

Cloudkaders gemeente Hoorn

T.b.v. outsourcing werkplek-, datacenter-, netwerk-, en
integratiediensten en (technisch) applicatiebeheer

Team Informatiemanagement & Automatisering

Architectuur

19 januari 2021

V1.0



Inhoudsopgave

1	Inleiding	3
1.1	Doelstelling van dit document	3
1.2	Waarom cloud	3
2	Richtinggevende factoren	5
2.1	Interne factoren	5
2.2	Externe factoren	6
3	Roadmap	9
4	Randvoorwaarden cloudlandschap	10
4.1	Algemene Verordening Gegevensbescherming	10
4.2	Informatiebeveiliging	10
4.3	Continuïteit	10
4.4	Randvoorwaarden	10
Bijlage 1: Bronverwijzingen.....		13
Bijlage 2: Definities.....		14

1 Inleiding

1.1 Doelstelling van dit document

Dit document is geschreven met het oog op de voorgenomen aanbesteding van de ICT-outsourcing. Onderhoud van de eigen datacenters wordt steeds meer specialisten werk waarbij generalisten binnen de gemeente Hoorn het steeds lastiger krijgen onderhoud uit te voeren op het eigen datacenter en de beveiliging op orde te houden. Daarnaast zijn er cloud-ontwikkelingen die tegemoet komen aan de door gemeente Hoorn benodigde schaalbare en flexibele infrastructuur behoefte.

Ten aanzien van cloud kun je constateren dat je, naast de vergroting van flexibiliteit en schaalbaarheid ook voor een deel van de technische en infrastructurele beheertaken wordt ontzorgd. Daarbij lever je wel in op de invloed van planning en uitvoering van werkzaamheden. Wel voordelig echter is de afname van de noodzaak om hardware in eigendom en eigen beheer te hebben. De doelstelling is dan ook om binnen twee jaar geen hardware meer op locatie te hebben en afscheid te nemen van het datacenter in het stadhuis en de uitwijklocatie bij SSC DeSom. De technische beheeractiviteiten zullen worden belegd bij de geselecteerde opdrachtnemer van de aanbesteding.

Naast de verplaatsing van (en het beheer op) infrastructuur naar de cloud zien we dit ook gebeuren binnen het applicatielandschap. Het gebruik van SaaS zorgt voor een vermindering van technisch applicatiebeheer en eventueel eigendom en beheer van voorwaardelijke infrastructuur. Daar tegenover staan wel taken als regie en integratie van clouddiensten en SAAS applicaties.

De focus in dit document ligt op het formuleren van kaders rondom de (reeds in uitvoering zijnde) transitie van on-premise infrastructuur naar de cloud. Een reis waarmee gemeente Hoorn in 2019 is gestart en die door middel van outsourcing een versnelling zal doormaken. Ook cloud middelen moeten worden beheerd en de kaders moeten we daar nu al voor opstellen. Tenslotte heeft gemeente Hoorn te maken met wet- en regelgeving waaraan moet worden voldaan en waar ook een te selecteren opdrachtnemer aan zal moeten voldoen.

Onze gemeenteraad heeft met het vaststellen van “ICT-visie en beleid” (zie bijlagen) benoemd dat de ICT-voorzieningen continu moeten vernieuwen. De steeds groeiende en veranderende digitalisering van de samenleving eist een gemeente die digitaal actief aanwezig is en goed aansluit op de eisen en mogelijkheden van nieuwe technologie. De toepassing van digitale technologie moet helpen om effectiever en slimmer te werken en mogelijk maken om bij te dragen aan het oplossen van maatschappelijke vraagstukken.

We hebben besloten dat we kiezen om zoveel mogelijk ICT-voorzieningen als dienst af te nemen om flexibiliteit, schaalbaarheid en veiligheid beter te kunnen borgen. Het gevolg hiervan is dat ons werk veranderd van 'zelf beheren' naar 'regie voeren op leveranciers'.

In vervolg op de vastgestelde ICT-visie en het ICT-beleidsplan is een programma gestart om de gewenste verandering van de ICT-organisatie te realiseren. Een onderdeel hiervan is een keuze voor outsourcing van beheer en voorzieningen. Op basis van een businesscase is gekozen om het beheer en eigendom van de ICT-voorzieningen maximaal te outsourcen.

