

E D 3

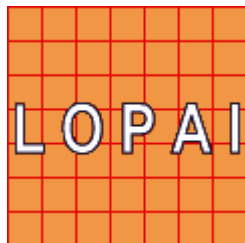
Eisen Duurzaam Digitaal Depot

toetsingskader voor de beheersomgeving
van blijvend te bewaren digitale informatie

Versie 1

Landelijk Overleg Provinciale Archief Inspecteurs
mei 2008

foto omslag: Koninklijke Bibliotheek Den Haag



Inhoudsopgave	
Voorwoord	5
1. Inleiding	6
2. Terminologie	13
3. Criteria	18
A. Organisatie, beleid en procedures	18
B. Beheer van digitale archiefbescheiden	22
C. Technologie, technische infrastructuur en beveiliging	30
4. Concordans TRAC – ED₃ – TRAC	37

Dit document mag worden gekopieerd, verspreid en doorgegeven,
als daarbij de aangegeven naam en herkomst worden vermeld.
Het document mag niet bewerkt of voor commerciële
doeleinden gebruikt worden.

Bij hergebruik of verspreiding dient de gebruiker deze voorwaarden
kenbaar te maken aan derden, bijvoorbeeld door middel van een
link naar <http://creativecommons.org/licenses/by-nc-nd/3.0/nl/>.



Op dit werk is een [Creative Commons Licentie](http://creativecommons.org/licenses/by-nc-nd/3.0/nl/) van toepassing.

 **creative
commons** nederland

Voorwoord

ED₃ (Eisen Duurzaam Digitaal Depot) is binnen de context van de Nederlandse archiefwetgeving een eerste poging tot een uitgewerkt toetsingskader voor de beheersomgeving van blijvend te bewaren digitale informatie.

Met de verschijning van het rapport "Een demeterende overheid?" van de Rijksarchiefinspectie in januari 2005 is het besef gegroeid, dat nieuwe wet- en regelgeving nodig is op het gebied van het beheer van digitale overheidsinformatie. De toenemende digitalisering van overheidsinformatie, of het nu gaat om *born digital* informatie of om vervangen papieren informatie, vereist nieuwe beheersregimes en een nieuwe toezichtspraktijk. Samenwerking tussen de documentaire informatievoorziening, archiefwezen en ICT is daarbij onontbeerlijk.

Op 29 juni 2006 hebben de Staatssecretaris van Cultuur en de Minister voor Bestuurlijke Vernieuwing en Koninkrijksrelaties de nota "Informatie op orde: vindbare en toegankelijke overheidsinformatie" toegezonden aan de Tweede Kamer. Hierin wordt geconstateerd dat bestaande regels ten aanzien van de digitale documenthuishouding onvoldoende worden nageleefd. In de nota worden de actielijnen vermeld die ervoor moeten zorgen dat overheidsinformatie vindbaar, toegankelijk, betrouwbaar, authentiek en volledig is. Aansluitend is de rijksoverheid begonnen met de uitwerking van deze acht actielijnen.

Ook bij decentrale overheden heeft de digitale informatiestroom een flinke vlucht genomen, zodat ook daar vergelijkbare vraagstukken aan de orde zijn. De provinciale archiefinspecties zien zich steeds vaker geconfronteerd met praktische vragen rondom de inrichting van een digitale archieffunctie. Gemeenten staan op het punt om hun informatiehuishouding volledig te digitaliseren. Machtigingsverzoeken tot vervanging beginnen binnen te komen bij alle overheidslagen. Daarom is in januari 2008 door de minister een beleidsregel vervanging in digitale vorm vastgesteld en hebben de provincies hun beleidsregel uit 2000 herzien, waarbij onder andere vervanging van analoge archieven in digitale vorm mogelijk wordt.

Blijvend te bewaren digitale overheidsinformatie komt terecht in een digitaal depot, ook wel eDepot genoemd. Tot nu toe ontbreekt echter op de Archiefwet gebaseerde regelgeving gericht op eDepots, zoals die wel bestaat voor analoge archiefbewaarplaatsen. In afwachting van nieuwe regelgeving op dit gebied heeft het LOPAI in samenwerking met Het Expertise Centrum (HEC) een toetsingskader ontwikkeld. De volgende personen hebben commentaar aangeleverd op het concept daarvan:

J. Beens, R. Camps, L. Gruppelaar en W. Mastenbroek	- Regionaal Archief Nijmegen
R. van den Belt, E. Fleurbaay, R. Gillesse, M. Holtman en A. de Jonker	- Stadsarchief Amsterdam
I. Broos en F. Schoonheim	- Provinciale Archiefinspectie Utrecht
M. Jansen	- Regionaal Archief Tilburg
E. Kretzschmar	- Provinciale Archiefinspectie Zuid-Holland
J. van Oss	- Het Utrechts Archief
J. Schuurman Hess	- Gemeentearchief Rotterdam
B. te Vaarwerk	- Provinciale Archiefinspectie Gelderland
A. de Vries	- Provinciale Archiefinspectie Groningen

Er is dankbaar gebruik gemaakt van dit commentaar bij het opstellen van het hier weergegeven eindresultaat. Uiteraard blijven de samenstellers eindverantwoordelijk voor de gemaakte keuzes.

Digitale depots staan in Nederland nog in de kinderschoenen. Voortrekkers op dit gebied zijn de Koninklijke Bibliotheek (niet bedoeld voor archiefbescheiden), het Nationaal Archief, dat met het Gemeentearchief Rotterdam werkt aan een eigen depot, en de Justitiële Informatiedienst van het Ministerie van Justitie met haar CDD+ (Centraal Digitaal Depot). Het is nog onduidelijk in welke richting de ontwikkelingen zullen gaan en hoeveel eDepots er uiteindelijk zullen komen. Met ED₃, Eisen Duurzaam Digitaal Depot, hoopt het LOPAI in elk geval een instrument en terminologie aan te bieden voor de bewustwording over en de opbouw, ontwikkeling en toetsing van de kwaliteit van eDepots. Het eDepot bevindt zich op het snijvlak van archief en ICT en dat noodzaakt tot samenwerking tussen deze twee werelden. Er kan niet genoeg nadruk op gelegd worden, dat niet alleen de archiefwaardigheid (metadata) van bestanden - een voor archivariissen vertrouwd onderwerp - maar ook het behoud ervan door een stevige ICT-infrastructuur (onderdeel C van ED₃) essentieel is voor een eDepot.

Veel zal in de komende jaren nog verder moeten worden ontwikkeld aan de hand van nieuwe inzichten en ervaringen in de praktijk. Ook de te verwachten wijzigingen in de archiefwetgeving, waaraan wij met dit stuk hopen bij te dragen, zal verdere ontwikkeling noodzakelijk maken. Op basis van alle bouwstenen, zoals de door de rijksoverheid binnenkort te ontwikkelen Baseline, de implementatie van (inter)nationale standaarden en de invoering van de aangepaste archiefregelingen, zal dit uiteindelijk moeten leiden tot een vast kader voor de beheersomgeving tijdens de gehele levenscyclus van digitale archiefbescheiden. Nadrukkelijk wil het LOPAI commentaar op ED₃, evenals ervaringen met het gebruik ervan, meenemen in de verdere ontwikkeling.

De samenstellers:

LOPAI

Dick Bunscoeke
Lolke Folkertsma
Chido Houbraken
Ingmar Koch

HEC

Marianne Loef
Boudien Glashouwer
Chris Wauters

1. Inleiding

1.1 Kaders

In het eerste artikel van de *Archiefwet 1995* is vastgelegd dat ook digitale informatie van de overheid tot de archiefbescheiden kan worden gerekend. In de *Regeling geordende en toegankelijke staat archiefbescheiden* (Stcrt. 2002, 43) is vervolgens uitgewerkt welke kenmerken een te bewaren archiefstuk moet hebben:

- Authentiek het is wat het beweert te zijn
- Betrouwbaar het is een accurate voorstelling van de transactie waar het over handelt
- Integer het is niet ongeautoriseerd te veranderen en veranderingen zijn na te gaan
- Bruikbaar het is vindbaar, raadpleegbaar en begrijpelijk binnen de originele context

Voor digitale archiefbescheiden is dat met de *Regeling* verder uit te werken met de volgende steekwoorden:

- Uitvoerbaar de dragers moeten intacte bitstreams bevatten
- Visualiseerbaar art. 7, 8.2 en 8.3, de bitstreams moeten door de computer correct weergegeven worden op het scherm
- Standaarden art. 6, maar deze lijst is niet uitputtend en aan verandering onderhevig
- Metadata art. 8.1 en 9, vergelijk ook NEN-ISO 23081-1:2006
Hierbij komen verschillende aspecten aan de orde:
 - archiefbescheiden en de bijbehorende metadata
 - alle processen die daar betrekking op hebben
 - alle systemen waar deze bescheiden en metadata in voorkomen
 - elke organisatie die verantwoordelijk is voor beheer van deze bescheiden
- Duurzaamheid art. 5, 10.2, 10.3 en 11.2

Het internationaal aanvaarde *Open Archival Information System* (OAIS) model kan helpen bij de ontwikkeling van een informatiebeheer- en archiveringssysteem dat bovenstaande eigenschappen ondersteunt. OAIS werd ontwikkeld door Nasa's Consultative Committee for Space Data Systems en is daarna als ISO-standaard vastgelegd (ISO-14721:2002). Alhoewel het OAIS-model toepasbaar is op zowel papieren als digitale documenten, is het model voornamelijk op deze tweede categorie gericht.

De definitie voor een eDepot die we willen hanteren komt voort uit de op basis van OAIS door de RLG-National Archives and Records Administration Digital Repository Certification Task Force ontwikkelde *Trustworthy Repositories Audit & Certification: Criteria and Checklist* (TRAC), versie 1.0 februari 2007:

"The entire system in which the digital information is managed, including the organization running the repository, its governance, organizational structure and staffing policies and procedures, financial fitness and sustainability, the contracts, licenses and liabilities under which it must operate and trusted inheritors of data, as applicable. Additionally, the digital object management practices, technological infrastructure, and data security in place must be reasonable and adequate to fulfil the mission and commitments of the repository."

