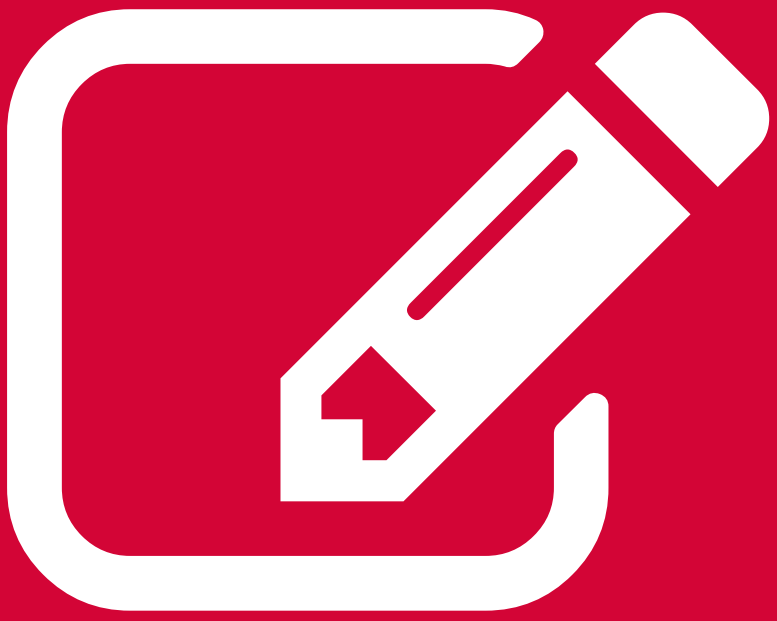
E-depot Achterhoek

Toetsingskader



2015

Werkgroep Toetsingskader

- Martijn Heringa (Waterschap Rijn en IJssel)
- Frans Wessels (DiVault)
- Hans Berende (Erfgoedcentrum Achterhoek en Liemers)
- Gerard van de Woerdt (gemeente Doetinchem)
- Anke Weijenborg (gemeente Lochem)

Deelnemende partijen

Inhoud

Managementsamenvatting

Doel

Het 'Toetsingskader E-depot Achterhoek' is opgesteld als één van de kennisproducten van het Project E-depot Achterhoek.

Doel van het Toetsingskader E-depot Achterhoek is eisen te formuleren waaraan het E-depot Achterhoek moet voldoen om kwalitatief duurzaam beheer van digitale archiefbescheiden mogelijk te maken. Zorgdragers kunnen dit toetsingskader gebruiken om te bepalen of de beheerorganisatie van het e-depot voldoet aan alle eisen die wet- en regelgeving stellen. De beheerorganisatie kan het toetsingskader gebruiken voor het borgen van kwalitatief duurzaam beheer van de digitale archiefbescheiden. Daarnaast kan dit kennisproduct dienen om een programma van eisen vorm te geven in het geval van een aanbesteding voor een bewaaromgeving voor digitale archiefbescheiden.

Aanpak

Bij het opstellen van het Toetsingskader E-depot Achterhoek is gebruikgemaakt van de Eisen Duurzaam Digitaal Depot (ED_3), versie 2 december 2012 van de Landelijke Vereniging van Provinciale Archiefinspecteurs (LOPAI). ED_3 is gebaseerd op wet- en regelgeving en landelijke en internationale kaders zoals het internationaal aanvaarde Open Archival Information System (OAIS) waarin de verschillende stadia (aanbieden, opnemen, beschikbaar stellen) van digitale archiefbescheiden in een e-depot worden beschreven. ED_3 heeft onder andere de structuur van het OAIS overgenomen. De toetsingscriteria in ED_3 worden onderverdeeld in:

- criteria waaraan de beheerorganisatie, waaronder de bewaaromgeving, moet voldoen;
- criteria waaraan de beheerprocessen van de beheerorganisatie moeten voldoen;
- criteria waaraan de techniek van de bewaaromgeving moet voldoen.

Het Toetsingskader E-depot Achterhoek volgt de structuur van ED_3.
De criteria zoals genoemd in ED_3 zijn beoordeeld op interpretatie, praktische toepasbaarheid en abstractieniveau. Daar waar nodig is een toelichting toegevoegd.

ED_3 is gericht op het overbrengen van permanent te bewaren archiefbescheiden twintig jaar na afhandeling. Het plaatsen van te bewaren en te vernietigen archiefbescheiden vóór deze tijd wordt uitplaatsen genoemd. Voor het opnemen en beheren van uitgeplaatste archiefbescheiden in het E-depot Achterhoek zijn in bijlage 1 een aantal aanvullende criteria opgenomen.

Conclusies en aanbevelingen

1 De eisen die worden gesteld aan de beheerorganisatie voor het beheer van digitale archiefbescheiden in een e-depot zijn van een geheel andere orde dan het beheer van analoge archiefbescheiden. De werkgroep adviseert daarom:
   - Voer een impactanalyse uit om te bezien welke inspanningen geleverd moeten worden om de toekomstige beheerorganisatie in te richten conform ED_3.
   - Overwogen kan worden om een prioritering aan te brengen in de elementen uit ED_3 om zo een overgangsfase te creëren voor de beheerorganisatie. Daardoor heeft deze de tijd om zich te ontwikkelen zodat het conform de gestelde eisen kan gaan functioneren.

2 Het uitplaatsen van archiefbescheiden heeft gevolgen voor het beheer en de beschikbaarstelling van de archiefbescheiden. Te vernietigen archiefbescheiden moeten verwijderd kunnen worden. Uitgeplaatste archiefbescheiden vallen niet onder de openbaarheid zoals de Archiefwet dit regelt maar onder de Wet Openbaarheid van Bestuur. De werkgroep adviseert:
   - Indien gekozen wordt om (vernietigbare) archiefbescheiden uit te plaatsen naar het e-depot, moeten de elementen uit de ED_3 aangevuld worden met eisen die gesteld worden aan uitgeplaatste archiefbescheiden (bijlage 1).

1 Algemeen

Dit is een kennisproduct dat vervaardigd is als onderdeel van het Project E-depot Achterhoek.

Bij het opstellen van het 'Toetsingskader E-depot Achterhoek' is gebruikgemaakt van de Eisen Duurzaam Digitaal Depot (ED_3), versie 2 december 2012, van de Landelijke Vereniging van Provinciale Archiefinspecteurs (LOPAI). De toetsingscriteria zoals genoemd in het ED_3 zijn door de werkgroep beoordeeld. Daar waar nodig is er per toetsingscriterium een toelichting gegeven die de te toetsen criteria beter interpretabel, meer praktisch toepasbaar en concreter maken. Ook heeft de werkgroep enkele toetsingscriteria toegevoegd.

1.1 Doel toetsingskader

In het eerste artikel van de Archiefwet 1995 staat dat ook digitale informatie van de overheid tot archiefbescheiden kan worden gerekend. In de Archiefregeling is vervolgens uitgewerkt waaraan (te bewaren) archiefbescheiden moeten voldoen. Samengevat:

- Het is wat het beweert te zijn (authentiek).
- Het is een accurate voorstelling van de transactie waar het over handelt (betrouwbaar).
- Het is niet ongeautoriseerd te veranderen en veranderingen zijn na te gaan (integer).
- Het is vindbaar, raadpleegbaar en begrijpelijk binnen de originele context (bruikbaar).

De werkgroep verwacht dat zorgdragers met dit Toetsingskader E-depot Achterhoek eisen kunnen formuleren voor de beheerorganisatie van het e-depot. De beheerorganisatie kan het toetsingskader gebruiken voor het borgen van kwalitatief duurzaam beheer van de digitale archiefbescheiden.
Daarnaast kan dit kennisproduct dienen om een programma van eisen vorm te geven in het geval van een aanbesteding voor een bewaaromgeving voor digitale archiefbescheiden.

1.2 Scope

- Dit toetsingskader is geschreven met de over te brengen digitale archiefbescheiden in gedachten. In principe is het mogelijk om ook archiefbescheiden uit te plaatsen voordat ze overgebracht moeten worden, of om te vernietigen archiefbescheiden in een e-depot te beheren.
- Dit toetsingskader is geschreven voor zorgdragers zodat zij eisen kunnen stellen aan de beheerorganisatie van het e-depot en deze hierop kunnen toetsen.
- Dit is een kennisproduct dat als hulpmiddel kan dienen voor zorgdragers om in de toekomst aan te kunnen sluiten bij het E-depot Achterhoek.

2 Achtergronden, kaders en conformiteit

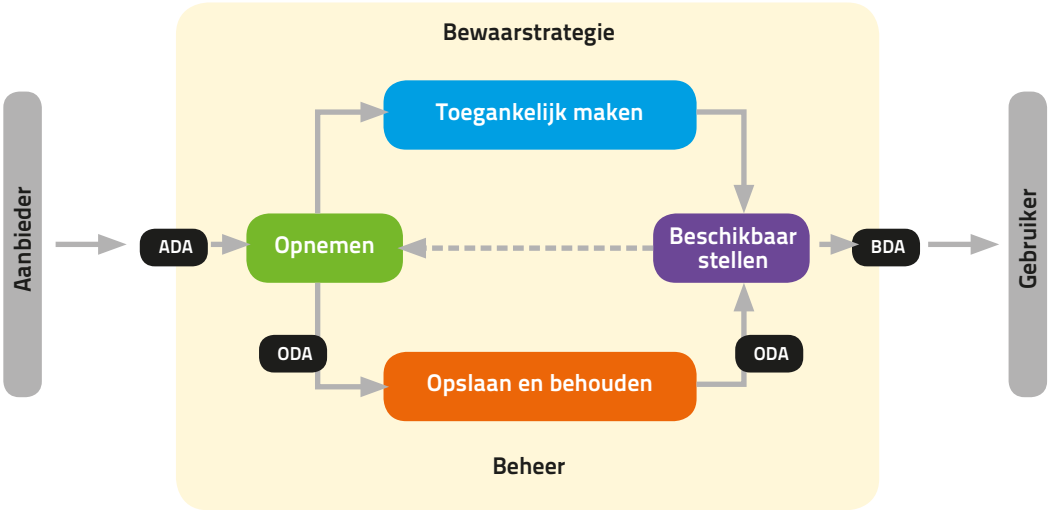
2.1 Achtergrond ED_3

In ED_3 wordt uitgegaan van de volgende definitie van een e-depot:

Een e-depot is het geheel van organisatie, beleid, processen en procedures, financieel beheer, personeel, databeheer, databeveiliging en aanwezige hard- en software, dat duurzaam beheren en raadplegen van te bewaren digitale archiefbescheiden mogelijk maakt.

