Wat te doen met een digitaal bestand

Onderzoek naar duurzame toegankelijkheid van digitale informatie bij overheden in Noord-Nederland

Assen, Groningen, Leeuwarden, november 2013

Afbeelding voorpagina is afkomstig van de gemeente Putten (Gld.)

Inhoudsopgave

‘Uit veel onderzoeken is inmiddels duidelijk geworden dat duurzame digitale toegankelijkheid vooral te maken heeft met informatieverwerking. Digitale archivering richt zich niet alleen op digitale media. De kern is het bestaan, de bewerking, het gebruik, de terugvindbaarheid en het behoud van betrouwbare informatie. En dat in combinatie met dat je kunt aantonen dat wet- en regelgeving zijn nageleefd (“Compliance”).

De kern van informatiemanagement ligt in de informatiewaardeketen; het informatieproces van begin tot bittere eind. De informatiewaardeketen regelt vier dimensies: kwaliteit, context, relevantie – de economische, bedrijfsmatige of cultuurhistorische waarde – en het voortbestaan van informatie. Met een e-depot is het probleem van duurzame digitale toegankelijkheid niet opgelost. Daarmee heb je een middel om het probleem op te kúnnen lossen. Het in stand houden van informatie is ons doel, dat mogen we nooit uit het oog verliezen. En bij voorkeur vindt archivering plaats op een intuïtieve manier, “just like an Apple”’.

(Dr. Geert-Jan van Bussel, lector Digital Archiving & Compliance aan de Hogeschool van Amsterdam)

Managementsamenvatting

De Landelijke Erfgoedinspectie constateerde in 2012 dat het digitale geheugen van de centrale overheid nog niet op orde is. Dit ondanks alle inspanningen die er de afgelopen jaren zijn verricht. De logische vraag voor de provincies Drenthe, Fryslân en Groningen was of het digitale geheugen van lagere overheden in Noord-Nederland dan wel op orde is. Dit hebben wij onderzocht bij zeven representatieve overheden als grondslag voor het thema 'een duurzame en adequate digitale beheer- en bewaaromgeving'. Dit thema maakt deel uit van het Interbestuurlijk archieftoezicht.

Doel van dit onderzoek was om inzicht te krijgen in de juridische waarde, de bruikbaarheid en de staat van de duurzame toegankelijkheid van de digitale informatie. Centrale vraag hierbij was welke maatregelen (eventueel) nodig zijn om de beheeromgeving bij overheidsorganisaties hiervoor geschikt te maken. Maar dit onderzoek was ook bedoeld om bewustwording te kweken c.q. te vergroten bij overheden om hun informatiehuishouding (beter) op orde te krijgen. Dit met het oogmerk verantwoording te kunnen afleggen van genomen besluiten en het gevoerde beleid, zaken te kunnen reconstrueren en voor een deel vanuit cultuurhistorisch belang. Het onderzoek had nadrukkelijk het karakter van een pilot om ervaring op te doen met het thema 'een duurzame en adequate digitale beheer- en bewaaromgeving'. Met het oog op het interbestuurlijk archieftoezicht moeten de resultaten vervolgens toepasbaar zijn bij meerdere organisaties.

Op basis van dit onderzoek concluderen wij het volgende:

a. Organisaties voldoen deels aan wettelijke verplichtingen voor duurzame toegankelijkheid van digitale informatie;

b. Wij zien positieve ontwikkelingen binnen informatiebeheer in Document Management Systemen, het informatiebeheer daarbuiten is zorgwekkend;

c. Sommige organisaties zien digitalisering als alleen een technische uitdaging;

d. Organisaties hebben behoefte aan concrete handvatten.

Daarom bevelen het volgende aan:

a. Benader duurzame digitale toegankelijkheid als een organisatorische uitdaging en niet als een technisch probleem;

b. Versterk de rol van informatiebeheerders;

c. Breng digitale huishouding in kaart;

d. Onderzoek de mogelijkheden om te komen tot een extra voorziening in de eigen digitale beheeromgeving die openbare raadpleging en langdurige bewaring mogelijk maakt;

e. Vergaar en deel kennis en maak gebruik van ervaringen bij andere organisaties.

1 Inleiding

De Landelijke Erfgoedinspectie constateerde in 2012 dat het digitale geheugen van de centrale overheid nog niet op orde is. Dit ondanks alle inspanningen die er de afgelopen jaren zijn verricht. De logische vraag voor de provincies Drenthe, Fryslân en Groningen was of het digitale geheugen van lagere overheden in Noord-Nederland dan wel op orde is. Dit hebben wij onderzocht bij zeven representatieve overheden als grondslag voor het thema 'een duurzame en adequate digitale beheer- en bewaaromgeving'. Dit thema maakt deel uit van het Interbestuurlijk archieftoezicht.

Doel van dit onderzoek was om inzicht te krijgen in de juridische waarde, de bruikbaarheid en de staat van de duurzame toegankelijkheid van de digitale informatie. Centrale vraag hierbij was welke maatregelen (eventueel) nodig zijn om de beheeromgeving bij overheidsorganisaties hiervoor geschikt te maken. Maar dit onderzoek was ook bedoeld om bewustwording te kweken c.q. te vergroten bij overheden om hun informatiehuishouding (beter) op orde te krijgen. Dit met het oogmerk verantwoording te kunnen afleggen van genomen besluiten en het gevoerde beleid, zaken te kunnen reconstrueren en voor een deel vanuit cultuurhistorisch belang. Het onderzoek had nadrukkelijk het karakter van een pilot om ervaring op te doen met het thema 'een duurzame en adequate digitale beheer- en bewaaromgeving'. Met het oog op het interbestuurlijk archieftoezicht moeten de resultaten vervolgens toepasbaar zijn bij meerdere organisaties.

Dit onderzoek biedt – helaas- niet de ultieme oplossing voor duurzame toegankelijkheid van digitale informatie. Daarvoor is de materie te complex en is elke organisatie te verschillend. Wat dit onderzoek wel biedt is een aantal maatregelen die getroffen kunnen worden door organisaties om (gezamenlijk) de beheeromgeving geschikt te maken voor duurzame digitale toegankelijkheid. Deze maatregelen, lijken misschien een 'open deur'. En in zekere zin zijn ze dat ook. Toch valt er in de praktijk nog heel veel winst te halen.

De volgende organisaties hebben deelgenomen aan dit onderzoek. De provincies Groningen en Fryslân, de gemeenten Franekeradeel, Midden-Drenthe en Veendam/Pekela (De Kompanjie), het waterschap Hunze en Aa's en het ICT Samenwerkingsverband Zuidwest Fryslân (ISZF). Naar aanleiding van hun antwoorden op onze schriftelijke vragen (zie bijlage), zijn interviews gevoerd met deze organisaties. Ook zijn diverse applicaties nader bekeken. Wij hebben er in dit verslag bewust voor gekozen om de verkregen informatie niet te kunnen herleiden tot een organisatie. Verder zijn er, naast literatuuronderzoek, oriënterende gesprekken gevoerd met personen van de gemeenten Weststellingwerf, Tytsjerksteradiel, Leeuwarden, Emmen, Zeewolde en Putten, alsmede met T. van Dijk (Prover), J. Jansen (Pagefreezer) en dr. G.J. van Bussel, lector Digital Archiving & Compliance aan de Hogeschool van Amsterdam. Wij bedanken alle betrokkenen van harte voor hun medewerking. Bovendien is een 'Roadshow Recordsmanagement' van het bedrijf VHIC bezocht.

Kader

De Archiefwet 1995 definieert archiefbescheiden als bescheiden, *ongeacht hun vorm*, door de overheidsorganen ontvangen of opgemaakt en naar hun aard bestemd daaronder te berusten. Het maakt dus niet uit of die informatie op papier is of digitaal. De eisen die de Overheid hieraan stelt staan in de Archiefregeling 2009. Voor de lagere overheden oefenen de provinciale archivarissen toezicht uit op de archieven. Met het van kracht worden van de wet Revitalisering Generiek Toezicht (RGT) in 2012, is het toezicht van het ene overheidsorgaan op het andere fors veranderd. Zo is het specifiek toezicht door de provincies op grond van de Archiefwet 1995 vervangen door generiek toezicht op de archiefketen. Vertrouwen in de bestuurslaag waar een taak is belegd, zoals de archivering en het informatiebeheer, staat voortaan voorop. Daarbij past dat gemeenten, waterschappen en andere decentrale overheden inzicht geven in hun eigen kwaliteit, die zij vervolgens aan hun eigen algemene besturen voorleggen. Daarmee kunnen de algemene besturen hun controlerende taak uitoefenen, zoals past in de duale opzet van overheden.

