ELEKTRONISCH DOCUMENTBEHEER …

…. op zoek naar een normenkader

Teamnummer: 1052

Johan van der Galiën

Chris Schaerlaeckens

Maart 2011

Voorwoord

Hierbij presenteren wij onze scriptie “Elektronisch documentenbeheersystemen”, die is geschreven in het kader van de postgraduate IT-audit opleiding aan de Vrije Universiteit van Amsterdam. Onze scriptie vormt het sluitstuk van de opleiding en via deze scriptie tonen wij aan over voldoende niveau te beschikken om een IT-audit vraagstuk op wetenschappelijk niveau aan te pakken. Wij vinden het van belang vooraf een kanttekening te maken. De eisen die de Vrije Universiteit aan de scriptie stelt leiden ons inziens tot een beperking in de mogelijke diepgang. Wij doelen dan met name op het beperkt aantal beschikbare studieuren die aan de een scriptie worden besteed. Desalnietemin zijn wij van mening dat onze scriptie een wetenschappelijk verantwoord “werk” vertegenwoordigd.

In onze scriptie behandelen wij het vraagstuk van de vereiste inrichting van een elektronisch documentbeheersysteem om te waarborgen dat documenten te allen tijde in oorspronkelijke en onveranderde vorm beschikbaar zijn. Het antwoord op dit vraagstuk is een door ons gecreëerd raamwerk (normenkader) dat in eerste instantie is ontworpen voor IT-auditors, maar het raamwerk kan eveneens voor de inrichting van het vereiste stelsel van beheersmaatregelen worden gebruikt.

Wij zijn beiden werkzaam bij de Belastingdienst als EDP-auditmedewerker. Ons dagelijks werk bestaat voornamelijk uit het ondersteunen van collega’s die belast zijn het controleren van aangiften in de vorm van boekenonderzoeken bij belastingplichtigen. In praktijk bestaat de ondersteuning uit het geven van een oordeel over de opzet van de AO/IC rondom de geautomatiseerde gegevensverwerkende systemen, het verwerken en aanbieden van gegevens uit de administratie van belastingplichtigen, en het ondersteunen van collega’s bij het gebruik van audit-tools.

Wij danken een ieder die op zijn of haar wijze heeft bijgedragen aan ons eindresultaat en wensen u veel leesplezier toe!

Inhoudsopgave

1 Inleiding

Wij hebben gekozen om onderzoek te doen naar het beheersen een “Elektronisch Documentbeheersysteem”. De reden voor onze keuze en de doelstelling die wij met ons onderzoek proberen te realiseren kunt u lezen in het eerste gedeelte van dit hoofdstuk. De doelstelling mondt uit in een centrale onderzoeksvraag, die nader wordt gespecificeerd in een aantal deelvragen. Wij besluiten dit hoofdstuk met het beschrijven van de door ons gehanteerde onderzoeksmethode en de beperkingen van ons onderzoek.

1.1 Aanleiding

Documenten hebben een grote waarde voor de bedrijfsvoering en dragen in sterke mate bij aan de ondersteuning en uitvoering van bedrijfsprocessen. Een organisatie kan niet goed functioneren als medewerkers documenten niet kunnen raadplegen of gebruiken. Nog erger is het als beslissingen worden genomen op basis van documenten met een verkeerde inhoud en/of status. Het goed beheren van digitale documenten en de processen waarin deze worden verwerkt, is van essentieel belang voor iedere organisatie.

In het hedendaagse digitale tijdperk worden documenten steeds meer elektronisch verwerkt. In toenemende mate zijn documenten alleen in digitale vorm beschikbaar. Er blijven weliswaar nog steeds stukken op papier binnenkomen en uitgaan, maar dit zal steeds beperkter worden. De nadruk komt steeds meer te liggen op het gebruik van digitale documenten voor het uitvoeren van de bedrijfsprocessen.

1.2 Doelstelling van de scriptie

Er bestaat een grote diversiteit aan organisaties, wijze van inrichting van processen en het beheren van documenten. Het beheren van elektronische documenten maakt deel uit van de informatievoorziening van een organisatie. De toename van het gebruik van digitale documenten zorgt voor een groei van data. Dit gaat gepaard met toenemende complexiteit om digitale documenten te beheersen.

Door de digitalisering verbetert de beschikbaarheid van documenten. Een papieren documentstroom door een organisatie is geheel verschillend van een elektronische documentstroom. Voor de elektronische documentstroom gebruikt men vaak additionele programmatuur in de vorm van workflowmanagement om de processen beter te besturen en te beheersen. Dit vereist andere beheersmaatregelen voor elektronische documenten. Het risico dat elektronische documenten kunnen worden gemanipuleerd blijft bestaan.

Wij onderkennen dat de behoefte bestaat aan een algemeen geldend kader voor de beheersing van digitale documenten. Deze beheersing ziet op toegang, bewerken, bewaren en beschikbaarheid van digitale documenten binnen procesgangen, waarbij een aantal kwaliteitsaspecten zijn gewaarborgd. De kwaliteitscriteria, vertrouwelijkheid, integriteit, beschikbaarheid en controleerbaarheid moeten gewaarborgd en toetsbaar zijn voor het beheersen van digitale documenten. Dit is overigens niet anders dan bij papieren documenten, maar de aard van deze beheersmaatregelen is verschillend. De inhoud van de genoemde kwaliteitscriteria wordt in onze scriptie nader uiteengezet.

Als randvoorwaarde is het vermelden waard dat voor de inrichting van elektronisch documentbeheer geen wettelijk kader bestaat. Iedere organisatie kan documentbeheer vormvrij inrichten. Er zijn echter wel diverse algemene eisen, los van de beheersbaarheid, zoals bijvoorbeeld de Archiefwet 1995 en de Algemene Wet Rijksbelastingen. Deze algemene eisen zijn met name gericht op het bewaren van digitale documenten, die na het doorlopen van een bedrijfsproces als archiefstuk zijn 'opgeborgen'.

De doelstelling van onze scriptie is het creëren van een raamwerk voor het verschaffen van een redelijke mate van zekerheid over de werking van een elektronisch documentbeheer-systeem. Het raamwerk is in eerste instantie ontworpen voor IT-auditors die zijn belast met een onderzoek naar het verschaffen van de genoemde zekerheid. Vanzelfsprekend kan het raamwerk ook worden gebruikt door andere belanghebbenden of geïnteresseerden, bijvoorbeeld voor functionarissen belast met de inrichting van een elektronisch documentbeheersysteem. Tijdens ons onderzoek hebben wij vastgesteld dat er in het verleden audits zijn uitgevoerd op de werking van elektronische documentbeheersystemen, maar deze zijn sterk 'rule-based' georiënteerd. Een voorbeeld is een rapport dat wij aantroffen van een audit op een systeem van het Amerikaanse Ministerie van Defensie. De focus van deze audit lag in dit geval op de beveiligingsaspecten en de general controls die hierop toezien.

1.2.1 Beperking aandachtsgebied

Een afbakening van het onderzoeksgebied is noodzakelijk om de bruikbaarheid van het beoogde raamwerk mogelijk te maken. Zonder deze afbakening bestaat het risico dat een omvangrijk en onsamenhangend raamwerk ontstaat. De afbakening richt zich met name op het toepassingsgebied van documentbeheer en workflowmanagement.