Aansluitend op bovenstaande Engelse definitie verstaan we daarom onder het eDepot:

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

1.2 Verantwoording: van TRAC naar ED₃

1.2.1 Keuze voor TRAC

Bij de voorbereiding van de werkzaamheden werden verschillende bestaande toetsingsinstrumenten bekeken, zoals:

- *Catalogue of Criteria for Trusted Digital Repositories* (nestor),
- *Digital Repository Audit Method Based on Risk Assessment* (DRAMBORA) en
- *Trustworthy Repositories Audit & Certification: Criteria and Checklist* (TRAC).

Al deze instrumenten zijn gerelateerd aan het *Open Archival Information System* (OAIS) en worden beschouwd als "Birds of a feather" (BoF) bij de internationale pogingen om te komen tot standaardisatie van eDepots.

DRAMBORA en *nestor* vielen af omdat ze niet gericht zijn op toezichthouders, maar op beheerders. Het eerste is een methode voor risicoanalyse en zelftoetsing, het tweede is een handleiding voor ontwerp, planning en invoering, die tevens geschikt is voor zelftoetsing van een eDepot. *TRAC* kwam het dichtste in de buurt van wat LOPAI voor ogen stond: een bruikbaar kader voor de externe toetsing van eDepots, dat ook als hulpmiddel bij de opbouw en ontwikkeling ervan kan dienen. Ook bestaande initiatieven, zoals bij de Koninklijke Bibliotheek en het Gemeentearchief Rotterdam, bleken in meer of mindere mate rekening te houden met de eisen uit *TRAC*.

De werkgroep van het LOPAI is daarom samen met medewerkers van Het Expertise Centrum (HEC) aan de slag gegaan op basis van de in *TRAC* geformuleerde eisen.

De opbouw van TRAC kan op de volgende manier kort worden samengevat:

A. De organisatie

1. opdracht, mensen en middelen duurzaam en bestuurlijk vastgelegd
2. procedures en overeenkomsten toetsbaar en transparant vastgelegd

B. Het beheer

1. gereguleerde opname van informatie, waarbij eigenschappen en context worden vastgelegd en de integriteit wordt gecontroleerd
2. gereguleerde beschrijving van opgenomen informatie, waarbij herkomst, bewerking en beheer worden vastgelegd
3. procedurele toetsing van duurzaamheid en integriteit van opgenomen informatie
4. documentatie van onderhoud en beheer van opgenomen informatie
5. beschrijving van vereiste metadata, duurzaam gekoppeld aan opgenomen informatie
6. gereguleerde en gedocumenteerde toegang tot opgenomen informatie
7. beschikbaarheid van opgenomen informatie, die aantoonbaar integer en volledig is

C. De techniek

1. betrouwbare, toegesneden en beheersbare besturingssoftware, infrastructuur en back-up functionaliteiten
2. getoetste procedures voor en documentatie van het kwaliteitsbeheer
3. gestructureerde en toegesneden beveiliging met een doelmatig calamiteitenplan

1.2.2 De vertaling, normering en waardering

De eerste stap behelsde een integrale vertaling van de eisen uit TRAC, zodat die voor een breder publiek toegankelijk kunnen worden. Deze vertaling is vervolgens voorgelegd aan vakgenoten in Nederland en België ter becommentariëring (zie voorwoord).

Op basis van de vertaling en het aangeleverde commentaar is nader gekeken naar de inhoud van de eisen. Sommige werden overbodig geacht en sommige werden samengevoegd. In een enkel geval werd er gesplitst. Daarnaast is hier en daar de volgorde gewijzigd. Voorop stond, dat er een voor de Nederlandse situatie duidelijk, hanteerbaar en uitvoerbaar instrument diende te ontstaan. Het aantal eisen werd teruggebracht van 84 naar 75. In de concordans (hoofdstuk 4) is dat uitvoeriger weergegeven.

Vervolgens werden de overgebleven criteria gekoppeld aan de huidige wettelijke eisen, iets wat uiteraard niet in TRAC is opgenomen maar wel noodzakelijk is voor een volwaardig toetsingskader binnen de Nederlandse context. Natuurlijk zal ED₃ worden aangepast bij wijzigingen van de wet- en regelgeving.

Ook is gekeken naar het gewicht van de verschillende eisen binnen het geheel van het toetsingskader, iets wat TRAC evenmin doet. Gekozen is voor een drietal verschillende waarderingsniveaus:

1. vierendertig eisen van doorslaggevend belang (gemarkt met ★)
2. drieëndertig eisen van groot belang (gemarkt met ■)
3. acht eisen van normaal belang

Deze verschillende niveaus kunnen de zorgdragers en beheerders helpen bij de opbouw van een eDepot. Voor de toezichthouders vormen zij een hulpmiddel bij het vormen van een eendoordeel over de kwaliteit van een specifieke situatie. Het "professional judgment" van de toezichthouder zal in de boven gegeven volgorde van toenemend belang zijn bij de beoordeling. De eisen van de eerste categorie zijn cruciaal: deze moeten allemaal als voldoende worden beoordeeld, wil er een positief oordeel over het eDepot worden gegeven.

Bewust is niet gekozen voor een puntennormering, omdat die de schijn van exacte beoordeling wekken zou.

Het aldus ontstane initiële document is binnen de kring van het LOPAI gepresenteerd. Daarna is nogmaals om commentaar gevraagd, zowel binnen als buiten het LOPAI. Ook is er een eerste test op bruikbaarheid in de praktijk door provinciale inspecteurs uitgevoerd.

Tenslotte is met het commentaar en de ervaringen die inmiddels waren opgedaan het stuk aangepast en van een inleiding voorzien.

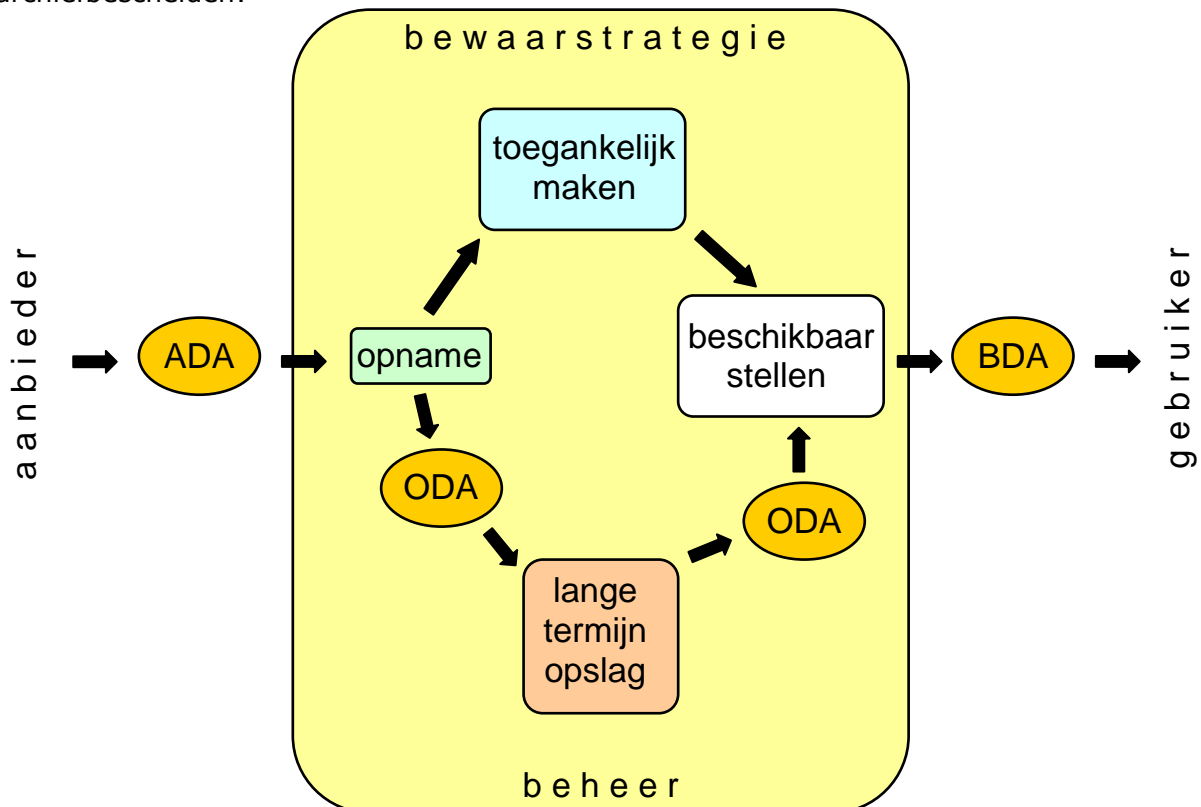
1.2.3 Digitale archiefbescheiden

Het OAIS biedt een kader waarbinnen procedures voor de lange termijn archivering van digitale informatie worden uitgewerkt. In kort bestek zijn daarbij de volgende onderdelen onderscheiden:

opname	kwaliteitscontrole, registratie, beschrijving, extractie metadata, transformatie archiefdocumenten
lange termijn opslag	goede materiële omstandigheden voorzien, vervangen dragers, foutopsporing (checksums), rampenplan, back-ups maken, leesbaar houden
toegankelijk maken	beheren en bijwerken beschrijvingen en metadata, zoekmogelijkheden voorzien

beheer	formuleren beleid, overleggen met archiefvormers, standaarden vastleggen, beheer digitaal depot, bijhouden documentatie, opvolgen technologische veranderingen
bewaarstrategie	regelmatige evaluatie inhoud depot, advisering eventuele migraties, ontwikkeling standaarden en beleid, monitoren technische ontwikkelingen en wensen gebruikersgroepen
beschikbaar stellen	archieftoegangen en archiefdocumenten beschikbaar stellen

