De Nationale ombudsman

Cloudbeleid Nationale ombudsman

Beleid en afwegingskader voor gebruik clouddienstverlening

Status: Definitief
Versie: 1.1

Wouter Sallé
23-5-2022

Inhoud

1 MANAGEMENT SAMENVATTING 3

2 DOELSTELLINGEN 4

2.1 BRONNEN 4

3 CLOUD NADER UITGELEGD 5

3.1 KARAKTERISTIEKEN EN VOORDELEN 5
3.2 IMPLEMENTATIE MODELLEN (CLOUD"TYPEN") 5
3.3 SERVICEMODELLEN 6
3.4 ROLLEN MET BETREKKING TOT CLOUDDIENSTVERLENING 6

4 AFWEGINGSKADERS VOOR DE INZET VAN CLOUDDIENSTEN 8

4.1 FINANCIERING: 8
4.2 SNELHEID VAN BESCHIKBAARHEID: 8
4.3 LEVENSDUUR: 8
4.4 INFORMATIE GEVOELIGHEID 8
4.5 SCHAALBAARHEID 8
4.6 CONNECTIVITEIT EN LOCATIE 9
4.7 INNOVATIE 9
4.8 APPLICATIE (DOOR)ONTWIKKELING 9
4.9 LEGACY 9
4.10 AANPASBAARHEID 9
4.11 LIFE CYCLE MANAGEMENT 9
4.12 VENDOR LOCK-IN 9

5 VEILIG GEBRUIK CLOUDDIENSTEN 11

5.1 WET- EN REGELGEVING 11
5.2 RISICO BEPERKENDE MAATREGELEN 11
5.2.1 DATAOPSLAG BIJ EXTERNE PARTIJ 12
5.2.2 INFORMATIE IN KETENS 12
5.2.3 AFHANKELIJKHEID 13
5.2.4 CLOUD ACT 13
5.2.5 SPIONAGE 13
5.2.6 BEVEILIGINGSBELEID EN NO KADER VOOR VEILIG GEBRUIK VAN CLOUDDIENSTEN 13
5.3 UITGANGSPUNTEN EN RICHTLIJNEN VEILIG GEBRUIK CLOUDDIENSTEN 14
5.3.1 NO KADER VOOR VEILIG GEBRUIK VAN CLOUDDIENSTEN 14
5.3.2 RISICOPROFIELEN VAN VERSCHILLENDE CLOUDMODELLEN 14
5.3.3 INTEGRALE WERKING VAN DE INFORMATIEVOORZIENING 15
5.3.4 EÉN IDENTITEIT EN ACCESS MANAGEMENT SYSTEEM 15
5.3.5 EXCLUSIVITEIT 15
5.3.6 DATAPRIVACY EN DATA-INTEGRITEIT 16

5.3.7 BEVEILIGINGSASPECTEN VAN DE OVEREENKOMST 16

6 IMPACT OP DE NO 18

6.1 BELEID NIET MET TERUGWERKENDE KRACHT. 18
6.2 VERPLAATSEN WERKZAAMHEDEN EN WERKLAST 18

Versie	Auteur	Status	Datum	Toelichting
0.1	WS	Concept	15-04-2020	Initiële versie
0.2	WS	Concept	24-04-2020	Review commentaar Martijn verwerkt, hoofdstuk 6 en 7 uitgebreid
0.9	WS	Concept	12-05-2020	Review commentaar Edwin en Dorien verwerkt, aanpassingen gedaan om doel van het document te verduidelijken
1.0	WS	Definitief	25-5-2020	Goedgekeurd door BVO
1.1	MdB	Concept	16-5-2022	Aanpassing strategie van fit-for-purpose naar Cloud-first.
1.1	MdB	Definitief	23-5-2022	Goedgekeurd door BVO

1 Management samenvatting

Het cloudbeleid van de Nationale ombudsman is opgesteld om aansluiting te vinden in de snel ontwikkelende markt van de informatie technologie. Om te zorgen dat de Nationale ombudsman (No) nu en in de toekomst gebruik kan blijven maken van moderne ICT oplossingen en technologieën is het belangrijk om afwegingskaders en eisen op te stellen die als handvatten dienen bij het nemen van besluiten of en hoe gebruik gemaakt kan worden van welke clouddiensten bij welke leverancier. De No kiest bewust voor een '*cloud first*' strategie.

In dit beleid wordt uitleg gegeven over wat de cloud inhoud, de verschillende vormen van cloud en clouddiensten die er zijn en de verschillende rollen die we identificeren bij het afnemen van een cloudoplossing.

Om een besluit te nemen of en hoe een clouddienst afgenomen gaat worden, zijn er een aantal afwegingskaders opgesteld, te weten:

- Financiering
- Snelheid van beschikbaarheid
- Levensduur
- Informatie gevoeligheid
- Schaalbaarheid
- Connectiviteit en locatie
- Innovatie
- Applicatie (door)ontwikkeling
- Legacy
- Aanpasbaarheid
- Life cycle management
- Vendor lock-in

Door bij het opstellen van een marktuitvraag de afwegingskaders te gebruiken, wordt de keuze voor niet cloud of wel cloud en ook welk type cloud bewust gemaakt. Dit voorkomt verrassingen of ongewenste situaties.

Indien gekozen wordt voor een cloudoplossing dient er nadrukkelijk nagedacht worden over het veilig gebruik van clouddiensten. Dit is onderverdeeld drie delen:

- Wet- en regelgeving
- Risico beperkende maatregelen
- Uitgangspunten en richtlijnen veilig gebruik clouddiensten

Het is van belang dat cloudoplossingen voldoen aan alle relevante wet- en regelgevingen, maar ook dat de No zich houdt aan (zelfopgelegde) richtlijnen, zie hiervoor het Informatiebeleid en de Enterprise principes.

Als laatste wordt de impact op de bestaande organisatie besproken. Hierbij gaat het niet om de impact op de gebruikers, deze wordt namelijk minimaal geacht, maar wel over de impact op de huidige werkzaamheden en de werklast bij de bedrijfsvoering. Deze gaan verschuiven en veranderen. Er zal bij gebruik van clouddiensten andere en voor de ombudsman nieuwe expertise verwacht en geëist worden.

2 Doelstellingen

Bij de Nationale ombudsman (No) is de behoefte om in meerdere disciplines (No, Kinderombudsman (Kom), Veteranen ombudsman (Vo)) datagedreven en zaakgericht te werken volgens één primair proces. Daarnaast dient ook de I-Visie zoals vastgesteld in het informatiebeleid uitgevoerd te worden. Om datagedreven en zaakgericht werken en de I-Visie te realiseren heeft de No een schaalbaar, innovatief en flexibele infrastructuur- en technologieplatform nodig. Hiervoor zijn ingrijpende wijzigingen in de huidige opzet van de ICT nodig.

