Referentiekader Opbouw Digitaal Informatiebeheer

RODIN

Landelijk overleg van provinciale archiefinspecteurs
Werkverband gemeentelijke archiefinspectie

Referentiekader Opbouw Digitaal Informatiebeheer RODIN

RODIN is tot stand gekomen in samenwerking met: Het Expertise Centrum | Consultants voor ICT en bestuur in de publieke sector.

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 van toepassing.

Inleiding

1.1 Digitale overheidsinformatie moet ook beheerd worden

De meeste overheidsinstellingen besteden veel tijd aan het managen van de papieren poststroom en de papieren dossiers, terwijl deze steeds minder geraadpleegd worden.
Tegelijkertijd worden digitale documenten steeds belangrijker als medium voor het vastleggen van bedrijfskritische informatie. Het ontbreekt echter veelal aan waarborgen voor de betrouwbaarheid, volledigheid, authenticiteit en duurzame toegankelijkheid van digitale overheidsinformatie. Cruciale informatie zit verstopt in persoonlijke mailboxen, netwerkschijven, vakapplicaties en is niet beschikbaar en bruikbaar als bewijsmateriaal bij geschillen, voor WOB-aanvragen van burgers of als bron voor verantwoording bij audits, enquêtes en onderzoeken.[1]
Gelukkig zien steeds meer overheidsorganisaties dit in. Zij zijn volop bezig met het invoeren van systemen voor digitaal werken en archiveren, om digitale informatie te structureren, duurzaam te bewaren en organisatiebreed toegankelijk te maken. Zij worden daarbij geconfronteerd met een veelheid aan wet- en regelgeving, normen en standaarden. Zeker kleinere organisaties zien vaak door de bomen het bos niet meer. RODIN biedt een rode draad door dit bos.

1.2 Doel van het referentiekader

Het hier gepresenteerde referentiekader is nadrukkelijk niet bedoeld als weer een nieuwe set met eisen, maar als een handzame, begrijpelijke samenvatting van alle relevante wet- en regelgeving, normen en standaards. En dat onder het motto: denk na voor je begint. Het biedt een handvat voor inrichting, gebruik en beoordeling van een (in ontwikkeling zijnde) digitale beheeromgeving, waarin digitale archieven duurzaam en toegankelijk worden beheerd. Het kan worden gebruikt door informatiemanagers, adviseurs DIV en interne auditors in overheidsorganisaties die onder de Archiefwet vallen, maar ook door archiefinspecteurs en externe auditors. Ook niet-overheidsorganisaties, die hun digitale informatie duurzaam toegankelijk willen beheren, kunnen er gebruik van maken. RODIN kan gebruikt worden als checklist en daarmee dienen als instrument voor good governance (adequate sturing, beheersing, verantwoording en toezicht) en inzicht geven in de mate waarin de organisatie op dit gebied ‘in control’ is.

[1] Zie onder andere het recente rapport van de Algemene Rekenkamer: Informatiehuishouding van het Rijk, februari 2010

1.3 Toepassingsgebied

Het referentiekader heeft betrekking op de gehele digitale beheeromgeving, oftewel:

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

De digitale beheeromgeving is een systeem in organisatiekundige zin, en omvat naast hardware, software, en bestanden, ook beleid, degelijke organisatie, goed opgeleid en voldoende personeel, vastgelegde procedures en financiële soliditeit. De eisen van RODIN kunnen dan ook onderdeel uitmaken van een kwaliteitssysteem of van kwaliteitsmanagement. Het is niet alleen toepasbaar op documentbeheer in Document Management Systemen/Record Management Applicaties, maar ook op beheer van informatie en documenten in alle procesgebonden (vak)applicaties, Enterprise Content Managementsystemen, of een samenspel van deze typen applicaties. RODIN is niet bedoeld als referentiekader voor digitale depots (Trusted Digital Repositories), bestemd voor blijvende bewaring van digitale archiefbescheiden. Hiervoor gelden zwaardere eisen, geformuleerd in het referentiemodel voor digitale depots OAIS (ISO-14721: 2002) en de daarvan afgeleide checklists TRAC en ED3[2].

1.4 Opzet van RODIN

Het referentiekader is gebaseerd op de Archiefwet 1995, de Archiefregeling, de normenfamilie voor archief- en informatiebeheer NEN-ISO 15489, NEN 2082 en ISO 23081, de Informatiebeveiligingsnorm NEN-ISO/IEC 27002, en delen van het referentiemodel voor digitale depots OAIS (ISO-14721: 2002) en de daarvan afgeleide checklists TRAC en ED3 (zie voor een volledige lijst paragraaf 1.7). Deze worden als bron vermeld bij de betreffende eisen in het referentiekader. Voor een meer gedetailleerde uitwerking van de eisen is het raadzaam om de oorspronkelijke bron te raadplegen.