Dezelfde informatie gaat ook naar de toezichthoudende provincie. Die moet kunnen beoordelen of een organisatie al of niet voldoet aan de Archiefwet en regelgeving. Daarbij gaan de provincies voortaan meer uit van risicoanalyse. En zij blijven daar, waar het goed gaat, meer op afstand. Welke informatie de provincies precies nodig hebben, hoe zij met de verkregen informatie zullen omgaan, en hoe en wanneer zij gaan ingrijpen, staat beschreven in het zogenaamde 'aanvullende beleidskader voor het interbestuurlijk archieftoezicht Nieuwe Schoenen'. Het bestuur van het Interprovinciaal Overleg heeft dit aanvullende beleidskader op 24 mei 2012 vastgesteld. Het is een aanvulling op de regels voor 'In de plaats treden bij taakverwaarlozing', die in 2011 door het kabinet zijn vastgesteld. Daarin staat hoe de provincies in het algemeen zullen handelen als zij taakverwaarlozing constateren, dat wil zeggen als een overheid zijn taken niet conform wetgeving uitvoert. In de 'Nieuwe Schoenen' staan aanvullend specifieke situaties beschreven en voorbeelden op het terrein van de Archiefwet. Dat was nodig, omdat er op dit vakgebied veranderingen spelen, er bij de regering zorgen leven over de kwaliteit van de informatiehuishouding bij alle overheden, een aantal provinciale taken op het terrein van de Archiefwet blijven bestaan, en er in het veld behoefte aan was. De provinciale archivarissen in Drenthe, Fryslân en Groningen hebben op basis van 'Nieuwe schoenen' in december 2012 hun werkwijze geformuleerd. Daarin staan vier cruciale thema's (speerpunten) centraal namelijk:

- Het beheer van zowel analoge als digitale overheidsinformatie voldoet aan toetsbare eisen van een toe te passen kwaliteitssysteem;
- Zowel analoge als digitale overheidsinformatie wordt in goede, geordende en toegankelijke staat gebracht;
- Zowel analoge als digitale overheidsinformatie wordt tijdig vernietigd dan wel overgebracht, openbaar gemaakt en beschikbaar gesteld;
- Zowel analoge als digitale overheidsinformatie wordt duurzaam beheerd en is geplaatst in daartoe geëigende omgevingen

Per thema (speerpunt) staan referenties vermeld naar de handreiking Kritische Prestatie Indicatoren (KPI's) van de Vereniging van Nederlandse Gemeenten (VNG). In deze handreiking staat onder meer de relatie beschreven met diverse kaders en kwaliteitsinstrumenten op het gebied van archiefbeleid en wat de verhouding is tot de archief KPI's. Eén van die instrumenten is het Referentiekader Opbouw Digitaal Informatiebeheer (RODIN) dat uitgangspunt is geweest bij dit onderzoek. De relatie met de KPI's is dat RODIN kan bijdragen aan verdieping en verbreding van het beeld van de stand van zaken van de digitale informatiehuishouding.

2. Bevindingen

In maart 2013 ontvingen alle deelnemende organisatie de in bijlage genoemde brief met een aantal vragen. Deze vragen zijn ontleend aan RODIN. Hieronder staan de bevindingen, die zijn gebaseerd op de gegeven antwoorden en de op basis daarvan gevoerde gesprekken met de betrokkenen.

2.1. Beleid en organisatie

Dit onderdeel van RODIN gaat in op de beleidsmatige en organisatorische eisen voor een goede digitale beheeromgeving. De NEN-ISO 15489-1 (NEN-ISO 15489-1:2001 nl, Informatie en documentatie - Informatie- en archiefmanagement*)* omschrijft het doel van beleid als volgt: Het doel van het beleid behoort te zijn de totstandkoming en het beheer van authentieke, betrouwbare en bruikbare archiefbescheiden, die bedrijfsfuncties en -activiteiten kunnen ondersteunen zo lang als nodig is. Beleid behoort te worden vastgesteld op het hoogste beslissingsniveau. Ook een goed functionerende organisatie is een randvoorwaarde voor de digitale beheeromgeving.

Organisatie A

Organisatie A heeft weliswaar een informatiebeleidsplan, maar de in RODIN beschreven onderdelen zijn hierin nog niet opgenomen. Bij de verdere ontwikkeling van de informatievoorziening gaat deze organisatie, waarbij het totale informatiebeheer centraal is georganiseerd, uit van een aantal principes om kwaliteit en integraliteit te kunnen waarborgen. Een principe dat aansluit bij dit onderzoek is, dat het informatieplan van toepassing is op alle in de organisatie voorkomende informatie, ongeacht vorm, herkomst of inhoud. Het gaat daarbij dus om documenten, databases, geo- en administratieve data, analoog (op papier) of digitaal, schriftelijk of multimedia etc. Deze vullen elkaar aan en vormen gezamenlijk de informatiehuishouding. Door de toenemende digitale informatie- en documentstromen neemt de vraag naar specialisten toe. Zij moeten volgens deze organisatie 'kennis hebben van documentmanagement, relevante wet- en regelgeving en de doelstellingen van de organisatie', aldus het informatiebeleidsplan. Zij starten in 2013 het 'Project Baseline' ('Baseline Informatiehuishouding Gemeenten'), waarin de hierboven genoemde aspecten uit RODIN worden opgenomen.

Organisatie B

Organisatie B zit in een proces van het centraliseren van diverse ondersteunende afdelingen. Zij zijn bezig met het ontwikkelen van informatiebeleid, waarin de aspecten uit RODIN worden opgenomen. De informatiebeheerders (lees: DIV- of archiefmedewerkers) voeren hierbij de regie, andere ondersteunende afdelingen worden hierbij betrokken, gevraagd om mee te denken en input te leveren. De organisatie constateert zelf dat zij onvoldoende in 'control' is als het gaat om sturing op het beleidsproces. En dat het daarbij kwetsbaar is bij politieke gevoelige dossiers in het bijzonder. Terecht wordt in het plan opgemerkt dat de wijze waarop de informatievoorziening hierin is beschreven alleen kans van slagen heeft als er een cultuuromslag tot stand komt en de medewerkers van de organisatie over een basisset aan digitale vaardigheden beschikt. Deze organisatie beschikt over een Documentair Structuurplan (DSP). Dit is een plan waarin zijn vastgelegd de organisatie van het informatiebeheer, de indeling van de gegevensbestanden en de manier waarop de onderdelen van de gegevensbestanden zijn gerangschikt.

Organisatie C

Organisatie C, waarbij informatiebeheerders en ICT organisatorisch van elkaar zijn gescheiden, heeft in 2004 een informatieplan opgesteld. Dat plan is sterk ICT-gericht en bevat geen enkele paragraaf over het bewaren van (digitale) informatie en bewaar strategieën. Beveiligingsbeleid wordt in het plan weliswaar zeer summier genoemd, maar taken en verantwoordelijkheden voor informatiebeveiliging zijn niet belegd. Hoewel deze organisatie geen beschrijving heeft tussen bedrijfsprocessen en opgenomen informatie, werken zij hier in het kader van het vaststellen van een informatiearchitectuur wel aan. Dit maakt echter geen onderdeel uit van het Informatiebeleidsplan. Er is wel een beveiligingsplan gemaakt, maar deze is verouderd en zal in 2013 geactualiseerd worden.

Organisatie D

Organisatie D kent een centrale afdeling voor informatiebeheer en ICT. Zij hebben een vastgesteld informatiebeleid, maar deze is niet meer actueel gelet op het digitaal werken. Zij zijn bezig met de realisatie van een handboek om hier opnieuw invulling aan te geven. Dit handboek wordt naar verwachting in 2013 vastgesteld. Volgens deze organisatie voldoet hun huidige werkwijze in basis aan de wettelijke eisen en voldoen gedigitaliseerde stukken aan de kwaliteitseisen die hieraan zijn gesteld. Op welke wijze wordt voldaan aan de wettelijke eisen zal beschreven worden in het handboek. De organisatie beschikt over een informatiebeveiligingsplan. Hierin zijn de taken en verantwoordelijkheden rondom informatiebeveiliging beschreven. In de tweede fase zal bij het opstellen van het handboek getoetst worden of het informatiebeveiligingsplan op alle punten aansluit bij digitaal werken en archiveren.

Organisatie E

Organisatie E, waarbij informatiebeheerders en ICT organisatorisch van elkaar zijn gescheiden, constateert in haar Informatiebeleidsplan dat er voor de realisatie van de ICT-doelen nog veel moet gebeuren. Dit betreft niet alleen techniek, maar vraagt vooral ook om samenhang met de wijze waarop er binnen deze organisatie gewerkt gaat worden. Daarom zal er bij de uitvoering een nauwe relatie zijn met de organisatieontwikkeling. In het plan staat expliciet vermeld dat voor wat betreft informatie rond zowel bedrijfsprocessen en projecten als de klantprocessen, digitaal centraal gearchiveerd gaat worden en conform de Archiefwet bewaard.

Organisatie F

Organisatie F heeft enkele jaren geleden met behulp van RODIN geïnventariseerd of zij hun informatiehuishouding ‘in control’ hebben. Hoewel de uitkomsten daarvan inmiddels enigszins gedateerd zijn is dit wel een basis geweest voor het opstellen van een ‘Strategisch informatiebeleidsplan’ waar zij mee bezig zijn. In 2013 is ervoor gekozen om ICT en informatiebeheer te decentraliseren. Ten tijde van het onderzoek was nog niet te zeggen of deze keuze een verbetering is of niet.

