Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Whitepaper NCSC

Cloudcomputing & security

Whitepaper NCSC

Cloudcomputing & Security

Nationaal Cyber Security Centrum

Wilhelmina van Pruisenweg 104 | 2595 AN Den Haag
Postbus 117 | 2501 CC Den Haag

T 070-888 75 55
F 070-888 75 50

E info@ncsc.nl
I www.ncsc.nl

Januari 2012

Nationaal Cyber Security Centrum

Het Nationaal Cyber Security Centrum (NCSC) draagt via samenwerking tussen bedrijfsleven, overheid en wetenschap bij aan het vergroten van de weerbaarheid van de Nederlandse samenleving in het digitale domein.

Het NCSC ondersteunt de Rijksoverheid en organisaties met een vitale functie in de samenleving met het geven van expertise en advies, response op dreigingen en het versterken van de crisisbeheersing. Daarnaast voorziet het in informatie en advies voor burger, overheid en bedrijfsleven ten behoeve van bewustwording en preventie.
Het NCSC is daarmee het centrale meld- en informatiepunt voor ICT-dreigingen en -veiligheidsincidenten.

INHOUDSOPGAVE

Hoofdstuk 4 > Beveiligingsaspecten van clouddiensten 25

Hoofdstuk 5 > Beveiligingsarchitectuur en -standaarden 35

HOOFDSTUK 1

Inleiding

1.1 Waarom een whitepaper over cloudcomputing en security?

Over cloudcomputing bestaat veel onduidelijkheid. Leveranciers van clouddiensten komen met zeer positieve voorbeelden over de mogelijkheden, terwijl er ook veel negatieve verhalen circuleren over de onzekerheden die cloudcomputing met zich meebrengt.

Deze whitepaper wil zo objectief mogelijk feitelijke informatie geven over cloudcomputing en mogelijke risico's ervan. Met andere woorden: als ik als organisatie kies voor 'cloudcomputing', hoe kan dat dan veilig, zijn er risico's voor de bedrijfsvoering en heeft deze keuze gevolgen voor de informatiebeveiliging van de organisatie? Bij het kiezen voor cloudcomputing draait het om een afweging van de voor- en nadelen en risico's. Het gaat over de impact op uw eigen bedrijfsvoering.

Deze whitepaper heeft tot doel om u te helpen een antwoord te formuleren op vragen over 'cloudcomputing'. Mogelijke vragen zijn:

- Wat is cloudcomputing en hoe 'doe' ik het veilig?
- Is cloudcomputing voor mijn organisatie interessant?
- Welke soorten informatie zijn geschikt voor 'de cloud'?
- Ik wil een bepaald proces of systeem migreren naar de cloud waar moet ik dan aan denken?
- Wat zijn de risico's van cloudcomputing en hoe weeg ik af of een risico acceptabel is?
- Hoeveel controle heb ik eigenlijk op het gebruik van de cloud door mijn werknemers en hoe ga ik daarmee om?

Een andere reden voor deze whitepaper houdt verband met de motie Van der Burg [1]. Als antwoord op deze motie werkt de Nederlandse overheid aan een Cloudcomputing Strategie en een Cloud First Strategie. Beide documenten brengen de mogelijkheden voor de inrichting van de overheidscloud in kaart, met de bijbehorende voor- en nadelen. Veel overheidsorganisaties zijn zich daarom aan het oriënteren op de cloud.

1.2 Voor wie is dit document bedoeld?

Dit document is bestemd voor adviseurs, informatiebeveiligingsfunctionarissen en architecten. Het kan als achtergrond-document en naslagwerk dienen, of als basis om een organisatie te informeren en adviseren over het gebruik van (toekomstige) clouddiensten.
Deze whitepaper bevat informatie over techniek, maar is niet overwegend technisch van aard. U hoeft als lezer dan ook niet te beschikken over specifieke technische kennis om deze whitepaper te kunnen lezen.

1.3 Leeswijzer

De whitepaper 'Cloudcomputing & Security' is zo opgebouwd, dat u ook middenin kunt beginnen, bijvoorbeeld bij hoofdstuk 4 'Beveiligingsaspecten van clouddiensten'.

Hoofdstuk 2 gaat in op de keuze voor een clouddienst en de afwegingen. Wordt u geconfronteerd met claims vanuit de markt, of vragen vanuit management of werknemers? Dan raden we u aan om te beginnen met hoofdstuk 2, waarin we de mogelijke keuze voor clouddiensten in een bredere context plaatsen.

Hoofdstuk 3 geeft definities van cloudcomputing, soorten clouddiensten en cloud-modellen.

Hoofdstuk 4 vormt (samen met Bijlage E: Handige vragen en aandachtspunten) de kern van het document, vanuit het perspectief van informatiebeveiliging en gaat in op de risico's van cloudcomputing en de te nemen maatregelen.

Hoofdstuk 5 geeft een overzicht van architectuurmodellen en standaarden die relevant zijn bij cloudcomputing.

Een overzicht van alle gebruikte afkortingen en termen staat in bijlage A. We hebben voor deze whitepaper een groot aantal literatuurbronnen geraadpleegd. Op plaatsen waar we informatie uit de literatuurbronnen verwerkt hebben, verwijzen we hiernaar in de vorm van '[x]'.
'[x]' verwijst naar een document opgenomen in bijlage B.

1.4 Totstandkoming en onderhoud

Dit document bevat de stand van zaken over cloudcomputing, gebaseerd op kennis en ervaring van het NCSC. In een vroeg stadium hebben wij, via een workshop, input gevraagd vanuit diverse onderdelen van de Nederlandse overheid, om zo goed mogelijk aan te sluiten bij vragen die in de praktijk leven.

Daarnaast is op regelmatige basis contact geweest met de programmamanager die verantwoordelijk is voor het beantwoorden van de motie Van der Burg c.s.

Dit document is niet uitputtend en zal het NCSC met regelmaat bijwerken. Het eerstvolgende moment is de publicatie van de Cloudcomputing - en Cloud First Strategie voor de Nederlandse overheid.

Aanvullingen, opmerkingen of eigen ervaringen ontvangen wij graag via info@ncsc.nl.

NOOT: Als dit document de naam van een product, dienst, fabrikant of leverancier noemt, betekent dit niet dat het NCSC deze op enige wijze goedkeurt, afkeurt, aanraadt, afraadt of op een andere manier hiermee verbonden is.

HOOFDSTUK 2

Waarom en hoe kies je voor Cloudcomputing?

Cloudcomputing[1] is 'hot', ook in overheidsland. Omdat dit zo is, kunt u als organisatie er niet omheen om u erin te verdiepen en een mening te vormen. Bijvoorbeeld over de mogelijkheden, de schaal- en efficiëntievoordelen. Maar vooral ook over de vraag over veiligheid en cloudcomputing.
Hoe doet u 'het' veilig, wat zijn risico's en wat zijn daarin afwegingen?
En wat doet u als u werknemers met de cloud willen werken of dat al doen, terwijl de organisatie hier zelf nog geen beleid voor heeft. Wat zijn goede argumenten en afwegingen?

Deze whitepaper is geschreven om bovenstaande vragen te beantwoorden. We willen daarin objectief zijn en onze focus is steeds ICT-beveiliging. Als u voor een clouddienst kiest, zijn daar dan beveiligings-risico's aan verbonden en hoe weegt u die af?

In hoofdstuk 2 gaan we in op de achterliggende motieven om voor cloudcomputing te kiezen.

2.1 Business drivers

Cloudcomputing is vaak een wens van het management of van medewerkers. Zij hebben hun eigen *business drivers*, redenen en motieven om als organisatie in de cloud te stappen. De business drivers (drijfveer) voor het management zijn:

- Voldoen aan wet- en regelgeving (compliance);
- Verhogen van het beveiligingsniveau;
- Kostenbesparing (op ICT);
- Concentreren op kernactiviteiten;
- Verhogen van de productiviteit.

Specifiek voor de overheid spelen de Cloudcomputing Strategie en Cloud First Strategie een rol. Deze strategieën kunnen voor de overheid belangrijke business drivers bevatten. Medewerkers hebben vooral behoefte aan gebruikersgemak (business driver '*convenience*').

In paragraaf 2.1 gaan we kort in op business drivers en de relatie met clouddiensten. Vanwege onze focus op informatiebeveiliging is dit niet meer dan een korte beschrijving van de meest voorkomende situaties.

Business Drivers

Business drivers vanuit management:

A. Cloudstrategieën;
B. Voldoen aan wet- en regelgeving;
C. Verhogen van het beveiligingsniveau;
D. Kostenbesparing (op ICT)
   - Schaalvoordeel;
   - Onderhouden kennisniveau;
E. Focus op kernactiviteiten;
F. Productiviteitsverhoging
   - Standaardisatie.

Business driver vanuit medewerkers:

A. Gebruikersgemak.

Deze business drivers zijn vrij algemeen en daarom ook constant. Het enige dat in de loop van de tijd verandert is de invulling van de business drivers. Het is dan ook uw taak om voor deze veranderende invulling steeds de risico's[2] helder in kaart te brengen, zodat u een goed onderbouwd advies kunt geven aan uw organisatie op basis van een juiste (risico)afweging.
Kortom, voor u en uw organisatie zou dit *business as usual* moeten zijn.

2.1.1 Business drivers van het management

In deze paragraaf gaan we kort in op business drivers van het management.

A. Cloudstrategieën: de Cloudcomputing Strategie en Cloud First Strategie

Naar aanleiding van de motie Van der Burg (zie kader 'Motie Van der Burg c.s.') is een 'Cloudcomputing Strategie' en 'Cloud First Strategie' - een '*comply or explain* strategie' (zie kader 'Comply or explain strategie') - geformuleerd voor de hele overheid.

Motie Van der Burg c.s. [1]

Motie Van der Burg c.s. inzake Cloudcomputing en Cloud First Strategie:

- Verzoekt de regering in navolging van landen als Japan, het Verenigd Koninkrijk en de Verenigde Staten een strategie voor de hele Nederlandse overheid te ontwikkelen voor Cloudcomputing en een Cloud First Strategie waarbij mogelijkheden voor de inrichting van de overheidscloud duidelijk omschreven worden met de bijbehorende voor- en nadelen;
- Verzoekt deze strategie voor 1 november 2010 aan de Tweede Kamer aan te bieden.

Overwegingen:

- Dat er de afgelopen jaren belangrijke ontwikkelingen zijn geweest inzake het aanbod van ICT-toepassingen waarbij gebruik werd gemaakt van het internet, dit wordt in vaktermen als cloudcomputing aangeduid;
- Dat door deze ontwikkelingen de dienstverlening aan burgers en bedrijven en de bedrijfsvoering van de overheid verbetert, de kosten voor het gebruik van IT flink omlaag kunnen en het duurzame gebruik van IT wordt gestimuleerd;
- Dat over de veiligheidsrisico's en mogelijke afhankelijkheidsrisico's die mogelijk samenhangen met deze ontwikkelingen geen onduidelijkheid mag bestaan.

1. Voor een definitie van de cloud, zie hoofdstuk 3. U kunt dit hoofdstuk lezen zonder deze definitie te kennen.
2. In hoofdstuk 4 wordt ingegaan op de beveiligingsaspecten van clouddiensten.

Het dwingt organisaties om goed naar informatievoorziening en bedrijfsprocessen te kijken. Een strategie kan kaders stellen, keuzes maken en richting geven, maar kan u uiteindelijk geen inzicht geven in de specifieke doelstellingen van uw organisatie. Uw organisatie moet zelf de organisatiedoelstellingen formuleren (bijv. Wat zijn de resultaten die we willen bereiken?). Deze doelstellingen moeten worden uitgewerkt in scenario's, maatregelen en/of verbeteracties waarmee concreet wordt uitgewerkt wat uw organisatie gaat doen en welke eisen hieraan worden gesteld om de voorgenomen resultaten te gaan bereiken. Denk hierbij aan het opstellen van een applicatie- en informatiearchitectuur.

Op 20 april 2011 heeft de minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK), de tweede Kamer geïnformeerd over een cloud computing strategie en een cloud first strategie als reactie op de motie [2]. De conclusie is dat cloudcomputing voor de overheid op dit moment nog te onvolwassen is. Deze conclusie is de uitkomst van een verkenning die eind 2010 en begin 2011 is uitgevoerd. Uit deze verkenning is naar voren gekomen dat er mogelijkheden zijn voor de inzet van cloudcomputing binnen het Rijk, maar dat de argumenten tegen het toepassen van open[3] cloud computing op dit moment globaal zwaarder wegen dan de voordelen. Deze argumenten hebben te maken met de onvolwassenheid van de markt en de eisen die worden gesteld aan de informatiebeveiliging.

Het aantal leveranciers en clouddiensten is vrij groot, maar slechts een klein deel daarvan is bedrijfsmatig volwassen genoeg om daadwerkelijk ingezet te kunnen worden voor de Nederlandse overheid.

Wat informatiebeveiliging betreft blijkt dat het via een 'open' cloud uitbesteden van ICT diensten, dan wel opslag van informatie buiten Nederland, risico's met zich meebrengt die nog niet voldoende kunnen worden afgedekt.

Het kabinet kiest er daarom voor een gesloten Rijkscloud 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, zoals aangekondigd in het Uitvoeringsprogramma Compacte Rijksdienst [3].

'Comply or explain strategie'
De comply or explain- strategie houdt in dat organisaties bij aanschaf van een clouddienst of -product, kiezen voor een cloudoplossing op basis van het 'pas toe of leg uit'-principe of anders geformuleerd 'cloud tenzij'. Als dat tot onoverkomelijke problemen leidt, mag de organisatie ervoor kiezen om een cloudoplossing niet te gebruiken. In zo'n geval moet gebruik worden gemaakt van de 'leg uit'-optie.

Het gaat dan bijvoorbeeld om een of meerdere van de volgende situaties:
- Als een clouddienst of -product naar verwachting onvoldoende zal worden aangeboden;
- Als een clouddienst of -product naar verwachting niet veilig of zeker genoeg zal functioneren. De bedrijfsvoering en/of dienstverlening, inclusief beveiligingsrisico's, komen daardoor onverantwoord in gevaar;
- Bij andere redenen van bijzonder gewicht. Het gaat hierbij bijvoorbeeld om aspecten van geld, tijd en capaciteit.

B. Voldoen aan wet- en regelgeving (compliance)
Elke organisatie en zeker een overheidsorganisatie, moet voldoen aan relevante wet- en regelgeving, ook als uw organisatie gebruik maakt van clouddiensten. Voorbeelden hiervan zijn:
- Wet Bescherming Persoonsgegevens (Wbp);
- Voorschrijft Informatiebeveiliging Rijksdienst (Vir);
- Voorschrijft Informatiebeveiliging Rijksdienst - Bijzondere Informatie (Vir-bi)
- Archiefwet;
- Wet veiligheidsonderzoeken;
- Telecommunicatiewet;
- Wetsvoorstel Computercriminaliteit (WCC);
- Wet Openbaarheid Bestuur (WOB);
- Wet Elektronisch Bestuurlijk Verkeer.

Gebruik maken van clouddiensten kan diep ingrijpen op de informatiehuishouding van uw organisatie. Daarom hebben we het als apart risico benoemd in hoofdstuk 4 'Beveiligingsaspecten van clouddiensten'.

C. Verhogen van het beveiligingsniveau
Deze business driver hangt nauw samen met de volgende twee business drivers: kostenbesparing en focus op kernactiviteiten.

3. Met 'open' cloud wordt een publieke cloud bedoeld en met 'gesloten' cloud wordt een privé cloud bedoeld.

Organisaties moeten continue bezig zijn om het beveiligingsniveau van hun organisatie op het gewenste niveau te houden. Het gewenste niveau is voor ieder bedrijf of orgaan verschillend, maar moet vastgesteld zijn op basis een risicoafweging (zie paragraaf 2.4 'Risicoafweging').
Om nu het vastgestelde beveiligingsniveau te garanderen moeten organisaties maatregelen implementeren en deze maatregelen monitoren op effectiviteit. Relevante vragen hierbij zijn: welke procedures zijn er en hoe zijn deze vastgelegd, vinden er audits plaats en is elke activiteit te traceren? Dit vraagt om specifieke (ICT-)kennis en vaardigheden, die niet altijd bij organisaties beschikbaar zijn.

U mag veronderstellen dat de cloudleverancier de procedures en processen rondom informatiebeveiliging efficiënt en effectief heeft geïmplementeerd, omdat de cloudleverancier kennis heeft van zijn cloudproducten en -diensten. De cloudleveranciers blijven in beveiliging investeren omdat het onderdeel is van hun kernactiviteiten. De kosten zijn vervolgens te verdelen over al hun klanten, waardoor u tegen een relatief lage prijs beschermd bent. De cloudleverancier kan zich ook geen slechte publiciteit veroorloven, omdat dit meteen marktaandeel kost.

Kortom het kost uw organisatie veel inspanningen en vereist specifieke kennis om het gewenste beveiligingsniveau te waarborgen. Door deze activiteiten nu onder te brengen bij een derde partij bespaart u kosten, kunt u zich richten op uw kernactiviteiten en wordt het beveiligingsniveau verhoogd.

D. Kostenbesparing
Clouddiensten zorgen voor lagere personeelskosten en minder kosten voor de infrastructuur, zo wordt vaak gedacht. Dat is echter te simpel gedacht, u kunt nooit het complete ICT-personeelsbestand afstoten. Bepaalde functies blijven nodig, afhankelijk van de exacte implementatievorm. Denk hierbij aan functioneel en technisch (applicatie)beheer en eerste- en tweedelijns support. Ook worden, afhankelijk van het type cloud (zie hoofdstuk 3 voor een beschrijving van cloudcomputing), juist nieuwe functies geïntroduceerd zoals cloudbeheer.

Daarnaast zie je dat functies veranderen. Er is minder behoefte aan operationele functies en meer aan tactische functies (de aansturing). Dit heeft twee gevolgen:
- Medewerkers hebben omscholing nodig;
- Er moet ander gekwalificeerd personeel geworven worden.

Ook voor de Nederlandse overheid is cloudcomputing een maatregel om kosten te besparen, zie het kader 'Brede heroverwegingen'.

Brede heroverwegingen
Op 1 april 2010 zijn de rapporten 'Brede heroverwegingen' aan de Tweede Kamer aangeboden [4]. Op 20 beleidsterreinen zijn beleidsvarianten met besparingsmogelijkheden geïnventariseerd.

Deze brede heroverwegingen zijn op Prinsjesdag 2009 bij de presentatie van de rijksbegroting voor 2010 aangekondigd. Als gevolg van de financiële en economische crisis zijn de overheidsfinanciën zoveel slechter geworden dat fundamentele keuzes voor de toekomst noodzakelijk zijn. Doel van de brede heroverwegingen is om politieke besluitvorming zo goed mogelijk voor te bereiden en onderbouwde keuzes mogelijk te maken over de omvang en het niveau van de collectieve voorzieningen. Het is aan de politiek en aan het volgende kabinet om deze keuzes te maken.

In rapport nr. 19, het beleidsterrein bedrijfsvoering (inclusief ZBO's) waar ook ICT onder valt, staat het volgende met betrekking tot mogelijke ICT bezuinigingsmaatregelen:
- Alle kantoorapplicaties van alle rijkswerkplekken (170.000) worden gebaseerd op 'cloud' applicaties;
- Als doorontwikkeling van de digitale werkplek rijk[4] (DWR) wordt structureel gebruikgemaakt van kantoorapplicaties vanuit een (rijks en/of overheids) 'cloud'. Het gaat dan om het combineren van interoperabiliteit en het gebruik van open standaarden en open source in het DWR-domein. Hierdoor kan sterk worden bespaard op licentie-, beheer- en hardwarekosten.

E. Focus op kernactiviteiten
Een andere driver om de dienstenverlening in de cloud onder te brengen is de trend waarbij veel organisaties zich meer gaan concentreren op hun kerntaken om daarmee flexibeler te kunnen reageren op vragen van hun klanten.

F. Productiviteitsverhoging
De laatste business driver van het management die we hier noemen is productiviteitsverhoging, indirect ook een vorm van kostenbesparing.

De productiviteit kun je als organisatie verhogen door te standaardiseren en door het gebruikersgemak voor medewerkers te verhogen.
Standaardiseren biedt een aantal voordelen, zoals:
- Het verhogen van de interoperabiliteit [5] en de portabiliteit[6];
- Een efficiëntere en effectievere werkwijze;
- Betere vergelijkingsmogelijkheden (benchmarking);
- Mogelijkheid tot certificering;
- Verbetering van communicatie door het hanteren van dezelfde definities en begrippen.

4. Ook omschreven als 'digitale werkomgeving Rijksdienst'.
5. Interoperabiliteit = uitwisselbaarheid tussen verschillende omgevingen.
6. Portabiliteit = herbruikbaarheid bij het veranderen van omgeving.

2.1.2 Business drivers van medewerkers

Medewerkers willen vooral gewoon goed hun werk doen, met zoveel mogelijk gebruikersgemak en waar en wanneer zij dat willen. Bepaalde cloudtoepassingen zijn daarom voor de gebruiker erg aantrekkelijk. Voor een cloudtoepassing hoef je niks te installeren: de drempel is dus laag. De kans is groot dat binnen uw organisatie al met de cloud gewerkt wordt, ook al is uw organisatie er 'officieel' nog niet aan toe of is hiervoor nog geen beleid opgesteld.

Een clouddienst als Google Docs[7] voor het maken van documenten, spreadsheets en presentaties sluit aan op wat veel medewerkers willen. Ze kunnen hiermee online document maken en er altijd, vanaf een willekeurige plek bij. Ook kunnen ze met Google Docs heel gemakkelijk documenten delen of samen bewerken.

Andere cloudtoepassingen, zoals Twitter[8] of sociale netwerken als LinkedIn[9] of Hyves[10], zijn niet meer weg te denken en steeds vaker onderdeel van de interne (informele) communicatie. Ook binnen de Rijksoverheid zijn veel ambtenaren actief op het web 2.0, veelal privé, soms zakelijk en vaak op het snijvlak van privé en zakelijk. Voor de Rijksambtenaren heeft de Voorlichtingsraad (VoRa) en het Secretaris Generaal Overleg (SGO) dan ook de 'Uitgangspunten Online communicatie rijksambtenaren' [5] vastgesteld.

Het is goed mogelijk dat bepaalde processen of informatie niet geschikt zijn voor cloudtoepassingen in uw organisatie, in paragraaf 2.4 wordt een uitleg gegeven hoe u dit op basis van een risicoafweging voor uw organisatie bepaalt. Maak dit duidelijk en bespreek het met u medewerkers, zodat zij hiervoor begrip kunnen hebben en de grenzen duidelijk zijn.

2.2 Kiezen voor cloudcomputing

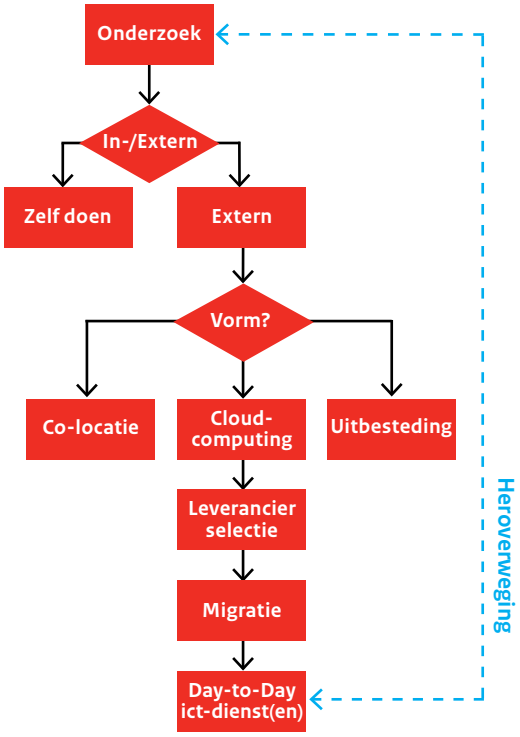
Hoe bepaalt u of cloudcomputing geschikt is voor uw organisatie? Dat kan via een haalbaarheidsonderzoek (zie figuur 2-1).

Twee factoren zijn van cruciaal belang om de (mogelijke) vorm van ICT-dienstverlening voor uw organisatie vast te stellen:

- Schaalvoordeel/schaalbaarheid (*economies of scale*); heeft schaalvergroting voordelen?
- Opleidings- en ontwikkelkosten; om de kennis van de medewerkers van uw organisatie op niveau te houden is investeren noodzakelijk (*economies of skill*).

De uitkomst van het onderzoek kan zijn:

- De ICT in huis houden (doe het zelf);
- Co-locatie;
- Uitbesteding;
- Cloudcomputing.



Figuur 2-1: Besluitvorming, migratie en uitvoeringstraject

Om een gedegen beslissing te kunnen nemen, gebaseerd op een goede business case, moet u bij deze afweging ook in kaart brengen wat de impact is op uw bedrijfs- en beheerprocessen. Om het uiteindelijke transitie- en migratieproces voor uw organisatie zo soepel mogelijk te laten verlopen, moet u de wijzigingen op uw processen in kaart brengen en het verandertraject starten voordat met de migratie van uw ICT-dienstverlening kan worden gestart.

2.2.1 Zelf doen (ICT in eigen beheer)

Kunt u weinig schaalvoordeel halen en zijn ICT-opleidingskosten laag? Dan kiest u er waarschijnlijk voor om uw ICT in huis te houden.

2.2.2 Co-locatie

Kunt u schaalvoordeel halen (dit is vaak het geval bij standaarddiensten) en zijn de ICT-opleidingskosten laag dan is co-locatie een passende optie. Kennis en deskundigheid blijven in uw organisatie en de hard- en software wordt bij een externe partij ondergebracht.

Co-locatie biedt meestal diensten als een beveiligd datacenter, back-up/restore, hogere beschikbaarheid voor zowel netwerk als servers, airconditioning, brandblusinstallatie, noodstroomvoorzieningen, etc.

7. https://docs.google.com
8. http://twitter.com/
9. http://www.linkedin.com/home
10. http://hyves.nl/

De kosten worden onder andere vastgesteld op basis van de afgenomen diensten en het aantal servers (benodigde rack-space) die worden ondergebracht bij de externe leverancier, de hoeveelheid dataverkeer, etc. De medewerkers die het server-park beheren blijven in dienst van uw eigen organisatie.

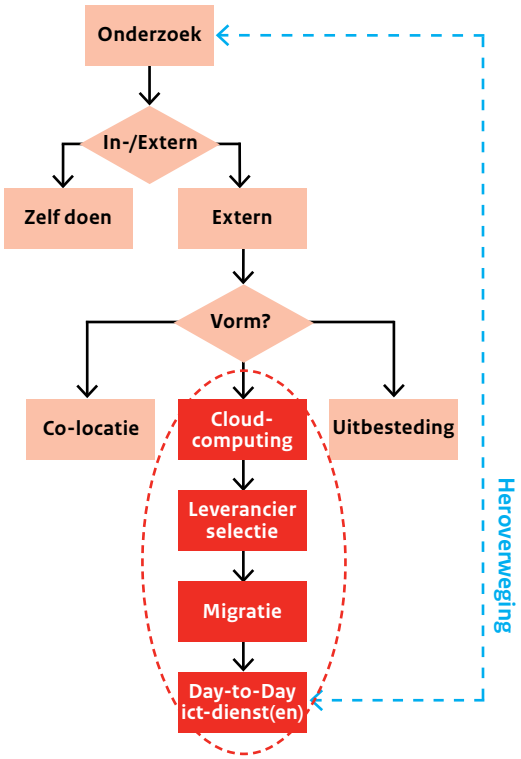
2.2.3 Uitbesteding

Uitbesteden is een optie bij weinig schaalvoordeel en hoge(re) opleidingskosten. Uitbesteden betekent dat uw organisatie het serverpark buitenshuis plaatst inclusief de bijbehorende dienstverlening. Denk hierbij aan ICT-dienstverlening, callcenterdiensten en salarisadministratie.

2.2.4 Cloudcomputing

Als u schaalvoordeel kunt behalen en de opleidingskosten hoog zijn, dan kunt u kiezen voor cloudcomputing.

Dit document focust - het zal u niet verbazen - op 'veilig cloudcomputen' als uitkomst van het onderzoek, zie de omcirkelde activiteiten in figuur 2-2. Op de andere activiteiten gaan we niet verder in.



Figuur 2-2: Focus op Cloudcomputing

2.3 Eisen stellen aan de dienstverlening

Het is belangrijk om vast te stellen aan welke eisen de dienstverlening die 'cloudcomputing' heet, moet voldoen. In deze paragraaf gaan we in op twee hulpmiddelen van de The Open Group Cloud Work Group[11]: de 'Cloud Buyers' Requirements Questionnaire' [6] en de 'Cloud Buyers' Decision Tree' [7].

De 'Cloud Buyers' Requirements Questionnaire' helpt u om de eisen van uw organisatie gestructureerd te identificeren, zonder dat u over specifieke kennis van cloudcomputing hoeft te beschikken voor het beantwoorden van de vragen. De vragen uit deze questionnaire zijn verdeeld in de volgende categorieën:

- Probleemdefinitie en doelstelling die u hiermee wil bereiken (bedrijfssituatie);
- Beschrijving van de context, omgevingsfactoren, voor uw bedrijfssituatie;
- Beschrijving van de bedrijfsprocessen met daarbij de belangrijkheid voor uw organisatie vermeld;
- Beschrijving van het marktsegment waarin uw organisatie opereert; Beschrijving van de financiële doelstelling en de contract- en leveringsvoorwaarden voor de oplossing;
- Beschrijving van de verschillende aspecten van Quality of Service (QoS);
- Beschrijving van de functionele karakteristieken met betrekking tot de workload;

De 'Cloud Buyers' Decision Tree' helpt u om vast te stellen waar cloudcomputing binnen uw organisatie van toepassing kan zijn.

2.4 Risicoafweging

Kiezen voor een andere vorm van ICT-dienstverlening, betekent niet in de laatste plaats dat je als organisatie de risico's in kaart brengt en afweegt. Wat zijn de risico's, zijn ze aanvaardbaar of juist niet en hoe weeg je ze af tegen de voordelen van kostenbesparing, focus op kernactiviteiten, productiviteitsverhoging en gebruikersgemak.

Het correct inschatten van mogelijke risico's vormt de kern van deze whitepaper. Vanuit onze focus op informatiebeveiliging zijn de risico's het allerbelangrijkst in de 'cloudafweging' en daarom besteden we er veel aandacht aan. In het hoofdstuk 4 gaan we uitgebreid in op de belangrijkste beveiligingsaspecten die een organisatie in overweging moet nemen bij het kiezen van een clouddienst.

