Handreiking Beheer Internetdomeinen Rijksoverheid

Juli 2021 - Versie 1.0

Rijksprogramma
Duurzaam
Digitale
Informatiehuishouding

Colofon

In opdracht van en in samenwerking met het
Rijksprogramma voor Duurzame Digitale
Informatiehuishouding (RDDI)

Projectnaam
Opschonen Websites

Projectleider
B. van den Brande

Auteur
Valentijn Grapperhaus (Bureau Forum Standaardisatie)

Datum
juli 2021

Contact
S. Kester
T +31 6 15 35 93 74
s.p.kester@minocw.nl
Rijnstraat 50 | Den Haag
Postbus 16375 | 2500 BJ Den Haag

Wijzigingshistorie

Versie 0.15	Maandag 15 maart 2021	Eerste versie tbv startbijeenkomst
Versie 0.40	Maandag 22 maart 2021	Concept voor projectgroep
Versie 0.50	Maandag 29 maart 2021	Concept voor projectgroep
Versie 0.80	Donderdag 8 april 2021	Concept voor projectgroep
Versie 0.85	Donderdag 15 april 2021	Concept voor projectgroep
Versie 0.90	Maandag 19 april 2021	T.b.v. interdepartementale reviewgroep
Versie 0.95	Maandag 26 april 2021	T.b.v. interdepartementale reviewgroep
Versie 0.96	Maandag 3 mei 2021	Reviewcommentaar verwerkt
Versie 0.97	Woensdag 5 mei 2021	Redactie door RDDI Communicatie
Versie 0.98	Maandag 17 mei 2021	Concept t.b.v. implementatieworkshops
Versie 1.0	Donderdag 1 juli 2021	Definitieve versie voor publicatie

Samenvatting

Voor een veilige en duurzame dienstverlening en informatievoorziening moeten organisaties binnen de Rijksoverheid hun domeinportfolio actueel en relevant houden. Deze handreiking:

- biedt deze organisaties een aanpak om hun domeinportfolio (verder) op orde te brengen. De aanpak beschrijft de belangrijkste aandachtsgebieden die een organisatie moet afstemmen, uitwerken, uitvoeren en/of regelen om de domeinportfolio inzichtelijk en effectief te maken.
- gaat in op de vraag hoe organisaties domeinnaambeheer structureel kunnen inbedden om de kennis en procedures om internetdomeinen te beheren te borgen in de organisatie

Inhoud

1 Inleiding

1.1 Probleemstelling

In onze digitale samenleving zijn internetdomeinen inmiddels kritieke infrastructuur. Ze staan centraal in de toegang tot digitale dienstverlening en informatievoorziening van de overheid aan miljoenen burgers en bedrijven. Maar het beheer van internetdomeinen binnen de Rijksoverheid schiet tekort. Gevolg is:

- internetdomeinen raken uit het zicht
- internetdomeinen voldoen mogelijk niet aan (veiligheids)eisen voor websites
- internetdomeinen lopen reële risico's op misbruik en fraude
- de kwaliteit van informatie en dienstverlening van de Rijksoverheid aan burgers, bedrijven en andere organisaties is onvoldoende

Voor een veilige en duurzame dienstverlening en informatievoorziening moeten organisaties binnen de Rijksoverheid hun domeinportfolio actueel en relevant houden.

1.2 Aanleiding

Aan internetdomeinen en websites worden vanuit de (Europese) wet- en regelgeving diverse eisen gesteld:

- beveiliging
- open standaarden
- privacyrichtlijnen (op grond van de Algemene verordening gegevensbescherming, AVG)
- toegankelijkheidseisen
- webarchivering

Uit analyses van Forum Standaardisatie blijkt dat lang niet alle overheidssites voldoen aan de gestelde eisen. Tekortschietend beheer speelt daarin een belangrijke rol. Voldoen aan de eisen gaat namelijk niet vanzelf; iedere domeinnaam en website heeft aandacht nodig. Actief beheer van internetdomeinen staat bij veel organisaties binnen de Rijksoverheid niet hoog op de agenda. Hierdoor ontstaat achterstallig onderhoud. En er komen ook steeds nieuwe internetdomeinen bij, zonder dat verouderde internet-domeinen worden geëvalueerd en eventueel uitgefaseerd.

Structureel domeinnaambeheer is noodzaak; iedere organisatie binnen de Rijksoverheid moet het domeinportfolio op orde brengen én houden. Opschoning van het domeinportfolio is voorwaarde voor een transparante, overzichtelijke, veilige en duurzame digitale informatiehuishouding én een coherente en adequate communicatie van overheidsinformatie richting de samenleving.

1.3 Doel en doelgroep

Het doel van deze handreiking is organisaties binnen de Rijksoverheid te stimuleren om het beheer van internetdomeinen op orde te brengen. Door 1. een projectmatige opschoningsactie en 2. verankering van structureel en duurzaam beheer in de organisatie.

Deze handreiking biedt een aanpak om hun domeinportfolio, de internetdomeinen die op hun naam staan, (verder) op orde te brengen. Bij het ontwikkelen van de aanpak is er dankbaar gebruikt gemaakt van de eerdere ervaringen van de kerndepartementen van VWS, SZW en BZK met inventarisaties, opschoonacties en/of beheer van internetdomeinen.

Idealiter volgt elke organisatie binnen de Rijksoverheid deze aanpak, zodat duidelijk wordt welke internetdomeinen er zijn en of ze voldoen aan de geldende eisen. Wie het domeinportfolio op orde heeft, ervaart een lagere beheerlast en kan de wildgroei van internetdomeinen het hoofd bieden.

De handreiking laat ook zien hoe organisaties domeinnaambeheer structureel kunnen inbedden, opdat de kennis en procedures om internetdomeinen te beheren, worden geborgd in de organisatie.

1.4 Scope

De handreiking is bedoeld voor alle organisaties binnen de Rijksoverheid en toepasbaar op alle typen internetdomeinen, zoals gebruikt voor of in de vorm van websites, e-maildomeinen, sub-domeinen, online magazines, parkeerpagina's, redirects, typosquatting domeinnamen, portalen etc.[1]

1.5 Opbouw

Deze handreiking bevat twee modules - die over en weer verwijzen voor verdieping:

1. Het domeinportfolio op orde brengen (hoofdstuk 2)
2. Duurzaam beheer internetdomeinen (hoofdstuk 3)

1.5.1 Het domeinportfolio op orde brengen

Deze module geeft een praktisch stappenplan richting (duurzaam) domeinnaambeheer: alle internet-domeinen van een organisatie op orde brengen door ze te inventariseren en te laten voldoen aan de eisen. De module beschrijft:

- doel en bereik van het traject
- de wettelijke eisen en richtlijnen die gelden voor internetdomeinen
- de belangrijkste aandachtsgebieden die een organisatie moet afstemmen, uitwerken, uitvoeren en/of regelen om te komen tot een inzichtelijk en effectief domeinportfolio
- omvang en kwaliteit van het bestaande domeinportfolio
- wie het project uitvoert
- welke partij(en) betrokken moeten worden
- de gewenste werkwijze
- hoe je voldoende draagvlak en middelen (bij betrokkenen) kunt realiseren
- de activiteiten en producten die nodig zijn

1.5.2 Stroomdiagram op orde brengen van het domeinportfolio

Het stroomdiagram (Figuur 1) schetst de verschillende fases, processen en activiteiten die onderdeel zijn van het op orde brengen van het domeinportfolio. Bovenaan staan de drie verschillende fases van dit onderdeel. Fases 1 en 2 linken door naar processen. Deze processen omvatten weer activiteiten die de werkzaamheden beschrijven die het (project)team dan moet uitvoeren.