Organisatie G

Deze organisatie heeft een vastgesteld informatiebeleid, waarin hun archiefbeleid is opgenomen. In dit beleid is de relatie tussen bedrijfsprocessen en informatie deels opgenomen. 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 hebben zij niet. Een beschrijving van het beveiligingsbeleid waarin taken en bevoegdheden zijn vastgelegd is wel aanwezig.

Het algemene beeld voor wat betreft beleid en organisatie ziet er op basis van de ingevulde vragenlijst en de daarna gevoerde gesprekken als volgt uit:

	Ja	Nee	Deels
1. Heeft uw organisatie een door het bestuur en/of management vastgesteld informatiebeleid dat aansluit bij de geformuleerde organisatiedoelstellingen?	6	1	0
2. Worden hierin de volgende onderdelen tenminste vermeld?			
a. het voldoen aan de wettelijke eisen voor het bewaren van informatie	4	3	0
b. een beschrijving van de relatie tussen de bedrijfsprocessen en de opgenomen informatie	4	2	1
c. een beschrijving van of verwijzing naar de bewaar strategie van de organisatie die rekening houdt met conversie, migratie of emulatie in geval van veranderende (technische) omstandigheden	2	4	1
d. een beschrijving van het beveiligingsbeleid waarin taken en verantwoordelijkheden voor informatie beveiliging zijn belegd	5	2	0

2.2. Informatiebeheer

Dit onderdeel van RODIN gaat in op de manier waarop de archiefbescheiden worden beheerd in de Document Management System/Record Management Applicatie (DMS/RMA), maar ook in andere applicaties. Veel eisen zijn afgeleid van de NEN norm 2082. NEN 2082 is een Nederlandse norm met eisen voor functionaliteit van informatie- en archiefmanagement in programmatuur. Document Management is 'het geheel van mensen, middelen, kennis en procedures gericht op de creatie, het hergebruik en de opslag van documenten en de daarin opgenomen gegevens in de bedrijfsprocessen van organisaties.' Records Management is 'het geheel van mensen, middelen, kennis en procedures gericht op de duurzame opslag en raadpleging van documenten (en de daarin opgenomen gegevens) alsmede de daarbij behorende context, zodat deze documenten gebruikt kunnen worden als informatiebron in de bedrijfsprocessen van een organisatie en ter verantwoording en bewijs.'[1]

Organisatie A

Organisatie A converteert alle opgeslagen documenten in hun DMS naar de open standaard PDF/A. Het bestuur is hier mondeling akkoord mee gegaan en dit zal worden vastgelegd in het nog op te stellen Informatiebeleidsplan. Digitale archiefstukken kunnen op elke aggregatieniveau worden getoond (dossier, zaak, document). Door het toekennen van verschillende vertrouwelijkheidscodes wordt onderscheid gemaakt in de autorisaties. De bewaartermijn van de digitale archiefbescheiden worden op dossierniveau vastgelegd en overgeërfd op zaak type en document niveau. De bewaartermijnen worden nageleefd met inachtneming van de wettelijke selectietermijnen. Dossiers worden periodiek vernietigd na het opmaken van en vernietigingslijst. Overdragen en exporteren zijn niet van toepassing.

Organisatie B

Organisatie B heeft voor wat betreft de actuele en oorspronkelijke technische aard, ook van de hard- en softwareomgeving de eerste aanzetten vastgelegd in een Producten- en Dienstencatalogus. Deze zullen uiteindelijk in een applicatieregister worden opgenomen. De digitale archiefstukken in het DMS worden opgeslagen in PDF/A en het is mogelijk om door middel van een zoekopdracht alle archiefstukken en hun meta data te tonen. De digitale en analoge archiefbescheiden worden geselecteerd en gewaardeerd op dossierniveau. De archiefbescheiden en meta data in het DMS zijn gekoppeld aan het betreffende dossier. Er wordt dus niet stuksgewijs geselecteerd en vernietigd.

De daarvoor in aanmerking komende digitale en analoge archiefbescheiden, gekoppeld aan de te vernietigen dossiers, worden uiteindelijk na een zorgvuldige procedure daadwerkelijk vernietigd. Het is de informatiebeheerders bekend dat zich in andere informatiesystemen archiefwaardige informatie kan bevinden. In een memo aan het management heeft de archiefafdeling zijn zorg hierover uitgesproken. De afdeling wil de organisatie bewust maken dat ook deze informatie op basis van de selectielijst en onder verantwoordelijkheid van de informatiebeheerders wordt verwijderd (vernietigen of overbrengen). Tijdens overleggen in het kader van de Producten- en Dienstencatalogus wordt hier onder meer op gewezen. Bij het waarderen, selecteren en verwijderen (vernietigen, overbrengen, exporteren) wordt de vigerende selectielijst toegepast.

Organisatie C

Organisatie C legt voor uitgaande brieven de inhoud, structuur, verschijning en gedrag vast in een sjabloon. Van ingekomen documenten leggen zij de inhoud en de structuur vast. De verschijningsvorm is mogelijk af te leiden uit het bestandsformaat, maar geven zij niet specifiek aan in de meta data. In het DMS is bekend wanneer door wie en waarom archiefstukken zijn opgemaakt en ontvangen. Bij andere systemen in de organisatie is dit niet bekend. Dit geldt ook voor de samenhang met andere archiefstukken. In het DMS worden scans opgeslagen in PDF/A formaat. Digitaal binnengekomen bestanden slaan zij op zoals ze binnenkomen. Het bestuur van deze organisatie heeft overigens wel vastgesteld dat zij gebruik maken van open standaarden volgens het principe 'pas toe of verklaar'. In het DMS kunnen door middel van een zoekopdracht alle digitale archiefstukken en hun meta data op

[1] www.vbds.nl/bedrijfsprofiel

elk aggregatieniveau worden getoond, met inachtneming van autorisaties. Of dit in andere systemen ook kan is niet bekend. De bewaartermijn leggen zij in het DMS op document en/of dossierniveau vast. Alle documenten die binnen een periode van 10 jaar vernietigbaar zijn, plaatsen zij in numerieke series op 10 jaar en worden na 10 jaar vernietigd.

Organisatie D

Binnen het DMS beschikt organisatie D over een zaaktypencatalogus. Daarin zijn alle bedrijfsprocessen opgenomen die voorkomen binnen de organisatie. Hiermee is een directe relatie tussen de bedrijfsprocessen en de opgenomen informatie. Per zaak type is de bewaarstrategie gedefinieerd. Afhankelijk van het resultaat van een zaak worden termijnen voor overbrenging en vernietiging bepaald. Waar gewenst zetten of controleren zij de termijnen handmatig. Technisch beschikken zij hiermee ook over mogelijkheden om documenten binnen zaakdossiers op gezette momenten gedurende het proces geautomatiseerd om te zetten naar pdf/a formaat. Denk daarbij aan het omzetten van documenten ten behoeve van de dienstverlening of op moment van bevriezen van een zaakdossier.

Conversie heeft nog niet plaatsgevonden. Voor toekomstige conversies gaat deze organisatie hier gericht plannen voor opstellen op de dan ontstane situatie. Hier zal op voorhand niet in voorzien worden. Aan emulatie is tot op heden geen aandacht besteed. Ze leggen de inhoud digitaal vast in een database. Ze benoemen het documenttype. Ook de verschijningsvorm (pdf, doc. etc.) wordt vastgelegd. Het gedrag van de archiefstukken leggen ze vast in versiebeheer. Binnen een versie kunnen meerdere verschijningsvormen aanwezig zijn. De datum en opsteller worden vastgelegd. Ook de context van het archiefstuk wordt vastgelegd doordat een archiefstuk altijd in een zaak voorkomt. Voor wat betreft de samenhang met andere beheerde archiefstukken: het DMS is het archief. Alle archiefstukken zijn hierin opgeslagen binnen zaken. Samenhang met andere zaken is op verschillende manieren mogelijk. Allereerst kennen zij deel- en vervolgzaken een (archief)relatie met hoofdzaken. Verder worden zaken gerelateerd aan objecten. Denk daarbij aan burgers (GBA), bedrijven (Kvk/NHR), adressen (BAG) of andere zelf te definiëren registraties. Nieuwe functionaliteit van het DMS maakt het mogelijk om archivering te relateren aan de status van gerelateerde objecten. Denk daarbij aan bijvoorbeeld contracten (datum einde contract), medewerkers (datum uit dienst) of burgers (datum overlijden). Hiermee worden de functionele mogelijkheden voor het relateren van informatie sterk uitgebreid.

