Basiseisen voor betrouwbare, digitaal duurzaam toegankelijke archieven

Nederlandse vertaling

Core Trustworthy Data Repository Requirements

DSA-WDS, 2016

Nederlandse vertaling

Maart 2017

The Core TDR Standards and Certification Board does not offer formal approval of translations but has been made aware of this work. The Board re-iterates that all self-assessments and reviews must be undertaken against the English language Core TDR Requirements and reminds users of translations to ensure that the translation refers to the latest version of the standard. For further information about the Core TDR certification please contact info@datasealofapproval.org or go to https://www.icsu-wds.org/contact-info.

De Nederlandse vertaling is tot stand gekomen door
- Kees Waterman, DANS
- Margriet van Gorsel, Nationaal Archief
- Barbara Sierman, Koninklijke Bibliotheek
- Marcel Ras, Nationale Coalitie Digitale Duurzaamheid

Vertaling: Ad van Heijst eMIM, VHIC

This translation of the Core TDR Requirements V.1 (2016) (https://drive.google.com/file/d/0B4qnUFYMgSc-eDRSTE53bDUwd28/view) was undertaken by the Dutch Coalition on Digital Preservation (NCDD). Further information about this translation may be found at www.ncdd.nl with details of terminological extensions or amendments to the standard glossary at.

Voor meer informatie over de vertaling:
Nationale Coalitie Digitale Duurzaamheid
Postbus 90407
2509 LK Den Haag
info@ncdd.nl

Context en verantwoording

Toelichting op de basiseisen voor betrouwbare, duurzaam toegankelijke digitale archieven
Voor u ligt de Nederlandse vertaling van de basiseisen voor betrouwbare, duurzaam toegankelijke archieven zoals die door de *DSA-WDS Working Group on Repository Audit and Certification* in 2016 zijn opgesteld. De werkgroep heeft hierin de vereisten van het keurmerk Data Seal of Approval (DSA) en de ICSU World Data System (ICSU-WDS) samengevoegd. Deze basiseisen voor betrouwbare, duurzaam toegankelijke archieven (vertaling van *Core Trustworthy Data Repository Requirements*[1]) zijn bedoeld om de eigenschappen van digitale archieven, in eerste instantie in de (wetenschappelijke) onderzoekswereld te toetsen aan de hand van zestien richtlijnen[2]. Met deze Nederlandse vertaling hopen wij Nederlandstalige organisaties tegemoet te treden die zich oriënteren op of starten met een certificeringstraject.

Het belang van certificering
Archieven, musea en bibliotheken beheren in toenemende mate de digitale producten van onze samenleving en vervullen daarmee de rol van digitaal archief. Subsidieverstrekkers en financiers, dataproducenten en depotgevers, consumenten en gebruikers moeten erop kunnen vertrouwen dat deze beheerders de digitale collecties die zij onder hun hoede hebben voor de lange termijn veiligstellen en toegankelijk houden. De begrippen duurzaamheid en vertrouwen brengen in vele opzichten uitdagingen mee. Deze uitdagingen liggen op allerlei terreinen: organisatie, techniek, financiële en juridische aspecten, etc. Certificering kan een belangrijke bijdrage leveren aan het garanderen van de betrouwbaarheid en duurzaamheid van digitale archieven en daarmee delen van de digitale informatie-objecten die ons gezamenlijk erfgoed vormen. Vertrouwen ligt daar mede aan ten grondslag. Certificering biedt de mogelijkheid om dat vertrouwen meer meetbaar en inzichtelijk te maken – en bij alle belanghebbenden.

Certificering is geen kwestie van ‘alles of niets’. Daadwerkelijke en formele certificering en het behalen van keurmerken is van belang voor beheerders en e-depotvoorzieningen. Daarnaast kunnen de verschillende certificeringsinstrumenten ook gebruikt worden als checklists en handreikingen die helpen bij het evalueren van de eigen organisatie en de eigen processen. Het primaire doel is dan professionalisering, later mogelijk gevolgd door certificering.

Internationaal raamwerk
Informatiebeheerders en andere betrokkenen kunnen terugvallen op een raamwerk van verschillende internationale certificeringstandaarden voor digitale archieven om de kwaliteit van hun werkprocessen en beheersystemen te toetsen en te verbeteren. Een ‘trustworthy digital repository’

(tdr) is een term die dan vaak wordt gebruikt. In toenemende mate van complexiteit en diepgang zijn de volgende drie instrumenten beschikbaar: de *Core Trustworthy Data Repository Requirements (DSA-WDS)*, het nestorSeal (toetsing op DIN-standaard 31644) en de ISO-certificering (16363). De

[1] https://drive.google.com/file/d/0B4qnUFYMgSc-eDRSTE53bDUwd28/view
[2] http://www.datasealofapproval.org/en/information/requirements/

toetsing loopt in intensiteit uiteen van een 'peer review' van opgeleverde documentatie in het geval van DSA-WDS, tot een voorbereid 'on-site' bezoek van een extern audit-team in het geval van ISO. Dit stelsel van certificeringsinstrumenten is vastgelegd in het European Framework for Audit and Certification of Digital Repositories[3].

Samenwerking

Voor individuele collectiebeherende organisaties is het een lastige opgave om bij alle ontwikkelingen beargumenteerde keuzes in te maken. Vanuit verschillende programma's en initiatieven wordt hiervoor in Nederland ondersteuning geboden:

- Het Netwerk Digitaal Erfgoed (NDE) ontwikkelt een stelsel van landelijke voorzieningen en diensten voor het verbeteren van de zichtbaarheid, de bruikbaarheid en de houdbaarheid van digitaal erfgoed[4].
- De Nationale Coalitie Digitale Duurzaamheid (NCDD) heeft als missie het realiseren van een landelijk netwerk van voorzieningen die de duurzame toegang tot digitale collecties garandeert[5]. Vanuit deze missie geeft de NCDD invulling aan een van de drie werkpakketten van het Netwerk Digitaal Erfgoed, namelijk 'Digitaal Erfgoed Houdbaar'[6].
- Tot slot heeft het innovatieprogramma voor de Nederlandse archiefsector, Archief2020, een reeks aan activiteiten uitgevoerd de duurzame toegankelijkheid van (digitale) overheidsinformatie en een toekomstvaste archieffunctie ondersteunt[7].

Deze programma's en organisaties delen een landelijke ambitie tot samenwerking en hebben van daaruit een bijdrage geleverd aan de totstandkoming van de Nederlandse vertaling van de DSA-WDS-basiseisen voor betrouwbare, duurzaam toegankelijke archieven.