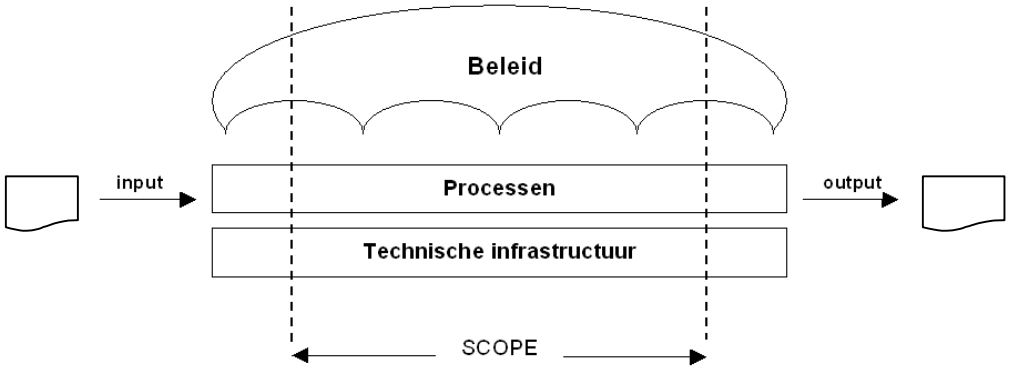
Het onderzoeksobject van deze scriptie vormt een systeem dat de verwerking en opslag van digitale documenten verzorgt, een elektronisch documentbeheersysteem. Dit systeem is een samenhangend geheel van hard- en software dat procesmatig wordt gevoed en beheerst. Elektronisch documentbeheer maakt onderdeel uit van het brede begrip Enterprise Content Management (ECM).

Enterprise Content Management is een zeer brede term die all-in-one gebruik van gegevens en beheer van vele aspecten daar omheen omvat. Van Bussel omschrijft ECM als:

> *"Het geheel van beleid, procedures en informatiesystemen binnen een organisatie om content (documenten, archiefdocumenten en "nodes") te creëren, te ontvangen, vast te leggen, op te slaan, te bewerken, te distribueren, te ordenen, te publiceren, te waarderen, te vernietigen en/of te bewaren, te beveiligen en te behouden"[1].*

[1]Geert-Jan van Bussel, Ferdinand Ector, Op zoek naar herinnering. Helmond, 2009

Hieronder is het aandachtsgebied schematisch weergegeven.

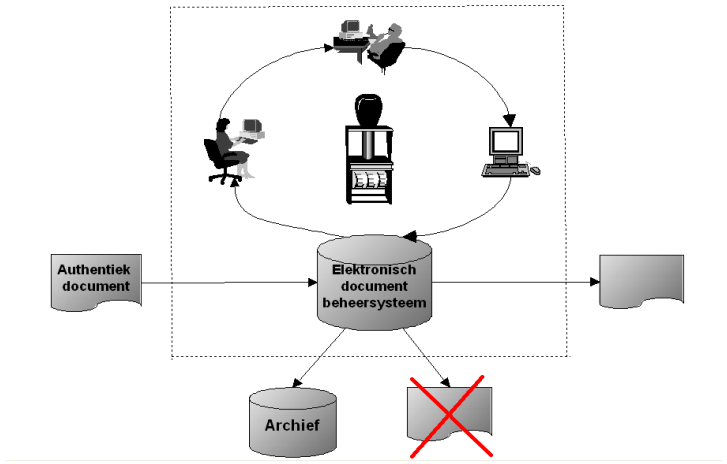


Figuur 1: *Aandachtsgebied*

Toelichting onderzoeksgebied:

Het elektronisch documentbeheersysteem beschouwen wij als een “black box”. Het document zien wij hierin als een feit. Een document dat deze blackbox verlaat kan worden vernietigd of voor impliciete doeleinden worden gearchiveerd. Deze documenten vallen buiten het onderzoeksgebied. Tijdens ons onderzoek is gebleken dat naar archiefbeheer diepgaand onderzoek is verricht, en dat voor archiefbeheer uitgebreide normen zijn geformuleerd.

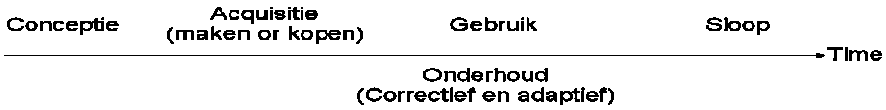
Binnen de black box regelt het elektronisch documentbeheersysteem het registreren, eventueel creëren, autoriseren, routeren, presenteren, rapporteren en behandelen van document. Deze aspecten vragen om normering ter mitigering van de risico’s die er bestaan (zie paragraaf 3.3).



Figuur 2: *Onderzoeksgebied*

1.2.1.1 Lifecycle

Naast de lifecycle van een document, onderkennen wij ook een lifecycle bij het gebruik van systemen voor het beheren van elektronische documenten. Deze laatste lifecycle begint bij de selectie of definiëren van de systeemeisen tot en met het uitfaseren van het systeem (zie figuur 3 hieronder).



Figuur 3: *Lifecycle systeem*

De start van deze lifecycle is de aanschaf van een elektronisch documentbeheersysteem. Hierbij is het van belang om te onderkennen hoe deze aanschaf tot stand is gekomen. Heeft de organisatie een weloverwogen keuze gemaakt op basis van gedegen beslissingen in samenhang met economische en strategische beleidsuitgangspunten, of heeft men simpelweg een selectie gemaakt uit beschikbare producten.

De wijze waarop de keuze voor een dergelijke systeem tot stand komt kan van grote invloed zijn op de kwaliteit van de informatievoorziening in de organisatie. Het systeem moet passen binnen de bestaande architectuur en processen. De aanschaf van een elektronisch documentbeheersysteem moet daarnaast bedrijfseconomisch verantwoord zijn.

1.2.1.2 Toepassingsgebied

Binnen documentaire informatievoorziening bestaat er onderscheid tussen twee toepassingsgebieden.

Enerzijds kan men omgevingen beschouwen met gestandaardiseerde informatievoorziening, gebaseerd op strakke processen die vastliggen. Hierbij valt te denken aan standaard administratieve omgevingen, zoals aanvragen van vergunningen bij een gemeente of het inkoop- en verkoopproces in een commerciële organisatie.

Anderzijds onderkennen wij omgevingen met meer ongestructureerde processen en een ongedefinieerde stroom van documenten. Hierbij valt te denken aan meer kennisachtig of projectgerelateerde omgevingen, zoals advocatuur of een architectbureau, met een veelheid aan en een combinatie van interne en externe documenten. De nadruk ligt bij ongestructureerde processen sterker op dossierbeheer en heeft daardoor impliciet een sterke relatie met archiefbeheer. Dit in tegenstelling tot een proces met een gestandaardiseerde documentstroom.

Ons onderzoek beperkt zich tot een gestandaardiseerde documentstroom. De reden hiervoor is dat het onderzoek nadrukkelijk is gericht op de “flow” van documenten binnen processen en de daarvoor geldende kwaliteitseisen.

Het is niet zo dat normen voor de ongestructureerde informatievoorziening niet kunnen worden gedefinieerd, echter de benadering zal anders zijn, en in de meeste gevallen is de relatie met dossier- en archiefbeheer doorgaans sterker.