De huidige ICT inrichting voor de ondersteuning van het primaire proces voldoet niet aan de toenemende behoefte aan flexibiliteit (snel ontwikkelende en veranderende ICT vragen) en continuïteit en voldoet ook niet aan de schaalbaarheid die in de toekomst nodig is. Het aanpassen van de huidige ICT oplossingen ter ondersteuning van de toekomstige digitale behoeften zoals deze hiervoor genoemd zijn is niet mogelijk. Hier zijn meerdere oorzaken voor aan te wijzen, de belangrijkste zijn:

- applicaties worden in de nabije toekomst niet meer door leveranciers ondersteund
- het maatwerk is minimaal tot niet gedocumenteerd.
- serversoftware is outdated en wordt niet meer ondersteund
- backup strategie is complex en foutgevoelig

De hiervoor genoemde punten zijn een (toekomstig) veiligheids- en continuïteits-risico. Daarnaast is het huidige datacenter van de No onderhoudsintensief en er is geen uitwijk locatie ingericht. Om goed in control te komen op de infrastructuur en de daarop draaiende (maatwerk) applicaties is het nodig om de hard- en software future ready te maken.

Publieke- en private clouddiensten zijn uniek gepositioneerd om de toekomstige strategische technologie eisen van de No te ondersteunen. Om deze redenen volgt de No een *cloud first strategy* maar wanneer Cloud geen optie is vanwege de aard van de werkzaamheden of de gevoeligheid van de data hanteerd de No een *fit for purpose* benadering. Bij elke nieuwe behoefte of vervanging van bestaande middelen ligt daarmee de voorkeur bij een Cloudoplossing, echter wordt in bovengenoemde uitzonderingsituaties een afweging gemaakt worden tussen non-cloud opties. Het merendeel van de huidige applicatie portfolio is non-cloud.

Als gevolg hiervan zal de No cloud diensten gebruiken volgens de strategie die in dit document wordt beschreven.

2.1 Bronnen

Bij het opstellen van dit cloudbeleid is gebruik gemaakt van de volgende bronnen:

- Het cloudbeleid van het ministerie van Infrastructuur en Waterstaat;
  - IWEA - Katern - IenW Cloudbeleid (1.0) – 20191105
- Gartner;
  - Designing a Cloud Strategy Document; Published 13 June 2019 - ID G00376856
- Government of Canada Right Cloud Selection Guidance;
- Centrum Informatiebeveiliging en Privacybescherming;
  - Beveiligingsbeleid clouddiensten
- EAR, Enterprise Architectuur Rijk;
  - Gesloten Rijkscloud Doelarchitectuur
- NORA, Nederlandse Overheid Referentie Architectuur
  - Cloud
- National Institute of Standards and Technology (NIST)
  - NIST Cloud Computing Standards Roadmap

3 Cloud nader uitgelegd

Er bestaan meerdere definities van een cloud. De definitie van cloud(computing) is volgens het Amerikaanse *National Institute of Standards and Technology* (NIST[1]) als volgt: "*Cloud Computing is een model om vanaf iedere locatie gemakkelijk en op afroep via een netwerk toegang te verlenen tot computermiddelen (netwerken, servers, storage, applicaties en diensten) die snel kunnen worden aan- en opgeleverd met minimale beheerinspanning of interactie van de leverancier van de dienst*".

Uitleg van de cloud is bewust in dit document opgenomen zodat bij het lezen van dit document en het gebruik van de afwegingskaders er altijd een helder beeld is over wat de cloud inhoud, welke vormen van clouddiensten en soorten implementaties er zijn. Daarnaast is het belangrijk om een beeld te hebben van de governance en de rollen die daarbij horen.

3.1 Karakteristieken en voordelen

Cloud is een generieke term voor een omgeving waarin één of meer leveranciers functionaliteit en/of diensten aanbieden in de vorm van een technologische "black box". De afnemer van een clouddienst heeft geen inzicht in wat er binnen de black box precies gebeurt en hoe deze technisch in elkaar zit. De meest essentiële karakteristieken van clouddiensten zijn:

- *On Demand Self service*: Een afnemer kan zelfstandig diensten aanvragen en geleverd krijgen zonder de tussenkomst van de service provider;
- *Brede toegang via het netwerk*: De dienst is beschikbaar via het netwerk en toegankelijk via standaard mechanismen;
- *Resource Pooling*: De computermiddelen worden vanuit een grote pool toegewezen aan meerdere afnemers;
- *Snelle elasticiteit*: De middelen kunnen snel en elastisch worden op- en afgeschaald. Voor de afnemer lijken de middelen onbeperkt;
- *Dienst op maat*: De middelen worden automatisch gecontroleerd en geoptimaliseerd, gebruik makend van een meetsysteem dat gebruik op enige wijze meet en rapporteert aan zowel de afnemer als de leverancier.

Voordelen zijn onder andere:

- De klant hoeft de voorziening (software en hardware) niet aan te schaffen, maar betaalt slechts voor het gebruik;
- De software en hardware worden niet bij de klant geïnstalleerd, maar bij de leverancier. De klant heeft toegang tot de dienst via een publiek of privaat netwerk;
- De inzet van een clouddienst is relatief laagdrempelig door het gebruik van webstandaarden.
- Kant en klare voorzieningen voor eindgebruikers (SaaS oplossing) zijn snel beschikbaar.

Nadelen en risico's zijn er ook. Zij komen uitgebreid aan de orde in Hoofdstuk 4: Afwegingskaders voor de inzet van clouddiensten en in paragraaf 5.2: Risico beperkende kaders.

3.2 Implementatie modellen (cloud"typen")

De implementatie van een dienst geeft aan hoe een dienst wordt aangeboden. De keuze van een implementatie model moet worden meegenomen bij de keuze van een cloudoplossing. We onderscheiden de volgende modellen:

- *Private cloud*: is exclusief voor één afnemer ingericht, volgens tussen de leverancier en de afnemer overeengekomen normen. Dit is een niet-commercieel beschikbaar cloudaanbod op maat van de No. Onder dit implementatiemodel is de No de enige huurder die in deze cloudoplossing verblijft. Deze cloudoplossing kan volledig worden ontworpen en beheerd in opdracht van de No of met ondersteuning van de particuliere sector.

[1] Het **National Institute of Standards and Technology** (**NIST**) is een wetenschappelijke instelling die onder de Amerikaanse federale overheid valt. Het NIST zet zich in voor standaardisatie in de wetenschap, zoals het definiëren van eenheden.

