VNG Realisatie

Referentieachitectuur Cloud Basis Infrastructuur Gemeenten

Vereniging van Nederlandse Gemeenten

Nassaulaan 12
2514 JS Den Haag

Auteurs: André Boonzaaijer
Datum: 31 maart 2023

Versie	Datum	Auteur	Belangrijkste wijzigingen
0.1	31-03-2023	André Boonzaaijer	Initiële versie
0.2	31-03-2023	André Boonzaaijer	Verwerken reviewresultaten Jurgen Allewijn (Amsterdam), Roderick Shaefer, Jan Brinkkemper, Joost Tholhuijsen, Jule Hintzbergen, Arnoud Quanjer, Pieter-Bas Nederkoorn

Inhoud

1. Inleiding

Voor u ligt de referentiearchitectuur CBI, *Cloud Basis Infrastructuur*, samengesteld vanuit VNG. Dit document is tot stand gekomen vanuit de constatering dat veel gemeenten bezig zijn met het toepassen van diverse clouddiensten in hun IT-landschap, veelal zonder expliciet kader hiervoor met richtlijnen en uitgangspunten. Deze referentiearchitectuur heeft tot doel dit kader te bieden zodat handvatten geboden worden aan gemeenten voor een stabiele en gedegen inrichting, conform de bestaande richtlijnen en standaarden, van hun clouddienstenportfolio.

In het eerste hoofdstuk na de samenvatting zal dit document ingaan op de aanpak van de totstandkoming en de scope van dit document. Vervolgens gaan we in op de bestaande normen en kaders in gemeenteland die op dit onderwerp van toepassing zijn. Daarna volgen de uitkomsten van diverse gehouden interviews, en onderkennen we een aantal basisprincipes, organisatieprincipes en implementatieprincipes voor de inzet van clouddiensten. Bij dit document zijn ook een aantal relevante bijlagen gevoegd waarnaar verwezen wordt in de voornoemde principes.

2. Samenvatting

CBI beoogt gemeenten te voorzien van handvatten en richtlijnen om tot een gedegen inrichting van hun clouddienstenportfolio te komen, conform richtlijnen en regelgeving. Vanuit een groot aanbod aan bestaande standaarden en richtlijnen zijn in dit document de basisprincipes opgenomen voor het realiseren en/of afnemen van diensten in de cloud door gemeenten. Dit is gecombineerd met de uitkomsten van een aantal interviews en een enquête gehouden onder gemeenten, om een beeld te krijgen van de behoefte en de huidige situatie bij gemeenten.

Dit document schetst een referentiearchitectuur in de vorm van een aantal principes, die ingedeeld zijn in basisprincipes, organisatieprincipes en implementatieprincipes. Dit zijn waar mogelijk vertalingen van reeds bestaande principes, richtlijnen en kaders naar toepassing op gebruik, implementatie en beheer van clouddiensten.
In de basis is het van belang dat er een strategie en exitplan is voordat er diensten uit de cloud betrokken worden door gemeenten. Ook is een op clouddiensten toegespitste vorm van risicomanagement vereist. Daarnaast is het belangrijk dat de competenties, regie en werkwijze aansluiten bij het uitvoeren van automatisering in de cloud. Tenslotte zijn er een aantal harde randvoorwaarden aan de diensten zelf, en de (technische) inrichting hiervan, waaraan moet worden voldaan. Deze gaan hoofdzakelijk over privacy/security, locatie van dataopslag, uitwisselbaarheid, back-ups en interoperabiliteit/deelbaarheid van data tussen systemen.

Alle gebruikte bronnen en kaders zijn in bijlagen en referenties bij dit document gevoegd.

3. Context

Het project CBI beoogt synergie en uniformiteit te vergroten tussen gemeenten die bezig zijn om clouddiensten te implementeren in hun IT-landschap. Gemeenten zijn enerzijds organisatorisch (vanwege krapte op de technische arbeidsmarkt), anderzijds marktgedreven meer en meer geneigd om clouddiensten te gaan toepassen. Met name op het gebied van bemensing en kennis van zaken is het vaak niet houdbaar om voor iedere gemeente een eigen (technische) beheerorganisatie voor het IT landschap te bestieren. De belofte van cloudcomputing is ook dat IT goedkoper kan door meer uit te besteden: je betaalt voor wat je gebruikt en meer niet.

Een referentieachitectuur heeft tot doel om een set principes, kaders en richtlijnen te schetsen waarbinnen bepaalde oplossingen (in dit geval in de automatisering/informatietechnologische context met behulp van clouddiensten) gerealiseerd (zouden moeten) worden. Het doel is dat de uniformiteit van de oplossingen binnen de reikwijdte van deze architectuur vergroot wordt zodat zaken als overdraagbaarheid, synergie, beheer(s)baarheid vergroot danwel verbeterd worden. Daarnaast biedt een architectuur kaders en richtlijnen die werkzaamheden die plaatsvinden onder deze achitectuur ondersteunen en richting geven.
Een architectuur is dus géén concreet ontwerp of een blauwdruk. Desalniettemin bevat dit document verwijzingen naar een aantal voorbeelden, uitwerkingen en blauwdrukken die sterk samenhangen met de geschetste kaders, principes en richtlijnen. Die kunnen gebruikt worden om de norm die geschetst wordt in deze architectuur concreter in te vullen.

Een architectuur heeft pas waarde als deze breed gedragen en toegepast wordt. Deze referentiearchitectuur is dan ook niet alleen voor, maar ook door gemeenten: tijdens de totstandkoming hiervan is op verschillende manieren achterhaald waar gemeenten nu al gebruik van maken en ook voornamelijk wat de behoeften zijn van gemeenten op dit vlak. Er zijn diverse interviews geweest met gemeenten,

Kortom, dit document is tot stand gekomen door ‘bottom-up’ te verzamelen wat behoeften zijn en gebruik is bij gemeenten op dit moment, en ‘top-down’ door vanuit de markt en via experts te onderzoeken wat de mogelijkheden zijn – tevens in context geplaatst van wettelijke en bestuurlijke kaders en reeds bestaande principes, kaders en richtlijnen (BIO, NORA, GEMMA, Common Ground, Rijkscloudbeleid, AVG, HAVEN). Vervolgens is dit gefilterd en waar mogelijk toegepast op het centrale thema, cloudcomputing.

Cloudcomputing

Cloudcomputing is een zeer brede term en het is dan ook van belang dat we hier een duidelijke definitie voor hanteren voor het gebruik van dit document.

De algemeen geaccepteerde definitie van National Institute of Science and Technology (NIST) luidt:

Cloud computing is een model om op afroep op een gemakkelijke manier via een netwerk toegang te krijgen tot een gedeelde verzameling van configureerbare computer resources (bijvoorbeeld netwerken, servers, opslag, applicaties en diensten) die snel kunnen worden geleverd en vrijgegeven met minimale inspanning of interactie met leveranciers. Cloud computing heeft vijf essentiële karakteristieken:

- On-demand selfservice: naar behoefte verkrijgbaar zonder menselijke interactie met de leverancier
- Breed beschikbare netwerktoegang: te gebruiken via een gestandaardiseerde netwerkverbinding
- Gedeelde resources: computermiddelen worden gedeeld door verschillende afnemers
- Snelle elasticiteit: gebruik is snel op en af te schalen. Beschikbare computermiddelen lijken onbeperkt
- Afgemeten dienstverlening: het verbruik is meetbaar, transparant en eenduidig

Binnen deze vorm van dienstverlening is een onderverdeling te maken in het niveau van dienstverlening. Over het algemeen worden drie niveaus van cloudcomputing onderkend:

- IaaS, ofwel *Infrastructure as a Service*, waarbij infrastructurele componenten (bijvoorbeeld opslagruimte, rekenkracht of netwerkinfrastructuur) bij de leverancier worden betrokken.
- PaaS, ofwel *Platform as a Service*, waarbij beheerde platformen waarop software ontwikkeld kan worden bij de leverancier worden betrokken. Dit zijn vaak een set aan technische functionele componenten of diensten gebruikt binnen ontwikkelteams. Hierbij is de onderliggende infrastructuur, dus de netwerken, storage en (virtuele) machines verborgen achter de functionele facade van deze diensten.
- SaaS, ofwel *Software as a Service*, waarbij kant-en-klare software als dienst wordt afgenomen. Denk hierbij aan Microsoft365 (voorheen Office 365) of Google Workspace (waaronder o.a. Gmail).

On-premises	IaaS	PaaS	SaaS
Applicatie	Applicatie	Applicatie	Applicatie
Database	Database	Database	Database
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
OS	OS	OS	OS
Virtualisatie	Virtualisatie	Virtualisatie	Virtualisatie
Server	Server	Server	Server
Opslag	Opslag	Opslag	Opslag
Netwerk	Netwerk	Netwerk	Netwerk
Beheerd door:	Klant	Leverancier	

Bovenstaande afbeelding illustreert de verdeling van beheertaken tussen klant en leverancier, bij elk van de niveaus. Hoe verder naar rechts in de dienstverlening, hoe meer beheertaken uit handen worden genomen.
Belangrijk om hierbij aan te tekenen is dat de informatie die verwerkt wordt uiteindelijk altijd beheerd wordt door de klant. Daarnaast is het ook zo dat dit de suggestie wekt dat bij SaaS een heleboel verantwoordelijkheden op lagere technische lagen wegvallen bij de klant. Dat is uiteindelijk, en met name voor overheden, niet het geval. Daar zal in het vervolg van dit document nog uitgebreid bij stilgestaan worden.

Inmiddels zijn er talrijke andere '.. as a Service' indelingen bedacht, maar voor de eenvoud laten we het hier even bij deze klassieke indeling in drie niveau's. Het is van groter belang om het dienstenportfolio, zowel in termen van behoeften als termen van aanbod, van gemeenten in het algemeen te schetsen. Door dit in kaart te brengen kunnen we een zinnige set aan uitgangspunten geven voor het al dan niet cloud-based benaderen van deze diensten.

