

Bijlage 16 - Cloudstrategie CIZ





Inleiding

Omdat Cloud zo'n breed vertegenwoordigd onderwerp is levert dit vaak vragen op. "Wat is Cloud?" en "Mag Cloud binnen het CIZ toegepast worden, of niet?". We kunnen het onderwerp niet meer af doen met 'het mag niet', maar zullen moeten onderbouwen op welke wijze we de toepassing afwegen. In deze notitie komen de volgende zaken aan de orde:

- In hoofdstuk 1 worden eerst de definities van de Cloudcomputing, de voordelen en risico's toegelicht;
- In hoofdstuk 2 wordt de visie van VWS uiteengezet m.b.t. de toepassing van Cloudcomputing;
- Hoofdstuk 3 geeft de normen en kaders weer die gehanteerd worden als onderdeel van het Cloudbeleid;
- Hoofdstuk 4 geeft de vereiste certificering en assurance afgegeven door de Cloud provider in het kader van de dienstverlening (specifiek op gebied van informatiebeveiliging/AVG);
- Afsluitend wordt de conclusie weergegeven op welke basis, CIZ in de praktijk Cloudcomputing kan toepassen;
- De inhoudelijke en achtergrond informatie zijn in aparte bijlagen opgenomen.

1. Cloudcomputing, voordelen en risico's

Cloudcomputing omvat het leveren van computerdiensten (servers, netwerkfuncties, software, opslag en daarmee verwante diensten) doorgaans via internet ('de Cloud'). Cloudcomputing kan ervoor zorgen dat gegevens en applicaties gemakkelijker beschikbaar zijn, sneller kunnen worden aangepast, zowel groei als krimp schaalbaar zijn en eenvoudiger kunnen worden beheerd. De gebruikte infrastructuur kan efficiënter worden benut en aangepast aan de behoefte van de gebruiker. Cloudcomputing is vaak een wens van het management of van medewerkers. Zij hebben hun eigen business drivers, redenen en motieven om als organisatie in de Cloud te stappen. De business drivers (drijfveer) kunnen voor het CIZ zijn:

- Kostenbesparing op ICT;
- Verhogen van het beveiligingsniveau;
- Verhogen van de productiviteit;
- Concentreren op kernactiviteiten;
- Voldoen aan wet- en regelgeving (compliance).

In het algemeen zijn er drie soorten te onderscheiden: Private Cloud, Public Cloud en hybride Cloud. De meest bekende clouddiensten zijn: SaaS, PaaS en IaaS (zie bijlage, 1).

Wat zijn risico's?

De essentie is dat de controle over de Clouddiensten en daarin verwerkte gegevens buiten het CIZ plaatsvindt, terwijl we wel verantwoordelijk blijven voor het gebruik en de gevolgen daarvan. Door goed te begrijpen welke risico's dit met zich meebrengt, kunnen we maatregelen treffen en afspraken maken om deze te mitigeren. Er zijn een aantal risico's om rekening mee te houden in de afweging voor het gebruik maken van de Clouddiensten.

Groter raakvlak met de buitenwereld



Centrum Indicatiestelling Zorg

Door een Cloud dienst buiten de organisatie af te nemen wordt de informatievoorziening breder toegankelijk voor de buitenwereld. Gebruik van de voorziening loopt via Internet. Dit betekent dat de dienst zodanig ingericht en ontworpen moet zijn dat het betrouwbaar en veilig kan werken binnen deze context. Dit is in de kern waarom beveiligingsmaatregelen en privacyaspecten zo belangrijk zijn.

Privacywetgeving

Europese regelgeving stelt eisen aan de opslag van data. Het CIZ moet ervoor zorgdragen dat data die (mogelijk) vertrouwelijke gegevens bevat op een veilige manier worden opgeslagen. Het CIZ kan aansprakelijk gesteld worden als dit soort gegevens uitlekken en moet dan kunnen aantonen dat we afdoende maatregelen hebben getroffen om dat te voorkomen. Als we gebruikmaken van clouddiensten zijn we daarin afhankelijk van Cloudleveranciers.

Informatieveiligheid

Het niet goed organiseren van informatiebeveiliging brengt risico's met zich mee. In de Baseline Informatiebeveiliging Overheid (BIO) liggen de eisen vast waar een informatievoorziening aan moet voldoen op het gebied van beschikbaarheid, integriteit en vertrouwelijkheid. Voor veilig uitwisselen van zorgdata kunnen aanvullende normen gelden.

