Clouddiensten van de Rijksoverheid en de rol van de IT-auditor

Een verkenning naar auditmogelijkheden van clouddiensten bij de Rijksoverheid, uitgevoerd door de AIVD, de Auditdienst Rijk, en het NCSC.

Versie 1.0 definitief - 4 december 2013

NB: Deze versie heeft nog niet de definitieve layout en vormgeving, maar hij heeft wel de definitieve inhoud. Er is geen bezwaar tegen bredere verspreiding binnen de (Rijks-) overheid.

Inhoudsopgave

1 Inleiding

De verkenning wil een beknopt antwoord te geven op drie cloudvragen die voor IT-auditors, maar ook voor gebruikersorganisaties en beheerorganisaties van de Rijksoverheid relevant zijn. Deze zijn:

- Welke gegevens mag ik in welk type clouddienst opslaan en verwerken?
- Welke afspraken moet ik met de cloudleverancier maken?
- Welke aandachtspunten zijn belangrijk bij een audit op de de cloudleverancier?

De rode draden in deze verkenning zijn:

- De cloudstrategie van de Rijksoverheid is leidend. Deze stelt dat gebruik moet worden gemaakt van de gesloten Rijkscloud.
- Binnen deze cloudstrategie is nog onderscheid te maken in meer en minder gevoelige informatie. Meer gevoelige informatie vraagt om zwaardere beveiligingsmaatregelen, afspraken en audits.

De verkenning is als volgt opgebouwd:

- Eerst wordt een korte beschrijving gegeven van clouddiensten en de bijbehorende trends en vraagstukken.
- Vervolgens wordt een antwoord gegeven op de drie bovengenoemde vragen over gegevens, afspraken en toezicht.
- Relevante achtergrondinformatie wordt in de bijlagen samengevat.

Er is bewust voor gekozen om deze verkenning kort te houden en in voetnoten zoveel mogelijk naar bestaande documenten te verwijzen. In het publieke domein zijn vele uitstekende publicaties beschikbaar. Hiermee kan de lezer zich een goed onderbouwd beeld vormen van de cloud problematiek.

De situatie rondom clouddiensten is sterk in beweging. Hype en echte trends zijn niet altijd te onderscheiden. Daarom is deze verkenning als discussiestuk bedoeld en niet als definitief antwoord. Reacties, discussies en nieuwe ontwikkelingen worden in volgende versies van deze verkenning verwerkt.

2 Korte introductie cloudcomputing

In dit hoofdstuk wordt een korte introductie van cloudcomputing gegeven. Ook wordt ingegaan op overeenkomsten en verschillen met klassieke vormen van uitbesteding.

2.1 Definities

Het fenomeen cloudcomputing is nog volop in ontwikkeling maar volgens toonaangevende waarnemers is al enige mate van volwassenheid bereikt. [1] Van cloudcomputing circuleren vele definities waarvan drie eenvoudige en informatieve voorbeelden als volgt luiden:

- Cloudcomputing is een on-demand service model voor de levering van IT-diensten, veelal gebaseerd op virtualisatietechnieken en gedistribueerde computeromgevingen. [2]
- Cloudcomputing is de opslag, verwerking en het gebruik van data op het internet waarbij de informatie toegankelijk is vanaf alle denkbare typen clientapparatuur (desktops, laptops, tablets en smartphones).
- Cloudcomputing is het online op afroep leveren van computerverwerkingskracht, opslag, IT-infrastructuur, software en diensten. De daarachter liggende schaalgrootte verlaagt doorgaans de kosten en de eindgebruiker kan de diensten vanaf elke vorm van randapparatuur (met een internetbrowser) benaderen.[3] [4]

De meest bekende en geadopteerde definitie is die van het National Institute of Standards and Technology (NIST) die in het onderstaande plaatje wordt samengevat. [5] [6] De 5 essentiële kenmerken van Cloud computing uit de definitie van NIST zijn:

- Gebruik via selfservice - Een afnemer kan zelfstandig een IT dienst aanvragen.
- Grote netwerkcapaciteit - Toegang is geregeld via een breedband verbinding.
- Deling van opslag en rekencapaciteit - De beschikbare middelen worden gedeeld met anderen.
- Snelle schaalbaarheid - De IT diensten kunnen snel en flexibel worden toegewezen en afgebouwd.
- Meten van gebruik - Het gebruik van de IT diensten worden automatisch gemonitord en bestuurd.

Een deel van deze kenmerken gelden ook voor de klassieke uitbesteding van IT-diensten. Het grootste verschil met uitbesteding zijn de zelfbedieningsmogelijkheden en de snelle schaalbaarheid. De gebruiker kan bijvoorbeeld zelf besluiten om extra servers en opslagcapaciteit in te zetten. Bij klassieke uitbesteding is de flexibiliteit vaak kleiner.

---

[1] Hype Cycle for Emerging Technologies, 2012 (31 juli 2012, Gartner), http://www.gartner.com/DisplayDocument?doc_cd=233931

[2] DNB Circulaire Cloudcomputing (6 december 2011, kenmerk 2011/643815), http://www.toezicht.dnb.nl/binaries/Cloud%20computing_tcm50-224828.pdf

[3] ICCIO - Subcommissie Generieke Informatievoorziening

[4] Sommige sceptici beweren zelfs dat er geen goede definitie van cloudcomputing bestaat, omdat er niet echt iets nieuws is om te definiëren. Volgens deze sceptici is cloudcomputing een moderne vorm van uitbesteding, omgeven met verkoop propaganda. - Cloud computing: nietszeggend begrip, 22 april 2011, Mike Chung, http://www.automatiseringgids.nl/achtergrond/2011/16/cloud-computing-nietszeggend-begrip

[5] NIST Special Publication 800-145 The NIST Definition of Cloudcomputing (September 2011), http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[6] Gesloten Rijkscloud, Functionele Doelarchitectuur, Concept versie 0.9, 13 mei 2013, (aangeboden aan ICCIO op 27 juni 2013)

2.2 Servicemodellen

De drie servicemodellen uit de definitie van NIST zijn: [5] [6]

- Software as a Service (Saas) - Een afnemer gebruikt een applicatie van derden, die ergens in de cloud draait. Feitelijk heeft een afnemer geen controle over de applicatie en infrastructuur.
- Platform as a Service (PaaS) - Een afnemer draait een eigen applicatie ergens in de cloud op een Cloud infrastructuur. Een afnemer heeft alleen controle over de applicatie, niet over de infrastructuur.
- Infastructure as a Service (IaaS) - Een afnemer betrekt IT infrastructuur (netwerk, servers, storage) uit de cloud en draait daar eigen applicaties op. Een afnemer heeft controle over applicatie en (gedeeltelijk) ook de infrastructuur.

2.3 Implementatiemodellen

De vier implementatiemodellen uit de definitie van NIST zijn: [5] [6]

- Public Cloud - Dit is de meest pure vorm van cloud computing. De IT clouddiensten zijn beschikbaar voor alle afnemers. De cloud resources en diensten zijn eigendom van de cloud leverancier. De cloud leverancier kan op zijn beurt ook weer clouddiensten afnemen om er bijvoorbeeld voor te zorgen dat continuïteit gewaarborgd blijft. Zo zijn er bijvoorbeeld aanbieders van data opslag clouddiensten die zelf de opslag capaciteit elders inkopen. Zo is het voor een afnemer vaak onduidelijk waar nu werkelijk een dienst wordt afgenomen of waar bijvoorbeeld gegevens staan. Daartegenover staat dat een dergelijke dienst vaak relatief goedkoop is.
- Private Cloud - De cloud capaciteit is exclusief beschikbaar voor één afnemer en wordt niet gedeeld met andere afnemers. Als de afnemer de capaciteit niet gebruikt wordt die capaciteit dan ook niet toebedeeld aan andere afnemers. Men noemt dit single tenancy. Vaak wordt hiervoor gekozen vanuit privacy of security motieven. Hiermee is de afnemer in grote mate “in control” van de eigen gegevens.
- Community Cloud - Deze vorm van cloud is nagenoeg hetzelfde als een private cloud. Alleen is er niet één afnemer. De cloud capaciteit wordt gedeeld door verschillende organisaties uit een specifieke gemeenschap (bijvoorbeeld een consortium van organisaties die gemeenschappelijke belangen hebben, gelijksoortige eisen stellen aan beveiliging van hun gegevens en die elkaar in redelijke mate vertrouwen).
- Hybrid Cloud - Een hybride model, dat ontstaat wanneer twee of meer van bovenstaande cloud modellen (private, community, public) worden gekoppeld.

De meest gebruikte, bekende en wijdverspreide public clouddiensten zijn bijvoorbeeld Facebook, Gmail, Twitter en Dropbox. Deze diensten zijn voornamelijk voor persoonlijk gebruik door consumenten bedoeld en worden vaak gratis aangeboden. De infrastructuur is volledig onder beheer van de leverancier en wordt met vele andere gebruikers gedeeld. De leverancier bepaalt hoe de dienst geleverd wordt en de gebruiker moet akkoord gaan met de dienstverleningsovereenkomst van de leverancier. De dienstverleningsovereenkomst is er vooral op gericht om de gegevens van de gebruiker te kunnen analyseren en te verkopen.

De public cloud is het meest kosteneffectief maar geeft de minste zekerheid over de vertrouwelijkheid van de opgeslagen gegevens. De private en community cloud geven de meeste

zekerheid over de beveiliging maar zullen duurder zijn omdat er minder schaalvoordelen te halen zijn.

Bij de private en community cloud kan nog het volgende onderscheid worden gemaakt:

- Cloud in eigen beheer – Hierbij voert de organisatie of het consortium zelf het beheer over de cloud infrastructuur en de hierin opgeslagen gegevens. De private cloud draait bijvoorbeeld in een eigen rekencentrum met eigen beheer.
- Cloud uitbesteed – Hierbij heeft de organisatie of het consortium het beheer over de cloud infrastructuur en gegevens uitbesteed aan een bekende en vertrouwde leverancier, waarbij de cloud leverancier het beheer doet.

Bij uitbesteding van private en community clouddiensten is schaalgrootte aan de klantzijde belangrijk voor de mate waarin de klant eisen kan stellen aan de cloudleverancier. Bij grootschalige gezamenlijke inkoop kan de inkoopcombinatie door de sterkere onderhandelingspositie stringentere eisen stellen.