1.2.1.3 Documenten

De input van een elektronisch documentbeheersysteem vormen verschillende soorten documenten. Van Bussel hanteert de volgende definitie:

> *Een document is een vastgelegd of reproduceerbaar gegeven of een vastgelegde verzameling reproduceerbare, samenhangende gegevens, die met gebruikmaking van een presentatievorm als eenheid wordt gedragen en weergegeven door middel van een medium, die de expliciete bedoeling heeft informatie te bewaren en/of over te dragen, die gecommuniceerd kan worden en die, indien nodig, een sociale rol vervult*[2]*.*

Tijdens een gesprek met Van Bussel voegde hij toe dat deze documenten voor 95% een verantwoordingsfunctie hebben. Daarmee benadrukte hij het belang van documenten in een organisatie en daarmee het belang van documenten in een geautomatiseerde omgeving.

Een document heeft de volgende kenmerken:

- gegevens (letters, cijfers, afbeeldingen, video's, bits en pixels);
- presentatievorm, de manier waarop de inhoud van de gegevens wordt getoond;
- medium, datgene waarmee of waarop de gegevens en de presentatievorm in een bepaalde samenstelling worden vastgelegd, weergegeven, bewaard of gecommuniceerd.

Een document kan in twee verschijningsvormen voorkomen, fysiek en virtueel. Virtuele documenten zijn documenten die geen fysieke vorm (meer) hebben, maar deze als kopie of print wel toegekend kunnen krijgen. In ons onderzoek beperken wij ons tot de virtuele documenten.

Een ander onderscheid is het verschil tussen interne en externe documenten. De interne documenten komen uit de organisatie zelf en kunnen bestaan uit nieuw gecreëerde dan wel uit het archief opgehaalde documenten. Externe documenten zijn documenten die van buiten de organisatie in het systeem worden gebracht, bijvoorbeeld een inkoopfactuur al dan niet in digitale vorm. Papieren documenten worden doorgaans met behulp van scanning digitaal beschikbaar gemaakt. De vereisten die noodzakelijk zijn om te garanderen dat de conversie van niet digitale documenten naar een digitaal formaat, maken geen onderdeel uit van ons onderzoek.

Binnen de documentaire informatievoorziening bestaat onderscheid tussen een dynamisch, semi-statisch en een statisch archief. De documenten in het dynamisch archief worden dagelijks gebruikt. Voor deze documenten is snelheid een belangrijk aspect. Documenten in het semi-statisch archief bevinden zich in een 'tussenarchief'. Deze documenten hoeven niet direct beschikbaar te zijn, maar moeten wel toegankelijk zijn. Dit in tegenstelling tot documenten die zich in het statisch archief bevinden.

Deze documenten worden niet of nauwelijks meer geraadpleegd, maar worden bewaard tot ze vernietigd worden. De snelle beschikbaarheid speelt hier een ondergeschikte rol ten opzichte van documenten in het dynamische of semi-statische archief.

[2] Geert-Jan van Bussel, Ferdinand Ector, Op zoek naar herinnering. Helmond, 2009

W.J. Keller maakt in zijn boek "Zaakgericht werken: warme en koude dossiers"[3] onderscheid tussen warme en koude systemen. Een koud systeem is een archiefsysteem, waarin documenten en dossiers ter vernietiging worden geplaatst, maar ook om opgehaald te worden, indien de documenten nog nodig zijn. De term koud betekent: "lang geleden voor het laatst aangeraakt". Een warm systeem wordt daarentegen in de loop van een proces gebruikt, of het nu een min of meer gestructureerde zaak is of een erg ongestructureerd proces zoals kennisvergaring. Bij een koud systeem ligt de nadruk op archivering, ontsluiting en vernietiging; bij een warm systeem staat het proces voorop. Het warme deel van een documentsysteem wordt documentmanagement genoemd en het koude deel recordmanagement. Ons onderzoek is uitsluitend gericht op het warme deel, namelijk documentmanagement.

1.2.1.4 Toegepaste systemen

Voor het onderzoek gaan wij uit van "standaardpakketten". Wij richten ons impliciet niet op maatwerksystemen die door of namens een organisatie zijn ontwikkeld. Deze afbakening is mede ingegeven door een gesprek met W.J. Keller en M. Roovers[3] tijdens ons vooronderzoek.

In Nederland wordt veelal gebruik gemaakt van standaardpakketten, omdat deze aan alle basisvereisten voor documentbeheer voldoen. De kwaliteit van systeemontwikkeling van deze pakketten ten opzichte van Anglosaksische programmatuur bevindt zich op hoger level, volgens onderzoek van Argitek[4]. Er is in Nederland sprake van een voorkeur voor "proven technology" bij de keuze voor elektronisch documentbeheersystemen.

1.2.1.5 Begrippen

Er is veel geschreven en gepubliceerd rondom documentbeheer en workflowsystemen. Wij hebben tijdens het literatuuronderzoek vastgesteld dat er geen eenduidig definitiekader bestaat voor het object van onderzoek en de daarbij gebezigde begrippen. Op basis van het literatuuronderzoek, hanteren wij de volgende "eigen" definities:

- ***Documentaire informatievoorziening:*** Activiteiten met betrekking tot de creatie, verwerving, distributie, opslag en preservering van documenten;
- ***Documentbeheer:*** Het beheer van documenten tijdens het bedrijfsproces;
- ***Workflowmanagement:*** Beheer en sturing van processen.

Deze begrippen zijn bewust ruim geformuleerd zodat het in een breed scala van toepassingsgebieden kan worden toegepast. Het belang van zorgvuldig gedefiniëerde definities is nodig om overbodige discussie en schijndiscussie te voorkomen.[5] Het begrip Elektronisch Documentbeheersysteem wordt in paragraaf 2.2 van deze scriptie uitgebreid gedefinieerd.

---

[3] M&I Argitek, e-business architecten, Capelle aan de IJssel

[4] Zaakgericht werken: koude en warme digitale dossiers, W.J. Keller

[5] H.J. de Jager, A.L. Mok; Grondbeginsel der sociologie. Gezichtspunten en begrippen (Leiden, Antwerpen; 1978, blz 28-29)

1.2.2 Centrale vraagstelling

Op grond van de doelstelling van onze scriptie zijn wij tot onderstaande onderzoeksvraag gekomen:

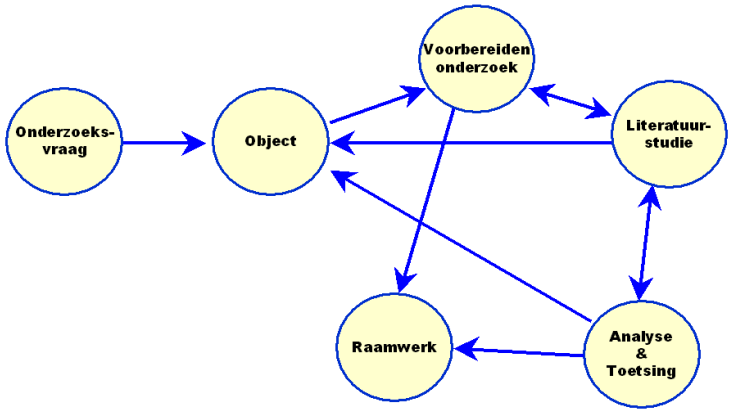
Welke beleidsmatige en organisatorische maatregelen spelen een rol bij de inrichting van een elektronisch documentbeheersysteem om te waarborgen, dat documenten gedurende de gehele levensduur in oorspronkelijke en onveranderde vorm beschikbaar zijn, en welke technische aspecten ondersteunen deze maatregelen?