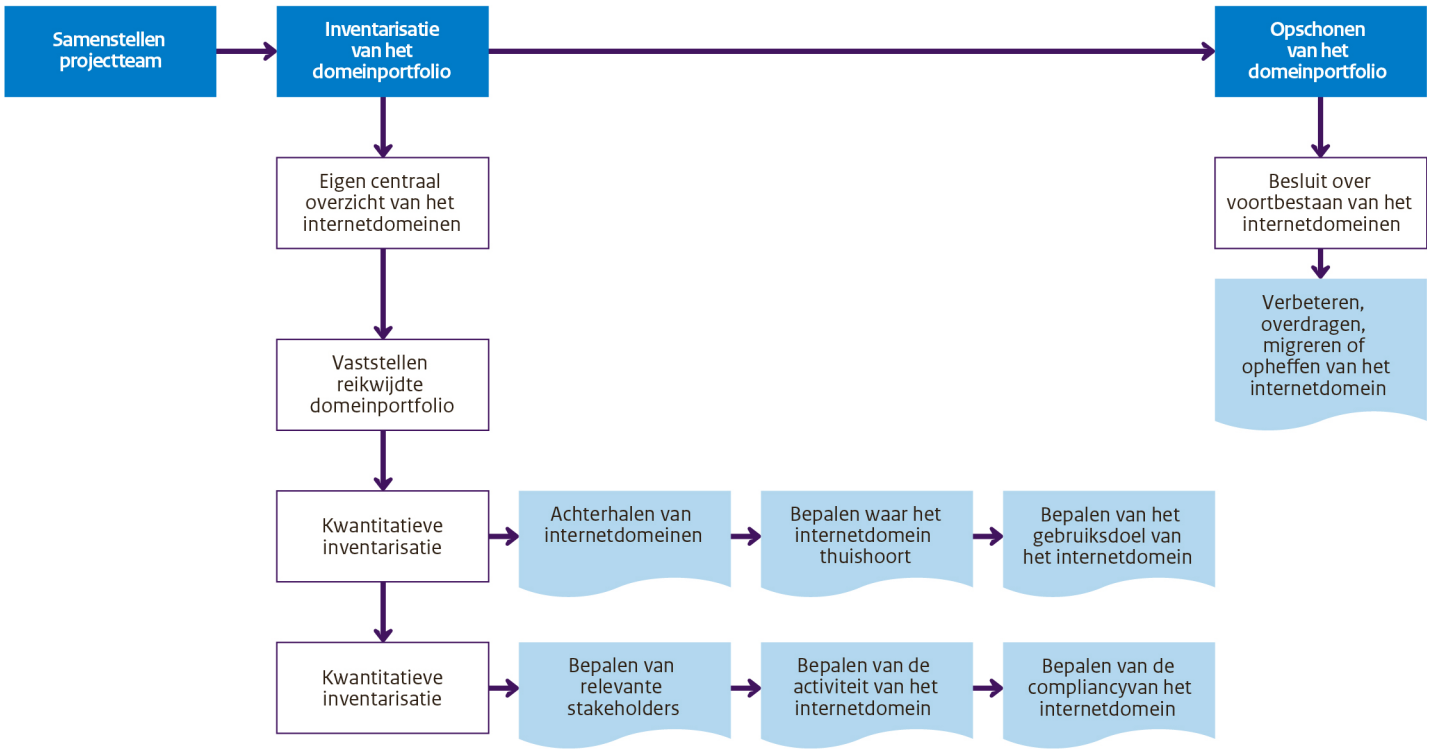
- **Fase 1 van 3:** Samenstellen (project)team (zie sectie 2.1)
  In deze fase stel je samen met de te betrekken partijen het projectteam en de aanpak vast.

- **Fase 2 van 3:** Inventarisatie van domeinportfolio (zie sectie 2.2)
  In deze fase brengt het (project)team het domeinportfolio in kaart aan de hand van 4 processen zoals aangegeven in Figuur 1 Stroomdiagram modelaanpak op orde brengen domeinportfolio.

- **Fase 3 van 3:** Opschonen van het domeinportfolio (zie sectie 2.3)
  In deze fase buigt het (project)team zich over het voortbestaan van elk internetdomein: moet het worden verbeterd of opgeheven?

1 Andere online middelen vallen niet binnen de scope van deze handreiking maar kunnen wel worden opgenomen in het projectplan voor opschoning van internetdomeinen.

Figuur 1: *Stroomdiagram modelaanpak op orde brengen domeinportfolio*



1.5.3 Duurzaam beheer internetdomeinen

Houd bij het orde brengen van de domeinportfolio (fase 1) rekening met hoe je het beheer op termijn duurzaam wilt inrichten (fase 2):

- **Beheer het domeinportfolio**
  Doel: Door zicht te hebben op je internetdomeinen wordt de beheerlast minder en wordt het makkelijker om te sturen op veiligheid, toegankelijkheid, grootte, overlappende informatie in- en relevantie van het domeinportfolio.

- **Beheer de levenscyclus van internetdomeinen**
  Doel: Doordat elk internetdomein aan de hand van een vooraf opgesteld plan actief wordt beheerd, blijft het domeinportfolio relevant en actueel. Dat vergroot de vindbaarheid en legitimiteit van informatie op websites.

- **Laat internetdomeinen voldoen aan open standaarden en webeisen**
  Doel: online informatievoorziening en dienstverlening bereikbaar via internetdomeinen voldoen aan afgesproken kwaliteitseisen t.a.v. onder meer veiligheid, betrouwbaarheid en toegankelijkheid. Internetdomeinen (en andere online middelen) die niet voldoen aan de eisen leveren risico's op voor zowel gebruikers als de organisatie zelf.

- **Hanteer herkenbare en eenduidige naamgeving van internetdomeinen**
  Doel: duidelijkheid; verwarring voorkomen. Verwarring over de echtheid van overheidsdomeinen heeft negatieve impact op het vertrouwen van burgers in (de echtheid van) andere overheidsdomeinen.

- **Zorg voor interne beheersing**
  Doel: goede coördinatie en een centrale controle met mandaat. Om samenhang en effectiviteit van het domeinportfolio te bewaken.

2 Het domeinportfolio op orde brengen

2.1 Samenstellen (project)team

Stel een betrokken en multidisciplinair team samen. Om het domeinportfolio van een Organisatie binnen de Rijksoverheid volledig inzichtelijk te krijgen, is er kennis nodig vanuit allerlei verschillende disciplines (communicatie, CIO, Bedrijfsvoering, ICT, afdeling archiefbeheer), organisatieonderdelen, werkprocessen en externe partijen.

Start het opschoningstraject alleen met een opdracht van een voldoende gemandateerde opdrachtgever die het traject kan regisseren en faciliteren. De opdrachtgever kan het mandaat halen bij de CIO (of eventueel via bestuursraad) waar duidelijke opdracht en deadlines worden afgesproken.

Spreek af hoeveel tijd de vertegenwoordigers van ieder betrokken discipline in het project steken.

Betrek de juiste partijen binnen de organisatie bij het samenstellen van het (project)team. Immers, internetdomeinen raken meerdere afdelingen en disciplines. Zie Figuur 2 voor een indicatie van de te betrekken stakeholders in het project.

Neem de 'liaison' (taak: registratieverzoeken beoordelen en doorgeven aan de Dienst Publieke Communicatie (DPC) die het centrale overzicht heeft van de Rijksoverheid; zie: Domeinnaambeleid van de Rijksoverheid) vanaf het begin mee in het traject. Maak de liaison actief onderdeel van het (project) team.

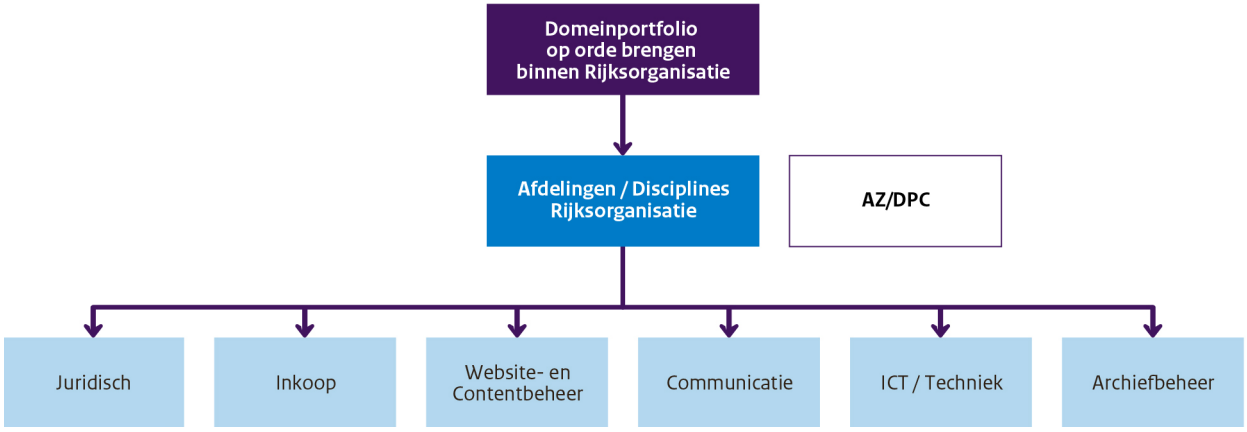
Kies voor één van de twee volgende aanpakken:[2]

- **Projectmatige aanpak:**
  Er is een duidelijk mandaat. De projectleider is de trekker en de stuurgroep opdrachtgever. Budget en resources zijn beschikbaar gesteld om het traject uit te voeren. Wees er van bewust dat na een projectmatige aanpak de activiteiten ook in de lijn ingericht moeten worden.

