Vragen om open standaarden bij ICT inkoop

Een handreiking voor opdrachtgevers en inkoopadviseurs

Datum 2 december 2020
Status Concept versie 1.14 voor de vergadering van het Forum Standaardisatie op 9 december 2020

Colofon

Projectnaam	Handreiking vragen om open standaarden
Auteurs versie 1 2016	drs. R.M.A. (Wob) Rombouts mr. drs. B. (Bart) Knubben (Bureau Forum Standaardisatie)
Auteurs versie 2 2020	mr. Dr. M.H. (Mathieu) Paapst mr. I.(Iris) de Groot mr. D. B. (Desiree) Castillo Gosker (Bureau Forum Standaardisatie)
Organisatie	Forum Standaardisatie Postbus 96810 2509 JE Den Haag forumstandaardisatie@logius.nl www.forumstandaardisatie.nl

Inhoudsopgave

1 Inleiding

1.1 **Waarom deze handreiking?**

*Geen goede publieke dienstverlening zonder goede ICT, geen goede ICT zonder open standaarden***.**

De overheid streeft naar goede publieke dienstverlening. Hiervoor is samenwerking nodig en dat moet gebeuren met goed ingerichte ICT met allerlei partijen, zowel binnen als buiten de publieke sector. Voor de inrichting van goede ICT zijn duidelijke afspraken nodig en het gebruik van standaarden. Om te beginnen bij de overheid.

Zoals verkeersregels het verkeer regelen op de weg, zo regelen ICT-standaarden het verkeer in de digitale wereld. Zo kan het verkeer van digitale gegevensuitwisseling vlot en vloeiend doorstromen (interoperabiliteit), veilig verlopen en vrij toegang bieden aan alle verkeersdeelnemers; de mensen in een open en vrije samenleving die informatie willen vinden, begrijpen, delen en (her)gebruiken.

Voldoet een open ICT-standaard aan een aantal criteria voor openheid, dan spreken we van een open standaard en open standaarden zijn de norm. De openheid waarborgt dat er niet op voorhand (juridische of financiële) hindernissen zijn voor leveranciers om de standaard in te bouwen of aan te bieden. Gebruik van open ICT-standaarden biedt niet alleen interoperabiliteit maar stimuleert ook de markt, waardoor weer lagere kosten en leveranciersonhankelijkheid kan ontstaan. Open standaarden zorgen voor goede ICT.

Dit is geen nieuw besef. Al sinds 2008 voert het kabinet beleid om het gebruik van open standaarden te bevorderen.

Open standaarden worden echter nog te weinig gebruikt…

Maar zoals blijkt uit jaarlijks onderzoek, is er nog veel ruimte voor verbetering als het gaat om het gebruik van open standaarden. Open standaarden gebruiken, begint bij het bewust vragen om open standaarden en hiervoor kiezen, telkens als er sprake is van een nieuwe aanschaf. Vaak in de vorm van een aanbesteding. Uit jaarlijkse bestudering van aanbestedingen en gesprekken met aanbestedende diensten, blijkt dat aanbestedende overheidsorganisaties nog te weinig vragen om open standaarden en dat hierover nog te weinig bewustzijn leeft. Tweede Kamerleden zijn daarom kritisch als het gaat over de voortgang van het ‘pas toe of leg uit’- beleid en vinden de ontwikkelingen niet snel genoeg gaan.

In de afgelopen jaren zijn diverse moties ingediend om het gebruik van open standaarden te laten toenemen. Dit heeft onder meer geleid tot een grondslag voor de nadere wettelijke verplichting van open standaarden in het wetsvoorstel Digitale Overheid. Zodra dit wetsvoorstel – naar verwachting in 2021- is aangenomen door de Eerste Kamer zullen een aantal standaarden op de lijst van het Forum Standaardisatie wettelijk verplicht worden. Het zal dan vooral gaan om standaarden die ondanks het ‘pas toe of leg uit’-beleid nog onvoldoende gebruikt worden en waarvan het achterwege laten hiervan nijpend begint te worden. Bij een verplichting op grond van de wet Digitale Overheid zal het moment van een eerstvolgende aanschaf niet meer afgewacht kunnen worden, zoals dat bij het ‘pas toe of let uit’- beleid nog wél het geval is. Het is daarom zaak om de ‘pas toe of leg uit’- standaarden te kennen en niet te lang te wachten met implementatie ervan. Uiterlijk bij een eerstvolgende aanschaf van ICT-diensten of ICT-producten.

ICT aanschaffen kan van alles betekenen en over van alles gaan. Hardware, software, een product of een dienst, een aanbesteding of inbesteding, een heel nieuw project of beheer

en verbouw van reeds bestaande systemen. Iedereen die hier wel eens bij betrokken is geweest, weet dat ICT-projecten complex kunnen zijn. Er is veel om rekening mee te houden, en veel dat (achteraf) mis kan gaan. Tijdig de relevante open standaarden in beeld krijgen en toepassen kan bijdragen aan het succesvol laten verlopen van ICT projecten. Vooral met het oog op de langere termijn en voor de publieke dienstverlening als geheel.

1.2 Doelgroep en doel van deze handreiking

Deze handreiking is bedoeld voor opdrachtgevers en inkoopadviseurs. Vooral bij overheidsorganisaties, maar ook bij andere organisaties in de (semi) publieke sector.

Voldoen aan het 'pas toe of leg uit'- beleid en hierop aangesproken kunnen worden is de verantwoordelijkheid van de opdrachtgever of budgethouder onder wiens mandaat een ICT-aanschaf plaatsvindt. Het ligt echter op de weg van de inkoopadviseur om de opdrachtgever zo nodig te wijzen op het bestaan van het 'pas toe of leg uit'-beleid en het gesprek hierover te beginnen zodra sprake is van een ICT aanbesteding van € 50.000 of meer.

Deze handreiking heeft het doel om dit gesprek te stimuleren. Door het belang van de 'pas toe of leg uit'-standaarden te benadrukken, het kiezen voor de juiste standaarden in een specifiek geval makkerlijker te maken, voorbeelden te geven voor bestekteksten en uitleg te geven over hoe gemotiveerd uitgelegd moet worden bij het achterwege laten van standaarden. De rest van deze handreiking ziet er dan ook als volgt uit:

Hoofdstuk 2 geeft het overzicht van de standaarden op de 'pas toe of leg uit'-lijst van het Forum Standaardisatie van 1 januari 2021 met het doel van de standaarden. Verder in dit hoofdstuk meer informatie over hoe het nu precies zit met 'pas toe of leg uit'- beleid en het juridisch kader hiervan.

Hoofdstuk 3 gaat over het bepalen van de relevante open standaarden van de 'pas toe of leg uit'- lijst en verwijst naar een aantal belangrijke online instrumenten, waaronder De Beslisboom Open Standaarden.

Hoofdstuk 4 geeft tien praktijkvoorbeelden van het toepassen van de relevante open standaarden.

Hoofdstuk 5 gaat over hoe gevraagd moet worden in een aanbesteding naar de relevante open standaarden van de 'pas toe of leg uit'- lijst.

Hoofdstuk 6 biedt in vervolg hierop specifieke voorbeeld-bestekteksten.

Hoofdstuk 7 gaat over uitleggen met een geldige reden in het jaarverslag wanneer relevante standaarden bewust achterwege worden gelaten.

2 Open standaarden

2.1 **Kenmerken open standaarden**

De openheid van standaarden zorgt ervoor dat alle open standaarden in het algemeen zorgen voor interoperabilliteit en leveranciersonafhankelijkheid. Afhankelijk van aard van de standaard, zorgen ze daarnaast ook voor veiligheid en toegankelijkkheid in het digitale verkeer en goede vindbaarheid, toegankelijkheid, uitwisseling en (her)gebruik van data.

Kenmerken van voor open standaarden zijn:

1. dat er geen hindernissen zijn om de inhoud van de afspraken te kennen (laagdrempelig beschikbare documentatie),
2. dat de afpraken vervolgens vrij (her)bruikbaar zijn omdat geen intellecturele eigendomsrechten dit beperken,
3. dat een ieder inpraak kan hebben op de inrichting van de standaard
4. en hiervoor terecht kan bij een onafhankelijke en duurzaam ingerichte non-profit beheerorganisatie van de standaard.

   NB: Open standaarden worden vaak in een adem genoemd met open source. Hoewel open standaarden en open source elkaar kunnen versterken als het gaat om goede ICT te gebruiken in de publieke ruimte, zijn het toch ook twee verschillende dingen. Open standaarden gaan over koppelvlakken die iedere ICT leverancier kan inbouwen. Open source software betreft software waarbij de broncode voor iedereen beschikbaar is. Open standaarden kunnen zowel in open source software als in gesloten software geïmplementeerd zijn.

2.2 **'Pas toe of leg uit'-standaarden**

Forum Standaardisatie toetst standaarden voor electronische gegevensuitwisseling onder andere op bovengenoemde kenmerken voor openheid. Dit gebeurt in een openbare procedure. Komt een standaard met succes hierdoor, dan kan de standaard op de lijst gezet worden met open standaarden van het Forum Standaardisatie. Standaarden op deze lijst hebben twee statussen: 'pas toe of leg uit' óf aanbevolen. Een open standaard komt op de 'pas toe of leg uit'- lijst als de standaard nog een extra stimulans nodig heeft om gebruikt te worden.

In deze handreiking bedoelen wij verder met open standaarden, de standaarden voor elektronische gegevensuitwisseling die op de 'pas toe of leg uit'- lijst staan van het Forum Standaardisatie.

De 'pas toe of leg uit' -lijst staat op de website van het Forum Standaardisatie www.forumstandaardisatie.nl en bevat eind 2020 ruim 40 standaarden. Deze lijst verandert ongeveer ieder half jaar een beetje. Er komen standaarden bij of er gaan standaarden af. Deze handreiking zal op dit punt dan ook snel verouderen. Het is dus belangrijk om de lijst op website van het Forum Standardisatie in de gaten te houden voor de meest actuele stand van zaken.

'Pas toe of leg uit'- lijst d.d. 1 januari 2021

Domein	Open standaard	Over	Belangrijkste doel
Internet en beveiliging	IPv4 & IPv6	Internetnummers	Interoperabiliteit
	DNSSEC	Domeinnaambeveiliging	Veiligheid
	TLS	Beveiligde verbinding	Veiligheid
	DKIM	Anti-phising	Veiligheid
	SPF	Anti-phising	Veiligheid
	DMARC	Anti-phising	Veiligheid
	HTTPS & HSTS	Beveiligde websiteverbinding	Veiligheid
	SAML	Inloggegevens	Veiligheid
	RPKI	Beveiliging routing infrastructuur	Veiligheid
	STARTTLS en DANE	Beveiligde verbinding tussen mailservers	Veiligheid
	WPA2 Enterprise	Beveiligde WiFi netwerken	Veiligheid
	STIX en TAXII	Uitwisseling van cyberdreigingsinformatie	Veiligheid
	ISO 27001	Managementsysteem informatiebeveiliging	Veiligheid
	ISO 27002	Richtlijnen en principes informatiebeveiliging	Veiligheid
Documenten en (web)content	PDF/A-1 en -2	Documentpublicatie / archivering	Openbaarheid
	PDF 1.7	Documentpublicatie	Openbaarheid
	ODF	Formaat voor bewerkbare documenten	Openbaarheid
	Ades Baseline Profiles	Digitale handtekeningen	Veiligheid
	Digitoegankelijk	Toegankelijkheid websites	Toegankelijkheid
	OWMS	Metadata overheidsinformatie	Openbaarheid
	SKOS	Thesauri en begrippenwoordenboeken	Openbaarheid
	OpenAPI Specification	Beschrijven van REST APIs	Interoperabiliteit
E-facturatie en administratie	SETU	Informatie flexibele arbeidskrachten	Interoperabiliteit
	XBRL	Bedrijfsrapportages	Interoperabiliteit
	NLCIUS	Elektronisch factureren	Interoperabiliteit
	WDO	Douane-informatie	Interoperabiliteit

Domein	Open standaard	Over	Doel
Stelsels	Digikoppeling	Veilige berichtuitwisseling	Interoperabiliteit
	StUF	Uitwisseling administratieve overheidsgegevens	Interoperabiliteit
	Geo-standaarden	Geografische informatie	Interoperabiliteit
Water en bodem	Aquo-standaarden	Waterbeheer	Interoperabiliteit
	SIKB0101	Bodeminformatie	Interoperabiliteit
Bouw	VISI	Bouwprocesinformatie	Interoperabiliteit
	NLCS	Tekenstandaard	Interoperabiliteit
	COINS	Uitwisseling bouwinformatie	Interoperabiliteit

	IFC	Bouwwerkinformatiemodellen	Interoperabiliteit
Wetgeving Regelgeving Jurisprudentie	BWB	Verwijzingsmechanisme voor wet- en regelgeving	Openbaarheid
	JCDR	Verwijzingsmechanisme decentrale regelgeving	Openbaarheid
	ECLI	Verwijzingsmechanisme rechterlijke uitspraken	Openbaarheid
Onderwijs en loopbaan	e-Portfolio	Uitwisseling werkervaring en competenties	Interoperabiliteit
Verkiezingen	EML_NL	Verkiezingsgegevens	Openbaarheid

In het overzicht hierboven staat in de laatste kolom per open standaard een doel genoemd om in een oogopslag duidelijk te maken op welke manier het gebruik van de standaard waardevol is. Hier kort iets meer over over deze doelen:

Interoperabiliteit
Standaardisatie van ICT zorgt ervoor dat systemen naadloos op elkaar aansluiten. Het digitale verkeer stroomt door. Organisaties kunnen doen waarvoor ze in het leven geroepen zijn, door onderling goed samen te werken en door goed in verbinding te staan met de burgers en bedrijven waar de meeste publieke dienstverlening uiteindelijk voor bedoeld is. Alle open standaarden op de 'pas toe of leg uit'- lijst zorgen in beginsel voor interoperabiliteit en leveranciersonafhankelijkheid maar bij sommige standaarden is deze goede doorstroom van gegevens het het meest prominente doel.