De eisen zijn ingedeeld in de volgende hoofdstukken:

1 Beleid en organisatie;

2 Informatiebeheer;

3 ICT-beheer en -beveiliging.

In de praktijk zullen voor deze drie onderwerpen vaak drie verschillende organisatie-onderdelen verantwoordelijk zijn.

1.5 Verantwoording

RODIN is samengesteld door een werkgroep, bestaande uit vertegenwoordigers van het Landelijk Overleg van Provinciale Archiefinspecteurs (LOPAI), Werkverband Gemeentelijke Archiefinspectie (WGA) en Het Expertise Centrum (HEC):

Jan Beens (WGA)
Dick Bunskoeke (LOPAI)
Lolke Folkertsma (LOPAI)
Chido Houbraken (LOPAI)
Ingmar Koch (LOPAI)
Marianne Loef (LOPAI)
Bernard Mantel (WGA)
Jeroen van Oss (WGA)
Hajo de Roo (WGA)
Maarten de Roos (HEC)
Arjan de Vries (LOPAI)
Chris Wauters (HEC)

[2] ED3, Eisen Duurzaam digitaal depot, toetsingskader voor de beheersomgeving van blijvend te bewaren digitale informatie, LOPAI 2008, www.lopai.nl

1.6 Definities

Aggregatieniveau Niveau binnen de ordeningsstructuur, bijvoorbeeld: het individuele stuk, het dossier of de zaak, het zaaktype of het onderwerp.
Archiefbestanddeel Geheel van archiefstukken met onderlinge samenhang, zoals een dossier, een rubriek, een serie, een zaak, een zaaktype.
Archiefstukken Documenten die door een organisatie in het kader van haar werkprocessen worden opgemaakt en ontvangen; archiefbescheiden in de zin van de Archiefwet 1995.
Classificatieschema of ordeningsstructuur logisch plan waarmee archiefstukken of archiefbestanddelen systematisch worden geordend, nauw aansluitend aan de werkprocessen.
Systeem (met name in Hoofdstuk 2: Informatiebeheer)
Het geheel van apparatuur en besturings- en toepassings-programmatuur.

1.7 Bronnen

Hier is de volledige titel weergegeven met tussen haakjes de weergave in de checklist.

Wettelijke regelingen

- Archiefwet 1995 (AW)
- Archiefregeling (AR)

Normen

- ISO-14721:2003 - Reference Model for an Open Archival Information System (OAIS)
- NEN 2082 – Eisen voor functionaliteit van informatie- en archiefmanagement in programmatuur (2082)
- NEN 3434:2007 - Applicatiemanagement - Eisen aan applicatiemanagement (3434)
- NEN-ISO 15489-1:2001 – Informatie- en archiefmanagement – Deel 1 (15489)
- NEN-ISO/IEC 27002:2007 - Informatietechnologie - Beveiligingstechnieken - Code voor informatiebeveiliging (NEN-ISO/IEC 27002)

Referentiekaders

- Business Information Services Library (BiSL)
- ED3 Eisen duurzaam digitaal depot. Toetsingskader voor de beheersomgeving van blijvend te bewaren digitale informatie, LOPAI 2008 (ED3)
- Information Technology Infrastructure Library (ITIL)
- TRAC: OCLC and CRL, Trustworthy Repositories Audit & Certification: Criteria and Checklist Version 1.0 February 2007 (TRAC)

