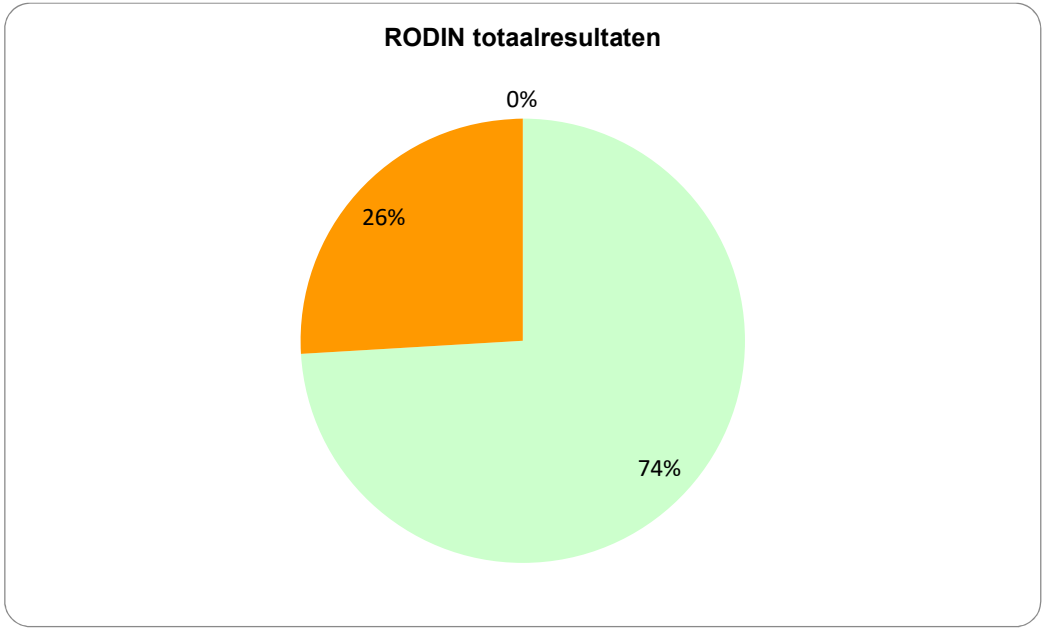

RODIN totaalresultaten
0%
26%
74%

**RODIN Referentiekader Opbouw Digitaal Informatiebeheer**

| categorie | sub-cat. | lid | vraag | ja/deels/nee | Onderbouwing antwoorden | Toelichting op de vragen | voorbeelden | verwijzingen |
|---|---|---|---|---|---|---|---|---|
| **1** | **1.** | | **Beleid en Organisatie** | | | | | |
| 1 | 1.1 | | De organisatie heeft een door het bestuur en/of management vastgesteld informatiebeleid. | ja | Het opstellen van een nieuw informatiebeleidsplan is begonnen. Eén van de onderdelen hiervan is het vormen van een visie op DIV. | Het vastgestelde informatiebeleid kan uit één document of meerdere documenten bestaan. Onderdelen van het informatiebeleid zijn tenminste:<br>a beschrijving van de manier waarop de organisatie zorgt dat zij voldoet aan de wettelijke eisen voor het bewaren van informatie;<br>b beschrijving van de bewaarstrategie (waaronder preserveringsmaatregelen);<br>c beschrijving van het beveiligingsbeleid, waarin taken en verantwoordelijkheden voor informatiebeveiliging zijn belegd.<br>Zie ook hoofdstuk 3. | | Rodin 2010<br>1.1<br>Wetgeving<br>AR 25<br>NEN-ISO 15489<br>6.2<br>ISO 16363<br>3.1.1, 3.1.2, 3.3.2 en 5<br>KIDO 1.0<br>Hoofdstuk 3 |
| 1 | 1.1 | a | beschrijving van de manier waarop de organisatie zorgt dat zij voldoet aan de wettelijke eisen voor het bewaren van informatie; | ja | Dit wordt meegenomen bij het opstellen van het informatiebeleidsplan | | Een informatiebeleidsplan of ander plan waarin (onder meer) beschreven staat hoe men voldoet aan de Archiefwet en aanverwante regelgeving. | |
| 1 | 1.1 | b | beschrijving van de bewaarstrategie (waaronder preserveringsmaatregelen) | ja | Dit is nog niet van toepassing voor de BWB gezien het relatief korte bestaan. Er wordt wel aandacht gevraagd bij de informatiemanager voor het opstellen van een bewaarstrategie. | | 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. | |
| 1 | 1.1 | c | beschrijving van het beveiligingsbeleid, waarin taken en verantwoordelijkheden voor informatiebeveiliging zijn belegd. | deels | De beschrijving is gereed maar implementatie van de BIG dient nog volledig afgerond te worden. | | Voor gemeenten conform de BIG, voor waterschappen de BIWA, voor provincies de IBI en voor het Rijk de BIR. | |
| 1 | 1.2 | | Voor de continuïteit van de digitale beheeromgeving zijn structureel voldoende middelen beschikbaar gesteld. | ja | | 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<br>ISO 16363; 3.4<br>KIDO 1.0; Hoofdstuk 3 |
| 1 | 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. | ja | In 2020 is een tweede medewerker DIV aangetrokken. Deze medewerker dient in 2020 volledig ingewerkt te worden. | 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<br>NEN-ISO 15489; 6.5<br>KIDO 1.0; Hoofdstuk 3 |
| 1 | 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.<br><br><u>Het kwaliteitssysteem bevat tenminste de volgende onderdelen:</u> | | | | Zie de Handreiking Kwaliteitssysteem Informatiebeheer Decentrale Overheden (KIDO). | Rodin 2010: 1.2, 1.3, 1.4, 1.5<br>Wetgeving; AW 4 en 5.1.1; Ar 16 en 18<br>NEN-ISO 15489; 6.1, 6.2 en 6.3<br>ISO 16363; 3.3.4, 3.3.6, 4.3.3 en 5.1.1<br>KIDO 1.0; Hoofdstuk 3, 4.1.1, 4.1.2<br>DUTO: Eis 2 |
| 1 | 1.4 | a | een risicoanalyse als basis voor het informatiebeheer | deels | Jaarlijk wordt het informatiebeheer ge-audit door het WBA. Dit dekt echter niet alle werkzaamheden die verricht worden binnen de BWB. | | | |
| | 1.4 | b | een beschrijving van de organisatie van het informatiebeheer die de duurzame toegankelijkheid en betrouwbaarheid van de informatie borgt | ja | Er is binnen de BWB geen formele organisatie die dit borgt. Wel is er wekelijks overleg tussen de volgende disciplines: DIV, FG, CISO, informatieamanager. Dit is niet beschreven/vastgelegd. | | Ad b: De samenwerking tussen de disciplines I&A, archief en lijnafdelingen bij het informatiebeheer. | |
| 1 | 1.4 | c | vastgestelde en belegde bevoegdheden, verantwoordelijkheden en taken op het terrein van het informatiebeheer | ja | Hiertoe zijn de Archiefverordening en Besluit informatiebeheer in 2017 vastgesteld. | | 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. | |
| 1 | 1.4 | 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 | ja | Er zijn handleidingen opgesteld voor postregistratie, scannen van de post, controle van de gescande post | | Ad d: Procedures voor bijvoorbeeld registratie en archivering, scannen etc., zie de taken onder ad c. | |
| 1 | 1.4 | 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 | ja | Het WBA auditeert jaarlijks de organisatie en haar werkwijze. | | 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 Referentiekader Opbouw Digitaal Informatiebeheer**