Een e-depot is dus te vergelijken met een analoge bewaarplaats, die conform de Nederlandse archiefwetgeving bestemd is voor permanent te bewaren archiefbescheiden. In de praktijk zullen er, net als bij analoge archiefruimten, ook vernietigbare archiefbescheiden in een e-depot worden beheerd. Alle archiefbescheiden die pas na langere termijn vernietigbaar zijn, moeten immers gedurende die tijd net zo nauwgezet worden behandeld als te bewaren archiefbescheiden. Voor digitale archiefbescheiden die zeven jaar[1] of langer moeten worden bewaard, is plaatsing onder controle van een e-depot daarom geen onlogische keuze. Een en ander betekent echter wel, dat ook het uitvoeren van procedures voor waardering, selectie en vernietiging en overbrenging van digitale archiefbescheiden in een e-depot mogelijk moet zijn. Eisen met betrekking tot de waarderings- en selectieprocedures zelf vallen echter buiten het bestek van ED_3.

Als basis voor een e-depot en daarmee ook voor ED_3 geldt het internationaal aanvaarde Open Archival Information System (OAIS)-model. Voor het begrip van de behandeling van digitale informatie maakt het OAIS onderscheid tussen verschillende stadia (aanbieden, opnemen, beschikbaar stellen). Dit is overgenomen in ED_3 als indeling voor digitale archiefbescheiden:



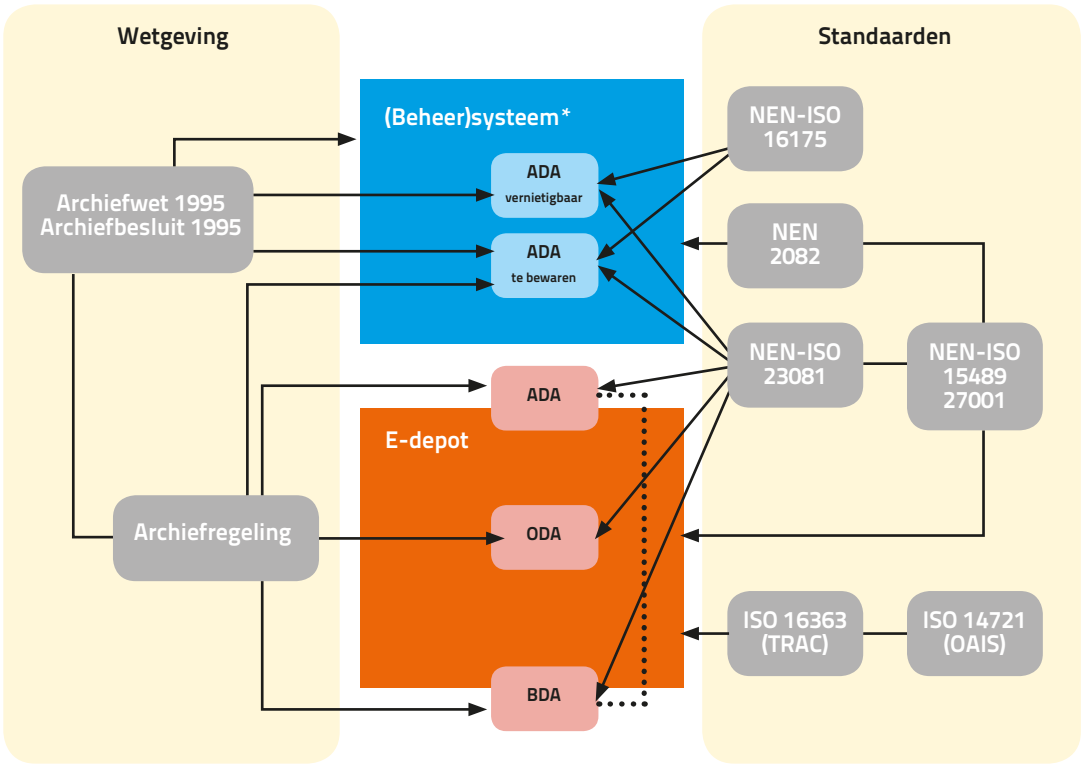
Figuur 1. Digitale archiefbescheiden in samenhang

1 Zeven jaar is een voorlopige keuze.

Het digitale archiefstuk, zoals ontstaan en gebruikt in de werkprocessen van de archiefvormer (de zorgdrager), wordt bij de overdracht het aangeboden digitaal archiefstuk (ADA) voor het e-depot. Daar wordt het via de procedure van opname bewerkt tot opgenomen digitaal archiefstuk (ODA), geschikt voor blijvende bewaring. Op basis van vraagstelling van geautoriseerde gebruikers wordt door het e-depot het beschikbare digitale archiefstuk (BDA) aangeboden.

2.2 Kaders

Om een duurzame digitale beheeromgeving voor archiefbescheiden mogelijk te maken zijn er kaders gedefinieerd waarlangs ED_3 is opgebouwd. Naast wet- en regelgeving spelen ook erkende standaarden een rol. In onderstaand overzicht is dat schematisch in beeld gebracht:



* Niet alleen een DMS en/of RMA, maar ieder systeem waarin archiefbescheiden kunnen voorkomen die opname in een e-depot kunnen vergen

Figuur 2. Verhouding digitale archiefbescheiden met wetgeving en standaarden.

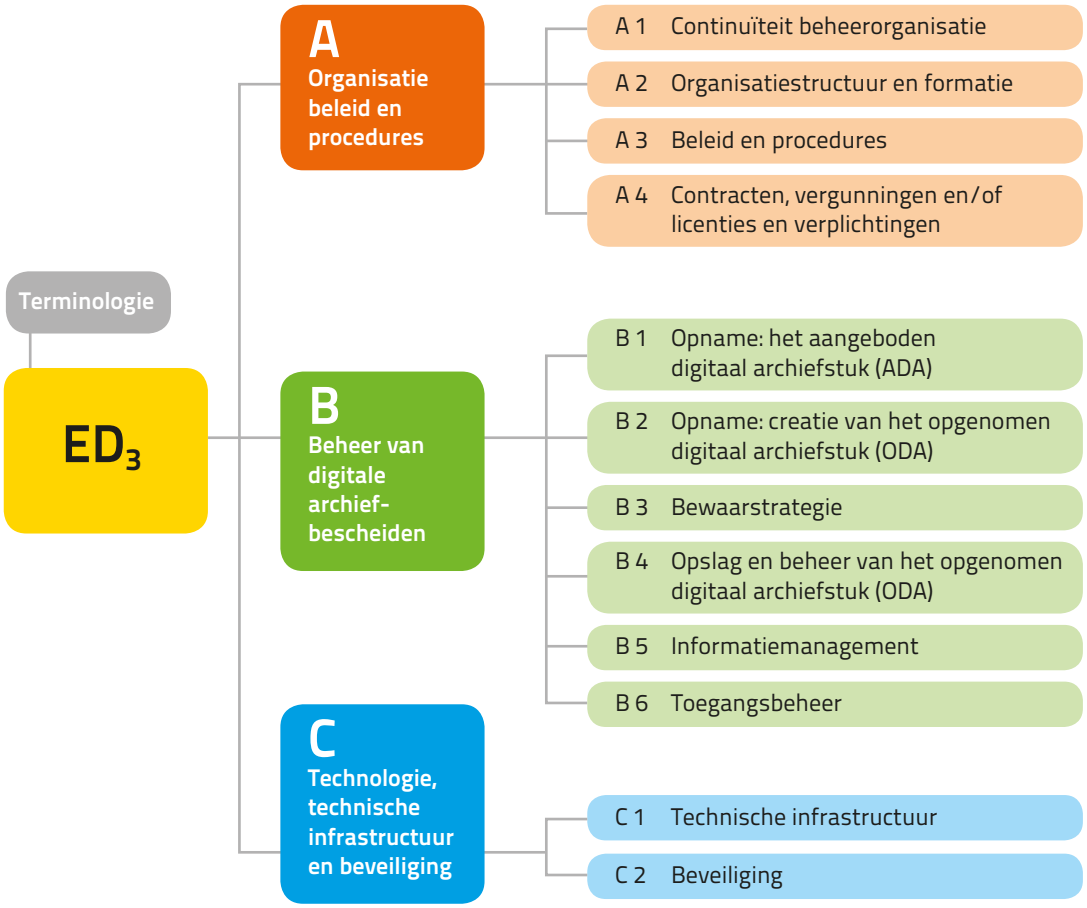
De archiefwetgeving richt zich op de zorg voor en het beheer van archiefbescheiden, waarbij de Archiefregeling een nadere invulling hiervan geeft. De NEN-ISO 15489 is bedoeld voor het informatiemanagement en de NEN-ISO 27001 voor de beveiligingsaspecten daarvan. Een nadere invulling voor de te gebruiken programmatuur wordt in de NEN 2082 gegeven. De NEN-ISO 23081 biedt standaarden voor de toe te kennen metadata en de NEN-ISO 16175 geeft standaarden voor archiefbescheiden in kantooromgevingen. De ISO 14721 ten slotte, is een model archiveringssysteem voor lang te bewaren digitale archiefbescheiden, uitgewerkt in een set van eisen in de ISO 16363.

