de Nationale Ombudsman

Enterprise Principes

Uitgangspunten voor de informatie voorziening van de Nationale ombudsman.

Status: Definitief
Versie: 1.0

Wouter Sallé
1-5-2020

Inhoudsopgave

Revisiehistorie:

Versie	Auteur	Status	Datum	Toelichting
0.1	WS	Concept	26-03-2020	Initiële versie
0.2	WS	Concept	07-04-2020	Review commentaar Edwin Valentijn verwerkt
0.9	WS	Concept	01-05-2020	Review commentaar Dorien Sanders en Ger Slagboom verwerkt
1.0	WS	Definitief	21-05-2020	

1 Inleiding

Digitalisering is een onlosmakelijk onderdeel van het realiseren van de missie en de visie van de Nationale ombudsman. Zonder goede digitale ondersteuning is dienstverlening door de overheid en de No in het bijzonder welhaast onmogelijk.
Door een veranderende maatschappij en de veranderende eisen en mogelijkheden op digitaal gebied is verandering een constante geworden. Om goed invulling te blijven geven aan de doelstellingen van de No (missie, visie en doelstellingen) zullen processen doorlopend aangepast worden. Ook zijn taken en rollen van medewerkers aan verandering onderhavig en zullen informatiesystemen moeten worden vernieuwd.

De uitdaging is om de groeiende complexiteit van de informatievoorziening bij de No te overzien en hier grip op te houden. Inzicht en overzicht in hoe producten en diensten, processen en ondersteunende voorzieningen zich verhouden is hiervoor essentieel. Deze architectuur benadering is daarbij een belangrijk hulpmiddel.

Omdat de No een verhoudingsgewijs kleine organisatie is, is er een balans gezocht tussen een groots opgezette enterprise architectuur en geen of alleen infra- en technische architectuur. Er is voor gekozen om een architectuur dossier te maken waarin in ieder geval de volgende documenten worden opgenomen:

- Principes (en kaders en richtlijnen)
- Cloudbeleid
- Doelarchitectuur
- Aansluitvoorwaarden

Bij het schrijven van dit document is gebruik gemaakt van het *Informatiebeleid No 2020-2024 - definitief* Daarnaast is waar mogelijk gebruik gemaakt van reeds bestaande (rijksbrede) bronnen zoals de Nederlandse Overheid Referentie Architectuur (NORA) en de Enterprise Architectuur Rijk (EAR). Ook is er gekeken naar enkele reeds bestaande enterprise architecturen binnen de rijksoverheid: *IenW Enterprise Architectuur (IWEA)* en *Bedrijfsvoering_Enterprise_Architectuur_OCW_v1_0*

Kenmerkend voor dit document is dat het de volgende doelen wil borgen in de organisatie. Deze doelen komen uit het informatiebeleid.

Flexibel
Beschikbaar en betrouwbaar
Veilig
Toegesneden op de werkprocessen
Slim
Beheer- en beheersbaar
Betaalbaar

Daarnaast zijn er nog een tweetal doelen die vanuit een ICT oogpunt nagestreefd worden:
Toekomstvast

- De principes, kader en richtlijnen (PKR) alsook de overige documenten in het Architectuur dossier dragen bij aan de (door) ontwikkeling en realisatie van een wendbare en flexibele informatievoorziening
- Doelstellingen en producten worden gerealiseerd en geselecteerd op basis van de PKR
- Keuzes voor de informatievoorziening zijn onderbouwd en dragen bij aan de strategische doelstellingen van de No.

- Informatievoorziening wordt toekomstvast gemaakt. Door te kiezen voor moderne technieken kunnen toekomstige eisen, ontwikkelingen en wensen eenvoudig toegevoegd of geïmplementeerd worden.

Kwaliteit

- De informatievoorziening sluit volledig aan op de eisen, wensen en principes van de No
- De architectuur principes bieden handvatten om de professionaliteit, effectiviteit en efficiëntie van de organisatie te vergroten waardoor de kwaliteit van de informatievoorziening verbeterd wordt.

2 Principes

2.1 Bedrijf architectuur principes

In de bedrijf architectuur worden de principes met betrekking tot de organisatie, de processen en de diensten en producten beschreven.