De keuze voor een bepaald type cloudmodel (privaat, publiek, community of hybride) en de soort clouddienst (SaaS, PaaS of IaaS) zijn van invloed op welke aandachts-punten specifiek van toepassing zijn op uw organisatie. In 'Bijlage E: Handige vragen en aandachtspunten' vindt u een lijst met punten aan de hand waarvan u kunt inschatten welke maatregelen u daar tegenover kunt zetten.

11. The Open Group Cloud Work Group heeft als doel een gemeenschappelijke visie te creëren voor cloudgebruikers en -leveranciers waardoor cloudcomputing op een veilige en beveiligde manier in hun architectuur kan worden geïntegreerd, zodat optimaal kan worden geprofiteerd van de voordelen zoals kostenverlaging, schaalbaarheid en flexibiliteit.

Dit document gebruikt de volgende, breed geaccepteerde definitie van risico: 'Risico is het product van de kans op optreden van een ongewenste gebeurtenis en de schade als gevolg van deze ongewenste gebeurtenis', of kortweg:

risico = kans x schade

Figuur 2-3: Illustreert de definitie met een matrix die drie risiconiveaus onderscheidt: hoog risico (kwadrant I), gemiddeld risico (kwadranten II en IV) en laag risico (kwadrant III).

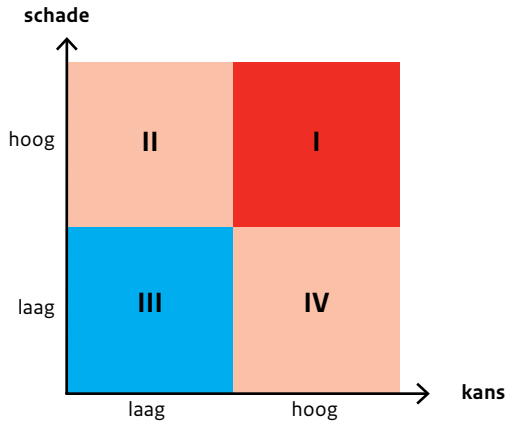
Elke maatregel uit deze whitepaper heeft tot doel om het risico met betrekking tot cloudcomputing te verlagen. Dit kan worden gerealiseerd door de kans op een ongewenste gebeurtenis te verminderen, de schade die door een ongewenste gebeurtenis ontstaat te verminderen of beide.

2.4.1 Inschatting van kans

Statistische gegevens over ongewenste gebeurtenissen binnen de ICT, en zeker op het gebied van clouddiensten, zijn er niet of zijn slechts erg beperkt.

Als gevolg daarvan is het inschatten van de kans op een bepaalde gebeurtenis erg lastig en heeft het meer weg van een kunst dan een wetenschap. Incidenten die de media halen, eigen kennis en gezond verstand helpen om een inschatting te kunnen maken.

De kans dat ongewenste gebeurtenissen plaatsvinden op het gebied van cloudcomputing is uiteraard afhankelijk van het soort clouddienst en het soort cloudmodel.



2.4.2 Verschillende soorten schade

Ongewenste gebeurtenissen veroorzaken meestal schade. De belangrijkste soorten schade zijn politieke of imagoschade, financiële schade, juridische schade en operationele schade.

Politieke of imagoschade

Politieke of imagoschade is voor overheden misschien wel de belangrijkste soort schade, aangezien dit onder andere kan leiden tot verminderd vertrouwen. Dit type schade is moeilijk te voorspellen. Soms kan een incident objectief gezien (qua duur, of financiële omvang) klein zijn, maar de imagoschade onverwacht groot vanwege de timing of relatie met andere incidenten.

Financiële schade

Financiële schade als gevolg van diefstal van vertrouwelijke informatie die in de cloud is opgeslagen is reëel. Wanneer een gebruiker bijvoorbeeld creditcardgegevens of wachtwoorden in de cloud onbeveiligd opslaat kan een kwaadwillende deze gegevens eenvoudig in zijn (financiële) voordeel misbruiken.

Juridische schade

Wanneer gegevens op straat komen te liggen door toedoen van werknemers of de cloudleverancier, kan de aansprakelijkheid hiervoor belanden bij u als werkgever als u niet voldoende maatregelen heeft getroffen.

Operationele schade

Wanneer een gebruiker of organisatie zeer afhankelijk is van de dienstverlening in de cloud, kan dit bij een ongewenste gebeurtenis leiden tot productiviteitsverlies en operationele schade.

2.5 Dataclassificatie

Om vast te stellen welke data in de cloud geplaatst kan/mag worden, moet wel bekend zijn over welke data de organisatie beschikt en welke betrouwbaarheidseisen[12] daar aan zijn gesteld. Deze betrouwbaarheidseisen kunnen op basis van de risicoafweging uit paragraaf 2.4 worden bepaald. Vervolgens moet er op basis van de toegekende BIV-classificatie vastgesteld worden welke data wel en welke niet in de cloud geplaatst mogen worden. Om deze BIV-classificaties eenduidig te kunnen bepalen moet de organisatie over heldere richtlijnen beschikken.
Het vervolg van deze paragraaf licht de drie belangrijkste richtlijnen toe:

1. Wbp. De belangrijkste regels voor de omgang met persoonsgegevens zijn vastgelegd in de Wet bescherming persoonsgegevens (Wbp) [8].
2. Vir-bi. Met betrekking tot vertrouwelijkheid geldt voor de Rijksdienst het voorschrift informatiebeveiliging rijksdienst - bijzondere informatie (Vir-bi) [9].
3. ISO 27002. Een andere belangrijke standaard die binnen Nederland veelvuldig wordt gehanteerd is de ISO 27002 'Code voor informatiebeveiliging' [10].

12. Onder de betrouwbaarheidseisen worden beschikbaarheid, integriteit en vertrouwelijkheid verstaan, vaak afgekort met BIV.

2.5.1 Wet bescherming persoonsgegevens (Wbp)

Zeer veel instanties verzamelen, verwerken en wisselen persoonsgegevens en informatie over personen uit De belangrijkste regels voor de omgang met persoonsgegevens zijn vastgelegd in de Wet bescherming persoonsgegevens (Wbp). De Wbp is de Nederlandse uitwerking van de Europese richtlijn bescherming persoonsgegevens [11], zie kader herziening Europese Privacyrichtlijn, en is sinds 1 september 2001 van kracht.

Herziening Europese Privacyrichtlijn

Op 4 november 2010 is een herziene versie van de Europese Privacyrichtlijn[13] getiteld 'Een integrale aanpak van de bescherming van persoonsgegevens in de Europese Unie' [12] gepubliceerd. In deze mededeling constateert de Europese Commissie dat de Europese regelgeving op het gebied van dataprotectie toe is aan modernisering. Dit is het gevolg van de globalisering en nieuwe technologische ontwikkelingen, waarbij de Commissie onder meer denkt aan fenomenen als cloudcomputing en sociale netwerksites (bijvoorbeeld Hyves en Facebook[14]).

De Wbp geeft via de Handreiking 'Achtergrond Studies en Verkenningen 23 (AV-23) [13] een methodiek aan voor het classificeren van persoonsgegevens, de risicoklasse. Deze risicoklasse wordt bepaald door de kans dat onzorgvuldig of onbevoegd gebruik zich voordoet en door de schade die daaruit voortvloeit. De uitkomst van een analyse bepaalt de risicoklasse en daarmee het vereiste niveau van maatregelen en procedures. Het College bescherming persoonsgegevens (CBP)[15] gaat daarbij uit van een indeling van persoonsgegevens in vier risicoklassen.
De opbouw van de risicoklassen is cumulatief: hogere klassen geven additionele normen aan die passen bij die hogere risicoklasse:

- risicoklasse 0 publiek niveau;
- risicoklasse I basis niveau;
- risicoklasse II verhoogd risico;
- risicoklasse III hoog risico.

De verantwoordelijke komt tot een afweging in welke risicoklasse de gegevens vallen.

Richtsnoeren

In richtsnoeren geeft het CBP op deelgebieden aan welke uitleg van wettelijke voorschriften het CBP in zijn handhavingspraktijk hanteert. Twee richtsnoeren zijn relevant in verband met cloudcomputing en de overheid, dit zijn (zie Bijlage I: Relevante artikelen Wbp en Richtsnoeren):

- Richtsnoeren 'publicatie van persoonsgegevens op internet' [14]. Iedereen die persoonsgegevens publiceert is zélf verantwoordelijk voor de naleving van de wet en moeten dus zelf voorafgaand aan de publicatie beoordelen of dat wel is toegestaan, en zo ja, aan welke voorwaarden zij daarbij moeten voldoen. Met deze richtsnoeren wil het College bescherming persoonsgegevens het eenvoudiger maken dat te beoordelen. Dat is in het belang van degenen die op internet publiceren en in het belang van de mensen over wie (mogelijk) gegevens worden gepubliceerd.
- Richtsnoeren 'Actieve openbaarmaking en eerbiediging van de persoonlijke levenssfeer' [15].Deze nieuwe richtsnoeren vormen een aanvulling op de vorige Richtsnoeren. Zij behandelen uitsluitend de situatie, waarin het recht op openbaarheid van overheids-informatie en het recht op bescherming van persoons-gegevens samenkomen.

Ondanks het feit dat deze twee richtsnoeren niet specifiek voor cloudcomputing zijn opgesteld, geven ze wel kaders aan welke persoonsgegevens onder welke omstandigheden gepubliceerd mogen worden.

2.5.2 Voorschrift informatiebeveiliging rijksdienst - bijzondere informatie (Vir-bi)

Het Vir-bi geeft regels voor de beveiliging van bijzondere informatie bij de rijksdienst. Deze regels hebben als doel het aantal personen dat met bijzondere informatie in aanraking komt, zo beperkt mogelijk te houden. Daarnaast is het van belang dat zo spoedig mogelijk actie wordt ondernomen bij kennisname door niet gerechtigden (compromittering).

Voorschrift informatiebeveiliging rijksdienst - bijzondere informatie (Vir-bi)

Het Vir-bi [9] bevat regels, gericht op de bescherming van de vertrouwelijkheid. Het is een aanvulling op het Besluit voorschrift informatiebeveiliging rijksdienst 2007 (Vir) [16] waarin beveiliging van informatie in het algemeen binnen de Rijksdienst is geregeld. Dit betekent dat bij de beveiliging van bijzondere informatie zowel de regels van het Vir als die van het Vir-bi gevolgd moeten worden.

Informatiebeveiliging volgens het Vir richt zich op de bescherming van integriteit, vertrouwelijkheid en beschikbaarheid van de informatie. Het Vir schrijft voor dat het lijnmanagement op basis van een risicoanalyse de betrouwbaarheidseisen en de bijbehorende beveiligingsmaatregelen voor een informatiesysteem bepaalt.

13. Mededeling van de commissie aan het Europees Parlement, de raad, het Europees economisch en sociaal comité en het comité van de regio's [10].
14. http://www.facebook.com/
15. http://www.cbpweb.nl

Het Vir-bi gebruikt de term 'rubricering' in plaats van 'classificatie' en hier wordt het volgende onder verstaan: het vaststellen en aangeven dat een gegeven bijzondere informatie is en het bepalen en aangeven van de mate van beveiliging die aan deze informatie moet worden gegeven.

Het rubriceren kan worden opgesplitst in een aantal stappen. In de eerste plaats moet worden vastgesteld of informatie als staatsgeheim of als niet-staatsgeheime bijzondere informatie moet worden beschouwd. Er is sprake van een staatsgeheim als het belang van de Staat of zijn bondgenoten in het geding is en indien kennisname door niet-gerechtigden kan leiden tot schade aan deze belangen.

Er is sprake van niet-staatsgeheime bijzondere informatie indien kennisname door niet-gerechtigden kan leiden tot nadeel aan het belang van één of meer ministeries. Indien bij de schending van de geheimhouding het nadeel aan het belang van één of meer ministeries zo ernstig is, dat sprake is van schade, zal er doorgaans sprake zijn van schade aan de belangen van de Staat of van zijn bondgenoten en dus van een staatsgeheim.

In de tweede plaats moet de rubricering worden vastgesteld. De rubricering zelf, wordt bepaald door de mate van nadeel of schade die kan worden geleden, indien een niet gerechtigde kennis neemt van de informatie.

2.5.3 ISO 27002 'Code voor informatiebeveiliging'

Hoofdstuk 5 uit de ISO 27002 gaat over classificatie en beheer van bedrijfsmiddelen van uw organisatie. De maatregelen die in dit hoofdstuk worden weergegeven hebben een relatie met dataclassificatie, alleen is de reikwijdte breder dan alleen de data. Het gaat hierbij om alle bedrijfsmiddelen en beperkt zich niet alleen tot data. Maatregelen die worden aangegeven zijn:

- Alle bedrijfsmiddelen moeten geïdentificeerd zijn en er moeten een administratie van bijgehouden worden, bijv. in een Configuratiebeheer Database (Paragraaf 7.1.1 uit de ISO 27002 'Inventarisatie van bedrijfsmiddelen').
- Alle bedrijfsmiddelen moeten over een eigenaar beschikken (Paragraaf 7.1.2 uit de ISO 27002 'Eigendom van bedrijfsmiddelen')
- Er moeten regels worden opgesteld zodat op een acceptabele manier met de bedrijfsmiddelen wordt omgegaan (Paragraaf 7.1.3 uit de ISO 27002 'Aanvaardbaar gebruik van bedrijfsmiddelen')
- Informatie moet worden geclassificeerd in termen van waarde, wettelijke bepalingen, gevoeligheid en belangrijkheid voor de organisatie (Paragraaf 7.2.1 uit de ISO 27002 'Richtlijnen voor classificatie')
- Er moeten procedures worden opgesteld met betrekking tot het labelen en verwerken van informatie (Paragraaf 7.2.2 uit de ISO 27002, 'Labeling en verwerking van informatie')

ISO 27002

ISO 27002 'Code voor informatiebeveiliging' [10] geeft richtlijnen en principes voor het initiëren, het implementeren, het onderhouden en het verbeteren van informatiebeveiliging binnen een organisatie. ISO 27002 kan dienen als een praktische richtlijn voor het ontwerpen van veiligheidsstandaarden binnen een organisatie en is een effectieve methode voor het bereiken van deze veiligheid.

ISO 27002 staat vermeld op de lijst met open standaarden[16] waarvoor geldt dat (semi-)publieke organisaties het 'pas toe of leg uit'-principe[17] moeten volgen.

2.6 Assurance

Organisaties die, uiteraard op basis van een uitgevoerde risicoanalyse (paragraaf 2.4) en dataclassificatie (paragraaf 2.5), voor cloudcomputing kiezen, willen zekerheid over de kwaliteit van hun in de cloud geplaatste ICT en de dienstverlening. Deze zekerheid is niet alleen van belang voor de continuïteit en kwaliteit van de dienstverlening, maar ook vanwege de eisen die tegenwoordig worden gesteld aan transparantie, governance en het voldoen aan geldende wet- en regelgeving, standaarden, richtlijnen, gedragscodes en certificeringen.

Als u een overeenkomst bent aangegaan (bijvoorbeeld een contract of een SLA) met een cloudleverancier, dan wilt u zekerheid dat de cloudleverancier ook voldoet aan de afspraken die in deze overeenkomst zijn vastgelegd.
U wilt ook zekerheid over de afgenomen dienstverlening zodat u imagoschade, inkomstenderving en schadeclaims kunt voorkomen.

Het draait om het vertrouwen in de zich verantwoordende partij, in dit geval de cloudleverancier. Het antwoord op de vertrouwensvraag is assurance. Assurance is een veel gebruikt begrip met verschillende definities. In dit document verstaan wij onder assurance: monitoring van processen en producten, het objectief vaststellen of processen en producten voldoen aan normen en er op toe zien dat afwijkingen gestructureerd en gecontroleerd worden opgelost.

16. In de lijsten met open standaarden vindt u de open standaarden die zijn goedgekeurd door Forum en College Standaardisatie < http://www.open-standaarden.nl/>.
17. http://www.open-standaarden.nl/open-standaarden/het-pas-toe-of-leg-uit-principe/

HOOFDSTUK 3

Wat is ‘Cloudcomputing’?

In dit hoofdstuk leggen we uit wat wij onder ’cloudcomputing’ verstaan. Onze omschrijving is gebaseerd op de definitie van het National Institute of Standards and Technology (NIST) [17].

We kijken naar de belangrijkste eigenschappen van cloudcomputing, de verschillende typen clouddiensten en -modellen.

Eigenschappen
- Direct en op verzoek;
- Internettechnologie;
- Schaalbaar;
- Betalen voor gebruik;
- Gedeelde ICT-resources;
- Efficiënt met capaciteit.

Modellen
- Private cloud;
- Publieke cloud;
- Communitycloud;
- Hybride cloud.

Diensten
- Software;
- Platform;
- Infrastructuur.

3.1 De belangrijkste eigenschappen van cloudcomputing

3.1.1 Cloudcomputing biedt diensten direct aan

Clouddiensten kunt u als organisatie snel en eenvoudig afnemen en direct aan medewerkers en klanten aanbieden. De meeste clouddiensten kunt u direct online kopen, bijvoorbeeld met een creditcard. Ze zijn dan direct beschikbaar.

Google Docs
Google Docs biedt u de mogelijkheid om werk, zoals documenten, spreadsheets en presentaties, online te maken en delen met anderen. U kunt nieuwe documenten maken maar ook bestaande documenten uploaden. U geeft zelf aan met wie u deze documenten wil delen en samenwerken in realtime, zodat degene die u hebt uitgenodigd om uw document, spreadsheet of presentatie te bewerken of bekijken, dit kan doen zodra ze zijn aangemeld.

U hoeft niets te downloaden; u hebt toegang tot uw documenten, spreadsheets en presentaties vanaf elke computer met een internetverbinding en een standaard browser. Met de functies voor online opslag en automatisch opslaan hoeft u zich geen zorgen te maken over problemen met de lokale vaste schijf of stroomuitval. Natuurlijk hebt u ook de mogelijkheid om uw documenten en spreadsheets op uw eigen computer op te slaan.

U kunt uw bestanden als normale webpagina publiceren voor de hele wereld, een aantal mensen of niemand: u bepaalt het helemaal zelf. (U kunt de publicatie ook op elk moment weer ongedaan maken.)

Het gemak van cloudcomputing is ook aantrekkelijk voor individuele werknemers. Iemand die snel een document wil delen met anderen buiten of binnen de organisatie, zou daarvoor Google Docs kunnen gebruiken, zie kader 'Google Docs'.

3.1.2 Een clouddienst is toegankelijk via standaard technologieën

Clouddiensten zijn gebaseerd op standaard internettechnologieën. Dit heeft als voordeel dat ze overal en altijd (meestal via een internetbrowser) te gebruiken zijn, als er maar een internetverbinding is.

3.1.3 Een clouddienst is gemakkelijk schaalbaar

Een clouddienst speelt automatisch in op de vraag van een klant: ICT-resources (capaciteit) kunnen namelijk automatisch gemakkelijk 'opgeschaald' en afgebouwd worden.

Cloudcomputing levert dus maatwerk, omdat je als klant nooit te weinig of te veel capaciteit tot je beschikking hebt en dus ook nooit teveel betaalt. Voorbeelden van ICT-resources zijn reken- (CPU) en opslagcapaciteit. Schaalbaarheid is vooral interessant als uw behoefte aan de clouddienst sterke pieken heeft.

Voor het Rijksinstituut voor Volksgezondheid en Milieu (RIVM)[18] is cloudcomputing bijvoorbeeld interessant vanwege de schaalbaarheid. Het RIVM kan met cloudcomputing tijdelijk extra rekencapaciteit afnemen voor het doorrekenen van modellen.

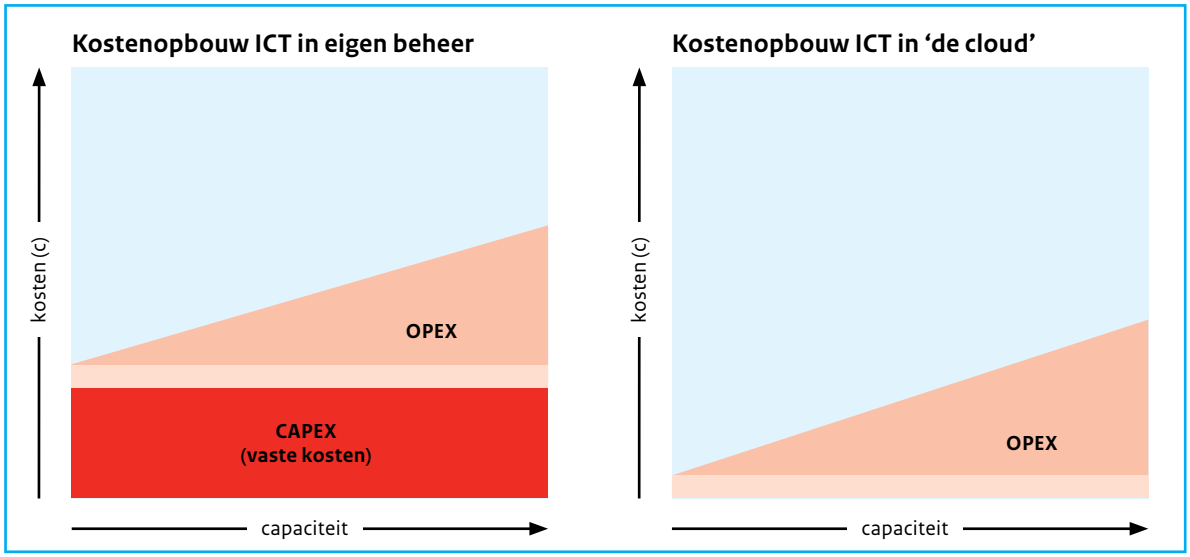
3.1.4 Bij een clouddienst betaalt u alleen voor gebruik

Bij een clouddienst, zeker bij de publieke cloud variant, betaalt u als gebruiker alleen voor het gebruik van ICT-resources (OPEX) en niet voor de aanschaf van de ICT-resources (CAPEX). De aanschafkosten van de ICT-resources zijn voor rekening van de cloudleverancier, althans bij een publieke cloud (zie paragraaf 3.3 voor de definitie van de verschillende cloudmodellen). Tabel 3-1 geeft een beschrijving van OPEX en CAPEX en figuur 3-1 laat het verschil in kosten zien.
Bij cloudcomputing vindt er een verschuiving plaats van CAPEX naar OPEX, grote financiële investeringen vooraf maken plaats voor minimale initiële investeringen en gespreide betalingen per maand of per jaar.

Definitie	Omschrijving
CAPEX (capital expenditure)	CAPEX zijn de (kapitaal)investeringen in ICT-resources zoals faciliteiten, software, computer- en netwerkapparatuur. Deze kosten zijn éénmalig tijdens de aanschaf van de (ICT-)middelen en worden meestal over een bepaalde periode afgeschreven. Uiteraard moeten deze ICT-middelen na een aantal jaren vervangen worden. Bij cloudcomputing zijn deze initiële investeringen voor u overbodig daar u gebruik maakt van de ICT-middelen van de cloudleverancier. Dit geldt overigens ook bij co-locatie en uitbesteding.
OPEX (operating expenditure)	OPEX(exploitatiekosten)zijndeoperationele kosten voor een product, systeem of dienst. Deze operationele uitgaven zijn terugkerende kosten voor leveranciers van uitbestede (cloud)diensten, personeelskosten en daaraan gerelateerde kosten. Kosten en capaciteit nemen bij cloudcomputing evenredig toe en af (betaal voor gebruik).

Tabel 3-1 CAPEX en OPEX

18. http://www.rivm.nl/



Figuur 3-1 Kostenopbouw ICT in eigen beheer vs. ICT in 'de cloud'

3.1.5 Bij een clouddienst worden ICT-resources gedeeld

ICT-resources van een cloudleverancier zijn gekoppeld, hierdoor beschikt niet iedere organisatie over zijn 'eigen' resources maar worden de resources met meerdere organisaties gelijktijdig gedeeld (in het Engels: *multi-tenancy*). Het gaat om resources als rekencapaciteit, opslag, geheugen, toepassingen, besturingssysteem, servers en het netwerk.

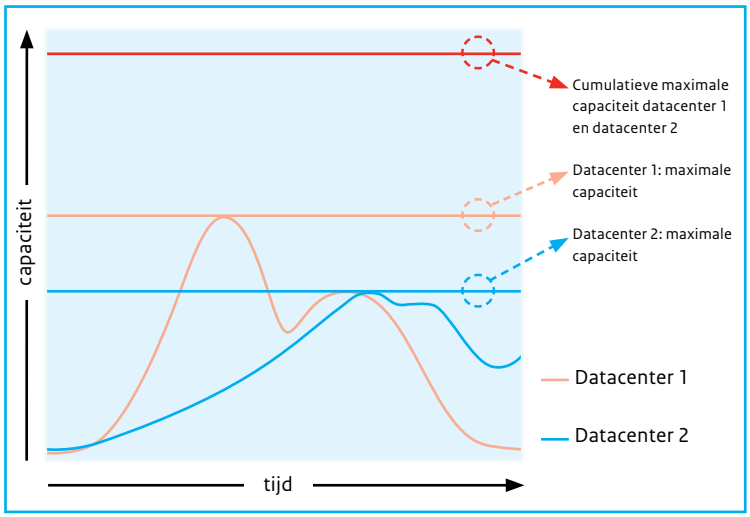
3.1.6 Een cloudleverancier gaat efficiënt met capaciteit om

Bij cloudcomputing worden ICT-resources gedeeld. Dat maakt niet alleen schaalbaarheid mogelijk, maar zorgt er ook voor dat een cloudleverancier efficiënt met zijn capaciteit omgaat. Dit levert tevens energiebesparing op. Een datacenter in de cloud kan namelijk efficiënter met capaciteit omgaan dan een datacenter in eigen beheer.

Een datacenter moet piekcapaciteit kunnen leveren en daarop ingericht zijn. In daluren staat vaak veel apparatuur 'niets' te doen. De capaciteit van het datacenter wordt dus niet efficiënt gebruikt. Figuur 3-2 toont de capaciteitsvraag van twee datacenters inclusief de cumulatieve piekbelasting. Tabel 3-2 licht figuur 3-2 toe met een rekenvoorbeeld.

Datacenter	Maximaal aantal servers i.v.m. piekbelasting	Opmerking
Datacenter 1	**10**	Datacenter 1 heeft continue 10 servers nodig om de piekbelasting op te vangen.
Datacenter 2	**7**	Datacenter 2 heeft continue 7 servers nodig om de piekbelasting op te vangen.
Som	**17**	De cumulatieve maximale capaciteit van Datacenter 1 plus Datacenter 2 is continue 17 servers.

Tabel 3-2 Rekenvoorbeeld afzonderlijke datacenters

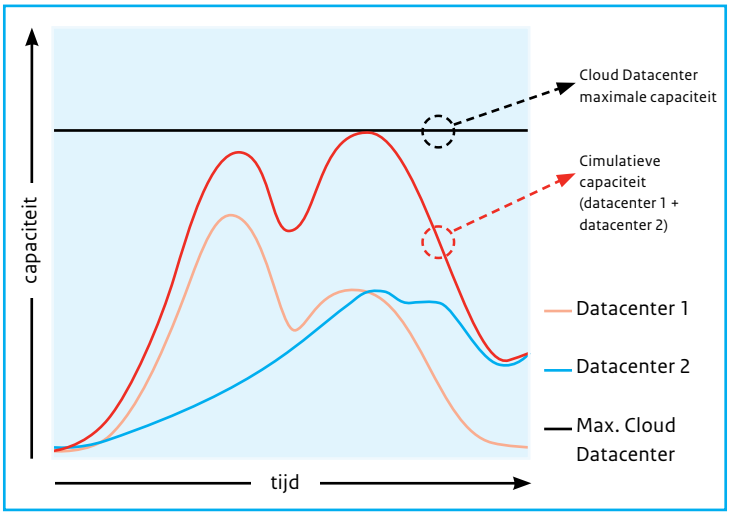


Figuur 3-2 Cumulatieve capaciteit voor twee afzonderlijke datacenters

Het datacenter in de cloud is vanwege de (grote) omvang en het delen van ICT-resources in staat om de wisselende capaciteitsvraag van verschillende organisaties gemakkelijk op te vangen.
Figuur 3-3 geeft de maximale piekbelasting weer op het moment dat de twee afzonderlijke datacenters uit figuur 3-2 zijn ondergebracht in één (cloud) datacenter. Tabel 3-3 licht figuur 3-3 toe met een rekenvoorbeeld.

Datacenter	Maximaal aantal servers i.v.m. piekbelasting	Opmerking
Datacenter 1	**10**	De maximale benodigde capaciteit van Datacenter 1 is 10 servers om de piek-belasting op te vangen.
Datacenter 2	**7**	De maximale benodigde capaciteit van Datacenter 2 is 7 servers om de piek-belasting op te vangen.
Cloud datacenter	**14**	Het maximaal aantal benodigde servers voor het datacenter in de cloud. *Toelichting:* *Daar de piekbelasting van Datacenter 1 en Datacenter 2 niet samenvallen, heeft het Cloud datacenter minder servers (capaciteit) dan de som van de twee afzonderlijke Datacenters (1 en 2). In dit voorbeeld komt het totaal aantal servers op 14 i.p.v. 17.*

Tabel 3-3 Rekenvoorbeeld cloud datacenter



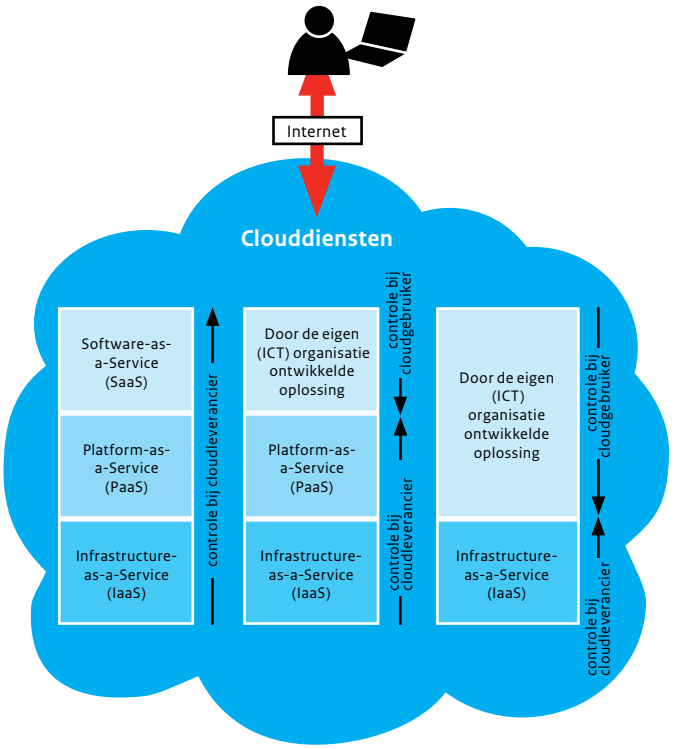
Figuur 3-3 Cumulatieve capaciteit voor cloud datacenter

3.2 Soorten Clouddiensten

Er zijn verschillende soorten clouddiensten. Van kant-en-klare toepassingen die u direct kunt gebruiken, tot omgevingen waarmee u zelf applicaties kunt ontwikkelen. Er zijn ruwweg drie soorten clouddiensten (zie figuur 3-4):

- *Software as a service (SaaS)*
  De software (applicatie) staat volledig onder controle van de cloudleverancier. De afnemer van deze clouddienst kan er gebruik van maken, maar kan er over het algemeen niets aan wijzigen.
- *Platform as a service (PaaS)*
  In deze laag wordt naast de ICT-infrastructuur, zoals servers, netwerken en opslagcapaciteit, ook het besturingssysteem, databasemanagement en ontwikkeltools aangeboden. Dit geeft de afnemer van deze clouddienst de vrijheid om eigen systemen en diensten te ontwikkelen.
- *Infrastructure as a service (IaaS)*
  In deze laag wordt alleen de ICT-infrastructuur, zoals servers, netwerken en opslagcapaciteit, aangeboden. Dit geeft de afnemer van deze clouddienst de volledige vrijheid om eigen systemen en diensten te implementeren vanaf de keuze voor het besturingssysteem tot en met de aan te bieden clouddienst.