Voor wat betreft uitgevoerde beheeractiviteiten: alle handelingen ten aanzien van archiefstukken worden vastgelegd binnen het DMS. Per documentversie slaan zij meta data op. Ook op zaakniveau worden activiteiten vastgelegd. De actuele en oorspronkelijke technische aard, ook van de hard- en softwareomgeving: het formaat van archiefstukken wordt opgeslagen. Informatie over hard- en software nemen zij niet op. Stukken slaan ze op in PDF/A-formaat. Wanneer een stuk digitaal is opgemaakt, wordt daarnaast ook het oorspronkelijke formaat opgeslagen. Het bestuur heeft hier nog geen formele uitspraak over gedaan. Dit gaat gebeuren in een nog op te stellen handboek. De bewaartermijnen leggen ze vast op zaakniveau gebaseerd op de definitie binnen de zaaktypencatalogus. Deze definitie is opgesteld aan de hand van de selectielijst en de stukkenlijst.

Organisatie E

Organisatie E legt in hun DMS van elk stuk vast waar het over gaat en hoe het is ontvangen. Het origineel wordt als TIFF-bestand en als PDF/A-bestand bewaard. Voor documenten die de organisatie zelf aanmaakt wordt het WORD-bestand en een PDF/A-bestand bewaard. Hiervoor geldt dezelfde omschrijving van de inhoud. Daarbij worden de volgende meta data geregistreerd: datum ontvangst, datum poststuk (de datum die de afzender aangeeft als creatiedatum), de afzender en onderwerp van het document en welk organisatieonderdeel het document in behandeling neemt.

Bij elk document wordt/kan worden aangegeven in welk dossier het thuis hoort. Ook is het mogelijk om relaties tussen documenten/cases en personen te leggen. Behalve versiebeheer is in het DMS ook na te gaan wie welk stuk wanneer heeft afgehandeld, dan wel als laatste heeft bewerkt. En wanneer een relatie is gelegd en het document eventueel in het dossier is geboekt. De hard- en software om-

geving is up-to-date. De server is een dedicated server waar verder geen taken op worden uitgevoerd, Qua software omgeving kijkt deze organisatie bij nieuwe versies of deze problemen oplossen en of nieuwe functionaliteiten toegevoegd zijn. Hoewel zij geen 'officiële' digitale handtekening gebruiken, gebruiken zij in sommige gevallen een gescande handtekening bij ontvangstbevestigingen, uitspraken bezwaarschriften en eventueel informerende brieven aan burgers en instanties.

Organisatie F

Organisatie F maakt in haar DMS gebruik van de zogenaamde kenniskaart, een ordening die samen met de organisatie is opgesteld, met vier lagen. De vierde laag is het dossier. Aan het dossier wordt een bewaartermijn gekoppeld. Voor het toekennen van bewaartermijnen maakt deze organisatie gebruik van de vastgestelde selectielijst. Alle stukken worden gekoppeld aan de kenniskaart (hier ook procesgericht). Daarnaast maakt het DMS gebruik van een vastgesteld proces voor Subsidies en Vergunningen. Zij hebben inmiddels een machtiging voor vervanging van papieren bescheiden door digitale gekregen voor de periode vanaf 1 januari 2013. De wijze waarop is beschreven in een handboek.

Alle gescande documenten worden opgeslagen als PDF/A formaat. Indien kleur van betekenis is wordt in kleur gescand. Voor wat betreft de vastlegging van meta data: voor de inhoud gebruiken zij bij een zaakomschrijving de zogenaamde gehopte methode. Voor de structuur de kenniskaart. De verschijningsvorm is een ingekomen- of uitgaande brief. Tot slot het gedrag: in de historie van de zaak wordt verschillende informatie vastgelegd waaronder afdeling, behandelaar, datum parafering, datum verzending etc. Bij uitgaande brieven worden automatisch meta data toegevoegd (behandelaar, verzenddatum) en er is versiebeheer: Alle versies van uitgaande documenten in het DMS worden bewaard. Wanneer een document wordt uitgecheckt, aangepast en weer ingecheckt wordt een nieuwe versie aangemaakt. Bij het archiveren worden alle versies bewaard. Er is geen limiet.

In het DMS is herleidbaar en (veilig) geborgd over welke versies de beslissingsbevoegde een besluit heeft genomen. Ze kunnen achterhalen op welke versie van het document de beslissingsbevoegde zijn paraaf heeft gezet. Ook kunnen ze achterhalen of de inhoud van het document is gewijzigd na het paraferen. Door verschillende versies met elkaar te vergelijken, kunnen ze zien wat er gewijzigd is. Daarnaast is te zien wie een versie heeft ingecheckt en wanneer dit is gebeurd. Zaken met onderliggende documenten worden in hetzelfde dossier geordend. Controle op volledigheid van aangeleverde fysieke en digitale stukken: ingekomen stukken worden opgeslagen in PDF-A. Uitgaande stukken worden gescand en eveneens opgeslagen als PDF-A. Aan elk dossier wordt handmatig een handeling van de selectielijst en een bewaartermijn gekoppeld. Op dit moment zijn ze bezig om de procedure tot daadwerkelijk vernietiging op te zetten.

Organisatie G

Van alle archiefstukken legt deze organisatie tenminste de volgende informatie vast in meta data: inhoud, structuur, verschijningsvorm en gedrag. Bovendien wanneer, door wie en waarom de archiefstukken zijn opgemaakt. Niet vastgelegd worden de samenhang met andere beheerde archiefstukken, uitgevoerde beheeractiviteiten en de actuele en oorspronkelijke technische aard. Dit geldt ook voor de aard van de digitale handtekening en de wijze van versleuteling (algoritme) en descryptiesleutel. Digitale archiefstukken worden opgeslagen in pdf/a formaat. Maar deze stukken (inclusief hun meta data) kunnen niet volledig door middel van een zoekopdracht op elk aggregatieniveau worden getoond. Ook niet met inachtneming van autorisaties. Ook de bewaartermijn van digitale archiefbescheiden wordt niet in alle gevallen op elk aggregatieniveau vastgelegd. Dit geldt ook voor het naleven van de bewaartermijnen met inachtneming van de wettelijke selectietermijnen, procedures en vervolgacties.

Het algemene beeld voor wat betreft Informatiebeheer ziet er op basis van de ingevulde vragenlijst en de daarna gevoerde gesprekken als volgt uit. Hierbij met de kanttekening dat dit beeld alleen betrekking heeft op informatie die is opgeslagen in Document Management Systemen en niet in andere applicaties.

	Ja	**Nee**	**Deels**
1. Wordt van alle archiefstukken tenminste de volgende informatie in de meta data vastgelegd?			
a. Inhoud, structuur, verschijningsvorm en gedrag	6	0	1
b. Wanneer, door wie en waarom de archiefstukken zijn opgemaakt en werden ontvangen	7	0	0
c. Samenhang met andere beheerde archiefstukken	6	1	0
d. Uitgevoerde beheeractiviteiten	6	1	0
e. Actuele en oorspronkelijke technische aard, ook van de hard- en softwareomgeving	4	2	1
f. Aard van de digitale handtekening (indien aanwezig)	0	6	1
g. Wijze van versleuteling (algoritme) en decryptiesleutel (indien van toepassing)	0	7	0
2. Worden digitale archiefstukken opgeslagen in door het bestuur aangewezen, valideerbare en volledig gedocumenteerde bestandsformaten, die voldoen aan een open standaard, tenzij dit redelijkerwijs niet kan worden verlangd?	6	0	1
3. Kunnen door middel van een zoekopdracht alle digitale archiefstukken en hun meta data op elk aggregatieniveau worden getoond, met inachtneming van autorisaties?	5	1	1
4. Wordt de bewaartermijn van digitale archiefbescheiden automatisch op elk aggregatieniveau vastgelegd?. En worden die bewaartermijnen nageleefd met inachtneming van de wettelijke selectietermijnen, procedures en vervolgacties (vernietigen, overdragen of exporteren)?	5	0	2

2.3. ICT-beheer en beveiliging

ICT-beheer en beveiliging, is de derde component van RODIN, die bepaalt of er een veilige beheer-omgeving is voor de digitale archiefstukken. Hoewel ICT al weer behoorlijk wat jaren deel uitmaakt van het archiveringssysteem is in de op de Archiefwet gebaseerde regelgeving nog geen normering opgenomen ten aanzien van 'goed ICT-beheer. ICT is echter een bepalende factor bij het goed functioneren van het systeem en hiermee voor de betrouwbaarheid en raadpleegbaarheid van de archiefbescheiden.

Organisatie A

Organisatie A doet aan systematische risicoanalyse en heeft de wijze waarop dit gebeurt vastgelegd in het Informatiebeveiligingsplan. De serverruimte wordt 24 uur per dag gekoeld, met twee condensorunits op het dak. Alarm en brandmeldingsvoorziening en toegangscontrole is uitbesteed aan een externe partij. Een noodstroomvoorziening is aanwezig in de hoedanigheid van een dieselaggregaat, die jaarlijks wordt getest en onderhouden door een externe partij.