De Nederlandse vertaling

De Nederlandse vertaling van de DSA-WDS basiseisen is een product van het project 'Routekaart van certificering van e-depots' dat wordt uitgevoerd in het kader van de nationale strategie voor digitaal erfgoed. Dit project is onderdeel van het werkpakket Digitaal Erfgoed Houdbaar en richt zich op het vergroten van de bewustwording over certificering van digitale archieven en het benadrukken van de voordelen hiervan voor erfgoedinstellingen. Certificering op zichzelf is niet het enige doel, van belang is de mate van "volwassenheid" van een organisatie bij het omgaan met digitale collecties. Hiervoor is er door de projectgroep een zogenaamde routekaart voor certificering van digitale archieven opgesteld. Deze routekaart bevat een stapsgewijze aanpak, waarbij de eerste stap bestaat uit een evaluatie van de competenties van de eigen organisatie. Binnen het Netwerk Digitaal Erfgoed is hiervoor het 'Scoremodel Digitale Duurzaamheid' beschikbaar[8]. Deze tool biedt een overzicht van de sterktes en zwaktes van de organisaties en geeft aanwijzingen voor verbeteringen zodat men zich

[3] Memorandum of Understanding to create a European Framework for Audit and Certification of Digital Repositories. – 2010, http://www.trusteddigitalrepository.eu.
[4] http://www.den.nl/pagina/511/netwerk-digitaal-erfgoed/
[5] http://www.ncdd.nl
[6] http://www.ncdd.nl/projecten/netwerk-digitaal-erfgoed/
[7] Zie https://archief2020.nl . De looptijd van dit programma is t/m 2016.
[8] https://www.scoremodel.org

kan opmaken voor daadwerkelijke en formele certificering. Vervolgens propageert de projectgroep de gefaseerde aanpak van certificering conform het Europese raamwerk waarbij de toepassing van de DSA-WDS basiseisen de eerste formele stap is.

Hoewel men in het formele certificeringsproces gebruik dient te maken van de Engelse richtlijnen in het geval van een DSA-WDS certificeringsaanvraag, en deze ook in het Engels opgesteld dient te worden, is een Nederlandse vertaling van de eisen een hulpmiddel voor iedereen die aan het begin staat van een certificeringsproces. Een Nederlandse vertaling verlaagt voor erfgoedinstellingen de drempel om een dergelijk proces in te gaan en vergemakkelijkt de eerste stappen op weg naar formele certificering te zetten.

Vertaling nestor-seal

Naast de vertaling van de DSA-WDS basiseisen is er tevens een Nederlandse vertaling van de tweede certificeringsstap beschikbaar, het nestor-keurmerk, DIN 31664. Ook voor deze vertaling geldt dat hij hulp biedt bij de eerste stappen van het proces[9]. Nestor heeft een procedure ontwikkeld voor uitgebreide zelfevaluatie van digitaal duurzaam toegankelijke archieven op basis van de DIN 31644-standaard. Deze procedure biedt een gestandaardiseerde en praktische methode om de betrouwbaarheid van de digitaal duurzaam toegankelijke archieven te beoordelen. Het nestor-keurmerk is als certificeringsinstrument uitgebreider dan DSA-WDS en levert een grotere nauwkeurigheid dan een eenvoudige zelfevaluatie. Anderzijds is nestorcertificering minder compleet dan een intensieve externe audit, zoals die bij DSA-WDS plaatsvindt.

De vertaling van de DSA-WDS basiseisen is ondersteund, begeleid en medegefinancierd vanuit de overtuiging dat een Nederlandse vertaling de toepasbaarheid van het certificeringsinstrument zal vergroten.

Vertaling naar de eigen situatie

De tekst die voor u ligt is een Nederlandse vertaling van de Engelstalige basiseisen. De oorspronkelijke eisen zijn ontstaan binnen de context van het duurzaam beheren van wetenschappelijke data. Daarom wordt er in de oorspronkelijke Engelse tekst de term ‘(data) repository’ gehanteerd, daar waar de Nederlandse vertaling spreekt van ‘digitaal archief’. Deze laatste term is meer generiek van aard en daarmee breder toepasbaar op niet-wetenschappelijke instellingen. Over het algemeen is de terminologie in deze vertaling echter zo dicht mogelijk bij de oorspronkelijke tekst gebleven, dit om te voorkomen dat er een geheel nieuwe interpretatie van de richtlijnen ontstaat.

[9] http://www.ncdd.nl/wp-content/uploads/2016/02/Toelichting_nestor_keurmerk_NL.pdf

Basiseisen voor betrouwbare, digitaal duurzaam toegankelijke archieven (Basiseisen voor Digitale Archieven)

Achtergrond en algemene toelichting

De Basiseisen voor betrouwbare, digitaal duurzaam toegankelijke archieven[10] zijn bedoeld om de eigenschappen van digitale archieven weer te geven. Als zodanig zijn alle eisen verplicht en zijn zij gelijkwaardige, zelfstandige onderdelen. Alhoewel enige overlapping onvermijdelijk is, is deze waar mogelijk tot een minimum beperkt. De keuzes in deze checklist (bijvoorbeeld het type digitaal archief[11] en het niveau van preservering) zijn niet uitputtend en in alle gevallen is aanvullende ruimte voor het toevoegen van opties, waar deze worden gemist. Deze commentaren kunnen in de toekomst gebruikt worden om de basiseisen te verfijnen.

Elke eis in dit overzicht is voorzien van een toelichting om de aanvragers te helpen bij het aanleveren van voldoende bewijs dat hun digitale archieven aan de eisen voldoen. Er is aangegeven welke informatie een reviewer verwacht bij het uitvoeren van de toets. Verder moet de aanvrager het niveau aangeven tot welke hoogte aan een bepaald eis wordt voldaan.

0 Niet van toepassing
1 Het digitaal archief[12] heeft dit nog niet overwogen
2 Het digitaal archief heeft een theoretisch concept
3 Het digitaal archief is in de implementatiefase
4 De richtlijn is volledig geïmplementeerd in het digitaal archief.

Niveaus van compliance[13] vormen een bruikbaar onderdeel van het proces van zelfevaluatie, maar alle aanvragers zullen worden beoordeeld op verklaringen die onderbouwd zijn met deugdelijk bewijs, niet op zelf ingevulde niveaus van compliance. Zo moet een aanvrager ook, wanneer hij vindt dat een bepaalde eis niet van toepassing is, de reden hiervoor in detail documenteren. Merk ook op dat de complianceniveaus 1 en 2 kunnen gelden voor interne zelfevaluaties, terwijl certificering pas toegekend wordt wanneer een zeker aantal richtlijnen zich op niveau 3 bevindt, in de implementatiefase, omdat de eisen uitgaan van de continue verbetering van het digitaal archief.