2.4 Voordelen en nadelen

Voor een gebruiker van cloudcomputing zijn de definities minder belangrijk. Een gebruiker gaat het vooral om de geboden functionaliteit, die makkelijk via het internet toegankelijk is en die vaak zowel privé als zakelijk kan worden ingezet. De gebruiker is vooral geïnteresseerd in de voordelen van cloudcomputing zoals de “self service”, de grotere flexibiliteit, lagere kosten, hogere beschikbaarheid en minder intern beheer. De onderliggende techniek is voor de gebruiker, over het algemeen, minder interessant. De nadelen van cloudcomputing zoals afhankelijkheid van netwerkkoppelingen, “vendor lock-in”, locatie van de data en juridische aspecten kunnen hierbij ten onrechte op de achtergrond raken. [7] [8] [9]

De nadelen en risico’s van cloudcomputing zijn op hoofdlijnen vergelijkbaar met de nadelen en risico’s van uitbesteding, namelijk verlies van controle over de eigen ICT-processen en infrastructuur. Dit wordt veroorzaakt door het “op afstand” zetten van gegevens, systemen en applicaties bij de dienstverlener. De nadelen worden groter bij het afnemen van een clouddienst, waar de leverancier nog verder weg staat van de gebruiker. Hierdoor worden de eigen ICT-processen nog afhankelijker van de prestaties van de leverancier, van zijn infrastructuur en van de tussenliggende netwerkverbindingen.

Daarbij kan tegelijk minder gesteund worden op persoonlijk toezicht en informeel vertrouwen en moeten meer zaken formeel en contractueel worden geregeld. De belangrijkste nadelen en risico’s zijn: afhankelijkheid van de dienstverlener, afhankelijkheid van algemene voorwaarden en dienstverleningsovereenkomsten, het ontbreken van een “right to audit”, onduidelijkheid over afhandeling van incidenten en beperkte informatie over beheer en beveiliging. Daarnaast is het relatief makkelijk om gegevens en verwerkingsprocessen naar de cloud uit te besteden, maar veel lastiger om de gegevens weer uit de cloud terug te halen, bijvoorbeeld door niet-standaard gegevensformaten bij de cloudleverancier. Vooral bij uitbesteding van applicaties naar een

[7] Eindrapportage CLOUDCOMPUTING, FUNDAMENT OP ORDE (versie 1.1, 2012), http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2012/03/15/cloud-computing-fundament-op-orde.html
[8] NIST Special Publication 800-144 Guidelines on Security and Privacy in Public Cloudcomputing, December 2011, http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf
[9] NIST Special Publication 800-146 Cloudcomputing Synopsis and Recommendations, Mei 2012, http://csrc.nist.gov/publications/nistpubs/800-146/sp800-146.pdf

cloudleverancier (SaaS) kan een exit-strategie lastig zijn. [10] [11] Al deze risico's leggen een zwaardere verantwoordelijkheid bij de organisatie die de cloud dienst afneemt, want deze is en blijft eindverantwoordelijk voor de gegevens.

Een nieuw soort risico wordt veroorzaakt door de "persoonlijke" clouddiensten die vooral op consumenten zijn gericht, zoals Dropbox, GMail en Google Docs. Deze zijn ook vanuit overheidsorganisaties bereikbaar en vergroten het risico op verlies en uitlekken van vertrouwelijke gegevens zodra overheidsmedewerkers ze gebruiken voor uitwisseling van documenten. Dit geldt uiteraard ook voor "persoonlijke" clouddiensten zoals LinkedIn en Twitter waarin overheidsmedewerkers hun persoonlijke profiel kunnen opslaan en informatie met sociale netwerken kunnen delen.

Ondanks de risico's verwachten toonaangevende waarnemers dat de markt van cloudcomputing sterk zal blijven groeien en dat organisaties steeds meer en steeds gevoeliger gegevens bij cloudleveranciers zullen opslaan en verwerken, omdat de voordelen en significant lagere kosten het winnen van de nadelen. [12]

Voor een meer uitgebreide analyse van cloudcomputing verwijzen wij naar het whitepaper van het Nationaal Cyber Security Centrum (NCSC). [13]

[10] Cloud security, Checklist en de te stellen vragen, Surfnet, Guido van der Harst, SURFibo, December 2010, http://www.surfnet.nl/Documents/rapport_201012_Cloud_Security_checlist_v1.0.pdf
[11] Cloud computing, Wikipedia, paragraaf 11: Issues, http://en.wikipedia.org/wiki/Cloud_computing
[12] Gartner persbericht 1 december 2011, http://www.gartner.com/it/page.jsp?id=1862714
[13] Whitepaper NCSC Cloudcomputing & security, Januari 2012, NCSC, https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/whitepaper-cloudcomputing.html

3 De cloudstrategie van de Rijksoverheid

De cloudstrategie van de Rijksoverheid schrijft voor dat overheidsgegevens altijd worden opgeslagen in de gesloten Rijkscloud. Dit wordt in dit hoofdstuk nader toegelicht en afgebeeld op de verschillende implementatiemodellen van clouddiensten.

3.1 Gesloten Rijkscloud

De Rijksoverheid heeft er voor gekozen om een gesloten Rijkscloud (GRC) in eigen beheer in te richten als een voorziening die generieke diensten levert binnen de Rijksdienst. Deze voorziening wordt ingericht binnen een eigen beveiligd netwerk en beheerd door een eigen, rijksbrede organisatie. Er is dus gekozen voor een community/private clouddienst in eigen beheer. Binnen de gesloten Rijkscloud kunnen diensten zoals dataopslag, servercapaciteit, infrastructuurcapaciteit en diensten zoals E-mail, werkplekomgeving, samenwerkingsfunctionaliteit en aansluiting op applicaties worden afgenomen. [14] [15]

Strikte eisen hierbij zijn dat de gegevens in Nederland blijven, de veiligheid voor alle afnemers adequaat is en op een voor de gekozen toepassingen acceptabel niveau kan worden geregeld. Daar waar dat opportuun is, wordt bij het realiseren van een gesloten Rijkscloud gebruik gemaakt van diensten van marktpartijen. De regie op de inrichting en het beheer zal echter binnen de Rijksoverheid blijven. [16]

3.2 Gesloten Rijkscloud als maatregel van I-Strategie Rijk

De inrichting van de gesloten Rijkscloud is een maatregel van de Informatiseringstrategie (I-strategie) Rijk en wordt als volgt gedefinieerd: [17] [18]

- De gesloten Rijkscloud is een schaalbare, generieke basisvoorziening voor de Rijksdienst waarmee rijksmedewerkers plaats-, tijd- en apparaatonafhankelijk de voor hun werk noodzakelijke applicaties op veilige wijze, kunnen gebruiken.

[14] Tweede Kamer der Staten-Generaal, Vergaderjaar 2010–2011, 26 643 Informatie- en communicatietechnologie (ICT), Nr. 179, Brief Van De Minister Van Binnenlandse Zaken En Koninkrijksrelaties, Den Haag, 20 april 2011, https://zoek.officielebekendmakingen.nl/behandelddossier/21109/kst-26643-179.html

[15] Brief van de minister van Binnenlandse Zaken en Koninkrijksrelaties, Mevrouw mr. drs. J.W.E. Spies, Betreft Het rapport over Cloudcomputing van Capgemini Nederland 2012Z04165/2012D11844, 27 april 2012, http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2012/05/01/kamerbrief-over-rapport-cloudcomputing.html

[16] Tweede Kamer der Staten-Generaal, Vergaderjaar 2010–2011, 26 643 Informatie- en communicatietechnologie (ICT), Nr. 183, Verslag Van Een Schriftelijk Overleg, juni 2011

[17] Brief van de minister van Binnenlandse Zaken en Koninkrijksrelaties, J.P.H. Donner, Betreft I-strategie Rijk, 15 november 2011, http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/kamerstukken/2011/11/15/kamerbrief-informatiseringstrategie-rijk/kamerbrief-informatiseringstrategie-rijk.pdf

[18] Implementatieplan I-strategie Rijk 2012-2015, Concept Versie 1.1, 28 maart 2012

3.3 Maatregelen I-Strategie die de gesloten Rijkscloud ondersteunen

De inrichting van de gesloten Rijkscloud hangt sterk samen met andere maatregelen uit de I-Strategie. Om de gesloten Rijkscloud optimaal te benutten zijn een aantal samenhangende functionaliteiten en componenten noodzakelijk: [17] [18]

- Ondersteuning apparaatonafhankelijk werken, Bring Your Own Device (BYOD) - Om Het Nieuwe Werken te ondersteunen zal het Rijk de ICT infrastructuur aanpassen zodat informatie en systemen worden gescheiden van de apparatuur (bijvoorbeeld: tablets en smartphones) waarmee toegang wordt verkregen. Hierdoor kunnen medewerkers hun eigen apparatuur gebruiken voor apps uit de Rijks-Application Store (RAS) en diensten uit de gesloten Rijkscloud.
- Inrichting Rijks-Application Store - De Rijks-Application Store zorgt ervoor dat diensten (services, apps) in de gesloten Rijkscloud beschikbaar komen voor hergebruik bij de andere overheden, dan wel in de publieke cloud. De RAS maakt het mogelijk om softwarefunctionaliteit uitsluitend te installeren en te gebruiken wanneer die functionaliteit echt nodig is.
- Invoering Identiteits- en Toegangsmanagement Rijk (IAM) - Het Rijk streeft naar een situatie waarbij de rijksmedewerker zich éénmalig op een unieke wijze registreert waardoor het mogelijk wordt dat de rijksmedewerker vanuit die ene registratie toegang wordt verleend tot alle informatiebronnen waarvoor deze is geautoriseerd.
- Rijksinternetkoppeling - Het Rijk wil het aantal internetkoppelingen terugdringen tot maximaal 5. Verplichte afname en afstoting van niet-generieke voorzieningen moet zorgen voor kostenbesparing en verhoging van het beveiligingsniveau (door standaardisatie en betere monitoring).

De hosting van de gesloten Rijkscloud wordt gefaciliteerd door de volgende maatregel uit de I-Strategie:

- Consolidatie Datacenters Rijk (CDC) - Het Rijk streeft er naar om het aantal datacenters in de Rijksdienst terug te brengen van ruim 60 naar 4 of 5 en hierbij een kostenbesparing en kwaliteitsverbetering te realiseren op het gebied van continuïteitvoorziening en verlaagde kans op gegevensverlies. De datacentervoorziening Rijk vormt de basis voor de gesloten Rijkscloud en ook de RAS.

Volgens de planning van de I-Strategie Rijk wordt de gesloten Rijkscloud samen met de meeste ondersteunende functionaliteiten en componenten in 2015 opgeleverd.

