2017

Referentiekader
opbouw digitaal informatiebeheer

RODIN
versie 2

Inhoudsopgave

Inleiding

WAT IS RODIN?

Het Referentiekader Opbouw Digitaal Informatiebeheer, kortweg RODIN, is een handzaam toetsingsinstrument. Het kan gebruikt worden voor het bepalen van, sturen op en verantwoording afleggen over de kwaliteit van de beheeromgeving waarin digitale informatie bij organisaties ontstaat of wordt ontvangen. Het is gebaseerd op de belangrijkste wet- en regelgeving, normen en standaarden op het gebied van duurzaam informatiebeheer. RODIN biedt houvast bij de inrichting, het gebruik en de beoordeling van een bestaande of zich nog ontwikkelende beheeromgeving waarin digitale informatie conform wettelijke eisen gecontroleerd en duurzaam beheerd moet worden zodat de betrouwbaarheid en toegankelijkheid daarvan gegarandeerd is. Toepassing van het referentiekader geeft inzicht in de mate waarin de organisatie op het gebied van digitaal informatiebeheer 'in control' is. RODIN kan gebruikt worden als onderdeel van het in de Archiefregeling vereiste kwaliteitssysteem voor de (digitale) archivering en van andere vormen van kwaliteitsmanagement.

De eerste versie van RODIN verscheen in 2010. Het instrument is sindsdien veelvuldig en naar tevredenheid gebruikt. De (inter)nationale wet- en regelgeving, standaarden en normen op dit terrein zijn sinds 2010 in volop in ontwikkeling gebleven en sterk toegenomen. Daardoor is het voor informatieprofessionals en toezichthouders moeilijk om door al die bomen het bos nog te zien. Bovendien is de digitalisering van informatiestromen in de hele maatschappij, dus ook bij de overheid, in de afgelopen jaren in hoog tempo doorgegaan. In veel organisaties is een groot deel van de bedrijfskritische informatie alleen nog in digitale vorm beschikbaar. Het wordt daarom met de dag belangrijker om te kunnen waarborgen dat digitale informatie betrouwbaar, volledig, authentiek en toegankelijk is en blijft zolang dat nodig is. Gelukkig zijn ook steeds meer organisaties zich bewust van het belang van duurzaam informatiebeheer. De behoefte aan een goed toetsingsinstrument is dan ook alleen maar toegenomen. Daarom is het hoog tijd voor deze geactualiseerde en verbeterde versie van het beproefde toetsingsinstrument: RODIN 2.0.
RODIN 2.0 is een generiek instrument, Daarom bevat het geen eisen voor de aansluiting op een e-depot, aangezien deze niet voor ieder e-depot hetzelfde hoeven te zijn. Wel kan toepassing van RODIN 2.0 veel informatie opleveren die van belang is bij het voorbereiden van organisaties en hun digitale informatiebeheer op de aansluiting op een e-depot.

VOOR WIE EN WAARVOOR IS RODIN?

RODIN 2.0 is bedoeld voor informatiemanagers, adviseurs DIV en informatiebeheer, interne auditors, archiefinspecteurs en externe auditors bij organisaties die onder de Archiefwet vallen. Ook niet-overheids-organisaties die hun digitale informatie gecontroleerd en langdurig toegankelijk willen beheren, kunnen er desgewenst gebruik van maken.
RODIN kan eveneens goede diensten bewijzen in het geval van privaat-publieke samenwerking, in samen-werkingsverbanden tussen overheden onderling en keteninformatisering. Het is dan wel nodig dat de betrokken partijen vooraf afspraken hebben vastgelegd over zaken als metadata, formaten, beschikbaarstelling, selectie en waardering. Zie hiervoor ook de Handreiking Inrichting informatie- en archiefbeheer bij samenwer-kingsverbanden (Verbonden Partijen) van LOPAI en KVAN/BRAIN uit januari 2017.
RODIN is toepasbaar op informatiebeheer in op een gehele architectuur centrale archiefsystemen, alsook op beheer van zowel te bewaren als op termijn vernietig-bare informatie in (vak)applicaties, decentrale systemen op afdelingen. Artikel 3 van de Archiefwet 1995 bepaalt immers dat overheidsorganisaties verplicht zijn de onder hen berustende archiefbescheiden in goede, geordende en toegankelijke staat te brengen en te bewaren. Voor digitale informatie die langer bewaard moet worden dan een periode van circa 6 jaar, zal het nodig zijn om maat-regelen te treffen om ervoor te zorgen dat deze infor-matie tot aan het eind van de bewaartermijn toeganke-lijk en betrouwbaar blijft. Met behulp van RODIN kan de beheeromgeving waarin de digitale informatie ontstaat of wordt ontvangen, worden getoetst, verbeterd en doorontwikkeld.
Het referentiekader heeft betrekking op de gehele digitale beheeromgeving:

> Het geheel van organisatie, beleid, processen en procedures, financieel beheer, personeel, databeheer,databeveiligingen aanwezige hard- en software, dat het duurzame beheer van digitale informatie mogelijk maakt.