De antwoorden op de vragen moeten in het Engels worden gesteld. Alhoewel geprobeerd zal worden om reviewers qua taal en discipline te koppelen aan organisaties, zal dit niet altijd mogelijk zijn. Als

[10] Omwille van de leesbaarheid wordt in het vervolg van dit document gesproken over digitale archieven, waar het betrouwbare, digitaal duurzaam toegankelijke (in casu: digitaal duurzame) archieven betreft. Deze worden ook wel aangeduid als repositories.
[11] In de oorspronkelijke tekst: repository.
[12] Ook hier en bij de andere niveaus is repository vertaald met digitaal archief.

[13] Compliance is het begrip waarmee wordt aangeduid dat een persoon of organisatie werkt in overeenstemming met de geldende wet- en regelgeving. Het gaat over het *nakomen* van normen of het *zich er naar schikken*.

de bewijsvoering in een andere taal is gesteld, dient een Engelse samenvatting geleverd te worden in de zelfevaluatie.

Omdat de basiscertificering geen bezoek op locatie inhoudt, moeten de eisen voorzien worden van links naar openbaar toegankelijk bewijs. Desondanks zal het om beveiligingsredenen niet altijd mogelijk zijn om alle informatie te vermelden op de website van een organisatie. Er zullen daarom binnen het certificeringsproces voorzorgsmaatregelen worden getroffen voor digitale archieven die gevoelig bewijs vertrouwelijk willen houden.

Digitale archieven dienen elke drie jaar opnieuw gecertificeerd te worden. Onderkend wordt dat, alhoewel basissystemen en mogelijkheden continue ontwikkelen dankzij techniek en gebruikersbehoeften, zij binnen deze periode geen grote veranderingen mogen ondergaan. De ISO-standaard voor Digitale Archieven (ISO 16363, Audit and Certification of Trustworthy Digital Repositories) heeft een vijfjarige reviewcyclus. Voor de basiseisen voor digitale archieven wordt een kortere reviewcyclus nodig geacht, zodat na het aanbrengen van verbeteringen en correcties een hernieuwde review binnen drie jaar mogelijk wordt.

Verklarende woordenlijst
Gebruik hiervoor de Core Trustworthy Data Repositories Requirements Glossary:
https://goo.gl/rQK5RN

Eisen

Achtergrondinformatie

Context

R0. Vul hieronder de context van uw digitaal archief in.

- ***Type digitaal archief*. Selecteer alle relevante types:**
  - **Op domein- of onderwerp gebaseerd digitaal archief**
  - **Digitaal archief van een instelling[14]**
  - **Nationaal digitaal archief, inclusief overheid**
  - **Digitaal archief voor data**
  - **Bibliotheek/museum/archief**
  - **Digitaal archief ten behoeve van een onderzoeksproject**
  - **Anders (graag omschrijven)**

Commentaar:

- ***Korte beschrijving van de gedefinieerde doelgroep[15] van het digitaal archief***
- ***Niveau van preservering*. Meerdere keuzes zijn mogelijk:**

  A. Content wordt beschikbaar gesteld zoals deze is gedeponeerd.

  B. Basispreservering– bijv. eenvoudige controle, toevoeging van basale metadata of documentatie.

  C. Uitgebreide preservering– bijv., het migreren naar nieuwe bestandsformaten, het verbeteren van documentatie.

  D. Informatie-niveau preservering– zoals bij C, maar aangevuld met het verrijken van gedeponeerde digitale objecten in verband met correctheid.

Commentaar:

- ***Partners in outsourcing*. Indien van toepassing, maak een lijst van de samenwerkingspartners**

- ***Andere relevante informatie***

Antwoord

Toelichting:

Om een digitaal archief te beoordelen, moeten reviewers informatie hebben om het digitaal archief in zijn context te plaatsen. Maak een keuze uit de opties en lever details aan voor de items uit de Contexteisen.

(1) ***Type digitaal archief*.** Dit onderdeel helpt de reviewers om de functie van het digitaal archief te begrijpen. Kies het antwoord dat het beste past voor uw type digitaal archief (selecteer meerdere opties als die van toepassing zijn). Als geen van de categorieën passend is, voegt u een beschrijving toe van het type waaraan

[14] Institutioneel repository
[15] Met gedefinieerde doelgroep wordt de designated community bedoeld in OAIS-termen.

uw digitaal archief voldoet. U kunt ook meer details leveren om de reviewer uw digitaal archief beter te doen begrijpen.

(2) ***De gedefinieerde doelgroep*** [16] ***van het digitaal archief***. Dit onderdeel helpt bij het beoordelen van de interactie tussen het digitaal archief en de beoogde gebruikersgroep. Zorg dat u er zeker van bent dat het antwoord specifiek is, dat u de doelgroep zo expliciet mogelijk omschrijft.

(3) ***Niveau van preservering***: Dit item is bedoeld om aan te geven of het digitaal archief zijn inhoud ongewijzigd distribueert naar gebruikers of waarde toevoegt door de content op een of andere manier te verrijken. Alle niveaus van preservering nemen aan dat de initiële deponeringen (SIP's) ongewijzigd blijven en dat wijzigingen uitsluitend worden gemaakt op kopieën van deze originelen. Annotaties of wijzigingen moeten onderdeel uitmaken van de termen van de licentie die met de producent is overeengekomen en moeten duidelijk vallen binnen de vaardigheden van wie de preserveringsacties uitvoert. Van het digitaal archief wordt daarom verwacht om te demonstreren dat elke annotatie of wijziging die is uitgevoerd, is gedaan en gedocumenteerd door deugdelijke experts en dat de integriteit van alle originele kopieën is behouden. Deze kennis helpt reviewers bij het beoordelen van andere certificeringseisen. Om de niveaus van preservering te begrijpen kunnen nadere details worden toegevoegd.

