Cloud beleid

Gemeente Borne

Definitief 1.0
17 november 2020

Inhoud

1 Inleiding

De ontwikkelingen op het gebied van ICT en informatievoorziening volgen elkaar in hoog tempo op. Dit betreft dan zowel de technische infrastructuur, denk aan servers, opslag, netwerk, etc., als ook de in gebruik zijnde applicaties van de gemeente zelf en de samenwerkingspartners. Bij veel van deze ontwikkelingen komt de term Cloud om de hoek kijken. Hierbij is het niet altijd duidelijk wat er met Cloud bedoeld wordt en wat het betekent voor de gemeente.

Deze notitie is opgesteld om daarin duidelijkheid te creëren, wat verstaan we onder Cloud, en om uitgangspunten vast te stellen voor de gemeente als het gaat om gebruik maken van een Cloud omgeving of oplossing. Doelstelling is om na vaststelling van het Cloudbeleid een kader te hebben op basis waarvan bewuste keuzes worden gemaakt om applicaties al dan niet aan te schaffen resp. te verplaatsen in een Cloud-omgeving.

Het gebruiken van een Cloud gaat verder dan alleen technische infrastructuur, zoals nu afgenomen wordt bij de gemeente Enschede. Meer en meer leveranciers van softwarepakketten willen de software niet meer leveren om het door de gemeente zelf te laten installeren op haar ICT-omgeving, maar bieden het aan als een dienst in een door hen geleverde Cloud omgeving (zoals Office365 van Microsoft of ZorgNed van ZorgNed Automatisering).

Bij het opstellen van deze notitie is gebruik gemaakt van materiaal van VNG Realisatie / KING, de Taskforce Bestuur, informatieveiligheid dienstverlening (IBD) en toolkit van Native Consulting.

Maatregelen die betrekking hebben op informatiebeveiliging en/of privacybescherming maken geen onderdeel van het Cloudbeleid. Het belang ervan om maatregelen te nemen (aangezien dat extern wordt opgeslagen), neemt echter wel toe. Hiervoor wordt separaat onder verantwoordelijkheid van de CISO kaders geformuleerd.

2 Definitie van Cloud

Cloud Computing wordt door gemeenten gebruikt om via het internet, of een andere breedbandige verbinding gebruik te maken van hardware, software en gegevens. Deze Cloud kan zich overal bevinden.

Het woord Cloud komt van het woord ‘wolk’ waarmee in een netwerk ontwerpen vaak het internet of een netwerk wordt getekend. Deze wolk staat voor een netwerk dat met al de computers die erop aangesloten zijn een soort 'wolk van computers' vormt. De eindgebruiker weet niet waar de computers zich in de Cloud bevinden en ook niet waar de software draait of waar gegevens zich bevinden. Afhankelijk van het type Cloud is men meer of minder eigenaar van de infrastructuur.

Men zou kunnen zeggen dat het gaat om virtuele infrastructuur en diensten. Met Cloud Computing worden servers, desktops en ook applicaties gevirtualiseerd.

Cloud Computing is niet hetzelfde als outsourcing (uitbesteden), ook gaat het wel vaak samen. Bij cloud computing gaat het om de ‘applicaties/techniek’ en bij outsourcing gaat het om de ‘IT-processen’ die worden uitbesteed. Meestal wordt met het plaatsen van een applicatie in de cloud ook het technische

beheer uitbesteed. In dit beleidskader gaat het expliciet om cloud computing en niet om outsourcing van de processen als doel op zich. Daarvoor gelden andere wegingskaders.

Er bestaan meerdere servicemodellen voor Cloud computing. De volgende wijze van het aanbieden van Cloud Computing worden onderkend:

- SaaS – Software as a Service
- PaaS – Platform as a Service
- IaaS – Infrastructure as a Service

Deze drie vormen staan bewust in deze volgorde, van onderaf aan begint men met infrastructuur waarop platforms draaien die het mogelijk maken applicaties te draaien.