2.3 Conformiteit

Net als bij alle andere vormen van toetsing, is conformiteit aan ED_3 en aan dit 'Toetsingskader E-depot Achterhoek' het resultaat van interpretatie en beoordeling: het e-depot voldoet, wanneer de auditor/toezichthouder vindt dat aan alle eisen van ED_3 is voldaan. Daarnaast is het doel van een ED_3-toetsing het in gang zetten en beoordelen van het proces van continue verbetering van het e-depot. Dit impliceert dat een eindoordeel niet simpel een 'goed' of 'fout' zal behelzen, maar tevens onderdelen aangeeft die verbetering behoeven.

3 Structuur van het toetsingskader ED_3

Dit toetsingskader is primair gebaseerd op ED_3. De structuur van de toetsingscriteria in dit kennisproduct is daarom ook van ED_3 overgenomen en bestaat uit drie onderdelen:



Figuur 5. Structuur van ED_3

In **onderdeel A** staan de criteria waaraan de beheerorganisatie, waaronder de bewaar-omgeving functioneert, moet voldoen. Bij de inrichting van een e-depot, bijvoorbeeld als gemeenschappelijke regeling tussen meerdere overheden, kunnen deze criteria worden gebruikt als checklist. Nog meer dan bij een (analoge) archiefbewaarplaats strekken de eisen zich bij een e-depot ook uit tot de organisatie, omdat de inrichting daarvan cruciaal is voor het waarborgen van de kwaliteit van de interne beheerprocessen.

Onderdeel B bevat criteria voor de beheerprocessen van de beheerorganisatie. Deze zijn gebaseerd op de eisen van de archiefwetgeving en moeten vooral de kwaliteit van digitale archiefbescheiden waarborgen. In elk stadium waarin een digitaal archiefstuk kan verkeren (ADA, ODA, BDA) moeten de juiste metadata opgenomen, gegenereerd, toegevoegd en in samenhang beheerd kunnen worden om aan de archiefwetgeving te kunnen voldoen. De criteria zijn bedoeld als middel om de kwaliteit van zorg en beheer te beoordelen, zodat op basis daarvan vertrouwen kan worden gesteld in de beheerde digitale overheidsinformatie.

Onderdeel C gaat over de techniek van de bewaaromgeving. In de praktijk zullen deze criteria grotendeels samenvallen met een uitgebreide ICT-audit, omdat er al vele standaarden voor een goed werkende digitale infrastructuur bestaan. Nieuw in deze versie zijn de apart geformuleerde eisen met betrekking tot de serverruimte.

4 Toetsingskader E-depot Achterhoek

4.1 Leeswijzer

In dit hoofdstuk zijn de toetsingscriteria die in het ED_3 zijn opgenomen indien nodig toegelicht met als doel ze beter te kunnen interpreteren, ze concreter te maken (gezien het abstractieniveau) en ze daardoor toepasbaarder te maken voor gebruik door zorgdragers en de beheerorganisatie.
Het hoofdstuk is als volgt opgebouwd. Er zijn drie hoofdonderdelen die gezamenlijk het ED_3 vormen. Dit zijn de onderdelen A, B en C. Elke onderdeel kent diverse subonderdelen, die zijn verdeeld in de diverse bijbehorende criteria. Bijvoorbeeld:

Hoofdonderdeel A

Subonderdeel A 1

Criterium A 1.1

Elk hoofdonderdeel en elk subonderdeel wordt toegelicht aan de hand van de bijbehorende cursieve tekst (in kleur) uit het ED_3.

De criteria zijn rechtstreeks ontleend aan de wijze waarop de opstellers van ED_3 deze hebben vormgegeven. Ze moeten als volgt gelezen worden:

- Onder criteriumnummer wordt met standaardtekst het criterium uit ED_3 beschreven.
- Daaronder staat met gekleurde tekst een uitleg die slaat op het betreffende criterium.
- Bij sommige criteria worden bepalingen uit bijvoorbeeld de Archiefregeling aangehaald. Deze zijn weergegeven in `dit lettertype.`
- De werkgroep heeft aan de criteria een eigen toelichting toegevoegd indien dit nodig werd geacht. Deze toelichtingen zijn te vinden in een kader.

4.2 Onderdeel A ▪ Organisatie, beleid en procedures

De opzet van de beheerorganisatie heeft grote invloed op de kwaliteit van het beheer. Daarom bevat onderdeel A criteria aan de hand waarvan de beheerorganisatie kan worden beoordeeld.

A 1. Continuïteit beheerorganisatie

Onafhankelijk van de omvang, doelgroep of aard van de werkzaamheden toont de beheerorganisatie aan over langere tijd te kunnen functioneren.

A 1.1
De beheerorganisatie heeft een vastgestelde missie en organisatiedoelen, waarin de verplichting tot langetermijnbeheer van digitale archiefbescheiden is opgenomen.
De beheerorganisatie moet aangeven, dat het e-depot wordt beheerd conform de bepalingen uit de wet- en regelgeving.

Toelichting op A 1.1
De beheerorganisatie toont aan in haar missie en doelen, dat het e-depot wordt beheerd conform de Archiefwet 1995, het Archiefbesluit en de Archiefregeling. Daarnaast toont de beheerorganisatie aan, dat het voldoet aan de relevante erkende standaarden NEN2082, NEN-ISO 23081, NEN-ISO 15489, NEN-ISO 27001 en ISO 16363/ISO 14721. Dat kan bijvoorbeeld aan de hand van auditrapportages door een onafhankelijke partij, die cyclisch worden herhaald. De beheerorganisatie heeft haar missie en organisatiedoelen waarin de verplichting tot langetermijnbeheer van digitale archiefbescheiden is opgenomen ontleend aan de hiervoor genoemde wettelijke kaders en erkende standaarden.

A 1.2
De beheerorganisatie heeft een opvolgingsplan, een continuïteitsplan en een escrowovereenkomst om de continuïteit van het e-depot te garanderen.
Als de beheerorganisatie ophoudt te bestaan, regelt het opvolgingsplan het verder beheer van de opgenomen archiefbescheiden. Een continuïteitsplan regelt hoe de beheerorganisatie de opgenomen archiefbescheiden veilig kan stellen; vergelijk ook het calamiteiten- en herstelplan bij storingen, zoals dat in C 2.2 wordt genoemd.

Toelichting op A 1.2
Zie hiervoor de input vanuit het Continuïteitsplan E-depot Achterhoek

A 1.3
De beheerorganisatie zorgt voor het in stand houden van het e-depot.
Dit houdt ten minste in dat:
- de beheerorganisatie financieel in staat is om haar beheertaken uit te voeren;
- de beheerorganisatie jaarlijks haar bedrijfsplannen actualiseert;
- de financiële systemen en procedures van de beheerorganisatie transparant en conform relevante accountantsstandaarden en richtlijnen zijn ingericht en door derden worden ge-audit conform de wettelijke eisen;
- de beheerorganisatie zich verplicht om permanent risico's, opbrengsten, investeringen en kosten (inclusief eigendommen, licenties en verplichtingen) te analyseren en daarover te rapporteren;
- de beheerorganisatie zich verplicht tekorten in de begroting te monitoren en aan te vullen.

Toelichting op A 1.3, 1e bullet
De beheerorganisatie toont aan dat zij volledig transparant is naar de zorgdragers in haar financiële bedrijfsvoering en geeft heldere informatie over het gevoerde financiële beleid. Daarnaast maakt de beheerorganisatie jaarlijks zichtbaar waar de financiële risico's liggen, hoe groot deze zijn (de mate van bedreiging voor de instandhouding van het e-depot) en welke maatregelen er getroffen worden om deze risico's op de korte termijn (tot één jaar) en middellange termijn (twee tot vijf jaar) weg te nemen.

Toelichting op A 1.3, 2e bullet
De beheerorganisatie toont aan te werken met een meerjarenbeleidsplan, dat inzicht geeft in de plannen voor de taken die de zorgdragers bij de beheerorganisatie hebben belegd. Het meerjarenbeleidsplan is uitgewerkt in een beheerplan dat jaarlijks wordt geactualiseerd op basis van de PDCA-cyclus en waarover wordt gerapporteerd aan de zorgdragers.

Toelichting op A 1.3, 5e bullet
De beheerorganisatie toont aan hoe zij tekorten in de begroting monitort en rapporteert hierover tijdig aan de zorgdragers.

A 2. Organisatiestructuur en formatie

Er is een bestendige, omgevingsbewuste organisatie die over voldoende en deskundige medewerkers beschikt en die taken, verantwoordelijkheden en procedures duidelijk heeft vastgelegd.

A 2.1
De beheerorganisatie heeft haar taken en de bijbehorende processen, die zij moet uitvoeren, beschreven in procedures en de daarbij behorende verantwoordelijkheden belegd.
Vergelijk NEN-ISO 15489-1:2001, hoofdstuk 6.

Toelichting op A 2.1
De beheerorganisatie toont aan hoe zij haar beleid, procedures, en werkprocessen documenteert en uitvoert waarbij de handelingen, actoren en verantwoordelijkheden zijn beschreven. Ook laat zij periodiek (externe) audits en/of certificering hierop uitvoeren, die zijn gericht op het ontvangen, opnemen, behouden en beschikbaar stellen van archiefbescheiden.

A 2.2
De beheerorganisatie beschikt over voldoende medewerkers, met voldoende kennis en competenties, om al haar taken en diensten te kunnen uitvoeren en bijhouden.
Binnen de beheerorganisatie dient ook voldoende aansturing en/of coördinatie van alle verantwoordelijke en/of betrokken medewerkers aanwezig te zijn. Vergelijk NEN-ISO 15489-1:2001, paragraaf 6.3 en hoofdstuk 11.