Scope

Dit document is bedoeld voor alle Nederlandse gemeenten. Omdat deze 342 gemeenten allen een eigen unieke inrichting van de IT-huishouding hebben kiezen we er in dit document voor om een opdeling te maken in enerzijds technische thema's op het gebied van cloud computing, anderzijds een organisatiegerichte opdeling in hoe deze technische thema's in de eigen gemeente kunnen worden ingericht.
Er is gezocht naar de belangrijkste onderwerpen in de grote verzameling van standaarden en richtlijnen die reeds beschikbaar zijn, en deze zijn toepasbaar gemaakt in een aantal principes die slaan op cloudcomputing voor gemeenten in de breedste zin des woords: van uitbestede SaaS-diensten als email tot en met virtuele servers die betrokken worden bij een IaaS-leverancier.

4. Bestaande normen, kaders en standaarden

Binnen de diverse overheden in Nederland, en specifiek binnen gemeenten, zijn al veel standaarden, kaders en normen vastgelegd. Dit hoofdstuk biedt een kort overzicht van relevante standaarden die gebruikt zijn om de CBI-principes verderop te schetsen. Dit overzicht is geenszins compleet maar dient ter referentie naar de relevante bronnen die geraadpleegd zijn op dit vlak.

We noemen hier de belangrijkste normen op gebied van security en privacy, alsmede de beleidslijn die uitgezet wordt door onze landelijke overheid. Dit zijn vrij harde en concrete normen die feitelijk te allen tijde gevolgd zouden moeten worden. Daarbinnen kennen we een set aan informatiearchitectuurprincipes, ook vanuit het rijk verstrekt. Deze principes zijn vervat in een ‘familie’ van architecturen, waarbij de overkoepelende architectuur (NORA) specifiek is ingevuld voor gemeenten (GEMMA). Daarbinnen kennen we nog een aantal concretere richtlijnen (Common Ground) en standaarden (HAVEN).

BIO

BIO, de *Baseline Informatiebeveiliging Overheid*[1], is een invulling van de ISO 27001:2017 informatiebeveiligingsnorm. Deze norm dekt via een groot aantal zgn. ‘controls’ de zaken die afgedekt moeten worden om informatie grondig en afdoende te beveiligen. Gecombineerd met deze controls wordt binnen de BIO een drietal beveiligingsniveau’s, BBN1 t/m BBN3 (*Basis BeveiligingsNiveau)* onderscheiden. Informatie en processen kunnen geclassificeerd worden op basis van deze niveau’s, en specifiek is op basis van deze niveau’s een overzicht opgenomen in het BIO Thema Clouddiensten[2], zoals hieronder geschetst.

Voorgenomen Cloudbeleid 1-okt-2019 in een matrix overzicht:

Classificatie volgens QIS:	Non-Cloud in ODC	Private Cloud in ODC	Private Cloud bij leverancier	Public of Hybride Cloud
BIO-BBN1	Toegestaan, mits (1)	Toegestaan, mits (1)	Toegestaan, mits (1)	Toegestaan, mits (1)
BIO-BBN2 en ongerubriceerd	Toegestaan, mits (1)	Toegestaan, mits (1,2)	Toegestaan, mits (1,2)	Toegestaan, mits (1,2)
BIO-BBN2 en DepV-gerubriceerd	Toegestaan, mits (1)	Toegestaan, mits (1,2,3)	Toegestaan, mits (1,2,3)	Niet toegestaan, tenzij (1,2,3,4)
BIO-BBN3, incl. EU/NATO gerubriceerd	Toegestaan, mits (1)	Thans niet mogelijk	Niet toegestaan	Niet toegestaan

Zonder specifiek in te gaan op de voorwaarden zien we in elk geval het beeld onstaan dat voor de meeste gevallen, d.w.z. bronnen geclassificeerd binnen BBN1 of BBN2, mogelijkheden bestaan om externe private clouddiensten en zelfs public clouddiensten te gebruiken.

AVG

De *Algemene verordening gegevensbescherming* (AVG) is sinds mei 2018 van kracht. Het is een europese privacywet die strikte eisten stelt aan organisaties die persoonsgegevens verzamelen en/of verwerken. In feite heeft de AVG beperkt invloed op het al dan niet verwerken van gegevens met behulp van clouddiensten; het is meer een kader voor de manier waarop met persoonsgegvens omgegaan moet worden. Hetgeen uiteraard wel belangrijk is blijft natuurlijk dat de gegevens, eenmaal wel opgenomen in systemen, goed beveiligd worden. De overige geschetste normen vanuit met name het rijk die in dit document geschetst worden dekken de AVG voldoende af – immers, al deze normen zijn ook opgesteld om binnen de in de AVG gestelde kaders te opereren.

Rijksbeleid

Vanuit het ministerie van binnenlandse zaken is per 2022 een rijkscloudbeleid geformuleerd[3]. In deze kamerbrief wordt gesproken over het onder voorwaarden kunnen inzetten van publieke clouddiensten door overheidsinstanties. Alle in dit document genoemde diensten van externe leverenciers vallen onder deze vlag van ‘publieke clouddiensten’.

Beleid

De in de kamerbrief gestelde voorwaarden voor gebruik van deze diensten zijn:

- Voor verwerking van persoonsgegevens dient altijd een pre-scan DPIA (*Data Protection Impact Assessment*) uitgevoerd te worden. Bij een uitkomst ‘hoog risico’ dient een volledige DPIA uitgevoerd te worden.
- Defensie en staatsgeheimen (nooit toegestaan) vallen buiten de scope van dit beleid.
- Een eigen cloudbeleid en -strategie dient geformuleerd te zijn.
- Een risicoafweging dient gemaakt te worden, met auditeerbare besluitvorming.
- Gekend gebruik: rijksbreed wordt gesproken over jaarlijkse rapportage m.b.t. verwerking persoonsgegevens aan CIO-Rijk.
- Exit-strategie: Er dient altijd geregeld te zijn hoe data worden overgedragen en verzamelde data bij leveranciers worden vernietigd bij beëindiging van de overeenkomst.
- Risicoanalyse t.b.v. materieel publiek cloudgebruik (d.w.z. de ingekochte dienst is van wezenlijk belang).
- Specifieke risicoanalyse op gebied van geografische regio waar gegevens worden opgeslagen en is er ‘right-to-audit’ voor opdrachtgever.
- Aandacht voor Cyberveiligheid m.b.t. statelijke actoren – aan te sluiten bij Europees beleid.
- Wet Open Overheid: openbaarmaking van besluitvorming over de gegevensbeschermingseffectbeoordelingen (DPIA’s).
- Voldoen aan privacy-vereisten AVG, minimaal aan één van onderstaande eisen voldoen:
    - Opslag en verwerking gegarandeerd binnen EER of
    - Opslag in landen waarvoor een adequaatheidsbesluit bestaat, of
    - Op basis van een een passend doorgiftemechanisme dat voldoet aan de vereisten (art. 46, hoofstuk V van AVG)
- Bijzondere persoonsgegevens: Dan en slechts dan in publieke cloud als voorgaande punt 1 of 2 voldoet. Punt 3 (doorgiftemechanisme) alleen via ‘pas-toe-of-leg-uit’.

Implementatiekader
Naast deze beleidsbrief is een aanvullend implementatiekader[4] gepubliceerd. Deze bevat in artikel 4 een risicoafweging die samengevat neerkomt op:

- Een risicomanagementmethodiek conform BIO is vastgesteld;
- Hergebruik ervaringen vanuit SLM-rijk[5] (*Strategisch LeveranciersManagement)*;
- De toegespitste risicoanalyse omvat ten minste:
    - Context en karakteristieken van het cloudgebruik (leveranciersselectie, type dienstverleding, gevoeligheid en geografische regio van verwerking/opslag);
    - Relevante risico's met aandacht voor C2000 criteria, veiligheid en continuïteit;
    - Hoofdstuk 15 BIO (informatiebeveiligingseisen), met aandacht voor recht van audit, beschrijving van exitstrategie en ketenrisico's (hoe beoordeelt leverancier zijn onderleveranciers);
    - Beoordeling van opzet, bestaan en werking van de maatregelen;
    - Afweging dat risico's voldoende gemitigeerd worden met eventuele restrisico's en borging daarvan.
- Risicoanalyse is formeel vastgesteld conform het cloudbeleid.

NORA

De Nederlandse OverheidsReferentie Architectuur ofwel NORA biedt principes, kaders en richtlijnen voor de inrichting van de IT organisatie van overheden. In de bijlage zijn de basisprincipes van de NORA opgenomen. De verderop opgesomde CBI architectuurprincipes bevatten de verwijzingen naar de betreffende NORA principes die als basis hebben gediend.