(4) ***Partners in outsourcing.*** Lever een lijst aan van partners waarmee de organisatie werkt op het gebied van digitale preservering. Beschrijf de aard van de relatie (organisatorisch, contractueel, etc.) en of de partner een assessment voor een digitaal archief heeft uitgevoerd. Zulke relaties hoeven niet beperkt te blijven tot diensten die geleverd worden door de instelling waar u deel van uitmaakt, door opslagcapaciteit van derden als deel van een meervoudige opslagpolicy, of lidmaatschap van organisaties die de zorg voor uw collectie overnemen als een probleem rijst in de continuïteit van het bedrijf. Maak een lijst van certificeringseisen waarin uw partner voorziet (geheel of gedeeltelijk), de relevante functionaliteit/service, zoals gesloten contracten of dienstverleningsovereenkomsten. Omdat outsourcing bijna altijd slechts gedeeltelijk zal zijn, zult u steeds zelf afdoende bewijs moeten leveren voor de certificeringseisen die niet uitbesteed zijn en voor de delen van de gegevenslevenscyclus, die u zelf beheerst. Kwalificaties, certificeringen, waaronder (maar niet beperkt tot) de DSA of WDS-certificeringen, genieten voorkeur voor partners. Het is echter voor hen niet nodig dat zij gecertificeerd zijn. We begrijpen dat dit een complex gebied kan zijn om te definiëren en te beschrijven, maar zulke details zijn nodig om zeker te zijn van een allesomvattend reviewproces.

(5) ***Andere relevante informatie.*** Het digitaal archief kan extra contextuele informatie toevoegen die niet in de eisen is opgenomen, maar die de reviewers helpt bij hun onderzoek. U kunt bijvoorbeeld beschrijven:

a. Het gebruik en de impact van de informatiebestanden in het digitaal archief (verwijzingen, gebruik in andere projecten, etc.);
b. Een nationale, regionale of globale rol die het digitaal archief dient;
c. Elke samenwerkingsorganisatie waar het digitaal archief onderdeel van uitmaakt.

[16] Hiermee worden bedoeld de designated communities, een binnen het OAIS, ISO 14721:2012, gehanteerde term.

Organisatorische infrastructuur

I. Missie/Scope

R1. Het digitaal archief heeft een expliciete missie om te voorzien in toegang tot informatieobjecten en deze te preserveren binnen een specifiek domein.

Compliance niveau:

Antwoord

Toelichting:
Digitale archieven nemen de verantwoordelijkheid voor het beheer van digitale informatieobjecten en om te verzekeren dat materialen in de geschikte omgeving worden bewaard gedurende de termijnen die van toepassing zijn. Het moet voor producenten van informatie en gebruikers duidelijk zijn dat preservering en een continue toegang tot de informatie een uitgesproken rol is voor het digitaal archief.

Beschrijf voor deze eis:

- De missie van uw organisatie in het preserveren en toegang verlenen tot de informatie, inclusief links naar expliciete verklaringen van deze missie.
- Het niveau binnen de organisatie waarop dit beleidsplan is goedgekeurd (bijv. goedgekeurde openbare verklaringen, rollen die zijn gemandateerd door financiers, door het bestuur ondertekende beleidsbesluiten).

II. Licenties

R2. Het digitaal archief onderhoudt alle toepasselijke licenties die betrekking hebben op de toegankelijkheid van informatie en het gebruik ervan en bewaakt de naleving.

Compliance niveau:

Antwoord

Toelichting:
Digitale archieven moeten alle toepasselijke licenties onderhouden betreffende de toegankelijkheid van informatie en gebruik, dienen hierover met gebruikers te communiceren en de naleving ervan te bewaken. Deze eis heeft betrekking op de regels voor toegang en de toepasbare licenties die door het digitaal archief zelf zijn bepaald. Eveneens voor de algemeen geaccepteerde gedragscodes voor de uitwisseling en het correcte gebruik van kennis en informatie in het relevante domein. Reviewers zullen bewijs willen dat het digitaal archief voldoende controlemomenten heeft ingebouwd in de toegangscriteria van hun informatie, en ook bewijs dat relevante licenties en de bijbehorende processen goed worden beheerd.

Beschrijf voor deze eis:

- De geldende licentieovereenkomsten;
- Gebruiksvoorwaarden (distributie, gebruiksdoelen, bescherming van gevoelige informatie, etc.)
- Documentatie over maatregelen in het geval van niet-nakoming van de toegangs- en gebruiksvoorwaarden

Wanneer informatieobjecten volledig openbaar zijn en zonder condities aan gebruikers beschikbaar worden gesteld kan dit worden vermeld. Een verdere toelichting is dan niet nodig.

Deze eis moet worden gelezen in samenhang met R4 (Vertrouwelijkheid/Ethiek) in zoverre dat ethische- en privacyregels impact hebben op de openbaarheid en toestemming tot gebruik. De zekerheid dat deze opslaglicenties voldoende rechten geven aan het digitaal archief om de informatieobjecten te beheren, preserveren en toegang tot de informatie te geven wordt behandeld onder R10 (preserveringsplan).

III. Continuïteit in toegankelijkheid

R3. Het digitaal archief heeft een continuïteitsplan om permanente toegankelijkheid te verzekeren tot de informatieobjecten en de preservering ervan.

Compliance niveau:

Antwoord

Toelichting:
Deze eis behandelt de maatregelen die genomen zijn om de toegankelijkheid en beschikbaarheid van zowel huidige als toekomstige informatieobjecten te garanderen. Reviewers zoeken bewijs dat de organisatie zich heeft voorbereid om de risico's die inherent zijn aan de veranderende omstandigheden, op te vangen.

Beschrijf voor deze eis:

- De mate waarin verantwoordelijkheid is genomen voor digitale informatieobjecten, inclusief de gegarandeerde perioden voor preservering.
- De middellange termijnplannen (drie tot vijf jaar) en lange termijnplannen (> vijf jaar) die opgesteld zijn om de continuïteit van beschikbaarheid en toegankelijkheid van de informatieobjecten te garanderen. In het bijzonder moeten zowel het antwoord op snelle verandering van omstandigheden als die voor langetermijnplanning zijn beschreven, waarin aangegeven is wat de mogelijkheden zijn voor verplaatsing of overdracht van activiteiten naar een andere instelling of teruggave van informatieobjecten aan hun eigenaren (dat wil zeggen, de producenten). Wat gebeurt er bijvoorbeeld als de financiering stopt. Dit kan het geval zijn bij een onverwachte intrekking van de subsidie, een gepland einde van de looptijd van de investering voor een in de tijd begrensd projectarchief of een verschuiving in de aandachtsgebieden van de instelling die de informatieobjecten als gastheer beheert.

Bewijs voor deze eis is meer gerelateerd aan governance[17] dan aan de technische informatie die nodig is voor R10 (Preserveringsplan) en R14 (Informatiehergebruik) en zou moeten leiden tot verandering van R1 (Missie/Scope). Deze eis is in contrast met R15 (Technische infrastructuur) en R16 (Beveiliging); het dekt de volledige bedrijfszekerheid van de functies van toegang en preservering.

