Duiding en Maatregelen Monitor Open Standaarden 2023

Vergadering:	Forum Standaardisatie 13 december 2023
Agendapunt:	4A
Documentnummer:	FS-20231213.4A
Aan:	OBDO via Forum Standaardisatie
Van:	Bureau Forum Standaardisatie via Stuurgroep lijsten & adoptie
Bijlagen:	Geen

Deze concept notitie is een oplegger bij de Monitor Open Standaarden 2023, waarin de resultaten uit de monitor worden geduid, en verbetermaatregelen worden voorgesteld gericht aan het OBDO.

Na bespreking in het Forum gaat de Monitor Open Standaarden 2023, inclusief deze Duiding & Maatregelen notitie, onderweg naar het (1e of 2e) OBDO van 2024. Na behandeling in het OBDO stuurt BZK de Monitor naar de Tweede Kamer.

In de vergadering van het Forum Standaardisatie van 27 september 2023 presenteerde Siwert de Groot van ICTU een *sneak-preview* van de resultaten.

Duiding

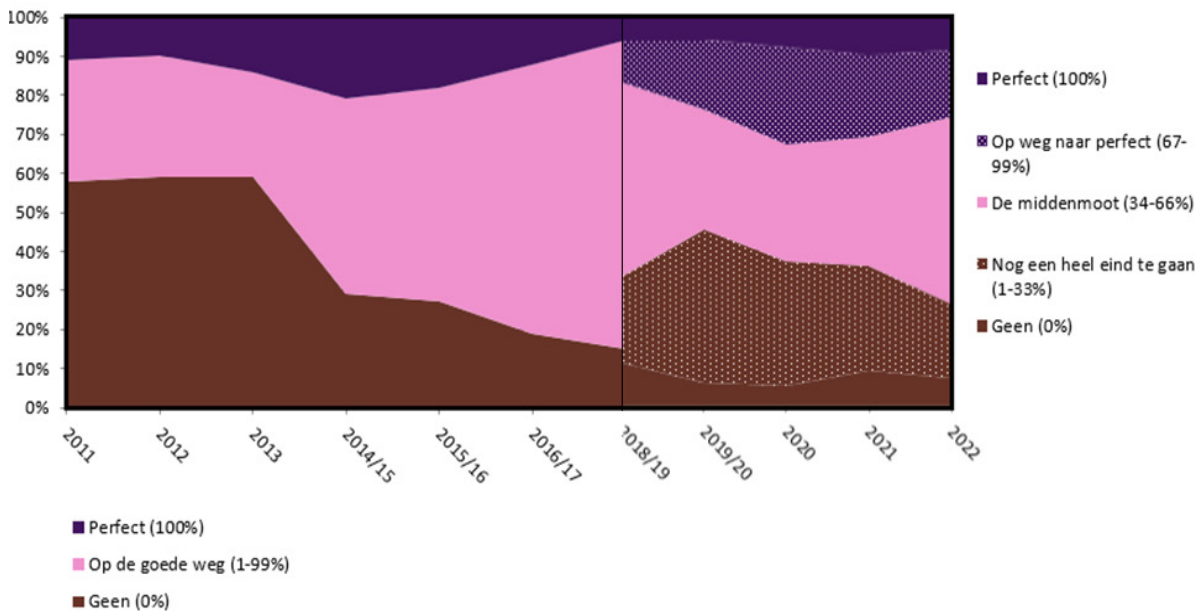
In de Monitor Open Standaarden staat ieder jaar de vraag centraal hoe het staat met het gebruik in de praktijk van de open de standaarden die op de 'pas toe of leg uit'-lijst staan van het Forum Standaardisatie.

In 2023 richtte het onderzoek zich vooral rond het moment van aanschaf van ICT. Dat is ten eerste onderzocht door te kijken naar hoe de relevante open standaarden gevraagd worden in 69 openbare aanbestedingen (pas toe) en door te onderzoeken of bij nalaten hiervan goed uitgelegd wordt (let uit). Vervolgens door nader in gesprek te gaan naar aanleiding van zes van deze aanbestedingen. Nieuw in 2023 is dat PBLQ verdiepend onderzoek heeft uitgevoerd

naar aanleiding van tien aanbestedingen die al in 2022 waren onderzocht, maar waarvan het de vraag was hoe het hiermee verder is gegaan in de fase van implementatie en in beheer name. Wat is er gebeurd ná de levering als het gaat om open standaarden?

