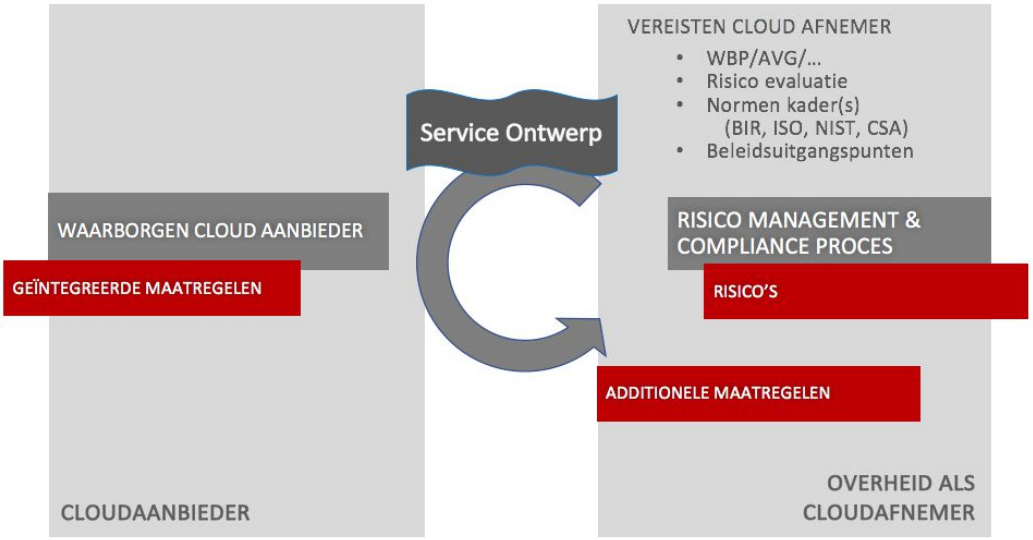
Cloud Governance

Rollen en Verantwoordelijkheden van de Overheid voor Succesvol en Veilig Cloudgebruik



Status	Becommentarieerde Praktijk
Opdrachtgevers	Rijkscloud en CIP
Auteurs	CIP XaaS werkgroep
Datum	22 November 2017

Vraagstuk Cloud Informatiebeveiliging en Privacybescherming

Om beter aan de vraag van burgers en snelle verandering van wet- en regelgeving te kunnen voldoen, zijn overheidsorganisaties steeds meer "*as a Service*" IT-modellen gaan adopteren, zoals "*Software as a Service*" (SaaS), "*Platform as a Service*" (PaaS) en "*Infrastructuur as a Service*" (IaaS). In het vervolg van dit whitepaper zullen deze worden aangeduid als *XaaS*. Deze modellen kenmerken zich door kosten per gebruik en grotere flexibiliteit ten opzichte van traditionele IT-omgevingen.

Maar hoe kunnen overheidsorganisaties garanderen dat vanuit het oogpunt van informatiebeveiliging en privacybescherming dergelijke XaaS modellen op juiste wijze worden gebruikt?
Het antwoord hierop begint met het regelen van eigen verantwoordelijkheden door middel van Cloud Governance. Een Framework hiervoor wordt bijvoorbeeld door The Open Group gegeven.

In deze eerste van een beoogde serie van whitepapers wordt uiteengezet waarom Cloud Governance noodzakelijk is voor dergelijke garanties, wat de implicaties zijn, en een aanzet wordt gegeven hoe overheidsorganisaties hiermee om zouden dienen te gaan. Het is de bedoeling dat deze thematiek in aanvullende whitepapers verder wordt uitgewerkt.
Cloud Governance regelt de verantwoordelijkheden van Cloud–Aanbieders en –Afnemers, als ook Cloud Gebruikers. In dit whitepaper worden de volgende definities gebruikt:

- De *Cloud Gebruiker* is de daadwerkelijke gebruiker van Cloud Services. Dat kan voor SaaS-services een medewerker en/of burger zijn, voor IaaS en PaaS Services zijn dat typisch infrastructuur- of applicatieteams werkzaam binnen of voor de Cloud Afnemer.
- De *Cloud Afnemer* is het overheidsonderdeel dat de Cloud Service inkoopt en beschikbaar maakt voor de Cloud Gebruiker. De Cloud Afnemer selecteert op basis van functionele en niet-functionele eisen Cloud Aanbieders. Daarbij is de Cloud Afnemer ook verantwoordelijk voor het toetsingsproces.
- De *Cloud Aanbieder* biedt standaard Cloud Services aan, inclusief benodigde waarborgen die de Cloud Afnemer in staat stellen het evaluatieproces te doorlopen.