Beperkingen bij gebruik Cloud

Cloud kan schaalbaar en goedkoper zijn omdat het uitgaat van de brede afname van standaard diensten (meer gebruikers). Vaak zijn er minder opties om de oplossing op maat te maken voor de eigen organisatie. Je moet het doen met wat je krijgt. Het kan erg duur zijn om van Cloudleverancier te wisselen of diensten van verschillende leveranciers te combineren, waardoor een vendor lock-in ontstaat.

Governance aspecten

Door toepassing van Cloud drijft het informatielandschap fysiek uit elkaar (meerdere SaaS oplossing op verschillende Cloudleveranciers). Aanvullende regie op gegevens door het CIZ is nodig om data weer bij elkaar te brengen. Bij het omvallen van een Cloud leverancier valt dienstverlening uit en er kan niet zomaar vanuit worden gegaan dat overdragen van broncode en data tot een continuering van het werk leidt.

2. Wat is VWS visie met betrekking tot de toepassing van Cloudcomputing?

Gegeven het feit dat steeds meer organisaties van Cloudcomputing gebruik maken heeft het Ministerie van VWS op 19 november 2020 een visie, strategie en beleid geformuleerd op het gebied van het gebruik van Clouddiensten gepubliceerd. Het volgende wordt door het Ministerie van VWS aangegeven:

We geloven dat innoveren en optimaliseren van ons werk zonder inzet van Cloud op termijn niet meer mogelijk is. VWS maakt het daarom mogelijk om Cloud als volwaardige oplossing in te zetten. Daar waar de dienstverlening vanuit het eigen rekencentrum niet past bij de behoefte vanuit de organisatie creëren we ruimte om Cloud in te zetten. Als we de keuze maken voor informatiseren van ons werk kijken we naar de functionele behoefte en aan welke kaders een oplossing moet voldoen. Daarbij stellen



Centrum Indicatiestelling Zorg

we eisen op het gebied van governance, privacy en informatiebeveiliging. We realiseren ons de mogelijkheden van Cloud als het gaat om wendbaarheid en innovatie. Zo ontstaat er ruimte om Cloud toe te passen daar waar het toegevoegde waarde heeft.

Bij de toepassing van Cloudcomputing speelt op het gebied van de AVG en informatiebeveiliging het volgende stelt VWS:

Als overheid wordt ons veel gevoelige gegevens toevertrouwd. Vaak is dit zorgdata. Daar willen en moeten we verantwoord mee om gaan. De kaders daarvoor zijn vastgelegd in de wet AVG en de baseline informatiebeveiliging (BIO). Door te sturen op een verwerkersovereenkomst en aantoonbaar toepassen van de veiligheidskaders kunnen we onderbouwen dat we de gegevens kunnen toevertrouwen aan een derde partij. Zo wordt Cloud voor een groot deel van onze informatievoorziening een optie. Op het gebied van vitale infrastructuur en staatsgeheimen zijn we terughoudend en passen we voorsnog geen Cloud toe.

Uiteindelijk is de keuze voor informatievoorziening een integrale afweging binnen het CIZ. Daarom is het aan CIZ om zelf de keuze voor Cloudbeleid te bepalen.

3. Cloud Normen en kaders

Om vast te stellen welke data in de Cloud geplaatst kan/mag worden, moet wel bekend zijn over welke data het CIZ beschikt en welke betrouwbaarheidseisen daar aan worden gesteld. Deze betrouwbaarheidseisen kunnen op basis van de eerder genoemde risico's worden bepaald. Vervolgens moet er op basis van de toegekende beschikbaarheid, integriteit en vertrouwelijkheid classificatie vastgesteld worden welke data wel en welke niet in de Cloud geplaatst mag worden. Om deze classificaties eenduidig te kunnen bepalen hanteren we de normen en kaders voor Clouddiensten.