Leveranciersonafhankelijkheid
Staat hierboven niet apart genoemd bij een standaard maar geldt eigendlijk voor alle standaarden, net als interoperabiliteit. De openheid van de standaarden maakt dat in principe meer marktwerking mogelijk. Meer marktwerking betekent meer keuze in leveranciers, meer innovatie en minder hoge kosten voor ICT voor de publieke sector.

Veiligheid
Veilig verkeer in de digitale wereld, zoals bijvoorbeeld betrouwbare websites en e-mails waar niet zomaar iedereen bij kan. Nalaten van het gebruik van de informatie-veiligheidsstandaarden kan tot grote schade leiden en tast het vetrouwen in overheidsorganisaties en andere publieke dienstverleners aan. De open standaarden niet gebruiken die hiervoor verplicht zijn of dringend aanbevolen valt bijna niet uit te leggen.

Toegankelijkheid
Iedereen moet mee kunnen doen, ook digitaal. Een functiebeperking mag geen drempel zijn voor deelname aan het digitale verkeer en informatie moet beschikbaar zijn in begrijpelijke taal voor iedereen. Inclusie dus, ook in de digitale wereld.
Meer over toegankelijkheid: https://www.digitoegankelijk.nl/

Openbaarheid
Openbaarheid van bestuur en rechtspraak, openbare informatie, open data, en linked data. Zonder het gebruik van de juiste open open standaarden niet waar te maken. Open bare informatie dient toegankelijk, vindbaar en begrijpelijk en (her)bruikbaar te zijn.

2.3 **'Pas toe of leg uit' betekenis**

Wat betekent de 'pas toe of leg uit'- status van de open standaarden op de lijst van het Forum Standaardisatie nu precies?

Pas toe
Gebruik de relevante standaarden op de lijst van het Forum Standaardisatie, uiterlijk bij aanschaf van ICT, wanneer deze aanschaf € 50.000 of meer bedraagt. Een ICT aanschaf kan gaan om een dienst, een product, een aanbesteding of inbesteding, verbouw of nieuwbouw. Een standaard is relevant als de ICT valt onder het toepassingsgebied zoals beschreven op de 'pas toe of leg uit'-lijst van het Forum Standaardisatie.

> NB: Vaak gaat een aanschaf gepaard met inkoop en aanbesteding, vandaar dat deze handreiking Vragen om open standaarden bij inkoop heet. Maar eigenlijk moeten de relevante standaarden toegepast worden bij aanschaf, wat een ruimer begrip is.

Leg uit
Relevante standaarden toch niet gebruiken mag alleen met een geldige reden, die terug te vinden is in het jaarverslag. Een geldige redenen is wanneer een ICT-dienst of product naar verwachting in onvoldoende mate wordt aangeboden, onvoldoende veilig of zeker functioneert, of een andere reden van bijzonder gewicht.

2.4 **Juridische verankering**

'Pas toe of leg uit' is juridisch wat versnipperd geregegeld. Misschien dat het beleid daarom vaak wat vrijblijvend geïnterpreteerd wordt (het hoeft niet echt) en niet als een verplichting.

Het is echter een misvatting om te denken dat verplichtingen alleen zouden kunnen voortvloeien op grond van een wet in formele zin. Verplichtingen kunnen ook volgen uit bestuursafspraken en richtlijnen, die nagekomen dienen te worden.

In tegenstelling tot wat vaak wordt gedacht, geldt 'pas toe of leg uit'- als een verplichting voor de meeste overheidsorganisaties. Het gaat daarbij (nog) niet om een verplichting op grond van een wet in formele zin (maar de wet Digitale Overheid kan hier vanaf 2021 wellicht verandering in brengen), maar om een verplichting op grond van een ministeriële regeling, namelijk de Instructie Rijksdienst bij aanschaf van ICT -diensten of ICT-producten (BWBR0024717) én -in aansluiting hierop- de afspraken die bestuurders van gemeenten, provincies, waterschappen en uitvoeringsorganisaties hebben gemaakt en die in de loop der tijd herhaaldelijk zijn bevestigd.

Over deze ministeriële regeling en bestuursafspraken nog het volgende:

2.4.1 Overheidsorganisaties

Voor rijksoverheidsorganisaties geldt sinds 2008 de Instructie Rijksdienst bij aanschaf ICT -diensten of ICT-producten (BWBR0024717). Door het Overheidsbreed Beleidsoverleg Digitale Overheid is in 2018 uitdrukkelijk afgesproken dan ZBO's ook gehouden zijn aan deze instructie.

In deze instructie wordt in artikel 3, lid 1 bepaald dat:

> Bij de aanschaf van een ICT-dienst of ICT-product
> voor een toepassingsgebied dat voorkomt op de lijst die op de website www.forumstandaardisatie.nl is gepubliceerd,
> wordt gekozen voor een ICT-dienst of een ICT-product dat gebruikt maakt van een bij het desbetreffende toepassingsgebied vermelde open standaard.

Uit de toelichting blijkt dat deze verplichting geldt voor de aanbesteding, inkoop of ontwikkeling van ICT-producten en -diensten ter waarde van € 50.000 en meer. Niet alleen voor nieuwe producten of diensten, maar ook als het gaat om aanpassing van bestaande producten of diensten.

Daarnaast staat in de RijksBegrotingsVoorschriften een bepaling m.b.t. de paragraaf 'Rijksbrede bedrijfsvoeringsonderwerpen':

> Gebruik open standaarden en open source software: Dit onderwerp wordt in deze paragraaf alleen vermeld indien is afgeweken (het 'comply of explain'-beginsel) van artikel 3, eerste lid van de Instructie rijksdienst bij aanschaf ICT-diensten of ICT-producten). De Tweede Kamer wil dat de overheid meer gebruik maakt van open standaarden en open source software. De Instructie rijksdienst schrijft voor dat bij de aanschaf en ontwikkeling van ICT-diensten of ICT-producten in beginsel gebruik moet worden gemaakt van open standaarden van de lijst van het College Standaardisatie. Valide afwijkingsgronden zijn opgenomen in de Instructie Rijksdienst. Als er sprake is van afwijking van de Instructie Rijksdienst dan wordt dit gemotiveerd aangegeven.

NB: Het College Standaardisatie bestaat al een aantal jaren niet meer en het Overheidsbreed Beleidsoverleg Digitale Overheid is hiervoor sinds 2018 in de plaats gekomen. Een wijziging van de Rijksbegrotingsvoorschriften is eind 2020 nog niet doorgevoerd.

In 2008 is in de iNUP-bestuursakkoorden als Resultaatafspraak 20 opgenomen, voor zover het open standaarden betreft:
Gemeenten maken gebruik van de open standaarden zoals vastgesteld door het College standaardisatie en werken hierbij volgens het principe "pas toe of leg uit".
Deze resultaatafspraak was van toepassing op gemeenten, provincies en waterschappen.

Deze afspraak is hierna herhaaldelijk herbevestigd in het College Standaardisatie en het Nationaal Beraad Digitale Overheid.

Op 18 april 2018 heeft het Overheidsbreed Beleidsoverleg Digitale Overheid voor het laatst besloten dat ook mede-overheden bij aanschaf van ICT moeten kiezen voor de relevante open standaarden van de 'pas toe of leg uit"-lijst.

2.4.2 Andere organisaties in de publieke sector

Is een organisatie géén overheidsorganisatie zoals hierboven genoemd, dan is het gebruik van de 'pas toe of leg uit'- standaarden strikt genomen niet verplicht.' Pas toe of leg uit' mag dan worden opgevat als een dringend advies.

Er is geen toezicht of handhaving als 'pas toe of leg uit' niet wordt nageleefd of opgevolgd. Het onderscheid 'verplicht' of 'dringend aanbevolen' heeft wat dat betreft geen consequenties.

2.5 **Monitor Open Standaarden en IV-meting**

Er is dus geen toezicht en handhaving op 'pas toe of leg uit'. Wél vindt jaarlijks monitoring plaats en halfjaarlijks een meting van de internet- en beveiligingsstandaarden om te zien hoe het staat met het gebruik van de standaarden op de 'pas toe of leg uit'-lijst. Om het gebruik van de 'pas toe of leg uit'-standaarden te meten en tegelijkertijd ook van ook om de adoptie een impuls te geven.

In de Monitor Open Standaarden worden aanbestedingsdocumenten onderzocht en jaarverslagen. De onderzoekers bekijken in de aanbestedingsdocumenten of organisaties om de relevante open standaarden vragen en of zij goed verantwoording afleggen in jaarverslagen als dit niet gebeurt. Zoals al eerder gezegd anno 2020 is er nog veel ruimte te zien voor verbetering op dit punt.

Daarnaast voert het Forum Standaardisatie twee keer per jaar een meting uit naar het gebruik van een aantal internet en beveiligheidsstandaarden, met behulp van de webtool internet.nl. In dit onderzoek is overigens wél een stijgende lijn te zien.

Zie voor de laatste resultaten van zowel de Monitor als de IV-metingen:

https://magazine.forumstandaardisatie.nl/

3 Relevante standaarden bepalen

Om met het oog op ICT kwaliteit bij de overheid de relevante open standaarden te selecteren en op te nemen in een aanbesteding, zijn zijn online een aantal tools beschikbaar die elkaar aanvullen.

3.1 De Beslisboom Open Standaarden

Op de website van het Forum Standaardisatie staat het meest aangewezen instrument om de weg te vinden in de toepassingsgebieden bij de standaarden op de 'pas toe of leg uit'- lijst: de Beslisboom Open Standaarden.

Deze Beslisboom is bedoeld om tot een eerste inschatting te komen van de standaarden die met het oog op een ICT aanschaf relevant zijn.

De vragen van de Beslisboom dienen bij voorkeur zo veel mogelijk beantwoord te worden met de betrokkenen van een aanbesteding.

De Beslisboom geeft een eerste ruwe selectie van relevante stanaarden voor nadere overweging. Neem voor meer advies op maat contact op met het Bureau Forum Standaardisatie.
info@forumstandaardisatie.nl

3.2 Meer specifiek voor BIO beveilingseisen: de ICO-Wizard

De ISO 27001 en ISO 27002 standaarden staan op de 'pas toe of leg uit'-lijst en zijn heel vaak van toepassing als het gaat om een nieuwe aanschaf van ICT. Voor overheidsorganisaties zijn de ISO 270001 en ISO 27002 vertaald naar de BIO (Baseline Informatiebeveiliging Overheid) en dus ook heel vaak van toepassing.