Daarnaast is in 2023 een begin gemaakt met het thema 'cloud'. Want nu het aantal cloudoplossingen toeneemt bij publieke organisaties rijst daarbij de vraag hoe het gesteld is met de aandacht voor leveranciersonafhankelijkheid, digitale soevereiniteit, interoperabiliteit, veiligheid en dataportabiliteit. Met andere woorden, de waarden achter het belang van de toepassing van open standaarden.

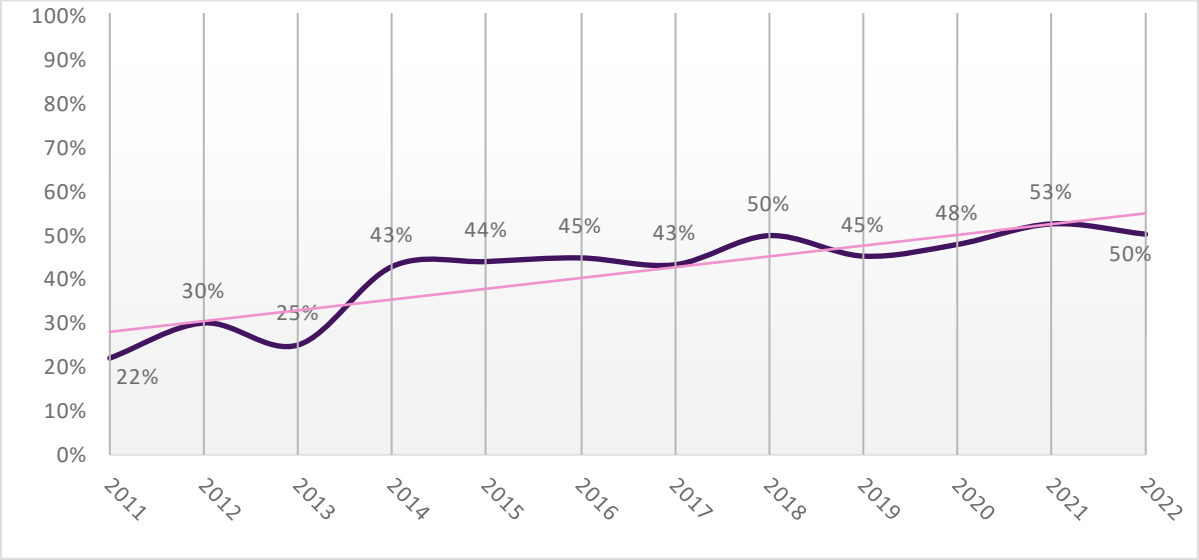
In 2023 is de toepassing van de standaarden in overheidsbrede voorzieningen van de GDI bewust een keer overgeslagen ten behoeve van de verdieping rond het moment van aanschaf van ICT. Grosso modo zijn de resultaten uit de monitor op het gebied van aanbestedingen niet veel anders dan in voorgaande jaren, al is wel een lichte opwaartse trend te zien in het gebruik. De twee figuren in de pagina's hierna laten dit goed zien.



De vraag om de relevante open standaarden in aanbestedingen blijft gemiddeld rond de 50% schommelen. Onderdeel daarvan zijn de informatieveiligheidstandaarden (die vaak relevant zijn in een aanbestede ICT-dienst of product). Dat is te weinig, gelet op de veiligheidsrisico's (phishing, ceo-fraude, ransomware, fake-news), en gelet op wettelijke verplichting die geldt sinds 1 juli 2023. Dit beeld wordt bevestigd door de meest recente meting van deze IV-standaarden met peildatum 1 juli 2023 Meting Informatieveiligheidstandaarden | Forum Standaardisatie [wordt toegevoegd zodra definitief] waarnaar in ook in deze monitor van 2023 wordt verwezen.

Verder blijkt uit het kwalitatieve deel van het onderzoek (de gesprekken gevoerd door ICTU en PBLQ) dat de aanbesteding weliswaar professionaliseert, maar na de gunning de aandacht voor open standaarden verflauwt. Tijdens de implementatie en in beheer name wordt er vaak niet structureel gecontroleerd of de gevraagde standaarden daadwerkelijk geleverd worden.

Samenvattend: met de adoptie van open standaarden lijkt het de goede kant op te gaan, maar het gaat heel langzaam. Zo worden de beleidsdoelstelling van 100% pas in 2046 gehaald.



Verder laat het onderzoek zien dat – net als in 2022 - open standaarden meer aandacht krijgen in departementale jaarverslagen. Daarin wordt weliswaar niet specifiek uitgelegd als er niet is toegepast, maar er is wel in algemene zin aandacht besteed aan het 'pas toe of leg uit'-beleid. Dat is mogelijk te danken aan de aangepaste specifiekere formulering in de Rijksbegrotingsvoorschriften.