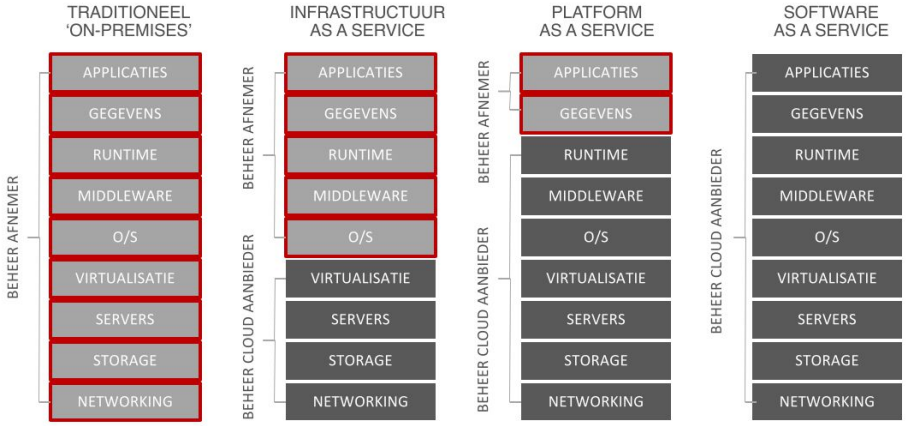
Gebaseerd op gemeenschappelijke ervaringen voor succesvol en veilig Cloud gebruik, zijn de volgende criteria van essentieel belang om door de Cloud Afnemer geregeld te worden:

- Criteria die aan XaaS providers gesteld dienen te worden, op gebied van informatiebeveiliging en privacybescherming
- Criteria voor hoe overheidsorganisaties zich dienen te veranderen om XaaS modellen veilig te gebruiken, waaronder:
    - Het inregelen van gepaste Governance maatregelen
    - Het inregelen van IT-functies voor het ondersteunen van selecteren, contracteren, uitrollen, en gebruiken van XaaS modellen

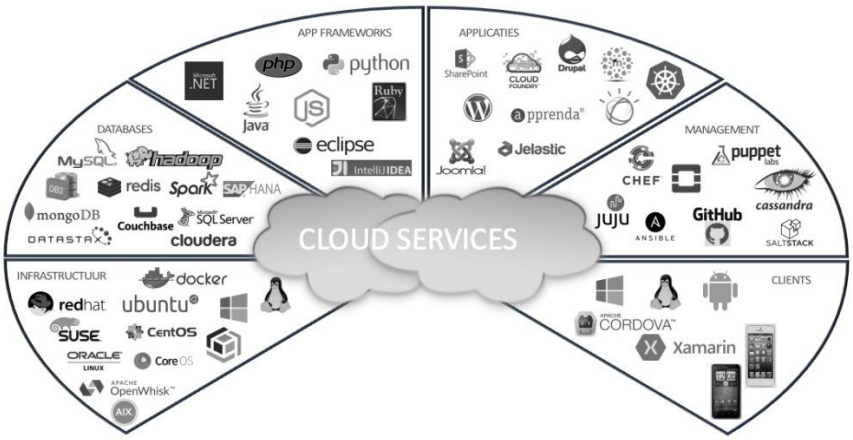
Hiermee kunnen overheidsorganisaties zich terdege voorbereiden op de impact die XaaS modellen hebben op de informatiebeveiliging en privacybescherming van hun omgevingen.

Belang van Cloud Governance

Als aangegeven dienen met XaaS modellen de verantwoordelijkheden van Cloud-Aanbieders en –Afnemers vastgesteld te worden. Deze verantwoordelijkheden kunnen inzichtelijk gemaakt worden aan de hand van de figuur hieronder. Dit wordt als startpunt gebruikt om belang van Govenance te illustreren. Hierop zal dieper worden ingegaan in de beoogde serie van whitepapers. Gegeven is een overzicht van de gangbare XaaS modellen, gebaseerd op NIST (*National Institute of Standards and Technology*) modellen. NIST staat ook aan de basis van de Cloud Referentie Architectuur die binnen de overheid wordt gehanteerd.
Van links naar rechts gezien verandert de verantwoordelijkheid van het onderhouden van de verschillende lagen van de eigen organisatie naar de gekozen aanbieder en daarmee ook van de genomen maatregelen aangaande informatiebeveiliging en privacybescherming. Deze verandering van eigen verantwoordelijkheid, welke bij de adoptie van Cloud goed moet worden begrepen en gedefinieerd, vormt een fundamenteel uitgangspunt voor succesvol en veilig Cloud gebruikt. Hierbij dient opgemerkt te worden dat de Cloud Afnemer natuurlijk altijd verantwoordelijk blijft voor het juiste *gebruik* en *toepassing* van de gehele Cloud oplossing.