Ten tijde van het actualiseren van deze handreiking in 2020, ontwikkelt het Centrum voor Informatie en Privacybescherming de ICO-Wizard. Dat is net als de Beslisboom Open Standaarden ook een instrument om vroeg in het proces nadere afwegingen te maken, maar dan specifiek over beveiliging.

Met de ICO-Wizard kunnen organisaties ervoor zorgen dat bij inkoop de juiste BIO veiligheidsnormen in beeld komen, zodat de organisatie ze ook kan opnemen in het programma van eisen van een aanbesteding.

De ICO- Wizard vult de Beslisboom Open Standaarden nader aan en gaat dieper in op de veiligheidsnormen van de BIO. Veel veiligheidsstandaarden van de 'pas toe of leg uit'- lijst komen ook inde ICO-Wizard terug.

https://www.bio-overheid.nl/ico-wizard/

3.3 Internet.nl

Met internet.nl kunnen organisaties bepalen of hun websites en e-mailadressen voldoen aan een aantal van de internet en beveiligingsstandaarden van de 'pas toe of let uit'- lijst.

Op internet.nl is sinds 2020 ook een Hall of Fame opgenomen van hosters die een 100% score hebben.

3.4 Speciaal voor gemeenten: de GIBIT Toolbox en overeenkomstengenerator

De VNG biedt in het kader van de GIBIT een toolbox aan met een overeenkomstengenerator. Bij de GIBIT horen kwaliteitsnormen en in deze kwaliteitsnormen is een verwijzing in algemene zin opgenomen naar de 'pas toe of leg uit'-lijst van het Forum Standaardisatie. Gemeenten moeten voor een aanbesteding hieruit een keuze maken welke standaarden specifiek van toepassing zijn en hierom vragen. De overeenkomstengenerator kan hierbij helpen.

De GIBIT toolbox is ten tijde van het schrijven van deze handreiking sinds kort beschikbaar en alleen voor gemeenten.

4 Relevante standaarden toepassen

Voor iedere standaard op de 'pas toe of leg uit'- lijst is een formeel toepassingsgebied gedefinieerd. Vaak zijn dit vrij uitgebreide en technisch geformuleerde definities die niet gelijk gemakkelijk te begrijpen zijn. De toepassingsgebieden van de 'pas toe of leg uit'-standaarden zijn daarom ook verwerkt in de hierboven genoemde Beslisboom Open Standaarden. Hierin worden de standaarden minder formeel maar wel gebruiksvriendelijker aangeboden dan op de 'pas toe of leg uit lijst.

Tegenover de abstracte toepassingsgebieden van de 'pas toe of leg uit' standaarden staat de werkelijkheid van een enorme variëteit in toepassingen. Dat maakt maatwerk van het bepalen van de relevante standaarden en het toepassen in de praktijk.

Bij het aanschaffen van nieuwe ICT moet telkens de toepasselijkheid van een 'pas toe of leg uit'- standaard herkend worden.

Om dit te illustreren en om meer gevoel te krijgen bij de toegevoegde waarde van de standaarden in de praktijk, staan in dit hoofdstuk tien voorbeelden van aanbestedingen genoemd die onderzocht zijn in het kader van de Monitor Open Standaarden. De praktijkvoorbeelden illustreren de volgende 10 ICT-producten of -diensten:

1. Websites/ webapplicaties
2. Werkplek en kantoorsoftware
3. E-mail
4. Spraak- of datacommunicatiediensten
5. Multi-functionals
6. Financieel/administratieve systemen
7. e-HRM-systemen
8. Netwerken
9. Basisregistraties/overheidsgegevens
10. Inhuur

Meer voorbeelden van onderzochte aanbestedingen zijn te vinden in de bijlage van de Monitor Open Standaarden die op de website van het Forum Standaardisatie staat.
https://www.forumstandaardisatie.nl/metingen/monitor

Disclaimer: De techniek verandert snel en zo raken de voorbeelden die hier gegeven zijn uit de Monitor van 2018 en 2019 ook snel verouderd. Standaarden die anno 2020 relevant zijn kunnen ontbreken of niet meer relevant zijn. Kijk voor de meest actuele versie van de lijst met 'pas toe of leg uit'- standaarden op de website van het Forum Standaardisatie of gebruik de Beslisboom Open Standaarden.

4.1 Websites of webapplicaties

De Nederlandse Publieke Omroep doet in 2018 een openbare aanbesteding voor het leveren van development en design voor de ontwikkeling van 9 nieuwe apps voor NPO Radio algemeen en de diverse radiomerken van de NPO, inclusief beheer, ondersteuning en onderhoud. De apps moeten d.m.v. gestandaardiseerde en gedocumenteerde koppelvlakken (bijv. API's) kunnen koppelen met andere systemen en databases in de keten.
https://www.tenderned.nl/tenderned-tap/aankondigingen/132192

Het gaat hier om webapplicaties en bij deze aanbesteding zijn waarschijnlijk de volgende standaarden relevant:

- SAML, want in het bestek is gevraagd om koppeling met NPO single sign-on en profielendata.

- Digitoegankelijk, want het gaat over applicaties voor burgers.
- HTTPS, HSTS en TLS, want het betreft een webapplicatie en voor beveiliging van netwerkverbindingen.
- Open API, vanwege de wens om gebruik te maken van gestandaardiseerde en gedocumenteerde koppelvlakken.

4.2 **Werkplek en kantoorsoftware**

Het Huis voor Klokkenluiders publiceert eind 2017 een aanbesteding voor een onafhankelijke ICT-dienstverlener om de kleine organisatie op ICT-gebied te ontzorgen en een digitale werkomgeving bij onder te brengen. De werkzaamheden van Het Huis zijn zeer vertrouwelijk en vragen om een beveiligde digitale werkomgeving. De scope van de aanbesteding bevat het leveren van een beveiligde digitale werkomgeving, ICT infrastructuurdiensten/hosting, hardware incl. software voor werkplekken (incl. onderhoud en beheer), en koppelingen met het SaaS-systeem en Citrix werkomgeving. https://www.tenderned.nl/tenderned-tap/aankondigingen/125308

Bij deze aanbesteding zijn waarschijnlijk de volgende standaarden relevant:

- WPA2 Enterprise, voor beschikking kantoor over internettoegang.
- TLS, voor inrichting mailkoppeling naar zaaksysteem.
- SAML, vanwege single-sign-on mogelijkheid.
- IPv4 en IPv6, voor internetverbinding van de digitale werkomgeving.
- DNSSEC, voor domeinnaam van de digitale werkomgeving.
- STARTTLS, DANE, SPF en DKIM, voor beveiliging e-mail.
- ISO 27001 / 27002, voor informatiebeveiliging.
- HTTPS en HSTS, voor beveiligde toegang tot o.a. email.
- PDF en ODF, vanwege het werken met reviseerbare en niet-reviseerbare documenten.

Toelichting
Alle bovengenoemde standaarden worden in deze aanbesteding ook daadwerkelijk gevraagd. Er wordt bovendien in het bestek vaak verwezen naar het gebruik van open standaarden en men verwijst ook vaak naar de 'Pas toe of leg uit'-lijst van Forum Standaardisatie. Bovendien spoort men aan het gebruik van niet algemeen geaccepteerde standaarden nadrukkelijk te vermijden.

4.3 **E-mail**

Het ministerie van Algemene Zaken vraagt in 2018 in een aanbesteding om het leveren en beheren van een e-mailmanagementvoorziening voor het Platform Rijksoverheid Online (PRO), inclusief facultatieve dienstverlening rondom optimalisatie van het e-mailkanaal.
https://www.tenderned.nl/tenderned-tap/aankondigingen/146062

In deze aanbesteding zijn waarschijnlijk de volgende standaarden relevant:
- IPv4 en IPv6, voor internetverbinding van de e-mailvoorziening.
- HTTPS en HSTS, voor een beveiligde verbinding.
- TLS, voor versleuteling van de verbinding.
- DKIM, DMARC, SPF, want het betreft inkomend en uitgaand e-mailverkeer.
- STARTTLS/DANE, want het gaat hier om een ontvangende en verzendende e-mailserver.

- ISO 27001 / 27002, voor informatiebeveiliging.
- PDF en ODF vanwege het werken met reviseerbare en niet-reviseerbare documenten (zoals kunnen uitdraaien van managementrapportages).
- Open API specificatie, vanwege de mogelijkheid dat gebruik zal worden gemaakt van een API.

Toelichting
Zoals hiervoor al aangegeven is de BIO, danwel zijn de standaarden ISO 27001/27002 relevant voor vrijwel alle aanbestedingen. In dit specifieke geval al helemaal omdat er door de nieuwe leverancier een groot aantal persoonsgegevens (immers emailadressen) gemigreerd moest gaan worden van het oude naar het nieuwe systeem.

In de Baseline Informatiebeveiliging Overheid (BIO) is opgenomen dat persoonsgegevens niet onversleuteld over onbeveiligde/onvertrouwde netwerken verzonden mogen worden. Informatie die is opgenomen in een elektronisch berciht behoord passend te worden beschermd. Deze baseline verplicht zodoende afgedwongen versleuteling van verbindingen zoals STARTTLS die in combinatie met DANE ondersteunt.

Ook het gebruik van ODF is in deze aanbesteding terecht van de toekomstige leverancier geeist:
"Opdrachtnemer stelt ook verzendstatistieken beschikbaar in ODF-formaat.
Opdrachtnemer stelt tevens een gebruikershandleiding beschikbaar in ODF-formaat."

En omdat er mogelijk gebruik moet worden gemaakt van een API, is er ook het volgende op voorhand al geeist:
"Voor het gebruik van een API is de open API-Specification vastgesteld als open standaard. Opdrachtgever volgt deze standaard gecombineerd met de standaarden voor web en e-mail".

Zoals ook uit bovengenoemd praktijkvoorbeeld blijkt: let er op dat bij software ten behoeve van email, dat meerdere standaarden relevant kunnen zijn uit de domeinen "Internet en beveiliging" en "Documenten en webcontent".
Het gaat gaat bij e-mail niet alleen om het aanschaffen of in gebruik nemen van een e-mail client, maar vaak ook om de inrichting van allerlei ICT-systemen van waaruit door middel van het e-mail-protocol een bericht of nieuwsbrief kan worden verzonden. Denk bijvoorbeeld aan de verderop nog te bespreken multifunctionals, waarbij het vaak mogelijk is om vanuit de multifunctional gescande documenten te verzenden aan een mailadres.

4.4 **Spraak en/ of datacommunicatiediensten**

Luchtverkeersleiding Nederland wil in 2019 een overeenkomst sluiten met een telecomprovider voor het leveren, onderhouden en verder evolueren van vaste spraakdiensten, gekoppeld aan telefonie platformen zoals deze in gebruik zijn binnen LVNL. Het betreft hier met name SIP-trunk dienstverlening op diverse LVNL locaties in Nederland. Er wordt ook een webportaal geeist waarmee LVNL zelf de configuratie kan instellen.

https://www.tenderned.nl/tenderned-tap/aankondigingen/162632

Voor deze aanbesteding zijn waarschijnlijk de volgende standaarden relevant:

- IPv4 / IPv6, want SIP is een VoIP technologie.
- HTTPS en HSTS, voor een beveiligde verbinding voor het webportaal.

- TLS, voor versleuteling van verbindingen.
- PDF, omdat er niet-reviseerbare rapportages worden gevraagd.
- ISO27001 / 27002. De leverancier is immers de spil in het communicatienetwerk van LVNL.

Toelichting
Waar het gaat om (hardware bevattende) software ten behoeve van spraak en/of datacommunicatie, zijn meerdere standaarden relevant uit het cluster "Internet en beveiliging". Daarbij kan gedacht worden aan de inkoop van Voice over IP diensten (internetbellen), maar ook aan smartphones of tablets waarmee verbinding kan worden gemaakt met het internet.

WPA2 Enterprise maakt het bijvoorbeeld mogelijk dat gebruikers automatisch enveilig toegang krijgen tot aangesloten WiFi-netwerken. Ook als deze WiFi-netwerken zich buiten de eigen organisatie bevinden. De authenticatie vindt plaats op basis van bestaande identiteitsgegevens van de gebruiker, hierdoor hoeven gebruikers niet opnieuw in te loggen. Met het gebruik van WPA2 Enterprise is ook de integriteit van de netwerkverbinding geborgd.