- *Community cloud*: ook wel shared cloud genoemd, is voor meerdere afnemers ingericht, waarbij de afnemers bepaalde gemeenschappelijke eisen en wensen hebben en deze gezamenlijk aan een leverancier opleggen. De Shared cloud wordt ingericht volgens de grootste gemene deler van de gemeenschappelijke eisen en wensen. De Rijkscloud is hier een voorbeeld van.
- *Public cloud*: Een verzameling van inrichtingen voor meerdere afnemers die niet noodzakelijkerwijs dezelfde eisen en wensen hebben. In een Public cloud bepaalt de leverancier in hoge mate de eisen en wensen die aan de dienst kunnen worden gesteld. Afnemers hebben slechts de keuze deze te accepteren of niet; Het is een commercieel verkrijgbaar aanbod dat is aangeschaft en op beveiliging is beoordeeld voor het gebruik van de No. Onder dit implementatiemodel deelt de No de huur met commerciële bedrijven, non-profitorganisaties en individuen.
- *Hybrid cloud*: dit is een combinatie van twee of meer van de andere modellen die weliswaar gescheiden zijn en daardoor hun eigen karakteristieken behouden, maar wel zijn gekoppeld op enigerlei wijze.
- *Non-Cloud* of *On Premise:* een omgeving voor het hosten van applicaties die niet kunnen worden ingezet in een cloudomgeving. Het grootste deel van het huidige No applicatieportfolio past in deze categorie.

Ongeacht welke clouddienst gekozen wordt, de gegevens en middelen van de No blijven altijd strikt gescheiden van de gegevens en middelen van andere afnemers.

3.3 Servicemodellen

Bij de clouddiensten worden services aangeboden. Hierbij kan onderscheid gemaakt worden tussen verschillende servicemodellen. De belangrijkste servicemodellen zijn:

- *Software as a Service (SaaS)*: hierbij wordt de complete standaardfunctionaliteit van een applicatie geleverd;
- *Platform as a Service (Paas)*: hierbij wordt functionaliteit op middlewareniveau geleverd waarmee de afnemer een applicatie kan inrichten;
- *Infrastructure as a Service (IaaS)*: hierbij worden slechts de servers, storage en netwerkverbindingen geleverd waarop de afnemer of een door de afnemer geselecteerde leverancier middleware en applicatiesoftware kan installeren.

3.4 Rollen met betrekking tot clouddienstverlening

Een belangrijke voorwaarde voor succesvol afnemen van cloud oplossingen is de governance van clouddienstverlening. Zonder volledig te zijn en uitputtend te zijn is het toch van belang om enkele belangrijke zaken uit lichten.

Governance zoals hier bedoeld gaat over wie welke rol heeft, wie waarvoor verantwoordelijk is, binnen welk verzorgingsgebied, welke mandaten er zijn, hoe processen rondom financiering, beheer en ontwikkeling georganiseerd zijn, wie adviseert wie en wie controleert wie, etc.
De NIST heeft een governancemodel ontwikkeld als onderdeel van de (door de NIST) opgestelde Referentie Architectuur voor Cloudcomputing[2]. Deze referentiearchitectuur wordt vanuit BZK gezien als de beoogde standaard voor de Nederlandse Rijksoverheid (programma RijksCloud) en binnen NORA wordt deze referentie architectuur ook aangehaald.

- *Cloud consumer*
  Een persoon of organisatie die een zakelijke relatie onderhoudt met en diensten gebruikt van een cloud provider.
- *Cloud provider*
  leverancier van cloud services aan geïnteresseerde partijen en consumenten.

[2] https://www.noraonline.nl/images/noraonline/4/4f/NIST_Cloud_Computing_reference_Architecture.pdf

- *Cloud auditor*
  Een persoon of organisatie die een onafhankelijk assessment kan doen van geleverde cloud services, operatie, prestaties en beveiliging van de cloud voorzieningen
- *Cloud broker*
  Een tussenpersoon of organisatie die de prestaties en levering van cloud services managet en de afstemming regelt tussen cloud consument en cloud provider.
- *Cloud carrier*
  Een intermediair die de connectiviteit verzorgt en de transport van cloud services van cloud provider naar cloud consument.

Het is van belang dat deze rollen belegd worden. Het moet voor de organisatie (cloud consumer) en haar gebruikers duidelijk zijn hoe ze cloud diensten kunnen afnemen. De organisatie moet weten op welke manier het gebruik van cloud diensten wordt doorbelast. Bijna alle cloud diensten kunnen geautomatiseerd worden afgenomen, zonder menselijke tussenkomst. Echter het moet duidelijk zijn, bij wie of welke organisatie men terecht kan voor customer support en hoe customer support werkt.

Als het model toegepast wordt op de generieke cloud dienstverlening voor de No, kan je het volgende voorstellen: de No als organisatie is cloud consumer en dat is de afnemers van de 3 soorten van clouddienst verlening.
Voorbeelden van diensten zijn:

- Opslag en rekenkracht (IAAS)
- Toegangsbeheer of integratiefaciliteiten (PAAS)
- Email en Office (SAAS)
- Een zaakgericht werken systeem (SAAS).

Het moet voor de No als organisatie, de cloud consumer, duidelijk zijn hoe de cloud diensten worden afgenomen. De No moet weten op welke manier het gebruik van cloud diensten wordt doorbelast.

4 Afwegingskaders voor de inzet van clouddiensten

Het besluit om voor een cloud of een non cloud oplossing te kiezen dient weloverwogen genomen te worden. Om dit te doen is er een hulpmiddel gemaakt in de vorm van een afwegingskader.
Hierin worden de voor en nadelen van de verschillende implementatiemodellen benoemd.

Het spectrum van cloud implementatiemodellen dat beschikbaar is voor de No wordt hieronder weergegeven. De Nationale ombudsman dient dit document te gebruiken als leidraad bij het selecteren van de juiste cloud oplossing.

De beslissing over welk implementatiemodel en zelfs servicemodel het beste werkt, is organisatie specifiek en wordt gebaseerd op de eisen en wensen van de No. Bij het kiezen van het implementatiemodel moet rekening worden gehouden met een aantal factoren.

4.1 Financiering:

Er wordt niet geïnvesteerd in vernieuwingsprojecten, maar in exploitatie en beheerkosten.
Wat is beter voor de organisatie: investeren in vernieuwingstrajecten of doorontwikkelingskosten en exploitatiekosten. Clouddiensten worden afgerekend naar gebruik, dit is wenselijk als het gebruik onder controle gehouden kan worden, maar als er situaties zijn waarin verbruik kan pieken moet de vraag gesteld worden of dit de kosten niet (onverwacht hoog) kan opdrijven.
Bij een al beschikbare private cloud moet meegenomen worden dat dit een initiële investering is waarvan de investering voor de vernieuwing in het verleden al gedaan is. Bij een eigen gedeelde private cloudoplossing weegt het gebruik hiervan zwaar mee in de overweging om voor een cloudoplossing te kiezen.

4.2 Snelheid van beschikbaarheid:

Neem de snelheid waarmee een oplossing beschikbaar moet zijn mee in de overweging. Oplossingen met standaard functionaliteit en standaard prijzen zijn snel beschikbaar en toegankelijk. De mogelijkheden tot aanpassing zullen beperkt zijn. Als implementatiesnelheid niet belangrijk is, kan elk implementatiemodel gekozen worden.