2.1.1 Organiseer vanuit één concern gedachte

De No functioneert als één organisatie, het benutten van kennis en samenwerking organisatiebreed geeft invulling aan de meerwaarde van de omvang van onze organisatie. Om samenhang en samenwerking tussen de onderdelen van No te behouden/ verbeteren wordt gewerkt vanuit de één concerngedachte.

De gevolgen hiervan zijn:

- De onderlinge afhankelijkheid van de verschillende organisatieonderdelen neemt toe. Het belang van goede sturing, communicatie en informatievoorziening neemt daardoor eveneens toe
- Bij een oplossingsvoorstel wordt er altijd een afweging gemaakt of iets organisatiebreed kan worden geregeld of dat het specifiek voor een afdeling wordt geregeld.

Raakt de volgende doelen:

- Beheer en beheersbaar
- Betaalbaar
- Toegesneden op de werkprocessen

2.1.2 Generieke, herbruikbare en gestandaardiseerde oplossingen

De No standaardiseert waar mogelijk processen en informatievoorzieningen door generieke en herbruikbare oplossingen die organisatiebreed ingezet worden. Hierbij wordt de 'pas toe of leg uit'-standaarden van het forum standaardisatie gebruikt. Wettelijk verplichte standaarden worden in specifieke wetgeving kenbaar gemaakt[1]. Standaardisatie en generieke oplossingen verhogen mogelijkheden tot data-uitwisseling met andere overheidsorganisaties.

Interoperabiliteit op basis van standaarden bevordert de mogelijkheden tot samenwerking en het uitwisselen van gegevens en diensten tussen organisaties, afdelingen, mensen en computers.

De gevolgen hiervan zijn:

- Aanbestedingen leveren minder exotische applicaties op en daarmee minder risico op 'vendor lock in'
- Het gebruik van rijks-, open en de facto standaarden en bewezen technieken geldt voor informatie, applicaties, gegevens, -uitwisseling en techniek;

Raakt de volgende doelen:

- Betaalbaar
- Beheer- en beheersbaar
- Veilig

[1] Voorbeelden van wetgeving waarin standaarden verplicht worden gesteld: "Tijdelijk besluit digitale toegankelijkheid overheid" en "Wet gelijke behandeling op grond van handicap of chronische ziekte".

- Toegesneden op de werkprocessen
- Kwaliteit
- Toekomstvast

2.1.3 De No is transparant

De Nationale ombudsman stelt zich open en zichtbaar op; informatie is toegankelijk en in beginsel openbaar. De No hanteert daarbij het adagium ‘Open, tenzij…’. ‘Tenzij’ geldt daarbij wanneer de vertrouwelijkheid van gegevens in het geding is.

De gevolgen hiervan zijn:

- De No is eigenaar van en verantwoordelijk voor de kwaliteit van de data in het primair proces ontstaan
- Data wordt bewust vastgelegd.

Raakt de volgende doelen:

- Beschikbaar en betrouwbaar
- Kwaliteit

2.1.4 No past 'archivering by design', 'privacy by design' en 'security by design' toe bij het inrichten van processen en informatievoorziening.

Door processen en informatievoorziening in te richten volgens specifieke ontwerpprincipes en eisen worden deze robuust en toekomstvast ingericht en wordt tegelijkertijd ook rekening gehouden met geldende wet- en regelgeving. Met name de volgende wet- en regelgeving is hierbij belangrijk:

- AVG (wet)
- BIO (Rijksbreed beveiligingskader)
- Archiefwet (wet)
- WOO (wet)
- Besluit digitale toegankelijkheid overheid (AMvB)
- VIRBI Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie (voorschrift voor de rijksdienst)

De gevolgen hiervan zijn:

- Informatie voorzieningen zijn in beginsel betrouwbaar en voldoen aan wet en regelgeving.

Raakt de volgende doelen:

- Beschikbaar en betrouwbaar
- Beheer- en beheersbaar
- Veilig
- Kwaliteit

2.1.5 Daar waar we goed in zijn en waar we capaciteit voor hebben, voeren we zelf uit en daar waar het elders beter kan of we de capaciteit niet hebben, besteden we uit.

Bedrijfsvoering voert haar kerntaken uit met eigen mensen. Bepalende taken worden daarmee ook vervuld met eigen mensen. Ondersteunende taken worden ingekocht/als dienst afgenomen van een leverancier, tenzij het gunstiger is om dit bij de No zelf te doen. Hierdoor blijft de bedrijfsvoering van de No in controle op de informatievoorziening.