En omdat er bij dit soort diensten vrijwel altijd sprake is van (vertrouwelijke) gegevensverwerking door een leverancier, is de eis om ISO 27001/27002 hier ook absoluut noodzakelijk.

4.5 **Multifunctionals**

IUC-Noord vraagt in 2019 in een aanbesteding om het leveren, installeren en onderhouden van een fullcolour hoogvolume rolprintoplossing en bijbehorende randapparatuur. Niet limitatief zijn de volgende standaarden relevant:

https://www.tenderned.nl/tenderned-tap/aankondigingen/168900

- ISO 27001 / 27002, vanwege informatieveiligheid.
- PDF, omdat de printbestanden soms in een niet-reviseerbaar formaat geleverd worden.
- TLS, voor versleuteling van verbindingen tussen de printers en andere netwerkcomponenten.
- Open API Specification, vanwege de wens om documentatie waarin de koppelvlakken/interfaces tot in detail bescheven staan.

Toelichting
Waar het gaat om (hardware bevattende) software ten behoeve van, of om te gebruiken op werkplekken, zijn meerdere standaarden relevant uit de clusters "Internet en beveiliging" en "Documenten en webcontent". Zo maakt een multifunctional in veel gevallen verbinding via een (inter)netwerk waardoor bijvoorbeeld versleuteling via TLS en bereikbaarheid via IPv6 belangrijk is; Maar ook moet het in staat zijn om ODF documenten te verwerken, en indien de multifunctional ook gebruikt kan worden om mee te scannen dan moet er de mogelijkheid zijn voor een output in het pdf formaat. Indien het mogelijk is om vanuit de multifunctional te emailen, dan dienen ook de beveiligingstandaarden uit de inkoopcategorie "email" hier geeist te worden.

4.6 **Financieel/ administratieve systemen**

ZonMw financiert gezondheidsonderzoek. Het doel van de nieuwe applicatie die zij aanbesteden in 2017 is om het subsidieproces te faciliteren en te ondersteunen. Middels het portaal, kunnen organisaties, externen (beoordelaars) en individuele aanvragers het traject van aanvraag tot en met de vaststelling van de subsidie (inclusief de verantwoording) volledig digitaal afhandelen. Intern binnen ZonMw wordt de subsidieaanvraag verder verwerkt en beoordeeld in het te verwerven pakket.
https://www.tenderned.nl/tenderned-tap/aankondigingen/119454

Standaarden die waarschijnlijk relevant zijn:

- XBRL, want het betreft rapportages met een financiële component en gegevensuitwisseling met een financieel systeem.
- HTTPS en HSTS & TLS, want het betreft een webportaal.
- ISO 27001 / 27002, vanwege de beveiliging van persoonsgegevens.
- ODF, want het betreft het opstellen van documenten en rapportages.
- PDF, want het betreft niet-reviseerbare documenten en archivering.
- SAML, want door middel van inloggen moet een indiener zijn aanvraag. kunnen opstellen, indienen, aanpassen en intrekken.
- Digitoegankelijk, want het een betreft een portaal voor burgers en bedrijven.
- DMARC, SPF en DKIM, want het betreft inkomend en uitgaand e-mailverkeer.

Waar het gaat om software ten behoeve van, of om te gebruiken als financieel/administratieve systemen, zijn meerdere standaarden relevant uit de domeinen "Internet en beveiliging", "Documenten en webcontent" en "E-facturatie en administratie". De internet en beveiligingstandaarden zijn bijvoorbeeld relevant indien het financieel/administatieve systeem benaderbaar wordt via het internet. Ook dient het in geval van rapportages mogelijk te zijn om de output te krijgen in ODF.

NLCIUS geeft duidelijkheid aan overheden en bedrijven over de elementen en gegevens die op facturen naar overheidsorganisaties gebruikt dienen te worden in Nederland.

4.7 **E-HRM-systemen**

De Nederlandse Zorgautoriteit zoekt in 2018 een partij voor het leveren van een integrale SaaS oplossing voor de HRM en F&C processen waarbij de salaris administratie/-verwerking als dienstverlening wordt aangeboden,waarmee de beschreven gebruikersproblemen worden verholpen en waardoor de opdrachtgever goede en efficiënte dienstverlening kan leveren aan haar medewerkers. Er moeten ook koppelingen komen met andere oplossingen van externe partijen en er moet data van de oude naar de nieuwe omgeving worden gemigreerd.

https://www.tenderned.nl/tenderned-tap/aankondigingen/129833

De volgende standaarden zijn hier waarschijnlijk relevant:

- e-Portfolio, want het gaat hier om een e-HRM systeem waarin ook het HRM proces "Talent management" is opgenomen.
- ISO 27001 / 27002, voor informatie-veiligheid van o.a. persoonsgegevens.
- SAML, want single sign on functionaliteit gevraagd.
- HTTPS, HSTS en TLS, voor beveiliging portals en websites.
- DNSSEC, voor beveiliging van webverkeer.
- XBRL, voor uitwisseling van documenten met financiële informatie d.m.v. gelegde koppelingen.

- ODF en PDF, voor het genereren van rapporten.

Toelichting
Waar het gaat om e-HRM systemen, zijn meerdere standaarden relevant uit de domeinen "Internet en beveiliging", "onderwijs en loopbaan" en "Documenten en webcontent". Zo zijn e-HRM systemen vaak benaderbaar via het internet, waardoor vrijwel alle standaarden die voorkomen bij de inkoopcategorie "website of webapplicatie" ook in dit geval relevant zijn. Denk daarbij niet alleen aan beveiliging, maar ook aan Digitoegankelijk en -voor het kunnen inloggen- aan SAML.

Binnen het domein "onderwijs en loopbaan" kan gedacht worden aan e-Portfolio. Met E-portfolio NL kunnen de competenties van een individu worden bijgehouden. Het voordeel van deze standaard is dat de student/lerende medewerker zijn profiel mee kan nemen naar verschillende organisaties.

Binnen "Documenten en webcontent" kan worden gedacht aan ODF of PDF, bijvoorbeeld omdat er vanuit de systemen rapportages uitgedraaid moeten kunnen worden.

4.8 **Netwerken**

De RDW heeft besloten de complete Wifi dienstverlening extern af te nemen zodanig dat Wifi op alle RDW-locaties in Nederland als een managed service wordt aangeboden. In 2018 publiceren zij hiervoor een aanbesteding. Onderdeel van deze aanbesteding is een volledige dienst die end-2-end de gewenste functionaliteit levert, inclusief de complete installatie, implementatie en onderhoud & support. Ook gasten maken hier gebruik van. De opdracht bestaat uit levering van apparatuur t.b.v. wifi dienstverlening, implementatie en installatie van apparatuur en dienst, beheer en support van apparatuur en dienst, en internetconnectiviteit incl. DNS en DHCP.

https://www.tenderned.nl/tenderned-tap/aankondigingen/145911

In deze aanbesteding eist de RDW in ieder geval de volgende twee standaarden:
- ISO 27001 / 27002, vanwege informatieveiligheid.
- WPA2 Enterprise, vanwege de toegang tot het Wifi-netwerk.

De volgende standaarden hadden echter ook gevraagd kunnen worden:

- DNSSEC, vanwege een beveiligde DNS.
- IPv4 en IPv6, vanwege het gebruik van IP-reeksen.
- HTTPS, HSTS en TLS, voor een beveiligde verbinding met internet.

Toelichting
Waar het gaat om software ten behoeve van, of om te gebruiken in netwerken zijn meerdere standaarden relevant uit het cluster "Internet en beveiliging". Hier is de eis om ondersteuning van IPv6 in combinatie met IPv4 (duall stack) absoluut noodzakelijk. IPv6 is niet backwards compatible. Dit wil zeggen dat een IPv4-systeem niet een IPv6-systeem kan bereiken, of andersom. Om die reden moet een organisatie bij de aanschaf van een ICT-product/-dienst beide versies uitvragen.

En aangezien via de netwerkdiensten vrijwel altijd persoonsgegevens verwerkt kunnen worden, ligt ook een ISO 27001/27002 eis voor de hand. Het is overigens niet nodig om deze ISO standaarden bij alle inkopen van ICT-producten en diensten te vereisen. Inkopende organisaties dienen zelf, ten aanzien van een specifieke aanschaf, risicogebaseerd te bepalen of zij de naleving van deze standaarden van hun leverancier

vereisen, mede op basis van de eigen intern geldende baseline informatiebeveiliging. In de communicatie dient helder te zijn dat niet beoogd wordt om in alle gevallen van toepassing van deze standaarden certificering van de leverancier te eisen; in eerste instantie kan naleving van de standaarden vereist worden en daarna, voor zover opportuun voor de inkopende organisatie in het specifieke geval, kan certificering van de leverancier vereist worden.

4.9 **Basisregistraties/ overheidsgegevens**

Het Ministerie van Sociale Zaken en Werkgelegenheid doet in 2018 een aanbesteding voor een zaakgericht werken systeem die de processen van de afdeling CAV kan ondersteunen. Om hun taken op het gebied van Cao-aanmelding, AVV en Pensioenen uit te kunnen voeren maakt de afdeling gebruik van applicaties die het eind van hun levensduur hebben bereikt en dienen te worden vervangen. De opdracht bestaat uit het beheren en (door)ontwikkelen van een website, de aanschaf van een licentie voor een zaakgericht werken systeem, en het beheren, onderhouden en doorontwikkelen van dat systeem. Het systeem bevat tevens een e-mailfunctionaliteit.

https://www.tenderned.nl/tenderned-tap/aankondigingen/128880

Waarschijnlijk zijn de volgende standaarden relevant:

- StUF, voor uitwisseling gegevens uit de basisregistraties.
- ISO 27001 / 27002, m.b.t. informatiebeveiliging.
- DNSSEC, voor domeinnaam voor website/webportaal.
- SAML, voor authenticatie bij inloggen.
- Digitoegankelijk, want het betreft o.a. een webapplicatie.
- HTTPS/HSTS en TLS, voor het tot stand komen van veilig webverkeer.
- PDF, voor documenten die moeten worden omgezet naar een niet-reviseerbaar formaat.
- DMARC, SPF en DKIM, vanwege een email mogelijkheid.

Toelichting
Men spreekt in dit bestek bovendien de wens uit om maximaal gebruik te maken van open standaarden en daarbij wordt verwezen naar Forum Standaardisatie en de ‘pas toe of leg uit’-lijst.

Waar het gaat om software en informatiesystemen ten behoeve van basisregistraties en ten behoeve van het registreren en uitwisselen van informatie met een geografische component, zijn meerdere standaarden relevant uit de clusters “stelselstandaarden” en “Water en bodem”. StUF is bijvoorbeeld een universele berichtenstandaard voor het elektronisch uitwisselen van gegevens tussen applicaties. Het domein van de StUF-taal omvat informatieketens tussen overheidsorganisaties (basisregistraties en landelijke voorzieningen) en gemeentebrede informatieketens en -functionaliteit. StUF is beschreven in XML en gebaseerd op geaccepteerde internetstandaarden. Digikoppeling is van toepassing bij aanschaf of ontwikkeling van systemen bedoeld voor gestructureerde berichtenuitwisseling met voorzieningen zoals de basisregistraties en berichtverkeer dat sectoroverstijgend is. Indien het ICT-systeem een rapportagemogelijkheid moet hebben, dient ook gedacht te worden aan standaarden uit het cluster “ Documenten en webcontent” zoals ODF of PDF.

4.10 **Inhuur**

De Belastingdienst deed in 2017 een aanbesteding voor het leveren van een Rijksbrede HR werving & selectie oplossing ter ondersteuning van in-, door- en uitstroom van medewerkers van het Rijk en Defensie. De oplossing dient geleverd te worden als SaaS (Software as a Service).

