

Aanpak voor het vaststellen van Digitale Autonomie

Een accreditatie voor digitale autonomie

Concept document
19 februari 2026

Inhoudsopgave

1. Waarom een accreditatie	3
2. Introductie	4
3. De noodzaak van een breed geaccepteerde accreditatie aanpak	5
3.1 Context: de ontwikkelingen die hebben geleid tot de actualiteit van het thema digitale autonomie	5
3.2 Wat verstaan we onder digitale autonomie: de verwarring en de claims	
3.3 Waarom een accreditatie: de gedachte erachter	8
3.4 Hoe verhoudt zich dit tot certificeringen en/of standaarden	8
3.5 Conclusie	8
4. Beschrijving van de componenten: de criteria	9
4.1 Juridische autonomie (CSP niveau)	9
EU & NL regelgeving	9
Toepasselijke jurisdictie	9
UBO-verhouding	9
Zeggenschap & controle	9
4.2 Technische autonomie (dienst niveau)	9
Data-interoperabiliteit	9
Portabiliteit	9
Technologische onafhankelijkheid	9
Exit-strategie & continuity	9
Escrow-regeling (optioneel)	9
4.3 Organisatorische transparantie (CSP en Dienst niveau)	9
Organisatiestructuur	9
Strategische besluitvorming	9
Ketenverantwoordelijkheid	9
Jaarrekeningen en financiële rapportages	9
4.4 Accreditatie en volgorde in niveau van accreditatie	10
Criteria, volgorde en niveau's	10
5. In de praktijk	11
5.1 Gebruik van de accreditatie: hoe toe te passen / een handleiding	11
5.2 Adoptie van de accreditatie: hoe autonoom zijn aangeboden oplossingen in onze sector	11
6. De accreditatie en de toekomst: statisch gegeven of ontwikkelend inzicht	12
7. Bijlage 1 Conformiteitsbeoordeling	13

1. Waarom een accreditatie

Veel organisaties vinden het belangrijk om zeker te stellen dat hun diensten betrouwbaar zijn en op generlei wijze onder invloed staan van actoren buiten de EU en/of dat het snel mogelijk is te schakelen naar een alternatief indien gewenst.

Dit onderwerp is erg urgent geworden door de recente geopolitieke ontwikkelingen en leidt bij veel organisaties tot het prioriteren van digitale autonomie.

Een accreditatie 'Digitale Autonomie' geeft aan dat een Cloud Service Provider (CSP) voldoet aan de verschillende aspecten van digitale autonomie.

De accreditatie helpt organisaties en met name overheden om inzicht te krijgen in digitale onafhankelijkheid van hun clouddiensten.



2. Introductie

Als branchevereniging van de Nederlandse cloud- en internetsector zijn wij diep betrokken bij de discussie rond digitale autonomie. Wij proberen in dit debat op een constructieve manier de verschillende partijen te helpen om stappen te maken die organisaties en bedrijven uit verschillende sectoren kunnen helpen om, zonder afbreuk te doen aan wat er al gebouwd is, een balans te vinden waarin meer ruimte gevonden kan worden voor samenwerking met de eigen Nederlandse industrie.

Digitale soevereiniteit, digitale onafhankelijkheid, digitale autonomie: allemaal termen om een thema te benoemen dat heel lang ondergeschoven bleef en dat opeens center stage is geworden.

Controle over onze digitalisering is een onderwerp dat de politiek, de overheid en de media belangrijk vinden.

Er zijn meerdere redenen waarom het thema naar de voorgrond is gekomen:

- De geopolitieke ontwikkelingen zorgen ervoor dat de hele EU zich bewust is geworden van het belang van onafhankelijk blijven of worden van buitenlandse mogendheden.
- Daaraan gelieerd is de bezorgdheid over de afhankelijkheid van een klein groepje hele grote techreuzen die we in Nederland en in de EU hebben laten ontstaan en het gebrek aan een 'Plan B voor het geval dat wij later van die afhankelijkheid af zouden willen.
- Een derde reden mag gezocht worden in de alsmaar toenemende cyberdreigingen die bedrijf en burger steeds meer bezighouden.
- Tot slot is er nog een vierde reden: het gunnen van grote projecten en investeringen aan Nederlandse en Europese partijen die daar klaar voor staan. Investeren in je eigen mensen en je eigen economie. Investeren in werkgelegenheid en het uitbouwen van de infrastructuur en het mogelijk maken voor de eigen industrie om zich verder te ontwikkelen.