Het verschil in de soorten zit in de hoeveelheid werk die u er als organisatie zelf nog aan hebt.

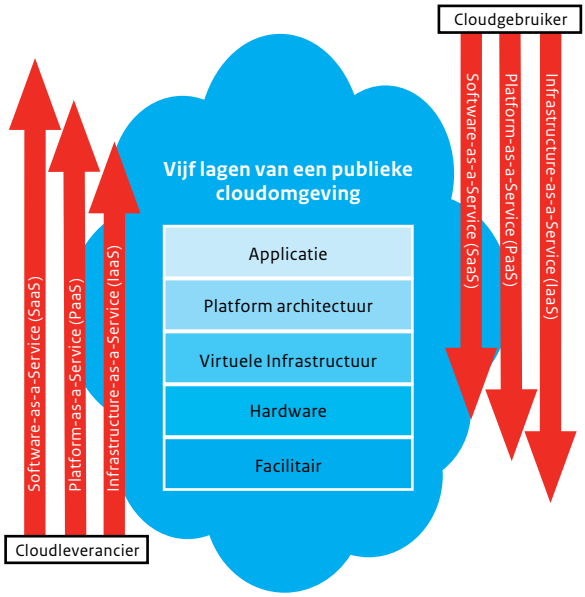


Figuur 3-4 Clouddiensten gezien vanuit de (ICT-)organisatie [18]

3.2.1 Reikwijdte en mate van controle van clouddiensten

Figuur 3-5 geeft de vijf lagen van een publieke cloudomgeving weer. De pijlen links en rechts van het diagram geven de reikwijdte en mate van controle aan, van de clouddiensten. Hoe hoger het dienstniveau van de cloudleverancier, hoe beperkter de reikwijdte en controle van de cloudgebruiker is op de cloudomgeving.

De onderste twee lagen geven de fysieke componenten van een cloudomgeving weer. Deze vallen, ongeacht de soort clouddienst, onder de volledige controle van de cloudleverancier. De facilitaire laag (onderste) bestaat o.a. uit huisvesting, ventilatie, airconditioning, stroom en andere aspecten van de fysieke installatie. De hardware-laag bevat computers, netwerk, opslagcomponenten en andere fysieke ICT-infrastructuurcomponenten.



Figuur 3-5 Verschillen in bereik en controle tussen de clouddiensten

De resterende drie lagen vormen de logische componenten van een cloudomgeving. De gevirtualiseerde infrastructuurlaag bevat software- elementen, zoals hypervisors, virtuele machines en virtuele dataopslag (zie Bijlage D: Achtergrondinformatie over Virtualisatie). Deze laag ondersteunt middleware componenten zodat de infrastructuur wordt gecreëerd waarop de platformarchitectuur kan worden gerealiseerd. Hoewel in deze laag vaak gebruik wordt gemaakt van virtualisatietechnologie, zijn andere implementatievormen niet uitgesloten.

De platformarchitectuur omvat compilers, bibliotheken, softwaretools en ontwikkelomgevingen die nodig zijn om toepassingen te implementeren. De applicatielaag representeert de softwareapplicaties gericht op eindgebruikers en die beschikbaar worden gesteld via de cloud.

3.2.2 Software as a service (SaaS)

Software as a service (SaaS) biedt applicatiefunctionaliteit via het internet aan. De afnemer heeft geen controle over het applicatieplatform, de software met het bijbehorende platform en de onderliggende ICT-infrastructuurcomponenten. Voorbeelden van SaaS-clouddiensten incl. leveranciers zijn [19]:

Dienst	Omschrijving van de toepassing/omgeving	Voorbeelden van leveranciers
Financieel	Beheer van financiële processen.	Concur Workday
Content Management	Beheer en toegang tot content van webapplicaties.	SpringCM
Samenwerking	Gebruikers kunnen samenwerken in werkgroepen, binnen bedrijven en tussen ondernemingen.	CubeTree
E-mail	Beheer van webmail.	Google mail (Gmail) Microsoft (Hotmail) Yahoo! Mail
Verkoop	Beheer van verkoopprocessen.	StreetSmarts
Facturering	Beheer van factureringsprocessen.	Aria systems
Sociale Netwerken	Ontwikkelen en beheer van sociale netwerken.	Ning
Customer Relation Management (CRM)	CRM-toepassingen voor o.a. call centers.	Salesforce.com Oracle OnDemand
Document Management	Beheer van documenten en de bijbehorende workflow.	NetDocuments
Enterprise Resource Planning (ERP)	Beheren van interne en externe middelen (materiële vaste activa, financiële middelen, materialen en Human Resources (HR)).	SAP Business By Design Plex Online
Project Management	Beheer van projecten.	
Persoonlijke productiviteit	O.a. tekstverwerking, spreadsheets en presentaties.	Google Docs Microsoft Web Apps
Informatiebeveiliging	Informatiebeveiliging clouddiensten zoals malware en virusscanning, single sign on, etc.	MessageLabs Hosted Email AntiSpam Trend Micro Titanium Internet Security Panda Managed Office Protection

Andere SaaS-leveranciers zijn:

- Google Apps Engine
- Amazon Web Services (AWS)
- Microsoft Business Productivity Online Standard Suite (BPOS)

3.2.3 Platform as a service (PaaS)

Platform as a service (PaaS) biedt applicatieplatforms en/of besturingssystemen via het internet aan, waarop een afnemer eigen toepassingen kan plaatsen of ontwikkelen. U hebt geen controle over de onderliggende ICT-infrastructuur. Voorbeelden van PaaS-clouddiensten incl. leveranciers zijn [20]:

Dienst	Omschrijving	Voorbeelden van leveranciers
Algemeen	Een omgeving die geschikt is voor applicatieontwikkeling. Bestaat vaak uit een database, een webserver en webservices die de integratie ondersteunen.	Microsoft Azure Force.com
Business Intelligence (BI)	Een omgeving voor de ontwikkeling van BI-toepassingen zoals dashboards, rapportages en data-analyse.	Cloud9 Analytics Amazon Simple Notification Service (SNS)
Integratie	Clouddiensten voor het integreren van toepassingen.	Amazon Simple Queue Services (SQS) IBM Cast Iron
Ontwikkeling en Testen	Toepassingen die softwareontwikkeling en de test levenscyclus ondersteunen.	Keynote systems SOASTA
Database	Schaalbare databasetoepassingen.	Amazon SimpleDB Amazon Relational Database Service (RDS)

Andere PaaS-leveranciers zijn:

- Cloud Burst van IBM

3.2.4 Infrastructure as a service (IaaS)

Infrastructureasaservice(IaaS)steltICT-infrastructuurcomponenten via het internet beschikbaar, zoals rekencapaciteit, netwerk of dataopslag.Voorbeelden van IaaS-clouddiensten incl. leveranciers zijn [21]:

Dienst	Omschrijving	Voorbeelden van leveranciers
Opslag	Schaalbare opslagcapaciteit die o.a. wordt gebruikt voor backups, archivering en opslag van bestanden.	Amazon Simple Storage Service (S3)
Rekencapaciteit	Schaalbare rekencapaciteit.	Amazon Elastic Compute Cloud (EC2) Verizon CaaS
Service Management	Clouddiensten om de cloudinfrastructuur te beheren.	Serve Path GoGrid Amazon CloudWatch Amazon Virtual Private Cloud (VPC)
Cloud Broker	Tools die het mogelijk maken om clouddiensten te beheren op meer dan een cloudinfrastructuur.	RightScale

Andere IaaS-leveranciers zijn:

- IBM Blue Cloud
- 3Tera
- Citrix Cloud
- AppNexus
- Vmware vCloud Express

3.3 Cloudmodellen

Er bestaan drie primaire cloudmodellen: privaat, publiek en community. Ieder model kan beschikken over de eigenschappen uit paragraaf 3.1 'De belangrijkste eigenschappen van cloudcomputing'. Ieder model kan ook de clouddiensten uit paragraaf 3.2 'Soorten Clouddiensten' leveren. De verschillen zitten vooral in de omvang en de toegang tot de geleverde clouddiensten. Combinaties van de drie modellen zijn uiteraard ook mogelijk en wordt de 'hybride cloud' genoemd.

3.3.1 Private cloud

Een private cloud is een infrastructuur die uitsluitend wordt geëxploiteerd voor één organisatie. Deze cloud kan intern of extern gehost worden en is in beheer van de eigen organisatie of een externe partij. Een private cloud heet ook wel 'interne cloud' of 'on-premise cloud'.

3.3.2 Publieke cloud

Een publieke cloud is een cloudinfrastructuur voor het grote publiek (markt of industrie). De afnemers van de clouddiensten zijn geen eigenaar van de middelen want dat is de cloudleverancier. Een publieke cloud heet ook wel 'externe cloud' of 'multi-tenant cloud'.

3.3.3 Community cloud

Een community cloud ondersteunt een specifieke groep businesspartners, die gezamenlijk werken aan één doel, project of product. Een community cloud is in beheer bij één van de businesspartners, of bij een externe partij. Eigenaar van de middelen zijn één of meerdere businesspartner(s) of externe partij(en).

3.3.4 Hybride cloud

De hybride cloud bestaat uit twee of meer van de hierboven beschreven modellen die als afzonderlijke unieke entiteiten blijven bestaan. Deze afzonderlijke entiteiten zijn met elkaar verbonden via gestandaardiseerde (open)- of proprietary (gesloten) technologieën die de interoperabiliteit van gegevens en applicaties mogelijk maken.

HOOFDSTUK 4

Beveiligingsaspecten van clouddiensten

In dit hoofdstuk beschrijven wij de belangrijkste aspecten van clouddiensten, waar u vanuit het oogpunt van informatiebeveiliging aandacht aan moet schenken.

U kunt dit hoofdstuk doorlezen om een algemene indruk te krijgen van de beveiligingsaspecten, maar we raden u aan om het zeker door te nemen als u overweegt om een bepaalde clouddienst af te nemen. Dan kunt u de aspecten beter beoordelen in het kader van de dienst die u op het oog heeft en de eigen gegevens en processen die daarbij betrokken zijn.

Rechtsgebieden
Als het in deze whitepaper gaat over rechtsgebieden, dan bedoelen we hiermee verschillende grondgebieden zoals werelddelen en landen, maar ook bijvoorbeeld de Europese Unie.

De afgelopen jaren is het steeds moeilijker geworden om te bepalen, in welk rechtsgebied bepaalde wetgeving al dan niet geldig is. Dit komt o.a. door de toegenomen globalisering en het gebruik van nieuwe technologieën.

Dat geldt ook voor cloudcomputing. Cloudcomputing maakt het veel eenvoudiger om diensten op afstand te verlenen en in een virtuele omgeving gegevens te verzamelen en te delen.

Hierdoor is het moeilijk om te bepalen, waar de gegevens en de apparatuur zich bevinden die je op dat moment gebruikt.

We benoemen per paragraaf een beveiligingsaspect en bij elk aspect geven we enkele voorbeelden van oorzaken waarom zaken fout kunnen gaan, en wat mogelijke gevolgen daarvan zijn.

Wilt u specifieker per beveiligingsaspect weten waar u op moet letten, dan verwijzen we u naar 'Bijlage E: Handige vragen en aandachtspunten'.

In welke mate de benoemde aspecten specifiek op u van toepassing zijn is onder andere afhankelijk van de keuze voor een bepaald type cloudmodel (privaat, publiek, community of hybride) en het soort clouddienst (SaaS, PaaS of IaaS).

Voor het in kaart brengen van de belangrijkste risico's hebben we gebruik gemaakt van drie publicaties van onafhankelijke instanties[19]:
- European Network and Information Security Agency (ENISA) [22];
- Cloud Security Alliance (CSA) [23];
- Gartner [24].

4.1 Naleving van wet- en regelgeving

Als u gegevens of processen migreert naar de cloud, dan kan dit gevolgen hebben voor bestaande certificeringen, maar ook voor de mate waarin u voldoet aan wet- en regelgeving. Wet- en regelgeving is door de complexiteit, een heikel punt bij het maken van afspraken met de cloudleverancier.

Zorg er dus voor dat u weet welke certificeringen u gebruikt, en dat u weet aan welke wet- en regelgeving u moet voldoen. Dit is relevant voor de clouddienst die u overweegt. Maak vervolgens gebruik van 'Bijlage E: Handige vragen en aandachtspunten'. Hiermee kunt u achterhalen of u aanvullende zaken moet regelen om te blijven voldoen aan wet- en regelgeving op het moment dat u een bepaalde clouddienst gaat afnemen.

Wet- en regelgeving variëren per rechtsgebied (zie kader 'rechtsgebieden'). Per rechtsgebied kunnen beperkingen bestaan. Voorbeelden zijn:
- Export van data (bijv. eisen gesteld aan persoonsgegevens vanuit de Wbp);
- Eisen gesteld aan beveiligingsmaatregelen (bijv. eisen gesteld aan gerubriceerde gegevens vanuit Vir-bi) of
- Eisen in relatie tot compliance en het uitvoeren van audits.

4.1.1 Mogelijke gevolgen van niet voldoen aan wet- en regelgeving

Als een organisatie niet voldoet aan wet- en regelgeving, of certificering verliest, kan dit verstrekkende gevolgen hebben, zoals:
- Juridische consequenties;
- Sancties van toezichthouders;
- Verlies van bestaande certificeringen zoals ISO 27001 [25], NEN 7510 [26], SAS 70[20] [27] en PCI-DSS [29];[21]
- Financiële schade;
- Imagoschade.

4.1.2 Oorzaken van niet voldoen aan wet- en regelgeving

In paragraaf 4.1.2 geven we voorbeelden van oorzaken die ertoe kunnen leiden dat uw organisatie niet (meer) voldoet aan geldende wet- en regelgeving en standaarden/certificeringen:
- U hebt geen inzicht in de geldende wet- en regelgeving, standaarden, richtlijnen, gedragscodes en certificeringen waaraan uw organisatie moet voldoen.
- Gegevens zijn in meerdere rechtsgebieden opgeslagen, zonder dat u daar inzicht in heeft en/of de consequenties daarvan kunt inschatten.
- De cloudleverancier kan geen of onvoldoende bewijs leveren dat hij aan de geldende eisen voldoet.
- De cloudleverancier staat geen externe audits toe, waardoor u geen onafhankelijk beeld krijgt of de cloudleverancier voldoet aan de geldende eisen.
- De cloudleverancier maakt geen gebruik van (open) standaardtechnologieën en -oplossingen. Hierdoor is het lastig vast te stellen of de cloudleverancier voldoet aan de gestelde beveiligingseisen.

19. Zie ook 'Bijlage C'.
20. Vanaf 1 juli 2011 wordt SAS70 vervangen door ISAE3402 [28].
21. Zie Bijlage F: Relevante certificeringen' voor een korte uitleg van deze certificeringen.

4.1.3 Een specifiek geval: privacywetgeving

Als het gaat om informatiebeveiliging en wetgeving, dan is de Wet Bescherming Persoonsgegevens (Wbp) een van relevantste wetten waaraan je moet voldoen. Om die reden besteden we er in deze paragraaf apart aandacht aan.

Belangrijk bij het vaststellen of de Wbp van toepassing is, zijn de definities ´verantwoordelijke´ en ´bewerker' (zie Bijlage I: Relevante artikelen Wbp en Richtsnoeren'). De vestigingslocatie van de verantwoordelijke - de zetel van de rechtspersoon - is hierbij bepalend. [30] Is deze locatie in Nederland, dan is de Wbp van toepassing, ongeacht waar de ICT-faciliteiten zich bevinden. Als de zetel van de rechtspersoon zich in een EU-lidstaat bevindt, dan is de Europese richtlijn[22] van toepassing, ook al bevinden de ICT-activiteiten en faciliteiten zich buiten het grondgebied van de EU-lidstaten.

Het grote verschil tussen 'verantwoordelijke' en 'bewerker' zit in het feit dat de bewerker niet de doelen en middelen voor de verwerking van persoonsgegevens bepaalt, maar slechts in opdracht van de verantwoordelijke persoonsgegevens verwerkt.

De Europese Commissie

Eurocommissaris Neelie Kroes (Digitale Agenda & ICT) waarschuwt voor de gevaren van cloudcomputing. De Europese Commissie heeft daarom ook nieuwe regels opgesteld voor grensoverschrijdende dataverwerking en - opslag door cloudleveranciers (zie ook paragraaf 2.5 'Dataclassificatie').

'Cloudcomputing is meer dan een technische uitdaging. Door onze persoonlijke data op servers op afstand te zetten, lopen we het risico om de controle over die data te verliezen. Omdat de bescherming van privégegevens een fundamenteel recht in de EU is, moet er actie worden ondernomen,' aldus Eurocommissaris Neelie Kroes in een toespraak aan de Université Paris-Dauphine [31].

Privacy

Privacy is een paraplubegrip, een fundamenteel recht dat nauw verbonden is met persoonlijke vrijheid. Het bevat verschillende dimensies van privacy, zoals relationele, informationele, lichamelijke, ruimtelijke en medische privacy.

In deze whitepaper doelen wij op informationele privacy. Dat is het recht om zelf te beschikken over de eigen persoonsgegevens en om zelf te bepalen wanneer, hoe en in welke mate je die gegevens aan anderen beschikbaar stelt.

Amerika en het 'Safe Harbor' principe

Amerika lijkt de bescherming van Europese privégegevens geregeld te hebben in de zogenaamde 'Safe Harbor'-principes [32]. Als ze daaraan voldoen, mogen ze data van Europese burgers en bedrijven verwerken. Helaas is de Safe Harbor niet helemaal 'safe', want andere partijen kunnen toch ongewenst toegang krijgen. Zo heeft de Amerikaanse overheid volgens de antiterreurwet 'Patriot Act' het recht deze data toch te vorderen en in te zien (zie kader 'Microsoft: Data Use Limits' voor een voorbeeld). Eurocommissaris Neelie Kroes en onderzoeksbureau Forrester waarschuwen [33] dan ook voor het onderbrengen van data in de cloud bij Amerikaanse cloudleveranciers. Een recent voorbeeld hiervan is te lezen in het artikel 'Twittergegevens WikiLeaks-sympathisanten opgevraagd door VS' [34].

Microsoft: Data Use Limits

Als invulling van de Patriot Act heeft Microsoft het volgende statement in hun gebruiksvoorwaarden opgenomen [35]:

'In a limited number of circumstances, Microsoft may need to disclose data without your prior consent, including as needed to satisfy legal requirements, or to protect the rights or property of Microsoft or others (including the enforcement of agreements or policies governing the use of the service).'

Bovenstaande geldt voor alle gebruikers en gegevens van de Microsoft online diensten, waaronder het huidige aanbod van BPOS (Business Productivity Online Suite) en Office 365 suite.

4.2 Beheersbaarheid van processen en systemen

Wanneer uw organisatie gebruikmaakt van clouddiensten, staat u op een aantal onderdelen, een deel van uw controle en beheersmogelijkheden af aan de cloudleverancier. Dit kan van invloed zijn op uw beveiligingsniveau. In 'Bijlage E: Handige vragen en aandachtspunten' vindt u een lijst met punten aan de hand waarvan u kunt inschatten in welke mate u controle en beheersmogelijkheden verliest en welke maatregelen u daartegen kunt nemen.

Controleverlies kan echter ook worden veroorzaakt vanuit de eigen organisatie. Een afdeling of medewerker kan eenvoudig zelf aan de slag met de cloud, zonder te realiseren wat de impact ervan is op de informatiebeveiliging (zie paragraaf 2.1.2 'Business drivers van medewerkers').

22. Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.

4.2.1 Mogelijke gevolgen van verminderde beheersbaarheid

Het belangrijkste risico van verminderde controle en beheersbaarheid is dat een cloudleverancier mogelijk niet voldoet aan beveiligingseisen die uw organisatie stelt aan beschikbaarheid, integriteit en vertrouwelijkheid. Dit kan leiden tot incidenten

De eigenaar van systemen en processen kan zijn verantwoordelijkheden op het gebied van beveiliging delegeren aan de cloudleverancier. Desondanks blijft de eigenaar uiteindelijk zelf verantwoordelijk voor de beveiliging van de bedrijfsmiddelen en moet hij in staat zijn vast te stellen of de gedelegeerde verantwoordelijkheid op de juiste manier is ingevuld.

Een ander risico is de gevolgen voor het niet voldoen aan de geldende wet- en regelgeving. Denk hierbij ook aan de van toepassing zijnde standaarden/certificeringen voor uw organisatie. Deze zijn eerder uitgewerkt in paragraaf 4.1 'Naleving van wet- en regelgeving'.

4.2.2 Oorzaken die leiden tot verminderde beheersbaarheid

Hieronder enkele voorbeelden van oorzaken die ertoe leiden dan een organisatie minder controle heeft over de eigen systemen en processen.

- Onduidelijkheid over de taken, bevoegdheden en verantwoordelijkheden van relevante functies en rollen van uw organisatie en de cloudleverancier. Hierdoor kan verwarring en discussie ontstaan over wie nu welke taken uitvoert.
- Gebrek aan goede afspraken over het dienstenniveau met de cloudleverancier. Denk hierbij aan openingstijden, bereikbaarheid en reactietijd van de incidentmelding en afhandeling, escalatieprocedures, beveiligingseisen, het recht op audit.
- Gebrek aan inzicht in beheerprocessen bij de cloudleverancier, zoals beheer op afstand, toegangsbeheer, incidentbeheer, wijzigingsbeheer en patchmanagement.
- Clouddiensten worden door organisaties niet op beveiligingsrisico's geëvalueerd vóór implementatie in de organisatie [36].
- Organisaties hebben geen overzicht van de clouddiensten die toegepast worden [36].

4.3 Gegevensbescherming

De bescherming van gegevens in de cloud is uiteraard een van de belangrijkste aspecten van clouddiensten, samen met de zekerheid dat de cloudleverancier voldoet aan de eisen die door organisaties hieraan zijn gesteld.

Uw organisatie is en blijft namelijk altijd verantwoordelijk voor de beveiliging van uw gegevens, zelfs wanneer deze gegevens zijn ondergebracht bij een cloudleverancier.

U moet dan ook kunnen controleren of de verwerking van uw gegevens plaatsvindt op een veilige en legale manier, conform geformuleerde eisen.

Gegevensbescherming is van belang gedurende de hele levenscyclus van informatie: vanaf het moment van creatie, tijdens opslag, gebruik, verwerking en archivering, tot en met vernietiging van de informatie.

Gegevensbescherming heeft een nauwe relatie met de elders in dit hoofdstuk beschreven aspecten zoals de naleving van wet- en regelgeving (paragraaf 4.1), beheersbaarheid van processen en systemen (paragraaf 4.2) en beheer van gebruikers (paragraaf 4.6).

Kwetsbaarheidsanalyse Spionage [37]

De minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK) constateert dat economische, strategische en technisch-wetenschappelijke spionage een actuele dreiging vormt voor de Nederlandse nationale veiligheid. Om deze dreiging beter in beeld te brengen en aanbevelingen te doen hoe deze dreiging (verder) te reduceren, hebben de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en het Directoraat-Generaal Veiligheid (DGV) gezamenlijk onderzoek gedaan naar spionagerisico's op de gebieden van economisch welzijn & wetenschappelijk potentieel en openbaar bestuur & vitale infrastructuur. De AIVD heeft in zijn contraspionage namelijk geconstateerd verschillende buitenlandse inlichtingendiensten juist in deze gebieden actief inlichtingen verzamelen.

Uit dit onderzoek, de Kwetsbaarheidsanalyse, blijkt dat de toenemende verwevenheid en complexiteit van computersystemen en het koppelen van dataopslagsystemen, de gevoelige gegevens in systemen kwetsbaar maakt. Het uitbesteden van activiteiten als systeem- en serverbeheer, datawarehousing en gegevensverwerking brengt eveneens spionagerisico's met zich mee. Conclusies en aanbevelingen die in het onderzoeksrapport zijn vermeld gelden ook voor cloudcomputing! In de Kwetsbaarheidsanalyse wordt verder de dreiging in beeld gebracht en aanbevelingen gegeven hoe die (verder) te reduceren.

4.3.1 Mogelijke gevolgen van onvoldoende gegevensbescherming

Het onvoldoende beveiligen van gegevens kan verstrekkende gevolgen hebben. Hieronder volgen de belangrijkste gevolgen.

- Opgeslagen gegevens zijn toegankelijk voor derde partijen. Dit kan tot verlies, diefstal, misbruik of openbaarmaking van gegevens en imagoschade leiden. Tevens kan dit uw dienstverlening verstoren.

- Derde partijen kunnen verwijderde gegevens achterhalen. Dit kan tot verlies, diefstal, misbruik of openbaarmaking van gegevens en imagoschade leiden. Tevens kan dit uw dienstverlening verstoren.
- Gegevens worden onderschept tijdens het transport, door middel van 'sniffing', 'man in the middle' of 'replay'-aanvallen (zie voor een korte omschrijving Bijlage G: Aanvalsmethoden').
- Gegevens zijn toegankelijk of zelfs op te eisen door andere overheden, als gevolg van opslag in een ander rechtsgebied. Bijvoorbeeld: De Amerikaanse overheid heeft volgens de antiterreurwet 'Patriot Act' het recht data te vorderen en in te zien (zie ook paragraaf 4.1.3). Als uw cloudleverancier activiteiten zoals systeem- en server-beheer, datawarehousing en gegevensverwerking uitvoert, brengt dit mogelijk spionagerisico's met zich mee (zie kader 'Kwetsbaarheidsanalyse Spionage').

4.3.2 Oorzaken van onvoldoende gegevensbescherming

Hieronder enkele voorbeelden van oorzaken die ertoe leiden dat gegevens mogelijk onvoldoende worden beschermd.

- Uw organisatie heeft geen risicoanalyse uitgevoerd om de gegevens te classificeren, waardoor vertrouwelijke gegevens in de cloud zijn geplaatst.
- Uw organisatie heeft geen geheimhoudingsverklaringen opgesteld en laten ondertekenen, voor toegang te verlenen tot uw gegevens.
- Door kwetsbaarheden in of te zwakke implementatie van versleutelstandaarden en -toepassingen, authenticatie, autorisatie en accountingsystemen, kunnen ongeautoriseerde toegang krijgen tot systemen en gegevens. In de cloud hebben aanvallen die gebaseerd zijn op wachtwoordauthenticatie meer impact op uw organisatie, aangezien bedrijfstoepassingen via het internet benaderbaar zijn.
- Gegevens, inclusief alle kopieën en back-ups, worden in andere geografische locaties opgeslagen dan vastgelegd in het contract, SLA en/of regelgeving.
- Externe partijen kunnen bij de informatie van uw organisatie komen, zeker als die externe partijen zich in het buitenland bevinden waar ook nog andere wet- en regelgeving gelden (zie ook paragraaf 4.1 'Naleving van wet- en regelgeving').
- Door gebruik te maken van een virtuele architectuur (zie Bijlage D: Achtergrondinformatie over Virtualisatie') bestaat de mogelijkheid dat de resources van de ene cloudgebruiker die van andere cloudgebruikers nadelig beïnvloeden. Kwetsbaarheden in de hypervisor kunnen ongeautoriseerde toegang geven tot gedeelde ICT-resources. Mogelijke bedreigingen bij scheidingsmechanismen binnen een virtuele infrastructuur zijn 'side channel', 'guest hopping', 'hyperjacking' en 'SQL-injectie' (zie Bijlage G: Aanvalsmethoden').
- Uw organisatie heeft geen patchmanagement geïmplementeerd, waardoor beveiligingsupdates niet of niet tijdig worden geïnstalleerd.
- Organisaties schatten de waarde van informatie niet altijd goed in. Uit onderzoek (zie kader 'Kwetsbaarheidsanalyse Spionage') blijkt dat organisaties zich niet altijd bewust zijn van het feit dat zij over informatie of kennis beschikken die van waarde is voor derden zoals inlichtingendiensten.

4.4 Relatie tot de leverancier

De cloudmarkt is op dit moment nog onvolwassen en de relatie die u met uw leverancier aangaat verdient daarom aandacht. Vendor lock-in (kritieke afhankelijkheid van de leverancier) is namelijk een risico van cloudcomputing.

Cloudleveranciers maken meestal geen gebruik van hulpmiddelen die portabiliteit (uitwisselbaarheid) garanderen. Een organisatie kan daardoor niet gemakkelijk over stappen naar een andere cloudleverancier of data en diensten weer naar de eigen ICT-omgeving migreren. Het is te duur, neemt teveel tijd in beslag of is zelfs onmogelijk. Het gevolg is dat je als organisatie op een onacceptabele manier afhankelijk bent van je leverancier.

Eurocommissaris Neelie Kroes tijdens de Open Forum Europe Summit 2010 te Brussel. [38]
De strekking van de speech van Eurocommissaris Neelie Kroes is: Maak gebruik van open software en standaarden zodat interoperabiliteit wordt gegarandeerd en organisaties niet afhankelijk worden van een bepaalde leverancier.