Voor het begrip van de behandeling van digitale informatie maakt het OAIS onderscheid tussen verschillende stadia. Dit is overgenomen in ED₃ als indeling voor digitale archiefbescheiden:

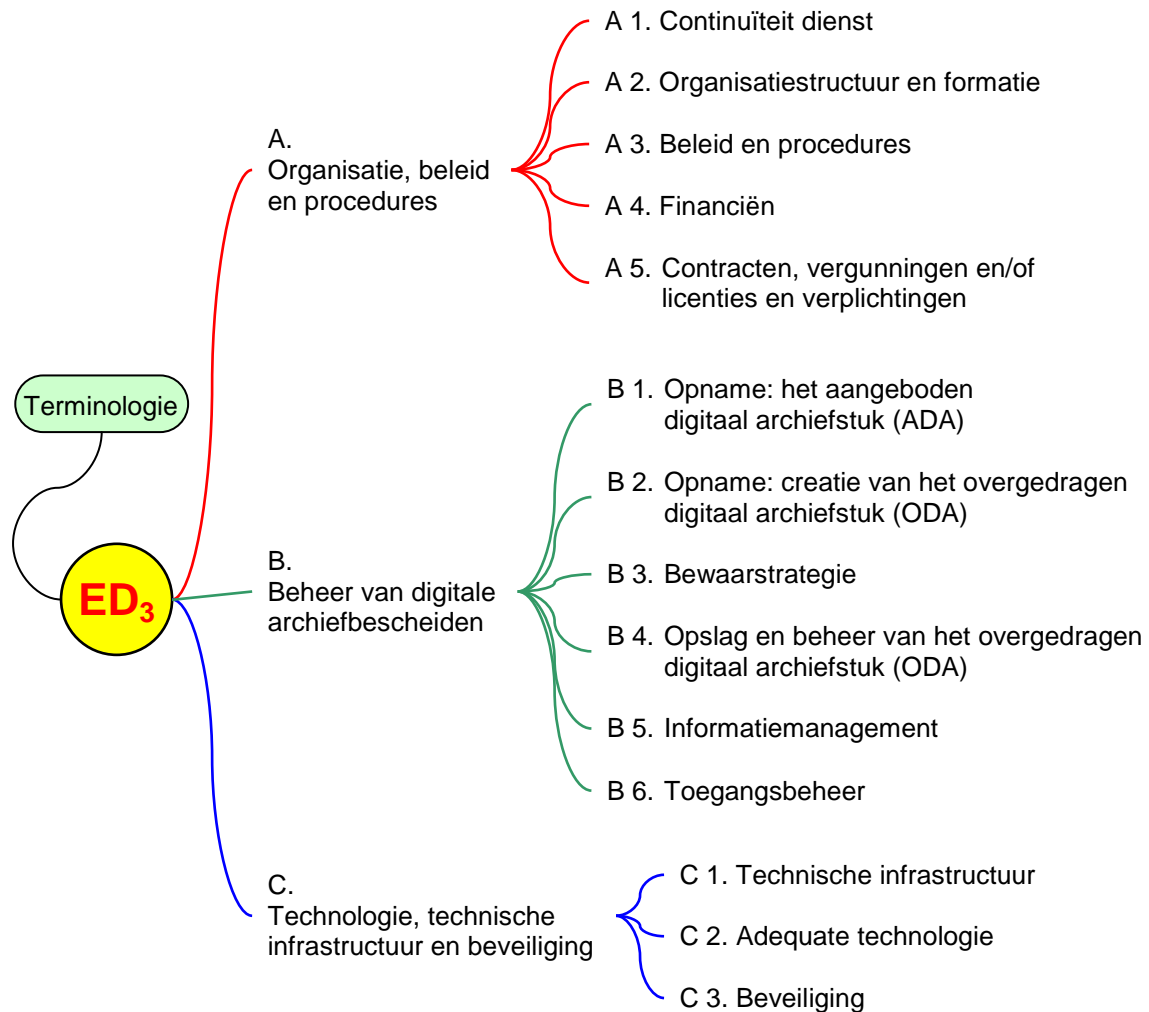


Afb. 1. digitale archiefbescheiden in samenhang

Het digitaal archiefstuk (DA), zoals ontstaan en gebruikt in de werkprocessen van de archiefvormer, wordt bij overdracht het *aangeboden digitaal archiefstuk* (ADA) voor het eDepot. Daar wordt het via de procedure van opname bewerkt tot *overgedragen digitaal archiefstuk* (ODA), geschikt voor lange termijn bewaring in het eDepot. Er kunnen naast nieuw gevormde representaties ook oorspronkelijke representaties worden beheerd als ODA, bijvoorbeeld naast PDF's ook Wordbestanden, zodat later eventueel opnieuw (aan nieuwe inzichten aangepaste) representaties zijn te formeren. Op basis van de vraagstelling van gebruikers wordt door het eDepot het *beschikbare digitaal archiefstuk* (BDA) verspreid. Dit levert niet alleen nieuwe (gebruiks)metadata voor het ODA, maar kan ook zelf als nieuwe representatie van het ODA weer opgenomen worden in het eDepot.

1.2.4 Gebruik van ED₃

Op basis van het voorgaande is geleidelijk een toetsingsinstrument ontstaan. Evenals TRAC is het opgebouwd uit drie onderdelen:



Afb. 2. structuur ED₃

In onderdeel A staan de criteria waaraan de dienst, waaronder het eDepot functioneert, moet voldoen. Bij de inrichting van een eDepot, bijvoorbeeld als gemeenschappelijke regeling tussen een aantal overheden, kunnen deze criteria worden gebruikt als checklist wanneer de organisatie wordt ingericht.

Nog meer dan bij een (analoge) archiefbewaarplaats strekken de eisen zich bij een eDepot ook uit tot die organisatie, omdat de inrichting daarvan cruciaal is voor de waarborging van de kwaliteit van de interne beheersprocessen. Digitale archiefbescheiden zijn kwetsbaarder en dynamischer dan analoge archiefbescheiden.

Onderdeel B bevat criteria voor de beheersprocessen van de dienst. Deze zijn gebaseerd op de eisen van de archiefwetgeving en moeten vooral de kwaliteit van digitale archiefbescheiden waarborgen. In de verschillende fases van de betrokken digitale archiefbescheiden, ADA-ODA-BDA, moeten de juiste metadata opgenomen, gegenereerd, toegevoegd en in samenhang beheerd kunnen worden om aan de archiefwetgeving te kunnen voldoen.

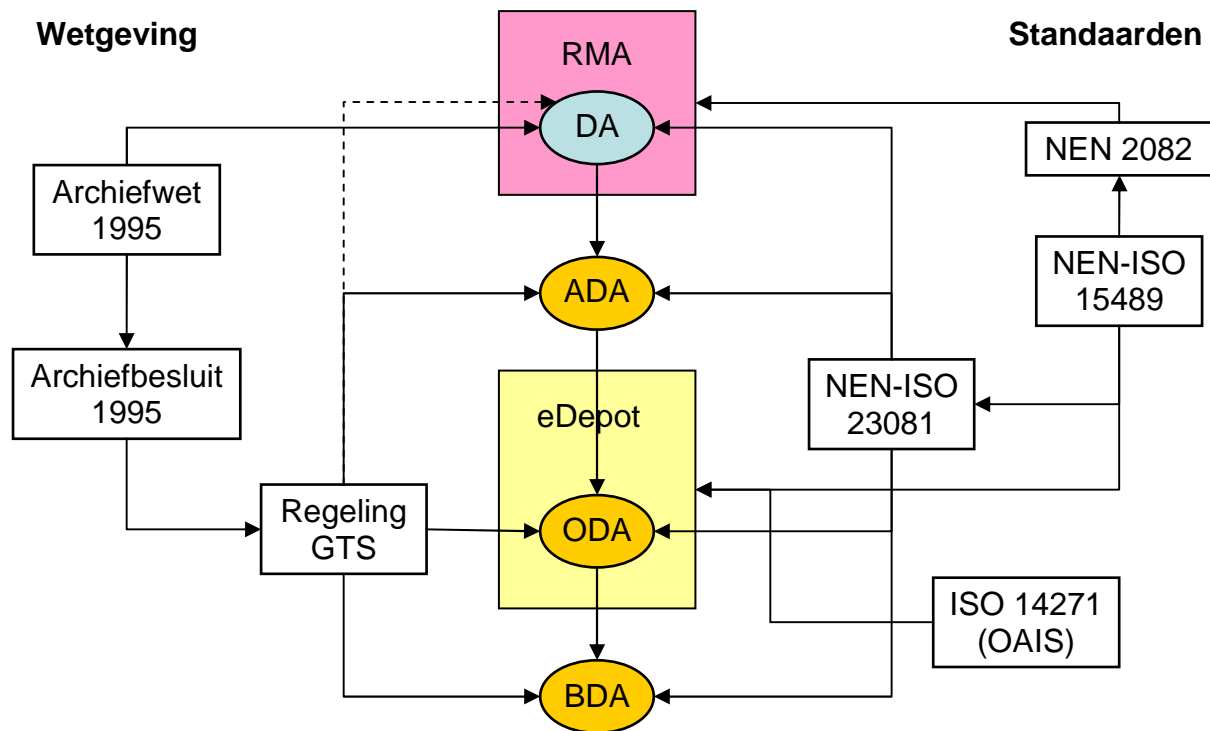
De criteria voor de beheerde digitale archiefbescheiden zijn bedoeld als middel om de kwaliteit van zorg en beheer te kunnen beoordelen, zodat op basis daarvan vertrouwen in deze digitale overheidsinformatie kan worden gesteld. Dit komt overeen met de archiefregelingen op basis van artikel 11 en 12 van het *Archiefbesluit 1995*.

Onderdeel C gaat over de techniek van het eDepot zelf, vergelijkbaar met de regeling op basis van artikel 13 van het *Archiefbesluit 1995* voor de analoge bewaarplaatsen van archiefbescheiden. 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.