Dit vertaalt zich voor de bedrijfsvoering als volgt:

1. Functioneel beheer in eigen beheer, om goed aan te sluiten op de gebruikers.
2. Informatiemanagement in eigen beheer om een sterke opdrachtgever te zijn.
3. Applicatiebeheer en applicatieontwikkeling in de markt, tenzij in eigen beheer gunstiger is.
4. Technisch beheer in de markt, tenzij in eigen beheer gunstiger is.

De gevolgen hiervan zijn:

- Er wordt geïnvesteerd in de medewerkers bij bedrijfsvoering , zodat zij in staat zijn om, met de juiste kennis, deskundigheid, kwaliteit en gewenste competenties, de kerntaken van de bedrijfsvoering uit te blijven voeren.
- Door taken zelf uit te blijven voeren blijft de afdeling bedrijfsvoering in controle en wordt structureel regie gevoerd op leveranciers.
- De No is zich bewust van de werkzaamheden die niet zelf uitgevoerd worden en kan hier maatregelen op nemen.

Raakt de volgende doelen:

- Betaalbaar
- Beheer- en beheersbaar
- Flexibel
- Kwaliteit

2.1.6 Taken, verantwoordelijkheden en bevoegdheden zijn duidelijk, eenduidig vastgelegd en bekend

De NO is een krachtige organisatie waarin de klachtbehandeling (proactief en reactief) centraal staat. De organisatie wordt in haar kerntaken ondersteund door bedrijfsvoering Hierin werkt de No als één team samen. Iedereen draagt vanuit zijn eigen rol bij aan de resultaten van de NO.

De gevolgen hiervan zijn:

- Helder is hoe de rollen zijn opgebouwd in taken, verantwoordelijkheden en bevoegdheden
- Voor elk proces is een proceseigenaar, deze draagt de verantwoordelijkheid dat de processen met de daarbij behorende taken, verantwoordelijkheden en bevoegdheden helder beschreven en geïmplementeerd worden
- Elke informatie systeem heeft een systeemeigenaar. De systeemeigenaar fungeert als opdrachtgever voor de gehele levenscyclus[2] van een informatie systeem.
  De autorisaties voor dit systeem zijn herleidbaar en er wordt beheer op het systeem uitgevoerd.

Raakt de volgende doelen:

- Toegesneden op werkprocessen
- Veilig
- Beheer- en beheersbaar

[2] Onder de levenscyclus wordt verstaan: algemene aankoop, ontwikkeling, integratie, wijziging, bediening, onderhoud, uitfasering.

2.1.7 De No stelt medewerkers in staat om plaats- en tijdonafhankelijk te werken.

Bij de No is het '*nieuwe werken'* omarmd. Dit houdt in dat er minder kantoorwerkplekken zijn en er geen medewerkers een vaste werkplek hebben. Daarnaast is het mogelijk om op eenvoudige wijze plaats en tijd onafhankelijk (niet op kantoor) te werken met de middelen die de No beschikbaar stelt.

Hiermee omarmt de No de filosofie dat er meer tijd wordt besteed aan ontmoeten, netwerken, overleggen en samenwerken.

De gevolgen hiervan zijn:

- Voorzieningen en applicaties worden aangeboden vanuit een centrale omgeving. Dit zorgt voor een verhoging van de flexibiliteit en de onafhankelijkheid van de werkomgeving (thuis/kantoor/onderweg). Dit vergroot de mogelijkheden tot samenwerken omdat gegevens centraal beschikbaar zijn en ook centraal worden opgeslagen.
- Ondersteuning dient toepassingsgericht te zijn bij het middel, de omgeving of het proces. Alleen gebruikershandleidingen schieten te kort voor adoptie van moderne complexe omgevingen en systemen.

Raakt de volgende doelen:

- Toegesneden op werkprocessen
- Slim
- Beheer- en beheersbaar
- Toekomstvast
- Flexibel

2.2 Applicatie principes

De applicatie principes beschrijven wat de principes zijn achter de keuzes die gemaakt worden bij modernisering van het applicatielandschap

2.2.1 ‘Hergebruik’ gaat voor ‘kopen’, gaat voor ‘laten maken’

Standaard oplossingen en producten (COTS, commercial off the shelf) worden ingezet zoals geleverd. Producten die zonder aanpassingen gebruikt worden voldoen beter aan standaarden en kennen een marktconform kostenniveau.