Ze zegt hierover: 'Veel overheden hebben zich decennia lang onbedoeld afhankelijk gemaakt van 'leverancier eigen technologie' (proprietary technology). Na een bepaalde tijd is een punt bereikt dat de oorspronkelijke keuze zo zit ingebakken, dat alternatieve oplossingen stelselmatig worden genegeerd, ongeacht de mogelijke voordelen. Dit is een verspilling van publieke gelden dat de meeste overheidsinstanties zich niet meer kunnen veroorloven.'. In feite zegt ze hiermee dat vendor lock-in door overheden een verspilling is van publieke gelden.

Ze stelt dan ook voor om gedetailleerde Europese richtlijnen voor overheidsaanbestedingen op te stellen, die overheden moeten behoeden voor vendor lock-in. Daarnaast wil ze softwarefabrikanten verplichten om hun producten 'open' te maken. Ook wil ze er structureel voor zorgen dat 'significante marktspelers' interoperabiliteit binnen hun producten niet langer kunnen negeren: 'De Commissie zou niet iedere keer een epische antitrust-zaak moeten hoeven voeren, iedere keer dat software interoperabiliteit mist. Zou het niet fijn zijn om al zulke problemen in één keer op te lossen?'

Eurocommissaris Neelie Kroes wil gedetailleerde Europese richtlijnen voor overheidsaanbestedingen opstellen, die overheden moeten behoeden voor vendor lock-in (zie kader 'Eurocommissaris Neelie Kroes tijdens de Open Forum Europe Summit 2010 te Brussel.').

4.4.1 Mogelijke gevolgen van kritieke afhankelijkheid van de leverancier

Als je afhankelijk bent van een cloudleverancier, brengt dat risico's met zich mee.

- Uw eigen organisatie kan het gewenste niveau van dienstverlening niet garanderen, doordat uw cloudleverancier wordt overgenomen of failliet gaat.
- De cloudleverancier gaat gebruik maken van onderaannemers, waardoor u niet meer compliant bent.
- U maakt onnodig hoge kosten door het ontbreken van marktwerking. U zit namelijk vast aan de cloudleverancier en het ontbreekt dus aan concurrentie op kosten, kwaliteit en dienstverlening. De tarieven van de cloudleverancier kunnen onevenredig stijgen en/of de kwaliteit van de geleverde dienstverlening kan afnemen.

4.4.2 Oorzaken die tot kritieke afhankelijkheid van de leverancier kunnen leiden

Onderstaand volgen enkele voorbeelden van mogelijke oorzaken die ertoe kunnen leiden dat uw organisatie te afhankelijk wordt van een cloudleverancier.

- De cloudleverancier maakt geen gebruik van standaardtechnologieën en -oplossingen.
- Het programma van eisen[23] houdt onvoldoende rekening met de afhankelijkheid van de cloudleverancier wat kan leiden tot een slechte/verkeerde keuze van cloudleverancier.
- Beheerprocessen zijn niet of niet afdoende ingericht door de cloudleverancier.
- De gebruiksvoorwaarden zijn onvolledig en niet transparant, zoals:
  - privacy geldende voorwaarden;
  - (uitsluiting van) aansprakelijkheid;
  - producten en diensten;
  - disclaimer en
  - verwachtingen en intentieverklaringen.

4.5 Beschikbaarheid van de clouddienst

De beschikbaarheid van het internet wordt steeds belangrijker voor de cloud. Clouddiensten worden immers met behulp van internettechnologieën op afstand aangeboden. Voor de beschikbaarheid van deze diensten bent u dan ook volledig afhankelijk van de internetverbinding tussen u en de dienst.

4.5.1 Mogelijke gevolgen van onvoldoende beschikbaarheid van de clouddienst

Als clouddiensten onvoldoende beschikbaar zijn, brengt dat risico's met zich mee voor uw organisatie

- Uw dienstverlening aan uw klanten is onmogelijk (zie kader 'Hyves niet beschikbaar door storing bij datacenter leverancier').
- U kunt geen beheer op afstand uitvoeren op systemen.
- Uw interne processen komen stil te liggen, doordat ondersteunende systemen zijn ondergebracht in de cloud.
- U ondervindt imagoschade door negatieve publiciteit in de media (zie kader 'Storing clouddienst Amazon levert imagoschade op').
- U ondervindt financiële schade doordat klanten overstappen naar een andere cloudleverancier (inkomstenderving) of omdat ze schadeclaims indienen.

Hyves niet beschikbaar door storing bij datacenter leverancier [39]

Hyves, grootste netwerksite van Nederland, was niet beschikbaar omdat de noodstroomvoorziening van het 'hypermoderne' datacenter van Evoswitch faalde, nadat het datacenter was getroffen door een stroomstoring. De stroomstoring duurde van 6:12 tot 6:50 uur.
Dit zou normaal gesproken geen problemen mogen opleveren voor een datacenter, omdat dit beschikt over noodstroom in de vorm van UPS (uninterruptible power supply) in combinatie met dieselaggregaten. Ook Evoswitch beschikt over verschillende noodstroomvoorzieningen. Alle servers zitten aangesloten op een UPS, benadrukt Evoswitch. Maar dat systeem faalde, omdat de batterijen er al na 6 seconden mee ophielden en het 20 seconden duurt voordat de dieselaggregaten actief zijn.

4.5.2 Oorzaken die tot onvoldoende beschikbaarheid van de clouddienst kunnen leiden

In deze paragraaf geven we voorbeelden van oorzaken die ertoe kunnen leiden dat clouddiensten onvoldoende beschikbaar zijn.

- Een storing bij uw internetleverancier (zie kader 'Hyves niet beschikbaar door storing bij datacenter leverancier' en 'Storing clouddienst Amazon levert imagoschade op').
- Uw internetverbinding (zoals througput, up- en downloadsnelheid) is niet berekend op de hoeveelheid dataverkeer en/of het aantal connecties.
- De capaciteit van de netwerkcomponenten (zoals routers, switches en firewalls) is onvoldoende.
- De cloudleverancier beschikt niet over een disaster en recovery plan, zodat hij niet adequaat op calamiteiten kan inspelen.

23. Een Programma van Eisen (PvE) is een document in een ontwerp-, aanschaf of selectieproces en is het medium waarin de verwachtingen van de opdrachtgever of gebruiker zijn vastgelegd. Een PvE wordt geschreven voor de ontwerper of (mogelijke) leverancier die daarmee weet aan welke voorwaarden zijn product zal moeten voldoen. <http://nl.wikipedia.org/wiki/Programma_van_eisen>.

- Kwaadwillenden hebben een aanval op de cloud-leverancier uitgevoerd, bijvoorbeeld door middel van de (distributed) Denial-of-Service ((d)DoS) aanval [56][24].
- De fysieke beveiliging van het datacenter is niet afdoende waardoor ongeautoriseerde toegang kunnen krijgen tot computerruimten en apparatuur.

4.6 Beheer van gebruikers

Alle toegang tot (vertrouwelijke) informatie en ICT-voorzieningen moet worden gecontroleerd en beperkt zijn tot geautoriseerde personen. Toegangscontrole is bij cloudcomputing belangrijker dan ooit aangezien 'iedereen' via het internet toegang heeft tot uw gegevens en systemen.
Mogelijke gevolgen van onvoldoende toegangscontrole

4.6.1 Mogelijke gevolgen van onvoldoende toegangscontrole

Mogelijke risico's van onvoldoende toegangscontrole van gebruikers zijn:

- Ongeautoriseerde personen hebben toegang tot gegevens en systemen.
- Geen dienstverlening meer kunnen uitvoeren voor klanten, doordat ongeautoriseerde personen een aanval hebben uitgevoerd op de systemen van de cloudleverancier.
- Imagoschade vanwege negatieve publicaties in de media.
- Financiële schade doordat klanten bijvoorbeeld schadeclaims indienen.

4.6.2 Mogelijke oorzaken die tot onvoldoende toegangscontrole kunnen leiden

Onderstaand volgt een overzicht van mogelijke oorzaken van onvoldoende toegangscontrole van gebruikers

- Er wordt gebruik gemaakt van groepsidentificatie (groep-ID), in plaats dat alle gebruikers (inclusief beheerders) een unieke gebruikersidentificatie (gebruikers-ID) hebben.
- Het autorisatieproces is niet beschreven of afgestemd tussen de verschillende partijen.
- Er wordt geen lijst van geautoriseerde personen bijgehouden, waardoor er geen overzicht is wie welke rechten bezit.
- Er worden geen audittrails[25] bijgehouden van wie toegang heeft. Hierdoor heeft de organisatie geen inzicht wie, welke activiteit op het systeem heeft uitgevoerd.
- Kwetsbaarheden in de gebruikte authenticatiemethode worden misbruikt (zie kader 'RSA slachtoffer van targeted attack').

RSA slachtoffer van targeted attack [44]
RSA heeft in een 'Open Letter to RSA Customers' aangegeven dat zij slachtoffer is geworden van een targeted attack. De informatie die tijdens deze targeted attack is buitgemaakt was specifiek gerelateerd aan 'RSA SecurID's two-factor authenticatieproducten'.

Storing clouddienst Amazon levert imagoschade op
Voorbeelden van krantenkoppen die in de Nederlandse media verschenen zijn:

- Data definitief verloren na storing Amazon [40].
- Veel websites offline door storing Amazon [41].
- Sites offline door storing Amazon [42].
- Megastoring Amazon EC2 door menselijke fout [43].

Door een storing in een datacenter van Amazon waren een groot aantal websites, die in de cloud van Amazon zijn geplaatst, slecht bereikbaar of volledig offline. Amazon meldde problemen met drie diensten, databasemanager Relational Database Service (RDS), Elastic Compute Cloud (EC2) dat rekencapaciteit in de cloud aanbiedt en Elastic Block Storage (EBS) de opslagruimte die bij EC2 hoort.
Amazon kan een deel van de data die verloren is gegaan tijdens de storing niet meer terughalen. Het percentage schijven dat niet volledig hersteld kan worden is relatief klein, 0,07 procent (zie figuur 4-1), maar gezien het aantal klanten gaat het in absolute aantallen waarschijnlijk evengoed om een substantiële hoeveelheid.
Dat heeft dus niet alleen imagoschade opgeleverd voor Amazon, maar nu ook schade voor klanten, die hun data verloren hebben zien gaan.

4.7 Beheer van incidenten

De doelstelling van incidentbeheer is om zo snel mogelijk verstoringen in de ICT-infrastructuur, op een adequate en gestructureerde manier te verhelpen en gebruikersvragen te beantwoorden. Waardoor het de ICT-dienstverlening weer voldoet aan het niveau van de SLA's.

4.7.1 Mogelijke gevolgen door slecht incidentenbeheer

Mogelijke risico's van slecht of geen incidentenbeheer zijn:

- Incidenten worden niet structureel opgelost, waardoor de dienstverlening bij herhaling verstoord blijft.
- Bij (een vermoeden van) het overtreden van beveiligings-regels worden bewijzen (zoals audittrails en loggegevens) niet tijdig veiliggesteld.
- Cloudgebruikers worden niet of niet tijdig geïnformeerd over incidenten, waardoor deze niet adequaat kunnen reageren.

24. Zie voor een korte omschrijving 'Bijlage G: Aanvalsmethoden'.
25. Logboek waarin alle relevante gegevens worden geadministreerd.

4.7.2 Mogelijke oorzaken van slecht incidentenbeheer

Onderstaand een overzicht met mogelijke oorzaken die slecht incidentenbeheer tot gevolg hebben.

- Er zijn geen verantwoordelijkheden en procedures vastgesteld, die waarborgen dat beveiligingsincidenten snel, effectief en ordelijk worden afgehandeld.
- Er zijn geen (goede) afspraken over het classificeren van incidenten vast gelegd, waardoor incidenten niet de juiste urgentie en prioriteit krijgen.
- Er zijn geen (goede) afspraken vastgelegd over het melden en classificeren van incidenten (bepalen soort, impact, urgentie en prioriteit) en de maximale termijn waarbinnen ze verholpen moeten zijn.
- Incidenten worden niet (goed) geregistreerd, beheerd en geëvalueerd, waardoor er geen goede probleemanalyse kan plaatsvinden.
- Er vindt geen goede administratie plaats van de ICT-resources (de zogenaamde Configuration Items - CI's), waardoor verkeerde ICT-resources aan een incident worden gekoppeld.
- De cloudleverancier en/of onderaannemers staan het uitvoeren van digitaal (forensisch) onderzoek en audits niet toe (zie paragraaf 4.7.3), waardoor u geen analyse en evaluatie kunt uitvoeren van de incidenten.

4.7.3 Digitaal (forensisch) onderzoek en uitvoeren audits

Paragraaf 4.7.1 'Mogelijke gevolgen door slecht incidentenbeheer' geeft al aan dat bewijsmateriaal, zoals audittrails en loggegevens, niet tijdig veiliggesteld worden bij (een vermoeden van) het overtreden van beveiligingsregels. Aan deze onderzoeksdata worden echter juridische eisen gesteld op het moment dat ze dienst doen als bewijsmateriaal voor illegale activiteiten (zie kader 'Kwaliteitseisen aan gegevens').

De juridische eisen zijn 'goed' te realiseren bij eigen beheer van de ICT-omgeving, maar hoe zit het als een deel van de systemen en/of gegevens bij een cloudleverancier zijn geplaatst? Dan wordt het een stuk lastiger of zelfs onmogelijk, omdat de cloudleverancier niet bereid is om de noodzakelijke maatregelen te implementeren.
Dat kan te maken hebben met kosten die deze aanpassing met zich meebrengt. Ook kan het zijn dat de maatregelen niet passen in de standaard dienstverlening of niet geïmplementeerd kunnen worden binnen de huidige ICT-infrastructuur.

Digitaal (forensisch) bewijs moet een relatie leggen tussen slachtoffer, dader en de illegale activiteiten (chain of evidence). Uitgangspunten voor het verzamelen van dit bewijs zijn:

- Creëer uitgebreid bewijsmateriaal (zoals audittrails en logs).
- Maak een kopie (image) van de gegevens.
- Zet een digitale handtekening onder deze gegevens en werk tijdens het onderzoek alleen met de kopie. Zorg dat het origineel niet meer wordt gewijzigd.
- Documenteer alle handelingen (wie, wat, wanneer en waarom) die plaatsvinden op de kopie.

Kwaliteitseisen aan gegevens [45]

Ervan uitgaande dat opgeslagen gegevens bewijskracht moeten hebben, zijn waarborgen nodig. Deze waarborgen richten zich vooral op twee aspecten:
1. De kwaliteit van de vastgelegde gegevens;
2. De kwaliteit van het gegevensbeheer.

Gegevens moeten voldoen aan een aantal kwaliteitseisen om daarmee aan wet- en regelgeving te kunnen voldoen. Deze kwaliteitseisen zijn niet afhankelijk van de gebruikte informatiesystemen en de gebruikte informatievoorziening en realiseren de historiciteit van gegevens. Dit betekent dat de gegevens kunnen worden gereconstrueerd zoals ze ooit, op een eerder moment in de tijd, zijn gegenereerd.

Gegevens moeten blijven zoals ze oorspronkelijk zijn vastgesteld. Het gaat dus om een zodanige vastlegging (conversie, bewaring en selectie) dat de blijvende juistheid en volledigheid in alle omstandigheden gewaarborgd is en, indien gegevens in de processen zijn gewijzigd, achteraf kan worden vastgesteld wie, wanneer welke wijzigingen heeft aangebracht.

De historiciteit van gegevens wordt bepaald door:

- **Integriteit:** dat is de mate waarin de gegevens en de weergave van gegevens zijn zoals ze waren, waarbij niets ten onrechte is toegevoegd, verdwenen, achtergehouden of veranderd;
- **Authenticiteit:** dat is de mate waarin, ongeacht de gebruikte compressiemethodiek, de weergave van gegevens de juiste oorspronkelijk vorm en inhoud bevatten;
- **Controleerbaarheid:** dat is de mate waarin de gegevens en de weergave van gegevens toetsbaar zijn.

Gegevens moeten meermalen, onafhankelijk van tijd, kunnen worden samengesteld, met dezelfde inhoud, presentatievorm en samenhang als op het moment van ontstaan of ontvangst. Tegelijkertijd is het voor de bewijswaarde belangrijk dat de omstandigheden waarin de gegevens zijn bewerkt en afgehandeld bekend zijn. Gedurende de tijd dat de gegevens als bewijs gebruikt worden moet het mogelijk zijn om de omstandigheden te reconstrueren waarin ze zijn ontstaan, bewerkt, afgehandeld en beheerd.

4.8 Beheer van wijzigingen

Wijzigingsbeheer zorgt ervoor dat wijzigingen op onderliggende systemen zo min mogelijk impact hebben op de dienstverlening. Het gecontroleerd doorvoeren van wijzigingen leidt ertoe, dat de kans op verstoringen afneemt en de impact van de verstoring kleiner is.

Een belangrijk aspect bij het gecontroleerd doorvoeren van wijzigingen is, dat ze ook op beveiligingsconsequenties worden getoetst, voordat ze worden uitgevoerd. Dit vermindert de kans op beveiligingsincidenten en zorgt ervoor dat de ICT-infrastructuur én aan de beveiligingsnorm(en) voldoet én aan het afgesproken niveau blijft voldoen.

Ook zorgt wijzigingsbeheer ervoor dat relevante instellingen van de ICT-infrastructuur gecontroleerd en geautoriseerd gewijzigd worden. Alle wijzigingen worden bijgehouden in een audit-logboek.

Bij cloudcomputing zijn de ICT-resources ondergebracht bij een cloudleverancier. De cloudleverancier is verantwoordelijk voor de wijzigingen op deze ICT-resources. Cloudgebruikers hebben hier dan ook (bijna) geen invloed op.

4.8.1 Mogelijke gevolgen van slecht wijzigingsbeheer

Slecht wijzigingsbeheer door de cloudleverancier kan de volgende risico's genereren

- Het doorvoeren van wijzigingen leidt tot verstoringen van de dienstverlening (zie kader 'Oorzaak storing clouddienst Amazon').
- Cloudgebruikers worden niet of niet tijdig geïnformeerd over wijziging.
- De verkeerde versie wordt in productie genomen.

Oorzaak storing clouddienst Amazon

Zie ook het kader bij 4.6 'Storing clouddienst Amazon levert imagoschade op', dit is een vervolg...

De oorzaak van de storing in een datacenter van Amazon is een fout van een beheerder bij het doorvoeren van een wijziging in de configuratie [46].
Korte beschrijving incident: Het doel van de configuratiewijziging was de capaciteit van het primaire netwerk te upgraden. Eén van de standaard stappen tijdens deze configuratiewijziging is, om het netwerkverkeer van de primaire router om te leiden naar een redundante router in het primaire netwerk. In plaats van het netwerkverkeer te routeren naar de redundante router op het primaire netwerk, werd het netwerkverkeer omgeleid naar een netwerk met een lagere capaciteit.

4.8.2 Mogelijke oorzaken van slecht wijzigingsbeheer

Onderstaand volgt een overzicht van mogelijke oorzaken die slecht wijzigingsbeheer tot gevolg hebben:

- Wijzigingen worden niet voldoende getest voordat deze in productie worden genomen.
- Er vindt geen goede administratie plaats van de ICT-resources (de zogenaamde Configuration Items - CI's), waardoor de impact op de bestaande infrastructuur verkeert wordt ingeschat.
- Er is geen fallback-scenario uitgewerkt, waardoor de wijziging niet kan worden teruggedraaid op het moment dat het doorvoeren van de wijziging tot verstoring leidt.
- Er is geen goedkeuringsproces met betrekking tot wijzigingen ingevoerd, zodat ook ongeautoriseerde wijzigingsverzoeken in behandeling genomen.
- Er is geen procedure voor spoedeisende wijzigingen, zoals beveiligingsupdates.
- Er vindt geen afstemming met gebruikers plaats wanneer wijzigingen worden doorgevoerd.
- Versiebeheer is niet of niet goed ingericht.
- Wijzigingen doorlopen niet de OTAP-cyclus[26], maar worden direct in productie doorgevoerd.
- De wijziging wordt verkeerd uitgevoerd (zie kader 'Oorzaak storing clouddienst Amazon').

4.9 Back-up en recovery

Een back-up maakt een reservekopie van gegevens en heeft een tweeledig doel. Het eerste doel is herstel van gegevens bij verlies ervan. Het tweede doel is om gegevens over een bepaalde periode, terug te kunnen halen vanuit historisch oogpunt, bijvoorbeeld vanwege de wettelijke bewaartermijn van deze gegevens. Recovery zorgt ervoor dat u weer beschikt over de gegevens uit de back-up.
Ook voor back-up en recovery geldt dat u afhankelijk bent van de cloudleverancier.

4.9.1 Mogelijke gevolgen van het ontbreken van back-up en recovery

Zonder een goede back-up en recovery strategie bij de cloudleverancier loopt uw organisatie de volgende risico's.

- Gegevens kunnen niet worden hersteld, omdat de back-ups zijn beschadigd of vernietigd.
- De dienstverlening wordt verstoord, doordat de verkeerde back-up is teruggezet.
- U bent uw gegevens definitief kwijt omdat bij het uitvoeren van de recovery bleek dat de back-up was beschadigd of mislukt.

26. TAP staat voor ontwikkeling, test, acceptatietest en productie.

4.9.2 Mogelijke oorzaken van het niet goed uitvoeren van back-up en recovery

Deze paragraaf geeft een overzicht met mogelijke oorzaken van het niet (goed) uitvoeren van back-up en recovery:

- Er is geen back-up strategie of de strategie wordt niet opgevolgd.
- Er worden niet periodiek van alle relevante gegevens- en programmabestanden back-ups gemaakt.
- Back-ups worden niet op een externe locatie bewaard.
- Er wordt niet periodiek getest of back-ups ook teruggezet kunnen worden.

4.10 Transparantie

Om een juiste risicoafweging te maken welke diensten u gaat afnemen uit de cloud, heeft u inzicht nodig in de complexiteit van cloudcomputing. Om hierin inzicht te verkrijgen bent u voor een groot gedeelte afhankelijk van de cloudleverancier.

Biedt de cloudleverancier voldoende transparantie over de aangeboden clouddiensten en achterliggende (cloud) architectuur, standaarden, processen en procedures om deze risicoafweging te maken? Biedt de cloudleverancier transparantie met betrekking tot het gehanteerde reken-model voor het vaststellen van prijzen, zodat het aanbod en de prijzen van verschillende cloudleveranciers beter vergelijkbaar zijn? Cloudleveranciers moeten aantonen dat hun diensten voorzien zijn van effectieve beveiligings-maatregelen.

HOOFDSTUK 5

Beveiligingsarchitectuur en -standaarden

Dit hoofdstuk geeft u een overzicht van beveiligingsarchitecturen en standaarden die uw organisatie kunnen helpen om op een gestructureerde wijze cloudcomputing te implementeren.

5.1 Security Architectuur

In deze paragraaf wordt een opsomming gegeven van een aantal architecturen die vanuit het oogpunt van beveiliging zijn opgesteld. Deze architecturen geven uw organisatie een startpunt en houvast op het moment dat u daadwerkelijk aan de slag gaat met cloudcomputing. Een architectuur zorgt voor een samenhang, doordat gewerkt wordt met gemeenschappelijke afspraken. We noemen deze afspraken 'architectuurprincipes' of kortweg 'principes'.

Specifiek voor beveiliging zijn er in de loop van de jaren een aantal raamwerken ontwikkeld. Dit zijn onder andere:

- Open Security Architecture (OSA, zie paragraaf 5.1.1);
- Sherwood Applied Business Security Architecture (SABSA) framework;
- Enterprise Information Security Architecture (EISA).

In paragraaf 5.1.1. wordt het 'Open Security Architecture' raamwerk toegelicht, omdat dit raamwerk een specifieke uitwerking beschrijft voor cloudcomputing.

5.1.1 Open Security Architecture: een open source architectuur

Op de website van de Open Security Architecture (OSA) is een beveiligingsarchitectuur te vinden, die gebaseerd is op open standaarden [47 en 48].

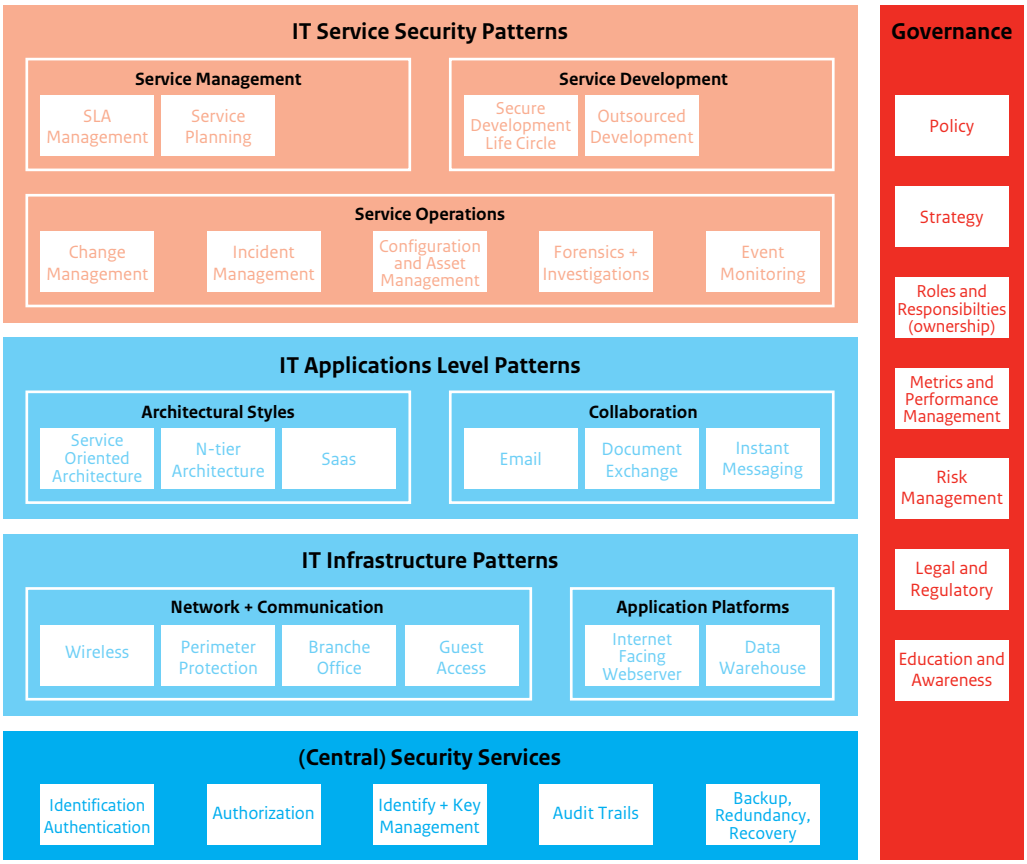
OSA componenten

OSA bevat een bibliotheek met 'patterns' (patronen), 'controls' (beheersmaatregelen), 'threats' (bedreigingen),' icons' (pictogrammen) en 'pattern templates' (patroon-sjablonen). Daarnaast identificeert OSA 'actors', dat zijn de functionarissen die een specifieke rol spelen in het beveiligingsproces.

Patronen

OSA definieert een patroon als een architectuuroplossing voor een probleem. Het is de bedoeling dat op termijn de patronen voor industry verticals geclusterd worden aangeboden, denk aan uitgewerkte securityarchitecturen voor branches als banken of logistieke organisaties.

De patronen zijn geclusterd in het pattern landscape (zie figuur 5-1) en bevatten oplossingen voor beveiligingsproblemen.



Figuur 5-1 Pattern Landscape

Ook maakt OSA zo veel mogelijk gebruik van andere standaarden, zoals de 'National Institute of Standards and Technology (NIST)[27] 800-53'-set, die als basis geldt voor de beheersmaatregelen binnen OSA. Daarnaast refereert OSA aan standaarden als CobiT[28] en de ISO 27002, door kruisverwijzingen binnen de architectuur.

Voorbeeld van een beheersmaatregel: SC-12 Cryptographic Key Establishment And Management Control: When cryptography is required and employed within the information system, the organization establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures.

Supplemental Guidance: NIST Special Publication 800-56 provides guidance on cryptographic key establishment. NIST Special Publication 800-57 provides guidance on cryptographic key management.
Control Enhancements: (0) None.
Baseline: LOW Not Selected MOD SC-12 HIGH SC-12
Family: System And Communications Protection
Class: Technical
ISO 17799 mapping[29]**:** 12.3.1, 12.3.2
COBIT 4.1 mapping: DS5.8

Een beheersmaatregel bevat achtereenvolgens:
- de beheerdoelstelling;
- extra richtlijnen eventueel aangevuld met een beschrijving van de risico's;
- aanvullende maatregelen ((0) None);
- de vast te stellen Baseline (geldig of niet);
- de categorie (System And Communications Protection);
- de klasse (technisch);
- de kruisverwijzing met ISO 17799 en CobiT 4.1.

5.2 ISO 27002 en andere standaarden

Tegenwoordig kunnen we niet meer om standaarden heen. Ook binnen het werkveld informatiebeveiliging en cloud-computing zijn er diverse nationale en internationale standaarden. In deze paragraaf wordt de relatie gelegd tussen de Code voor Informatiebeveiliging en diverse internationale standaarden.

De Code voor Informatiebeveiliging werd oorspronkelijk uitgegeven in 1994 en was gebaseerd op de conceptversie van BS 7799. Het biedt een uitgebreide verzameling maatregelen voor een goede implementatie (best practices) van informatiebeveiliging. De Code voor Informatie-beveiliging is bedoeld als het referentiepunt voor het vaststellen van de reeks beveiligingsmaatregelen die nodig zijn als informatiesystemen worden gebruikt.

NEN-ISO/IEC 27002:2007 nl 'Code voor Informatie-beveiliging' [10] is de geldende standaard (sinds 2007).

5.2.1 ISO/IEC 27002 en Open Security Architecture (OSA)

Zoals paragraaf 5.1.1 aangeeft, heeft de Open Security Architecture (OSA) een koppeling gelegd tussen beheersmaatregelen uit de ISO 27002 en die de OSA voor het patroon cloudcomputing heeft opgesteld. In Bijlage J: ISO 27002 is deze koppeling uitgewerkt.

5.2.2 ISO/IEC 27002 en Cloud Security Alliance Controls Matrix (CM)

De Cloud Security Alliance is een non-profit organisatie die is opgericht om het gebruik van best practices bij cloud-computing te bevorderen. Het biedt bewustwordings-programma's en educatie, zodat cloudcomputing op een veilige manier kan worden toegepast.
De Cloud Security Alliance Controls Matrix (CSA CM) [49] biedt een kader dat inzicht geeft in de beveiligingsconcepten en principes die zijn gerelateerd aan dertien domeinen. De CSA CM is om twee redenen samengesteld: Het biedt fundamentele beveiligingsprincipes aan cloudleveranciers en het helpt potentiële klanten van clouddiensten bij de beoordeling van het beveiligingsrisico van de cloudleverancier.

