



gemeente
Barneveld

Zaaknr. 1103254

Collegevoorstel

Onderwerp:

Kadernotitie Cloudbeleid

Gevraagde beslissing:

1. Vaststellen van de kadernotitie Cloudbeleid
2. Instemmen met de in hoofdstuk 3 genoemde condities waarbinnen een digitale oplossing of infrastructureel onderdeel in de cloud afgenomen wordt
3. Instemmen met de in hoofdstuk 4 genoemde procesmaatregelen waarmee de werkwijze van de cloudgang van applicaties of infrastructurele onderdelen wordt geborgd
4. Instemmen met de jaarlijkse evaluatie van het cloudbeleid en indien nodig bijstellen van de condities, werkwijze en procesmaatregelen

Raad

- ☒ Ter kennisname naar de raad
Nummer beleidsproduct:
- ☐ Op overzicht Bestaand beleid (website)

Datum: 26 april 2019

Steller: A.H. Scholing

Afd: Team Informatie en Automatisering

Aantal bijlagen 1

Afd.hoofd:

Portefeuillehouder

A.M. Van de Burgwal

Openbaarheid

Besluit (voorblad) openbaar: ☒ Ja ☐ Nee, zie beslispunt :
Groentje openbaar: ☒ Ja ☐ Nee, zie beslispunt :
Bijlagen openbaar: ☒ Ja ☐ Nee, vermelden op bijlage

	Akkoord	Bespreken	Aantekeningen
Secretaris			
Burgemeester			
Wethouder A. de Kruijf			
Wethouder P.J.T. van Daalen			
Wethouder A.H. van de Burgwal			
Wethouder D. J. Dorrestijn-Taal			

Beslissing burgemeester en wethouders :

conform advies
II

27 JUNI 2019

Nummer op besluitenlijst:

26/12

1. Inleiding

Op 14 september 2017 heeft het college van B&W in het kader van de heroriëntatie IT-strategie ingestemd met de uitgangspunten van het cloudbeleid. In de toen onderliggende notitie werden ook de contouren van dit beleid beschreven met de randvoorwaarde dat een beleidsproces ten behoeven van cloudtechnologie verder diende te worden uitgewerkt. Deze uitwerking is nu vastgelegd in de kadernotitie cloudbeleid 'Veranderproces naar een schaalbare en flexibele ICT-omgeving'.

Op dit moment wordt het beleids- en uitvoeringsplan 'Digitaal Werken' opgesteld. In dit beleidsplan zal verwezen worden naar deze kadernotitie cloudbeleid als één van de belangrijke veranderingen die nodig zijn voor een toekomstbestendige ICT-omgeving. In de voorliggende kadernotitie 'Cloudbeleid' wordt uitgebreider dan in het beleidsplan 'Digitaal Werken' beschreven:

- wat cloudtechnologie is
- welke kansen cloudtechnologie biedt
- welke bedreigingen er zijn
- welke kaders er (nodig) zijn bij het gebruik van cloudtechnologie
- welke werkwijze en procesmaatregelen nodig zijn om gebruik te maken van cloudtechnologie

Cloudtechnologie biedt kansen om de ICT-omgeving flexibeler te maken. Cloudtechnologie brengt met zich mee dat er eenvoudiger van verschillende devices als pc, laptop, tablet en smartphone gebruik gemaakt kan worden en biedt nieuwe mogelijkheden voor werknemers om in projecten en teams samen te werken, maar ook met burgers en andere organisaties. Nieuwe digitale oplossingen kunnen sneller geïmplementeerd worden en zijn minder afhankelijk van één ICT-infrastructuur. Door de dataopslag in het rekencentrum als cloudservice af te nemen wordt deze eenvoudig schaalbaar en gebruiken we alleen de opslag die we nodig hebben.

2. Beoogd effect

a) Meetbaar effect

- Een toename van het aantal digitale oplossingen en ict-onderdelen dat middels cloudtechnologie wordt afgenomen.
- Afname van het aantal digitale oplossingen en ict-onderdelen dat via het eigen rekencentrum beschikbaar gesteld wordt of werkt

b) Maatschappelijk effect

- Door gebruik te maken van oplossingen en infrastructuur in de cloud zullen burgers en bedrijven merken dat de gemeentelijke organisatie sneller oplossingen kan bieden die aansluiten bij hun behoefte. Te denken valt bijvoorbeeld aan gebruiksvriendelijke apps om te melden, informatie te ontvangen, maar ook oplossingen die samenwerken aan projecten en comités goed faciliteren.

3. Argumenten

2. Conditie cloudgang

Cloudtechnologie biedt kansen om de ICT-omgeving flexibeler en schaalbaarder te maken. Maar cloudtechnologie brengt ook bedreigingen met zich mee. Doordat digitale oplossingen nu grotendeels in ons eigen netwerk staan hebben we zelf een grote invloed op het beheer waardoor we zelf grip hebben op randvoorwaarden als:

- Beveiliging tegen ongewenste inzage en gebruik
- Beschikbaarheid en continuïteit
- Exitstrategie
- Privacy

Als digitale oplossingen via cloudtechnologie worden ontsloten leveren we deze sturing over aan de leverancier. Om er zeker van te zijn dat deze randvoorwaarden ook bij cloudtechnologie gewaarborgd blijven zijn het toepassen van diverse (wettelijke) kaders nodig bij de keuze voor cloudgang, keuze van welke cloudtype en goede contractuele borging.

3. Werkwijze en procesmaatregelen

Nog meer dan nu al het geval is, is het nodig dat een idee waarvoor een ICT-oplossing gezocht of vervangen wordt, afgewogen en aan de condities en kaders getoetst wordt via een vastgestelde

werkwijze met duidelijke procesmaatregelen. Dit biedt de zekerheid dat voor elke nieuwe aanschaf van een digitale oplossing een afgewogen 'cloudkeuze' wordt gemaakt met een passende overeenkomst.

3. Jaarlijkse evaluatie cloudbeleid

Toepassing van cloudtechnologie binnen onze gemeentelijke organisatie en binnen overheidsinstanties is nog relatief nieuw. Het toepassen van het principe 'cloud tenzij' is een veranderproces van langere tijd. Inzichten die er nu zijn kunnen door ervaring met de praktijk, verandering van wet- en regelgeving of leveranciersaanbod in de tijd veranderen. Hierop dient het cloudbeleid regelmatig bijgesteld te worden om op een verantwoorde wijze gebruik te maken van cloudtechnologie.

4. Kanttekeningen

Het toepassen van cloudtechnologie is nieuw binnen de gemeentelijke organisatie. Hierdoor ontstaat behoefte aan nieuwe competenties en rollen. Er zal een toenemende behoefte zijn aan de rol van informatieadviseur, inkoopadviseur, privacy officer en ciso (adviseren en orkestreren van het cloudwerkproces) en de rol van regievoerder (controle op naleving van de contracten). Daarnaast zal een verschuiving optreden bij het technisch ICT-beheer (technisch beheer wordt meer door de leveranciers gedaan, internetverbindingen worden belangrijker). Deze veranderingen zullen door de teamleider I&A samen met team P&O begeleidt en verder ingevuld worden.

5. Financiën

De financiële consequenties van het cloudbeleid zijn al bij de besluiten over de heroriëntatie IT-strategie meegenomen.

6. Uitvoering

Planning:

Het toepassen van het cloudbeleid is een groeiproces. De cloudgang van bestaande digitale oplossingen hangt af van de wens tot gebruikmaken van nieuwe mogelijkheden of het aflopen van de bestaande contracten en oplossingen die leveranciers bieden.

Communicatie:

De organisatie zal op een laagdrempelige wijze geïnformeerd worden over de inhoud van de kadernotitie cloudbeleid, waarbij de nadruk zal liggen op de kansen, bedreigingen en de cloudwerkwijze.

