PBLQ

BEVINDINGEN GESPREKSRONDE MONITOR 2022

29 november 2022

Inleiding en onderzoeksvragen

Als vervolg op het voorzieningenonderzoek voor de Monitor 2022 zijn een aantal verdiepende gesprekken met voorzieningen en andere partijen gevoerd. De door ons gesproken partijen zijn in de rechter kolom opgesomd. Tijdens de gesprekken hebben drie onderwerpen en bijbehorende onderzoeksvragen centraal gestaan:

1. **Succesfactoren voor compliancy aan de standaarden van de pas-toe-of-leg-uit-lijst**
   - Op welke wijze wordt de hoge compliancy aan de PTOLU-lijst bereikt en geborgd?
   - Welke lessen zijn hieruit te trekken op het gebied van organisatie, processen, techniek en bemensing?
2. **Manier van doorwerking van bestuurlijke afspraken in het OBDO voor standaardisatie**
   - Hoe wordt invulling gegeven aan de afspraken in het OBDO? Hoe werken deze door?
3. **Borging van standaarden bij grote vervangingsoperaties van voorzieningen**
   - Hoe zorg je voor de borging van open standaarden bij volledige vervanging binnen je life cycle management?
   - Welke rol spelen de CIO en de architect daarbij?

Op de volgende pagina wordt op hoofdlijnen antwoord gegeven op deze vragen. De slides hierna geven een nadere toelichting en duiding bij de hoofdbevindingen.

Gesproken partijen
Kadaster
KOOP
DigiInkoop
Logius
Ministerie van BZK, afvaardiging van CIO-Rijk en de directie DS

De bevindingen uit deze interviewronde zeggen wat over de partijen die geïnterviewd zijn, maar zijn niet zomaar door te trekken naar andere partijen. Daarvoor is met een te beperkte groep aan mensen gesproken.

Hoofdbevindingen

Succesfactoren

Standaardisatie zit in het DNA van de partijen die we spraken. Geïnterviewden geven aan dat het gebruik van standaarden bij hen gedegen is belegd in de processen, rollen en verantwoordelijkheden. Daarnaast zijn er enkele losse succesfactoren aan te wijzen:

- Kennis van en ervaring met (het belang van) standaarden bij individuele medewerkers
- Beschikking over voldoende middelen (financieel en deskundige personeelsinzet)
- Aandacht voor standaardisatie bij het management en prioriteit bij de externe opdrachtgever

Doorwerking van OBDO-besluiten

Voor de geïnterviewde partijen is het OBDO een van de verschillende manieren waarop de aandacht voor open standaarden kan groeien. Het voordeel van het OBDO is dat besluiten bestuurlijk legitimiteit krijgen. Het OBDO is een bestuurlijk gremium en de lijnen vanuit het OBDO naar de beheerorganisaties en voorzieningen lijken betrekkelijk lang en het is voor geïnterviewden niet altijd duidelijk hoe ze lopen. Uit de interviews blijkt dat men op de werkvloer niet op de hoogte is van wat in het OBDO is besproken. Dat wil niet zeggen dat de invulling van de besluiten hen niet bereikt. Dat gebeurt normaliter wel via de CIO, CISO, beleidsopdrachtgever of via de relevante kaders voor de voorziening.