SETU was hierbij expliciet als eis in het bestek opgenomen aangezien er sprake is van berichtenuitwisseling rondom flexibele arbeidskrachten.

https://www.tenderned.nl/tenderned-tap/aankondigingen/113868

In de aanbesteding waren waarschijnlijk meerdere standaarden uit het cluster "Internet en beveiliging" , "Documenten en webcontent", en uit het cluster "onderwijs en loopbaan" van belang:

- HTTPS en HSTS & TLS, want de toegang tot het systeem gaat volledig via een web browser
- ISO 27001 / ISO 27002, want het SaaS systeem bevat te beschermen persoonsgegevens.
- SAML, want er wordt in het bestek gesproken over single sign on.
- DNSSEC, want het SaaS systeem is bereikbaar via een domeinnaam.
- Digitoegankelijk, want er is ook sprake van interactie via een webportaal voor burgers.
- ODF en PDF, want het systeem moet kunnen omgaan met reviseerbare en niet-reviseerbare documenten.
- STARTTLS, DANE, SPF en DKIM, want het betreft inkomend en uitgaand e-mailverkeer.
- ePortfolio, want het betreft uitwisseling van gegevens over werkervaring en competenties.

Toelichting
Waar het gaat om software of diensten ten behoeve van de inhuur van personeel, zijn meerdere standaarden relevant uit de clusters "Internet en beveiliging" en "E-Facturatie en administratie". Zo kan aan de dienstverlener gevraagd worden te voldoen aan ISO 27002 aangezien de uitvraag en het aanbod vrijwel altijd persoonsgegevens bevatten, waaronder uurtarieven.

De SETU-standaarden zijn ontwikkeld door de grote uitzendorganisaties en is de Nederlandse implementatie van de internationale HR-XML standaard. Door toepassing van de SETU standaarden ontstaat uniformering van het elektronisch berichtenverkeer tussen aanbieders en afnemers (inleners) van tijdelijk personeel (flexibele arbeid). Het eisen van deze standaarden kan ook relevant zijn bij de inkoop van e-HRM systemen, of bij financieel/administratieve systemen.

NB: Als het gaat om eisen die *inhoudelijk* gesteld mogen worden aan de mensen die ingehuurd worden (en niet aan de ICT systemen) dan mag kennis en kunde gevraagd worden van de 'pas toe of leg uit'- lijst in het algemeen of van een aantal specifieke standaarden, afhankelijk van wat de dienst inhoudt. Denk bijvoorbeeld aan Digitoegankelijkheid voor het ontwerpen van websites en SKOS voor de inhuur van diensten voor inhouds- of datastandaardisatie en –classificatie.

5 Vragen om open standaarden

5.1 Inleiding

In dit en het volgende hoofdstuk staan voorbeeld-bestekteksten. De teksten dienen op maat gemaakt te worden voor de betreffende opdracht van de aanbestedende dienst. Hierbij moeten de algemene uitgangspunten van AW2012 (met name het beginsel van proportionaliteit) toegepast worden.

Om die reden zijn er geen bedragen, aantallen, jaartallen en dergelijke opgenomen in de teksten maar wel het in te vullen veld [x]. Ook andere velden die nog ingevuld moeten worden zijn op die wijze gemarkeerd, bijvoorbeeld [naam standaard]. Daarnaast is in de voorbeeld- bestekteksten rekening gehouden met twee mogelijke aanbestedingsprocedures: 'niet-openbaar' waarbij er sprake is van een gegadigde en 'openbaar' waarbij er sprake is van een inschrijver.

5.2 Toelichtende bestektekst

Om de eisen en wensen met betrekking tot Standaarden in een kader te plaatsen kan de aanbestedende dienst onderstaande toelichtende teksten opnemen:

Toelichtende bestektekst
Open Standaarden
[Aanbestedende dienst] wil graag dat de dienst of product, conform het openstandaardenbeleid van de Nederlandse overheid, werkt op basis van open standaarden met als achterliggende doelen de bevordering van de interoperabiliteit en de vergroting van de leveranciersonafhankelijkheid.
Verwijzing naar verplichte Open Standaarden
[Aanbestedende dienst] verwijst in de specificatie van de dienst of product expliciet naar de relevante, verplichte open standaarden die op de 'pas toe of leg uit'-lijst van Forum Standaardisatie staan (www.forumstandaardisatie.nl).
Beoordeling 'of gelijkwaardig'
Mocht de inschrijver/gegadigde een 'gelijkwaardige' standaard aanbieden, dan dient deze aan te tonen dat dit alternatief voldoet aan de door het Forum Standaardisatie gehanteerde en gepubliceerde criteria voor opname op de 'pas toe of leg uit'-lijst, zodat interoperabiliteit en leveranciersonafhankelijkheid in voldoende mate voor de [aanbestedende dienst] zijn gewaarborgd.
Garanties naar de toekomst
In het kader van Preventief en/of Innovatief Onderhoud garandeert inschrijver/gegadigde ten minste: i) dat de dienst of het product steeds tijdig zal blijven voldoen aan de relevante Wet- en regelgeving; ii) dat de dienst of het product steeds tijdig geschikt zal blijven voor gegevensuitwisseling met de overige relevante onderdelen van het Applicatielandschap (voor zover bekend bij inschrijver/gegadigde) en in dat kader aan de overeengekomen interoperabiliteitseisen zal blijven voldoen; iii) dat de dienst of het product door middel van het tijdig uitbrengen van updates en/of upgrades steeds tijdig zal blijven voldoen aan nieuwe versies van de relevante open standaarden die in de Overeenkomst als vereiste normen zijn gespecificeerd;

5.3 **Geschiktheidseisen**

Onderstaande geschiktheidseisen kan een aanbestedende dienst hanteren om de geschiktheid en bekwaamheid van een leverancier met de desbetreffende relevante Open Standaard te kunnen beoordelen.

Bestektekst geschiktheidseisen	Doel en toelichting
Kerncompetentie Ervaring	
De [gegadigde/inschrijver]dient aan te tonen dat hij in de afgelopen [x] jaar ervaring heeft opgedaan met het succesvol implementeren van ICT-systemen die gegevens uitwisselen conform de open standaard [naam standaard] zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig. Om aan te tonen dat [gegadigde/inschrijver] voldoet aan deze kerncompetentie dient u bij [het verzoek tot deelneming/de inschrijving] [x] relevante referentie[s] op te geven waaruit blijkt dat [gegadigde/inschrijver] voldoende ervaring heeft met betrekking tot deze kerncompetentie.	Inzicht in de aantoonbare ervaring van de gegadigde/inschrijver met de gevraagde Open Standaard. De vraag kan verder worden gespecificeerd door in deze eis een specifiek ICT-systeem te noemen. Deze eis, de vraag naar referenties, kan eventueel worden ingepast in de andere referentie-eisen.
Bekwaamheid	
De [gegadigde/inschrijver] geeft een duidelijk inzicht in het kwaliteitsniveau en de beschikbaarheid van zijn personeel dat de [gegadigde/inschrijver] voornemens is in te zetten bij de implementatie van het ICT-systeem dat gegevens uitwisselt conform de open standaard [naam standaard] zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig. De [gegadigde/inschrijver] overlegt daartoe een overzicht van minimaal [x] medewerkers en hun CV's en opleidingscertificaten waarover [gegadigde/inschrijver] kan beschikken waaruit hun ervaring met en kennis van [naam standaard] duidelijk blijkt.	Inzicht in bekwaamheid van het in te zetten personeel. Voor diverse open Standaarden bestaan er opleidingstrajecten. Deze kunnen worden aangeboden door leveranciers en door onafhankelijke onderwijsinstellingen.

5.4 **Selectiemethode**

Doorgaans is de mate van ervaring (bijv. het meer of minder vaak een open standaard in een ICT-product of dienstverlening toegepast hebben) geen adequate geschiktheidseis, ook niet vanuit het oogpunt van proportionaliteit. Het is in veel gevallen beter om uit te gaan van de hiervoor beschreven knock-out geschiktheidseisen. Om die reden zijn er geen voorbeeld-bestekteksten voor selectiecriteria opgenomen.

Dat laat onverlet dat het in specifieke gevallen toch passend kan zijn om een geschiktheidseis voor een open standaard op te nemen. Het is aan de aanbestedende dienst om dat te bepalen.

5.5 **Open standaarden als technische specificatie**

Het opnemen van een open standaard in een bestektekst kwalificeert in aanbestedingsrechtelijke termen als het verwijzen naar technische specificaties conform artikel 2.76 van de Aanbestedingswet 2012.

Een dergelijke verwijzing is in principe toegestaan. Uiteraard mag deze niet strijdig zijn met de beginselen van de AW2012.

Dat betekent onder andere dat deze specificatie objectief toepasbaar en niet discriminatoir mag zijn.

De wet schrijft wel voor dat de aanbestedende partij de zinsnede "of gelijkwaardig" toevoegt aan de formulering van de technische specificatie. Het is daarbij van belang dat de aanbestedende dienst aangeeft hoe de gelijkwaardigheid aangetoond moet worden met passende middelen door de leverancier die hier een beroep op doet.

De aanbestedende dienst kan hiervoor de toetsingscriteria voor opname op de 'pas toe of leg uit'-lijst hanteren en daarbij verwijzen naar achterliggende doelen van interoperabiliteit en leveranciersonafhankelijkheid.

Indien geen criteria opgenomen worden, is een gegadigde/inschrijver vrij in de methode om zelf aan te tonen of de alternatieve standaard 'gelijkwaardig' is.

Omdat een open standaard door alle leveranciers te implementeren is, werkt deze in principe niet discriminerend. Toch kan er in gevallen sprake zijn van alternatieven die ook in de behoeften voorzien. Zo kan een nieuwere versie van een standaard uit de 'pas toe of leg uit'-lijst interoperabel zijn met hetgeen wordt gevraagd. Zoals eerder beschreven, zijn open standaarden op zichzelf niet in strijd met deze algemene beginselen van mededinging.

Gelet op het voorgaande is het bij verwijzing naar een open standaard aan te raden om:
1. De achterliggende ratio, namelijk vergroten van interoperabiliteit én bevorderen van leveranciersonafhankelijkheid, te vermelden.
2. Te vermelden dat de gevraagde standaard is opgenomen op de 'pas toe of leg uit'-lijst en dat eventueel aangeboden 'gelijkwaardige' standaarden ook aan de toetsingscriteria van het Forum Standaardisatie moeten voldoen.

6 Voorbeeld bestekteksten, specifiek per standaard

Dit hoofdstuk bevat voor een paar 'pas toe of leg uit'-standaarden voorbeelden voor gunningseisen (Eis) en gunningscriteria (Wens). Hieronder een begrippenlijst die in de onderdelen van het gebruikte sjabloon staan:

Toepassing
Een verkorte omschrijving van de toepassing op basis van het formele toepassingsgebied op de 'pas toe of leg uit'-lijst. Indien er twee toepassingen zijn, is er een sjabloon per toepassing en wordt de nummering van Toepassing 1, Toepassing 2 etc. aangehouden.

Volledige naam
De volledige naam van de open standaard, inclusief eventuele actuele versie.

Standaardisatie-organisatie
De naam van de organisatie die de open standaard beheert.

Specificatie-document
De online vindplaats (URL) waar het specificatie-document van de open Standaard beschikbaar is. Omwille van de transparantie en de objectiviteit is het aan te raden om in een bestek deze vindplaats ook op te nemen.

ICT-diensten of producten
De categorie uit hoofdstuk 4 waarbij de standaard vaak relevant is.

Onderdelen bestekteksten

Besteksonderdeel	Voorbeeld-bestektekst
Eis	De gunningseis die gesteld kan worden aan de te leveren dienst of product.
Verificatie van de eis	De wijze van verificatie van deze gunningseis.
Wens	De mogelijkheid om bovenop de eis een wens te formuleren die een onderdeel van de EMVI gunning kan zijn; indien een wens op dat gebied doorgaans niet passend is, dan is in het sjabloon 'Geen' opgenomen.
Beoordeling wens	De wijze van beoordeling en verificatie van de reactie van de inschrijver op de wens.
Opmerkingen	Eventuele aanvullende opmerkingen ten behoeve van de voorbeeld-bestekteksten.