Het is inmiddels wel duidelijk dat we in Nederland en Europa moeten beginnen om de implementatie van deze technologieën aan onze eigen bedrijven te durven gunnen om daarmee de ontwikkeling en opschaling ervan mogelijk te maken.

Het doel van dit document is om te duiden waar de discussie om gaat: over welke definities kunnen alle stakeholders het eens worden? Wat zijn de verschillende aspecten die komen kijken bij dit thema? En belangrijk: hoe kan een selectie richting autonome oplossingen en partijen die dit leveren eruit zien. De accreditatie aanpak gebruik makend van een combinatie van criteria dient voor een ieder begrijpelijke en heldere elementen en stappen te bevatten.

3. De noodzaak van een breed geaccepteerde accreditatie aanpak

3.1 Context: de ontwikkelingen die hebben geleid tot de actualiteit van het thema digitale autonomie

De evolutie van clouddiensten in Nederland, de impact op de IT-markt en het veranderende overheidsbeleid.

Vroege adoptie (rond 2015)

Hoewel het uitbesteden van IT al gebruikelijk was, kwam de uitbesteding van kernelementen zoals servers (IaaS) en opslag naar de cloud in 2015 nog maar net op gang. SaaS-applicaties waren de belangrijkste drijfveer en beeldbepaler van de cloudgroei in die periode. De overstap naar cloud gebaseerde infrastructuur (IaaS) was destijds nog niet mainstream en verliep langzaam.

Huidige situatie

Clouddiensten zijn in de afgelopen twee decennia sterk gestegen en zijn nu breed geaccepteerd, ook voor bedrijfskritische toepassingen. Cloud wordt meer en meer de standaard voor de ontwikkeling van applicaties en diensten. Lokale IT-bedrijven integreren publieke cloudoplossingen in hun aanbod. Voor aanbieders is specialisatie in cloud-gerelateerd aanbod nu een vereiste om relevant te blijven.

IT-dienstverleners

Meer dan de helft van de IT-dienstverleners (zoals MSP's, resellers en VAR's) heeft het beheer van IT-infrastructuur in haar dienstenportfolio. Dit is vooral het geval bij kleinere MKB-bedrijven (zzp'ers tot 50 fte), wat bevestigt dat zij hun infrastructuur uitbesteden aan een vertrouwde, lokale ICT-professional. De meest bediende verticale segmenten zijn de zorg en de overheid, gevolgd door onderwijs, zakelijke dienstverlening en de financiële sector.

Overheidsbeleid

De overheid is verschoven van een beleid van IT in eigen hand naar het gebruik van commerciële clouddiensten vanwege de flexibiliteit en kostenbesparing. In 2022 is een nieuwe cloudstrategie vastgesteld. Deze staat commercieel cloudgebruik toe, maar met strenge restricties om veiligheidsrisico's te minimaliseren. Belangrijke voorwaarden zijn een verplichte risicoanalyse, een verbod op opslag van staatsgeheimen en uitsluiting van leveranciers uit landen met een actief cyberprogramma tegen Nederlandse belangen. Voor basis- en bijzondere persoonsgegevens geldt het principe 'nee, tenzij'. Hoewel de centrale overheid dit beleid opstelt, wordt de ICT-besteding in de praktijk nog grotendeels autonoom door tientallen departementale CIO's beslist. De staatssecretaris voor Digitale Zaken wil hierin meer centralisatie aanbrengen.



3.2 Wat verstaan we onder digitale autonomie: de verwarring en de claims

Digitale autonomie kent vele facetten. Er is zeer veel verschillende uitleg over te vinden. Men gebruikt de term vaak naar eigen inzicht en voordeel. Als brancheorganisatie hechten we belang aan een heldere uitleg en willen daarmee ook een basis bieden voor verdere discussie. In een eerder in februari van dit jaar gepubliceerd whitepaper hebben we deze uiteenzetting ook gedeeld.

Doel: hebben we het over hetzelfde?