4.3 Levensduur:

Voor oplossingen die tijdelijk/voor een korte periode beschikbaar moeten zijn, zoals bijvoorbeeld een proof of concept is de public cloud zeer geschikt voor in het bijzonder SaaS oplossingen. Indien er een lange termijn behoefte is, volstaat elke implementatie methode.

4.4 Informatie gevoeligheid

Naast informatie categoriseren op vertrouwelijkheid, moet ook de gevoeligheid van de te verwerken gegevens in ogenschouw worden genomen. Stakeholders kunnen bezorgd zijn over het hosten van bepaalde data bij een externe partij. In dat geval biedt private cloud of non-cloud mogelijk de gewenste of zelfs vereiste zekerheid en veiligheid.

4.5 Schaalbaarheid

Werkzaamheden waarbij grote of snelle groei van data opslag, bandbreedte of rekenkracht verwacht wordt vereisen schaalbaarheid. Bij toename in het gebruik van de middelen is het belangrijk om extra capaciteit op aanvraag toe te voegen. Cloud oplossingen zijn zeer goed en snel schaalbaar, echter moet in het schalen van de resources in de cloud rekening gehouden worden met de financiële impact die dit tot gevolg heeft. Bij applicaties die in een stabiele omgeving gebruikt worden waarbij groei volgens een linear patroon gaat kan elke implementatie methode overwogen worden.

4.6 Connectiviteit en locatie

Applicaties zijn niet zelden sterk geïntegreerd met andere toepassingen om zo bedrijfsprocessen te ondersteunen. Men moet rekening houden met de impact van het verspreiden van applicaties over meerdere omgevingen. Daarnaast presteren sommige applicaties minder goed als ze ver van de gebruiker af staan. Bovendien is tegenwoordig de hoeveelheid en locatie van (bron-)data voor de goede werking van apps en applicaties relevant (data-gravity[3]). Omwille van beveiliging, performance en optimale gebruikerservaring is het in die gevallen te overwegen om applicaties dichtbij de gebruikers en/of data te plaatsen.
Het data aspect vraagt ook om afwegingen voor een exit strategie: wanneer een clouddienst beëindigd wordt moet duidelijk zijn of er gevoelige data achter kan blijven, en of er mogelijkheden zijn binnen de dienst om deze definitief en controleerbaar te bewaren, exporteren of juist vernietigen (exit-strategie).

4.7 Innovatie

Public cloud omgevingen voegen doorgaans in snel tempo nieuwe services en technologieën toe, zonder of tegen lage kosten voor de afnemer. Technologietrends evolueren met de introductie van mobile, big data, internet of things, socialemedia, artificial intelligence etc. Public cloudproviders hebben een bewezen staat van dienst bij het snel introduceren van deze technologieën. Als een project met een proof of concept (PoC) wil profiteren van deze nieuwe technologietrends, heeft een public cloud de voorkeur. Anders kan elk implementatiemodel worden gekozen.

4.8 Applicatie (door)ontwikkeling

Ontwikkelen van software vereist een breed scala aan tools en testmogelijkheden (DevOps en Continuous Integration / Continuous Delivery). Public cloud providers bieden een uitgebreide set aan tools die voortdurend evolueren om te voldoen aan de huidige best practices.

4.9 Legacy

De meeste bestaande applicaties zijn niet ontworpen om te functioneren in een cloud omgeving. Om deze reden zijn oudere applicaties vaak niet geschikt voor cloud, totdat ze opnieuw worden ontwikkeld of worden vervangen door modernere oplossingen. Dit is bij uitstek het moment om de inzet van cloudoplossingen te overwegen.

4.10 Aanpasbaarheid

Het public cloud aanbod is vaak gebaseerd op standaardoplossingen (bijvoorbeeld SaaS applicaties). De mate van vrijheid om die oplossingen aan te passen op wensen en eisen is niet altijd toereikend. Daarnaast kan er afwijkende dienstverlening vereist zijn die niet vanuit de public cloud geleverd wordt.

4.11 Life Cycle Management

Aanbieders van clouddiensten hanteren veelal een strak en hoogfrequent update en upgrade schema voor hun diensten. Afnemers hiervan zijn genoodzaakt deze systematiek en dit ritme te volgen, hetgeen kan leiden tot knelpunten ten aanzien van de (doorgaans) gehanteerde test- en acceptatiemethodieken. Dit vraagt om aanpassing hiervan.

4.12 Vendor lock-in

De risico's rond vendor lock-in zijn niet noodzakelijkerwijs een onderscheid tussen het kiezen van publieke, private of niet-cloud implementatiemodellen. De No dient in alle gevallen maatregelen te nemen om zich te wapenen tegen de volgende scenario's:

[3] Letterlijk de “zwaarte” van data, die zowel in omvang als in aantallen bronnen tot stand komt. Meer informatie en voorbeelden op https://www.cloudtp.com/doppler/data-gravity-straddling-on-premises-and-cloud-service-providers/ (in het Engels)

- Een leverancier houdt op te bestaan vanwege een faillissement of vanwege een andere reden. Hierdoor wordt de ondersteuning abrupt beëindigd en zullen er eventueel juridische maatregelen genomen moeten worden
- Een leverancier wordt overgenomen en de nieuwe eigenaar kan niet aan de BIO voldoen
- De doorontwikkeling van een product of dienst van een leverancier gebeurt in een richting die niet past bij het (strategisch) belang van de No.
- Een leverancier (of dienstverlener) voert een prijsverhoging door die onacceptabel hoog is.

Bij een nieuwe aanbesteding voor een dienst of product kiest de No voor het product of dienst met de hoogste toegevoegde waarde. De kosten van het overstappen van de ene leverancier naar de andere zijn vaak aanzienlijk, omdat niet alleen nieuwe producten en diensten worden afgenomen, maar ook personeel moet worden bijgeschoold. Mitigatiestrategieën om de risico's die samenhangen met vendor lock in zijn onder meer:

- Neem producten en diensten af van verschillende leveranciers
- Koop producten en diensten van volwassen leveranciers met een groot aantal klanten en een geschiedenis van dienstverlening aan die klanten
- Gebruik open standaarden die door meerdere leveranciers worden ondersteund

Cloudomgevingen kunnen extra risico's lopen omdat de applicaties en gegevens worden gehost binnen de faciliteiten van een andere partij. Om deze reden moeten aanvullende mitigatiestrategieën worden gebruikt, zoals:

- Host disaster recovery en/of back-up oplossingen bij een andere leverancier
- Houd data en applicaties gescheiden.
- Zorg ervoor dat er een exit strategie is bedacht die is afgestemd op de eisen die gesteld worden om de continuïteit van de organisatie te waarborgen.