Organisatie B

Deze organisatie gaf aan dat zij hun informatiebeveiliging op orde hebben, zonder verder in detail te treden.

Organisatie C

Organisatie C geeft aan dat zij weliswaar aan systematische risicoanalyse doen, maar dat dit waarschijnlijk onvoldoende is. Eén keer per jaar wordt er van buitenaf een penetratietest uitgevoerd. Verder moeten gebruikers wachtwoorden periodiek wijzigen en moet er zorgvuldiger met wachtwoorden worden omgegaan (briefjes op beeldscherm).

Organisatie D

Deze organisatie gaf aan dat zij hun informatiebeveiliging op orde hebben, zonder verder in detail te treden.

Organisatie E

Organisatie E gaf aan dat op alle locaties gebruik gemaakt wordt van toegangscontrole door middel van een pas system. En dat gebruikers toegang tot het netwerk hebben via ‘logon’. De serverruimte is aangepast aan de laatste eisen die hieraan gesteld worden. Alleen mensen met de juiste autorisatie mogen de serverruimte betreden. Ook vind er regelmatig controle plaats op de productieserver, waar onder andere het volgende wordt gecontroleerd: of ingeplande taken worden uitgevoerd, er foutmeldingen zichtbaar zijn in de managementconsole, wat het geheugen- en processorgebruik van de server is en wat de status van het RAID 5 volume[2] is. Deze organisatie maakt dagelijks een back-up van de productieomgeving die met enige regelmaat wordt gecontroleerd. In de serverruimte is een adequate klimaatbeheersing en toegangscontrole aanwezig.

Organisatie F

Deze organisatie doet deels aan een systematische risicoanalyse voor factoren als data, systemen, personeel, fysieke locatie en beveiligingseisen. Hiervoor is een methodiek voorhanden. Zij hebben serverruimtes die voldoen aan intern opgestelde kwaliteitseisen gebaseerd op de Code voor Informatiebeveiliging.

[2] Een RAID 5 volume is een afkorting van redundant array of independent disks, ook bekend als redundant array of inexpensive disks (of drives). Het is de benaming voor een set methodieken voor fysieke data-opslag 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

Organisatie G

Deze organisatie doet aan systematische risicoanalyse voor factoren als data, systemen, personeel, fysieke locatie en beveiligingseisen. En zij beschikken over een adequate serverruimte met onder meer klimaatbeheersing, alarm en brandmeldvoorziening, ordelijke bekabeling en noodstroomvoorziening.

Het algemene beeld voor wat betreft ICT-beheer en- beveiliging ziet er op basis van de ingevulde vragenlijst en de daarna gevoerde gesprekken als volgt uit:

	Ja	Nee	Deels
1. Doet u aan een systematische risicoanalyse voor factoren als data, systemen, personeel, fysieke locatie en beveiligingseisen?	5	0	2
2. Heeft u een adequate serverruimte met onder meer klimaatbeheersing, alarm en brandmeldvoorziening, toegangscontrole, ordelijke bekabeling en noodstroomvoorziening (UPS)?	7	0	0

3. Conclusies

Doel van dit onderzoek was om te kijken in hoeverre het digitale geheugen van overheden in Noord-Nederland op orde is en om inzicht te verkrijgen in de juridische waarde, de bruikbaarheid en de staat van de duurzame toegankelijkheid van de digitale informatie. Centrale vraag hierbij was welke maatregelen (eventueel) nodig zijn om de beheeromgeving bij overheidsorganisaties hiervoor geschikt te maken. Secundaire doelstelling was om bewustwording te kweken c.q. te vergroten bij organisaties om hun informatiehuishouding (beter) op orde te krijgen met het oogmerk verantwoording te kunnen afleggen van genomen besluiten en het gevoerde beleid, zaken te kunnen reconstrueren en voor een deel vanuit cultuurhistorisch belang.

Op basis van dit onderzoek concluderen wij het volgende:

Organisaties voldoen deels aan wettelijke verplichtingen voor duurzame toegankelijkheid van digitale informatie

Op het gebied van ICT-beheer en beveiliging lijken organisaties hun zaakjes deels op orde te hebben. Positief is dat er minimaal één organisatie is die voldoet aan de norm NEN-ISO/IEC 17799. Dat betekent dat zij op dit punt technisch gezien klaar lijken te zijn voor het op termijn inrichten van een zogenaamd E-depot. Het is echter de vraag of organisaties hun informatiebeveiliging procesmatig zodanig ingericht hebben, zodat zij de beveiligingsmaatregelen uit die norm kunnen effectueren, zoals NEN-ISO/IEC 27001 verplicht voor overheden. Deze norm specificeert eisen voor het vaststellen, implementeren, uitvoeren, controleren, beoordelen, bijhouden en verbeteren van een gedocumenteerd Information Security Management System (ISMS) in het kader van de algemene bedrijfsrisico's voor de organisatie.

Ook voor wat betreft ‘Beleid en organisatie’ zijn er organisaties die al stappen maken naar duurzame digitale toegankelijkheid, dan wel het op korte termijn gaan doen. Dat geldt vooral voor die organisaties waarbij ICT en informatiebeheer deel uitmaken van één afdeling. Duurzame digitale toegankelijkheid wordt hier, net als ICT, als strategisch onderwerp gezien. Eén organisatie heeft ervoor gekozen de ‘Baseline Informatiehuishouding Gemeenten’ te gaan gebruiken om hun informatiehuishouding verder op orde te krijgen. Zij verdient hiervoor een compliment en kan als voorbeeld dienen voor andere organisaties. Bij de organisaties waar het huidige informatiebeleidsplan nog sterk ICT gericht is, lijkt wel het besef aanwezig, dat bij het opstellen van een nieuw plan duurzame digitale toegankelijkheid een belangrijk onderwerp zal moeten zijn.

Het al dan niet voldoen aan wettelijke verplichtingen lijken organisaties echter niet echt als een probleem te ervaren. En hoewel die verplichtingen natuurlijk nooit op doel op zich mogen zijn, is dit zorgelijk. Immers, organisaties die van burgers verwachten dat zij zich houden aan ‘de Wet’ en dit zelf (deels) niet doen, dragen niet bij aan een betrouwbare overheid. Los van imagoschade, lopen zij hiermee zelf grote financiële en juridische risico’s.

Wij zien positieve ontwikkelingen binnen informatiebeheer in Document Management Systemen, het informatiebeheer daarbuiten is zorgwekkend

Ondanks bovenstaande kritische opmerking zien wij in de praktijk op het gebied van informatiebeheer positieve ontwikkelingen. Tenminste, als wij ons beperken tot het Document Management Systeem (DMS). Bij één organisatie is digitale informatie inmiddels leidend ten opzichte van papier. Een moedige stap die op termijn leidt tot een situatie waar én de bedrijfsvoering én de bewijsvoering én het cultuurhistorisch belang bij gebaat zijn. Volgens deze organisatie kan het DMS met een aantal aanpassingen als voortzetting van de bedrijfsvoering dienen als E-depot. De basis daarvoor is ED 3 Eisen Duurzaam Digitaal Depot.

Het is echter zorgwekkend gesteld met het overgrote deel van informatie die zich buiten het DMS bevindt. Hierop hebben de organisaties vanuit het perspectief van de Archiefwet geredeneerd geen grip. Dit blijkt niet alleen uit de antwoorden op onze vragen, die zich beperkten tot hun DMS terwijl in onze brief duidelijk was aangegeven ook andere bedrijfsapplicaties bij de beantwoording te betrekken. Ook uit de gesprekken kwam naar voren dat deze informatie niet 'in control' is. Het gaat hierbij om informatie in bedrijfsapplicaties en databases (bijvoorbeeld personeelsinformatiesystemen, financiële systemen), e-mail, informatie op websites, mobiel berichtenverkeer, werk gerelateerde informatie op mobiele apparaten en tablets, digitale fotografie, informatie gevormd bij ketenvragen, SharePoint etc. etc. Het gevolg van het niet 'in control' hebben kan zijn dat er (bestuurlijke) besluiten kunnen worden genomen of wellicht genomen zijn op basis van onvolledige en/of onjuiste informatie. Maar ook dat er onnodig veel, dus dure, opslagcapaciteit gebruikt wordt. Ook is er geen tot weinig opruimdiscipline. Hierdoor neemt de hoeveelheid informatie waarin gezocht moet worden toe. En daardoor de kans dat relevante informatie gevonden af. Uit onderzoek door het Amerikaanse onderzoeksbureau International Data Corporation (IDC) blijkt bovendien dat kenniswerkers ongeveer 20% van hun tijd besteden aan het zoeken van de juiste informatie. Dat is (voor het gemak) 4,5 uur per medewerker per week.