Cloud-applicaties: Software as a Service (SaaS)
Bij Software as a Service worden applicaties via de Cloud aangeboden aan eindgebruikers. Vaak worden hier webapplicaties aangeboden die met moderne technologieën gemaakt zijn. Voor de eindgebruiker is onbekend waar de applicatie zich bevindt, op welk platform de applicatie draait en waar de gegevens zich bevinden.

Cloud-platforms: Platform as a Service (PaaS)
Als de gemeente zelf software wil installeren in een Cloud dan kan gebruik worden gemaakt van PaaS. Bij PaaS kan men binnen grenzen de software en de configuratie zelf regelen. De eindklant van een PaaS-oplossing is vaak de eigen ICT-organisatie. Op de PaaS-omgeving worden vaak weer de eigen applicaties geplaatst voor de eindgebruiker.

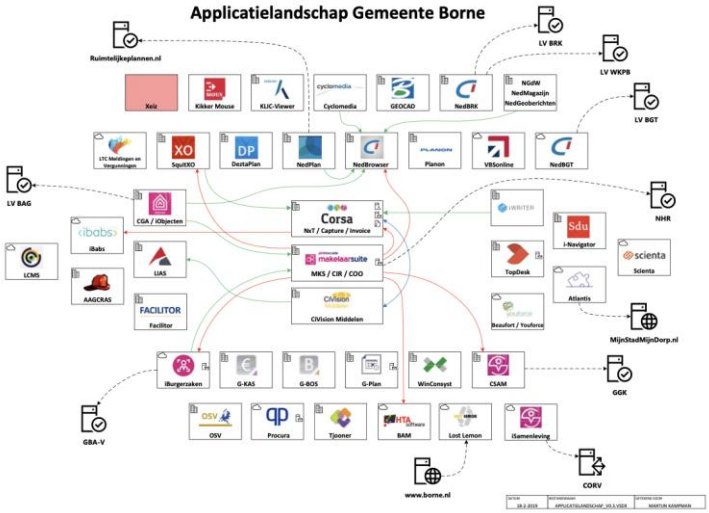
Cloud-infrastructuur: Infrastructure as a Service (IaaS)
Indien men nog meer vrijheden wil hebben kan men alleen de (gevirtualiseerde) infrastructuur afnemen. Hier vindt men servers, netwerkcomponenten, opslagcapaciteit en andere infrastructuur.
Dit geeft de gemeentelijke ICT-afdeling volledige vrijheid over de hardware die virtueel wordt afgenomen, bovenop de IaaS hardware kan de ICT-afdeling weer platform services draaien en daar bovenop weer eigen software. Beheer kan op afstand worden gedaan vanaf iedere plek.

2.1 De status voor de gemeente Borne

Voor de gemeente Borne wordt een virtuele server omgeving incl. dataopslag gehost door de gemeente Enschede in het rekencentrum van de gemeente Enschede. Hierbij beheert de gemeente Borne de verschillende besturingssystemen op de virtuele servers zelf en beheert zij ook zelf de daarop geïnstalleerde applicaties. Hierbij is het netwerk van de gemeente Borne gescheiden van het netwerk van de gemeente Enschede door toepassing van virtuele LAN's[1] en firewalls.
Een deel van de applicaties die door de gemeente Borne worden gebruikt staan al in een Cloud omgeving, hierbij valt te denken aan:

- VOIP telefonie in de KPN cloud (weliswaar staat deze voor een deel in het rekencentrum van de gemeente Enschede) (SaaS).
- Office365 Teams in de Microsoft cloud (SaaS).
- Daarnaast worden 30% van de vakapplicaties ook uit de Cloud onttrokken de overige applicaties zijn nog op de servers van Borne geïnstalleerd. Hieronder een overzicht.

[1] *LAN staat voor Local Area Network. Met LAN wordt een groep computers lokaal met elkaar worden verbonden. Deze techniek wordt ook voor draadloos internet gebruikt, beter bekend als WLAN.*



3 Uitgangspunten en afwegingskader voor de gemeente Borne

3.1 Uitgangspunten

Om grip te krijgen op de ontwikkelingen omtrent Cloud en Cloudgebruik zijn uitgangspunten opgesteld. Deze uitgangspunten zijn leidend bij het maken van keuzes als het gaat om wel of niet gebruik maken van een Cloud oplossing.