1.2 Waarom cloud

Binnen de gemeente Hoorn is behoefte aan een schaalbare en flexibele infrastructuur die past bij de ambities uit de ICT-Visie. In ons ICT-beleid hebben we vastgesteld dat we niet kunnen ontkomen aan het gebruik van de cloud. De doelstelling is dat we in staat zijn om de ICT aan te kunnen passen aan de voortdurende verandering van eisen en wensen. Cloudtechnologie biedt hiervoor de beste mogelijkheden. Daarnaast worden applicaties steeds vaker alleen als cloudapplicatie door leveranciers aangeboden.

Het is daarmee niet de vraag óf we de cloud gaan gebruiken. De vraag is hoe we de cloud gaan gebruiken: Op een verantwoorde en veilige manier, waarbij we regie houden op onze systemen en informatie.

Door inzet van de cloud kan de gemeente:

- eenvoudig snel en flexibel opschalen, dan wel afbouwen van ICT-diensten;
- grote investeringen verschuiven naar 'huren op maat';
- functionele vernieuwing sneller beschikbaar maken;
- gewenste dienstverlening of gegevens plaatsonafhankelijk, snel en gemakkelijk afnemen;
- opslag- en reken capaciteit delen met andere interne gebruikers van de cloud (bijvoorbeeld een gedeelde gemeentecloud).

Cloud heeft voor gemeenten impact op het voldoen aan de Baseline Informatiebeveiliging Overheid (BIO) en de Algemene Verordening Gegevensbescherming (AVG) omdat het afnemen van clouddiensten gevolgen heeft voor de plaats waar informatiebeveiligingsmaatregelen worden uitgevoerd.

2 Richtinggevende factoren

2.1 Interne factoren

2.1.1 ICT-visie en -beleid

Begin 2019 is de raad akkoord gegaan met het plan: ICT-visie en beleid. De ICT-visie beschrijft de richting waarin we het gebruik van ICT-voorzieningen willen ontwikkelen. De visie van Gemeente Hoorn is als volgt verwoord:

"ICT creëert waarde voor de stad en haar inwoners. Het versnelt de ontwikkeling van onze organisatie door inzet van data en digitalisering.

We digitaliseren onze dienstverlening en ons werk. We organiseren datagedreven en moderniseren onze informatievoorziening. Onze ICT is veilig, zorgeloos en vanzelfsprekend beschikbaar voor onze organisatie en haar partners"

In onze visie zijn een aantal ambities opgenomen. Voor de cloudkaders zijn de meest relevante:

- we bieden een open informatievoorziening waarin we samenwerken met onze partners;
- onze informatievoorziening is veilig en betrouwbaar;
- we vernieuwen continu onze informatievoorziening.

Voor het realiseren van de visie kiezen we ervoor om aan te sluiten op ontwikkelingen bij de overheid en de markt. We volgen de koplopers in modernisering en bewezen technologie. Er is wel ruimte om kleinschalig te experimenteren, daarmee maken we ook ruimte voor innovatieve oplossingen.

Bij de beschrijving van ons ICT toekomstbeeld staat dat de ICT-organisatie zich richt op het organiseren en regisseren van goed werkende functionaliteit voor gebruikers. Beschikbaar als deze nodig is: tijd-, plaats- en apparaat onafhankelijk. Onze business zal meer gebruik gaan maken van kleinschalige services die goed met elkaar samenwerken. We zien flexibiliteit en schaalbaarheid als belangrijkste succesfactoren en ongewenst gebruik wordt voorkomen. Er is een noodzaak voor het gebruik van de cloud. We maken gebruik van de verschillende cloud deployment modellen (zie bijlage 2) om ons ICT-landschap in te richten.

2.1.2 Speerpunten van beleid

Het realiseren en beheren van dit landschap vraagt een grote verandering van zowel de techniek als de organisatie waar we nu mee werken. Eén van de speerpunten van het ICT-beleid is daarom een blijvende vernieuwing van ICT-voorzieningen. Concreet is afgesproken dat we werken aan:

- een flexibele, moderne en toegankelijke ICT-voorziening waar continu doorontwikkeling; plaatsvindt op basis van de veranderende wensen en eisen;
- regie voeren op leveranciers van ICT-voorzieningen;
- sourcing van beheer van ICT-voorzieningen;
- het realiseren van een nieuwe digitale werkplek die flexibel en veilig is en netwerkend partnerschap echt ondersteunt.