De basis voor de CSA CM ligt bij de beveiligingsstandaarden, zoals ISO 27001/27002, ISACA CoBiT en NIST. De CSA CM biedt organisaties de benodigde structuur, detaillering en duidelijkheid met betrekking tot informatiebeveiliging, toegesneden op de cloudindustrie.

De CSA CM koppelt de beheersmaatregelen uit ISO 27002 en geeft tevens aan wie verantwoordelijk is voor de beheersmaatregel, namelijk de klant of de cloudleverancier. In Bijlage J: ISO 27002 is deze koppeling uitgewerkt.

5.2.3 ISO/IEC 27002 en NIST Special Publication 800-53

Het 'National Institute of Standards and Technology' (NIST) is een onderdeel van het Amerikaanse Ministerie van Economische Zaken. NIST ontwikkelt standaarden voor Amerikaanse overheidsinstanties ter bevordering van de innovatie en industriële concurrentie in de VS.

27. NIST is een onderdeel van het Amerikaanse ministerie van Economische Zaken.
28. CoBiT staat voor 'Control Objectives for Information and related Technology' en is opgesteld door de Amerikaanse beroepsvereniging van IT-auditors en informatiebeveiligers 'Information Systems Audit and Control Association' (ISACA).
29. In de beschrijving wordt nog verwezen naar ISO17799 maar dit moet ISO27002 zijn.

Een relevante en bekende standaard van NIST betreft NIST SP 800-53 de 'Recommended Security Controls for Federal Information Systems'. Deze standaard somt de minimale beveiligingsmaatregelen op, die nodig zijn voor een acceptabel niveau van informatiebeveiliging. In de NIST SP 800-53 is een koppeling gelegd met de beheersmaatregelen uit de ISO 27002.

5.2.4 Checklist(s)

Deze paragraaf beschrijft twee checklists die u kunnen helpen om in te schatten, in hoeverre uw cloudleverancier voldoet aan de beschreven standaarden.

Code voor Informatiebeveiliging

Er is een gestructureerde checklist [50] beschikbaar die gebaseerd is op een eerdere versie van de Code voor informatiebeveiliging[30]. Deze kan uw organisatie gebruiken om een zo'n compleet mogelijk overzicht te krijgen van vragen die uw organisatie en/of de cloud-leverancier moet(en) beantwoorden. Ondanks het feit dat deze checklist niet is gebaseerd op ISO 27002, geeft het een goed beeld van het type vragen en dekt deze checklist het overgrote deel van ISO 27002 af.

Cloudcomputing: Benefits, risks and recommendations for information security

Het document 'Cloudcomputing: Benefits, risks and recommendations for information security' dat ENISA in november 2009 publiceerde [22], bevat ook een compleet overzicht met relevante vragen, dat als uitgangspunt kan fungeren om een checklist samen te stellen. De vragen in dit document zijn gebaseerd op de ISO 27001[31] [25], ISO 27002[32] en BS 25999[33].

30. Code voor Informatiebeveiliging:2000 – Deel 1, een vertaling van de Britse standaard BS7799 d.d. september 2000.
31. 27001:2005, ISO/IEC Information technology - Security techniques - Information security management systems - Requirements.
32. 27002:2005, ISO/IEC Information technology - Security techniques - Code of practice for information security management.
33. Group, BSI BS 25999 Business Continuity.

Bijlagen

Afkortingen

A	
AICPA	American Institute of Certified Public Accountants
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
API	Application programming interface
AES	Advanced Encryption Standard
AWS	Amazon Web Services
B	
BAU	Business as Usual
BI	Business Intelligence
BIV	Beschikbaarheid, integriteit en vertrouwelijkheid
BPOS	Business Productivity Online Standard Suite
BZK	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
C	
CAPEX	Capital Expenses / Capital Expenditure
CBP	College bescherming persoonsgegevens
CoBiT	Control Objectives for Information and related Technology
CP	Cloud Provider
CPU	Central Processing Unit
CRM	Customer Relation Management
CSA	Cloud Security Alliance
CSA CM	Cloud Security Alliance Controls Matrix
D	
DGV	Directoraat-Generaal Veiligheid
DWR	Digitale Werkplek/Werkomgeving Rijk
E	
EC2	Elastic Compute Cloud
ENISA	European Network and Information Security Agency
ERP	Enterprise Resource Planning
F	
FTP	File Transfer Protocol
G	-
H	
HR	Human Resource
HTTP	Hypertext Transfer Protocol
I	
IaaS	Infrastructure as a service
IBF	Informatiebeveiligingsfunctionaris
ICT	Informatie- en Communicatietechnologie
IETF	Internet Engineering Task Force
IPSec	IP Security
ISACA	Information Systems Audit and Control Association
ISF	Information Security Forum
ISMS	Information Security Management System
J	-
K	-
L	
LDAP	Lightweight Directory Access Protocol
M	-
N	
NBA	Nederlandse Beroepsorganisatie van Accountants
NIST	National Institute of Standards and Technology
NOREA	Nederlandse Orde van Register EDP-Auditors
O	
OPEX	Operating Expenses / Operating Expenditure
OASIS	Organization for the Advancement of Structured Information Standards
OSA	Open Security Architecture
P	
PaaS	Platform as a Service
PCI-DSS	Payment Card Industry - Data Security Standards
PUE	Power usage effectiveness
Q	
QoS	Quality of Service
R	
RDS	Relational Database Service
RIVM	Rijksinstituut voor Volksgezondheid en Milieu
RSA	Ronald Rivest, Adi Shamir, and Leonard Adleman

S	
S3	Simple Storage Service
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SAS70	Statement on Auditing Standards Number 70
SGO	Secretaris Generaal Overleg
SLA	Service Level Agreement
SMTP	Simple Mail Transfer Protocol
SNS	Simple Notification Service
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SQL	Structured Query Language
SQS	Simple Queue Services
SSL	Secure Sockets Layer
T	-
TCO	Total Cost of Ownership
TCP/IP	Transmission Control Protocol (TCP) en het internetprotocol (IP).
TLS	Transport Layer Security
U	-
V	
VDI	Virtuele Desktop Infrastructuur
Vir	Voorschrift Informatiebeveiliging Rijksdienst
Vir-bi	Voorschrift Informatiebeveiliging Rijksdienst - Bijzondere Informatie
VLAN	Virtual Local Area Networks
VoRa	Voorlichtingsraad
VPC	Virtual Private Cloud
VPLS	Virtual Private LAN Service
VPN	Virtual Private Network
W	
Wbp	Wet bescherming persoonsgegevens
WCC	Wetsvoorstel Computercriminaliteit
W3C	World Wide Web Consortium
WOB	Wet Openbaarheid Bestuur
X	
XML	Extensible Markup Language
Y	-
Z	
ZBO	Zelfstandig Bestuursorgaan

Literatuurlijst

[1] Dossier 26 643 Informatie- en communicatie-technologie (ICT), nummer 157 'MOTIE VAN HET LID VAN DER BURG C.S.', voorgesteld 19 mei 2010
> https://zoek.officielebekendmakingen.nl/kst-26643-157.html

[2] 'Kamerbrief over cloud computing', 20 april 2011
> http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2011/04/20/kamerbrief-over-cloud-computing.html

[3] Dossier 31 490 Vernieuwing van de rijksdienst, nummer 54 ' Het uitvoeringsprogramma compacte rijksdienst.', 14 februari 2011
> https://zoek.officielebekendmakingen.nl/dossier/31930/kst-31490-54.html

[4] Ministerie van Financiën 'Rapport brede heroverwegingen: 19. Bedrijfsvoering', d.d. april 2010
> https://minfin.nl/Onderwerpen/Begroting/Brede_heroverwegingen/19_Bedrijfsvoering_inclusief_ZBO_s

[5] www.rijksoverheid.nl 'Uitgangspunten online communicatie rijksambtenaren', d.d. 30 juni 2010[34]
> http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2010/06/30/uitgangspunten-online-communicatie-rijksambtenaren.html

[6] The Open Group 'Cloud Buyers' Requirements Questionnaire', d.d. juli 2010
> https://www2.opengroup.org/ogsys/jsp/publications/PublicationDetails.jsp?publicationid=12236

[7] The Open Group 'Cloud Buyers' Decision Tree', d.d. juli 2010
> https://www2.opengroup.org/ogsys/jsp/publications/PublicationDetails.jsp?publicationid=12235

[8] Wet bescherming persoonsgegevens, d.d. 6 juli 2000
> http://wetten.overheid.nl/BWBR0011468

[9] 'Voorschrift informatiebeveiliging rijksdienst – bijzondere informatie', d.d. maart 2004
> http://wetten.overheid.nl/BWBR0016435

[10] Nederlands Normalisatie-instituut (www.nen.nl) 'NEN-ISO/IEC 27002:2007 nl - Informatietechnologie - Beveiligingstechnieken - Code voor informatiebeveiliging', d.d. 1 november 2007
> http://www.nen.nl/web/Normshop/Norm/NENISOIEC-270022007-nl.htm

[11] Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, d.d. 23 november 1995
> http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:NL:HTML

[12] Mededeling van de commissie aan het Europees Parlement, de raad, het Europees economisch en sociaal comité en het comité van de regio's 'Een integrale aanpak van de bescherming van persoonsgegevens in de Europese Unie', d.d. 4 november 2010
> http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_nl.pdf

[13] College bescherming persoonsgegevens (CBP) 'Achtergrond Studies en Verkenningen 23 (AV-23)', d.d. april 2001
> http://www.cbpweb.nl/downloads_av/AV23.pdf

[14] College bescherming persoonsgegevens (CBP) 'CBP Richtsnoeren publicatie van persoonsgegevens op internet', d.d. december 2007
> http://www.cbpweb.nl/downloads_rs/rs_20071211_persoonsgegevens_op_internet_definitief.pdf

[15] College bescherming persoonsgegevens (CBP) 'CBP Richtsnoeren Actieve openbaarmaking en eerbiediging van de persoonlijke levenssfeer', d.d. 13 augustus 2009
> http://www.cbpweb.nl/downloads_rs/rs_20090813_actieve_openbaarmaking.pdf

[16] 'Besluit Voorschrift informatiebeveiliging Rijksdienst 2007', d.d. 1 juli 2007
> http://wetten.overheid.nl/BWBR0016435

[17] National Institute of Standards and Technology (NIST) 'SP800-145 - DRAFT Definition of Cloud Computing', d.d. januari 2011
> http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf

34. De website Communicatieplein.nl zal per 1 januari 2011 ophouden te bestaan als aparte website. De content wordt gemigreerd naar Rijksoverheid.nl en Rijksportaal.

[18] Burton Group 'Cloudcomputing : Transforming IT', d.d. 20 april 2009
> http://www.burtongroup.com/Guest/Cloud/CloudComputingOverview.aspx

[19] > http://cloudtaxonomy.opencrowd.com/taxonomy/software-as-a-service

[20] > http://cloudtaxonomy.opencrowd.com/taxonomy/platform-as-a-service

[21] >http://cloudtaxonomy.opencrowd.com/taxonomy/infrastructure-as-a-service

[22] ENISA 'Cloudcomputing: Benefits, risks and recommendations for information security', d.d. november 2009
> http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

[23] CSA 'Top Threats Cloudcomputing', d.d. maart 2010
> http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[24] Gartner 'Assessing the Security Risks of Cloudcomputing' d.d. juni 2008
> http://www.gartner.com/DisplayDocument?id=685308

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

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

[27] 'Statement on Auditing Standards (SAS) No. 70'
> http://sas70.com

[28] 'International Standards for Assurance Engagements (ISAE) No. 3402'
> http://isae3402.com
en KPMG - Compact 'SAS 70 herzien, focus ISAE 3402 blijft op beheersingsmaatregelen financiële verantwoording', d.d. 2010
> http://www.compact.nl/artikelen/C-2010-1-Beek.htm

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

[30] SURFnet/Kennisnet Innovatieprogramma 'Rapport De wolk in het onderwijs : Privacy aspecten bij cloud computing services', d.d. maart 2011
> http://www.surfnet.nl/nl/nieuws/pers/Pages/Privacyisaandachtspuntbijgebruikclouddiensten.aspx

[31] Speech Neelie Kroes aan Université Paris-Dauphine 'Cloud computing and data protection', d.d. 25 November 2010
> http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/686

[32] The U.S.-EU & U.S.-Swiss Safe Harbor Frameworks
> http://www.export.gov/safeharbor

[33] Forrester Research 'Do You Know Where Your Data Is In The Cloud?'
http://www.forrester.com/cloudprivacyheatmap

[34] Volkskrant 'Twittergegevens WikiLeaks-sympathisanten opgevraagd door VS', d.d. 8 januari 2011
> http://www.volkskrant.nl/vk/nl/3884/WikiLeaks/article/detail/1790177/2011/01/08/Twittergegevens-WikiLeaks-sympathisanten-opgevraagd-door-VS.dhtml

[35] Microsoft 'Trust Center: Security, Privacy and Compliance Information for Microsoft Online Services.'
> http://www.microsoft.com/online/legal/v2/?docid=23

[36] CA Technologies en Ponemon Institute 'Security of Cloud Computing Providers Study', d.d. april 2011
> http://www.ca.com/~/media/Files/IndustryResearch/security-of-cloud-computing-providers-final-april-2011.pdf

[37] AIVD 'Kwetsbaarheidsanalyse spionage - Spionagerisico's en de nationale veiligheid', d.d. 1 april 2010
> https://www.aivd.nl/publish/pages/1627/kwetsbaarheidsanalysespionageapril2010.pdf

[38] Speech Neelie Kroes tijdens Open Forum Europe 2010 Summit: 'Openness at the heart of the EU Digital Agenda', d.d. 10 juni 2010
> http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/300

[39] > http://webwereld.nl/nieuws/106548/hyves-onderuit-door-falend-datacenter-evoswitch---update.html

[40] > http://webwereld.nl/nieuws/106486/data-definitief-verloren-na-storing-amazon.html

[41] > http://webwereld.nl/nieuws/106456/veel-websites-offline-door-storing-amazon.html

[42] > http://www.telegraaf.nl/digitaal/9608884/__Sites_offline_door_storing_Amazon__.html

[43] > http://webwereld.nl/nieuws/106529/megastoring-amazon-ec2-door-menselijke-fout.html

[44] RSA 'Open Letter to RSA Customers', d.d. 17 maart 2011
> http://www.rsa.com/node.aspx?id=3872

[45] ECP.NL 'Bewaren en bewijzen', ISBN 978-90-76957-21-0 d.d. maart 2007
> www.ecp.nl/sites/default/files/BewarenBewijzen.pdf

[46] Summary of the Amazon EC2 and Amazon RDS Service Disruption in the US East Region
> http://aws.amazon.com/message/65648/

[47] > http://www.opensecurityarchitecture.org

[48] > http://www.opensecurityarchitecture.org/cms/library/patternlandscape/251-pattern-cloud-computing

[49] Cloud Security Alliance 'CSA Cloud Controls Matrix V1.1', d.d. 15 december 2010
> http://www.cloudsecurityalliance.org/cm.html

[50] Checklist 'Code voor Informatiebeveiliging:2000 - Deel 1'
> http://www.euronet.nl/users/ernstoud/praktijkgids/Checklist%20D1.pdf

[51] GovCERT.NL Factsheet 'Massale SQL injectie aanvallen' versie 1.0, d.d. 23 juni 2008
> http://www.govcert.nl/dienstverlening/Kennis+en+publicaties/factsheets/massale-sql-injectie-aanvallen.html

[52] Forum Standaardisatie 'Expertadvies SAML v 2.0', d.d. 19 februari 2009
> http://www.open-standaarden.nl/fileadmin/os/documenten/FS21-09-05%20bijlage%2007%20Expertadvies%20SAML.pdf

[53] > http://nl.wikipedia.org/wiki/Xml

[54] > http://nl.wikipedia.org/wiki/SOAP

[55] > http://nl.wikipedia.org/wiki/LDAP

[56] GovCERT.NL factsheet 'Bescherm uw online dienst(en) tegen (d)DoS-aanvallen', versie 1.1, 3 januari 2011
> http://www.govcert.nl/dienstverlening/Kennis+en+publicaties/factsheets/factsheet-over-bescherming-tegen-dos-aanvallen.html

BIJLAGE C

De Cloud Security Alliance, ENISA en Gartner

In de publicatie van European Network and Information Security Agency (ENISA) [22], worden 24 risico's onderkend, die zijn onderverdeeld in de volgende drie categorieën: beleid en organisatorische risico's, technische risico's en juridische risico's. Hieronder volgt een overzicht van de 24 risico's en de toegepaste onderverdeling:

1 Policy and organizational risks
- R.1 Lock-in;
- R.2 Loss of governance;
- R.3 Compliance challenges;
- R.4 Loss of business reputation due to co-tenant activities;
- R.5 Cloud service termination or failure;
- R.6 Cloud provider acquisition;
- R.7 Supply chain failure.

2 Technical risks
- R.8 Resource exhaustion (under or over provisioning);
- R.9 Isolation failure;
- R.10 Cloud provider malicious insider - abuse of high privilege roles;
- R.11 Management interface compromise (manipulation, availability of infrastructure);
- R.12 Intercepting data in transit;
- R.13 Data leakage on up/download, intra-cloud;
- R.14 Insecure or ineffective deletion of data;
- R.15 Distributed denial of service (DDoS);
- R.16 Economic denial of service (EDOS);
- R.17 Loss of encryption keys;
- R.18 Undertaking malicious probes or scans;
- R.19 Compromise service engine;
- R.20 Conflicts between customer hardening procedures and cloud environment.

3 Legal risks
- R.21 Subpoena and e-discovery;
- R.22 Risk from changes of jurisdiction;
- R.23 Data protection risks;
- R.24 Licensing risks.

Hieronder volgt een overzicht met de top security risico's die zijn onderkend door ENISA en die zijn gebruikt bij het opstellen van dit document.

Top Security Risks (European Network and Information Security Agency - ENISA)
- Loss of governance;
- Vendor Lock-In;
- Isolation failure;
- Compliance risks;
- Management interface compromise;
- Data protection;
- Insecure or incomplete data deletion;
- Malicious insider;
- Performing audits / IT forensics.

In de publicatie van de Cloud Security Alliance (CSA) [23] wordt een overzicht gegeven van de grootste bedreigingen en die zijn gebruikt bij het opstellen van dit document.

Top Threats Cloudcomputing (CSA version 1.0)
- Threat #1: Abuse and Nefarious Use of Cloudcomputing;
- Threat #2: Insecure Interfaces and APIs;
- Threat #3: Malicious Insiders;
- Threat #4: Shared Technology Issues;
- Threat #5: Data Loss or Leakage;
- Threat #6: Account or Service Hijacking;
- Threat #7: Unknown Risk Profile.

In de publicatie van Gartner [21] wordt een overzicht gegeven van specifieke veiligheidsproblemen die organisaties moeten adresseren bij cloudleveranciers voordat de cloudleverancier wordt gekozen en die zijn gebruikt bij het opstellen van dit document.

Seven Cloudcomputing security Risk (Gartner)
- Privileged user access;
- Regulatory compliance;
- Data location;
- Data segregation;
- Recovery;
- Investigative support;
- Long-term viability.

Achtergrondinformatie over Virtualisatie

Virtualisatie is een veel gebruikte methode om een cloud-infrastructuur te implementeren, maar wat houdt dit nu eigenlijk in? In deze bijlage geven we een korte introductie.

Virtualisatie maakt het mogelijk dat meerdere besturingssystemen gelijktijdig, in een geïsoleerde omgeving, op één (fysieke) computer kunnen draaien, waarbij elk systeem *denkt* dat het alleen op het eigen systeem draait. Dat is mogelijk door middel van een hypervisor (zie kader). Een besturingsysteem ziet geen verschil tussen een virtuele machine en een fysieke machine, dat geldt ook voor de applicaties of andere computers in een netwerk. Zelfs de virtuele machine denkt dat het een 'echte' computer is. Toch is een virtuele machine volledig uit software samengesteld en bevat het geen hardwarecomponenten.

Hypervisor
Een hypervisor, is de virtuele machinemanager, die het mogelijk maakt om meerdere besturingssystemen, virtuele machines, gelijktijdig op één fysieke computer te laten draaien. Het hoofdbesturingssysteem wordt de 'host' genoemd en het besturingssysteem dat in de virtuele omgeving draait, heet de 'gast'.

Ieder afzonderlijk gastbesturingssysteem lijkt volledig te beschikken over de hardware zoals de processor, het geheugen, harde schijf en alle andere hardware componenten van de computer. Het is echter de hypervisor die deze hardware van de computer beheert. Ook wijst de hypervisor aan verschillende gastbesturingssystemen de noodzakelijke capaciteit toe en voorkomt de hypervisor, dat gastbesturingssystemen elkaar kunnen verstoren.

Waarom virtualiseren?
Virtualisatie heeft technische en zakelijke voordelen. De zakelijke voordelen vloeien voort uit de technische voordelen van virtualisatie.

Technische voordelen
Over het algemeen beschikken virtuele machines over technische kenmerken die de organisatie ten goede komen. Het gaat dan om de volgende kenmerken.

- *Isolatie*
  Hoewel virtuele machines de fysieke hardware componenten van een enkele computer delen, blijven ze volledig geïsoleerd van elkaar als waren het aparte fysieke machines.

  Als bijvoorbeeld een van de virtuele machines crasht, blijven de overige virtuele machines beschikbaar. Isolatie is een belangrijke reden waarom de beschikbaarheid en beveiliging van applicaties die draaien in een virtuele omgeving hoger is dan bij traditionele niet-gevirtualiseerde systemen.

- *Inkapseling*
  Een virtuele machine is in feite een geïsoleerde software-container die een complete set van virtuele hardware, een besturingssysteem en alle geïnstalleerde toepassingen binnen een softwarepakket bundelt ('inkapselt').

  Inkapseling maakt virtuele machines overdraagbaar en eenvoudig te beheren. Het is bijvoorbeeld mogelijk om een virtuele machine van de ene locatie naar een andere locatie te verplaatsen of te kopiëren zoals alle andere bestanden.

- *Hardware-onafhankelijkheid*
  Virtuele machines zijn volledig onafhankelijk van hun onderliggende fysieke hardware. U kunt bijvoorbeeld een virtuele machine configureren met virtuele hardware componenten (bijvoorbeeld CPU en netwerkkaart) die volledig verschillen van de fysieke componenten van de computer (onderliggende hardware).

- *Standaardisatie*
  Een bijkomend voordeel van de hardware onafhankelijkheid van de virtuele machine in relatie tot de hardware van de computer is, dat deze onafhankelijkheid ook geldt voor de toepassingen die op de virtuele machine draaien. Door deze onafhankelijkheid is het mogelijk om de virtuele hardware identiek te configureren. Dat maakt ook standaardiseren gemakkelijker. Bij het implementeren van een toepassing hoeft dus maar met één configuratie van de virtuele hardware rekening worden gehouden.

Weeg steeds af wat er kan gebeuren en welk risico uw organisatie loopt als deze technische mechanismen falen.

Zakelijke voordelen
Virtualisatie heeft drie belangrijke zakelijke voordelen: een lagere *total cost of ownership* (TCO), verhoogde beschikbaarheid en verbeterde flexibiliteit van uw organisatie. De kostprijs is meestal de belangrijkste overweging voor een organisatie om gebruik te maken van virtualisatie. Deze zijn natuurlijk in lijn met de voordelen die te behalen zijn door cloudcomputing. Virtualisatie is immers één van de manieren om cloudcomputing te implementeren.

Overige voordelen zijn:
- toenemende utilisatie van de hardware wat resulteert in een efficiënter gebruik van middelen;
- loadbalancing van gebruikers;
- hogere beschikbaarheid;
- disaster/recoveryprocedures eenvoudiger en sneller;
- vermindering van het energieverbruik;
- ruimtebesparing in de computerruimte (datacenter);
- vermindering van uw licenties kosten en andere aanloopkosten;
- verlagen van operationele kosten voor onderhoud en beheer;
- dynamische uitbreiding fysieke server bij grotere belasting.

Aandachtspunten van virtuele machines
In deze paragraaf gaan we in op een aantal aandachtspunten, die van belang zijn als u kiest voor virtualisatie. Gaat u gebruik maken van een clouddienst, dan komen deze nadelen natuurlijk voor rekening van de cloudleverancier.

- *Introductie van een nieuw Single Point of Failure*
  Het grootste nadeel van virtualisatie is een mogelijke hardwarestoring. Dit heeft namelijk effect op alle virtuele machines die op de computer zijn geïnstalleerd en dus ook op de toepassingen die binnen deze virtuele omgevingen draaien. Een voordeel is wel dat virtuele machines weer snel online kunnen zijn op een andere computer.

- *Inzicht in piekbelasting is belangrijk*
  U moet op de hoogte zijn van de piekbelasting van iedere individuele virtuele machine. Met deze informatie kunt u een verdeling maken, zodat de virtuele machines zo optimaal mogelijk worden verdeeld over de fysieke computers. Het is belangrijk, dat de computer over voldoende hulpmiddelen beschikt om de piekbelasting op te vangen.

- *Virtualisatie stelt hogere eisen aan de hardware*
  Een aandachtspunt dat nauw samenhangt met het vorige (opvangen piekbelasting) is, dat er extra eisen worden gesteld aan de hardware. Denk hierbij aan extra geheugencapaciteit, opslagcapaciteit en netwerkbandbreedte.

- *Patchmanagement wordt complexer*
  Installeer op alle virtuele machines het hostbesturingssysteem en de relevante patches (beveiligingsadviezen). Die zorgen voor een stabiele en veilige omgeving[35].
  U moet ook weten welke virtuele omgevingen zijn geïnstalleerd en welke toepassingen hierop draaien. U kunt dan een juiste afweging maken, of een beveiligingsadvies voor u van toepassing is of niet.

- *Virtualisatie heeft gevolgen voor uw licenties*
  Virtualisatie maakt het eenvoudig om een nieuwe virtuele omgeving te implementeren. Houd wel rekening met het aantal licenties waarover u beschikt, met andere woorden: wat zijn de licentievoorwaarden.

35. Zie ook whitepaper 'Patch Management', versie 1.1, d.d. 23 juni 2008. http://www.govcert.nl/dienstverlening/Kennis+en+publicaties/whitepapers/patch-management.html

Handige vragen en aandachtspunten

Bijlage E hoort bij hoofdstuk 4 'Beveiligingsaspecten van clouddiensten' en volgt de indeling van de onderwerpen uit dat hoofdstuk. De keuze van uw organisatie voor een bepaald type cloudmodel (privaat, publiek, community of hybride) en soort clouddienst (SaaS, PaaS of IaaS) is van invloed op welke aandachtspunten uit hoofdstuk 4 specifiek van toepassing zijn op uw organisatie. In deze bijlage vindt u een lijst met punten aan de hand waarvan u kunt inschatten, welke maatregelen u daar tegen kunt nemen. N.B. Leg overeengekomen afspraken altijd helder en eenduidig vast in contracten en/of SLA's met de cloudleverancier.

Naleving van wet- en regelgeving (zie 4.1)
Vanwege de complexiteit van dit onderwerp adviseren wij u om juridische expertise in te schakelen, zodat u later niet voor ongewenste verassingen komt te staan.

Overzicht wet en regelgeving
Zorg er altijd voor dat uw organisatie beschikt over een actueel overzicht van wet- en regelgeving, standaarden, richtlijnen, gedragscodes en certificeringen waar uw organisatie aan moet voldoen. Stel op basis van dit overzicht vast welke eisen aan uw bedrijfsvoeringen worden gesteld en welke maatregelen uw organisatie moet implementeren om aan deze eisen te voldoen. Alle (belangrijke) ICT-resources moeten een eigenaar hebben die verantwoordelijk is voor het handhaven van het juiste beveiligingsniveau en –maatregel.

Classificatie van gegevens
Uw gegevens moeten zijn geclassificeerd (gerubriceerd) zodat deze worden voorzien van het juiste beveiligingsniveau. Hierbij zijn wet- en regelgeving en de betrouwbaarheidseisen die uw organisatie aan deze gegevens stelt, een belangrijk uitgangspunt. Op basis van deze classificatie (rubricering) moet uw organisatie vaststellen, welke gegevens wel en welke niet in de cloud geplaatst mogen worden.Breng daarnaast in kaart welke processen, procedures en maatregelen door de cloudleverancier minimaal geïmplementeerd moet zijn, zodat u blijft voldoen aan geldende wet- en regelgeving, standaarden, richtlijnen, gedragscodes en certificeringen.

Zorg dat u antwoorden krijgt op onderstaande, niet eindige lijst, met vragen op het moment dat u gebruik gaat maken van clouddiensten:

- Hebt u inzicht welke beperkingen gelden voor de gegevens die u in de cloud gaat onderbrengen?
- Kunt u aangeven in welke rechtsgebieden uw gegevens wel en in welke juist niet mogen worden opgeslagen?
- Mogen persoonsgegevens worden doorgegeven naar of verwerkt worden in landen buiten de EU?
- Indien persoonsgegevens buiten de EU worden verwerkt, in hoeverre worden die gegevens dan in de praktijk daadwerkelijk beschermd door het Europese recht?
- Moeten medewerkers van de cloudleverancier geheimhoudingsverklaringen ondertekenen, een Verklaring Omtrent het Gedrag (VOG) overhandigen, AIVD of MIVD[36] gescreend zijn?

Op het moment dat de classificaties en de bijbehorende maatregelen zijn vastgesteld, weet u hoe uw gegevens moet worden behandeld en beschermd. Als u gebruik gaat maken van clouddiensten, moet dit beveiligingsniveau natuurlijk gewaarborgd blijven en mag het niet in gevaar worden gebracht. Om inzicht te verkrijgen of de cloudleverancier kan voldoen aan uw eisen, moet de cloudleverancier inzicht geven in zijn bedrijfsvoering. Eisen aan cloudleverancier Hieronder volgt een aantal aandachtspunten en vragen om vast te stellen of de cloudleverancier voldoet aan eisen op het gebied van wet- en regelgeving.