De uitgangspunten zijn:

1. De gemeente huldigt het principe ‘Cloud tenzij…..’ voor het gebruik van applicaties voor de primaire en secondaire processen in de Cloud;
2. Voor het maken van een afgewogen keuze of een informatiesysteem in de Cloud gebruikt mag en kan worden, wordt gebruik gemaakt van het afwegingskader in dit document;
3. Uitbesteding is goedgekeurd door de teamleider die verantwoordelijk is voor het informatiesysteem. De gemeente blijft verantwoordelijk voor de betrouwbaarheid (beschikbaarheid, exclusiviteit en integriteit) van uitbestede diensten;
4. Op basis van een risicoanalyse wordt bepaald wat de beschikbaarheidseis is van een ICT-voorziening en wat de impact bij uitval is. Afhankelijk daarvan worden maatregelen bepaald, zoals automatisch werkende mechanismen om uitval van (fysieke) ICT-voorzieningen, waaronder verbindingen, dataopslag en/of lokale applicaties op te vangen;
5. Beveiligingskenmerken, niveaus van dienstverlening en eisen voor beheer van alle netwerkdiensten behoren te worden geïdentificeerd en zijn opgenomen in elke overeenkomst voor netwerkdiensten, zowel voor diensten die intern worden geleverd als voor uitbestede diensten;
6. Op basis van voorspellingen van het gebruik wordt actie genomen om tijdig de benodigde uitbreiding van capaciteit te bewerkstelligen;
7. Er zijn continuïteitsplannen voor het herstel van incidenten, zoals aanvallen met virussen waarin minimaal maatregelen voor back-ups en herstel van gegevens en programmatuur zijn beschreven;
8. Bij transport van vertrouwelijke informatie over onbetrouwbare netwerken, zoals het internet, dient altijd geschikte encryptie te worden toegepast;
9. Gegevensuitwisseling tussen vertrouwde en niet vertrouwde zones dient inhoudelijk geautomatiseerd gecontroleerd te worden op aanwezigheid van malware;
10. Er worden afspraken gemaakt over de inhoud van rapportages, zoals over het melden van incidenten en autorisatiebeheer;