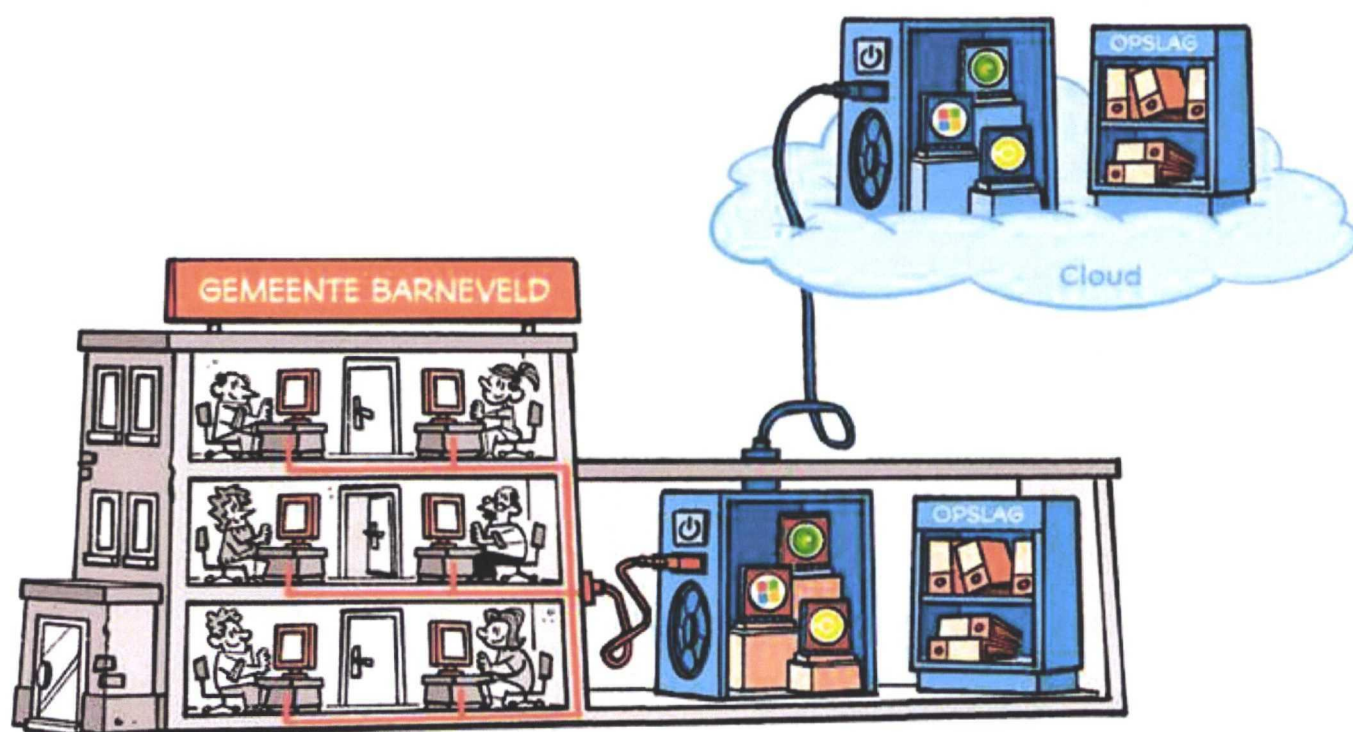
Evaluatie/controle

Conform beslispunt 3 zal het cloudbeleid ieder jaar geëvalueerd worden, waarbij ingrijpende aanpassingen op de huidige besluiten opnieuw aan het college zullen worden voorgelegd,

7. Bijlagen

Kadernotitie Cloudbeleid 'Veranderproces naar een schaalbare en flexibele ICT-omgeving'

VERANDERPROCES NAAR EEN SCHAALBARE EN FLEXIBELE ICT-OMGEVING



KADERNOTITIE CLOUDBELEID

Deze kadernotitie gaat niet over een technische zaken. Een beschrijving van wat Cloud computing is, is weliswaar nodig, maar goed beschouwd gaat het in deze notitie vooral over de wijze waarop we **samen een verander-, leer- en verbeterproces van een traditionele ICT-omgeving naar een toekomstgerichte ICT-omgeving vormgeven**. Daarom beschrijft deze kadernotitie:

- ✓ de visie op cloud: het waarom, de kansen en de bedreigingen
- ✓ de kaders voor cloud: waar moeten we rekening mee houden bij cloudgang
- ✓ welke werkwijze en procesmaatregelen we rond het gebruik van cloud samen afspreken

Omdat deze kadernotitie belangrijk is voor verschillende groepen wordt gestart met een voor iedereen leesbare samenvatting.

Tot stand gekomen met medewerking van o.a.:

Chief Information Security Officer (CISO)

Thomas Arends

Privacy Officer (PO)

Corry-Anne van der Tang

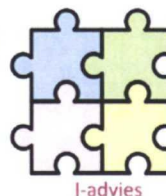
Cloud architecten

Harry Kuijlaars en Falco Dam

Door:

Strategisch informatie adviseur

Anno Scholing



Afbeelding voorzijde:

Verbeelding van de situatie op basis van de genomen besluiten in het kader van cloud: 'software in cloud, tenzij' en 'eigen ICT-infrastructuur vervangen door ingehuurde' (op eigen locatie)'



SAMENVATTING

AANLEIDING

In 2017 heeft Native Consulting het onderzoeksrapport 'Herorientatie IT-strategie' opgeleverd. In dit rapport is vastgesteld dat cloudtechnologie een belangrijke aanjager van veel ontwikkelingen is. Wil de gemeente Barneveld ontwikkelen naar een moderne data-gedreven, dienstverlenende organisatie dan is een belangrijke randvoorwaarde dat een cloudbeleid wordt gedefinieerd. In navolging van deze conclusies heeft het college van B&W eind 2017 besloten om in te stemmen met de uitgangspunten van het cloudbeleid, kort gezegd:

- cloud tenzij
- het eigen datacenter wordt afgebouwd en onderdelen worden ondergebracht in een extern datacenter (co-locatie) met toegang voor haar eigen systeembeheerders

Op dit moment wordt het beleids- en uitvoeringsplan 'Digitaal Werken' opgesteld. In dit beleidsplan zal cloudtechnologie aangegeven worden als één van de belangrijke veranderingen. In deze kadernotitie Cloudbeleid wordt uitgebreider dan in het beleidsplan 'Digitaal Werken' beschreven wat cloudtechnologie inhoudt, wat de kansen en bedreigingen zijn, met welke kaders we de bedreigingen in de hand houden en borgen en welke werkwijze we in onze organisatie daarvoor afspreken.

WAT IS CLOUD?

Met cloudtechnologie worden digitale oplossingen met bijbehorende data niet meer op de eigen ICT-infrastructuur van onze organisatie geïnstalleerd en beschikbaar gesteld, maar staat deze software met bijbehorende data in een externe datacenter elders in de wereld en wordt deze door een leverancier aangeboden als dienst via internet.

Daarnaast is het mogelijk om ook de ICT-infrastructuur geheel of gedeeltelijk als dienst af te nemen in plaats van deze in een eigen datacenter te plaatsen.

Op dit moment staat circa 95% van al onze digitale oplossingen in een eigen datacenter van onze organisatie. Met de nieuwe uitgangspunten zullen, waar dit mogelijk is, alle digitale oplossingen bij nieuwe aanschaf of bij vervanging in de cloud geplaatst worden. Dit zelfde geldt ook voor onderdelen in het eigen datacenter.

WAAROM CLOUD?

De in de inleiding genoemde conclusies en besluiten ten aanzien van cloud technologie passen uitstekend bij het coalitieakkoord 2018-2022, waarin onder andere gesteld wordt dat de gemeente Barneveld een uitstekende kwaliteit van dienstverlening biedt voor het verzamelen en delen van informatie en diensten via een samenhangende en geïntegreerd digitaal platform. Ditzelfde geldt ook voor de in de organisatievisie verwoorde visie en ambitie dat we werken met slimme moderne digitale middelen waarmee we informatie makkelijk beschikbaar stellen.

Cloud technologie stelt ons namelijk in staat om flexibel digitale middelen aan te bieden aan de burgers en de medewerkers in onze organisatie doordat:

- de software of hardware al klaar staat bij een leverancier en er dus een minder langdurig implementatietraject nodig is;



SAMENVATTING

- we minder afhankelijk zijn van type besturingssysteem of database;
- meer leveranciers innovatieve oplossingen kunnen bieden dan nu het geval is;
- het gebruik van verschillende devices in de regel beter ondersteund wordt;
- er meer mogelijkheden geboden worden die samenwerken binnen en buiten de organisatie mogelijk maken.

Cloud technologie maakt daarnaast schaalbaarheid mogelijk doordat door inhuur van externe dataopslag de opslagcapaciteit op elk moment snel verlaagd of verhoogd kan worden.

Door gebruik te maken van oplossingen en infrastructuur in de cloud zullen burgers en bedrijven merken dat de gemeentelijke organisatie sneller oplossingen kan bieden die aansluiten bij de behoefte. Te denken valt bijvoorbeeld aan gebruiksvriendelijke apps om te melden of informatie te ontvangen, maar ook oplossingen die samenwerken aan projecten goed faciliteren.

WAT IS NODIG VOOR CLOUDGANG?

Tegenover de kansen levert cloudtechnologie ook een aantal mogelijke bedreigingen op. Doordat digitale oplossingen niet meer door onszelf beheerd worden, komt een deel van de sturing in de handen van de leverancier te liggen. Daarom moeten onder andere veiligheid, privacy, beschikbaarheid, continuïteit en compliance van cloudoplossingen op een goede manier gewaarborgd worden. Dit doen we door cloudoplossingen steeds te toetsen aan belangrijke (wettelijke) kaders als de Baseline Informatiebeveiliging Gemeenten (BIG, ingaande 1-1-2020 wordt dit de BIO=Baseline Informatiebeveiliging Overheid), de Algemene Verordening gegevensbescherming (AVG), dataclassificatie en het Gemeentelijk Model Architectuur (GEMMA) en in contracten de gemeentelijk inkoopvoorwaarden bij IT (GIBIT) toe te passen en de juiste verwerkings-overeenkomsten en Service Level Agreement (SLA)'s af te sluiten.