Zo heeft de Cloud Afnemer vele keuzemogelijkheden voor de lagen onder de eigen verantwoordelijkheid, zeker waar het IaaS en PaaS betreft. Illustratief daarvoor is het onderstaande overzicht, dat een -niet uitputtend- overzicht geeft van wat er op verschillende lagen kan worden ingezet. Om tot een verantwoord en succesvol gebruik te komen van verschillende Cloud Services, zal de Cloud Afnemer Cloud-Strategie, -Ontwerp en -Uitrolprocessen dienen te hebben ingericht. Deze dienen invulling te geven aan zowel functionele als niet-functionele vereisten zoals geldende informatiebeveiliging- en privacy-vereisten als ook het inregelen van de benodigde Audit Controls. De Cloud Afnemer zal dus regie moeten voeren op de architectuur en werking van in- en externe Cloud Services in zijn voortbrengingsketen.



Eigen Verantwoordelijkheden van Overheid en Cloud Aanbieders

Zoals aangegeven zijn voor het succesvol en veilig Cloud Services gebruik het hebben van Cloud-Strategie, -Ontwerp en -Uitrolprocessen doorslaggevend. Welke laag door de Cloud Aanbieder wordt beheerd, bepaalt de scope van controles van resources. Dit resulteert in zowel verantwoordelijkheden van de Cloud Aanbieder als ook de betreffende overheidsorganisatie. Vanuit het oogpunt van audit processen is dit onderscheid cruciaal.

Zowel Cloud-Afnemers als -Aanbieders moeten voldoen aan respectievelijk op hen van toepassing zijnde wet- en regelgeving. Beiden hebben verantwoordelijkheden betreffende continuïteit, informatiebeveiliging en privacybescherming. De scope van controle en service-leveringsmodellen zijn dan ook fundamenteel voor de demarcatie van verantwoordelijkheden en controleerbaarheid voor succesvol Cloud gebruik.
Cloud Aanbieders, zoals IBM en Microsoft, realiseren in de ontwikkeling en de operatie van hun oplossingen intrinsieke security en privacy maatregelen. Deze dragen bij aan het vertrouwen in de geboden Cloud Services. Ze leveren vervolgens veiligheidscontroles, rapportages en mogelijkheden. Een Cloud Afnemer kan hiermee inzicht verkrijgen in de lagen die beheerd worden door de Cloud Aanbieder en hoe de Afnemers-data en -applicaties te beschermen. De Cloud Afnemer moet de eigenaar en controleur van de eigen data en digitale identiteiten zijn, en heeft dan ook de verantwoordelijkheid om die te beschermen, en zal dan ook gepaste maatregelen dienen te hebben.
Een aanzet hoe bovenstaande in te regelen wordt beschreven in de volgende paragrafen. Hierbij wordt eerst gekeken naar het belang van continue kwaliteitsverbetering, en daarop gebaseerd een Cloud Governance Aanpak met Evaluatieproces.

Doorlopende Kwaliteitsverbetering van Cloud Services

Het doorlopend verbeteren van de kwaliteit van Cloud Services is een must voor iedere Cloud-Aanbieder en -Afnemer. Hiermee wordt de mogelijkheid gecreëerd om de kwaliteit, prestaties en dienstverlening van de organisatie te verbeteren. Gebaseerd op gemeenschappelijke praktijkervaringen kan het gebruik van Cloud alleen dan succesvol en veilig zijn.
In deze context betekent "*Kwaliteit Leveren*" het kunnen voldoen aan de uitgesproken of vanzelfsprekende verwachtingen van de Cloud Gebruikers. Om daartoe in staat te zijn moeten niet alleen processen op orde zijn, maar moet ook het Plan-Do-Check-Act denken in de genen van de Cloud-Aanbieder en -Afnemer zitten. In onderstaande wordt aangegeven waar deze bij Cloud Services van belang zijn, en waar deze bepaald en vastgelegd dienen te zijn in de Strategie, Ontwerp, Transitie en Operatie van Cloud Services:

- *PLAN*: Kijk naar huidige werkzaamheden en ontwerp een plan voor de verbetering van deze werkzaamheden. Stel voor deze verbetering doelstellingen vast
  - *Cloud Service Strategie en Ontwerp*
- *DO*: Voer de geplande verbetering uit in een gecontroleerde proefopstelling
  - *Cloud Service Transitie*
- *CHECK*: Meet het resultaat van de verbetering en vergelijk deze met de oorspronkelijke situatie en toets deze aan de vastgestelde doelstellingen
  - *Cloud Service Operatie*
- *ACT*: Bijstellen aan de hand van de gevonden resultaten bij CHECK
  - *Cloud Service Ontwerp*

Ervaring leert dat "*PLAN-DO*" vaak wel lukt, maar "*CHECK-ACT*" vaak achterwege blijven wegens nieuwe projecten en dergelijke. Zo worden er wel plannen gemaakt en uitgevoerd. Maar er wordt geen check gedaan op de resultaten in relatie tot de gestelde doelen. Door middel van Cloud Governance kan dit inzichtelijk gemaakt worden en dagelijkse gang van zaken worden bijgesteld. Hiervoor dienen rollen, output en verantwoordelijkheden van betrokken functionarissen/partijen duidelijk te zijn belegd door de Cloud Afnemer.

Doorlopende Kwaliteitsverbetering van Cloud Services in de Praktijk

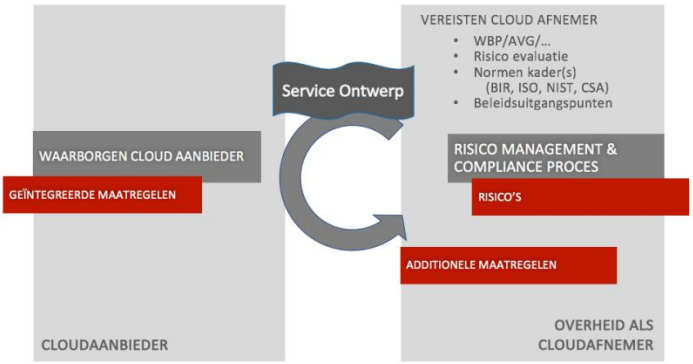
Kwaliteit staat en valt met visie en beleid. Hebben de stakeholders een duidelijke visie op de benodigde kwaliteit die geleverd moet worden en dragen ze die visie ook uit? En uitdragen is niet alleen zeggen wat je moet doen maar vooral doen wat je zegt. Maar doen wat je zegt is niet voldoende. Daarom komt het doorlopend verbeteren van Cloud Services in de kern op het volgende neer:

- Service Level Managementproces dient in voldoende mate te zijn ingericht, zodat op basis van goed beschreven uitkomst afspraken mogelijk zijn over de belangrijke en benodigde kwaliteitsaspecten van de Cloud Service: performance, beschikbaarheid, continuïteit , beveiliging en ondersteuning
- Afspraken zijn in meetbare begrippen gedefinieerd, zodat daar ook over gerapporteerd kan worden
- Noodzakelijk maatregelen (zoals diverse beveiligingsmaatregelen) worden afgedwongen door audits en certificeringen
- Stel iemand aan die verantwoordelijk is voor het doorlopend verbeteren van de Cloud Service
- Zorg voor besluitvorming en voldoende resources om daadwerkelijk na besluitvorming verbeteringen in de kwaliteit van de processen en de service te kunnen realiseren
- Het beëindigen van het gebruik van de afgenomen Cloud Service voldoet aan één of meerdere in de exit-strategie vastgelegde condities

Bovenstaand proces zorgt ervoor dat de kwaliteit van de geleverde Cloud Services gewaarborgd en doorlopend verbeterd worden. Dit alles om bij te dragen aan de benodigde rechtmatigheidsdoelstellingen als compliance tegenover wet- en regelgeving, informatiebeveiliging en privacybescherming.