Sommige organisaties zien digitalisering als alleen een technische uitdaging

Het is zorgwekkend dat sommige organisaties digitalisering als alleen een technische uitdaging zien. Uiteraard is een goed werkende techniek essentieel. Maar ICT is 'slechts' een enabler. Het maakt dingen mogelijk die anders niet mogelijk zouden zijn. De echte uitdaging is van organisatorische aard. Sommige organisaties onderschatten het belang van een kwalitatief en kwantitatief goed uitgeruste afdeling informatiebeheer (lees: DIV). De (digitale) archieffunctie staat zelden in de schijnwerpers, tenzij er iets misgaat in de bedrijfs- en of bewijsvoering. Dan blijkt juist die archieffunctie vaak de achilleshiel. Kortom, archieven (papier of digitaal) zijn niet sexy genoeg voor bestuur en management van organisaties, terwijl het op orde zijn van die informatie essentieel is voor een efficiënte bedrijfsvoering. Daar staat tegenover dat afdelingen informatiebeheer zich vaak ook niet voldoende profileren om aan te geven waar hun meerwaarde kan liggen. Ook hebben de organisaties te maken met een aantal belemmerende factoren. Denk aan bezuinigingen, interne reorganisaties, 'eiland denken', onvoldoende draagvlak bij proceseigenaren en (bij gemeenten) herindelingen. En taken die vanuit het Rijk naar lagere overheden worden overgeheveld hebben uiteraard impact op elke organisatie. Dat geldt ook voor de ambitie van het Rijk dat in 2017 alle diensten door burgers digitaal afgenomen moeten kunnen worden.

Organisaties hebben behoefte aan concrete handvatten

Uit dit onderzoek is duidelijk naar voren gekomen dat organisaties vooral behoefte hebben aan concrete handvatten waarmee zij direct aan de slag kunnen en voorbeelden ter inspiratie. Dat betekent dat de grondhouding positief lijkt te zijn om stappen te zetten en zij, binnen de mogelijkheden die zij hebben, graag aan de slag willen gaan.

4. Aanbevelingen en ‘best practices’

Benader duurzame digitale toegankelijkheid als een organisatorische uitdaging en niet als een technisch probleem

Duurzame digitale toegankelijkheid is volgens ons geen technisch probleem, zoals vaak verondersteld, maar een organisatorische uitdaging. Dat betekent dat elke organisatie zich bewust moet zijn van het belang van duurzame toegankelijkheid van digitale informatie. Daarbij is het essentieel om een communicatiestrategie te ontwikkelen over de manier waarop dit onder de aandacht kan worden gebracht binnen de organisatie. Ons advies hierbij is om primair te focussen op de zaken die wel goed gaan en op de voordelen voor de bedrijfs- en bewijsvoering. En niet direct van de kelder naar de zolder te springen. Verder, benader zaken die beter kunnen op een positief kritische manier en richt je pas als het echt niet anders kan op de wettelijke verplichtingen. In feite gaat het hier dus vooral gedragsbeïnvloeding. C'est le ton qui fait la musique, ofwel het gaat er niet om wat je zegt, maar hoe je het zegt.

Versterk de rol van informatiebeheerders

De inbreng van de informatiebeheerders (lees: DIV-afdelingen) is vaak nog te passief. Het is essentieel dat zij een actievere rol gaan spelen, zodat elke organisatie blijft beschikken over authentieke, integere, betrouwbare en bruikbare digitale informatie. Ofwel, informatiebeheerders moeten actief oplossingen aanbieden voor het duurzaam toegankelijk houden van digitale informatie. Daarmee realiseren zij een toegevoegde waarde voor de gehele organisatie. En alleen dan raken zij betrokken bij de vele veranderingstrajecten en is er bereidheid om andere wegen in te slaan. Uitgaande van een aantal basisprincipes van de archiefwetenschap en de vele normen als fundament, komt het er dan op aan om dit in concrete, praktische en efficiënte archiefoplossingen te vertalen. En hiervoor zijn ‘best practices’ beschikbaar (zie hierna).

Voorwaarde is wel dat informatiebeheerders moeten beschikken over nieuwe competenties. Zowel op vakinhoudelijk gebied, als een andere houding en het bewustzijn dat aspecten anders zijn in een digitale omgeving in vergelijking tot de traditionele. In het vakgebied informatiemanagement gerenommeerde instituten organiseren hier workshops, cursussen en trainingen voor. Wij adviseren daarom dat informatiebeheerders opleidingen gaan volgen om hun kennis van duurzame digitale toegankelijkheid op peil te brengen. Hierdoor kunnen zij een gelijkwaardige partner worden van ICT-specialisten en kunnen beide disciplines zich vanuit hun eigen vakgebied integraal bezighouden met het op orde krijgen en houden van hun digitale informatiehuishouding. Bij voorkeur worden beide disciplines centraal aangestuurd.

Een andere voorwaarde is dat informatiebeheerders en ICT-specialisten, maar ook de ‘organisatie’ elkaars taal leren spreken. ‘Een zelfde object, gebeurtenis of wat dan ook kan vanuit verschillende achtergronden benaderd worden. Dat levert dan per achtergrond eigen gezichtspunten, benaderingswijzen en bijbehorend jargon. Deze verschillen kunnen vaak aanleiding zijn tot spraakverwarring, elkaar niet begrijpen, verschil van inzicht en langs elkaar werken zonder van ieders bestaan af te weten en wat niet meer. Dit komt op veel terreinen voor en natuurlijk ook binnen het informatiebeheer’, aldus gemeentearchivaris en informatieadviseur Rienk Jonker van de gemeente Leeuwarden.

Breng digitale huishouding in kaart

Door de digitale huishouding in kaart te brengen is te bepalen welke informatie essentieel is voor een goede bedrijfs- en bewijsvoering. Hiervoor zijn diverse hulpmiddelen beschikbaar, waaruit een keuze gemaakt kan worden welke het beste past bij elke afzonderlijke organisatie.

Een handig hulpmiddel om dit snel en efficiënt te doen is RODIN, dat als basis heeft gediend voor dit onderzoek. In RODIN zijn eisen beschreven voor het beleid en organisatie, voor het informatiebeheer en voor ICT-beheer en beveiliging. Het is een handzaam instrument voor een adequate en toekomstbestendige inrichting van digitale beheeromgevingen. In de vorm van een checklist kunnen informatiemanagers, informatiebeheerders, archiefinspecteurs en auditors meten in welke mate hun organisatie 'in control' is als het gaat om de verschillende vastgestelde normen en standaarden op het gebied van digitale informatievoorziening. Bij het invullen van deze checklist kan paragraaf 3.2.4 van de VNG handreiking "Horizontale verantwoording Archiefwet 1995 via Kritische Prestatie Indicatoren (KPI's)" als ondersteuning dienen. Er zijn diverse praktijkvoorbeelden beschikbaar van onder meer de gemeenten Tiel, Heemstede en Moerdijk.

Ook goed bruikbaar is de 'Baseline Informatiehuishouding Gemeenten' Deze is bedoeld om gedetailleerd in kaart te brengen in hoeverre de digitale informatiehuishouding 'in control' is. De baseline is in opdracht van de Vereniging van Nederlandse Gemeenten (VNG) ontwikkeld. Het is een handleiding voor gemeenten, maar ook voor andere overheidsorganen, om grip en sturing te krijgen op het informatiebeheer. De richtlijn verbindt het informatiebeheer, inclusief archivering, met de doelstellingen en werkwijze van een modern elektronische overheid. Risicomanagement en kwaliteitsbeleid vormen belangrijke uitgangspunten. Doel is de toegankelijkheid en de betrouwbaarheid van informatie te bevorderen. Voor provincies is overigens ook een baseline aanwezig, die minder uitgebreid is dan die van gemeenten, maar desalniettemin goed bruikbaar.

Een ander hulpmiddel is het Kwaliteitssysteem volgens de ISO-norm 'Managementsystemen voor archivering'. Deze is bedoeld als hulpmiddel voor organisaties om de naleving van de eisen voor archief- en informatiemanagement uit de NEN-ISO 15489:2001 nl te sturen en te beheersen. Dit wordt gedaan door het gebruik van:

a. vastgestelde rollen en verantwoordelijkheden;
b. systematische processen;
c. meting en evaluatie;
d. beoordeling en verbetering.

Goed bruikbaar lijkt ook het (concept) 'Risicomodel informatiebeheer' dat de gemeente Rotterdam in 2013 heeft ontwikkeld. Doel hiervan is dat het proceseigenaren aan de hand van een risicoanalyse stap voor stap helpt een beheerregime op maat voor procesinformatie te kiezen bij het (her)inrichten hun processen. Uitgangspunt bij deze methode is dat het proces leidend is: de aard van het proces bepaalt grotendeels de eisen die aan de informatie gesteld worden. Procesinformatie waarderen zij vanuit vier perspectieven:

a. Proceswaardering: belang en type proces;
b. Procescontext: relevante wet- en regelgeving;
c. Procesverloop: betrokkenen, afhankelijkheden;
d. Procesinformatie: documentflow.