3.4 Beveiligingsniveau gesloten Rijkscloud

De gesloten Rijkscloud en alle ondersteunende functionaliteiten en componenten worden ingericht volgens het Baseline Informatiebeveiliging Rijksdienst (BIR) [19] beveiligingsniveau niveau. [18] Dit is vergelijkbaar met het Departementaal Vertrouwelijk (Dep.V) niveau van het Voorschrift Informatie-beveiliging Rijksdienst - Bijzondere Informatie (VIR-BI) [20] zolang de volgende dreigingen niet spelen:

- Terreurgroep,
- Inlichtingendienst,
- Georganiseerde criminaliteit.

[19] Baseline Informatiebeveiliging Rijksdienst, Tactisch Normenkader (TNK), Versie 1.0, Definitief, 1 december 2012
[20] Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere informatie 2012, 1 september 2012, http://wetten.overheid.nl/BWBR0016435/ - NB: Deze versie van het VIR-BI moet nog formeel worden goedgekeurd.

Met deze uitgangspunten is de gesloten Rijkscloud – mits vooraf een inschatting van dreigingsniveaus en een risicoanalyse is gemaakt - geschikt voor het grootste deel van de overheidsgegevens, namelijk de niet-gevoelige en laaggevoelige gegevens. De gesloten Rijkscloud is niet geschikt voor hooggevoelige gegevens die tegen terreurgroepen, (statelijke) inlichtingendiensten en georganiseerde criminaliteit beschermd moeten worden.

3.5 Beveiligingsniveau van overheidsdiensten vergelijkbaar met gesloten Rijkscloud

Bij de inrichting van de geconsolideerde datacenters Rijk wordt minimaal gestreefd naar het bereiken van een Staatsgeheim Confidentieel (STG.C) beveiligingsniveau voor de "housing" van de datacenters. [21] Het niveau voor "hosting" van de diensten wordt waarschijnlijk Dep.V. [22]

Organisaties die al lang met de dreiging van georganiseerde criminaliteit, inlichtingendiensten of terreurgroepen, te maken hebben - zoals de Inlichtingen en Opsporingsdiensten (Fiscale Inlichtingen en Opsporingsdienst, Inspectie SZW (voorheen Sociale Inlichtingen- en Opsporingsdienst), Politie en Defensie – bezitten op dit moment meestal eigen – extra beveiligde - rekencentra en maken geen gebruik van clouddiensten. In het algemeen rubriceren deze organisaties hun informatie als Stg.C. Voor deze organisaties is het BIR en Dep. V beveiligingsniveau van de gesloten Rijkscloud te laag.

Organisaties die behoefte hebben aan opslag en verwerking van informatie die als Stg.C en Staatsgeheim Geheim (Stg.G) is gerubriceerd kunnen gebruik maken van de gemeenschappelijke rekencentrumdienst – Digitale Werkomgeving Rijk Geheim (DWR-G). Deze dienst kan volgens het eigen projectplan [23] in 2014 beschikbaar zijn:

- De DWR-G dienst zal bestaan uit de gehele keten van een DWR-compliant secure werkplek, secure netwerk en een secure backend (servers/storage) en een datacenter, waarbij de hele keten geschikt is voor opslag, transport en beheer van hoog gerubriceerde informatie. De dienst zal geleverd gaan worden door V&J/GDI.
- Hiermee kunnen werkplekomgevingen worden aangeboden waar informatie wordt verwerkt die gerubriceerd is als Stg.C of Stg.Geheim. De werkplekdienst DWR-G ondersteunt ook het verwerken van hoog gerubriceerde informatie van de internationale partners NATO en EU conform de voor die omgevingen geldende regelgeving.

[21] Aanbiedingsformulier 4 SIB Tactisch normenkader housing STG CONFI, 22-08-2012, Ministerie BZK, Edgar Heijmans

[22] Datacenter housing omvat de fysieke toegang en beveiliging, datacenternetwerkbekabeling en -beveiliging, het onderhoud van technische installaties voor stroomvoorziening en klimaatbeheersing, alsook facilitaire beheeraspecten in en rondom het datacenter. Datacenter hosting omvat het technisch beheer van hardware voor servers, storage en datacenternetwerken en basissoftware als virtualisatiesoftware en beheertools. Het beheer van besturingssystemen, databases en middleware, valt hierbuiten. - Interdepartementale Commissie van CIO's - Samenvatting Business Case Consolidatie Datacenters - KPMG IT Advisory, Den Haag, 8 juli 2010

[23] Projectplan DWR-G, aangepast n.a.v. governance en financiering, Concept versie 1.3, 29 mei 2013

3.6 Beveiligingsafwegingen bij het afnemen van clouddiensten

Bij uitbesteding van gegevens moet altijd een risicoafweging worden gemaakt. Een proces-, systeem- of gegevenseigenaar blijft altijd verantwoordelijk bij het uitbesteden van processen, systemen en informatie en moet altijd kunnen aantonen dat hij "in control" is. Daarom heeft de Rijksoverheid in 2011 een overkoepelende risicoafweging gemaakt en een strategie geformuleerd voor uitbesteding van overheidsgegevens naar de cloud. Deze blijft onverminderd geldig:

- Zodra er sprake is van (gevoelige) overheidsgegevens dan mag geen gebruik worden gemaakt van een publieke cloud.
- De argumenten tegen het gebruik van publieke cloud wegen op dit moment zwaarder dan de voordelen, vanwege de onvolwassenheid van de markt en de eisen die vanuit de Rijksoverheid worden gesteld aan informatiebeveiliging. [14] [15] Publieke cloudleveranciers komen (over het algemeen) nog niet tegemoet aan de specifieke eisen en wensen van de overheid. Privacybescherming is bijvoorbeeld nog geen integraal onderdeel van de wijze waarop publieke clouddiensten en -toepassingen nu worden vormgegeven. [24]

De argumenten tegen het gebruik van publieke cloud zijn in de afgelopen maanden versterkt door de toegenomen aandacht voor de mogelijkheden van statelijke actoren om zich toegang tot clouddiensten te verschaffen. De verwachting is dat ontwikkelingen rond PRISM en de Patriot Act de ontwikkeling van nationale en Europese clouddiensten zullen stimuleren. [25] [26] [27] Hierbij moet zeker niet vergeten worden dat de VS niet de enige statelijke actor die zich toegang tot clouddiensten zou kunnen verschaffen. [28]

Maar ook al wordt gebruik gemaakt van een private of een community cloud moet toch rekening worden gehouden met de gevoeligheid van de gegevens, de geldende dreiging voor de gegevens en het daarbij behorende beveiligingsniveau. Dit wordt in de onderstaande tabel samengevat.

[24] Cloud computing voor de Nederlandse overheid, Eindrapport Werkpakket 3; KPMG IT Advisory, oktober 2010

[25] How Much Will PRISM Cost the U.S. Cloud Computing Industry?, Daniel Castro, The Information Technology & Innovation Foundation, August 2013

[26] How we're boosting trust in the cloud, post PRISM, July 3rd, 2013, Weblog of Neelie Kroes, Vice-President of the European Commission

[27] Cloud diensten in hoger onderwijs en onderzoek en de USA Patriot Act, Dr. J.V.J. van Hoboken, Mr. A.M. Arnbak & prof. Dr. N.A.N.M. van Eijk, m.m.v. mr. N.P.H. Kruijsen, Instituut voor Informatierecht
Universiteit van Amsterdam, september 2012

[28] A Sober Look at National Security Access to Data in the Cloud, Analyzing the Extravagant Claims About U.S. Access That Ignore Access by Foreign Jurisdictions, Winston Maxwell, Christopher Wolf, May 22, 2013

Gevoeligheid gegevens	Dreiging	Consequenties cloudstrategie van de Rijksoverheid
Alle soorten overheids-gegevens	Alle dreigings-niveaus	**Persoonlijke clouddiensten <u>niet</u> gebruiken** **Publieke commerciële clouddiensten <u>niet</u> gebruiken** • Consumenten clouddiensten zoals Google Docs, Gmail en Dropbox zijn niet ontworpen voor zakelijk gebruik. Bij het gebruik van dergelijke diensten is de gegevenseigenaar niet "in control". Dit levert risico's op voor de vertrouwelijkheid van gegevens en het imago van de Rijksoverheid. [29] [30]
Gegevens tot en met WBP risicoklasse 2 of rubricering Dep.V	**Geen** dreiging aanwezig van georganiseerde criminaliteit, inlichtingen-diensten of terreurgroepen	**Community cloud (GRC) of private clouddiensten van de overheid gebruiken** • Gegevens opslaan en verwerken in Gesloten Rijkscloud (in ontwikkeling). • Gegevens opslaan en verwerken in een (of meer) van de geconsolideerde datacenters (deels in bedrijf, deels in ontwikkeling).
Gegevens tot en met WBP risicoklasse 2 of rubricering Dep.V	**Wel** dreiging aanwezig van georganiseerde criminaliteit, inlichtingen-diensten of terreurgroepen	**Gespecialiseerde community cloud (DWR-G) of gespecialiseerde private clouddiensten van de overheid gebruiken** • DWR-G dienst (in ontwikkeling) – dit heeft veruit de voorkeur omdat hier een centrale en geconsolideerde dienst wordt aangeboden. Dit past het beste bij de geformuleerde cloudstrategie. • Bestaande datacenters van organisaties die te maken hebben met georganiseerde criminaliteit, inlichtingendiensten en terrorisme – zoals de politie, opsporingsdiensten en inlichtingendiensten (in bedrijf).
Gegevens met WBP risicoklasse 3 of rubricering Stg.C en hoger	Alle dreigings-niveaus	

3.7 Richtlijnen voor gevoeligheid van gegevens

Concrete richtlijnen voor het bepalen van de gevoeligheid van gegevens zijn te vinden in de volgende documenten:

- De Kwetsbaarheids-analyse spionage gaat uitgebreid in op de vele soorten gevoelige gegevens die binnen de overheid en het bedrijfsleven aanwezig zijn en geeft aanwijzingen hoe deze gegevens geïnventariseerd en beveiligd kunnen worden. [31]
- De Baseline Informatiebeveiliging Rijksdienst (BIR) [19] beschrijft in hoofdstuk 2 (Uitgangspunten en werkingsgebied) de dreigingen waarmee rekening gehouden moet worden en geeft in

[29] Een uitzondering is denkbaar voor de dataklasse die "Open Data" wordt genoemd. Maar hoewel hier geen risico voor de exclusiviteit bestaat zijn nog steeds garanties nodig voor integriteit en beschikbaarheid. Hierdoor zullen commerciële clouddiensten de voorkeur hebben boven persoonlijke clouddiensten.