Cloud Evaluatie Aanpak ten behoeve van Audit Controls

Om te kunnen vaststellen hoe de verschillende verantwoordelijkheden zijn vastgelegd, ingeregeld en gehandhaafd door middel van Cloud Governance is het noodzakelijk een Cloud Evaluatie aanpak in te regelen en uit te voeren. Hierin worden de niet-functionele attributen, zoals onder andere privacy, security en beschikbaarheid van de geboden Cloud Services geëvalueerd en getoetst tegen de eisen van de Cloud Afnemer. Ook hier dient dit beschouwd te worden tegen het licht van het paradigma van de eigen verantwoordelijkheden. Een fundamenteel uitgangspunt moet daarbij zijn dat de Cloud Aanbieder zich principieel transparant opstelt: Cloud Afnemers hebben informatie nodig aangaande hoe gegevens worden verwerkt in de Cloud, zodat de (potentiële) Cloud Afnemer in staat wordt gesteld voldoende beeld te krijgen om aan gestelde verplichtingen te voldoen.
Hoe een evaluatieproces eruit kan zien, is in grote lijnen weergegeven in onderstaande figuur, welke gebaseerd is op gemeenschappelijke CIP XaaS werkgroep leden ervaringen. In het vervolg worden kort de belangrijkste stappen beschreven; in een volgend whitepaper wordt het proces meer uitgewerkt.



Voorafgaande aan de feitelijke evaluatie van de services van een Cloud Aanbieder, dient door de afnemende organisatie helder vastgelegd te worden wat de beoogde doelstellingen, vereisten en vragen zijn. Daarbij gaat het in de praktijk over het algemeen over rechtmatigheidsdoelstellingen (compliance tegenover wet- en regelgeving), informatiebeveiliging en privacy. Concreet wordt dan vaak gekozen voor evaluatie tegen de Wet Bescherming Persoonsgegevens en de Algemene Verordening Gegevensbescherming en vanuit informatiebeveiliging wordt de BIR:2012 baseline als toetsingskader gehanteerd. Het is van belang de toetsing niet slechts op een (verouderde) baseline te baseren, maar zoveel mogelijk te werken vanuit risicomanagement. Er bestaan goede internationaal geaccepteerde raamwerken die kunnen helpen bij een risicomanagement programma, zoals ISO 27001 en het NIST CSF. Ook de herziening van BIR, de BIO, zal zich meer conformeren aan ISO-standaarden.

Na het zorgvuldig vaststellen van de vereisten, kan men het daadwerkelijke evaluatieproces starten. In dat proces worden echter niet alleen de waarborgen en maatregelen van de Cloud Aanbieder gevalueerd, maar zullen ook de (aanvullende) maatregelen en proceskeuzes die de Cloud Afnemer zal kunnen (of moeten) nemen worden geadresseerd. Denk daarbij aan Governance maatregelen, maar ook additionele IT-functies, zoals toegangsbeheer, datamanagement en Cloud Monitoring.

Het evaluatieproces omvat verder de volgende belangrijkste stappen:

- Uitvoeren van een risico inschatting van het service ontwerp van de in te zetten Cloud gebaseerde oplossing. Dit leidt tot een overzicht van mogelijke risico's en gewenste maatregelen.
- Uitvragen maatregelen en waarborgen aan de Cloud Aanbieder voor die maatregelen die onder de uitvoeringsverantwoordelijkheid liggen van de Cloud Aanbieder. Dit is in de basis afhankelijke van het gekozen Cloud Service Model.
- De Cloud Aanbieder biedt een pakket van waarborgen, ter beoordeling van de Cloud Afnemer. Belangrijk onderdeel daarvan moeten zowel contractuele waarborgen (SLA, verwerkersovereenkomst) als derden-verklaringen (ISO-certificeringen, ISAE3000 SOC 2 verklaringen) zijn.
- Evaluatie van de claims en waarborgen van de provider in combinatie met de maatregelen genomen/voorgesteld door de afnemer zelf binnen het risicomanagement proces.
- Adresseren rest risico's en demonstreren van compliance. In de praktijk zullen een aantal uitgangspunten of risico's niet volledig geadresseerd zijn. Het is dan mogelijk om in dialoog met de Cloud Aanbieder te bepalen of er nog extra waarborgen/maatregelen mogelijk zijn. De afnemer kan in overleg met de Cloud Afnemer ook bepalen of er wellicht andere technische en organisatorische maatregelen te nemen zijn of dat -in overleg met de bedrijfsvoering- het risico geaccepteerd (en gedocumenteerd) wordt. Vervolgens kan de evaluatie door een interne of externe audit organisatie (zoals bijvoorbeeld de ADR) beoordeeld worden om compliance te demonstreren.