De No sluit daar waar mogelijk aan op generieke rijksbrede voorzieningen. Hierdoor wordt bespaard op aanschaf-, ontwikkel- en beheerkosten. Daarnaast worden ook de interoperabiliteit en de mogelijkheden tot samenwerking vergroot. Randvoorwaardelijk is dat aansluiten op de rijksbrede voorzieningen de onafhankelijkheid van de No niet aantast.

De gevolgen hiervan zijn:

- Applicaties zijn configurabel en vereisen specialisten in de ondersteuning. Beheerders moeten daarom gedegen getraind zijn om hun taak uit te kunnen voeren
- Hergebruik geldt bij informatievoorziening ook voor gegevens en authentieke bronnen.
- De No stuurt op de inzet van c.q. aansluiting op generieke rijksbrede voorzieningen.

Raakt de volgende doelen:

- Toegesneden op werkprocessen
- Slim
- Beheer- en beheersbaar
- Toekomstvast

- Flexibel

2.2.2 De No wil een slimme volger zijn van technologische ontwikkelingen.

Dit betekent dat we niet de allernieuwste ontwikkelingen volgen, onder meer vanwege het risico van kinderziektes. In het versiebeleid is t-1 het uitgangspunt. Dat wil zeggen dat No tenminste de op een na laatste productversie gebruikt. Soms kan dat niet, als de leverancier alleen de meest actuele versie wil ondersteunen.

No wil zeker ook niet achterop raken, waardoor ondersteuning kan wegvallen. Elke component moet minimaal nog 3 jaar ondersteund worden door de leverancier.

De gevolgen hiervan zijn

- De No gebruikt moderne applicaties en heeft een doorlopende cyclus van vernieuwing.
- Beheerders en informatie managers houden bij welke versie er gebruikt wordt en tot wanneer deze ondersteund wordt in de PDC.

Raakt de volgende doelen:

- Slim
- Beheer- en beheersbaar
- Beschikbaar en betrouwbaar
- Veilig
- Toekomstvast
- Kwaliteit
- Flexibel

2.2.3 De informatievoorziening bij de No is flexibel, toekomstvast, doelmatig en veilig vormgegeven

Door veranderende wet- en regelgeving, ontwikkelingen in de techniek en samenleving en organisatorische wijzigingen is de No continue in beweging. Informatievoorziening bij de No moet deze veranderingen kunnen opvangen.

De informatie van de No wordt zowel voor in- als extern gebruik veilig, transparant, actueel en betrouwbaar ontsloten voor zover dit binnen de wettelijke kaders mogelijk is.

In de userinterfaces en de inrichting van de informatievoorziening staan de wensen, eisen en vragen van gebruikers centraal. Functionaliteiten die ontworpen zijn naar de behoefte van de gebruiker zullen meer en gemakkelijker gebruikt worden. Hierbij wordt in de opzet en vorm rekening gehouden met de vaardigheden en voorkeuren van de gebruikers.

De gevolgen hiervan zijn:

- De kosten moeten in verhouding staan met (de kwaliteit van) de geleverde diensten en producten en daarnaast marktconform zijn;
- De vereiste inspanning (kosten) voor de informatievoorziening moet in verhouding zijn met de verwachte (efficiëntie) voordelen
- Een functionaliteit moet vanuit het perspectief van de gebruiker meerwaarde hebben en geen andere functionaliteiten overlappen
- De gebruiker van de informatievoorziening staat centraal, het gebruiksgemak voorop, zonder dat dit ten koste gaat van de informatiebeveiliging.

Raakt de volgende doelen:
- Flexibel
- Beheer- en beheersbaar
- Toekomstvast
- Veilig
- Toegesneden op werkprocessen
- Kwaliteit

2.2.4 De informatievoorziening van de No is volgens standaarden ingericht.

Het gebruik van open standaarden bevordert de interoperabiliteit zoals bijvoorbeeld bij het uitwisselen van informatie. Open standaarden kunnen vrijelijk gebruikt en toegepast worden zonder door private partijen opgelegde beperkingen aan het gebruik.

Indien applicaties volgens standaarden worden ingericht biedt dit ook de mogelijkheid om met andere overheidsinstanties samen te werken. Dit levert schaalvoordeel op in de aanschaf, beheer en ondersteuning van deze applicaties. Daarnaast zorgt standaardisatie voor meer keuzemogelijkheden en hogere beschikbaarheid van expertise in de markt. Door alleen te werken volgens standaarden wordt de (technologische) diversiteit en complexiteit beperkt en blijft deze beheersbaar.