2.1.3 Programma ICT-regie en sourcing

In vervolg op de vastgestelde ICT-visie en het beleidsplan is een programma gestart om de gewenste verandering van de ICT-organisatie te realiseren. Een onderdeel hiervan is een keuze voor outsourcing van beheer en voorzieningen. Op basis van een businesscase is gekozen om het beheer en eigendom van de ICT-voorzieningen maximaal te outsourcen.

2.1.4 Datagedreven organiseren (Programma Innovatieve Stad)

Data is een nieuw terrein dat andere eisen stelt aan de vaardigheden van de business en de inrichting van het informatielandschap:

- werken vanuit de (onderzoeks)vraag;
- toegang tot data;
- slimmer vastleggen van data;
- bekende kwaliteit van data;
- verantwoorde toepassing van data;
- transparante verwerkingsprocessen en algoritmes.

en kansen:

- beter gefundeerde besluiten;
- oordeelvorming en inzicht op basis van analyse van feiten;
- slimmer werken door beter inzicht in het effect en waarde van het eigen handelen;
- digitalisering van werkprocessen.

De betekenis voor de infrastructuur is dat we een nieuw soort applicaties (middleware en endpoints) introduceren, die andere eisen stellen aan technologie. Denk hierbij aan het Internet Of Things (IOT), met een grote toename aan sensoren, en edge computing (sensoren die ook verwerking uitvoeren), waardoor het aantal verschillende endpoint-apparaten sterk kan toenemen. Cloud is hiervoor een belangrijke voorwaarde met als gevolg een ander soort beveiligingsvraagstukken. Binnen de gemeente Hoorn zijn dit onder andere: schakelbare straatlantaarns die in geval van calamiteiten ingeschakeld kunnen worden, en signalering van volle vuilnisbakken: Bigbelly's.

Om het werken met data binnen gemeente Hoorn te faciliteren is in de huidige Azure tenant een data-ontwikkelplatform ingericht op basis van Microsoft architectuur en producten.

2.1.5 SaaS tenzij

De gemeente Hoorn kent een SaaS tenzij beleid. Dat betekent dat in de toekomst een groei wordt verwacht van het aantal SaaS applicaties en een afname van het aantal on-premise applicaties. Ongeveer 40% van de applicaties wordt op dit moment in een SaaS vorm afgenomen. De snelheid waarmee on-premise applicaties worden vervangen zal onder andere afhangen van de ontwikkelingen bij de diverse applicatie leveranciers.

2.2 Externe factoren

2.2.1 Digitalisering bij de overheid

De rijksoverheid streeft in haar digitaliseringsstrategie naar een open en toegankelijke overheid. Hierbij staan innovatie, data, burgers en ondernemers centraal.

Bij het realiseren van deze ambitie is een grote verandering van het informatie- en applicatielandschap van overheidsorganisaties noodzakelijk. Om dit te bereiken wordt door het rijk en koepelorganisaties innovatie sterk gestimuleerd.

2.2.2 Samen Organiseren

De gezamenlijke gemeenten hebben in 2017 afgesproken om "Samen te organiseren". Door zelf meer regie te nemen en beter te standaardiseren is het de bedoeling om onder andere een efficiëntere (overheids)informatievoorziening te realiseren en gegevens beter herbruikbaar te maken. Naar aanleiding hiervan zijn verschillende ontwikkelingen gestart die invloed hebben op de ICT-voorzieningen van de individuele gemeenten.

2.2.3 Common Ground

Voor gemeenten is een nieuwe, informatiekundige, visie vastgesteld. Deze moet ervoor zorgen dat de gemeentelijke dienstverlening snel en flexibel kan worden gemoderniseerd. Gekozen is om de realisatie van de visie ook door de gemeenten gezamenlijk op te pakken. Kenmerkend is dat de realisatie hiervan *agile* plaatsvindt en dat standaarden werkend worden getoond.

Common Ground is naast een informatiekundige visie tevens een (her)ontwikkeling van het applicatielandschap om het proces- en informatielandschap voor gemeenten in 10 jaar om te vormen. Intenties hierbij zijn onder andere data los trekken van de werkprocessen, en applicaties in te richten op basis van gestandaardiseerde services. De technologie die hierbij gebruikt gaat worden wijkt af van de huidige ICT, met name op het gebied van koppelingen. Dit stelt daarom ook andere eisen aan de onderliggende infrastructuur, onder meer door het gebruik van containertechnologie. Gemeente Hoorn neemt deel aan deze ontwikkeling.