Toelichting op A 2.2
- De beheerorganisatie toont aan welke bevoegdheden en verantwoordelijkheden organisatieleden dragen als het gaat om het correct uitvoeren van het ontvangen, opnemen, behouden en beschikbaar stellen van archiefbescheiden.
- Daarnaast toont de organisatie aan wie de specifieke hoofdverantwoordelijkheid voor de bedrijfsvoering draagt binnen de beheerorganisatie.
- Ook toont de beheerorganisatie aan dat het een permanent programma voor opleiding heeft opgezet voor het beheren en verder ontwikkelen en implementeren van een e-depot. Opleidingsprogramma's met betrekking tot eisen voor informatie- en archiefmanagement en specifieke praktijktoepassingen behoren gericht te zijn op

alle leden van het management, werknemers, en alle andere individuen die verantwoordelijk zijn voor het geheel of een deel van de bedrijfsactiviteit van de beheerorganisatie. De opleidingsprogramma's moeten aandacht besteden aan de rollen en verantwoordelijkheden ten aanzien van het ontvangen, opnemen, behouden en beschikbaar stellen van archiefbescheiden.

A 3. Beleid en procedures

De beheerorganisatie heeft transparant vastgelegd wat zij nodig heeft, besluit, ontwikkelt en doet ten behoeve van langetermijnbeheer.

A 3.1
De beheerorganisatie heeft haar gebruikersgroepen gedefinieerd en maakt openbaar hoe zij tegemoet komt aan de eisen die de gebruikers stellen aan toegankelijkheid en begrijpelijkheid van de informatie.

A 3.2
De beheerorganisatie toetst en evalueert periodiek haar beleid en procedures, waaronder die voor het behandelen van opmerkingen en klachten van zorgdragers en gebruikers.
De beheerorganisatie kan aangeven op welke wijze en hoe vaak beleid en procedures worden getoetst en beargumenteert de gekozen toetsingsfrequentie. Het gaat hierbij om interne toetsen en audits.
Archiefregeling art. 16
De zorgdrager zorgt ervoor dat het beheer van zijn archiefbescheiden voldoet aan toetsbare eisen van een door hem toe te passen kwaliteitssysteem.

Toelichting op A 3.2
De beheerorganisatie toont aan een kwaliteitssysteem te hanteren dat toetsbaar is, bijvoorbeeld op basis van het INK-model. De toetsbare elementen moeten gebaseerd zijn op archiefwet- en regelgeving en relevante NEN-(ISO-)normen (zoals NEN15489-1:2001 en NEN2082:2008 nl). Uit het kwaliteitssysteem moet blijken op welke manier en met welke frequentie getoetst wordt en hoe de toetsresultaten leiden tot verbeteringen of aanpassingen (bijvoorbeeld op basis van de PDCA-cyclus). De beheerorganisatie rapporteert hierover aan de zorgdragers.
De beheerorganisatie heeft voor deze kwaliteitsprocessen een verantwoordelijke aangewezen die juistheid, werkbaarheid en actualiteit van de processen borgt.
Het Wijzigingen Management-proces bevat een risico- & impactanalyse en borgt de continuïteit van de geboden diensten. Terugdraaien van wijzigingen is daar een integraal onderdeel van.

A 3.3
De beheerorganisatie beschikt over een overzicht van alle wijzigingen in werkwijzen, procedures, soft- en hardware waarbij is vastgelegd wat de mogelijke invloed van de wijzigingen is op de digitale archiefbescheiden. Ook is zij in staat verantwoording af te leggen over alle activiteiten ten behoeve van de werking en het beheer van de bewaaromgeving, met name die activiteiten die van invloed kunnen zijn op de permanente bewaring van de digitale informatie.
Er is een logfile van de wijzigingen beschikbaar (changemanagement).

Toelichting op A 3.3
De beheerorganisatie is in staat om verantwoording af te leggen over alle activiteiten (bijvoorbeeld in de vorm van een logfile) die verbonden zijn met het beheer van de informatie van de zorgdragers. Dit gebeurt op basis van toetsbare eisen van een toe te passen kwaliteitssysteem waarvan in ieder geval de voor de betreffende zorgdragers vastgestelde eisen aan de ODA en de resultaten van audits en archiefinspecties deel uitmaken.

A 3.4
De beheerorganisatie heeft een ICT-strategie die aansluit bij de geformuleerde organisatiedoelen (missie).
Een ICT-strategie is een document dat door het hoogste management wordt gedragen en beschrijft op welke wijze ICT bijdraagt aan de organisatiedoelstellingen en de continuïteit van de organisatie. In de ICT-strategie staat ook welke ICT-doelstellingen de komende planperiode (drie tot vijf jaar) worden nagestreefd, welke programma's en projecten worden gestart en wat de kosten en risico's zijn.

Toelichting op A 3.4
De ICT-strategie is rechtstreeks ontleend aan het langetermijnbeheer van digitale archiefbescheiden in een e-depot.

A 3.5
De beheerorganisatie laat periodiek (externe) audits uitvoeren op het beheer van de digitale archiefbescheiden.
Het gaat om audits, waarin minimaal strategie, beleid, procedures, processen en technische omgeving beoordeeld moeten worden op onder andere de ontvankelijkheid voor technologische ontwikkelingen en de invoering daarvan en het voldoen aan veranderende eisen. Vergelijk NEN-ISO 15489-1:2001, hoofdstuk 10.

Toelichting op A 3.5
Deze audits behoren te worden gedocumenteerd en gerapporteerd aan de zorgdrager. Tekortkomingen uit audits moeten waar noodzakelijk en overeengekomen met de zorgdrager in een verbeterplan worden uitgewerkt en ingevoerd.

A 4. Contracten, vergunningen en/of licenties en verplichtingen

De beheerorganisatie heeft alle voor het beheer noodzakelijke rechten en verplichtingen vastgelegd. Daarbij zijn onder andere functies, verantwoordelijkheden, looptijden en voorwaarden duidelijk en toegankelijk beschreven.

A 4.1
De beheerorganisatie beschikt over actuele en geldige contracten/overeenkomsten met de zorgdrager(s) aangaande het opnemen, bewaren en beschikbaar stellen van digitale archiefbescheiden.
De beheerorganisatie zou een gemeenschappelijke regeling kunnen zijn.

A 4.2
De beheerorganisatie beschikt over actuele en geldige contracten/overeenkomsten met de zorgdrager(s) of andere relevante partijen aangaande onderhoud, toegankelijkheid en verwijdering.
Dit heeft onder meer betrekking op de uitvoering van processen gericht op duurzaamheid, zoals conversie en/of migratie, waarbij de oorspronkelijke informatie mogelijk wordt aangepast. Opgestelde beheerovereenkomsten specificeren alle benodigde rechten en zijn overgedragen aan de beheerorganisatie. Deze overgedragen rechten zijn gedocumenteerd. Vooral bij niet-overheidsarchieven, die voor opname in de bewaaromgeving worden aangeboden en vaak voorzien zijn van zogenaamde bruikleen- of schenkingsovereenkomsten, zijn mogelijk beperkende bepalingen opgenomen. Verwijdering moet hier gelezen worden als verplaatsing naar een ander systeem of e-depot.

Toelichting op A 4.2
Verwijdering moet in dit kader niet alleen gelezen worden als verplaatsing naar een ander systeem of e-depot, maar ook als verwijdering uit een bestaand systeem of e-depot.

A 4.3
Voor het geval de beheerorganisatie digitale archiefbescheiden opneemt waarvan de eigendom of de rechten onduidelijk zijn, beschikt zij over procedures om aansprakelijkheid en vragen om uitleg daaromtrent af te handelen.
Het kan bijvoorbeeld zijn dat de rechthebbenden van digitale foto's niet bekend zijn, terwijl deze foto's wel blijvend bewaard moeten worden.

4.3 Onderdeel B ▪ Beheer van digitale archiefbescheiden

Het gaat in deze afdeling om functies, procedures en processen voor het opnemen, toegankelijk maken, beschikbaar stellen, opslaan en bewaren van digitale archiefbescheiden, conform de voorschriften van de Archiefregeling.

B 1. Opname: het aangeboden digitaal archiefstuk (ADA)

De procedure voor opname van het aangeboden digitaal archiefstuk (ADA) moet zodanig zijn, dat het verdere beheer adequaat kan worden uitgevoerd.

B 1.1
De beheerorganisatie beschrijft welke relatie-informatie van het aangeboden digitaal archiefstuk (ADA) bewaard moet blijven.

Archiefregeling art. 17
De zorgdrager zorgt ervoor dat van elk van de archiefbescheiden te allen tijde kan worden vastgesteld:
a. de inhoud, structuur en verschijningsvorm bij het ontvangen of opmaken ervan door het overheidsorgaan, een en ander voor zover deze aspecten kenbaar moesten zijn voor de uitvoering van het betreffende werkproces (…).

Archiefregeling art. 21
In toelichting op artikel 17, aanhef en onderdeel a, zorgt de zorgdrager ervoor, dat van elk van de digitale archiefbescheiden te allen tijde het gedrag kan worden vastgesteld.

B 1.2

De beheerorganisatie legt vast welke beheerinformatie ten tijde van de opname moet zijn toegevoegd aan het aangeboden digitaal archiefstuk (ADA) en controleert de aanwezigheid van deze informatie bij opname.

Archiefregeling art. 19

1. De zorgdrager legt een metagegevensschema als bedoeld in NEN-ISO 23081:2006 vast.
2. De zorgdrager koppelt aan archiefbescheiden metagegevens aan de hand waarvan te allen tijde de aspecten, bedoeld in artikel 17, kunnen worden herleid.

Toelichting op B 1.2

De beheerorganisatie legt in samenspraak met de deelnemers aan het e-depot (lees: zorgdragers) vast hoe en of er wijzigingen in de aan te bieden beheerinformatie verwerkt worden. Denk hierbij aan een wijziging in het Toepassingsprofiel e-depot Achterhoek. Dit gebeurt in een overleggremium waarin zowel de beheerorganisatie als de deelnemers vertegenwoordigd zijn, bijvoorbeeld via een Strategisch Informatie Overleg (SIO).

Er is een procedure voor de controle op de aanwezigheid van beheerinformatie.