6.1 Internet en beveiliging

IPv4 & IPv6 (Internetnummers) voor servers

Toepassing: bereikbaarheid van ICT-systemen, zoals websites, e-mailsystemen en DNS-systemen
Volledige naam: Internet Protocol versie 6 en 4 (RFC2460 en RFC791)
Standaardisatie-organisatie: IETF
Specificatie-document
https://tools.ietf.org/html/rfc2460
https://tools.ietf.org/html/rfc791

Relevante ICT-diensten of producten uit hoofdstuk 4:
- Website of webapplicatie
- E-mail
- Spraak- en/of datacommunicatiediensten
- Netwerken
- En alle overige aan internet te koppelen ICT-systemen, zoals multifunctionals

Besteksonderdeel	Voorbeeld-bestektekst
Eis	Het ICT-systeem biedt volledig werkende ondersteuning voor de open standaarden IPv4 én IPv6 ('dual stack') -zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig. Dit betekent in ieder geval dat: 1. Gebruikers en andere ICT-systemen het ICT-systeem kunnen bereiken via zowel IPv4 als IPv6 zonder dat er sprake is van functionele of non-functionele (bijv. qua prestatie) verschillen. *2.* Configuratiefunctionaliteit voor IP-adressen (bijv. een IP-whitelist) in het ICT-systeem zowel voor IPv4 als IPv6 beschikbaar is.
Verificatie eis	Na opleveren: testresultaat in website- en e-mailtest op https://www.internet.nl
Wens	Beschrijf de wijze van het monitoren en de incidentoplossing die u toepast, zodat het opgeleverde ICT-systeem goed bereikbaar blijft via zowel IPv6 als IPv4.
Beoordeling wens	Hoe beter het monitoren en de incidentoplossing is gewaarborgd door de gegadigde/inschrijver, hoe hoger de score is. Criteria waaraan de invulling van de wens getoetst wordt, moeten objectief bepaalbaar en controleerbaar zijn.

NB: Voor gedetailleerde eisen en wensen m.b.t. IPv6 zie RIPE554 "Requirements for IPv6 in ICT Equipment", ook beschikbaar in het Nederlands via de website van Forum Standaardisatie.
De beschreven wens is met name van belang voor kritieke ICT-systemen. Het is voor kritieke ICT-systemen aan te raden om aanvullend algemene eisen en wensen op te nemen ten aanzien van de beveiliging en de beschikbaarheid.

IPv6 is niet backwards compatible met IPv4. Daarom is het cruciaal om voorlopig beide te ondersteunen.

IPv4 & IPv6 (Internetnummers) voor clients

Naam en versie	**IP versie 6 en 4**
Toepassing	Internetverbinding van cliëntsystemen, zoals desktops, laptops en mobiele apparaten
Volledige naam	Internet Protocol versie 6 en 4 (RFC2460 en RFC791)
Standaardisatie-organisatie	IETF
Specificatie-document	https://tools.ietf.org/html/rfc2460 https://tools.ietf.org/html/rfc791
ICT-diensten of producten	• Werkplek en kantoorsoftware • Netwerken
Besteksonderdeel	**Voorbeeld-bestektekst**
Eis	De internetverbinding van het client-systeem biedt volledig werkende ondersteuning voor de Open Standaarden IPv4 én IPv6 (‘dual stack’) -zoals opgenomen op de ‘pas toe of leg uit’-lijst van Forum Standaardisatie- of daaraan gelijkwaardig. Dit betekent in ieder geval dat gebruikers websites kunnen bezoeken, e-mail kunnen verzenden en ontvangen, en andere ICT-systemen kunnen bereiken zowel via IPv4 als via IPv6 zonder dat er sprake is van functionele of non-functionele (bijv. qua prestatie) verschillen.
Verificatie eis	Na opleveren: testresultaat voor IPv6 in internetverbinding-test op https://www.internet.nl
Wens	Beschrijf de wijze van monitoring en incidentoplossing die u toepast zodat cliëntsystemen goed bereikbaar blijven via zowel IPv6 als IPv4.
Beoordeling wens	Hoe beter de monitoring en incidentoplossing is gewaarborgd door de gegadigde/inschrijver, hoe hoger de score is. Criteria waaraan de invulling van de wens getoetst wordt, moeten objectief bepaalbaar en controleerbaar zijn.
Opmerkingen	De beschreven wens is met name van belang voor kritieke ICT-systemen. Het is voor kritieke ICT-systemen aan te raden om aanvullend algemene eisen en wensen op te nemen ten aanzien van de beveiliging en de beschikbaarheid.

DNSSEC (Domeinnaambeveiliging)

Ondertekening

Naam en versie	**DNSSEC**
Toepassing	Digitale ondertekening van eigen domeinnaaminformatie
Volledige naam	Domain Name System Security Extensions (RFC4033, RFC4034, RFC4035 en verder)
Standaardisatie-organisatie	IETF
Specificatie-document	https://datatracker.ietf.org/doc/rfc4033/ e.v.
ICT-diensten of producten	Website of webapplicatie E-mail Spraak- en/of datacommunicatiediensten Netwerken Alle overige aan internet te koppelen ICT-systemen
Besteksonderdeel	**Voorbeeld-bestektekst**
Eis	De domeinnaam van het ICT-systeem biedt volledig werkende ondersteuning voor de Open Standaard DNSSEC -zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig. Dit betekent dat de domeinnaaminformatie, zoals bijbehorende IP-adressen, met een geldige DNSSEC-handtekening is ondertekend.
Verificatie eis	Na opleveren: testresultaat voor DNSSEC-ondertekening in website- en e-mailtest op https://www.internet.nl.
Wens	Beschrijf uw beheerprocedure om de betrouwbaarheid en beschikbaarheid van de ondertekening met de Open Standaard DNSSEC of gelijkwaardig te waarborgen.
Beoordeling wens	Het beoordelingskader voor dit criterium is RFC6781 "DNSSEC Operational Practices, Version 2" van IETF of vergelijkbaar.
Opmerkingen	De beschreven wens is met name van belang voor kritieke ICT-systemen. Het is voor kritieke ICT-systemen aan te raden om aanvullend algemene eisen en wensen op te nemen ten aanzien van de beveiliging en de beschikbaarheid.

Validatie

Naam en versie	DNSSEC
Toepassing	Validatie van digitale handtekening van opgevraagde domeinnamen
Volledige naam	Domain Name System Security Extensions (RFC4033, RFC4034, RFC4035 en verder)
Standaardisatie-organisatie	IETF
Specificatie-document	https://datatracker.ietf.org/doc/rfc4033/ e.v.
ICT-diensten of producten	Werkplek en kantoorsoftware Netwerken
Besteksonderdeel	**Voorbeeld-bestektekst**
Eis	De opvragende DNS-software (resolver) biedt volledig werkende ondersteuning voor validatie c.q. verificatie van handtekeningen conform de Open Standaard DNSSEC -zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig. Dit betekent dat de DNSSEC-handtekeningen van opgevraagde domeinnamen worden gevalideerd.
Verificatie eis	Na opleveren: testresultaat voor DNSSEC-validatie in internetverbinding-test op https://www.internet.nl.
Wens	Beschrijf uw procedure voor het omgaan met validatie-fouten van met DNSSEC ondertekende domeinnamen (bijv. afhandeling vragen eindgebruikers en inzet zogenaamde "Negative Trust Anchors").
Beoordeling wens	Het beoordelingskader voor dit criterium is RFC7646 "Definition and Use of DNSSEC Negative Trust Anchors" van IETF.
Opmerkingen	Het is voor kritieke ICT-systemen aan te raden om algemene eisen en wensen op te nemen ten aanzien van de beveiliging en de beschikbaarheid.

TLS (Beveiligde verbinding)

Naam en versie	**TLS versie 1.3 én 1.2**
Toepassing	TLS moet worden toegepast op de uitwisseling van gegevens tussen clients en servers, inclusief machine-to-machine communicatie. .
Volledige naam	Transport Layer Security (RFC5246)
Standaardisatie-organisatie	IETF
Specificatie-document	http://datatracker.ietf.org/doc/rfc5246/
ICT-diensten of producten	Website of webapplicatie E-mail Spraak- en/of datacommunicatiediensten
Besteksonderdeel	**Voorbeeld-bestektekst**
Eis	Het ICT-systeem (bijv. de website) biedt volledig werkende ondersteuning voor beveiligde verbindingen conform de Open Standaard TLS (versie 1.3 én 1.2) -zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig. Dit betekent dat: 1. er een geldig (PKIoverheid-)certificaat is geïnstalleerd op het ICT-systeem; 2. op basis waarvan andere systemen een TLS-verbinding kunnen opzetten met dit ICT-systeem; 3. waarvan de veiligheid van de TLS-configuratie voldoet aan de "ICT-beveiligingsrichtlijnen voor TLS" van NCSC; 4. en in geval van een website zowel het TLS protocol als het HTTPS protocol een veilige configuratie hebben.
Verificatie eis	Na opleveren: testresultaat voor TLS in website- of e-mailtest op https://www.internet.nl.
Wens	Beschrijf uw beheerprocedure om 1. het PKI overheid-certificaat veilig te beheren tijdig te vernieuwen; 2. de correcte en veilige werking van de TLS-verbinding te monitoren en incidenten op te lossen.
Beoordeling wens	Ad 1: Het beoordelingskader hiervoor is de factsheet "Veilig beheer van digitale certificaten" van NCSC of vergelijkbaar. Ad 2: Hoe beter de monitoring en incidentoplossing is gewaarborgd door de gegadigde/inschrijver, hoe hoger de score is. Criteria waaraan de invulling van de wens getoetst wordt, moeten objectief bepaalbaar en controleerbaar zijn.
Opmerkingen	Controleer na het inkoopmoment regelmatig met behulp van beschikbare validatie-tools, zoals Internet.nl, of TLS 1.3 en TLS 1.2 nog worden toegepast en controleer ook de veilige configuratie daarvan aan de hand van de geactualiseerde TLS-richtlijnen van NCSC.

DKIM (Anti-phishing)

Naam en versie	**DKIM versie 1**
Toepassing	Digitale ondertekening van mails door verzender zodat ontvanger de authenticiteit en integriteit van de mail kan vaststellen. DKIM is complementair aan de Open Standaard SPF.
Volledige naam	DomainKeys Identified Mail (DKIM) Signatures (RFC6376)
Standaardisatie-organisatie	IETF
Specificatie-document	https://tools.ietf.org/html/rfc6376
ICT-diensten of producten	E-mail
Besteksonderdeel	**Voorbeeld-bestektekst**
Eis	De e-mailvoorziening biedt volledig werkende ondersteuning voor DKIM versie 1-zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig. Dit betekent dat: 1. op het systeem een publiek/privaat sleutelpaar is gegenereerd of kan worden gegenereerd; 2. de publieke DKIM-sleutel is gepubliceerd in de DNS van de e-maildomeinnaam; 3. alle uitgaand e-mailberichten worden ondertekend met de private DKIM-sleutel; 4. alle inkomende e-mailberichten worden gecontroleerd op de geldigheid van een eventuele DKIM-handtekening en het systeem hieraan mogelijke acties verbindt.
Verificatie eis	Na opleveren: testresultaat voor DKIM in e-mailtest op https://www.internet.nl, https://www.mail-tester.com of via de tools op https://dmarc.org/resources/deployment-tools/.
Wens	Beschrijf uw beheerprocedure om: 1. de DKIM-sleutels veilig te genereren, te beheren en te vernieuwen; en 2. de correcte werking van DKIM te monitoren zowel voor inkomende als uitgaande e-mail.
Beoordeling wens	Het beoordelingskader hiervoor is de NCSC-factsheet "Factsheet Bescherm domeinnamen tegen phishing" en de relevante Best Practices van M3AAWG (m.n. "DKIM Key Rotation Best Common Practices" en "Best Practices for Implementing DKIM To Avoid Key Length Vulnerability").
Opmerkingen	Het is voor kritieke ICT-systemen aan te raden om algemene eisen en wensen op te nemen ten aanzien van de beveiliging en de beschikbaarheid.