Realisatie van het cloudbeleid is een continu proces van verandering en verbetering, want niet alle digitale oplossingen kunnen zomaar vervangen worden door een cloudvariant, omdat leveranciers nog geen goed alternatief bieden. Om een goed proces van cloudgang te garanderen is het volgende nodig:

- Nieuwe of versterking van rollen/competenties zoals informatie-advies, cloud-architect, registreren van de afspraken en projectleiding) zijn nodig terwijl andere rollen/competenties (technisch beheer) op termijn veranderen. Werving, opleiding en instructie van medewerkers zijn daarom belangrijke activiteiten;
- Om te zorgen dat steeds nagedacht wordt over toe te passen cloudoplossingen en de toepassing van de verschillende kaders en de aankoop vast te leggen met de juiste contracten, verwerkingsovereenkomsten en SLA's, maken we gebruik van het in hoofdstuk 4 beschreven werkproces
- Jaarlijks het cloudbeleid evalueren en waar nodig aanpassen aan de opgedane ervaringen en veranderende ontwikkelingen
- Onder de kop 'bedrijfsvoering' in het afdelingsplan benoemen welke applicaties in de begroting van het komende jaar worden vervangen door een cloudoplossing



1 WAT IS CLOUD

Clouddiensten worden gebruikt om via het internet, of een andere breedbandige verbinding gebruik te maken van hardware, software en gegevens óf deze beschikbaar te stellen aan anderen. Deze Cloud kan zich overal bevinden.

Het woord Cloud komt van het woord 'wolk' waarmee in een netwerkontwerp 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 deze wolk 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. Omdat men niet altijd precies weet waar afgenomen clouddiensten zich bevinden, is wetgeving relevant voor de afgenomen Clouddiensten.

Bij Cloud Computing wordt vaak gebruik gemaakt van hardware die het mogelijk maakt om flexibel te schalen naar de behoefte van de eindgebruiker. Men zou kunnen zeggen dat het gaat om virtuele infrastructuur en diensten. Met Cloud Computing worden servers, desktops en ook applicaties gevirtualiseerd. Dit heeft zowel voordelen als nadelen.

Soorten Cloud Computing

Cloud Computing kan op verschillende manieren worden toegepast. Er zijn 3 verschillende vormen: een externe of publieke Cloud, waarbij diensten en gegevens bij een externe partij zijn opgeslagen, een private Cloud binnen bijvoorbeeld een rekencentrum van een gemeente, en er is een hybride vorm.

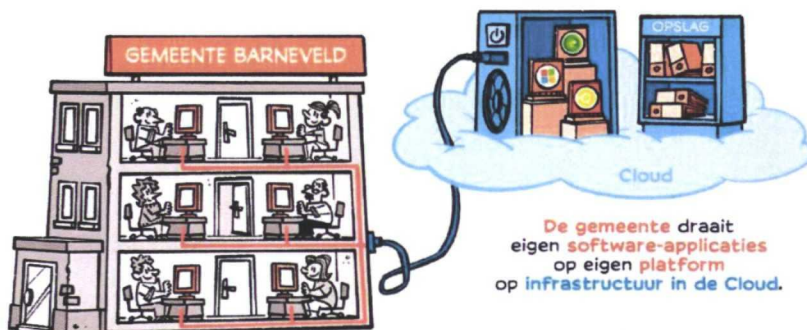
- Bij een **publieke of externe Cloud** staan de hardware, software en de gegevens volledig bij de externe dienstverlener en er wordt een generieke (voor alle afnemers gelijke) dienst geleverd.
- Bij een **private Cloud** werkt men op een private ICT-infrastructuur waarop servers/desktops en applicaties worden gevirtualiseerd. In deze Cloud heeft de gemeente de volledige controle over gegevens, beveiliging en kwaliteit van de dienst. Vaak ligt de verantwoordelijkheid voor onderhoud en beheer bij de gemeente zelf maar in de praktijk wordt dit vaak door een leverancier uitgevoerd. De private Cloud kan in een gemeentelijk datacentrum draaien, maar ook bij een leverancier. In dat geval wordt de gevirtualiseerde infrastructuur niet gedeeld met andere klanten.
- Een bijzondere vorm van een private Cloud is de **Community Cloud**, hierbij wordt Cloud-infrastructuur gebruikt door een specifieke groep afnemers die een gemeenschappelijk belang hebben. Denk hierbij aan taak, missie, beveiligingseisen, beleid en naleving eisen. Deze Cloud kan in eigendom zijn en beheerd worden door één van de deelnemers, een derde partij of een combinatie. Men kan hierbij denken aan een overheids-Cloud of een gemeentelijke Cloud.
- De **hybride Cloud** is een combinatie van een publieke en private Cloud. Dat wil zeggen dat er Cloud-diensten worden afgenomen van een derde aanbieder terwijl men daarbij ook gebruik maakt van een eigen Cloud.

FIG. 1: CLOUD-SERVICEMODELLEN

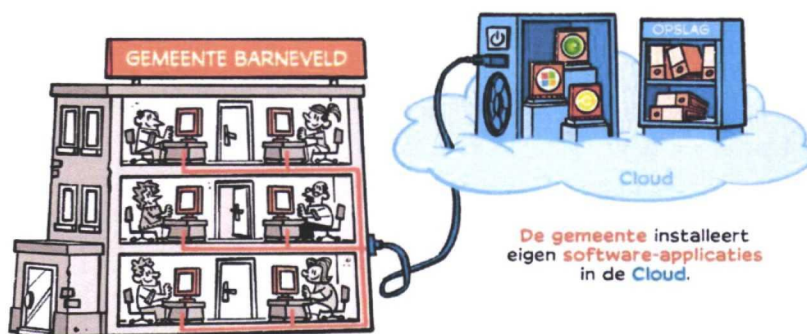
EIGEN REKENCENTRUM



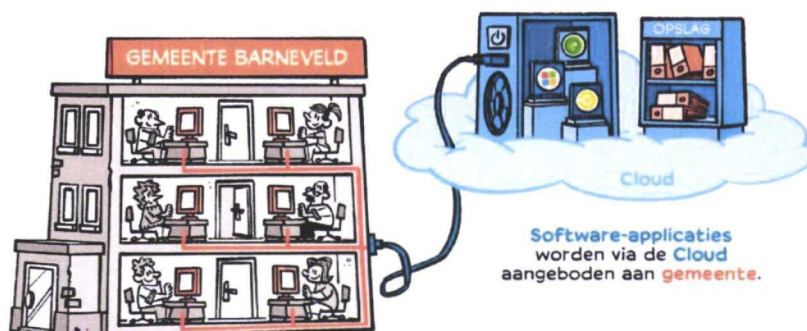
INFRASTRUCTUUR ALS EEN SERVICE



PLATFORM ALS EEN SERVICE



SOFTWARE ALS EEN SERVICE





Servicemodellen Cloud Computing

De volgende manieren van het aanbieden van Cloud Computing worden onderkend. 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. Er zijn verschillende gemeenten die applicaties nu al via een SaaS-model afnemen en dat gebeurt in publieke en private Clouds. Vaak worden hier webapplicaties aangeboden die met moderne technologieën zoals Ajax en HTML5 gemaakt zijn. Voor de eindgebruiker is volledig onduidelijk 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 gemaakt worden 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 uiteindelijk 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.

Genomen besluiten

De gemeente Barneveld heeft geconcludeerd qua ICT-infrastructuur niet klaar te zijn voor de toekomst. Daarom heeft de gemeente een tweetal besluiten genomen waarbij cloud computing een belangrijke rol speelt. Voor Barneveld is Informatisering strategisch. Automatisering is weliswaar randvoorwaardelijk, maar in beginsel geen kerntaak voor de gemeente. Waar mogelijk maakt Barneveld gebruik van cloudconcepten. Dit betekent concreet het volgende:

1) 'Cloud tenzij' voor applicaties

De gemeente Barneveld heeft besloten dat bij selectie en vernieuwing van applicaties bij voorkeur gekozen wordt voor een cloud-variant: 'Cloud, tenzij' in plaats van 'Lokaal, tenzij'.

2) Uitbesteden ICT-infrastructuur en het bijbehorende onderhoud/beheer

Voor de on-premise ICT-infrastructuur kiest Barneveld voor het afbouwen van haar eigen datacenter en het onderbrengen van deze lokale componenten in een extern datacenter (co-locatie) met toegang voor haar eigen systeembeheerders.



1 WAT IS CLOUD

Veranderproces en cloudbeleid

De veranderingen die het gevolg zijn van bovengenoemde besluiten, zullen gestalte krijgen door een langdurig veranderproces. Veel applicaties kunnen nog niet naar de cloud omdat er nog geen cloudvariant beschikbaar is en leveranciers nog veel tijd nodig zullen hebben om deze te ontwikkelen. Ook het veranderen van de huidige ICT-infrastructuur naar een infrastructuur op basis van clouddiensten zal in fases gaan. Omdat cloud computing bij gemeenten nog in ontwikkeling is, zal dit veranderproces ook een leer- en verbeterproces zijn waarin van de praktijk geleerd moet worden en het geleerde omgezet in verbeteringen. Om dit veranderproces goed te ondersteunen heeft het college ingestemd met het definiëren van randvoorwaardelijk cloudbeleid. In deze kadernotitie wordt aan dit cloudbeleid onderbouwing en invulling gegeven.



2 VISIE OP CLOUD

Waarom naar de cloud?