2.2.4 Software leveranciers

Veel software leveranciers zijn hun applicaties aan het verschuiven van een on-premise naar een cloud variant. On-premise varianten zullen steeds minder onderhouden worden, of zelfs beschikbaar komen. De markt leidt ons door deze ontwikkeling de Cloud in.

2.2.5 GEMMA

De GEMMA is de referentie voor de gemeentelijke informatievoorziening. Deze wordt zoveel mogelijk in applicaties gerealiseerd. De huidige GEMMA 2.0 kent geen implementatievoorschriften en stelt geen specifieke eisen aan technologie.

Met de nieuwe informatiekundige visie, Common Ground, worden de principes en modellen van de GEMMA aangescherpt en stuurt deze meer op de manier waarop implementatie plaatsvindt. Een duidelijk voorbeeld hiervan is het GEMMA gegevenslandschap. Hierin wordt met meer detaillering aangegeven dat het gegevenslandschap servicegericht wordt ingericht en hoe de gegevens worden gescheiden van proces en interactie. Met name voor de technische lagen betekent dit dat het type componenten, waaronder databasemanagementsystemen, en het gegevensverkeer gaan veranderen. Dit kan ook andere eisen stellen aan de technische infrastructuur. Deze verandering wordt gedreven door de vernieuwing van applicaties.

2.2.6 Gemeentelijke Gemeenschappelijke Infrastructuur (GGI)

In het kader van [Samen Organiseren](#) hebben gemeenten aan VNG en VNG-Realisatie opdracht gegeven te werken aan meer collectiviteit op ICT-voorzieningen. De [Gemeentelijke Gemeenschappelijke Infrastructuur \(GGI\)](#)¹ creëert een veilige, samenhangende digitale infrastructuur waardoor samenwerken tussen gemeenten en andere overheden beter, veiliger en gemakkelijker wordt. De GGI vormt de technische basis waarin toegewerkt wordt naar een gemeentelijke community Cloud, die is aangesloten op de landelijke [Generieke Digitale Infrastructuur \(GDI\)](#). Onderdeel van deze Cloud is ook het ontsluiten van softwareproducten die leveranciers als clouddienst aanbieden.

Het realiseren van een GGI schept de voorwaarden om op een goede, veilige en flexibele wijze de overstap te maken naar de Cloud. De GGI wordt tegelijkertijd ontwikkeld met het organiseren van meer gezamenlijke processen en dienstverlening bij gemeenten. Daarnaast staan zij door de schaalgrootte van het collectief van gemeenten sterker in de onderhandelingen met leveranciers. Ze bepalen zelf wat zij doen en ze zijn in staat om er actief regie op te voeren. Bovendien leidt de efficiency van gezamenlijkheid dikwijls tot lagere meerkosten. Cloud leveranciers zullen hun diensten via de Gemeentelijke Gemeenschappelijke Infrastructuur (GGI) gaan aanbieden. De gemeente Hoorn volgt deze ontwikkelingen met grote belangstelling. Waar dit waarde oplevert wil gemeente Hoorn inzetten op deze ontwikkelingen.

GGI bestaat uit de volgende drie componenten (zie figuur 1):

- [GGI-Netwerk](#), een beveiligd landelijk datanetwerk van en voor gemeenten;
- [GGI-Afspraken](#), dit zijn de voorwaarden die gelden voor het ontsluiten van commerciële cloud-omgevingen op het GGI-Netwerk;
- [GGI-Veilig](#), dit zorgt voor de actieve beveiliging van het dataverkeer over het GGI-Netwerk en over de eigen bedrijfsnetwerken van gemeenten.

¹ <https://www.vngrealisatie.nl/ggi>



Figuur 1: Gemeentelijke Gemeenschappelijke Infrastructuur (GGI)

Gemeente Hoorn heeft deelgenomen aan de aanbestedingen voor GGI-netwerk en GGI-Veilig. De afname verplichtingen vanuit GGI-Veilig (SIEM/SOC) vervallen voor de gemeente Hoorn als gevolg van de voorgenomen outsourcing. De verplichting om een SIEM/SOC systeem operationeel te hebben (BIO) blijft onverminderd van kracht. Dit zal gerealiseerd moeten worden door de toekomstige opdrachtnemer.