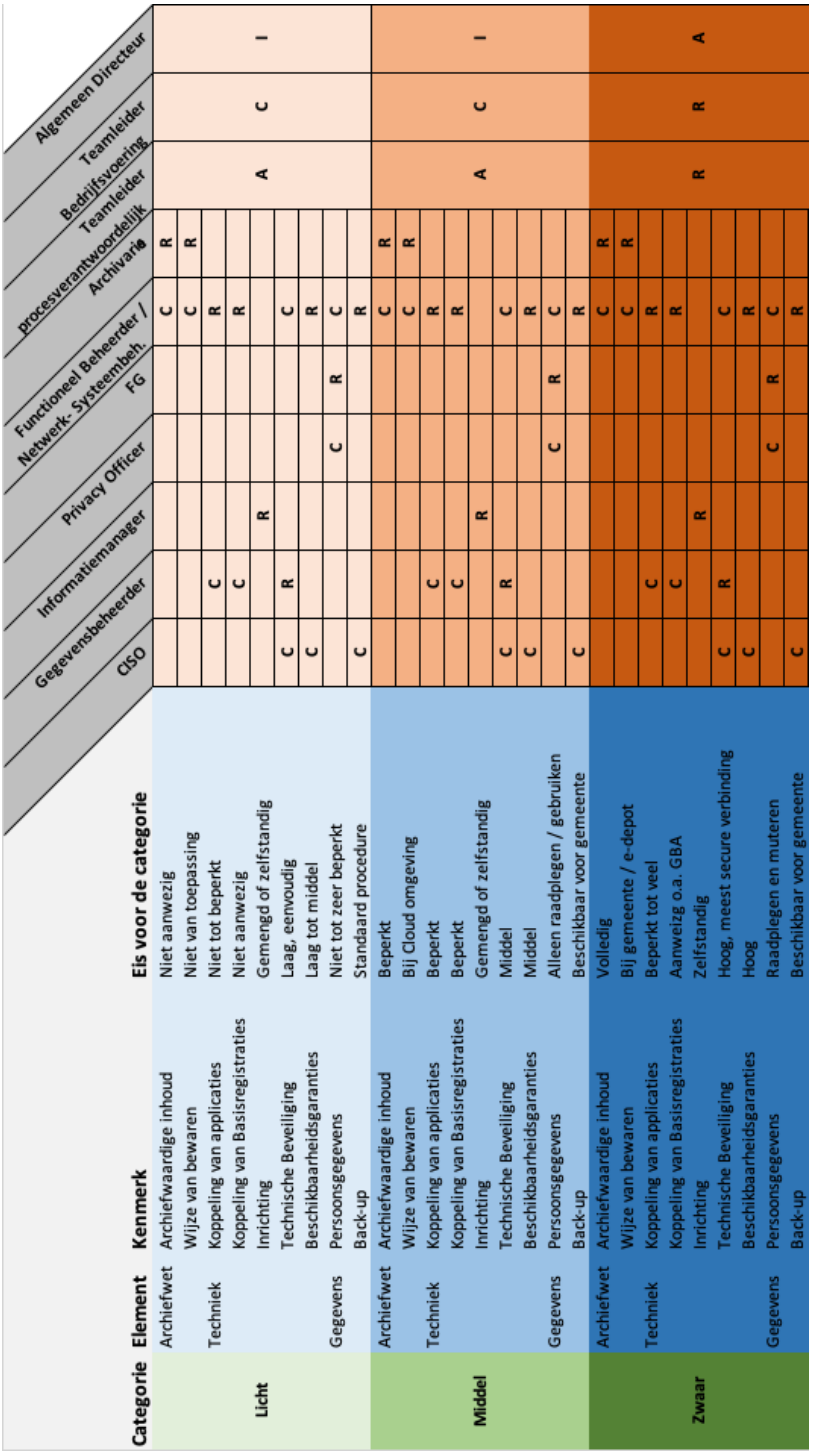
11. De in de bewerkersovereenkomst of dienstverleningscontracten vastgelegde betrouwbaarheidseisen worden gemonitord. Dit kan bijvoorbeeld door audits of rapportages en gebeurt minimaal eens per jaar (voor ieder systeem);
12. Er zijn voor beide partijen eenduidige aanspreekpunten;
13. In het geval van verwerking van persoonsgegevens is er een bewerkersovereenkomst;
14. De gemeente blijft ten alle tijden eigenaar van de opgeslagen data. Er worden vooraf afspraken gemaakt over de format waarop data beschikbaar wordt gesteld na beëindiging van de overeenkomst.
15. Bij aanbestedingen worden de GIBIT-voorwaarden als uitgangspunt genomen.

3.2 Afwegingskader

Om een onderbouwde keuze te maken voor het wel of niet in de cloud plaatsen van een applicatie of omgeving is een afwegingskader gewenst. Met behulp van dit afwegingskader wordt de applicatie ingedeeld in een categorie. De categorie bepaalt welke personen en rollen advies moeten uitbrengen over de stap naar de cloud en waar het mandaat ligt voor besluitvorming. Hierbij wordt vooral gekeken naar inhoudelijke kant van de applicatie en dan met name naar de daarin gebruikte / verwerkte gegevens.

In het afwegingskader zijn de volgende onderdelen opgenomen:
- Wegingscategorie, deze kent 3 niveaus:
    - Licht: applicatie bevat geen tot weinig privacy gevoelige gegevens, is niet bedrijfskritisch en is niet archiefwaardig;
    - Middel: applicatie bevat gegevens die, evt. in combinatie met andere gegevens, herleidbaar zijn tot personen;
    - Zwaar: applicatie bevat persoonsgegevens, is bedrijfskritisch en of bevat archiefwaardige informatie.
- De functies en rollen, die een rol kunnen spelen bij de beoordeling / besluitvorming
    - Algemeen Directeur
    - Teamleider bedrijfsvoering
    - Teamleider procesverantwoordelijke
    - Chief Information Security Officer (CISO)
    - Gegevensbeheerder
    - Privacy officer
    - Functionaris voor de gegevensbescherming
    - Functioneel beheerder
    - Gemeentelijk archivaris
- Eisen aan de omgeving waar de applicatie gaat draaien, waarbij onderdelen zijn:
    - Fysieke locatie technische omgeving (in Nederland of Europese Unie)
    - Gescheiden of gedeelde omgeving
    - Wijze van back-up en recovery
    - Technische beveiliging (o.a. verbindingen)