B 1.3

De beheerorganisatie legt vast welke representatie-informatie een aangeboden digitaal archiefstuk (ADA) moet hebben en controleert het ADA op juistheid, volledigheid, duurzaamheid en veiligheid bij opname.

Archiefregeling art. 24

In toelichting op de metagegevens, bedoeld in artikel 19, tweede lid, koppelt de zorgdrager aan digitale archiefbescheiden metagegevens aan de hand waarvan te allen tijde gegevens over het navolgende kunnen worden herleid:

A. De oorspronkelijke technische aard van de digitale archiefbescheiden, alsmede van de hard- en softwareomgeving daarvan;
B. De actuele technische aard van de digitale archiefbescheiden, alsmede van de hard- en softwareomgeving daarvan, zodanig dat reproductie ervan te allen tijde mogelijk is; en
C. Voor zover gebruik is gemaakt van een digitale handtekening:
   1°. de houder van de digitale handtekening;
   2°. het moment van validatie van de digitale handtekening, alsmede het resultaat daarvan;
   3°. de voor de validatie verantwoordelijke functionaris; en
   4°. voor zover bekend ten tijde van het werkproces: de identificatie van het certificaat van de digitale handtekening.

Archiefregeling art. 26

1. Digitale archiefbescheiden worden, uiterlijk op het tijdstip van overbrenging, opgeslagen in een valideerbaar en volledig gedocumenteerd bestandsformaat dat voldoet aan een open standaard, tenzij dit redelijkerwijs niet van de zorgdrager kan worden verlangd. Alsdan vindt met de beheerder van de voor overbrenging aangewezen archiefbewaarplaats overleg plaats over een alternatief bestandsformaat.

2. Voor zover op het tijdstip van overbrenging gebruik wordt gemaakt van encryptietechniek, wordt aan de beheerder van de archiefbewaarplaats de bijbehorende decryptiesleutel verstrekt.
3. Gebruikmaking van compressietechniek is slechts toegestaan, voor zover daarbij niet zodanig verlies van informatie optreedt, dat niet langer aan de bij deze regeling gestelde eisen ten aanzien van de toegankelijke en geordende staat van digitale archiefbescheiden kan worden voldaan.

N.B. Ook de beoordeling van representatie-informatie kan zich in de tijd verder ontwikkelen, zodat de eisen voor het ADA geen statisch karakter hebben. Het ADA moet vanwege de veiligheid ook worden gezuiverd van infecties met zogenaamde malware (zoals een computervirus, spyware, een computerworm of Trojaans paard) zodat de bewaaromgeving deze niet overneemt.

Toelichting op B 1.3

- Beheerorganisatie legt vast welke representatie-informatie verwacht wordt. Zorgdragers conformeren zich daaraan.
- Er is een procedure voor de controle op juistheid, volledigheid, duurzaamheid en veiligheid van de representatie-informatie van de ADA-stukken, bijvoorbeeld controle op omvang en bestandsformaat.

B 1.4

De beheerorganisatie voegt de voor bewaring relevante informatie over opnametijdstip, opnameactiviteiten en beheerprocessen toe aan de beheerinformatie.
Vanaf het moment van opnemen moet de beheerorganisatie al haar activiteiten kunnen verantwoorden.

Toelichting op B 1.4

Er moeten afspraken worden gemaakt tussen zorgdrager en beheerorganisatie over wat 'voor bewaring relevante informatie van ADA-stukken' is, en hoe deze worden toegevoegd. Hierbij gaat het ook om de wijze waarop autorisatiebeheer, functioneel beheer, databeheer geregeld is. Deze afspraken moeten worden opgenomen in de procedures van de beheerorganisatie.

B 2. Opname: creatie van het opgenomen digitaal archiefstuk (ODA)

Bij de opname dient het aangeboden digitaal archiefstuk (ADA) qua vorm, structuur en inhoud geschikt te zijn voor langetermijnbewaring.

B 2.1

De beheerorganisatie beschikt over ontsluitingsinformatie van ieder opgenomen digitaal archiefstuk (ODA) en over een beschreven procedure om de representatie-informatie te testen en waar nodig naar een vooraf vastgesteld niveau te brengen.

Archiefregeling art. 20

De zorgdrager zorgt ervoor dat het archiveringssysteem de toegankelijke staat van archiefbescheiden waarborgt, zodanig dat elk van de archiefbescheiden binnen een redelijke termijn
A. kan worden gevonden

```
   1°. aan de hand van de daaraan gekoppelde metagegevens; of
   2°. door middel van een andere ontsluitingsmethode; en
B. leesbaar of waarneembaar te maken is.
```

N.B. Soms is het nodig om aanvullende informatie over het gebruik van de gegevens op te nemen. Zo kan het bijvoorbeeld van belang zijn om aan te geven dat bitdiepte en resolutie cruciaal zijn voor correcte interpretatie van bestanden.

Toelichting op B 2.1
De beheerorganisatie beschikt over een beschreven procedure om de representatie-informatie te testen en waar nodig naar een vooraf vastgesteld niveau te brengen.

B 2.2
De beheerorganisatie controleert bij de creatie van het opgenomen digitaal archief-stuk (ODA) op volledigheid en juistheid en documenteert het proces rond de opname en creatie.
Het ADA moet aantoonbaar consistent, volledig en correct worden getransformeerd tot ODA. Afhankelijk van de aard van de beheerorganisatie kan een ADA ook pas na verloop van tijd getransformeerd worden. Voor ieder ADA moet ook dan kunnen worden aangetoond of en wanneer het is getransformeerd, dan wel geweigerd (=vernietigd). Dat laatste kan bijvoorbeeld het geval zijn als het ADA niet in overeenstemming is met de eisen uit B 1.3.

Toelichting op B 2.2
De beheerorganisatie stelt een procedure op voor de opname en creatie van het ODA.

B 2.3
De beheerorganisatie gebruikt bruikbare, persistente en unieke identificatie-kenmerken voor ieder opgenomen digitaal archiefstuk (ODA) en bewaart eventuele historische identifi-catiekenmerken.
De kenmerken moeten bruikbaar zijn voor het beheer en de toetsing van de bewaaromge-ving, maar niet noodzakelijkerwijs voor de ontsluiting van de inhoud voor eindgebruikers.

Toelichting op B 2.3
Zie voor een nadere toelichting op dit element het kennisproduct 'Toepassingsprofiel e-depot Achterhoek'.

B 2.4
De beheerorganisatie beschikt voor het opnemen en registreren van de beheerinformatie bij de brongegevens over een beschreven procedure en documenteert de uitvoering daarvan.
Het gaat erom dat alle (soms afzonderlijk geregistreerde) beheerinformatie aantoonbaar op de juiste wijze aan de brongegevens gekoppeld blijft en de integriteit van het ODA gewaar-borgd is.

Toelichting op B 2.4
De beheerorganisatie stelt een procedure op voor de opname en registratie van de be-heerinformatie, inclusief de documentatie van de uitvoering.

B 3. Bewaarstrategie

De beheerorganisatie bewaart archiefbescheiden volgens de van tevoren beschreven, risicogerichte strategie en volgt externe ontwikkelingen om de gewenste resultaten te verzekeren.

B 3.1
De beheerorganisatie toetst en signaleert het verouderen of onbruikbaar worden van representatie-informatie en documenteert de resultaten van deze toetsen.

Archiefregeling art. 25.1
Indien gerede kans bestaat dat als gevolg van wijziging of in onbruik raken van besturingsprogrammatuur of toepassingsprogrammatuur niet langer voldaan kan worden aan de bij deze regeling gestelde eisen ten aanzien van de toegankelijke en geordende staat van digitale archiefbescheiden, zorgt de zorgdrager ervoor dat conversie of migratie van die digitale archiefbescheiden plaatsvindt, dan wel dat die digitale archiefbescheiden door toepassing van emulatie kunnen worden gebruikt of geraadpleegd overeenkomstig de wijze ten tijde van het ontvangen of opmaken ervan door het overheidsorgaan.

Toelichting op B 3.1
Beoordelen van de strategie voor kwaliteitsborging, specifiek op dit onderdeel, vastgelegd door de beheerorganisatie, aan de hand van A 3.2.

B 3.2
De beheerorganisatie beoordeelt de resultaten van de toegepaste bewaarstrategieën en past de werkwijze zo nodig aan.

Toelichting op B 3.2
Zie B 3.1, inclusief documenteren van de beoordeling en eventuele aanpassingen.

B 4. Opslag en beheer van het opgenomen digitale archiefstuk (ODA)

Zaken als de toepassing van migratie, conversie, checksums, kopiëren, gescheiden opslag en de procesgeschiedenis moeten worden vastgelegd als beheerinformatie, zodat de betrouwbaarheid van de beheerde archiefbescheiden kan worden aangetoond en gecontroleerd.

B 4.1
De beheerorganisatie documenteert de uitvoering van de bewaarstrategieën en bewaart de bron- en beheergegevens van het opgenomen digitaal archiefstuk (ODA).

Archiefregeling art. 25.3
De zorgdrager maakt van de conversie of migratie een verklaring op, die ten minste een specificatie bevat van de digitale archiefbestanden die zijn geconverteerd of gemigreerd, en waarin tevens is aangegeven op welke wijze en met welk resultaat getoetst is of na de conversie of migratie aan de bij deze regeling gestelde eisen ten aanzien van de geordende en toegankelijke staat is of kan worden voldaan.

Het bewaren van brongegevens gebeurt altijd in samenhang met beheergegevens. Deze laatste bevatten in het geval van conversie of migratie ook de verantwoording daarvan. Het is niet altijd noodzakelijk of gewenst om alle representaties van brongegevens te bewaren in de bewaaromgeving. Dat kan betekenen dat soms representatie-informatie moet of kan worden verwijderd.

Toelichting op B 4.1
Er is een protocol voor het uitvoeren van de bewaarstrategie, inclusief de documentatie daarvan. Dit protocol wordt getoetst aan de hand van A 3.2. De bewijslast van de toetsing wordt vastgelegd voor de zorgdrager.