RODIN Referentiekader

		ja	nee	deels	opmerkingen	afgeleid van
1	**Beleid en organisatie**					
1.1	De organisatie heeft een door het bestuur en/of management vastgesteld informatiebeleid dat aansluit bij de geformuleerde organisatiedoelstellingen. Onderdelen van informatiebeleid zijn tenminste:	○	○	○		AR: 19; 15489: 5, 6.1, 6.2, 7.1
	a het voldoen aan de wettelijke eisen voor het bewaren van informatie;	○	○	○		
	b een beschrijving van de relatie tussen de bedrijfsprocessen en de opgenomen informatie;	○	○	○		
	c een beschrijving van of verwijzing naar de bewaarstrategie van de organisatie die rekening houdt met conversie, migratie of emulatie in geval van veranderende (technische) omstandigheden;	○	○	○		ED3: A3.7, B3.1
	d een beschrijving van het beveiligingsbeleid waarin taken en verantwoordelijkheden voor informatiebeveiliging zijn belegd.	○	○	○		NEN-ISO/IEC 27002
1.2	De organisatie is in staat verantwoording af te leggen over alle activiteiten ten behoeve van de werking en het beheer van de digitale beheeromgeving op basis van toetsbare eisen van een door haar toe te passen kwaliteitssysteem.	○	○	○		AR: 16 ED3: A3.6
1.3	De organisatie heeft de processen en procedures voor de digitale beheeromgeving beschreven.	○	○	○		ED3: A2.1
1.4	De organisatie ondergaat periodiek (externe) audits en/of certificering op het gebied van de digitale beheeromgeving.	○	○	○		15489: 10 ED3: A3.8

		ja	*nee*	*deels*	*opmerkingen*	*afgeleid van*
1.5	De taken, verantwoordelijkheden en bevoegdheden voor de digitale beheeromgeving waaronder: digitalisering, duurzame toegankelijkheid, archiefbeheer en betrouwbaarheid van informatie zijn vastgelegd en belegd. Tevens is op basis hiervan de continuïteit gewaarborgd in het geval van organisatiewijziging.	○	○	○		AW: 4; 15489: 6.3; Baseline IR: Norm 2
1.6	De digitale beheeromgeving is opgenomen in de meerjarenbegroting van de organisatie, waarbij voldoende middelen beschikbaar worden gesteld om de continuïteit ervan te waarborgen.	○	○	○		AW: 3 memorie van toelichting; ED3: A4.1
1.7	De organisatie beschikt over voldoende medewerkers, met voldoende kennis en competenties, om al haar taken en verantwoordelijkheden op het gebied van de digitale beheeromgeving te kunnen uitvoeren.	○	○	○		AW: 3 memorie van toelichting; 15489: 6.3, 11; ED3: A2.2
2	**Informatiebeheer**					
2.1	Alle digitale archiefstukken worden geklasseerd op basis van een classificatieschema/ordeningsstructuur.	○	○	○		2082: 25, 26; 15489: 9.3, 9.5
2.2	Het systeem kent automatisch een uniek identificatiekenmerk toe aan alle onderdelen die op basis van het classificatieschema/de ordeningsstructuur worden vastgelegd, bijvoorbeeld aan zaaktypen/processen, zaken en digitale archiefstukken.	○	○	○		2082: 2
2.3	Het systeem kan in het classificatieschema veranderingen aanbrengen en bij deze wijzigingen moet de consistentie binnen het schema alsmede tussen het schema en de archiefbestanddelen gewaarborgd blijven.	○	○	○		2082: 140, 141

		ja	nee	deels	opmerkingen	afgeleid van
2.4	Van alle archiefstukken wordt tenminste de volgende informatie in de metadata vastgelegd:	○	○	○		AR: 17, 21, 24, 26.2
	a Inhoud, structuur, verschijningsvorm en gedrag;	○	○	○		
	b Wanneer, door wie en waarom de archiefstukken zijn opgemaakt en werden ontvangen;	○	○	○		
	c Samenhang met andere beheerde archiefstukken;	○	○	○		2082: 4, 82, 121
	d Uitgevoerde beheeractiviteiten;	○	○	○		
	e Actuele en oorspronkelijke technische aard, ook van de hard- en softwareomgeving;	○	○	○		
	f Aard van de digitale handtekening (indien aanwezig);	○	○	○		
	g Wijze van versleuteling (algoritme) en decryptiesleutel (indien van toepassing).	○	○	○		
2.5	Metadata worden op gestandaardiseerde wijze toegekend, bijvoorbeeld met behulp van standaard woordenlijsten.	○	○	○		AR: 24; 23081
2.6	Het systeem gebruikt een door het bestuur en/of management vastgesteld autorisatieschema waarmee alle gebruikerstaken en beheeractiviteiten als rollen aan medewerkers worden toegekend.	○	○	○		2082: 99
2.7	Digitale archiefstukken worden opgeslagen in door het bestuur aangewezen, valideerbare en volledig gedocumenteerde bestandsformaten, die voldoen aan een open standaard, tenzij dit redelijkerwijs niet kan worden verlangd.	○	○	○		AR: 26.1; 2082: 20
2.8	De koppeling tussen een digitaal archiefbestanddeel (op elk aggregatieniveau) en de daarbij behorende metadata moet tot het moment van verwijdering kunnen worden gereconstrueerd.	○	○	○		AR: 24; 2082: 22
2.9	Het systeem importeert, converteert, migreert en exporteert digitale archiefstukken en de bijbehorende metadata uitsluitend met behoud van de authenticiteit, betrouwbaarheid, integriteit en bruikbaarheid op elk aggregatieniveau.	○	○	○		2082: 36

