Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Praktische kaders bij ICT-gerelateerde aanschaffen

Versie 0.10

Datum 15-04-14
Status Concept

Colofon

Projectnaam	Bevordering adoptie open standaarden bij inkoop
Projectnummer	
Versienummer	0.10
Locatie	
Projectleiders	Bart Knubben
Contactpersoon	Bart Knubben Senior Adviseur Open Standaarden bart.knubben@logius.nl Logius | Bureau Forum Standaardisatie Rijkskantoor Beatrixpark | Wilhelmina van Pruisenweg 52 | 2595 AN Den Haag
Auteurs	Walter van Holst

Inhoud

Inleiding

Dit document bevat een beknopte handreiking voor inkopers en andere betrokkenen bij aanbestedingen om vast te stellen welke open standaarden uitgevraagd moeten worden. Het is nadrukkelijk geen uitputtende, alles dekkende, handleiding om de eenvoudige reden dat dit eerder het kennisdomein van IT-architecten raakt dan dat van de inkoopfunctie in overheidsorganisaties. Het bevat een reeks van vuistregels en beslisbomen die de inkoper in staat moet stellen een inschatting te maken in hoeverre een aanbesteding extra aandacht verdient om aan de Rijksinstructie inzake aanschaf van ICT-diensten en -producten (zie kader) te kunnen voldoen. Die aandacht kan bestaan uit het doen van aanpassingen in het bestek of door het opnemen van een uitleg in het jaarverslag van de aanbestedende dienst. In het geval de aanbestedende dienst tot de Rijksoverheid gerekend wordt zal dit conform de Rijksbegrotingsvoorschriften 2013 plaats moeten vinden. Deze zijn te vinden op http://rbv.minfin.nl/2013/modellen/verantwoording/3-24-bedrijfsvoeringsparagraaf

De Rijksinstructie verplicht om bij verwervingen van ICT-middelen te kiezen voor die aanbiedingen die conform de toepasselijke open standaarden van de lijst van het College Standaardisatie werken, als deze verwervingen de ICT-middelen raken en een grotere besteding dan 50.000 Euro vergen. Dit tenzij er een zwaarwegende reden bestaat om dit niet te doen. In dat geval dient er uitleg plaats te vinden in de jaarverslaggeving.

Door middel van bestuurlijke akkoorden geldt dit tevens voor provincies, waterschappen en gemeenten.

Tekst Rijksinstructie: https://zoek.officielebekendmakingen.nl/stcrt-2008-837.html

Primaire doelstelling is om de dialoog tussen de inkoop- en ICT-functies binnen de overheid te verbeteren op dit terrein en de inkoopfunctie te ondersteunen bij hun rol om te waarborgen dat er voldaan wordt aan alle (beleids-)regels bij het inkoopproces.

1.1 Structuur en leeswijzer

Dit document heeft de volgende structuur:

- Als eerste wordt een hulpmiddel gegeven om de vraag óf standaarden van de 'pas toe of leg uit'-lijst van het College Standaardisatie een rol spelen te kunnen beantwoorden;
- Vervolgens wordt aan de hand van een lijst van 'typische' aanbestedingen aangegeven wélke koppelvlakken en daarmee standaarden wellicht aan de orde zijn. Daarbij wordt de volgende paragraafstructuur gehanteerd:
  - typering van het product of de productgroep;
  - beschrijving van het functioneel domein;
  - voorzienbaar relevante koppelvlakken;
  - standaarden relevant voor deze koppelvlakken, gesplitst in:
    - standaarden van de verplichte 'pas toe of leg uit'-lijst;
    - facultatieve, maar veelgebruikte standaarden;
  - selectie-eisen en -wensen, met iedere keer:
    - een toelichting die geschikt is om opgenomen te worden in een programma van eisen; en
    - een ratio bedoeld voor interne beraadslagingen over dit onderwerp.
  - gunningseisen en -wensen;
  - meetinstrumenten, indien beschikbaar, voor de toetsing achteraf of er ook conform de eisen en -wensen geleverd is.

- Tot slot wordt aangegeven hoe aanbestedingen waarbij bewust wordt afgeweken van de 'pas toe of leg uit'-lijst uitgelegd moeten worden bij de jaarverslaggeving.

Bij het opstellen van deze bestekteksten hebben wij een inschatting gemaakt welke vragen beter als eis of als wens kunnen fungeren, bij daadwerkelijke toepassing van deze teksten kan een aanbestedende dienst hierover uiteraard een eigen afweging maken. Tenzij anders aangegeven zijn de eisen en wensen naast elkaar hanteerbaar, in sommige gevallen is er sprake van alternatieve voorbeelden. De gegeven toelichtingen lenen zich in beginsel voor opname in het bestek, de gegeven ratio's zijn vooral bedoeld voor de interne besluitvorming

1.2 Aanbestedingsrechtelijke aspecten

1.2.1 Algemeen

Hoewel het 'pas-toe-of-leg-uit'-beleid van toepassing is op alle ICT-bestedingen, dus ook die waar geen onderhands of Europees aanbestedingstraject aan voorafgaat, speelt het Europees aanbestedingsrecht uiteraard vaak een rol. In deze paragraaf een aantal aandachtspunten vanuit aanbestedingsrechtelijk perspectief, aan de hand van de algemene beginselen van het aanbestedingsrecht: proportionaliteit, transparantie, non-discriminatie en objectiviteit.

1.2.2 Proportionaliteit

Bij een verwerving via een aanbestedingsprocedure, of deze nu Europees of onderhands is, is het zaak de proportionaliteit van de selectie- en gunningscriteria in het oog te houden. Uit het enkele feit dat dit document *best practices* ten aanzien van open standaarden aangeeft kan niet worden afgeleid dat deze eisen en wensen categorisch proportioneel zijn. Dit blijft iets wat van geval tot geval vastgesteld dient te worden, waarbij de Gids Proportionaliteit (http://www.pianoo.nl/regelgeving/aanbestedingswet-2012/gids-proportionaliteit) aanknopingspunten biedt om dit vast te stellen.

1.2.3 Transparantie

Vanuit oogpunt van transparantie is het wenselijk, zo niet noodzakelijk, om met name bij wensen in bestekteksten van te voren aan te geven hoe deze beoordeeld worden. In dit document is er voor gekozen om met voorbeeldboordelingen te werken. Vanzelfsprekend zijn deze indicatief. Wel verdient het heel nadrukkelijk aanbeveling om voor voorzienbare scenario's van inschrijvingen aan te geven hoe deze beoordeeld worden, ongeacht de puntentelling die daadwerkelijk gehanteerd wordt. Vanuit datzelfde oogpunt zijn er voorbeeldteksten voor toelichtingen bij zowel selectie- als gunningscriteria opgenomen in dit document.

1.2.4 Non-discriminatie

Door het open karakter van de standaarden op de 'pas toe of leg uit'-lijst is het niet snel discriminatoir om om deze standaarden te eisen. In uitzonderingsgevallen is dit echter wel denkbaar, bijvoorbeeld als nog maar één partij op de markt ze ondersteunt (ondanks dat brede beschikbaarheid in de markt een criterium is voor opname op deze lijst). In dergelijke situaties is het aanbevelenswaardig om ze niet als eisen, maar als wensen te hanteren. De Rijksinstructie geeft ook nadrukkelijk aan dat het ontbreken van brede beschikbaarheid in de markt een reden kan zijn om een standaard van de 'pas toe of leg uit'-lijst als gunningscriterium voor een oplossing te kiezen, in dat geval is uitleg (zie ook hoofdstuk 4) op zijn plaats.