In onderstaand diagram is het afwegingskader uitgewerkt. Uitgangspunt is dat door de vaststelling van het cloudbeleid, en daarmee ook voor dit afwegingskader, het college akkoord gaat met het afwegingskader en de bijbehorende mandaten voor besluitvorming.



Categorie	Element	Kenmerk	Eis voor de categorie	CISO	Gegevensbeheerder	Informatiemanager	Privacy Officer	Functioneel Beheerder / Netwerk- Systeembeh.	procesverantwoordelijk Archivaris	Teamleider Bedrijfsvoering	Teamleider	Algemeen Directeur
Licht	Archiefwet	Archiefwaardige inhoud	Niet aanwezig					C	R			
		Wijze van bewaren	Niet van toepassing					C	R			
	Techniek	Koppeling van applicaties	Niet tot beperkt		C			R				
		Koppeling van Basisregistraties	Niet aanwezig		C			R				
		Inrichting	Gemengd of zelfstandig			R				A	C	I
		Technische Beveiliging	Laag, eenvoudig	C	R			C				
		Beschikbaarheidsgaranties	Laag tot middel	C				R				
	Gegevens	Persoonsgegevens	Niet tot zeer beperkt				C	R	C			
		Back-up	Standaard procedure	C				R				
Middel	Archiefwet	Archiefwaardige inhoud	Beperkt					C	R			
		Wijze van bewaren	Bij Cloud omgeving					C	R			
	Techniek	Koppeling van applicaties	Beperkt		C			R				
		Koppeling van Basisregistraties	Beperkt		C			R				
		Inrichting	Gemengd of zelfstandig			R				A	C	I
		Technische Beveiliging	Middel	C	R			C				
		Beschikbaarheidsgaranties	Middel	C				R				
	Gegevens	Persoonsgegevens	Alleen raadplegen / gebruiken				C	R	C			
		Back-up	Beschikbaar voor gemeente	C				R				
Zwaar	Archiefwet	Archiefwaardige inhoud	Volledig					C	R			
		Wijze van bewaren	Bij gemeente / e-depot					C	R			
	Techniek	Koppeling van applicaties	Beperkt tot veel		C			R				
		Koppeling van Basisregistraties	Aanweizg o.a. GBA		C			R				
		Inrichting	Zelfstandig			R				R	R	A
		Technische Beveiliging	Hoog, meest secure verbinding	C	R			C				
		Beschikbaarheidsgaranties	Hoog	C				R				
	Gegevens	Persoonsgegevens	Raadplegen en muteren				C	R	C			
		Back-up	Beschikbaar voor gemeente	C				R				

RACI staat voor:
R (Responsible, NL: Verantwoordelijk).
A (Accountable, NL: Eindverantwoordelijk).
C (Consulted, NL: Geraadpleegd).
I (Informed, NL: Geïnformeerd).

4 Conclusie

De ontwikkelingen omtrent Cloud zijn niet tegen te houden, het is een algemene marktontwikkeling op alle onderdelen van de ICT. De gemeente Borne omarmd Cloud computing en is van mening dat deze bij draagt aan het toekomstbestendig zijn van de organisatie.

