersteunt de cloud aanbieder meerdere VPN verbindingen (Virtual Private Network) per virtueel netwerk?*

22.	*NETWERKEN – IPSEC VPN ONDERSTEUNING:* *Geeft de cloud aanbieder gebruikers toegang tot cloud services via een een IPsec (internetprotocol security) VPN tunnel (virtual private network) of SSL (secure sockets layer) VPN tunnel (virtual private network) over het openbare internet?*
23.	*NETWERKEN – BGP ONDERSTEUNING:* *Maakt de cloud aanbieder gebruik van het border gateway protocol (BGP) om failover over IPsec (internetprotocol security) VPN tunnels (virtual private network) te verbeteren?*
24.	*NETWERKEN – EIGEN SPECIFIEKE CONNECTIVITEIT* *Biedt de cloud aanbieder een directe, privéconnectiviteitsdienst tussen de locaties van de cloud aanbieder en de datacenter-, kantoor- of colocatie omgeving van een gebruiker die grote en snelle gegevensoverdracht mogelijk maakt?*
25.	*NETWERKEN – FRONT-END LOADBALANCER:* *Biedt de cloud aanbieder een front-end (internetgeoriënteerde) loadbalancer dienst aan die verzoeken van klanten via het internet opvangt en deze verzoeken verdeelt over instances die bij de loadbalancer zijn geregistreerd?*
26.	*NETWERKEN – BACK-END LOADBALANCER:* *Biedt de cloud aanbieder een back-end (privé) loadbalancing service die verkeer routeert naar instances die worden gehost in privé subnetten?*
27.	*NETWERKEN – LAYER 7 LOADBALANCER:* *Biedt de cloud aanbieder een Layer 7 (Hypertext Transfer Protocol - HTTP) loadbalancer service die netwerkverkeer over meerdere instances kan verdelen?*
28.	*NETWERKEN – LAYER 4 LOADBALANCER:* *Biedt de cloud aanbieder een Layer 4 (transmission control protocol - TCP) loadbalancer service die netwerkverkeer over meerdere instances kan verdelen?*
29.	*NETWERKEN – SESSIE-AFFINITEIT VOOR LOADBALANCERS:* *Biedt de cloud aanbieder een loadbalancing dienst die sessie affiniteit ondersteunt?*
30.	*NETWERKEN – DNS-GEBASEERDE LOADBALANCING:* *Biedt de cloud aanbieder een loadbalancing dienst aan die in staat is om verkeer te loadbalancen naar instances die gehost worden in meerdere hosts die tot één domein behoren?*
31.	*NETWERKEN – LOADBALANCER LOGBOEKEN:* *Biedt de cloud aanbieder logboeken aan die gedetailleerde informatie bevatten over alle verzoeken die naar een loadbalancer worden gestuurd?*
32.	*NETWERKEN – DNS:* *Biedt de cloud aanbieder een zeer beschikbare en schaalbare DNS dienst (Domain Name System) aan?*
33.	*NETWERKEN – OP LATENCY GEBASEERDE DNS ROUTERING:* *Biedt de cloud aanbieder een DNS dienst (Domain Name System) aan die routering op basis van latency ondersteunt (d.w.z. DNS service reageert op DNS query's met de middelen die de beste latency bieden)?*
34.	*NETWERKEN – GEO-GEBASEERDE DNS ROUTERING:* *Biedt de cloud aanbieder een DNS dienst (Domain Name System) die geografisch gebaseerde routering ondersteunt (d.w.z. dat de DNS dienst reageert op DNS query's op basis van de geografische locatie van gebruikers)?*

35.	*NETWERKEN – FAILOVER-GEBASEERDE DNS ROUTERING:* *Biedt de cloud aanbieder een DNS dienst (Domain Name System) die failover-gebaseerde routering ondersteunt (d.w.z. dat de DNS-dienst DNS-query's doorstuurt naar de bron die op dat moment actief is, terwijl een tweede bron wacht en alleen actief wordt in het geval van een storing in de primaire bron)?*
36.	*NETWERKEN – DOMEINREGISTRATIEDIENST:* *Biedt de cloud aanbieder domeinnaamregistratiediensten aan (d.w.z. dat gebruikers beschikbare domeinnamen kunnen zoeken en registreren)?*
37.	*NETWERKEN – DNS STATUSCONTROLES:* *Biedt de cloud aanbieder een DNS dienst (Domain Name System) aan die gebruik maakt van statuscontroles om de status en prestaties van middelen te bewaken?*
38.	*NETWERKEN – DNS EN LOAD BALANCING INTEGRATIE:* *Biedt de cloud aanbieder een DNS dienst (Domain Name System) aan die integreert met de loadbalancer van de cloud aanbieder?*
39.	*NETWERK – VISUELE EDITOR:* *Biedt de cloud aanbieder een tool waarmee gebruikers een beleid voor verkeersbeheer kunnen opbouwen?*
40.	*CONTENT DELIVERY NETWORK (CDN):* *Biedt de cloud aanbieder een CDN service (content delivery network) om content met lage latency en hoge gegevensoverdrachtsnelheden te verdelen?*
41.	*NETWERKEN – CDN CACHE VERVALPERIODE:* *Biedt de cloud aanbieder een content delivery network (CDN) dienst die het mogelijk maakt om een object uit de edge caches te verwijderen voordat het afloopt, met inbegrip van functies zoals het ongeldig maken van objecten en objectversiebeheer?*
42.	*NETWERKEN – CDN EXTERNE OORSPRONG:* *Biedt de cloud aanbieder een content delivery network (CDN) dienst aan die een aangepaste oorsprong ondersteunt, oftewel een HTTP-server (Hypertext Transfer Protocol)?*
43.	*NETWERKEN – CDN OPTIMALISATIE:* *Biedt de cloud aanbieder een content delivery network (CDN) service met gedetailleerde controle voor het configureren van meerdere origin servers en caching eigenschappen voor verschillende gelijkmatige bron locators (URL's)?*
44.	*NETWERKEN – CDN GEOGRAFISCH BEPERKT:* *Biedt de cloud aanbieder een content delivery network (CDN) dienst aan die geografische beperking ondersteunt, d.w.z. dat gebruikers in specifieke geografische gebieden geen toegang hebben tot content?*
45.	*NETWERKEN – CDN TOKENS:* *Biedt de cloud aanbieder een content delivery network (CDN) dienst aan die ondertekende gelijkmatige resource locators (URL's) ondersteunt, die doorgaans aanvullende informatie bevatten zoals vervaldatum/tijd om gebruikers meer controle te geven over de toegang tot hun content?*
46.	*NETWERKEN – CDN CERTIFICATEN:* *Biedt de cloud aanbieder een content delivery network (CDN) dienst die aangepaste SSL-certificaten (Secure Sockets Layer) ondersteunt om content veilig te leveren via HTTPS (Hypertext Transfer Protocol Secure) vanaf de edgelocaties?*
47.	*NETWERKEN – CDN CACHE MET MEERDERE LAGEN* *Biedt de cloud aanbieder een CDN service (content delivery network) die gebruikmaakt van een cache benadering met meerdere lagen met het gebruik van regionale edge caches om de latency te verminderen?*

48.	***NETWERKEN – CDN COMPRESSIE:*** *Biedt de cloud aanbieder een content delivery network (CDN) dienst aan die bestandscompressie ondersteunt?*
49.	***NETWERKEN – CDN GECODEERDE UPLOADS:*** *Biedt de cloud aanbieder een content delivery network (CDN) dat gebruikers in staat stelt om hun gevoelige gegevens veilig te uploaden op een manier dat dergelijke informatie alleen kan worden bekeken door bepaalde componenten en diensten in de oorspronkelijke infrastructuur van de gebruiker?*
50.	***NETWERKEN – EINDPUNTEN:*** *Biedt de netwerkdienst van de cloud aanbieder gebruikers met eindpunten die in staat zijn om verkeer te routeren via de interne netwerkconnectiviteit van de provider (d.w.z. privé-connectiviteit) om de communicatiekosten te verlagen en de beveiliging van het verkeer te verbeteren?*
51.	***NETWERKEN – SERVICELIMIETEN:*** *Heeft de cloud aanbieder beperkingen (d.w.z. servicelimieten) ten aanzien van het bovenstaande netwerkgedeelte?* *Voorbeeld:* *Maximaal aantal virtuele netwerken per account* *Maximaal aantal virtuele netwerken* *Maximaal aantal subnetten per account* *Maximaal aantal loadbalancers per account* *Maximaal aantal vermeldingen in de toegangscontrolelijst (ACL)* *Maximaal aantal virtual private network (VPN) tunnels* *Maximaal aantal oorsprongen per distributie* *Maximaal aantal certificaten per loadbalancer*

3.3 Opslag

	Vereiste
1.	***BLOKOPSLAGSERVICE:*** *Biedt de cloud aanbieder opslagvolumes op blokniveau aan voor gebruik met compute instances?*
2.	***BLOKOPSLAG – IOPS:*** *Biedt de cloud aanbieder de mogelijkheid om een expliciet prestatiedoel of prestatieniveau aan te schaffen op blokopslagvolumes, zoals een bepaald aantal in-/uitvoerbewerkingen per seconde (IOP's) of megabytes per seconde (MB/S) doorvoer?*
3.	***BLOKOPSLAG – SOLID-STATE DRIVES:*** *Ondersteunt de cloud aanbieder SSD-back-ups (solid-state drive) met vertragingen van één cijfer in milliseconden?* • *Zo ja, wat is het maximum aantal SSD's dat per instance kan worden bevestigd?*
4.	***BLOKOPSLAG – SCHALING:*** *Biedt de cloud aanbieder gebruikers de mogelijkheid om de omvang van een bestaand blok opslagvolume te vergroten zonder een nieuw volume te hoeven leveren en de gegevens te kopiëren/verplaatsen?*
5.	***BLOKOPSLAG – SNAPSHOTS:*** *Heeft de cloud aanbieder snapshot capaciteit voor zijn blokopslagservice?*

6.	*BLOKOPSLAG – GEGEVENSVERWIJDERING:* *Ondersteunt de cloud aanbieder een volledige verwijdering van gegevens, zodat gegevens niet meer leesbaar of toegankelijk zijn voor onbevoegde gebruikers en/of derden?*
7.	*BLOKOPSLAG – ENCRYPTIE IN RUSTSTAND:* *Biedt de cloud aanbieder server-side encryptie van gegevens aan voor gegevens die zijn opgeslagen op hoeveelheden en de bijbehorende snapshots?* • *Zo ja, wat is het gebruikte cryptografische algoritme?*
8.	*OBJECTOPSLAGSERVICE:* *Biedt de cloud aanbieder veilige, duurzame en zeer schaalbare objectopslag voor het opslaan en ophalen van elke hoeveelheid gegevens van het web?*
9.	*OBJECTOPSLAG – NIET-FREQUENTE TOEGANG:* *Biedt de cloud aanbieder een lager kostenniveau voor de opslag van minder vaak gebruikte objecten en bestanden?*
10.	*OBJECTOPSLAG – LAGERE DUURZAAMHEID:* *Biedt de cloud aanbieder een gereduceerde redundantielaag waar een gebruiker niet-belangrijke gemakkelijk te reproduceren objecten kan opslaan tegen een lagere prijs?*
11.	*OBJECTOPSLAG – MINDER FREQUENTE TOEGANG:* *Biedt de cloud aanbieder een niveau voor minder vaak geraadpleegde gegevens, maar waarbij toch een snelle toegang is vereist?*
12.	*OBJECTOPSLAG – GELAAGDHEID VAN OBJECTEN:* *Biedt de cloud aanbieder de mogelijkheid om een object gelaagd op te slaan, d.w.z. de mogelijkheid om de overgang tussen objectopslagklassen of -niveaus aan te bevelen op basis van de toegangsfrequentie?*
13.	*OBJECTOPSLAG – LEVENSCYCLUSBEHEER:* *Ondersteunt de cloud aanbieder het beheer van de levenscyclus van een object door gebruik te maken van een levenscycusconfiguratie, die bepaalt hoe objecten worden beheerd tijdens hun levensduur, van creatie tot verwijdering?*
14.	*OBJECTOPSLAG – BELEIDSGESTUURD BEHEER:* *Biedt de cloud aanbieder de mogelijkheid om beleid te maken en te gebruiken voor het beheer van opgeslagen gegevens, de levenscyclus ervan en de gelaagde instellingen?*
15.	*OBJECTOPSLAG - LOCATIE EN TIJDGEBASEERD BELEID:* *Biedt de cloud aanbieder gebruikers de mogelijkheid om beleid te maken dat de toegang tot de gegevens kan beperken op basis van de locatie van de gebruiker en het tijdstip van de aanvraag?*
16.	*OBJECTOPSLAG – WEBSITEHOSTING:* *Ondersteunt de cloud aanbieder het hosten van statische websites uit zijn objectopslagservice?*
17.	*OBJECTOPSLAG – ENCRYPTIE IN RUSTSTAND:* *Ondersteunt de cloud aanbieder server-side encryptie (SSE) van gegevens in ruststand, waarbij de cloud aanbieder de encryptiecodes beheert?* • *Zo ja, wat is het gebruikte cryptografische algoritme?*
18.	*OBJECTOPSLAG – ENCRYPTIE MET GEBRUIKERSSLEUTELS:* *Biedt de cloud aanbieder mogelijkheden voor server-side encryptie (SSE) met behulp van door de klant verstrekte cryptografische sleutels?*