In de onderlinge samenhang tussen de drie genoemde onderdelen geeft ED₃ een toetsingskader voor de kwaliteit van de archiefzorg, waar het te bewaren digitale archiefbescheiden betreft. Dit instrument kan zorgdragers en beheerders helpen bij de inrichting van eDepots, omdat het de uitgangspunten voor wettelijke toezichthouders in beeld brengt.

1.2.5 Relatie tot wetgeving en standaarden

Bij het opstellen van de eisen spelen naast wet- en regelgeving ook de erkende standaarden een rol. In onderstaand overzicht is dat schematisch in beeld gebracht:



Afb. 3. verhouding digitale archiefbescheiden met wetgeving en standaarden

De archiefwetgeving richt zich op de zorg voor en het beheer van archiefbescheiden, waarbij de *Regeling geordende en toegankelijke staat archiefbescheiden* (= Regeling GTS) speciaal voor te bewaren archiefbescheiden nadere invulling geeft. De NEN-ISO 15489 regelt het archiefmanagement, nader ingevuld voor de te gebruiken programmatuur in de NEN 2082. De NEN-ISO 23081 geeft standaarden voor de toe te kennen metadata en de ISO 14271 geeft een model voor een beheersysteem voor (met name) de lange termijn bewaring van digitale archieven

1.2.5 Korte lijst van gebruikte literatuur¹

Catalogue of Criteria for Trusted Digital Repositories (nestor), december 2006
<http://edoc.hu-berlin.de/series/nestor-materialien/8/PDF/8.pdf>

Digital Repository Audit Method Based on Risk Assessment (DRAMBORA), februari 2007
<http://www.repositoryaudit.eu/>

Expertisecentrum DAVID (F.Boudrez), "Basisprocessen voor een digitaal archiefdepot", 2006
http://www.expertisecentrumdavid.be/digitaaldepot/basisprocessen_digitaalarchiefdepot.pdf

Expertisecentrum DAVID (F.Boudrez), "Digitale containers voor het digitaal archiefdepot", 2005
http://www.expertisecentrumdavid.be/docs/digitale_containers.pdf

Hans Hofman, "Een uitdijend heelal? Context van archiefbescheiden", in: P.J. Horsman, F.C.J. Ketelaar en T.H.P.M. Thomassen (red.), *Context. Interpretatiekaders in de archivaliek*, Jaarboek 2000 Stichting Archiefpublicaties, pp. 45-65.

Reference Model for an Open Archival Information System (OAIS), januari 2002
<http://public.ccsds.org/publications/archive/650x0b1.pdf>

Trustworthy Repositories Audit & Certification: Criteria and Checklist, februari 2007
<http://www.crl.edu/PDF/trac.pdf>

¹ De gebruikte linken zijn gecontroleerd op 17 mei 2008.

2. Terminologie

Deze terminologie is beperkt tot een omschrijving van de meest elementaire en relevante begrippen uit ED₃, waarbij tevens de corresponderende term uit OAIS of TRAC is aangegeven. De verhouding tussen de verschillende begrippen wordt nader verklaard in bijgevoegd relatieschema.

2.1 ARCHIEFBESCHEIDEN

Digitaal archiefstuk (DA)

Digitaal bronobject met metadata, zoals opgemaakt, ontvangen en onderhouden als bewijs van het handelen van een organisatie of persoon bij het vervullen van taken en functies. Dit is het archiefstuk, zoals het ontstaan is en gebruikt wordt in de werkprocessen van de archiefvormer. Het wordt, voor zover afkomstig van de overheid, beheerd conform de eisen uit de Archiefwet in een gecontroleerde omgeving, bijvoorbeeld een *Records Management Application* (RMA) conform NEN 2082 of *Principles and Functional Requirements for Records in Electronic Office Environments* van de ICA, die getoetst wordt door de archivaris.

OAIS-term: Information Package (IP).

Aangeboden digitaal archiefstuk (ADA)

Digitaal archiefstuk (DA), zoals de archiefvormer het aanbiedt aan het depot. Hiertoe wordt het door de zorgdrager verwijderd uit zijn "gecontroleerde omgeving" en aangeleverd aan het depot. De bijbehorende (soorten) metadata worden door de dienst, in overleg met de zorgdrager vastgesteld.

Als de informatie afkomstig is van de overheid moet die voldoen aan de eisen van de archiefwetgeving. In de praktijk wordt dit gewaarborgd door de kwaliteit van de gebruikte RMA en de organisatie daar omheen. Bij de metadata worden onder meer de (institutionele) herkomst, gerelateerde bedrijfsprocessen, technische beperkingen en openbaarheidsbeperkingen vastgelegd. De controle van de kwaliteit van de RMA valt onder de verantwoordelijkheid van de archivaris en buiten de eigenlijke toetsing van ED₃.

OAIS-term: Submission Information Package (SIP).

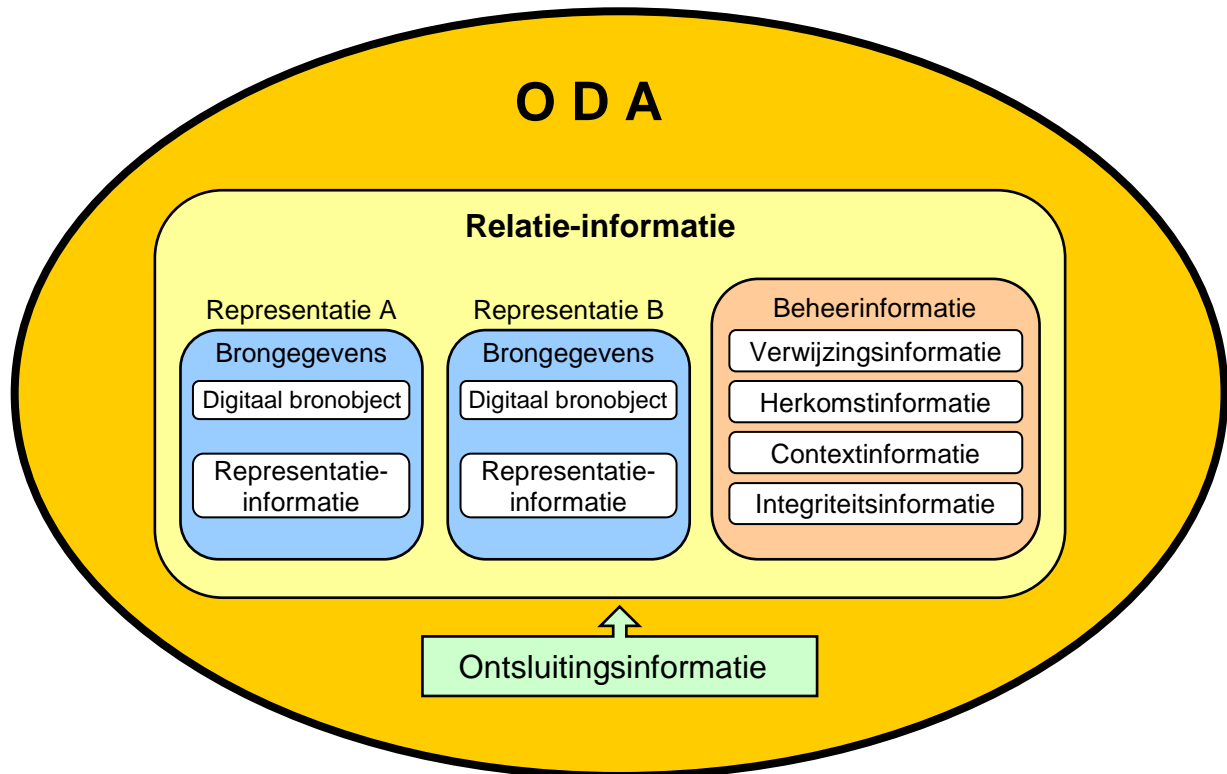
Overgedragen digitaal archiefstuk (ODA)

Aangeboden digitaal archiefstuk (ADA), zoals het in verschillende representaties in het depot wordt opgenomen en bewaard voor de lange termijn. Het archiefstuk met de bijbehorende metadata is zodanig vormgegeven en beschreven, dat het in goede, geordende en toegankelijke staat beheerd kan worden.

Bij de opname wordt gecontroleerd of het ADA voldoet aan de eisen van de archiefwetgeving. Indien dat nodig en mogelijk is, worden onvolkomenheden hersteld. Daarnaast worden formaat en metadata aangepast aan duurzame opslag en beheer. Dit kan betekenen dat samengestelde informatie in onderdelen uiteen wordt genomen, waarbij de onderlinge relatie wordt geregistreerd, maar ook dat samenhangende informatie als één geheel wordt beheerd.

De verschillende representaties worden gezamenlijk als één logische eenheid samengebonden door de relatie-informatie en ontsloten en beheerd door middel van de ontsluitingsinformatie. Zie verder het relatieschema ODA.

OAIS-term: Archival Information Package (AIP).



Afb. 4. relatieschema ODA

Beschikbaar digitaal archiefstuk (BDA)

Overgedragen digitaal archiefstuk (ODA) dat op aanvraag van gebruikers aangeboden wordt. Het bevat die metadata, die nodig zijn om de gebruikers vertrouwen te geven in de integriteit en authenticiteit van het archiefstuk én hen in staat te stellen om het te raadplegen. Vorm, structuur en metadata van het BDA hoeven niet identiek te zijn aan die van het ODA.

Het BDA bestaat feitelijk uit een authentieke kopie van het ODA, maar kan op basis van de vraagstelling ook als uittreksel of samengevoegde informatie worden aangeboden.

OAIS-term: Dissemination Information Package (DIP).

2.2 METADATA

Zie voor een relatieschema van metadata van het ODA de pagina hiervoor, afbeelding 4.

Beheerinformatie

De structurele metadata die nodig zijn voor het beheer van brongegevens. De beheerinformatie bestaat uit verwijzingsinformatie, herkomstinformatie, contextinformatie, integriteitsinformatie en de onderlinge samenhang daarvan.

Zie hiervoor ook de Regeling geordende en toegankelijke staat archiefbescheiden art. 9 lid 1.