- **Aanpak in de lijn:**
  Het mandaat ligt of bij de eigenaar van een specifiek onderdeel dat betrokken is bij domeinnaam-beheer of bij de verantwoordelijke voor domeinnaambeheer. Budget en resources zijn veelal afkomstig van de betrokken afdelingen/directies. De trekker is hier veelal een medewerker van een CIO-office, afdeling informatievoorziening of communicatieafdeling.

2 Aanpak op een andere manier uitvoeren is natuurlijk ook mogelijk, bijvoorbeeld door middel van de scrum methode.

Figuur 2: *Te betrekken disciplines bij het op orde brengen van het domeinportfolio*



2.2 Inventarisatie van het domeinportfolio

Inventariseer de internetdomeinen van jouw organisatie. Hier kun je niet vroeg genoeg mee starten. Kwantiteit: welke domeinen behoren toe aan jouw organisatie? Kwaliteit: in hoeverre voldoen internet-domeinen en websites aan kwaliteitseisen, zoals verplichte standaarden en wet- en regelgeving? Het werkt het meest efficiënt als je de kwantitatieve en kwalitatieve inventarisatie van de websites combineert.

2.2.1 Vaststellen reikwijdte domeinportfolio

Stem de scope van het domeinportfolio af voordat je de grootte en relevantie van het domeinportfolio inventariseert: wat valt wel/niet onder het domeinportfolio van je organisatie? Welke (deel)organisatie(s) vallen er onder de organisatie en welke afspraken worden hiermee gemaakt?

2.2.2 Een eigen (centraal) overzicht internetdomeinen

Documenteer wat je inventariseert. Houd continu een overzicht bij van alle internetdomeinen samen met de kwantitatieve en kwalitatieve karakteristieken. Dit overzicht heb je ook nodig om informatie in op te slaan die uit externe bronnen kunnen worden gevonden, zoals het Domeinnaamregister van AZ/DPC, en om het duurzaam domeinnaambeheer structureel in te regelen. In Bijlage 1 zie je voorbeeld van een centraal overzicht in een Excel-tabel.

2.2.3 De kwantitatieve inventarisatie

De kwantitatieve inventarisatie is nodig om inzicht te krijgen in het aantal internetdomeinen dat een organisatie op haar naam heeft staan, wat het gebruiksdoel is, wie de eigenaar is van elk internetdomein en wie de beheerder.

De kwantitatieve inventarisatie kan uitgevoerd worden door de projectleider/het projectteam en/of de eigenaar in de lijn die de aanpak op zich heeft opgenomen. Op dit moment is het nog niet noodzakelijk alle betrokken stakeholders te spreken en daadwerkelijk te besluiten of een site blijft of niet. Deze stap is bedoeld om de omvang van het bestaande portfolio te bepalen en om het te verzetten werk in te schatten.

Het achterhalen van internetdomeinen

Wat betreft bestaande (externe) bronnen is het domeinnaamregister van AZ/DPC[3] het meest compleet. In het domeinnaamregister staan alle bij AZ/DPC geregistreerde internetdomeinen. Domeinnaambeheer van AZ/DPC houdt per domein bij of het nog actief is, welke karakteristieken gelden, zoals gebruiksdoel, communicatie over het domein en de uitslagen van de internet.nl web- en mailtest (o.a. compliancy op IPv6,: bereikbaar via modern internetadres; DNSSEC: domeinnaam ondertekend en HTTPS: beveiligde verbinding; DMARC, DKIM en SPF: echtheidswaarmerken tegen e-mailphishing en STARTTLS en DANE: beveiligde mailserver-verbinding).

Registratie van domeinen in het domeinnaamregister is verplicht. Volgens het Domeinnaambeleid moeten alle domeinnaamregistraties via AZ/DPC verlopen. Zij voegen deze toe aan het domeinnaam-register. Toch staan niet alle domeinen die in gebruik zijn bij departementen in het register. Dat heeft drie oorzaken:

- Ministeries hebben websites laten maken door externe partijen, die niet altijd de expertise en ingangen rondom webeisen hebben.
- Er zijn domeinen geregistreerd buiten het zicht van de liaison om.
- Er staan verouderde en vergeten domeinen online.

Om praktische redenen is het handig om naast het domeinnaamregister van AZ/DPC een eigen overzicht bij te houden met daarin de meest actuele status en overige gegevens over een domein. Zorg ervoor dat het eigen overzicht en het domeinnaamregister van AZ/DPC gelijk blijven door AZ/DPC tijdig te voorzien van de juiste informatie voor het rijksbrede domeinnaamregister.

Bepalen waar het internetdomein thuishoort

Bij de kwantitatieve inventarisatie hoort ook:

- bepalen waar het internetdomein thuishoort
- achterhalen wie verantwoordelijk is voor het internetdomein
- wie fungeert als contactpersoon. Dit is niet per sé de eigenaar: voor domeinen als ‘parkeerpagina’s’ en redirects is er soms geen duidelijke eigenaar. Neem als organisatie de regie over deze internetdomeinen.

Bepalen van het (gebruiks)doel van een internetdomein

Kies voor de kwantitatieve inventarisatie een passende aanpak om aan ieder internetdomein een gebruiksdoel te koppelen. Inventariseer dit ook voor de internetdomeinen die niet bij AZ/DPC bekend waren. Neem dit over in het centrale overzicht en geef het door aan AZ/DPC. Het bij hen bekende doel kan achterhaald zijn.

AZ/DPC houdt in het overzicht per internetdomein het (gebruiks)doel bij:

- Aliasdomein website
- Aliasdomein webapplicatie
- Beheer
- Commercieel
- Parkeerpagina-DPC
- E-mail
- Eigen parkeerpagina
- Hoofddomein website
- Intra-/extranet
- Nameserver
- Onbekend
- Onbestemd
- Quarantaine
- Redirectpagina

3 Het domeinnaamregister is anders dan het openbare websiteregister. Het websiteregister is een afsplitsing van het domeinnaamregister en bevat alleen domeinnamen met gebruiksdoel ‘Hoofddomein website’.

- Reservering
- Subsite
- Testdoeleinden
- Veiligheid
- Webapplicatie

Bijlage 5 geeft een overzicht met uitleg van elk van verschillende gebruiksdoelen die AZ/DPC aanhoudt.

2.2.4 De kwalitatieve inventarisatie

Na de kwantitatieve inventarisatie kun je inschatten hoeveel werk het is om de kwaliteit van het domeinportfolio te inventariseren. Er zijn twee inventarisatie-methodes:

1. Doorloop de stappen uit deze fase één voor één:
   - per stap alle internetdomeinen, of
   - per internetdomein alle stappen
2. Doe per type internetdomeinen (bijvoorbeeld voor alle websites) een uitvraag – tegelijkertijd naar de eigenaren/contactpersonen (Bijlage 3 is een voorbeeld van zo'n uitvraag).

Beoordeel in hoeverre de domeinen voldoen aan de webeisen en open standaarden en of een domein actueel is: is een website recent nog geactualiseerd en genereert een website nog bezoekers?

Kennis over de mate waarin het internetdomein voldoet aan de eisen en of deze nog actueel en noodzakelijk is, helpt later om te beslissen of je de site wilt verbeteren, migreren, saneren, archiveren en of je wel ovf niet wilt investeren in een toegankelijkheidsverklaring en beveiligingsmaatregelen. (In Bijlage 2 vind je de Instructie 'Hoe kom ik tot een toegankelijkheidsverklaring?').

Bepalen van relevante stakeholders bij een internetdomein

Bepaal relevante stakeholders bij internetdomeinen, zoals contactpersonen en verantwoordelijken/eigenaren, om te weten bij wie je moet zijn. De namen/contactpersonen uit het domeinregister van AZ/DPC zijn lang niet altijd actueel. Om te achterhalen wie verantwoordelijk is voor internetdomeinen en/of websites zal je in de organisatie navraag moeten doen, het kan ook zijn dat de verantwoordelijkheid nog niet eenduidig is belegd.