Op dit moment gebruikt iedereen de termen soevereiniteit, autonomie en onafhankelijkheid meestal door elkaar en zonder dat er eenduidige definities zijn. Er is behoefte aan een terminologie die door iedereen gebruikt kan worden, met begrippen die een breed draagvlak hebben. Wij willen hiermee een voorzet geven. Wij nodigen iedereen daarom uit om deze definitie zelf aan te vullen, om er kritiek op te hebben en commentaar op te leveren. Het is belangrijk dat wij allemaal (industrie, beleidsmakers, wetgevers en klanten) meedenken en het uiteindelijk eens worden over definities die breed gedragen worden. Een heldere definitie van digitale autonomie is belangrijk omdat deze:

- herkenbaar en relevant is voor alle stakeholders (waaronder cloudproviders, cloudgebruikers, beleidsmakers op zowel nationaal als internationaal niveau, maatschappelijke organisaties),
- (grotendeels) door deze stakeholders word onderschreven,
- het mogelijk maakt de mate van digitale autonomie van een product, dienst, proces of organisatie vast te stellen,
- wordt ingezet in het publieke debat over digitale autonomie,
- kan dienen voor een eenduidige inkoop en contractering van soevereine clouddiensten

Digitale autonomie voor wie?

Het is belangrijk om vast te stellen voor wie en in welk verband we het hebben over digitale autonomie. We hebben het hier over de clouddienst en diens leverancier. Meer specifiek de Europese digitale autonomie. We laten dus nationale of niet-Europese autonomie buiten beschouwing. De autonomie van de cloudgebruiker is mede afhankelijk van de autonomie van de leverancier en diens diensten.

Hoe is digitale autonomie vast te stellen?

Digitale autonomie kan worden bepaald aan de hand van de onderstaande, niet-uitputtende lijst van aspecten:

- A.** Uitsluitend en exclusief voldoen aan aan Europese en nationale regelgeving.
- B.** Toepasselijke jurisdictie voor de clouddienst/dataverwerking en cloudleverancier is EU only. Er is dus geen sprake van een andere jurisdictie anders dan die van de EU.
- C.** Organisatorische eigenschappen van de cloudleverancier.
- D.** Mate van controle door de data-eigenaar over de data(verwerking) en de rechtsbescherming en handhaving van die controle.
- E.** Interoperabiliteit tussen clouddiensten van dezelfde en andere cloudleveranciers en de transparantie daarover.
- F.** Portabiliteit tussen clouddiensten van andere cloudleveranciers. Eenvoudig in te richten en transparant
- G.** Mate van afhankelijkheid van de voor de clouddienst gebruikte technologie.

Ad a. Over dit aspect is waarschijnlijk weinig discussie nodig. Cloudleveranciers en hun diensten moeten voldoen aan Europese en nationale regelgeving.

Ad b. Als naleving van niet-Europese regelgeving vereist is, mag dat niet in strijd zijn met Europese regelgeving. Als er wel een conflict is, diskwalificeert deze leverancier of dienst zich als Europese soevereine partij. Het is wenselijk dat er een strengere eis komt, waarbij naleving van niet-Europese regelgeving geheel wordt verboden.

Ad c. Dit aspect gaat over de toegang tot en controle over de leverancier, dienst en data-verwerking. Als een niet-Europese entiteit de uiteindelijke belanghebbende (UBO) en/of beslisser is over deze elementen, diskwalificeert de leverancier of dienst zich als Europees soeverein.

Ad d. In hoeverre heeft de eigenaar van de data zelf zeggenschap over en controle op het proces van dataverwerking? Als die er in te beperkte mate (wat is dat dan precies?) is, is het proces van dataverwerking niet digitaal autonoom.

Ad e. Dataverwerking tussen verschillende cloud-diensten van dezelfde en van verschillende cloudleveranciers is mogelijk. Het is daardoor niet noodzakelijk om alle clouddiensten bij één en dezelfde leverancier af te nemen. Er is verdere discussie nodig om dit aspect beter te definiëren. Is het bijvoorbeeld vereist om een single-sign-on dienst over verschillende cloudleveranciers te laten werken?

Ad f. Het is mogelijk om een clouddienst bij de ene leverancier in te ruilen voor een soortgelijke dienst van een andere leverancier. Het is noodzakelijk om hiervoor standaardproducttypes te definiëren voor zover die (nog) niet aanwezig zijn. De leverancier moet transparant zijn over eventuele afwijkingen van de standaard en de inspanning die nodig is voor migratie naar een andere, volledig compatibele leverancier.