OAIS-term: Preservation Description Information (PDI).

Contextinformatie

Metadata, die een beschrijving geven van de relaties tussen brongegevens en hun omgeving. Dit omvat naast de administratief-procedurele context ook de relatie tot andere brongegevens.

Zie hiervoor ook de Regeling geordende en toegankelijke staat archiefbescheiden art. 9 lid 1 sub d ten 1^o, 3^o en 4^o. Dit is onderdeel van de ontstaanscontext van de archiefbescheiden.

OAIS-term: Context information.

Herkomstinformatie

Metadata over de institutionele context van de brongegevens, waarin o.a. veranderingen qua inhoud, structuur en vorm en het beheersproces zijn opgenomen.

Zie hiervoor ook de Regeling geordende en toegankelijke staat archiefbescheiden art. 8 lid 1 en 9 lid 1 sub d ten 1^o, 3^o en 7^o. Dit is onderdeel van de ontstaanscontext van de archiefbescheiden.

OAIS-term: Provenance information.

Integriteitsinformatie

Metadata waarmee de fysieke integriteit van de brongegevens gecontroleerd kan worden (checksum, etc).

Zie hiervoor ook de Regeling geordende en toegankelijke staat archiefbescheiden art. 9 lid 1 sub d ten 2^o en 7^o.

OAIS-term: Fixity information.

Ontsluitingsinformatie

Inhoudelijke metadata die het opzoeken, ordenen en terugvinden van het overgedragen digitaal archiefstuk (ODA) in het depot mogelijk maken.

Deze zijn specifiek voor het depot bij de opname gegenereerd of toegekend.

OAIS-term: Descriptive information.

Relatie-informatie

Inhoudelijke metadata die brongegevens en beheerinformatie van representaties van het overgedragen digitaal archiefstuk (ODA) als één logisch geheel verbinden ten behoeve van het beheer.

Zie hiervoor ook de Regeling geordende en toegankelijke staat archiefbescheiden art. 9 lid 1.

OAIS-term: Packaging Information

Representatie-informatie

Metadata die nodig zijn om de bitstream van het digitaal 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.

Zie hiervoor ook de Regeling geordende en toegankelijke staat archiefbescheiden art. 9 lid 1 sub a, b en c en sub d ten 5°, 6° en 8°. Dit is onderdeel van de beheercontext van de archiefbescheiden.

OAIS-term: Representation information.

Verwijzingsinformatie

Metadata, die de unieke kenmerken ("identifiers") voor de brongegevens bevatten.

Zie hiervoor ook de Regeling geordende en toegankelijke staat archiefbescheiden art. 9 lid 1 sub d ten 2°, 5° en 7°. Dit is onderdeel van de beheercontext van de archiefbescheiden.

OAIS-term: Reference information.

2.3 OVERIGE TERMEN

Brongegevens

De combinatie van digitaal bronobject en representatie informatie, die bewaard moet blijven.

OAIS-term: Content information.

Depot

Het geheel van ruimten, apparatuur, programmatuur en procedures waarmee een dienst in staat is digitale informatie te beheren. Synoniem is eDepot.

OAIS-term: Repository.

Dienst

Organisatie verantwoordelijk voor en belast met het lange termijn beheer van digitale archiefbescheiden.

OAIS-term: Repository.

Digitaal bronobject

Het dataobject dat bewaard moet blijven, "de te bewaren bits en bytes".

OAIS-term: Content data object / digital object.

Escrow-regeling

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 (Van Dale, 14^e druk, 2005).

Het gaat er hierbij vooral om, dat de broncode wordt gedeponneerd. Deze kan in geval van niet-nakoming van contractuele verplichtingen of bij calamiteiten binnen de contractstermen toegankelijk worden gemaakt voor de beheerder/zorgdrager.

Open Archival Information System (OAIS)

ISO-standaard (ISO-14721:2002), waarin een conceptueel model voor een archiveringssysteem wordt beschreven. Het biedt een kader waarbinnen procedures voor de lange termijnarchivering van digitale informatie worden uitgewerkt.

TRAC-term: Archive.

3. Criteria

A Organisatie, beleid en procedures

De opzet van de dienst heeft grote invloed op de kwaliteit van het beheer. Daarom zijn in vijf onderdelen criteria geformuleerd waarop een beoordeling kan worden gebaseerd.

A 1. Continuïteit dienst

Onafhankelijk van de omvang, doelgroep of aard van de werkzaamheden moet de dienst aantonen over langere tijd te kunnen functioneren conform de doelstellingen.

■ A 1.1

De dienst heeft een vastgestelde missie en organisatiedoelen waarin de verplichting tot lange termijn beheer van digitale archiefbescheiden is opgenomen.

De dienst moet in haar missie aangeven, dat het depot wordt beheerd conform de bepalingen uit de Archiefwet.

*** A 1.2**

De dienst heeft een opvolgingsplan, continuïteitsplan en/of escrow-regelingen om de continuïteit van het depot te garanderen.

A 2. Organisatiestructuur en formatie

Er moet een vaste, omgevingsbewuste organisatie zijn die over deskundige medewerkers beschikt en die taken, verantwoordelijkheden en procedures duidelijk heeft vastgelegd.

*** A 2.1**

De dienst heeft de taken en de bijbehorende processen die hij moet uitvoeren beschreven in procedures.

Kwaliteitszorgsysteem (ISO 9001), ITIL

*** A 2.2**

De dienst beschikt over voldoende medewerkers, met voldoende kennis en competenties, om al zijn taken en diensten te kunnen uitvoeren.

Binnen de dienst dient ook voldoende aansturing en/of coördinatie van alle verantwoordelijke en/of betrokken medewerkers aanwezig te zijn.

■ A 2.3

De dienst beschikt over een actief personeelsopleidingsprogramma, waardoor medewerkers de benodigde vakbekwaamheid en expertises verder kunnen ontwikkelen.

A 3. Beleid en procedures

Er moet transparant en expliciet zijn vastgelegd wat de dienst nodig heeft, besluit, ontwikkelt en doet ten behoeve van lange termijn beheer.

A 3.1

De dienst heeft zijn gebruikersgroepen gedefinieerd en maakt openbaar hoe hij tegemoet komt aan de eisen die door de gebruikers worden gesteld aan toegankelijkheid en begrijpelijkheid van de informatie.

■ A 3.2

De dienst toetst en evalueert periodiek zijn beleid en procedures.

De dienst 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/of audits. Mogelijke hulpmiddelen zijn kwaliteitssystemen of bijvoorbeeld de in de inleiding genoemde Digital Repository Audit Method Based on Risk Assessment (DRAMBORA).

A 3.3

De dienst heeft beleid vastgesteld, waarin de juridische toestemming om digitale informatie voor de lange termijn te bewaren wordt geregeld en kan, indien nodig, aantonen dat deze toestemming is verkregen.

Dit heeft betrekking op de uitvoering van processen gericht op duurzaamheid, zoals conversie en/of migratie, waarbij de oorspronkelijke informatie mogelijk wordt aangepast. Vooral bij niet-overheidsarchieven die voor opname in het depot worden aangeboden, vaak voorzien van zogenaamde bruikleen- of schenkingsovereenkomsten, zijn mogelijk beperkende bepalingen opgenomen. Zie verder ook onder A 5.2.

A 3.4

De dienst heeft beleid en procedures vastgesteld voor het behandelen van opmerkingen of klachten van zorgdragers en gebruikers.

*** A 3.5**

De dienst 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 te bewaren informatie.

Er is een logfile van de wijzigingen beschikbaar.

A 3.6

De dienst is in staat verantwoording af te leggen over alle activiteiten ten behoeve van de werking en het beheer van het depot, met name die activiteiten die van invloed kunnen zijn op de permanente bewaring van de digitale informatie.

*** A 3.7**

De dienst heeft een ICT-strategie die aansluit bij de geformuleerde organisatiedoelen (missie).

Een ICT-strategie is een door het hoogste management gedragen document dat beschrijft op welke wijze ICT bijdraagt aan de organisatiedoelstellingen en de continuïteit van de organisatie, welke ICT-doelstellingen de komende planperiode (3- 5 jaar) worden nagestreefd, welke programma's en projecten worden opgestart en wat de kosten en risico's zijn.

*** A 3.8**

De dienst ondergaat periodiek audits of certificering.

Het gaat om externe audits, waarin minimaal strategie, beleid, procedures, processen en technische omgeving beoordeeld moeten worden op de ontvankelijkheid voor technologische ontwikkelingen en veranderende eisen.

A 4. Financiën

De dienst moet financieel in staat zijn om zijn beheerstaken te blijven uitvoeren. De hiervoor benodigde zekerheden moeten in de planning en toetsing zijn betrokken.

*** A 4.1**

De dienst doet aan bedrijfsplanning gericht op het in stand houden van het depot.

Dit houdt onder andere in dat:

- De dienst jaarlijks zijn bedrijfsplannen actualiseert.*
- De financiële systemen en procedures van de dienst transparant en conform relevante accountantsstandaarden en richtlijnen zijn ingericht en door derden worden geaudit conform de wettelijke eisen.*
- De dienst zich verplicht om permanent risico's, opbrengsten, investeringen en kosten (inclusief eigendommen, licenties en verplichtingen) te analyseren en daarover te rapporteren.*
- De dienst zich verplicht tekorten in de begroting te monitoren en aan te vullen.*

A 5. Contracten, vergunningen en/of licenties en verplichtingen

De dienst moet alle voor het beheer noodzakelijke zaken hebben vastgelegd. Daarbij moeten onder andere functies, verantwoordelijkheden, looptijden en voorwaarden duidelijk en toegankelijk beschreven worden.

A 5.1

Als de dienst digitaal materiaal beheert ten behoeve van meerdere zorgdragers, dan gebeurt dit op basis van actuele en geldige contracten of overeenkomsten.

De dienst zou een gemeenschappelijke regeling kunnen zijn.