Om de Cloud normen en kaders binnen het CIZ vast te leggen wordt gebruik gemaakt van de richtlijnen van Het College bescherming persoonsgegevens (voorganger van de Autoriteit Persoonsgegevens), BIO, ISO en NEN op het gebied van informatiebeveiliging. Het doel van de clouddiensten van cloudleveranciers is te waarborgen dat, overeenkomstig specifieke beleidsuitgangspunten, een betrouwbare en veilige dienstverlening geleverd wordt en dat de werking voldoet aan de eisen die door het CIZ zijn gesteld. (zie bijlage, 2)

Om risicomanagement hanteerbaar en efficiënt te houden, kiest de BIO (zie bijlage, 3) voor een uitwerking van het risicomanagement op basis van drie Basis BeveiligingsNiveaus (BBN) (zie bijlage, 4).

- BBN1: op dit niveau ligt de nadruk op wat minimaal verwacht mag worden van alle overheidssystemen.
- BBN2: op dit niveau ligt de nadruk op de bescherming van de meest voorkomende categorieën informatie volgens het principe 'valt de maatregel onder goed huisvaderschap; toont deze beveiliging de betrouwbare overheid? Dat is het geval als:
 - er vertrouwelijke informatie wordt verwerkt;
 - mogelijke incidenten leiden tot bestuurlijke commotie;
 - de veiligheid van andere systemen afhankelijk is van de veiligheid van het eigen systeem.
- BBN3: dit uitzonderlijke niveau is van toepassing op gerubriceerde informatie Departementaal Vertrouwelijk dan wel vergelijkbaar vertrouwelijk bij andere overheidslagen, waarbij weerstand



Centrum Indicatiestelling Zorg

tegen statelijke actoren of vergelijkbare dreigers nodig is. Bijvoorbeeld als: verlies van informatie een grote impact heeft, waarvan niet uit te leggen is als deze niet gerubriceerd is en beschermd wordt op BBN3.

De meest gevoelige data/informatie binnen het CIZ zijn de cliëntengegevens (met name medische gegevens en BSN), justitiële gegevens, personeelsgegevens. Het overgrote deel van de gegevens die het CIZ verwerkt vallen onder BBN2. De overige gegevens binnen het CIZ vallen onder BBN1 niveau.

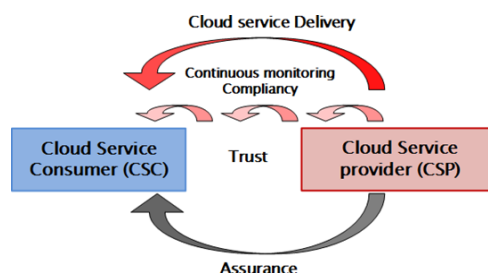
In het volgende overzicht is data classificatie in relatie tot de public Cloud weergegeven.

Data	Authenticatie	Autorisatie	Beveiliging data	Opslag in de Cloud
Publiek toegankelijk informatie Openbaar	Geen	Geen	Versleutelde opslag van gegevens	Mogelijk
Ongerubriceerd	• Laag • EH2 eIDAS: Laag • UserID/ Password	Autorisatie vereist (lid van organisatie)	Versleuteling tijdens transport buiten eigen netwerk van organisatie en versleutelde opslag van gegevens. Sleutels in eigen beheer	• Mogelijk • Maatregelen BBN2
Bedrijfsvertrouwelijk informatie	• Ssubstantieel • EH2+ eIDAS: Substantieel • 2FA • SMS/Token	Autorisatie op specifieke rol	Versleuteling tijdens transport en versleutelde opslag van gegevens. Sleutels in eigen beheer	• Mogelijk • Maatregelen BBN2
Verwerking standaard persoonsgegevens	• Ssubstantieel • EH3 eIDAS: Substantieel • 2FA • SMS/Token	Autorisatie op specifieke rol	Versleuteling tijdens transport buiten eigen netwerk en versleutelde opslag van gegevens. Sleutels in eigen beheer	• Afweging van type applicatie/systeem PIA • Maatregelen BBN2
Verwerking bijzondere persoonsgegevens w.o. zorggegevens	• Hoog • EH4 eIDAS: Hoog • 2FA • Login met PKI-certificaat	Autorisatie op specifieke rol	Versleuteling tijdens transport en versleutelde opslag van gegevens. Sleutels in eigen beheer	• Afweging van type PIA • Maatregelen BBN2
Strafrechtelijke en justitiële	• Hoog • EH4 eIDAS: Hoog	Autorisatie op	Versleuteling tijdens transport en	• Afweging van type