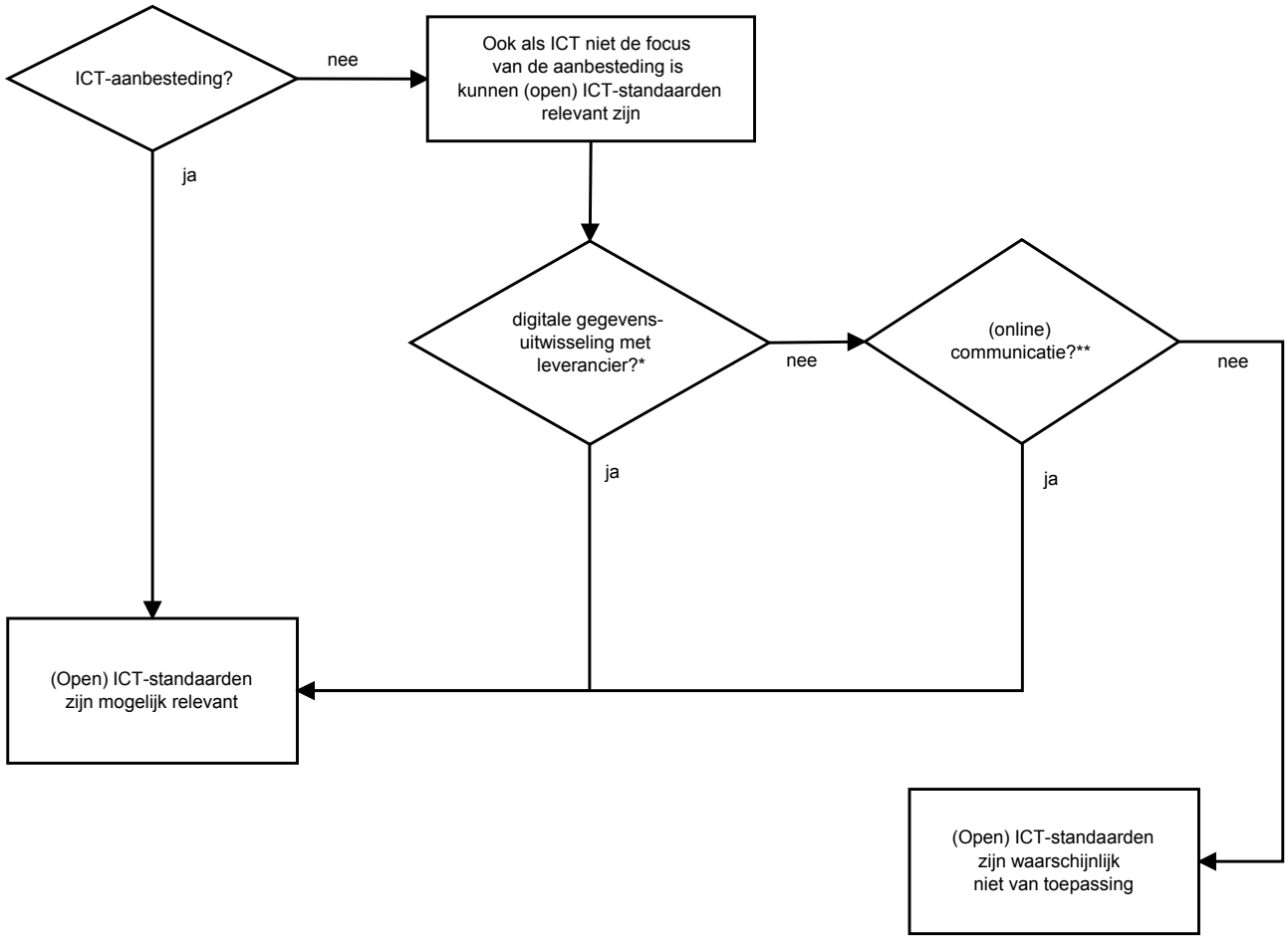
1.2.5 Objectiviteit

Gunningsbeslissingen dienen objectief controleerbaar te zijn. Juist het vragen naar standaarden (en vervolgens kiezen voor aanbiedingen die die standaarden ondersteunen) verhoogt de objectiviteit. Hier ligt haast vanzelfsprekend wel een taak voor de aanbestedende dienst om ook daadwerkelijk te toetsen op ondersteuning van de standaard, al is het achteraf.

2 Toepasselijkheid van standaarden

ICT-standaarden spelen niet alleen een rol bij zuivere ICT-aanbestedingen waarbij een ICT-dienst of -product wordt aangeschaft. Bijvoorbeeld bij het (laten) voeren van online campagnes, tevredenheidsonderzoeken en andere activiteiten waar online communicatie naar en met burgers en bedrijven een middel is bij de uitvoering van een activiteit die niet primair als ICT-dienstverlening getypeerd zal worden, maar waar wel degelijk ICT-middelen of diensten ingezet worden bij de levering van de kernprestatie.

In onderstaand stroomdiagram is het voorgaande vervat. Het verdient aanbeveling om dit stroomdiagram te doorlopen bij alle aanbestedingen op het vlak van zakelijke dienstverlening.



*Een voorbeeld van dergelijke uitwisseling is gegevensuitwisseling rondom afvalinzameling. Afvalinzameling zelf is geen ICT-dienst, er is wel elektronisch gegevensverkeer van inzamelcontainers, vuilnisophaalwagens en het beheer daarvan.

**Bijvoorbeeld:

- een arbeidsmarktcampagne, waar een website bij hoort;
- een online tevredenheidsonderzoek.

3 Veelvoorkomende aanbestedingen

In de praktijk blijken de volgende typen aanbestedingen waarbij ICT-standaarden relevant zijn het meeste voor te komen[1]:

- Communicatiecampagnes en/of tevredenheidsonderzoeken
- Inhuur van personeel en/of payrollingdiensten
- Softwarelicenties en/of resellercontracten
- Computerhardware
- **Websites, CMS en/of contentbeheer**
- **Webapplicaties**
- Spraak- en/of datacommunicatiediensten
- Gegevensopslag (data storage)
- Werkplekvoorzieningen
- Multifunctionals
- e-HRM systemen
- Financieel/administratieve systemen
- Lokale netwerken

In dit hoofdstuk zijn Websites, CMS en/of contentbeheer en Webapplicaties in het algemeen uitgelicht als productgroepen. De reden hiervoor is dat deze een relatief grote groep van open standaarden raken en als zodanig goede voorbeelden opleveren. In een latere editie zullen de overige aanbestedingen meegenomen worden.

3.1 Websites, CMS en/of contentbeheer

3.1.1 Typering:

- toegankelijk via browser
- publiek toegankelijk
- informerend
- soms ook: vastleggen en verwerken van (persoons-)gegevens

3.1.2 Beschrijving functioneel domein

Het functioneel domein is het online ontsluiten van overheidsinformatie voor burgers en/of bedrijven. Daarbij komt het voor dat tweerichtingsverkeer plaatsvindt, bijvoorbeeld door middel van vragenformulieren of het inschrijven op verzendlijsten van nieuwsbrieven.

3.1.3 Relevante koppelvlakken

- webinterface bezoekers
- webinterface redacteuren

1 Deze opsomming is gebaseerd op de ruwe dataset van het monitor-onderzoek naar de toepassing van open standaarden bij ICT-aanbestedingen van zowel de Rijksoverheid als de decentrale overheden over het jaar 2012.

- gepubliceerde documenten
- (optioneel) koppelingen met andere back-end systemen

3.1.4 Relevante standaarden

Voor websites en/of contentbeheer gelden niet alleen dezelfde standaarden als voor individuele campagnes en tevredenheidsonderzoeken, maar spelen nog een aantal andere standaarden een rol. Met name op het gebied van doorzoekbaarheid. Daarbij moet niet vergeten worden dat het aan de standaarden voldoen ook onderdeel is van de werkzaamheden in het geval er contentbeheer plaatsvindt, ook nieuwe content moet toegankelijk zijn voor alle burgers en doorzoekbaar zijn. Daarnaast is het uit oogpunt van betrouwbare informatievoorziening van burgers en bedrijven wenselijk om te voorkomen dat domeinnaamgegevens gemanipuleerd worden en/of het surfgedrag van burgers niet met derden gedeeld worden.

3.1.5 Standaarden van past-toe-of-leg-uit-lijst

Standaarden die eigenlijk knock-out vragen (eisen) zouden moeten zijn, zijn:

- Webrichtlijnen
- OWMS (voor metadatering)
- DNSsec (beveiligingsstandaard)
- DKIM (beveiligingsstandaard)
- ODF (voor gepubliceerde documenten)
- PDF/A (voor archiveerbaarheid)
- IPv6 (netwerkstandaard)

Standaarden die mogelijk van toepassing zijn, zijn:

- OAI-PMH
- NL-LOM (met name voor educatieve inhoud)
- ISO 27001/27002 (*best practices* op het gebied van informatiebeveiliging)

3.1.6 Veelgebruikte standaarden:

- HTTPS (om SSL toe te passen op beveiligde HTTP-verbindingen)
- X.509 (om HTTPS mogelijk te maken en voor het gebruik van gekwalificeerde certificaten in het kader van PKI-overheid)

Relevante kaders en richtlijnen

- Eisen aan websites Rijksoverheid van (Ministerie van Algemene Zaken): https://www.rijksoverheid.nl/onderwerpen/overheidscommunicatie/eisen-aan-websites-rijksoverheid en https://www.rijksoverheid.nl/onderwerpen/overheidscommunicatie/documenten-en-publicaties/richtlijnen/2013/07/01/overzicht-rijksoverheidwebsites-eisen-richtlijnen-centrale-dienstverlening.html
- Beveiligingsrichtlijnen voor webapplicaties (NCSC): https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html

Bestekteksten

3.1.7 Selectie-eisen en -wensen

3.1.7.1 Webrichtlijnen versie 2 (http://www.webrichtlijnen.nl/)

De Webrichtlijnen zijn bedoeld om toegankelijkheid, doorzoekbaarheid en browseronafhankelijkheid van websites te waarborgen. De richtlijnen voor toegankelijkheid van webcontent van W3C, W3C Web Content Accessibility Guidelines (WCAG) versie 2.0[2], vormen een integraal onderdeel van Webrichtlijnen versie 2. Naast WCAG 2.0 omvatten de Webrichtlijnen 2.0 universele richtlijnen die zich richten op het creëeren van content die betekenisvol, voor iedereen bruikbaar, uitwisselbaar en duurzaam is.

Eis

De gegadigde/inschrijver dient aan te tonen dat hij in de afgelopen X jaar ervaring heeft opgedaan met het succesvol implementeren van websites die voldoen aan de Webrichtlijnen versie 2 -zoals opgenomen op de 'pas toe of leg uit'-lijst van College Standaardisatie- of daaraan gelijkwaardig. Dit kan door het overleggen van ten minste Y relevante referenties waarbij eerdergenoemde Webrichtlijnen versie 2 of gelijkwaardige standaarden op het gebied van toegankelijkheid, doorzoekbaarheid en browseronafhankelijkheid van websites een significante rol hebben gespeeld.

Een typische waarde voor X zou twee of drie zijn. Voor Y zou dit drie zijn.