Het gevolg hiervan is:
- Het gebruik van rijks-, open en de facto standaarden en bewezen technieken geldt voor informatie, applicaties, gegevens, -uitwisseling en techniek.
- Applicatie(componenten) zijn eenvoudig te vervangen en te upgraden.

Raakt de volgende doelen:
- Toegesneden op werkprocessen
- Beschikbaar en betrouwbaar
- Beheer- en beheersbaar
- Veilig
- Toekomstvast
- Betaalbaar

2.3 Beveiligingsprincipes:

Beveiligingsprincipes zorgen voor handvatten bij het selecteren en implementeren van (nieuwe) applicaties. Ook wordt de onderlinge samenhang tussen applicaties en omgevingen bewaakt omdat deze volgens de zelfde principes opgezet zijn. Het toepassen van de principes zorgt niet alleen voor een beter beveiligde omgeving, maar ook voor bewustwording en eenduidigheid in het gebruik van applicaties.

2.3.1 Beveiliging op basis van risico afweging

De eisen voor beschikbaarheid, integriteit en vertrouwelijkheid zijn afgeleid van een expliciete risicoafweging in de keten. Het besluit Voorschrift Informatiebeveiliging Rijksdienst stelt dat het lijnmanagement op basis van een expliciete risicoafweging de betrouwbaarheidseisen voor zijn informatiesystemen vaststelt. Het gaat om eisen aan de beschikbaarheid, de integriteit en vertrouwelijkheid van de informatie.

De No kan het besluit Voorschrift Informatiebeveiliging Rijksdienst naast zich neerleggen omdat de No geen rijksdienst is, echter is het raadzaam om dit voorschrift te volgen omdat het een breed geaccepteerd besluit over een methodiek van beveiligen beschrijft. Op basis hiervan is het logisch om ook de BIR/BIO te omarmen (wat al gedaan wordt)

Een belangrijke aanvulling hierop is dat voor elk informatiesysteem moet worden vastgesteld of het basis beveiligingsniveau de risico's voor de vereiste beschikbaarheid, integriteit en vertrouwelijkheid voldoende afdekt, of dat aanvullende maatregelen nodig zijn om de risico's nog verder te beperken. Het lijnmanagement moet te allen tijde op de hoogte zijn van de geaccepteerde restrisico's.

De gevolgen hiervan zijn:
- De informatievoorziening van de No is BIO getoetst en voldoet aan de eisen van de BIO conform het 'pas toe of leg uit' principe;
- Niet de aanbieder, maar de No als afnemer van een voorziening voert (of laat uitvoeren) een risicoanalyse uit en bepaalt op basis daarvan welke passende maatregelen er genomen kunnen en moeten worden en weegt de restrisico's af. Dit gebeurt uiteraard met inachtneming van de aspecten beschikbaarheid, integriteit en vertrouwelijkheid.

Raakt de volgende doelen:
- Veilig
- Slim
- Beheer- en beheersbaar
- Betaalbaar
- Beschikbaar en betrouwbaar

2.3.2 Beveiliging is laagdrempelig

Veilig werken in de informatie voorziening moet gebruiksvriendelijk en eenvoudig zijn, anders worden beveiligingsmaatregelen omzeild.

Beveiligingsmaatregelen worden zowel vanuit een technisch als een gebruikersoogpunt benaderd. Met slimme technische voorzieningen kan veiligheid geboden worden zonder dat de gebruiker het merkt of er hinder van ervaart. Omdat gedrag van de gebruiker dé bepalende factor is voor een goede beveiliging moeten de technische middelen de gebruiker helpen en stimuleren in het zo veilig mogelijk werken.

We willen voorkomen dat eindgebruikers op zoek gaan naar mogelijkheden om de beveiligingsmaatregelen te omzeilen waarmee grotere beveiligingsrisico's geïntroduceerd worden. Denk hierbij aan het hypothetische voorbeeld van persoonsgegevens op een memorystick omdat de kantoor automatisering niet voldoet en de medewerker vol goede bedoelingen thuis op eigen ICT middelen aan de slag gaat.