(persoons) gegevens	• 2FA (legitimatie fysiek o.b.v. origineel identiteitsbewijs, uitgifte betrouwbaar) • EH4 login met PKI-certificaat	specifieke rol	versleutelde opslag van gegevens. Sleutels in eigen beheer	applicatie/systeem PIA • Maatregelen BBN2
Staatsgeheim Confidentiële informatie	• Zeer hoog vereist legitimatie fysiek o.b.v. origineel identiteitsbewijs, uitgifte fysiek	Autorisatie 'need to know basis'	Versleuteling tijdens transport en op tussen stations via berichtbeveiliging. Versleutelde opslag van gegevens. Sleutels in eigen beheer. Transport van gegevens minimaliseren. Alleen transport en opslag binnen vaste netwerk van de eigen organisatie	Niet mogelijk

4. Vereiste certificering en assurance rapporten bij Cloudcomputing

Omdat de gegevens worden verwerkt door een Cloud provider voor het CIZ zal deze verantwoording moeten afleggen in hoeverre aan de gestelde eisen op het gebied van informatiebeveiliging en toepassing van de AVG is voldaan. Deze onderlinge relatie ziet er schematisch zo uit:



In de volgende tabel is aangegeven welke certificaten en rapporten noodzakelijk zijn per BBN niveau. Voor de volledigheid zouden we BBN3 niveau qua kolom moeten opnemen echter toepassing van de Cloud voor dit soort gegevens is niet toegestaan binnen de Rijksoverheid.

Eisen en toepassingen	BBN1	BBN2
Informatiebeveiliging	Toepassing van: • ISO-27001 • BIO • NEN-7510	Toepassing van: • ISO-27001 • BIO • NEN-7510



Centrum Indicatiestelling Zorg

AVG		Toepassing van: • ISO-27701
Certificering		
Informatiebeveiliging	Certificaat: • ISO-27001 • NEN-7510	Certificaat: • ISO-27001 • NEN-7510 • ISO-27017
AVG		Certificaat: • ISO-27701 • ISO-27018
Verklaringen		
Assurance rapport		Eén van deze rapporten: • SOC 2 rapport • ISAE 3000 (ISAE 3402 type 2 aangevuld met regels toepassing AVG)

Cloudbeleid

Het Cloudbeleid dient duidelijkheid te scheppen hoe veilig gebruik gemaakt kan worden van Private, Public en Hybride Clouddiensten binnen het CIZ. Met de voorgaande overwegingen en de input van veiligheidsexperts zijn de volgende beleidsvoornemens tot stand gekomen.

De gegevens die het CIZ verwerkt vallen onder BBN1 en BBN2. Een aanvullende risicoanalyse is noodzakelijk indien de dataclassificatie hoger wordt dan BBN2. Data classificatie BBN3 vergt aanvullende maatregelen om weerstand te kunnen bieden tegen statelijke actoren of criminele organisaties (of gelijksoortige actoren) of waar informatie wordt verwerkt die door de bronhouder een bepaalde classificatie (boven BBN2) heeft mee gekregen. De BIO schrijft voor BBN3 geen standaard maatregelen voor, aangezien op dit niveau vanwege de hoge complexiteit veelal maatwerk en risicoanalyse is vereist.

Classificatie	Cloud omgeving
BBN1	Als aan de voorwaarden is voldaan, zijn Public, Hybride en Private Cloud oplossingen toegestaan.
BBN2 en ongerubriceerd	Als aan de voorwaarden is voldaan, zijn Public, Hybride en Private Cloud oplossingen toegestaan.
BBN2 en vertrouwelijk gerubriceerd	Als aan de voorwaarden is voldaan en de verwerking van de gerubriceerde gegevens is vóóraf door de CIZ Raad van Bestuur goedgekeurd, zijn Public, Hybride en Private Cloud oplossingen toegestaan.

Conclusie



Centrum Indicatiestelling Zorg

Aansluitend bij de visie van VWS op het gebied van het toepassen van Cloudcomputing is het ook voor het CIZ mogelijk om onder voorwaarden (met name de vereiste certificeringen/ assurance rapporten) gegevens te laten verwerken door een Cloud provider.



Bijlage: Achtergrond informatie

1. Clouddiensten

Er zijn verschillende soorten clouddiensten. Van kant-en-klare toepassingen die u direct kunt gebruiken, tot omgevingen waarmee u zelf applicaties kunt ontwikkelen.