En ook in 2023 zijn er weer organisaties die het heel goed doen. Zes van de negenzestig aanbestedingen scoorden perfect. Alle relevante standaarden werden uitgevraagd. Het lijkt erop dat organisaties die in het algemeen hun informatievoorziening en ICT-huishouding in orde hebben, ook goed scoren op de toepassing van open standaarden. Die zullen later als goede voorbeelden op de website van het Forum Standaardisatie gepubliceerd worden bij de uitstekende aanbestedingen.

En niet te vergeten, ook de overheidsbrede voorzieningen die in 2022 voor het laatst zijn onderzocht, lieten een positief beeld zien als het gaat over het toepasen van open standaarden. Zijn de relevante standaarden nog niet toegepast, dan staat dit wel gepland: comply, explain *and commit.*

Maatregelen

1. Het Forum Standaardisatie adviseert het OBDO de volgende maatregelen te nemen en hierbij prioriteit te geven aan het inlopen van de achterstand bij de (sinds 1 juli 2023) wettelijk verplichte informatieveiligheidstandaarden (https/hsts), gevolgd door de informatieveiligheidstandaarden waarvoor in het OBDO streefbeeldafspraken zijn gemaakt. Het voorstel aan het OBDO is om deze adviezen over te nemen:
   Neem in de plannen van aanpak die daarvoor worden ontwikkeld deadlines op, waarna websites bij non-compliance worden uitgeschakeld (deze aanpak leverde zeer goede resultaten op). Stel op 'koepel' en rijksniveau een programmamanager van formaat aan, die de voortgang in de gaten houdt en aanjaagt.

   NB: Deze maatregel is in lijn met de afspraak die gemaakt is op 1 december 2022 naar aanleiding van de bespreking van de IV-meting van voorjaar 2022. Toen is in het OBDO al afgesproken dat CIO-Rijk (trekker) in samenwerking met VNG, Manifestgroep en BZK/Digitale Overheid een ('licht') plan van aanpak zal opstellen, waarmee collectief door het OBDO op adoptie bij achterblijvers kan worden gestuurd.

2. Verweef de aandacht voor open standaarden in reeds bestaande kaders.
   De aandacht voor verplichte open standaarden structureel moet structureel in bestaande kaders verweven zijn en het onderwerp belegd bij de functies van CIO, CISO en CTO.
   a. Kaders rond i-Control & ICT-kwaliteitsaspecten (CIO's)
   b. Informatiebeveiliging (BIO) en bedrijfsvoering (CISO's)
   c. Aanschaf en inkoop (gebruik de Beslisboom Open Standaarden)
   d. Architectuurkaders (zoals NORA, en Enterprise Architectuur Rijk)

   Ad. a. CIO-overleggen
   Agendeer de (wettelijke) verplichtingen en metingen ook in de CIO-overleggen tussen (moeder)departementen en uitvoeringsorganisaties/zbo's. Sommige organisaties geven aan nog niet (eerder) het belang op hun achterstanden te zijn gewezen.

   Ad. b: BIO.
   Zorg dat de informatieveiligheidstandaarden waarvoor een wettelijke verplichting, een streefbeeldafspraak of een 'pas toe of leg uit' verplichting geldt, in de nieuwe versie van de BIO worden verweven (of dat ernaar verwezen wordt). Zodat de verhouding tussen deze normenkaders duidelijk is, structurele aandacht voor adoptie wordt georganiseerd (*planning & control* cyclus BIO), en stapeling van kaders en audits kan worden voorkomen.

   Maak daarnaast expliciet dat websites, e-mail adressen en internetdomeinen onderdeel uitmaken van de bedrijfsmiddelen, waarvan de BIO voorschrijft dat ze geïnventariseerd moeten zijn. Dat helpt het website & internetdomein portfolio overzichtelijk te krijgen.

Het implementatie werk van de standaarden en digitoegankelijkheid behapbaar te maken. En voor burgers en bedrijven om door het bos de bomen beter te kunnen zien.

3. Laat aan beleidszijde uitwerken op welke wijze naleving, handhaving en/of toezicht op respectievelijk wettelijke verplichte standaarden, de streefbeeldafspraken en 'pas toe of leg uit' beter kan plaatsvinden. Betrek daarbij de audit-dienst(en). Geef daarbij speciale aandacht aan overheidsorganisaties die zich niet door OBDO besluitvorming gebonden achten.