Ad g. De cloudleverancier moet inzicht hebben in de mate van afhankelijkheid van niet-Europese technologie. Bij sterke afhankelijkheid moet duidelijk zijn welke mitigatie- of migratiemogelijkheden er zijn als de toegang tot deze technologie wordt geblokkeerd. Daarover moet transparant worden gecommuniceerd naar (potentiële) gebruikers. Over dit aspect is een uitgebreide discussie nodig. Het gaat niet alleen om hardware (zoals chiptechnologie) maar ook om software (zoals besturingssystemen, applicaties, SDN). In hoeverre is een cloudleverancier autonoom als de ene niet-Europese technologie eenvoudig vervangen kan worden door een andere? Worden alleen eindproducten zoals compute-faciliteiten in beschouwing genomen, of omvat dit ook toegang tot grondstoffen die noodzakelijk zijn voor deze compute-faciliteiten?

3.3 Waarom een accreditatie: de gedachte erachter

Een accreditatie voor digitale autonomie biedt afnemers direct inzicht in de mate waarin de applicaties of clouddiensten die zij gebruiken voldoen aan eisen rondom controle, juridische bescherming en datalocatie. Omdat de markt sterk versnipperd is en aanbieders uiteenlopende keuzes maken in infrastructuur, eigenaarschap en wetgeving, ontbreekt voor gebruikers nu een helder referentiekader.

Met een accreditatie wordt zichtbaar hoe “autonoom” een dienst daadwerkelijk is, zodat organisaties en consumenten een bewuste keuze kunnen maken die past bij de eigen risicoanalyse en bijbehorend beleid.

Een concreet voorbeeld illustreert dit: een boekhoudpakket dat alle gegevens opslaat op infrastructuur van AWS valt onder buitenlands recht, terwijl een dienst die draait op een Nederlandse aanbieder die volledig onder de Nederlandse jurisdictie valt. Dat heeft gevolgen voor datatoegang, risico's en naleving.

Een transparant en herkenbaar keurmerk maakt deze verschillen vooraf zichtbaar, nog vóór een afnemer een contract afsluit.

3.4 Hoe verhoudt zich dit tot certificeringen en/of standaarden

Een accreditatie voor digitale autonomie staat niet los van bestaande certificeringen en internationale standaarden, maar vult deze juist aan. Certificeringen zoals ISO 27001, SOC2 of NEN-ISO 27701 richten zich primair op informatiebeveiliging, privacybeheer en proceskwaliteit. Zij zeggen echter weinig over de herkomst van de infrastructuur, het eigenaarschap van de gegevens, de toepasbare jurisdictie of de mate van afhankelijkheid van buitenlandse partijen; precies de elementen die centraal staan bij digitale autonomie.

De accreditatie fungeert daarom als een bovenliggende, domeinspecifieke indicator: het bouwt voort op bestaande standaarden, maar introduceert extra criteria die vandaag ontbreken, zoals datalocatie, eigenaarschap, jurisdictie, controlerichtlijnen, exit-mogelijkheden en governance-voorwaarden.

Waar bestaande certificeringen vooral “zijn de processen op orde?” beantwoorden, geeft deze accreditatie antwoord op de vraag: “heb ik daadwerkelijke zeggenschap en juridische bescherming over mijn digitale diensten?”

3.5 Conclusie

Een accreditatie voor digitale autonomie is noodzakelijk om eindgebruikers te helpen een verantwoorde keuze te maken in een markt die complex en ondoorzichtig is. Het biedt transparantie, vergelijkbaarheid en helderheid over risico's die nu onvoldoende zichtbaar zijn.

Als brancheorganisatie is de Dutch Cloud Community bij uitstek de partij om hierin het voortouw te nemen: door samen met leden, experts en toezichthouders een gedragen, betrouwbaar en toetsbaar instrument te ontwikkelen dat de sector vooruitbrengt en eindgebruikers beschermt.

4. Beschrijving van de componenten: de criteria

4.1 Juridische autonomie (CSP niveau)

EU & NL regelgeving

Dienstverlener voldoet aantoonbaar en uitsluitend aan Europese en Nederlandse privacy- en veiligheidswetgeving (o.a. AVG, NIS2, Data Act). Credo is dus EU / NL law only.

Toepasselijke jurisdictie

Dataopslag, -verwerking en toegang vinden uitsluitend plaats onder rechtsmacht van de EU. Geen toegang door wetgeving van derde landen.

UBO-verhouding

UBO's zijn uitsluitend natuurlijke personen met domicilie in de EU. Maximaal 24% eigendom per niet-EU entiteit; samen niet meer dan 39%.

Zeggenschap & controle

Geen enkele niet-EU partij mag feitelijke zeggenschap hebben over de dienst of onderliggende infrastructuur.