Voor de beantwoording van de onderzoeksvraag splitsen wij deze op in de volgende deelvragen:

1. *Beschrijvende vraag:* Welke beleidsmatige, organisatorische en technische voorwaarden spelen een rol bij het inrichten en beheren van een elektronisch documentbeheersysteem?
2. *Analyserende vraag:* Welke risicogebieden kunnen worden onderscheiden bij elektronische documentsystemen en op welke wijze kunnen adequate beheersmaatregelen worden genomen?
3. *Beschouwende vraag:* Welke elementen en kenmerken bevat een IT-audit control-framework voor elektronische documentsystemen?

1.2.3 Onderzoeksmethode

De methodiek van ons onderzoek is afgeleid van de methode Yin[6]. Deze op case-studies gerichte methode hebben wij als volgt vertaald, zie figuur 4 hieronder.



Figuur 4: *Onderzoeksmethode*

Het raamwerk is door ons opgebouwd volgens de 'principle based' benadering. De p*rinciple based* benadering resulteert in "open normen" en laat het aan de organisatie over om te bepalen op welke wijze zij eraan voldoen. In een *principle based uitwerking* worden de algemene normen in een normenkader minder strikt uitgewerkt dan bij een *rule based uitwerking.* Daarnaast wordt, bij het hanteren van de *principle based gedachte,* bij de toetsing van het normenkader vooral gekeken of aan de doelstellingen van een norm wordt voldaan, en niet zozeer naar de wijze waarop dat gebeurt. De open norm geeft alleen het doel weer. De organisatie moet de normen zelf interpreteren.

De *rule based* benadering streeft ernaar om de regels waaraan moet worden voldaan zo nauwkeurig mogelijk te omschrijven. Daarbij wordt uitwerking gegeven aan de achterliggende gedachte van regels, met als resultaat zoveel mogelijk helderheid voor de gebruiker. Het risico hiervan is dat de regels vaak worden uitgewerkt op een wijze die in de praktijk niet de meest gunstige is voor de organisatie. Een ander nadeel is dat deze regels vaak in de richting van een bepaalde technische oplossing gaan. Deze technische oplossingen verouderen snel.

Daarnaast hanteren wij een zogenaamde 'risk based approach'. Wij hebben een inventarisatie gemaakt van de risico's die kunnen optreden bij het beheersen van elektronische documenten binnen het beschreven aandachtsgebied, rekening houdend met de eerder in dit hoofdstuk genoemde kwaliteitsaspecten. Om deze risico's te kunnen detecteren hebben wij een literatuuronderzoek uitgevoerd en diverse deskundigen geïnterviewd. Op basis van de gedetecteerde risico's is het raamwerk opgesteld met "open normen".

6 Robert K Yin, 1984

Het ontwerpen van het raamwerk volgens een risk approach brengt ook risico's met zich mee. Mogelijkerwijs zien wij risico's over het hoofd, of wij schatten wij risico's verkeerd of onvolledig in. Wij hebben ervoor gekozen om onafhankelijke externe deskundigen de volledigheid van de gedetecteerde risico's te laten valideren.

Om het onderzoek te structureren hebben wij in de opstartfase zoveel mogelijk informatie verzameld in de vorm van literatuur, bestaande normenkaders en hebben wij op het internet uitvoerig gesurft om whitepapers te verzamelen, sites van pakketleveranciers bekeken en onderzoeksresultaten van andere bronnen bekeken. Vervolgens hebben wij ons onderzoeksgebied definitief afgebakend.

De stappen die wij gedurende het onderzoek hebben uitgevoerd zijn hieronder in de tabel weergegeven.

Stap	Omschrijving
1. Verzamelen informatie	Literatuur-onderzoek; verzamelen van literatuur, white-papers en het verzamelen van normenkaders en wet- en regelgeving.
2. Bepalen scope	Afbakening van het onderzoeksgebied.
3. Risico's detecteren	Brainstormsessie.
4. Vaststellen normen	Selecteren uit bestaande normenkaders en "eigen" normen formuleren.
5. Toetsing deskundigen	Interviews en workshop deskundigen.
6. Resultaten verwerken	De uitkomsten van zijn gespiegeld aan de eerder geformuleerde normen.
7. Samenvatten en concluderen	Afronden en een definitief raamwerk opgesteld.

Tabel 1: *Opzet onderzoek (stappenplan)*

1.3 Indeling van de scriptie

Wij starten in hoofdstuk 2 met de geschiedenis van een elektronisch documentbeheersysteem, waarna wij in dit hoofdstuk een beschrijving geven van een elektronisch documentbeheersysteem en haar kenmerken.

In hoofdstuk 3 is aandacht voor de door ons gebruikte kwaliteitsaspecten en de risico's die bestaan bij het inrichten van een elektronisch documentbeheersysteem. In hoofdstuk 4 is het antwoord op onze onderzoeksvraag beschreven in de vorm van een raamwerk, "principle based". In hoofdstuk 5 beschrijven wij de reacties van de deskundigen, die ons raamwerk hebben geverifieerd.

2 Elektronisch Documentbeheer

Elektronisch documentbeheer bestaat al een ruime tijd. Sinds de laatste jaren is er meer aandacht om een dergelijk systeem in te voeren. Dit wordt veroorzaakt door de toenemende automatisering en het besef van de voordelen van een elektronisch documentbeheersysteem.

In dit hoofdstuk beschrijven wij eerst de geschiedenis van een elektronisch documentbeheersysteem, waarbij in de loop der tijd een toename van het gebruik elektronisch documentbeheer valt waar te nemen.

Verder besteden wij in dit hoofdstuk aandacht aan de redenen voor het gebruik van een elektronisch documentbeheersysteem. Wij staan uitgebreid stil bij de werking en de voor- en nadelen.

2.1 Geschiedenis Elektronisch Documentbeheer

De eerste elektronische documentbeheersystemen zagen het levenslicht in de jaren tachtig van de vorige eeuw. Het gebruik beperkte zich tot organisaties met massale verwerking van documenten.

Door de vooruitgang in technologie van met name de beschikbaarheid en snelheid van personal computers, de toepassing van internet, de verschuiving van papieren naar elektronische documenten, en de veel goedkopere scanning mogelijkheden, zijn elektronische documentbeheersystemen ook bereikbaar geworden voor kleinere organisaties. Elektronisch documentbeheer vormt tegenwoordig een essentieel onderdeel voor de beheersing van bedrijfsprocessen binnen een organisatie. In de huidige tijd van economische neergang wordt de inzet van dergelijke systemen wellicht iets vertraagd, maar in de meeste gevallen is zo'n verschuiving kortzichtig. Door een juiste implementatie, gebruik en onderhoud werkt een elektronisch documentbeheersysteem kostenverlagend en is het een krachtige hulpmiddel voor het efficiënt en effectief laten verlopen van de bedrijfsvoering. De voordelen komen later in dit hoofdstuk aan de orde.