Cloud computing is niet een ontwikkeling op zichzelf. Dit is onderdeel van de brede zin van de digitale transformatie[2] waar elke gemeente zich in bevind. Dit gaat niet alleen over inzet van ICT-producten, maar ook over ontsluiting en gebruik van data t.b.v. de bedrijfsvoering en beleidsvorming en verantwoording. Daarom wordt ook geïnvesteerd in de professionalisering van de I&A-omgeving van Borne. Dit betekent niet alleen de omvorming van team ICT naar I&A (informatievoorziening & Automatisering), maar professionaliseren van gegevensbeheer, realiseren van dashboards door ontsluiting van informatie en meervoudig gebruik er van en aansluitend het belang van Informatie- en privacybeveiliging. Kortom ICT als gebruiksmiddel wordt steeds een strategische Informatievoorziening (IV).

Belangrijk is dat bij het beoordelen van het aangaan van een samenwerking met een leverancier met een Cloud oplossing / omgeving te toetsen aan de uitgangpunten en het afwegingskader (zoals opgenomen in hoofdstuk 3), de risico's van cloud gebruik te wegen (checklist in bijlage 2) en de belangrijke onderdelen voor het contract te toetsen (checklist in bijlage 1).

De overgang naar applicaties in de cloud betekent ook een andere financieringssystematiek voor ICT-middelen van investeringskredieten naar exploitatiebegroting. Waar voorheen er een krediet aangevraagd werd om te investeren in een nieuwe toepassing (of vervanging). Gaat het nu om een structurele exploitatiekosten (licentie- en gebruikerskosten). Het is noodzakelijk om de reguliere ICT-budgetcyclus te wijzigen, d.w.z. hogere structurele kosten en minder investeringskosten.

[2] *Digitale transformatie is een fundamenteel nieuwe benadering van klantervaring, dienstverlening en processeninrichting. Het gaat om het vinden van nieuwe manieren om meerwaarde te creëren voor burgers en ondernemers en de efficiëntie van de bedrijfsvoering te verbeteren. Bedrijven gebruiken daarvoor innovatieve technologieën.*

Bijlage 1 Checklist voor contract bij Clouddienst

In het geval de gemeente gebruik wil gaan maken van een Clouddienst moeten een aantal zaken meegenomen worden in het op te stellen contract.

Er moet aandacht zijn voor:

- Specifieke beveiligingsmaatregelen afkomstig uit een risicoanalyse of de BIO
- Het verplicht melden van beveiligingsincidenten aan de gemeente
- Looptijd van het contract
- Beschrijving van basispakket en aanvullende (optionele) diensten en de daarvoor gehanteerde tarieven
- Een escrow regeling[3] (of Cloud escrow regeling)
- Software licenties (van wie zijn deze en mogen deze in een Cloud worden gebruikt)
- Conversie van gegevens
- Overdacht van gegevens van- en naar de Cloud-omgeving
- Vernietiging van gegevens bij contract beëindiging
- Continuïteit van het systeem
- Overdracht naar een andere leverancier
- Back-up en uitwijk voorzieningen
- Locatie gegevens en programmatuur
- Additionele regels bij persoonsgegevens (bewerkersovereenkomst)
- Geheimhoudingsovereenkomst
- Encryptie, versleutelen van gegevens
- Onderaanneming en overdracht van rechten en plichten (of geen onderaanneming toestaan)
- Opschortingsrecht
- Naleving wet- en regelgeving
- Logging gegevens kunnen opvragen en inzien
- Het recht om audits te mogen (laten) uitvoeren over alle afspraken
- Welk recht van toepassing is
- Exit regels: wat als je de Cloud provider wilt verlaten, of de gegevens/diensten wilt migreren naar een andere provider? Hier wordt in de praktijk weinig over nagedacht
- Beheerafspraken

[3] Escrow regeling: de broncode van de software wordt veilig gesteld bij een escrow-agent, zodat bij bijvoorbeeld faillissement van een leverancier de, de bronbestanden en het gebruikersrecht ter beschikking komen van de klant. Voor Cloud-escrow gaat het m.n. om het veiligstellen van de data.

Bijlage 2 Checklist weging risico's en maatregelen bij Cloud gebruik

Het gebruik van Cloud omgevingen / oplossingen brengen risico's met zich mee. De wijze van inrichting en samenwerking maken dat deze in meer of mindere mate spelen.