De volgende redenen geven aanleiding om gebruik te maken van cloud computing:

A) Beleidskeuze 'cloud tenzij' leidt tot veranderende ICT-inrichting

Op dit moment staan de meeste applicaties met hun data nog niet in de cloud, maar op onze eigen ICT-infrastructuur. De ontwikkeling van steeds meer applicaties via de cloud maakt dat de opslagcapaciteit kleiner of veranderlijker wordt. Dit vraagt om een maximaal flexibele en schaalbare ICT-infrastructuur. Ook hier worden keuzes gemaakt waar cloud computing een belangrijke rol speelt.

B) Technische innovaties en kwetsbaarheid leiden naar 'betalen naar gebruik'

Technische innovaties zorgen er voor dat steeds meer lagen in de ICT infrastructuur als een generieke dienst kunnen worden afgenomen. Als deze diensten worden aangeboden volgens het principe 'betalen naar gebruik' en self-servicemogelijkheden bieden, dan spreken we van clouddiensten. Voor gemeenten –organisaties met een doorgaans kleine en kwetsbare ICT formatie –verschuift met de komst van clouddiensten de grens van 'zelf doen of uitbesteden/inkopen' steeds meer naar inkopen.

C) Veranderende aanbod van leveranciers leid tot verplichte cloudoplossingen

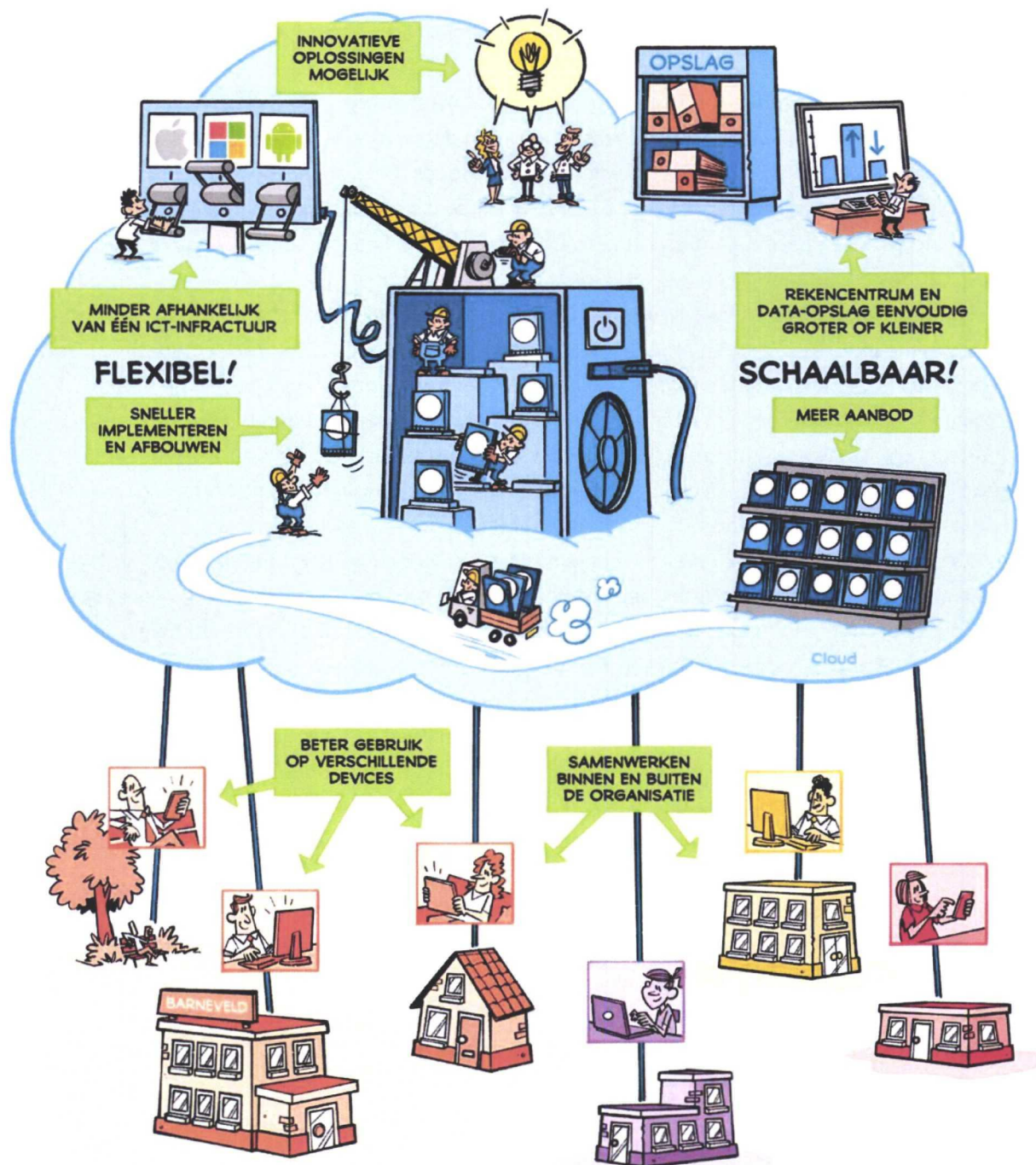
Het aanbieden van software als een service (SaaS) is een onvermijdelijke ontwikkeling. Iedere applicatie leverancier in ons land is bezig haar verdienmodel om te bouwen naar een clouddienst: de klant ontzorgen op het gebied van technisch beheer. Daardoor zal langzaam maar zeker het lokale datacenter krimpen en het technische beheer afnemen. Klassieke onderdelen van de ICT-infrastructuur zoals de kantoorautomatisering en telefonie zullen ook steeds meer als clouddienst worden afgenomen. Zij krijgen steeds meer het karakter van 'water uit de kraan', een nutsvoorziening. De gemeente Barneveld heeft vervolgens geen of weinig keuze meer om applicaties on premise te laten draaien, maar moet overstappen naar cloudoplossingen.

D) Wendbaar inspelen op klantbehoefte leidt tot veranderende ICT-inrichting

De gemeente Barneveld wil graag snel inspelen op schommelingen in de klantbehoeften en landelijke ontwikkelingen. Deze wendbaarheid zoekt de gemeente niet in uitbesteding of samenwerking, maar bij voorkeur door taken zelf te doen. Daarnaast is de gemeente gericht op het blijven vernieuwen en verbeteren van dienstverlening en de manier van werken door de implementatie van bewezen oplossingen.

Om mee te kunnen gaan met de nieuwe ontwikkelingen en de bedrijfsvoering en dienstverlening goed te kunnen ondersteunen is een maximaal flexibele en schaalbare ICT-infrastructuur en -ondersteuning nodig waarmee het eenvoudiger wordt apps of applicaties in gebruik te nemen of te vervangen. Applicaties in de cloud en het uitbesteden van de onderliggende ICT-infrastructuur met behulp van clouddiensten zijn de methoden die helpen om deze ondersteuning te kunnen bieden.

Fig. 2: KANSEN





Kansen en bedreigingen

Kansen

Met het besluit om over te stappen op 'cloud-tenzij' voor applicaties en de onderliggende ICT-infrastructuur en het bijbehorende onderhoud/beheer uit te besteden kiest de gemeente voor een aantal voordelen die ondersteuning bieden aan de opgaven die geformuleerd zijn in de strategische visie en het coalitieakkoord 2018-2022, waaronder dat wij *'een uitstekende kwaliteit van dienstverlening bieden via een samenhangende en geïntegreerd digitaal platform'* en de kernwaarden die geformuleerd zijn in de organisatievisie. Deze voordelen zijn:

Flexibel

Infrastructuur en oplossingen worden met cloud computing flexibeler, omdat:

- ✓ Betere oplossingen om binnen en buiten de organisatie samen te werken mogelijk worden
- ✓ Leveranciers met cloud-oplossingen beter in staat zijn om deze op verschillende devices zoals PC, tablet of smartphone te laten werken
- ✓ Het implementeren en afbouwen van cloud-oplossingen sneller gedaan kan worden, omdat de leverancier ze meestal al klaar heeft staan. Volledige installatie is niet meer nodig
- ✓ Cloud-oplossingen niet meer afhankelijk zijn van één ICT-infrastructuur en platform
- ✓ Innovatieve oplossingen mogelijk worden
- ✓ Er op den duur meer aanbod van oplossingen zal komen, omdat meer leveranciers oplossingen kunnen gaan leveren

Schaalbaar

De ICT-infrastructuur wordt schaalbaar, omdat:

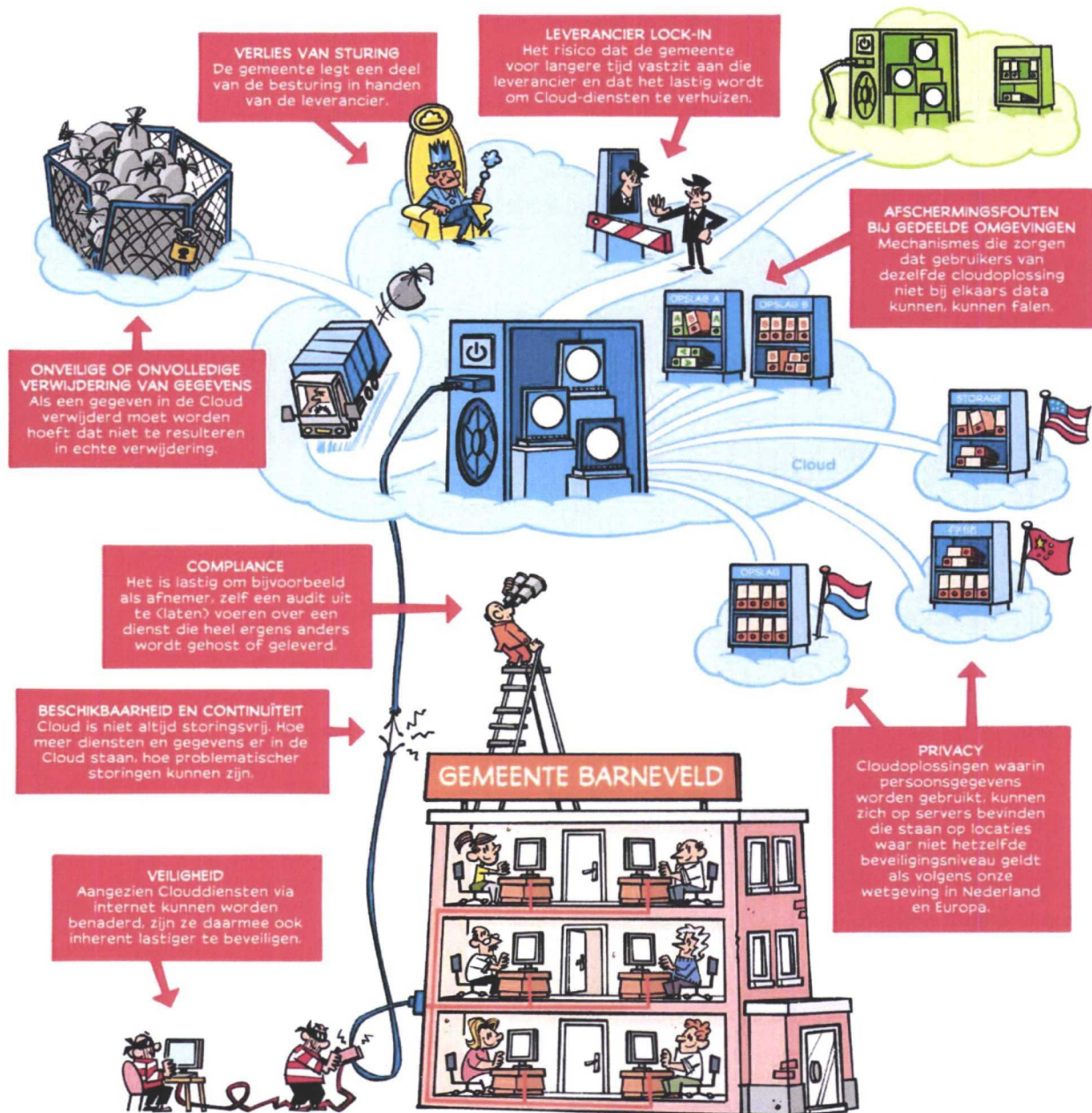
- ✓ Afhankelijk van de behoefte aan de constant veranderende capaciteit en eisen opslagruimte bijgeplaatst of weggehaald kan worden

What is in it voor de burger?

Door gebruik te maken van oplossingen en infrastructuur in de cloud zullen burgers en bedrijven merken dat de gemeentelijke organisatie sneller oplossingen kan bieden die aansluiten bij hun behoefte. Te denken valt bijvoorbeeld aan gebruiksvriendelijke apps om te melden, informatie te ontvangen, maar ook oplossingen die samenwerken aan projecten en comités goed faciliteren.



FIG. 3: BEDREIGINGEN





Bedreigingen

Cloud computing brengt ook een aantal bedreigingen met zich mee. Deze zullen op een vastgestelde wijze geëlimineerd of zo klein mogelijk gemaakt / beantwoord moeten worden. In hoofdstuk 3 en 4 zijn kaders en hulpmiddelen beschreven die zorgdragen voor het opheffen of minimaliseren van de bedreigingen. De risico's van cloud computing zijn:

✓ **Verlies van sturing**

De gemeente legt een deel van de besturing in handen van de leverancier, dit betreft ook informatiebeveiliging

✓ **Leverancier lock-in**

Leveranciers van cloudoplossingen 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

✓ **Afschermingsfouten bij gedeelde omgevingen**

Bij Cloud Computing kunnen meerdere afnemers werken met dezelfde software waarbij de data wel geschieden wordt. Dit brengt het risico met zich mee dat de mechanismes die zorgen voor het scheiden van opslag, geheugen en routing tussen de verschillende afnemers kunnen falen

✓ **Compliance**

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.

✓ **Privacy**

Bij het verwerken van (bijzondere) persoonsgegevens in een cloudoplossing stelt de privacywetgeving hoge eisen aan de inrichting, locatie en beveiliging van persoonsgegevens. Ook de toegankelijkheid van de persoonsgegevens bij het beheer van de Cloud door de Cloud-aanbieder voegt een risico toe voor de vertrouwelijkheid van gegevens, zeker bij meerdere of wisselende beheerders.

✓ **Veiligheid**

Aangezien Clouddiensten via internet kunnen worden benaderd, zijn ze daarmee ook inherent lastiger te beveiligen

✓ **Onveilige of onvolledige verwijdering van gegeven**

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 opslagmedium vaak niet te doen omdat andere afnemers van Clouddiensten ook gebruik maken van bijvoorbeeld een disk.

✓ **Beschikbaarheid en continuïteit**

Cloud is niet altijd storingsvrij. Bij het gebruik van een externe Cloud ben je voor de continuïteit afhankelijk van een derde partij. Hoe meer diensten en gegevens er in de Cloud staan, hoe problematischer storingen kunnen zijn. Daarnaast heb je als afnemer weinig invloed op de volgorde en voortgang bij het oplossen van storingen.



3 KADERS

In het beslisdocument 'De toekomst begint morgen al' zijn een viertal uitgangspunten voor het cloudbeleid vastgesteld, namelijk:

1. Voor Barneveld is Informatisering strategisch. Automatisering is weliswaar randvoorwaardelijk, maar in beginsel geen kerntaak voor de gemeente. Waar mogelijk maakt Barneveld gebruik van cloudconcepten
2. De vervanging van ieder onderdeel van onze ICT-omgeving (zowel applicaties als infrastructuur componenten) zal op dit cloudbeleid worden gebaseerd.
3. Voor iedere databron/component van de ICT-omgeving die in een cloudconcept wordt ondergebracht zal een exitstrategie worden uitgewerkt en overeen gekomen met de leverancier.
4. Voor (resterende) on-premise infrastructuur kiest Barneveld voor het afbouwen van haar eigen datacenter en het onderbrengen van deze lokale componenten in een extern datacenter (co-locatie) met toegang voor haar eigen systeembeheerders
5. Barneveld wil gebruik maken van (standaard) applicaties van leveranciers. Indien deze niet optimaal aansluiten bij de gestelde behoeften en/of manier van werken, dan wordt eerst onderzocht of die aan te passen zijn aan de functionaliteit van de applicatie of dat de applicatie zo ingericht kan worden dat het beter aansluit. Dit betekent ook dat er in principe geen eigen ontwikkelde applicaties meer ontwikkeld zullen worden, tenzij er echt geen fit te creëren is met een applicatie. Ook moeten de momenteel in gebruik zijnde zelf ontwikkelde applicaties beoordeeld worden op vervangbaarheid door standaard applicaties

Deze vier uitgangspunten vormen de basis voor een proces dat gericht is op continu verbeteren van de huidige situatie naar een cloud-tenzij-situatie. Om de bedreigingen te elimineren of te minimaliseren zijn een aantal kaders nodig waarmee we de cloudgang uitvoeren.

Kaders

De doorgroei naar cloud computing is een constant verbeterproces waarbij op geschikte momenten nieuwe applicaties en bestaande applicaties en onderdelen van de infrastructuur in het cloudconcept worden ondergebracht.

Bij het afnemen van clouddiensten worden geen verantwoordelijkheden overgedragen. De gemeente is en blijft verantwoordelijk voor de manier waarop een cloud leverancier omgaat met privacy, informatieveiligheid, digitale duurzaamheid en andere wetgeving. Ook als data in de cloud staat, moeten de gemeente regelen dat zij altijd eigenaar blijft van de data en deze altijd weer over kunnen zetten naar een andere omgeving (data, content en documenten). Dit vraagt om kaders voor het besluitvormingsproces.

Deze kaders worden hieronder beschreven onder de verschillende stappen in het verbeterproces. Hierbij gebruiken we de landelijke standaarden die er reeds op het gebied van cloud zijn. De Informatie Beveiligings Dienst (IBD) en Nationaal Cyber Security Centrum hebben voor de Nederlandse overheid een uitwerking voor cloud gemaakt.



Onder welke condities naar de cloud?