[30] Het is belangrijk dat de GRC infrastructuur snel beschikbaar komt omdat anders de aanzuigende werking van persoonlijke en commerciële clouddiensten te groot wordt en de overheid met voldongen feiten wordt geconfronteerd. Dit risico is extra groot bij de combinatie van tablets en clouddiensten zoals iCloud, GoogleDrive, GoogleDocs, EverNote en DropBox.

[31] Kwetsbaarheids-analyse spionage, Spionagerisico's en de nationale veiligheid, Algemene Inlichtingen- en Veiligheidsdienst, Februari 2010

hoofdstuk 4 (Risicobeoordeling en risicobehandeling) aanwijzingen voor het uitvoeren van een risicoanalyse.

- Het Voorschrift Informatiebeveiliging Rijksdienst - Bijzondere Informatie (VIR-BI) [20] beschrijft in artikel 4 (Rubriceringen) de relevante rubriceringsniveaus en de wijze waarop informatie gerubriceerd moet worden op basis van schade en belang. In artikel 6 (Risicomanagement) wordt ingegaan op de noodzaak van een inzichtelijke risicoanalyse.

Bij het bepalen van de gevoeligheid van gegevens moet ook rekening worden gehouden met de concentratiefactor. Een grote collectie ongerubriceerde of laaggerubriceerde gegevens heeft als som een hogere gevoeligheid dan de onderdelen afzonderlijk. Dit geldt in het bijzonder voor grootschalige clouddiensten.

Voor een uitgebreider beschrijving van de gesloten Rijkscloud verwijzen wij naar de Functionele Doelarchitectuur van de Gesloten Rijkscloud. [6]

Voor een uitgebreider beschrijving van DWR-G verwijzen wij naar het informatiemateriaal van VenJ/GDI. [23]

In bijlage A gaan wij in meer detail in op de inhoud en eisen van het BIR en VIR-BI in relatie tot clouddiensten.

4 Audits van clouddiensten

In dit hoofdstuk wordt het uitvoeren van audits op clouddiensten behandeld. Hierbij wordt als uitgangspunt genomen dat: clouddiensten een moderne variant zijn van uitbesteding zijn, en dat audits van clouddiensten vergelijkbaar zijn met audits van uitbestede diensten. Tenslotte wordt het effect van de cloudstrategie van de Rijksoverheid op de rol van de IT-auditor toegelicht.

4.1 De levenscyclus van uitbesteding en rol van de IT-auditor

Als een gebruikersorganisatie, op basis van bedrijfsmatige overwegingen, beslist om IT-diensten uit te besteden dan kunnen daarin de volgende vier fasen worden onderscheiden: [32] [33]

- Sourcing beslissing - Het besluit om tot uitbesteding over te gaan en de beslissing welke activiteiten en diensten voor uitbesteding in aanmerking komen.
- Selectie leverancier - Selectie van een leverancier op basis van vooraf bepaalde selectiecriteria.
- Contractbeheer - Contractbeheer en service level management op basis van de tussen IT-beheerorganisatie, gebruikersorganisatie en leverancier overeengekomen dienstenniveaus.
- Afbouw – Beëindigen van de dienst, migreren van de dienst naar een andere leverancier of dienst weer in-huis nemen.

In elk van deze fasen kan de IT-auditor ondersteuning geven en helpen om de volgende vragen te beantwoorden. Deze zijn geldig voor de meeste vormen van uitbesteding en daardoor ook van toepassing op clouddiensten. [32] [33]

[32] IT-auditing en de praktijk, Rob Fijneman, Edo Roos Lindgreen, Kai Hang Ho, Academic Service, 2006, Paragraaf 4.6: IT-beheer in geval van uitbesteding

[33] CISA Review Manual 2013, ISACA, Paragraaf 2.9.2: Sourcing practices

Stap	Mogelijke vragen voor de IT-auditor
Sourcing beslissing	Hoe gevoelig zijn de gegevens die worden uitbesteed? Hoe strategisch zijn de processen die worden uitbesteed? Hebben de gebruikers- en IT-beheerorganisatie voldoende ervaring om leveranciers aan te sturen? Wegen de voordelen op tegen de risico's? Is het proces van uitbesteding rechtmatig, betrouwbaar en controleerbaar verlopen?
Selectie leverancier (en "due diligence" bij selectie leverancier)	Zijn de eisen van de gebruikersorganisatie volledig, toetsbaar en meetbaar vastgelegd? Kan de leverancier aan de eisen voldoen? Over welke certificaten en accreditaties beschikt de leverancier en hoeveel zekerheid geven zij? Passen de gebruikersorganisatie en de leverancier bij elkaar wat betreft cultuur, aanpak, ervaring en volwassenheid (hoe moet dit objectief worden vastgesteld? Heeft de leverancier een overwicht op de klant (bijvoorbeeld in kennis, ervaring of volume) en levert hem dit contractuele voordelen op? Waar vindt de verwerking plaats en waar worden de gegevens opgeslagen?
Contractbeheer	Krijgt de gebruikersorganisatie voldoende informatie om de prestaties van de leverancier te beoordelen? Voldoet de leverancier aan de afspraken in het contract? Voldoet de leverancier aan de vooraf contractueel vastgestelde verwachtingen van de gebruikersorganisatie? Hoe verhouden de diensten van deze leverancier zich met andere leveranciers (bijvoorbeeld qua prestaties, kwaliteit en kosten)? Moet het contract worden aangepast?
Afbouw	Zijn alle gegevens op een bruikbare wijze overgedragen van leverancier naar gebruikersorganisatie? Zijn alle gegevens gewist bij de leverancier?

4.2 De cloud en de rol van de IT-auditor

De NIST [34] beschrijft de rol van de cloud auditor als volgt:

- De cloud auditor geeft een onafhankelijk oordeel over het stelsel van beheersmaatregelen van een cloud dienst en kan daarbij aandacht geven aan (ondermeer) naleving van voorschriften, beveiliging, privacy en performance.
- Bij de beoordeling van de beveiliging kan de auditor aandacht geven aan opzet, bestaan en werking van beveiligingsmaatregelen en de naleving van beveiligingsregelgeving en beveiligingsbeleid.
- Bij de beoordeling van privacy aspecten kan de auditor aandacht geven aan wetgeving, regelgeving en beleid die gelden voor de beschikbaarheid, integriteit en exclusiviteit van persoonsgegevens.
- Onafhankelijke audits zijn extra belangrijk voor overheidsorganisaties. Daarom moeten zij extra aandacht geven aan contractuele afspraken zodat derden de (fysieke, organisatorische, procedurele en technische) beveiligingsmaatregelen van cloudleveranciers kunnen toetsen.

[34] US Government Cloud Computing Technology Roadmap, Volume II, Release 1.0 (Draft), Useful Information for Cloud Adopters, NIST Special Publication 500-293, November 2011

4.3 Soorten clouddiensten en de rol van de IT-auditor

Vanwege de keuzes die gemaakt zijn in de cloudstrategie van de Rijksoverheid zal een IT-auditor slechts een beperkt aantal clouddiensten kunnen tegenkomen. Daarbij zijn de volgende aandachtspunten relevant:

- Vaststellen dat geen publieke of commerciële clouddiensten gebruikt worden.
- Vaststellen dat de juiste clouddiensten van de Rijksoverheid worden gebruikt passend bij de gevoeligheid van de gegevens en het aanwezige dreigingsniveau.
- Vaststellen dat de clouddiensten van de Rijksoverheid aan de geldende beveiligingsvoorschriften voldoen.

Dit wordt in de onderstaande tabel samengevat.

Het is zinvol om de IT-auditor in een vroeg stadium bij clouddiensten te betrekken. Bij voorkeur op het moment dat een Rijksoverheidsorganisatie denkt aan een specifieke variant van clouddiensten en zeker voordat het contract met een leverancier is afgesloten. Advisering waarbij ook een risicoanalyse plaatsvindt, is nuttiger en effectiever dan een audit achteraf. Achteraf is het (vaak) niet meer mogelijk om bij te sturen.

Naarmate de leverancier meer “op afstand” staat van de gebruikersorganisatie wordt het lastiger om de vragen te beantwoorden. Maar binnen de Rijksoverheid zal de leverancier nooit op grote afstand staan. Binnen deze context is het goed mogelijk om te werken met een “Third Party Mededeling” bijvoorbeeld afgegeven door de Auditdienst Rijk.

Soort gegevens	Dreiging	Cloudstrategie van de Rijksoverheid Mogelijke vragen voor de IT-auditor
Alle soorten overheids-gegevens	Alle dreigings-niveaus	**Persoonlijke clouddiensten <u>niet</u> gebruiken** **Publieke commerciële clouddiensten <u>niet</u> gebruiken** Worden externe clouddiensten (zoals Gmail en DropBox) binnen de gebruikt en in welke mate? Welke overheidsgegevens worden gedeeld via clouddiensten? Zijn de risico's hiervan bekend bij de gebruikersorganisatie en de gebruikers? Is er een duidelijk en goed gecommuniceerd beleid aanwezig dat het gebruik verbiedt of reguleert? Hoe wordt het gebruik gedetecteerd en eventueel geblokkeerd? Zijn meer beheersbare alternatieven mogelijk?
Gegevens tot en met WBP-2 of Dep.V	**Geen** dreiging van georgani-seerde criminaliteit, inlichtingen-diensten of terreurgroepen	**Community cloud (GRC) of private clouddiensten van de overheid gebruiken** Wie is de organisatie (of consortium) dat de clouddienst heeft opgezet? In hoeverre kunnen (en willen) wij deze organisatie vertrouwen? Welke belangen heeft deze organisatie en in hoeverre komen ze overeen met onze eigen belangen? Vanuit welke locatie worden de diensten geleverd en waar worden gegevens opgeslagen? Is de leverancier geaccrediteerd en gecertificeerd volgens de relevante voorschriften en normen en kan op deze certificering gesteund worden ten behoeve van een assuranceverklaring? Is een juiste inschatting gemaakt van de gevoeligheid van de gegevens en het geldende dreigingsniveau? Kan de leverancier aantonen dat de genomen beveiligingsmaatregelen passen bij de gevoeligheid van de opgeslagen gegevens en het aanwezige dreigingsniveau? Kan de leverancier garanderen en aantonen dat hij geen diensten uitbesteedt aan andere leveranciers met lagere beveiliging en mindere "faam en naam"?
Gegevens tot en met WBP-2 of Dep.V	**Wel** dreiging van georgani-seerde crimi-naliteit, inlich-tingendiensten of terreur-groepen	**Gespecialiseerde community cloud (DWR-G) of gespecialiseerde private clouddiensten van de overheid gebruiken** Gelijke vragen als boven. Hier gelden echter hogere beveiligingseisen vanwege de grotere gevoeligheid van de opgeslagen gegevens en het hogere dreigingsniveau.
Gegevens vanaf WBP-3 of Stg.C en hoger	Alle dreigings-niveaus	

In bijlagen A, B en C geven wij een uitgebreid overzicht van de normenkaders die de IT-auditor kan gebruiken bij het beantwoorden van deze vragen. In bijlage D geven wij een korte schets van de Europese ontwikkelingen op dit gebied.