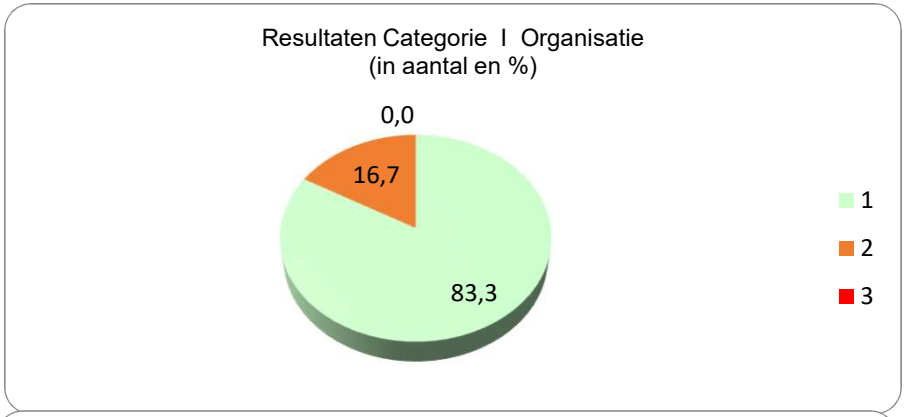
| categorie | sub-cat. | lid | vraag | ja/deels/nee | Onderbouwing antwoorden | Toelichting op de vragen | voorbeelden | verwijzingen |
|---|---|---|---|---|---|---|---|---|
| 1 | 1.4 | f | Een actueel, compleet en logisch samenhangend en geordend overzicht bijhoudt van de informatieobjecten die de organisatie beheert. | ja | In de de applicatie i-Navigator, gecombineerd met de de Procesmap wodt een overzicht bijgehouden van de informatieobjecten die beheerd worden | | | |
| **2** | **2.** | | **Informatiebeheer** | | | | | |
| 2 | 2.1 | | Informatieobjecten zijn gekoppeld aan een ordeningsstructuur die is aan te passen zonder de al aanwezige structuur met zijn koppelingen te verstoren. | deels | Binnen het zaaksysteem worden verschillende ordeningsstructuren ondersteund en gebruikt door de BWB. De applicaties die vanaf het najaar 2020 worden gebruikt ondersteunen dit wel (Alfresco). | Alle aanwezige informatieobjecten zijn volgens een logische opzet geordend en te presenteren.<br>Voorheen werd hiervoor bijvoorbeeld een Documentair Structuur Plan (DSP) of Informatie Structuur Plan (ISP) gebruikt.<br>Hierna, zie 2.3, worden gedetailleerde eisen gesteld aan het metagegevensschema, dat eveneens nodig is om de context van informatieobjecten te documenteren.<br>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:<br>• Basisarchiefcode<br>• GEMMA zaaktypecatalogus<br>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<br>Wetgeving; Ar 18<br>NEN 2082; 25, 26, 140, 141 en 143<br>NEN-ISO 15489; 8.3 en 9.4<br>NEN-ISO 30301; A 2.1.2 en A 2.1.3<br>KIDO 1.0; 5.1.1 en 6.5<br>DUTO 1.0; 1 |
| 2 | 2.2 | | Ieder afzonderlijk informatieobject heeft een uniek identificatiekenmerk. | deels | Het zaaksysteem ondersteund dit volledig. Hiervoor wordt gebruikt van standaard metadata. Het schema is nog niet vastgesteld. De applicaties die vanaf het najaar 2020 worden gebruikt ondersteunen dit wel (Alfresco). | 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<br>Wetgeving; Ar 23 (afgeleide)<br>NEN 2082; 2<br>NEN-ISO 15489; 9.3<br>ISO 16363; 4.2.4<br>NEN-ISO 30301; A 2.1.1<br>KIDO 1.0; 6.1 en 6.3 |
| 2 | 2.3 | | Informatieobjecten bevatten de voor het beheer benodigde kenmerken, die zijn ontleend aan een vastgesteld metagegevensschema | deels | Het zaaksysteem ondersteund dit volledig. Hiervoor wordt gebruikt van standaard metadata. Het schema is nog niet vastgesteld. De applicaties die vanaf het najaar 2020 worden gebruikt ondersteunen dit wel (Alfresco). | Metagegevens waarborgen de authenticiteit, betrouw- baarheid, bruikbaarheid en integriteit van informatie- objecten. De volgende essentiële eigenschappen voor het beheer van informatieobjecten worden op het laagste aggregatieniveau vastgelegd:<br>• inhoud, structuur, verschijningsvorm en gedrag, voor zover die een rol spelen in het beheer;<br>• wanneer, door wie en waarom de informatieobjecten zijn opgemaakt en/of werden ontvangen;<br>• samenhang met andere beheerde informatieobjecten en basisregistraties;<br>• uitgevoerde beheeractiviteiten;<br>• actuele en oorspronkelijke technische aard (hard- en softwareomgeving);<br>• aard van de digitale handtekening, indien aanwezig;<br>• wijze van versleuteling (algoritme) en decryptie- sleutel, indien van toepassing.