■ **A 5.2**

Beheerovereenkomsten moeten alle benodigde rechten specificeren en overdragen aan de dienst. Deze overgedragen rechten dienen te zijn gedocumenteerd.

Zie ook onder A 3.3.

■ **A 5.3**

De dienst heeft alle relevante aspecten van opname, onderhoud, toegang en verwijdering vastgelegd in schriftelijke overeenkomsten met de zorgdrager en andere relevante partijen.

Verwijdering is zowel verplaatsing naar een ander systeem of depot als vernietiging als gevolg van verwijdering (zie B 2.5).

A 5.4

Als de dienst digitale informatie opneemt waarvan het eigendom of de rechten onduidelijk zijn, beschikt hij 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.

B Beheer van digitale archiefbescheiden

Onder het beheer vallen functies, procedures en processen die nodig zijn voor de opname, toegankelijk maken, beschikbaar stelling en lange termijn opslag van digitale bronobjecten met de bijbehorende metadata.

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

De juiste procedure voor opname van het aangeboden digitaal archiefstuk (ADA) is bepalend voor de mate waarin het verdere beheer adequaat kan worden uitgevoerd.

*** B 1.1**

De dienst beschrijft voor het aangeboden digitaal archiefstuk (ADA) welke eigenschappen bewaard zullen blijven.

Vergelijk de Regeling geordende en toegankelijk staat archiefbescheiden art. 2: De zorgdrager zorgt ervoor dat van elk van de archiefbescheiden te allen tijde kan worden vastgesteld:

- a. *de inhoud, structuur en vorm bij het ontstaan, één en ander voor zover de inhoud, structuur en vorm kenbaar moesten zijn voor de uitvoering van het betreffende werkproces.*

*** B 1.2**

De dienst legt duidelijk vast welke metadata ten tijde van de opname moeten zijn toegevoegd aan het aangeboden digitaal archiefstuk (ADA).

Vergelijk de Regeling geordende en toegankelijk staat archiefbescheiden art. 9:

1. De zorgdrager zorgt voor het vastleggen en het bewaren van tenminste de volgende gegevens:

- a. *de benaming van de toepassingsprogrammatuur waarmee de digitale archiefbescheiden zijn ontvangen en opgemaakt, inclusief het versienummer;*
- b. *de beschrijving van het platform, met naam en versie van de besturingsprogrammatuur en met naam en type van de apparatuur;*
- c. *de documentatie die aangeeft hoe de toepassingsprogrammatuur heeft gewerkt met inbegrip van de nieuwere versies;*
- d. *een beschrijving van de opgeslagen bestanden, omvattende ten minste de volgende gegevens:*
 - 1°. *de naam van het overheidsorgaan dat de digitale archiefbescheiden heeft ontvangen en opgemaakt en de benaming van het werkproces waarbinnen de digitale archiefbescheiden zijn ontvangen en opgemaakt;*
 - 2°. *de benaming en omvang van elk opgeslagen bestand;*
 - 3°. *een specificatie van de digitale archiefbescheiden met begin- en einddatum;*
 - 4°. *de relatie met andere bestanden;*
 - 5°. *het opslagformaat;*
 - 6°. *in voorkomende gevallen de toegepaste compressiemethode;*
 - 7°. *de datum en het tijdstip van de opslag van het bestand op de gegevensdrager;*

8°. *in geval van een database: de documentatie over de structuur, tenminste omvattende een compleet logisch datamodel met beschrijving van de entiteiten.*

Naast deze minimumeisen kan de NEN-ISO 23081 bij de vaststelling van metadata voor het depot worden gebruikt.

B 1.3

De dienst zorgt ervoor dat de herkomst van het aangeboden digitale archiefstuk (ADA) altijd wordt vastgesteld en gedocumenteerd.

De dienst dient er zeker van te zijn dat de opnamepakketten afkomstig zijn van de "correcte" organisatie.

*** B 1.4**

De dienst legt duidelijk vast in welke bestandsformaten een aangeboden digitaal archiefstuk (ADA) moet zijn opgemaakt en analyseert daartoe ook nieuwe ontwikkelingen.

Momenteel zijn in de Regeling geordende en toegankelijk staat de wettelijke standaarden benoemd (art. 6):

- a. voor character sets: ASCII (ISO/IEC 8859-1) of Unicode (ISO/IEC 10646-1);*
- b. voor tekstbestanden: Portable document format (PDF) of SGML dan wel XML vergezeld van een stylesheet (XSL, CSS) dan wel TIFF of PDF met de metadata in een XML-wrapper;*
- c. voor CAD/CAM bestanden; Portable document format (PDF) en STEP (Standard for the exchange of product data) als metadata standaard (ISO 10303);*
- d. voor images/beelden (bitmapped): Portable document format (PDF) en, indien gebruik gemaakt wordt van compressie: ITU T4 of ITU T6;*
- e. voor databases: het oorspronkelijke opslagformaat of ASCII (flatfile, met veldscheidingstekens), vergezeld van documentatie bij voorkeur in XML-DTD over de structuur van de database, tenminste omvattende een compleet logisch datamodel met beschrijving van de entiteiten; queries dienen in de vraagtaal SQL (SQL2) te worden vastgelegd.*

Daarnaast moet de dienst de actuele ontwikkelingen volgen om, ten gunste van het beheer, te kunnen anticiperen op basis van nieuwe informatie.

*** B 1.5**

Het opnameproces waarborgt dat ieder aangeboden digitaal archiefstuk (ADA) is gecontroleerd op veiligheid, toegankelijkheid, alsmede volledigheid en juistheid conform de eisen uit B 1.2 en B 1.4.

Het moet zeker zijn dat het ADA is wat het zegt te zijn, dat het b.v. niet door een wachtwoord wordt afgeschermd of is geïnfecteerd door een virus.

■ B 1.6

De dienst kan aantonen vanaf welk moment hij verantwoordelijk is geworden voor het bewaren van het aangeboden digitaal archiefstuk (ADA).

■ B 1.7

De dienst legt de voor bewaring relevante informatie over opnameactiviteiten en beheersprocessen (beheermetadata) vast en bewaart deze.

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

Bij de opname is het noodzakelijk dat het aangeboden digitaal archiefstuk (ADA) wordt aangepast voor lange termijn bewaring qua vorm, structuur en inhoud.

*** B 2.1**

De dienst beschikt over een identificeerbare beschrijving van ieder overgedragen digitaal archiefstuk (ODA) dat hij bewaart.

De dienst dient te beschikken over een beschrijving van de manier waarop de onderdelen van het ODA (zie afb. 4) aan elkaar zijn gekoppeld of aan elkaar zijn gerelateerd. Op basis van deze beschrijvingen moeten ODA's in het depot kunnen worden gevonden en beheerd.

■ B 2.2

De beschrijving van ieder overgedragen digitaal archiefstuk (ODA) voldoet aan de eisen die lange termijn bewaring stelt.

In de meeste gevallen wordt aan deze eis voldaan, wanneer aan B 2.1 is voldaan. In sommige gevallen kan het echter noodzakelijk zijn 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 een correcte interpretatie van de bestanden.

■ B 2.3

De dienst beschikt over een beschrijving van de manier waarop een overgedragen digitaal archiefstuk (ODA) wordt gecreëerd uit een aangeboden digitaal archiefstuk (ADA).

In sommige gevallen zullen ADA en ODA nauwelijks verschillen, afgezien van de beheersomgeving, en kan worden volstaan met die beschrijving. Het kan echter ook nodig zijn om in individuele gevallen, naast de gebruikelijke procedure, meer details te beschrijven over de opname van metadata. Van ieder ODA moet in elk geval vast te stellen zijn welke procedure is gevolgd.

■ B 2.4

De dienst controleert ieder overgedragen digitaal archiefstuk (ODA) op het moment van creatie op volledigheid en juistheid.

■ B 2.5

De dienst kan aantonen dat ieder aangeboden digitaal archiefstuk (ADA) ofwel is opgenomen als overgedragen digitaal archiefstuk (ODA) of als onderdeel van een ODA, ofwel op voorgeschreven wijze is verwijderd.

Afhankelijk van de aard van de dienst kan het ADA meteen of pas na verloop van tijd getransformeerd worden naar een ODA. De dienst moet in elk geval kunnen aantonen of en wanneer het ADA is getransformeerd.

Met verwijderen van een ADA wordt in dit geval geen vernietiging in archiefwettelijke zin bedoeld. Het gaat hier om het weigeren (vernietigen in het depot) van een ADA, bijvoorbeeld omdat het niet in overeenstemming is met de eisen uit B 1.5.

*** B 2.6**

De dienst hanteert zodanige naamgevingconventies dat zichtbare, duurzame, unieke identificatiekenmerken worden gegenereerd voor ieder overgedragen digitaal archiefstuk (ODA).

*** B 2.7**

Als er vóór de opname al unieke kenmerken zijn gerelateerd aan een aangeboden digitaal archiefstuk (ADA), dan bewaart de dienst deze zodanig, dat ze permanent gerelateerd worden aan het overgedragen digitaal archiefstuk (ODA).

Vergelijk de Regeling geordende en toegankelijke staat archiefbescheiden, art. 4: De zorgdrager zorgt ervoor dat het archiefbeheerssysteem de toegankelijke staat van archiefbescheiden waarborgt, zodanig dat:

- a. *elk van de archiefbescheiden binnen een redelijke termijn kan worden gevonden, hetzij aan de hand van een onderwerp dat in het stuk is behandeld, hetzij aan de hand van het werkproces uit hoofde waarvan het stuk is ontvangen of opgemaakt, hetzij aan de hand van de afzender, dan wel de datum en het nummer dat door de afzender aan het stuk is gegeven, hetzij aan de hand van het nummer waaronder het stuk bij het ontstaan is geregistreerd.*

■ B 2.8

De dienst beschikt voor het opnemen en registreren van de beheer informatie voor de brongegevens over een beschreven procedure en handelt conform deze procedure.

*** B 2.9**

De dienst beschikt over een beschreven procedure om de leesbaarheid en begrijpelijkheid van de digitale bronobjecten te testen en deze indien nodig naar het vooraf vastgestelde niveau van begrijpelijkheid te brengen.