De digitale beheeromgeving omvat dus meer dan de hardware, software en bestanden. Ook alle randvoor-waardelijke voorzieningen, zoals afgewogen beleid, een degelijke organisatie, goed opgeleid en voldoende personeel, vastgelegde en gecontroleerde procedures en financiële soliditeit maken onlosmakelijk deel uit van de beheeromgeving en kunnen met behulp van RODIN worden getoetst en bijgestuurd. Daarom kan RODIN ook onderdeel uitmaken van een breder kwaliteitssysteem en van integraal kwaliteitsmanagement.
RODIN is niet bedoeld als referentiekader voor e-depots, bestemd voor blijvende bewaring van digitale informatie. Hiervoor gelden zwaardere eisen, zoals beschreven in de ISO-norm 16363. Ook is RODIN niet bedoeld als toetsings-kader voor een geïntegreerde oplossing van digitale beheeromgeving en een e-depotvoorziening.

HOE WERKT RODIN?

RODIN benoemt eisen voor alle aspecten van de digitale beheeromgeving. Met elkaar vormen deze 19 eisen de belangrijkste voorwaarden voor verantwoord digitaal informatiebeheer in eerste aanleg.
Een korte toelichtende tekst per eis geeft houvast voor de toepassing ervan. Waar mogelijk zijn de eisen verder verduidelijkt door middel van voorbeelden. Per eis zijn verwijzingen opgenomen naar de bron of bronnen waaruit deze afkomstig zijn en naar de corresponderende eis in RODIN 1.0. Voor een meer gedetailleerde uitwerking van de eisen is het raadzaam om de oorspronkelijke bron te raadplegen. Bijlage 1 bevat de volledige lijst van in RODIN verwerkte kaders. Bijlage 2 bevat een begrippenlijst.
In sommige eisen worden termen als 'voldoende' en 'passend' gebruikt. Het is van belang dat auditor en de organisatie die onderwerp van toetsing is voorafgaand aan de audit in samenspraak bepalen wanneer er voldoende of passend is voldaan aan de eis.
De eisen zijn ingedeeld in de volgende hoofdstukken:

1. Beleid en organisatie (4 eisen)
2. Inhoudelijk informatiebeheer (7 eisen)
3. ICT-beheer (8 eisen)

Deze drie hoofdstukken corresponderen vaak met verschillende onderdelen van de organisatie en sluiten meestal aan op verschillende niveaus: hoofdstuk 1 op het management, hoofdstuk 2 op het informatiebeheer en de informatievoorziening, hoofdstuk 3 op ICT-beheer en beveiliging. Deze onderdelen en/of niveaus kunnen zodoende aan de hand van RODIN apart worden bevraagd. De optelsom van de uitkomsten van de drie sets eisen leidt tot het gewenste organisatiebrede inzicht. De ervaring leert dat deze aanpak in de praktijk goed werkt.

VERANTWOORDING

RODIN 2.0 is samengesteld door een werkgroep bestaande uit vertegenwoordigers van het Landelijk Overleg Provinciale Archiefinspecteurs (LOPAI), het samenwerkingsverband van de Koninklijke Vereniging van Archivarissen in Nederland en de Brancheorganisatie Archiefinstellingen in Nederland en (KVAN/BRAIN) en de Erfgoedinspectie (EGI), sectie Archieven:
Jan Beens (KVAN/BRAIN)
Dick Bunskoeke (LOPAI)
Stinie Francke (KVAN/BRAIN)
Chantal Menting (KVAN/BRAIN)
Marianne Loef (LOPAI)
Ronald van der Steen (EGI)

Hoofdstuk 1

Beleid en Organisatie

NR.	EIS	TOELICHTING	VOORBEELDEN	VERWIJZINGEN
1.1	**De organisatie heeft een door het bestuur en/of management vastgesteld informatiebeleid.**	Het vastgestelde informatiebeleid kan uit één document of meerdere documenten bestaan. Onderdelen van het informatiebeleid zijn tenminste: a beschrijving van de manier waarop de organisatie zorgt dat zij voldoet aan de wettelijke eisen voor het bewaren van informatie; b beschrijving van de bewaarstrategie (waaronder preserveringsmaatregelen); c beschrijving van het beveiligingsbeleid, waarin taken en verantwoordelijkheden voor informatiebeveiliging zijn belegd. Zie ook hoofdstuk 3.	Ad a: Een informatiebeleidsplan of ander plan waarin (onder meer) beschreven staat hoe men voldoet aan de Archiefwet en aanverwante regelgeving. Ad b: Voorbeelden bewaarstrategie: het vervroegd overbrengen of uitplaatsen naar een extern e-depot; het creëren van een interne omgeving voor duurzame en permanente bewaring. Voorbeelden preserveringsmaatregelen: het monitoren op in onbruik raken van formaten, tijdig migreren en/of converteren van bestanden, emulatie. Ad c: Voor gemeenten conform de BIG, voor waterschappen de BIWA, voor provincies de IBI en voor het Rijk de BIR.	**Rodin 2010** 1.1 **Wetgeving** AR 25 **NEN-ISO 15489** 6.2 **ISO 16363** 3.1.1, 3.1.2, 3.3.2 en 5 **KIDO 1.0** Hoofdstuk 3