Een aantal belangrijke risico's zijn:

Verlies van besturing (governance)
De afnemer legt een deel van de besturing in handen van de leverancier, dit betreft ook informatiebeveiliging.

Eventuele maatregelen: verwerkingsovereenkomst, beschikbaarheidsgaranties (boete clausule), audits (pentest)

Leverancier lock-in
Leveranciers hebben nog weinig te bieden aan tools, procedures of services om te kunnen migreren naar een andere Cloud-leverancier. Daarmee ontstaat het risico dat men, met een eenmaal gemaakte keuze, voor langere tijd vastzit aan die leverancier en dat het lastig wordt om Cloud-diensten te verhuizen.

Eventuele maatregelen: afspraken over exit, eigendom van data en termijn van beschikbaarheid stelling

Omgeving afschermingsfouten bij gedeelde omgevingen (isolation failure)
In de definitie van Cloud Computing staat onder andere dat meerdere afnemers kunnen werken met software die hetzelfde is waarbij de data wel gescheiden wordt. Dit brengt het risico met zich mee dat de mechanismes falen die zorgen voor het scheiden van opslag, geheugen en routering tussen de verschillende afnemers. Dit is vooral van toepassing bij SaaS omgevingen.

Eventuele Maatregelen: inzicht in en afspraken over maatregelen van leveranciers om dit te voorkomen resp. boeteclausule

Compliance risico's
Het is lastig om bijvoorbeeld als afnemer, zelf een audit uit te (laten) voeren over een dienst die heel ergens anders wordt gehost of geleverd. Afgezien daarvan moet men ook kunnen vertrouwen op auditrapporten of -certificeringen die op verzoek kunnen worden aangeleverd. Men kan ook slecht controle uitoefenen of er wel binnen de kaders van bepaalde wetten wordt omgegaan met gegevens van de afnemer.

Eventuele Maatregelen: Afspraken over tonen auditrapporten en – certificeringen op regelmatige basis.

Gegevensbeveiliging
Het beheer van de Cloud door de Cloud-aanbieder voegt een risico toe dat beheerders overal bij kunnen van alle Cloud-afnemers.

Eventuele Maatregelen: inzicht in en afspraken over maatregelen van leveranciers om dit te voorkomen

Gegevensbeveiliging verwachting
De verwachting van de beveiliging van de Cloud-dienst van de afnemer kan verschillen met die van de Cloud-aanbieder. Daarnaast kan de aanbieder in het kader van kostenreductie keuzes maken die de beveiliging doen afnemen die de afnemer niet zou willen.

Eventuele Maatregelen: afspraken maken over verplichting om melding te doen van wijziging beveiligingsmaatregelen. Eventuele exit-voorwaarden als gaat om wijziging van beveiligingsniveaus.

Onveilige of onvolledige verwijdering van gegevens

Als een gegeven in de Cloud verwijderd moet worden hoeft dat niet te resulteren in echte verwijdering, bijvoorbeeld doordat er data op andere plaatsen staat die vergeten wordt (back-up). Bovendien is het fysiek verwijderen van data door het vernietigen van het opslag medium vaak niet te doen omdat andere afnemers van Cloud-diensten ook gebruik maken van bijvoorbeeld een disk. Daarnaast heeft men geen controle over hergebruik van apparatuur of her inzet van Cloud resources voor andere Cloud-afnemers.

Eventuele Maatregelen: Auditrapport van gecertificeerde organisatie voor verwijdering van data.

Uitbreiding perimeter

Met het afnemen van Cloud-diensten wordt ook het eigen domein vergroot waar men verantwoordelijk voor is. Dus waar men standaard alleen hoefde te kijken naar het eigen fysieke pand of de panden wordt de beveiligingsfocus nu verlegd naar een grotere en moeilijker te controleren omgeving.

Eventuele Maatregelen: uitwijkmogelijkheden leverancier toetsen en contractueel vastleggen.

Beschikbaarheid en continuïteit.
Met het gebruiken van Cloud-diensten wordt Internet connectiviteit (of een andere breedbandige verbinding) van de afnemer ineens een grotere afhankelijkheid en dus een risico voor continuïteit.