De GGI-netwerk aansluiting is gerealiseerd en gemeente Hoorn is op dit moment bezig de (landelijke) voorzieningen die nog via Gemnet worden afgenomen te migreren naar het GGI-netwerk.

Voor aanvullende informatie omtrent GGI-Netwerk en BIO, zie Bijlage 1: Bronverwijzingen.

3 Roadmap

Voor de gemeente Hoorn is een aantal fases te onderscheiden in de ambitie om geen lokale datacenters meer in eigendom te hebben en te beheren enerzijds, en de voortzetting van de Cloud gang anderzijds. Op dit moment zijn delen van de on-premise infrastructuur naar de Azure Cloud gebracht. Er wordt een SaaS-tenzij-beleid gevolgd waarbij er altijd een afweging wordt gemaakt of een nieuwe SaaS-oplossing geen extra complexiteit oplevert voor koppelingen met on-premise applicaties en/of data.

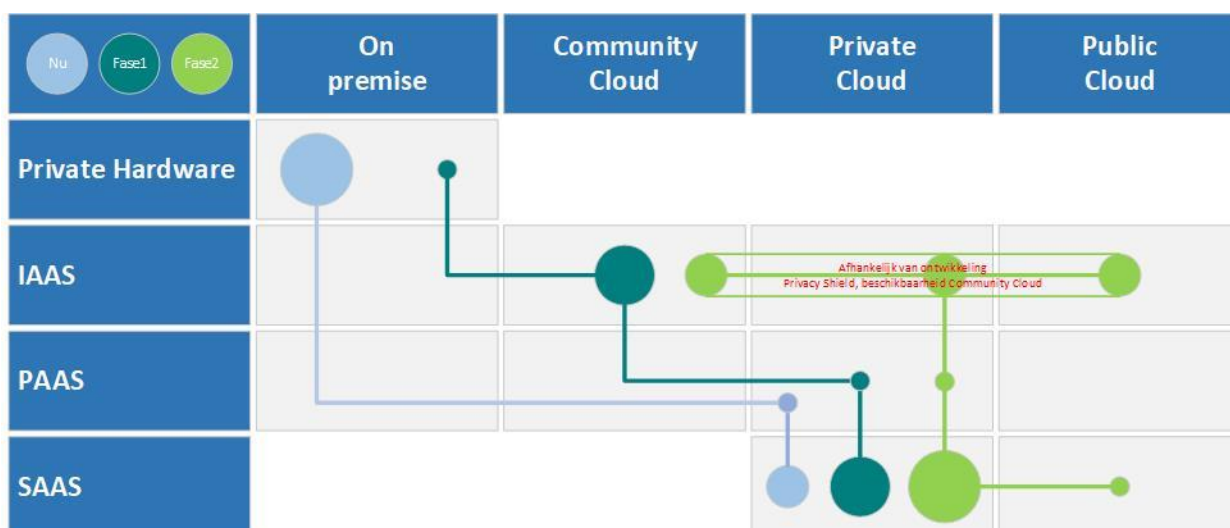
In de volgende fase komt een Private IaaS infrastructuur beschikbaar als vervanging van de resterende on-premise infrastructuur. In deze fase groeit het SaaS-aandeel ten opzichte van het IaaS-aandeel. Doelstelling hierbij is om alle belangrijke en benodigde (redundante) netwerkverbindingen te koppelen op de locatie(s) van de private IaaS provider.

“Op voorhand is niet te zeggen hoe het landschap ingericht gaat worden en welke ICT in een centraal datacenter draait en welke bij andere leveranciers of partner-organisatie worden geleverd. Hierbij zien we een hybride cloud als eindvorm.

Het is niet de bedoeling om voor elke microservice een eigen leverancier te hebben. In het eindbeeld is een optimale clustering van samenhangende services gerealiseerd, waarbij wij optimaal ontzorgt worden in beheer en integratievraagstukken terwijl gelijktijdig we de gewenste functionaliteit conform onze eisen en wensen kunnen realiseren.”