<br>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 ver- schijningsvorm van een als PDF bewaard informatie- object. Gedrag is o.a. een formule in een Excelsheet of een animatie in een Powerpointpresentatie. De tech- nische aard beschrijft hoe en waarmee een informatie- object gebruikt kan worden.<br>Voor de opzet van een metagegevensschema wordt veel gebruik gemaakt van:<br>• NEN-ISO 23081<br>• NEN 2084<br>• Richtlijn Metagegevens Overheidsinformatie.<br>• Toepassingsprofiel Metadatering Rijk<br>• Toepassingsprofiel Metadatering Lokale Overheden (TMLO)<br>• 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<br>Wetgeving; Ar 17, 19, 21, 22 en 24<br>NEN 2082; 4, 9, 22, 29, 30 en 89<br>NEN-ISO 15489; 8.2<br>ISO 16363; 4.1.2<br>KIDO 1.0; 5.1.3, 6.3, 6.4 en 6.6<br>DUTO 1.0; 11 |
| 2 | 2.4 | | Informatieobjecten worden beschikbaar gesteld, tenzij anders is bepaald. | ja | | 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.<br>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.<br>Grote hoeveelheden informatieobjecten, zoals alle e- mails, kunnen geautomatiseerd via een algoritme aangeboden worden. | Rodin 2010; 2.11<br>Wetgeving; Aw 14, Ar 20<br>NEN 2082; 42, 46 en 100<br>NEN-ISO 15489; 8.4 en 9.5<br>NEN-ISO 30301; A 2.2.2<br>KIDO 1.0; 5.1.11, 5.1.12, 8.1 en 8.2<br>DUTO 1.0; 2, 4, 5, 6, 7 en 8 |
| 2 | 2.5 | | Informatieobjecten zijn, indien dit redelijkerwijs mogelijk is, opgeslagen in een open standaardformaat. | ja | In Zaaksysteem.nl wordt automatisch geconverteerd naar PDF-A.<br>In ADP worden alleen maar in PDF opgeslagen. | Er moet worden vastgelegd welke formaten zijn toe- gestaan in de aanwezige beheeromgeving(en) en voor hergebruik.<br>Als is vastgelegd wat is toegestaan, is het handig om de omzetting naar de toegestane formaten in te bouwen in het beheerssysteem, bijvoorbeeld automatische over- zetting 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<br>Wetgeving; Ar 26, Who 5.1<br>NEN 2082; 20 en 33<br>NEN-ISO 15489; 9.7<br>NEN-ISO 30301; A 1.3.1, A 2.3.2 en A 2.3.3<br>ISO 16363; 4.2.5<br>KIDO 1.0; 5.1.4 en 6.7<br>DUTO 1.0; 10 |
| 2 | 2.6 | | De betrouwbaarheid van informatieobjecten is aantoonbaar en gewaarborgd. | ja | Aan de hand van de BIG wordt dit ingericht binnen de BWB. | 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.<br>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.<br>Aantasting van de betrouwbaarheid van informatie- objecten kan plaatsvinden door onder andere:<br>• virussen, malware;<br>• bitrot (veroudering);<br>• storingen (stroomuitval, defecten);<br>• calamiteiten (brand, wateroverlast, etc.);<br>• afwijking van procedures, verkeerd gebruik;<br>• ongewenste aanpassingen (ongeautoriseerd, hackers).<br>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<br>Wetgeving; Ar 14, 21, 22, 23 en 25<br>NEN 2082; 9, 12, 16, 32, 36, 76, 82 en 108<br>NEN-ISO 15489; 9.6<br>NEN-ISO 30301; A 2.3.1, A 2.5.4 en A 2.5.6<br>ISO 16363; 4.2.6, 4.2.7, 4.3.1, 4.3.2, 4.3.3 en 4.6.2.1<br>KIDO 1.0; 6.6, 6.7, 7.2, 7.3, 7.4 en 8.2<br>DUTO 1.0; 9 |