NR.	EIS	TOELICHTING	VOORBEELDEN	VERWIJZINGEN
1.2	**Voor de continuïteit van de digitale beheeromgeving zijn structureel voldoende middelen beschikbaar gesteld.**	Besturen van organisaties die onder de Archiefwet vallen, zijn zorgplichtig. Dat wil onder meer zeggen: verantwoordelijk voor de randvoorwaarden voor goed archief- en informatiebeheer, zoals voldoende financiën. Voor digitaal informatiebeheer zijn een meerjarenplanning en financiële continuïteit onontbeerlijk. Zie Memorie van Toelichting bij de Archiefwet 1995 (TK 1992-1993, 22866 nr. 3) bij de artikelen 3, 27.2, 30.2, 35.2 en 41.3.		**Rodin 2010** 1.6 **ISO 16363** 3.4 **KIDO 1.0** Hoofdstuk 3

NR.	EIS	TOELICHTING	VOORBEELDEN	VERWIJZINGEN
1.3	**De organisatie beschikt over voldoende medewerkers, met voldoende kennis en competenties, om uitvoering te geven aan al haar taken, bevoegdheden en verantwoordelijkheden op het gebied van de digitale beheeromgeving.**	Onderdeel van de zorgplicht uit de Archiefwet is ook, dat het bestuur moet zorgen dat er voldoende en deskundig personeel aanwezig is voor de taakuitvoering. Bij uitbesteden van taken die de digitale beheeromgeving raken moeten uiteraard ook eisen gesteld worden aan de kwalitatieve en kwantitatieve personele capaciteit bij de beoogde uitvoerder(s). Zie *Memorie van Toelichting* bij de Archiefwet 1995 (TK 1992-1993, 22866 nr. 3) bij artikel 3.	Indicaties voor onvoldoende kwantitatieve en kwalitatieve capaciteit kunnen bijvoorbeeld zijn: achterstanden, incidenten, te hoge werkdruk, taken die blijven liggen.	**Rodin 2010** 1.7 **NEN-ISO 15489** 6.5 **KIDO 1.0** Hoofdstuk 3

NR.	EIS	TOELICHTING	VOORBEELDEN	VERWIJZINGEN
1.4	**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 de toetsbare eisen van een door haar toe te passen kwaliteitssysteem.**	Het kwaliteitssysteem bevat tenminste de volgende onderdelen: a een risicoanalyse als basis voor het informatiebeheer; b een beschrijving van de organisatie van het informatiebeheer die de duurzame toegankelijkheid en betrouwbaarheid van de informatie borgt; c vastgestelde en belegde bevoegdheden, verantwoordelijkheden en taken op het terrein van het informatiebeheer; d vastgestelde procedures voor het informatiebeheer in de staande organisatie en bij organisatiewijziging, bij het aangaan van samenwerking en/of overgang van taken naar een andere overheid; e periodieke interne monitoring als onderdeel van de Plan-Do-Check-Act-cyclus en externe monitoring, toetsing en/of certificering op het gebied van de digitale beheeromgeving en het informatiebeheer; f Een actueel, compleet en logisch samenhangend en geordend overzicht bijhoudt van de informatieobjecten die de organisatie beheert. Zie ook hoofdstuk 3.	*Zie de Handreiking Kwaliteitssysteem Informatiebeheer Decentrale Overheden (KIDO).* Ad b: De samenwerking tussen de disciplines I&A, archief en lijnafdelingen bij het informatiebeheer. Ad c: In besluiten zoals bijvoorbeeld het Besluit informatiebeheer, mandaatregelingen en inrichtingsplannen is vastgelegd wie op diverse niveaus verantwoordelijk is voor taken in het kader van informatiebeheer. Voorbeelden van taken: registratie en archivering, waardering en selectie, overbrenging naar een e-depot, I architectuur, informatiebeveiliging en change management. Ad d: Procedures voor bijvoorbeeld registratie en archivering, scannen etc., zie de taken onder ad c. Ad e: Systematisch intern monitoren en toetsen of procedures correct worden gevolgd en of het resultaat voldoet (bijvoorbeeld kwaliteit digitale dossiers). Regulier extern (laten) toetsen op zaken als geschiktheid en inrichting van systemen, correcte registratie, gebruik van metadata, compleetheid van dossiers, preserveringsmaatregelen.	**Rodin 2010** 1.2, 1.3, 1.4, 1.5 **Wetgeving** AW 4 en 5.1.1; Ar 16 en 18 **NEN-ISO 15489** 6.1, 6.2 en 6.3 **ISO 16363** 3.3.4, 3.3.6, 4.3.3 en 5.1.1 **KIDO 1.0** Hoofdstuk 3, 4.1.1, 4.1.2 **DUTO** Eis 2