[17] Governance is te vertalen als: goed en verantwoord bestuur, dat overeenkomt met alle eisen en verplichtingen die daaraan zijn te stellen.

IV. Vertrouwelijkheid/ethiek

R4. Het digitaal archief garandeert tot een zo hoog mogelijk niveau dat de informatieobjecten die worden gecreëerd, verrijkt, geraadpleegd en gebruikt, voldoen aan domeinspecifieke gedragscodes en ethische normen.

Compliance niveau:

Antwoord

Toelichting:

Het naleven van ethische normen is een kritische factor voor verantwoorde wetenschap. Openbaarmakingsrisico's - bijvoorbeeld het risico dat een persoon die deelnam aan een onderzoek kan worden geïdentificeerd, of dat de precieze locatie van een bedreigde diersoort kan worden bepaald, dat de privacy van personen wordt geschaad – zijn een zorgpunt waarop digitale archieven een antwoord moeten hebben. Het gezochte bewijs betreft niet alleen de good practices voor informatie met geheimhoudingsrisico's, maar ook de noodzaak om het vertrouwen van hen die persoonlijke/gevoelige informatie hebben opgeslagen in het digitaal archief niet te beschamen.

Voor deze eis moeten de antwoorden bewijs leveren op de volgende vragen:

- Op welke wijze voldoet het digitaal archief aan geldende gedragsregels, indien deze op het gebruik van de informatieobjecten van toepassing zijn?
- Vraagt het digitaal archief om bevestiging dat de verzameling of creatie van informatie is uitgevoerd in overeenstemming met de juridische en ethische standaarden die gelden in het geografische gebied of vakgebied van de producent van de informatie?
- Worden specifieke procedures toegepast voor het beheer van informatie waarop openbaarmakingsrisico's van toepassing zijn?
- Wordt informatie met openbaarmakingsrisico's opgeslagen met beperkende toegang?
- Wordt informatie met openbaarmakingsrisico's gedistribueerd onder gepaste voorwaarden?
- Zijn er procedures op basis waarvan gereviewd wordt of informatie onderhevig is aan openbaarmakingsrisico's, en worden maatregelen genomen om bestanden te anonimiseren en/of een beveiligde toegang te bieden?
- Is het personeel opgeleid in het beheer van informatie waarvoor een openbaarmakingsrisico's geldt?
- Zijn er maatregelen vastgelegd als niet aan voorwaarden wordt voldaan?
- Voorziet het digitaal archief in richtlijnen met betrekking het verantwoord gebruik van informatie die privacygevoelig is, niet openbaar of beperkt openbaar en daardoor een potentieel openbaarmakingsrisico's bevat?

Het bewijs voor deze eis moet in overeenstemming zijn met wat is aangeleverd als bewijs voor de procedures die genoemd zijn in R12 (Werkprocessen) en voor licenties in R2 (Licenties).

V. Organisatorische infrastructuur

R5. Het digitaal archief beschikt over voldoende financiële middelen en voldoende gekwalificeerd personeel dat wordt aangestuurd op basis van een helder governance-model om doelmatig de missie te kunnen uitvoeren.

Compliance niveau:

Antwoord

Toelichting:

Digitale archieven hebben financiële middelen nodig om hun verantwoordelijkheden te kunnen uitvoeren en daarnaast bekwaam personeel met expertise in digitale archivering. Niettemin is de continuïteit van de financiering zelden gegarandeerd. Dit moet gewogen worden tegen de noodzaak tot stabiliteit.

Voor deze eis moeten de antwoorden bewijs leveren met betrekking tot de volgende vragen:

- Het technisch beheer van het digitale archief vindt plaats bij een daarvoor erkende instelling (wat stabiliteit op lange termijn en duurzaamheid garandeert) die aansluit bij de specifieke doelgroep.
- Het digitaal archief beschikt over voldoende middelen, inclusief personeel, IT-middelen en een opleidingsbudget. Idealiter beslaat dit budget een periode van drie tot vijf jaar.
- Het digitaal archief zorgt ervoor dat het personeel voldoende trainingsmogelijkheden heeft en zich professioneel kan ontwikkelen.
- De verschillende terreinen en diepgang van de expertise van de organisatie en het personeel, inclusief relevante lidmaatschappen van de organisatie (bijv. nationale en internationale instellingen) sluiten aan bij de missie.

Volledige beschrijvingen van de taken die worden uitgevoerd door het digitaal archief – en de nodige vaardigheden- moeten worden geleverd, indien deze beschikbaar zijn. Zulke beschrijvingen zijn niet verplicht omdat dit detailniveau verder gaat dan de scope van de basiscertificering.

VI. Expertise

R6. Het digitaal archief voorziet in mogelijkheden om voldoende ondersteuning in expertise veilig te stellen en feedback te ontvangen (intern dan wel extern, inclusief inhoudelijke ondersteuning indien dit relevant is).

Compliance niveau:

Antwoord

Toelichting:

Een doelmatig werkend digitaal archief streeft ernaar om de evolutie in datatypes, datavolumes en data verwerkingssnelheden te volgen en zich de nieuwste en meest effectieve technologieën eigen te maken om zo waarde te behouden voor de specifieke doelgroep. Gelet op de snelle technische veranderingen in de wereld van de digitale informatie is het daarom aan te bevelen voor een digitaal archief om op regelmatige basis advies en feedback van gebruikers (de designated community) te verkrijgen, om te zorgen dat zij haar waarde behoudt en zorgt voor voortdurende verbetering.

Voor deze eis moeten de antwoorden bewijs leveren met betrekking tot de volgende vragen:

- Heeft het digitaal archief interne adviseurs of een externe adviesraad die mogelijk beschikt over technici, materiedeskundigen en experts op het gebied van digitale archivering en de typen informatieobjecten die worden beheerd?
- Hoe communiceert het digitaal archief met experts voor het verkrijgen van advies?
- Hoe communiceert het digitaal archief met zijn specifieke doelgroep om feedback te ontvangen?

Deze eis zoekt bevestiging dat het digitaal archief toegang heeft tot objectief advies van experts naast dat van de getrainde eigen staf die genoemd is in R5 (Organisatorische infrastructuur).

Het beheer van digitale informatieobjecten

VII. Informatie integriteit en authenticiteit

R7. Het digitaal archief garandeert de integriteit en authenticiteit van de informatieobjecten

Compliance niveau:

Antwoord

Toelichting:
Het digitaal archief moet bewijs leveren dat het gebruik maakt van een informatie- en metadata managementsysteem dat geschikt is om integriteit en authenticiteit te waarborgen gedurende ingest, archiefopslag en toegang tot de informatieobjecten.