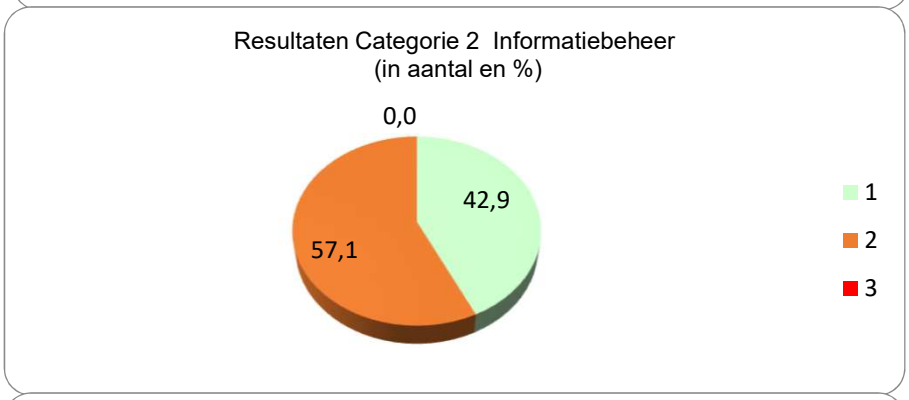
| categorie | sub-cat. | lid | vraag | ja/deels/nee | Onderbouwing antwoorden | Toelichting op de vragen | voorbeelden | verwijzingen |
|---|---|---|---|---|---|---|---|---|
| 2 | 2.7 | | Informatieobjecten zijn van een bewaartermijn voorzien en worden na het verstrijken daarvan vernietigd. | deels | De vernietigingstermijnen zijn vastgelegd. De daadwerkelijke vernietiging heeft een achterstand opgelopen. Dit is opgenomen in het jaaroverzicht. | 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 ver- nietiging 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 ver- nietigbare gegevens via back-ups langer dan toegestaan bewaard blijven. | Rodin 2010; 2.12, 2.13 en 2.14<br>Wetgeving; Ab 8<br>NEN 2082; 62, 73, 74 en 80<br>NEN-ISO 15489; 9.9<br>NEN-ISO 30301; A 1.1.4, A 2.4.1, A 2.4.4 en A 2.4.6<br>KIDO 1.0; 6.2 en 7.4<br>Moreq2; 5.3.18, 5.3.19 en 5.3.20<br>DUTO 1.0; 3, 12 en 13 |
| **3** | **3.** | | **ICT-beheer en -beveiliging** | | | | | |
| 3 | 3.1 | | De organisatie doet aan een systematische risicoanalyse voor factoren als data, systemen, personeel, fysieke locatie en beveiligingseisen. | ja | Voor de fysieke toegang vinden voortdurend risico-analyses plaats. | 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.<br>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).<br>Het continu doorlopen van deze kwaliteitscirkel zorgt op elk moment voor het adequate beveiligingsniveau. | | Rodin 2010; 3.1, 3.3<br>BIR, BIG, IBI, BIWA; Hoofdstuk 5<br>ISO 16363; 5.1.1 |
| 3 | 3.2 | | De organisatie hanteert een informatiebeveiligingsplan gebaseerd op de NEN-ISO 27001 of vergelijkbare richtlijnen. | ja | Binnen de BWB wordt de BIG ingezet voor het inrichten van de informatiebeveiliging. Deel van deze werkzaamheden wordt uitgevoerd door de gemeente Breda, zijnde onze kantoorautomatiseringsleverancier | 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<br>BIR, BIG, BIWA, IBI; Hoofdstuk 6<br>ISO 16363; 5.2.1 |
| 3 | 3.3 | | De ICT-beheerprocessen zijn uitgewerkt conform standaarden. | deels | Het strategisch en tactisch niveau moet terug te vinden zijn in het informatiebeleidsplan. Aan het informatiebeleidsplan wordt gewerkt.<br><br>Het technisch beheer van de kantoorautomatisering is belegd bij gemeente Breda. Als kantoorautomatiseringspartner.<br>En het technisch beheer van de software is belegd bij de software leveranciers.<br><br>Het functioneel beheer van de software wordt uitgevoerd door de BWB. Hier is nog geen beheerproces voor uitgewerkt conform genoemde standaard(en). | De belangrijkste taak van het functioneel beheer is het op elkaar afstemmen en uitlijnen van de wensen van de organisatie en IT.<br>Dat dient op drie niveaus te gebeuren:<br>1. Het strategische niveau; betreft de aansluiting van de informatievoorziening op de strategische doelen van de organisatie.<br>2. Het tactische niveau; betreft de aansluiting van de informatievoorziening op het bedrijfsproces.<br>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 referentie- kaders 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<br>BIR, BIG, BIWA, IBI; Hoofdstuk 2<br>ISO 16363; 5.2.3 |
| 3 | 3.4 | | Operationele aansturing van de informatievoorziening vindt plaats conform standaarden (toegang, incidenten, change, release etc.) | ja | Voor het beheer van incidenten en gebruikersvragen wordt aangesloten bij de gemeente Breda. Gemeente Breda is de kantoorautomatiseringsleverancier voor de BWB. | 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 geautori- seerde personen worden opgelost. Wijzigingen mogen alleen plaatsvinden indien aan de gestelde kwaliteits- criteria 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 gegevensbestan- den, gegevens in databases, functies en taken in applicaties, etc. | Rodin 2010; 3.7<br>BIR, BIG, BIWA, IBI; Hoofdstuk 9<br>ISO 16363; 5.1.1 |
| 3 | 3.5 | | De organisatie beschikt over adequate serverruimtes; de systeembeheerders beschikken over vastgestelde protocollen voor de afhandeling van storingen, alarmeringen en andere uitzonderlijke situaties. | ja | | 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<br>BIR, BIG, BIWA, IBI; Hoofdstuk 9<br>ISO 16363; 4.1.2<br>Richtlijnen; Handboek ICT huisvesting en bekabeling (HIB) versie 1.0 |