Bron: ICT-landschap Hoorn

De uiteindelijke gewenste situatie voor de gemeente Hoorn is afgebeeld als laatste fase in figuur 2. Een on-premise datacenter ontbreekt en de infrastructuur is verdeeld over Private, Community en Public Cloud. Een precieze invulling is op dit moment nog niet te bepalen vanwege onder meer de impact van het niet accepteren van het Amerikaans Privacy Shield door het Europese Hof van Justitie in de zomer van 2020. Ook de ontwikkeling van een gemeentelijke Community Cloud kan in de toekomst een alternatief blijken te zijn voor de Private IaaS-cloud. Op termijn kunnen ook SaaS-diensten via de Community Cloud afgenomen worden. Dit leidt technisch niet tot een fundamenteel andere implementatie maar kan gevolgen hebben voor compliance. Een exacte invulling en verdeling is op dit moment niet te geven. Dit is mede afhankelijk van de snelheid van de ontwikkelingen binnen de gemeentelijke Community cloud en de applicatieleveranciers.



Figuur 2. Roadmap

4 Randvoorwaarden cloudlandschap

4.1 Algemene Verordening Gegevensbescherming

Privacy is een grondrecht. De bescherming van persoonsgegevens valt hieronder en is uitgewerkt in de Algemene Verordening Gegevensbescherming (AVG). De AVG geldt in de hele Europese Unie. Waar de AVG ruimte laat voor nationale keuzes, zijn deze ingevuld in de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG). In de (U)AVG staan de verplichtingen waar organisaties aan moeten voldoen en de privacyrechten van personen. Voor de cloud zijn dus beide kaders van toepassing.

4.2 Informatiebeveiliging

Gemeenten hebben met elkaar afgesproken informatiebeveiliging in te richten volgens de Baseline Informatiebeveiliging Overheid (BIO). Het afnemen van clouddiensten heeft gevolgen voor de plaats waar informatiebeveiligingsmaatregelen worden getroffen. Dit geldt ook bij outsourcing /uitbesteding. Als een gemeente gebruik maakt van clouddiensten blijft de gemeente verantwoordelijk voor de beveiliging van de informatie(systemen) en persoonsgegevens. Voor de gemeente Hoorn en de opdrachtnemer is de BIO daarom van toepassing.

4.3 Continuïteit

Een goede backup voorziening is onder andere voorwaardelijk voor wat betreft de borging van continuïteit in de ICT voorzieningen. Alleen het maken van een backup is niet voldoende. Backup dient op een dusdanige manier ingericht te worden dat deze o.a. beveiligd is tegen ransomware en offline storage mogelijk maakt. Daarnaast is een voorziening nodig die backup faciliteert in een constant veranderende wereld waar infrastructuur en applicaties verdeeld zijn over on-premise en diverse cloud modellen.

Voor verdere informatie over het onderwerp 'continuïteit', met name de afhankelijkheden van informatieveiligheid-BIO-BCM wordt verwezen naar Handreiking "Bedrijfscontinuïteitsbeheer" van de IBD (zie link in bijlage 1).

4.4 Randvoorwaarden

4.4.1 Verantwoording (ENSIA)

Gemeenten zijn verplicht om verantwoording af te leggen over informatiebeveiliging via ENSIA. Dat staat voor Eenduidige Normatiek Single Information Audit. De Opdrachtnemer is verplicht de benodigde informatie aan te leveren ten aanzien van de diverse audits en verantwoording die de gemeente moet afleggen.

Via ENSIA verantwoord de gemeente Hoorn over:

- Baseline Informatiebeveiliging Overheid (BIO)
- Suwinet- en DigiD-aansluitingen
- Basisregistratie Adressen en Gebouwen (BAG)
- Basisregistratie Grootschalige Topografie (BGT)
- Basisregistratieonderhoud (BRO)
- Basisregistratie Personen (BRP)
- Paspoorten en Nederlandse Identiteitskaarten (PNIK)

De onderdelen Suwinet en DigiD moeten worden getoetst door een externe auditor. Voor DigiD is gemeente Hoorn ook verplicht een Pentest te doen.

4.4.2 Dataclassificatie

De eisen ten aanzien van het gebruik van cloud kunnen alleen worden vastgesteld wanneer bekend is wat de gevoeligheid en waarde van de data is die erbij betrokken zijn. Dit inzicht is te verkrijgen met behulp van dataclassificatie. Nadat de data zijn geclassificeerd wordt met een beslisboom bekeken welke, of op welke manier, er data van de gemeente Hoorn naar de Cloud gaat.