Het proces van continu verbeteren begint steeds bij de vraag onder welke condities en naar welke cloud een applicatie of infrastructureel onderdeel moet gaan. Voor deze overwegingen dient de projectleider in overleg met specialisten (privacy-officer, ciso en cloud-architect) gebruik te maken van de volgende kaders:

Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG/na 1-1-2020 BIO)

In 2012 hebben alle gemeenten de convenant: "Informatieveiligheid Gemeenten" getekend naar aanleiding van de resolutie: "Informatieveiligheid, randvoorwaarde voor de professionele gemeente". Hiermee heeft de gemeente Barneveld zich geconformeerd aan het toepassen/implementeren van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Sinds juli 2017 is er nieuw verantwoordingsnormenkader voor gemeenten geïmplementeerd, Eenduidig Normatief Single Information Audit (ENSIA). De ENSIA verplicht gemeenten o.a. om verantwoording af te leggen over de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). In de BIG & ENSIA staan veel richtlijnen waaraan gemeente in sommige kaders wettelijke verantwoording hebben (bijvoorbeeld voor DigiD/Suwinet) voor het faciliteren/uitvoeren van een dienst. Daarnaast staan er veel maatregelen in die op basis van 'pas toe of verklaar' principe werken. De BIG wordt opgevolgd door de Baseline Informatiebeveiliging Overheid (BIO). Ingaande 1-1-2020 moet de gemeente hieraan voldoen. De BIO is het gezamenlijk normenkader voor informatiebeveiliging van de overheid.

Algemene verordening gegevensbescherming (AVG)

Sinds 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. Dat betekent dat in de hele Europese Unie (EU) dezelfde privacywetgeving geldt. De Wet bescherming persoonsgegevens (Wbp) geldt niet meer. De AVG stelt een aantal eisen voor organisaties (o.a. gemeenten) om te bewerkstelligen dat privacy gerelateerde informatie op een veilige en gestructureerde manier wordt verwerkt, datalekken tijdig worden gemeld en betrokkenen hun rechten kunnen uitoefenen zodat zij beschikking hebben over hun persoonsgegevens.

Dataclassificatie

Data is het nieuwe goud en verkeerd gebruik kan enorme gevolgen hebben. Dataclassificatie is het toekennen van een beveiligingsniveau aan data en informatie. Dit is in de eerste plaats belangrijk, omdat met behulp van deze classificatie maatregelen genomen kunnen worden om risico's af te dekken. Een tweede belangrijke reden is dat hiermee ingeschat kan worden waar de informatie gebruikt en ontsloten kan en mag worden. Aan deze classificatie hangen maatregelen hoe er mee om gegaan dient te worden. Middels dataclassificatie worden de risico's en kwetsbaarheden van processen, applicaties en/of databronnen in kaart gebracht, zodat daarop de benodigde graad van bescherming afgestemd en gewaarborgd kan worden.

VNG Realisatie heeft in de handreiking dataclassificatie een richtlijn gegeven voor de classificatie van data. Deze methode is bekend als de uitgebreide methode.

De gemeente Barneveld maakt gebruik van de eenvoudige methode waarbij eisen gebruikt worden uit de uitgebreide methode rond authenticatie, autorisatie, monitoring en beveiliging. De gemeente hanteert hierbij het uitgangspunt NL-Cloud tenzij (alle databronnen gehost bij Nederlandse Cloudleveranciers, tenzij er geen Nederlandse oplossing beschikbaar is).

FIG. 4: KADERS EN BORGING

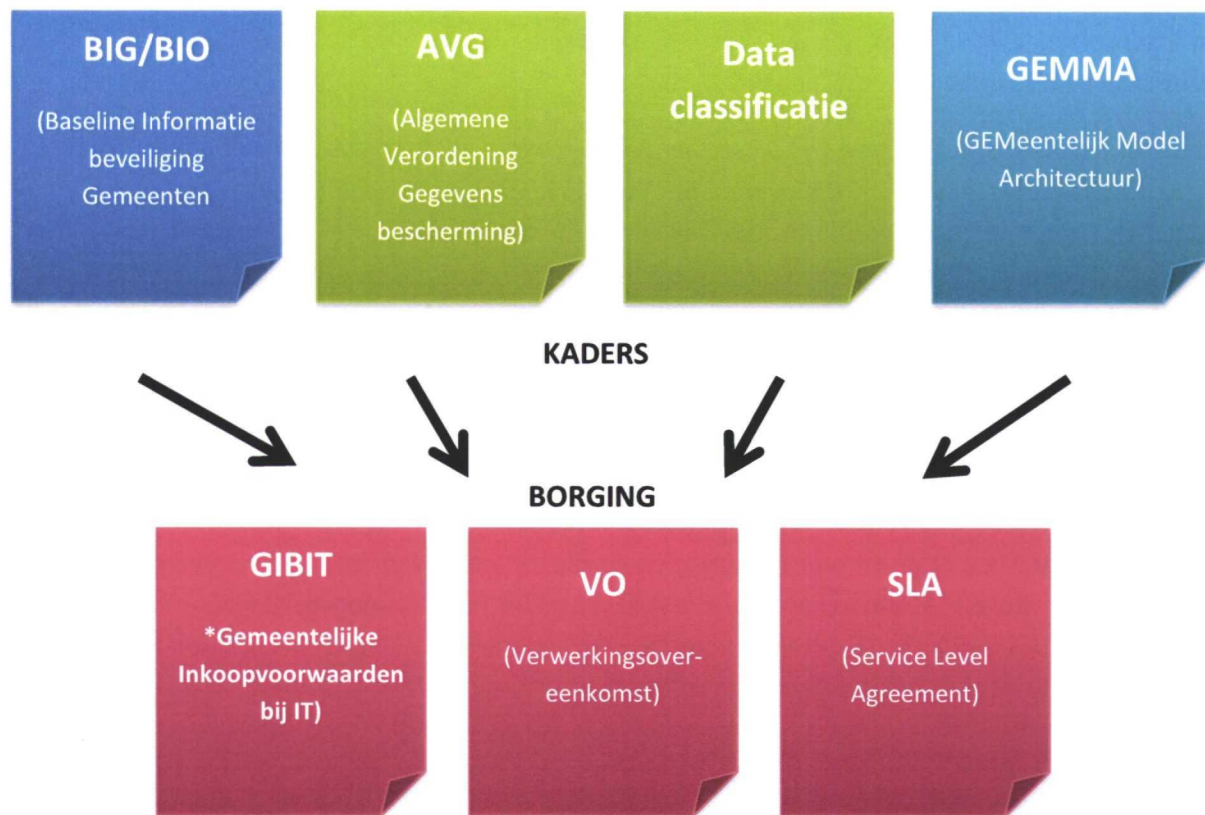
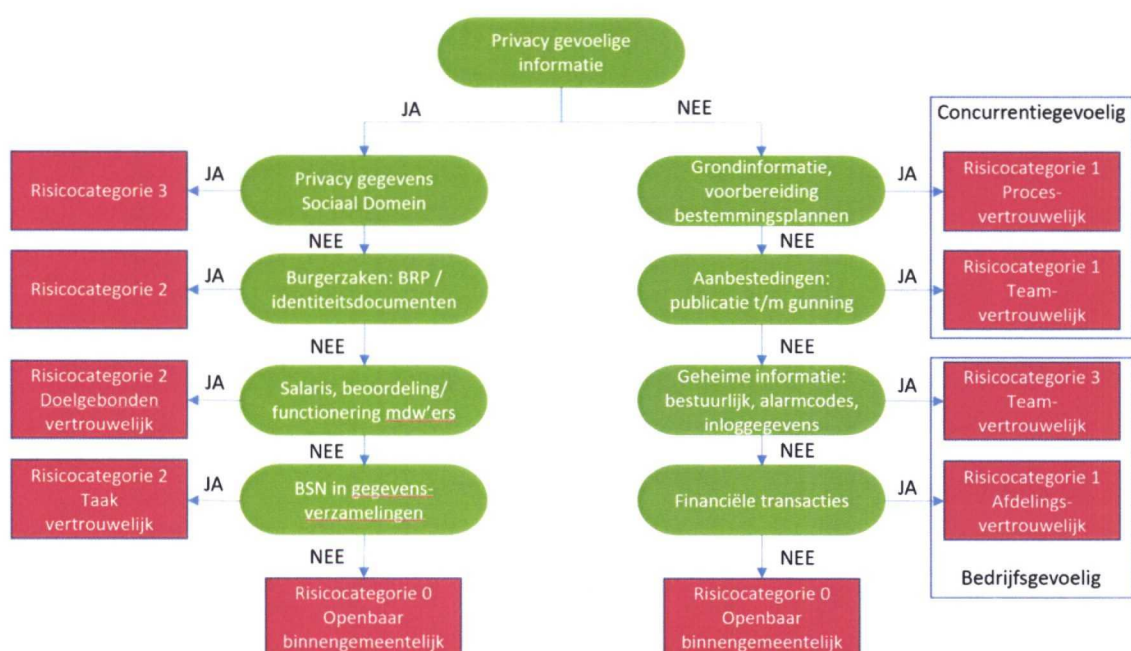


FIG. 5: BESLISSCHEMA DATACLASSIFICATIE





De eenvoudige methode kent de volgende risico-categorieën:

- 0 – publiek niveau
- I – basis niveau
- II – verhoogd niveau
- III – hoog risico

Deze risico-categorieën kunnen als volgt geplaatst worden in de volgende hostingtypes:

1. NL-CLOUD

Databronnen van de *risico-categorieën II en III* mogen gehost worden bij Nederlandse Cloudleveranciers onder voorwaarde dat zij zich conformeren aan het cloudbeleid van Barneveld, voldoen aan Privacy by design en een verwerkersovereenkomst tekenen.