Integriteit zorgt ervoor dat wijzigingen in informatie en metadata zijn gedocumenteerd en herleid kunnen worden tot de reden voor een wijziging en degene of datgene waardoor de verandering werd geïnitieerd.

Authenticiteit betreft de mate van betrouwbaarheid van de originele gedeponeerde informatie en de bijbehorende herkomst, inclusief de relatie tussen de originele en de beschikbaar gestelde informatie en de vraag of de relaties tussen informatie en/of metadata al dan niet behouden zijn.

Voor deze eis moeten de antwoorden over data-integriteit bewijs leveren met betrekking tot het volgende:

- Beschrijving van controles om te verifiëren dat een informatieobject niet is gewijzigd of corrupt is geraakt (dat wil zeggen: *fixity* controles).
- Documentatie over de volledigheid van informatie en metadata.
- Details met betrekking tot de vraag hoe alle wijzigingen in informatie en metadata worden gelogd.
- Beschrijving van de strategie van versiebeheer.
- Gebruik van relevante internationale standaarden en richtlijnen (specificeer deze).

Bewijs van de authenticiteit betreft de onderstaande vragen:

- Heeft het digitaal archief een strategie voor wijziging van de informatie? Is deze strategie bekend gemaakt?
- Houdt het digitaal archief informatie over herkomst en bijbehorende *audit trails* bij?
- Houdt het digitaal archief, indien van toepassing, verwijzingen naar metadata en andere datasets bij? Zo ja, hoe?
- Vergelijkt het digitaal archief essentiële eigenschappen van verschillende versies van hetzelfde bestand? Hoe is het versiebeheer geregeld?
- Controleert het digitaal archief de identiteit van degenen die informatie aanleveren in het digitaal archief?

Deze eis betreft de gehele levenscyclus van informatie die zich in het digitaal archief bevindt en heeft dus relaties met stappen in werkprocessen t.a.v. andere eisen – bijvoorbeeld R8 (Waardering) voor ingest, R9 (Gedocumenteerde opslagprocedures) en R10 (Duurzaamheidsplan of Preserveringsplan) voor opslag in het archief en R12-R14 (Werkprocessen, het ontdekken en identificeren van informatie en hergebruik) voor distributie. Niettemin kan het bewaken van de integriteit en authenticiteit van de informatie ook worden beschouwd als de verantwoordelijkheid van de beheerder van het digitaal archief.

VIII. Waardering

R8. Het digitaal archief accepteert informatie en metadata gebaseerd op gedefinieerde criteria om de relevantie en begrijpelijkheid van de informatieobjecten voor de gebruikers zeker te stellen.

Compliance niveau:

Antwoord

Toelichting:
De waarderingsfunctie is kritiek om te bepalen of informatie voldoet aan alle criteria voor opname in de collectie en om de juiste wijze van preservering ervan vast te stellen. Op een zorgvuldige manier moet ervoor gezorgd worden dat de informatie relevant en begrijpelijk is voor de specifieke doelgroep die door het digitaal archief wordt bediend.

Voor deze eis moeten de antwoorden bewijs leveren met betrekking tot de volgende vragen:

- Gebruikt het digitaal archief een ontwikkelbeleid voor de collectie om de informatie te selecteren die voor archivering in aanmerking komt?
- Hanteert het digitaal archief kwaliteitscontroles om de volledigheid en begrijpbaarheid van de opgeslagen informatie zeker te stellen? Zo ja, geef verwijzingen naar kwaliteitsstandaarden en rapportagemethodieken die geaccepteerd zijn door het vakgebied en geef details over hoe problemen worden opgelost (bijv. wordt de informatie teruggestuurd naar de producent voor herstel, wordt het hersteld door het digitaal archief, worden metadata m.b.t. de kwaliteit[18] gemaakt in het informatiebestand en/of opgenomen in de bijbehorende metadata)?
- Gebruikt het digitaal archief procedures om te bepalen of de vereiste metadata [19] en het gebruik van informatie zijn aangeleverd?
- Hoe gaat het digitaal archief om met metadata die niet voldoende blijken te zijn voor preservering op lange termijn?
- Heeft het digitaal archief een lijst van voorkeursformaten gepubliceerd?
- Zijn er kwaliteitscontroles om ervoor te zorgen dat producenten zich conformeren aan de voorkeursformaten?
- Wat is het beleid ten aanzien van informatie-objecten die zijn gedeponeerd in niet-voorkeursformaten?

Deze eis betreft kwaliteitsborging vanuit het perspectief van de interactie tussen de leverancier van de informatie en metadata en het digitaal archief. Dit in tegenstelling tot R11 (gegevenskwaliteit) dat gaat over metadata en datakwaliteit vanuit het perspectief van de specifieke doelgroep.

[18] In oorspronkelijke tekst: quality flags
[19] In de oorspronkelijke tekst: metadata, nodig voor de interpretatie: “metadata required to interpret and use the data”

IX. Gedocumenteerde opslagprocedures

R9. Het digitaal archief past gedocumenteerde processen en procedures toe bij het beheer van de gearchiveerde informatie

Compliance niveau:

Antwoord

Toelichting:

Digitale archieven moeten informatie en metadata opslaan van het moment van deponering, via het proces van ingest tot en met de toegang door de speciale doelgroepen. Digitale archieven met een preserveringstaak moeten duurzame archiefopslag bieden, gebaseerd op de OAIS-uitgangspunten.

Voor deze eis moeten de antwoorden bewijs leveren met betrekking tot onderstaande vragen:

- Hoe worden de relevante processen en procedures gedocumenteerd en beheerd?
- Welke beveiligingsniveaus zijn vereist en hoe worden deze ondersteund?
- Hoe wordt met informatieopslag omgegaan in het preserveringsbeleid?
- Heeft het digitaal archief een strategie voor het maken van backups/meervoudige kopieën? Zo ja, welke is dat?
- Zijn er informatieherstel/recoveryvoorzieningen binnen het digitaal archief? Welke zijn dat?
- Wordt er gebruik gemaakt van risicomanagementmethodieken als input voor de strategie?
- Welke controles zijn er om de consistentie tussen meerdere gearchiveerde kopieën te waarborgen?
- Hoe wordt het verval van opslagmedia voorkomen en gemonitord?

Deze eis betreft maatregelen op hoog niveau met betrekking tot continuïteit. Verwijs ook naar R15 (Technische infrastructuur) en R16 (Beveiliging) voor details over specifieke maatregelen voor back-up, fysieke en logische beveiliging en bedrijfscontinuïteit.