Bijlage A – Toelichting BIR en VIR-BI

Bij de inrichting en beveiliging van clouddiensten voor de Rijksoverheid zijn (met name) twee beveiligingsnormen van de Rijksoverheid relevant:

- BIR – De Baseline Informatiebeveiliging Rijksdienst richt zich op beschikbaarheid, vertrouwelijkheid en integriteit van niet-gerubriceerde informatie tot en met WBP Risicoklasse 2 en gerubriceerde informatie tot en met Departementaal Vertrouwelijk niveau. Hij is gebaseerd op de ISO 27001 norm aangevuld met rijksspecifieke implementatierichtlijnen. [19]
- VIR-BI - Het Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie richt zich op vertrouwelijkheid van gerubriceerde informatie voor Departementaal Vertrouwelijk niveau en hoger. [20]

BIR en VIR-BI zijn van toepassing op alle ICT-diensten van de Rijksoverheid (zowel in eigen beheer als uitbesteed) en daarmee ook voor clouddiensten.

De combinatie van de toepassingsgebieden van de BIR en het VIR-BI wordt in de onderstaande tabel geïllustreerd.

	Beschikbaarheid	Integriteit	Vertrouwelijkheid
Ongerubriceerd	BIR	BIR	BIR
Departementaal Vertrouwelijk	BIR	BIR	BIR + VIR-BI
Staatsgeheim Confidentieel	BIR	BIR	BIR + VIR-BI
Staatsgeheim Geheim	BIR	BIR	BIR + VIR-BI
Staatsgeheim Zeer Geheim	BIR	BIR	BIR + VIR-BI

BIR

Het BIR is op hoofdlijnen gelijkwaardig met de eerder genoemde cloudnormen (NIST, ENISA, CSA) omdat het BIR, net als deze normen op ISO 27001 gebaseerd is. Als een leverancier aan een van deze internationale normen voldoet dan is de kans groot dat hij, eventueel met een beperkt aantal extra maatregelen, ook aan de eisen van het BIR voldoet.

Voor een overheidsorganisatie die als klant (K) gebruik maakt van de diensten van een cloudleverancier (L) is slechts een deel van de BIR eisen relevant, omdat de meeste beveiligings-maatregelen door de leverancier moeten worden genomen. In de onderstaande tabel geven wij een eerste aanzet voor een cloud specifieke interpretatie van de relevante BIR eisen. (Dit is geen volledig uitgewerkte audit norm.)

BIR paragraaf	Wie		Cloud aandachtspunten
	K	L	
6.2. Externe Partijen	K	L	Met een risicoanalyse moet worden vastgesteld of het mogelijk is om gegevens in de cloud, en daardoor buiten het directe zicht van de organisatie, te laten verwerken. Hierbij moet extra aandacht worden gegeven aan gegevens met een WBP risicoklasse of VIR-BI rubricering die extra beveiliging nodig hebben. De noodzakelijke beveiligingsmaatregelen moeten worden vastgelegd in contracten met de cloudleverancier. Hierbij zijn alle paragrafen van het BIR (en/of ISO 27001, NIST 800-53 of

			ENISA/CSA normen) relevant, met name personele beveiliging, fysieke beveiliging, beheer, toegangsbeveiliging, ontwikkeling, onderhoud en naleving.
7.1. Verantwoordelijkheid voor bedrijfsmiddelen	K		Het moet duidelijk zijn welke lijnmanagers verantwoordelijk zijn voor de gegevens en bedrijfsprocessen die naar de cloud zijn uitbesteed.
7.2. Classificatie van informatie	K	L	Gerubriceerde informatie moet worden gemarkeerd en moet extra worden beveiligd volgens de eisen van het VIR-BI.
10.1. Bedieningsprocedures en verantwoordelijkheden	K		Er moeten gedocumenteerde procedures zijn voor een veilig en verantwoord gebruik van de clouddienst.
10.2. Exploitatie door een derde partij	K	L	Er moet een overeenkomst van dienstverlening met de cloudleverancier worden afgesloten met daarin definities van dienstverlening, niveaus van dienstverlening en beveiligingsmaatregelen. Er moeten regelmatig rapportages over de dienstverlening worden opgeleverd en audits op de dienstverlening worden uitgevoerd. Zie ook 6.2.
10.3. Systeemplanning en –acceptatie	K	L	Er moeten duidelijke en haalbare afspraken zijn over capaciteit en beschikbaarheid van de clouddienst. Er moet een acceptatieproces zijn voor ingebruikname en wijzigingen van de clouddienst.
10.5. Back-up	K	L	Er moeten afspraken en procedures zijn waarmee de klant altijd de eigenaar kan blijven van zijn eigen gegevens. Uitval van de clouddienst, beëindiging van het contract of faillissement van de leverancier mag nooit tot verlies van gegevens leiden.
10.6. Beheer van netwerkbeveiliging		L	Toegang tot de clouddienst moet via een veilige, geauthenticeerde en versleutelde verbinding plaatsvinden.
10.7. Behandeling van media		L	Er moeten afspraken en procedures zijn waarmee gewaarborgd is dat gegevens van de klant betrouwbaar worden gewist van alle media bij de cloudleverancier.
10.8. Uitwisseling van informatie		L	De locatie waar klantgegevens worden verwerkt moet contractueel vastgelegd en controleerbaar zijn. Als de gegevens in het buitenland of buiten Europa worden verwerkt moeten de toegangsmogelijkheden van de verantwoordelijke overheid duidelijk vastgelegd en acceptabel zijn.
10.10. Controle		L	De leverancier van de clouddienst moet voldoende logbestanden beschikbaar stellen om toezicht op correcte verwerking en detectie van storingen en (beveiligings-) incidenten mogelijk te maken.
11.2. Beheer van toegangsrechten van gebruikers		L	Toegang tot de clouddienst moet worden verleend op basis van een veilige identificatie, authenticatie en autorisatie. Er moet voorzien zijn in voldoende en aantoonbare functiescheiding.
12.6. Beheer van technische kwetsbaarheden	K	L	De leverancier van de clouddienst moet over controleerbare procedures beschikken om zijn technische infrastructuur te voorzien van updates en patches. Er moeten penetratietests op de infratsructuur van de leverancier worden uitgevoerd.
13. Beheer van Informatiebeveiligingsincidenten		L	De leverancier moet incidenten en kwetsbaarheden direct rapporteren als zij een risico voor de klant opleveren.
14. Bedrijfscontinuïteitsbeheer	K		Er moet een risicoanalyse gemaakt worden van de kans op uitval van de clouddienst. Op basis hiervan moet een calamiteitenplan aanwezig zijn voor voortzetting van de bedrijfsvoering bij uitval

			van de clouddienst.
15.1. Naleving van wettelijke voor-schriften	K		Bij gebruik van clouddiensten van buitenlandse leveranciers en bij verwerking van gegevens buitens nationaal grondgebied moet extra aandacht worden gegeven aan de wettelijke consequenties hiervan. Hierbij moet rekening worden gehouden met toegangs-mogelijkheden van buitenlandse overheden tot de gegevens.
15.3. Overwegingen bij audits van informatiesystemen	K	L	De leverancier moet voldoende mogelijkheden voor toezicht op de verwerking van de klantgegevens beschikbaar stellen zodat de klant aantoonbaar “in control” kan blijven van zijn bedrijfsproces.

VIR-BI

Het is niet te verwachten dat gerubriceerde informatie aan een externe clouddienstverlener zal worden uitbesteed. Naar verwachting zal dergelijke informatie altijd in de nationale gesloten rijkscloud worden verwerkt. Dit is niet alleen het Nederlandse beleid maar ook het beleid van bijvoorbeeld het Verenigd Koninkrijk, de Verenigde Staten en de NATO.

De situatie kan op langere termijn echter veranderen. Op dit moment zijn externe dienstverleners al bezig om commerciële private clouddiensten te ontwikkelen die geschikt zijn voor gebruik door overheden.

Voor de volledigheid vermelden wij in de onderstaande tabel een aanzet voor een cloud specifieke interpretatie van enkele opvallende VIR-BI eisen. Hierbij vermelden wij de eisen voor het rubriceringsniveau Staatsgeheim Confidentieel en hoger. (Dit is geen volledig uitgewerkte audit norm.)

VIR-BI artikel	Cloud aandachtspunten
2.3	Gerubriceerde informatie die krachtens een internationaal verdrag is verkregen (denk aan: NATO en EU informatie) moet worden beveiligd conform de eisen die behoren bij het verdrag.
3.b	De Secretaris Generaal moet vooraf toestemming verlenen voor het verwerken van gerubriceerde informatie.
6.1	Aleen geautoriseerde personen mogen toegang hebben tot gerubriceerde informatie. Inbreuken op de beveiliging moeten gedetecteerd en onderzocht worden.
6.2	Gerubriceerde informatie die krachtens een internationaal verdrag is verkregen (denk aan: NATO en EU informatie) wordt uitsluitend verwerkt nadat de autoriteit die voor het verdrag verantwoordelijk is haar goedkeuring aan de beveiliging heeft gegeven.
7.1	Als gerubriceerde informatie buiten de Rijksdienst gebracht wordt blijven de eisen voor beveiliging en toezicht onverminderd van kracht. De Secretaris Generaal moet vooraf toestemming verlenen voor buiten de Rijksdienst brengen van gerubriceerde informatie.
7.2	Gerubriceerde informatie die krachtens een internationaal verdrag is verkregen wordt uitsluitend doorgegeven aan externe partijen na toestemming van het land of de organisatie van wie de informatie is verkregen.
Bijlage	
2.B	Personen die te maken hebben met gerubriceerde informatie dienen te beschikken over een verklaring van geen bezwaar (VGB).