Rijksoverheidsorganisaties kunnen gebruik maken van het contract van AZ/DPC bij SIDN. Via SIDN kun je nagaan wie geregistreerd staat als houder, registrar, administratieve en technisch contactpersoon (zie ook https://www.sidn.nl/whois). Of gebruik een (gratis) tool om informatie op te vragen over de dns- en/of hosting instellingen van het domein en de subdomeinen. Als een domeinnaam via AZ/DPC geregistreerd is, staan deze gegevens altijd op Rijksoverheid en domeinnaam@minaz.nl.

Breng in kaart wie welke rol heeft: welk onderdeel/welke directie/welk programma is opdrachtgever? Welke collega is intern aanspreekpunt voor het beheer van deze site?
Neem deze stakeholders op in het overzicht.

Heb je geen contactpersoon/eigenaar gevonden? Kies dan voor een gezamenlijke aanpak: stuur bijvoorbeeld een lijst met deze internetdomeinen langs het CIO-office en de directie communicatie als laatste poging om de eigenaar, verantwoordelijke en/of contactpersonen te achterhalen. Levert dit geen naam op? Beschouw het domein dan als 'verweesd'.

Bepalen van de activiteit binnen het internetdomein
Ga de bezoekersstatistieken van websites in het afgelopen jaar na. Zelf, of door navraag bij de betreffende stakeholder. AZ/DPC neemt deze gegevens op in het domeinregister. Controleer dit.
Vraag mailactiviteit via de contactpersonen, of vanuit de liaison op bij de ICT-dienstverlener, zoals SSC-ICT.

Stel bij maildomeinen vast voor welke doeleinden wordt gemaild en welke partijen dat faciliteren.
Bepaal de actualiteit: wordt er iedere week, maand of kwartaal iets gepubliceerd, of is er lang niks gepubliceerd?

Bepalen van de compliancy van het internetdomein
In het register van AZ/DPC staan de uitslagen van de internet.nl web- en mailtesten zijn. Je kunt dit maandelijks automatisch gegenereerde overzicht opvragen bij AZ/DPC.

Er zijn ook tools om te kijken of een domein voldoet aan de webeisen, om een vollediger inzicht te krijgen of om tussentijds te controleren op verbeteringen. Deel deze metingen met relevante stakeholders, zoals een leverancier. Zo zien zij zelf ook wat de kwaliteit van het internetdomein is en op welke punten er nog werk aan de winkel is.

Afhankelijk van het type internetdomein (website-, e-mail-, redirect- etc.) gelden er bepaalde web-eisen. Kijk voor het meest actuele overzicht op: www.communicatierijk.nl/vakkennis/rijkswebsites/verplichte-richtlijnen.

In de Handreiking Verplichte richtlijnen websites en andere online middelen vind je meer informatie over de verschillende webeisen en open standaarden en hoe eraan te voldoen.[4]

2.2.5 Resultaat
De omvang van het domeinportolio is in kaart gebracht.
De status, kwaliteit en relevantie per internetdomein zijn duidelijk.

2.3 Opschonen van het domeinportfolio
2.3.1 Besluit over voortbestaan internetdomein
Waardeer de internetdomeinen:
- Is het internetdomein nog actief en actueel?
- Voldoet het internetdomein aan de webeisen?
- Spelen er politiek-bestuurlijke belangen?

Bepaal:
- Is het domein het waard om te investeren in verbeteringen?
- Worden de doelen met die verbeteringen (wel) bereikt?

Baseer je op de uitkomsten van de kwalitatieve inventarisatie.
Bespreek je bevindingen met de leverancier, eigenaar of opdrachtgever van het internetdomein en de projectleider en/of medewerker.
Schets de domein-eigenaar of opdrachtgever duidelijk de opties voor internetdomeinen die niet voldoen aan de verplichte kaders:
1. verbeteren
2. veilige redirect
3. opheffen conform vastgestelde procedures AZ/DPC
4. overdragen
5. migreren (content)

4 Zie ook: Modeltoets voldoen aan overige eisen websitearchivering.

Maak alle partijen de afspraken duidelijk:
- welke optie is er gekozen?
- binnen welke termijnen gebeurt er wát?
- wie is aanspreekbaar op wat?
- hoe wordt de voortgang gemonitord?

Noteer de beoogde actie voor elk internetdomein in het centrale overzicht. (Bijlage 1 is een voorbeeld van een centraal overzicht.)

Uitfaseren?
Is het domein niet meer actueel/nodig/relevant? Heeft een domein geen doel (meer)? Heeft een domein geen eigenaar en is een domein 'verweesd'? Faseer een domein dan uit. Volg de stappen uit 2.3.5.

2.3.2 Het verbeteren van een Internetdomein

Algemeen
Als het internetdomein nog wel relevant is, maar niet voldoet aan de kwaliteitseisen die eraan gesteld worden is het nodig om het domein te verbeteren. Het uitgangspunt is dat het domein na verbetering voldoet aan verplichte internetstandaarden (zorg dat je 100% scoort op internet.nl, zowel op de web- als de mailtest) en aan alle overige web eisen die van toepassing zijn op het internetdomein.

Website verbeteren
Een website kan verbeteringen nodig hebben op een of meer van de punten die naar voren zijn gekomen in de kwalitatieve inventarisatie. Bijvoorbeeld:
- Is de website niet actueel en/of trekt de website weinig bezoekers? Maak concrete afspraken. Bijvoorbeeld dat de eigenaar een content-agenda maakt en regelmatig publiceert. Spreek een bezoekersaantal als doel af. Beoordeel binnen een redelijke termijn of de website verbetert en nog bewezen nut heeft.
- Is de website onveilig? Neem op zo kort mogelijke termijn zoveel mogelijk mitigerende maatregelen.
- Ontbreekt de toegankelijkheidsverklaring? Stel deze op (zie: de instructie in bijlage 2).
- Wordt een niet-PRO-website niet automatisch gearchiveerd? (Voor alle PRO-websites is website-archivering geregeld.) Vraag binnen je organisatie hoe dit geregeld kan worden.

Redirects
Een redirect is een automatische doorverwijzing naar de juiste website. Als de oorspronkelijke naam van een website niet meer bestaat, voorkomt een redirect dat bezoekers een 404 foutmelding krijgen Vrijwel alle departementen gebruiken redirects voor een aantal websites. De SSC-ICT-departementen hebben in totaal meer dan 1.500 redirect-domeinnamen in bezit.

Redirects moeten voldoen aan verplichte internetstandaarden, daarom zijn TLS-certificaten ook noodzakelijk voor redirects. Er moet een logische –liefst uniforme- samenhang zijn tussen websites en subsites en bijbehorende redirects en typosquattingpagina's. Let hierbij ook op het gebruik van www.

Wanneer de organisatie veel redirects heeft is het handig als deze bij één dienstverlener in beheer zijn. De dienstverlener kan de redirects op een uniforme wijze configureren, zodat ze altijd voldoen aan de verplichte internetstandaarden. Ook verklein je hiermee de beheerlast over het totale domeinportfolio.

2.3.3 Het overdragen van een internetdomein

Behoort een internetdomein tot de organisatie, maar is de organisatie niet de eigenaar, bijvoorbeeld doordat het is opgericht in een samenwerkingsverband dat niet meer bestaan of door organisatorische herindeling? Draag het internetdomein zorgvuldig over, zodat het eigendom van de organisatie zelf wordt. Let op de aanvullende dienstverlening, zoals websitearchivering. Documenteer duidelijk dat, wanneer en aan wie de verantwoordelijkheden voor het domein zijn overgedragen. En geef het domein door aan AZ/DPC ter opname/aanpassing in het domeinregister van AZ/DPC.

Behoort het domein niet meer tot de Rijksoverheidsorganisatie? Draag het domein dan zorgvuldig over aan (stoot het af naar) de eigenlijke eigenaar. De overdracht aan een organisatie buiten de Rijksoverheid gaat via een gestandaardiseerd proces. Let op de aanvullende dienstverlening, zoals websitearchivering: zorg ervoor dat de archivering vanuit het departement stopt en dat de domeinnamen worden vrijgegeven. Laat AZ/DPC het domein uit het domeinregister halen.

2.3.4 Opheffen en het migreren van (de content) een internetdomein

Websites

Wordt de (PRO-)website niet meer gebruikt, maar is (bepaal)de content nog wel relevant?