5 Veilig gebruik clouddiensten

5.1 Wet- en regelgeving

Er bestaat nog geen cloudbeleid voor de Rijksoverheid, dit is nog in ontwikkeling. Er is wel een document *'Nota Verkenning Cloudbeleid Rijksdienst'*[4] van de CIO Rijk en een reactie van het NCSC op dit document, te weten: *'Reactie NCSC Cloudverkenning CIO Rijk'*[5]. In dit hoofdstuk zijn de redeneerlijn en het voorgestelde afwegingskader uit het voorgaande hoofdstuk (*3 Afwegingskaders voor de inzet van clouddiensten*) al wel meegenomen. De huidige wettelijke verplichtingen voor de opslag en verwerking van informatie bepalen ook de kaders voor verwerking en opslag in de (public) cloud.

Het grootste gedeelte van deze wet- en regelgeving die betrekking heeft op het Nationale ombudsman is ook van toepassing op de cloud. De No is verplicht om de wettelijke kaders te volgen. Daarnaast heeft de No besloten om voor de inrichting van informatievoorziening de voorschriften voor de rijksdienst te volgen waar mogelijk. Binnen deze kaders zijn dan met name de volgende punten van belang:

- Met betrekking tot de besturing en het aantoonbaar in control zijn is de "Baseline Informatiebeveiliging Overheid" (BIO) het wettelijk vastgestelde kader voor de Rijksdienst. De Nationale ombudsman heeft zich ook gecommitteerd aan deze baseline
- Met betrekking tot informatiebeveiliging volgen we de Rijksdienst[6]:
  - Beveiligingsvoorschrift Rijksdienst (BVR) 2013,
  - Voorschrift informatiebeveiliging Rijkdienst (VIR) 2007 en
  - Voorschrift informatiebeveiliging Rijksdienst Bijzondere informatie (VIR-BI) 2013 (toegelicht in de “Handleiding Rubricering” van de Rijksoverheid);
- Met betrekking tot de bescherming van persoonsgegevens (privacy) zijn de Algemene verordening gegevensbescherming (AVG) en de bijbehorende Uitvoeringswet AVG het belangrijkste wettelijke kader.
- Via de Instructie Rijksdienst[7] zijn een aantal zaken verplicht gesteld voor de overheid. De No heeft in het informatiebeleid vastgelegd dat de No het rijk volgt waar mogelijk en daarmee ook deze instructie. Onder de verplichte zaken worden verstaan:
  - Digikoppeling 2.0 voor veilige berichtwisseling;
  - Het Forum Standaardisatie publiceert verplichte technische normen voor websites, netwerken en applicatieconstructie: DKIM, DNSSEC, SAML, SPF, STARTTLS en DANE, WPA2 Enterprise;
  - Informatiebeveiligingsrichtlijnen: NEN-ISO/IEC 27001/2. Deze normen liggen ook ten grondslag aan de BIO.

Daarnaast zijn bij de No de enterprise principes en het informatiebeleid leidend.

5.2 Risico beperkende maatregelen

Om veiligheidsrisico’s te voorkomen is het uitgangspunt dat informatiesystemen en daarmee ook clouddiensten moeten voldoen aan de voorwaarden van het algemene geldende beleid. Deze voorwaarden zijn in grote lijnen beschreven in de strategische i-agenda voor de Rijksdienst 2019-2021. Dienstverleners moeten voldoen aan alle wetten en regels, voor zover relevant voor hun dienstverlening, zoals de AVG en BIO/VIRBI. Voorwaarden zijn altijd vastgelegd in contracten die geverifieerd kunnen worden.

Zoals beschreven in No Enterprise principes paragraaf 2.3.1: “Beveiliging op basis van risico afweging” wordt de geschiktheid van een clouddienst voor gegevensverwerking en opslag getoetst met een risico

[4] 2019_0916 Nota Verkenning Cloudbeleid voor de Rijksdienst; zie bijlage
[5] Reactie NCSC Cloudverkenning CIO Rijk 20191018; zie bijlage
[6] Zie ook Enterprise principes hoofdstuk 2.3.1
[7] https://wetten.overheid.nl/BWBR0024717/2008-11-23

analyse. Afhankelijk van de risicocategorieën waarin de gegevens vallen, kan het gebruik van een clouddienst al of niet acceptabel zijn.
Bij het wegen van de risico's is het van belang onderscheid te maken in de mate van vertrouwelijkheid van de verschillende typen gegevens in de organisatie. Voor dit doel wordt de vertrouwelijkheidclassificatie van de BIO gehanteerd voor bedrijfs- en persoonsgegevens.

Er zijn drie Basis BeveiligingsNiveaus:

- BBN1
- BBN2
- BBN3

Bij BBN1 gaat het om wat er minimaal verwacht mag worden van de overheid voor de bescherming van informatie. We hebben hier te maken met een laag betrouwbaarheidsniveau en daarom blijven complexe eisen hier achterwege. Het gaat puur om een minimale basis.

Bij BBN2 komen we op het niveau waar de meeste informatie van de overheid in valt. Het gaat hier om goed huisvaderschap voor informatie. BBN2 is het standaardniveau. BBN2 is het minimale niveau waarop met persoonsgegevens gewerkt wordt. BBN2 ligt qua zwaarte op hetzelfde niveau als de oude baselines. Bij BBN2 ligt voor statelijke actoren en vergelijkbare dreigers de nadruk op 'detectie'.

BBN3 is een set van maatregelen gebaseerd op relevante NAVO-regelgeving en specifiek ontwikkeld voor processen waarbinnen weerstand tegen statelijke of criminele actoren (of gelijksoortige dreigers) gewenst is of waar informatie wordt verwerkt die door de bronhouder een bepaalde classificatie heeft mee gekregen.

Het vaststellen van de systeem classificatie gebeurt d.m.v. een baselinetoets. Op basis van een aantal vragen wordt duidelijk welke BBN van toepassing is.

De inzet van clouddiensten kent een aantal specifieke en ook aanvullende risico´s die in een risico analyse om een afweging vragen, deze worden hieronder toegelicht.

5.2.1 Dataopslag bij externe partij

Dienstverlening waarbij overheidsdata wordt opgeslagen in een datacenter van de leverancier. Aan het besluit om een externe partij in te zetten of om een dienst aan te besteden gaat – in het kader van privacy en informatiebeveiliging - altijd een risico analyse en een Privacy Impact Assessments[8] (PIA's) en Data Protection Impact Assessments[9] (DPIA's) vooraf. Daarin wordt de rubricering van de data bepaald en vastgesteld dat de rubricering aantoonbaar wordt toegepast. De afweging zal afhankelijk zijn van de gevoeligheid van de data. .