Hoofdstuk 2

Informatiebeheer

NR.	EIS	TOELICHTING	VOORBEELDEN	VERWIJZINGEN
2.1	**Informatieobjecten zijn gekoppeld aan een ordeningsstructuur die is aan te passen zonder de al aanwezige structuur met zijn koppelingen te verstoren.**	Alle aanwezige informatieobjecten zijn volgens een logische opzet geordend en te presenteren. Voorheen werd hiervoor bijvoorbeeld een Documentair Structuur Plan (DSP) of Informatie Structuur Plan (ISP) gebruikt. Hierna, zie 2.3, worden gedetailleerde eisen gesteld aan het metagegevensschema, dat eveneens nodig is om de context van informatieobjecten te documenteren. Iedere wijziging in de ordeningsstructuur leidt tot nieuwe metagegevens over die ordening. De metadatering zorgt ervoor dat alle informatieobjecten in de tijd zowel naar hun oorspronkelijke ordeningsstructuur als naar eventuele nieuwe ordeningsstructuren kunnen worden gereconstrueerd.	Veel gebruikte decentrale ordeningsstructuren zijn: • Basisarchiefcode • GEMMA zaaktypecatalogus Volgens het zogenaamde structuurbeginsel (“respect voor de oude orde”) werd traditioneel bijvoorbeeld met een concordans de eerdere ordening gedocumenteerd, zodat reconstructie mogelijk was. In de digitale wereld kan dit principe worden toegepast door bijvoorbeeld oorspronkelijke metagegevens uit de administratieve fase te behouden bij overbrenging of uitplaatsing naar een e-depotvoorziening.	**Rodin 2010** 2.1 en 2.3 **Wetgeving** Ar 18 **NEN 2082** 25, 26, 140, 141 en 143 **NEN-ISO 15489** 8.3 en 9.4 **NEN-ISO 30301** A 2.1.2 en A 2.1.3 **KIDO 1.0** 5.1.1 en 6.5 **DUTO 1.0** 1

NR.	EIS	TOELICHTING	VOORBEELDEN	VERWIJZINGEN
2.2	**Ieder afzonderlijk informatie-object heeft een uniek identificatiekenmerk.**	Doordat het unieke identificatiekenmerk van ieder informatieobject in het beheersysteem slechts één keer voorkomt, zijn alle in een beheersysteem beheerde en geordende informatieobjecten ook afzonderlijk te vinden.	Toekenning van zogenaamde persistent identifiers. Dit kunnen vanwege de duurzaamheid meestal geen zaak- of documentnummers zijn.	**Rodin 2010** 2.2 **Wetgeving** Ar 23 (afgeleide) **NEN 2082** 2 **NEN-ISO 15489** 9.3 **ISO 16363** 4.2.4 **NEN-ISO 30301** A 2.1.1 **KIDO 1.0** 6.1 en 6.3

NR.	EIS	TOELICHTING	VOORBEELDEN	VERWIJZINGEN
2.3	**Informatieobjecten bevatten de voor het beheer benodigde kenmerken, die zijn ontleend aan een vastgesteld meta-gegevensschema.**	Metagegevens waarborgen de authenticiteit, betrouwbaarheid, bruikbaarheid en integriteit van informatieobjecten. De volgende essentiële eigenschappen voor het beheer van informatieobjecten worden op het laagste aggregatieniveau vastgelegd: • inhoud, structuur, verschijningsvorm en gedrag, voor zover die een rol spelen in het beheer; • wanneer, door wie en waarom de informatieobjecten zijn opgemaakt en/of werden ontvangen; • samenhang met andere beheerde informatieobjecten en basisregistraties; • uitgevoerde beheeractiviteiten; • actuele en oorspronkelijke technische aard (hard- en softwareomgeving); • aard van de digitale handtekening, indien aanwezig; • wijze van versleuteling (algoritme) en decryptiesleutel, indien van toepassing. Sommige van deze metagegevens kunnen al op een hoger aggregatieniveau worden vastgelegd en werken dan via overerving ook door op een lager niveau.	Structuur is bijvoorbeeld een sjabloon of formulier in Word. Bij scannen is TIFF vaak de oorspronkelijke verschijningsvorm van een als PDF bewaard informatieobject. Gedrag is o.a. een formule in een Excelsheet of een animatie in een Powerpointpresentatie. De technische aard beschrijft hoe en waarmee een informatieobject gebruikt kan worden. Voor de opzet van een metagegevensschema wordt veel gebruik gemaakt van: • NEN-ISO 23081 • NEN 2084 • Richtlijn Metagegevens Overheidsinformatie. • Toepassingsprofiel Metadatering Rijk • Toepassingsprofiel Metadatering Lokale Overheden (TMLO) • Overheid.nl Web Metadata Standaard (OWMS) Omwille van uniformiteit kunnen gecontroleerde, standaard woordenlijsten (thesauri) worden gebruikt, die vaak al worden toegepast in de administratie.	**Rodin 2010** 2.4, 2.5 en 2.8 **Wetgeving** Ar 17, 19, 21, 22 en 24 **NEN 2082** 4, 9, 22, 29, 30 en 89 **NEN-ISO 15489** 8.2 **ISO 16363** 4.1.2 **KIDO 1.0** 5.1.3, 6.3, 6.4 en 6.6 **DUTO 1.0** 11