GEMMA

De eerdergenoemde NORA is een familie van architecturen, waarvan de GEMMA een dochter is specifiek voor gemeenten. Waar NORA logischerwijs wat abstracter blijft bevat de GEMMA een heel aantal specifieke en concrete invullingen. Een aantal bronnen die in het kader van cloudcomputing relevant zijn:

- Het *Globaal programma van eisen voor pakketsoftware*[6] geeft een goed overzicht van de vereisten waar alle standaardsoftware aan dient te voldoen.
- De GIBIT[7], *Gemeentelijke Inkoop bij IT Toolbox*,
- De informatiearchitectuurprincipes[8]

Common Ground

Common Ground[9] is een zienswijze hoe om te gaan met gegevens binnen Gemeenten. Het doel hiervan is om eenvoudiger, sneller en slimmer te kunnen bijdragen op gebied van digitalisering aan grote maatschappelijke opgaven.
De uitgangspunten van Common Ground zijn

- Uniforme gegevens
- Uitwisseling van gegevens via API's
- Eén gemeenschappelijke integratielaag (*NLX*[10])
- Gegevens blijven in de bron

Daarnaast bevat Common Ground een aantal principes, op gebied van:

- Samenwerking
    - Gemeenten bepalen zelf het tempo en de manier waarop Common Ground wordt toegepast
    - Rollen en verantwoordelijkheden worden per opgave expliciet gemaakt
    - Agile (kortcyclisch en iteratief) werken is de norm
    - Via het College van Dienstverlening van VNG worden standaarden vastgesteld
- Informatiearchitectuur
    - Componentgebaseerde implementatie met gestandaardiseerde interfaces
    - Open en transparant werken
    - Vertrouwd – beveiliging en privacy zijn op orde
    - Eenmalige vastlegging – 'single point of truth'
    - Regie op gegevens wordt gefaciliteerd
    - Standaardisering wordt gemaximaliseerd
- Realisatie
    - Gemeenten en overige stakeholders werken als community samen om Common Ground te realiseren
    - Agile
    - Nieuw naast oud – geleidelijke vervanging van bestaande architectuur
    - Moderne IT – moderne technologie benutten mits van meerwaarde
    - Open source wordt gestimuleerd
    - Uitwisseling: veilig, betrouwbaar en snel

Tevens bevat Common Ground een abstracte omschrijving van de invulling van deze uitgangspunten en principes in een gelaagd model. De essentie van Common Ground is met name dat er een logische en robuuste opdeling in componenten gedaan is zodat verregaande integratie en hergebruik mogelijk is tussen deze diverse componenten, waardoor aan bovenstaande principes voldaan kan worden.

HAVEN

Onder de paraplu van Common Ground is er op één specifiek technisch vlak een concrete implementatiestandaard voor *containerized* applicaties gedefinieerd genaamd *HAVEN*. Een containerized applicatie wil zeggen dat de applicatielogica in een geïsoleerde, snel uitrolbare en schaalbare standaard-runtime is verpakt die doormiddel van zogenaamde 'orchestratie-engines' op verzoek in enkele of meervoudige verschijningsvorm uitgerold kan worden. Het is in feite een soort lichtgewicht server waarvan kopieën zeer snel aan en uitgezet kunnen worden, afhankelijk van de vraag naar capaciteit op een bepaald moment. Bijkomend voordeel van deze techniek is dat deze gestandaardiseerde containers bij vrijwel alle moderne cloudleveranciers zonder veel moeite kunnen worden neergezet. Het biedt dan ook een mooie oplossing ter voorkoming van vendor lock-

in en garandeert een robuustere, toekomstvaste infrastructuur die verregaand geautomatiseerd beheer ondersteuntd.
HAVEN definieert bovenop een standaard *kubernetes* omgeving (kubernetes is een orchestratie-engine die containers op een cloudplatform kan beheren) een 16-tal aanvullende eisen op gebied van o.a. beschikbaarheid, encryptie, infrastructuur. De volledige lijst van eisen die de HAVEN standaard vormt is terug te vinden in de bijlagen.

5. Uitkomsten interviews & Enquête

Naast voorgaande inventarisatie van relevante richtlijnen en kaders is dit document tot stand gekomen op basis van de uitkomsten van een aantal interviews met gemeenten en een breed uitgestuurde enquête. De resultaten van de enquête zijn terug te vinden in (enqueteresultaten).

De belangrijkste bevindingen vanuit de interviews onder gemeenten zijn hier kort samengevat opgenomen.

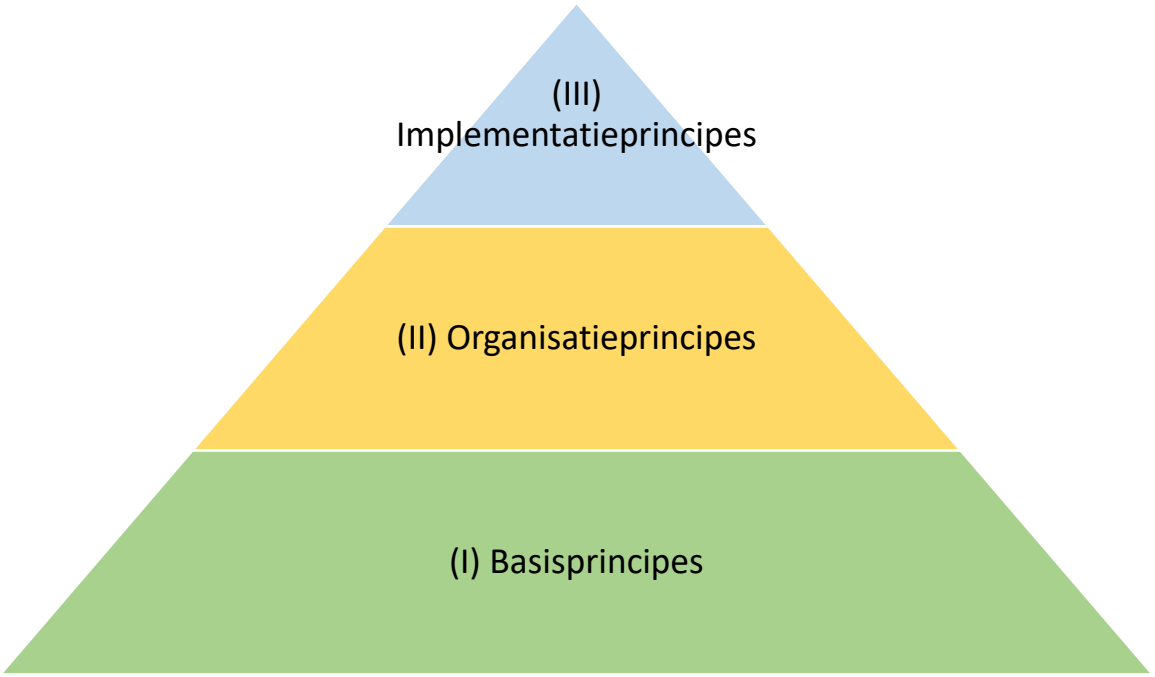
- Geïnterviewde gemeenten hebben voor het grootste deel (80%) een ‘cloud-first’ strategie. Daarbij wordt ‘SaaS boven PaaS boven IaaS’ gehanteerd. Daarmee wordt eerst gekeken naar een automatiseringsalternatief als SaaS (bruikbare panklare software), vervolgens PaaS (bruikbare panklare bouwblokken), vervolgens IaaS (panklare servers).
- De meeste gemeenten geven aan zelf geen software te ontwikkelen.
- Veel gemeenten hebben nog een (grote) on-premises infrastructuur. Deze is in vrijwel alle gevallen gevirtualiseerd maar omvat vaak tientallen tot honderden virtuele machines (servers). Een grove statistische analyse schetst het beeld van ongeveer één virtuele machine (VM) per 500 inwoners.
- Van de ‘grote’ leveranciers staat bij vrijwel alle gemeenten Microsoft bovenaan. Er zijn geen gemeenten gevonden die een ‘multi-cloud’ strategie hebben, slechts wat sporadische initiatieven met andere leveranciers.
- De 'vendor lock-in’ die hiermee gepaard gaat wordt door sommige gemeenten opgevangen door off-site back-ups of een specifieke keuze voor bepaalde systemen om toch nog on-premises te draaien. Het algemene beeld is echter dat de vendor lock-in als een feit wordt gezien dat niet te voorkomen is (bij gebrek aan alternatieven en/of capaciteit om de kennis over meerdere platforms te ontwikkelen).
- Door verregaande keuze voor één platform zien we een aantal interessante ervaringen en concretere producten op gebied van Microsoft Azure in gemeenteland.
- Initiatieven en standaarden als Common Ground en HAVEN zijn voor met name kleinere gemeenten te weinig concreet om bruikbaar te zijn. De consensus is wel heel breed dat dit goede standaarden zijn en de wil om hier meer aan te conformeren is groot.
- Onder de uitdagingen bij meer gebruik van clouddiensten wordt de organisatieverandering vrijwel overal genoemd.
- Samenwerkingen tussen gemeenten blijken bestuurlijk lastig. Gemeenten die onder een dergelijke paraplu vallen blijven vaak wel een eigen koers varen. Met name door laagdrempelige clouddiensten zien we hier nog weleens een wat bontere omgeving ontstaan.
- Grotere gemeenten laten zich veel ondersteunen op organisatieinrichting/proces door partijen als Weolcan, en bij specifieke Azure inrichtingen wordt InSpark vaak genoemd.
- Met de verschuiving van dienstverlening naar SaaS-proposities door leveranciers, met name in de specifieke gemeentelijke markt, zijn er zorgen over de traceerbaarheid, auditeerbaarheid en algemene toegankelijkheid van dit soort systemen. Doordat de platformen niet meer zelf gehost worden is er ook geen toegang meer tot de runtime, storage, databases en berichtenstromen, waardoor auditing op een andere manier ingeregeld moet worden.

6. Architectuurprincipes CBI

Dit hoofdstuk bevat de kern van deze referentiearchitectuur: de ontwerpprincipes waar alles op voortbouwt. Zoals de GEMMA zich verhoudt tot de NORA, verhouden deze principes zich ook weer tot deze bovenligende architecturen. Het is belangrijk hierbij aan te tekenen dat de in dit document gestelde principes bovengenoemde architecturen aanvullen en op sommige vlakken concreter invullen, en dus niet vervangen. Kortom, alle informatiekundige principes vanuit NORA, GEMMA en Common Ground gaan voor op alle in dit document genoemde principes en het is dan ook noodzakelijk deze bij implementatie van clouddiensten nog steeds bij de hand te houden en toe te passen.