19.	*OBJECTOPSLAG – SLEUTELBEHEERSERVICE:* *Ondersteunt de cloud aanbieder server-side encryptie (SSE) met behulp van een sleutelbeheerservice die encryptiesleutels creëert, het beleid definieert dat bepaalt hoe sleutels kunnen worden gebruikt, en het sleutelgebruik controleert om aan te tonen dat ze correct worden gebruikt?*
20.	*OBJECTOPSLAG – HOOFDSLEUTEL KLANTZIJDE:* *Biedt de cloud aanbieder gebruikers de mogelijkheid om de controle over de encryptiesleutels te behouden en de encryptie/decryptie van objecten aan de klantzijde te voltooien?*
21.	*OBJECTOPSLAG – STERKE SAMENHANG:* *Ondersteunt de cloud aanbieder read-after-write -samenhang voor PUT-bewerkingen voor nieuwe objecten?*
22.	*OBJECTOPSLAG – LOCATIE VAN GEGEVENS* *Biedt de cloud aanbieder een sterk regionaal isolement, zodat objecten die in een regio zijn opgeslagen nooit de regio verlaten, tenzij de gebruiker ze expliciet naar een andere regio verplaatst?*
23.	*OBJECTOPSLAG – REPLICATIE:* *Biedt de cloud aanbieder een regio-overschrijdende replicatiefunctie waarmee objecten automatisch worden gerepliceerd in door de gebruiker geselecteerde regio's?*
24.	*OBJECTEOPSLAG – VERSIEBEHEER:* *Ondersteunt de cloud aanbieder versiebeheer, d.w.z. de mogelijkheid om meerdere versies van een object op te slaan en te onderhouden?*
25.	*OBJECTOPSLAG – MARKERING HERSTELLEN:* *Staat de cloud aanbieder toe dat een gebruiker een item als niet verwijderbaar markeert?*
26.	*OBJECTOPSLAG – MFA VERWIJDERING:* *Ondersteunt de cloud aanbieder multi-factor authentication (MFA) voor verwijderingsbewerkingen als extra beveiligingsoptie?*
27.	*OBJECTOPSLAG – MEERDELIGE UPLOAD:* *Staat de cloud aanbieder het uploaden van een object als een set onderdelen toe, waarbij elk onderdeel een aaneengesloten deel van de gegevens van het object is en deze objecten afzonderlijk en in elke volgorde kunnen worden geüpload?*
28.	*OBJECTOPSLAG – TAGS:* *Biedt de cloud aanbieder de mogelijkheid om veranderlijke, dynamische tags op objectniveau te creëren en te verbinden?*
29.	*OBJECTOPSLAG – KENNISGEVINGEN:* *Biedt de cloud aanbieder de mogelijkheid om meldingen te versturen wanneer bepaalde gebeurtenissen op objectniveau plaatsvinden (d.w.z. toevoegingen/verwijderingen)?*
30.	*OBJECTOPSLAG – LOGBOEKEN:* *Biedt de cloud aanbieder de mogelijkheid om auditlogboeken te genereren die details bevatten over een enkel toegangsverzoek, zoals de aanvrager, het tijdstip van het verzoek, de actie van het verzoek, de responsstatus en de foutcode?*
31.	*OBJECTOPSLAG – INVENTARISATIE VOOR OBJECTEN:* *Biedt de cloud aanbieder de mogelijkheid om objecten te inventariseren zodat gebruikers snel objecten en hun status kunnen visualiseren, waardoor ze snel objecten met openbare toegang kunnen herkennen?*

32.	*OBJECTOPSLAG - INVENTARISATIE VOOR METAGEGEVENS:* *Biedt de cloud aanbieder de mogelijkheid om objecten te inventariseren, zodat gebruikers de mogelijkheid hebben om snel de metagegevens van objecten te visualiseren?*
33.	*OBJECTOPSLAG – OPTIMALISATIE VAN UPLOADS:* *Heeft de cloud aanbieder de mogelijkheid om gegevens van edgelocaties naar de opslagdienst te routeren via een geoptimaliseerd netwerktraject?*
34.	*OBJECTOPSLAG – QUERY MOGELIJKHEID:* *Biedt de cloud aanbieder gebruikers de mogelijkheid om zijn objectopslagdienst te bevragen door gebruik te maken van bepalingen in gestructureerde query taal (SQL)?*
35.	*OBJECTOPSLAG – SUBSET OPHALEN:* *Biedt de cloud aanbieder gebruikers de mogelijkheid om slechts een deel van de gegevens van een object op te halen door gebruik te maken van eenvoudige uitdrukkingen in gestructureerde query taal (SQL)?*
36.	*BESTANDSOPSLAGSERVICE:* *Biedt de cloud aanbieder een eenvoudige en schaalbare bestandsopslagservice om te gebruiken met compute instances in de cloud?*
37.	*BESTANDSOPSLAG – REDUNDANTIE:* *Slaat de cloud aanbieder de objecten van het bestandssysteem (d.w.z. de directory, het bestand en de link) redundant op in meerdere datacenters of faciliteiten om een hoger niveau van beschikbaarheid en duurzaamheid te bereiken?*
38.	*BESTANDSOPSLAG – GEGEVENSVERWIJDERING:* *Ondersteunt de cloud aanbieder een volledige verwijdering van bestandsopslaggegevens, zodat deze niet meer leesbaar of toegankelijk zijn voor onbevoegde gebruikers of derden?*
39.	*BESTANDSOPSLAG – HOGE BESCHIKBAARHEID:* *Biedt het beheerde bestandssysteem van de cloud aanbieder een hoge mate van beschikbaarheid?*
40.	*BESTANDSOPSLAG – NFS:* *Ondersteunt de cloud aanbieder het protocol van het network file system (NFS)?*
41.	*BESTANDSOPSLAG – SMB:* *Ondersteunt de cloud aanbieder het SMB-protocol (Server Message Block)?*
42.	*BESTANDSOPSLAG – ENCRYPTIE IN RUSTSTAND:* *Ondersteunt de bestandsopslagservice van de cloud aanbieder encryptie van gegevens in ruststand?*
43.	*BESTANDSOPSLAG – ENCRYPTIE IN OVERDRACHT:* *Ondersteunt de bestandsopslagdienst van de cloud aanbieder de encryptie van gegevens in overdracht?*
44.	*BESTANDSOPSLAG – GEGEVENSMIGRATIETOOL:* *Biedt de cloud aanbieder een gegevensmigratietool om gebruikers in staat te stellen gegevens te verplaatsen van systemen op locatie naar het cloud-gebaseerde bestandssysteem?*
45.	*ARCHIEFOPSLAGSERVICE:* *Biedt de cloud aanbieder een zeer goedkope opslagservice die gericht is op het archiveren van minder vaak geraadpleegde en bijna onveranderlijke objecten en bestanden?*
46.	*ARCHIEFOPSLAG – FOUTTOLERANTIE:* *Biedt de architectuur van de cloud aanbieder een fouttolerantie voor zijn archiefopslagservice?*

47.	***ARCHIEFOPSLAG – ONVERANDERLIJKHEID:*** *Ondersteunt de cloud aanbieder de onveranderlijkheid van de gearchiveerde objecten en bestanden?*
48.	***ARCHIEFOPSLAG – WORM:*** *Biedt de cloud aanbieder WORM (Write Once Read Many) -mogelijkheden?*
49.	***ARCHIEFOPSLAG – SUBSET OPHALEN:*** *Biedt de cloud aanbieder gebruikers de mogelijkheid om slechts een deel van de gegevens van een gearchiveerd object op te halen door gebruik te maken van eenvoudige uitdrukkingen in structured query language (SQL)?*
50.	***ARCHIEFOPSLAG – SNEL OPHALEN:*** *Biedt de cloud aanbieder gebruikers meerdere opties voor het ophalen van gegevens met verschillende kosten en ophaaltijden?*
51.	***ARCHIEFOPSLAG – ENCRYPTIE IN RUSTSTAND:*** *Ondersteunt de archiefopslagservice van de cloud aanbieder encryptie van gegevens in ruststand?*
52.	***OPSLAG – SERVICELIMIETEN:*** *Heeft de cloud aanbieder beperkingen (d.w.z. servicelimieten) ten aanzien van het bovenstaande gedeelte over opslag?* *Voorbeeld:* *Maximale volumegrootte* *Maximaal aantal drives dat aan een instance is gekoppeld* *Maximale ingangs-/uitgangsbewerkingen per seconde (IOPS)* *Maximale objectgrootte* *Maximaal aantal objecten per opslagaccount* *Maximaal aantal snapshots*

4. Beheer

	Vereiste
1.	***BEHEER – GEBRUIKERS EN GROEPEN:*** *Biedt de cloud aanbieder een dienst aan om gebruikers en groepen gebruikers van de infrastructuur en middelen te creëren en te beheren?*
2.	***BEHEER – WACHTWOORD RESET:*** *Staat de cloud aanbieder gebruikers toe om hun eigen wachtwoord op een zelfstandige manier opnieuw in te stellen?*
3.	***BEHEER – MACHTIGINGEN:*** *Biedt de cloud aanbieder de mogelijkheid om rechten toe te voegen aan gebruikers en groepen op bronniveau?*
4.	***BEHEER – TIJDELIJKE MACHTIGINGEN:*** *Biedt de cloud aanbieder de mogelijkheid om machtigingen te maken die geldig zijn voor een specifiek tijdsinterval?*

5.	***BEHEER – TIJDELIJKE AANMELDINGSGEGEVENS:*** *Biedt de cloud aanbieder gebruikers de mogelijkheid om tijdelijke beveiligingsreferenties te maken en te verstrekken aan vertrouwde gebruikers die zijn geconfigureerd om overal van een paar minuten tot enkele uren mee te gaan?*
6.	***BEHEER – TOEGANGSCONTROLE*** *Biedt de cloud aanbieder gedetailleerde toegangscontroles tot zijn infrastructuurmiddelen?* • *Zo ja, welke voorwaarden kunnen door deze controles worden gebruikt (d.w.z. tijdstip van de dag, oorspronkelijk IP-adres, enz.)?*
7.	***BEHEER – INGEBOUWD BELEID:*** *Bevat de infrastructuur van de cloud aanbieder een geïntegreerd toegangsbeheerbeleid dat aan gebruikers en groepen kan worden gekoppeld?*
8.	***BEHEER – AANGEPAST BELEID:*** *Maakt de infrastructuur van de cloud aanbieder het mogelijk om een beleid voor toegangscontrole aan te maken en aan te passen aan gebruikers en groepen?*
9.	***BEHEER – BELEIDSSIMULATOR:*** *Biedt de cloud aanbieder een mechanisme om de effecten van het toegangscontrolebeleid te testen alvorens dit beleid in productie te nemen?*
10.	***BEHEER – CLOUD MFA:*** *Ondersteunt de cloud aanbieder het gebruik van multi-factor authenticatie (MFA) als extra laag van toegangscontrole en verificatie voor zijn infrastructuur?*
11.	***BEHEER – SERVICELIMIETEN:*** *Heeft de cloud aanbieder beperkingen (d.w.z. servicelimieten) ten aanzien van het bovenstaande beheer gedeelte?* *Voorbeeld:* *Maximaal aantal gebruikers* *Maximaal aantal groepen* *Maximaal aantal beheerde beleidslijnen*

5. Beveiliging

	Vereiste
1.	***BEVEILIGING – ACHTERGRONDCONTROLES:*** *Zijn alle medewerkers van de cloud aanbieder die toegang hebben tot de service infrastructuur (fysiek of niet-fysiek) onderworpen aan achtergrondcontroles?*
2.	***BEVEILIGING – FYSIEKE TOEGANG:*** *Beperkt de cloud aanbieder het personeel om toegang te krijgen tot de service infrastructuur, tenzij er sprake is van een specifiek trouble ticket, wijzigingsverzoek of een vergelijkbare formele autorisatie?*
3.	***BEVEILIGING – TOEGANGSLOGBOEKEN:*** *Registreert de cloud aanbieder de toegang van het personeel tot zijn infrastructuur, waarbij deze toegang altijd wordt vastgelegd en de logboeken minimaal 90 dagen worden bewaard?*

4.	*BEVEILIGING – HOST LOGINS:* *Beperkt de cloud aanbieder het personeel van de aanbieder om in te loggen op compute hosts, en in plaats daarvan alle taken automatiseert die worden uitgevoerd op compute hosts waar de inhoud van deze geautomatiseerde taken wordt vastgelegd, waarbij de logboeken minimaal 90 dagen worden bewaard?*
5.	*BEVEILIGING – CRYPTOGRAFISCHE SLEUTELS:* *Biedt de cloud aanbieder een dienst aan om de cryptografische sleutels te creëren en te controleren die worden gebruikt om gebruikersgegevens te versleutelen?*
6.	*BEVEILIGING – BEHEER TOEGANGSSLEUTELS:* *Biedt de cloud aanbieder de mogelijkheid om te identificeren wanneer een toegangssleutel voor het laatst is gebruikt, oude sleutels te roteren en inactieve gebruikers te verwijderen?*
7.	*BEVEILIGING – DOOR DE KLANT VERSTREKTE SLEUTELS:* *Staat de cloud aanbieder gebruikers toe om sleutels te importeren van de eigen sleutelbeheerinfrastructuur naar de sleutelbeheerdienst van de cloud aanbieder?*
8.	*BEVEILIGING – INTEGRATIE DIENST CRYPTOGRAFISCHE SLEUTELS:* *Is de sleutelbeheerdienst van de cloud aanbieder geïntegreerd met andere cloud services om gegevens te kunnen versleutelen?*
9.	*BEVEILIGING – HSM:* *Biedt de cloud aanbieder speciale hardware-beveiligingsmodules (HSM), d.w.z. hardware apparaten die zorgen voor veilige opslag van sleutels en cryptografische bewerkingen binnen een sabotagebestendige hardwaremodule?*
10.	*BEVEILIGING – DUURZAAMHEID CRYPTOGRAFISCHE SLEUTELS:* *Ondersteunt de cloud aanbieder de duurzaamheid van sleutels, inclusief het opslaan van meerdere kopieën, zodat sleutels beschikbaar zijn wanneer dat nodig is?*
11.	*BEVEILIGING – SSO:* *Biedt de cloud aanbieder een beheerde SSO-service (single sign-on) waarmee gebruikers de toegang tot meerdere accounts en bedrijfsapplicaties centraal kunnen beheren?*
12.	*BEVEILIGING – CERTIFICATEN:* *Biedt de cloud aanbieder een managed service voor de levering, het beheer en de inzet van secured sockets layer (SSL)/transport layer security (TLS) certificaten?*
13.	*BEVEILIGING – VERLENGING CERTIFICATEN:* *Faciliteert de certificaatbeheerdienst van de cloud aanbieder de verlenging van de certificaten?*
14.	*BEVEILIGING – WILDCARD CERTIFICATEN:* *Ondersteunt de certificaatbeheerdienst van de cloud aanbieder het gebruik van wildcard certificaten?*
15.	*BEVEILIGING – CERTIFICAATAUTORITEIT:* *Functioneert de certificaatbeheerdienst van de cloud aanbieder ook als een certificaatautoriteit (CA)?*
16.	*BEVEILIGING – ACTIVE DIRECTORY:* *Biedt de cloud aanbieder een beheerde Microsoft active directory service (AD) aan in de cloud?*
17.	*BEVEILIGING – ACTIVE DIRECTORY OP LOCATIE:* *Ondersteunt de beheerde Microsoft active directory service (AD) van de cloud aanbieder de integratie met Microsoft active directory (AD) op locatie?*