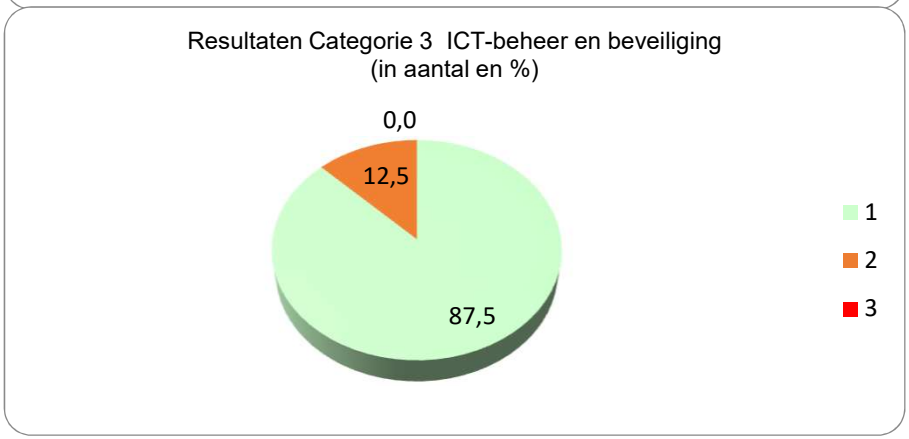
**RODIN Referentiekader Opbouw Digitaal Informatiebeheer**