Vergelijk de Regeling geordende en toegankelijke staat archiefbescheiden, art. 4: De zorgdrager zorgt ervoor dat het archiefbeheerssysteem de toegankelijke staat van archiefbescheiden waarborgt, zodanig dat:

(...)

- b *elk van de archiefbescheiden binnen een redelijke termijn leesbaar of waarneembaar te maken is.*

■ B 2.10

De dienst zorgt ervoor dat de integriteit van de inhoud van zijn depot onafhankelijk te verifiëren is.

Dit betekent dat ieder aangeboden digitaal archiefstuk (ADA) is opgenomen of verwijderd en ieder overgedragen digitaal archiefstuk (ODA) is geregistreerd.

■ B 2.11

De dienst legt bij de creatie van een overgedragen digitaal archiefstuk (ODA) relevante informatie over de uitvoering en het proces vast en bewaart die als bewijs van het doorlopen van de voor het beheer vereiste procedures.

B 3. Bewaarstrategie

De dienst moet, wil hij positief worden beoordeeld, volgens een van tevoren beschreven strategie archiefbescheiden bewaren en inspelen op veranderende inzichten en nieuwe technische mogelijkheden bij de uitvoering van deze strategie.

*** B 3.1**

De dienst documenteert zijn bewaarstrategieën.

In de bewaarstrategieën moet minstens aandacht zijn voor de achteruitgang van opslagmedia, het in onbruik raken van bestandsformaten, het waarborgen tegen (on)opzettelijke vermindering van bestanden en de aanleidingen om bewaaractiviteiten, zoals bijvoorbeeld migratie of conversie, te ondernemen.

*** B 3.2**

De dienst beschikt over mechanismen voor het toetsen en signaleren van het verouderen of onbruikbaar worden van representatie-informatie (inclusief bestandsformaten).

Dit kan betekenen dat een dienst niet in alles voldoet aan vigerende wet- en regelgeving, omdat het behoud van geordende en toegankelijke staat voorop staat. De technologische ontwikkelingen kunnen bijvoorbeeld het gebruik van een bepaald bestandsformaat noodzakelijk maken, terwijl dit op basis van de huidige Regeling geordende en toegankelijke staat archiefbescheiden nog niet mag.

■ B 3.3

De dienst is in staat om de bewaaracties aan te passen naar aanleiding van de resultaten van de toetsing en signalering uit B 3.2.

■ B 3.4

De dienst kan aantonen dat zijn bewaarstrategieën effectief zijn.

Dit zou kunnen aan de hand van een overgedragen digitaal archiefstuk uit het depot en de documentatie uit B 4.1.

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

Zaken als de toepassing van migratie, conversie, checksums, kopiëren, gescheiden opslag en de procesgeschiedenis moeten worden vastgelegd als beheermetadata, zodat de betrouwbaarheid van het depot kan worden aangetoond en gecontroleerd.

*** B 4.1**

De dienst documenteert de uitvoering van de bewaarstrategieën.

Vergelijk de Regeling geordende en toegankelijke staat archiefbescheiden, art. 5: (...)

3. De zorgdrager maakt van de conversie of de migratie een verklaring op, die ten minste een specificatie van de geconverteerde of gemigreerde digitale archiefbescheiden bevat en waarin tevens is aangegeven op welke wijze en met welk resultaat getoetst is of na de conversie of migratie aan de artikelen 2, 3 en 4 is of kan worden voldaan.

B 4.2

De dienst reageert alert op wijzigingen in strategieën voor de opslag en migratie van het overgedragen digitaal archiefstuk (ODA) en past deze toe.

*** B 4.3**

De dienst bewaart de brongegevens van het overgedragen digitaal archiefstuk (ODA).

Dit wil zeggen dat het digitale bronobject met representatie-informatie, zoals die initieel in het depot zijn opgenomen, altijd bewaard moeten blijven. Ook als er al conversies zijn uitgevoerd om de toegankelijkheid en bruikbaarheid te waarborgen.

*** B 4.4**

De dienst beschikt voor ieder overgedragen digitaal archiefstuk (ODA) over gerelateerde integriteitsinformatie en bewaart die (ook) los van het archiefstuk zelf.

■ B 4.5

De dienst legt de voor bewaring relevante informatie over activiteiten en beheersprocessen vast en bewaart deze.

B 5. Informatiemanagement

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

*** B 5.1**

De dienst stelt vast welke ontsluitingsinformatie minimaal nodig is om de beoogde gebruikersgroepen in staat te stellen specifieke informatie te vinden en te herkennen.

Vergelijk de Regeling geordende en toegankelijke staat archiefbescheiden, art. 4: De zorgdrager zorgt ervoor dat het archiefbeheerssysteem de toegankelijke staat van archiefbescheiden waarborgt, zodanig dat:

- a. elk van de archiefbescheiden binnen een redelijke termijn kan worden gevonden, hetzij aan de hand van een onderwerp dat in het stuk is behandeld, hetzij aan de hand van het werkproces uit hoofde waarvan het stuk is ontvangen of opgemaakt, hetzij aan de hand van de afzender, dan wel de datum en het nummer dat door de afzender aan het stuk is gegeven, hetzij aan de hand van het nummer waaronder het stuk bij het ontstaan is geregistreerd.*

*** B 5.2**

De dienst ontvangt of maakt een minimumset van beschrijvende metadata (ontsluitingsinformatie) en zorgt ervoor dat deze gerelateerd worden aan het overgedragen digitaal archiefstuk.

Zie ook B 5.1, hier aangevuld met metadata voor het (interne) depotbeheer. Hierbij kan de NEN-ISO 23081 worden gebruikt.

*** B 5.3**

De dienst kan aantonen dat er blijvend is gezorgd voor referentiële integriteit tussen ieder overgedragen digitaal archiefstuk (ODA) en de gerelateerde ontsluitingsinformatie.

Ieder ODA moet ontsluitingsinformatie hebben en alle ontsluitingsinformatie moet bij tenminste één ODA horen.

B 6. Toegangsbeheer

Voor het verspreiden van beschikbare digitale archiefstukken (BDA's) moeten regels zijn opgesteld, die recht doen aan de voor de beoogde gebruikersgroep gewenste openbaarheid en toegankelijkheid.

■ B 6.1

De dienst legt vast op welke manier de inhoud van het depot beschikbaar is en maakt dat bekend aan de gebruikers.

■ B 6.2

De dienst heeft procedures voor het vastleggen van toegangsacties van gebruikers, zodat voldaan wordt aan de behoeften van de dienst en de zorgdrager(s).

■ B 6.3

De dienst zorgt dat afspraken over toegangsvoorwaarden worden nagekomen.

*** B 6.4**

De dienst beschikt over toegangsbeleid (autorisatieregels, authenticatie-eisen) in overeenstemming met de eisen van de zorgdrager(s).

*** B 6.5**

Het toegangsbeleid is volledig opgenomen in het toegangbeheersysteem van het depot.

■ B 6.6

De dienst registreert toegangsfouten en afwijkende toegangsacties en beoordeelt die.

Naast gevolgen voor de ontsluiting van de overgedragen digitale archiefstukken (ODA's) kan dit ook gevolgen hebben voor de beveiliging van de toegang tot het depot.

■ B 6.7

De dienst kan aantonen dat het proces dat het beschikbaar digitaal archiefstuk (BDA) genereert correct en volledig (doorlopen) is.

■ **B 6.8**

De dienst kan aantonen dat alle toegangsverzoeken beantwoord worden met een goedkeuring of een afwijzing.

■ **B 6.9**

De dienst maakt mogelijk dat een, van één of meerdere overgedragen digitale archiefstukken (ODA's) afgeleid, beschikbaar digitaal archiefstuk (BDA) wordt verspreid onder gebruikers.

C Technologie, technische infrastructuur en beveiliging

Hierin wordt aangegeven hoe het depot in elkaar zit en technisch kan voldoen aan de eisen voor lange termijn beheer van digitale archiefbescheiden. Veel hiervan is terug te vinden in bestaande standaarden voor informatiebeveiliging, zoals de ISO 17799.

C 1. Technische infrastructuur

*** C1.1**

De dienst beschikt ten aanzien van het depot over een actuele beschrijving van de ICT-architectuur.

Voor het depot 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.

*** C 1.2**

De dienst werkt met goed ondersteunde en onderhouden besturingssoftware en infrastructuur.

De aanwezige besturingssoftware en infrastructuur moeten voldoende actueel zijn, zodat ondersteuning door leveranciers of de beheerorganisatie mogelijk is. Voor kritieke onderdelen van de infrastructuur moeten minimaal servicecontracten of service level agreements aanwezig zijn. Deze contracten moeten ook beheerd worden (service level / leveranciers management). Periodiek moet aantoonbaar onderhoud worden gepleegd op de aanwezige hard- en software. Voor alle software moeten periodiek (beveiligings)updates worden uitgevoerd op basis van een risicoafweging.

*** C 1.3**

De dienst toont aan dat de back-up functionaliteit adequaat werkt voor de overgedragen digitale archiefbescheiden (ODA's) en de beheerdata.

■ C 1.4

De dienst beheert alle van de opgenomen overgedragen digitale archiefstukken (ODA's) gemaakte identieke kopieën en hun verblijfplaats.

De dienst is verantwoordelijk voor alle exemplaren van beheerde kopieën (bijvoorbeeld dubbel uitgevoerde opslag).

■ C 1.5

De dienst beschikt over mechanismen die ervoor zorgen dat alle identieke kopieën van overgedragen digitale archiefstukken (ODA's) worden gesynchroniseerd.

Bij meerdere exemplaren moeten alle opzettelijke wijzigingen van (de metadata van) het ene exemplaar ook worden doorgevoerd aan het andere.

*** C 1.6**

De dienst heeft de geïmplementeerde maatregelen voor het garanderen van de integriteit van informatie beschreven.