5.2.2 Informatie in ketens

Met de mogelijk bredere toepassing van voorzieningen voor de Rijksoverheid om sneller te reageren op veranderende wet- en regelgeving of wensen van burgers, bedrijven en ambtenaren, wordt opgemerkt dat het kader voor 'rubriceringen' (VIR, VIRBI) thans geldingskracht heeft voor de Rijksdienst. VIR en VIRBI houden geen rekening met data uitwisseling tussen overheidslagen, er wordt alleen naar de rijksdienst gekeken. Het is daarom op dit moment (nog) onduidelijk hoe om dient te worden gegaan met het delen van informatie (zinvol en met doelbinding) tussen verschillende overheidslagen, en de eisen die daarvoor gesteld zullen moeten worden.

[8] Model voor PIA https://www.rijksoverheid.nl/onderwerpen/privacy-en-persoonsgegevens/documenten/rapporten/2017/09/29/model-gegevensbeschermingseffectbeoordeling-rijksdienst-pia
[9] Informatie over DPIA https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia

5.2.3 Afhankelijkheid

Verder spelen in de context van veilig en verantwoord cloudgebruik criteria als continuïteit van de dienstverlening (exit-strategie), het risico van afhankelijkheid van één leverancier (vendor lock-in) of beschikbaarheid van beperkte cruciale expertise een rol. Dit zal, zeker voor bedrijfskritische applicaties, een essentieel onderdeel van de risico analyse moeten zijn.

5.2.4 CLOUD Act

Naast wet- en regelgeving en beleid waar bij de No aan moet worden voldaan, dient ook rekening gehouden te worden met wetgeving die invloed heeft op de gegevens in de cloud. Met name de Cloud Act7 (CLOUD = Clarifying Lawful Overseas Use of Data) in de VS kan consequenties hebben voor de vertrouwelijkheid van de gegevens die in de cloud zijn opgeslagen. Deze en andere externe kaders dienen dan ook een belangrijke rol te spelen in de keuze of het sowieso kan om zaken in de cloud op te nemen en vervolgens welke maatregelen om dit te mitigeren, dan genomen moeten worden.

5.2.5 Spionage

Spionage (al dan niet in combinatie met Big Data) wordt in dit kader als een risico gezien. Het is thans onduidelijk welke consequenties de Cloud Act en vergelijkbare wetgevingsvoorbereiding in EU verdragen hebben op verplichtingen van informatie deling met buitenlandse partijen zonder dat deze informatieverstrekking juridisch is getoetst en is gemeld aan betrokkenen.

5.2.6 Beveiligingsbeleid en No kader voor veilig gebruik van clouddiensten

In deze paragraaf is in het kader van risicomanagement de No beleidslijn uitgewerkt rond het toepassen van ‘Basis Beveiligings Niveau’ (BBN) 1, 2 en 3 voor de Public en Rijks Cloud langs de lijnen van de BIO. Het onderscheid in drie BBN’s voorkomt dat voor eenvoudige systemen zonder vertrouwelijke informatie teveel administratieve last wordt opgeroepen.

De beleidslijn in combinatie met de daarvoor genoemde handelswijze ten aanzien van risico’s en restricties, brengt ons tot het volgende kader voor veilig gebruik van clouddiensten, weergegeven in matrixvorm. Ter vergelijking en voor de volledigheid is ook de Non-Cloud oftewel On Premise optie hierin opgenomen.
Voor alle toegestane (incl. mits) varianten geldt dat:

1. Er een samenhangende risicoanalyse is uitgevoerd door de juiste stakeholders en formeel is geaccordeerd, en restrisico’s zijn geaccepteerd door de daarvoor verantwoordelijke functionaris;
2. De gegevens aantoonbaar conform het vigerende beleid t.a.v. informatiebeveiliging van de Rijksoverheid (BIO of opvolger) worden beschermd.
3. Persoonsgegevens aantoonbaar beschermd worden conform de AVG.

Risico analyse	On Premise	Rijks Cloud	Private Cloud bij leverancier	Public Cloud
BBN1	Toegestaan	Toegestaan	Toegestaan	Toegestaan
BBN2	Toegestaan	Toegestaan	Toegestaan mits (1,2)	Toegestaan mits (1,2)
BBN3	Toegestaan	**Nog geen kader, nvt**	Niet toegestaan	Niet toegestaan

Hieronder zijn de voorwaarden (mits) bij BBN2

(1) In de risicoanalyse:
   a) is beoordeeld dat gebruik gemaakt kan worden van de specifieke clouddienst en
   b) is bepaald welke passende maatregelen daarbij worden genomen en welke contractuele eisen gesteld worden, welke ook gemonitord worden.

(2) Er zijn passende voorzieningen beschikbaar om activiteiten van Advanced Persistent Threats[10] (APT’s) zoals statelijke actoren te kunnen signaleren en daarop in te grijpen. Dit betreft een set aan detectievoorzieningen en maatregelen, waarvan expertdiensten (AIVD, MIVD of NCSC)

[10] https://en.wikipedia.org/wiki/Advanced_persistent_threat

hebben aangegeven dat deze zinvol zijn ten opzichte van het risico dat het departement met de voorziening of proces loopt[11].

5.3 Uitgangspunten en richtlijnen veilig gebruik clouddiensten

De volgende uitgangspunten en richtlijnen zijn bedoeld als handvatten bij de besluitvorming voor het afnemen van een nieuw of vervangend product of dienst voor de informatievoorziening. Bij het uitvragen van een leverancier dienen deze uitgangspunten meegenomen worden zodat de dienstverlening geborgd wordt. Afhankelijk van het soort dienst waar gebruik van gemaakt wordt dienen onderstaande uitgangspunten te worden meegenomen. Bij diensten waar geen informatie of geen gevoelige informatie verwerkt wordt, kunnen minder uitgangspunten toegepast worden.

5.3.1 No kader voor veilig gebruik van clouddiensten

Alle (gecontracteerde) clouddiensten en daarmee samenhangende processen moeten voldoen aan de beveiligingsnorm zoals die is gedefinieerd voor de 'traditionele' IT-voorzieningen, waarvan de organisatie gebruik maakt. De richtlijnen in dit document zijn aanvullende, cloudspecifieke richtlijnen.

Richtlijn (RL)	Omschrijving
	Minimale beveiligingseisen
RL 1	De leverancier toont aan dat hij en zijn dienst ten minste voldoen aan de standaarden ISO27001/2017 en ISO27002/2017 samen met de richtlijnen voor Informatiebeveiliging bij de No
RL 2	De uiteindelijke keuze wordt gebaseerd op een businesscase waarvan een beveiligingsrisicoanalyse onderdeel uitmaakt.
RL 3	De resultaten van de beveiligingsrisicoanalyse zijn verwerkt in het contract (bijvoorbeeld in de vorm van een toegevoegde beveiligingsovereenkomst) en afgeleiden zoals de SLA e.d.

5.3.2 Risicoprofielen van verschillende cloudmodellen

Public cloud

De opzet van de *Public cloud* kent een relatief groot '*attack surface*'– dit is het gedeelte van een dienst dat wordt blootgesteld aan aanvallen door kwaadwillenden. Dit is inherent aan het publieke karakter van deze dienst. Omdat bovendien in een Public cloud de leverancier in hoge mate de eisen en wensen bepaalt die aan de dienst worden gesteld, is de Public cloud *ongeschikt* voor verwerking van gegevens in de klasse BBN 3.