NR.	EIS	TOELICHTING	VOORBEELDEN	VERWIJZINGEN
2.4	**Informatieobjecten worden beschikbaar gesteld, tenzij anders is bepaald.**	Met inachtneming van vastgestelde regels voor beperkingen van de openbaarheid en/of het gebruik zijn informatieobjecten met een zoekopdracht binnen redelijke tijd en inspanning te vinden, te tonen en te (her)gebruiken. Wanneer er beperkingen zijn, dient wel aangegeven te worden dat er informatieobjecten bestaan, voor zover dat naar de aard van die objecten mogelijk is. De beperkende regels moeten zijn gebaseerd op zowel wettelijke voorschriften, waaronder de Wbp en Wob, als interne regelingen, zoals een vastgesteld autorisatieschema.	Met eerbiediging van beperkingen in verband met de privacy en veiligheid kunnen openbare gegevens door de overheid via een website worden aangeboden. Grote hoeveelheden informatieobjecten, zoals alle e-mails, kunnen geautomatiseerd via een algoritme aangeboden worden.	**Rodin 2010** 2.11 **Wetgeving** Aw 14, Ar 20 **NEN 2082** 42, 46 en 100 **NEN-ISO 15489** 8.4 en 9.5 **NEN-ISO 30301** A 2.2.2 **KIDO 1.0** 5.1.11, 5.1.12, 8.1 en 8.2 **DUTO 1.0** 2, 4, 5, 6, 7 en 8

NR.	EIS	TOELICHTING	VOORBEELDEN	VERWIJZINGEN
2.5	**Informatieobjecten zijn, indien dit redelijkerwijs mogelijk is, opgeslagen in een open standaardformaat.**	Er moet worden vastgelegd welke formaten zijn toegestaan in de aanwezige beheeromgeving(en) en voor hergebruik. Als is vastgelegd wat is toegestaan, is het handig om de omzetting naar de toegestane formaten in te bouwen in het beheerssysteem, bijvoorbeeld automatische overzetting naar PDF-a.	Zie de lijst van Open Standaarden op de website van het Forum Standaardisatie. Voor veel formaten geldt het “pas-toe-of-leg-uit” principe.	**Rodin 2010** 2.7 **Wetgeving** Ar 26, Who 5.1 **NEN 2082** 20 en 33 **NEN-ISO 15489** 9.7 **NEN-ISO 30301** A 1.3.1, A 2.3.2 en A 2.3.3 **ISO 16363** 4.2.5 **KIDO 1.0** 5.1.4 en 6.7 **DUTO 1.0** 10

NR.	EIS	TOELICHTING	VOORBEELDEN	VERWIJZINGEN
2.6	**De betrouwbaarheid van informatieobjecten is aantoonbaar en gewaarborgd.**	Informatieobjecten zijn authentiek, integer en volledig. Beheeracties, waaronder importeren, bewaren, converteren, migreren en exporteren, hebben geen of alleen toegestane gevolgen voor de informatieobjecten en worden regelmatig geëvalueerd op hun werking. Alle beheeracties die leiden tot aantasting van de beheerde informatieobjecten worden gesignaleerd, gedocumenteerd en leiden tot een reactie. Dit alles wordt uitgevoerd conform de in 1.4 bedoelde procedures en afspraken.	De Baseline Informatiehuishouding Gemeenten (2011), deel 2a, geeft bijvoorbeeld in par. 6.1.2 en overzicht van verschillende functionele eisen. Aantasting van de betrouwbaarheid van informatieobjecten kan plaatsvinden door onder andere: • virussen, malware; • bitrot (veroudering); • storingen (stroomuitval, defecten); • calamiteiten (brand, wateroverlast, etc.); • afwijking van procedures, verkeerd gebruik; • ongewenste aanpassingen (ongeautoriseerd, hackers). De controle hierop vindt onder meer plaats aan de hand van loggings of automatische signaleringen en door de beschreven beheermaatregelen.	**Rodin 2010** 2.8, 2.9 en 2.10 **Wetgeving** Ar 14, 21, 22, 23 en 25 **NEN 2082** 9, 12, 16, 32, 36, 76, 82 en 108 **NEN-ISO 15489** 9.6 **NEN-ISO 30301** A 2.3.1, A 2.5.4 en A 2.5.6 **ISO 16363** 4.2.6, 4.2.7, 4.3.1, 4.3.2, 4.3.3 en 4.6.2.1 **KIDO 1.0** 6.6, 6.7, 7.2, 7.3, 7.4 en 8.2 **DUTO 1.0** 9