De CBI principes worden in dit hoofdstuk opgesomd met omschrijving, implicaties en bronverwijzingen. De principes zijn ingedeeld in drie categorieën:

- Basisprincipes: hierin is een aantal basisvoorwaarden vervat die essentieel zijn alvorens met cloud computing aan de gang te gaan binnen de gemeente. Deze zijn niet zo zeer technisch van aard maar scheppen een aantal randvoorwaarden om beheerst en gestructureerd aan de slag te kunnen gaan met cloud computing.
- Organisatieprincipes: hierin stellen we een aantal belangrijke principes die betrekking hebben over de organisatie. De werkwijze, interactie met leveranciers en benodigde competenties zijn de thema's waarover nagedacht dient te worden om succesvol te zijn in de cloud.
- Implementatieprincipes: dit zijn meer technische zaken die geregeld moeten worden om te voldoen aan de eisen die gesteld worden vanuit de diverse bestaande richtlijnen en standaarden.



Gezien de technische aard van cloud computing zijn deze implementatieprincipes het grootst in aantal. Zoals echter bovenstaande piramide suggereert is het niet erg zinvol om slechts met de techniek aan de slag te gaan; de basis in de vorm van beleid en risicomanagement en een juist ingerichte organisatie zijn randvoorwaardelijk om op een gedegen manier, onder deze architectuur, met cloud computing aan de slag te gaan.

Basisprincipes

titel **CBI-Basisprincipe01: "Er is een onderbouwde cloudstrategie met bijbehorend beleidskader gedefinieerd waardoor nieuwe cloudinitiatieven toetsbaar en conform dit beleid worden ingevuld."**
omschrijving De manier van sourcing van IT systemen heeft zijn weerslag op de organisatie, processen en technologie binnen de gemeente. Het omvormen van deze basiselementen van de bedrijfsvoering is een tijdrovend en intensief proces. Het is dan ook essentieel om hier bewuste keuzes in te maken zodat de keuzes voor clouddiensten, en alles wat hierbij komt kijken, in lijn zijn met een beleidslijn voor de langere termijn. De keuze om bepaalde beheerstaken wel of niet zelf in de organisatie in te vullen moeten expliciet gemaakt worden zodat de binnen de gemeente aanwezige expertise aansluit bij de implementatie van nieuwe en vervanging van bestaande diensten. Binnen deze strategie en beleid is het van groot belang dat een aantal essentiële onderdelen benoemd worden. Deze komen allen aan bod in de overige principes. Concrete onderdelen van deze strategie zijn: - Eén of meerdere leveranciers (voor PaaS/IaaS). - SaaS t.o.v. PaaS/IaaS gebruik (bijvoorbeeld: SaaS boven PaaS boven IaaS) - Per geclassificeerde databron (BIO/BBN classificatie), beslisboom wat de specifieke maatregelen zijn en opties voor het gebruik van clouddiensten - Lijst met voorkeursleveranciers voor clouddiensten Elk van deze te maken keuzes heeft invloed op de inrichting van de organisatie en de technische implementatie; dit komt in verdere principes uitgebreider aan bod.
Implicaties - Er is duidelijk vastgelegde en gedeelde cloudstrategie aanwezig in de gemeente. - Er is duidelijk en concreet beleid gedefinieerd om deze strategie in te vullen binnen de gemeente.
bronnen & referenties: - Rijkscloudbeleid/Implementatiekader - GEMMA: GEM08, GEM03 - NORA: NAP06

titel

CBI Basisprincipe02: “Relevante risico’s zijn onderkend en gemanaged in een risicomanagementsysteem”

omschrijving

In deze context beschouwen we een risicomanagementsysteem niet per se als een specifiek stuk automatisering. Het risicomanagement kan ook op papier of in een set documenten vervat zijn: als er maar centrale procedures en verantwoordelijken omtrent zijn ingericht.
Risico’s dienen in dit systeem te zijn vastgelegd en proactief beheerd te worden. Dit principe geldt als kapstok voor alle verdere verwijzingen naar risicomanagement; daarvoor is het randvoorwaardelijk dat een risicomanagementsysteem aanwezig is en bijgehouden wordt.
Belangrijke cloudspecifieke risicothema’s zijn:

- Securitybeheer & monitoring van clouddiensten. Gemeenten blijven (eind)verantwoordelijk voor de data ook al is deze niet meer in eigen beheer.
- Kostenbeheersing van clouddiensten
- Regionale wetgeving bij gebruik van clouddiensten buiten EER (Europese Economische Regio)
- Auditeerbaarheid/monitorbaarheid van SaaS/PaaS-diensten
- Kennis en kunde in de organisatie

Veel belangrijke risicothema’s zullen in de verdere principes worden uitgewerkt.

Implicaties

- Er is een risicomanagementsystematiek aanwezig en er zijn verantwoordelijken die dit systeem beheren
- Relevante risico’s zijn in het risicomanagementsysteem opgenomen en worden periodiek geëvalueerd
- Aan risico’s toe te kennen gebeurtenissen worden gelogd en bijgehouden in dit risicomanagementsysteem.

Bronnen & referenties:

- NORA: NAP13, NAP17
- BIO (geheel)
- Implementatiekader, artikel 4
- BIO uitwerking clouddiensten (CIP)[11], B.06

titel

CBI Basisprincipe03: “Er is een exitstrategie voor clouddiensten”

Omschrijving

Waar er voor klassieke ‘on-premises’ softwareproducten vaak al sprake was van een vendor lock-in, is dit met clouddiensten een nog groter risico. Eenmaal onderkende kandidaatsystemen voor migratie naar clouddiensten zijn, na eenmaal in gebruik genomen te zijn, vaak lastig elders onder te brengen zonder lange en kostbare migratietrajecten.

Er dient dan ook per afgenomen dienst, op welk niveau dan ook, een plan te zijn voor een mogelijke exit; dit kan nodig zijn omdat er een conflict is ontstaan met de leverancier, of door interessantere andere aanbieders, of welke andere reden dan ook.

Naast een plan voor de verhuizing van de operatie dient er ook een calamiteitenplan te zijn voor het onverwacht onbeschikbaar zijn of raken van de clouddienst. Denk hierbij aan ‘off-site’ backups van data betreffende deze clouddienst, of anderszins mitigerende maatregelen zodat belangrijke onderdelen van de dienst (bijvoorbeeld de data of bepaalde tools) op een andere manier beschikbaar zijn.

Uiteraard kan de aard en het belang van de dienst tevens impliceren dat er juist geen exitplan is. Denk hierbij aan een tijdelijk, of niet essentieel systeem voor bijvoorbeeld een evenement of overbruggingsperiode bij migraties. Ook dit dient dan vastgelegd te worden en in de lijn te worden bekrachtigd.

Zie ook https://blog.weolcan.eu/wat-is-een-cloud-exit-strategie-precies-en-hoe-voer-je-het-uit

implicaties

- Per clouddienst is er een omschrijving van de extistrategie voorhanden
- Als de exitstrategie dat voorschrijft is er per dienst een plan dat omschrijft hoe de exit plaatsvindt, en eventueel een plan voor het opvangen van een calamiteit
- De strategie en het plan worden waar nodig afgestemd en formeel overeengekomen met de leverancier zodat de medewerking van daaruit kan worden afgedwongen.
- In deze exitstrategie zijn concrete en duidelijke afspraken gemaakt met de cloudleveranciers omtrent dataformaten en inhoud van de data die overgedragen moet worden bij een exit.

Bronnen & referenties:

- Rijkscloudbeleid
- GEMMA: GEM08

Organisatieprincipes

Bovenop de basisprincipes is het van belang de organisatie ook aan te sluiten bij de geschetste strategie en het beleid. De uitvoering hiervan stelt de nodige vereisten aan de bemensing: dit impliceert dan ook vaak een vrij ingrijpende personele verandering. .

Titel **CBI Basisprincipe04: ”Competenties binnen de organisatie sluiten aan bij de strategie”**
omschrijving Na vastleggen van een strategie is het van groot belang dat de organisatie hierop passend gemaakt wordt voor zover dat nog niet het geval is. Zo kan de focus van technisch beheer/virtualisatie bijvoorbeeld afgebouwd worden en verschuift de nadruk van de IT die overblijft binnen de gemeente veel meer naar het voeren van regie richting leveranciers.
implicaties - Een duidelijk beeld van de benodigde competenties binnen de organisatie dient geschetst te worden - Omscholing/training van medewerkers en/of aannemen van nieuwe medewerkers op gebieden waar gaten zijn in de benodigde competenties - Specifiek is er bij gebruik van SaaS-clouddiensten een veel minder sterke behoefte aan technisch beheer. Regie en functioneel beheer, toegespitst op de diensten zelf, zullen hier een veel groter deel van de werkzaamheden gaan uitmaken. - Specifiek is er bij gebruik van PaaS-clouddiensten een vrij sterke behoefte aan kennis en kunde op gebied van ontwikkeling en operations. PaaS-diensten zullen altijd nog op een bepaalde manier ingezet moeten gaan worden in een samen te stellen product, en hiervoor is het bijvoorbeeld raadzaam om een keuze te maken voor een ontwikkelplatform (eventueel Low-code bijvoorbeeld).
bronnen & referenties: - nvt

Titel **CBI Basisprincipe05: “Uitbesteding van werk vindt plaats onder degelijke regie”**
omschrijving Cloud computing hangt onlosmakelijk samen met het ‘minder zelf doen’ door organisaties op gebied van IT beheer en infrastructuur, dus een impliciete outsourcing. Afhankelijk van het niveau van de betreffende ingekochte dienst zal de leverancier steeds meer van het beheer en onderhoud voor zijn rekening nemen. Des te belangrijker is het dat deze leverancier wel de juiste kaders en richtlijnen meekrijgt om deze taken op een juiste manier in te vullen. Daarnaast is het van groot belang dat de gemeente in staat is om de juiste audits uit te voeren – de verantwoordelijkheid voor deze taken blijft wel degelijk bij de gemeente dus is een goede en duidelijke samenwerking essentieel.
implicaties - Verantwoordelijkheden van gemeente en leverancier omtrent geleverde diensten zijn duidelijk vastgelegd - Auditeerbaarheid wordt door de leverancier gefaciliteerd en door de verantwoordelijken binnen de gemeente uitgevoerd