Om bovenstaande te verifiëren en om een beeld te krijgen over het gebruik van elektronische documentbeheersystemen hebben wij inzage gevraagd en gekregen in een onderzoeksrapport[7] dat door Cantab Marketing Services (gevestigd in Amsterdam) in 2005 is uitgevoerd. Cantab heeft in opdracht van BCT Automatisering (een van de grotere leveranciers van elektronische documentbeheersystemen) onderzoek uitgevoerd naar het gebruik van elektronische documentbeheersystemen door Nederlandse gemeenten.

Vanuit BCT bestond de behoefte om van alle gemeenten in Nederland te weten of ze momenteel gebruik maken van enige vorm van documentmanagementsoftware en in welke mate ze hier tevreden over zijn. Het onderzoek was voor BCT met name van belang om hun positie te bepalen ten opzichte van concurrenten.

[7] Cantab Services BV, Amsterdam, 2005

Wij hebben ter verificatie gekozen voor een uitgevoerd onderzoek onder Nederlandse gemeenten, omdat er binnen gemeenten sprake is van een omvangrijke documentstroom, en omdat gemeenten vergelijkbaar zijn vanwege overeenkomstige bedrijfsactiviteiten en -processen.

De onderstaande tabel geeft het aantal gemeenten dat gebruik maakt van een volwaardig documentbeheersysteem, onderverdeeld naar het aantal inwoners per gemeente. Uit onderstaande tabel blijkt dat de kleinere gemeenten minder vaak software gebruiken met betrekking tot documentbeheer. In gemeenten met minder dan 10.000 inwoners beschikt slechts 18,8% van deze gemeenten over een elektronisch documentbeheersysteem. In gemeenten met meer dan 75.000 inwoners beschikt daarentegen 76,7% van deze gemeenten over een elektronisch documentbeheersysteem.

		Software?		
Inwoners	Gegevens	Ja	Nee	Eindtotaal
< 10.000	Aantal	9	39	48
	%	18,8%	81,2%	100,0%
10.001 – 20.000	Aantal	52	66	118
	%	44,1%	55,9%	100,0%
20.001 – 30.000	Aantal	53	27	80
	%	66,3%	33,7%	100,0%
30.001 – 75.000	Aantal	62	28	90
	%	68,9%	31,1%	100,0%
75.000	Aantal	23	7	30
	%	76,7%	23,3%	100,0%

Tabel 2: *Gebruik DMS door gemeenten*

De volgende tabel geeft vervolgens antwoord op de vraag of gemeenten die op het tijdstip van onderzoek nog niet over een elektronisch documentbeheersysteem beschikken, de intentie hebben om hier op korte termijn in te gaan investeren. Het blijkt dat een substantieel aantal gemeenten de intentie hebben om op korte termijn een elektronisch documentbeheersysteem te implementeren. Van alle onderzochte gemeenten die niet over een elektronisch documentbeheersysteem beschikken heeft namelijk 61,1% aangegeven dat zij de intentie hebben op korte termijn in een elektronisch documentbeheersysteem te gaan investeren. Elektronisch documentbeheer gaat dus in toenemende mate een essentieel onderdeel vormen voor de beheersing van bedrijfsprocessen binnen een organisatie.

Investeren?	Gegevens	
Ja	Aantal	102
	%	61,1%
Nee	Aantal	65
	%	38,9%
Eindtotaal Aantal		167
Eindtotaal %		100,0%

Tabel 3: *Intentie investeren in elektronisch documentbeheersysteem*

Het onderzoek van Cantab bevestigt de toename in de loop der tijd van het implementeren van elektronisch documentbeheersystemen. Van de in het onderzoek betrokken gemeenten heeft slechts 7,8% een elektronisch documentbeheersysteem geïmplementeerd voor het jaar 1996. De daarop volgende jaren vertonen een oplopend percentage van het aantal gemeenten dat een elektronisch documentbeheersysteem heeft geïmplementeerd.

Implementatie		
<1996	Aantal	15
	%	7,8%
1997-1998-1999	Aantal	41
	%	21,2%
2000-2001-2002	Aantal	56
	%	29,0%
2003-2004-2005	Aantal	81
	%	42,0%
Eindtotaal Aantal		193
Eindtotaal %		100,00%

Tabel 4: *Tijdstip implementatie*

2.2 Wat is een Elektronisch Documentbeheersysteem?

Iedere organisatie maakt een veelvoud van documenten aan. Een groot deel van deze documenten wordt digitaal aangemaakt, uitgeprint om te verspreiden en uiteindelijk gearchiveerd. Andere documenten komen ongestructureerd de organisatie binnen en zijn daardoor lastiger te beheren. Voorbeelden van ongestructureerde documenten zijn reguliere post, pakbonnen, faxen, e-mailberichten etc.. In hoofdstuk 1 van deze scriptie hebben wij beschreven dat wij ons beperken tot het verwerken van digitale documenten. Digitale documenten worden opgemaakt en ontvangen op een verscheidenheid van media met gebruik van technologie die constant verandert. Het primaire kenmerk is de dynamische aard. Verschillende personen bewerken documenten, ze bestaan in verscheidene versies en bevinden zich in stadia met variërende tijdsduur.

Voor iedere organisatie is het essentieel dat informatie in de vorm documenten snel en betrouwbaar beschikbaar is om bedrijfsprocessen optimaal te kunnen uitvoeren. Wanneer het beheer van documenten niet efficiënt en effectief plaatsvindt, beïnvloedt dit in hoge mate de interne en externe communicatie, waardoor de productiviteit in negatieve zin wordt beïnvloed. Dit kan naast onnodige extra kosten ook leiden tot vermindering van arbeidsvreugde (intern), imagoschade, verlies van klanten etc.. Het is dus voor iedere organisatie belangrijk om het beheer van digitale documenten stevig in de grip te houden.

Een elektronisch documentbeheersysteem zorgt ervoor dat informatie in de vorm van digitale documenten betrouwbaar en snel beschikbaar is om bedrijfsprocessen optimaal te kunnen uitvoeren. Dit levert voordelen voor het efficiënt en effectief beheren van documenten en draagt bij in een substantiële kostenbesparing.

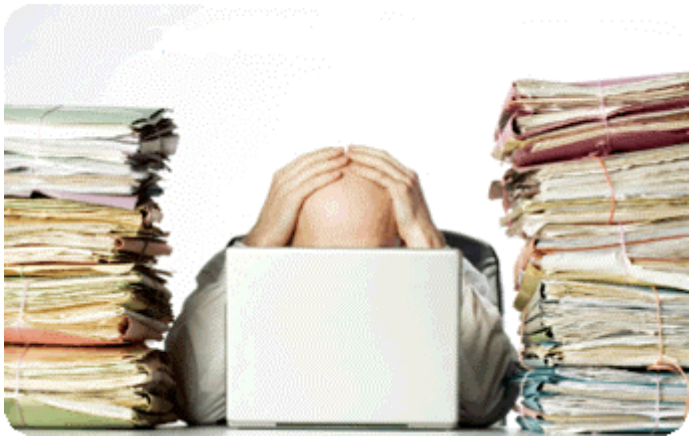
De optimale uitvoering van de bedrijfsprocessen vindt plaats door het managen van de creatie, ontvangst, vastlegging, zoekfuncties, raadpleging, wijziging, routering en archivering van digitale documenten. De software van een elektronisch documentbeheersysteem zorgt tevens voor beheersing van het wijzigingsproces van digitale documenten.