In het algemeen zijn er drie soorten IT-Clouds te onderscheiden:

- Private: De IT-voorzieningen zijn ingericht slechts voor CIZ met een dedicated infrastructuur en opgezet met de standaarden van de Cloudleverancier.
- hybride: De IT-voorzieningen zijn toegankelijk voor het CIZ en deelt de onderliggende infrastructuur met andere klanten om kosten te besparen (bijvoorbeeld de opslag en het netwerk).
- Public: De voorzieningen worden meestal gedeeld met andere klanten. Een Public Cloud is open voor gebruik buiten het CIZ. Hier vallen ook de externe partijen onder die software en infrastructuur als dienst aanbieden.

Er zijn ruwweg drie soorten clouddiensten:

- Software as a service (SaaS)

De software (applicatie) staat volledig onder controle van de cloudleverancier. De afnemer van deze clouddienst kan er gebruik van maken, maar kan er over het algemeen niets aan wijzigen.

- Platform as a service (PaaS)

In deze laag wordt naast de ICT-infrastructuur, zoals servers, netwerken en opslagcapaciteit, ook het besturingssysteem, databasemanagement en ontwikkeltools aangeboden. Dit geeft de afnemer van deze clouddienst de vrijheid om eigen systemen en diensten te ontwikkelen.

- Infrastructure as a service (IaaS)

In deze laag wordt alleen de ICT-infrastructuur, zoals servers, netwerken en opslagcapaciteit, aangeboden. Dit geeft de afnemer van deze clouddienst de volledige vrijheid om eigen systemen en diensten te implementeren vanaf de keuze voor het besturingssysteem tot en met de aan te bieden clouddienst.

Voordelen Cloud computing

- Schaalvoordelen: het is gemakkelijk om de fysieke capaciteit te vergroten of verkleinen. Uitbreiding van de capaciteit is altijd eenvoudig, inkrimping verloopt niet altijd probleemloos.
- Alleen betalen voor daadwerkelijk gebruik (pay per user). Waarschijnlijk wordt geappelleerd aan de angst om te veel licenties aan te schaffen. De claim noemt tactisch 'alleen betalen', niet 'minder betalen'.
- Kosten van hard- en software liggen vast. Wijzigingen in het aantal gebruikers zijn snel en eenvoudig door te voeren waarbij de kosten duidelijk zijn.
- Updates van programma's worden automatisch doorgevoerd. Dit scheelt in beheerskosten.
- Minder investeringen in hardware (met name servers).
- Minder onderhouds- of beheerskosten.



- Er is minder technische kennis nodig. Maar: het ontbreken van kennis kan ook als nadeel uitpakken.

2. Cloud normen en kaders

- Het College bescherming persoonsgegevens richtsnoer “Beveiliging van Persoonsgegevens”
- AVG - Algemene verordening gegevensbescherming
- BIO:2019 - De Baseline Informatiebeveiliging Overheid
- NEN-ISO/IEC 27001:2017 – Informatietechnologie - Beveiligingstechnieken - Management-systemen voor informatiebeveiliging.
- NEN-ISO/IEC 27017:2015 – Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services.
- NEN-ISO/IEC 27018:2019 – Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.

3. Baseline Informatiebeveiliging Overheid (BIO)

De BIO (“Baseline Informatiebeveiliging Overheid”) is de specifieke norm voor informatiebeveiliging voor overheidsinstanties (gemeenten, provincies, waterschappen, etc.). Een nieuwe norm die vanaf 1 januari 2020 van kracht is.

Dit normenkader is een samenvoeging en update van voorgaande baselines, zoals de BIG, BIR, IBI en BIWA, die hierdoor worden vervangen. Om de helderheid over de eisen die daarin worden gesteld zo groot mogelijk te maken is de structuur van de BIO gebaseerd op de ISO 27001 en 27002 normen.

Bij de BIO staat het risicomanagement centraal. Essentieel is het risicobewustzijn en de wijze waarop de organisatie omgaat met risico's op het gebied van informatiebeveiliging. Zoals bijvoorbeeld privacy schendingen door een datalek, reputatieschade door het uitlekken van vertrouwelijke plannen of fysieke schade door storingen in systemen in de openbare ruimte.

