Deventer, Olst-Wijhe en Raalte: samen staan we sterker.

Aansluitvoorwaarden 2025-2028

Auteur	:	M. Nijeboer
Collegiale toetsing	:	DOWR-ID (Architectuur; Security)
Team	:	Vakgroep Regie & Ontwikkeling
Datum	:	13 oktober 2025
Versie	:	1.1

Inhoud

Versiebeheer

Versie	Wijziging	Review door	Datum
0.9	Initiële versie	Architectuur, Security, Delivery management	9-9-2025
1.0	Ter kennisneming	Stakeholders	27-9-2025
1.1	Versie ter vaststelling	MT DOWR-ID	10-11-2025

Accordering

Akkoord gegeven door	Rol/ gremium	Datum	Opmerkingen
	MT DOWR-ID		

1 Inleiding

Het DOWR landschap is continu aan verandering onderhevig; er worden met regelmaat nieuwe oplossingsrichtingen toegevoegd en bestaande oplossingsrichtingen worden gewijzigd.

Om grip en regie te houden op het landschap zijn er kaders, richtlijnen, processen, etc. in werking om er voor te zorgen dat oplossingsrichtingen ook wenselijk zijn in het landschap. Nieuwe en gewijzigde oplossingsrichtingen worden in een vroeg stadium getoetst op basis van de aansluitvoorwaarden. De huidige vastgestelde aansluitvoorwaarden zijn verouderd, daarnaast worden er vanuit verschillende expertises soms aanvullende vragen en voorwaarden gesteld. Om vanuit een uniform toepasbaar uitgangspunt te werken is in 2025 een herijking van de aansluitvoorwaarden uitgevoerd door architectuur en security binnen DOWR-ID.

1.1 NORA 5-lagen model

De herijking is gebaseerd op het NORA 5-lagenmodel[1]. Dit model specificeert 5 invalshoeken waarop analyses ten behoeve van architectuur gebaseerd kunnen worden. Gezien de herkenbaarheid van de invalshoeken is het model zeer goed toepasbaar op de aansluitvoorwaarden.

Het model kent de volgende lagen:

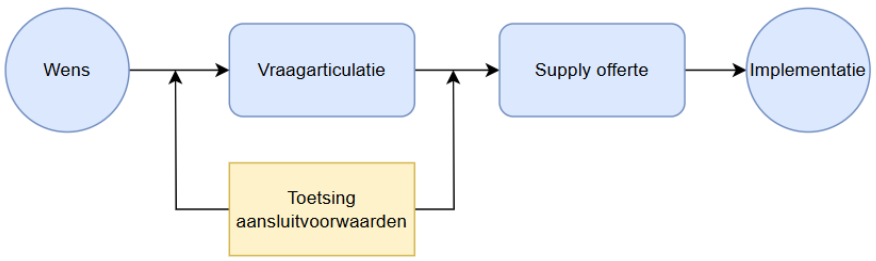
- Grondslagen – de formele afspraken die gelden
- Organisatie – de toetsing van de achterliggende organisatie (zoals bijvoorbeeld de leverancier of supportpartner)
- Informatie – de gegevens die betrekking hebben op de oplossingsrichting
- Applicatie – de automatisering van de oplossingsrichting
- IT-Infrastructuur – de onderliggende techniek (netwerk, hosting, etc.) die nodig is om de oplossingsrichting te gebruiken.

1.2 Procesbeschrijving (Supply & Demand)

Het toetsen van de aansluitvoorwaarden is een onderdeel van het Supply & Demand proces dat ingezet wordt om nieuwe oplossingsrichtingen te introduceren.

Deze aansluitvoorwaarden zijn opgesteld vanuit een security en architectuur oogpunt en hebben als doel de eerste kaders en richtlijnen af te geven ten opzichte van oplossingsrichtingen.

Het is niet mogelijk om voor elke (mogelijke) wijziging of oplossingsrichting een gedetailleerde analyse uit te voeren. De aansluitvoorwaarden bieden handvaten voor een eerste inschatting. In vervolgtrajecten is diepgaande kadering mogelijk via andere producten zoals risico analyses, technische ontwerpen, en project startarchitecturen.