1. Migreer de relevante content naar Rijksoverheid.nl. Op Rijksoverheid.nl krijgt de content een plek, bijvoorbeeld bij een bestaand dossier of wordt een nieuw dossier aangemaakt. Is de url of domeinnaam een merknaam of begrip geworden? Maak dan een redirect naar de betreffende pagina op Rijksoverheid.nl. Stem de migratie van content goed af met de redactie van Rijksoverheid.nl, bijvoorbeeld via de liaison. Is de migratie afgerond? Hef de (PRO-)website dan op volgens de stappen in 2.3.5 .

2. Migreer de content naar een nieuwe website op het Platform Rijksoverheid Online (PRO, zie www.platformrijksoverheiddemo.nl). PRO-websites hebben veel mogelijkheden en worden aangeraden omdat ze automatisch voldoen aan de eisen voor online communicatie. Wil je een PRO-site aanvragen? Vraag eerst akkoord van de liaison en vul dan een intakeformulier in.

Migreer je de content van een website? Denk er dan over na wat er met de oorspronkelijke domeinnaam gebeurt:

- Blijft de domeinnaam bestaan en maak je een redirect?
- Faseer je de domeinnaam uit? Zo ja: geef je de domeinnaam vrij?

Wordt de (PRO-)website niet meer gebruikt en is de content niet langer relevant?

3. Laat de website archiveren en maak een redirect naar de archiefversie.

2.3.5 Opheffen conform vastgestelde procedures AZ/DPC

PRO-websites

Hef je een PRO-website op? Faseer dan uit in samenwerking met de collega's van AZ/DPC. Archiveer de website en maak duidelijke afspraken over het wel of niet vrijgeven van de domeinnaam.

Algemeen

Hef je een niet-PRO-site op? Neem dan deze stappen om zorgvuldig uit te faseren.

Archiveer het domein. Gaat het gaat om een website? Archiveer op de aangewezen dienstverlener voor webarchivering. Overleg met het aanspreekpunt binnen de organisatie. Dit is afhankelijk van de datum van de laatste update en de laatste 'harvest'.

Spaar de vrij te geven domeinnamen op en geef ze periodiek vrij.

Wordt een domeinnaam vrijgegeven door de opdrachtgever?

- Behoud de domeinnaam voor ten minste 6 maanden (geen A/AAAA/CNAME-records, incl. no-mail policy, no-CAA policy).
- Verhuis de DNS-hosting naar DPC.
- Zet hem in quarantaine bij de registry.
  Andere organisaties kunnen niet 'shoppen'.
  AZ/DPC beoordeelt of interessante domeinnamen (generieke, 2/3-letters, etc.) behouden moeten blijven voor toekomstig gebruik.
- Is er voldaan aan alle vereisten voor een vrijgave? En is er bij andere rijksoverheidsorganisaties geen behoefte de domeinnaam te gebruiken? Dan doorloopt elke vrij te geven domeinnaam een quarantaine-termijn van minstens 6 maanden. In deze periode wordt het internetdomein geparkeerd en worden alle andere bestaande functionaliteiten uitgeschakeld (websites, e-mail, redirects, subdomeinen, etc.), en worden stricte no-mail- en no-index-policies ingesteld.

De no-mail policy beperkt (m.b.v. SPF-, DKIM-, DMARC- en Null MX-records in de DNS) de kans op e-mailmisbruik en informeert mailsystemen dat er geen e-mail (meer) in gebruik is op het domein. De no-index policy verzoekt (met robots.txt en HTML-metatags) externe zoekmachines zoals bijv. Google en Bing om het domein niet meer te indexeren, en de bestaande zoekresultaten van het domein te verwijderen uit hun zoekindices. Dit ondersteunt het opschonen van verouderde zoekresultaten in de indices van externe zoekmachines. DPC beheert in deze quarantainetermijn de DNS.

- Is de quarantainetermijn verstreken? Dan kan AZ/DPC de daadwerkelijke vrijgave in gang zetten bij de betrokken registries (voor .nl: SIDN).
  DNSSEC wordt uitgeschakeld en de DNS-gegevens worden verwijderd. Vanaf dit moment is het domein technisch volledig buiten gebruik.
- Is een vrijgave bij de registry ingediend? Dan start de quarantainetermijn van de registry (voor .nl domeinnamen: 40 dagen).
- Na de quarantaine bij de registry, is de registratie door de Rijksoverheid beëindigd en weer vrij ter registratie.
- Is het internetdomein veilig uitgefaseerd, dat wil zeggen zijn alle voorgaande stappen succesvol doorlopen? Verwijder het domein dan uit het centrale overzicht en vraag AZ/DPC het domein te verwijderen uit het domeinregister.

3 Duurzaam beheer internetdomeinen

Duurzaam beheer van internetdomeinen, of domeinnaambeheer, betekent: continue zorgdragen dat het domeinportfolio relevant en actueel is – en zorgen dat de éénmalige actie als beschreven in Hoofdstuk 5 niet/nooit meer nodig is. Het goed inregelen van duurzaam beheer van internetdomeinen vraagt vooral om tactische en strategische acties.

Neem als organisatie de regie om het beheer van internetdomeinen duurzaam en toekomstbestendig (her) in te richten. Voldoe aan alle eisen die aan de informatiehuishouding worden gesteld. Duurzaam beheer maakt het makkelijker voor een organisatie om online herkenbaar en weerbaar te blijven en om eenduidige onlinedienstverlening te bieden.

Er bestaat geen blauwdruk voor duurzaam domeinnaambeheer; het is organisatieafhankelijk. Dit hoofdstuk laat zien welke focus daarvoor nodig is, welke verantwoordelijkheden belegd kunnen/moeten worden, welke processen en procedures belangrijk (kunnen) zijn en (verder) gestroomlijnd moeten worden en hoe je naleving van die processen kunt controleren.

Dit hoofdstuk biedt handvatten om de eerste stappen richting een duurzaam beheer van internetdomeinen te zetten.

3.1 Beheer het domeinportfolio

Zorg dat je als organisatie zicht hebt op het domeinportfolio. Het inzichtelijk hebben van alle internet-domeinen verlicht de beheerlast en vergemakkelijkt de sturing op veiligheid, toegankelijkheid, grootte, overlappende informatie in- en relevantie van het domeinportfolio.

Centraal overzicht

Beheer van het domeinportfolio gaat vooral om: overzicht van alle internetdomeinen houden – en niet zo zeer om technische 'beheer'-werkzaamheden. Het helpt als dit centraal gebeurt.
Het is niet wenselijk dat verschillende onderdelen van een organisatie een eigen overzicht bijhouden (dat geeft meer afhankelijkheden en dus een grotere beheerlast).

Het centrale overzicht kan eruit komen te zien zoals in hoofdstuk 2 is beschreven. Om ervoor te zorgen dat het overzicht daadwerkelijk up-to-date is, kun je het periodiek naast het domeinregister van AZ/DPC leggen om de volledigheid van beide registers te controleren.

Met het centrale overzicht kun je sneller acteren, bijvoorbeeld als een internetdomein uit het domein-portfolio om aandacht vraagt. Geef elke wijziging wel door aan AZ/DPC.

Geef het centrale overzicht een goede plek binnen de organisatie. Beleg de verantwoordelijkheden daar waar voldoende kennis is. En zorg voor genoeg mandaat om op te treden en anderen aan te sturen of te bewegen, als het gaat om het verbeteren/uit faseren van internetdomeinen.

3.2 Beheer de levenscyclus van internetdomeinen

Vaak worden internetdomeinen simpelweg vergeten, of wordt er geen tijd (en geld) meer in geïnvesteerd om ze te verbeteren. Dat heeft tot gevolg dat er nog steeds internetdomeinen bestaan die verouderd zijn en dus een risico vormen. Ook websites met overbodige informatie hangen nog vaak in de lucht met dezelfde oorzaken. Uiteindelijk verminderen deze verouderde en/of overbodige internetdomeinen de vindbaarheid en legitimiteit van relevantie overheidsinformatie voor burgers en bedrijven.

Plan voor elk nieuw internetdomein

Voorkom dat er domeinen in de lucht blijven, terwijl zij hun doel al bereikt hebben en/of niet meer relevant zijn. Maak voordat een domein online gaat een plan voor elk (nieuw) internetdomein. Neem in dat plan op hoe lang je verwacht dat een internetdomein relevant blijft en met welk doel. Schat tevoren in wanneer het internetdomein zal worden uitgefaseerd. Neem een exit-strategie voor het internetdomein op in het plan. Toets periodiek de relevantie en beslis op basis daarvan of het domein blijft voorbestaan (zie ook: 2.3.1).