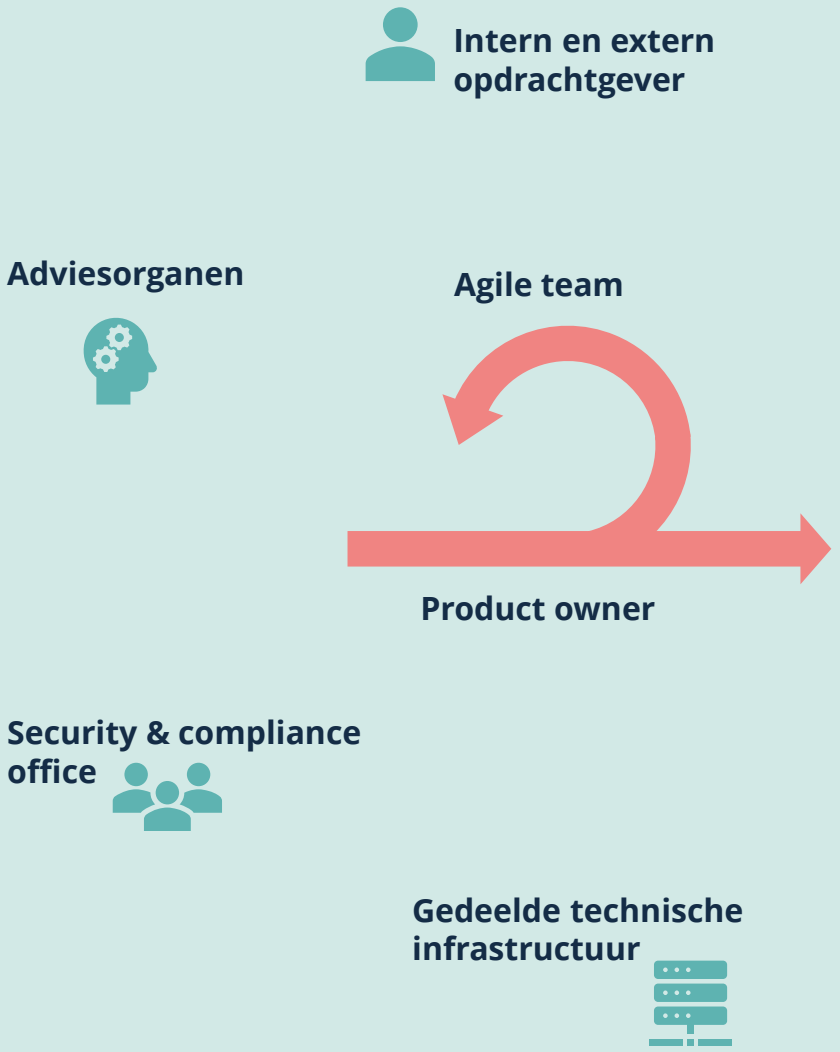
Borging bij vervangingsoperaties

Er is met twee voorzieningen gesproken die recentelijk gedeeltelijk of volledig zijn vervangen. Aandacht en prioriteit voor open standaarden wordt hierbij beschouwd als going concern en de vereiste standaarden zijn opgenomen in de kaders die ook bij vervanging gehanteerd worden. Er wordt dan ook geen gevaar onderkend dat standaarden uit het oog worden verloren. De vervangingsoperatie wordt als kans gezien om standaardisatie vanaf de start goed in te richten. Voor een standaard als digitoegankelijk kan dat eenvoudiger zijn dan het later aanpassen van de voorziening.

Succesfactoren: organisatie en processen

Bij ieder van de gesproken beheerorganisaties van voorzieningen wordt min of meer conform eenzelfde organisatiemodel gewerkt. Bij alle voorzieningen is aandacht voor standaarden bij verschillende rollen belegd en aanwezig. Centraal hierin staat de **product owner**. Deze persoon is *end-to-end* verantwoordelijk voor het realiseren van functionele en niet-functionele eisen van de voorziening. De product owner wordt gesteund en ontzorgd door een aanverwant netwerk aan stakeholders. Bij elke van de stakeholders is in deze gevallen aandacht voor het gebruik van standaarden.

- Intern en extern opdrachtgever: zorgt voor middelen en prioriteiten
- Agile team: zorgt voor gebruik, implementatie en beheer van standaarden
- Security & compliance office: faciliteert het kwaliteitskader waarbinnen standaarden moeten worden geïmplementeerd en informeert de product owner bij nieuwe (externe) ontwikkelingen
- Gedeelde technische infrastructuur: implementeert en beheert standaarden voor de hele organisatie op de technische laag zoals TLS, IPv6 en RPKI
- Adviesorganen: zijn sparringpartner voor de juiste toepassing van standaarden of de afweging welke standaarden moeten worden gebruikt. Bijvoorbeeld een architectuurboard of bij Logius het Centrum voor Standaarden