Toelichting: overheidswebsites horen toegankelijk te zijn voor alle burgers dus ook burgers met een beperking. Tevens is het voor de ontsluiting van overheidsinformatie wenselijk dat zij toegankelijk zijn voor zoekmachines en dat zij browseronafhankelijk functioneren.

Ratio: het gaat hier om het selecteren van een partij met ervaring op het terrein van de Webrichtlijnen. Daarbij zijn eerdere versies van de Webrichtlijnen te zeer verouderd dat referenties op dit terrein nog relevant kunnen zijn voor de beoordeling van de geschiktheid van gegadigde. Als het voorzienbaar is dat te weinig gegadigden geselecteerd kunnen worden valt het aan te bevelen hier een wens van te maken.

Wens

De gegadigde biedt inzicht in de bekwaamheid van zijn personeel door aan te tonen dat dit in de afgelopen jaren ervaring heeft opgedaan met het conform de Webrichtlijnen versie 2 of daaraan gelijkwaardige standaarden op het gebied van toegankelijkheid, doorzoekbaarheid en browseronafhankelijkheid van websites bouwen en/of beheren van websites. Dit inzicht biedt hij door cv's aan te leveren van medewerkers die bij eventuele gunning ingezet zullen worden waaruit dit blijkt. De Webrichtlijnen versie 1 worden niet als gelijkwaardig beschouwd aan versie 2.

Toelichting: toepassing van de webrichtlijnen komt in de praktijk ook aan op de betrokken mensen, zowel bij bouw als bij later beheer, en niet alleen op de gebruikte techniek. Het is daarom nuttig om de gegadigde op de in zijn organisatie aanwezige kennis op dit terrein toetsen.

Ratio: het hebben van referenties op zich bewijst niet dat de vereiste kennis nog steeds in de organisatie aanwezig is. Uit oogpunt van transparantie is het wenselijk om aan te geven dat versie 1 niet als gelijkwaardig wordt beschouwd.

Voorbeeldbeoordeling (minimaal 6, maximaal 10 punten):

2 http://www.w3.org/WAI/intro/wcag

Voor de ze wens kunnen maximaal tien (10) punten worden behaald waarbij de punten worden berekend op basis van het aantal jaren ervaring met de Webrichtlijnen versie 2 in ieder cv in de afgelopen X jaar. Het aanleveren van één cv met daarin drie jaar ervaring levert dan drie punten op, met een maximum van vijftien. Inschrijvingen die minder dan zes (6) punten behalen voor deze vraag zullen terzijde worden gelegd.

Een typische waarde voor X zou twee zijn .

3.1.7.2 OWMS (Overheid.nl Web Metadatering Standaard)[3]

OWMS is een standaard om gestructureerde verzamelingen die online gepubliceerd worden te metadateren en zo beter te ontsluiten. Voorbeelden zijn publicaties van vergunningen en van wet- en regelgeving.

Eis

De gegadigde dient aan te tonen dat hij in de afgelopen X jaar ervaring heeft opgedaan met het succesvol implementeren en/of beheren van metadatering van webpublicaties conform de OWMS 4.0 standaard of gelijkwaardig (waarbij de Dublin Core Application Profile voor de beantwoording van deze vraag als gelijkwaardig geldt) aan de hand van ten minste Y referenties op dit terrein.

Typische waarden voor X en Y zouden twee of drie zijn.

Toelichting: OWMS is een Nederlands profiel op de open standaard Dublin Core Application Profile voor metadatering van websites. Om de geschiktheid van gegadigde te beoordelen is bekendheid met OWMS of ten minste de Dublin Core Application Profile relevant.

Ratio: het is waarschijnlijk disproportioneel om uitsluitend OWMS-referenties te eisen.

3.1.7.3 ISO 27001:2005 (beveiligingsstandaard op beleidsniveau)

De ISO 27001:2005 standaard is een standaard op het gebied van de procesmatige inrichting van informatiebeveiliging.

Eis

Gegadigde opereert aantoonbaar conform de ISO 27001:2005 standaard (of gelijkwaardig). Een wijze om dit aan te tonen is de desgevraagde overlegging van een certificaat.

Alternatief:

Gegadigde heeft aantoonbaar ervaring met het leveren van diensten aan ISO 27001:2005 (of gelijkwaardig) gecertificeerde organisaties en toont dit aan door ten minste X referenties van opdrachten voor dergelijke organisaties in de afgelopen Y jaar te verschaffen.

Typische waarden voor X en Y zouden twee of drie zijn.

Toelichting: opdrachtgever is ISO 27001:2005 gecertificeerd of is voornemens dit in de toekomst te worden. In het kader hiervan is het wenselijk dat gegadigden bekend zijn met de daarmee samenhangende veranderingen die in een organisatie met betrekking tot informatiebeveiliging en het daarmee samenhangende bewustwording plaatsvinden. De ISO 27001:2013 standaard die als opvolger van de ISO 27001:2005 standaard beschouwd kan worden maar (nog) niet op de 'pas toe of leg uit'-lijst is opgenomen wordt als gelijkwaardig aan de ISO 27001:2005 beschouwd.

Ratio: het is doorgaans al uitdagend genoeg om in de eigen organisatie een cultuuromslag op dit terrein plaats te laten vinden, het is dan nuttig dat leveranciers hier geen remmende factor in worden.

3 http://standaarden.overheid.nl/owms

Wens

Gegadigde is ISO 27001:2005 gecertificeerd (of gelijkwaardig) en kan dit desgevraagd aantonen.

Toelichting: opdrachtgever wenst zaken te doen met een partij die informatiebeveiliging in zijn organisatorische processen ingebed hebben.

Toelichting: informatiebeveiliging moet zowel organisatorisch als technisch op een adequaat niveau zijn, zeker in het geval de leverancier doorlopend verantwoordelijk is voor dienstverlening, zoals het hosten van een website en/of CMS. De ISO 27001:2013 standaard die als opvolger van de ISO 27001:2005 standaard beschouwd kan worden maar (nog) niet op de 'pas toe of leg uit'-lijst is opgenomen wordt als gelijkwaardig aan de ISO 27001:2005 beschouwd.

Ratio: het kan gezien de marktsituatie te zwaar zijn om van alle gegadigden een volledige certificatie te vragen, daarom kan het verdedigbaar zijn deze als wens te vragen. Een en ander is tevens afhankelijk van de risico-inschatting van de gegevensverwerking en de aard van de dienstverlening. Andere denkbare alternatieven zijn een zogenaamd ISAE 3402 *in control statement*[4] of een aantoonbaar groeipad naar een ISO 27001:2005 certificering. Ongeacht de hoogte waarop de lat gelegd wordt moet deze wel SMART geformuleerd worden.

Voorbeeldbeoordeling (maximaal 15 punten):

- Gegadigde is niet ISO27001:2005 gecertificeerd: 0 punten;
- Gegadigde verwacht op datum X ISO27001:2005 gecertificeerd te zijn: 10 punten
- Gegadigde is ISO27001:2005 gecertificeerd: 15 punten.

X zou bijvoorbeeld een jaar in de toekomst kunnen liggen.

3.1.7.4 ISO 27002:2005 (best practices op het gebied van informatiebeveiliging)

Eis

Gegadigde/inschrijver toont door middel van X referenties uit de afgelopen Y jaar aan dat hij ervaring heeft met de *best practices* van de ISO 27002:2005 norm of daaraan gelijkwaardig.

Typische waarden voor X en Y zouden twee of drie zijn.

Toelichting: opdrachtgever wil uitsluitend zaken doen met een partij die aantoonbaar ervaring heeft met het toepassen van gangbare *best practices* op het gebied van informatiebeveiliging. De ISO 27002:2005 standaard omvat de omschrijving van wat minimaal gangbaar wordt beschouwd. In de context van deze selectie-eis wordt de Baseline Informatiebeveiliging Rijksoverheid (BIR)[5] als gelijkwaardig aan ISO 27002:2005 beschouwd. Dit geldt evenzeer voor de ISO 27002:2013 standaard die als opvolger van de ISO 27002:2005 standaard beschouwd kan worden maar (nog) niet op de past-toe-of-leg-uit-lijst is opgenomen.

Ratio: het procesmatig ingericht hebben van informatiebeveiliging betekent nog niet dat meer technisch-operationele *best practices* niet eveneens vereist zijn. ISO 27002:2005 is vooral van betekenis voor het nemen van feitelijke maatregelen op dit terrein.

4 ISAE (International Standard on Assurance Engagements) 3402 is een internationale standaard voor het door auditors afgeven van verklaringen in hoeverre een organisatie 'in control' is op een bepaald (gespecificeerd) proces, bijvoorbeeld informatiebeveiliging.

5 In het geval de aanbestedende dienst een gemeente of provincie is zijn de Baseline Informatiebeveiliging Gemeenten (BIG) en de Interprovinciale Baseline Informatiebeveiliging toepasselijker.

3.1.8 Gunningseisen en -wensen

3.1.8.1 Webrichtlijnen versie 2 (http://www.webrichtlijnen.nl/)

Eisen

Bij bouw:
De op te leveren website dient te voldoen aan de Webrichtlijnen versie 2 (of gelijkwaardig). Het is aan de opdrachtnemer om aanspraken op conformiteit te onderbouwen. Een geschikt middel hiervoor is het laten uitvoeren van een onafhankelijke evaluatie of toetsing zoals beschreven op http://www.webrichtlijnen.nl/verantwoorden/evaluatie.