18.	***BEVEILIGING – LDAP:*** *Ondersteunt de beheerde Microsoft active directory service (AD) van de cloud aanbieder het Lightweight Directory Access Protocol (LDAP)?*
19.	***BEVEILIGING – ACTIVE DIRECTORY:*** *Ondersteunt de beheerde Microsoft Active Directory service (AD) van de cloud aanbieder de Security Assertion Markup Language (SAML)?*
20.	***BEVEILIGING – GEGEVENSBEHEER:*** *Biedt de cloud aanbieder een beheerde dienst die gebruikers helpt om referenties zoals API-sleutels (Application Programming Interface), referenties van databases en andere geheimen eenvoudig te roteren, te beheren en op te halen?*
21.	***BEVEILIGING – WAF:*** *Biedt de cloud aanbieder een firewall voor webapplicaties (WAF) die helpt bij het beschermen van webapplicaties tegen veelvoorkomende webactiviteiten die de beschikbaarheid van applicaties kunnen beïnvloeden, de beveiliging in gevaar kunnen brengen of buitensporige middelen kunnen verbruiken?*
22.	***BEVEILIGING – DDOS:*** *Biedt de cloud aanbieder een dienst aan ter bescherming tegen veelvoorkomende DDoS-aanvallen (Distributed Denial of Service) op het netwerk en de transportlaag, en de mogelijkheid om aangepaste regels te schrijven om geavanceerde aanvallen op de applicatielaag te beperken?*
23.	***BEVELIGING – BEVEILIGINGSAANBEVELINGEN:*** *Biedt de cloud aanbieder een dienst aan om potentiële kwetsbaarheden in applicaties en middelen automatisch te beoordelen?*
24.	***BEVELIGING – THREAT DETECTION:*** *Biedt de cloud aanbieder een beheerde threat detection service?*
25.	***BEVEILIGING – SERVICE LIMITS:*** *Heeft de cloud aanbieder beperkingen (d.w.z. service limits) ten aanzien van het bovenstaande gedeelte over beveiliging?* *Voorbeeld:* *Maximaal aantal hoofdsleutels van de klant* *Maximaal aantal hardware beveiligingsmodules (HSM's)*

6. Compliance

Onderstaande lijst is slechts ter illustratie en moet niet worden beschouwd als een uitputtende opsomming van de certificeringen en normen die van toepassing zouden kunnen zijn op cloud services.

Geef aan aan welke reeks van internationale en sectorspecifieke navelingsnormen de cloud aanbieder heeft voldaan:

Certificeringen/Attesten	*Wet- en regelgeving en privacy*	*Compliance/FrameworksFramework*
☐ C5 (Duitsland)	*☐ EU gegevensbeschermingsrichtlijn*	*☐ CDSA*
☐ CISPE gedragscode voor gegevensbescherming	*☐ EU-modelbepalingen*	

☐ *CNDCP (Climate Neutral Data Centre Pact)*		
☐ *DIACAP*	☐ *FERPA*	☐ *CIS*
☐ *DoD SRG niveaus 2 en 4*	☐ *AVG (GDPR)*	☐ *Criminal Justice Info. Service (CJIS)*
☐ *FedRAMP*	☐ *GLBA*	☐ *CSA*
☐ *FIPS 140-2*	☐ *HIPAA*	☐ *EU-VS Privacy Schild*
☐ *HDS (Frankrijk, Gezondheidszorg)*	☐ *HITECH*	☐ *EU Safe Harbor*
☐ *ISO 9001*	☐ *IRS 1075*	☐ *FISC*
☐ *ISO 27001*	☐ *ITAR*	☐ *FISMA*
☐ *ISO 27017*	☐ *PDPA - 2010 [Maleisië]*	☐ *G-Cloud [VK]*
☐ *ISO 27018*	☐ *PDPA– 2012 [Singapore]*	☐ *GxP (FDA CFR 21 Deel 11)*
☐ *IRAP [Australië]*	☐ *PIPEDA [Canada]*	☐ *ICREA*
☐ *MTCS Tier 3 [Singapore]*	☐ *Privacy Act [Australië]*	☐ *IT Grundschutz (Duitsland)*
☐ *PCI DSS Level 1*	☐ *Privacy Act [Nieuw-Zeeland]*	☐ *MARS – E*
☐ *SEC-regel 17-a-4(f)*	☐ *Spaanse DPA-autorisatie*	☐ *MITA 3.0*
☐ *SOC1/ISAE 3402*	☐ *U.K. DPA - 1988*	☐ *MPAA*
☐ *SOC2/SOC3*	☐ *VPAT/Section 508*	☐ *NIST*
☐ *SWIPO IaaS Code*		
		☐ *Uptime Institute Tiers*
		☐ *VK Cloud Security Principles*

Door gebruik te maken van de bovenstaande compliancerapporten kunnen overheidsorganisaties unieke aanbiedingen beoordelen aan de hand van geaccepteerde beveiligings-, compliance- en uitvoerende normen. Dergelijke rapporten kunnen laten zien dat de CISP, door de naleving ervan, voldoet aan de onderstaande controles op de werking van het datacenter, die vereist zijn van de openbare cloud service aanbieder. Door te eisen dat dergelijke verslagen worden nageleefd, hebben overheidsinstellingen de zekerheid dat de onderstaande controles worden uitgevoerd.

- *Gecontroleerde toegang: De CISP moet de fysieke toegang beperken tot die mensen die om een legitieme zakelijke reden op een locatie moeten zijn. Als de toegang wordt verleend, moet deze worden ingetrokken zodra de noodzakelijke werkzaamheden zijn voltooid.*
- *Toegang gecontroleerd en bewaakt: Het invoeren van de Perimeter Data Centre Layer moet een gecontroleerd proces zijn. De CISP moet voor ingangspoorten personeel, zoals beveiligingsbeambten en toezichthouders, in dienst*

hebben die via beveiligingscamera's functionarissen en bezoekers in de gaten houden. Wanneer goedgekeurde personen op locatie zijn, moeten zij een badge krijgen die een multi-factor authenticatie vereist en de toegang tot vooraf goedgekeurde gebieden beperkt.

- *CISP medewerkers van datacenters: Medewerkers van een CISP die routinematig toegang tot een datacenter nodig hebben, moeten toestemming krijgen voor relevante percelen van de faciliteit op basis van hun functie, waarbij de toegang regelmatig wordt gecontroleerd. Personeelslijsten moeten routinematig worden gecontroleerd door een toegangsmanager van de ruimte om er zeker van te zijn dat de autorisatie van elke medewerker nog steeds nodig is. Als een werknemer geen doorlopende bedrijfsbehoefte heeft in een datacenter, moet hij of zij het bezoekersproces doorlopen.*

- *Bewaking voor ongeoorloofde toegang: CISP's moeten voortdurend controleren op ongeoorloofde toegang tot de eigendommen van het datacenter, met behulp van videobewaking, inbraakdetectie en logboekbewakingssystemen. Ingangen moeten worden beveiligd met apparaten die alarm slaan als een deur wordt geforceerd of opengehouden.*

- *CISP Security Operations Centres houdt toezicht op de wereldwijde beveiliging: CISP Security Operations Centres moeten over de hele wereld gevestigd zijn en verantwoordelijk zijn voor het bewaken, testen en uitvoeren van beveiligingsprogramma's voor CISP datacenters. Zij moeten toezicht houden op het fysieke toegangsbeheer en de reactie op inbraakdetectie en tegelijkertijd de beveiligingsteams van de datacenters ter plaatse 24/7 wereldwijd ondersteunen; zij moeten voortdurend toezicht houden op activiteiten, zoals het volgen van toegangsactiviteiten, het intrekken van toegangsrechten en het beschikbaar zijn om te reageren op een mogelijk beveiligingsincident en dat analyseren.*

- *Toegangscontrole per laag: De toegang tot de infrastructuurlaag moet worden beperkt op basis van de bedrijfsbehoeften. Door het implementeren van een toegangscontrole per laag wordt het recht om elke laag in te voeren niet standaard toegekend. Toegang tot een bepaalde laag mag alleen worden verleend als er een specifieke behoefte bestaat om toegang te krijgen tot die specifieke laag.*

- *Het onderhoud van de apparatuur is een onderdeel van de reguliere werkzaamheden: CISP teams moeten diagnostiek uitvoeren op machines, netwerken en back-up apparatuur om ervoor te zorgen dat ze op het moment in orde zijn, en in geval van nood. Routinematige onderhoudscontroles van de apparatuur en voorzieningen van het datacenter dienen deel uit te maken van de reguliere werkzaamheden van het CISP datacenter.*

- *Back-up apparatuur klaar voor noodgevallen: Water, stroom, telecommunicatie en internetconnectiviteit moeten met redundantie worden ontworpen, zodat de CISP in geval van nood ononderbroken kan blijven functioneren. Elektrische stroomsystemen moeten zo worden ontworpen dat ze volledig redundant zijn, zodat in het geval van een storing ononderbroken stroomvoorzieningseenheden kunnen worden ingeschakeld voor bepaalde functies, terwijl de generatoren back-upstroom kunnen leveren voor de hele faciliteit. Mensen en systemen moeten de temperatuur en de vochtigheidsgraad bewaken en controleren om oververhitting te voorkomen, waardoor mogelijke storingen verder worden beperkt.*

- *Technologie en mensen werken samen voor extra beveiliging: Er moeten verplichte procedures zijn om toestemming te krijgen om de gegevenslaag te betreden. Dit omvat de beoordeling en goedkeuring van de toegangsaanvraag van een persoon door geautoriseerde personen. Intussen moeten threat en electronic intrusion detectiesystemen toezicht houden op geïdentificeerde dreigingen of verdachte activiteiten en deze automatisch in werking stellen. Als bijvoorbeeld een deur wordt vastgehouden of geforceerd wordt geopend, wordt er een alarm geactiveerd. Een CISP moet beveiligingscamera's inzetten en beeldmateriaal bewaren in overeenstemming met de wettelijke en compliancevoorschriften.*

- *Het voorkomen van fysieke en technologische indringing: Toegangspunten tot serverruimtes moeten worden versterkt met elektronische controleapparaten die een multi-factor authenticatie vereisen. Een CISP moet ook voorbereid zijn om technologische indringing te voorkomen. CISP servers moeten werknemers kunnen waarschuwen voor pogingen om gegevens te verwijderen. In het onwaarschijnlijke geval van een storing moet de server automatisch worden uitgeschakeld.*

- *Servers en media krijgen de nodige aandacht: Mediaopslagapparaten die worden gebruikt om klantgegevens op te slaan, moeten door de CISP worden geclassificeerd als belangrijk en dienovereenkomstig worden behandeld, als impactvol, gedurende hun gehele levenscyclus. De CISP zou strenge normen moeten hanteren voor het installeren, onderhouden en uiteindelijk vernietigen van de apparaten als ze niet meer bruikbaar zijn. Wanneer een opslagapparaat het einde van zijn levensduur heeft bereikt, stelt de CISP de media buiten gebruik met behulp van*

technieken die in NIST 800-88 zijn beschreven. Media die klantgegevens hebben opgeslagen, worden pas uit de CISP controle verwijderd als ze veilig zijn ontmanteld.