4.2 Technische autonomie (dienst niveau)

Data-interoperabiliteit

Data kan in open, gedocumenteerd formaat geëxporteerd worden, zonder lock-in.

Portabiliteit

Data en diensten zijn binnen redelijke termijn overdraagbaar naar andere EU-aanbieders, zonder onredelijke kosten of belemmeringen.

Technologische onafhankelijkheid

Bij het stoppen van technologie moet een gelijkwaardig alternatief beschikbaar zijn. Leverancier biedt exitplan.

Exit-strategie & continuity

De leverancier beschikt over een geverifieerd exitplan. Klant behoudt toegang tot data, ongeacht faillissement of overname.

Escrow-regeling (optioneel)

Software en data zijn via escrow beschikbaar voor afnemer bij discontinuïteit van dienstverlener.

4.3 Organisatorische transparantie (CSP en Dienst niveau)

Organisatiestructuur

De auditor ontvangt een overzicht waaruit blijkt wie aan wie rapporteert

Strategische besluitvorming

Met de auditor wordt gedeeld welke strategische keuzes er gemaakt zijn, waarom, welke alternatieven overwogen zijn en wat de risico's zijn, het betreft minimaal;

- de locatie(s) van de data / dienst
- de leverancier/beheerder van de data / dienst

Ketenverantwoordelijkheid

De auditor ontvangt een overzicht met het onderdeel of de onderdelen van de dienstverlening die door één externe partij ingevuld is/zijn. Er is een adequaat plan hoe deze leverancier(s), in geval van een calamiteit, binnen de door de partij zelf bepaalde continuïteits KPI's te vervangen is/zijn.

Jaarrekeningen en financiële rapportages

Worden gedeeld met de auditor, hieruit dient te blijken dat er geen redenen zijn om aan te nemen dat er acute financiële problemen zijn.



4.4 Accreditatie en volgorde in niveau van accreditatie

Het idee is dat we werken met niveaus in de accreditatie. Waarbij niveau 1 de 'basis' is en je een leverende partij digitaal autonoom kunt noemen indien met aan de juridische criteria voldoet. Deze basis is dus van toepassing op de organisatie en zegt nog niets over de producten en diensten die worden aangeboden.

Indien vastgesteld is dat een bedrijf juridisch gezien autonoom is, kan worden gekeken naar de producten en diensten van dat bedrijf. Deze volgorde is essentieel. Van digitaal autonome oplossingen kan geen sprake zijn zonder een partij die niet aan de juridische criteria voldoet.

Wanneer de producten en/of diensten in beeld komen is het raadzaam te kijken naar de technische aspecten. En het voldoen daaraan eventueel aangevuld met vereisten van transparantie voor de organisatie, zoals hieronder opgesomd kan er sprake zijn van een digitaal autonome oplossing.

Criteria, volgorde en niveau's

Juridisch	Technisch	Transparatie
Knock out of minimale criteria	Belangrijke criteria	Relevante criteria
EU & NL regelgeving	Data-interoperabiliteit	Organisatiestructuur
Toepasselijke jurisdictie	Portabiliteit	Strategische besluitvorming
UBO-verhouding	Technologische onafhankelijkheid & Exit-strategie	Ketenverantwoordelijkheid
Zeggenschap & controle	Continuity/ Escrow regeling	Jaarrekeningen en financiële rapportages

5. In de praktijk

5.1. Gebruik van de accreditatie: hoe toe te passen / een handleiding

Dutch Cloud Community stelt de criteria van het accreditatie vast en publiceert hierbij een duidelijke toelichting op de definities, beoordelingsmethodiek en toepassingsvoorwaarden. Deze informatie wordt centraal beschikbaar gemaakt via de eigen website en een speciaal daartoe opgezette thematische website. Indien gewenst organiseren wij bovendien informatiesessies en workshops voor zowel aanbieders als afnemers, zodat zij deze accreditatie juist en consequent kunnen gebruiken.

Aanbieders toetsen zichzelf aan de hand van een gestandaardiseerde self-assessment. Op basis van steekproeven of aanvullende vragen kunnen wij een onafhankelijke audit verzoeken, zodat de geclaimde mate van autonomie gecontroleerd en bevestigd kan worden.

Na succesvolle beoordeling mogen aanbieders de accreditatie gebruiken in hun communicatie, marketingmaterialen en offertes. Het keurmerk kan worden toegekend op dienstniveau of, waar relevant, op organisatieniveau. Dit stelt aanbieders in staat transparant aan te tonen hoe hun oplossingen scoren, bijvoorbeeld bij aanbestedingen, commerciële trajecten en vergelijkingsplatformen.