| categorie | sub-cat. | lid | vraag | ja/deels/nee | Onderbouwing antwoorden | Toelichting op de vragen | voorbeelden | verwijzingen |
|---|---|---|---|---|---|---|---|---|
| 3 | 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. | ja | Hiervoor wordt gebruik gemaakt van de gemeente Breda. De gemeente Breda is de kantoorautomatiseringsleveranciers voor de BWB. | Bedreigingen voor de bedrijfscontinuiteit 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).<br>De back-upstrategie en het calamiteiten- en herstelplan is op basis van het informatiebeveiligingsplan uitge- werkt 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.<br>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 bijvoor- beeld gemaakt zijn met leveranciers over vervangende apparatuur. | | Rodin 2010; 3.4, 3.5, 3.6<br>BIR, BIG, BIWA, IBI; Hoofdstuk 6<br>ISO 16363; 5.1.1.2, 5.1.1.3<br>Moreq 2010; 12.13 |
| 3 | 3.7 | | De organisatie stelt in een Service Level Agreement (SLA) eisen aan de interne of externe ICT-diensten ten aanzien van beheerprestaties. | ja | Met de diverse leveranciers zijn overeenkomsten gesloten over de inspanningsverplichtingen en diensten die zij leveren. | 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<br>BIR, BIG, BIWA, IBI; Hoofdstuk 10 |
| 3 | 3.8 | | De organisatie heeft een risicoafweging gemaakt met betrekking tot privacy, beveiliging en beschikbaarheid van de informatie bij outsourcing. | ja | De FG wordt structureel gevraagd om inzake deze materie te adviseren. | 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.<br>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.<br>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).<br>(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.<br>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<br>BIR, BIG, BIWA, IBI; Hoofdstuk 10<br>Norea; Studierapport "Algemene beheersing van ITdiensten" (2015) |
| 3 | | | | | | | | |