		ja	*nee*	*deels*	*opmerkingen*	*afgeleid van*
2.10	De integriteit en leesbaarheid van digitale archiefstukken kan worden vastgesteld, gecontroleerd, gedocumenteerd en geborgd tegen ongeautoriseerde wijzigingen en beschadigingen.	○	○	○		2082: 9, 12, 32 AR: 26.3
2.11	Door middel van een zoekopdracht kunnen alle digitale archief-stukken en hun metadata op elk aggregatieniveau worden getoond, met inachtneming van autorisaties.	○	○	○		2082: 42, 46
2.12	De bewaartermijn van digitale archiefbescheiden wordt automatisch op elk aggregatieniveau vastgelegd. De bewaartermijnen worden nageleefd met inachtneming van de wettelijke selectietermijnen, -procedures en vervolgacties (vernietigen, overdragen of exporteren).	○	○	○		15489: 6.8, 9.2 2082: 62, 65, 69
2.13	Ter waarborging van de samenhang en volledigheid wordt een waarschuwing gegeven wanneer er een link of verwijzing bestaat tussen verschillende digitale archiefbestanddelen op alle aggregatieniveaus, waarvan een onderdeel op het punt staat te worden vernietigd, overgedragen of geëxporteerd en het andere niet.	○	○	○		2082: 76
2.14	Vernietigen van archiefstukken moet zo gebeuren dat deze op geen enkele wijze kunnen worden gereproduceerd.	○	○	○		2082: 80
3	**ICT-BEHEER EN -BEVEILIGING**					
3.1	De organisatie doet aan een systematische risicoanalyse voor factoren als data, systemen, personeel, fysieke locatie en beveiligingseisen.	○	○	○		ED3: C3.1
3.2	De organisatie hanteert een beveiligingsplan m.b.t. informatiebeveiliging gebaseerd op de Code voor Informatiebeveiliging of vergelijkbare richtlijn.	○	○	○		NEN-ISO/IEC 27002

		ja	*nee*	*deels*	*opmerkingen*	*afgeleid van*
3.3	De organisatie heeft een overzicht van de gehanteerde beveiligingsmaatregelen en laat periodiek (extern) toetsen of de mate van beveiliging nog passend is.	○	○	○		
3.4	De organisatie beschikt over een passende back-upstrategie, calamiteiten- en herstelplan.	○	○	○	Zie bijvoorbeeld calamiteitenbeheer ITIL (versie 2)	ED3: C3.4
3.5	De organisatie maakt periodiek back-ups van alle opgeslagen informatie en bewaart deze informatie in een kluis op een andere locatie.	○	○	○	Zie bijvoorbeeld calamiteitenbeheer ITIL (versie 2)	
3.6	Back-ups en herstelplannen worden periodiek gecontroleerd op juiste werking.	○	○	○		AR: 16; ED3: C 1.3
3.7	De organisatie heeft de taken en verantwoordelijkheden voor functioneel beheer, applicatiebeheer en technisch beheer belegd en ingericht voor de digitale beheeromgeving op basis van gangbare beheerstandaarden.	○	○	○	Zoals bijvoorbeeld beheerstandaarden ITIL, ASL (NEN 3434) en BiSL	
3.8	De organisatie stelt in een Service Level Agreement (SLA) eisen aan de interne of externe ICT-dienstverlener ten aanzien van beveiliging en beheerprestaties.	○	○	○		
3.9	De organisatie heeft een adequate serverruimte met onder meer klimaatbeheersing, alarm en brandmeldvoorziening, toegangs-controle, ordelijke bekabeling en noodstroomvoorziening (UPS).	○	○	○		Handboek ICT, Huisvesting en Bekabeling, deel 1, hoofdstuk 5[3]

[3] http://www.rgd.nl/fileadmin/redactie/Actueel/Publicaties/HIB/HIB versie 1.0 deel 1 01.pdf

juni 2010

LOPAI Landelijk overleg van provinciale archiefinspecteurs
WGA Werkverband gemeentelijke archiefinspectie

Ontwerp en lay-out
R1 grafische vormgeving, Nijmegen

Druk
Drukkerij Trioprint Nijmegen bv, Nijmegen