4. BasisBeveiligingsNiveaus (BBN)

De BIO kent drie beschermingsniveaus, de zogenaamde Baseline Beschermingsniveaus (BBN). De zwaarte van de te nemen technische en organisatorische maatregelen moet afgestemd zijn op het risiconiveau van een proces of systeem.

Wanneer bijvoorbeeld een proces wordt vastgesteld op BBN-niveau 2 dan moeten zowel de maatregelen van BBN1 als van BBN2 ingericht worden. Vanuit het hoogste basisbeveiligingsniveau (BBN3) moet er bovendien voldaan worden aan relevante eisen uit o.a. het NAVO-verdrag voor de Beveiliging van Informatie en het Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie (VIR-BI). Welke BBN niveau nodig of gewenst is wordt bepaald aan de hand van een BBN-toets.

Informatiesystemen op BBN1 niveau zijn systemen waarvoor BBN2 als te zwaar wordt gezien. Het kan voorkomen dat er nog wel hogere beschikbaarheids- en integriteitseisen nodig zijn. BBN1 is waar alle overheidssystemen als minimum aan moeten voldoen.

Voor informatiesystemen binnen de overheid vormt BBN2 het uitgangspunt. BBN2 is van toepassing indien er vertrouwelijke informatie wordt verwerkt, mogelijke incidenten leiden tot bestuurlijke commotie, er onzekerheid bestaat of ook alle informatie van derden open is en de veiligheid van andere systemen afhankelijk is van de veiligheid van het eigen systeem.



Het te beschermen belang van BBN2 is maximaal Departementaal Vertrouwelijk (DepV), (zoals gedefinieerd in het VIR-BI)/vergelijkbaar vertrouwelijk bij andere overheidslagen en privacygevoelige informatie met een verhoogd vertrouwelijkheidsniveau. Dergelijke informatie komt veelvuldig voor bij de overheid. Het gaat verder om commercieel vertrouwelijke informatie of informatie in het kader van beleidsvorming; het is dus niet beperkt tot DepV/vergelijkbaar vertrouwelijk bij andere overheidslagen gerubriceerde informatie. BBN2 informatie wordt preventief beschermd tegen alle dreigingen met uitzondering van geavanceerde dreigingen, zoals Advanced Persistent Threats (APT's), afkomstig van statelijke actoren of beroepscriminelen. Daarvoor geldt een bescherming achteraf: zij dienen te kunnen worden gedetecteerd, waarop vervolgens passend gereageerd moet worden. Voor informatiesystemen waar Departementaal Vertrouwelijke informatie en vergelijkbaar vertrouwelijk bij andere overheidslagen wordt verwerkt en waar weerstand tegen de geavanceerde dreiging van statelijke actoren of gelijkwaardige beroepscriminelen is vereist, is het BBN2 dus niet voldoende.

BBN3 richt zich op de bescherming van Departementaal Vertrouwelijk en vergelijkbaar vertrouwelijk bij andere overheidslagen gerubriceerde informatie waarbij weerstand geboden moet worden tegen de dreiging, zoals Advanced Persistent Threat's (APT's), die uitgaat van statelijke actoren en beroepscriminelen. BBN3 is van toepassing indien: verlies van informatie een grote impact heeft, waarvan niet uit te leggen is als deze niet gerubriceerd is en beschermd wordt op het niveau van BBN3; informatie met een rubricering (niet zijnde BBN2) wordt geleverd door derden; aansluiting op een infrastructuur BBN3 is vereist om informatie te kunnen verwerken op deze infrastructuur (bijvoorbeeld om al op de infrastructuur aanwezige gerubriceerde informatie niet in gevaar te brengen)

5. Relatie tussen de CSC en de CSP

In de verhouding tussen de CSC (Cloud Service Consumer) en de CSP (Cloud Service Provider) zijn drie issues waar organisaties steeds op focussen. Vanuit de CSC beredeneerd zijn dit:

1. On-going

Krijgt de CSC qua prestaties op dagelijkse basis de juiste diensten geleverd? Anders gezegd, voldoen de geleverde diensten aan prijs, kwaliteit, veiligheid- en continuïteitseisen? Dus hoe het gesteld is met de performance?

2. Continuous monitoring (near real time)

Krijgt de CSC de zekerheid dat hij regulier, conform contracten, bedrijfseisen en beveiligingseisen, de juiste diensten ontvangt? Dus hoe het gesteld is met de beoogde conformiteit?