Bovenstaande beschrijving is vooral van toepassing op websites en subsites en dus ook op daarmee samenhangende redirects en typosquattingpagina's. De levencyclus van intra/extranetten, webapplicaties, emaildomeinen vraagt mogelijk een andere benadering. En die van test- en beheerdomeinen zijn ook weer anders. Specifieke strategieën hiervoor moeten worden uitgedacht.

Relevantie van internetdomeinen

Houd de relevantie van domeinen en onderliggende websites voortdurend in de gaten.
Zorg ervoor dat de content en informatie klopt en actueel is en de doelgroep wordt bereikt.
Dat kun je doen door naar bezoekersaantallen of de conversie te kijken, door de feedback van de doelgroep goed in de gaten te houden en ook door er specifiek naar te vragen bij je doelgroep.

3.3 Laat internetdomeinen voldoen aan open standaarden en web eisen

Internetdomeinen die niet voldoen aan eisen leveren risico's op voor zowel gebruikers als de organisatie zelf. Zorg dat je op de hoogte bent van webeisen en open standaarden. En zorg dat de staat en status van domeinen inzichtelijk zijn. Met een centraal overzicht heeft de organisatie al genoeg input om ook te monitoren op de staat en status. Daardoor kun je snel schakelen als dat nodig blijkt.

Periodiek meten van compliancy domeinportfolio

Door het constant of periodiek monitoren van de status van internetdomeinen, zijn problemen meteen zichtbaar en worden risico's maximaal beperkt.

Internetdomeinen compliant-by-design

Zorg ervoor dat (nieuwe) internetdomeinen bij oprichting al toekomstbestending zijn door bij aanvang al te voldoen aan alle eisen die aan het (type) internetdomein worden gesteld. Dit geldt ook bij inkoop/aanbestedingen: neem standaard de verplichte webeisen en open standaarden mee. Doordat internetdomeinen al bij inkoop compliant-by-design zijn, wordt de totale beheerlast minder.

3.4 Hanteer herkenbare en eenduidige naamgeving van internetdomeinen

De naamgeving van internetdomeinen moet duidelijk, herkenbaar en niet dubbelzinnig zijn. Verwarring over de echtheid van overheidsdomeinen heeft een negatieve impact op het vertrouwen van burgers in (de echtheid van) andere overheidsdomeinen. Het komt bijvoorbeeld vaak voor dat er een nieuwe website wordt geregistreerd, terwijl de content onder een bestaande website past. Door deze aanwas van nieuwe internetdomeinen is het lastig voor de burger om overheidswebsites te onderscheiden van private websites.

Het Rijksbreed afwegingskader online middelen schrijft zelfs voor dat je moet aansluiten op bestaande communicatiekanalen. Alleen als de bestaande kanalen geen uitkomst bieden, mag je een eigenstandig kanaal starten of behouden.

Sub domeinen

Gebruik sub domeinen van 'sterke merken', in plaats van nieuwe internetdomeinen te registreren,
Daarmee vergroot je de herkenbaarheid.
Kies voor overheidswebsites domeinnaamextensie die eindigen op .nl.

Domeinnaambeleid

Het kan voor burgers lastig zijn om domeinnamen van een organisatie binnen de Rijksoverheid te onderscheiden van private domeinnamen. Daarom zijn er voor domeinnamen van de Rijksoverheid afspraken gemaakt over communicatie van domeinnamen voor websites, social media en mobiel in het Domeinnaambeleid. Deze afspraken zorgen onder andere voor eenduidigheid en transparantie van beleid en gebruik van internetdomeinen. Het toplevel domein '.info' staat bijvoorbeeld niet in het Domeinnaambeleid.

3.5 Zorg voor interne beheersing

Zorg dat de verantwoordelijkheden voor content en beheer van internetdomeinen niet verspreid over en binnen de verschillende organisatieonderdelen liggen. Voor een goede coördinatie en om samenhang en effectiviteit van het domeinportfolio te bewaken, is een centrale controle met mandaat vereist.

Expertise binnen handbereik

Zorg dat er voldoende expertise over internetdomeinen voorhanden is. De liaison van de organisatie (vastgelegd in het https://domeinnaambeleid.nl) is vaak als enige aangewezen om de registratie en/of beheer van de internetdomeinen te coördineren. Maar de liaison heeft vaak geen technische achtergrond, waardoor sommige aspecten van internetdomeinen te weinig aandacht dreigen te krijgen. Dit geldt ook voor de eigenaren en/of verantwoordelijken van internetdomeinen.

Toezicht en controle

Beleg de rollen van toezicht en controle, bijvoorbeeld in de vorm van een poortwachter, en implementeer en beheer een centraal overzicht. Daarmee kun je actief handhaven op de volledigheid en compliancy van het domeinportfolio.

Een poortwachter kan de registratie en oprichting van internetdomeinen in goede banen leiden.
De rol van de poortwachter hoeft niet gelijk te zijn aan die van de liaison. De poortwachter kan bijvoorbeeld ook als houder/beheerder van het overzicht fungeren en nauw in contact staan met de bestaande liaison. De liaison heeft de taak om registratieverzoeken te beoordelen en door te geven aan de Dienst Publieke Communicatie (DPC) die het centrale overzicht hebben van de Rijksoverheid.

Overweeg om te zorgen dat je de bevoegdheid krijgt om internetdomeinen die niet aan de vereisten voldoen uit de lucht te halen. Komt dit (vaak) voor is er geen deugdelijke verklaring en/of komt er op korte termijn geen oplossing? Bevries het domein dan en plaats het in quarantaine. Hiervoor is mandaat van bijvoorbeeld de Bestuursraad nodig, omdat deze maatregel ingrijpt op het eigenaarschap van het domein.

Houd het centrale overzicht actueel en kloppend!

Sturende processen

Voorbeelden van sturende processen zijn:
- een routekaart voor een nieuwe website of
- een stappenplan voor het uitfaseren van internetdomeinen

Geef deze zelf vorm (in Bijlage 4 vind je als voorbeeld de routekaart van SZW).

Wat betreft de liaison-rol binnen de organisatie binnen de Rijksoverheid blijkt in praktijk de strikte variant het meest effectief. In deze constructie gaat AZ/DPC alleen in op de registratieverzoeken die via de liaisons zelf lopen, en dus niet van een andere medewerker van de betreffende organisatie. Sommige suborganisaties of ZBO's hebben eigen gemandateerde liaisons.

Inkoopopdrachten

Omdat er veel via inkoop wordt gedaan, moet je ook daarop sturen. Het is al Rijksbreed beleid dat alle domeinen bij DPC worden geregistreerd, dus de liaison móet al worden ingeschakeld voor een domeinnaam (en huisstijl). Maar de liaison heeft geen rol om ervoor te zorgen dat inkoopopdrachten ook rekening houden met andere eisen, zoals toegankelijkheid. Dat moet je borgen in het inkoopproces. Het beleid kan zijn om alle inkoopprocessen voor internetdomeinen ook langs de liaison te laten gaan of voorschrijven de handreiking van BKZ/UBR altijd te gebruiken, dan wel bij te voegen bij elke aanbesteding.

Let op: niet alle inkoop loopt via de centrale inkooporganisatie, bijvoorbeeld omdat het aan te besteden bedrag onder de drempel van de aanbestedingsplicht uitkomt of omdat een andere partij de aanbesteding uitvoert. Let ook op subsidierelaties en samenwerkingsverbanden.

4 Definities en begrippen

De (werk)definities van begrippen in het domein van domeinnaambeheer kunnen nogal uiteenlopen. Om verwarring over de betekenis en het gebruik van bepaalde begrippen en omschrijvingen te voorkomen lichten we in dit hoofdstuk een aantal begrippen kort toe.

Internetdomein

In deze handreiking gebruiken we omwille van de leesbaarheid vooral het begrip 'internetdomeinen', of kort: 'domeinen'. Wat er onder Besluit beveiligde verbinding met overheidswebsites en -webapplicaties als website en webapplicatie wordt begrepen, wordt hier aangeduid als (internet)domein.

Domein of domeinnaam?

Een domeinnaam, of domein, is letterlijk een naam in het DNS (Domain Name System). Het DNS is een naamgevingsysteem waarmee servers als webservers, mailservers of andere toepassingen kunnen worden geïdentificeerd. Normaal gesproken is de domeinnaam gekoppeld aan een (uniek) IP-adres.