B 4.2
De beheerorganisatie kan de integriteit van ieder opgenomen digitaal archiefstuk (ODA) aantonen door middel van de bewaarde beheerinformatie.
Het moet aantoonbaar zijn, dat digitale archiefbescheiden consistent, volledig en betrouwbaar zijn en blijven.

B 5. Informatiemanagement

Het is noodzakelijk dat tevoren wordt vastgelegd welke minimumeisen worden gesteld aan metadata voor beheerde archiefbescheiden.

B 5.1
De beheerorganisatie stelt vast welke ontsluitingsinformatie minimaal nodig is om de beoogde gebruikersgroepen in staat te stellen specifieke informatie te vinden, te herkennen en te interpreteren en zorgt ervoor dat deze gerelateerd wordt aan het opgenomen digitaal archiefstuk (ODA).

Toelichting op B 5.1
Te denken valt onder andere aan:
- Er moet vastgesteld zijn welke ontsluitingsinformatie nodig is.
- Er moet vastgesteld zijn welke beoogde gebruikersgroepen er zijn.
- Er moet vastgesteld zijn of er specifieke informatie vindbaar, herkenbaar en toonbaar is
- De relatie tussen bovenstaande elementen moet duidelijk zijn.

De zorgdrager van de informatie wordt geïnformeerd over de verrijking van de informatie.

B 5.2
De beheerorganisatie kan aantonen dat er een duurzame relatie is tussen ieder opgenomen digitaal archiefstuk (ODA) en de gerelateerde ontsluitingsinformatie.
Ieder ODA moet ontsluitingsinformatie hebben en alle ontsluitingsinformatie moet bij tenminste één ODA horen (= referentiële integriteit).

Toelichting op B 5.2
Metadata en ODA blijven onlosmakelijk verbonden.

B 6. Toegangsbeheer

Voor het inzien van een beschikbaar digitaal archiefstuk (BDA) zijn regels opgesteld, die recht doen aan de door de beoogde gebruikersgroep gewenste openbaarheid en toegankelijkheid alsmede aan de in de toegangsinformatie vastgelegde voorwaarden.

B 6.1
De beheerorganisatie legt vast op welke manier de bewaaromgeving toegankelijk is en maakt dat bekend aan de gebruikers.

Toelichting op B 6.1
Hierbij moet gedacht worden aan:
- gebruikerssoorten;
- autorisaties m.b.t. e-depot, zowel op niveau van gebruikers (zorgdragers, derden), als daarbinnen;
- bescherming van bepaalde data (privacy/openbaarheid);
- juridische status van in e-depot opgenomen te bewaren, te vernietigen (incl. te schonen) archiefbescheiden.

B 6.2
De beheerorganisatie registreert iedere toegang tot de bewaaromgeving en controleert de registratie periodiek op (toegangs)fouten en afwijkingen.

Toelichting op B 6.2
Het gaat hier om een logfile om misbruik te voorkomen en onjuistheden in het functioneren van het systeem te detecteren.

B 6.3
De beheerorganisatie beschikt over vastgesteld en geïmplementeerd toegangsbeleid (autorisatieregels, authenticatie-eisen), dat past bij de voorwaarden in de toegangsinformatie van de archiefbescheiden waartoe toegang wordt gegeven.

B 6.4
De beheerorganisatie kan aantonen dat het proces dat het beschikbaar digitaal archiefstuk (BDA) genereert correct en volledig (doorlopen) is. Ook maakt de beheerorganisatie mogelijk dat, indien dit proces goed doorlopen is, het BDA wordt verspreid onder gebruikers.

4.4 Onderdeel C ▪ Technologie, technische infrastructuur en beveiliging

In dit onderdeel wordt aangegeven hoe de bewaaromgeving technisch is opgebouwd en kan voldoen aan de eisen voor langetermijnbeheer van digitale archiefbescheiden. Veel hiervan is terug te vinden in bestaande standaarden voor informatiebeveiliging, zoals de NEN-ISO/IEC 27001.

C 1. Technische infrastructuur

Met de technische infrastructuur wordt bedoeld dat deel van de ICT-infrastructuur, dat gericht is op het gebruik van de systemen (zoals hardware, systeemsoftware en bijbehorende documentatie).

C 1.1

De beheerorganisatie beschikt ten aanzien van de bewaaromgeving over een actuele beschrijving van de ICT-architectuur.

Voor de bewaaromgeving is een juist, actueel en volledig overzicht van de aanwezige systemen, hard- en software in hun onderlinge samenhang (ICT-architectuur) aanwezig. Deze architectuur moet in lijn zijn met de inrichting van de organisatie uit onderdeel A.

Toelichting op C 1.1

- De beheerorganisatie heeft een configuratie-managementproces ingericht dat deze actualiteit en volledigheid borgt.
- Deze ICT-architectuur is passend voor zijn doel, schaalbaar en flexibel (aanpasbaar bij onder meer nieuwe technologieën of veranderende wet- en regelgeving).
- De ICT-architectuur mag niet leiden tot complexiteit van gebruik.

C 1.2

De beheerorganisatie werkt met besturingssoftware en een infrastructuur die is toegesneden op haar taak.

De aanwezige besturingssoftware en infrastructuur zijn voldoende actueel, zodat ondersteuning door leveranciers of de beheerorganisatie mogelijk is. Voor kritieke onderdelen van de infrastructuur zijn minimaal servicecontracten of service level agreements aanwezig, die ook worden bijgehouden (service level/leveranciersmanagement).

Het is aantoonbaar dat periodiek onderhoud wordt gepleegd op de aanwezige hard- en software en voor alle software worden periodiek (beveiligings)updates uitgevoerd op basis van een risicoafweging.

Toelichting op C 1.2

- De beheerorganisatie heeft een releasebeleid, dat deze eisen ondersteunt en uitvoerbaar is binnen de in de service level agreements (SLA) overeengekomen beschikbaarheidseisen.
- De beheerorganisatie heeft een procedure om tijdig op de hoogte te zijn van fouten in software en bedreigingen (virussen en malware) en maatregelen te treffen om de beschikbaarheid, integriteit en betrouwbaarheid van de operationele ICT-infrastructuur en de ODA-stukken te garanderen. Deze procedure is geborgd in de organisatie.

C 1.3
De beheerorganisatie heeft de geïmplementeerde maatregelen voor het garanderen van de integriteit van ieder opgenomen digitaal archiefstuk (ODA) beschreven.
Hieronder vallen onder andere maatregelen die ervoor zorgen dat in het geval van dubbel uitgevoerde opslag de wijzigingen (bijvoorbeeld in metadata) gesynchroniseerd worden en dat eventuele kopieën van ODA's geregistreerd worden.

Toelichting op C 1.3
Voor deze stukken is met belanghebbenden een overzicht met eisen (per type ODA) opgesteld, waar de beheerorganisatie zich aan heeft geconformeerd. De maatregelen borgen deze eisen.

C 1.4
De beheerorganisatie hanteert effectieve methoden om datacorruptie of dataverlies vast te stellen en te registreren, inclusief genomen tegenmaatregelen.

Toelichting op C 1.4
De beheerorganisatie beschikt over een procedure om juist en tijdig te kunnen reageren op dit soort incidenten, bijvoorbeeld naar aanleiding van een continuïteitsplan. Deze procedure is actueel, met regelmaat getest en geborgd in de beheerorganisatie. Communicatie met de belanghebbenden is geborgd.

C 1.5
De beheerorganisatie beschikt over vastgestelde procedures voor de vervanging van opslagmedia en/of hardware.
Er moet worden gegarandeerd dat wordt ingegrepen ruim vóórdat informatie onleesbaar dreigt te worden of dragers onbruikbaar zijn. Dit staat los van de in B 3 beschreven bewaarstrategieën voor die informatie zelf.

C 1.6
De beheerorganisatie heeft de taken en verantwoordelijkheden voor functioneel beheer, applicatiebeheer en technisch beheer belegd en ingericht op basis van gangbare beheerstandaarden.
Hieronder vallen onder andere het uitvoeren van wijzigingen (inclusief testen).
Voorbeelden van veel voorkomende (kwaliteits)standaarden zijn:
- IT Governance: Control Objectives for Information and Related Technology (CobiT); IT Governance raamwerk Algemene Rekenkamer;
- beveiliging: NEN-ISO/IEC 27001; Voorschrift informatiebeveiliging Rijksdienst (VIR); Voorschrift informatiebeveiliging Rijksdienst-bijzondere informatie (VIRbi);
- software-ontwikkeling: Capability Maturity Model (CMM / CMMI); Rational Unified Process (RUP); ISO 9000-3 (Guidelines for the application); ISO 9001 (development, supply and maintenance of software) ISO 15504 (Spice);
- projectmanagement: Prince-2 projectmanagement; MSP: Managing successful programmes; IPMA: International Project Management Association;
- technisch beheer: Information Technology Infrastructure Library (ITIL);
- applicatiebeheer: Application Service Library (ASL);
- functioneel beheer: Business information Services Library (BISL).

Toelichting op C 1.6
De beheerorganisatie mag ook andere vergelijkbare standaarden inzetten, op voorwaarde de beheerorganisatie kan aantonen dat deze afdoende zijn. De ITIL (V2)-processen zijn tenminste:

- incidentmanagement;
- wijzigingenmanagement;
- probleemmanagement;
- configuratiemanagement;
- capaciteitsmanagement;
- beschikbaarheidsmanagement.

C 2. Beveiliging

De maatregelen die genomen zijn om de bewaaromgeving te beschermen zodat informatie- en functieverlies zijn te voorkomen.

C 2.1
De beheerorganisatie doet aan een systematische risicoanalyse voor factoren als data, systemen, personeel, fysieke locatie en beveiligingseisen en heeft voor iedere beveiligingseis adequate maatregelen getroffen.
Er is een informatiebeveiligingsplan op basis van de NEN-ISO/IEC 27001.