- *Externe auditors controleren de procedures en systemen van de CISP: De CISP moet worden gecontroleerd door externe auditors om datacenters te inspecteren, waarbij diep wordt gegraven om te bevestigen dat de CISP zich houdt aan de vastgestelde regels die nodig zijn voor het verkrijgen van de beveiligingscertificaten van de CISP. Afhankelijk van het complianceprogramma en de vereisten ervan, kunnen externe auditors CISP medewerkers interviewen over hoe zij omgaan met en zich ontdoen van media. Auditors kunnen ook beveiligingscamera's bekijken en ingangen en gangen in een datacenter observeren. En ze kunnen apparatuur onderzoeken zoals CISP elektronische toegangscontrole apparatuur en beveiligingscamera's.*

- *Voorbereid op het onverwachte: De CISP moet zich proactief voorbereiden op potentiële milieubedreigingen, zoals natuurrampen en brand. Het installeren van automatische sensoren en responsieve apparatuur zijn twee manieren waarop de CISP datacenters zal beschermen. Er moeten waterdetectie apparaten worden geïnstalleerd om medewerkers te waarschuwen voor problemen, aangezien automatische pompen werken om vloeistof te verwijderen en schade te voorkomen. Ook automatische branddetectie- en -bestrijdingsapparatuur vermindert het risico en kan CISP medewerkers en brandweerlieden op de hoogte brengen van een probleem.*

- *Hoge beschikbaarheid via meerdere beschikbaarheidszones: De CISP moet meerdere beschikbaarheidszones bieden voor een grotere fouttolerantie. Elke beschikbaarheidszone moet bestaan uit een of meer datacenters, die fysiek van elkaar gescheiden zijn en beschikken over redundante stroomvoorziening en netwerken. Beschikbaarheidszones dienen met elkaar verbonden te zijn met een snel, privé glasvezelnetwerk, om applicaties te ontwerpen die automatisch en zonder onderbreking tussen de beschikbaarheidszones heen en weer gaan.*

- *Simuleren van verstoringen en het meten van onze respons: De CISP moet een bedrijfscontinuïteitsplan hebben als leidraad voor het operationele proces, waarin wordt aangegeven hoe verstoringen als gevolg van natuurrampen kunnen worden voorkomen en verminderd, met gedetailleerde stappen die vóór, tijdens en na een gebeurtenis moeten worden genomen. Om het onverwachte te verminderen en voor te bereiden, moet de CISP het bedrijfscontinuïteitsplan regelmatig testen met oefeningen die verschillende scenario's simuleren. De CISP moet documenteren hoe zijn medewerkers en processen presteren, en vervolgens debriefen over de geleerde lessen en eventuele corrigerende maatregelen die nodig zijn om het responspercentage te verbeteren. CISP personeel moet worden getraind en klaar zijn om snel te herstellen van verstoringen, met een methodisch herstelproces om verdere stilstand als gevolg van fouten tot een minimum te beperken.*

- *Helpen de efficiëntiedoelstellingen te behalen: Naast het aanpakken van milieurisico's moet de CISP ook duurzaamheidsoverwegingen in het ontwerp van datacenters opnemen. De CISP zou details moeten verstrekken over zijn belofte om hernieuwbare energie te gebruiken voor zijn datacenters en informatie moeten verstrekken over hoe zijn klanten de koolstofuitstoot kunnen verminderen ten opzichte van hun eigen datacenters.*

- *Selectie van de locatie: Voorafgaand aan de keuze van een locatie moet de CISP een eerste milieu- en geografische beoordeling uitvoeren. De locaties van de datacenters moeten zorgvuldig worden geselecteerd om de milieurisico's, zoals overstromingen, extreem weer en seismische activiteit, te beperken. De CISP beschikbaarheidszones moeten zo worden gebouwd dat ze onafhankelijk zijn en fysiek van elkaar zijn gescheiden.*

- *Redundantie: Datacenters moeten worden ontworpen om te anticiperen op storingen en deze te tolereren met behoud van het service level. In geval van een storing moeten de geautomatiseerde processen het verkeer uit het getroffen gebied verplaatsen. Kernapplicaties moeten worden ingezet volgens een N+1-standaard, zodat er bij uitval van een datacenter voldoende capaciteit is om het verkeer naar de overige locaties te brengen.*

- *Beschikbaarheid: De CISP moet de belangrijke systeemonderdelen identificeren die nodig zijn om de beschikbaarheid van het systeem te handhaven en de service te herstellen in geval van een storing. Er moet een back-up worden gemaakt van essentiële systeemonderdelen op meerdere, geïsoleerde locaties. Elke locatie of beschikbaarheidszone moet zodanig zijn ontworpen dat deze onafhankelijk en met een hoge betrouwbaarheid kan functioneren. Beschikbaarheidszones dienen te worden aangesloten om applicaties in staat te stellen automatisch en zonder onderbreking van de ene naar de andere beschikbaarheidszone over te schakelen. Zeer veerkrachtige systemen, en dus ook de beschikbaarheid van diensten, zouden een functie moeten zijn van het systeemontwerp. Het ontwerp van datacenters met beschikbaarheidszones en datareplicatie moet CISP klanten in staat stellen om een extreem korte recovery time en recovery point objectives te bereiken, evenals de hoogste niveaus van beschikbaarheid van dienstverlening.*

- ***Capaciteitsplanning:*** *De CISP moet voortdurend toezicht houden op het gebruik van de diensten om de infrastructuur in te zetten ter ondersteuning van de beschikbaarheidsverplichtingen en -eisen. De CISP moet een model voor capaciteitsplanning handhaven dat het gebruik en de eisen van de CISP infrastructuur ten minste maandelijks beoordeelt. Dit model moet de planning van toekomstige eisen ondersteunen en rekening houden met overwegingen zoals informatieverwerking, telecommunicatie en opslag van auditlogboeken.*

BEDRIJFSCONTINUÏTEIT en DISASTER RECOVERY L

- ***Bedrijfscontinuïteitsplan:*** *Het CISP Bedrijfscontinuïteitsplan moet maatregelen schetsen om omgevingsverstoringen te voorkomen en te verminderen. Het moet operationele details bevatten over de stappen die voor, tijdens en na een gebeurtenis moeten worden genomen. Het Bedrijfscontinuïteitsplan moet worden ondersteund door testen die simulaties van verschillende scenario's bevatten. Tijdens en na het testen, moet de CISP de prestaties van mensen en processen, de corrigerende maatregelen en de geleerde lessen documenteren met het oog op voortdurende verbetering.*

- ***Pandemische reactie:*** *De CISP moet het beleid en de procedures voor pandemie opnemen in zijn rampenherstelplanning om zich voor te bereiden op een snelle reactie op de dreiging van een uitbraak van een besmettelijke ziekte. Mitigatiestrategieën omvatten alternatieve personeelsmodellen om belangrijke processen over te brengen naar middelen buiten de regio, en de activering van een crisisbeheerplan ter ondersteuning van belangrijke bedrijfsactiviteiten. Pandemieplannen moeten verwijzen naar internationale gezondheidsinstellingen en -voorschriften, inclusief contactpunten voor internationale instellingen.*

BEWAKING en REGISTRATIE

- ***Toegangscontrole datacenter****: De toegang tot de datacenters moet regelmatig worden herzien. De toegang moet automatisch worden ingetrokken wanneer het dossier van een werknemer in het HR-systeem van de CISP wordt beëindigd. Bovendien moet, wanneer de toegang van een werknemer of aannemer afloopt in overeenstemming met de goedgekeurde aanvraagduur, zijn of haar toegang worden ingetrokken, zelfs als hij of zij werknemer blijft van de CISP.*

- ***Logboeken toegang tot datacenters****: Fysieke toegang tot CISP datacenters moet worden geregistreerd, bewaakt en bewaard. De CISP moet de informatie die wordt verkregen uit logische en fysieke bewakingssystemen met elkaar in verband brengen om de beveiliging te verbeteren wanneer dat nodig is.*

- ***Toegangscontrole datacenter:*** *De CISP moet datacenters bewaken met behulp van wereldwijde Security Operations Centers - die verantwoordelijk zijn voor het bewaken, testen en uitvoeren van beveiligingsprogramma's. Zij moeten dag en nacht wereldwijde ondersteuning bieden door het beheren en bewaken van de toegangsactiviteiten tot de datacenters, het uitrusten van lokale teams en andere ondersteuningsteams om te reageren op beveiligingsincidenten door middel van triage, consultancy, analyse en het verzenden van reacties.*

TOEZICHT en DETECTIE

- ***CCTV:*** *Fysieke toegangspunten tot serverruimtes moeten worden opgenomen door middel van bewakingscamera's (CCTV). Beelden moeten worden bewaard volgens de wettelijke en compliancevoorschriften.*

- ***Ingangspunten datacenter:*** *De fysieke toegang tot het gebouw moet worden gecontroleerd door professioneel beveiligingspersoneel dat gebruik maakt van toezicht- en detectiesystemen en andere elektronische middelen. Bevoegd personeel dient gebruik te maken van multi-factor authenticatie mechanismen om toegang te krijgen tot datacenters. De toegang tot de serverruimtes moet worden beveiligd met apparaten die een alarm afgeven, om een reactie op een incident te initiëren als de deur wordt geforceerd of open wordt gehouden.*

- ***Inbraakdetectie:*** *Binnen de datalaag moeten elektronische inbraakdetectiesystemen worden geïnstalleerd om het juiste personeel te bewaken, te detecteren en automatisch te waarschuwen bij beveiligingsincidenten. In- en uitgangen naar serverruimtes moeten worden beveiligd met apparaten die elke persoon vereisen om multi-factor authenticatie te bieden voordat toegang of vertrek is toegestaan. Deze apparaten geven een alarm af als de deur zonder authenticatie wordt geforceerd of open wordt gehouden. Deuralarmerende apparaten moeten ook worden geconfigureerd om gevallen te detecteren waarin een individu een datalaag verlaat of binnengaat zonder dat er sprake is van multi-factor authenticatie. Alarmmeldingen moeten onmiddellijk worden verzonden naar de 24/7 CISP Security Operations Centers voor onmiddellijke logboekregistratie, analyse en respons.*

APPARAATBEHEER

- ***Assetbeheer:*** *CISP assets moeten centraal worden beheerd via een voorraadbeheersysteem dat eigenaar, locatie, status, onderhoud en beschrijvende informatie voor CISP assets opslaat en volgt. Na de aankoop moeten de assets worden gescand en getraceerd, en moeten de assets die onderhoud ondergaan worden gecontroleerd op eigendom, status en resolutie.*

- ***Vernietiging van media:*** *Mediaopslagapparaten die worden gebruikt om klantgegevens op te slaan, moeten door CISP worden geclassificeerd als belangrijk en dienovereenkomstig als impactvol worden behandeld gedurende hun gehele levenscyclus. De CISP zou strenge normen moeten hanteren voor het installeren, onderhouden en uiteindelijk vernietigen van de apparaten als ze niet meer bruikbaar zijn. Wanneer een opslagapparaat het einde van zijn levensduur heeft bereikt, moet de CISP de media buiten gebruik stellen met behulp van technieken die in NIST 800-88 zijn beschreven. Media waar klantgegevens op opgeslagen zijn, mogen niet uit het CISP beheer worden verwijderd totdat deze veilig ontmanteld zijn.*

OPERATIONELE ONDERSTEUNINGSSYSTEMEN

- ***Stroom:*** *De elektriciteitssystemen van het CISP datacenter moeten 24 uur per dag volledig redundant en onderhoudsvrij zijn, zonder gevolgen voor de bedrijfsvoering. De CISP dient ervoor te zorgen dat de datacenters zijn uitgerust met back-up stroomvoorziening om ervoor te zorgen dat er stroom beschikbaar is, zodat de werkzaamheden voortgezet kunnen worden in geval van een elektrische storing voor belangrijke en essentiële workloads in de faciliteit.*

- ***Klimaat en temperatuur:*** *CISP datacenters moeten mechanismen gebruiken om het klimaat te controleren en een passende bedrijfstemperatuur voor servers en andere hardware te handhaven om oververhitting te voorkomen en de kans op uitval van de dienstverlening te verkleinen. Personeel en systemen moeten de temperatuur en de vochtigheidsgraad op het juiste niveau bewaken en controleren.*

- ***Branddetectie en bestrijding****: CISP datacenters moeten worden uitgerust met automatische branddetectie- en -bestrijdingsapparatuur. Branddetectiesystemen moeten gebruik maken van rookdetectiesensoren binnen netwerken, mechanische en infrastructurele ruimtes. Deze gebieden moeten ook worden beschermd door bestrijdingssystemen.*

- ***Lekdetectie:*** *Om de aanwezigheid van waterlekken te detecteren, moet de CISP datacenters uitrusten met de functionaliteit om de aanwezigheid van water te detecteren. Als er water wordt gedetecteerd, moeten er mechanismen zijn om water te verwijderen om extra waterschade te voorkomen.*

INFRASTRUCTUURONDERHOUD

- ***Apparatuuronderhoud****: CISP dient preventief onderhoud van elektrische en mechanische apparatuur te bewaken en uit te voeren om de blijvende bruikbaarheid van systemen binnen CISP datacenters te waarborgen. De procedures voor het onderhoud van de apparatuur moeten door bevoegde personen en volgens een gedocumenteerd onderhoudsschema worden uitgevoerd.*

- ***Omgevingsbeheer:*** *CISP moet toezicht houden op elektrische en mechanische systemen en apparatuur, zodat problemen onmiddellijk kunnen worden opgespoord. Dit moet worden uitgevoerd door gebruik te maken van doorlopende controle instrumenten en informatie die wordt verstrekt via CISP gebouwbeheer- en elektrische bewakingssystemen. Preventief onderhoud dient te worden uitgevoerd om de apparatuur operationeel te houden.*

GOVERNANCE en RISICO

- ***Permanent datacenter risicobeheer:*** *Het CISP Security Operations Center dient regelmatig dreigings- en kwetsbaarheidsanalyses van datacenters uit te voeren. Een voortdurende evaluatie en beperking van potentiële kwetsbaarheden moeten worden uitgevoerd via activiteiten voor risicobeoordeling van datacenters. Deze beoordeling moet worden uitgevoerd in aanvulling op het risicobeoordelingsproces op ondernemingsniveau dat wordt gebruikt om de risico's voor het bedrijf als geheel te identificeren en te beheren. Bij dit proces moet ook rekening worden gehouden met regionale regelgevings- en milieurisico's.*

- ***Beveiligingsverklaringen van derden:*** *Het testen van CISP datacenters door derden, zoals gedocumenteerd in de verslagen van derden, moet ervoor zorgen dat de CISP op passende wijze beveiligingsmaatregelen heeft*

geïmplementeerd, die zijn afgestemd op de vastgestelde regels die nodig zijn om beveiligingscertificaten te verkrijgen. Afhankelijk van het complianceprogramma en de eisen die daaraan worden gesteld, kunnen externe auditors testen uitvoeren op de verwijdering van media, beveiligingscamera's bekijken, ingangen en gangen in een datacenter controleren, elektronische toegangscontroleapparaten testen en de apparatuur van het datacenter onderzoeken.