Aandachtspunten voor toepassing en gebruik van Cloud Services

In dit whitepaper is een overzicht gegeven van de eigen verantwoordelijkheden van Cloud-Aanbieders en –Afnemers, en hoe Cloud Governance daar een rol in speelt. Dit is gedaan aan de hand van XaaS modellen en wat hun implicaties zijn. Op basis hiervan is een aanzet gegeven tot hoe overheidsorganisaties hier mee om dienen te gaan. Hiervoor is een aanzet beschreven voor een aanpak die de volgende elementen heeft:

- Criteria die aan XaaS Providers gesteld dienen te worden, op gebied van informatiebeveiliging en privacybescherming
- Criteria voor hoe overheidsorganisaties zich dienen te veranderen om XaaS modellen veilig te gebruiken, waaronder:
    - Het inregelen van gepaste Governance maatregelen
    - Het inregelen van IT-functies voor het ondersteunen van selecteren, contracteren, uitrollen, en gebruiken van XaaS modellen

Al deze elementen zijn cruciaal voor succesvol en veilig Cloud gebruik met de benodigde rechtmatigheids-doelstellingen als compliance tegenover wet- en regelgeving, informatiebeveiliging en privacybescherming. Verdere detaillering en handvatten worden gegeven in een beoogde serie van whitepapers.

De oproep is dan ook om voordat Cloud Services gebruikt gaan worden, u als Cloud Afnemer de volgende zaken geregeld dient te hebben: *Cloud-Strategie, -Ontwerp en -Uitrolprocessen alsmede Audit Controls.*

CIP XaaS Werkgroep Leden

CIP XAAS white paper "Cloud Governance" is een product van de CIP-werkgroep Xaas, actief is sinds begin 2016. Dit document heeft in de tweede helft van 2017 zijn huidige vorm gekregen dankzij de bijdragen van de volgende groepsleden:

A. Donkers, DUO
A. Haijen, Oracle
A. Kint, CIP
A.C.J. Koedijk, Belastingdienst
C. van der Struijf, IBM
D. Brocker, DJI
D. Kerssens, Rijkscloud
E. Bos, SSO Noord
E. Strijland, SVB
F. Vos, DUO
I. Profijt, Oracle
J. Geskus, PWC
J. Harms, Min BZK
L. vd Tas, DJI
M. van de Berg, Rijkscloud
M. Vliem, Microsoft
P. Kazil, NL NCSA
P. Visser, ATOS
R. Bergsma, IUC Noord
R. Spuibroek, Min BZK
T. Slebioda , CIP
T. Sondermeijer, Capgemini
W. Tewarie, CIP

Considerans

Met het doel informatie-uitwisseling en kennisdeling te bevorderen, wil CIP onder andere 'good practices' ter beschikking stellen. Dit kunnen praktijkvoorbeelden zijn, handreikingen voor beleid, beschrijvingen van de stand van zaken in bepaalde ontwikkelingen, en dergelijke. De herkomst is van oorsprong een reflectie op een onderwerp door mensen in de CIP-kring, maar het kunnen ook notities zijn uit de praktijk van de CIP-organisaties die zonder verder commentaar worden gepubliceerd. De kern is dat de bijdragen altijd zijn gebaseerd op de expertise van de opstellers en deelnemende reviewers en/of het idee dat wat in n organisatie goed werkt, ook voor andere organisaties nuttig zou kunnen zijn. Soms is het resultaat dus de uitkomst van een groepsproces en in andere gevallen wordt iets 'as is' ter kennisneming of overname aangeboden. CIP heeft categorie n geformuleerd waarmee reikwijdte, intentie, status en/of draagvlak van CIP-publicaties wordt aangegeven. Deze publicatie valt in categorie 2: "*becommentarieerde praktijk: een door meerdere professionals veralgemeniseerde praktijk als handreiking voor hergebruik binnen ge nteresseerde organisaties*".
Een nadere uitleg hiervan staat op www.cip-overheid.nl.

De CIP-documenten hebben geen ander doel dan kennisoverdracht en reflecteren niet noodzakelijk de opvattingen van alle contribuanten, CIP-deelnemers en/of alle CIP-partijen. Publicatie vindt plaats op zowel de openbare website www.cip-overheid.nl als de besloten community site cip.pleio.nl.

CIP-documenten kunnen van tijd tot tijd aanpassingen ondergaan of worden ingetrokken als gevolg van veranderde inzichten. De CIP-redactie streeft binnen haar mogelijkheden naar een zo actueel mogelijke status van de documenten. In de praktijk zal enige tijd verstrijken voordat wijzigingen kunnen zijn doorgevoerd. Suggesties voor aanpassingen kunnen ook door lezers worden aangedragen en worden altijd in behandeling genomen.