Toelichting op C 2.1

- De risicoanalyse en het bijbehorende risicobeheersingsplan (maatregelen) worden met regelmatige tussenpozen uitgevoerd en opgesteld (actueel) en bevatten zowel de organisatie, haar werkzaamheden als de technische infrastructuur.
- Het informatiebeveiligingsplan met bijbehorende maatregelen zal jaarlijks worden ge-audit, in ieder geval door de organisatie (interne audit), maar bij voorkeur door een externe auditor.
- De organisatie zal zorgen voor officiële certificering zoals opgenomen in de SLA.
- Ten minste de volgende delen van de NEN-ISO/IEC 27001 (actuele versie) maken deel van het informatiebeveiligingsplan, de maatregelen en certificering:
  - eisen voor gerelateerde partijen;
  - belangen van betrokkenen;
  - fysieke beveiliging;
  - logische beveiliging;
  - wijzigingenbeheer;
  - incidentenbeheer;
  - veilige ontwikkeling van programmatuur (eventueel door externen);
  - beveiliging en continuïteit;
  - wet- en regelgeving.
- De organisatie heeft een uitgewerkt overzicht van de wet- en regelgeving (wettelijke eisen) die van toepassing is en de maatregelen om aan deze wettelijke eisen te voldoen.
- De beheerorganisatie beschikt over een procedure voor behandelen van informatiebeveiligingsincidenten en het rapporteren aan de belanghebbenden. Verantwoordelijkheid voor juiste afhandeling van deze incidenten is eenduidig vastgelegd en geborgd.

C 2.2
De beheerorganisatie beschikt over passende calamiteiten- en herstelplannen, die ten minste bestaan uit een back-up van alle opgeslagen informatie en een kopie van het herstelplan op een andere locatie.

Toelichting op C 2.2
- De beheerorganisatie heeft passende calamiteiten- en herstelplannen, die de organisatie in staat stellen om binnen de in de SLA opgestelde termijn weer operationeel beschikbaar zijn (een volledig functionerend e-depot met het gebruik daarvan als voor de calamiteit).
- De passende calamiteiten- en herstelplannen worden aantoonbaar minstens één keer per jaar getest. Deze test is een reële representatie van een echte calamiteit. Een testrapport met bevindingen en mogelijke verbeteringen is beschikbaar. De bevindingen worden tijdig opgevolgd.

C 2.3
Back-ups en herstelplannen worden periodiek gecontroleerd op juiste werking.

Toelichting op C 2.3
- De back-upstrategie moet dusdanig zijn opgezet dat individuele stukken volgens het geldende regime kunnen worden verwijderd van iedere back-up (aantoonbaar verwijderd uit het archief en andere gegevensdragers), zonder dat de nog te bewaren stukken gecompromitteerd worden.
- Restore-testen (controle op juiste werking van back-up) mogen niet leiden tot compromittering van ODA-stukken. Deze stukken mogen niet in de operationele omgeving achterblijven.

C 2.4
De beheerorganisatie heeft een adequate serverruimte met onder meer klimaatbeheersing, alarm en brandmeldvoorziening, toegangscontrole, ordelijke bekabeling en noodstroomvoorziening (UPS).
Zie bijvoorbeeld het 'Handboek ICT, huisvesting en bekabeling' van de Rijksgebouwendienst.

Toelichting op C 2.4:
- Het gebruik van een serverruimte voorziet ook in het juiste niveau van continuïteit en indien noodzakelijk uitwijkmogelijkheden bij calamiteiten. De opzet van serverruimte(n) past binnen de passende calamiteiten- en herstelplannen, zoals opgesteld en operationeel gemaakt.
- De serverruimte(n) bieden het juiste niveau van fysieke toegangsbeveiliging (onder andere compartimentering).
- De in deze ruimte(n) opgestelde apparatuur is beschermd volgens het juiste fysieke beschermingsniveau en alleen toegankelijk voor de beheerorganisatie.
- Andere partijen dan de beheerorganisatie hebben alleen dan toegang tot de genoemde ruimte(n) indien hierover afspraken zijn gemaakt tussen de beheerorganisatie en deze andere partijen.

5 Conclusies en aanbevelingen

De werkgroep doet naar aanleiding van dit rapport de volgende aanbevelingen:

1 De eisen die worden gesteld aan de beheerorganisatie voor het beheer van digitale archiefbescheiden in een e-depot zijn van een geheel andere orde dan het beheer van analoge archiefbescheiden.
- Voer een impactanalyse uit om te bezien welke inspanningen geleverd moeten worden om de toekomstige beheerorganisatie in te richten conform ED_3.
- Overwogen kan worden om een prioritering aan te brengen in de elementen uit ED_3 om zo een overgangsfase te creëren voor de beheerorganisatie, zodat deze tijd heeft zich te ontwikkelen om conform de gestelde eisen te gaan fungeren.

2 Het uitplaatsen van archiefbescheiden heeft gevolgen voor het beheer en de beschikbaarstelling van de archiefbescheiden. Te vernietigen archiefbescheiden moeten verwijderd kunnen worden. Uitgeplaatste archiefbescheiden vallen niet onder de openbaarheid zoals de Archiefwet dit regelt, maar onder de Wet Openbaarheid van Bestuur.
- Indien gekozen wordt om (vernietigbare) archiefbescheiden uit te plaatsen naar het e-depot, wordt aanbevolen de elementen uit de ED_3 aan te vullen met eisen die gesteld worden aan uitgeplaatste archiefbescheiden (bijlage 1).

3 Als dit kennisproduct als basis wordt gebruikt voor een programma van eisen ten behoeve van een aanbesteding van een bewaaromgeving, wordt aanbevolen om de beschreven en toegelichte elementen eerst in een programma van eisen geschikt te maken voor de vorm waarin deze toegepast moeten worden.

Bijlage 1. Toelichting op criteria bij uitgeplaatste archiefbescheiden

De werkgroep heeft bij een aantal criteria in eerste instantie toegelicht waar rekening mee gehouden moet worden bij de keuze om (vernietigbare) archiefbescheiden uit te plaatsen door de zorgdrager bij het e-depot. Het gaat hierbij om archiefbescheiden die in aanmerking komen voor vernietiging of voor toekomstige overbrenging. Uitgeplaatste archiefbescheiden bevinden zich nog in de 'semi-statische fase'. De hieronder opgesomde toelichtingen zijn voorbeelden en moeten nog nader uitgewerkt worden. Bovendien gaan deze voorbeelden slechts over enkele criteria. Daarom moeten alle criteria uit ED_3 nader doorgelicht worden, zodat aanvullingen en/of toelichtingen kunnen worden toegevoegd die slaan op uitgeplaatste archiefbescheiden.

B 2.5 (toegevoegd criterium vanuit de werkgroep):
Er is in ED_3 geen aandacht voor de waarderings- en selectieprocedures, inclusief daadwerkelijke vernietiging. Het moet mogelijk zijn om op termijn te vernietigen informatie uit het e-depot te verwijderen. Dit is inclusief verwijderen van informatie uit op te schonen archief (zie nieuwe Selectielijst).

- Er moeten procedures zijn. Die moeten getoetst worden.
- De metadata dienen te worden vastgelegd.
- Vernietiging moet ook daadwerkelijk vernietiging zijn.
- De zorgdrager blijft verantwoordelijk voor de vernietiging.

B 4.3 (toegevoegd criterium vanuit de werkgroep):
Wanneer opgenomen digitale archiefstukken (ODA's) vernietigd moeten worden, moet de beheerorganisatie deze vernietiging vastleggen. Het moet mogelijk zijn ze te vernietigen. Bovendien moet er bewijs zijn dat deze stukken ook daadwerkelijk zijn vernietigd, wanneer dit heeft plaatsgevonden en wat de grondslag (het besluit) ervan is geweest.

Aanvullende toelichting op B6:
In de overeengekomen afspraken met betrekking tot het inzien van een digitaal archiefstuk tussen zorgdrager en beheerorganisaties moet de volgende informatie voor de ODA's (en daarmee voor de BDA's) zijn opgenomen:

- Zijn de te bewaren archiefbescheiden overgebracht of uitgeplaatst? Welk regime geldt: de Wob of de Archiefwet?
- Bij overplaatsing: wie beslist over de inzage in de stukken (zeker ook bij te vernietigen archiefbescheiden)? Een regeling voor bezwaar en beroep moet hiervan deel uitmaken.
- Bij overbrenging van te bewaren zaken met te vernietigen archiefbescheiden (opschoningstermijn): wie zorgt voor uitvoering van opschoning en voor inzage?
- Tot welke gebruikersgroepen het inzien van toepassing is voor ODA's die niet voor iedereen toegankelijk zijn.