2. EER-cloud

Databronnen die gehost worden in de Europese Economische Ruimte moeten voldoen aan het beschermingsniveau van de AVG. Als er geen Nederlandse leverancier kan worden gevonden, is een leverancier uit de EER een oplossing.

3. BCR-cloud

Leveranciers buiten de EER, maar die voldoen aan de Binding Corporate Rules (BCR) die zijn goedgekeurd door een Europese toezichthouder, komen als derde in zicht.

4. Privacyshield Cloud

Databronnen van de *risico-categorie I* mogen gehost worden bij internationale Cloudleveranciers die een Privacyshieldovereenkomst met de EU hebben ondertekend), mits internationale ontwikkelingen dit niet tegenwerken.

5. Model contracten

Voor leveranciers die geen van de voorgaande privacywaarborgen kunnen bieden, kan het aangaan van modelcontracten die goedgekeurd zijn door de Europese Commissie een oplossing zijn.

6. Internationale public cloud

Databronnen van de *risico-categorie 0* mogen bij afwezigheid van de voorgaande mogelijkheden gehost worden bij internationale public cloud Leveranciers die geen Privacyshieldovereenkomst met de EU hebben ondertekend.

De afbeelding hiernaast geeft het beslisschema weer dat leidt tot de verschillende risico-categorieën. **De opdrachtgever is verplicht** om deze dataclassificatie in overleg met de ciso en de cloud-architect uit te voeren.

GEMMA Architectuur

GEMMA staat voor de GEMEentelijke Model Architectuur. Dit is de landelijke referentie-architectuur voor gemeenten. GEMMA is afgeleid van de Nederlandse Overheid Referentie Architectuur (NORA). Samen met andere NORA-dochters als WILMA (waterschappen), PETRA (provincies) en EAR (Rijksoverheid) maakt GEMMA deel uit van de groeiende familie van overheids-referentiearchitecturen. Hiermee is een belangrijke basis gelegd voor interoperabiliteit tussen de verschillende overheden en landelijke voorzieningen.

GEMMA helpt gemeenten om (ICT-)ontwikkelingen in samenhang aan te sturen. Ontwikkelen, bouwen, aanschaffen en implementeren onder architectuur zorgt ervoor dat de oplossingen onderling goed samenwerken. Ook ontstaat er een overzicht dat bestuur en management helpt alle ontwikkelingen in samenhang aan te sturen.



3 KADERS

Met GEMMA, de Gemeentelijke Model Architectuur, is er inzicht in en grip op de informatievoorziening. GEMMA helpt om samenwerken tussen gemeenten, met ketenpartners en aansluiten op landelijke voorzieningen mogelijk te maken.

Contractuele borging van de implementatie

Op het moment dat een keuze gemaakt is voor een applicatie of infrastructureel onderdeel is het belangrijk dat deze afgenomen wordt met de juiste contractuele borging. Deze contractuele borging is de basis waarop door de gemeente Barneveld regie gevoerd kan worden, zodat de techniek, werking en het beheer van de gekozen oplossing zodanig functioneert dat naleving van de wet- en regelgeving en de eliminatie van de risico's gegarandeerd is. Hierbij moet gebruik worden gemaakt van de volgende methoden:

Gemeentelijke Inkoopvoorwaarden bij IT (GIBIT)

Gemeenten zijn voor de kwaliteit van hun dienstverlening en uitvoering steeds meer afhankelijk van ingekochte ICT-producten en –diensten. Goede gemeenschappelijke ICT-inkoopvoorwaarden zijn daarom uiterst nuttig om deze kwaliteit goed aan te laten sluiten op de gemeentelijke behoeften en doelstelling. Onder andere compliance (het aantoonbaar voldoen aan bestaande normen en standaarden en architectuur), aansluiting op de generieke digitale infrastructuur van de overheid (GDI) en cloud- en hostingservices en informatiebeveiliging en privacy zijn hierbij belangrijke onderwerpen. Binnen het programma Digitale Agenda 2020 is door KING de GIBIT (Gemeentelijke Inkoopvoorwaarden bij IT) gerealiseerd. Op 24 februari 2017 heeft de gemeente Barneveld besloten om de GIBIT te gaan gebruiken bij de inkoop van ICT-producten en –diensten. Bij de aanschaf van een cloudapplicatie of infrastructureel onderdeel in de cloud is de opdrachtgever daarom verplicht de GIBIT te hanteren en gebruik te maken van de GIBIT-overeenkomstengenerator.

Door de gemeentelijke inkoopvoorwaarden bij IT (GIBIT) van toepassing te verklaren op inkooptrajecten van clouddiensten borgen we een belangrijke set regels waaraan providers zich moeten houden:

Garanties dat de dienst steeds tijdig zal blijven voldoen aan

- ✓ relevante wet- en regelgeving;
- ✓ interoperabiliteitseisen;
- ✓ nieuwe versies van de Gemeentelijke ICT-kwaliteitsnormen;
- ✓ bepalingen uit de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)

Afspraken/regels over

- ✓ Het in staat stellen van de opdrachtgever om toegang te krijgen tot de data en autorisatie instellingen;
- ✓ Opschorting, opzegging en ontbinding van de online ICT-dienst;
- ✓ Privacy, beveiliging en archivering (bewerksrelatie, verwerking persoonsgegevens, Meldplicht beveiligingsincidenten, etc.);
- ✓ Archivering

Basis SLA-bepalingen



Verwerkersovereenkomst (VO)

Voor cloudoplossingen die persoonsgegevens verwerken geldt dat deze ook moeten voldoen aan Privacy by design. Bij de inrichting van de infrastructuur zal dan de privacy officer moeten worden betrokken. In het kader van de privacy zal bij het verwerking van persoonsgegevens nodig zijn om een verwerkersovereenkomst af te sluiten. Hierin moeten bepalingen worden opgenomen over beveiliging, geheimhouding, meldplicht datalekken, doorgifte buiten de EER, audits en vernietiging van persoonsgegevens.

Service Level Agreement (SLA)

In een vroeg stadium zullen juristen betrokken moeten worden voor het opstellen van een Service Level Agreement voor afspraken over aansprakelijkheid etc. De afdelingsverantwoordelijke, applicatiebeheerder, gebruikers en informatie adviseur en collega's Automatisering zijn betrokken bij het opstellen van de SLA en het Dossier Afspraken en Procedures (DAP).



4 PROCESMAATREGELEN

4 PROCESMAATREGELEN

Cloud computing is bij de gemeente Barneveld grotendeels een nieuw fenomeen. Dat betekent dat de borging van de werkwijze bij cloudgang en de verdere cloudgang een aantal belangrijke **maatregelen** vereisen. Figuur 6 toont schematisch deze procesmaatregelen. Daaronder volgen, in de kleur van elke processtap de bijbehorende beschrijving

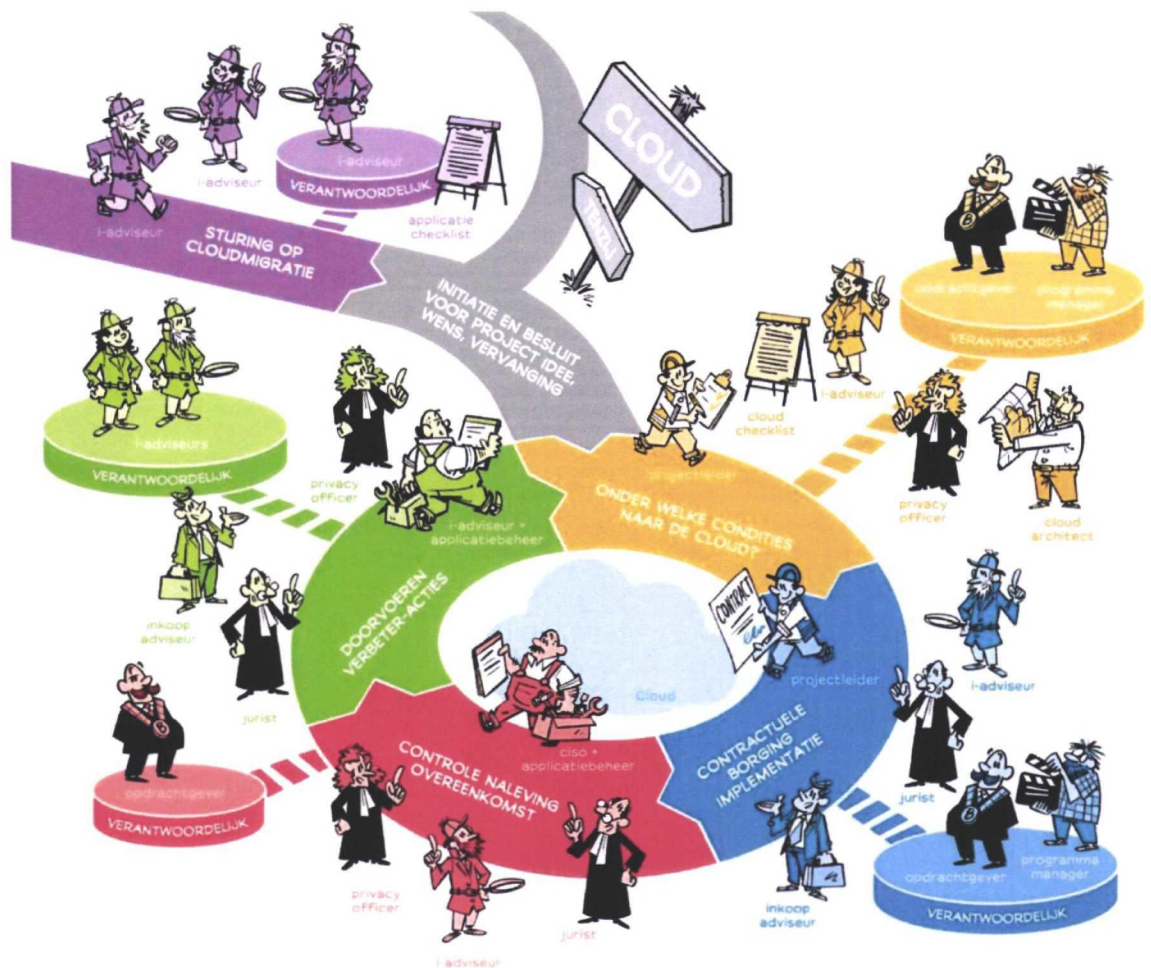


FIG. 6: PROCESMAATREGELEN

Sturing op cloudmigratie

Vanwege verschillende redenen kan de cloudmigratie van de nu in gebruik zijnde softwareoplossingen nog een proces van jaren zijn, zoals