Bij exploitatie
De te onderhouden website dient te blijven voldoen aan de Webrichtlijnen versie 2 Level AA (of gelijkwaardig). Het is aan de opdrachtnemer om aanspraken op conformiteit te onderbouwen. Een geschikt middel hiervoor is het laten uitvoeren van een onafhankelijke evaluatie of toetsing zoals beschreven op http://www.webrichtlijnen.nl/verantwoorden/evaluatie.

Toelichting: de Webrichtlijnen versie 2 omvatten de W3C Web Content Accessibility Guidelines (WCAG) versie 2.0[6], een wereldwijde standaard om de toegankelijkheid van websites te waarborgen. Opdrachtgever wenst, conform het Nederlandse beleid op dit terrein, dat de/het te realiseren website/CMS geen concessies doet op het terrein van toegankelijkheid, doorzoekbaarheid en browseronafhankelijkheid.

Ratio: overheidsinformatie dient toegankelijk te zijn voor alle burgers, ongeacht of zij een (audio)visuele beperking hebben of gebruik maken van uiteenlopende webapparaten, besturingssystemen, *user agents* en hulptechnologieën.

Wens

Naast de eis te voldoen aan de webrichtlijnen dient leverancier aan te geven hoe het blijvend voldoen aan de Webrichtlijnen versie 2 geborgd is in het beheerproces.

Toelichting: online overheidsinformatie is inherent dynamisch, het bij implementatie bewerkstelligen van toegankelijkheid biedt geen waarborgen voor de toekomst, opdrachtgever wil daarom inzicht hebben hoe dit voor de toekomst gewaarborgd wordt.

Ratio: overheidsinformatie dient toegankelijk te zijn voor alle burgers, ongeacht of zij een (audio)visuele beperking hebben of niet. Dit dient blijvend gewaarborgd te worden.

Voorbeeldbeoordeling (maximaal 10 punten):
De onderbouwing van de borging in het beheerproces wordt beoordeeld op de mate waarin helderheid wordt gegeven over de wijze waarop dit zijn weerslag krijgt in:

- werkbeschrijvingen en protocollen;
- testmethodieken;
- technisch signaleren van afwijkingen van de Webrichtlijnen versie 2;
- kennisborging bij de betrokken medewerkers.

3.1.8.2 OWMS (Overheid.nl Web Metadatering Standaard)[7]

Eisen

6 http://www.w3.org/WAI/intro/wcag
7 http://standaarden.overheid.nl/owms

Bij bouw:

De op te leveren website dient de mogelijkheid te bieden om te publiceren webpagina's te voorzien van metadata die voldoet aan de OWMS-standaard versie 4.0 of daaraan gelijkwaardig. Dit zal onderdeel vormen van de acceptatiecriteria.

Bij exploitatie:

Bij het onderhoud van de website dient de doorzoekbaarheid gewaarborgd te worden door op zijn minst er zorg voor te dragen dat de informatie voorzien is van metadata die voldoet aan de OWMS-standaard versie 4.0 of daaraan gelijkwaardig. Dit zal periodiek getoetst worden.

Toelichting: OWMS is een Nederlands profiel op de open standaard Dublin Core Application Profile voor metadatering van websites. Opdrachtgever wil de mogelijkheid hebben om gestructureerde data via de website te metadateren conform deze standaard.

Ratio: in het geval er gestructureerde data wordt aangeboden via de te leveren of te exploiteren website/CMS dient deze als zodanig gemetadateerd te kunnen worden middels de OWMS-standaard versie 4.

Wens

Leverancier geeft aan hoe blijvend voldoen aan de OWMS-standaard versie 4 of daaraan gelijkwaardig geborgd wordt in het beheersproces.

Toelichting: OWMS 4.0 is een Nederlands profiel op de zogenaamde Dublin Core Application Profile voor metadatering van publicaties. Hiermee wordt bereikt dat Nederlandse overheidspublicaties op uniforme wijze van metadata worden voorzien wat de vindbaarheid vergroot en het combineren van informatie vergemakkelijkt.

Ratio: in het geval er gestructureerde data wordt aangeboden via de te leveren of te exploiteren website/CMS dient deze als zodanig gemetadateerd te worden middels de OWMS-standaard versie 4.0.

Voorbeeldbeoordeling (maximaal 10 punten):

- De aangeboden oplossing voldoet niet aan OWMS versie 4.0: 0 punten;
- De aangeboden oplossing zal binnen nu en twee jaar voldoen aan OWMS versie 4.0 en dit zit inbegrepen in het de aanbieding: 5 punten;
- De aangeboden oplossing voldoet nu aan OWM versie 4.0: 10 punten.

3.1.8.3 ODF

ODF is een standaard voor reviseerbare documenten (tekstdocumenten, rekenbladen en presentaties).

Eis

Managementrapportages over bezoek en gebruik van de website zijn beschikbaar in ODF 1.2 formaat of daaraan gelijkwaardig.

Toelichting: opdrachtgever wil geen (nieuwe) afhankelijkheden van andere documentformaten dan ODF 1.2 scheppen in zijn organisatie.

(In geval van documentgeneratie) Documentgeneratie moet ODF 1.2 of daaraan gelijkwaardige formaten ondersteunen. Gelijkwaardigheid van hogere versies van de ODF standaard wordt verondersteld. De OOXML standaard wordt niet als gelijkwaardig met ODF 1.2 gezien.

Toelichting: niet zelden worden documenten in een bewerkbaar formaat om bijvoorbeeld hergebruik te bevorderen. Om te voorkomen dat burgers gedwongen

worden tekstverwerkingssoftware van specifieke leveranciers aan te schaffen is het noodzakelijk dat dit in een open documentformaat zoals ODF 1.2 gebeurt.

Ratio: ODF 1.2 is een strategisch documentformaat om leveranciersonafhankelijkheid over documentenstromen in de overheid te bereiken. Dit maakt het met name mogelijk om de kantoorautomatisering los te koppelen van *back-end* verwerkingssystemen.

3.1.8.4 PDF/A

Eis

(In geval van documentgeneratie) Documentgeneratie moet PDF/A daaraan gelijkwaardige formaten ondersteunen.

Toelichting: documenten welke van overheidswege verstrekt zijn moeten ook in de toekomst ontsloten kunnen worden. Uit oogpunt van digitale duurzaamheid vindt opdrachtgever het dan ook wenselijk een gegevensformaat te gebruiken wat hiervoor bedoeld is. Tevens is dit een vereiste om aan de archiefwet te kunnen voldoen.

3.1.8.5 DKIM

Eis

E-mail-alert en -notificatiefuncties van de website zorgen er voor dat de authenticiteit van overheidsberichten gewaarborgd kan worden door middel van de DKIM-standaard (of daaraan gelijkwaardig).

Toelichting: opdrachtgever wil het '*spoofen*' van e-mails uit zijn naam voorkomen en wil daarom gebruik kunnen maken van de DKIM-standaard.

3.1.8.6 DNSsec

Eisen

(in geval van DNS-hosting) De DNS-hostingdienst voorziet in ondersteuning van de DNSsec-standaard.

De DNSsec-standaard (of een gelijkwaardige standaard) ondersteund dient te worden bij het verzenden van e-mailberichten en -notificaties.

Toelichting: opdrachtgever beoogt een oplossing die het verspreiden van (onjuiste) informatie uit naam van opdrachtgever door kwaadwillende derden bemoeilijkt, zowel als het om de website zelf gaat als bij e-mailberichten en -notificaties.

Ratio: bij gebruik van deze standaarden is enerzijds de kans dat e-mailberichten van overheden in spamfilters van burgers terechtkomen kleiner en anderzijds kunnen burgers er meer op vertrouwen dat berichten die zij ontvangen ook daadwerkelijk van de overheid afkomstig zijn. Tevens draagt DNSsec er aan bij dat burgers en bedrijven meer zekerheid hebben dat de informatie die zij van een website opvragen daadwerkelijk van de overheid afkomstig is en niet van een kwaadwillende derde. Om dit te bereiken zijn gebruik van zowel de DKIM als de DNSsec-standaarden noodzakelijk.

3.1.8.7 IPv6

Eisen

De website/het CMS is benaderbaar via IPv6 met dezelfde functionaliteit als via IPv4.

(in geval van DNS-hosting) De DNS-hostingdienst is tevens voor IPv6-gebaseerde "user agents" beschikbaar en een domeinnaambevraging resulteert ("resolves") in een geldig IPv6-adres voor de website.

Toelichting: gezien de schaarse IPv4-adresruimte en de voordelen van IPv6 wil de opdrachtgever op termijn over kunnen stappen op IPv6 zonder dat een dergelijke migratie impact heeft op zijn informatiehuishouding en tegen zo laag mogelijke kosten. Opdrachtgever eist derhalve toekomstbestendigheid op dit terrein.

Ratio: nu niet strategisch inzetten op IPv6 betekent bij een toekomstige IPv6-migratie waarschijnlijk voortijdig uitfaseren van ICT-middelen die uitsluitend IPv4 ondersteunen. Uit doelmatigheidsoverwegingen is dit onwenselijk. Tevens biedt IPv6 meer mogelijkheden op het terrein van informatiebeveiliging, bijvoorbeeld bij het bestrijden van Distributed Denial-of-Service (DDoS) aanvallen.