Bijlage 2. Afkortingen en begrippen

Afkortingenlijst

ADA	Aangeboden digitaal archiefstuk
BDA	Beschikbaar digitaal archiefstuk
BRAIN	Branchevereniging Archiefinstellingen Nederland
DA	Digitaal Archiefstuk
DRP	Disaster Recovery Plan (Calamiteiten Herstel Plan)
DVO	Dienstverleningsovereenkomst
ECAL	Erfgoedcentrum Achterhoek en Liemers
ED3	Eisen Duurzaam Digitaal Depot
GR	Gemeenschappelijke regeling
ICTU	ICT Uitvoeringsorganisatie overheidsdiensten
KING	Kwaliteits Instituut Nederlandse Gemeenten
DMS	Document Management Systeem
LOPAI	Landelijk Overleg van Provinciale Archiefinspecteurs
OAIS	Open Archival Information System (ISO 14721)
ODA	Opgenomen digitaal archiefstuk
PDCA	Plan Do Check Act cyclus
RAZ	Regionaal Archief Zutphen
RMA	Record Management Applicatie
SIO	Strategisch Informatie Overleg
SLA	Service Level Agreement
TMLO	Toepassingsprofiel Metadatering Lokale Overheden
WRIJ	Waterschap Rijn en IJssel
XML	Extensible Markup Language

Begrippenlijst

Aanbieder	De aanbieder is, in het OAIS-model, de organisatie die de digitale archiefbescheiden aanbiedt aan het e-depot.
Adapter	Een hulpmiddel dat twee delen verbindt die niet zonder meer aan elkaar passen.
Aggregatieniveau	Het niveau waarop een record kan worden beschreven.
Archiefstuk	Informatieobject, ongeacht zijn vorm, met de bijbehorende metadata ontvangen of opgemaakt door een natuurlijke en/of rechtspersoon bij de uitvoering van taken en bewaard om te voldoen aan wettelijke en/of administratieve eisen en/of maatschappelijke behoeften.
Audit	Onderzoek naar het functioneren van een bedrijf als geheel of op onderdelen.
Audit trails	Controletrajecten.
Baseline Informatie-huishouding Gemeenten	De Baseline Informatiehuishouding Gemeenten is beoogd als het algemene, voor alle gemeenten en voor alle onder-

	delen van de gemeente - ook samenwerkingsverbanden en uitvoerende diensten - geldende normenkader voor informatiebeheer, dat de toegankelijkheid en betrouwbaarheid van overheidsinformatie bevordert.
Bewaaromgeving	Het geheel van ruimten, apparatuur, programmatuur en systeemprocedures waarmee de beheerorganisatie in staat is digitale informatie te beheren.
Bitdiepte	Of Kleurdiepte. Meeteenheid voor de hoeveelheid kleuren die een enkele punt kan weergeven.
Compressietechniek	Techniek om de omvang van een bestand te verkleinen.
Conformiteit	In overeenstemming met.
Contextinformatie	Metadata die een beschrijving geven van de relaties tussen brongegevens en hun omgeving.
Conversie	Omzetting of overzetting van gegevens in een ander bestandsformaat.
Decryptiesleutel	Een hulpmiddel voor het weer leesbaar maken van vercijferde gegevens.
Digitale archiefbescheiden	Archiefbescheiden die uitsluitend met besturingsprogrammatuur of toepassingsprogrammatuur geraadpleegd kunnen worden (Archiefregeling). Meervoud van digitaal archiefstuk (ED_3). De aangeboden (ADA), opgenomen (ODA), ter beschikking gestelde (BDA) duurzaam te bewaren en beheren digitale informatie-objecten inclusief de bijbehorende metadata.
Digitaal archiefstuk	Het DA is het enkelvoud van digitale archiefbescheiden.
Digitaal bronbestand	Bestand dat door de zorgdrager wordt aangeleverd aan de beheerorganisatie van het e-depot.
Digitale handtekening	Een methode voor het bevestigen van de juistheid van de digitale informatie.
E-conservator	Een functionaris verantwoordelijk voor de opname, toegankelijkheid en duurzaam behoud van digitale archiefbescheiden in het e-depot.
E-depot	Het geheel van organisatie, beleid, processen en procedures, financieel beheer, personeel, databeheer, databeveiliging en aanwezige hard- en software dat duurzaam beheren en raadplegen van digitale archiefbescheiden mogelijk maakt.
ED_3	Eisen Duurzaam Digitaal Depot is binnen de Nederlandse archiefwetgeving een toetsingskader voor langetermijnbeheer van blijvend te bewaren digitale informatie.
Emulatie	Nabootsen en reconstrueren van originele hard- en software zodat de originele computerbestanden in hun oorspronkelijk formaat raadpleegbaar zijn.
Encryptietechniek	Het coderen van gegevens op basis van een bepaald algoritme. De versleutelde gegevens kunnen later weer gedecrypteerd worden.

Escrow overeenkomst	Afspraak tussen een softwarehuis en zijn klant om de software te plaatsen in handen van een onafhankelijke derde, die deze bewaart en in een omschreven situatie overdraagt aan een of meer andere personen.
Eventplan	Plan waarin een activiteit of gebeurtenis is opgenomen die in de toekomst moet/zal gebeuren.
Extensible Markup Language	XML is een standaard van het World Wide Web Consortium voor de syntaxis van formele opmaaktalen waarmee men gestructureerde gegevens kan weergeven in de vorm van platte tekst.
Fallbackscenario	Terugvalscenario. Een alternatieve werkwijze als de reguliere werkwijze als gevolg van een incident niet meer tot het gewenste resultaat leidt.
ICT-strategie	Een document over de bijdrage van ICT aan de doelstellingen en de continuïteit van de organisatie.
Identity management	Het geheel van processen en hulpmiddelen waarmee een identiteit kan worden geverifieerd en kan worden gekoppeld aan de juiste toegangsrechten.
Integriteitsinformatie	Metadata waarmee de fysieke integriteit van de brongegevens gecontroleerd kan worden.
ISO 14721	Space data and information transfer systems – Open archival information system (OAIS) – Reference model.
ISO 16363	Space data and information transfer systems – Audit and certification of trustworthy digital repositories.
Liquidatieplan	Een plan waarin staat wat er moet worden geregeld om een organisatie/bedrijf op te heffen.
Logging	Het vastleggen in een log, bijvoorbeeld een systeemlog of een securitylog, van feitelijk uitgevoerde bewerkingen en/of pogingen daartoe.
Malware	Is elke software die gebruikt wordt om computersystemen te verstoren, gevoelige informatie te verzamelen of toegang te krijgen tot private computersystemen. Computervirus, spyware, computerworm, Trojaans paard, etc.
Metadata	Metadata zijn gegevens (data) over gegevens (data). Naast de gegevens over inhoud, structuur en vorm van archiefbescheiden moeten bij digitale archiefbescheiden ook de technische kenmerken (bijv. bestandsformaat, soft- of hardwareafhankelijkheden) worden vastgelegd en bewaard. Dit is van belang om de omstandigheden waarin de data zijn gemaakt en bewaard te kunnen herleiden en daarmee de digitale archiefbescheiden te allen tijde te kunnen reconstrueren.
Metadataschema	Logische structuur die het verband aangeeft tussen elementen van metagegevens, doorgaans door regels vast te stellen voor het gebruik en beheer van metagegevens, vooral met betrekking tot de semantiek, de syntaxis en de keuzevrijheid (mate van verplichting) van waarden.

Migratie	Overzetting van gegevens en toepassingsprogrammatuur naar een ander platform, met behoud van authenticiteit, integriteit, betrouwbaarheid en bruikbaarheid.
NEN-ISO 23081	Informatie en documentatie - Processen voor informatie- en archiefbeheer – Metagegevens voor archiefbescheiden.
NEN-ISO 15489	Informatie en documentatie – Informatie- en archief-management.
NEN-ISO 27001	Informatietechnologie – Beveiligingstechnieken – Managementsystemen voor informatiebeveiliging – Eisen.
NEN 2082	Eisen voor functionaliteit van informatie- en archief-management in programmatuur.
NEN-ISO 16175	Informatie en documentatie: principes en functionele eisen voor archiefbescheiden in een elektronische kantooromgeving.
Ontsluitingsinformatie	Metadata, voornamelijk bestaande uit inhoudelijke beschrijvingen, die het vinden, ordenen en opvragen van het opgenomen digitale archiefstuk (ODA) in de bewaaromgeving mogelijk maken. De ontsluitingsinformatie is specifiek voor de bewaaromgeving bij de opname als een soort index gegenereerd of toegekend en wordt gewoonlijk afgeleid van de beheerinformatie.
Opvolgingsplan	Plan waarin wordt geregeld wat er moet gebeuren als de beheerorganisatie ophoudt te bestaan.
Overbrenging	Procedure waarbij een zorgdrager van een overheidsorgaan archiefbescheiden overdraagt aan de archiefbeheerder van een archiefbewaarplaats.
Pixel	Een gekleurde punt op het beeldscherm van de computer of in een digitaal beeld. Veel punten bij elkaar geven een beeld.
Portabiliteit	Mate van integratie met de bestaande IT-infrastructuur.
Preservering	Proces van bewaren en beheren binnen het archiefsysteem. Het geheel van activiteiten gericht op de zorg voor het technische en intellectuele behoud van archiefdocumenten.
Recovery	Herstellen van data na dataverlies.
Relatie-informatie	Metadata die brongegevens en beheerinformatie van het digitale archiefstuk (DA) als één logisch geheel verbinden voor identificatie en gebruik.
Representatie-informatie	Metadata die nodig zijn om het digitale bronobject reproduceerbaar (leesbaar) en juist interpreteerbaar te maken. Dit kan een beschrijving van hard- en software of een samenvatting/beschrijving van de juiste interpretatie van het digitaal bronobject zijn.
Resolutie	Term om het aantal gebruikte pixels op bijvoorbeeld een beeldscherm te beschrijven. Hoe hoger dat aantal, hoe hoger de maximale resolutie van het scherm.

Security scans	Een scan om zwakke punten in de informatiebeveiliging te laten zien.
Semantiek	Wetenschap die zich bezighoudt met de betekenis van symbolen en in het bijzonder van taal en woorden.
Syntax	De vorm en structuur van de informatie.
Toegangsinformatie	Metadata die (wettelijke) beperkingen van de toegang tot brongegevens beschrijven en tevens de bij opname overeengekomen voorwaarden voor toegang en verspreiding bevatten. Hieronder vallen auteursrechten, licentierechten, technische beperkingen, openbaarheidsbeperkingen en toegangscontrole.
Uitplaatsing	Het plaatsen van te bewaren en te vernietigen digitale archiefbescheiden in een e-depot voordat deze moeten worden overgebracht of vernietigd.
Validatie	Het controleren van een waarde op geldigheid of juistheid.
Verwijzingsinformatie	Metadata, die de unieke kenmerken ('identifiers') voor de brongegevens bevatten en eenduidige verwijzing naar brongegevens mogelijk maakt, ook voor externe systemen.
Virtual machine	Een computerprogramma dat een computer nabootst.
Zaakgericht werken	Een concept dat helpt om digitaal te werken en te archiveren.
Zorgdragers	Degene die bij of krachtens de wet is belast met de zorg voor de archiefbescheiden (Archiefwet 1995, art. 1).