7. Migraties

	Vereiste
1.	*MIGRATIEDIENST:* *Hoeveel verschillende datamigratiediensten biedt de cloud aanbieder aan?*
2.	*MIGRATIES – CENTRAAL TOEZICHT:* *Biedt de cloud aanbieder organisaties een gecentraliseerde (d.w.z. één venster) dienst, waarbij de status van hun server- en applicatiemigraties wordt gevolgd en bewaakt?*
3.	*MIGRATIES – DASHBOARD:* *Biedt de migratietool van de cloud aanbieder een dashboard om snel de migratiestatus, de bijbehorende statistieken en de migratiegeschiedenis te bekijken?*
4.	*MIGRATIES – CLOUD AANBIEDER TOOLS:* *Biedt de migratietool van de cloud aanbieder integratie met andere migratietools van de cloud aanbieder die server- en applicatiemigraties kunnen uitvoeren?*
5.	*MIGRATIES – TOOLS VAN DERDEN:* *Laat de migratietool van de cloud aanbieder toe om migratietools van derden te integreren?* • *Zo ja, wat zijn de ondersteunde migratietools van derden?*
6.	*MIGRATIES – MIGRATIES OVER MEERDERE REGIO'S:* *Biedt de migratietool van de cloud aanbieder mogelijkheden voor het traceren en bewaken van server- en applicatiemigraties die in verschillende regio's plaatsvinden?*
7.	*MIGRATIES – SERVERMIGRATIE:* *Biedt de migratietool van de cloud aanbieder een manier om lokale gevirtualiseerde servers naar de cloud te migreren?* • *Zo ja, welke gevirtualiseerde omgevingen worden momenteel ondersteund?*
8.	*MIGRATIES – SERVERONTDEKKING:* *Biedt de migratietool van de cloud aanbieder de mogelijkheid om automatisch lokale virtuele servers te vinden die naar de cloud moeten worden gemigreerd?*
9.	*MIGRATIES – SERVERPRESTATIEGEGEVENS:* *Biedt de migratietool van de cloud aanbieder de mogelijkheid om server- en/of virtuele machineprestaties te verzamelen en weer te geven, zoals het gebruik van een centrale verwerkingseenheid (CPU) en willekeurig toegankelijk geheugen (RAM)?*
10.	*MIGRATIES – DISCOVERY DATABASE:* *Biedt de migratietool van de cloud aanbieder de mogelijkheid om alle verzamelde gegevens op te slaan in een gecentraliseerde database?* • *Zo ja, hebben organisaties de mogelijkheid om deze gegevens te exporteren? Naar welke indelingen?*
11.	*MIGRATIES – ENCRYPTIE IN RUSTSTAND:* *Versleutelt de cloud aanbieder alle informatie die wordt verzameld en opgeslagen in de discovery database?*

12.	*MIGRATIES – INCREMENTELE SERVERREPLICATIE:* *Biedt de migratietool van de cloud aanbieder een geautomatiseerde, live incrementele serverreplicatie tijdens de server- of virtuele machinemigratie, als een manier om ervoor te zorgen dat alle wijzigingen die aan de server of virtuele machine worden aangebracht, worden opgenomen in het uiteindelijke gemigreerde beeld?* • *Zo ja, hoe lang kan deze dienst dan nog worden uitgevoerd?*
13.	*MIGRATIES – VMWARE:* *Ondersteunt de migratietool van de cloud aanbieder Hyper-V migratie van virtuele machines van on-premise naar de cloud?*
14.	*MIGRATIES – HYPER-V:* *Ondersteunt de migratietool van de cloud aanbieder Hyper-V migratie van virtuele machines van on premise naar de cloud?*
15.	*MIGRATIES – DETECTIE VAN APPLICATIES* *Biedt de migratietool van de cloud aanbieder de mogelijkheid om applicaties te ontdekken en te groeperen voordat ze worden gemigreerd?*
16.	*MIGRATIES – AFHANKELIJKHEIDSTOEWIJZING* *Biedt de migratietool van de cloud aanbieder de mogelijkheid om afhankelijkheden tussen servers en applicaties te ontdekken voordat ze worden gemigreerd?*
17.	*MIGRATIES – DATABASE MIGRATIE:* *Beschikt de migratietool van de cloud aanbieder over de mogelijkheid om lokale databases naar de cloud te migreren?*
18.	*MIGRATIES – UITVALTIJD DATABASE MIGRATIE:* *Biedt de migratietool van de cloud aanbieder de mogelijkheid om een database migratie naar de cloud uit te voeren met een minimale uitvaltijd, d.w.z. dat de bron database tijdens het migratieproces volledig operationeel moet blijven?*
19.	*MIGRATIES – BRONDATABASE:* *Ondersteunt de migratietool van de cloud aanbieder het migreren van verschillende database middelen zoals Oracle, SQL Server enz…?* • *Zo ja, vermeld dan alle ondersteunde bron databases die naar de cloud kunnen worden gemigreerd.*
20.	*MIGRATIES – HETEROGENE MIGRATIES:* *Biedt de migratietool van de cloud aanbieder de mogelijkheid om heterogene databasemigraties uit te voeren, d.w.z. van de ene brondatabase naar een andere doeldatabase, zoals van Oracle naar SQL Server?* • *Zo ja, vermeld dan alle mogelijke heterogene databasemigratiecombinaties.*
21.	*MIGRATIES – GEGEVENSMIGRATIE OP PETABYTE SCHAAL:* *Biedt de cloud aanbieder een oplossing voor gegevenstransport op petabyte schaal die gebruik maakt van veilige apparaten om grote hoeveelheden gegevens naar en uit de cloud te transporteren?*
22.	*MIGRATIES – GEGEVENSMIGRATIE OP EXABYTE-SCHAAL:* *Biedt de cloud aanbieder een oplossing op exabyte-schaal voor gegevenstransport om extreem grote hoeveelheden gegevens naar de cloud te verplaatsen?*
23.	*MIGRATIES – BEDRIJFSBACK-UPS:* *Biedt de cloud aanbieder een dienst aan om het datacenter van een klant probleemloos te integreren met cloud opslagdiensten die het mogelijk maken om gegevens over te dragen en op te slaan in de opslagdienst van de cloud aanbieder?*

24.	*MIGRATIES – BEDRIJFSBACK-UPS – OBJECTOPSLAG:* *Biedt de back-updienst van de cloud aanbieder een integratie met de cloud objectopslagdienst van de aanbieder?*
25.	*MIGRATIES – BEDRIJFSBACK-UPS – BESTANDSTOEGANG:* *Staat de back-updienst van de cloud aanbieder gebruikers toe om objecten op te slaan en op te halen met behulp van bestandsprotocollen zoals het NFS-protocol (Network File System)?*
26.	*MIGRATIES – BEDRIJFSBACK-UPS – TOEGANG BLOKKEREN:* *Staat de back-updienst van de cloud aanbieder gebruikers toe om objecten op te slaan en op te halen met behulp van blokprotocollen zoals het iSCSI-protocol (Internet small computer systems interface)?*
27.	*MIGRATIES – BEDRIJFSBACK-UPS – TAPETOEGANG:* *Staat de back-updienst van de cloud aanbieder gebruikers toe om een back-up te maken van hun gegevens via een virtuele tapebibliotheek en deze tapeback-ups op te slaan in de cloud van de aanbieder?*
28.	*MIGRATIES – BEDRIJFSBACK-UPS – ENCRYPTIE:* *Biedt de back-updienst van de cloud aanbieder encryptie van gegevens in ruststand en in overdracht?*
29.	*MIGRATIES – BEDRIJFSBACK-UPS – SOFTWARE INTEGRATIE VAN DERDEN:* *Integreert de back-updienst van de cloud aanbieder met veelgebruikte back-upsoftware van derden?*
30.	*MIGRATIES – SERVICELIMIETEN:* *Heeft de cloud aanbieder beperkingen (d.w.z. servicelimieten) ten aanzien van het bovenstaande migratiegedeelte?* *Voorbeeld:* *Maximum aantal gelijktijdige migraties van virtuele machines* *Maximaal bestelbaar aantal datatransportoplossingen*

8. Facturatie

	Vereiste
1.	*FACTURERING – TRACERING EN RAPPORTAGE:* *Biedt de cloud aanbieder een tracering- en rapportagedienst voor facturering om gebruikers te helpen hun gebruik van het cloud aanbod te beheren en te bewaken?*
2.	*FACTURERING – ALARMEN EN MELDINGEN:* *Biedt de cloud aanbieder gebruikers een mechanisme om alarmen in te stellen met meldingen om gebruikers te waarschuwen wanneer hun uitgaven een bepaalde drempel hebben overschreden?*
3.	*FACTURERING – KOSTENBEHEER:* *Biedt de cloud aanbieder een mechanisme om grafieken te maken en weer te geven die de kosten en uitgaven samenvatten?*
4.	*FACTURERING – BUDGETTEN:* *Biedt de cloud aanbieder een mechanisme om budgetten te tonen en te beheren en geschatte kosten te voorspellen?*
5.	*FACTURERING – TOTAALOVERZICHT:* *Biedt de cloud aanbieder een mechanisme om de facturering van meerdere rekeningen samen te voegen onder één enkele, primaire betaalrekening?*

6.	***FACTURERING – SERVICELIMIETEN:*** *Heeft de cloud aanbieder beperkingen (d.w.z. servicelimieten) ten aanzien van het bovenstaande gedeelte over facturering?* *Voorbeeld:* *Maximaal aantal rekeningen dat kan worden gegroepeerd* *Maximaal aantal alarmen dat kan worden aangemaakt* *Maximaal aantal budgetten dat kan worden beheerd*

9. Beheer

	Vereiste
1.	***BEHEER – BEWAKINGSDIENST*** *Biedt de cloud aanbieder een bewakingsdienst voor het beheer van cloudmiddelen en -applicaties die vooraf gedefinieerde cijfers verzamelen, controleren en rapporteren?*
2.	***BEHEER – ALARMEN:*** *Staat de bewakingsdienst van de cloud aanbieder gebruikers toe om alarmen in te stellen?*
3.	***BEHEER – AANGEPASTE MEETGEGEVENS*** *Staat de bewakingsdienst van de cloud aanbieder gebruikers toe om aangepaste meetgegevens in te stellen?*
4.	***BEHEER – BEWAKINGSNAUWKEURIGHEID*** *Biedt de bewakingsdienst van de cloud aanbieder verschillende niveaus van bewakingsnauwkeurigheid, tot op het niveau van 1 minuut?*
5.	***BEHEER – API-TRACEERDIENST*** *Biedt de cloud aanbieder een dienst aan die activiteiten registreert, bewaakt en opslaat tegen cloudmiddelen, zowel op console- als op API-niveau (Application Programming Interface) voor een beter inzicht?* • *Zo ja, wat zijn de diensten van de cloud aanbieder die integreren met deze traceerdienst?*
6.	***BEHEER – MELDING:*** *Maakt de cloud aanbieder het mogelijk om meldingen te versturen op basis van de activiteitenniveaus van de applicatieprogrammeringsinterface (API)?*
7.	***BEHEER – COMPRESSIE:*** *Biedt de cloud aanbieder een mechanisme voor het comprimeren van de logboeken die worden gegenereerd door het applicatieprogrammeringsinterface (API) traceersysteem om gebruikers te helpen de opslagkosten voor deze dienst te verlagen?*
8.	***BEHEER – SAMENVOEGING VAN REGIO'S*** *Biedt de cloud aanbieder de mogelijkheid om de activiteit van de account applicatieprogrammeringsinterface (API) in alle regio's op te nemen en deze informatie op een samengevoegde manier te leveren voor het gebruiksgemak?*
9.	***BEHEER – BRONINVENTARISATIE:*** *Biedt de cloud aanbieder een dienst aan om de configuraties van de door een gebruiker ingezette middelen te beoordelen, te controleren en te evalueren?*

10.	*BEHEER – CONFIGURATIEWIJZIGINGEN:* *Neemt de cloud- aanbieder automatisch een wijziging van de bronconfiguratie op wanneer deze zich voordoet?*
11.	*BEHEER – CONFIGURATIEGESCHIEDENIS:* *Biedt de cloud aanbieder de mogelijkheid om de configuratie van de middelen op elk willekeurig moment in het verleden te onderzoeken?*
12.	*BEHEER – CONFIGURATIEREGELS:* *Biedt de cloud aanbieder richtlijnen en aanbevelingen voor inrichting, configuratie en continue bewaking van compliance?*
13.	*BEHEER – BRON TEMPLATES:* *Biedt de cloud aanbieder gebruikers de mogelijkheid om een verzameling van middelen te creëren, te leveren en te beheren op een template-achtige manier?*
14.	*BEHEER – REPLICATIE BRON TEMPLATES:* *Biedt de cloud aanbieder de mogelijkheid om deze resource templates snel te repliceren in verschillende regio's, zodat ze mogelijk kunnen worden gebruikt in situaties van noodherstel (DR)?*
15.	*BEHEER –TEMPLATE ONTWERPER:* *Biedt de cloud aanbieder een eenvoudig te gebruiken grafische tool met drag-and-drop functionaliteit die het proces van het maken van dergelijke resource templates versnelt?*
16.	*BEHEER – SERVICE CATALOGUS:* *Biedt de cloud aanbieder een dienst aan voor het maken en beheren van een service catalogus, d.w.z. servers, virtuele machines, software, databases enz.?*
17.	*BEHEER – CONSOLETOEGANG:* *Biedt de cloud aanbieder een webgebaseerde gebruikersinterface om het beheer en de controle van cloud services te vergemakkelijken?*
18.	*BEHEER – CLI TOEGANG:* *Biedt de cloud aanbieder een gelijkmatige tool om meerdere cloud services te beheren en te configureren vanuit de opdrachtregelinterface (CLI) en om beheertaken te automatiseren door het gebruik van scripts?*
19.	*BEHEER – MOBIELE TOEGANG:* *Biedt de cloud aanbieder een smartphone applicatie waarmee gebruikers verbinding kunnen maken met de cloud service en hun middelen kunnen beheren?* • *Zo ja, is deze applicatie beschikbaar voor zowel iOS als Android?*
20.	*BEHEER – BEST PRACTICES:* *Heeft de cloud aanbieder een dienst die gebruikers helpt hun cloud gebruik te vergelijken met best practices?*
21.	*BEHEER – SERVICELIMIETEN:* *Heeft de cloud aanbieder beperkingen (d.w.z. servicelimieten) ten aanzien van het bovenstaande gedeelte over beheer?* *Voorbeeld:* *Maximaal aantal configuratieregels per account* *Maximaal aantal alarmen dat kan worden aangemaakt* *Maximaal aantal logboeken die kunnen worden opgeslagen*