3.B	Er dienen tempest-maatregelen te zijn getroffen conform het Beleidsavies Compromitterende straling (VBV 32000).
5.A	Er worden door onafhankelijke deskundigen periodieke audits, inspecties, reviews en tests uitgevoerd om te controleren of de beveiligingsmaatregelen effectief zijn.
6.A.B	Digitale verzending van gerubriceerde informatie vindt plaats met door de verantwoordelijke autoriteit goedgekeurde cryptografische middelen.
6.H	Beveiligingsrelevante handelingen worden geregistreerd.

Overige (nationale) eisen voor gerubriceerde informatie

Tegelijk met de ontwikkeling van de VIR-BI 2012 normen zijn ook praktische richtlijnen ontwikkeld in het Programma Consolidatie Datacenters. Hierbij zijn alleen eigen gesteld aan housing diensten in rekencentra tot maximaal rubriceringsniveau Staatsgeheim Confidentieel. [21] In de onderstaande tabel vermelden wij de eisen die een bruikbare aanvulling vormen op de beveiligingseisen van het VIR-BI.

Tactisch normenkader housing tot en met Staatsgeheim Confidentieel – stuurgroep PCDC
2. Gegevens in het datacenter moeten binnen de Nederlandse beschikkingsmacht vallen;
3. In het datacenter moet (a)synchrone duplicatie en back-up van bedrijfskritische gegevens mogelijk zijn;
4. Het datacenter moet versleutelde informatie kunnen verwerken (voor zover nu reeds van versleuteling sprake is);
7. Relevante apparatuur, te gebruiken voor in ieder geval de gerubriceerde documenten, mag niet vanaf buiten het gebouw zichtbaar zijn, voorts mag deze apparatuur niet tegen de buitenmuur van het gebouw zijn geplaatst.
8. Bij uitbestedingen aan marktpartijen dienen deze te voldoen aan ISO 27001 en ISO 27002;
9. Er dienen op ITIL of gelijkwaardige modellen gebaseerde beheerprocessen te zijn ingericht.

Bijlage B - Accreditatie- en certificatienormen voor publieke clouddiensten

In het publieke domein is een ruim, bijna overweldigend, aanbod aan cloudnormen, checklists, voorbeeldarchitecturen en best practices beschikbaar.

De meest gerenommeerde, informatieve en actuele documenten hebben wij in de onderstaande tabel opgesomd. Alle hieronder genoemde documenten bevatten beschrijvingen van risico's, componenten en beveiligingsmaatregelen van clouddiensten. De documenten hebben wij als volgt gecategoriseerd:

- Risico's en maatregelen – Deze documenten zijn te lezen als richtlijn en "best practice" om de risico's van cloudoplossingen te verminderen. Zij zijn geschikt als een eerste kennismaking met de cloud problematiek vanuit audit oogpunt.
- Architectuur en bouwstenen – Deze documenten zijn te lezen als richtlijn en "best practices" voor de architectuur van cloudoplossingen en de bouwstenen die daar in aanwezig moeten zijn. Zijn geschikt als een eerste kennismaking met de cloud problematiek vanuit audit oogpunt.
- Normen en maatregelen – Deze documenten bevatten uitgebreide stelsels van normen voor cloudoplossingen, die zonder voorkennis niet altijd goed leesbaar zijn, maar die geschikt zijn als normenkader voor audits.

Op basis van de internationale en Europese ontwikkelingen op cloudgebied verwachten wij dat de normen van CSA, ENISA en NIST de beste kansen hebben om tot standaarden uit te groeien. Wij verwachten dat – vanwege uiteenlopende belangen - deze normenstelsels voorlopig naast elkaar blijven bestaan en niet zullen worden geconsolideerd.

Organisatie & Normenkader	Inhoud van document	Jaar publicatie
National Institute of Standards and Technology (NIST)		
Guidelines on Security and Privacy in Public Cloud Computing [35]	Risico's en maatregelen	2011
Cloud Computing Synopsis and Recommendations [36]	Risico's en maatregelen	2012
Cloud Computing Reference Architecture [37]	Architectuur en bouwstenen	2011
European Network and information Security Agency (ENISA)		
Cloud Computing Information Assurance Framework [38]	Risico's en maatregelen	2009
Security & Resilience in Governmental Clouds [39]	Risico's en maatregelen	2011

[35] SP 800-144 - Guidelines on Security and Privacy in Public Cloud Computing, NIST, December 2011

[36] NIST SP 800-146 - Cloud Computing Synopsis and Recommendations, NIST, May 2012

[37] NIST Cloud Computing Reference Architecture, Recommendations of the National Institute of Standards and Technology, Special Publication 500-292, September 2011

[38] Cloud Computing, Information Assurance Framework, ENISA, November 2009

[39] Security & Resilience in Governmental clouds, Making an informed decision, ENISA, 17 januari 2011

Cloud Security Alliance (CSA)		
Security Guidance for Critical Areas of Focus in Cloud Computing [40]	Risico's en maatregelen	2011
Cloud Security Alliance Controls Matrix [41]	Norm en maatregelen	2012
Open Security Architecture (OSA)		
Cloud Computing Pattern [42]	Architectuur en bouwstenen	2009
Bundesamt für Sicherheit in der Informationstechnik (BSI)		
Security Recommendations for Cloud Computing Providers, Minimum information security requirements [43] [44]	Norm en maatregelen	2012
Federal Risk and Authorization Management Program (FedRAMP)		
FedRAMP Baseline Security Controls [45] [46]	Norm en maatregelen	2012
Information Systems Audit and Control association (ISACA)		
IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud [47]	Norm en maatregelen	2011
Surfnet		
Cloud security, Checklist en de te stellen vragen [48]	Risico's en maatregelen	2010

Belangrijkste aandachtspunten van de publieke cloud normen

De normen en maatregelen zijn allemaal gebaseerd op bekende en algemeen geaccepteerde (IT beveiligings-) normen zoals International Organization for Standardization (ISO) 27001-2005, NIST Special Publication (SP)800-53 R3, Control Objectives for Information and related Technology (COBIT) en Information Technology Infrastructure Library (ITIL) en lijken, afgezien van structuur, indeling en terminologie sterk op elkaar. Om dit te illustreren hebben wij hieronder enkele richtlijnen en normen op hoofdlijnen vergeleken en naast elkaar gezet.

CSA [41]	FedRamp [45] [46]	ENISA [38]
Compliance	Certification, Accreditation, and Security Assessment	Legal requirements
Data Governance	Media Protection	Asset management Management of personal data Key management Encryption
- - -	- - -	Gegevens and Services Portability

[40] Security Guidance for Critical Areas of Focus in Cloud Computing, Cloud Security Alliance, Versie 3.0, 14 november 2011

[41] Cloud Security Alliance – CSA Cloud Controls Matrix, CSA_CCM_v1.3.xlsx, www.cloudsecurityalliance.org, 20 september 2012

[42] SP-011: Cloud Computing Pattern, www.opensecurityarchitecture.org

[43] White Paper, Security Recommendations for Cloud Computing Providers, Minimum information security requirements, Bundesamt für Sicherheit in der Informationstechnik, mei 2011

[44] Eckpunktepapier, Sicherheitsempfehlungen für Cloud Computing Anbieter, Mindestanforderungen in der Informationssicherheit, Bundesamt für Sicherheit in der Informationstechnik, februari 2012, BSI-Bro12/314

[45] FedRAMP, Concept of Operations (CONOPS), Version 1.0, February 7, 2012

[46] FedRAMP Security Controls Baseline, Version 1.1, 25 juli 2012

[47] IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud, ISACA, 2011, ISBN 978-1-60420-185-7

[48] Cloud security, Checklist en de te stellen vragen, Surfnet, Guido van der Harst, SURFibo, December 2010

Facility Security	Physical and Environmental Protection	Physical security Environmental controls
Human Resources Security	Personnel Security	Personnel security
Information Security	Awareness and Training Access Control Identification and Authentication Incident Response Audit and Accountability Contingency Planning Configuration Management System and Information Integrity	Operational security Software assurance Patch management PaaS – Application security SaaS – Application security Identity and access management Authentication Credential compromise or theft
Legal	- - -	Legal requirements
Operations Management	Maintenance	Resource provisioning
Risk Management	Risk Assessment	- - -
Release Management	System and Services Acquisition	Supply-chain assurance
Resiliency	Physical and Environmental Protection Contingency Planning	Business Continuity Management Incident management and response
Security Architecture	Access Control System and Information Integrity System and Communications Protection Audit and Accountability	Host architecture Network architecture controls

Wat opvalt is dat veel aandacht aan de standaard informatiebeveiliging wordt gegeven maar relatief weinig aandacht aan specifieke zorgpunten van clouddiensten zoals: [49]

- onvoldoende specifieke en evenwichtige contracten met cloud-leveranciers,
- het voorkomen van een technologische "lock-in",
- standaardisering en interoperabiliteit van gegevensformaten,
- toegankelijkheid en portabiliteit van gegevens,
- gebruik van open cloud technologie, [50]
- gebruik van gestandaardiseerde cloud API's, [51]
- controle over wijzigingen,
- eigendom van de gegevens die in cloud-toepassingen worden gecreëerd,
- gebruikersrechten met betrekking tot upgrades van het systeem waarover de leverancier unilateraal beslist,
- aansprakelijkheid voor calamiteiten en gebrekkige dienstverlening (zoals uitvaltijd of verlies van gegevens),
- faillissementsvraagstukken en het voorkomen van gegevensverlies (bijvoorbeeld via een escrow-regeling of een trusted third party), [52]
- de wijze waarop geschillen worden beslecht.

[49] Het aanboren van het potentieel van cloud computing in Europa, Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's, COM(2012) 529 final, Brussel, 27.9.2012

[50] OpenStack, Open source software for building private and public clouds, www.openstack.org

[51] The cloud computing interoperability forum, www.cloudforum.org

[52] Kamerbrief, Informatievoorziening over nieuwe Commissievoorstellen, DIE-BNC – 1387/12, Fiche 2: Mededeling aanboren van het potentieel van cloud computing in Europa, 2 november 2012

Algemene normen – bruikbaar voor alle soorten uitbesteding

Naast de specifieke cloudnormen zijn ook de volgende stelsels van eisen relevant en bruikbaar bij het overwegen van uitbesteding naar de cloud. Het geeft extra zekerheid als de leverancier kan aantonen in welke mate hij aan de volgende beheermodellen voldoet:

- SSAE 16 - Statement on Standards for Attestation Engagements No. 16
- ISAE 3402 - International Standards for Assurance Engagements No. 3402
- ISO 27001 - Informatietechnologie - Beveiligingstechnieken - Managementsystemen voor informatiebeveiliging [53]
- NEN 7510 - Medische informatica -Informatiebeveiliging in de zorg [54]
- SPICE – Software Process Improvement and Capability dEtermination (ISO/IEC 15504),
- CMMI – Capability Maturity Model Integration,
- ITIL – Information Technology Infrastructure Library
- COBIT – Control Objectives for Information and Related Technology,
- ISO 9001 – Quality Management Systems.