X. Preserveringsplan

R10. Het digitaal archief neemt verantwoordelijkheid voor langetermijnpreservering en voert deze functie op een geplande en gedocumenteerde manier uit.

Compliance niveau:

Antwoord

Toelichting:
Het digitaal archief, producenten en de specifieke doelgroep moeten het niveau van verantwoordelijkheid begrijpen voor elk item dat gedeponeerd wordt in het digitaal archief. Het digitaal archief moet de juridische mogelijkheden hebben om deze verantwoordelijkheden op zich te nemen. Procedures moeten gedocumenteerd zijn en hun volledigheid moet zijn gegarandeerd.

Voor deze eis moeten de antwoorden bewijs leveren met betrekking tot de volgende vragen:

- Is er een preserveringsplan opgesteld?
- Wordt het 'niveau van preservering' voor elk informatieobject begrepen? Hoe is dit gedefinieerd?
- Voorziet het contract tussen producent en digitaal archief in alle activiteiten die noodzakelijk zijn om de verantwoordelijkheden voor het beheer te kunnen nemen?
- Is de overdracht van beheer en verantwoordelijkheid duidelijk voor de producent en het digitaal archief?
- Heeft het digitaal archief de rechten om de objecten te kopiëren, transformeren, op te slaan en toegang tot de informatieobjecten te bieden?
- Zijn relevante preserveringsactiviteiten gedocumenteerd, inclusief overdracht van beheer, standaarden voor de opname en de archivering?
- Zijn er maatregelen die garanderen dat deze activiteiten worden uitgevoerd?

XI. Kwaliteit van informatie

R11. Het digitaal archief heeft adequate expertise over de kwaliteit van technische informatie en metadata en zorgt ervoor dat voldoende informatie beschikbaar is voor eindgebruikers om evaluaties met betrekking tot kwaliteit te maken.

Compliance niveau:

Antwoord

Toelichting:
Digitale archieven moeten samenwerken met producenten om ervoor te zorgen dat er voldoende beschikbare informatie is over de gegevens, zodat de specifieke doelgroep de inhoudelijke kwaliteit van de informatie kan beoordelen. Deze kwaliteitsbeoordeling neemt in belang toe wanneer de specifieke doelgroep multidisciplinair is, waar gebruikers persoonlijk niet de ervaring hebben om de kwaliteit van de informatie te kunnen beoordelen. Digitale archieven moeten ook in staat zijn om de technische kwaliteit van de opgenomen informatie te kunnen beoordelen in termen van volledigheid en kwaliteit van de aangeleverde materialen en kwaliteit van de metadata.

Bij de informatie, of de bijbehorende metadata, kunnen kwaliteitsaspecten spelen aangaande hun waarde voor onderzoek, maar dit verhindert niet hun toepassing wanneer een gebruiker een weloverwogen beslissing kan nemen over hun bruikbaarheid door de bijgeleverde documentatie.

Beschrijf voor deze eis:

- De door het digitaal archief gebruikte benadering voor kwaliteit van informatie en metadata.
- Elke geautomatiseerde controle van metadata volgens een relevant schema.
- De mogelijkheid van de specifieke doelgroep om commentaar te geven op en/of informatie en metadata te beoordelen.
- Zijn waar nodig verwijzingen opgenomen naar gerelateerde bronnen (literatuur) of andere typen referenties (zoals citatie-indexen)?

Voorzieningen voor informatiekwaliteit worden ook gerealiseerd door andere eisen. Verwijs in het bijzonder naar R8 (Waardering), R12 (Werkprocessen) en R7 (Informatie integriteit en authenticiteit).

XII. Werkprocessen

R12. Archivering vindt plaats volgens gedefinieerde werkprocessen vanaf de ingest tot en met de verspreiding.

Compliance niveau:

Antwoord

Toelichting:
Om consistentie te waarborgen van werkwijzen tussen datasets en dienstverlening en om ad hoc- acties te voorkomen, moeten de archiveringsprocessen gedocumenteerd zijn en moeten richtlijnen aanwezig zijn voor registratie van wijzigingen. De procedure zou toegesneden moeten zijn op de missie en activiteiten van het digitaal archief. Documentatie van de procedure voor archivering van informatieobjecten moet duidelijk zijn.

Voor deze eis moeten de antwoorden bewijs leveren met betrekking tot de volgende vragen:

- Beschrijvingen van werkprocessen/bedrijfsprocessen.
- Duidelijke communicatie richting producenten en gebruikers over het omgaan met informatie.
- Veiligheids- en impactniveaus voor werkprocessen (waarborgen van de privacy van personen, etc.).
- Kwalitatieve en kwantitatieve controle van output.
- Waardering en selectie van informatie.
- Beleid ten aanzien van informatie dat niet valt binnen de missie/het acquisitieprofiel.
- Typen van beheerde informatie en de impact op werkprocessen.
- Besluitvorming in werkprocessen (bijv. de transformatie van archiefinformatie).
- Beheer van de wijziging van werkprocessen.

Deze eis bevestigt dat alle werkprocessen zijn gedocumenteerd. Bewijs van zulke werkprocessen kan geleverd worden als onderdeel van andere taakspecifieke eisen, zoals voor ingest in R8 (Waardering), opslagprocedures in R9 (Gedocumenteerde opslagprocedures), veiligheidsmaatregelen in R16 (Beveiliging) en vertrouwelijkheid in R4 (Vertrouwelijkheid/Ethiek).

XIII. Het zoeken en vinden van informatie

R13. Het digitaal archief stelt gebruikers in staat om de informatie te zoeken en te vinden en hieraan op een persistente manier te refereren door correcte citering.

Compliance niveau:

Antwoord

Toelichting:

Een effectieve zoek- en vindfunctie is essentieel voor het delen van informatie en de meeste digitale archieven leveren doorzoekbare toegangen die beschrijvingen van de collectie bevatten, zodat potentiële gebruikers kunnen beoordelen of de informatie aan hun behoeften voldoet. Eenmaal gevonden, moet naar datasets kunnen worden verwezen door middel van volledige verwijzingen, inclusief *persistent identifiers* [20] om ervoor te zorgen dat de informatie ook in de toekomst geraadpleegd kan worden. Verwijzingen geven ook erkenning en waardering voor het individu dat bijgedragen heeft aan de creatie van de dataset.[21]

Voor deze eis moeten de antwoorden bewijs leveren met betrekking tot de volgende vragen:

- Biedt het digitaal archief zoekmogelijkheden?
- Houdt het digitaal archief een doorzoekbare metadatacatalogus bij op basis van (internationaal geaccepteerde) standaarden?
- Levert het digitaal archief mogelijkheid tot geautomatiseerde harvesting van metadata?
- Is het digitaal archief zo nodig opgenomen in een of meerdere domeinspecifieke of generieke registers of bronnen?
- Biedt het digitaal archief een overzicht van aanbevolen verwijzingen naar informatie aan?
- Biedt het digitaal archief persistent identifiers aan?