De voordelen van een elektronisch documentenbeheersysteem:

Efficiency:

- *Stroomlijnen van processen.*
- *Snelle toegang tot informatie.*
- *Sneller en makkelijker beheren van informatie.*

Een geautomatiseerd systeem voorziet in een aantal voordelen die veelvoorkomende problemen kunnen oplossen. Leveranciers van deze producten schermen met deze voordelen, die een organisatie inderdaad zal onderschrijven. Zoals wij verderop zullen beschrijven leidt de implementatie van een systeem tot risico's die uiteindelijk door middel van maatregelen beheerst moeten worden. Dit zorgt voor overhead hetgeen de softwareleveranciers niet in verkoopfolder zullen opnemen.



Figuur 5: *Sneller en makkelijker beheer van informatie*

Andere voordelen kunnen zijn:

- *Reductie van kosten met documentbeheer.*
- *Betere samenwerking door een documentbeheersysteem.*
- *Verbeterde kwaliteit met documentmanagement software.*

Deze voordelen zijn minder evident en brengen weer andere risico's en nadelen met zich mee. De reductie van kosten is zeer relatief. Er zullen kostenbesparingen zijn door het minder maken van fouten, doordat informatie onder andere sneller beschikbaar is en afgehandeld kan worden. Daar tegenover staat de aanschaf van een systeem (hard- en software) dat ingeregeld, onderhouden en beheerd dient te worden.

Verbeterde toegankelijkheid brengt bijvoorbeeld met zich dat er aanvullende autorisaties nodig zijn. Afhankelijk van de organisatie en de processen moeten dingen goed geregeld worden. Uiteindelijk bepaalt de organisatie zelf hoe ver zij wil gaan met betrekking tot de inrichtingsaspecten van een dergelijk systeem, en welke waarborgen zij daarbij wil nemen.

Door de implementatie van een elektronisch documentbeheersysteem kunnen er geen impliciete nadelige gevolgen genoemd worden. De geautomatiseerde verwerking zorgt immers voor talloze verbeteringen op het gebied van efficiency en effectiviteit. Echter voor het optimaal functioneren is het essentieel dat de keuze en implementatie gedegen plaatsvinden. Verderop in de scriptie beschrijven wij de risico's die gepaard gaan met het implementeren en het werken met een elektronisch documentbeheersysteem. De risico's in het geval van elektronisch documentbeheer zijn niet verschillend van een papieren documentstroom, maar kunnen in andere verschijningsvorm optreden. Een document kan zowel fysiek als virtueel verloren gaan, echter de oorzaak en bijbehorende maatregelen zijn anders van aard.

2.3 Kenmerken

In een eenvoudige situatie is er sprake van één gebruikersysteem, zonder de noodzaak het elektronisch documentbeheersysteem vanaf een andere locatie te benaderen. Dan volstaat een lokale installatie. Behoudens bescherming van volledigheid en beschikbaarheid van de informatie, is de toegevoegde waarde van een dergelijke implementatie minder groot dan in een situatie dat toegankelijkheid ook gewenst is voor gebruikers buiten de onderneming.

De implementatie van een elektronisch documentbeheersysteem is een grote investering, dit legt een grote druk op het budget van kleinere ondernemingen. Er verschijnen de laatste tijd leveranciers op de markt die een elektronisch documentbeheersysteem als een SaaS aanbieden. Zowel de programmatuur als de gegevensverzameling zijn daarbij op een externe server ondergebracht, en dus bereikbaar vanaf elke locatie en door elke gerechtigde gebruiker.

In deze scriptie beperken wij ons tot de situatie dat er sprake is van één lokaal gebruikerssysteem, zonder de noodzaak van het benaderen vanuit andere geografische locaties. Deze beperking is niet ingegeven door toenemende complexiteit, maar is meer gericht op de aspecten met betrekking tot documentbeheer "an sich". Zoals wij beschrijven in paragraaf 4.3 over het modulair opzetten van normenkaders zouden de aspecten die hiermee gepaard gaan, vallen onder het modulaire raamwerk voor "communicatie en internet gerelateerde systemen".

3 Risico's en beheersmaatregelen

In dit hoofdstuk beschrijven wij de noodzakelijke voorwaarden voor het optimaal functioneren van een elektronisch documentbeheersysteem. Om de voorwaarden te toetsen worden vervolgens de kwaliteitsaspecten benoemd. Dit leidt tot een stelsel van te nemen beheersmaatregelen die voortvloeien uit de door ons gedetecteerde risico's.

3.1 Voorwaarden

Een elektronisch documentbeheersysteem dient naadloos aan te sluiten op de werkprocessen in een organisatie. Daarom is het van groot belang dat er wordt gekozen voor een betrouwbaar, goed functionerend systeem. Het informatiemanagement is primair verantwoordelijk voor de keuze van de applicatie, binnen de randvoorwaarden die het organisatiebrede beleid stelt. Onder informatiemanagement verstaan wij de verantwoordelijkheid voor de efficiënte en systematische controle over het opmaken, ontvangen, onderhoud, gebruik en schoning van documenten. Informatiemanagement[8] omvat het vaststellen van beleid en standaarden voor:

- het toewijzen van verantwoordelijkheden en bevoegdheden;
- het vaststellen en bevorderen van procedures en bevoegdheden;
- het voorzien in een reeks van diensten met betrekking tot het beheer en gebruik van documenten;
- het ontwerpen, implementeren en beheren van gespecialiseerde systemen voor het beheer van documenten;
- het integreren van informatiemanagement in de bedrijfsprocessen en –systemen.

<u>Beleidsmatige voorwaarden:</u>

Een organisatie behoort beleid vast te stellen en te documenteren voor elektronisch documentbeheer. Dit om te verzekeren dat de bedrijfsprocessen te allen tijde worden ondersteund door betrouwbare documenten. Het beleid behoort te worden aangenomen en gesteund door het verantwoordelijke beslissingsniveau. Dit beleid dient vervolgens op alle niveaus binnen een organisatie bekend gemaakt en te worden geïmplementeerd. Het verdient de aanbeveling om het beleid regelmatig te beoordelen en te herzien, om er zeker van te zijn dat het de geldende organisatie- en bedrijfsbehoeften weergeeft.

Het beleid voor elektronisch documentbeheer behoort te worden afgeleid uit een analyse van de gehele bedrijfsactiviteiten en –processen binnen een organisatie. Op deze manier geeft een organisatie zich rekenschap van haar organisatorische omgeving en economische overwegingen.

Hieruit volgen de eisen waaraan het elektronisch documentbeheersysteem dient te voldoen. Dit geeft tevens inzicht waar de voordelen op het gebied van doelmatigheid en doeltreffendheid te behalen zijn, zodat de economische voordelen helder zijn.

[8] Deze definitie is afgeleid van de definitie in NEN-ISO 15489.

Organisatorische voorwaarden:

Verantwoordelijkheden en bevoegdheden met betrekking tot elektronisch documentbeheer behoren te worden vastgesteld, toegewezen en bekendgemaakt aan de gehele organisatie, zodat duidelijk is wie verantwoordelijk is voor het nemen van de benodigde actie. Deze verantwoordelijkheden behoren te worden opgedragen aan alle medewerkers van een organisatie. Het is aanbevolen om functiescheiding en voorgeschreven procedures/werkinstructies in te voeren om een verantwoorde werking van een elektronisch documentbeheersysteem te garanderen.