SPF (Anti-phishing)

Naam en versie	**SPF versie 1**
Toepassing	Het controleren of een e-mailserver gerechtigd is om namens een domeinnaam e-mail te mogen verzenden. SPF is complementair aan de Open Standaard DKIM.
Volledige naam	Sender Policy Framework (RFC7208)
Standaardisatie-organisatie	IETF
Specificatie-document	https://tools.ietf.org/html/rfc7208
ICT-diensten of producten	• E-mail
Besteksonderdeel	**Voorbeeld-bestektekst**
Eis	De e-mailvoorziening biedt volledige ondersteuning voor de open standaard SPF versie 1 -zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig. Dit betekent dat: 1. de IP-adressen van de verzendende systemen als SPF-record worden geregistreerd in de DNS van de verzendende domeinnaam; 2. alle inkomende e-mailberichten worden gecontroleerd op de geldigheid van het verzendend IP-adres tegen het IP-adres dat in SPF-record staat van de verzendende domeinnaam.
Verificatie eis	Na opleveren: testresultaat voor SPF in e-mailtest op https://www.internet.nl, https://www.mail-tester.com of via de tools op https://dmarc.org/resources/deployment-tools/.
Wens	Beschrijf uw beheerprocedure om: 1. de SPF-records te genereren en indien nodig aan te passen, en 2. de correcte werking van SPF te monitoren zowel voor inkomende als uitgaande e-mails.
Beoordeling wens	Het beoordelingskader hiervoor is de NCSC-factsheet "Factsheet Bescherm domeinnamen tegen phishing" .
Opmerkingen	Het is voor kritieke ICT-systemen aan te raden om algemene eisen en wensen op te nemen ten aanzien van de beveiliging en de beschikbaarheid.

SAML (Inloggegevens)

Naam en versie	SAML versie 2.0
Toepassing	Eenmalig inloggen (en uitloggen) waardoor een gebruiker via zijn/haar browser toegang heeft tot verschillende webdiensten. Onder andere DigiD en eHerkenning maken gebruik van SAML voor het koppelvlak met aangesloten organisaties.
Volledige naam	Security Assertion Markup Language
Standaardisatie-organisatie	OASIS
Specificatie-document	http://www.oasis-open.org/committees/security/
ICT-diensten of producten	• Website of webapplicatie
Besteksonderdeel	**Voorbeeld-bestektekst**
Eis	Het ICT-systeem biedt volledig werkende ondersteuning van SAML versie 2.0 -zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig, zodat gebruikers via eenmalig in- en uitloggen veilige toegang hebben tot verschillende gekoppelde webdiensten.
Verificatie eis	• Akkoordverklaring eventueel met toelichting hoe hij borgt dat zijn ICT-systeem aan deze standaard voldoet. • Succesvol doorlopen van Interoperability Certification Program van Kantara of vergelijkbaar (http://kantarainitiative.org/confluence/display/certification/Interoperability+Program). • Na oplevering:Volledig werkende aansluiting op systeem zoals DigiD en eHerkenning indien dat het doel is.
Wens	Geen
Beoordeling wens	Geen
Opmerkingen	Het is voor kritieke ICT-systemen aan te raden om algemene eisen en wensen op te nemen ten aanzien van de beveiliging en de beschikbaarheid.

ISO 27001 (Managementsysteem informatiebeveiliging)

Naam en versie	**ISO 27001 versie 2013**
Toepassing	Eisen voor een managementsysteem informatiebeveiliging.
Volledige naam	27001: Praktijkrichtlijn met beheersmaatregelen op het gebied van informatiebeveiliging (NEN-ISO/IEC 27001:2013 nl)
Standaardisatie-organisatie	NEN-ISO/IEC
Specificatie-document	https://www.nen.nl/NEN-Shop/Norm/NENISOIEC-270012013C112014-nl.htm
ICT-diensten of producten	Alle ICT-systemen/-diensten, met name die met privacy- en/of bedrijfs-gevoelige informatie.
Besteksonderdeel	**Voorbeeld-bestektekst**
Eis	De gegadigde/inschrijver heeft een managementsysteem informatiebeveiliging in werking voor te leveren ICT-systeem/-dienst conform de Open Standaard NEN-ISO/IEC 27001:2013- zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig, zoals de BIO.
Verificatie eis	• Akkoordverklaring eventueel met toelichting hoe hij borgt dat zijn ICT-systeem/-dienst aan deze standaard voldoet. • Certificaat betreffende te leveren ICT-systeem/-dienst inzake conformiteit met NEN-ISO/IEC 27001:2013 dat is verstrekt door een RvA-geaccrediteerde organisatie, of een gelijkwaardig certificaat.
Wens	Geen
Beoordeling wens	Geen
Opmerkingen	Afhankelijk van het product dat wordt gevraagd kan het voldoen aan ISO/IEC 27001 worden aangetoond door een certificaat te overleggen. Het kan gezien de marktsituatie te zwaar zijn om van alle gegadigden/inschrijvers vooraf volledige certificatie te vragen. Een en ander is tevens afhankelijk van de risico-inschatting van de gegevensverwerking en de aard van de dienstverlening.

ISO 27002 (Richtlijnen en principes informatiebeveiliging)

Naam en versie	**ISO 27002 versie 2013**
Toepassing	'Best practices' voor het nemen van maatregelen op het gebied informatiebeveiliging.
Volledige naam	27002: Praktijkrichtlijn met beheersmaatregelen op het gebied van informatiebeveiliging (NEN-ISO/IEC 27002:2013 nl)
Standaardisatie-organisatie	NEN-ISO/IEC
Specificatie-document	https://www.nen.nl/NEN-Shop/Norm/NENISOIEC-270022013C22015-nl.htm
ICT-diensten of producten	Alle ICT-systemen/-diensten, met name die met privacy- en/of bedrijfs-gevoelige informatie.
Besteksonderdeel	**Voorbeeld-bestektekst**
Eis	De gegadigde/inschrijver heeft voor te leveren ICT-systeem/-dienst beheersmaatregelen op het gebied van informatiebeveiliging in werking die zijn gebaseerd op de Open Standaard NEN-ISO/IEC 27002:2013 -zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig, zoals de BIO.
Verificatie eis	Akkoordverklaring eventueel met toelichtende beschrijving van getroffen beheersmaatregelen in relatie tot ISO 27002.
Wens	Geen
Beoordeling wens	Geen
Opmerkingen	Voldoen aan het gestelde in de Baseline informatiebeveiliging Overheid (BIO) kan aanbestedingsrechtelijk als gelijkwaardig aan ISO 27002 worden beschouwd. Het is van belang dat een aanbestedende dienst zelf een scherp beeld heeft van mogelijke risico's en noodzakelijke maatregelen, en op basis daarvan meer specifieke eisen en wensen opneemt naast de algemene verwijzing naar ISO 27002 of naar de Baseline Informatiebeveiliging Overheid.

HTTPS en HSTS

Begrip	**HTTPS & HSTS**
Toepassing	HTTPS en HSTS moeten worden toegepast op de communicatie tussen clients (zoals webbrowsers) en servers voor alle websites en webservices. HTTPS zorgt voor het gebruik van HTTP over een met TLS beveiligde verbinding. Dit betekent dat het webverkeer door middel een certificaat wordt versleuteld. HSTS zorgt ervoor dat een webbrowser, na het eerste contact over HTTPS, bij vervolgbezoek de website altijd direct over HTTPS opvraagt.
Volledige naam	HyperText Transfer Protocol Secure (HTTPS) en HTTP Strict Transport Security (HSTS)
Standaardisatie-organisatie	IETF
Specificatie-document	https://datatracker.ietf.org/doc/rfc2818/ https://tools.ietf.org/html/rfc6797
ICT-diensten of producten	• Website of webapplicatie • E-HRM systemen • Netwerken
Besteksonderdeel	**Voorbeeld-bestektekst**
Eis	Het ICT Systeem biedt volledig werkende ondersteuning voor HTTPS en HSTS -zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig.
Verificatie van de eis	• Akkoordverklaring eventueel met toelichting hoe hij borgt dat zijn ICT-systeem aan standaard voldoet. • Testresultaten van validatietooling voor HTTPS en HSTS zoals www.internet.nl en https://www.ssllabs.com/ssltest/
Wens	Geen
Beoordeling wens	Geen
Opmerkingen	

DMARC

Begrip	**DMARC**
Toepassing	DMARC maakt het mogelijk om beleid in te stellen over de manier waarop een e-mailprovider om moet gaan met e-mail waarvan niet kan worden vastgesteld dat deze afkomstig is van het vermelde afzenderdomein. Hierdoor kunnen organisaties voorkomen dat anderen e-mails versturen namens het e-maildomein van de organisatie. DMARC moet worden toegepast op alle overheidsdomeinnamen, ook op domeinen waarvan niet wordt gemaild, én op alle mailservers waarmee de overheid e-mail ontvangt.
Volledige naam	Domain-based Message Authentication, Reporting, and Conformance
Standaardisatie-organisatie	IETF
Specificatie-document	https://datatracker.ietf.org/doc/rfc7489/
ICT-diensten of producten	• E-mail
Besteksonderdeel	**Voorbeeld-bestektekst**
Eis	De e-mailvoorziening biedt volledig werkende ondersteuning voor DMARC -zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig.
Verificatie van de eis	• Akkoordverklaring eventueel met toelichting hoe hij borgt dat zijn ICT-systeem aan standaard voldoet. • Testresultaten van validatietooling voor DMARC zoals www.internet.nl, https://www.mail-tester.com of via de tools op https://dmarc.org/resources/deployment-tools/.
Wens	Geen
Beoordeling wens	Geen
Opmerkingen	Geen

Starttls/Dane

Begrip	**Starttls/Dane**
Toepassing	Mailverkeer tussen mailservers verloopt via SMTP. STARTTLS in combinatie met DANE gaan, in aanvulling op SMTP, afluisteren of manipuleren van dit mailverkeer door internetcriminelen tegen. Beide standaarden moeten in combinatie worden toegepast op ontvangende en verzendende e-mailservers.
Volledige naam	STARTTLS en DANE
Standaardisatie-organisatie	IETF
Specificatie-document	https://tools.ietf.org/html/rfc3207 https://tools.ietf.org/html/rfc7672
ICT-diensten of producten	• E-mail
Besteksonderdeel	**Voorbeeld-bestektekst**
Eis	De e-mailvoorziening biedt volledige ondersteuning voor de Open Standaard STARTTLS en DANE -zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig.
Verificatie van de eis	• Akkoordverklaring eventueel met toelichting hoe hij borgt dat zijn ICT-systeem aan standaard voldoet. • Testresultaten van validatietooling voor STARTTLS/DANE zoals www.internet.nl
Wens	Geen
Beoordeling wens	Geen
Opmerkingen	Organisaties die STARTTLS en DANE toepassen worden opgeroepen de standaarden te implementeren volgens de adviezen van het NCSC.

6.2 **Documenten en (web)content**

PDF/A (Formaat documentpublicatie / archivering)

Naam en versie	**PDF/A-1 en PDF/A-2**
Toepassing	Voor publicatie of archivering van documenten waarbij toegankelijkheid nu en in de toekomst van belang is. PDF/A is een gestandaardiseerde versie van PDF. Op de 'pas toe of leg uit'-lijst staat PDF als overkoepelende standaard genoemd.
Volledige naam	Portable Document Format Archivable (NEN-ISO 19005-1:2005 en NEN-ISO 19005-2:2011)
Standaardisatie-organisatie	NEN-ISO
Specificatie-document	https://www.nen.nl/NEN-Shop/Norm/NENISO-1900512005-en.htm https://www.nen.nl/NEN-Shop/Norm/NENISO-1900522011-en.htm
ICT-diensten of producten	• Website of webapplicatie • Werkplek en kantoorsoftware • Multi-functionals
Besteksonderdeel	**Voorbeeld-bestektekst**
Eis	1. Het te leveren ICT-systeem (bijv. webapplicatie) kan documenten genereren/beheren/publiceren in een formaat conform de Open Standaard PDF/A -zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig. 2. Met het te leveren kantoorsoftwarepakket kan de gebruiker documenten bekijken en/of creëren in een formaat conform de Open Standaard PDF/A -zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig. 3. Met de te leveren multi-functional kan de gebruiker scans maken en vastleggen in een formaat conform de Open Standaard PDF/A -zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig.
Verificatie eis	• Akkoordverklaring eventueel met toelichting hoe hij borgt dat zijn ICT-systeem aan standaard voldoet. • Testresultaten van validatietooling voor PDF/A zoals VeraPDF (https://verapdf.org), Adobe Preflight en tooling op https://forumstandaardisatie.nl/pdfa.
Wens	Geen
Beoordeling wens	Geen
Opmerkingen	Voor meer achtergrond zie de informatie over open documentformaten op de website van Forum Standaardisatie (https://www.forumstandaardisatie.nl/opendoc).