Informatiebeveiligingsbeleid
In het informatiebeveiligingsbeleid van de cloudleverancier moet beschreven zijn aan welke wet- en regelgeving wordt voldaan en hoe dit wordt gewaarborgd. Bij een internationaal opererende organisatie moet dit ook voor de verschillende rechtsgebieden zijn beschreven. Overige onderwerpen die in het informatiebeveiligingsbeleid beschreven moeten worden in relatie tot naleving van wet- en regelgeving, zijn:

- Beveiliging van de data;
- Export(beperkingen) van de data;
- Het bewaren en vernietigen van de data (wettelijke bewaar- en vernietigingstermijn);
- Het uitvoeren/toestaan van zowel in- als externe audits;
- Het toestaan van digitaal (forensisch) onderzoek.

Het beleid moet ook aangegeven hoe wordt omgegaan met (open) standaardtechnologieën en -oplossingen. Voor de Rijksoverheid geldt het 'pas toe of leg uit'-principe met betrekking tot open standaarden[37].

Wet- en regelgeving
De cloudleverancier moet u voldoende inzicht geven hoe hij zorg draagt dat hij aan wet- en regelgeving voldoet, zodat u de impact op uw organisatie hiervan kan inschatten. Heeft de cloudleverancier bijvoorbeeld een eigen juridische afdeling en/of compliance officer?

36. AIVD staat voor Algemene Inlichtingen- en Veiligheidsdienst en MIVD voor Militaire Inlichtingen- en Veiligheidsdienst.
37. Actieplan Nederland Open In Verbinding (NOIV), d.d. december 2007.

Geeft de cloudleverancier u voldoende informatie in welke rechtsgebieden de gegevens mogelijk worden opgeslagen? Kunt u als cloudgebruiker aangeven in welke rechtsgebieden uw gegevens wel (bijvoorbeeld in Nederland of Europese Unie) en in welke rechtsgebieden ze juist niet mogen worden opgeslagen (bijvoorbeeld de Verenigde Staten)?

Partners (onderaannemers)
Om vast te stellen of u ook blijft voldoen aan wet- en regelgeving als de cloudleverancier met partners (onderaannemers) werkt, moet de cloudleverancier over een actueel overzicht van zijn partners beschikken en u daarin volledig inzicht geven. De cloudleverancier moet ook aangeven hoe hij waarborgt dat zijn partners voldoen aan wet- en regelgeving.

Audits en security scans
Om vast te stellen of de cloudleverancier voldoet aan de afspraken die zijn vastgelegd in contracten en/of SLA's, moet hij (externe) audits toestaan. Dit geldt ook voor de eventuele partners van de cloudleverancier.

Om niet afhankelijk te zijn van de, bijvoorbeeld jaarlijkse uitgevoerde, (externe) audit bij de cloudleverancier, moet hij op regelmatige basis security scans, bijvoorbeeld vulnerability en policy compliancy scans, uitvoeren en u hierover op regelmatige basis rapporteren. Denk hierbij aan rapportages van de resultaten van deze security scans, geïnstalleerde (beveiligings)updates en patches en veiligheidsincidenten.

Beheersbaarheid van processen en systemen (zie 4.2)
Vertrouwen in de cloudleverancier is belangrijk bij uitbesteding van diensten, systemen en informatie naar de cloud. Alleen als u vertrouwen heeft in de cloudleverancier, bent u wellicht onder bepaalde voorwaarden bereid een deel van uw controle en beheersbaarheid van processen en systemen af te staan. Een grondige selectie van de cloudleverancier, zoals beschreven in paragraaf 2.2 'Kiezen voor cloudcomputing', is dan ook van cruciaal belang.

Om te bepalen onder welke voorwaarden u bereid bent om processen en systemen onder te brengen in de cloud moet u hiervoor beleid formuleren. Dit beleid moet ook beschrijven hoe uw organisatie dit beleid op naleving gaat controleren.

Onderstaand een niet eindige lijst met aandachtspunten en vragen aan de hand waarvan u, tijdens het selectieproces van de cloudleverancier, kunt inschatten in welke mate u controle en beheersmogelijkheden verliest en welke maatregelen u daartegen kunt nemen. Houd wel steeds in uw achterhoofd dat uw organisatie altijd eindverantwoordelijk blijft voor bijvoorbeeld de data of diensten die in de cloud worden geplaatst.

Taken, bevoegdheden en verantwoordelijkheden
De taken, bevoegdheden en verantwoordelijkheden van relevante functies en rollen van uw organisatie en de cloudleverancier moeten duidelijk zijn afgebakend en gedocumenteerd. Dit voorkomt onduidelijkheid en verwarring over wie nu welke taken uitvoert, zodat hierover later geen discussie kan ontstaan.

De uitvoering van bepaalde taken (of verantwoordelijkheden) moet gescheiden worden en worden verdeeld over meer personen zodat de kans op ongeautoriseerde wijzigingen of misbruik van informatie of diensten wordt verkleind. Functiescheiding vermindert het risico van nalatigheid en opzettelijk misbruik van systemen. Fraudegevoelige activiteiten moeten worden gescheiden, zodat minimaal samenspanning tussen meer personen nodig is om te kunnen frauderen. Denk hierbij bijvoorbeeld aan het aanvragen en accorderen van gebruikersaanvragen, het uitvoeren van het operationeel beheer en uitvoeren van audits.

Verantwoordelijkheden met betrekking tot juridische aangelegenheden moeten vastgelegd zijn. Denk aan privacywetgeving, dit is met name van belang op het moment dat het contract betrekking heeft op samenwerking met cloudleveranciers in andere landen (verschillende rechtsgebieden).

Overeenkomsten, contracten en SLA's
Zorg vooraf dat u beschikt over een lijst met afspraken die absoluut in het contract of de SLA opgenomen moeten worden.

Dienstenniveau
Maak goede afspraken over het dienstenniveau van de cloudleverancier en leg ze vast in een SLA. Denk hierbij aan openingstijden, bereikbaarheid en reactietijd van de incidentmelding en afhandeling, escalatieprocedures, beveiligingseisen, het recht op audit.

Beveiligingseisen
Leg beveiligingseisen vast in een contract of een SLA als uw organisatie alle of een deel van haar diensten, informatiesystemen, netwerken en /of gegevens in de cloud onderbrengt.

Clausules
Zorg dat u weet of de cloudleverancier SLA's heeft afgesloten met klanten, waarin clausules met tegenstrijdige beloften aan verschillende belanghebbenden zijn opgenomen. Welke klanten worden bijvoorbeeld het eerste geholpen bij een incident dat optreedt bij de cloudleverancier? Veel leveranciers hebben namelijk niet voldoende capaciteit om alle klanten gelijktijdig te ondersteunen. Ze geven dan meestal voorrang aan belangrijke of grote klanten.

Gebruiksvoorwaarden
Zorg dat de gebruiksvoorwaarden volledig helder zijn, zodat u later niet voor verrassingen komt te staan. Denk hierbij aan: privacyaspecten, geldende voorwaarden, (uitsluiting van) aansprakelijkheid, te leveren producten en diensten, disclaimers, verwachtingen en intentieverklaringen.
Laat de juridische afdeling van uw organisatie, de gebruikersvoorwaarden, contracten en SLA's bestuderen.

Classificatie van gegevens
Zorg dat uw data is geclassificeerd en leg vast welke maatregelen de cloudleverancier moet nemen om uw beveiligingseisen, voortkomend uit de classificatie, te waarborgen

Escrow
Zorg dat er een escrow-overeenkomst wordt afgesloten, zodat het voorbestaan van uw organisatie niet in gevaar komt op het moment dat de cloudleverancier de afgesproken diensten niet meer kan of wil leveren.

Audits
Om vast te stellen of de cloudleverancier voldoet aan de afspraken die zijn vastgelegd in contracten en/of SLA's, moet hij (externe) audits toestaan. Denk hierbij aan loggegevens en audittrails van de acties die de cloudleverancier heeft uitgevoerd. Dit geldt ook voor de eventuele partners van de cloudleverancier.

Beleid, processen, technologieën en oplossingen
Zorg dat u weet welke technologieën en oplossingen de cloudleverancier heeft geïmplementeerd. Vanwege de interoperabiliteit en portabiliteit gaat hierbij de voorkeur uit naar open standaarden en -oplossingen. Denk aan standaarden (best practices) bij de beveiliging van systemen (hardening).

Zorg dat u weet welke maatregelen de cloudleverancier heeft geïmplementeerd om kwetsbaarheden te detecteren (vulnerability assessment).

Zorg dat u weet welke beheerprocessen bij de cloudleverancier zijn ingericht en op welke manier dat is gerealiseerd. Denk aan toegangsbeheer (authenticatie en autorisatie), incidentbeheer, wijzigingsbeheer, patchmanagement en back-up & recovery.

Wet- en regelgeving
Zorg dat u inzicht heeft in en informatie krijgt over de rechtsgebieden (jurisdicties) waar uw gegevens zijn opgeslagen, vanwege geldende (privacy) wet- en regelgeving waaraan uw organisatie zich moet houden.

Worden audittrails en soortgelijk bewijsmateriaal verzameld en veilig opgeslagen? Dit in verband met:
- Uitvoeren van probleemanalyse(s).
- Gebruik als bewijsmateriaal bij overtreding van wettelijke voorschriften.

Gegevensbescherming (zie 4.3)
Onderstaand volgt een niet eindige lijst met aandachtspunten en vragen die van belang zijn bij de beveiliging van uw gegevens:

- *Locatie van de gegevens.*
  De cloudleverancier moet garanderen dat de gegevens, inclusief alle kopieën en back-ups, alleen in geografische locaties worden opgeslagen zoals bepaald in het contract, het SLA en/of de geldende regelgeving.

- *Achterhalen van verwijderde gegevens.*
  Gegevens moeten volledig verwijderd worden, zodat het onmogelijk is om ze terug te halen. Het is dan ook noodzakelijk dat gegevens in de cloud kunnen worden opgespoord, worden gewist/vernietigd en dat de cloudleverancier hiervoor garanties afgeeft.

- *Vermenging van gegevens met die van andere cloudgebruikers.*
  Gegevens - vooral vertrouwelijke gegevens - mogen niet worden vermengd met gegevens van andere cloudgebruikers.

- *Samenvoeging van gegevens en inferentie.*
  Door gegevens in de cloud te plaatsen, moet hier extra aandacht aan worden besteedt, zodat door data-aggregatie en inferentie geen ongewenste onthulling van vertrouwelijke informatie plaatsvindt.

- *Denk op voorhand na hoe u omgaat met situaties (scenario's) waarbij uw organisatie imagoschade kan oplopen.*
  - Welke maatregelen neemt u als in 'dezelfde' cloud bijvoorbeeld kinderporno wordt aangetroffen? En hoe kunt u deze situatie voorkomen?
  - Wat doet u als vertrouwelijke gegevens, zoals de medische gegevens van uw medewerkers burgers op straat komen te liggen?

- *Welke maatregelen heeft de cloudleverancier genomen om aanvallen van 'side channel'[38], 'guest-hopping' en 'hyperjacking' te voorkomen?*

Bewustwording
Bedrijfstoepassingen en gegevens in de cloud zijn in principe vanaf elke locatie te benaderen, maar niet elke locatie is even geschikt vanuit het oogpunt van informatiebeveiliging. Geef uw medewerkers voorlichting over de (on)veiligheid van toegang vanuit een internet café, of via een (onbeveiligd) publiek WiFi-netwerk.

38. http://people.csail.mit.edu/tromer/papers/cloudsec.pdf

Versleuteling van gegevens
De beste manier om de vertrouwelijkheid van data in rust te waarborgen is cryptografie, het versleutelen van de data. Dit kan op basis van real-time hardwareversleuteling of softwareversleuteling. Bij de hardwarevariant zijn alle gegevens op de harde schijf automatisch versleuteld. Softwareversleuteling heeft over het algemeen een grotere impact op de performance dan hardwareversleuteling Het biedt minder beveiliging, omdat de encryptiesleutel gekopieerd kan worden zonder dat dit wordt gedetecteerd. Het versleutelen geldt uiteraard niet alleen voor de productiedata maar ook voor back-ups.

Om vertrouwelijkheid gedurende het transport (binnen de cloud en op weg naar en van de cloud) van de data te garanderen, is versleuteling ook de beste optie. Tevens moet de authenticiteit en integriteit gewaarborgd worden.

Wie voert het sleutelbeheer uit?
Denk hierbij aan: wie mag sleutels aanvragen, genereren en weer intrekken? Hoe worden sleutels gepubliceerd? Wordt een kopie van de sleutels bewaard (back-up)? Kunnen sleutels worden gereproduceerd na verlies (restore)?

Beschikbaarheid van gegevens
Om beschikbaarheid van de data te garanderen, wordt de data vaak op meerdere locaties in de cloud opgeslagen. Dit heeft als voordeel dat bij een storing op één locatie, de data altijd benaderbaar zijn. Op het moment dat ze verwijderd worden, moeten ze natuurlijk op alle locaties worden verwijderd. Houd wel rekening met de wettelijke bewaartermijn van de data.

Toegangscontrole tot gegevens
Er is een groeiende behoefte aan sterkere of 'twee-factor'-authenticatie voor toegang tot cloudtoepassingen, aangezien de authenticatie op basis van een wachtwoord vaak onvoldoende is.

De cloudleverancier zal dus inzicht moeten geven hoe ongeautoriseerde toegang tot uw (vertrouwelijke) informatie wordt voorkomen
Een voorbeeld staat in een kader hierboven.

Scheiding van klantomgevingen
Scheiding van klantomgevingen is een van de grootste aandachtspunten van organisaties bij cloudcomputing. (N.B. Overige klanten kunnen concurrenten zijn, maar ook kwaadwillenden!)

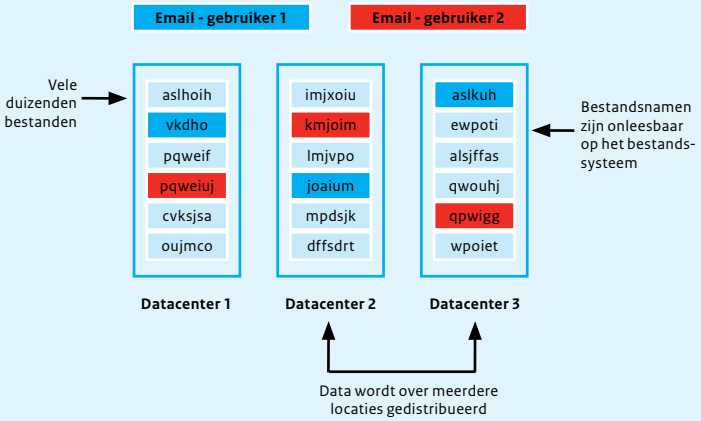
Virtualisatie is hierop het antwoord. Iedere klant maakt gebruik van een eigen virtuele machine en een virtueel netwerk. (Zie voor meer informatie m.b.t. virtualisatie Bijlage D: Achtergrondinformatie over Virtualisatie).

Voorbeeld van een cloudtoepassing met 'twee factor'-authenticatie: Google
Om de accounts van Gmail-gebruikers beter te beschermen heeft Google 'twee-factor'-authenticatie aan de e-maildienst toegevoegd.

Deze authenticatie gebruik een wachtwoord en een gegenereerde code. Naast het gebruikers-ID en het wachtwoord moet de gebruiker bij het inloggen een code invoeren, die via sms wordt verstuurd of wordt gegenereerd via een mobiele applicatie voor Android, BlackBerry of iPhones.

Figuur 0-11 Twee factor authenticatie voor Gmail-gebruikers

Cloudtoepassing met datascheiding: Google
Google-toepassingen draaien in een gedistribueerde omgeving. Google scheidt de gegevens van iedere klant niet op een of meerdere machines, maar verspreidt de gegevens van alle klanten over een gedeelde infrastructuur. Die infrastructuur bestaat uit veel gelijke machines, die verdeeld zijn over verschillende datacenters.



Figuur 0-12 Architectuur van het bestandssysteem van Google

Virtuele netwerken worden geïmplementeerd op basis van standaard technieken zoals VLANs (Virtual Local Area Networks), VPLS (Virtual Private LAN Service), of VPNs (Virtual Private Networks).

39. De huidige goedgekeurde versie is 1.2, http://tools.ietf.org/html/rfc5246
40. http://tools.ietf.org/html/rfc4301

De cloudleverancier moet duidelijk maken welke maatregelen hij heeft genomen om te voorkomen dat bijvoorbeeld de hypervisor wordt gecompromitteerd of om SQL-injectie te voorkomen. Deze bedreiging is niet nieuw, maar wel relevant bij SaaS-diensten. Hoe gaat de cloudleverancier om met de scheiding van data binnen databases van verschillende cloudgebruikers?

Een praktijkvoorbeeld van een cloudtoepassing waar datascheiding wordt toegepast staat in het kader 'Cloudtoepassing met datascheiding: Google'.

Interoperabiliteit
Om interoperabiliteit te garanderen moet de cloudleverancier gebruik maken van standaard protocollen (bijv. TLS[39] en IPSec[40]) en algoritmen (bijv. RSA en AES).

Verwijderen van gegevens
Wat gebeurt er met de data op het moment dat ze moeten worden verwijderd uit de cloud? Wat gebeurt er met de data waarvan de cloudleverancier een back-up heeft gemaakt? Worden die permanent vernietigd of simpel verwijderd? Vragen die de cloudleverancier moet beantwoorden. Bedenk wel dat je als organisatie vooraf zelf moet bepalen welke eisen je hieraan stelt!

Om misbruik van data bij o.a. 'gedeelde ICT-resources' te voorkomen, moeten de aanwezige data vernietigd worden en op geen enkele wijze meer toegankelijk gemaakt kunnen worden. Dit permanent vernietigen gaat veel verder dan het simpelweg verwijderen van losse bestanden en/of formatteren, want met deze laatste methoden is het bijzonder eenvoudig de data alsnog terug te winnen.
Houd ook rekening met de wettelijke bewaartermijn van data.

- Hoe garandeert de cloudleverancier dat daadwerkelijke alle 'instances' van de gegevens zijn verwijderd?
- Hoe gaat u om met noodvernietiging in bijvoorbeeld een oorlogssituatie?
- Hoe gaat de cloudleverancier om met bestaande recoverydata en back-ups? Deze bevatten ook nog de verwijderde gegevens.

Relatie tot de leverancier (zie 4.4)
Om met een gerust hart een deel van uw ICT-dienstverlening in de cloud te plaatsen zonder afhankelijk te worden van de cloudleverancier, moet hij u inzicht geven, welke procedures en processen hij heeft geïmplementeerd en van welke (open) standaarden hij gebruik maakt.

De cloudleverancier moet in het selectieproces, zoals beschreven in paragraaf 2.2, onderstaande vragen beantwoorden:

- Zijn er gedocumenteerde procedures en 'application programming interfaces' (API's) voor het exporteren van gegevens uit de cloud? Krijgt u de beschikking over deze documentatie, zodat u in staat bent op basis van deze documentatie te allen tijde uw gegevens te exporteren. Als dit niet zo is, dan kan dit een argument zijn om niet in zee te gaan met de cloudleverancier. Biedt de cloudleverancier interoperabele (open standaarden) exportformaten voor alle gegevens opgeslagen in de cloud? Zo ja, dan komt dit de interoperabiliteit met andere systemen ten goede en biedt dit een mate van onafhankelijkheid ten opzichte van de cloudleverancier. Als dit niet zo is, dan kan dit een argument zijn om niet in zee te gaan met de cloudleverancier.
- Kunt u als cloudgebruiker zelf gegevens exporteren of moet de cloudleveranciers die doen?

De antwoorden op bovenstaande vragen moeten voorkomen dat u voor (onaangename) verrassingen komt te staan. Ook moeten de antwoorden u voldoende informatie geven om weloverwogen te kiezen voor een cloudleverancier.

Op het moment dat u een cloudleverancier heeft geselecteerd, is ons advies om de volgende documenten op te (laten) stellen:

- Een escrow-overeenkomst
- Een escrow-overeenkomst beschermt de bedrijfscontinuïteit van uw organisatie voor de lange termijn. Dit wordt gedaan door de broncode van de programmatuur zeker te stellen, die u als licentienemer gebruikt, de zeker te stellen. Onder bepaalde voorwaarden krijgt de licentiehouder deze broncode ter beschikking, bijvoorbeeld faillissement of het niet voldoen aan de licentieovereenkomst.
- Een exitstrategie
  De exitstrategie moet zowel een migratie naar een andere cloudleverancier beschrijven als die naar de interne ICT-omgeving.

Beschikbaarheid van de clouddienst (zie 4.5)
Onderstaand volgt een niet eindige lijst met maatregelen die de beschikbaarheid van de internetverbinding verhogen:

- Sluit contracten af met een tweede internetleverancier die als failover kan fungeren als er een storing optreedt bij uw primaire internetleverancier.
- Implementeer alternatieve methoden. Maak naast de vaste internetverbinding gebruik van mobiel internet.

41. Identificatie en authenticatie van gebruikers / beheerders.

Beheer van gebruikers (zie 4.6)
Op basis van een risicoanalyse moet uw organisatie het benodigde beveiligingsniveau bepalen, om zodoende de juiste authenticatiemethode[41] vast te stellen. Hierbij zijn de volgende zaken van belang:

- Alle gebruikers (inclusief beheerders) moeten een unieke gebruikersidentificatie (gebruikers-ID) hebben, zodat activiteiten terug te voeren zijn tot de verantwoordelijke persoon. Houdt een zorgvuldige audittrail bij van iedereen die toegang heeft.
- Wachtwoorden zijn nog steeds een veelgebruikt hulpmiddel om de identiteit van een gebruiker te verifiëren. Er is wel een groeiende behoefte aan sterkere of 'tweefactor'-authenticatie voor toegang tot cloudtoepassingen aangezien de op wachtwoord gebaseerde authenticatie vaak onvoldoende is.
- De cloudleverancier moet inzicht geven hoe de authenticatie en autorisatie van gebruikers en beheerders plaats vindt, om vast te stellen of dat voldoet aan de eisen van uw organisatie.

Procedures
Er moeten procedures zijn voor:

- het aanvragen en muteren van toegang door gebruikers/beheerders inclusief toegang op afstand.
- het toewijzen van wachtwoorden.

Ook moet uw organisatie over een wachtwoordbeleid beschikken.

Authenticatiemethode
Hebt u inzicht welke wet- en regelgeving eisen stellen aan de authenticatiemethode die wordt gebruikt ter beveiliging van uw data, bijvoorbeeld Vir-bi of Wbp?
Stel vast aan welke eisen de authenticatiemethode van de cloudleverancier moet voldoen. Hierbij is onder andere van belang of uw organisatie zelf het beheer van gebruikers, wachtwoorden en rechten blijft uitvoeren of dat dit wordt ondergebracht bij de cloudleverancier.

Hebt u invloed op de manier waarop authenticatie en autorisatie van gebruikers en beheerders bij de cloudleverancier is geïmplementeerd? Denk hierbij aan wachtwoordbeleid en procedures.

Identiteitsmanagementsysteem
Maakt uw organisatie gebruik van een centraal identiteitsmanagementsysteem, of is het decentraal geregeld, waarbij ieder informatiesysteem zijn eigen gebruikersdatabase heeft?

Dwingt het identiteitsmanagementsysteem een wachtwoordbeleid af, om de kwaliteit van wachtwoorden te waarborgen?

Blijft u gebruik maken van u eigen identiteitsmanagementsysteem of stapt u over op dat van de cloudleverancier?

Een eigen identiteitsmanagementsysteem heeft als belangrijkste voordeel, dat je als gebruiker voor gebruikersauthenticatie en het vaststellen van de gebruikersrechten het eigen systeem kan raadplegen. Dit zorgt ervoor, dat de cloudleverancier altijd over up-to-date informatie van geautoriseerde gebruikers beschikt, omdat deze informatie wordt geverifieerd met uw eigen identiteitsmanagementsysteem. Het stelt wel extra eisen aan de cloudleverancier want die moet standaarden zoals Lightweight Directory Access Protocol (LDAP) en Security Assertion Markup Language (SAML) ondersteunen (zie Bijlage H: Standaarden' voor een korte omschrijving).

Loggegevens en audittrail
Wordt een audittrail bijgehouden van iedereen die toegang heeft gekregen en krijgt u toegang tot deze audittrail in verband met:

- het uitvoeren van probleemanalyse en,
- het gebruik als bewijsmateriaal bij overtreding van wet- en regelgeving.

Incidenten
Leg vast dat u tijdig wordt geïnformeerd bij incidenten met gebruikers. Neem in uw (informatiebeveiligings)beleid sancties op, over misbruik en wangedrag door gebruikers.

Beheer van incidenten (zie 4.7)
Cloudleveranciers moeten incidentbeheer geïmplementeerd en gedocumenteerd hebben en moeten minstens in staat zijn om incidenten te detecteren, de schade ervan te beperken en klanten hierover te informeren. Die informatie bestaat uit (vertrouwelijke) real-time gegevens over uw ICT-resources en gebruikers.

Incidentbeheer
Heeft uw organisatie incidentbeheer geïmplementeerd? Sluit dit aan bij dat van de cloudleverancier?

Hoe gaat u om met incidenten, inbreuk op de beveiliging of kwetsbaarheden bij de cloudleverancier?

Hoe reageert de cloudleverancier op incidenten en op welke manier worden klanten hierover geïnformeerd en betrokken? Hoe heeft de cloudleverancier z'n incidentbeheer geïmplementeerd? Hebt u hier inzicht in en zicht op?

Wordt u (tijdig) geïnformeerd bij incidenten? Worden periodiek incidentrapportages verstrekt? Dit zijn zaken waar u afspraken over moet en maken en deze vast moet leggen in contracten en/of SLA's.

Digitaal (forensisch) onderzoek en uitvoeren van audits
Staat de cloudleverancier het uitvoeren van digitaal (forensisch) onderzoek en audits toe (zie paragraaf 4.7.3)? Hoe gaan (eventuele) ketenpartners van de cloudleverancier hier mee om?

De cloudleverancier moet maatregelen treffen om het uitvoeren van digitaal (forensisch) onderzoek en audits te ondersteunen.
Maakt uw organisatie gebruik van derden of is u organisatie zelf in staat om digitaal (forensisch) onderzoek uit te voeren? Bij bijvoorbeeld voldoende capaciteit en competenties kunt dit wellicht ook zelf doen.

De volgende vragen en aandachtspunten zijn van belang:
- Welke gegevens moeten worden bewaard en voor hoe lang?
- Krijgt u als organisatie een kopie van de relevante logbestanden en in welke vorm? Als het een digitaal forensisch onderzoek is, mogen de logbestanden (achteraf) niet manipuleerbaar zijn.
- Hoe wordt voorkomen dat de loggegevens van mijn organisatie in de logbestanden van andere klanten terecht komen en vice versa?
- Hoe worden de digitale sporen veiliggesteld zodat ze gebruikt kunnen worden bij digitaal forensisch onderzoek (genereren van een fingerprint)? Een exacte kopie van de oorspronkelijke omgeving is nodig. Dit is haast onmogelijk op het moment dat data verspreid is opgeslagen in de cloud, je hebt dan een exacte kopie nodig van de cloud!
- Voor het generen van een fingerprint moet een machine 'offline' worden gehaald. Een machine die aan is, bevat namelijk continue wisselende data. In een cloud kun je niet echter zomaar een machine uitzetten. Dat zou namelijk betekenen dat andere organisaties ook niet meer bij hun data kunnen.

Beheer van wijzigingen (zie 4.8)
Bij cloudcomputing zijn de ICT-resources ondergebracht bij een cloudleverancier. Die is dan ook verantwoordelijk voor de wijzigingen op deze ICT-resources. Cloudgebruikers hebben hier dan ook (bijna) geen invloed op.

Wijzigingsbeheer
Hoe heeft de cloudleverancier wijzigingsbeheer geïmplementeerd? Hebt u als cloudgebruiker hier inzicht in en invloed op?

De volgende vragen/aandachtspunten zijn bij van belang:
- Worden wijzigingen getest voordat ze in productie worden genomen?
- Wordt er een administratie bijgehouden van alle ICT-resources (CI's), zodat er altijd een actueel overzicht van de huidige ICT-infrastructuur is?
- Zijn er fallbackscenario's uitgewerkt, waardoor wijzigingen kunnen worden teruggedraaid op het moment dat het doorvoeren van de wijziging tot verstoring leidt? Een fallbackscenario beschrijft in ieder geval onder welke condities de wijziging wordt teruggedraaid en wie hiertoe beslissingsbevoegd is.
- Is er een goedkeuringsproces voor wijzigingen ingevoerd, zodat alleen geautoriseerde wijzigingsverzoeken in behandeling worden genomen?
- Is er een procedure voor spoedeisende wijzigingen, zoals beveiligingsupdates?
- Is versiebeheer ingericht?
- Wordt bij wijzigingen de OTAP-cyclus toegepast?

Afstemming met gebruikers
De volgende vragen en aandachtspunten zijn van belang:
- Vindt er afstemming met gebruikers plaats wanneer wijzigingen worden doorgevoerd?
- Wordt u (tijdig) geïnformeerd bij wijzigingen aan de ICT-infrastructuur en vinden deze wijzigingen op het afgesproken moment plaats?
  Dit voorkomt dat uw dienstverlening onnodig wordt verstoord.

Back-up en recovery (zie 4.9)
Gegevens moeten beschikbaar zijn en om gegevensverlies bij ongewenst overschrijven of vernietigen te voorkomen, moet de cloudleverancier back-up- en recovery-procedures implementeren. Extra aandachtspunt: Hoe gaat u om met bestaande back-ups van uw gegevens die u in eigen beheer heeft? Voordat de gegevens gemigreerd worden naar de cloud, heeft u uiteraard zelf back-ups gemaakt. Houdt u deze back-ups in eigen beheer of brengt u ze ook in de cloud onder?

Contracten en Service Level Agreements
Hebt u afspraken (SLA) gemaakt met de cloudleverancier over back-up en recovery? Denk hierbij aan:
- Van welke data moet een back-up gemaakt worden? Met welke frequentie?
- Wat is de (wettelijke) bewaartermijn van de gegevens?
- Hoe worden back-ups bewaard? Worden ze bijvoorbeeld versleuteld?
- Wat zijn de recoverytijden? Binnen welke termijn moeten de gegevens vanaf de back-up terug worden gezet, zodat er weer over kunt beschikken?

Strategie en procedures
- Zijn procedures opgesteld voor het uitvoeren van de overeengekomen back-upstrategie, het maken van reservekopieën van gegevens en het oefenen van een tijdig herstel ervan?
- Mag u of een externe partij audits uitvoeren?

Procedures voor het maken van back-ups voor de afzonderlijke systemen moeten regelmatig worden getest, om te waarborgen dat ze voldoen aan de eisen die zijn vastgelegd.

- Wordt een nauwkeurige administratie bijgehouden van de back-ups die zijn gemaakt?