Publieke en nationale certificatieschema's voor cloudleveranciers

Om het vertrouwen in cloud oplossingen bij bedrijfsleven en overheden te verhogen en het gebruik te stimuleren zijn er vele nationale en internationale cloud projecten gestart. Bij sommige van deze projecten zijn ook beveiligings-normen opgesteld waartegen leveranciers van clouddiensten kunnen worden getoetst, gecertificeerd en geaccrediteerd voor gebruik door nationale overheden en industrie. Het succes hiervan is wisselend.

Enkele bij ons bekende projecten en schema's hebben wij in de onderstaande tabel samengevat. Deze opsomming is zeker niet volledig want er worden voortdurend nieuwe projecten en initiatieven gestart.

Binnen Nederland is nog geen nationaal certificeringsschema met bijbehorende normen aanwezig. Er worden ook geen acties ondernomen om tot een dergelijk schema te komen. Naar onze mening is dit een juiste beslissing en is het beter om aan te sluiten bij internationale of Europese schema's.

Op basis van de internationale en Europese ontwikkelingen op cloud gebied verwachten wij dat de certificatieschema's van de CSA en FedRamp het meest kansrijk zijn. Daarnaast verwachten wij dat het (nog te ontwikkelen) Europese certificatieschema's onder aansturing van ENISA succesvol zal worden.

[53] Nederlands Normalisatie-instituut, NEN-ISO/IEC 27001:2005 nl – Informatietechnologie - Beveiligingstechnieken - Managementsystemen voor informatiebeveiliging - Eisen, 1 november 2005, http://www.nen.nl/web/Normshop/Norm/NENISOIEC-270012005-nl.htm

[54] Nederlands Normalisatie-instituut, NEN 7510:2004 nl - Medische informatica -Informatiebeveiliging in de zorg - Algemeen, 1 april 2004, http://www.nen.nl/web/Normshop/Norm/NEN-75102004-nl.htm

Programma	Initiatief-nemer	Scope	Normenkader	Certificatie-schema
Security, Trust & Assurance Registry [55] [56] [57]	industrie	Internationaal	Ja – vragenlijst gebaseerd op Cloud Security Alliance Controls Matrix	Ja - self assesment
G-Cloud Programme [58] [59]	overheid	Verenigd Koninkrijk	Ja – norm gebaseerd op ISO 27001 en de Data Protection Act	Ja - externe toetsing
Andromède [60]	overheid	Frankrijk	Nee - status onduidelijk	Nee
Trusted Cloud [61]	overheid	Duitsland	Nee - alleen technologie onderzoeksprojecten	Nee
EuroCloud Star Audit SAAS [62] [63]	industrie	Duitsland	Ja – norm gebaseerd op BSI richtlijn	Ja – externe toetsing
FED-Ramp [45] [46]	overheid	Verenigde Staten	Ja – norm gebaseerd op NIST 800-53	Ja - externe toetsing
Cloud computing strategic direction [64] [65] [66]	overheid	Australië	Nee – alleen checklists	Nee

Algemene normen en certificatieschema's in gebruik bij cloudleveranciers

Naast de cloud-gerichte normen en certificatieschema's maken vele cloudleveranciers ook gebruik van reeds bestaande normen en schema's. Als voorbeeld hebben wij hieronder aangegeven aan welke normen en schema's enkele cloudleveranciers, volgens eigen mededeling, voldoen. De conclusie is dat dergelijke eisen van nagenoeg elke publieke cloudleverancier verwacht mogen worden.

Van deze certificatieschema's geven SOC [67], ISO 27001 en PCI-DSS [68] de meest controleerbare zekerheid over de beveiliging van de cloudleverancier.

---

[55] STAR Registry Entries : Cloud Security Alliance, https://cloudsecurityalliance.org/star/registry/

[56] Consensus Assessments Initiative Questionnaire v1.1

[57] STAR FAQ, www.cloudsecurityalliance.org/star

[58] The G-Cloud Programme, gcloud.civilservice.gov.uk

[59] G-Cloud Information Assurance Requirements and Guidance, G-Cloud Security Working Group, 03/05/12

[60] Canal Cloud, Andromède, http://www.canalcloud.com/etiquettes/andromede

[61] Das Technologieprogramm Trusted Cloud, Bundesministerium für Wirtschaft und Technologie, http://www.trusted-cloud.de/de/1258.php

[62] Requirements, Saas Star Audit, http://www.saas-audit.de/en/511/requirements/

[63] Europese Commissie Persbericht, Brussel, Digitale agenda: nieuwe strategie om bedrijfsleven en overheden in Europa productiever te maken met cloud computing, 27 september 2012

[64] Cloud computing strategic direction paper, Opportunities and applicability for use by the Australian Government, April 2011, Version 1.0

[65] Cloud Computing Security Considerations, Australian Government, Department of Defence, Cyber Security Operations Centre, September 2012

[66] Privacy and Cloud Computing for Australian Government Agencies, Better Practice Guide, Commonwealth of Australia 2012

[67] International Standards for Assurance Engagements (ISAE) No.3402, http://isae3402.com

[68] PCI Security Standards Council 'Payment Card Industry Data Security Standards (PCI-DSS), https://www.pcisecuritystandards.org

	Salesforce	Amazon	Microsoft
Service Organization Controls 1 (SOC 1) Type 2 report	Ja	Ja	Ja
SOC 1 audit in accordance with Statement on Standards for Attestation Engagements No. 16 (SSAE 16)	Ja	Ja	Ja
SOC 1 audit in accordance with International Standards for Assurance Engagements No. 3402 (ISAE 3402)	Ja	Ja	Ja
Service Organization Controls 2 (SOC 2) report in accordance with American Institute of Certified Public Accountants (AICPA) Trust Services Principles	Ja	Ja	Ja
Service Organization Controls 2 (SOC 3) report in accordance with SysTrust for Service Organisations	Ja	- - -	Ja
US Federal Information Security Management Act (FISMA) - Moderate level in accordance with NIST 800-53, Revision 3	Ja	Ja	Ja
Payment Card Industry (PCI) Data Security Standard (DSS) - Level 1 service provider	Ja	Ja	Deels Datacenters Ja Software Nee
ISO 27001 certification of the Information Security Management System	Ja	Ja	Ja
FIPS 140-2 security requirements for cryptographic modules	- - -	Ja	- - -
Suitable for Security and Privacy Rules of the Health Insurance Portability and Accountability Act (HIPAA)	Ja	Ja	Ja
Cloud Security Alliance (CSA) Consensus Assessments Initiative Questionnaire	- - -	Ja	Ja
EU Safe Harbor self-certification through the U.S. Department of Commerce	Ja	Ja	Ja
TRUSTe EU Safe Harbor Seal	Ja	- - -	Ja
TRUSTe Certified Privacy Seal	Ja	- - -	Ja

Publieke certificatie- en accreditatie schema's voor cloud specialisten

Naast de cloud-gerichte normen en certificatieschema's zijn ook normen en certificatieschema's aanwezig voor cloud specialisten. Slechts enkele hiervan zijn algemeen, de meeste zijn leverancier gebonden en gelden voor een specifieke cloud technologie. In de onderstaande tabel noemen wij enkele voorbeelden.

De aanwezigheid van deze certificaten geeft enige indicatie van het kennisniveau van het personeel van een cloudleverancier. Wij verwachten dat dergelijke certificatieschema's breed worden ingezet maar de aanwezigheid hiervan geeft slechts een beperkte zekerheid over het service- en beveiligingsniveau van een leverancier.

Initiatiefnemer	Type	Voorbeeld van een certificaat
Cloud Security Alliance	Algemeen	Certificate of Cloud Security Knowledge (CCSK)
Cloudschool	Algemeen	Cloud Certified Technology Professional (CCTP)
IBM	Productgebonden	IBM Certified Solution Architect – Cloud Computing Infrastructure
Google	Productgebonden	Google Apps Certified Deployment Specialist

Vmware	Productgebonden	VMware Certified Professional – Cloud (VCPCloud)
Microsoft	Productgebonden	MCSE: Private Cloud
Salesforce	Productgebonden	Administrator, Developer, Implementation Expert, Architect

Bijlage C – Aandachtspunten bij uitbesteding naar de cloud

Algemene aandachtspunten bij uitbesteding

Risico's bij uitbesteding – relevant voor alle soorten uitbesteding - zijn bijvoorbeeld: [32] [33]

- verlies van bestaande kennis en vaardigheden;
- verlies van het raakvlak met de IT -gebruikers;
- meer formele (en daarmee een meer onpraktische) werkwijze;
- het onvoldoende (kunnen) invullen van leveranciers- en service level management;
- verlies van flexibiliteit (te strakke contracten);
- bij strategische uitbesteding, het verlies van bedrijfsspecifieke kennis;
- een toenemende afhankelijkheid van derden;
- cultuurconflict met leverancier;
- moeilijkheid in definiëren van eisen en wensen;
- het niet kunnen realiseren/bewaken van het gewenste beveiligingsniveau;
- minder vrijheid in handelen als de leverancier niet voldoet;
- beperking in de bedrijfsvoering;
- beperkte keuze in dienstverleners;
- exclusiviteit (ideeën inzake toepassing van IT gaan naar concurrenten);
- motivatieverlies van bestaande medewerkers.

Eisen aan leverancier – relevant voor alle soorten uitbesteding - zijn bijvoorbeeld: [32]

- het kunnen leveren van de gewenste IT-diensten;
- continuïteit;
- bewezen prestaties;
- willen dragen van een stuk risico;
- passende bedrijfsculturen;
- zekerheid van dienstverlening;
- goede kennis van kerntaken klant;
- goede prijs/prestatieverhouding;
- operationele flexibiliteit.