| | |
|---|---|
| **ja** | **20** |
| **deels** | **7** |
| **nee** | **0** |
| indien cellen in kolom 'opmerking toets' zacht geel kleurt: Toelichting invullen | |
| Nog niet ingevuld of niet van toepassing | |

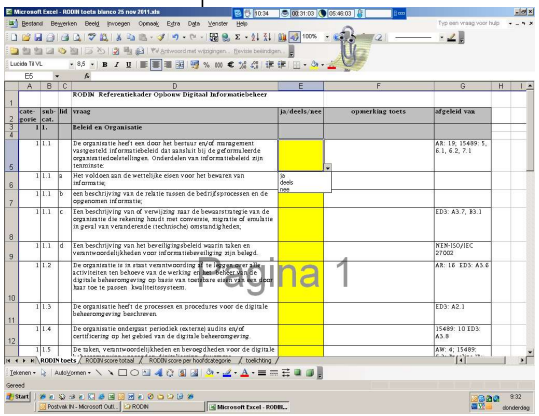

Resultaten Categorie I Organisatie
(in aantal en %)
0,0
16,7
83,3
1
2
3

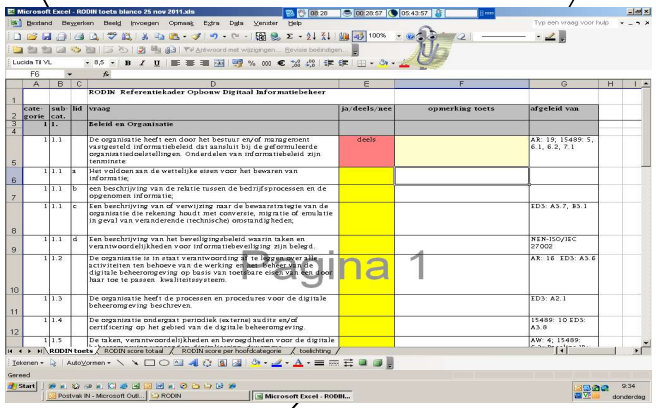

Resultaten Categorie 2 Informatiebeheer
(in aantal en %)
0,0
42,9
57,1
1
2
3


Resultaten Categorie 3 ICT-beheer en beveiliging
(in aantal en %)
0,0
12,5
87,5
1
2
3

Kolom E (ja/deels/nee) kleuren hard geel wanneer deze nog niet zijn ingevuld
Door op de cel te gaan staan wordt een keuzeveld aangeboden waaruit het antwoord kan worden gekozen

Wanneer er een keuze is gemaakt krijgt deze een eigen kleur: **ja** -> blauw, **deels** -> oranje/bruin, **nee** -> paars/menie-rood
Bij de keuzeantwoorden deels en nee wordt de cel in de kolom 'opmerking toets' zacht geel





Wanneer de cel in kolom 'opmerking toets' zacht geel kleurt betekent dit dat de reden/oorzaak van het antwoord 'deels' of 'nee' moet worden toegelicht. Neemt niet weg dat ook bij een 'ja' een toelichting kan worden ingevuld indien een vraag bijv. n.v.t. is, of om een andere reden een toelichting relevant is.