- Worden back-ups die minimaal nodig zijn om het systeem te herstellen, op een externe locatie bewaard? Deze externe locatie moet zich op zodanige afstand bevinden, dat geen schade kan worden aangericht als zich een calamiteit voordoet op de hoofdlocatie.
- De beveiliging van back-ups en de ruimte waarin deze zijn opgeslagen, moeten aan dezelfde beveiligingseisen voldoen als die voor de hoofdlocatie gelden.
- Back-ups moeten regelmatig worden getest, zodat het zeker is dat zij betrouwbaar zijn en in geval van nood kunnen worden gebruikt.
- Herstelprocedures dienen regelmatig te worden gecontroleerd en getest, om zeker te stellen dat ze effectief zijn en dat ze werken.

Transparantie (zie 4.10)
Cloudleverancier moeten inzicht geven over de aangeboden clouddiensten en de achterliggende (cloud)architectuur en de aanwezigheid van effectieve beveiligingsmaatregelen aantonen. Dit is noodzakelijk, om een risicoafweging te maken, of de cloudleverancier voldoet aan uw beveiligingseisen.

De volgende niet eindige lijst met vragen en aandachtspunten zijn hierbij van belang:

- Waar en wanneer wordt welke bedrijfsinformatie met welke software verwerkt?
- Op welke locaties vindt, al dan niet tijdelijk, gegevensopslag plaats?
- In welke formats vindt deze gegevensopslag plaats?
- Welke partijen (ketenpartners) vervullen bij het verwerkingsproces een rol?
- Wie is waarvoor verantwoordelijk en aansprakelijk?
- Welke werknemers van de cloudleverancier hebben toegang tot informatie van gebruikers?
- Is functiescheiding geregeld?
- Hoe wordt de informatie van verschillende klanten gescheiden?
- Welke maatregelen zijn geïmplementeerd om incidenten te voorkomen, op te sporen en om incidenten te reageren?

Relevante certificeringen

ISO 27001

ISO 27001 is een gedocumenteerd Information Security Management System (ISMS) [25]. Het ISMS brengt structuur en zorgt voor kwaliteit binnen uw informatiebeveiliging. De structuur van een ISMS zorgt voor een goede harmonie tussen mensen, processen en technologie. Het ISMS is gebaseerd op het vier stappen proces uit de Deming-cirkel. De cyclus bestaat uit de volgende vier stappen.

- Plan: Stel een plan op voor de benodigde werkzaamheden en zorg voor duidelijke eisen.
- Do: Implementeer het plan en voer het uit.
- Check: Controleer of de uitkomst voldoet aan de gestelde eisen en verwachtingen uit het plan.
- Act: Evalueer de uitkomst van de controle en bepaal of er aanpassingen plaats moeten vinden, of accepteer de uitkomst.

Deze cyclus heeft binnen een ISMS de belangrijke functie om continue risico's beheersbaar te houden en indien mogelijk, te verlagen. Door een gedegen plan worden risico's op een gestructureerde en eenduidige manier beoordeeld en geanalyseerd.
ISO 27001 staat vermeld op de lijst met open standaarden waarvoor geldt dat (semi-) publieke organisaties het 'pas toe of leg uit'-principe moeten volgen.

NEN7510

NEN 7510 (gezondheidszorg) [26] geeft richtlijnen en uitgangspunten ter beveiliging van de informatievoorziening. De norm richt zich op:

- individuele hulpverlener
- grote zorginstellingen
- organisaties die bij de informatievoorziening in de gezondheidszorg zijn betrokken, zoals netwerkorganisaties en zorgverzekeraars.

Maatregelen verschillen per type organisatie, evenals implementatiehandboeken. Samen met de implementatiehandboeken geeft de norm een leidraad voor het organisatorisch en technisch inrichten van informatiebeveiliging. Het biedt zo een basis voor vertrouwen in zorgvuldige informatievoorziening bij en tussen de verschillende organisaties in de zorg. De indeling is gebaseerd op ISO/IEC 17799 de voorloper van de ISO 27001.

SAS 70

SAS 70 (Statement on Auditing Standards Number 70: Service Organisations) [27] is een internationaal erkend certificaat voor leveranciers van ICT-diensten en is ontwikkeld door het American Institute of Certified Public Accountants (AICPA). Door SAS 70 moeten bedrijven hun controle aantonen op bedrijfsactiviteiten en -systemen (gebaseerd op beheersdoelstellingen en de beheersmaatregelen, Afhankelijk van de audit resulteert dit in een type I of type II certificaat.

- Type I verifieert de documentatie van betrokken bedrijfsactiviteiten en bepaalt of deze een afdoend kwaliteits- en beveiligingsniveau garanderen (toetsing op aanwezigheid).
- Type II controleert of de bedrijfsactiviteiten zich ook daadwerkelijk afspelen zoals gedocumenteerd (toetsing op effectieve werking).

De SAS 70-standaard komt per 15 juni 2011 te vervallen en wordt in internationaal verband door ISAE 3402 vervangen [28].

ISAE3402

ISAE 3402 (International Standard on Assurance Engagements 3402) [28]. De International Federation of Accountants (IFAC) heeft op 18 december 2009 een met SAS 70 vergelijkbare standaard gepubliceerd: ISAE 3402. Inmiddels hebben de Nederlandse Beroepsorganisatie van Accountants (NBA) en de Nederlandse Orde van Register EDP-Auditors (NOREA) de ISAE 3402-standaard vertaald en vastgesteld. De ISAE 3402 verschilt op de volgende punten van SAS 70:

- Het management van de ICT-dienstenleverancier moet een 'in control statement' (ICS) afgeven als onder-deel van het onderzoek en de rapportage. In SAS 70 ontbreekt een dergelijke verklaring van het management.
- Bij een SAS 70-onderzoek beoordeelt de auditor opzet, bestaan en eventueel werking van de beheers-maatregelen van de ICT-dienstenleverancier. Bij ISAE 3402 moet de auditor ook de toepasbaarheid van de beheersmaatregelen beoordelen. Voor het beoordelen van de toepasselijkheid zal de auditor inzicht moeten hebben in de risico's.

- De ICT-dienstenleverancier moet niet alleen een beschrijving opstellen van de beheersmaatregelen (zoals bij SAS 70), maar moet ook het gehele managementsysteem van interne beheersing beschrijven. De ICT-dienstenleverancier moet beschrijven hoe hij 'in control' blijft. Hierbij moet de relatie worden gelegd tussen de risico's, het managementsysteem van interne beheersing en de uiteindelijke beheersmaatregelen. [28]

PCI-DSS

PCI-DSS (Payment Card Industry - Data Security Standards) [29] is een internationale standaard voor de beveiliging van transacties en de opslag van bankgegevens en bevat eisen die Visa, MasterCard en American Express hebben opgesteld. Organisaties die transacties met betaalkaarten accepteren, moeten zich aan deze standaard houden. PCI DSS beschrijft 12 beveiligingsvoorwaarden en deze zijn in de volgende zes categorieën ingedeeld:

- netwerkbeveiliging opzetten en onderhouden,
- bescherming van kaarthoudergegevens,
- programma voor kwetsbaarheidsbeheer opstellen en onderhouden,
- sterk toegangsbeheer implementeren,
- regelmatig testen en controleren van netwerken;
- een beveiligingsbeleid voor werknemers en contractanten opstellen en handhaven.

Aanvalsmethoden

(Distributed) Denial-of-Service-aanvallen	Denial-of-Service-aanvallen (DoS) zijn elektronische aanvallen die een systeem, dienst of netwerk zo belasten dat ze niet meer beschikbaar zijn. Dit kan door de systemen uit te schakelen of een netwerk te overladen met dataverkeer. Een Denial of Service kan van een enkel systeem afkomstig zijn, maar ook van meerdere systemen tegelijkertijd. Een DoS-aanval vanaf meerdere systemen heet in jargon een Distributed-Denial-of-Service (DDoS).
Guest-hopping	Guest-hopping maakt gebruik van kwetsbaarheden in de hypervisor, die het mogelijk maken om de beveiliging, die strikte scheiding tussen verschillende virtuele machines moet garanderen, te compromitteren. Op deze manier wordt toegang verkregen tot andere virtuele machines of zelfs de hypervisor. Over het algemeen wordt gebruik gemaakt van de zwakste schakel, de minst beveiligde virtuele machine op het systeem. Die wordt gebruikt als vertrekpunt om aanvallen op andere virtuele machines uit te voeren. Op deze manier wordt van de ene naar de andere virtuele machine gesprongen. Bijvoorbeeld: Een aanvaller is geïnteresseerd in de gegevens van virtuele machine A, maar is niet in staat om direct tot A door te dringen. Dan zal de aanvaller proberen om virtuele machine B aan te vallen en vanaf deze virtuele machine proberen om toegang te krijgen tot A.
Hyper jacking	Hyper jacking is een methode waarbij een 'rogue' hypervisor onder de bestaande legitieme infrastructuur (hypervisor of besturingssysteem) wordt geïnstalleerd, met controle over alle acties tussen het doelwit en de hardware. Voorbeelden van hyper jacking zijn Blue Pill[42] en Vitriol[43].
Man-in-the-middle	Bij man-in-the-middle bevindt de aanvaller zich tussen een klant en een dienst. Hierbij doet hij zich richting de klant voor als de dienst en andersom. De dienst kan hier bijvoorbeeld een internetwinkel zijn. Als tussenpersoon kan de aanvaller nu uitgewisselde gegevens afluisteren en/of manipuleren.
Replay	Bij een 'replay'-aanval wordt een legitieme sessie van een doelwit opnieuw afgespeeld (meestal vastgelegd door het afluisteren van het netwerkverkeer).
Side channel	Een 'side channel'[44]- aanval maakt gebruik van een virtuele machine, die aanvallers hebben geïnstalleerd. Deze virtuele machine kan worden geïnstalleerd door gebruik te maken van kwaadaardige software of door zelf nieuwe virtuele machines af te nemen bij de cloudleverancier. Deze 'kwaadaardige' virtuele machine kan vervolgens gedeelde resources monitoren van andere virtuele machines. Deze resources bestaan uit geheugen en processoren op de gedeelde fysieke machine. Door deze gegevens te verzamelen en te analyseren, wordt het 'makkelijker' om vast te stellen wanneer een andere virtuele machine aangevallen kan vallen. Het is zelfs mogelijk om via zogenaamde 'keystroke timing attacks'[45], wachtwoorden en andere gevoelige informatie van een virtuele machine te achterhalen.
Sniffing	Sniffing is het onderscheppen en lezen van informatie, zoals e-mailberichten of gebruikersnamen en wachtwoorden. Afluisteren wordt ook wel 'sniffing' genoemd.

42. http://theinvisiblethings.blogspot.com/2006/06/introducing-blue-pill.html
43. http://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Zovi.pdf
44. http://people.csail.mit.edu/tromer/papers/cloudsec.pdf
45. http://www.ece.cmu.edu/~dawnsong/papers/ssh-timing.pdf

Spoofing	Je voordoen als een ander, dat is spoofing. Iemand kan het e-mailadres van een ander gebruiken als zogenaamd afzendadres, zodat de geadresseerde in verwarring raakt. Deze methode kan handig zijn voor de verspreiding van virussen, omdat de ontvanger zou kunnen denken dat de afzender betrouwbaar is. Spoofing gebeurt ook op netwerkniveau, veelal met het doel internetverkeer in de war te schoppen.
SQL-injectie [51]	Veel webapplicaties maken gebruik van een database om daarin allerlei informatie op te slaan. De informatie die een dergelijke database kan bevatten, is zeer gevarieerd. Denk bijvoorbeeld aan gebruikersnaam en wachtwoord voor besloten gedeelten van de website, nieuwsberichten, logging van bezochte pagina's, etc. Om de informatie uit de database beschikbaar te maken op de website, voert de code achter een website allerlei verzoeken naar de database uit, op het moment dat de gebruiker een pagina van de website opent. Dit soort verzoeken maakt in veel gevallen gebruik van de standaard databasetaal 'Structured Query Language', kortweg SQL. Vaak kan de gebruiker daarbij de inhoud van het SQL verzoek direct of indirect beïnvloeden via een zoekterm of een ander invoerveld. Kwaadwillende hebben de mogelijkheid om een extra SQL-verzoek toe te voegen (injecteren), waardoor bijvoorbeeld de inhoud van de database wordt aangepast. We noemen dit verschijnsel dan ook 'SQL-injectie'. SQL-injectie kan plaats vinden als invoer van gebruikers op onvoldoende gecontroleerde wijze wordt verwerkt in een SQL-verzoek. Deze bedreiging is niet nieuw maar wel relevant bij SaaS-diensten. De vraag is namelijk, hoe de cloudleverancier omgaat met de scheiding van data binnen databases van verschillende cloudgebruikers.

Standaarden

Security Assertion Markup Language (SAML) [52]	SAML wordt gebruikt voor het uitwisselen van authenticatie- en autorisatiegegevens en is gebaseerd op het Extensible Markup Language (XML) framework (raamwerk). Dit biedt gebruikers de mogelijkheid, om op één plek in te loggen en vervolgens direct toegang te krijgen (zonder opnieuw in te loggen) tot meerdere systemen van verschillende organisaties (Single Sign-On). Om te voorkomen dat SAML-berichten ongeautoriseerd worden aangepast, is het raadzaam het SAML-bericht te verpakken in SOAP (Simple Object Access Protocol). SOAP kan van een digitale handtekening worden voorzien. De Security Assertion Markup Language (SAML) is een internationaal erkende standaard, ontwikkeld door het Security Services Technical Committee van Organization for the Advancement of Structured Information Standards (OASIS)[46]. SAML staat vermeld op de lijst met open standaarden[47] waarvoor geldt, dat (semi-) publieke organisaties het 'pas toe of leg uit'-principe[48] moeten volgen.
Extensible Markup Language (XML) [53]	XML is een standaard van het World Wide Web Consortium (W3C) voor de (XML) [53] syntaxis van formele markup-talen, om gestructureerde gegevens weer te geven in de vorm van platte tekst. Deze representatie is zowel leesbaar voor de computer als de mens. Het XML-formaat wordt gebruikt om gegevens op te slaan (zoals in het OpenDocument-formaat) en om gegevens over het internet te versturen. XML-talen gebruiken zogenaamde elementen en attributen om gegevens te structureren. De XML-specificatie definieert de syntaxis van elementen, attributen en andere structuren die in XML-bestanden kunnen voorkomen. De XML-specificatie legt echter geen namen vast voor deze elementen en attributen, precies omdat deze keuze afhangt van het doel van het XML-bestand.
Simple Object Access Protocol (SOAP) [54]	SOAP is een protocol voor het uitwisselen van XML-berichten op basis van http, SMTP of FTP, tussen systemen van dezelfde of andere besturingssystemen. SOAP wordt door de Internet Engineering Task Force (IETF) beheerd.
Lightweight Directory Access Protocol (LDAP) [55]	LDAP is een netwerkprotocol, dat beschrijft hoe gegevens uit directoryservices benaderd moeten worden over bijvoorbeeld TCP/IP. Het is in beheer bij IETF. Een directory is in dit verband informatie die op een hiërarchische manier, gegroepeerd naar een bepaald attribuut, is opgeslagen. Denk aan een telefoonboek waarin telefoonnummers en adressen van personen per bedrijf worden opgeslagen. Een directorynaam komt overeen met de bedrijfsnaam. Iedere directory bevat dan alle personen binnen dat bedrijf als objecten, met contactgegevens zoals telefoon-nummer en e-mailadres als attributen.

46. http://www.oasis-open.org/standards#samlv2.0
47. In de lijsten met open standaarden vindt u de open standaarden die zijn goedgekeurd door Forum en College Standaardisatie < http://www.open-standaarden.nl/>.
48. http://www.open-standaarden.nl/open-standaarden/het-pas-toe-of-leg-uit-principe/

BIJLAGE I

Relevante artikelen Wbp en Richtsnoeren

Relevante artikelen Wbp
In onderstaande tabel worden de relevante onderdelen van artikelen weergeven uit Wet Bescherming Persoonsgegevens (Wbp) [9] die van belang zijn voor deze whitepaper.

In artikel 1 worden de definities geformuleerd.
In artikel 4 wordt aangegeven wanneer deze wet van toepassing is.
In artikel 12 wordt de relatie tussen verantwoordelijke, bewerker en derden toegelicht.

Artikel 1:	d. Verantwoordelijke: de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. e. Bewerker: degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen. f. Betrokkene: degene op wie een persoonsgegeven betrekking heeft. g. Derde: ieder, niet zijnde de betrokkene, de verantwoordelijke, de bewerker, of enig persoon die onder rechtstreeks gezag van de verantwoordelijke of de bewerker gemachtigd is om persoonsgegevens te verwerken.
Artikel 4:	1. Deze wet is van toepassing op de verwerking van persoonsgegevens in het kader van activiteiten van een vestiging van een verantwoordelijke in Nederland. 2. Deze wet is van toepassing op de verwerking van persoonsgegevens door of ten behoeve van een verantwoordelijke die geen vestiging heeft in de Europese Unie, waarbij gebruik wordt gemaakt van al dan niet geautomatiseerde middelen die zich in Nederland bevinden, tenzij deze middelen slechts worden gebruikt voor de doorvoer van persoonsgegevens. 3. Het is een verantwoordelijke als bedoeld in het tweede lid, verboden persoonsgegevens te verwerken, tenzij hij in Nederland een persoon of instantie aanwijst die namens hem handelt overeenkomstig de bepalingen van deze wet. Voor de toepassing van deze wet en de daarop berustende bepalingen, wordt hij aangemerkt als de verantwoordelijke’
Artikel 12:	1. Een ieder die handelt onder het gezag van de verantwoordelijke of van de bewerker, alsmede de bewerker zelf, voor zover deze toegang hebben tot persoonsgegevens, verwerkt deze slechts in opdracht van de verantwoordelijke, behoudens afwijkende wettelijke verplichtingen. 2. De personen, bedoeld in het eerste lid, voor wie niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift een geheimhoudingsplicht geldt, zijn verplicht tot geheimhouding van de persoonsgegevens waarvan zij kennis nemen, behoudens voor zover enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit. Artikel 272, tweede lid, van het Wetboek van Strafrecht is niet van toepassing.

	Richtsnoeren
CBP Richtsnoeren 'publicatie van persoonsgegevens op internet' [14]	Op internet worden op heel veel manieren persoonsgegevens gepubliceerd. Internet maakt het door zijn aard zeer laagdrempelig om persoonsgegevens te publiceren: via een website, in een discussieforum of in een online dagboek. Mensen kunnen gegevens over zichzelf of over anderen. Publicaties op internet zijn over het algemeen wereldwijd 24 uur per dag toegankelijk voor een potentieel zeer omvangrijk en divers publiek. Voor mensen van wie de persoonsgegevens op internet staan, kunnen de consequenties groot zijn, bijvoorbeeld als het gaat om onbewezen verdenkingen of intieme details uit het persoonlijke leven. Zelfs als de gegevens op zichzelf juist zijn, kan door de publicatie op internet een onvolledig beeld ontstaan van een persoon, met een negatieve beoordeling tot gevolg. Daarom stelt de wet grenzen aan de toelaatbaarheid van de publicatie vanpersoons-gegevens op internet. Hoofdregel van de Wbp is dat iedereen die persoonsgegevens publiceert, zélf verantwoordelijk is voor de naleving van de wet. Particulieren, ondernemingen, organisaties en instellingen die voornemens zijn gegevens over personen op internet te publiceren, moeten dus zelf voorafgaand aan de publicatie beoordelen of dat wel is toegestaan, en zo ja, aan welke voorwaarden zij daarbij moeten voldoen. Met deze richtsnoeren wil het CBP het eenvoudiger maken, dat te beoordelen. Dat is in het belang van degenen die op internet publiceren en in het belang van de mensen over wie (mogelijk) gegevens worden gepubliceerd.
CBP Richtsnoeren 'Actieve openbaarmaking en eerbiediging van de persoonlijke levenssfeer' [15]	Bestuursorganen zoals gemeenten publiceren in het kader van hun actieve openbaar-makingsplicht regelmatig persoonsgegevens op internet. Voor die situaties waarin het recht op openbaarheid van overheidsinformatie en het recht op eerbiediging van de persoonlijke levenssfeer samenkomen, heeft het CBP deze richtsnoeren opgesteld, ter aanvulling op de eerste richtsnoeren 'publicatie van persoonsgegevens op internet'. Deze richtsnoeren zijn van nut in situaties waarin een belangenafweging moet worden gemaakt tussen het belang van openbaarheid van overheidsinformatie en het belang van eerbiediging van de persoonlijke levenssfeer. Als de belangen-afweging ertoe leidt dat het bestuursorgaan op internet overheidsinformatie gaat publiceren waarin persoonsgegevens zijn opgenomen, moet die publicatie 'Wbp-proof' zijn, oftewel aan de in die wet neergelegde normen voldoen. Deze richtsnoeren beogen daaraan een bijdrage te leveren. De richtsnoeren zien daarmee alleen op de fase voorafgaand aan de publicatie. Als het bestuursorgaan eenmaal heeft besloten, dat het in het kader van zijn actieve openbaar-makingsplicht op grond van de Wet openbaarheid bestuur is gehouden tot publicatie, het daarbij het internet als instrument voor openbaarmaking kiest en heeft vastgesteld dat de eerbiediging van de persoonlijke levenssfeer aan publicatie niet in de weg staat, gelden de regels en het kader zoals uiteengezet in de Richtsnoeren 'publicatie van persoonsgegevens op internet'. Wat betreft de fasen 'bij publicatie' en 'na publicatie' wordt dan ook verwezen naar de Richtsnoeren 'publicatie van persoonsgegevens op internet'. Deze bijlage geeft de beheersmaatregelen uit de NEN-ISO/IEC 27002:2007 nl ' Code voor Informatiebeveiliging' [10] aan, waar de verantwoordelijkheid belegd moet worden: bij de klant (uw organisatie) of bij de cloudleverancier. Tevens wordt er een koppeling gelegd met de beheersmaatregelen die:

BIJLAGE J

ISO 27002

Deze bijlage geeft de beheersmaatregelen uit de NEN-ISO/IEC 27002:2007 nl ' Code voor Informatiebeveiliging' [10] aan, waar de verantwoordelijkheid belegd moet worden: bij de klant (uw organisatie) of bij de cloudleverancier.

Tevens wordt er een koppeling gelegd met de beheersmaatregelen die:

- de Open Security Architecture (OSA) voor het patroon cloudcomputing heeft opgesteld [48] (zie ook paragraaf 5.1.1 en 5.2.1;
- de Cloud Security Alliance (CSA) heeft vastgelegd in de Cloud Security Alliance Controls Matrix (CM) [49] (zie ook paragraaf 5.2.2).

Bij het vaststellen wie verantwoordelijk is voor de implementatie van een beheersmaatregel is er vanuit uitgegaan, dat uw organisatie gebruik wil gaan maken van clouddiensten van een externe cloudleverancier.

In deze situatie is aangegeven dat de verantwoordelijkheid zowel bij de klant (uw organisatie) als bij de cloudleverancier ligt. Zoals in paragraaf 3.2 aangegeven, kan een clouddienst bestaan uit een infrastructurele dienst (IaaS) of een platformdienst (PaaS), waarop u uw eigen toepassing(en) ontwikkelt. In dit geval ligt de verantwoordelijkheid voor bijvoorbeeld de ontwikkeling van de toepassing bij uw organisatie in plaats van bij de cloudleverancier. Neemt uw organisatie een kant en klare toepassing af (SaaS), dan ligt de verantwoordelijkheid voor de ontwikkeling van deze toepassing bij de cloudleverancier.

Risicobeoordeling en risicobehandeling

Deze paragraaf behandeld de beheersmaatregelen zoals die zijn beschreven in hoofdstuk 4 'Risicobeoordeling en risicobehandeling' uit de NEN-ISO/IEC 27002:2007 nl 'Code voor Informatiebeveiliging' [10].

Nr.	Titel	Verant. Klant	Verant. Cl. Lev.	OSA CSA	Code Open Security architecture - SP-011: Cloudcomputing Pattern [48] of Cloud Security Alliance Controls Matrix (CM) [49]
4.1	Beoordelen van beveiligingsrisico's	√		OSA	RA-03 Risk Assessment
		√		OSA	RA-04 Risk Assessment Update
			√	CSA	RI-02 Risk Management - Assessments
4.2	Behandelen van beveiligingsrisico's	√		OSA	RA-03 Risk Assessment
			√	CSA	RI-03 Risk Management - Mitigation/Acceptance

Beveiligingsbeleid

Deze paragraaf behandelt de beheersmaatregelen zoals die zijn beschreven in hoofdstuk 5 'Informatiebeveiligingsbeleid' uit de NEN-ISO/IEC 27002:2007 nl 'Code voor Informatiebeveiliging' [10].

Nr.	Titel	Verant. Klant	Verant. Cl. Lev.	OSA CSA	Code Open Security architecture - SP-011: Cloudcomputing Pattern [48] of Cloud Security Alliance Controls Matrix (CM) [49]
5.1	Informatiebeveiligingsbeleid				
5.1.1	Beleidsdocument voor	√	√	OSA	AT-01 Security Awareness And Training Policy And Procedures
	informatiebeveiliging	√	√	OSA	CP-01 Contingency Planning Policy And Procedures
			√	CSA	IS-03 Information Security - Policy
5.1.2	Beoordeling van het	√			
	informatiebeveiligingsbeleid		√	CSA	IS-05 Information Security - Policy Reviews

Organisatie van informatiebeveiliging

Deze paragraaf behandelt de beheersmaatregelen zoals die zijn beschreven in hoofdstuk 6 'Organisatie van informatiebeveiliging' uit de NEN-ISO/IEC 27002:2007 nl 'Code voor Informatiebeveiliging' [10].

Nr.	Titel	Verant. Klant	Verant. Cl. Lev.	OSA CSA	Code Open Security architecture - SP-011: Cloudcomputing Pattern [48] of Cloud Security Alliance Controls Matrix (CM) [49]
6.1	Interne organisatie	√	√	OSA	PL-01 Security Planning Policy And Procedures
6.1.1	Betrokkenheid van de directie bij informatiebeveiliging	√			
			√	CSA	IS-01 Information Security - Management Program
			√	CSA	IS-02 Information Security - Management Support/Involvement
6.1.2	Coördinatie van informatiebeveiliging		√	CSA	IS-01 Information Security - Management Program
		√	√	CSA	IS-13 Information Security - Roles/Responsibilities
6.1.3	Toewijzen van verantwoordelijkheden voor informatiebeveiliging		√	CSA	DG-01 Data Governance - Ownership/Stewardship
			√	CSA	IS-01 Information Security - Management Program
		√	√	CSA	IS-13 Information Security - Roles/Responsibilities
6.1.4	Goedkeuringsproces voor IT-voorzieningen	√	√	OSA	CA-01 Certification, Accreditation, And Security Assessment
					Policies And Procedures
			√	CSA	IS-01 Information Security - Management Program
			√	CSA	RM-01 Release Management - New Development/Acquisition
6.1.5	Geheimhoudingsovereenkomst	√	√	OSA	PS-06 Access Agreements
			√	CSA	IS-01 Information Security - Management Program
		√	√	CSA	LG-01 Legal - Non-Disclosure Agreements
6.1.6	Contact met overheidsinstanties		√	CSA	CO-04 Compliance - Contact/Authority Maintenance
			√	CSA	IS-01 Information Security - Management Program
6.1.7	Contact met special belangengroepen		√	CSA	CO-04 Compliance - Contact/Authority Maintenance
			√	CSA	IS-01 Information Security - Management Program
			√	CSA	IS-12 Information Security - Industry Knowledge/Benchmarking
6.1.8	Onafhankelijke beoordeling van informatiebeveiliging	√	√	OSA	CA-02 Security Assessments
			√	CSA	CO-02 Compliance - Independent Audits
			√	CSA	IS-01 Information Security - Management Program
6.2	Externe partijen				
6.2.1	Identificatie van risico's die betrekking hebben op externe partijen	√		OSA	RA-03 Risk Assessment
		√		OSA	PS-07 Third-Party Personnel Security
		√		OSA	SA-09 External Information System Services
			√	CSA	RI-05 Risk Management - Third Party Access
6.2.2	Beveiliging behandelen in de omgang met klanten	√	√	OSA	AC-02 Account Management
			√	CSA	SA-01 Security Architecture - Customer Access Requirements
6.2.3	Beveiliging behandelen in overeenkomsten met een derde partij	√		OSA	PS-07 Third-Party Personnel Security
		√		OSA	SA-09 External Information System Services
		√		OSA	AC-02 Account Management
		√		OSA	AT-02 Security Awareness
			√	CSA	CO-03 Compliance - Third Party Audits
			√	CSA	LG-02 Legal - Third Party Agreements

Beheer van bedrijfsmiddelen

Deze paragraaf behandelt de beheersmaatregelen zoals die zijn beschreven in hoofdstuk 7 'Beheer van bedrijfsmiddelen' uit de NEN-ISO/IEC 27002:2007 nl 'Code voor Informatiebeveiliging' [10].

Nr.	Titel	Verant. Klant	Verant. Cl. Lev.	OSA CSA	Code Open Security architecture - SP-011: Cloudcomputing Pattern [48] of Cloud Security Alliance Controls Matrix (CM) [49]
7.1	Verantwoordelijkheid voor bedrijfsmiddelen				
7.1.1	Inventarisatie van bedrijfsmiddelen		√	OSA	CM-02 Baseline Configuration
			√	CSA	FS-08 Facility Security - Asset Management
7.1.2	Eigendom van bedrijfsmiddelen		√	CSA	DG-01 Data Governance - Ownership/Stewardship
			√	CSA	FS-08 Facility Security - Asset Management
7.1.3	Aanvaardbaar gebruik van bedrijfsmiddelen		√	CSA	IS-26 Information Security - Acceptable Use
7.2	Classificatie van informatie				
7.2.1	Richtlijnen voor classificatie	√			
			√	CSA	DG-02 Data Governance - Classification
7.2.2	Labeling en verwerking van informatie	√			
			√	CSA	DG-03 Data Governance - Handling/Labeling/Security Policy

Beveiliging van personeel

Deze paragraaf behandelt de beheersmaatregelen zoals die zijn beschreven in hoofdstuk 8 'Beveiliging van personeel' uit de NEN-ISO/IEC 27002:2007 nl 'Code voor Informatiebeveiliging' [10].