NR.	EIS	TOELICHTING	VOORBEELDEN	VERWIJZINGEN
2.7	**Informatieobjecten zijn van een bewaartermijn voorzien en worden na het verstrijken daarvan vernietigd.**	Aan de hand van een vigerende selectielijst worden aan informatieobjecten bewaartermijnen toegekend. Digitale informatieobjecten kunnen brongegevens bevatten, die ook deel kunnen uitmaken van andere informatieobjecten. Deze brongegevens kunnen in die verschillende contexten uiteenlopende bewaartermijnen hebben. Het is daarom zaak om brongegevens altijd te waarderen en selecteren in de context van het informatieobject waar ze deel van uitmaken. Bij de vernietiging mogen contextgegevens bewaard blijven, indien die voor het vastleggen van de vernietiging nodig zijn en niet tot een inhoudelijke reconstructie kunnen leiden. De vernietiging van informatieobjecten wordt in elk geval op het laagste aggregatieniveau gedocumenteerd. Vernietiging van brongegevens heeft gevolgen voor alle aggregatieniveaus en ook voor het gebruik van back-ups. Beheermaatregelen moeten ervoor zorgen dat de vernietiging van brongegevens in de context van een bepaald informatieobject niet ongedaan gemaakt kan worden.	Metagegevens van informatieobjecten die vernietigd zijn, kunnen worden bewaard om als 'virtuele vernietigingslijst' te dienen. Dat kan bijvoorbeeld door behoud van een zaaknummer, zaaktype en datering, aangevuld met gegevens over de uitvoering van de vernietiging. Bij het terugzetten van informatie uit een back-up kunnen de sinds het maken van een back-up uitgevoerde vernietigingsacties opnieuw worden uitgevoerd. Door bijvoorbeeld iedere nieuwe back-up de voorgaande back-up te laten overschrijven, wordt voorkomen dat vernietigbare gegevens via back-ups langer dan toegestaan bewaard blijven.	**Rodin 2010** 2.12, 2.13 en 2.14 **Wetgeving** Ab 8 **NEN 2082** 62, 73, 74 en 80 **NEN-ISO 15489** 9.9 **NEN-ISO 30301** A 1.1.4, A 2.4.1, A 2.4.4 en A 2.4.6 **KIDO 1.0** 6.2 en 7.4 **Moreq2** 5.3.18, 5.3.19 en 5.3.20 **DUTO 1.0** 3, 12 en 13

Hoofdstuk 3

ICT-beheer

NR.	EIS	TOELICHTING	VOORBEELDEN	VERWIJZINGEN
3.1	**De organisatie doet aan een systematische risicoanalyse voor factoren als data, systemen, personeel, fysieke locatie en beveiligingseisen.**	Het primaire uitgangspunt van digitaal informatiebeheer is risicomanagement. De organisatie voert een systematische risicoanalyse uit en stelt periodiek processen bij via de Plan-Do-Check- Act-cyclus. In het kader van deze cyclus wordt gecontroleerd of de getroffen maatregelen het gewenste effect sorteren. Deze controle kan weer aanleiding geven tot bijsturing. Ook kan blijken dat het totaal van eisen, maatregelen en controle aan revisie toe is (evaluatie). Het continu doorlopen van deze kwaliteitscirkel zorgt op elk moment voor het adequate beveiligingsniveau.		**Rodin 2010** 3.1, 3.3 **BIR, BIG, IBI, BIWA** Hoofdstuk 5 **ISO 16363** 5.1.1

NR.	EIS	TOELICHTING	VOORBEELDEN	VERWIJZINGEN
3.2	**De organisatie hanteert een informatiebeveiligingsplan gebaseerd op de NEN-ISO 27001 of vergelijkbare richtlijnen.**	Informatiebeveiliging wordt uitgewerkt in een plan conform de geldende basisrichtlijnen. Indien uit de risicoanalyse (3.1) naar voren is gekomen dat er systemen aanwezig zijn die een zwaarder beveiligingsregime vergen dan het basisregime, zijn hierin ook de zwaardere richtlijnen opgenomen die dergelijke systemen vereisen.	De BIR, BIG, BIWA en IBI beschrijven de invulling van NEN-ISO 27001 voor de verschillende overheidslagen. Deze (verplichte) beveiligingsnormen bevatten implementatierichtlijnen en eisen voor de procesinrichting.	**Rodin 2010** 3.2 **BIR, BIG, BIWA, IBI** Hoofdstuk 6 **ISO 16363** 5.2.1

NR.	EIS	TOELICHTING	VOORBEELDEN	VERWIJZINGEN
3.3	**De ICT-beheerprocessen zijn uitgewerkt conform standaarden.**	De belangrijkste taak van het functioneel beheer is het op elkaar afstemmen en uitlijnen van de wensen van de organisatie en IT. Dat dient op drie niveaus te gebeuren: 1. Het strategische niveau; betreft de aansluiting van de informatievoorziening op de strategische doelen van de organisatie. 2. Het tactische niveau; betreft de aansluiting van de informatievoorziening op het bedrijfsproces. 3. Het operationele niveau; betreft het ondersteunen van de eindgebruikers in het dagelijkse gebruik en het in kaart brengen van de veranderingen die moeten worden doorgevoerd.	ITIL, BISL en ASL zijn bruikbare en gangbare referentiekaders voor het inrichten van de ICT-beheerprocessen binnen een organisatie. Deze kaders kunnen worden gebruikt bij de beoordeling van de kwaliteit van de functionele beheersing op de drie genoemde niveaus.	**Rodin 2010** 3.7 **BIR, BIG, BIWA, IBI** Hoofdstuk 2 **ISO 16363** 5.2.3

NR.	EIS	TOELICHTING	VOORBEELDEN	VERWIJZINGEN
3.4	**Operationele aansturing van de informatievoorziening vindt plaats conform standaarden (toegang, incidenten, change, release etc.).**	Het betreft de diensten rondom het beschikbaar stellen en in stand houden van met name de hardware, systeemprogrammatuur en de ontwikkelhulpmiddelen. De toegang tot gegevens binnen de IT-omgeving dient uitsluitend beperkt te zijn tot geautoriseerde gebruikers of beheerders.	Problemen en wijzigingen mogen alleen door geautoriseerde personen worden opgelost. Wijzigingen mogen alleen plaatsvinden indien aan de gestelde kwaliteitscriteria is voldaan. Het proces rondom operationeel beheer moet op de juiste wijze gevolgd worden. Er zijn meerdere logische niveaus waarop de toegang tot gegevens wordt beschermd. Denk aan gegevensbestanden, gegevens in databases, functies en taken in applicaties, etc.	**Rodin 2010** 3.7 **BIR, BIG, BIWA, IBI** Hoofdstuk 9 **ISO 16363** 5.1.1