Verschillende niveaus domeinen

Een domeinnaam kan in verschillende niveaus worden opgesplitst. Zo bestaat er hoofdniveau (Top Level Domain), middelniveau en onderniveau (subdomein). De verschillende niveaus worden gescheiden door punten in de domeinnaam. Het niveau is zichtbaar door de verschillende delen van de domeinnaam van rechts naar links te lezen.

Zie Tabel 1 voor een voorbeeld waarin het verschil tussen de verschillende niveaus en begrippen wordt geïllustreerd.

Tabel 1: *Definities en relaties*

.magazine	.forumstandaardisatie	.nl
Third-level domein Subdomein	Second-level domein	Top-level domein
	Domeinnaam	

4.1 Begrippenlijst

Domeinnaambeheer	alle processen, activiteiten en regels die betrekking hebben op beheer van internetdomeinen binnen een organisatie
Domeinportfolio	de verzameling van alle internetdomeinen die behoren (in)direct eigendom zijn van een organisatie
Open standaarden	Overheidsorganisaties zijn verplicht om, bij aanschaf van ICT-producten of ICT-diensten van € 50.000,- of meer, te kiezen voor de relevante standaarden die op de 'Pas toe of leg uit'-lijst staan.
Web eisen, verplichte richtlijnen	De Rijksoverheid hanteert verplicht toe te passen richtlijnen. Deze zijn vooral gericht op veiligheid, bescherming persoonsgegevens, toegankelijkheid en transparantie.
Typosquatting	Een vorm van misbruik van het internet gebaseerd op het feit dat mensen zich weleens vergissen bij het intypen van een website /domeinnaam (lees hier voor meer informatie). Typosquatting domeinen worden defensief geregistreerd om eventueel misbruik (registraties door kwaadwillenden) te voorkomen.
Redirect	Een redirect is een verwijzing. Een domein kan als redirect fungeren en re-direct door (3xx code) naar een andere bestemming op het internet.
Parkeerpagina	Een domein(naam) wordt (alvast) geregistreerd zonder dat het direct gebruikt wordt voor een website of een e-mailadres.

Bijlage 1
Voorbeeld centraal overzicht

Domein	Piwik URL redirect	Organisatie	directie/thema	Contactpersoon	Type	Mail	Aanpak	Domeinregistratie	DNS beheer	PKI certificaat	Hosting	Internet.nl web	Internet.nl mail	Digitoegankelijkheid indicatie	Webarchivering	AVG/cookiewet	Rijkshuisstijl websites en online formulieren	Piwik webanalyse	Bezoekersaantal per jaar	Bijzonderheden
mijnsite.nl		RIJK	Communicatie	-	Website	SSC-ICT	Opheffen	AZ/DPC	AZ/DPC	AZ/DPC	PRO	OK	OK	OK	OK	OK	OK	OK	180.000	In aanvraag
@emaildomein.nl		RIJK	Communicatie	-	E-mail		Verbeteren	n.v.t.			Extern	NOK	NOK	NOK	n.v.t.	NOK	NOK	n.v.t.	n.t.b.	Alternatief gewenst

Bijlage 2
Instructie Toegankelijkheid per website

Instructie toegankelijkheid website
Alle organisatieonderdelen van overheidsinstanties moeten een toegankelijkheidsverklaring publiceren voor iedere website waarvoor zij verantwoordelijk zijn.
In de verklaring staat in hoeverre de website al aan de eisen voldoet en welke maatregelen genomen worden om toegankelijkheid te borgen, inclusief planning. Bekijk het stappenplan op www.digitoegankelijk.nl.

Om de verklaring in te vullen moet je je website(s) laten onderzoeken op technisch en redactioneel gebied. Zo een onderzoek kost ongeveer 2500-4000 euro per website. Dit is afhankelijk van de grootte van je site en een aantal andere aspecten. Een dergelijk onderzoek moet je in het vervolg om de 3 jaar laten doen. Er bestaan verschillende bedrijven die je je websites kan laten onderzoeken.

Begin met een tijdelijke verklaring
Wanneer er niet de middelen beschikbaar zijn toegankelijkheidsonderzoek uit te voeren is het toch van belang (en verplicht) toch al de verklaring in te vullen zonder dat je de resultaten van je onderzoek hebt. Een tijdelijke verklaring geeft in ieder geval aan dat je er serieus mee bezig bent, wanneer het onderzoek gepland staat en dat in de nabije toekomst een update verwacht kan worden.

Ik beheer een PRO-site
In dat geval dien je alleen redactioneel onderzoek te laten doen. Het technische gedeelte is al ondervangen door AZ/DPC. Je kan bij het invullen van je verklaring de volgende informatie opnemen die geldt voor het technische gedeelte voor alle PRO-sites. https://www.platformrijksoverheiddemo.nl/toegankelijkheid/technische-afwijkingen-toegankelijkheid-pro.

Ik beheer een e-zine
In dit geval dien je ook alleen redactioneel onderzoek te laten doen. Het technische gedeelte wordt ondervangen door AZ/DPC, echter dit onderzoek loopt nog dus de verbeterpunten op dit gebied volgen nog.

Ik beheer een externe site
In dat geval moet je zowel technisch als redactioneel onderzoek laten doen om de verklaring op te kunnen stellen. Vraag ook de developer naar zijn efforts om jullie site digitaal te maken. Goed om te weten: wellicht kiest de developer een van de bedrijven om het onderzoek te laten doen en zullen ze 4000 declareren voor de kosten. Daar valt allicht nog wat op af te dingen: als het goed is stond in jullie contract dat de site digitoegankelijk zou moeten zijn. En zeer waarschijnlijk is het onderzoek naar het technische gedeelte nuttig en bruikbaar voor heel veel van hun andere sites, dus gebruik dat argument om niet het volle pond te betalen.

Mijn PRO-site/magazine moet nog live gaan
Laat dan een redactioneel onderzoek uitvoeren als de site/het magazine redelijk gevuld is. Als je site zich langzaam vult, kies dan een datum in de toekomst en vul deze datum vast in je tijdelijke toegankelijkheidsverklaring. Deze voldoet dan vast gedeeltelijk.

Mijn externe site moet nog live gaan

Zowel redactioneel als technisch zal dan een onderzoek moeten plaatsvinden. In principe geven we alleen opdrachten aan bureaus om technisch toegankelijk sites te ontwikkelen, laat het bureau bewijzen dat de site digitoegankelijk is. Dit zou je dus eigenlijk geen extra kosten moeten opleveren.
Redactioneel onderzoek kan je pas doen als de site gevuld is. Kies hier zelf een logische datum voor: de site moet redelijk gevuld zijn.

Invullen verklaring

De verklaring invullen is niet moeilijk. Er wordt ook gevraagd om 'de naam en functie van de tekenbevoegde manager of bestuurder die deze verklaring voor 'gezien en akkoord' tekent'. Dit betreft geen echte digitale handtekening, en die persoon komt zonder naam, maar wel in functie, op de verklaring te staan. Overleg met je manager of je haar/zijn naam en functie daar kan invullen.

Er wordt ook gesproken over het beschikbaar maken van de link naar alle online informatie en dienstverlening waarvoor de overheidsinstantie verantwoordelijk is. Een dergelijk overzicht komt er niet. De Rijksoverheid heeft al een openbaar webregister en daar komt de verklaring bij te staan. Je kan bij het invullen van de verklaring linken naar dit register: https://www.toegankelijkheidsverklaring.nl/register.

Bijlage 3
Voorbeeld uitvraag formulier

Project aanpak open standaarden domeinen BZK
Format plan van aanpak websitegerelateerde domeinen

Domeinnamen: de naam van het hoofddomein website, evt. bijbehorende subsites en alle gerelateerde domeinen.

Verantwoordelijke: contactgegevens van degene die verantwoordelijk is voor het gebruik en de instandhouding van de website. Als eigenaar/opdrachtgever beschouwen we in de regel de directeur van een BZK onderdeel. De inhoudelijk verantwoordelijke is het eerste aanspreekpunt voor zaken als het gebruik van de website en het voldoen aan de standaarden. De uitvoering van beheer en de implementatie van maatregelen wordt vaak door derden, bijvoorbeeld een technisch beheerder bij een externe dienstverlener, uitgevoerd.

Gebruik: korte beschrijving waar de website voor dient, wie er gebruik van maken (soort bezoekers, aantallen per maand) en het nut voor de organisatie. Indien van toepassing dient ook het gebruik van emailfunctionaliteit (inkomend en/of uitgaand) aangegeven te worden. In het geval er redirects naar deze website zijn, aangeven waarom deze nodig zijn. Als verwijzingspagina's niet per sé noodzakelijk zijn, dan dit aangeven en een planning maken voor het opheffen ervan.