- De activiteiten van IT verschuiven, met het meer en meer gebruiken van clouddiensten, van een beheer naar een regie. Dit impliceert ofwel om- of bijscholing, ofwel het reorganiseren van het personeelsbestand.
bronnen & referenties: - GEM08

Titel **CBI Basisprincipe06: "Organisatievorm: lean en agile werkwijze zijn de norm"**
omschrijving Het afnemen van diensten uit de cloud brengt flexibiliteit op gebied van afrekenmodel en capaciteit. Om de voordelen van het gebruik van clouddiensten te maximaliseren is het belangrijk om deze wendbare vorm van werken door te voeren in de organisatie. Door processen te stroomlijnen volgens de lean-methodiek sluiten deze beter aan bij het gebruik van clouddiensten.
Implicaties - Procesoptimalisatie/herontwerp waar nodig - Training/opleiding van mensen - Voldoende grip en overzicht over afgenomen clouddiensten, zodat ook daadwerkelijk de voordelen van het snel kunnen op maar met name ook afschalen van deze diensten genoten kunnen worden.
bronnen & referenties: - NAP16, NAP17, GEM02

Implementatieprincipes

Waar we de principes uit de voorgaande twee paragrafen kunnen zien als randvoorwaardelijke basisrichtlijnen, gaan we in dit onderdeel wat dieper in op de technische vereisten rondom clouddiensten. Hier spelen dan ook de klassiekere architectuurraamwerken als GEMMA en Common Ground een wat grotere rol, en richten we ons ook voornamelijk op het meest belangrijk geachte thema: security en privacy.

titel **CBI Basisprincipe07: "Privacy & security first voor alle systemen en diensten die persoonsgegevens bevatten of verwerken"**
omschrijving Vanuit wetgeving (AVG) en aanvullende richtlijnen (BIO) staat veiligheid en privacy bovenaan de prioriteitenlijst. Met name in systemen die persoonsgegevens verwerken. Op het gebied van connectiviteit houdt dit in dat gegevens 'in transit' te allen tijde versleuteld zijn.
Implicaties Voor alle clouddiensten: - Voor ingebruikname van clouddiensten waar persoonsgegevens worden verwerkt of opgeslagen dient te allen tijde een *pre-scan DPIA*[12] uitgevoerd te worden. - Als uit de pre-scan een hoog risico blijkt dient een DPIA uitgevoerd te worden. - Voor ingebruikname van clouddiensten waarvoor de juiste analyses zijn gedaan en voldoende bevonden dient formeel schriftelijk en auditeerbaar akkoord door de verwantwoordelijke Functionaris Gegevensbescherming te worden vastgelegd. - Op het moment dat er *bijzondere* persoonsgegevens verwerkt worden, d.w.z. gegevens omtrent gezondheid, religie, politieke voorkeur, etniciteit of vakkennis, dienen aanvullende maatregelen genomen te worden op gebied van beveiliging conform BIO – BBN2. Voor clouddiensten betrokken van een leverancier buiten de EER gelden specifieke maatregelen. Zie **CBI11**. Daarnaast wordt dit principe voor implementatie in de cloud verder uitgwerkt in **CBI08**.
bronnen & referenties: - BIO – 13.1, 13.2, 15.1.1.3, 18.1.4 - AVG - Rijkscloudbeleid - Zie bijlage "Voorbeelduitwerking strategie" hoe dit principe toegepast wordt binnen beslissingen aangaande gebruik van clouddiensten.

titel

CBI Basisprincipe08: “Clouddiensten worden onder security posture management beheerd”

omschrijving

Eén van de grootste risico’s bij migraties naar de cloud blijkt misconfiguratie van resources te zijn. Het niet onder controle zijn van configuratie van clouddiensten, gecombineerd met allerhande bij-effecten zoals grip op kosten en lifecyclebeheer vormt een reëel risico.
Grotere cloudproviders bieden zgn. CSPM, *Cloud Security Posture Management* oplossingen voor hun eigen en andermans veelgebruikte clouddiensten. Dit is vrij volwassen te noemen voor de grotere platformen op gebied van IaaS en PaaS. Voor SaaS zijn er soortgelijke oplossingen, onder de noemer SSPM ofwel *SaaS Security Posture Management* in opkomst. Hoewel deze oplossingen goed werken voor veel gebruikte, generieke SaaS diensten zoals mail en collaboration-oplossingen, is dit op gebied van niche-SaaSdiensten zoals zaaksystemen voor gemeenten nog niet of nauwelijks voorhanden. Desalniettemin worden dit soort systemen binnen gemeenten juist steeds vaker ingezet in een SaaS-vorm. Des te belangrijker om hier met de leverancier over in gesprek te gaan en in elk geval in de operatie de noodzakelijke ‘checks and balances’ van SPM te embedden, zodat er risciobewustzijn en controle ontstaat over de de geëxploiteerde diensten.

https://aws.amazon.com/security-hub/
https://azure.microsoft.com/nl-nl/products/defender-for-cloud/

implicaties

- Bij IaaS/PaaS: Een relevante vertaling van BIO controls met eventuele aanvullende securityvereisten is voor gebruik in het doelplatform beschikbaar
    - Voor Azure: https://github.com/Azure/Bio-Compliancy
    - Voor AWS: in overleg met AWS Nederland in te richten
- Bij SaaS:
    - Minimaal: een duidelijke set requirements aan beheerde SaaS-diensten is vastgelegd en ingevuld met de leverancier(s) (zie bijlage voorbeelduitwerking strategie)
    - Voor Microsoft 365: Microsoft 365 Defender
-

bronnen & referenties:

- BIO 12.2, 12.4, 12.5, 12.6
- Bijlage Security Posture Management

titel

CBI Basisprincipe09: “Er is een actief beleid en proces voor kostenbeheersing”

omschrijving

Het afrekenmodel van clouddiensten is vaak geheel anders dan zelfbeheerde systemen. Veelal geldt een ‘pay-as-you-go’ berekening, waarbij meer gebruik soms zelfs per dag of per uur meer kosten met zich meebrengt. Dit kan grote voordelen opleveren, maar vergt wel een rigoureus andere manier van kostenbeheersing: kortcyclisch moet bekeken worden of bepaalde diensten afgeschaald kunnen worden.

Dit is tevens in lijn met **CBI Basisprincipe06** en vergt dus ook aan de financiële kant een correcte invulling van de organisatie. Alternatieven voor automatisering kunnen gevonden worden onder de in **CBI Basisprincipe08** genoemde Posture Management oplossingen.

implicaties

- Kortcyclische evaluatieprocedures voor cloudportfoliobeheer moeten worden ingericht
- Idealiter wordt automatisch gemonitord en gerapporteerd over het kostenverloop en gebruik van clouddiensten.

bronnen & referenties:

- GEM08

titel

CBI Basisprinciep10 “De uitwisselbaarheid gegevens is in een afspraak met de CSP vastgelegd”

omschrijving

Met name bij SaaS-diensten is er al snel sprake van een functionele ‘black box’. Immers, de klant neemt slechts functionaliteit af en hoe de leverancier deze invult, is diens verantwoordelijkheid. Des te belangrijker is het om bij aanschaf/implementatie van dit soort diensten zeer scherp af te stemmen welke gegevens op welke manier worden uitgewisseld. Er zijn tegenwoordig breedgeaccepteerde technische standaarden; deze zijn echter op zich niet voldoende om de semantiek en reikwijdte van de uit te wisselen gegevens vast te leggen. Idealiter, als in GEMMA/Common Ground dan ook al is omschreven, wordt uitgewisseld tegen een centraal gegevensmodel dat als standaard is vastgelegd. Dat is echter nog voor veel soorten gegevens niet beschikbaar; vandaar dat het van groot belang is hier een goed beeld van te vormen en waar nodig af te stemmen met de leverancier. Het grijpt tevens in in **CBI11**. Systemen ondersteunen gegevensuitwisseling via standaarden, hierbij in acht nemende dat:

- Uitwisseling zoveel mogelijk geschiedt via gestandaardiseerde (RESTful/JSON) API’s
- Deze API’s voldoen (bij voorkeur) aan de OpenAPI 3 standaard[13]
- Alle relevante gegevens, in eigendom van de Gemeente (**CBI12**), zijn via deze API’s op te vragen danwel te importeren.

En waar relevant, als aanvulling als het een dienst die als ‘authentieke bron’ wordt aangeduid:

- Notificaties kunnen verstuurd worden vanuit het bronregister bij wijziging van gegevens
- Als gevolg van deze notificaties kunnen doelsystemen (/processen) gegevens ophalen bij deze bronregistraties

implicaties

- Clouddiensten of applicaties dienen relevante data en operaties aan te bieden via een gestandaardiseerde API
- Clouddiensten of applicaties moeten aan kunnen sluiten op bestaande databronnen
- Clouddiensten of applicaties moeten op deze manier kunnen dienen als bron voor andere applicaties in het landschap
- Gegevens worden uitgewisseld conform een standaard gegevensmodel

bronnen & referenties:

- GEMMA, Common Ground[6]

titel

CBI Basisprincipe11: "Data wordt opgeslagen bij leveranciers gevestigd binnen de EER"

omschrijving

Vanuit de AVG en het rijkscloudbeleid wordt gesteld dat data van overheden fysiek moet worden opgeslagen binnen de EER, de Europese Economische Regio. De gedachte achter deze regel is het beschermen van de burgers tegen eventueel kwaadwillende regimes: immers, data die op een fysieke locatie wordt opgeslagen valt juridisch onder het regime dat op die fysieke locatie geldt. Persoonsgegevens, en vooral bijzondere persoonsgegevens, dienen dus uitsluitend opgeslagen te worden in een regio binnen de EER waar de AVG ook daadwerkelijk geldt.