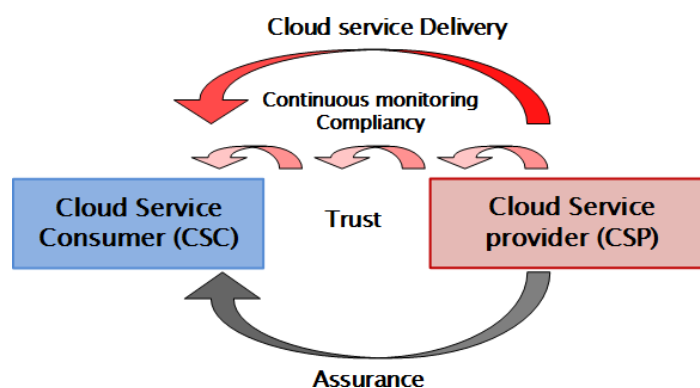
3. Compliancy (periodieke metingen en evaluaties)

Krijgt de CSC de zekerheid dat hij in de afgelopen periode, conform wet- en regelgeving, contracten, bedrijfseisen en beveiligingseisen de juiste diensten heeft ontvangen? Dus hoe het gesteld is met de beoogde compliance?

Bij de inkoop van clouddiensten levert de CSP niet alleen de gecontracteerde clouddiensten (ICT-servicelevering), maar ook de noodzakelijke continuous monitoring-, compliancy- en assurance-rapportages. (zie bijlage 1.2)

In het kader van risicomanagement zijn de mogelijke beleidslijnen uitgewerkt rond het toepassen van 'Basis Beveiligingsniveau' (BBN) 1, 2 en 3 voor diverse Cloudimplementatie-scenario's. De BIO bepaalt

op basis van eisen voor vertrouwelijkheid. Het onderscheid in drie BBN's voorkomt dat voor eenvoudige systemen zonder vertrouwelijke informatie of zonder eigen voor hoge beschikbaarheid teveel administratieve last wordt opgeroepen. Terwijl de BIO zich met name richt op vertrouwelijkheid van gegevens, wordt in Nederland, gedreven door internationale ontwikkelingen, ook meer aandacht gevraagd voor de beschikbaarheid van 'vitale systemen en processen'. In beide toepassingen is risicomanagement met een proportionele set aan maatregelen een logische aanpak.



ICT-servicelevering

Dit betreft de daadwerkelijk door de CSC gevraagde public of private clouddiensten, die aan bepaalde functionele en beveiligingseisen moeten voldoen. De levering gaat vergezeld van prestatiemetingen over de geleverde diensten en de noodzakelijke verbetermaatregelen voor leveringen en beveiliging.

Assurance

Dit betreft een jaarlijkse rapportage gebaseerd op een onderzoek uitgevoerd door een derde partij. Met de assurance-rapportage geeft de CSP zekerheid aan de CSC dat de geleverde diensten aan de contractuele eisen hebben voldaan. De assurance-rapportage komt tot stand met een onderzoekstraject waarin een referentiekader als toetsingsmiddel wordt gehanteerd.

Trust

De inkoop van clouddiensten gaat gepaard met een gedragen en haalbaar ICT-servicecontract. Echter er zullen altijd aspecten zijn die bij de contractvorming over het hoofd worden gezien. Voor een duurzame relatie is daarom een vertrouwensrelatie tussen de CSC en de CSP vereist, anders lopen zij steeds het risico in een juridische strijd verwickeld te raken.

Zowel aan de CSC-kant als aan de kant van de CSP spelen verschillende aspecten een rol. In de relatie tussen de CSC en CSP heeft iedere partij haar eigen rol. De relevante aspecten zijn hieronder beschreven.

CSC (vraagzijde)

Initieel stelt de CSC een Programma van Eisen en Wensen vast voor de te verwerven clouddiensten en communiceert dit met de potentiële CSP's. Wanneer de CSC en de gekozen CSP overeenstemming bereiken, worden de clouddiensten geleverd. Een belangrijke vraag voor overheidsdienstverlening is



Centrum Indicatiestelling Zorg

hierbij: 'Is de toepassing van Clouddienst, gelet op de, door de Tweede Kamer geaccepteerde risico's toegestaan?