Toegankelijkheid: aangeven van het huidige niveau (A-D) van de website en subsites en afhankelijk daarvan een beschrijving van de wijze waarop uiteindelijk naar niveau A wordt toegewerkt. Deze beschrijving graag zo SMART mogelijk, in elk geval dient duidelijk naar voren te komen:
Wie opdracht geeft voor het uitvoeren van een toegankelijkheidsonderzoek (zie de eerder toegezonden handleiding), wie dit gaat uitvoeren (bijv. welk bureau) en wanneer het onderzoeksresultaat verwacht wordt.

- Wie opdracht geeft om de maatregelen die voortvloeien uit het onderzoek te implementeren en wie dit gaat uitvoeren.
- Wanneer de implementatie zodanig zal zijn dat overgegaan kan worden naar niveau B (uiterlijk 31 december 2021) en wanneer naar niveau A.
- Hoe de realisatie hiervan geborgd is door sturing op resultaat (bijv. door hoge prioriteit er aan te geven in een agile werkwijze), voldoende beschikbare capaciteit en budget. Indien bekend ook graag de geschatte kosten en capaciteit aangeven.

Beveiliging: SMART beschrijving van de wijze waarop standaarden die nog niet zijn geïmplementeerd daadwerkelijk worden geïmplementeerd en wanneer dat gereed zal zijn. Voor alle standaarden geldt: hoe eerder hoe beter, maar uiterlijk 30 juni 2021 (m.u.v. Ipv6, deadline daarvoor ligt op 31 december 2021).
Evenals bij toegankelijkheid aangeven:

- Wie geeft opdracht en wie voert uit.
- Wanneer is de implementatie uiterlijk gereed.
- Hoe is realisatie hiervan geborgd.

Life cycle management: wat is naar verwachting de levensduur van de website (en daarmee ook van de gerelateerde domeinen)? Wellicht is de website na verloop van tijd minder relevant voor de beoogde doelgroep of komen er alternatieve informatiebronnen. Ook kan de website na verloop van tijd toe zijn aan een ingrijpende revisie, qua vormgeving, functies en inhoud. Als dit soort zaken worden voorzien, graag aangeven.

Datum:

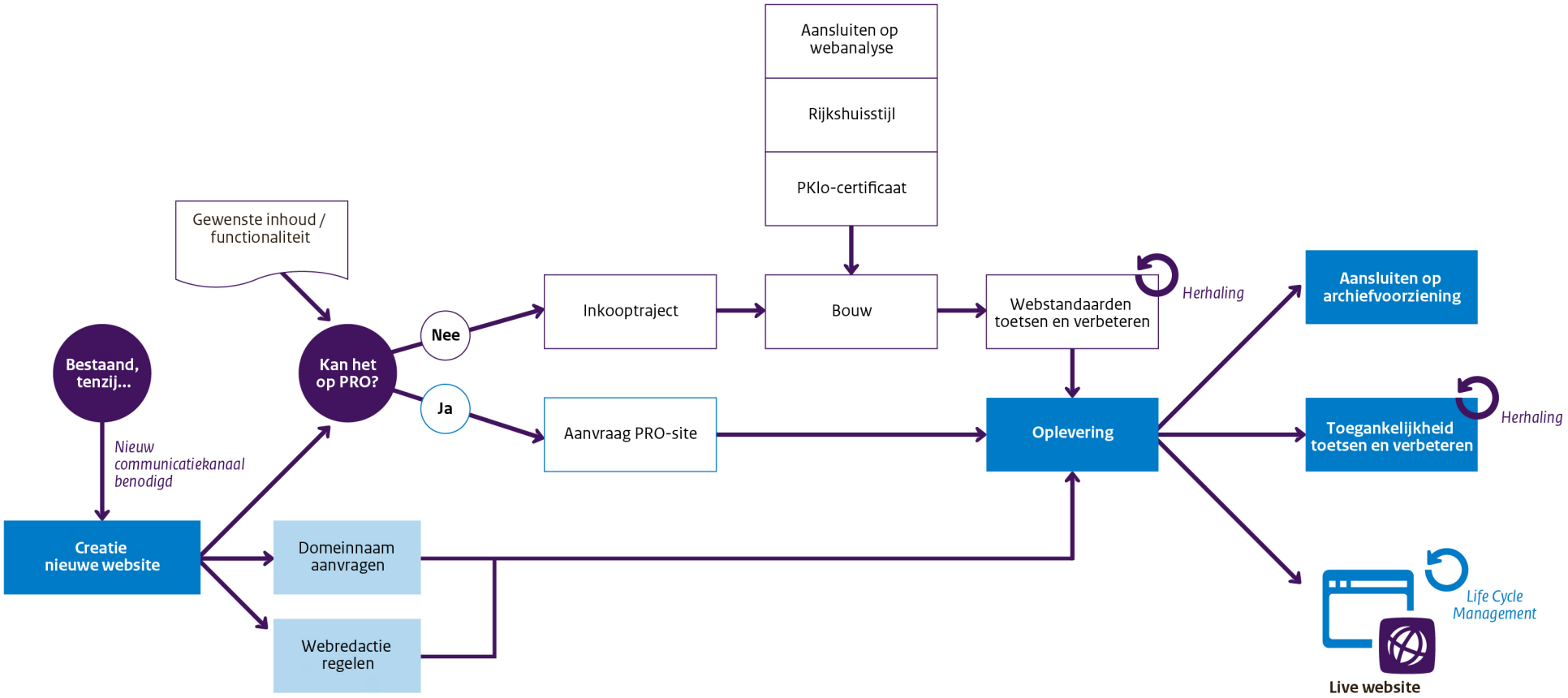
Opgesteld door: naam, functie, directie/afdeling.

Contactgegevens opsteller:

Afgestemd met: bij voorkeur in elk geval met de eigenaar /opdrachtgever (o.m. verantwoordelijk voor resultaat, financiering en capaciteittoedeling) en met de functioneel, technisch beheerder van de website (bijv. externe dienstverlener).

Bijlage 4
Routekaart nieuwe website SZW

Figuur 3: *Routekaart nieuwe website SZW (CONCEPT)*



Bijlage 5
Gebruiksdoelen domeinen volgens AZ/DPC

- **Aliasdomein website:** Domein wordt toegepast als alias van een hoofddomein website.
- Aliasdomein webapplicatie: Domein wordt toegepast als alias van een hoofddomein webapplicatie.
- **Beheer:** Domein wordt toegepast voor beheeractiviteiten zoals een fileserver.
- **Commercieel:** Domein wordt toegepast voor de exploitatie van commerciële activiteiten. Bevat vaak advertenties en/of is commercieel van aard.
- **Parkeerpagina-DPC:** Bevat de standaard parkeerpagina van DPC inclusief Rijkslogo en placeholder.
- **E-mail:** Domein wordt toegepast voor het ontvangen en/of versturen van e-mail.
- **Eigen parkeerpagina:** Bevat een parkeerpagina welke zelf ontwikkeld is, veelal een standaard template.
- **Hoofddomein website:** Domein wordt toegepast als hoofddomein van een website.
- **Intra-/extranet:** Domein wordt toepast om toegang te verkrijgen tot een intra-/extranet.
- **Nameserver:** Domein wordt toegepast als primaire- of secundair nameserver.
- **Onbekend:** Gebruiksdoel van dit domein is (nog) onbekend.
- **Onbestemd:** Gebruiksdoel van dit domein is onbestemd. Domein staat vaak op de nominatie om vrijgegeven te worden.
- **Quarantaine:** Vrijgaveproces van domein is in gang gezet.
- **Redirectpagina:** Domein re-direct door (3xx code) naar een andere bestemming op het internet.
- **Reservering:** Domein is gereserveerd voor toekomstig gebruik.
- **Subsite:** Domein bevat een website met dezelfde look-and-feel als hoofddomein website, maar bevat andere content.
- Testdoeleinden: Domein wordt toegepast voor testactiviteiten, bijvoorbeeld een staging-omgeving.
- **Veiligheid:** Domeinnaam is defensief geregistreerd uit veiligheidsoverwegingen.
- **Webapplicatie:** Domein bevat een webapplicatie, bijvoorbeeld een inlog van een CMS of applicatie.

Dit is een uitgave van:

Rijksprogramma Duurzaam Digitale
Informatiehuishouding (RDDI)

Juli 2021