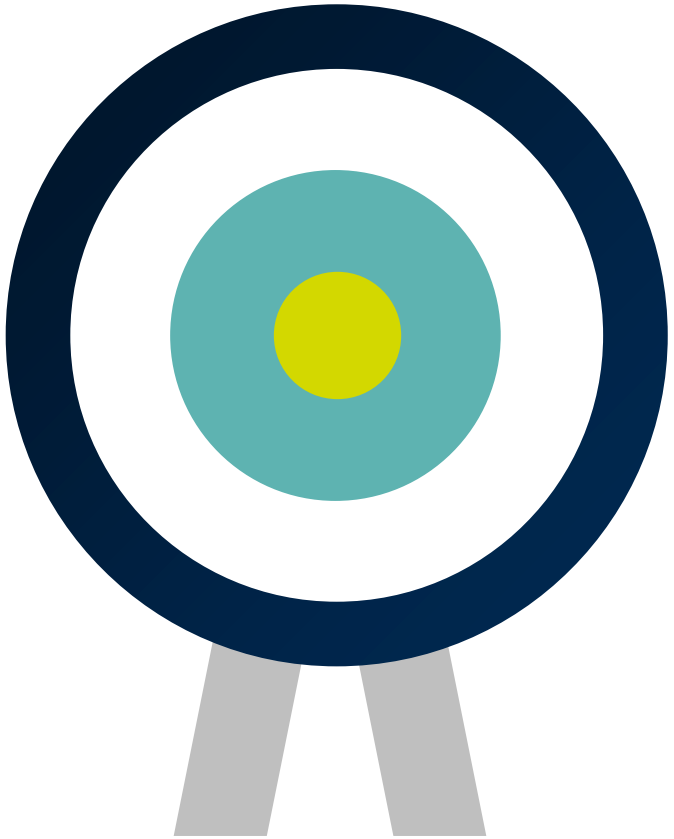
PBLQ

Succesfactoren: aansturing en bemensing

Aansturing en Opdrachtgeverschap

Het opdrachtgeverschap voor standaardisatie kent meestal een interne aansturingslijn via de CIO of CISO van de organisatie. Daarnaast bestaat er een externe aansturingslijn via het verantwoordelijke beleidsdepartement.

- Over het algemeen is het de beleving van de gesprekspartners dat er een groeiende interesse en betrokkenheid van de beleidsopdrachtgevers bij het onderwerp standaardisatie is.
- Geïnterviewden geven aan dat die betrokkenheid momenteel het meest herkenbaar is bij standaarden die dicht bij de beleidsdoelen van de opdrachtgever liggen. Een voorbeeld is de standaard digitoegankelijkheid. De afgelopen jaren is de aandacht voor inclusieve dienstverlening toegenomen en dit vertaalt zich in meer interesse vanuit de opdrachtgever voor de standaard. Daartegenover staat dat er verminderde interesse is voor de wijze waarop wordt voldaan aan de meer technische standaarden. Dat kan te maken hebben met de aanname dat dit geborgd via de lijnen van de CIO- en CISO-offices. Uit de Monitor blijkt bovendien dat de compliancy aan dit soort standaarden steeds hoger ligt.
- Het niet tijdig of volledig kunnen implementeren van standaarden door de teams wordt met de opdrachtgever overlegd. Dit verloopt op een constructieve en realistische manier, is de ervaring.



Bemensing en Deskundigheid

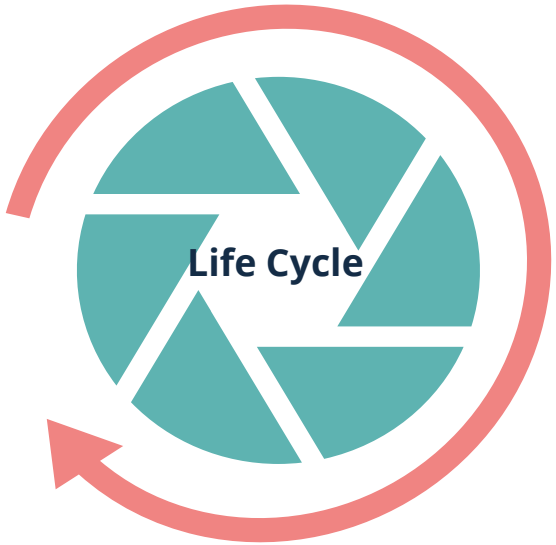
Daarnaast wijzen geïnterviewden bemensing en (personele) deskundigheid aan als belangrijke succesfactor. Alle goede organisatie- en governance-maatregelen ten spijt, standaardisatie vraagt om een specifieke deskundigheid die professionals bij zich dragen of niet. Het vergt doorzettingsvermogen en oprechte interesse om in bijzondere gevallen precies te snappen waarom een standaard wel of niet goed geïmplementeerd is. In andere woorden: standaardisatie vereist deskundige en toegewijde medewerkers die ook ruimte krijgen om zich in het onderwerp te verdiepen.