Het wordt ingewikkelder op moment dat er zaken gedaan wordt met partijen die de data wel degelijk (zeggen) op te slaan binnen de EER, maar juridisch wel onder een buiten de EU gevestigde partij vallen. Denk hierbij aan de vele voorbeelden waarbij bedrijven uit China bepaalde achterdeuren inbouwen in hun software zodat de Chinese regering kan meekijken. Het is dan ook ten zeerste af te raden om als (lokale) overheid zaken te doen met bedrijven uit die regio.
Landen die via een 'adequaatheidsbesluit' van de EU geschikt zijn bevonden vormen hier een uitzondering op (https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internationaal/doorgifte-binnen-en-buiten-de-eu#hoe-weet-ik-of-een-derde-land-een-passend-beschermingsniveau-heeft-1752).
De echte complexiteit in de praktijk is het gebruik van diensen van de bekende 'Big Tech' leveranciers uit de Verenigde Staten, in dit document veelvuldig benoemd. Hoewel deze bedrijven uiteraard beloven niets door te spelen en hier ook juridisch voor proberen te gaan liggen, vallen zij via het hoofdkantoor gevestigd in de VS wel degelijk onder Amerikaanse wetgeving als de 'patriot act'. Gegeven de situatie rond bijvoorbeeld Julian Assange (Wikileaks) is het glashelder wat daar van kan komen.
De VS staan dan ook niet op de bovengenoemde lijst.
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internationaal/doorgifte-binnen-en-buiten-de-eu#wanneer-mag-ik-persoonsgegevens-doorgeven-naar-de-vs-5539
Onder aan de streep betekent dit dat voor verwerking in de VS, dus ook gebruik van Azure/Microsoft 365/AWS/Google Cloud, aanvullende maatregelen noodzakelijk zijn zoals versleuteling van bijzondere persoonsgegevens.

Een voorbeeld van encryptie/sleutelbeheer, met het zogenaamde 'Bring your own key' in Microsoft Azure: https://learn.microsoft.com/en-us/azure/security/fundamentals/encryption-models#server-side-encryption-using-customer-managed-keys-in-customer-controlled-hardware

Implicaties - De gehele keten van verwerkers/leverenciers, inclusief geldende jurisdictie per verwerker/leverancier moet bekend zijn - Voor elke stap in de keten moet bepaald worden of deze verwerkt binnen de EER, of dat er aanvullende maatregelen genomen zijn - Bijzondere persoonsgegevens die bij verwerkende partijen buiten de EER zouden kunnen worden opgeslagen en waarbij ook geen adequaatheidsbesluit geldt dienen ontoegankelijk te zijn voor de betreffende verwekende partij. Dit kan doormiddel van encryptie gerealiseerd worden, waarbij de encryptiesleutels niet door de verwerkende partij zelf beheerd worden.
bronnen & referenties: - Rijkscloudbeleid - BIO - AVG

titel **CBI Basisprincipe12: “Data eigenaarschap en keuze voor locatie ligt bij de gemeente”**
omschrijving Data in cloudgebaseerde systemen is en blijft eigendom en verantwoordelijkheid van de gemeente. De gemeente kan op elk gewenst moment besluiten de data uit deze systemen te exporteren. De dataportabiliteit wordt gegarandeerd door de CSP: het formaat van geëxporteerde data volgt relevante standaarden en/of is voorzien van documentatie zodat deze bruikbaar zijn.
implicaties - Alle relevante input/output datastromen van en naar cloudgebaseerde diensten is geïnventariseerd - Er zijn concrete duidelijke afspraken met de leverancier vastgelegd over import/export mogelijkheden - Clouddiensten met ontkoppeling van data (opslag) en applicatie (logica) genieten hierbij de voorkeur, zodat afnemers de keuze hebben om data elders onder te brengen - Alle bovenstaande genoemde zaken gelden ook voor back-ups
bronnen & referenties: - Rijkscloudbeleid - GEMMA - NORA

titel **CBI Basisprincipe13: “Clouddiensten voldoen aan auditeerbaarheidsvereisten/monitoring”**
omschrijving Zoals eerder gesteld ontslaat het gebruik van clouddiensten, en dan met name SaaS, de gemeenten niet van de verantwoordelijkheid over de data. Alle in bovenliggende architecturen geschetste auditeerbaarheidseisen dienen dan ook geïmplementeerd te worden bij gebruik van clouddiensten.
Implicaties - Er is een duidelijk omschreven set aan vereisten aan auditeerbaarheid: niveau, frequentie en inhoud. - Per vereiste wordt met de (cloud)leverancier afgestemd hoe de auditeerbaarheid gewaarborgd wordt, liefst geautomatiseerd, anders in een duidelijk plan. - Idealiter alle audit- en monitoringrapportages samen in één centraal dashboard of systeem zodat er overzicht en grip ontstaat op de gehele datahuishouding.
bronnen & referenties: - Rijkscloudbeleid - BIO 12.4

titel **CBI Basisprincipe14: “Er is een back-up beleid en verantwoordelijkheden zijn duidelijk vastgelegd”**
omschrijving Conform BIO 12.3 dient een back-up beleid present te zijn, zo ook voor gegevens die via clouddiensten worden opgeslagen. Aanvullend geldt voor backups van en naar clouddiensten voldoende mate van encryptie op basis van de classificatie van de data. Daarnaast is het zo dat voor kritische systemen het advies luidt om back-ups niet alleen geografisch redundant, maar ook vendor-redundant uit te voeren.
implicaties - Een back-up beleid moet zijn vastgelegd in concrete back-up plannen en schema’s per clouddienst, als dat relevant is; - Per back-up moet een beeld zijn van de soort gegevens en classificatie die het betreft, zodat ook op de back-up infrastructuur de nodige maatregelen m.b.t. encryptie en dergelijjke genomen zijn; - Bij afname van SaaS diensten moet inzicht zijn in de door leverancier gehanteerde back-upprocedures, inclusief locatie (en invloed daarop moet mogelijk zijn conform **CBI12**).
bronnen & referenties: - BIO 12.3

titel **CBI Basisprincipe15: “Er is voorzien in een standaard voor porteerbare virtuele infrastructuur”**

omschrijving
Binnen PaaS/IaaS wordt zoveel mogelijk gestreefd naar een standaard infrastructuur zodat diensten zonder veel effort verplaatst kunnen worden. De huidige consensus op dit vlak spreekt van ‘containers’, lichtgewicht omgevingen lijkend op een *virtual machine* die een enkel proces kunnen hosten op een gedeeld operating systeem.
Binnen de gemeentewereld is hiervoor een standaard bovenop containerdeployment beschikbaar, genaamd *HAVEN*. Bij het in gebruik nemen van nieuwe PaaS/IaaS infrastructuur wordt zoveel mogelijk gepoogd deze standaard te volgen.

Implicaties
- Applicaties moeten waar mogelijk ‘containerized’ (conform HAVEN) uitgerold kunnen worden;
- Applicaties moeten gebruik maken van gestandaardiseerde protocollen zodat deze op alternatieve diensten (bijvoorbeeld storage, databases, serverless computing) kunnen worden aangesloten.

bronnen & referenties:
- Common Ground, GEMMA.

titel
CBI Basisprincipe16: “Open data worden zoveel mogelijk gedeeld”

omschrijving
Vanuit het Rijk, via de wet implementatie open data richtlijn, implementeert de Europese richtlijn voor hergebruik van overheidsdata. Als zodanig zijn gemeenten ook gebonden aan deze verplichting; data waar kan, zoveel mogelijk publiek maken.

Implicaties
- Dataclassificatie dient op orde te zijn zodat open databronnen geïdentificeerd zijn en publiek gemaakt kunnen worden
- Open databronnen dienen via geldende standaardformaten verstrekt te kunnen worden
- Infrastructuur waarop deze databronnen worden aangeboden dient voldoende schaalbaar te zijn om dataverzoeken uit het publieke domein te kunnen faciliteren.

bronnen & referenties:
- Wet implementatie Open data richtlijn[14]

titel
CBI Basisprincipe17: “Clouddiensten, inclusief de ontsluiting, moeten voldoen aan beschikbaarheidseisen”

omschrijving
Per clouddienst moet duidelijk zijn wat beschikbaarheidseisen zijn. De dienst zelf kan hierop worden gevalideerd middels een SLA. Van belang is echter ook de ontsluiting van de dienst; de aard van clouddiensten is dat zij op een andere locatie worden aangeboden, dit maakt de (netwerk)verbinding ernaartoe een essentiële schakel. Deze dient dus tevens gewaarborgd te zijn.