*** C 1.7**

De dienst hanteert effectieve methoden om datacorruptie of dataverlies vast te stellen.

■ C 1.8

De dienst rapporteert aan het management alle gevallen van datacorruptie of – verlies en de stappen die gezet zijn om de corrupte of verloren data te herstellen of vervangen.

*** C 1.9**

De dienst beschikt over vastgestelde procedures voor de vervanging van opslagmedia en/of hardware.

Er moet kunnen worden gegarandeerd dat er, ruim vóórdát informatie onleesbaar dreigt te worden of dragers "dood" zijn, wordt ingegrepen. Dit staat los van de in B 3 beschreven bewaarstrategieën voor die informatie zelf.

■ C 1.10

De dienst hanteert een beschreven proces voor wijzigingen in hard- en software.

Een voorbeeld hiervan is het Information Technology Infrastructure Library (ITIL) proces "Change Management".

Voor het uitvoeren van wijzigingen is het belangrijk dat er vastgestelde procedures zijn en dat deze ook worden toegepast. Alle uitgevoerde wijzigingen moeten gestructureerd worden vastgelegd. De impact van een wijziging moet daarbij door een ICT-deskundige worden ingeschat en er dient door het management autorisatie te worden gegeven voor het uitvoeren van risicovolle wijzigingen.

■ C 1.11

De dienst beschikt over een procedure om de gevolgen van wijzigingen aan kritische systeemonderdelen te testen.

Voor het testen van kritische onderdelen is het belangrijk dat een gestructureerde testmethode worden gehanteerd zoals bijvoorbeeld Test Management approach (TMap). Er moet een testplan en een testomgeving (bijv. testserver) zijn waar de testen worden uitgevoerd. Vervolgens moeten de wijzigingen op een acceptatieomgeving worden geaccepteerd, alvorens ze in productie worden gezet.

■ C 1.12

De dienst beschikt over een op risicoanalyse gebaseerde procedure om te reageren op nieuwe softwarebeveiligingsupdates.

Een functionaris moet de verantwoordelijkheid hebben voor het periodiek monitoren en uitvoeren van beveiligingsupdates (bijv. iedere tweede dinsdag van de maand Microsoft updates). Beveiligingsupdates moeten worden beschouwd als "wijzigingen". Zie ook C1.10

* C 1.13

De dienst werkt met vastgestelde kwaliteitsstandaarden en processen.

Voorbeelden van veel voorkomende (kwaliteits)standaarden zijn:

- **IT Governance**
Control Objectives for Information and Related Technology (CobiT)
IT Governance raamwerk Algemene Rekenkamer
- **Beveiliging**
De Code voor Informatiebeveiliging/BS7799/ISO17799
Voorschrift informatiebeveiliging Rijksdienst (VIR)
Voorschrift informatiebeveiliging Rijksdienst-bijzondere informatie (VIR-bi)
- **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)

C 2. Adequate technologie

■ C 2.1

De dienst gebruikt, in lijn met de gekozen ICT-strategie en de ICT-architectuur, op de depotfuncties aansluitende hard- en software en stelt periodiek vast of er wijzigingen in de hard- en software nodig zijn.

Bijvoorbeeld bewezen hardware en software ('proven technology'), het volgen van markstandaarden, open source, voldoende opslagcapaciteit voor het eDepot, etc.

C 3. Beveiliging

* C 3.1

De dienst doet aan een systematische risicoanalyse voor factoren als data, systemen, personeel, fysieke locatie en beveiligingseisen.

Er is een informatiebeveiligingsplan conform de NEN-ISO/IEC 17799.

■ **C 3.2**

De dienst heeft voor iedere vastgestelde beveiligingseis adequate maatregelen getroffen.

Conform de NEN-ISO/IEC 17799.

■ **C 3.3**

Medewerkers hebben ten aanzien van wijzigingen in het systeem afgebakende rollen, verantwoordelijkheden en autorisaties.

* **C 3.4**

De dienst beschikt over passende calamiteiten- en herstelplannen, bestaande uit minstens een back-up van alle opgeslagen informatie en een kopie van het herstelplan op een andere locatie.

4. Concordans TRAD – ED₃ – TRAC

TRAC	ED ₃
A	A
A 1	A 1
A 1.1	A 1.1
A 1.2	A 1.2
A 2	A 2
A 2.1	A 2.1
A 2.2	A 2.2
A 2.3	A 2.3
A 3	A 3
A 3.1	A 3.1
A 3.2	A 3.2
A 3.3	A 3.3
A 3.4	Vervallen vanwege overlap met A 3.8.
A 3.5	A 3.4
A 3.6	A 3.5
A 3.7	A 3.6
A 3.8	C 1.6
A 3.9	A 3.8
A 4	A 4
A 4.1	A 4.1
A 4.2	Vervallen, opgenomen als toelichting bij A 4.1.
A 4.3	Vervallen, opgenomen als toelichting bij A 4.1.
A 4.4	Vervallen, opgenomen als toelichting bij A 4.1.
A 4.5	Vervallen, opgenomen als toelichting bij A 4.1.
A 5	A 5
A 5.1	A 5.1
A 5.2	A 5.2
A 5.3	A 5.3
A 5.4	Vervallen, geen taak van de dienst.
A 5.5	A 5.4
B	B
B 1	B 1
B 1.1	B 1.1
B 1.2	B 1.2
B 1.3	B 1.3
B 1.4	B 1.5
B 1.5	Vervallen, omdat onduidelijk is wat "voldoende controle" inhoudt.
B 1.6	Vervallen, geen relevante eis.
B 1.7	B 1.6
B 1.8	B 1.7
B 2	B 2
B 2.1	B 2.1
B 2.2	B 2.2
B 2.3	B 2.3

TRAC	ED₃
B 2.4	B 2.5
B 2.5	B 2.6
B 2.6	B 2.7
B 2.7	Vervallen, zeer onduidelijk geformuleerde eis.
B 2.8	Vervallen.
B 2.9	B 2.8
B 2.10	B 2.9
B 2.11	B 2.4
B 2.12	B 2.10
B 2.13	B 2.11
B 3	B 3
B 3.1	B 3.1
B 3.2	B 3.2
B 3.3	B 3.3
B 3.4	B 3.4
B 4	B 4
B 4.1	B 4.1
B 4.2	B 4.2
B 4.3	B 4.3
B 4.4	B 4.4
B 4.5	B 4.5
B 5	B 5
B 5.1	B 5.1
B 5.2	B 5.2
B 5.3	B 5.3
B 5.4	Vervallen, samengevoegd met B 5.3.
B 6	B 6
B 6.1	B 6.1
B 6.2	B 6.2
B 6.3	B 6.3
B 6.4	B 6.4
B 6.5	B 6.5
B 6.6	B 6.6
B 6.7	B 6.7
B 6.8	Vervallen, samengevoegd met B 6.7.
B 6.9	B 6.8
B 6.10	B 6.9
C	C
C 1	C 1
C 1.1	C 1.2
C 1.2	C 1.3
C 1.3	C 1.4
C 1.4	C 1.5
C 1.5	C 1.7
C 1.6	C 1.8
C 1.7	C 1.9
C 1.8	C 1.10
C 1.9	C 1.11

TRAC	ED₃
C 1.10	C 1.12
C 2	C 2
C 2.1	C 2.1
C 2.2	Vervallen, samengevoegd met C 2.1.
C 3	C 3
C 3.1	C 3.1
C 3.2	C 3.2
C 3.3	C 3.3
C 3.4	C 3.4

ED₃	TRAC	ED₃	TRAC	ED₃	TRAC
A	A	B 1.6	B 1.7	B 6.2	B 6.2
A 1	A 1	B 1.7	B 1.8	B 6.3	B 6.3
A 1.1	A 1.1	B 2	B 2	B 6.4	B 6.4
A 1.2	A 1.2	B 2.1	B 2.1	B 6.5	B 6.5
A 2	A 2	B 2.2	B 2.2	B 6.6	B 6.6
A 2.1	A 2.1	B 2.3	B 2.3	B 6.7	B 6.7
A 2.2	A 2.2	B 2.4	B 2.11	B 6.8	B 6.9
A 2.3	A 2.3	B 2.5	B 2.4	B 6.9	B 6.10
A 3	A 3	B 2.6	B 2.5	C	C
A 3.1	A 3.1	B 2.7	B 2.6	C 1	C 1
A 3.2	A 3.2	B 2.8	B 2.9	C 1.1	-
A 3.3	A 3.3	B 2.9	B 2.10	C 1.2	C 1.1
A 3.4	A 3.5	B 2.10	B 2.12	C 1.3	C 1.2
A 3.5	A 3.6	B 2.11	B 2.13	C 1.4	C 1.3
A 3.6	A 3.7	B 3	B 3	C 1.5	C 1.4
A 3.7	-	B 3.1	B 3.1	C 1.6	A 3.8
A 3.8	A 3.9	B 3.2	B 3.2	C 1.7	C 1.5
A 4	A 4	B 3.3	B 3.3	C 1.8	C 1.6
A 4.1	A 4.1	B 3.4	B 3.4	C 1.9	C 1.7
A 5	A 5	B 4	B 4	C 1.10	C 1.8
A 5.1	A 5.1	B 4.1	B 4.1	C 1.11	C 1.9
A 5.2	A 5.2	B 4.2	B 4.2	C 1.12	C 1.10
A 5.3	A 5.3	B 4.3	B 4.3	C 1.13	-
A 5.4	A 5.5	B 4.4	B 4.4	C 2	C 2
B	B	B 4.5	B 4.5	C 2.1	C 2.1
B 1	B 1	B 5	B 5	C 3	C 3
B 1.1	B 1.1	B 5.1	B 5.1	C 3.1	C 3.1
B 1.2	B 1.2	B 5.2	B 5.2	C 3.2	C 3.2
B 1.3	B 1.3	B 5.3	B 5.3	C 3.3	C 3.3
B 1.4	-	B 6	B 6	C 3.4	C 3.4
B 1.5	B 1.4	B 6.1	B 6.1		