3.1.9 Meetinstrumenten

3.1.9.1 Webrichtlijnen versie 2

Voor de Webrichtlijnen geldt dat automatische toetsinstrumenten nuttig zijn, maar het nut is wel begrensd. Beweringen dat wordt voldaan aan WCAG of Webrichtlijnen, die enkel zijn gebaseerd op de uitkomsten van een automatisch toetsinstrument (zie o.a. http://www.webrichtlijnen.nl/toetsen/wat-u-moet-weten), zijn per definitie onvoldoende betrouwbaar. De reden daarvoor is dat dergelijke instrumenten niet alles kunnen toetsen, eenvoudigweg omdat de hoeveelheid tests die betrouwbaar volledig automatisch kan worden uitgevoerd beperkt is. De uitkomst van een automatisch toetsinstrument is dus altijd een deelresultaat. Aanvullende menselijke beoordeling is nodig om succesvol te kunnen claimen dat aan WCAG of Webrichtlijnen wordt voldaan. In de volgende situaties zijn uitkomsten van een automatisch toetsinstrument heel bruikbaar:

- Om snel fouten op webpagina's te kunnen opsporen, zodat ze kunnen worden hersteld,
- Om snel een indicatie te kunnen krijgen van (mogelijke) problemen op een website, of op groepen websites, en
- Om beweringen te kunnen falsifiëren dat aan de gestelde eisen wordt voldaan. Immers, als door het toetsinstrument fouten worden gerapporteerd is weerlegbaar dat de bewering waar is.

De belangrijkste, uit de auditpraktijk afkomstige, aspecten waarop beweringen en de ondersteunende informatie dienen te kunnen worden beoordeeld zijn:

- Actualiteit,
- Volledigheid,
- Juistheid, en
- (in gevallen waarbij een steekproef is gebruikt:) Representativiteit.

op het gebied van het aspect volledigheid zijn volledig automatische toetsinstrumenten tot dusverre ontoereikend gebleken.

3.1.9.2 IPv6

Een meetinstrument voor IPv6-compatibiliteit van een website of -service is te vinden op http://ip6.nl/

3.2 Webapplicaties

3.2.1 Beschrijving functioneel domein

De term webapplicaties is een generiek begrip voor eigenlijk alle toepassingen die als Software-as-a-Service worden aangeboden en/of voor hun primaire bediening een webinterface gebruiken, maar niet primair als een website fungeren. Dit kan

variëren van e-HRM tot het afnemen van examens. In de praktijk is er veelal wel sprake van zogenaamde bedrijfsvoeringsoftware.

Typering:
- toegankelijk via browser
- veelal niet publiek toegankelijk
- interactief
- vastleggen en verwerken van (persoons-)gegevens

3.2.2 Mogelijke koppelvlakken

Een webinterface als koppelvlak is in feite een gegeven. Andere koppelvlakken die veel voorkomen zijn:
- e-mail (voor bijvoorbeeld notificaties);
- archiveerbare documenten;
- authenticatie, bijvoorbeeld via DigiD;
- documentgeneratie en rapportages;
- berichtenverkeer met andere overheden en/of in ketens.

3.2.3 Relevante open standaarden (per koppelvlak)

Voor webinterfaces geldt net als voor 'gewone' websites dat de webrichtlijnen onverkort van toepassing zijn, ongeacht of de applicatie voor burgers of voor intern gebruik bedoeld is.

Voor e-mail is het van belang dat de authenticiteit van de e-mail gewaarborgd kan worden. Hiervoor is de DKIM-standaard van toepassing, die op haar beurt weer afhankelijk is van de DNSSec standaard.

Bij archivering speelt met name PDF/A een rol, waarbij opgemerkt moet worden dat zowel archiveerbaarheid en authenticiteit zijn niet alleen voor de eigen organisatie van belang zijn, maar ook voor de ontvangende partij(en), al dan niet uit hoofde van Algemene wet bestuursrecht (Awb).

Omdat er veelal sprake is van software die primaire processen ondersteunt, niet zelden in de uitvoeringssfeer, zal het niet zelden de verwerking van persoonsgegevens betreffen. Uit hoofde van de Wet bescherming persoonsgegevens (Wbp) horen daarbij passende technische en organisatorische maatregelen getroffen te worden. Hiervoor relevante standaarden op de pas-toe-of-leg-uit lijst zijn ISO 27001:2005 en ISO 27002:2005, waarbij de eerste vooral het organisatiebeleid ten aanzien van de beveiliging en continuïteit van de beveiliging betreft en de laatste meer een verzameling *best practices* is voor het daadwerkelijk uitvoeren van beveilings- en continuïteitsbeleid behelst.

Voor documentgeneratie en rapportages is ODF een standaard waar naar gevraagd moet worden, dit sluit overigens niet uit dat omwille van de interoperabiliteit een leveranciersspecifieke standaard náást ODF gevraagd kan worden.

Voor berichtenverkeer met andere overheden en in ketens (anders dan via e-mail) wordt vooral Digikoppeling 2.0 als standaard gehanteerd. Bovenop Digikoppeling 2.0 is er voor gemeenten nog een laag ontwikkeld die de StUF-standaard vormt.

Standaarden die naar alle waarschijnlijkheid knock-out criteria zijn:
- Webrichtlijnen (in het geval van publieke toegankelijkheid)
- PDF/A (voor archiveerbare documenten)
- DKIM (beveiligingsstandaard)
- DNSsec (beveiligingsstandaard)

- ODF (documentstandaard)

Standaarden die in ieder geval overwogen moeten worden om uit te vragen:
- ISO 27001/27002 (beveiligingsstandaarden)
- StUF (in de gemeentelijke sfeer)
- Digikoppeling
- SAML (authenticatiestandaard)

Gangbare standaarden die van toepassing zijn:
- HTTPS (beveiligingsstandaard)

Relevante centrale voorzieningen:
- DigiD
- PKIoverheid

Relevante kaders en richtlijnen:
- Zie: Eisen aan websites Rijksoverheid, http://www.rijksoverheid.nl/onderwerpen/overheidscommunicatie/eisen-aan-websites-rijksoverheid en http://www.rijksoverheid.nl/onderwerpen/overheidscommunicatie/documenten-en-publicaties/richtlijnen/2013/07/01/overzicht-rijksoverheidwebsites-eisen-richtlijnen-centrale-dienstverlening.html
- Beveiliging: NCSC, ICT-beveiligingsrichtlijnen voor webapplicaties, https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html
- Privacy:
  - CBP, Richtsnoeren, http://www.cbpweb.nl/Pages/ind_publ_rs.aspx
  - ACM, Cookies en spamverbod, https://www.acm.nl/nl/onderwerpen/telecommunicatie/internet/
- Archivering: http://www.rijksoverheid.nl/onderwerpen/archieven/archieven-van-de-overheid

Gerelateerde wet- en regelgeving:
- Wet gelijke behandeling op grond van handicap of chronische ziekte
- Besluit Kwaliteit Rijksoverheidswebsites (https://zoek.officielebekendmakingen.nl/stcrt-2006-136-p23-SC75949.html)
- Algemene wet bestuursrecht (met name afdeling 2.3)
- Archiefwet

In de praktijk kan het nuttig zijn de toepasselijke kaders, inclusief gerelateerde wet- en regelgeving aan gegadigden in een aanbesteding te communiceren zodat voor hen duidelijk is waar zij op afgerekend kunnen worden.

Bestekteksten

3.2.4 Selectie-eisen en -wensen

3.2.4.1 Webrichtlijnen

De Webrichtlijnen zijn bedoeld om toegankelijkheid, doorzoekbaarheid en browseronafhankelijkheid van webapplicaties te waarborgen. De richtlijnen voor toegankelijkheid van webcontent van W3C, W3C Web Content Accessibility

Guidelines (WCAG) versie 2.0[8], vormen een integraal onderdeel van Webrichtlijnen versie 2. Naast WCAG 2.0 omvatten de Webrichtlijnen universele richtlijnen die zich richten op het creëeren van content die betekenisvol, voor iedereen bruikbaar, uitwisselbaar en duurzaam is.

Webrichtlijnen versie 2 zijn vooral een knock-out eis als er sprake is van publieke toegankelijkheid van een webapplicatie. Ook in de gevallen dat hier geen sprake van is, is het uit oogpunt van gelijke behandeling en leveranciersonafhankelijkheid aanbevelenswaardig naar de Webrichtlijnen versie 2 of althans een subset van de Webrichtlijnen versie 2 te vragen (namelijk de eisen met betrekking tot browseronafhankelijkheid en toegankelijkheid). Zelfs als de Webrichtlijnen versie 2 niet als gunningscriterium gehanteerd zullen worden kan het vragen naar ervaring met de Webrichtlijnen een proportioneel selectiecriterium zijn omdat ze zelfs bij gedeeltelijke toepassing een *best practice* zijn in het gebruik van webtechnologieën en als zodanig een indicatie van de vakbekwaamheid van gegadigde zijn.

Eis

De gegadigde/inschrijver dient aan te tonen dat hij in de afgelopen X jaar ervaring heeft opgedaan met het succesvol implementeren van webapplicaties die voldoen aan de Webrichtlijnen versie 2 -zoals opgenomen op de ‘pas toe of leg uit’-lijst van College Standaardisatie- of daaraan gelijkwaardig. Dit kan door het overleggen van ten minste Y relevante referenties waarbij eerdergenoemde webrichtlijnen of gelijkwaardige standaarden op het gebied van toegankelijkheid en browseronafhankelijkheid van webapplicaties een significante rol hebben gespeeld.