Community cloud

De inzetbaarheid van een *Community cloud* wordt bepaald door het beveiligingsniveau zoals dat door de *community* is gedefinieerd. Afhankelijk van dit beveiligingsniveau is een Community cloud *mogelijk inzetbaar* voor alle gegevensklassen.

Private cloud

Binnen een *Private cloud* stelt de organisatie zelf de eisen aan het beveiligingsniveau, deze is *inzetbaar* voor alle gegevensklassen.

On Premise

Bij *On Premise* wordt gebruik gemaakt van een eigen datacenter. Hiervoor geldt dan ook dat de organisatie zelf de eisen stelt aan het beveiligingsniveau, deze is *inzetbaar* voor alle gegevensklassen. Onderhoud en de beveiliging op het gewenste niveau houden eist wel inzet en (up to date) kennis.

Richtlijn	Omschrijving
	Keuze voor cloudmodel
RL 4	Bij de keuze van het cloudmodel is de classificatie van de gegevens en processen bepalend.
RL 5	De onderbouwing en de keuze van het cloudmodel zijn vastgelegd en meegegeven in het

[11] Bron: BIO voorschrift voor BBN2

	proces voor de inzet van de (cloud)dienst.

5.3.3 Integrale werking van de informatievoorziening

Het is van belang dat de integrale werking - inclusief de veranderbaarheid - en de continuïteit van de bedrijfsinformatievoorziening gegarandeerd zijn. Een oplossing buiten de Private cloud vergroot de complexiteit en daarmee de kans dat de integrale werking van de informatievoorziening nadelig wordt beïnvloed. Om de integrale werking te verzekeren worden de volgende richtlijnen gehanteerd:

Richtlijn	Omschrijving
	De integrale werking en continuïteit worden gewaarborgd
RL 6	Clouddiensten voldoen aan de open overheids- en web standaarden zoals voorgeschreven door het Forum standaardisatie.
RL 7	Communicatie tussen de Private cloud en Public clouds vindt uitsluitend plaats via webservices of API's. Deze koppelingen zijn beveiligd volgens de digikoppeling standaarden
RL 8	Alleen clouds met vergelijkbaar beveiligingsniveau mogen gekoppeld worden.
RL 9	Oplossingen buiten de Private cloud vereisen géén aanpassingen binnen de Private Cloud, werkplekvoorzieningen daarbij inbegrepen.
RL 10	Een leverancier levert zijn diensten als één integraal werkende dienst (geaggregeerde dienst), waardoor geen additionele integratielast bij de organisatie ontstaat.
RL 11	De leverancier moet, ten behoeve van migratie naar een andere oplossing of mogelijke verwerking door een ander systeem, altijd een gegevensdump kunnen leveren van alle in zijn systeem aanwezige organisatiegegevens.

5.3.4 Eén Identiteit en Access Management systeem

Een centrale Identiteit en Access Management (IDM) omgeving borgt dat acties onweerlegbaar terug te leiden zijn naar natuurlijke personen en dat controles op toegang en functiescheiding mogelijk zijn. Clouddiensten, die buiten de Private cloud worden aangeboden, moeten gebruik maken van de centrale IDM-omgeving. Dit is mogelijk door middel van (bijvoorbeeld) een veilig gebruik van de protocollen SAML 2.0 en OAUTH. Clouddiensten binnen de private cloud mogen in plaats daarvan ook gebruik maken van een LDAP extensie op de Active Directory

Richtlijn	Omschrijving
	Clouddiensten in één integraal IDM-systeem
RL 12	Voor de gebruiker en het beheer van de digitale identiteit en de toegangsrechten is het niet merkbaar dat een oplossing binnen of buiten de No wordt aangeboden.
RL 13	Bij SaaS-diensten wijkt de digitale identiteit (de user-id) niet af van die binnen de Private cloud of de werkplekomgeving. Het beheer van toegangsrechten, inclusief de bewaking van functie-scheiding, geschiedt vanuit één (logisch) IDM-systeem. Implementatie bij voorkeur in een Single Sign On systeem met behulp van - bijvoorbeeld - SAML.
RL 14	Alle toegangsrechten worden beheerd vanuit één IDM-systeem.

5.3.5 Exclusiviteit

Als de No eist dat een specifieke dienst of infrastructuur exclusief door en voor de No ingezet wordt, dan impliceert dat op voorhand uitsluiting van diensten of infrastructuren in de public cloud of community cloud.

Richtlijn	Omschrijving
	Voor de inzet van cloud diensten geldt de exclusiviteitclausule

RL 15	Een leverancier levert de dienst(en) binnen het exclusiviteitprincipe

RL 16	De leverancier toont aan dat:
	• de gegevens van de No zijn logisch en functioneel gescheiden van de overige afnemers. Een logische en functionele scheiding wordt gegarandeerd;
	• het afgesproken beveiligingsniveau van de dienst en de No is gegarandeerd;
	• er geen afhankelijkheid bestaat van andere afnemers in geval van:
	  ○ onderhoud- en releasewerkzaamheden;
	  ○ technische uitwijk;
	• de performance niet lijdt onder de piekbelastingen door andere afnemers van de infrastructuur;
	• de schaalbaarheid en flexibiliteit niet worden beperkt.
	Voorts mag geen sprake zijn van ontvlechtingproblematiek bij afloop van het contract en wordt volledig inzicht gegeven in wijze waarop de infrastructuur wordt gedeeld. Dit inzicht wordt op verzoek geleverd d.m.v. een Third Party Mededeling[12] (TPM).

RL 17	De dienst dient enkel en alleen benaderbaar te zijn vanaf de No infrastructuur.[13]

5.3.6 Dataprivacy en data-integriteit

De Nationale ombudsman verwerkt privacygevoelige gegevens van burgers. Dit schept de verplichting om de vertrouwelijkheid en de integriteit van de gegevens te garanderen. Een passend beveiligingsniveau is daarbij essentieel.
De in potentie - en in de praktijk vaak daadwerkelijk aanwezige - internationale dimensie van opslag, beheer en verwerking van gegevens in de cloud vereist extra aandacht.

Richtlijn	Omschrijving
	De diensten kennen een passend beveiligingsniveau bij grensoverschrijdende gegevensverwerking
RL 18	De afnemer van de clouddienst blijft eigenaar van alle informatie die hij binnen de cloud verwerkt en/of opslaat.
RL 19	De leverancier waarborgt dat opslag van gegevens en bedrijfsprocessen en bedrijfsregels plaatsvindt in landen die geacht worden een passend beveiligingsniveau te hebben[14].
RL 20	Beheer op en monitoring van systemen waarbinnen privacygevoelige informatie wordt opgeslagen of verwerkt - is alleen toegestaan vanuit landen die geacht worden een passend beveiligingsniveau te hebben.