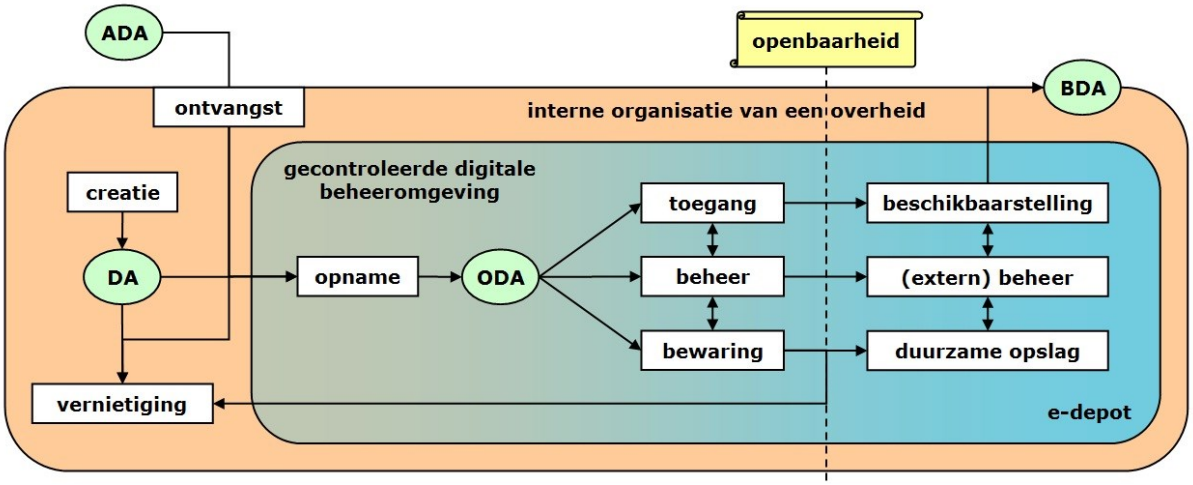
Deze vier factoren leiden tot een vijfde stap, waarbij aan een proces een risicoklasse wordt gegeven.

Onderzoek de mogelijkheden om te komen tot een extra voorziening in de eigen digitale beheeromgeving die openbare raadpleging en langdurige bewaring mogelijk maakt

Elke overheidsorganisatie staat de komende jaren voor de uitdaging hun digitale informatie duurzaam te beheren en te bewaren. Niet alleen omdat het wettelijk verplicht is, maar vooral om te komen tot een situatie waar én de bedrijfsvoering én de bewijsvoering én het cultuurhistorisch belang bij gebaat zijn. Minister Bussemaker (OCW), het Interprovinciaal Overleg (IPO), de Unie van Waterschappen (UvW) en de Vereniging van Nederlandse Gemeenten (VNG) hebben hiervoor in december 2012 een 'Archiefconvenant' gesloten. Belangrijke doelen voor 2016 zijn een landelijk dekkend netwerk van elektronische depotvoorzieningen voor alle overheden (e-depots), tijdiger overdracht van relevante overheidsinformatie naar een archief (nu kan dat nog 20 jaar of meer duren) en digitale toegang tot archieven van de overheid

Het is echter zeer de vraag of deze doelen haalbaar zijn voor overheden in Drenthe, Fryslân en Groningen. In tegenstelling tot andere provincies beschikken bijna alle overheden in deze provincies namelijk niet over een dekkend net van archiefdiensten. Hierdoor is er een grotere afstand tussen lokaal bestuur en een mogelijk te kiezen extern e-depot door onvoldoende interne deskundigheid op archiefterrein. Uitbreiding van de eigen beheeromgeving met extra functionaliteit is daarom volgens ons vanuit actief zorgdragerschap in de noordelijke context de beste oplossing. Bovendien kan hiermee in eigen tempo, op eigen schaal en kostenplaatje gewerkt worden. Uiteraard kunnen het ontwikkelen van extra functionaliteiten gezamenlijk plaatsvinden, immers elke organisatie staat voor dezelfde uitdaging. De basis voor deze uitbreiding van de eigen beheeromgeving is ED 3 Eisen Duurzaam Digitaal Depot.

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 Word bestanden, 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) meta data voor het ODA, maar kan ook zelf als nieuwe representatie van het ODA weer opgenomen worden in het eDepot.



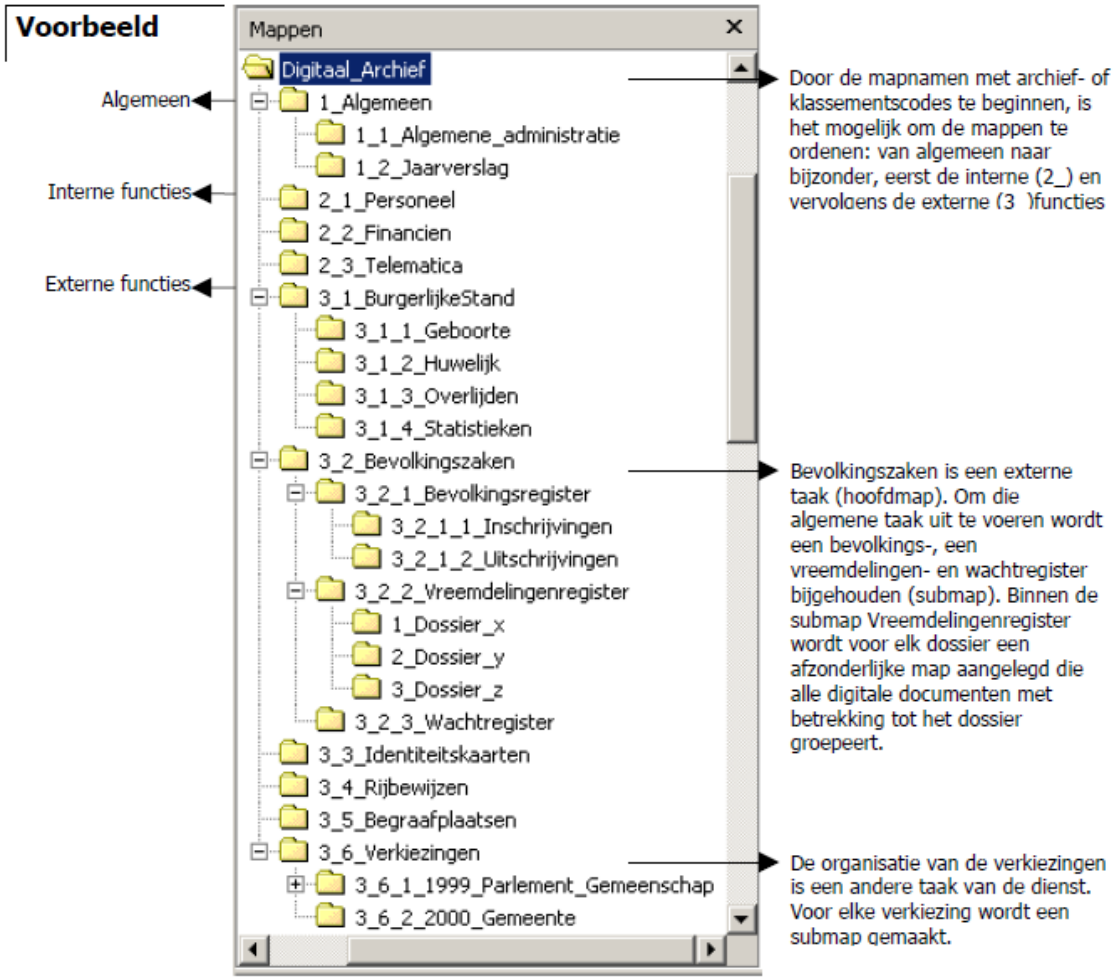
Vergaar en deel kennis en maak gebruik van ervaringen bij andere organisaties

Omdat veel organisaties behoefte hebben aan concrete handvatten noemen wij hier een aantal 'best practices'. Bovendien verwijzen wij naar websites met achtergrondinformatie. Het is hierbij wel van belang om te realiseren dat de 'best practices' middelen zijn en geen alomvattende oplossingen bieden voor duurzame digitale toegankelijkheid. "De kern van informatiemanagement ligt in de informatiewaardeketen; het informatieproces van begin tot bittere eind. De informatiewaardeketen regelt vier dimensies: kwaliteit, context, relevantie – de economische, bedrijfsmatige of cultuurhistorische waarde – en het voortbestaan van informatie. Het in stand houden van informatie is ons doel, dat mogen we nooit uit het oog verliezen." Aldus dr. Geert-Jan van Bussel, lector Digital Archiving & Compliance aan de Hogeschool van Amsterdam op 16 oktober 2012 uitgesproken in zijn Lectorale rede 'Archiving should be just like an Apple, en acht andere nuttige (?) stellingen'.