Toelichting: opdrachtgever wenst zaken te doen met een partij die aantoonbaar ervaring heeft met toegankelijk en browseronafhankelijk toepassen van webtechnologieën.

Toelichting: overheidswebapplicaties horen toegankelijk te zijn voor alle burgers dus ook burgers met een beperking. Tevens is het voor de ontsluiting van overheidsinformatie wenselijk dat zij toegankelijk zijn voor zoekmachines en dat zij browseronafhankelijk functioneren.

Ratio: het gaat hier om het selecteren van een partij met ervaring op het terrein van de Webrichtlijnen. Daarbij zijn eerdere versies van de Webrichtlijnen te zeer verouderd dat referenties op dit terrein nog relevant kunnen zijn voor de beoordeling van de geschiktheid van gegadigde. Als het voorzienbaar is dat te weinig gegadigden geselecteerd kunnen worden valt het aan te bevelen hier een wens van te maken. Voor de interne afweging speelt mee dat het onder omstandigheden verdedigbaar is om de doorzoekbaarheidsaspecten van de Webrichtlijnen 2.0 niet te vergen bij een zeer dynamische webapplicatie.

Wens

De gegadigde biedt inzicht in de bekwaamheid van zijn personeel door aan te tonen dat dit in de afgelopen jaren ervaring heeft opgedaan met het conform de Webrichtlijnen versie 2 of daaraan gelijkwaardige standaarden op het gebied van toegankelijkheid, doorzoekbaarheid en browseronafhankelijkheid van websites bouwen en/of beheren van websites. Dit inzicht biedt hij door cv's aan te leveren van medewerkers die bij eventuele gunning ingezet zullen worden waaruit dit blijkt. De Webrichtlijnen versie 1 worden niet als gelijkwaardig beschouwd aan versie 2.

Toelichting: toepassing van de webrichtlijnen komt in de praktijk ook aan op de betrokken mensen, zowel bij bouw als bij later beheer, en niet alleen op de gebruikte techniek. Het is daarom nuttig om de gegadigde op de in zijn organisatie aanwezige kennis op dit terrein toetsen.

8 http://www.w3.org/WAI/intro/wcag

Ratio: het hebben van referenties op zich bewijst niet dat de vereiste kennis nog steeds in de organisatie aanwezig is. Uit oogpunt van transparantie is het wenselijk om aan te geven dat versie 1 niet als gelijkwaardig wordt beschouwd.

Voorbeeldbeoordeling (minimaal 6, maximaal 10 punten):

Een typische waarde voor X zou twee zijn .

Voor de ze wens kunnen maximaal tien (10) punten worden behaald waarbij de punten worden berekend op basis van het aantal jaren ervaring met de Webrichtlijnen versie 2 in ieder cv in de afgelopen X jaar. Het aanleveren van één cv met daarin drie jaar ervaring levert dan drie punten op, met een maximum van vijftien. Inschrijvingen die minder dan zes (6) punten behalen voor deze vraag zullen terzijde worden gelegd.

3.2.4.2 ISO 27001:2005 (beveiligingsstandaard op beleidsniveau)

De ISO 27001:2005 standaard is een standaard op het gebied van de procesmatige inrichting van informatiebeveiliging. De eis en de wens in de hiernavolgende paragraaf zijn een keuze, zij kunnen niet gelijktijdig ingezet worden.

Eis

Gegadigde is ISO 27001:2005 gecertificeerd (of gelijkwaardig) en kan dit desgevraagd aantonen.

Alternatief:

Gegadigde heeft aantoonbaar ervaring met het leveren van diensten aan ISO27001:2005 (of gelijkwaardig) gecertificeerde organisaties en toont dit aan door ten minste X referenties van opdrachten voor dergelijke organisaties in de afgelopen Y jaar te verschaffen.

Typische waarden voor X en Y zijn twee, respectievelijk drie.

Toelichting: informatiebeveiliging moet zowel organisatorisch als technisch op een adequaat niveau zijn, zeker in het geval de leverancier doorlopend verantwoordelijk is voor dienstverlening, zoals het hosten of volledig exploiteren van een webapplicatie. De ISO 27001:2013 standaard die als opvolger van de ISO 27001:2005 standaard beschouwd kan worden maar (nog) niet op de 'pas toe of leg uit'-lijst is opgenomen wordt als gelijkwaardig aan de ISO 27001:2005 beschouwd.

Ratio: met name bij webapplicaties wordt relatief vaak meer gevoelige (persoons)gegevens verwerkt.

Wens

Gegadigde is ISO27001:2005 gecertificeerd (of gelijkwaardig) en kan dit desgevraagd aantonen.

Toelichting: informatiebeveiliging moet zowel organisatorisch als technisch op een adequaat niveau zijn, zeker in het geval de leverancier doorlopend verantwoordelijk is voor dienstverlening, zoals het hosten of volledig exploiteren van een webapplicatie. De ISO 27001:2013 standaard die als opvolger van de ISO 27001:2005 standaard beschouwd kan worden maar (nog) niet op de 'pas toe of leg uit'-lijst is opgenomen wordt als gelijkwaardig aan de ISO 27001:2005 beschouwd.

Ratio: het kan gezien de marktsituatie te zwaar zijn om van alle gegadigden een volledige certificatie te vragen, daarom kan het verdedigbaar zijn deze als wens te vragen. Een en ander is tevens afhankelijk van de risico-inschatting van de gegevensverwerking en de aard van de dienstverlening. Andere denkbare alternatieven zijn een zogenaamd ISAE 3402 *in control statement*[9] of een

9 ISAE (International Standard on Assurance Engagements) 3402 is een internationale standaard voor het door auditors afgeven van verklaringen in hoeverre een organisatie 'in control' is op een bepaald (gespecificeerd) proces, bijvoorbeeld informatiebeveiliging.

aantoonbaar groeipad naar een ISO 27001:2005 certificering. Ongeacht de hoogte waarop de lat gelegd wordt moet deze wel SMART geformuleerd worden.

Voorbeeldbeoordeling (maximaal 15 punten):

- Gegadigde is niet ISO27001:2005 gecertificeerd: 0 punten;
- Gegadigde verwacht op datum X ISO27001:2005 gecertificeerd te zijn: 10 punten
- Gegadigde is ISO27001:2005 gecertificeerd: 15 punten.

X zou bijvoorbeeld een jaar in de toekomst kunnen liggen.

3.2.4.3 ISO 27002:2005 (best practices op het gebied van informatiebeveiliging)

Eis

Gegadigde/inschrijver toont door middel van X referenties uit de afgelopen Y jaar aan dat hij ervaring heeft met de *best practices* van de ISO 27002:2005 norm of daaraan gelijkwaardig.

Typische waarden voor X en Y zijn twee, respectievelijk drie.

Toelichting: opdrachtgever wil uitsluitend zaken doen met een partij die aantoonbaar ervaring heeft met het toepassen van gangbare *best practices* op het gebied van informatiebeveiliging. De ISO 27002:2005 standaard omvat de omschrijving van wat minimaal gangbaar wordt beschouwd. In de context van deze selectie-eis wordt de Baseline Informatiebeveiliging Rijksoverheid (BIR)[10] als gelijkwaardig aan ISO 27002:2005 beschouwd. Dit geldt evenzeer voor de ISO 27002:2013 standaard die als opvolger van de ISO 27002:2005 standaard beschouwd kan worden maar (nog) niet op de past-toe-of-leg-uit-lijst is opgenomen.

Ratio: het procesmatig ingericht hebben van informatiebeveiliging betekent nog niet dat meer technisch-operationele *best practices* niet eveneens vereist zijn. ISO 27002:2005 is vooral van betekenis voor het nemen van feitelijke maatregelen op dit terrein.

3.2.4.4 Digikoppeling (standaard voor sector-overstijgende koppelingen)

Digikoppeling is de standaard voor de logistieke afhandeling van berichtenverkeer tussen overheden. Met name in het geval van koppelingen met basisregistraties en/of uitwisseling van berichtenverkeer met overheden in andere bestuurslagen of andere sectoren (bijvoorbeeld tussen zorg en onderwijs) is deze standaard relevant.

Eis

Gegadigde/inschrijver toont door middel van X referenties uit de afgelopen Y jaar aan dat hij ervaring heeft met de Digikoppeling-standaard[11] of daaraan gelijkwaardig. De referenties dienen duidelijk te maken welke deelstandaarden van Digikoppeling (WUS, ebMS, Grote Berichten) (succesvol) geïmplementeerd zijn en hoe dit is verlopen.

Typische waarden voor X en Y zijn twee, respectievelijk drie.

Toelichting: opdrachtgever acht de vakbekwaamheid van gegadigden op het gebied van het succesvol implementeren van Digikoppeling relevant voor de aanbesteding. Omdat Digikoppeling een waaier aan standaarden (en onderliggende standaarden) omvat is het wenselijk dat de te geven referenties beschrijven welke delen van de Digikoppeling-standaard hierbij betrokken waren.

Ratio: inschrijvers die geen ervaring hebben met Digikoppeling geven een hoog afbreukrisico. Een lichtere variant van deze eis kan zijn door expliciet ervaring met

10 In het geval de aanbestedende dienst een gemeente of provincie is zijn de Baseline Informatiebeveiliging Gemeenten (BIG) en de Interprovinciale Baseline Informatiebeveiliging toepasselijker.