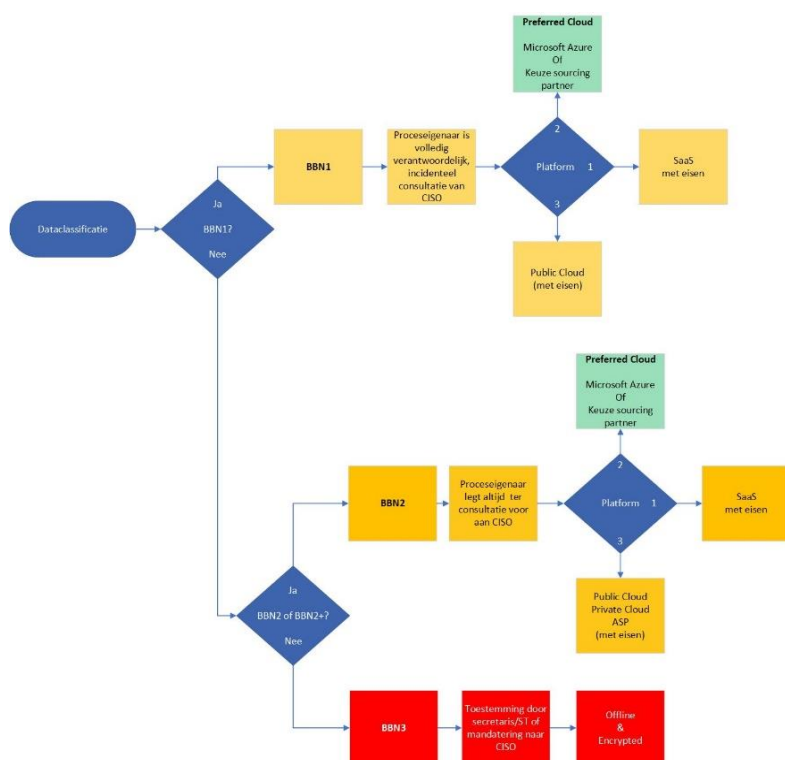
Dataclassificatie is het belangrijkste instrument om vast te kunnen stellen welke eisen er gesteld worden aan de benodigde graad van bescherming van de data. Voor iedere informatiedienst die in de cloud wordt geplaatst, wordt het onderstaande dataclassificatie beslisschema doorlopen. De uitkomst bepaalt welke cloudvariant gebruikt mag worden.

We onderscheiden de volgende risico-categorieën die zijn gebaseerd op de BBN-niveaus uit de BIO:

- BBN1 – basisniveau;
- BBN2 – verhoogd niveau;
- BBN2+;
- BBN3 – hoog risico.

De volgende afbeelding geeft de cloudmogelijkheden weer met betrekking tot dataclassificering. De opzet van het beslisschema beperkt zich slechts tot de Vertrouwelijkheid en laat de Integriteit en Beschikbaarheid van data buiten beschouwing. Voor wat betreft de Beschikbaarheid geldt dat rekening wordt gehouden met een maximale Recovery Point Objective (RPO) en Recovery Time Objective (RTO) tijd. RPO betekent: hoeveel dataverlies is maximaal acceptabel in het geval van een calamiteit. RTO betekent: hoelang mag het maximaal duren voordat data en functionaliteit weer beschikbaar zijn.

Met betrekking tot de Integriteit geldt dat de cloudapplicaties moeten beschikken over een goed log- en autorisatiesysteem (zie link “Handreiking Logging” in Bijlage 1), zodat de data niet gecorrumpereerd worden. Bij het bepalen van eisen aan data geldt als uitgangspunt dat de cloudpraktijk van het rijk of andere gemeenten wordt gevolgd.



Figuur 3. Dataclassificatie beslisboom

Daarmee geldt dat afhankelijk van de risico-categorie de volgende cloudvarianten zijn toegestaan:

Risico-categorie	Toegestane cloudvarianten:
BBN3	Geen
BBN1 & BBN2/2+	Gestructureerde data (databases): • SaaS- en ASP-oplossingen van Nederlandse providers die AVG compliant zijn; • Public IaaS oplossingen van providers die AVG compliant zijn; • Private IaaS oplossingen van providers die AVG compliant zijn; en ongestructureerde data (documenten met bijbehorende meta-data): • Public IaaS oplossingen van providers die AVG compliant zijn; • Private IaaS oplossingen van providers die AVG compliant zijn.

4.4.3 SaaS

Binnen de gemeente Hoorn wordt uitgegaan van een SaaS-tenzij beleid. Het omzetten van een on-premise naar een SaaS variant moet zoals eerder vermeld weloverwogen plaatsvinden en mag nooit leiden tot meer complexiteit.