- Er zijn nog geen vervangende cloudproducten op de markt
- Er is veel tijd en geld geïnvesteerd in het huidige softwareproduct. Het zou de bedrijfsvoering schaden als we zouden overstappen
- Het stopzetten van het huidige contract kost veel geld
- Techniek en/of wet- en regelgeving blokkeren een volledige gang naar de cloud



Om sturing op de cloudmigratie mogelijk te maken, is doorlopend inzicht en stimulering nodig door:

- *centraal inzichtelijk te maken welke softwareoplossingen op welke momenten een gang naar de cloud kunnen maken*

MAATREGEL:

De informatie-adviseurs gaan gebruik maken van een APPLICATIE-Checklist. Op deze lijst staan alle applicaties die in gebruik, maar nog geen cloudoplossing zijn, aangevuld met vervaldata van contract- en licenties. Jaarlijks kijken zij samen met de verantwoordelijken voor deze applicaties naar de mogelijkheden van cloudmigratie. Aanleidingen hiervoor kunnen bijvoorbeeld zijn:

- veranderwens van gebruikers
- veranderende wet- en regelgeving
- einde contractdatum
- leverancier stopt met het huidige product en biedt (alleen) een cloudoplossing aan

NB: De APPLICATIE-Checklijst kan ook ter informatie en informatietoevoeging door de cloud-architecten, privacy-officer, CISO, ICT-technisch medewerker en contract- en licentiebeheer gebruikt worden. Hierdoor ontstaat een praktische gegevensverzameling over alle aspecten die spelen rond cloudmigratie, architectuur en monitoring van contracten en licenties.

- *jaarlijks bestuurlijk inzichtelijk te maken voor welke applicaties met significante impact op de bedrijfsvoering gekeken wordt naar de mogelijkheid van cloudgang*

MAATREGEL:

De informatie-adviseurs dragen er samen met de afdelingsmanagers zorg voor dat onder de kop 'bedrijfsvoering' in het afdelingsplan benoemd wordt welke applicaties in de begroting van het komende jaar worden meegenomen om te vervangen door een cloudoplossing

Verantwoordelijk:	Informatie adviseur
Uitvoerend:	Informatie adviseur en opdrachtgever
Hulpmiddel:	APPLICATIE-Checklijst en afdelingsplan

Initiatie en besluit voor project, idee, wens of vervanging

In de organisatie ontstaan nieuwe initiatieven, ideeën, wensen of zijn vervanging nodig. De informatie-adviseurs begeleiden dit door een initiatiefdocument op te stellen waar alle belangrijke aspecten in benoemd worden zoals een integrale afweging van de doelen, financiële consequenties en beheeraspecten. Op basis hiervan besluit een programmamanager of afdelingshoofd of een project gestart moet worden.



4 PROCESMAATREGELEN

Verantwoordelijk:	Afdelingshoofd of programmamanager
Uitvoerend:	Informatie adviseur
Adviserend:	Cloud-architect, privacy-officer
Hulpmiddel:	Initiatiedocument

Onder welke condities naar de cloud

Wanneer een opdrachtgever een keuze moet gaan maken voor een nieuwe of te vervangen applicatie of een ICT-infrastructuuronderdeel dient deze ervoor zorg te dragen dat ICT-infrastructuur en applicaties voldoen aan de wet- en regelgeving en dat de bedreigingen die cloud computing met zich meebrengt zo goed mogelijk geëlimineerd of zo klein mogelijk gemaakt worden. De opdrachtgever wordt hierbij in het projectportfolioproses ontzorgd door de i-adviseur en specialisten. Dit doen zij met behulp van de CLOUD-Checklist. Hierin staan een aantal checks op basis waarvan zij een advies kunnen uitbrengen dat binnen de clouduitgangspunten past. De opgenomen checks zijn erop gericht risico's bij cloudoplossingen te elimineren of te minimaliseren en de integraal gebruik te bevorderen.

Verantwoordelijk:	Afdelingshoofd of programmamanager
Uitvoerend:	Informatie-adviseur
Adviserend:	Cloud-architect, privacy-officer
Hulpmiddel:	Cloudchecklist

Contractuele borging implementatie

Aanvullend aan de condities die in de vorige paragraaf beschreven zijn is het nodig om afspraken te maken over de dienstverlening die afgenomen wordt en hoe we die kunnen monitoren (SLA), over het toestaan van audits en een exitstrategie. Hierna kan aanbesteding /gunning plaatsvinden op basis van het vigerende inkoopbeleid en conform de aanbestedingswet.

Verantwoordelijk:	Afdelingshoofd of programmamanager
Uitvoerend:	Projectleider
Adviserend:	Informatie-adviseur, jurist, inkoopadviseur
Hulpmiddel:	GIBIT-contractgenerator, verwerkingsovereenkomst, SLA

Controle naleving overeenkomst

De beweging naar de cloud brengt een verandering binnen I&A-functies met zich mee. Het beheer van fysiek ijzer zal minder worden, maar er komen contractmanagement, regie- en audittaken voor in de plaats. Toenemende wetgeving rond informatiebeveiliging en privacy bescherming leiden tot een uitbreiding van de gemeentelijke auditkalender. Het auditen van de clouddiensten dient integraal onderdeel uit te maken van de organisatiebrede auditkalender. Hierin spelen de ciso, applicatiebeheerder, i-adviseur en inkoop-adviseur een belangrijke rol. Zij dragen in de praktijk samen zorg voor het monitoren en het voeren van regie op de vastgelegde overeenkomst, verwerkingsovereenkomst en SLA.



Verantwoordelijk:	Afdelingshoofd
Uitvoerend:	CISO, applicatiebeheerder
Adviserend:	Informatie-adviseur, privacy-officerm jurist

Doorvoeren verbeteracties

Het gebruik van cloudoplossingen is een relatief nieuwe ontwikkeling binnen de gemeenten. Er zal dus een leercurve zijn in de uitvoering van het cloudbeleid en het gebruik van cloudoplossingen binnen de organisatie. Het proces geeft hier ruimte toe. Geconstateerde aanpassingen en verbeteringen ten aanzien van cloudbeleid en de daaruit volgende afwegingen en aanpak zullen door de i-adviseurs jaarlijks worden vastgelegd in een actualisering van het cloudbeleid.

Verantwoordelijk:	Informatie-adviseurs
Uitvoerend:	Informatie-adviseurs
Adviserend:	Informatie-adviseur, privacy-officerm jurist

Rollen en verantwoordelijkheden

Het is belangrijk om hierbij de volgende rollen en verantwoordelijkheden onder de aandacht te brengen en te versterken door aannamebeleid en opleiding.

- **Goed opdrachtgeverschap**
een opdrachtgever dient zich verantwoordelijk te weten voor de implementatie en het gebruik van een betrouwbaar cloudproduct
- **Goed projectleiderschap**
Projectleiders dienen de juiste competenties te bezitten om het soms ingewikkelde proces van keuze en implementatie van cloudproducten efficiënt te kunnen handelen. De projectleidersrol is geen nevenactiviteit, maar een activiteit die tijd, aandacht en mandaat vraagt
- **Goed adviseurschap**
I-adviseurs dienen de opdrachtgever en projectleider te ondersteunen tijdens de verschillende fases van initiatie, planning, realisatie en evaluatie. De verschillende specialisten zoals privacy-officer, ciso en cloud-architect zijn onmisbare adviseurs tijdens het portfolioproses
- **Goed regisseurschap**
Meer als tot nu toe, is de rol van regisseur. Het is belangrijk om vooraf dit regisseurschap goed te beleggen. Dit kan bijvoorbeeld bij applicatiebeheerders. Regisseurs zijn samen met de ciso van groot belang bij het monitoren van de nakoming van overeenkomsten en contracten. Ook zijn voldoende tijd voor opleiding en uitvoering belangrijke randvoorwaarden om een goed werkende en verantwoorde ICT-infrastructuur te kunnen bieden.