Implicaties
- Beschikbaarheidseisen van clouddiensten moeten worden vastgelegd middels een SLA

- Monitoring om beschikbaarheid van clouddiensten te meten en zo de SLA kunnen valideren moet zijn ingericht
- De (netwerk)verbinding naar de dienst toe moet tevens voldoen aan deze vereisten. Voorbeelden om dit te realiseren zijn:
  o Azure ExpressRoute;
  o Diginetwerk.

bronnen & referenties: GEM08, NAP17

Bijlage: NORA Architectuurprincipes

Als beschikbaar op https://noraonline.nl ten tijde van de realisatie van dit document, zijn de 17 basisprincipes van NORA (Nederlandse Overheid Referentie Architectuur:

NAP01	Verplaats je in de gebruiker
NAP02	Geef inzicht in de afhandeling van de dienst
NAP03	Lever een kanaal-onafhankelijk resultaat
NAP04	Bundel diensten
NAP05	Bied de dienst proactief aan
NAP06	Hergebruik vóór kopen vóór maken
NAP07	Bouw diensten modulair op
NAP08	Standaardiseer waar mogelijk
NAP09	Beschrijf de dienst nauwkeurig
NAP10	Neem gegevens als fundament
NAP11	Pas doelbinding toe
NAP12	Informeer bij de bron
NAP13	Beheers risico's voortdurend
NAP14	Verifieer altijd
NAP15	Maak diensten schaalbaar
NAP16	Voorkom onnodige complexiteit
NAP17	Stuur cyclisch op kwaliteit

Bijlage: GEMMA Architectuurprincipes

https://www.gemmaonline.nl/index.php/Overzicht_GEMMA_Architectuurprincipes

GEM01	Onze gemeente biedt de klant een goede informatiepositie
GEM02	Onze gemeente denkt vanuit de positie van de klant
GEM03	Onze gemeente digitaliseert haar diensten en processen
GEM04	Onze gemeente gaat op een vertrouwelijke manier met gegevens om
GEM05	Onze gemeente gebruikt generieke processen en functies
GEM06	Onze gemeente hergebruikt gegevens
GEM07	Onze gemeente stelt gegevens als open data beschikbaar
GEM08	Onze gemeente voert regie over uitbestede diensten

Bijlage: Security Posture Management

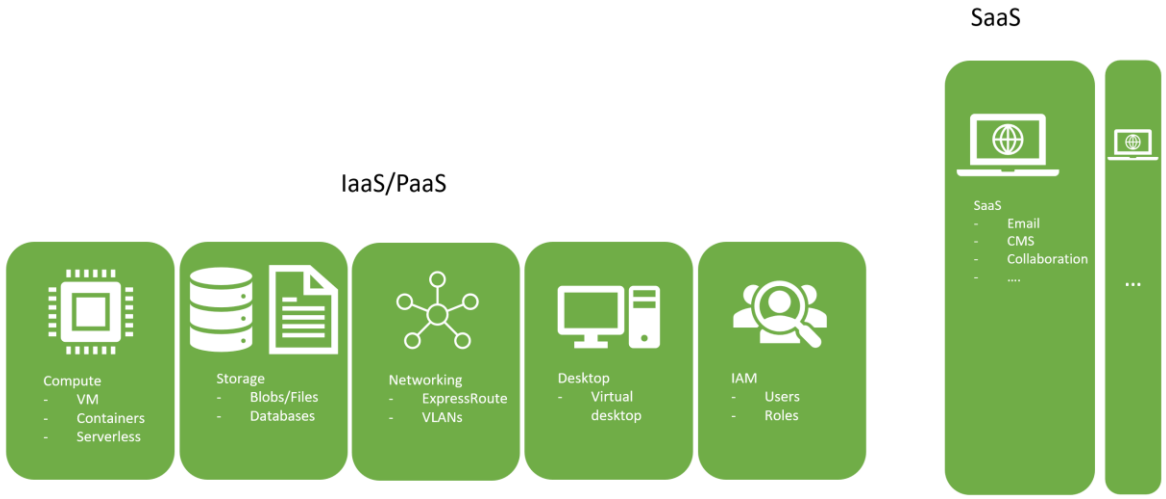
Er is nu zo'n 10 jaar ervaring in de markt met migratie naar cloud-based dienstverlening. Eenmaal in de cloud blijken de grootste beveiligingsrisico's voort te komen uit verkeerd geconfigureerde clouddiensten. Denk hierbij aan het gebrek aan encryptie, foute toewijzingen van rollen en rechten, enzovoorts. Het aanschaffen en gebruiken van cloudgebaseerde diensten is zeer laagdrempelig en dit kan met name in de beginfase van migratie naar de cloud zaken vlot en snel laten verlopen, echter de risico's worden op lange termijn naar mate grotere delen van de infrastructuur die in de cloud zijn gezet, groter en groter.

De grotere vendors van IaaS/PaaS dienstensuites (AWS, Google, Microsoft, Oracle) hebben deze ervaringen onderkend en zijn gekomen met diverse oplossingen, uiteraard cloudgebaseerd, die deze risico's in kaart brengen gecombineerd met tools om ze te mitigeren. Deze tools staan bekend onder de noemer **CSPM**, ofwel *Cloud Security Posture Management*. Deze tooling biedt de mogelijkheid om via zgn. *policies,* geautomatiseerd afdwingbare/monitorbare regels, bepaalde beleidsmatige keuzes af te dwingen en in de gaten te houden. Hoewel dit zeer waardevolle tooling is die grip biedt op IaaS/PaaS diensten en producten in de cloud, biedt het niet of nauwelijks faciliteiten voor SaaS diensten.
Hiervoor is er een groeiend aantal producten op de markt onder de noemer **SSPM**, ofwel *SaaS Security Posture Management*. De belofte van dit soort producten is dat de eerdergenoemde set beleidsregels in de vorm van policies ook toegepast kan worden op dit soort diensten. Hoewel deze producten beschikbaar zijn is het toepassingsgebied vooralsnog slechts op SaaS diensten gericht van de grotere vendors; denk aan SalesForce, Microsoft 365, Google Suite, en ServiceNow bijvoorbeeld. Domeinspecifieke kleinere SaaS producten, zoals bijvoorbeeld relevante gemeentesoftware van Pink Roccade of Centric, zijn hier nog niet zomaar in te beheren.

Hoewel de technische invulling van deze diensten dus met name voor specifieke gemeentelijke SaaS-producten nog onvoldoende beschikbaar is kunnen we wel degelijk een checklist identificeren die gebruikt kan worden als 'checklist' voor een inrichting conform standaard SSPM thema's. Deze kan vervolgens gebruikt worden om in samenspraak met de vendor een op maat te realiseren aansluiting te vinden met een reeds gebruikte, of eventueel nieuw in te richten SSPM oplossing.

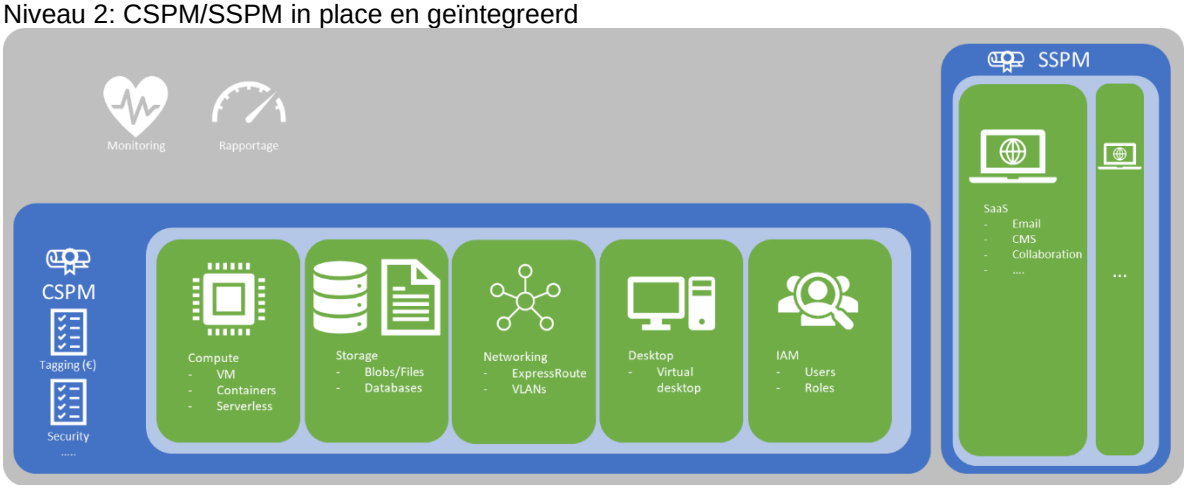
We illustreren hieronder drie niveaus van 'security posture management'. Voor wat betreft de inzet van clouddiensten voor de systemen die kernprocessen van de gemeente ondersteunen, al dan niet met (gevoelige) persoonsgegevens, is het gebruik van 'kale' niet gemanagede clouddiensten, zeer sterk af te raden. In de praktijk bieden vendors per dienst altijd wel een bepaalde mate van beheer hieromtrent, vooral in de SaaS-hoek, waardoor het soms minder urgent is omdat dit is geïntegreerd in de betreffende oplossing.

Niveau 0: Geen SPM



Niveau 1: CSPM en/of SSPM in gebruik

Niveau 2: CSPM/SSPM in place en geïntegreerd



Zodra clouddiensten gebruikt worden voor registraties of anderssoortige kernsystemen binnen de gemeente is het zeer sterk af te raden om dit zonder enige vorm van SPM in te richten.

Op het moment dat er een niveau 2 bereikt is op gebied van SPM, dus een integraal beheerde oplossing voor zowel SaaS als IaaS/PaaS diensten, is aan de basisvereisten voldaan om verdere stappen te zetten op informatievlak. Doordat de diensten en bijbehorende koppelvlakken degelijk gemanaged en gemonitord worden kan een meer Common Ground gerichte aanpak, dus met scheiding van data en applicaties, vormgegeven worden. Het advies is dan ook dat op moment dat dit in de cloud geambieerd wordt, minimaal niveau 1 maar liever niveau 2 bereikt te hebben qua SPM volwassenheid.

Omdat e.e.a. zoals aangegeven in de specifieke SaaS-markt nog erg onvolwassen is geven we hier een checklist om e.e.a. met de leverancier af te stemmen.

Checklist/PvE xSPM clouddiensten voor gemeentes

Security

Identity & access management
- Integratie met eigen IAM mogelijk
- Beheren rollen/rechten via eigen IAM

Malware bescherming

Datalekkage bescherming
- Encryptie
- Locatiegebaseerde monitoring

Externe toegang

Privacymaatregelen

Compliance op bestaande raamwerken (CIS, BIO, etc)

Monitoring

24/7 continue monitoring

Alarmen

Ticketing

Self-healing capabilities

Statusmonitoring/rapportage over de tijd

Kosten

Kostenbeheersing ongebruikte resources

Toekennen van kosten (tagging)

Bijlage: HAVEN Standaard

De HAVEN standaard omvat op moment van schrijven van dit document de volgende verplichte checks.

FUNDAMENTAL

Self test: HCC version is latest major or within 3 months upgrade window
Haven clusters must stay up to date

Self test: does HCC have cluster-admin
In order for the Haven Compliancy Checker to function properly elevated privileges are required.