5.3.7 Beveiligingsaspecten van de overeenkomst

Het primaire doel van informatiebeveiliging is het beschermen van de Beschikbaarheid, Integriteit en Vertrouwelijkheid van de gegevens van de Nationale ombudsman.

Richtlijn	Omschrijving
	De leverancier heeft aantoonbaar informatiebeveiliging ingericht cf. de organisatiestandaarden
RL 21	De dienstverlening vindt plaats onder de werking van een beveiligingsovereenkomst die is ondertekend met de leverancier. Daarin is vastgelegd dat de omgang met gegevens door de leverancier plaatsvindt binnen de vereisten die No daaraan stelt[15].

[12] Third Party Mededeling (TPM) ook wel Derdenverklaring is een audit-verklaring van een onafhankelijke auditor.
[13] VPN verbindingen naar de No zijn onderdeel van de No infrastructuur.
[14] Nadere toelichting: https://ec.europa.eu/info/law/law-topic/data-protection_nl

RL 22	De leverancier beschikt over een gecertificeerd (ISO27001 of vergelijkbaar) Informatie Beveiliging Management Systeem (ISMS), gerelateerd aan de te leveren diensten.
RL 23	De leverancier levert controleerbaar bewijs, in de vorm van een formele audit-verklaring, van de opzet, bestaan en werking van een passend stelsel van beveiligingsmaatregelen ten aanzien van het geheel van de te leveren dienst(en).
RL 24	De No heeft het recht de door de leverancier geleverde dienst en bijbehorende processen te auditen, deze audit door een derde partij te laten uitvoeren en de statutaire rechten van de auditors te benoemen.
RL 25	De leverancier monitort actief alle beveiligingsmaatregelen, correleert de status en de signalen (logging en events) afkomstig van deze beveiligingsmaatregelen.
RL 26	Activiteiten worden gelogd en gemonitord. Vooraf gedefinieerde activiteiten van gebruikers en alle activiteiten van beheerders, alle uitzonderingen en alle informatiebeveiligingsgebeurtenissen worden vastgelegd in logbestanden.
RL 27	De logbestanden, voor zover ze betrekking hebben op dienstverlening aan de No, worden gedurende een overeengekomen periode bewaard en op verzoek aan de No verstrekt.
	Er is een Service Level Agreement (SLA)
RL 28	Het beoogde serviceniveau en onaanvaardbare serviceniveaus zijn in de SLA beschreven.
RL 29	De leverancier meet en bewaakt de vooraf gedefinieerde en verifieerbare (K)PI's van de dienst en rapporteert hierover aan de No.
RL 30	De wijze waarop de noodzakelijke IT beheerprocessen[16] aan de kant van de No zijn gekoppeld aan de leverancier, zijn beschreven.
	Verplichtingen zijn vastgelegd
RL 31	De verplichting dat de leverancier na beëindiging van de overeenkomst alle vertrouwelijke gegevens van de No correct uit haar systemen verwijdert, is contractueel vastgelegd.
RL 32	Iedere wijziging op een dienst wordt door de leverancier beoordeeld op impact op de informatiebeveiliging en compliancy met BIO en andere relevante regels en wetgeving.
RL 33	Iedere wijziging (change) in/op de dienst met een hoge impact of geconstateerde afwijking op de beveiligingsbaseline en/of het beleid van de No, wordt door de leverancier aan de No ter beoordeling voorgelegd en waar mogelijk voorzien van een alternatief voorstel en/of een overzicht van mitigerende maatregelen, inclusief een indicatie van de tijdelijkheid van afwijking (gedoogsituatie).
RL 34	De respectievelijke aansprakelijkheden van de partijen die bij de overeenkomst zijn betrokken, zijn contractueel vastgelegd.
RL 35	De leverancier en bijgeval diens personeel ondertekenen een geheimhoudingsverklaring, als onderdeel van het contract.
RL 36	In het geval van een (dreigend) beveiligingsincident onderneemt de leverancier alle acties die noodzakelijk zijn om het risico voor de No tot een minimum te beperken en meldt deze onmiddellijk aan de No conform een vooraf afgesproken procedure.
RL 37	Ten aanzien van voorspelbare beveiligingsincidenten (o.a. malware-uitbraken, denial-of-service attacks, phishing attacks) beschikt de leverancier over periodiek geteste standaardscenario's, die in geval van een incident per direct in werking treden.

[15] Zie paragraaf 5.1 Wet- en regelgeving

[16] Dit betreft in ieder geval incident management

6 Impact op de No

De No zal de komende jaren veranderen van een organisatie die niet of nauwelijks gebruik maakt van clouddiensten naar een organisatie cloud en noncloud diensten naadloos in elkaar overgaan. Het is begrijpelijk dat bij deze transitie ook rollen in de organisatie gaan veranderen. In dit hoofdstuk wordt de impact hiervan nader beschreven

6.1 Beleid niet met terugwerkende kracht.

Het doel van het cloudbeleid is om keuzes voor de toekomst te borgen. Het is niet de bedoeling om dit cloudbeleid tegen in het verleden gemaakte keuzes aan te houden. Het cloudbeleid kan wel gebruikt worden om te controleren of de gevraagde dienstverlening van huidige cloudleveranciers voldoet aan de minimale eisen die gesteld moeten worden. Het advies is om waar nodig met de leveranciers aan tafel te gaan zitten om de dienstverlening op orde te brengen.

6.2 Verplaatsen werkzaamheden en werklast

Het verplaatsen van diensten of producten naar de cloud heeft tot gevolg dat een deel van de werkzaamheden die nu door eigen medewerkers wordt uitgevoerd gaat verplaatsten naar een leverancier. Hierdoor zullen er minder van de huidige werkzaamheden overblijven bij de huidige IT afdeling. De nieuwe diensten leveren wel nieuwe werkzaamheden op bij IT en andere afdelingen. Er zal daarnaast ook een verschuiving zijn naar andere en nieuwe kennisgebieden.

Bij de No zullen de operationele werkzaamheden verminderen en sommigen volledig verdwijnen. Daar staat tegenover dat er wel meer expertise opgebouwd dient te worden op tactisch gebied. Denk hierbij aan rollen als integratie specialist, data specialist, solution architect, leveranciersmanager (cloudbroker achtige rol) etc.

Dit betekent dat bij het veranderen van het IT landschap en het afnemen van nieuwe diensten constant de vraag gesteld moet worden of de huidige expertise bij de No de nieuwe dienstverlening kan beheersen en beheren. Indien dit niet het geval is, dient de afweging gemaakt te worden of die expertise ingehuurd/gekocht gaat worden of dat het eigen personeel door opleiding en trainingen naar het juiste kennis niveau gebracht kunnen (en willen) worden.