PDF 1.7 (Formaat documentpublicatie)

Naam en versie	**PDF 1.7**
Toepassing	Voor publicatie van documenten met dynamische content waarbij (duurzame) toegankelijkheid minder van belang is. PDF1.7 gestandaardiseerde versie van PDF. Deze versie is rijker qua functionaliteit dan PDF/A. Dit kan echter ten koste gaan van de interoperabiliteit. Daarom dient PDF1.7 alleen ingezet te worden als de functionaliteit van PDF/A tekortschiet. Op de 'pas toe of leg uit'-lijst staat PDF als overkoepelende standaard genoemd.
Volledige naam	Portable document format -- Part 1: PDF 1.7
Standaardisatie-organisatie	ISO
Specificatie-document	http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=51502
ICT-diensten of producten	• Website of webapplicatie • Werkplek en kantoorsoftware • Multi-functionals

Besteksonderdeel	**Voorbeeld-bestektekst**
Eis	1. Het te leveren ICT-systeem (bijv. webapplicatie) kan documenten genereren/tonen/beheren/publiceren in een formaat conform de Open Standaard PDF1.7 -zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig. 2. Met het te leveren kantoorsoftwarepakket kan de gebruiker documenten bekijken en/of creëren in in een formaat conform de Open Standaard PDF1.7 -zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig. 4. Met de te leveren multi-functional kan de gebruiker scans maken en vastleggen in een formaat conform de Open Standaard PDF1.7 -zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig.
Verificatie eis	• Akkoordverklaring eventueel met toelichting hoe hij borgt dat zijn ICT-systeem aan deze standaard voldoet. • Testresultaten van validatietooling voor PDF1.7 zoals Adobe Preflight.
Wens	Geen
Beoordeling wens	Geen
Opmerkingen	Voor meer achtergrond zie de informatie over open documentformaten op de website van Forum Standaardisatie (https://www.forumstandaardisatie.nl/opendoc).

ODF (Formaat documentbewerking)

Naam en versie	**ODF versie 1.2**
Toepassing	Voor het publiceren of uitwisselen van documenten (tekst, rekenbladen en presentatie) in bewerkbare vorm, zodat de ontvanger aanpassingen en toevoegingen kan doen.
Volledige naam	Open Document Formaat
Standaardisatie-organisatie	OASIS en ISO
Specificatie-document	https://www.oasis-open.org/committees/office/ http://standards.iso.org/ittf/PubliclyAvailableStandards/
ICT-diensten of producten	• Website of webapplicatie • Werkplek en kantoorsoftware • Multi-functionals
Besteksonderdeel	**Voorbeeld-bestektekst**
Eis	1. Het te leveren ICT-systeem (bijv. webapplicatie) kan documenten genereren/tonen/beheren/publiceren in ODF versie 1.2 -zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig. 2. Met het te leveren kantoorsoftwarepakket kan de gebruiker documenten bekijken en/of creëren in een formaat conform de Open Standaard ODF versie 1.2 -zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig. 3. Met de te leveren multi-functional kan de gebruiker scans maken en vastleggen in een formaat conform de Open Standaard ODF versie 1.2 -zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig.
Verificatie eis	• Akkoordverklaring eventueel met toelichting hoe hij borgt dat zijn ICT-systeem aan deze standaard voldoet. • Testresultaten van validatietooling voor ODF zoals ODF Validator (http://odf-validator.rhcloud.com/), ODFAutoTests (http://autotests.opendocumentformat.org/). Zie ook: https://www.gov.uk/government/publications/open-document-format-odf-validators-and-compliance-testing.
Wens	Geen
Beoordeling wens	Geen
Opmerkingen	Voor meer achtergrond zie de informatie over open documentformaten op de website van Forum Standaardisatie (https://www.forumstandaardisatie.nl/opendoc). Een wijdverbreid misverstand is dat ODF alleen ondersteund wordt door alternatieve office-pakketten zoals LibreOffice en OpenOffice. Dat klopt niet. Microsoft Office en Google Docs bieden ook ODF-ondersteuning. Over het algemeen geldt dat recentere software-versies betere ondersteuning bieden ten behoeve van ODF.

Digitoegankelijk

Naam en versie	**Digitoegankelijk (EN 301549 met WCAG 2.1)**
Toepassing	Inkoop, ontwerpen, bouwen en beheren van toegankelijke websites en webapplicaties. De richtlijnen zijn gebaseerd op Europese en internationale standaarden (met name EN 301 549 en WCAG2.1), en op in de praktijk beproefde oplossingen van professionals. Ze zijn van toepassing op alle webcontent dus bijvoorbeeld ook op gepubliceerde en nog te publiceren documenten.
Volledige naam	Digitoegankelijk
Standaardisatie-organisatie	ETSI
Specificatie-document	www.digitoegankelijk.nl
ICT-diensten of producten	• Website of webapplicatie
Besteksonderdeel	**Voorbeeld-bestektekst**
Eis	1. De op te leveren website voldoet aantoonbaar aan de toegankelijkheidsrichtlijnen van Digitoegankelijk -zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig. 2. Het op te leveren document voldoet aantoonbaar aan de toegankelijkheidsrichtlijnen van Digitoegankelijk -zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig
Verificatie eis	• Akkoordverklaring eventueel met toelichtende beschrijving van specifieke situaties en uitzonderingen op basis van digitoegankelijk.nl/beleid/specifieke-situaties. • Handmatig onderzoek en advies door een toegankelijkheidsexpert. • Automatisch onderzoek is deels geschikt omdat niet alle aspecten van WCAG 2.1 automatisch getoetst kunnen worden maar wel geschikt voor indicatief beeld: http://checkers.eiii.eu/
Wens	Geen
Beoordeling wens	Geen
Opmerkingen	• Digitoegankelijk (EN 301 549 met WCAG 2.1) vervangt Webrichtlijnen 2.0 op de pas-toe-of-leg-uit lijst sinds oktober 2016. Zowel Digitoegankelijk als Webrichtlijnen baseren zich op de technische toegankelijkheidsstandaard WCAG 2.1 van W3C, alleen gaat Digitoegankelijk uit van de Europese Norm EN 301 549 die ook instructies voor inkoop beschrijft. • Zie aanvullend 'EN 301 549 - Accessibility requirements suitable for public procurement of ICT products and services in Europe' van CEN, CENELEC en ETSI (http://www.etsi.org/deliver/etsi_en/301500_301599/301549/01.01.01_60/en_301549v010101p.pdf).

SKOS (Thesauri en begrippenwoordenboeken)

Naam en versie	**SKOS**
Toepassing	Ordenen en publiceren van kennissystemen (Knowledge Organization Systems), zoals thesauri, classificatieschema's en taxonomieën, binnen de context van het semantisch web en (linked) open data.
Volledige naam	Simple Knowledge Organization System (W3C Recommendation 18 August 2009)
Standaardisatie-organisatie	W3C
Specificatie-document	https://www.w3.org/TR/skos-reference/
ICT-diensten of producten	• Website of webapplicatie • Werkplek en kantoorsoftware
Besteksonderdeel	**Voorbeeld-bestektekst**
Eis	Het ICT-systeem biedt volledig werkende ondersteuning voor de Open Standaard SKOS -zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig.
Verificatie eis	• Akkoordverklaring eventueel met toelichting hoe hij borgt dat zijn ICT-systeem aan deze standaard voldoet. • Testresultaten van validatietooling zoals vindbaar op https://www.w3.org/2004/02/skos/validation.
Wens	Geen
Beoordeling wens	Geen
Opmerkingen	SKOS bouwt voort op de Linked Data Standaarden (RDF, RDFS, OWL). Naarmate de LD-standaarden breder toegepast worden en de hoeveelheid op LD-gebaseerde standaarden toeneemt, ontstaan er steeds meer toepassingsmogelijkheden voor SKOS-gebaseerde vocabulaires. SKOS-vocabulaires gaan in toenemende mate het hart vormen van semantische interoperabiliteit.

Open API specification (beschrijven van REST APIs)

Naam en versie	**Open API Specification 3.0**
Toepassing	OAS moet worden toegepast op het beschrijven en specificeren van een REST API
Volledige naam	OpenAPI Specification
Standaardisatie-organisatie	OpenAPI Initiative
Specificatie-document	https://github.com/OAI/OpenAPI-Specification/blob/master/versions/3.0.1.md
ICT-diensten of producten	Alle ICT-systemen/-diensten indien er gebruik wordt gemaakt van een REST API.
Besteksonderdeel	**Voorbeeld-bestektekst**
Eis	De eigenschappen van benodigde API's dienen in mee te leveren documentatie beschreven te zijn conform de OpenAPI Specification
Verificatie van de eis	• Akkoordverklaring eventueel met toelichting hoe hij borgt dat de documentatie aan deze standaard voldoet
Wens	Geen
Beoordeling wens	Geen
Opmerkingen	Met OAS 3.0 kunnen zowel mensen als machines de dataset attributen van een REST API vinden, bekijken en verwerken zonder toegang tot de programmatuur en zonder aanvullende documentatie. OAS 3.0 is zowel compatibel met de voorgaande versie OAS 2.0 als met de alternatieve standaard RAML (RESTful API Modeling Language) die ook veel gebruikt werd. Het Deelprogramma Digitaal Stelsel Omgevingswet gebruikt OAS 2.0 en OAS 3.0.

7 Leg uit

7.1 Met een geldige reden in het jaarverslag

Overheidsorganisaties mogen alleen afwijken van de toepasing van de 'pas toe of leg uit'-standaarden op twee voorwaarden: Het moet ten eerste gaan om reden van bijzonder gewicht en ten tweede moet die reden terug te vinden zijn in het jaarverslag.

Om hieraan te kunnen voldoen is het belangrijk dat reden wordt vastgelegd in het aanbestedingsdossier en de tweede om deze aan te bieden voor opname in het jaarverslag.

Geldige redenen om een 'pas toe of leg uit'- standaard niet te gebruiken kunnen zijn:

- onvoldoende aanbod van de standaard door de markt,
- onvoldoende veiligheid van de standaard,
- onvoldoende zekerheid bij het functioneren van de standaard,
- of een andere andere redenen van bijzonder gewicht.

De vermelding in het jaarverslag is voor rijksoverheidsorganisaties geregeld in de bijlage van de instructie rijksdienst bij aanschaf van ICT-diensten en ICT-producten artikel 3 en 4, die in samenhang moet worden gelezen met de bedrijfsvoeringsparagraaf van de Rijksbegrotingsvoorschriften, model 3.24.

Elementen die in het jaarverslag terug moeten komen zijn:

1. om welke aanschaf het nalaten van de relevante standaarden betrekking heeft,
2. welke standaarden hiervoor relevant waren maar achterwege zijn gelaten,
3. met welke reden deze standaarden achterwege zijn gelaten.

In algemene zin verklaren over al dan niet voldoen aan het 'pas toe of leg uit'- beleid of over open standaarden is mooi maar niet niet specifiek genoeg.

7.2 Uitleggen en de Monitor Open Standaarden

Via de Monitor Open Standaarden voert het Forum Standaardisatie jaarlijks onderzoek uit naar het gebruik van de standaarden op de 'pas toe of leg uit'-lijst. Hiertoe worden ook openbare aanbestedingsdocumenten en jaarverslagen onderzocht.

Sinds 2018 publiceert het Forum Standaardisatie de onderzoeksresultaten van het onderzoek naar de aanbestedingsdocumenten in een bijlage bij de Monitor Open Standaarden. Hierin staan alle onderzochte aanbestedingen met de standaarden die gevraagd zijn en de standaarden die niet gevraagd zijn en waar dus een uitleg verwacht mag worden.

De onderzoekers van de Monitor Open Standaarden sturen een e-mail naar de contactpersonen van alle aanbestdingen die zij onderzoeken. Als de aanbesteding wordt

beoordeeld, ontvangt de contactpersoon bericht met de vraag om uit te leggen waarom sommige standaarden achterwege zijn gelaten. Vaak is dit het geval.

De redenen kunnen in overleg met de aanbestedende dienst in aanmerking komen voor publicatie in de Monitor Open Standaarden, de beoordeling beïnvloeden en in de Monitor Open Standaarden gepubliceerd worden.

Het geven van een uitleg naar aanleiding van de Monitor Open Standaarden zou in de toekomst wellicht beter kunnen werken. Het zou meer nuttige informatie op kunnen leveren en meer bewustwording kunnen genereren in de praktijk dan een geldige reden opnemen in het jaarverslag. Dit is echter nog niet de officiële weg.