11 Te vinden op http://www.logius.nl/producten/gegevensuitwisseling/digikoppeling/

de belangrijkste aan Digikoppeling ten grondslag liggende standaarden (WSDL[12], UDDI[13] en SOAP[14])[15].

3.2.4.5 SAML (Security Assertion Markup Language)

SAML[16] is een standaard voor *browser single sign-on* authenticatiediensten. Hiermee kan een bepaald niveau van authenticatiebetrouwbaarheid gerealiseerd worden zonder dat gebruikers per website of -applicatie opnieuw hoeven in te loggen, maar dit slechts eenmalig bij een *identity provider* hoeven te doen.

Eis

Gegadigde/inschrijver toont door middel van X referenties uit de afgelopen Y jaar aan dat hij ervarming heeft met de authenticatiestandaard SAML of daaraan gelijkwaardige authenticatiestandaarden. Een authenticatiestandaard is eerst gelijkwaardig als er sprake is van interoperabiliteit met SAML.

Typische waarden voor X en Y zijn twee, respectievelijk drie.

Toelichting: opdrachtgever is gestandaardiseerd op SAML voor *single sign-on* authenticatie. Alternatieve toelichting: opdrachtgever beoogt op termijn te standaardiseren op SAML voor *single sign-on* authenticatie en deze webapplicatie ligt op het groeipad naar deze beoogde situatie.

Ratio: SAML is de beoogde standaard binnen overheden voor authenticatie op websites en -applicaties.

3.2.5 Gunningseisen en -wensen

3.2.5.1 Webrichtlijnen

Eisen

Bij bouw:
De op te leveren webapplicatie dient te voldoen aan die onderdelen van de Webrichtlijnen versie 2 die betrekking hebben op toegankelijkheid en browseronafhankelijkheid.

Opbouw front-end van de webapplicatie:

- Structuur en vormgeving zijn gescheiden.
- De functionaliteit van de webapplicatie is niet afhankelijk van optionele technologie, zoals CSS en client-side script.
- cross-browser compatibiliteit

Bij exploitatie:
De te onderhouden webapplicatie dient te blijven voldoen aan de Webrichtlijnen versie 2 ter zake van toegankelijkheid en browseronafhankelijkheid.

Toelichting: de Webrichtlijnen versie 2 omvatten de W3C Web Content Accessibility Guidelines (WCAG) versie 2.0[17], een wereldwijde standaard om de toegankelijkheid van websites te waarborgen. Opdrachtgever wenst, conform het Nederlandse beleid op dit terrein , dat de/het te realiseren website/CMS geen concessies doet op het terrein van toegankelijkheid, doorzoekbaarheid en browseronafhankelijkheid.

12 http://www.w3.org/TR/wsdl
13 http://uddi.xml.org/
14 http://www.w3.org/TR/2000/NOTE-SOAP-20000508/
15 Alle drie deze standaarden zijn opgenomen op de lijst van gangbare standaarden, https://lijsten.forumstandaardisatie.nl/lijsten/open-standaarden?terms=&lijst=Gangbaar&status[]=Opgenomen&pagetitle=gangbaar
16 Te vinden op http://saml.xml.org/
17 http://www.w3.org/WAI/intro/wcag

Ratio: overheidsinformatie dient toegankelijk te zijn voor alle burgers, ongeacht of zij een (audio)visuele beperking hebben of niet. In het geval van een interne webapplicatie kan toegankelijkheid nog steeds een overweging zijn uit oogpunt van de gelijke behandeling van gehandicapten en chronisch zieken in termen van arbeidsomstandigheden.

Wens

Naast de eis te voldoen aan de webrichtlijnen dient leverancier aan te geven hoe het blijvend voldoen aan de Webrichtlijnen versie 2 geborgd is in het beheerproces.

Toelichting: het bij implementatie bewerkstelligen van toegankelijkheid biedt geen waarborgen voor de toekomst, opdrachtgever wil daarom inzicht hebben hoe dit voor de toekomst gewaarborgd wordt als onderdeel van het onderhoudsproces.

Ratio: overheidsinformatie dient toegankelijk te zijn voor alle burgers, ongeacht of zij een (audio)visuele beperking hebben of niet. Dit dient blijvend gewaarborgd te worden.

Voorbeeldbeoordeling (maximaal 10 punten):
De onderbouwing van de borging in het beheerproces wordt beoordeeld op de mate waarin helderheid wordt gegeven over de wijze waarop dit zijn weerslag krijgt in:

- werkbeschrijvingen en protocollen;
- testmethodieken;
- technisch signaleren van afwijkingen van de Webrichtlijnen versie 2;
- kennisborging bij de betrokken medewerkers.

3.2.5.2 ODF

Eis

Managementrapportages over de webapplicatie zijn beschikbaar in ODF 1.2 formaat of daaraan gelijkwaardig.

Toelichting: opdrachtgever wil geen (nieuwe) afhankelijkheden van andere documentformaten dan ODF 1.2 scheppen in zijn organisatie.

(In geval van documentgeneratie) Documentgeneratie moet ODF 1.2 of daaraan gelijkwaardige formaten ondersteunen. Gelijkwaardigheid van hogere versies van de ODF standaard wordt verondersteld. De OOXML standaard wordt niet als gelijkwaardig met ODF 1.2 gezien.

Toelichting: niet zelden worden documenten in een bewerkbaar formaat om bijvoorbeeld hergebruik te bevorderen. Om te voorkomen dat burgers gedwongen worden tekstverwerkingssoftware van specifieke leveranciers aan te schaffen is het noodzakelijk dat dit in een open documentformaat zoals ODF 1.2 gebeurt.

Ratio: ODF 1.2 is een strategisch documentformaat om leveranciersonafhankelijkheid voor documentenstromen binnen de overheid te bereiken. Dit maakt het met name mogelijk om de kantoorautomatisering los te koppelen van *back-end* verwerkingssystemen.

3.2.5.3 PDF/A

Eis

(In geval van documentgeneratie) Documentgeneratie moet PDF/A daaraan gelijkwaardige formaten ondersteunen.

Toelichting: documenten welke van overheidswege verstrekt zijn moeten ook in de toekomst ontsloten kunnen worden. Uit oogpunt van digitale duurzaamheid is het dan ook wenselijk een gegevensformaat te gebruiken wat hiervoor bedoeld is.

3.2.5.4 DKIM

Eis

E-mail-alert en -notificatiefuncties van de website zorgen er voor dat de authenticiteit van overheidsberichten gewaarborgd kan worden door middel van de DKIM-standaard (of daaraan gelijkwaardig).

Toelichting: opdrachtgever wil het '*spoofen*' van e-mails uit zijn naam voorkomen en wil daarom gebruik kunnen maken van de DKIM-standaard.

3.2.5.5 DNSsec

Eisen

(in geval van SaaS van de webapplicatie) De DNS-hosting gerelateerd aan de SaaS van de webapplicatie voorziet in ondersteuning van de DNSsec-standaard.

De DNSsec-standaard (of een gelijkwaardige standaard) dient ondersteund te worden bij het verzenden van e-mailberichten en -notificaties.

Toelichting: opdrachtgever beoogt een oplossing die het verspreiden van (onjuiste) informatie uit naam van opdrachtgever door kwaadwillende derden bemoeilijkt, zowel als het om toegang tot de webapplicatie zelf gaat als bij e-mailberichten en -notificaties.

Ratio: bij gebruik van deze standaarden is enerzijds de kans dat e-mailberichten van overheden in spamfilters van burgers terechtkomen kleiner en anderzijds kunnen burgers er meer op vertrouwen dat berichten die zij ontvangen ook daadwerkelijk van de overheid afkomstig zijn. Tevens draagt DNSsec er aan bij dat burgers en bedrijven meer zekerheid hebben dat de informatie die zij uit een overheidswebapplicatie opvragen daadwerkelijk van de overheid afkomstig is en niet van een kwaadwillende derde. Om dit te bereiken zijn gebruik van zowel de DKIM als de DNSsec-standaarden noodzakelijk.

3.2.5.6 IPv6

Eisen

De webapplicatie is benaderbaar via IPv6 met dezelfde functionaliteit als via IPv4.

(in geval van DNS-hosting) De DNS-hostingdienst is tevens voor IPv6-gebaseerde "user agents" beschikbaar en een domeinnaambevraging resulteert ("resolves") in een geldig IPv6-adres voor de website.

Toelichting: gezien de schaarse IPv4-adresruimte en de voordelen van IPv6 wil de opdrachtgever op termijn over kunnen stappen op IPv6 zonder dat een dergelijke migratie impact heeft op zijn informatiehuishouding en tegen zo laag mogelijke kosten. Opdrachtgever eist derhalve toekomstbestendigheid op dit terrein.

Ratio: nu niet strategisch inzetten op IPv6 betekent bij een toekomstige IPv6-migratie waarschijnlijk vroegtijdig uitfaseren van ICT-middelen die uitsluitend IPv4 ondersteunen. Uit doelmatigheidsoverwegingen is dit onwenselijk. Tevens biedt IPv6 meer mogelijkheden op het terrein van informatiebeveiliging, bijvoorbeeld bij het bestrijden van Distributed Denial-of-Service (DDoS) aanvallen.

3.2.5.7 Digikoppeling (standaard voor sector-overstijgende koppelingen)

Digikoppeling is een verzameling van standaarden voor met name het routeren en logistiek afhandelen van berichtenverkeer tussen overheden. Met name in het geval

van koppelingen met basisregistraties en/of uitwisseling van berichtenverkeer met overheden in andere bestuurslagen of andere sectoren (bijvoorbeeld tussen zorg en onderwijs) is deze standaard relevant.