NR.	EIS	TOELICHTING	VOORBEELDEN	VERWIJZINGEN
3.5	**De organisatie beschikt over adequate serverruimtes; de systeembeheerders beschikken over vastgestelde protocollen voor de afhandeling van storingen, alarmeringen en andere uitzonderlijke situaties.**	Een adequate serverruimte is uitgerust met onder meer klimaatbeheersing, alarm- en brandmeldvoorziening, toegangscontrole, ordelijke bekabeling en noodstroom-voorziening (UPS). Door waarneming ter plaatse is de aanwezigheid van zaken als toegangsbeveiliging, brandblussers en klimaatregeling eenvoudig vast te stellen. Daarnaast dienen de operators met goedgekeurde instructies te werk te gaan.	De protocollen voor de systeembeheerders beschrijven bijvoorbeeld hoe te handelen bij het overschrijden van capaciteitsgrenzen of signalen van systemen voor intrusion detection en andere uitzonderlijke situaties die tijdens de uitvoering van de taak kunnen optreden.	**Rodin 2010** 3.9 **BIR, BIG, BIWA, IBI** Hoofdstuk 9 **ISO 16363** 4.1.2 **Richtlijnen** Handboek ICT huisvesting en bekabeling (HIB) versie 1.0

NR.	EIS	TOELICHTING	VOORBEELDEN	VERWIJZINGEN
3.6	**De organisatie beschikt over een passende back-upstrategie en een calamiteiten- en herstelplan, zodat informatie in geval van verstoringen snel weer beschikbaar gemaakt kan worden.**	Bedreigingen voor de bedrijfscontinuïteit zijn grofweg gelegen in het uitvallen of vastlopen van systemen, besmetting met virussen, corrupte schijven, vollopen van opslagruimte of gebrek aan verwerkingscapaciteit, calamiteiten zoals aanslagen, natuurrampen of een brand of het niet tijdig kunnen leveren van producten door leveranciers. Het testen hiervan moet een onderdeel zijn van de systematische risicoanalyse (zie 3.1). De back-upstrategie en het calamiteiten- en herstelplan is op basis van het informatiebeveiligingsplan uitgewerkt in concrete procedures en maatregelen. Gecontroleerd wordt of er uitwijktesten plaatsvinden. Met loggings zijn de tijdstippen van de back-ups en automatische signaleringen via RAID te controleren. In het calamiteitenplan moeten maatregelen zijn opgenomen hoe om te gaan met aanvallen van buitenaf. In dit plan staan ook de herstelmaatregelen. Daarnaast wordt nagegaan welke afspraken er bijvoorbeeld gemaakt zijn met leveranciers over vervangende apparatuur.		**Rodin 2010** 3.4, 3.5, 3.6 **BIR, BIG, BIWA, IBI** Hoofdstuk 6 **ISO 16363** 5.1.1.2, 5.1.1.3 **Moreq 2010** 12.13

NR.	EIS	TOELICHTING	VOORBEELDEN	VERWIJZINGEN
3.7	**De organisatie stelt in een Service Level Agreement (SLA) eisen aan de interne of externe ICT-diensten ten aanzien van beheerprestaties.**	Dienstverleners die worden ingeschakeld voor onderhoud en exploitatie van (delen van) de ICT-dienstverlening, moeten zich houden aan de serviceniveaus die in het contract zijn overeengekomen. De dienstverlening moet plaatsvinden onder strikt gemonitorde en beveiligde condities. Op basis van de in het contract afgesproken prestatie-indicatoren kan de behaalde kwaliteit worden gemeten. Het contract dient duidelijke afspraken te bevatten over het eigenaarschap van data, systemen, platforms en infrastructuren.		**Rodin 2010** 3.8 **BIR, BIG, BIWA, IBI** Hoofdstuk 10