[20] Een persistent identifier is permanente verwijzing en uniek label naar een digitaal object die onafhankelijk is van de bewaarlocatie. Het unieke label zorgt ervoor dat het digitale object altijd teruggevonden kan worden op het internet, ook als de naam van het digitale object of de bewaarplaats verandert. Daardoor is een digitaal object altijd en overal eenduidig terug te vinden op basis van zijn PI. Dit is belangrijk voor duurzame opslag (archivering) van digitale objecten in de snel veranderende wereld van internet. (Bron: Wikipedia).

[21] Dit is in specifiek het geval voor het beheer van wetenschappelijke datasets.

XIV. Informatie hergebruik

R14. Het digitaal archief maakt hergebruik van informatie in de loop van de tijd mogelijk en zorgt ervoor dat de juiste metadata beschikbaar is om het begrip en het gebruik van de informatie te ondersteunen.

Compliance niveau:

Antwoord

Toelichting:

Digitale archieven moeten ervoor zorgen dat informatie begrepen kan worden en in de toekomst effectief kan worden (her)gebruikt ondanks veranderingen in technologie. Deze eis evalueert de genomen maatregelen die ervoor moeten zorgen dat informatie herbruikbaar is.

Voor deze eis moeten de antwoorden bewijs leveren met betrekking tot de volgende vragen:

- Welke metadata wordt door het digitaal archief geëist op het moment dat de informatie wordt aangeleverd (bijv. Dublin Core of inhoudelijk georiënteerde metadata)
- Wordt informatie aangeleverd in formaten die worden gebruikt door de specifieke doelgroep? Welke formaten?
- Zijn er maatregelen genomen om rekening te houden met mogelijke verandering in formaten?
- Zijn er plannen die betrekking hebben op toekomstige migraties?
- Hoe zorgt het digitaal archief ervoor dat de informatie te begrijpen blijft?

Het concept van hergebruik is een kritische factor in omgevingen waar secundaire analyses in het digitaal archief worden toegevoegd aan de primaire informatie, waarmee de herkomstketen, met de bijbehorende rechtenstructuur in toenemende mate gecompliceerd wordt. Hergebruik is afhankelijk van de toepasbare toestemmingen die genoemd worden in R2 (Licenties).

Technologie

XV. Technische infrastructuur

R15. Het digitaal archief werkt op basis van goed ondersteunde besturingssystemen en andere centrale infrastructurele software en gebruikt hardware en softwaretechnologieën die geschikt zijn voor de diensten die zij verleent aan de specifieke doelgroep.

Compliance niveau:

Antwoord

Toelichting:
Digitale archieven moeten werken op betrouwbare en stabiele infrastructuren die de beschikbaarheid van diensten maximaliseren. Voorts moeten de gebruikte hardware en software relevant en geschikt zijn voor de specifieke doelgroep en voor de functies die een digitaal archief uitvoert. Standaarden zoals het OAIS-referentiemodel specificeren de functies die een digitaal archief moet uitvoeren om tegemoet te komen aan de behoeften van de gebruiker.

Voor deze eis moeten de antwoorden bewijs leveren met betrekking tot de volgende vragen:

- Welke referentiestandaarden gebruikt het digitaal archief? Zijn dit internationale en/of community standaarden (bijv. Spatial Data Infrastructure (SDI) standaarden, OGC, W3C of ISO 19115[22], DUTO, NORA, GEMMA)**.** Hoe vaak worden deze gereviewd?
- Hoe zijn de standaarden geïmplementeerd? Zijn er significante afwijkingen van de standaarden? Zo ja, leg uit.
- Heeft het digitaal archief een plan voor ontwikkeling van de infrastructuur? Zo ja, welk is dat?
- Wordt er een softwarecatalogus beheerd en is systeemdocumentatie beschikbaar?
- Is er software die door een bepaalde gebruikersgroep wordt ondersteund? Beschrijf deze.
- Zijn er voor real-time tot bijna real-time data streams 24/7-verbindingen met publieke en private netwerken met een bandbreedte die voldoende is om tegemoet te komen aan de verantwoordelijkheden van het digitaal archief?

[22] ISO 19115: norm voor geografische metadata

XVI. Beveiliging

R16. De technische infrastructuur van het digitaal archief zorgt voor de bescherming van het digitaal archief zelf en zijn informatie, diensten, dienstverlening en gebruikers.

Compliance niveau:

Antwoord

Toelichting:

Het digitaal archief wordt geacht potentiële bedreigingen te analyseren, risico's in te schatten en een consistent beveiligingssysteem te creëren. Het zou rampscenario's moeten beschrijven die gebaseerd zijn op handelingen te kwader trouw, menselijke fouten of technisch falen, die een bedreiging vormen voor het digitaal archief en zijn informatie, producten, services en gebruikers. Het zou de kans en impact moeten inschatten van zulke scenario's, besluiten welke risiconiveaus acceptabel zijn en bepalen welke maatregelen genomen zouden moeten worden om de bedreigingen voor het digitaal archief en specifieke doelgroep tegen te gaan. Dit zou een continu proces moeten zijn.

Beschrijf voor deze eis:

- Procedures en voorzieningen die genomen zijn om te voorzien in een snel herstel of back-up van essentiële diensten op het moment van storing.
- Uw IT-beveiligingssysteem, rampenplan en continuïteitsplan. Medewerkers met rollen op het gebied van beveiliging (bijv. beveiligingsmedewerkers) en risicoanalyse tools (bijv. DRAMBORA) die worden gebruikt.

Deze eis beschrijft enkele van de aspecten die in het algemeen worden ondervangen door andere – bijv. R12 (Werkprocessen) – en is complementair aan R9 (Gedocumenteerde opslagprocedures).

Feedback van de aanvrager

R18. De DSA-WDS s wordt niet gezien als definitief en we waarderen uw input om zo de basis-certificeringsprocedure te verbeteren. Plaats daarom hier eventuele opmerkingen die u wenst te maken over zowel de kwaliteit van de Catalogus en de relevantie ervan voor uw organisatie als andere gerelateerde ideeën.

Antwoord