Technische voorwaarden:

Het is aanbevolen dat de software van een elektronisch documentbeheersysteem de volgende kenmerken bezit om optimaal te kunnen functioneren:

- Het kan een verscheidenheid aan digitale documenten beheren (Office of PDF-document, een afbeelding, een blauwdruk (bijvoorbeeld uit een cad/cam programma), of zelfs een volledige databank).
- Het voorziet het document van metadata voor classificatie en vindbaarheid (indexen). Hierbij valt te denken aan versienummer, datum, eigenaar, klantnummer, factuurnummer, en vele andere). Hiermee wordt het document op alle relevante manieren toegedeeld.
- Het beheert de toewijzing van een document. Bijvoorbeeld: bij wie of bij welke groep het document in bewerking is, wat de toegangsrechten van anderen gedurende die tijd zijn, en dergelijke.
- Het kent versienummers toe, die het mogelijk maken, de historische evolutie van een document te volgen en verschaft daarmee een audittrail.
- Een document kan altijd met het voor de creatie gebruikte programma worden geopend en, indien men daartoe de benodige autorisaties heeft, worden gewijzigd.
- Een geavanceerd systeem biedt de mogelijkheid rechtstreeks op de inhoud van een document te zoeken.

Deze voorwaarden (die antwoord geven op deelvraag 1), worden mede ingevuld door het bestaan van general controls, die nader zijn uitgewerkt in hoofdstuk 3.4.

3.2 Kwaliteitsaspecten

Vanuit audit-perspectief zijn kwaliteitsaspecten vereist om een uitspraak te doen over een elektronisch documentbeheersysteem. Het uitgangspunt vormt een audit conform de regels en standaarden van NIVRA/NOREA[9].

[9] Norea, NV COS 3000

Op grond van keuze voor een 'risk-based' benadering hanteren wij in ons onderzoek de kwaliteitsaspecten zoals gedoceerd op de postgraduate IT-audit opleiding van de VU.

1. Confidentiality: vertrouwelijkheid
2. Integrity: integriteit
3. Availability: beschikbaarheid
4. Auditability: controleerbaarheid

Deze kwaliteitsaspecten hanteren wij om risico's te onderkennen. Bij het detecteren van risico's hebben wij mede gebruik gemaakt van bestaande normenkaders voor archiefbeheer vanwege de overeenkomsten, en zijn wij in discussie gegaan met deskundigen op het gebied van documentmanagement .

Om de risico's vervolgens te mitigeren onderkennen wij beheersmaatregelen. Beheersmaatregelen kunnen wij onderverdelen naar aard en toepassing in de volgende categorieën[10]:

1. Beleidsmatig
2. Organisatorisch
3. Technisch

In de literatuur en de auditpraktijk worden diverse kwaliteitsaspecten gehanteerd. De kwaliteitsaspecten hangen samen met informatiebeveiliging. Informatiebeveiliging verwijst naar bescherming van content tegen inbreuk. Wij hanteren de volgende veelgebruikte indeling voor kwaliteitsaspecten[11]:

Vertrouwelijkheid

Een document is vertrouwelijk indien het document alleen te benaderen is door degene die is gerechtigd om het document te benaderen. De vertrouwelijkheid moet worden gewaarborgd om ongeautoriseerde onthulling tegen te gaan.

Populair: "Heeft alleen een daartoe gerechtigd persoon toegang tot een document"

Integriteit

De integriteit van een document heeft betrekking op het feit dat het volledig en ongewijzigd is. Controlemaatregelen zoals bewaking van toegang, gebruikersidentificatie, geautoriseerde vernietiging en beveiliging behoren te worden geïmplementeerd om ongeautoriseerde toegang, vernietiging, verandering of verwijdering van digitale documenten te voorkomen.

In het geval van digitale documenten dient een organisatie te bewijzen dat enig feilen van het systeem, elke opwaardering of regelmatig onderhoud de integriteit van de documenten niet heeft beïnvloed.

Populair: "Bevat het document de juiste en volledige inhoud "

[10] J.C. van Praat, J.M. Suerink; Inleiding edp-auditing, SDU Uitgevers BV, Den Haag, 2008

[11] NEN-ISO 15489-1:2001,IDT

Beschikbaarheid

Het kwaliteitsaspect beschikbaarheid heeft betrekking op de continuïteit van de informatievoorziening. Documenten moeten ten behoeve van de bedrijfsvoering ten allen tijden beschikbaar zijn. Dit heeft een:

- technische kant: uitval en storingen systeem;
- organisatorische kant: verlies van vitale gegevens; onder andere afgedekt door beveiliging.

Populair: "Kan een document op ieder moment geraadpleegd worden"

Controleerbaarheid

Het aspect controleerbaarheid omvat de mate waarin het mogelijk is vast te stellen dat de informatieverwerking is uitgevoerd in overeenstemming met de eisen ten aanzien van de overige kwaliteitsaspecten. Elke geautoriseerde annotatie, toevoeging of verwijdering in een document behoort expliciet te worden aangegeven en herkenbaar te zijn.

Populair: "Kan van ieder document nagegaan worden wat ermee is gebeurd"

3.3 Risico's

Voor het detecteren van de risico's hebben wij een "Plan – Do – Check – Act"-benadering gebruikt. De "Plan"-fase komt overeen met de pakketkeuze. "Do" ziet op implementatie en het gebruik van het pakket. "Check" is de toetsing en monitoring van de werking van het systeem . En "Act" ziet tenslotte op aanpassingen van het systeem. Dit vindt aansluiting met de verschillende levensfasen van het elektronisch documentbeheersysteem, zoals weergegeven in figuur 3 van hoofdstuk 1.

Een deel van deze benadering is verweven met systeemontwikkeling, dat binnen ons vakgebied OTAP wordt genoemd. De afkorting ***OTAP*** staat voor **O**ntwikkeling, **T**est, **A**cceptatie en **P**roductie. In het kader van deze scriptie kan ontwikkeling evengoed voor selectie staan, waarna test, acceptatie en productie eveneens blijven gelden.

Wij hanteren de eerder beschreven levensfasen voor het implementeren en in productie nemen van een elektronisch documentbeheersysteem. Wij hebben deze fasering gekozen om het raamwerk te kunnen structureren.

Fase 1: Beleidsmatige keuzen

Het startpunt van onderzoeksgebied is de keuze tot het aanschaffen van een elektronisch documentbeheersysteem door een organisatie. Wij beperken ons tot zogenaamde "standaardapplicaties" en laten "maatwerk" buiten beschouwing. Deze keuze is reeds eerder beschreven in de paragraaf over toegepaste systemen ("proven technology").

Om een elektronisch documentbeheersysteem te implementeren is een implementatie-methodologie essentieel. In NEN-ISO 15489 is een methodologie opgenomen voor een duurzaam archiefsysteem. Hierbij dienen de volgende stappen te worden doorlopen:

- Voorbereidend onderzoek;
- Analyse bedrijfsfuncties;
- Identificatie-eisen documenten;
- Beoordeling bestaande systemen;
- Identificatie strategie.