Figuur 1: Toetsing aansluitvoorwaarden in het Supply & Demand proces.

In hoofdstuk 2 is uiteengezet hoe de aansluitvoorwaarden in de organisatie worden gepositioneerd en toegepast.

[1] NORA Vijflaagsmodel - NORA Online

2 Toepassing en aandachtspunten

Aangezien elke oplossingsrichting anders is qua complexiteit en context zijn de aansluitvoorwaarden bewust generiek en breed interpretabel opgesteld. De opgenomen vragen in hoofdstuk 3 t/m 6 zijn niet als checklist te gebruiken.

Dit hoofdstuk zet uiteen wie de stakeholders zijn ten aanzien van de aansluitvoorwaarden en in welke momenten tijdens het supply & demand proces er aandacht dient te zijn voor het toetsen en kaderen.

2.1 Stakeholders

Volgend aan het supply & demand proces ligt het aandachtsgebied voornamelijk binnen de afdeling data & digitalisering (D&D) en DOWR-ID.

Rol / Functie	Belang
Informatiemanagement adviseur (IMA)	Voert de vraagarticulatie uit en gebruikt daar waar nodig de toetsing van de aansluitvoorwaarden voor
Informatiemanager	Neemt kennis van de opgestelde aansluitvoorwaarden
Delivery Manager	Stelt het supply-formulier vast en is verantwoordelijk voor het opleveren van de toetsing als een product
MT DOWR-ID	Stelt de aansluitvoorwaarden vast als MT besluit
CIO	Neemt kennis van de opgestelde aansluitvoorwaarden
Security Officer	Toetst oplossingsrichtingen aan de aansluitvoorwaarden
Enterprise Architect	Neemt kennis van de opgestelde aansluitvoorwaarden
Informatie Architect	Toetst oplossingsrichtingen aan de aansluitvoorwaarden
Solution Architect	Toetst oplossingsrichtingen aan de aansluitvoorwaarden
Change manager / Project Manager	Neemt kennis van de opgestelde aansluitvoorwaarden
Functioneel / Technisch beheerder	Neemt kennis van de opgestelde aansluitvoorwaarden
Contractmanagement	Neemt kennis van de opgestelde aansluitvoorwaarden

2.2 Aanleiding tot toetsing

Een toetsing wordt in principe geïnitieerd door een informatiemanagement adviseur of een delivery manager. Zoals in hoofdstuk 1 besproken is er niet een vast startmoment te bepalen in het supply & demand[2] proces: sommige aansluitvoorwaarden zijn breed geformuleerd en kunnen een raakvlak hebben met het vaststellen van de vraag. In essentie zijn er twee momenten wanneer de aansluitvoorwaarden getoetst kunnen worden:

1. Tijdens het vaststellen van de vraagstelling
   In deze situatie initieert de IMA een toetsing van de benodigde vragen. Communicatie verloopt via de delivery manager. De architect of security officer geeft respons op de relevante onderwerpen. De respons is enigszins oppervlakkig en generiek.

[2] Het supply & demand proces is nog in ontwikkeling. De aansluitvoorwaarden zijn agnostisch opgesteld waarbij verwacht wordt dat eventuele wijzigingen in het supply & demand proces niet tot wijzigingen in de aansluitvoorwaarden gaat leiden.

2. Tijdens het vaststellen van het supply-formulier
   In deze situatie start de delivery manager een officieel verzoek tot toetsing bij architectuur en security. De betreffende architect(en) en security officer(s) bepalen welke randvoorwaarden getoetst moeten worden en koppelen deze in een beoordeling terug. De beoordeling is een product van het supply & demand proces.

Deze tweedeling is bewust gekozen om te voorkomen dat toetsing te vroeg of te laat plaatsvindt. Het is een verkwisting van resources om elk verkennend initiatief dat nog in onderzoek is volledig te toetsen, anderzijds is er een risico dat enkel toetsing ná vaststelling van de vraag niet tijdig is.

Uiteraard kunnen de voorwaarden ook op andere momenten getoetst of geraadpleegd worden[3].