Indien één van de volgende vragen bevestigend wordt beantwoord is het van belang om Digikoppeling uit te vragen:

- Gaat de applicatie informatie (berichten) uitwisselen met een van de stelselvoorzieningen zoals genoemd op de website van de e-Overheid (http://www.e-overheid.nl/onderwerpen/stelselinformatiepunt/stelsel-van-basisregistraties/basisregistraties)?
- Gaat de applicatie informatie (berichten) uitwisselen met een van de generieke voorzieningen van Logius zoals Digipoort, Digilevering, Digimelding en/of MijnOverheid?
- Gaat de applicatie informatie uitwisselen tussen twee of meer overheidsorganisaties anders dan met de bovengenoemde voorzieningen?

Digikoppeling is een set van standaarden waarbij veelal een keuze gemaakt zal worden die erg casuïstisch van aard is. Om deze eis uit te werken zal een dialoog met de betrokken IT-architecten onontbeerlijk zijn.

Ook als geen van deze vragen bevestigend beantwoord kan worden, is het voor de toekomst nuttig om Digikoppeling in de uitvraag mee te nemen als één van de volgende vragen bevestigend beantwoord kan worden:

- Gaat de applicatie informatie verwerken die gerelateerd is aan de informatie van de stelselvoorzieningen?
- Gaat de applicatie berichten uitwisselen met semi-overheidsorganisaties uit een van de volgende sectoren:
  - energie;
  - openbaar vervoer;
  - onderwijs;
  - sociale woningbouw;
  - gezondheidszorg;
  - publieke omroepen?
- Gaat de applicatie berichten uitwisselen met ZBO’s of andere organisaties met een publieke taak?
- Gaat de applicatie berichten uitwisselen over publieke dienstverlening zoals parkeren, zorg, veiligheid, rechtspraak, hulpverlening, publieke omroep, politiek, transport etc..

Eis

Bij bouw:

De aangeboden oplossing ondersteunt een koppelvlak op basis van Digikoppeling[18] of daaraan gelijkwaardig.

Bij exploitatie:

De aangeboden oplossing ondersteunt een koppelvlak op basis van Digikoppeling of gelijkwaardig en in het onderhoud worden nieuwe versies van deze standaard meegenomen.

18 Te vinden op http://www.logius.nl/producten/gegevensuitwisseling/digikoppeling/

3.2.5.8 SAML (Security Assertion Markup Language)

SAML[19] is een standaard voor *browser single sign-on* authenticatiediensten. Hiermee kan een bepaald niveau van authenticatiebetrouwbaarheid gerealiseerd worden zonder dat gebruikers per website of -applicatie opnieuw hoeven in te loggen, maar dit slechts eenmalig bij een *identity provider* hoeven te doen.

Eis

Bij bouw:

De aangeboden oplossing ondersteunt een authenticatiekoppelvlak op basis van SAML of daaraan gelijkwaardig. Voor de gelijkwaardigheid van een alternatief authenticatiekoppelvlak is interoperabiliteit met SAML een vereiste.

Bij exploitatie:

De aangeboden oplossing ondersteunt een koppelvlak op basis van SAML of gelijkwaardig en in het onderhoud worden nieuwe versies van deze standaard meegenomen. Voor de gelijkwaardigheid van een alternatief authenticatiekoppelvlak is interoperabiliteit met SAML een vereiste.

Toelichting: opdrachtgever is gestandaardiseerd op SAML voor *single sign-on* authenticatie. Alternatieve toelichting: opdrachtgever beoogt op termijn te standaardiseren op SAML voor *single sign-on* authenticatie en deze webapplicatie ligt op het groeipad naar deze beoogde situatie.

Ratio: SAML is de beoogde standaard binnen overheden voor authenticatie op websites en -applicaties.

3.2.6 Meetinstrumenten

3.2.6.1 Webrichtlijnen versie 2

Voor de Webrichtlijnen geldt dat automatische toetsinstrumenten nuttig zijn, maar het nut is wel begrensd. Beweringen dat wordt voldaan aan WCAG of Webrichtlijnen, die enkel zijn gebaseerd op de uitkomsten van een automatisch toetsinstrument (zie o.a. http://www.webrichtlijnen.nl/toetsen/wat-u-moet-weten), zijn per definitie onvoldoende betrouwbaar. De reden daarvoor is dat dergelijke instrumenten niet alles kunnen toetsen, eenvoudigweg omdat de hoeveelheid tests die betrouwbaar volledig automatisch kan worden uitgevoerd beperkt is. De uitkomst van een automatisch toetsinstrument is dus altijd een deelresultaat. Aanvullende menselijke beoordeling is nodig om succesvol te kunnen claimen dat aan WCAG of Webrichtlijnen wordt voldaan. In de volgende situaties zijn uitkomsten van een automatisch toetsinstrument heel bruikbaar:

- Om snel fouten op webpagina's te kunnen opsporen, zodat ze kunnen worden hersteld,
- Om snel een indicatie te kunnen krijgen van (mogelijke) problemen op een website, of op groepen websites, en
- Om beweringen te kunnen falsifiëren dat aan de gestelde eisen wordt voldaan. Immers, als door het toetsinstrument fouten worden gerapporteerd is weerlegbaar dat de bewering waar is.

De belangrijkste, uit de auditpraktijk afkomstige, aspecten waarop beweringen en de ondersteunende informatie dienen te kunnen worden beoordeeld zijn:

- Actualiteit,
- Volledigheid,

19 Te vinden op http://saml.xml.org/

- Juistheid, en
- (in gevallen waarbij een steekproef is gebruikt:) Representativiteit.

op het gebied van het aspect volledigheid zijn volledig automatische toetsinstrumenten tot dusverre ontoereikend gebleken.

3.2.6.2 IPv6

Een meetinstrument voor IPv6-compatibiliteit van een website of -service is te vinden op http://ip6.nl/

4 Afwijkingen: leg uit

4.1 Inleiding

Zoals in het inleidende hoofdstuk aangegeven ligt in het 'pas toe of leg uit'-beleid besloten dat er afgeweken kan worden, maar dat er dan een uitleg dient te volgen. In dit hoofdstuk de gronden voor afwijkingen en hoe de uitleg plaats kan vinden in het jaarverslag.

4.2 Gronden voor afwijkingen

In artikel 3 lid 2 van de Instructie rijksdienst inzake aanschaf ICT-diensten en ICT-producten worden een aantal mogelijke gronden voor het niet kiezen van producten die werken op basis van de open standaarden van de 'pas toe of leg uit'-lijst gegeven:

"Van het eerste lid kan worden afgeweken indien een dergelijke dienst of product naar verwachting in onvoldoende mate wordt aangeboden, onvoldoende veilig of zeker functioneert, of om andere redenen van bijzonder gewicht."

In de toelichting wordt daarover het volgende gezegd:

"Bij de laatste categorie zal het praktisch gezien gaan om aspecten van geld, tijd of capaciteit. Van onvoldoende aanbod zal bijvoorbeeld sprake zijn indien tevoren is te verwachten dat een product of dienst gebaseerd op een standaard uit de lijst naar verwachting niet of door een zeer gering aantal aanbieders wordt aangeboden.

De reden om niet te kiezen voor een open standaard zal wel enige substantie moeten hebben. Het is niet de bedoeling dat voor gesloten standaarden gekozen wordt enkel en alleen omdat het tijdsbeslag dan wat korter is of de kosten wat lager zijn. Het niet zelf beschikken over capaciteit is geen goede reden als die capaciteit eenvoudig valt in te huren of als er in de eigen organisatie nooit aandacht besteed wordt aan het op peil brengen van bestaande tekorten in de eigen capaciteit. "

Dat betekent dat in de gevallen dat er open standaarden als wens zijn uitgevraagd en er uiteindelijk voor een aanbieding is gekozen die één of meerdere open standaarden die relevant waren niet ondersteunen, er sprake is van een noodzaak tot uitleg. En ook dat er sprake moet zijn van een bijzondere situatie.

4.3 Jaarverslaggeving

In het geval er bij bestedingen in ICT (dus niet noodzakelijkerwijze aanbestedingen) niet is gekozen voor het toepassen van open standaarden die relevant zijn.

Voor het jaarverslag dient in ieder geval vermeld te worden voor welke investeringstrajecten er afgeweken is, waarbij er gekozen kan worden om vanuit het jaarverslag naar de daadwerkelijke uitleg op de eigen website te verwijzen.

Een goede uitleg over afwijkingen van een standaard bevat in elk geval de volgende onderdelen:

1. Specificatie: Welke standaard of welk(e) aspect(en) van de standaard betreft de 'leg uit'?
2. Oorzaak: Wat is de reden dat er (nog) niet aan kan worden voldaan?
3. Gevolg: Welke (mogelijke) gevolgen/beperkingen heeft het niet of niet volledig voldoen aan de standaard voor gebruikers of omgevingspartijen?

4. Alternatieven: Worden er alternatieven geboden voor de gevolgen/beperkingen die zijn ontstaan door het niet of niet volledig voldoen aan de standaard en waar zijn deze vindbaar?
5. Maatregelen: Welke maatregelen zijn of worden genomen om alsnog aan de standaard te kunnen voldoen?
6. Planning: Op welke termijn zullen de maatregelen zijn geïmplementeerd?