INFRASTRUCTURE

Multiple availability zones in use
Running a cluster on a single availability zone means a higher risk of downtime when that single zone runs into problems.

Running at least 3 master nodes
This ensures a highly available control plane.

Running at least 3 worker nodes
This enables running highly available workloads.

Nodes have SELinux, Grsecurity, AppArmor, LKRG or Talos enabled
Security matters on every layer of a system and should an attacker break out of a deployment onto a node increased node security will help prevent further escalation.

Private networking topology
Not directly exposing masters or workers to the public internet can increase the security of the cluster.

CLUSTER

Kubernetes version is latest stable or max 2 minor versions behind
This allows cluster users to access new functionality quickly and encourages a well-implemented update mechanism.

Role Based Access Control is enabled
Basic security option which is enabled by default in order to control who can do what on a cluster.

Basic auth is disabled
Basic authentication is hard to maintain. We encourage to use OpenID Connect for user authentication.

ReadWriteMany persistent volumes support
This ensures that storage can be created which can be used by highly available deployments.

LoadBalancer service type support
This ensures that Layer 4 loadbalancers can automatically be created from the Kubernetes API.

EXTERNAL

CNCF Kubernetes Conformance
Cloud Native Computing Foundation's Kubernetes checks ensure the Kubernetes cluster adheres to the standard Kubernetes API's.

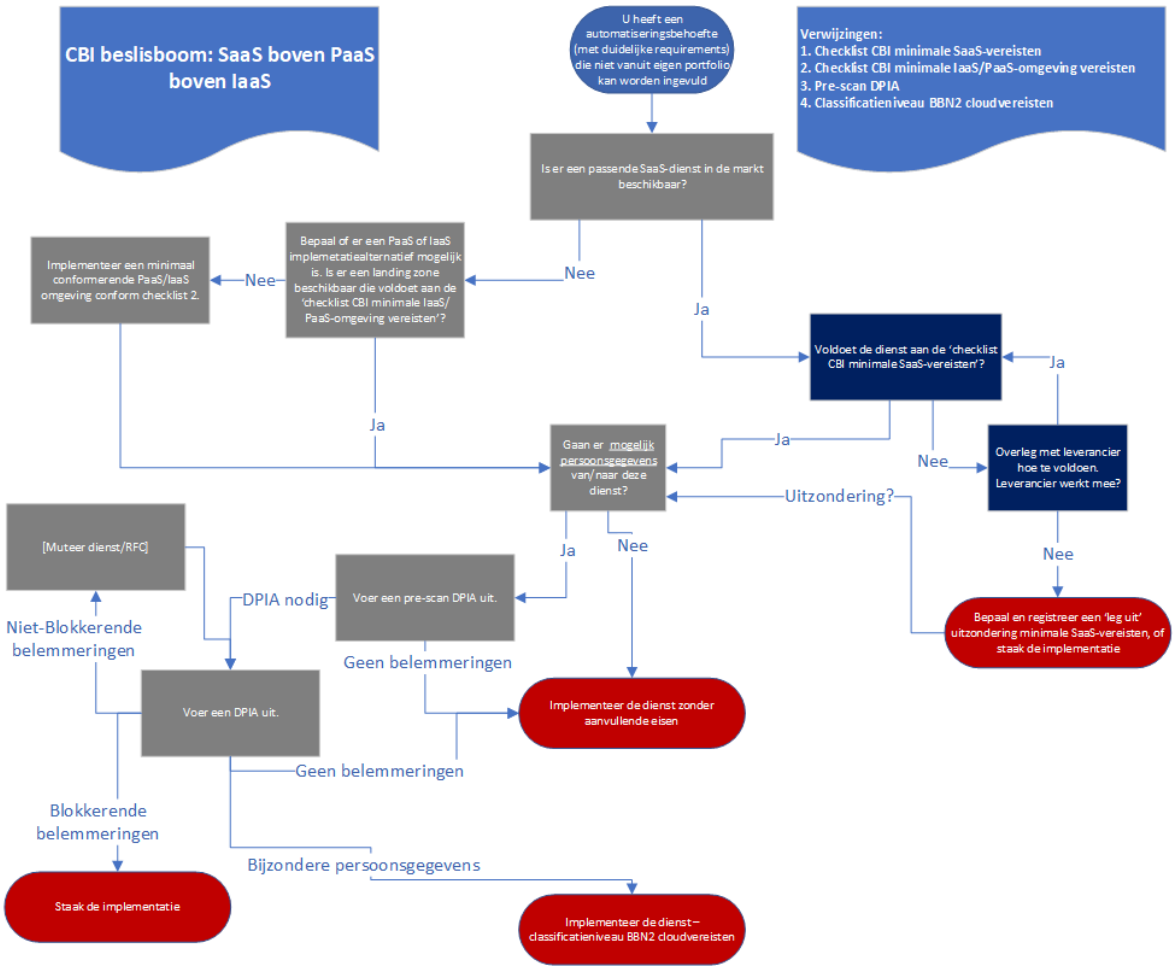
DEPLOYMENT

Automated HTTPS certificate provisioning
This makes it easy for engineers to expose an Ingress with a valid SSL certificate which automatically renews.

Log aggregation is running
In order to be in control of the workload on a cluster it's mandatory to aggregate all container logs.

Metrics-server is running
In order to be in control of a cluster it's mandatory to have eyes an ears on the cluster resources.

Bijlage: Voorbeelduitwerking strategie “SaaS boven PaaS boven IaaS”



1. Voorbeeld Checklist minimale SaaS-vereisten

	CBI07	**Security**
	CBI19	Identity & access management
		- Integratie met eigen IAM mogelijk
		- Beheren rollen/rechten via eigen IAM
	CBI07	Malware bescherming
		- Locatiegebaseerde monitoring
	CBI07	Privacymaatregelen – encryptie persoonsgegevens ‘at rest’
	CBI07	Geen passwords opgeslagen
		Azure AD integratie
		2-factor authenticatie
		Aantoonbare conformiteit op bestaande raamwerken (CIS, BIO)
		Data ‘in transit’ is altijd encrypted
	CBI18	**Monitoring**
		24/7 continue monitoring
		Alarmen
		Ticketing
		Self-healing capabilities
		Statusmonitoring/rapportage over de tijd
		Kosten
		Kostenbeheersing ongebruikte resources
		Toekennen van kosten (tagging)
		Auditeerbaarheid
		Alle relevant aangemerkte datamutaties zijn geautomatiseerd op te vragen
		Per mutatie is minimaal een tijdstempel, onderwerp, gebruiker danwel systeem, en bron ip-adres vastgelegd
		Integreerbaarheid
		Er worden voor relevante acties in het systeem API’s geboden conform OAGIS/OpenAPI 3.0 specificaties
		Data eigenaarschap

2. Voorbeeld Checklist minimale IaaS/PaaS-omgeving vereisten

	Security
	Identity & access management
	- Integratie met eigen IAM mogelijk
	- Beheren rollen/rechten via eigen IAM
	Compliance op bestaande raamwerken (CIS, BIO) via CSPM policies
	Data ‘in transit’ is altijd encrypted
	Monitoring
	24/7 continue monitoring
	Alarmen
	Ticketing
	Self-healing capabilities
	Statusmonitoring/rapportage over de tijd
	Kosten
	Kostenbeheersing ongebruikte resources
	Toekennen van kosten (tagging)
	Centrale monitoring over tijd van alle bovenstaande via CSPM dashboard

3. Pre-scan DPIA

https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/schema_dpia_na_25_mei.pdf

4. Voorbeeld Classificatieniveau BBN2 cloudvereisten

	Locatie
	Binnen EER?
	- Ja – Geen aanvullende eisen
	- Nee – Data encrypted ‘at rest’,
	Compliance op bestaande raamwerken (CIS, BIO) via CSPM policies
	Monitoring
	24/7 continue monitoring
	Alarmen
	Ticketing
	Self-healing capabilities
	Statusmonitoring/rapportage over de tijd
	Kosten
	Kostenbeheersing ongebruikte resources
	Toekennen van kosten (tagging)

Verwijzingen

[1] BIO, Baseline Informatiebeveiliging Overheid. https://bio-overheid.nl/
[2] NORA: BIO Thema Clouddiensten https://www.noraonline.nl/wiki/BIO_Thema_Clouddiensten/Standpunt_AIVD_en_beleidsverkenning_BZK
[3] Kamerbrief Rijkscloudbeleid https://open.overheid.nl/repository/ronl-a79331dc7c088f2cb6259f591c3b4f2fbcc9b5f1/1/pdf/kamerbrief-over-rijksbreed-cloudbeleid-2022.pdf
[4] Implementatiekader cloudgebruik https://www.rijksoverheid.nl/documenten/rapporten/2023/01/05/implementatiekader-risicoafweging-cloudgebruik
[5] SLM-Rijk, https://slmrijk.pleio.nl/
[6] GEMMA Globaal programma van eisen. https://www.gemmaonline.nl/images/gemmaonline/1/1b/GEMMA_Gegevenslandschap_-_Globaal_Programma_van_Eisen_v1.0.pdf
[7] GIBIT, https://vng.nl/projecten/gibit
[8] GEMMA Informatiearchitectuurprincipes https://www.gemmaonline.nl/images/gemmaonline/0/09/GEMMA_Gegevenslandschap_-_Informatiearchitectuurprincipes_v1_0.pdf
[9] Common Ground, https://commonground.nl
[10] NLX, https://nlx.io
[11] CIP, BIO thema uitwerking clouddiensten, https://cip-overheid.nl/media/1744/20211029-bio-thema-uitwerking-clouddiensten-v21-def.pdf
[12] Pre-scan DPIA: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/schema_dpia_na_25_mei.pdf
[13] OpenAPI 3 standaard https://spec.openapis.org/oas/latest.html
[14] Wet implementatie Open data richtlijn, https://wetgevingskalender.overheid.nl/Regeling/WGK009986