2.3 Afweging van toetsing

Niet elke aansluitvoorwaarde is relevant voor een supply & demand verzoek. Schaalgrootte van de oplossingsrichting, context van de vraag, het aantal gebruikers, etc. zijn aspecten die meespelen in de mate van detaillering die nodig is voor de toetsing. Het is aan de kaderstellende functionaris (architect, security officer) om per oplossingsrichting te bepalen welke aansluitvoorwaarde onderdeel moet zijn van de toetsing en op welke wijze van detaillering deze wordt vastgelegd.

Benadrukt moet worden dat de lijst met voorwaarden die in hoofdstuk 3 t/m 7 zijn opgenomen niet limitatief is: het staat de uitvoerenden van de toetsing vrij om daar waar relevant verdiepingen aan aansluitvoorwaarden toe te voegen of niet genoemde aansluitvoorwaarden op te nemen in een toetsmoment.

Zoals benoemd vormen de aansluitvoorwaarden geen exacte checklist; het is een middel om te beoordelen of een oplossingsrichting passend is binnen het landschap. Door de resultante van de toetsing op te nemen in het supply formulier is daarmee geborgd dat bij significante (negatieve) afwijking dit als blokkerende factor in het supply formulier opgenomen wordt.

2.4 Eigenaarschap en borging

De toetsing is onderdeel van het supply & demand proces, de delivery manager is als proceseigenaar van het supply onderdeel de facto ook verantwoordelijk voor het *laten* toetsen van de aansluitvoorwaarden.

De aansluitvoorwaarden zijn inhoudelijk de verantwoordelijkheid van architectuur en security binnen DOWR-ID; dit geldt voor zowel het opstellen van de aansluitvoorwaarden als de *uitvoering van* de toetsing.

Accordering van de aansluitvoorwaarden geschiedt in het MT DOWR-ID, waarop publicatie op de intranetpagina van architectuur volgt. De vastgestelde voorwaarden worden proactief gedeeld met de stakeholders (2.1).

In principe zijn de aansluitvoorwaarden vastgelegd voor de periode 2025 – 2028; eind 2028 zal een nieuwe herijking plaatsvinden. Eventuele tussentijdse wijzigingen kunnen daar waar nodig door architectuur en security worden verwerkt.

2.5 Bredere toepassing in de organisatie

De kern van de toepasbaarheid van de aansluitvoorwaarden ligt binnen DOWR-ID waar het door security en architectuur wordt ingezet als vastgestelde kaders ten behoeve van toetsing. Door de generieke opbouw en brede scope zijn de voorwaarden echter breder inzetbaar en kunnen ze door privacy officers, information security officers, informatiemanagement adviseurs, etc. gebruikt worden als kadering.

[3] Voor aanbestedingstrajecten kunnen de aansluitvoorwaarden als basis dienen, hierbij is echter het reguliere proces ten aanzien van het opstellen van een *programma van eisen* leidend

3 Laag 1: Grondslag

De eerste laag in het NORA model is generiek van aard en daarmee lastig te vatten in aansluitvoorwaarden. Het betreft hier wet- en regelgeving, generieke kaders, raamwerken, etc. die van toepassing zijn op het gehele DOWR landschap.

Toetsing vindt voornamelijk plaats door de context van de gemeentelijke organisatie mee te geven aan de eventuele leverancier. Dit betreft naast wetgeving als AVG, Woo, Wmebv, etc. ook generieke afspraken als BIO, GIBIT, DUTO, GEMMA/NORA, etc.

Aansluitvoorwaarde	Toelichting
Toetsen van de compliancy van de oplossingsrichting (minimaal AVG, Archiefwet, WOO, Wmebv, Digitale toegankelijkheid, Wet Electronisch publiceren, aanbestedingswet en domein specifieke wetgeving)	In essentie de totaliteit van wetgevingen waar de gemeentelijke organisaties aan gebonden zijn
Gibit	
DUTO	
GEMMA/NORA	
BIO / BIO2	Normenkader dat de minimale beveiligingseisen vastlegt voor informatiebeveiliging binnen Nederlandse overheidsorganisaties. Het helpt organisaties om risico's beheersbaar te maken en doelgerichte maatregelen te nemen.
NIS-2	
Common Ground	
I-visie	
Overige interne (architectuur)visies	Hier valt te denken aan architectuurvisies of doelarchitecturen
Zero Trust	DOWR hanteert een zero trust beleid (never trust, always verify)

4 Laag 2: Organisatie

In de toetsing wordt hier de organisatie achter de oplossingsrichting bedoeld. Dat kan een leverancier zijn of een supportpartner. Het dient als generieke toetsing van de betreffende organisatie en hoe die zich verhoudt tot de gemeentelijke organisatie.