4.4.4 Office365

Gemeente Hoorn maakt reeds gebruik van **Office365**. Bij de aanschaf van applicaties die afhankelijk zijn van de Office Suite dient hier rekening mee te worden gehouden.

4.4.5 Authenticatie

Gemeente Hoorn maakt reeds gebruik van **Active Directory**, **ADFS** en **SAML 2.0** en **MFA** voor authenticatie doeleinden. Bij de aanschaf van SaaS diensten dient hier rekening mee te worden gehouden.

4.4.6 Geen Cloud

Gemeente Hoorn dient nog vast te stellen wat er op dit moment niet naar de cloud wordt gebracht. Dit hangt samen met de uitkomst van dataclassificering, een workflow die niet in zijn geheel weggezet kan worden, het ontbreken van support van de leverancier, datavraagstukken etc.

Bijlage 1: Bronverwijzingen

Dit document is mede gebaseerd op een aantal externe documenten:

- IBD Handreiking Impact Cloudcomputing
- IBD Handreiking Inkoop Clouddiensten
- IBD Handreiking Cloudcomputing en Privacy
- IBD Handreiking Bedrijfscontinuïteitsbeheer
- IBD Handreiking Logging
- Baseline Informatiebeveiliging Overheid (BIO)
- Common Ground
- Gemeentelijke Gemeenschappelijke Infrastructuur
- GGI-Veilig
- GGI-Netwerk
- ENSIA

Bijlage 2: Definities

Onderwerp	Omschrijving
Cloud Servicemodel	Beschrijft hoe het service-aanbod van een leverancier is, en hoe een afnemer diensten geleverd krijgt: • 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 Servicemodel - Cloud-applicaties: SaaS	Bij het “Software as a Service” model wordt bedrijfsapplicatie functionaliteit aangeboden als een dienst. Deze functionaliteit wordt naar de gebruikers ontsloten via een Web gebruikersinterface.
Cloud Servicemodel - Cloud-platforms: PaaS	Bij het “Platform as a Service” model worden applicatie infrastructuur componenten als dienst aangeboden. Voorbeelden van applicatie infrastructuur diensten die via het PaaS servicemodel aangeboden worden zijn applicatie servers, portalen, service bussen en databases. Afnemers kunnen in het PaaS service model eigen applicaties op het platform laten hosten en kunnen deze laten integreren met de geboden applicatie-infrastructuur.
Cloud Servicemodel - Cloud-infrastructuur: IaaS	Bij dit model wordt de hardware en technische infrastructuur gevirtualiseerd als dienst aangeboden. Hierin is nog een onderscheid te maken in public IaaS (met andere klanten gedeelde infrastructuur) en private IaaS (infrastructuur in gebruik door één specifieke klant).
Cloud Deployment model	De wijze waarop Cloud diensten aan de afnemer worden aangeboden, hangt daarbij onder meer af van de eisen die de afnemer stelt ten aanzien van: - de beveiliging en performance van de dienst(en); - de eisen die wet- en regelgeving aan deze diensten stelt.
Cloud Deployment model - Private Cloud	Een private Cloud is een Cloud waarbij onderliggende resources worden gebruikt door één organisatie. In een private Cloud worden zware eisen gesteld aan zowel de beveiliging van infrastructuur en gegevens als de beschikbaarheid hiervan.
Cloud Deployment mode - Community Cloud (ook wel gedeelde Cloud)	Een Community Cloud is een Cloud infrastructuur die door verschillende organisaties wordt gebruikt. De organisaties die een gedeelde Cloud gebruiken zijn over het algemeen organisaties die in eenzelfde marktsegment opereren of eenzelfde soort dienst afnemen.
Cloud Deployment model - Public Cloud	Een public Cloud is een Cloud infrastructuur die ter beschikking wordt gesteld aan een grote markt waarbij onderliggende resources gezamenlijk worden gebruikt door de afnemers.
Cloud Deployment model - Hybrid Cloud	Een hybride Cloud is een Cloud infrastructuur die bestaat uit een samenstelling van twee of meer Clouds (private, community, public) die ieder afzonderlijk bestaan maar met elkaar zijn verbonden door middel van gestandaardiseerde koppelvlakken om interoperabiliteit tussen diensten te ondersteunen.

Gemeente Hoorn

Nieuwe Steen 1
Postbus 603
1620 AR Hoorn
T 0229 25 22 00
www.hoorn.nl