5.2. Adoptie van de accreditatie: hoe autonoom zijn aangeboden oplossingen in onze sector

Dutch Cloud Community stimuleert brede adoptie van de accreditatie door actief samen te werken met leden, branchepartners en andere stakeholders. Door gezamenlijk draagvlak te creëren, kan het keurmerk uitgroeien tot de sectorbrede standaard voor het beoordelen van digitale autonomie binnen de Nederlandse cloudindustrie.

Wij zullen de overheid actief adviseren om het instrument te gebruiken in aanbestedingen en in beoordelingskaders voor publieke diensten. Daarnaast worden andere sectoren aangemoedigd het keurmerk over te nemen, zodat een uniforme, herkenbare en sectoroverstijgende standaard ontstaat.

Om het accreditatie bekendheid te geven, zet Dutch Cloud Community in op gerichte PR-activiteiten: communicatiecampagnes, publicaties, inter-vIEWS en sectorbrede bijeenkomsten. Daarmee wordt niet alleen het belang van digitale autonomie onderstreept, maar ook de waarde van het instrument keurmerk als transparante en betrouwbare maatstaf.

Voor de financiering van communicatie-activiteiten en audits onderzoeken de wij diverse opties, waaronder bijdragen van leden, projectsubsidies, samenwerkingen met publieke partijen en een beperkte bijdrage van aanbieders die de accreditatie willen voeren.



6. De accreditatie en de toekomst: statisch gegeven of ontwikkelend inzicht

Digitale autonomie is geen statisch concept. Technologische mogelijkheden, dreigingsbeelden, internationale wetgeving en marktverhoudingen veranderen voortdurend. Een accreditatie die relevant en betrouwbaar wil blijven, moet daarom meebewegen met deze ontwikkelingen. Het is geen eenmalige kwalificatie, maar een levend instrument dat de sector helpt om steeds opnieuw te bepalen wat “autonoom” in de praktijk betekent.

Deze accreditatie zal zich ontwikkelen langs twee lijnen.

Ten eerste veranderen de criteria mee met de technologische realiteit. Denk aan nieuwe vormen van dataopslag, edge computing, AI-modellen die buiten de EU worden getraind, of nieuwe wet- en regelgeving die invloed heeft op datatoegang door buitenlandse partijen. De accreditatie moet aan deze ontwikkelingen tijdig worden aangepast zodat het een actueel en betrouwbaar beoordelingskader blijft.

Ten tweede ontstaat door gebruik en toetsing steeds meer inzicht in wat werkt. Naarmate aanbieders en afnemers het instrument breder toepassen, groeit

het begrip in de markt over welke eisen noodzakelijk, proportioneel of juist onvoldoende zijn. Op basis van deze praktijkervaring kan Dutch Cloud Community de accreditatie verfijnen, verdiepen of uitbreiden, bijvoorbeeld door nieuwe niveaus, extra categorieën of meer gedifferentieerde criteria toe te voegen.

Het instrument van accreditatie is daarmee een ontwikkelend inzicht: flexibel waar nodig, stabiel waar mogelijk. De kernwaarden blijven constant: transparantie, controleerbaarheid en bescherming van Nederlandse en Europese digitale autonomie, maar de operationalisatie ervan evolueert mee met de tijd.

Om deze ontwikkeling te waarborgen, zullen wij periodiek herijkingsrondes organiseren, onderbouwd door sector-feedback, technologische trends en juridische ontwikkelingen. Zo blijft het instrument niet alleen relevant, maar vormt het ook een richtinggevend kompas voor de toekomst van een autonome Nederlandse cloudsector.

Bijlage 1

Conformiteitsbeoordeling

Het proces om te beoordelen of je aan een bepaalde accreditatie voldoet heet meestal “conformiteitsbeoordeling” (ook genoemd: conformity assessment)

Daarbinnen vallen verschillende stappen, zoals:

- Self-assessment (zelfevaluatie)
- Audit (interne of externe audit)
- Certificering (als er een certificaat wordt verstrekt)
- Uiteindelijk de accreditatie zelf (als de partij die beoordeelt zelf officieel erkend moet zijn)

Voor een accreditatie wordt meestal gesproken over:

- “Toetsing aan de criteria”
- “Audit voor certificering”
- “Conformiteitsbeoordeling door een onafhankelijke instantie”