Invulling en doorwerking van OBDO-besluiten

Een van de vragen die centraal stond in deze interviewronde gaat over de invulling en doorwerking van de besluiten van het OBDO. In dit onderzoek hebben we geprobeerd daar een beeld van te krijgen door te spreken met afgevaardigden op CIO-niveau van de beheerorganisaties en met mensen bij BZK rondom het OBDO. Daarbij hebben op verzoek van de opdrachtgever gekeken naar de doorwerking van de OBDO-besluiten over standaardisatie van april 2022. Concreet gaat het over de besluiten (1) om de sturing op de toepassing van standaarden via de CIO's en opdrachtgevers te versterken en (2) verantwoording over niet toegepaste standaarden in het jaarverslag af te leggen. Dit levert de volgende bevindingen op:

- De meeste product owners van de voorziening geven aan niet bekend te zijn met het OBDO of met de besluiten van het OBDO. Ook wisten ze niet hoe ze achter de besluiten van het OBDO zouden moeten komen, via welke route ze tot hen zouden moeten komen (voor zover wij hebben kunnen achterhalen worden de besluiten van het OBDO niet openbaar gepubliceerd).
- Dat wil niet zeggen dat de invulling van de besluiten hen niet bereikt. Hun eigen verwachting is dat de besluiten via de CIO, CISO, beleidsopdrachtgever of via de relevante kaders (BIO of kaders vanuit NCSC) uiteindelijk ook de kaders van de voorzieningen bereiken.
- Ook de medewerkers van CIO-offices en CISO's van de voorzieningen die we spraken geven aan in hun dagelijkse praktijk niet met het ODBO te maken te hebben. Hun inschatting is dat het OBDO zich niet intensief bezighoudt met de meer tactisch en operationeel gerichte onderwerpen waar de CIO-offices verantwoordelijk voor zijn.
- Wel geven CIO-medewerkers aan zich te herkennen in de OBDO-besluiten. Zij beschouwen het als een reguliere taak om open standaarden vanuit hun rol aan te moedigen en daarop richting voorzieningen op te sturen.
- Geen van de gesproken partijen is bekend met het besluit om in het jaarverslag verantwoording af te leggen over het (niet)gebruik van standaarden. Een overall scan van de jaarverslagen van afgelopen jaren leert bovendien dat standaarden hierin niet (structureel) worden benoemd.
- Uit het gesprek met de secretaris van het OBDO kwam naar voren dat het vaak zoeken is naar de juiste route om opvolging te geven aan de besluiten van het ODBO. Daarnaast kent het ODBO een zeer volle agenda waardoor het soms lang kan duren voordat specifieke onderwerpen opvolging krijgen.

Vervangingstrajecten en aandacht voor standaardisatie



De gesprokken voorzieningen gaven in de interviews aan dat ze de vervanging van (onderdelen van) de voorziening niet als uitdaging maar juist als kans zagen.

Toepassing van de bestaande kaders

Voor de keuze en toepassing van standaarden worden door voorzieningen uiteenlopende bronnen, kaders en richtlijnen gebruikt. De pas-toe-of-leg-uit-lijst maakt daar deel van uit, maar is meestal niet het vertrekpunt. De lijst bevat overlap met andere (vaak uitgebreidere) kaders, vooral als het gaat om de informatiebeveiligingsstandaarden. Voorbeelden hiervan zijn de ICT-beveiligingsrichtlijnen voor webapplicaties van het NCSC en de Baseline Informatiebeveiliging Overheid. Daarnaast worden ook internationale ontwikkelingen gevolgd en gekeken naar overige eisen vanuit wet- en regelgeving. Al deze bronnen worden gebruikt om eigen kaders voor ontwikkeling en beheer op te stellen en meegenomen in een projectstartarchitectuur of programma van eisen waarin de eisen concreet gemaakt worden voor vervangingstrajecten.

Vervanging kan wel kansen bieden

Soms is het makkelijker om een standaard bij het vervangen of opnieuw opbouwen van een voorziening te implementeren dan bij het beheer van een bestaande voorziening. Een concreet genoemd voorbeeld is de standaard Digitoegankelijk. Om helemaal aan deze standaard te voldoen is het in sommige gevallen eenvoudiger om van scratch af aan dit mee te nemen dan om in bestaande systemen aanpassingen te doen.

De architect heeft een belangrijke borgingsrol bij vervangingstrajecten. Keuzes over het gebruik van standaarden worden in de startfase van een project gemaakt en opgeschreven in.

Inspelen op toekomstige ontwikkelingen

Voorzieningen willen graag inspelen op toekomstige ontwikkelingen, ook in de keuze van (duurzame) standaarden. De huidige (statische) kaders bevatten echter soms standaarden die slecht met elkaar verenigbaar zijn of niet langer volledig in de tijdgeest passen. Voorbeelden die gegeven werden zijn de keuze tussen het gebruik van Digikoppeling en de Diginetwerk-standaard ten opzichte van meer moderne REST API's-benadering.