Aansluitvoorwaarde	Toelichting
Is de leverancier bekend bij DOWR?	
Zijn er in het heden of verleden andere producten afgenomen bij deze leverancier?	
Wat is de positie van de leverancier in de markt ten opzichte van de concurrentie?	
Heeft de organisatie de gemeente wereld of decentrale overheid als specifiek aandachtsgebied?	
Heeft de organisatie het groeipact Common Ground ondertekend?	
Sluiten de door de organisatie geleverde SLA tijden aan bij wens van DOWR?	
Hoe heeft de organisatie het beheer (zoals afhandeling van incidenten, helpdesk, oppakken van wijzigingenverzoeken, etc.) ingericht?	
Hoe heeft de organisatie Zero Trust toegepast op het portfolio?	
Op welke wijze stelt de organisatie DOWR in staat om audits en controles uit te voeren?	
Welke faciliteiten levert de organisatie voor een exit strategie?	
Waar bevinden de vestigingen van de organisatie zich? Betreft het vestigingen buiten de EER?	
Over welke organisatie brede certificeringen (zoals ISO27001, NEN7510) beschikt de organisatie? En zijn deze certificeringen van toepassing op de betreffende oplossingsrichting?	
Wat is de werkwijze ten aanzien van procesondersteuning (DAP, PDC, DVO, etc.)?	

5 Laag 3: Informatie

Deze laag heeft data als aandachtsgebied. De aansluitvoorwaarden leggen een focus op de opslag van data, de modellering die in de oplossingsrichting wordt toegepast, hoe datascheiding is toegepast, etc.

Onderstaande tabel geeft een overzicht van de aansluitvoorwaarden voor de informatielaag, met bijbehorende toelichtingen.

Aansluitvoorwaarde	Toelichting
Tot op welk abstractieniveau is het datamodel beschreven? Betreft het een conceptueel of technische beschrijving?	
Is de applicatie opgebouwd op basis van het logische datamodel van het GGM of is een mapping op basis van het GGM op voorhand beschikbaar?	
Hoe wordt metadata binnen de applicatie beheerd en is deze te extraheren uit de applicatie?	
Hoe wordt datascheiding tussen omgevingen toegepast (zodat bijvoorbeeld productiedata buiten productieomgevingen niet mogelijk is, etc.)?	
Op welke wijze is datascheiding tussen gemeentelijke organisaties in te richten (is bijvoorbeeld Deventer data te scheiden van Raalte data)?	
Hoe is de backup & recovery procedure ingericht (RTO/RPO) en welke delen vallen onder verantwoordelijkheid van de organisatie?	
Hoe is verticale toegang tot de data ingericht (bijvoorbeeld ten behoeve van de WOO, recht op vergetelheid, en DUTO)?	
Welke faciliteiten biedt de applicatie ten aanzien van logging en auditing?	

6 Laag 4: Applicatie

De applicatie laag behelst alles dat te maken heeft met de automatisering van de oplossingsrichting. Dit heeft betrekking op de architectuur van de software, de interfacing, connectiviteit, etc.