NR.	EIS	TOELICHTING	VOORBEELDEN	VERWIJZINGEN
3.8	**De organisatie heeft een risicoafweging gemaakt met betrekking tot privacy, beveiliging en beschikbaarheid van de informatie bij outsourcing.**	Een organisatie moet zich bewust zijn van de risico's bij een cloud implementatie en andere vormen van outsourcing. Deze risico's zijn technisch, organisatorisch en juridisch van aard. De organisatorische maatregelen die de geïdentificeerde risico's dienen af te dekken, zijn onder te verdelen in maatregelen inzake het beheer van de kwaliteit van informatie, maatregelen voor de beveiliging van informatie en maatregelen met betrekking tot het beheer van informatie op afstand. Het gebruik van duidelijke beschrijvingen van de werking van interfaces, Public Key Infrastructure raamwerk, encryptie, monitoring en dergelijke voorkomt risico's. Tevens moeten er duidelijke afspraken gemaakt worden over het eigenaarschap van data, systemen, platforms en infrastructuren. Dit moet worden vastgelegd in de SLA's (zie 3.7). (Cloud)organisaties dienen aan hun klanten een verklaring te geven van de kwaliteit van de beheersing van deze maatregelen over een bepaald tijdvak. Idealiter wordt deze door een externe partij opgesteld.	De risico's kunnen betrekking hebben op bijvoorbeeld onveilige interfaces, een gebrek aan focus op beveiliging, een onlogische scheiding van virtualisatietechnieken, kwaadwillende medewerkers, dataverlies en niet of onvoldoende beschermde persoonsgegevens. Een ISAE 3402 verklaring is een mogelijke vorm van Service Organisation Control die opgelegd kan worden aan de (cloud)leverancier in geval van outsourcing.	**Rodin 2010** 3.7 **BIR, BIG, BIWA, IBI** Hoofdstuk 10 **Norea** Studierapport "Algemene beheersing van IT-diensten" (2015)

NR. BIJLAGE 1

BRONNEN

Wetgeving
Archiefwet 1995 (AW)
Archiefbesluit 1995 (AB)
Archiefregeling (AR)
Wet Hergebruik Overheidsinformatie (WHO)

Handreiking
KIDO Handreiking Kwaliteitssysteem Informatiebeheer Decentrale Overheden (KIDO)

Normen
DUTO versie 1.0
Normenkader Duurzaam Toegankelijke Overheidsinformatie (2016)
ISO 16363:2012
Audit and certification of trustworthy digital repositories
Moreq 2010 (Moreq2)
Modular requirements for records systems
NEN 2082: 2008 nl
Eisen voor functionaliteit van informatie- en archiefmanagement in programmatuur
NEN-ISO 15489-1:2016
Eisen voor informatie- en archiefmanagement
NEN-ISO 23081-1:2006 nl
Processen voor informatie- en archiefbeheer - Metagegevens voor archiefbescheiden
NEN-ISO 27001:2005
Eisen waar het managementsysteem voor informatiebeveiliging aan dient te voldoen

Overig
TMLO
Toepassingsprofiel Metadatering Lokale Overheden
TMR
Toepassingsprofiel Metagegevens Rijksoverheid
BIR
Baseline Informatiebeveiliging Rijksdienst (2012)
IBI
Interprovinciale Baseline Informatiebeveiliging (2010)
BIG
Baseline Informatiebeveiliging Gemeenten (2016)
BIWA
Baseline Informatiebeveiliging Waterschappen (2013)
NEN-ISO 30301:2011
Eisen voor managementsystemen voor archivering

NR. BIJLAGE 2

BEGRIPPEN

Aggregatieniveau
: Niveau binnen de ordeningsstructuur, bijvoorbeeld: het individuele stuk, het dossier of de zaak, het zaaktype of het onderwerp.

Bewaarstrategie
: Strategie voor de langetermijnbewaring van (digitale) informatie.

Brongegevens
: Te onderscheiden oorspronkelijke data, waarop het behoud gericht is en waarvan de bitstream leesbaar is te maken.

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

Duurzaam informatiebeheer
: Informatiebeheer waarbij de informatie vindbaar, authentiek en toegankelijk is en blijft gedurende de gehele voorgeschreven bewaartermijn.

Emulatie
: Methode waarbij de technische omgeving die noodzakelijk is voor het uitvoeren van oude programma`s softwarematig wordt nagebootst.

Informatiebeleid
: Beleid gericht op het beheer van (digitale) informatie.

Informatieobject
: Te identificeren geheel van gegevens (op ieder aggregatieniveau) waaraan in samenhang betekenis is gegeven.

Intrusion Detection System
: Een geautomatiseerd systeem dat hackpogingen en het optreden van ongeautoriseerde toegang tot een informatiesysteem of netwerk detecteert.

Kwaliteitssysteem
: De organisatorische structuur, verantwoordelijkheden, procedures, processen en voorzieningen die nodig zijn voor het ten uitvoer brengen van kwaliteitszorg (ISO 8402).

Metagegevens
: Gegevens die context, inhoud en structuur van informatieobjecten en hun beheer door de tijd heen beschrijven.

Metagegevensschema
: Beschrijving van de structuur en de betekenis van de gebruikte metagegevens.

Ordeningsstructuur
: Logisch verband tussen informatieobjecten, waardoor die terug te vinden zijn en hun relaties met processen en bewaartermijnen kunnen worden gelegd.

Preserveringsmaatregelen
: Maatregelen gericht op het behoud en de toegankelijkheid van digitale informatie op langere termijn.

RAID
: Redundant Array of Independent Disks; de benaming voor een set methodieken voor fysieke dataopslag op harde schijven waarbij de gegevens over meer schijven verdeeld worden, op meer dan één schijf worden opgeslagen, of beide, ten behoeve van snelheidswinst en/of beveiliging tegen gegevensverlies.

juni 2017

Branchevereniging Archiefinstellingen Nederland (BRAIN)
Koninklijke Vereniging van Archivarissen in Nederland (KVAN)
Landelijk Overleg van Provinciale Archiefinspecteurs (LOPAI)
m.m.v. Erfgoedinspectie (EGI)