Nr.	Titel	Verant. Klant	Verant. Cl. Lev.	OSA CSA	Code Open Security architecture - SP-011: Cloudcomputing Pattern [48] of Cloud Security Alliance Controls Matrix (CM) [49]
8.1	Voorafgaand aan het dienstverband				
8.1.1	Rollen en verantwoordelijkheden	√	√	OSA	PS-07 Third-Party Personnel Security
		√	√	CSA	IS-13 Information Security - Roles/Responsibilities
8.1.2	Screening	√	√	OSA	PS-07 Third-Party Personnel Security
			√	CSA	HR-01 Human Resources Security - Background Screening
8.1.3	Arbeidsvoorwaarden	√	√	OSA	PS-06 Access Agreements
		√	√	OSA	PS-07 Third-Party Personnel Security
		√	√	CSA	HR-02 Human Resources Security - Employment Agreements
8.2	Tijdens het dienstverband				
8.2.1	Directieverantwoordelijkheid	√	√	OSA	PS-07 Third-Party Personnel Security
			√	CSA	IS-14 Information Security - Management Oversight
8.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	√	√	OSA	AT-01 Security Awareness And Training Policy And Procedures
		√	√	OSA	PS-07 Third-Party Personnel Security
		√	√	OSA	AT-02 Security Awareness
		√	√	OSA	AT-03 Security Training
			√	CSA	IS-11 Information Security - Training/Awareness
8.2.3	Disciplinaire maatregelen	√			
			√	CSA	IS-06 Information Security - Policy Enforcement
8.3	Beëindiging of wijziging van dienstverband	√	√		
8.3.1	Beëindiging van verantwoordelijkheden	√			
			√	CSA	HR-03 Human Resources - Employment Termination
8.3.2	Retournering van bedrijfsmiddelen	√			
			√	CSA	IS-27 Information Security - Asset Returns
8.3.3	Blokkering van toegangsrechten	√	√	OSA	AC-02 Account Management
			√	CSA	IS-09 Information Security - User Access Revocation

Fysieke beveiliging en beveiliging van de omgeving

Deze paragraaf behandelt de beheersmaatregelen zoals die zijn beschreven in hoofdstuk 9 'Fysieke beveiliging en beveiliging van de omgeving' uit de NEN-ISO/IEC 27002:2007 nl ' Code voor Informatiebeveiliging' [10].

Nr.	Titel	Verant. Klant	Verant. Cl. Lev.	OSA CSA	Code Open Security architecture - SP-011: Cloudcomputing Pattern [48] of Cloud Security Alliance Controls Matrix (CM) [49]
9.1	Beveiligde ruimte				
9.1.1	Fysieke beveiliging van de omgeving		√	CSA	FS-03 Facility Security - Controlled Access Points
9.1.2	Fysieke toegangsbeveiliging		√	CSA	FS-02 Facility Security - User Access
			√	CSA	FS-04 Facility Security - Secure Area Authorization
9.1.3	Beveiliging van kantoren, ruimten en faciliteiten		√	CSA	FS-01 Facility Security - Policy
9.1.4	Bescherming tegen bedreigingen van buitenaf		√	CSA	RS-05 Resiliency - Environmental Risks
9.1.5	Werken in beveiligde ruimten		√	CSA	FS-01 Facility Security – Policy
			√	CSA	IS-17 Information Security - Workspace
9.1.6	Openbare toegang en gebieden voor laden en lossen		√	CSA	FS-05 Facility Security - Unauthorized Persons Entry
9.2	Beveiliging van apparatuur				
9.2.1	Plaatsing en bescherming van apparatuur		√	CSA	RS-06 Resiliency - Equipment Location
		√	√	CSA	SA-10 Security Architecture - Wireless Security
9.2.2	Nutsvoorzieningen		√	CSA	RS-07 Resiliency - Equipment Power Failures
			√	CSA	RS-08 Resiliency - Power/Telecommunications
9.2.3	Beveiliging van kabels		√	CSA	RS-08 Resiliency - Power/Telecommunications
9.2.4	Onderhoud van apparatuur		√	CSA	OP-04 Operations Management - Equipment Maintenance
		√	√	CSA	SA-10 Security Architecture - Wireless Security
9.2.5	Beveiliging van apparatuur buiten het terrein		√	CSA	FS-07 Facility Security - Off-Site Equipment
9.2.6	Veilig verwijderen of hergebruiken van apparatuur		√	CSA	DG-05 Data Governance - Secure Disposal
9.2.7	Verwijdering van bedrijfseigendommen		√	CSA	FS-06 Facility Security - Off-Site Authorization

Beheer van communicatie- en bedieningsprocessen

Deze paragraaf behandelt de beheersmaatregelen zoals die zijn beschreven in hoofdstuk 10 'Beheer van communicatie- en bedieningsprocessen' uit de NEN-ISO/IEC 27002:2007 nl 'Code voor Informatiebeveiliging' [10].

Nr.	Titel	Verant. Klant	Verant. Cl. Lev.	OSA CSA	Code Open Security architecture - SP-011: Cloudcomputing Pattern [48] of Cloud Security Alliance Controls Matrix (CM) [49]
10.1	Bedieningsprocedures en verantwoordelijkheden				
10.1.1	Gedocumenteerde bedieningsprocedures		√	CSA	OP-01 Operations Management - Policy
10.1.2	Wijzigingsbeheer	√	√	OSA	CM-03 Configuration Change Control
		√	√	OSA	CM-04 Monitoring Configuration Changes
		√		CSA	RI-04 Risk Management - Business/Policy Change Impacts
10.1.3	Functiescheiding		√	CSA	IS-15 Information Security - Segregation of Duties
10.1.4	Scheiding van faciliteiten voor ontwikkeling, testen en productie	√			
			√	CSA	DG-06 Data Governance - Non-Production Data
10.2	Beheer van de dienstverlening door een derde partij				
10.2.1	Dienstverlening	√		OSA	SA-09 External Information System Services
			√	CSA	CO-03 Compliance - Third Party Audits
10.2.2	Controle en beoordeling van dienst-verlening door een derde partij	√		OSA	SA-09 External Information System Services
			√	CSA	CO-03 Compliance - Third Party Audits

Vervolg op volgende pagina

Nr.	Titel	Verant. Klant	Verant. Cl. Lev.	OSA CSA	Code Open Security architecture - SP-011: Cloudcomputing Pattern [48] of Cloud Security Alliance Controls Matrix (CM) [49]
10.2.3	Beheer en wijzigingen in de	√		OSA	CM-03 Configuration Change Control
	dienstverlening door een derde partij	√		CSA	RI-04 Risk Management - Business/Policy Change Impacts
10.3	Systeemplanning en –acceptatie				
10.3.1	Capaciteitsbeheer	√	√	OSA	SA-02 Allocation Of Resources
		√	√	CSA	OP-03 Operations Management - Capacity/Resource Planning
10.3.2	Systeemacceptatie	√	√	OSA	CA-01 Certification, Accreditation, And Security Assessment Policies And Procedures
		√	√	OSA	AT-03 Security Training
		√	√	OSA	CA-04 Security Certification
		√	√	OSA	CA-06 Security Accreditation
			√	CSA	RM-03 Release Management - Quality Testing
10.4	Bescherming tegen virussen en 'mobile code'				
10.4.1	Maatregelen tegen virussen	√	√	OSA	CP-01 Contingency Planning Policy And Procedures
		√	√	OSA	AT-02 Security Awareness
		√	√	OSA	IR-01 Incident Response Policy And Procedures
		√	√	OSA	SC-18 Mobile Code
		√	√	OSA	SI-03 Malicious Code Protection
			√	CSA	IS-21 Information Security - Anti-Virus/Malicious Software
10.4.2	Maatregelen tegen 'mobile code'	√	√	OSA	SC-18 Mobile Code
		√	√	CSA	SA-15 Security Architecture - Mobile Code
10.5	Back-Up				
10.5.1	Reservekopieën maken (back-ups)	√	√	CSA	DG-04 Data Governance - Retention Policy
10.6	Beheer van netwerkbeveiliging				
10.6.1	Maatregelen voor netwerken		√	OSA	SC-08 Transmission Integrity
			√	OSA	SC-09 Transmission Confidentiality
			√	CSA	IS-18 Information Security – Encryption
		√	√	CSA	SA-10 Security Architecture - Wireless Security
10.6.2	Beveiliging van netwerkdiensten		√	OSA	SA-09 External Information System Services
			√	OSA	AC-04 Information Flow Enforcement
			√	OSA	CA-03 Information System Connections
			√	OSA	SI-04 Information System Monitoring Tools And Techniques
		√	√	CSA	IS-31 Information Security - Network/Infrastructure Services
10.7	Behandeling van media				
10.7.1	Beheer van verwijderbare media	√	√	CSA	IS-32 Information Security - Portable/Mobile Devices
10.7.2	Verwijdering van media		√	CSA	DG-05 Data Governance - Secure Disposal
		√	√	CSA	IS-32 Information Security - Portable/Mobile Devices
10.7.3	Procedures voor de behandeling van informatie	√	√		
10.7.4	Beveiliging van systeemdocumentatie	√	√	OSA	SA-05 Information System Documentation
			√	CSA	OP-02 Operations Management - Documentation
10.8	Uitwisseling van informatie				
10.8.1	Beleid en procedures voor informatie-uitwisseling		√	OSA	SC-08 Transmission Integrity
			√	OSA	SC-09 Transmission Confidentiality
			√	OSA	SC-01 System And Communications Protection Policy And Procedures
			√	OSA	SC-04 Information Remnance
			√	CSA	SA-03 Security Architecture - Data Security/Integrity
10.8.2	Uitwisselingsovereenkomsten	√			
			√	CSA	LG-02 Legal - Third Party Agreements
10.8.3	Fysieke media die worden getransporteerd	√	√	CSA	IS-32 Information Security - Portable/Mobile Devices
10.8.4	Elektronische berichtenuitwisseling		√	OSA	SC-05 Denial Of Service Protection
			√	CSA	IS-18 Information Security - Encryption

Vervolg op volgende pagina

Nr.	Titel	Verant. Klant	Verant. Cl. Lev.	OSA CSA	Code Open Security architecture - SP-011: Cloudcomputing Pattern [48] of Cloud Security Alliance Controls Matrix (CM) [49]
10.8.5	Systemen voor bedrijfsinformatie	√	√	CSA	SA-10 Security Architecture - Wireless Security
10.9	Diensten voor e-commerce		√		
10.9.1	E-commerce		√	OSA	SC-08 Transmission Integrity
			√	OSA	SC-09 Transmission Confidentiality
			√	OSA	CA-03 Information System Connections
			√	CSA	IS-28 Information Security - eCommerce Transactions
10.9.2	Onlinetransacties		√	OSA	SC-11 Trusted Path
			√	CSA	IS-18 Information Security – Encryption
			√	CSA	IS-28 Information Security - eCommerce Transactions
			√	CSA	SA-05 Security Architecture - Data Integrity
10.9.3	Openbaar beschikbare informatie	√			
			√	CSA	IS-18 Information Security – Encryption
			√	CSA	SA-05 Security Architecture - Data Integrity
10.10	Controle				
10.10.1	Aanmaken van audit-logbestanden		√	OSA	SI-04 Information System Monitoring Tools And Techniques
			√	CSA	SA-14 Security Architecture - Audit Logging/Intrusion Detection
10.10.2	Controle van systeemgebruik		√	OSA	RA-03 Risk Assessment
			√	OSA	SI-04 Information System Monitoring Tools And Techniques
			√	OSA	AC-13 Supervision And Review – Access Control
			√	OSA	AU-06 Audit Monitoring, Analysis, And Reporting
			√	CSA	SA-14 Security Architecture - Audit Logging/Intrusion Detection
10.10.3	Bescherming van informatie in logbestanden		√	CSA	SA-14 Security Architecture - Audit Logging/Intrusion Detection
10.10.4	Logbestanden van administrators en operators		√	OSA	SI-04 Information System Monitoring Tools And Techniques
			√	OSA	AU-06 Audit Monitoring, Analysis, And Reporting
			√	CSA	SA-14 Security Architecture - Audit Logging/Intrusion Detection
10.10.5	Registratie van storingen		√	OSA	RA-03 Risk Assessment
			√	OSA	SI-02 Flaw Remediation
			√	CSA	SA-14 Security Architecture - Audit Logging/Intrusion Detection
10.10.6	Synchronisatie van systeemklokken		√	CSA	SA-12 Security Architecture - Clock Synchronization

Toegangsbeveiliging

Deze paragraaf behandelt de beheersmaatregelen zoals die zijn beschreven in hoofdstuk 11 'Toegangsbeveiliging' uit de NEN-ISO/IEC 27002:2007 nl 'Code voor Informatiebeveiliging' [10].

Nr.	Titel	Verant. Klant	Verant. Cl. Lev.	OSA CSA	Code Open Security architecture - SP-011: Cloudcomputing Pattern [48] of Cloud Security Alliance Controls Matrix (CM) [49]
11.1	Bedrijfseisen ten aanzien van toegangsbeheersing				
11.1.1	Toegangsbeleid	√		OSA	AC-02 Account Management
		√		OSA	AC-01 Access Control Policies and Procedures
			√	CSA	IS-07 Information Security - User Access Policy
11.2	Beheer van toegangsrechten van gebruikers				
11.2.1	Registratie van gebruikers	√		OSA	PS-07 Third-Party Personnel Security
		√	√	CSA	IS-08 Information Security - User Access Restriction/Authorization
11.2.2	Beheer van speciale bevoegdheden	√	√	OSA	AC-02 Account Management
		√	√	CSA	IS-08 Information Security - User Access Restriction/Authorization

Vervolg op volgende pagina

Nr.	Titel	Verant. Klant	Verant. Cl. Lev.	OSA CSA	Code Open Security architecture - SP-011: Cloudcomputing Pattern [48] of Cloud Security Alliance Controls Matrix (CM) [49]
11.2.3	Beheer van gebruikerswachtwoorden	√	√	CSA	SA-02 Security Architecture - User ID Credentials
11.2.4	Beoordeling van toegangsrechten van gebruikers	√		OSA	AC-02 Account Management
		√		OSA	AC-13 Supervision And Review – Access Control
		√		OSA	AC-03 Access Enforcement
		√	√	CSA	IS-10 Information Security - User Access Reviews
11.3	Verantwoordelijkheden van gebruikers				
11.3.1	Gebruik van wachtwoorden	√	√	CSA	IS-16 Information Security - User Responsibility
			√	CSA	IS-17 Information Security - Workspace
11.3.2	Onbeheerde gebruikersapparatuur	√	√	OSA	AU-06 Audit Monitoring, Analysis, And Reporting
		√	√	CSA	IS-16 Information Security - User Responsibility
			√	CSA	IS-17 Information Security - Workspace
11.3.3	'Clear desk'- en 'clear screen'-beleid		√	CSA	IS-17 Information Security - Workspace
11.4	Toegangsbeheersing voor netwerken				
11.4.1	Beleid ten aanzien van het gebruik van netwerkdiensten		√	OSA	AC-01 Access Control Policies and Procedures
			√	CSA	IS-08 Information Security - User Access Restriction/Authorization
11.4.2	Authenticatie van gebruikers bij externe verbindingen		√	OSA	IA-03 Device Identification And Authentication
		√	√	CSA	SA-07 Security Architecture - Remote User Multi-Factor Authentication
11.4.3	Identificatie van netwerkapparatuur		√	OSA	IA-03 Device Identification And Authentication
			√	CSA	SA-13 Security Architecture - Equipment Identification
11.4.4	Bescherming op afstand van poorten voor diagnose en configuratie	√	√	CSA	IS-30 Information Security - Diagnostic/Configuration Ports Access
11.4.5	Scheiding van netwerken		√	OSA	AC-04 Information Flow Enforcement
			√	OSA	CA-03 Information System Connections
			√	OSA	AC-03 Access Enforcement
			√	OSA	SC-02 Application Partitioning
			√	OSA	SC-03 Security Function Isolation
		√	√	CSA	SA-09 Security Architecture - Segmentation
11.4.6	Beheersmaatregelen voor netwerkverbindingen		√	OSA	AC-04 Information Flow Enforcement
			√	OSA	CA-03 Information System Connections
			√	OSA	SC-07 Boundary Protection
		√	√	CSA	SA-11 Security Architecture - Shared Networks
11.4.7	Beheersmaatregelen voor netwerkroutering		√	OSA	AC-04 Information Flow Enforcement
			√	OSA	CA-03 Information System Connections
		√	√	CSA	SA-08 Security Architecture - Network Security
		√	√	CSA	SA-10 Security Architecture - Wireless Security
11.5	Toegangsbeveiliging voor besturingssystemen				
11.5.1	Beveiligde inlogprocedures	√	√		
11.5.2	Gebruikersidentificatie en –authenticatie	√	√	OSA	IA-05 Authenticator Management
11.5.3	Systemen voor wachtwoordbeheer	√	√	OSA	IA-05 Authenticator Management
11.5.4	Gebruik van systeemhulpmiddelen	√	√	CSA	IS-34 Information Security - Utility Programs Access
11.5.5	Time-out van sessies	√	√	CSA	SA-02 Security Architecture - User ID Credentials
11.5.6	Beperking van verbindingstijd		√	CSA	SA-04 Security Architecture - Application Security
11.6	Toegangsbeheersing voor toepassingen en informatie				
11.6.1	Beperken van toegang tot informatie	√	√	OSA	CM-05 Access Restrictions For Change
		√	√	CSA	IS-08 Information Security - User Access Restriction/Authorization
			√	CSA	SA-04 Security Architecture - Application Security
11.6.2	Isoleren van gevoelige informatie	√	√		
11.7	Draagbare computers en telewerken				

Vervolg op volgende pagina

Nr.	Titel	Verant. Klant	Verant. Cl. Lev.	OSA CSA	Code Open Security architecture - SP-011: Cloudcomputing Pattern [48] of Cloud Security Alliance Controls Matrix (CM) [49]
11.7.1	Draagbare computers en communicatievoorzieningen	√	√	OSA	AT-02 Security Awareness
		√	√	OSA	AT-03 Security Training
			√	OSA	IA-03 Device Identification And Authentication
		√	√	CSA	IS-32 Information Security - Portable/Mobile Devices
11.7.2	Telewerken	√	√	OSA	AC-02 Account Management
		√	√	CSA	IS-32 Information Security - Portable/Mobile Devices

Verwerving, ontwikkeling en onderhoud van informatiesystemen

Deze paragraaf behandelt de beheersmaatregelen zoals die zijn beschreven in hoofdstuk 12 'Verwerving, ontwikkeling en onderhoud van informatiesystemen' uit de NEN-ISO/IEC 27002:2007 nl 'Code voor Informatiebeveiliging' [10].

Nr.	Titel	Verant. Klant	Verant. Cl. Lev.	OSA CSA	Code Open Security architecture - SP-011: Cloudcomputing Pattern [48] of Cloud Security Alliance Controls Matrix (CM) [49]
12.1	Beveiligingseisen voor informatiesystemen	√	√	OSA	SA-01 System And Services Acquisition Policy And Procedures
12.1.1	Analyse en specificatie beveiligingseisen	√	√	OSA	SA-04 Acquisitions
			√	CSA	IS-04 Information Security - Baseline Requirements
			√	CSA	RM-03 Release Management - Quality Testing
12.2	Correcte verwerking in toepassingen				
12.2.1	Validatie van invoergegevens	√			
			√	CSA	SA-04 Security Architecture - Application Security
			√	CSA	SA-05 Security Architecture - Data Integrity
12.2.2	Beheersing van interne gegevensverwerking	√			
			√	CSA	SA-04 Security Architecture - Application Security
			√	CSA	SA-05 Security Architecture - Data Integrity
12.2.3	Integriteit van berichten	√	√	OSA	IA-02 User Identification And Authentication
			√	CSA	SA-04 Security Architecture - Application Security
			√	CSA	SA-05 Security Architecture - Data Integrity
12.2.4	Validatie van uitvoergegevens	√			
			√	CSA	SA-04 Security Architecture - Application Security
			√	CSA	SA-05 Security Architecture - Data Integrity
12.3	Cryptografische beheersmaatregelen				
12.3.1	Beleid voor het gebruik van cryptografische beheersmaatregelen	√	√	OSA	SC-12 Cryptographic Key Establishment And Management
			√	CSA	IS-18 Information Security – Encryption
		√	√	CSA	SA-10 Security Architecture - Wireless Security
12.3.2	Sleutelbeheer	√	√	OSA	SC-12 Cryptographic Key Establishment And Management
			√	CSA	IS-19 Information Security - Encryption Key Management
12.4	Beveiliging van systeembestanden				
12.4.1	Beheersing van operationele programmatuur		√	OSA	CM-03 Configuration Change Control
			√	OSA	SI-02 Flaw Remediation
			√	OSA	CM-01 Configuration Management Policy And Procedures
			√	CSA	RM-05 Release Management - Unauthorized Software Installations
12.4.2	Bescherming van testdata	√	√	OSA	IA-02 User Identification And Authentication
			√	CSA	DG-06 Data Governance - Non-Production Data
12.4.3	Toegangsbeheersing voor broncode van programmatuur	√			
			√	CSA	IS-33 Information Security - Source Code Access Restriction

Vervolg op volgende pagina

Nr.	Titel	Verant. Klant	Verant. Cl. Lev.	OSA CSA	Code Open Security architecture - SP-011: Cloudcomputing Pattern [48] of Cloud Security Alliance Controls Matrix (CM) [49]
12.5	Beveiliging bij ontwikkelings- en ondersteuningsprocessen				
12.5.1	Procedures voor wijzigingsbeheer	√	√	OSA	RA-03 Risk Assessment
		√	√	OSA	CM-03 Configuration Change Control
		√	√	OSA	SI-02 Flaw Remediation
		√	√	OSA	CM-01 Configuration Management Policy And Procedures
		√	√	OSA	SA-10 Developer Configuration Management
			√	CSA	DG-06 Data Governance - Non-Production Data
		√	√	CSA	RM-02 Release Management - Production Changes
12.5.2	Technische beoordeling van toepassingen na wijzigingen in het besturingssysteem	√	√	OSA	CM-03 Configuration Change Control
		√	√	OSA	SI-02 Flaw Remediation
		√	√	OSA	IA-02 User Identification And Authentication
		√	√	OSA	SA-10 Developer Configuration Management
		√	√	CSA	RM-02 Release Management - Production Changes
12.5.3	Restricties op wijzigingen in programmatuurpakketten	√	√	OSA	CM-03 Configuration Change Control
			√	CSA	SA-06 Security Architecture - Production/Non-Production Environments
12.5.4	Uitlekken van informatie	√			
			√	CSA	DG-07 Data Governance - Information Leakage
12.5.5	Uitbestede ontwikkeling van programmatuur	√			
			√	CSA	RM-04 Release Management - Outsourced Development
12.6	Beheer van technische kwetsbaarheden				
12.6.1	Beheersing van de technische kwetsbaarheden	√	√	OSA	RA-03 Risk Assessment
		√	√	OSA	SI-02 Flaw Remediation
			√	CSA	IS-20 Information Security - Vulnerability/Patch Management

Beheer van informatiebeveiligingsincidenten

Deze paragraaf behandelt de beheersmaatregelen zoals die zijn beschreven in hoofdstuk 13 'Beheer van informatiebeveiligingsincidenten' uit de NEN-ISO/IEC 27002:2007 nl 'Code voor Informatiebeveiliging' [10].

Nr.	Titel	Verant. Klant	Verant. Cl. Lev.	OSA CSA	Code Open Security architecture - SP-011: Cloudcomputing Pattern [48] of Cloud Security Alliance Controls Matrix (CM) [49]
13.1	Rapportage van informatiebeveiligings-gebeurtenissen en zwakke plekken		√	OSA	IR-01 Incident Response Policy And Procedures
13.1.1	Rapportage van informatiebeveiligings-gebeurtenissen		√	OSA	AT-02 Security Awareness
			√	OSA	AT-03 Security Training
			√	CSA	IS-23 Information Security - Incident Reporting
13.1.2	Rapportage van zwakke plekken in de beveiliging		√	CSA	IS-23 Information Security - Incident Reporting
13.2	Beheer van informatiebeveiligings-incidenten en –verbeteringen				
13.2.1	Verantwoordelijkheden en procedures	√	√	OSA	IR-01 Incident Response Policy And Procedures
			√	OSA	SC-05 Denial Of Service Protection
			√	CSA	IS-22 Information Security - Incident Management
13.2.2	Leren van informatiebeveiligingsincidenten		√	CSA	IS-25 Information Security - Incident Response Metrics
13.2.3	Verzamelen van bewijsmateriaal		√	CSA	IS-24 Information Security - Incident Response Legal Preparation

Bedrijfscontinuïteitsbeheer

Deze paragraaf behandelt de beheersmaatregelen zoals die zijn beschreven in hoofdstuk 14 'Bedrijfscontinuïteitsbeheer' uit de NEN-ISO/IEC 27002:2007 nl 'Code voor Informatiebeveiliging' [10].

Nr.	Titel	Verant. Klant	Verant. Cl. Lev.	OSA CSA	Code Open Security architecture - SP-011: Cloudcomputing Pattern [48] of Cloud Security Alliance Controls Matrix (CM) [49]
14.1	Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer				
14.1.1	Informatiebeveiliging opnemen in het proces van bedrijfscontinuïteitsbeheer	√		OSA	RA-03 Risk Assessment
		√	√	OSA	CP-01 Contingency Planning Policy And Procedures
			√	CSA	RS-01 Resiliency - Management Program
14.1.2	Bedrijfscontinuïteit en risicobeoordeling	√		OSA	RA-03 Risk Assessment
			√	CSA	RS-02 Resiliency - Impact Analysis
14.1.3	Continuïteitsplannen ontwikkelen en implementeren waaronder informatiebeveiliging	√	√	OSA	CP-01 Contingency Planning Policy And Procedures
			√	CSA	RS-03 Resiliency - Business Continuity Planning
14.1.4	Kader voor de bedrijfscontinuïtsplanning	√	√	OSA	AT-02 Security Awareness
		√	√	OSA	AT-03 Security Training
			√	CSA	RS-03 Resiliency - Business Continuity Planning
14.1.5	Testen, onderhoud en herbeoordelen van bedrijfscontinuïteitsplannen	√			
			√	CSA	RS-04 Resiliency - Business Continuity Testing

Naleving

Deze paragraaf behandelt de beheersmaatregelen zoals die zijn beschreven in hoofdstuk 15 'Naleving' uit de NEN-ISO/IEC 27002:2007 nl 'Code voor Informatiebeveiliging' [10].

Nr.	Titel	Verant. Klant	Verant. Cl. Lev.	OSA CSA	Code Open Security architecture - SP-011: Cloudcomputing Pattern [48] of Cloud Security Alliance Controls Matrix (CM) [49]
15.1	Naleving van wettelijke voorschriften				
15.1.1	Identificatie van toepasselijke wetgeving	√	√	OSA	AT-01 Security Awareness And Training Policy And Procedures
		√	√	OSA	CP-01 Contingency Planning Policy And Procedures
		√	√	OSA	PL-01 Security Planning Policy And Procedures
		√	√	OSA	CA-01 Certification, Accreditation, And Security Assessment
					Policies And Procedures
		√	√	OSA	IR-01 Incident Response Policy And Procedures
		√	√	OSA	SC-01 System And Communications Protection Policy And
					Procedures
		√	√	OSA	AC-01 Access Control Policies and Procedures
		√	√	OSA	SA-01 System And Services Acquisition Policy And Procedures
		√	√	OSA	CM-01 Configuration Management Policy And Procedures
		√	√	OSA	IA-01 Identification And Authentication Policy And Procedures
			√	CSA	CO-05 Compliance - Information System Regulatory Mapping
		√	√	CSA	DG-08 Data Governance - Risk Assessments
15.1.2	Intellectuele eigendomsrechten (Intellectual Property Rights, IPS)	√	√	OSA	CM-02 Baseline Configuration
			√	CSA	CO-06 Compliance - Intellectual Property
15.1.3	Bescherming van bedrijfsdocumenten	√	√	CSA	DG-08 Data Governance - Risk Assessments
15.1.4	Bescherming van gegevens en geheimhouding van persoonsgegevens	√	√	OSA	AT-02 Security Awareness
			√	CSA	DG-01 Data Governance - Ownership/Stewardship
		√	√	CSA	DG-08 Data Governance - Risk Assessments

Vervolg op volgende pagina

Nr.	Titel	Verant. Klant	Verant. Cl. Lev.	OSA CSA	Code Open Security architecture - SP-011: Cloudcomputing Pattern [48] of Cloud Security Alliance Controls Matrix (CM) [49]
15.1.5	Voorkomen van misbruik van IT-voorziening	√	√		
15.1.6	Voorschriften voor het gebruik van cryptografische beheersmaatregelen	√	√		
15.2	Naleving van beveiligingsbeleid en –normen en technische naleving				
15.2.1	Naleving van beveiligingsbeleid en –normen	√	√	OSA	CA-02 Security Assessments
			√	OSA	CA-07 Continuous Monitoring
			√	CSA	IS-14 Information Security - Management Oversight
15.2.2	Controle op technische naleving	√	√	OSA	CA-02 Security Assessments
			√	OSA	CA-07 Continuous Monitoring
			√	CSA	SA-14 Security Architecture - Audit Logging/Intrusion Detection
15.3	Overwegingen bij audits van informatiesystemen				
15.3.1	Beheersmaatregelen voor audits van informatiesystemen		√	CSA	CO-01 Compliance - Audit Planning
15.3.2	Bescherming van hulpmiddelen voor audits van informatiesystemen		√	CSA	IS-29 Information Security - Audit Tools Access

Colofon

uitgave
Nationaal Cyber Security Centrum, Den Haag | Januari 2012

Wilhelmina van Pruisenweg 104 | 2595 AN Den Haag
Postbus 117 | 2501 CC Den Haag

T 070-888 75 55
F 070-888 75 50

E info@ncsc.nl
I www.ncsc.nl

Nationaal Cyber Security Centrum

Het Nationaal Cyber Security Centrum (NCSC) draagt via samenwerking tussen bedrijfsleven, overheid en wetenschap bij aan het vergroten van de weerbaarheid van de Nederlandse samenleving in het digitale domein.

Het NCSC ondersteunt de Rijksoverheid en organisaties met een vitale functie in de samenleving met het geven van expertise en advies, response op dreigingen en het versterken van de crisisbeheersing. Daarnaast voorziet het in informatie en advies voor burger, overheid en bedrijfsleven ten behoeve van bewustwording en preventie. Het NCSC is daarmee het centrale meld- en informatiepunt voor ICT-dreigingen en -veiligheidsincidenten.

Nationaal Cyber Security Centrum
Wilhelmina van Pruisenweg 104 | 2595 AN Den Haag
Postbus 117 | 2501 CC Den Haag

T 070-888 75 55
F 070-888 75 50

E info@ncsc.nl
I www.ncsc.nl

Januari 2012