Aansluitvoorwaarden	Toelichting
In hoeverre is er sprake van modulaire opbouw van de applicatie?	
Op welke wijze is er scheiding van data, integratie, en functionaliteit toegepast?	
Over welke koppelvlakken beschikt de applicatie? Welke technieken kunnen er worden gebruikt (enkel StUF of ook modernere technieken als REST of GraphQL)?	Deze voorwaarde wordt aangescherpt zodra het integratieplatform is geïmplementeerd
Kan authenticatie plaatsvinden op basis van Oauth2 (OIDC/SAML)?	
Worden applicatie permissies geconfigureerd op basis van Graph API?	
Op welke wijze is e-mail verzending mogelijk? Beschikt de applicatie over een mogelijkheid om e-mail te versturen via onze eigen mailserver, of maakt zij gebruik van een eigen mailfaciliteit zoals een interne SMTP-server of externe dienst?	
Welke (landelijke) standaarden (zoals VNG standaarden, Forum standaardisatie, of overige internationale technische standaarden) worden er gevolgd?	
Is er functionele overlap met andere applicaties in het landschap?	Deze vraag is voornamelijk intern gericht
Zijn omgevingen (OTAP, etc.) logisch en fysiek van elkaar gescheiden?	
Op welke wijze wordt inloggen (SSO, MFA) ondersteund?	
Op welke wijze worden verwerkingen en toegang vastgelegd in de applicatie en zijn deze afdoende via logging inzichtelijk?	
Op welke wijze kan logging ingezien of geëxporteerd worden ten behoeve van gebruik in andere componenten binnen het landschap?	
Op welke wijze zijn gebruikersrechten in te richten zodat aspecten als 'need-to-know' en 'least privilege' toegepast kunnen worden?	
Wordt voldaan aan het n-2 principe ten opzichte van versiebeheer?	
In welke fase van lifecycle management bevindt de applicatie zich?	T.b.v. verankering in het APM proces
In hoeverre sluit de applicatie aan bij de gestelde BIO normen?	
Indien de applicatie een externe website of mailservice betreft: heeft deze een 100% score op internet.nl?	
Is er een roadmap voor de applicatie beschikbaar en tot welke toekomstdata is deze ingevuld?	
Voldoet de applicatie aan het 'SaaS, tenzij...' principe? En betreft het dan een webnative en webresponsive applicatie?	
Is het geaggregeerde risico op basis van de risico-analyse acceptabel?	
Welke faciliteiten biedt de applicatie in het kader van continuïteit (zoals back-up, recovery, fail-over)?	
Welke faciliteiten biedt de applicatie in het kader van beheer? Ondersteunt de applicatie een gestructureerd patch- en release managementproces	Hieronder vallen ook versiebeheer, testen, rollback faciliteiten, etc.
Worden er reguliere pentesten en vulnerability scans uitgevoerd op de applicatie?	

7 Laag 5: IT-Infrastructuur

Deze laag heeft de technische laag als aandachtsgebied. Onderwerpen als infrastructuur, hosting, netwerken, worden middels deze aansluitvoorwaarden getoetst.

Het betreft hier zowel de impact op de DOWR infrastructuur als die van de (toekomstige) leverancier.

Aansluitvoorwaarde	Toelichting
Waar wordt de oplossingsrichting gehost (public/private cloud, eigen datacenter)?	
Zijn er componenten van de applicatie (of die door de applicatie gebruikt worden) die buiten de EER worden gehost?	
Welke encryptie standaarden worden ondersteund?	• Minimaal SSL-certificaat SHA-256 (een bitlengte hoger dan 256 kan in overleg) • Sleutellengte dient 2048-bit te zijn
Zijn verbindingen enkel tot stand te brengen met HTTPS en ondersteunde TLS versies (1.2/1.3)?	
Welke functionaliteiten worden er geboden ten aanzien van geoblocking?	
Welke functionaliteiten worden er geboden ten aanzien van whitelisting/tunneling (in het geval van gebruik (bijzondere) persoonsgegevens)	
Hoe worden kwetsbaarheden beheerd (bijvoorbeeld middels een patchbeleid)	
In hoeverre kunnen/zijn standaard configuraties (zoals wachtwoorden, etc.) aan te passen?	
Welke maatregelen zijn er ingericht tegen DDOS aanvallen?	
Maakt de applicatie gebruik van een onderliggende infrastructuur zoals een besturingssysteem, webapplicatieplatform, containeromgeving (bijv. Kubernetes) of een andere vorm van hosting?	
Worden in het geval van meerdere diensten deze op één publiek adres aangeboden?	
Ondersteunt de applicatie een configuratie waarbij inkomend verkeer naar DOWR vanaf één IP-adres afkomstig is, zodat DOWR op dit IP-adres whitelisting kan toepassen.	
Worden verbindingen op basis van FQDN gelegd?	