De gevolgen hiervan zijn:
- Implementaties om veilig te kunnen werken moeten eenvoudig zijn in gebruik
- Het aantal authenticatiemiddelen moet tot een minimum beperkt worden, Single Sign On heeft de voorkeur.
- Menselijk handelen is een bewezen risico en daarmee ook een factor bij het omgaan met (digitale) informatie. Er wordt van medewerkers verwacht dat zij zich verantwoordelijk voelen voor de informatie die zij gebruiken. Om dit te borgen dient het bewustzijn op peil gebracht en gehouden te worden. Het gaat hierbij niet alleen om het brengen van informatie (bewustwordingstrainingen of aandacht van het management) maar ook door

eigen initiatief aan te wakkeren en het gezond verstand van de medewerkers aan te spreken.
- Bewustzijn omtrent informatiebeveiliging dient een constante te zijn. Hierbij is extra awareness nodig bij het IDU (instroom doorstroom en uitstroom) proces van medewerkers. Dit proces is bepalend voor het al dan niet mogen raadplegen van vertrouwelijke informatie.
- Beveiligingsmaatregelen voor een applicatie (op een apparaat) mogen geen nadelige gevolgen hebben voor de werking van andere applicaties of functionaliteiten op het apparaat.

Raakt de volgende doelen:
- Veilig
- Slim
- Beheer- en beheersbaar
- Beschikbaar en betrouwbaar

2.3.3 Beheer en beveiliging is integraal opgenomen in het ontwerp van voorzieningen

Beveiliging is een lijnverantwoordelijkheid en vormt een onderdeel van de kwaliteitszorg voor bedrijfs- en bestuursprocessen en de ondersteunende informatiesystemen.

Als gevolg van de stijgende doordringingsgraad van ICT in de processen van de No, is de organisatie in de loop der jaren steeds kwetsbaarder geworden voor verstoringen van en inbreuk op de informatievoorziening.

Vanwege het toenemende belang van beveiliging, de belangrijke rol van de beheerder tijdens de exploitatie en om problemen achteraf te voorkomen, is het zaak dat beheer- en beveiligingsaspecten in een zo vroeg mogelijk stadium geïncorporeerd worden in de ((door)ontwikkeling van) de informatievoorziening.

De gevolgen hiervan zijn:
- De proceseigenaar is eindverantwoordelijk voor de beveiligingsmaatregelen en contingency planning. Dit geldt zowel voor de processen als voor de ondersteunende informatiesystemen. De proceseigenaar bepaalt dus welk rest-risico hij bereid is te aanvaarden;
- Er moet een balans zijn tussen de risico’s en de te brengen offers om die risico's te beperken. Dit impliceert dat er bij het ontwerp van processen en systemen een risicoanalyse moet plaatsvinden;
- De beoogde beheerder van het informatiesysteem wordt vanaf de start betrokken bij de ontwikkeling ervan.

Raakt de volgende doelen:
- Veilig
- Kwaliteit
- Toekomstvast
- Beheer- en beheersbaar
- Beschikbaar en betrouwbaar

2.3.4 Wijzigingen aan de informatievoorziening vinden releasematig en gestructureerd plaats

Nieuwe (versies van) informatiesystemen wordt beheerst in productie genomen en wijzigingen worden op een gecontroleerde wijze doorgevoerd. Het proces rondom het testen en accepteren van (wijzigingen op) informatiesystemen vindt releasematig en volgens een gestructureerde aanpak of methodiek plaats.
Deze gestructureerde aanpak of methodiek zorgt voor:

- Een goede organisatorische inbedding;
- Inzet van de juiste hulpmiddelen en digitale infrastructuur;
- Bruikbare technieken voor de testactiviteiten;
- Minder risico op verstoring als gevolg van wijzigingen

De gevolgen hiervan zijn:

- Het releasematig aanbrengen van wijzigingen kan leiden tot een langere doorlooptijd van het implementatietraject. De traditionele beheerprocessen sluiten heden ten dage steeds slechter aan bij (de snelheid van) agile ontwikkelprocessen. Dit vraagt om een aanpassing en toepassing van technieken zoals als automatisch deployment (uitrol) en testen;
- De gestructureerde aanpak of methodiek vraagt om een onderlinge afstemming tussen de diverse beheerpartijen en belanghebbenden.

Raakt de volgende doelen:

- Veilig
- Slim
- Beheer- en beheersbaar
- Kwaliteit
- Beschikbaar en betrouwbaar