10. Ondersteuning

	Vereiste
1.	*ONDERSTEUNING – SERVICE:* *Biedt de cloud aanbieder ondersteuning op elk gewenst moment, 24 uur per dag, 7 dagen per week en 365 dagen per jaar via telefoon, chat en e-mail?*
2.	*ONDERSTEUNING – ONDERSTEUNINGSNIVEAUS:* *Biedt de cloud aanbieder verschillende ondersteuningsniveaus?*
3.	*ONDERSTEUNING – NIVEAUS VAN TOEWIJZING:* *Staat de cloud aanbieder toe dat gebruikers de verbruikte middelen/diensten zelf toewijzen aan verschillende niveaus van ondersteuning op basis van gedetailleerde classificatie, en niet door gebruikers te dwingen aparte cloud accounts te onderhouden om verschillende niveaus van ondersteuning te bereiken en te hebben?*
4.	*ONDERSTEUNING – FORUMS:* *Biedt de cloud aanbieder openbare ondersteuningsforums voor klanten om hun problemen te bespreken?*
5.	*ONDERSTEUNING – DASHBOARD VOOR SERVICESTATUS:* *Biedt de cloud aanbieder een dashboard voor de servicestatus dat actuele informatie over de beschikbaarheid van diensten in meerdere regio's weergeeft?*
6.	*ONDERSTEUNING – GEPERSONALISEERD DASHBOARD:* *Biedt de cloud aanbieder een dashboard dat een gepersonaliseerd beeld geeft van de prestaties en de beschikbaarheid van de diensten die ten grondslag liggen aan de specifieke middelen van de gebruiker?*
7.	*ONDERSTEUNING – DASHBOARDGESCHIEDENIS:* *Biedt de cloud aanbieder 365 dagen aan bruikbare geschiedenis van de servicestatus van het dashboard?*
8.	*ONDERSTEUNING – CLOUDADVISEUR:* *Biedt de cloud aanbieder een dienst die werkt als een op maat gemaakt cloud expert en die helpt het verbruik van middelen te vergelijken met best practices?*
9.	*ONDERSTEUNING – TAM:* *Biedt de cloud aanbieder een technische accountmanager (TAM) die technische expertise levert voor het volledige aanbod aan cloud services?*
10.	*ONDERSTEUNING – ONDERSTEUNING APPLICATIES VAN DERDEN:* *Biedt de cloud aanbieder ondersteuning voor gemeenschappelijke besturingssystemen en gemeenschappelijke applicatie stackcomponenten?*
11.	*ONDERSTEUNING – OPENBARE API:* *Biedt de cloud aanbieder een openbare applicatieprogrammeringsinterface (API) die programmatisch omgaat met ondersteuningscases om dergelijke cases te creëren, te bewerken en te sluiten?*
12.	*ONDERSTEUNING – SERVICE DOCUMENTATIE:* *Biedt de cloud aanbieder voor al zijn diensten hoogwaardige, openbaar toegankelijke technische documentatie, inclusief, maar niet beperkt tot gebruikershandleidingen, tutorials, veelgestelde vragen (FAQ's) en toelichtingen?*
13.	*ONDERSTEUNING – CLI DOCUMENTATIE:* *Biedt de cloud aanbieder goede kwaliteit, openbaar toegankelijke technische documentatie voor zijn opdrachtregelinterface (CLI)?*

14.	*ONDERSTEUNING – REFERENTIE ARCHITECTUREN:* *Biedt de cloud aanbieder een gratis, online verzameling van referentie architectuur documenten om klanten te helpen bij het bouwen van specifieke oplossingen die veel van de cloud services van de cloud aanbieder combineren?*
15.	*ONDERSTEUNING – REFERENTIE IMPLEMENTATIES:* *Biedt de cloud aanbieder een gratis, online verzameling van documenten met gedetailleerde, geteste en gevalideerde, stapsgewijze procedures, inclusief best practices, om gemeenschappelijke oplossingen (d.w.z. DevOps, Big Data, Data Warehouse, Microsoft workloads, SAP workloads, enz.) in zijn cloud aanbod te implementeren?*

Bijlage B – Live technische evaluatie

Bij het kiezen van een CISP is het belangrijk om de mogelijkheden van het cloud platform 'live' te beoordelen met behulp van de openbaar beschikbare diensten en infrastructuur van de CISP. We raden ten minste 1 volledige dag per geselecteerde CISP aan voor technische evaluatie. Tijdens de evaluatie kunt u: 1) een diepgaande evaluatie uitvoeren om te beoordelen of de getoonde mogelijkheden in overeenstemming zijn met uw RFP vereisten en de schriftelijke antwoorden van de CISP, 2) een platform bieden voor uw experts om de CISP te onderzoeken om te zorgen dat deze geschikt is voor en is afgestemd op uw specifieke technische en organisatorische behoeften, en 3) vertrouwen krijgen in CISP diensten en het vermogen van de CISP om te schalen, veilig te werken, veerkrachtig werkzaam te zijn en te blijven innoveren om in toekomstige behoeften te voorzien.

Wanneer CISP's reageren op de vereisten van een RFP voor cloud services, kunnen ze de naleving ervan verklaren op basis van een interpretatie op hoog niveau van de vereisten, die niet de volledige context van de behoeften van de bedrijfsomgeving/applicaties van een organisatie bevat. We raden u aan een live technisch beoordelingspanel in te zetten met toonaangevende technische, operationele, beveiligings en applicatie experts. Beoordelaars moeten de CISP tijdens de evaluatie uitdagen, en als best practice moeten ze onafhankelijke CISP's beoordelen op een vaste schaal, zoals 0–4 (0=onacceptabel, 1=marginaal, 2=acceptabel, 3=goed, 4=uitstekend). Daarna kunnen de demoscores worden samengevoegd, waarbij de gemiddelde score voor elk beoordelingsscenario wordt geïmplementeerd in de totale CISP beoordeling. Scenario's met een hoge standaardafwijking moeten voorafgaand aan de afronding als beoordelingsteam worden besproken. Als de scores eenmaal zijn samengevoegd, kan een weging worden toegepast op basis van het cruciale karakter van de scenario's.

Wat de omvang van de demo betreft, raden we aan om een holistische kijk te nemen op het platform van de CISP, en er vervolgens dieper op in te gaan om specifieke workloads op het platform te beoordelen. Hieronder volgt een voorbeeld van een platform- en workloadbeoordeling. Organisaties kunnen op dit uitgangspunt voortbouwen of deze aanpassen om ervoor te zorgen dat de geselecteerde CISP voldoet aan hun specifieke functionele en niet-functionele vereisten. Als best practice kunnen leveranciers die de lijst van scenario's en vereisten gepresenteerd krijgen, een agenda voor de live evaluatie voorstellen die de dekking maximaliseert en 20% aan Q&A tijd omvat.

Platform evaluatie: Meerdere CISP's gebruiken de term 'Well-architected' om te verwijzen naar een benadering van de cloud die optimale waarde biedt en risico's minimaliseert. Goed ontworpen scenario's in een live technische demonstratie kunnen omvatten:

1. Beveiliging: identiteit, gecentraliseerde governance, geautomatiseerde detectie van dreigingen, gegevensbescherming, voorbereiding op gebeurtenissen
2. Efficiëntie van prestaties: juiste grootte, schaalbaarheid/elasticiteit, serverloos
3. Betrouwbaarheid: hoge beschikbaarheid (bestendigheid tegen storingen), minder risico op verandering, noodherstel, back-up
4. Kostenbeheer: financiële activiteiten, commerciële optimalisatie, budgetten en kostentoewijzing
5. Operationele uitmuntendheid: automatisering, bewaking, ondersteuning, beheer en mogelijkheden die nodig zijn om te migreren naar en te opereren binnen de cloud

Beoordeling van de workload: Veel voorkomende applicatietypen die kunnen worden gedemonstreerd zijn:

- Webapplicatie: Openbare hosting van een dynamische website, inclusief back-end database en opslag van statische objecten.
- Gegevensanalyse: Een data lake- of lake house architectuur die de consolidatie van gegevens van verschillende gegevensproviders mogelijk maakt en de mogelijkheid biedt om om te gaan met hoge hoeveelheden (TB's/PBS-gegevens), verscheidenheid (gestructureerd, ongestructureerd, verschillende indelingen, enz.) en snelheid (snelheid van het genereren van gegevens, veranderingen en querypatronen).
- Data science platform: Een platform dat de ontwikkeling, implementatie en het gebruik van op AI/ML gebaseerde mogelijkheden in uw hele organisatie mogelijk maakt.
- IoT applicatie: Een IoT platform/ capaciteit dat de cloud, netwerkmogelijkheden en de apparaten omvat.

Voor elke representatieve workload die belangrijk is voor uw organisatie, kunt u de scenario's definiëren die door de CISP moeten worden aangetoond. De scenario's moeten de algemene mogelijkheden aantonen die de implementatie van de workload op een goed ontworpen manier mogelijk maakt. De volgende pagina's bevatten voorbeelden van Live technische evaluatie criteria voor; 1) het platform van de CISP en 2) een voorbeeld van de workload van webapplicaties.

Platform – Voorbeeld live technische evaluatie

Voorbeeld ID	Voorbeeldnaam	Mate van belang (1=Laag; 4=Kritiek)	Demonstratievoorschriften	Scoreoverwegingen
Plat.Sec.1	Identiteitscombinatie	4	De mogelijkheid tonen om een bestaande identiteitsopslag samen te brengen naar de cloud service.	• Ondersteuning voor standaardprotocollen zoals SAML. • Ondersteuning voor SCIM-gebaseerde identiteitsreplicatie. • De mogelijkheid om verschillende toegangsniveaus binnen de bedrijfsidentiteitsopslag te definiëren en deze toe te passen binnen de cloud aanbieder. • De mogelijkheid om specifieke teams/ personen alleen te beperken tot bepaalde accounts/projecten/workloads. • Mogelijkheid om Attribute Based Access Control (ABAC) te ondersteunen en deze kenmerken binnen het Identity and Access Management (IAM) systeem van de cloud aanbieder te gebruiken om de toegang tot cloudmiddelen te beheren.
Plat.Sec.2	Centrale governance	4	Het vermogen tonen om beleid en vereisten centraal te definiëren, op organisatorisch niveau (mondiaal beleid) en ook op bedrijfsniveau en projectniveau.	• Het beleid moet het volgende omvatten: diensten in-/uitschakelen, geografische beperkingen toepassen (regio's beperken). • Het beleid moet ook voorkomen dat gebruikers, inclusief beheerders, controle- en beheerscontroles uitschakelen.

Voorbeeld ID	Voorbeeldnaam	Mate van belang (1=Laag; 4=Kritiek)	Demonstratievoorschriften	Scoreoverwegingen
Plat.Sec.3	Beperking van gebruikerstoegang	3	Toon de automatische aanbevelingen voor het aanscherpen van gebruikersrechten.	• Mogelijkheid om huidige machtigingen te vergelijken met vereiste machtigingen. • Automatische generatie van beleid om de minste privileges te bevorderen.
Plat.Sec.4	Controlelogboekregistratie	4	Toon controlelogboekregistratie van cloudactiviteiten, inclusief toegestane en niet-toegestane handelingen.	• Gecentraliseerde logboeken voor de hele organisatie. • Account-/projectspecifieke logboeken ter ondersteuning van tracering op laag niveau en verantwoordingsplicht. • Tools om query's van logboeken toe te staan. • Tools waarmee handelingen ingeschakeld kunnen worden op basis van specifieke gebeurtenissen/logboekitems. • Mogelijkheid om ondersteuningsactiviteiten van leveranciers te bekijken. • Mogelijkheid om het verwijderen van logboeken te voorkomen, ook door beheerders.
Plat.Sec.5	Netwerkisolatie	4	Toon en bewijs waar mogelijk de isolatie van verschillende gebruikers binnen de cloud. Toon de configuratie van geïsoleerde (zonder connectiviteit), particuliere (zonder internet) en openbare (met internettoegang) subnetten.	• Scheiding van gebruikers, inclusief op VPN- en cross connection services. • Mogelijkheid om de verkeersstroom van buiten de cloudinfrastructuur (op locatie), binnen de IT en naar het internet te controleren. • Hoe de scheiding van toepassing is bij het gebruik van gedeelde diensten zoals containerhosting of functie als service.

Voorbeeld ID	Voorbeeldnaam	Mate van belang (1=Laag; 4=Kritiek)	Demonstratievoorschriften	Scoreoverwegingen
Plat.Sec.6	Encryptie in ruststand	4	De mogelijkheid tonen om ongebruikte gegevens te coderen, inclusief de opties voor BYOK en codering van de klant.	• Mogelijkheid om codering voor gevoelige gegevens te vereisen. • Mogelijkheid om door de aanbieder beheerde sleutels of door de klant beheerde sleutels te gebruiken. • Naleving van FIPS 140-2. • Mogelijkheid om te waarschuwen voor en te registreren dat er aan de coderingsvereisten wordt voldaan. • Extra invloed op kosten. • Invloed op de prestaties. • Ondersteuning voor kwantumbestendige algoritmen en sleutelgrootten.
Plat.Sec.7	Encryptie in overdracht	4	De mogelijkheid tonen om gegevens in overdracht te coderen.	• Standaard codering voor service API's. • Mogelijkheid om codering in overdracht (TLS) in te schakelen op load balancers en beheerde API's. • Ondersteuning voor wederzijdse verificatie (client en server).
Plat.Sec.8	Sleutelbeheer	4	Uw sleutelbeheer mogelijkheden tonen. Neem de volledige levenscyclus van de sleutel op. Integratie met cloud services opnemen.	• Het maken, gebruiken, roteren en vernietigen van sleutels in een logboek.
Plat.Sec.9	Configuratiebeheer	3	Toon uw configuratiebeheer mogelijkheden van het cloud platform.	• Zorg voor een nauwkeurige CMBD. • Controleer of aan de voorschriften wordt voldaan. • Automatisch activeren van acties op basis van niet-naleving. • Mogelijkheid om configuratiewijzigingen te evalueren aan de hand van best practices of aangepaste regels.