Aandachtspunten bij het afsluiten van contract - relevant voor alle soorten uitbesteding - zijn bijvoorbeeld: [33]

- eigendom van de gegevens,
- software en gegevensescrow mogelijkheden,
- maatregelen om beschikbaarheid, integriteit en vertrouwelijkheid van gegevens te waarborgen,
- toegangsrechten en toegangsbeheer voor gebruikersorganisatie, IT-beheerorganisatie en gebruikersorganisatie,
- mogelijkheid om contract te beëindigen bij overname van leverancier,
- gegevens over alle onderaannemers van de leverancier en mogelijkheid om contract te beëindigen bij wijziging van onderaannemers,
- certificaten en accreditaties waar leverancier over beschikt,
- calamiteitenprocedures,
- melding van (beveiligings-) incidenten aan gebruikersorganisatie en medewerking aan onderzoek hiernaar;
- "right to audit", waaronder toegang tot locaties, personeel, registraties, gegevensbestanden, logbestanden en documentatie van de leverancier.

Specifieke aandachtspunten bij uitbesteding naar de cloud

Bij (publieke) clouddiensten is het contract of Service Level Agreement (SLA) meestal het belangrijkste (en soms enige) document waarop gesteund kan worden. Het is daarom van belang dat er tussen de klantorganisatie en de clouddienstverlener eenduidige afspraken worden gemaakt om problemen zoals vendor lock-in, slechte beschikbaarheid en het niet kunnen monitoren van de kwaliteit te voorkomen. In vergelijking met uitbesteding moet daarom meer aandacht te worden besteed aan een aantal aspecten: [13]

- naleving van wet- en regelgeving,
- beheersing van processen en systemen,
- gegevensbescherming,
- beschikbaarheid van de clouddienst,
- beheer van gebruikers,
- beheer van incidenten
- beheer van wijzigingen,
- back-up en recovery,
- transparantie.

ENISA heeft zeer uitgebreide en gedetailleerde lijsten met aandachtspunten voor cloud uitbesteding opgesteld. Hierbij wordt niet alleen ingegaan op de relevante aandachtspunten maar ook op de wijze waarop deze aandachtpunten bewaakt, gemeten en getest kunnen worden. Daarnaast heeft de PCI Security Standards Council een speciaal op clouddiensten gericht normenkader opgesteld. Dit is onmisbare informatie voor de IT-auditor.

European Network and information Security Agency (ENISA)		
Procure Secure, A guide to monitoring of security service levels in cloud contracts [69]	Contractuele aandachtspunten	2012
Survey and analysis of security parameters in cloud SLA's across the European public sector [70]	Contractuele aandachtspunten	2011
Payment Card Industry (PCI) Security Standards Council		
Information Supplement: PCI DSS Cloud Computing Guidelines [71]	Contractuele aandachtspunten	2013

Hieronder worden de aandachtspunten van deze drie documenten op hoofdlijnen samengevat. Het is niet mogelijk om hier de volledige inhoud van deze documenten weer te geven.

[69] Procure Secure, A guide to monitoring of security service levels in cloud contracts, European Network and Information Security Agency (ENISA), 2012, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts/at_download/fullReport

[70] Survey and analysis of security parameters in cloud SLAs across the European public sector, European Network and Information Security Agency (ENISA), 2011, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/survey-and-analysis-of-security-parameters-in-cloud-slas-across-the-european-public-sector/at_download/fullReport

[71] Information Supplement: PCI DSS Cloud Computing Guidelines, February 2013, Cloud Special Interest Group PCI Security Standards Council, https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Cloud_Guidelines.pdf

Algemene vragen over SLA's voor clouddiensten zijn ondermeer:

- Welke normen zijn van toepassing?
- Hoe lang is het contract/SLA geldig?
- Welke infrastructuur en applicatie vallen onder het SLA/contract?
- Hoe snel moet de leverancier storingen melden?
- Bevat het SLA/contract en classificatie van (beveiligings-) incidenten?
- Hoe snel moet de leverancier (beveiligings-) incidenten melden?
- Welke hersteltijd is afgesproken voor storingen en (beveiligings-) incidenten?
- Heeft de leverancier procedures om het beveiligingsniveau van de clouddienst te meten en te rapporteren?
- Wie meet de beschikbaarheid? Zijn hier rapportages van beschikbaar?
- Wie voert penetratietests uit? Zijn hier rapportages van beschikbaar?
- Wie voert failover and backup tests uit? Zijn hier rapportages van beschikbaar?
- Wie voert conversie (data portability) tests uit? Zijn hier rapportages van beschikbaar?
- Wie voert stress-tests uit? Zijn hier rapportages van beschikbaar?
- Wie voert functionele tests uit?
- Zijn er boeteclausules in het SLA/contract aanwezig als niet aan afgesproken service levels wordt voldaan? Zijn hier uitsluitingen en beperkingen op?
- Wanneer kan vastgesteld/geconcludeerd worden dat de leverancier zich niet aan de afspraken in het SLA/contract houdt?
- Hoe lang moet een leverancier de afspraken in het SLA/contract overtreden voordat het opgezegd kan worden?

Relevante service levels waarover afspraken gemaakt moeten worden zijn ondermeer:

- fysieke beveiliging van de leverancier,
- beschikbaarheid van de dienst,
- elasticiteit van de dienst en tolerantie voor veranderingen in belasting,
- bewaartermijnen en beschikbaarheidstermijnen van gegevens,
- omgang met data (invoer, conversie, versleuteling, opslag, uitvoer, vernietiging) tijdens de gehele lifecycle van de gegevens,
- data isolatie, segmentering, compartimentering (hoe sterk is de scheiding tussen mijn data en de data van anderen, is dit fysiek, logisch of cryptografisch geregeld),
- fysieke locatie van de opgeslagen data en bijbehorend juridisch kader,
- naleving van technische beveiligingseisen,
- wijzigingsbeheer,
- beheer van kwetsbaarheden en updates,
- snelheid van incident response,
- omgang met (audit) logfiles en mogelijkheden van forensisch onderzoek.

Bijlage D - Europese visie op accreditatie- en certificatienormen

Het grote aantal uiteenlopende cloud normen levert problemen op voor aanbieders en afnemers van clouddiensten. Het probleem wordt ook op europees niveau gezien en men spreekt hier van "nationale hokjes" en "een oerwoud aan regelgeving". Het gebrek aan gemeenschappelijke normen en duidelijke contracten hindert potentiële gebruikers en leveranciers van clouddiensten. Ze weten niet met welke normen en certificaten ze aan hun behoeften en wettelijke verplichtingen kunnen voldoen; er bestaat bijvoorbeeld onzekerheid over het beveiligen van hun eigen gegevens en die van klanten en over de interoperabiliteit van toepassingen. [63]

Om het gebruik van clouddiensten in Europa te stimuleren, een goed werkende markt voor clouddiensten te ontwikkelen en de markt te laten groeien zal de Europese Commissie in 2013 (ondermeer) de normalisatie en certificatie voor clouddiensten oppakken en eind 2013 hierover een voortgangsrapport opstellen. Daaruit zal blijken of verdere beleids- en wetgevingsinitiatieven nodig zijn. In 2014 moet, onder aansturing van ENISA andere relevante organen, een lijst aanwezig zijn van certificeringsregelingen op het gebied van cloudcomputing en gegevensbescherming. [49] [72]

De huidige uitgangspunten voor het opzetten van normalisatie en certificatie zijn: [49] [72]

- Er zijn normen nodig die het mogelijk maken dat clouddiensten voldoen aan Europese regelgeving en tegelijk concurrerend, open en afdoende beveiligd zijn. Het initiatief voor het opstellen van de normen moet hierbij van de sector zelf uitgaan.
- Er is niet alleen behoefte aan normen, maar ook aan certificering van de naleving ervan. Gebruikers zijn zelden in staat om te verifiëren of de beweringen van leveranciers (dat zij voldoen aan normen) waar zijn. Hierbij ligt de voorkeur bij EU-wijde, vrijwillige certificeringsregelingen.

Nederland ondersteunt de standpunten van de Commissie over een Europese aanpak voor het ontwikkelen van standaarden, de Europese aanpak van de gegevensportabiliteit en gegevensprotectie, de eenduidige regelgeving en het willen benutten van economische kansen die cloudcomputing met zich meebrengt. Maar er zijn nog een aantal kanttekeningen te maken: [52]

- De Europese visie gaat er te veel van uit dat cloudcomputing in alle gevallen gewenst is en promotie behoeft. Er is meer duidelijkheid nodig of:
    - gevoelige privacygegevens en bedrijfsgeheimen/R&D in cloudcomputing oplossingen van internationale leveranciers kunnen worden verwerkt,
    - bilaterale en multilaterale overeenkomsten ongewenste mogelijkheden geven om persoonsgegevens of bedrijfsgeheimen op te eisen bij internationale cloudleveranciers,
    - de regelgeving voor internationale gegevensdoorgifte en grensoverschrijdend gegevensverkeer voldoende is toegesneden op cloudcomputing,
    - de voorgestelde "Algemene verordening gegevensbeschermingsrecht" geschikt is om persoonsgegevens in een cloudomgeving te beschermen.
- Omdat er geen barrières bestaan die grensoverschrijdende cloud-diensten tegenhouden, is internationale dialoog nodig.

[72] Europese Commissie Memo, Het aanboren van het potentieel van cloud computing in Europa – wat houdt dat in en wat betekent het voor mij? Brussel, 27 september 2012

Binnen het Europese cloud beleid is het voor overheidsdiensten nog steeds mogelijk om eigen private clouds op te zetten voor de verwerking van gevoelige gegevens, zoals de Gesloten Rijkscloud van de Nederlandse overheid. In het algemeen moeten zelfs cloud-diensten die door de overheidssector worden gebruikt in de mate van het mogelijke worden opengesteld voor concurrentie op de markt teneinde de beste prijs-kwaliteitverhouding te garanderen en tegelijk te garanderen dat deze diensten op bepaalde criteria, zoals beveiliging en bescherming van gevoelige gegevens, beantwoorden aan regelgevende verplichtingen of ruimere doelstellingen van openbaar beleid. [49]

Als de accreditatie en certificatie van clouddiensten op internationaal, Europees en nationaal niveau een hoge vlucht neemt zal het steeds moeilijker worden om overheidsorganisaties te verplichten om uitsluitend van de gesloten Rijkscloud gebruik te maken. Wij verwachten dat commerciële cloudleveranciers zullen proberen om op kosten, gemak, snelheid en gebruikersvriendelijkheid met de gesloten rijkscloud te concurreren. En vanwege de decentrale structuur van de Nederlandse overheid zullen sommige organisatieonderdelen voor de commerciële diensten kiezen.