De gemeente Putten (Gld.) is onder de noemer 'Ready, steady, go!' al enkele jaren bezig de archivering van start tot finish onder controle te krijgen. Hun werkwijze is het best te omschrijven als 'pragmatisch, korte lijnen, smart en keep it simple, recht op het doel af, doen wat je moet doen en risicobeheersing. Zij bouwen vanaf de bron alle informatie op, zodat aan het eind van het werkproces zo weinig mogelijk handelingen nodig zijn om aan de eisen en termijnen van bewaring wordt voldaan. Al een aantal jaren werkt deze gemeente aan een cultuuromslag van de organisatie. Daar ligt de grootste uitdaging. En om dat te bereiken richten zij een stap voor stap een digitale informatiestructuur in die aansluit op de bestaande basis. Belangrijk hierbij is dat medewerkers voldoende geschoold zijn.

Om de kwaliteit te borgen heeft de gemeente Putten in 2011 een Documentair Structuurplan (DSP) opgesteld. Uitgangspunten hierbij zijn onder andere de BAC, de begroting en zaakgericht werken. De volgende stap is de realisatie van een e-depot. Als middel en niet als doel. Het doel is immers het in stand houden van informatie. Zij zien het e-depot als meer dan een software-oplossing. Het is onderdeel van, of sluit aan op hun DMS, maar moet ook kunnen aansluiten aan andere applicaties/oplossingen. Het idee is dat andere organisaties kunnen aanhaken bij hun e-depot. Het delen van gebruik betekent dan dat ook de kosten en inzet voor beheer gedeeld kunnen worden. De gemeente Putten ziet het e-Depot als logische en noodzakelijke vervolgstap om in control te komen en te blijven met de gehele informatiehuishouding. Er is een business case uitgevoerd die hun inzicht heeft gegeven en de noodzaak van aanschaf van het e-Depot heeft onderstreept.

Heel veel informatie bij organisaties wordt opgeslagen in Windows verkenner mappen. Dit is waar medewerkers vertrouwd mee zijn. Alleen deelt iedereen dit op zijn/haar eigen wijze in, waardoor informatie voor anderen vaak moeilijk is terug te vinden. Het document 'Mappenstructuur en bestandsnamen voor digitale documenten' op de website van het Expertisecentrum 'Digitale archivering in/voor Vlaamse instellingen en diensten' (eDavid), bevat een aantal richtlijnen en aanbevelingen voor het uitwerken van een goede mappenstructuur en het toekennen van duidelijke bestandsnamen. Het eindigt met een aantal aanbevelingen voor de opslag van digitale documenten. Inmiddels is hier ook een zogenaamde recordmanagementtool voor op de markt, waarvan hierna een voorbeeld staat vermeld.



Pioniers van een E-depot in Nederland zijn de gemeenten Rotterdam en Amsterdam. Maar ook op de website van het Expertisecentrum 'Digitale archivering in/voor Vlaamse instellingen en diensten' (eDavid) is veel informatie beschikbaar.

Voor het archiveren van ruimtelijke digitale plannen heeft Geonovum een handreiking geschreven. Geonovum, een organisatie die geo-informatie van de publieke sector voor een breed publiek toegankelijk maakt, ontwikkelt en beheert de standaarden die daarvoor nodig zijn. Doel van de handreiking is een aanzet te geven voor personen die betrokken zijn bij het archiveren van data en zij die betrokken zijn bij de creatie en vaststelling van het ruimtelijke plan: ruimtelijke ordenaars, informatieverzorgers en archivarissen bij een gemeente, provincie en het rijk. Een aanzet om het werkproces zo in te richten dat ruimtelijke plannen worden gearchiveerd, conform de voorgeschreven wet- en regelgeving. De handreiking richt zich op het archiveren van de samenhangende set bronbestanden.

Heel veel achtergrondinformatie over duurzame toegankelijkheid van digitale informatie is te vinden op www.nationaalarchief.nl/informatiebeheer-archiefvorming, http://labyrinth.rienkjonker.nl. Maar ook de IWA-base, een kennisbank voor informatiewetenschap, archiefbeheer en archiefrecht bevat veel relevante informatie.

Bijlage Brief aan deelnemende organisaties

Aan:

Datum:

Onderwerp: Grondslagonderzoek naar digitale archivering

Geacht xxxx

Digitale informatie wordt steeds belangrijker in onze globale maatschappij. Niet alleen voor de individuele gebruiker gaan de ontwikkelingen bijna onnavolgbaar snel, ook organisaties en overheden krijgen steeds meer te maken met digitale bedrijfsinformatie en bijbehorende omgangsvormen. Hoe is betrouwbaarheid, volledigheid, authenticiteit en toegankelijkheid van digitale informatie te waarborgen? Recent onderzoek door de Erfgoedinspectie bij 23 Rijksoverheden heeft uitgewezen dat het digitale geheugen van de centrale overheid nog niet op orde is. Dit ondanks alle inspanningen die er de afgelopen jaren zijn verricht. U kunt het onderzoek, getiteld “Beperkt houdbaar? Duurzame toegankelijkheid in een digitale omgeving bij de rijksoverheid”, downloaden op www.erfgoedinspectie.nl.

Is uw digitale geheugen op orde?
De logische vraag is in hoeverre het digitale geheugen van lagere overheden op orde is. Dit gaan wij nader onderzoeken bij een aantal provincies, gemeenten en waterschappen in Drenthe, Fryslân en Groningen, als grondslag voor het thema ‘een duurzame en adequate digitale beheer- en bewaaromgeving’ voor het Interbestuurlijk archieftoezicht. Voor dit onderzoek vragen wij uw medewerking door de in de bijlage gestelde vragen te beantwoorden en uiterlijk 1 maart te retourneren. Deze vragen zijn ontleend aan RODIN, Referentiekader Opbouw Digitaal Informatiebeheer. Mocht u niet willen medewerken of het genoemde tijdstip u ongelegen komt, dan kunt u contact opnemen met ons opnemen. Wij adviseren u om bij de beantwoording van de vragen gebruik te maken van de informatie die in paragraaf 3.2.4 van de VNG handreiking “Horizontale verantwoording Archiefwet 1995 via Kritische Prestatie Indicatoren (KPI’s)” staat vermeld. Het gaat hierbij om alle digitale archiefbescheiden. U kunt daarbij denken aan applicaties met financiële en persoonsgegevens, CAD- en GIS-systemen, de e-mailomgeving, websites en persoonlijke- en gemeenschappelijke schijven. Over de opzet en het doel van de KPI’s bent u bij VNG-ledenbrief van 12 november 2012 al geïnformeerd. Deze stukken zijn met nadere uitleg ook te vinden op www.vng.nl.

Wat gebeurt er met uw antwoorden?
Nadat wij de antwoorden hebben ontvangen, maken wij een afspraak met u om deze te bespreken en enkele applicaties nader te bekijken. De uitkomsten hiervan zullen worden gebruikt voor het formuleren van algemene conclusies en het doen van aanbevelingen voor de opzet van digitale archivering. Uiteraard krijgt u door de beantwoording ook beter zicht op uw eigen situatie.

Heeft u vragen?
Voor alle vragen over het onderzoek kunt u contact opnemen met de heer J.B. de Vries, senior-beleidsmedewerker toezicht archieven Drenthe, Fryslân en Groningen telefoon: 058-2925309 of 058-2928205, e-mail: j.b.devries@fryslan.nl.

Wij hopen van harte op uw medewerking te mogen rekenen.

Met vriendelijke groet,

drs. D. Bunskoeke en drs. J. Dijkstra

Provinciale archiefinspecteurs in Drenthe, Fryslân en Groningen

Onze vragen aan u

Ontleend aan RODIN, Referentiekader Opbouw Digitaal Informatiebeheer
(www.lopai.nl/pdf/Brochure_RODIN_dubbelzijdig.pdf)

1. Heeft uw organisatie een door het bestuur en/of management vastgesteld informatiebeleid dat aansluit bij de geformuleerde organisatiedoelstellingen?

2. Worden hierin de volgende onderdelen tenminste vermeld?

   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;
   d. Een beschrijving van het beveiligingsbeleid waarin taken en verantwoordelijkheden voor informatiebeveiliging zijn belegd;

3. Wordt van alle archiefstukken tenminste de volgende informatie in de meta data vastgelegd?:

   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;
   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).

4. Worden digitale archiefstukken opgeslagen in door het bestuur aangewezen, valideerbare en volledig gedocumenteerde bestandsformaten, die voldoen aan een open standaard, tenzij dit redelijkerwijs niet kan worden verlangd?

5. Kunnen door middel van een zoekopdracht alle digitale archiefstukken en hun meta data op elk aggregatieniveau worden getoond, met inachtneming van autorisaties?

6. Wordt de bewaartermijn van digitale archiefbescheiden automatisch op elk aggregatieniveau vastgelegd?. En worden die bewaartermijnen nageleefd met inachtneming van de wettelijke selectietermijnen, procedures en vervolgacties (vernietigen, overdragen of exporteren)?

7. Doet u aan een systematische risicoanalyse voor factoren als data, systemen, personeel, fysieke locatie en beveiligingseisen?

8. Heeft u een adequate serverruimte met onder meer klimaatbeheersing, alarm en brandmeldvoorziening, toegangscontrole, ordelijke bekabeling en noodstroomvoorziening (UPS)?