Voorbeeld ID	Voorbeeldnaam	Mate van belang (1=Laag; 4=Kritiek)	Demonstratievoorschriften	Scoreoverwegingen
Plat.Sec.10	Netwerkbeveiliging	3	Toon de firewallmogelijkheden (al dan niet voor webapplicaties), inclusief integratie met rule sets/firewalls van derden en beveiliging tegen volumetrische aanvallen.	• WAF (Web Application Firewall)-capaciteiten: schaalbaarheid. • Ondersteuning voor zowel privé als openbare netwerken. • Mogelijkheid om in te schrijven op feeds van branche/leverancier voor rule sets. • Automatisch acties activeren binnen de infrastructuur op basis van gebeurtenissen van de WAF. • Firewall capaciteiten, schaalbaarheid. • Host- en netwerkgebaseerde firewalls. • Mogelijkheid om naar logische groepen of objecten te verwijzen naast de mogelijkheid om CIDR IP-blokken te specificeren. • Aantal regels dat op elk niveau/onderdeel wordt ondersteund. • Mogelijkheid om een gedistribueerd bedrijfsmodel (netwerkteam + ontwikkelingsteam) te ondersteunen door middel van beleid en netwerkconfiguratie.
Plat.Sec.11	Netwerkverbinding	3	De mogelijkheid tonen om verbinding te maken met netwerken op locatie en eindpunten/clients met privénetwerken binnen de cloud.	• Privé verbinding (hoge bandbreedte met meer dan 10GB) • De mogelijkheid om het routerings- en firewallbeleid in de hele organisatie te beheren. • VPN-verbinding (site-to-site en client-based) • IPV6-ondersteuning.

Voorbeeld ID	Voorbeeldnaam	Mate van belang (1=Laag; 4=Kritiek)	Demonstratievoorschriften	Scoreoverwegingen
Plat.Sec.12	Instantiebeheer	3	Toon de mogelijkheden voor instancebeheer.	• Mogelijkheid om de status van patches van een groot aantal instances te controleren en te beheren. • Ondersteuning voor patchbeheer voor Linux en Windows. • De mogelijkheid om opdrachten uit te voeren op een hele reeks servers zonder SSH nodig te hebben. • Mogelijkheid om externe toegang tot virtuele machines centraal te beheren en te controleren. • Mogelijkheid om de grootte van een instance te wijzigen, extra hoeveelheden toe te voegen, de netwerkconfiguratie te wijzigen, enz. via Console, CLI en API.
Plat.Sec.13	Toepassing van beleid	3	De mogelijkheid tonen om diensten te configureren om toegang tot het openbare internet te voorkomen.	• Mogelijkheid om verkeer te isoleren naar privénetwerken voor diensten die mogelijk belangrijke/vertrouwelijke gegevens bevatten. • Mogelijkheid om beleid te definiëren dat de toegang tot gegevens op basis van het bronnetwerk regelt. • Toepassing van deze toegangsbeperkingen voor alle gebruikers, inclusief gebruikers met referenties op hoog niveau.
Plat.Sec.14	Scannen op kwetsbaarheden	2	De mogelijkheid tonen om beelden (container en VM) te scannen op kwetsbaarheden.	• Mogelijkheid om containers in een register automatisch te scannen. • Mogelijkheid om virtuele machines te scannen op bekende kwetsbaarheden. • Mogelijkheid om netwerkscans uit te voeren.

Voorbeeld ID	Voorbeeldnaam	Mate van belang (1=Laag; 4=Kritiek)	Demonstratievoorschriften	Scoreoverwegingen
Plat.Sec.15	Netwerkinspectie	2	De mogelijkheid tonen om netwerkverkeer (NetFlow en full packet) te registreren/spiegelen vanuit een klantomgeving.	• Mogelijkheid om een deel van/al het verkeer binnen de infrastructuur van de cloud aanbieder te spiegelen (vanuit het perspectief van de klant), inclusief volledige pakketregistratie. • De mogelijkheid om eenvoudig te selecteren welk verkeer u wilt vastleggen. • Mogelijkheid om te schalen naar zeer grote verkeersvolumes (meer dan 50 GBps).
Plat.Sec.16	Bedreigingsdetectie	3	De detectiefunctie tonen voor indringers van uw platform, waaronder bedreigingen van een netwerk, gebruik van referenties en analyse van gebruikspatronen.	• Het vermogen om verdachte activiteiten zoals 'mining' te detecteren. • Mogelijkheid om kwaadaardige acties te detecteren voor verificatieaanvallen zoals SSH-aanmeldingen. • Mogelijkheid om lekken of misbruik van inloggegevens te detecteren. • Toepassing van ML, het analyseren van grote aantallen gebeurtenissen en het naar boven laten komen van geprioriteerde gebeurtenissen. • Pogingen om in te schakelen/te configureren (eenvoudig is beter). • Mogelijkheid om te integreren met externe diensten en meldingen te activeren. • Mogelijkheid om het IDS op een wereldwijd niveau te configureren voor alle projecten/accounts.
Plat.Perf.1	Compute optimalisatie	2	Automatische aanbevelingen tonen voor optimalisatie van virtuele machines en functioneren als onderhoudskosten.	• Aanbevelingen op basis van de werkelijke gebruikspatronen en workloadpatronen. • Aanbevelingen omvatten geschatte besparingen en inzichten in verwachte belastingsniveau's/technische implicaties.

Voorbeeld ID	Voorbeeldnaam	Mate van belang (1=Laag; 4=Kritiek)	Demonstratievoorschriften	Scoreoverwegingen
				• Optimalisaties moeten zowel besparingen als 'prestatierisico' omvatten, waarbij virtuele machines bijvoorbeeld ondermaats kunnen zijn.
Plat.Perf.2	Omgevingsoptimalisatie	2	Automatische aanbevelingen tonen voor andere cloud onderdelen zoals loadbalancers, netwerken, databases, opslag enz.	• Aanbevelingen identificeren besparingen en potentiële mogelijkheden voor prestatie efficiëntie in andere onderdelen die verder gaan dan de kernberekening.
Plat.Perf.3	Compute auto-scaling	4	De automatische schaalmogelijkheden tonen van een applicatie die achter een loadbalancer in een virtuele computeromgeving wordt geïmplementeerd. De verschillende beschikbare opties/benaderingen tonen en de mogelijkheid om andere (optionele) acties te activeren voor/na het schalen van gebeurtenissen, zoals een melding.	• Verschillende opties voor schalen, trigger gebaseerde, op tijd gebaseerde, handmatig of intelligentere benaderingen die machine learning toepassen om de vereiste capaciteit te voorspellen. • Volledig geautomatiseerd schalen, inclusief registratie met een loadbalancer en health checks. • De mogelijkheid om een willekeurig stuk code uit te voeren op specifieke punten van de schaal-levenscyclus.
Plat.Perf.4	Online schalen voor opslag	3	De mogelijkheid tonen om de capaciteit en de doorvoer van blokopslag te schalen zonder de workload te onderbreken.	• Mogelijkheid om blokopslag tussen verschillende opslagtypen over te schakelen zonder de noodzaak om diensten volledig opnieuw op te bouwen. • Mogelijkheid om de omvang van de aan VM's aangeboden hoeveelheden te vergroten.
Plat.Perf.5	Auto-scaling voor managed services	3	De mogelijkheid tonen voor de Object Store, API Gateway, het FaaS platform en de NoSQL-database om te schalen	• Probleemloos automatisch schalen, ideaal zonder tussenkomst van de beheerder.

Voorbeeld ID	Voorbeeldnaam	Mate van belang (1=Laag; 4=Kritiek)	Demonstratievoorschriften	Scoreoverwegingen
			van weinig (10s) naar veel (1000s) gelijktijdige gebruikers.	• Constante prestaties tijdens een aflopende opschaling die is afgestemd op de vereisten voor productieschaling. • Voor sommige onderdelen, zoals FaaS, kijkt u naar opties voor het voorbereiden en het beheren van limieten voor gelijktijdige uitvoering, indien nodig.
Plat.Perf.6	Containerbasis workloads	3	De mogelijkheid tonen om op containers gebaseerde workloads te hosten.	• Opties voor containerhostingplatforms. • Integratie met andere IaaS-onderdelen zoals loadbalancers. • Beschikbaarheid van een servicemesh-oplossing. • Niet-eigen opties voor containerhosting, zoals Kubernetes. • Standaard ondersteuning voor hoge beschikbaarheid binnen het containerbesturingsplatform. • Mogelijkheid om containerhosts op locatie te beheren.
Plat.Rel.1	Regionale veerkracht	4	De geautomatiseerde failover van een relationele database-instance binnen een regio tonen wanneer een geografisch gelokaliseerde storing (zoals een stroomstoring) wordt gesimuleerd.	• Automatische failover. • Geïsoleerde storingszones binnen een cloud regio. • Duidelijk afgebakend en eenvoudig te ontwerpen voor hoge beschikbaarheid.
Plat.Rel.2	Automatisch herstel van instance	2	Automatisch herstellen tonen van een instance/reeks instances na een mislukte statuscontrole.	• Configureerbare statuscontroles. • Volledig geautomatiseerd herstellen/ opnieuw inrichten van instances.

Voorbeeld ID	Voorbeeldnaam	Mate van belang (1=Laag; 4=Kritiek)	Demonstratievoorschriften	Scoreoverwegingen
Plat.Rel.3	Statusbewustzijn van de loadbalancer	3	Tonen hoe een loadbalancer automatisch een defecte instance detecteert en verkeer naar andere gezonde hosts omleidt.	• Configureerbare statuscontroles. • Geautomatiseerde routering van verkeer naar gezonde hosts.
Plat.Rel.4	Regionale failover	3	Een architectuur met meerdere regio's tonen, inclusief geautomatiseerde verkeersverschuiving naar een secundaire regio.	• Wereldwijd bewuste statuscontroles. • Geautomatiseerde routeringsopties: latency, gewogen en failover. • Ondersteuning voor virtuele machine workloads en managed services zoals een Object Store/NoSQL database service.
Plat.Rel.5	Backup en herstel	4	De opties tonen voor back-up en herstel voor: virtuele machines, databases, managed services.	• Niveau van automatisering. • Mogelijkheid om te herstellen naar dezelfde/een andere cloud regio. • Mogelijkheid om back-ups te kopiëren naar een andere cloud regio.
Plat.Cost.1	Budgetten	3	Een vermogen tonen voor budgetbeheer, inclusief hoe deze kan worden gestructureerd voor sub-accounts en projecten.	• Denk aan de mogelijkheid om budgetcontroles en toezicht toe te passen op de verschillende niveaus van uw organisatie. • Controleer op flexibiliteit, bijvoorbeeld voor de mogelijkheid om onderdelen te groeperen (door middel van tagging), budgetten in te stellen voor specifieke cloud services en drempels voor waarschuwingen/bewaking te configureren.
Plat.Cost.2	Budgettoewijzing	1	De levering van een nieuwe projectomgeving (account) tonen, inclusief het proces voor de toewijzing van de begroting voor het project.	• Het vermogen om zelf te voorzien, met de juiste goedkeuringen.

Voorbeeld ID	Voorbeeldnaam	Mate van belang (1=Laag; 4=Kritiek)	Demonstratievoorschriften	Scoreoverwegingen
			De inrichting moet handmatige goedkeuringsstappen omvatten voor 1) technische beoordeling/IT, 2) commerciële beoordeling/financiering.	• Automatisering van de configuratie van de juiste budgetinstelling, meldingen of budgetbeleid voor uw organisatie.
Plat.Cost.3	Budgetrapportage	2	Het vermogen tonen om over budgetten in de hele organisatie te rapporteren. Rapportage voor een specifieke afdeling versus de hele organisatie (wetenswaardigheden). De rapportage moet zowel de 'werkelijke' als de voorspelde/geschatte bestedingswaarden bevatten.	• Het vermogen om zichtbaarheid te bieden op verschillende niveaus van de organisatie, waardoor bewustzijn en transparantie worden gecreëerd, maar op een need-to-know-basis. • Prognoses moeten gebaseerd zijn op de huidige en eerdere consumptietrends en een vroegtijdige waarschuwing geven over mogelijke budgetoverschrijding.
Plat.Cost.4	Budgetcontroles	1	Het vermogen tonen om actie te ondernemen wanneer een budgetdrempel wordt bereikt. Acties omvatten bijvoorbeeld meldingen, het toepassen van beperkingen of actieve tussenkomst om te voorkomen dat het budget wordt overschreden.	• Het vermogen om acties eenvoudig te definiëren voor verschillende projecten. • Het vermogen voor de acties om van project tot project te verschillen, bijvoorbeeld door rekening te houden met de gevolgen van ontwikkeling productie. • De mogelijkheid om meerdere acties en drempels te definiëren voor hetzelfde budget/project. • De mogelijkheid om aangepaste acties te definiëren in aanvulling op standaardmogelijkheden.
Plat.Cost.5	Periodiciteit van het budget	1	Het vermogen tonen om budgetten toe te passen voor verschillende tijdsperioden, dagelijks/maandelijks/jaarlijks enz. Voor jaarlijkse budgetten tonen dat ze in staat zijn om een variabele verdeling van	• Mogelijkheid om budgetten voor verschillende perioden te definiëren. • Mogelijkheid om een verdeling van de uitgaven over het jaar te configureren voor jaarlijkse budgetten, vooral

Voorbeeld ID	Voorbeeldnaam	Mate van belang (1=Laag; 4=Kritiek)	Demonstratievoorschriften	Scoreoverwegingen
			de verwachte uitgaven gedurende het hele jaar toe te passen.	belangrijk voor seizoensgebonden/zeer flexibele workloads, zoals bijvoorbeeld een jaarlijkse belastingaangifte.
Plat.Cost.6	Marketplace van derden	3	De mogelijkheid tonen om producten van derden te kopen en te implementeren. Tonen hoe een budget kan worden vastgesteld voor een reeks producten van derden die beschikbaar zijn via een marketplace en de mogelijkheid om de beschikbare producten te beperken.	• Mogelijkheid om een budget vast te stellen voor een specifiek product; een wereldwijd budget, een budget voor een reeks projecten/accounts. • Mogelijkheid om alleen een subset van de bredere marketplace aan te tonen aan cloudgebruikers.
Plat.Cost.7	Compute prijsmodellen	3	De verschillende prijzen/commerciële modellen tonen die kunnen worden toegepast op virtuele machines.	• De mogelijkheden zouden on-demand moeten omvatten, zonder dat er een langetermijnverplichting nodig is en een gedetailleerde prijs (per minuut/uur). • Optionele langetermijnverplichtingen in ruil voor een korting. • Mogelijkheid om instances te kopen met bereidheid deze te onderbreken in ruil voor een korting. • Belangrijk is dat het mogelijk moet zijn om deze modellen te combineren binnen hetzelfde project/dezelfde accounts, en ook om voordelen te delen over verschillende accounts.
Plat.Cost.8	Aanbevelingen voor commerciële optimalisering	3	Het vermogen tonen om commerciële optimaliseringsaanbevelingen te ontvangen om de uitgaven te optimaliseren (zonder technische wijzigingen aan te brengen).	• Holistische aanbevelingen voor meerdere diensten, waaronder bijvoorbeeld Virtual machines en Managed databases. • Vermogen om aanbevelingen eenvoudig te doen en de verwachte besparingen/voordelen te begrijpen.

Voorbeeld ID	Voorbeeldnaam	Mate van belang (1=Laag; 4=Kritiek)	Demonstratievoorschriften	Scoreoverwegingen
Plat.Cost.9	Specifieke hosts	4	De mogelijkheid tonen om een speciale host te leveren om het gebruik van lokale licenties mogelijk te maken die aan een specifieke host zijn gekoppeld.	• Eenvoudige inrichting. • Mogelijkheid om het gebruik van de host te beheren. • De mogelijkheid om de host te delen over verschillende projecten/tenancies.
Plat.Ops.1	Migratie van virtuele machines	3	Toon het importeren van een virtuele machine van lokale naar een cloudgebaseerde VM-service.	• Mogelijkheid om zowel op Windows als Linux gebaseerde besturingssystemen te importeren. • Mogelijkheid om meerdere machines tegelijk te importeren. • Mogelijkheid om een replicatiesessie te onderhouden om een snelle 'failover' naar de cloud mogelijk te maken.
Plat.Ops.2	DevOps en automatiseringsmogelijkheden	4	DevOps/automatiseringsmogelijkheden tonen, inclusief hoe omgevingen worden gedefinieerd als code, ondersteuning van volledig geautomatiseerde implementaties, geautomatiseerde tests en rollbacks.	• Mogelijkheid om alle systeemonderdelen als code te definiëren, inclusief netwerk, virtuele machines, opslag, databases. • Mogelijkheid om een pijplijn te creëren. • Mogelijkheid om een code register te maken. • Mogelijkheid om builds te automatiseren. • Mogelijkheid om blue/green implementaties uit te voeren. • Mogelijkheid om meerdere omgevingen te creëren en meerdere fasen voor implementaties te hebben. • Geautomatiseerde rollback voor mislukte implementaties
Plat.Ops.3	Applicatie hosting	2	Het hosten tonen van een eenvoudige 2-laagse applicatie in een low-code/platform service. Inclusief een	• Eenvoudige configuratie via de gebruikersinterface.

Voorbeeld ID	Voorbeeldnaam	Mate van belang (1=Laag; 4=Kritiek)	Demonstratievoorschriften	Scoreoverwegingen
			relationele database en automatische schalen voor de applicatie-/weblaag.	• Inclusief statuscontroles, schalen, hoge beschikbaarheid. Platformondersteuning, Windows en Linux.
Plat.Ops.4	Beveiligingsintegratie	2	De integratiemogelijkheden van uw platform tonen vanuit het perspectief van Security incident and Event Management.	• De mogelijkheid om op eenvoudige wijze beveiligingsgerelateerde logboeken van de cloud aanbieder + API's te integreren en te gebruiken voor integratie.
Plat.Ops.5	ITSM integratie	3	De integratiemogelijkheden van uw platform tonen vanuit het perspectief van ITSM (IT Service Management).	• Mogelijkheid om een supportcase via een API te verhogen, te bewaken en bij te werken. • Mogelijkheid om diensten of servicereeksen als 'producten' te leveren via een API.
Plat.Ops.6	Ondersteuning	4	Uw ondersteuningsaanbod tonen.	• Verschillende ondersteuningsniveaus voor verschillende soorten workloads. • Mogelijkheid om ook het besturingssysteem/Database Engine enz. te ondersteunen, indien van toepassing voor een bepaalde service. • De mogelijkheid om een uitstekende aanbieding te bieden met benoemde ondersteuningsleads voor belangrijke workloads. • De mogelijkheid om een gestructureerd proces voor de gereedheid van gebeurtenissen en de evaluatie van de architectuur aan te bieden. • Inzicht in de planning van de aanbieder.

Voorbeeld ID	Voorbeeldnaam	Mate van belang (1=Laag; 4=Kritiek)	Demonstratievoorschriften	Scoreoverwegingen
Plat.Ops.7	Controleerbaarheid	4	De hulpmiddelen tonen die u nodig hebt om compliance-audits te ondersteunen.	• Mogelijkheid om details over compliance audits te verkrijgen via de console. • Mogelijkheid om milieu audits te beheren en te automatiseren.
Plat.Ops.8	VM naar container	1	De conversie tonen van een applicatie op een virtuele machine naar een container en deze bedienen met behulp van het containerplatform van de cloud aanbieder.	• Gebruiksgemak van de conversie. • Tijd om te converteren. • Platformondersteuning, .Net and Java.

Workload: Webapplicatie – voorbeeld van live technische evaluatie

Het volgende gedeelte bevat een voorbeeld van een evaluatieformulier voor de workload van een specifieke webapplicatie. Bij het ontwikkelen van een evaluatieformulier voor een bepaalde applicatie wordt ten zeerste aanbevolen de gebruikers, ontwikkelaars en beheerders van de applicatie erbij te betrekken, omdat zij waarschijnlijk het beste inzicht hebben in de vereisten, huidige uitdagingen en beperkingen.

Voorbeeld ID	Voorbeeldnaam	Mate van belang (1=Laag; 4=Kritiek)	Demonstratievoorschriften	Scoreoverwegingen
Web.Sec.1	Beveiliging – Bescherming van de applicatie	3	Toon aan dat u kwaadaardige pogingen om de applicatie te misbruiken kunt blokkeren via SQL Injection, XSS Scripting Attack en andere aanvallen.	• Mogelijkheid om 'out-of-the-box' bescherming te bieden tegen veelvoorkomende aanvallen met standaardregels/mogelijkheden. • Mogelijkheid om aangepaste controles/regels/functies te maken.
Web.Sec.2	Beveiliging – Op snelheid gebaseerde beveiliging	3	Aantonen dat u in staat bent om aanvallen te blokkeren/beschermen met betrekking tot grote aanvraagsnelheden of gegevenshoeveelheden gericht op een applicatie.	• Mogelijkheid om limieten te configureren en aanvraagtarieven te beperken van een bepaald IP-adres of een lijst met adressen.

Voorbeeld ID	Voorbeeldnaam	Mate van belang (1=Laag; 4=Kritiek)	Demonstratievoorschriften	Scoreoverwegingen
Web.Sec.3	Beveiliging – Op bron gebaseerde beveiliging	3	De mogelijkheid aantonen om toegang te beperken op basis van netwerk/geografische bron.	• Mogelijkheid om te beperken op netwerkblok of een lijst met netwerkblokken. • Mogelijkheid om te beperken op land van herkomst (zonder dat IP-lijsten moeten worden beheerd).
Web.Sec.4	Beveiliging – Netwerksegmentatie	4	De mogelijkheid tonen om onderdelen (webserver, App Server/DB Server) te isoleren/beschermen ter bescherming tegen zowel Noord-Zuid- als Oost-West-verspreiding via de infrastructuur.	• Mogelijkheid om onderdelen in verschillende subnetten te plaatsen en de verkeersstroom tussen verschillende subnetten te controleren. • Mogelijkheid om de verkeersstroom op netwerkinterfaceniveau te controleren. • Mogelijkheid om zowel logische groepen als CIDR blokken te verwijzen.
Web.Sec.5	Beveiliging – TLS ondersteuning en certificaatbeheer	4	De mogelijkheid tonen om een TLS-beveiligd eindpunt te leveren en de ondersteunende onderdelen automatisch te beheren om dit te verwezenlijken, zoals bijvoorbeeld de automatische rotatie van certificaten.	• Ondersteuning voor de nieuwste TLS protocollen en de mogelijkheid om indien nodig oudere versies uit te schakelen. • Certificaten eenvoudig genereren, beheren en roteren (idealiter volledig geautomatiseerd).
Web.Perf.1	Prestaties - Schaalbaarheid	4	Aantonen dat u kunt schalen van 10 naar 100.000 gelijktijdige gebruikers van de webapplicatie door middel van dynamische automatische schaalaanpassing.	• Mogelijkheid om zowel op tijd gebaseerde als op activering gebaseerde schaalregels te definiëren. • De eindgebruiker en beheerder kan probleemloos schalen. Automatisch schalen wanneer de belasting toeneemt en schalen wanneer de belasting afneemt.

Voorbeeld ID	Voorbeeldnaam	Mate van belang (1=Laag; 4=Kritiek)	Demonstratievoorschriften	Scoreoverwegingen
				• Zorgen dat er schaalbaarheid bestaat op elke laag van de webapplicatie (Load Balancer, Web Layer, Data Layer, enz.). • De beschikbaarheid van caching diensten op verschillende lagen van de applicatie, indien van toepassing.
Web.Perf.2	Prestaties - Wereldwijde levering	3	Uw CDN capaciteit aantonen, inclusief het tonen van latency vanuit verschillende punten over de hele wereld, waaronder Australië, Azië, Afrika, het Midden-Oosten, Noord-Amerika, Zuid-Amerika en Europa.	• Mogelijkheid om een CDN aan te maken en te configureren via de CISP console/API's. • Configureerbare distributieregels voor verschillende regio's. • Configureerbare caching voor verschillende gebruikssituaties/applicaties.
Web.Rel.1	Betrouwbaarheid – Veerkracht voor een enkele regio	4	Het vermogen tonen om een gelokaliseerde gebeurtenis te kunnen verduren, zoals het verlies van netwerkverbinding met het CISP datacenter.	• Geautomatiseerde failover en hoge beschikbaarheid binnen een cloud regio (stad).
Web.Rel.2	Betrouwbaarheid - Implementatie in meerdere regio's	3	Tonen van een implementatie van een webapplicatie in meerdere regio's, inclusief een wereldwijd gerepliceerde database.	• Mogelijkheid om een applicatie in meerdere regio's programmatisch te implementeren. • Replicatie tussen de regio's voor de gegevensopslag. • Geautomatiseerde routering van gebruikers naar hun optimale regio.
Web.Rel.3	Betrouwbaarheid - Failover in meerdere regio's	3	De automatische failover van een webapplicatie tonen in het geval van een serviceprobleem dat een hele regio treft.	• Geautomatiseerde failover en hoge beschikbaarheid door meerdere cloud regio's.

Voorbeeld ID	Voorbeeldnaam	Mate van belang (1=Laag; 4=Kritiek)	Demonstratievoorschriften	Scoreoverwegingen
Web.Cost.1	Kosten – Zichtbaarheid	2	De mogelijkheid tonen om de kosten per applicatie bij te houden	• Mogelijkheid om historische kosten voor een specifieke applicatie te bekijken, inclusief wanneer deze omhoog of omlaag geschaald kan worden.
Web.Cost.2	Kosten – Budgetten	2	De mogelijkheid tonen om budgetten en gerelateerde waarschuwingen per applicatie in te stellen.	• Budgetten die per applicatie zijn geconfigureerd en de mogelijkheid om acties/waarschuwingen te activeren op basis van geconfigureerde drempels.
Web.Ops.1	Ops – Onderhoudsvensters	3	De mogelijkheid tonen om onderhoudsvensters te configureren om aan de bedrijfsvereisten te voldoen, vooral waar onderhoud de beschikbaarheid van applicaties kan beïnvloeden.	• Configureerbare onderhoudsvensters voor onderdelen zoals een relationele databaseservice.
Web.Ops.2	Ops – Logboekregistratie	3	De mogelijkheid tonen om logboekregistratie te centraliseren voor een applicatie met meerdere onderdelen, inclusief het voortbestaan van logboeken bij beëindiging/uitval van virtuele machines.	• Mogelijkheid om een gecentraliseerde logboekservice te configureren die kan worden aangepast aan de vereisten van de applicatie. • Mogelijkheid om regels/filters te definiëren om waarschuwingen of acties te activeren op basis van specifieke gebeurtenissen in het logboek.
Web.Ops.3	Ops – Bewaking	3	De bewaking van de applicatie aantonen, inclusief prestaties, beschikbaarheid, responstijden, fouttellingen enz. en functionaliteit om actie-/triggermeldingen te doen op basis van verschillende drempelwaarden.	• Een verzameling standaard metingen die beschikbaar zijn, zoals schijf-IO, CPU, databasemetingen, netwerk, loadbalancer enz. • Mogelijkheid om aangepaste metingen en drempels te definiëren. • Mogelijkheid om een aangepast dashboard te maken om de belangrijkste metingen weer te geven en deze dashboards te delen met relevante gebruikers.