De belangrijkste door ons onderkende risico's:

BEL-01	Er wordt onvoldoende rekening gehouden met bedrijfsdoelstellingen waarbij documentbeheer van belang is.
BEL-02	Het onvoldoende raadplegen van alle betrokkenen functionarissen bij het keuzeproces.
BEL-03	Er wordt onvoldoende rekening gehouden met werkprocessen.
BEL-04	Er wordt onvoldoende rekening gehouden met bedrijfseconomische aspecten.
BEL-05	Er wordt niet gekozen voor de meest geschikte leverancier.
BEL-06	Er wordt onvoldoende rekening gehouden met bestaande architectuur.
BEL-07	Er wordt onvoldoende rekening gehouden met gebruikers (opleiding en wensen).
BEL-08	Er wordt onvoldoende rekening gehouden met onderhoud.
BEL-09	Er wordt onvoldoende rekening gehouden wet- en regelgeving.

De belangrijkste gevolgen van deze risico's zijn dat een systeem op onzorgvuldige wijze wordt geselecteerd en geïmplementeerd. Op voorhand ontstaan er dan problemen die zich gedurende de levensduur van het systeem alleen maar vergroten. Met name bij onzorgvuldige inpassing in de architectuur van de onderneming (BEL-06) en de bestaande werkprocessen (BEL-03) zullen er toekomstige problemen met het elektronisch documentbeheersysteem te verwachten zijn. Ook vanuit bedrijfseconomisch oogpunt is het noodzakelijk om op beleidsmatige wijze een systeem in de organisatie te verankeren. Dit volgt uit de risico's BEL-04, BEL-05 en zelfs BEL-08, onderhoud zal dan immers lastiger en duurder worden. Een onderbelicht aspect is eveneens de gebruikerskant (BEL-07). De medewerkers van een organisatie zijn verantwoordelijk voor de uitvoering van de processen en daarmee de kwaliteit van de informatieverzorging.

Fase 2: Ontwikkeling, Testen en Acceptatie

Na de keuze voor een elektronisch documentbeheersysteem vindt inrichting en implementatie in de bedrijfsprocessen van de organisatie plaats. De implementatie van een elektronisch documentbeheersysteem behoort systematisch te worden uitgevoerd.

In deze fase hebben wij de volgende risico's onderkend:

IMP-01	Het onvoldoende toekennen van verantwoordelijkheden en bevoegdheden.
IMP-02	Het onvoldoende inrichten van het systeem.
IMP-03	Het onvoldoende inrichten van interfaces met andere systemen.
IMP-04	Het onvoldoende opleiden van de gebruikersorganisatie.
IMP-05	Het onvoldoende testen van het systeem voor definitieve ingebruikname.
IMP-06	Het ontbreken van acceptatie van het systeem door de gebruikersorganisatie.

De belangrijkste gevolgen van deze risico's hebben betrekking op de integriteit en vertrouwelijk van de documenten binnen het elektronisch documentbeheersysteem. Testen is een randvoorwaarde om het systeem succesvol te laten werken conform de gestelde eisen. Niet alleen de technische zijde, maar juist de organisatorische aspecten dienen gedegen in de testsets te worden opgenomen. De belangrijkste voordelen van een documentbeheersysteem liggen juist in de verwerking en beheersing van documentstromen. Deze zijn van organisatorische aard, welke met behulp van een technische vertaling worden afgedwongen. Juist deze technische vertaling moet correct werken conform de kwaliteitskenmerken juistheid, volledigheid, tijdigheid.

Bij de implementatie dient de nadruk te liggen op de volgende aspecten:

- Organisatorische processen (vertaling in het systeem);
- Verantwoordelijkheden (logische toegangsbeveiliging).

Fase 3: Productie

Na de implementatie gaat het elektronisch documentbeheersysteem daadwerkelijk worden gebruikt. Tijdens deze productiefase kunnen ondanks een gedegen test- en acceptatietraject toch nog risico's worden onderkend. Het credo "waar gewerkt wordt, worden fouten gemaakt", vereist dat er maatregelen worden getroffen om deze risico's te mitigeren. De risico's kunnen zowel technisch als organisatorisch van aard zijn. De door ons onderkende risico's in de productiefase:

PROD-01	Het document wordt aangeleverd in een onleesbaar formaat.
PROD-02	Het document wordt na creatie niet opgenomen in het systeem.
PROD-03	Het document komt verminkt in het systeem terecht.
PROD-04	Het document komt niet op de juiste plaats in het systeem terecht.
PROD-05	Het document wordt niet juist geclassificeerd in een proces.
PROD-06	Het document is niet beschikbaar bij opvraag.
PROD-07	Het document wordt ten onrechte door een functionaris gecreëerd, geraadpleegd of gemuteerd.
PROD-08	Het document wordt niet conform werkinstructie voor elektronisch documentbeheer behandeld.
PROD-09	Het document wordt niet tijdig behandeld in de workflow.
PROD-10	Het document verliest haar integriteit tijdens opslag.
PROD-11	Onjuiste routering in de workflow.
PROD-12	Het document wordt onrechtmatig vernietigd.

De belangrijkste gevolgen van deze risico's zijn dat bepaalde bedrijfsprocessen niet, onvolledig of onjuist worden uitgevoerd en/of verkeerde beslissingen worden genomen. Dit zijn cruciale risico's die voorkomen moeten worden. De mogelijke gevolgen zijn beschreven in paragraaf 1.1.

Fase 4: Controle werking en onderhoud

De laatste fase ziet op het monitoren en onderhouden van het elektronisch documentbeheersysteem. Een goed functioneren van het systeem dient gewaarborgd te zijn. Aanpassingen aan veranderende omstandigheden, maar ook herstel en onderhoud gedurende de productiefase dienen gewaarborgd te zijn. Een en ander is mede afhankelijk van aspecten die onder de noemer “General Controls” vallen. De bijbehorende risico’s en bijbehorende maatregelen zijn beschreven in paragraaf 3.4. In deze fase onderkennen wij de volgende risico’s:

CONT-01	Het ontbreken van de audittrail van alle ‘bewegingen’ van een elektronisch document.
CONT-02	Het ontbreken van de mogelijkheid om terug te vallen op oorspronkelijke document.
CONT-03	Een foutief werkend elektronisch documentbeheersysteem wordt niet onderkend en/of hersteld.
CONT-04	Het ontbreken van onderhoud van het elektronisch documentbeheersysteem.

De belangrijkste gevolgen van deze risico’s hebben betrekking op de continuïteit en de controleerbaarheid. Als het systeem niet naar behoren functioneert worden de bedrijfsprocessen ondermijnd. Indien achteraf niet meer te reconstrueren valt hoe bepaalde processen zijn verlopen, kan dat kwalijke gevolgen hebben voor de bedrijfsvoering. Tevens vallen onder deze categorie aspecten waarmee de integriteit van gegevens wordt bewaakt.

3.4 Risico’s General Controls

Als men wil steunen op de informatietechnologie in een organisatie kunnen wij onderscheid maken in de zogenaamde general controls, application controls en user controls. Application controls omvatten alle maatregelen in en rond een specifieke toepassing[12]. User controls zijn controles die de gebruiker uitvoert op de uitkomsten van de applicatie.

Op basis van de scope van ons onderzoek besteden wij beperkte aandacht aan de risico’s die samenhangen met de General Controls. De algemene beheersmaatregelen voor IT, general controls genoemd, zijn maatregelen die worden getroffen ten behoeve van de beheersing van de geautomatiseerde informatieverzorging als geheel. Dit zou men kunnen zien als randvoorwaarden voor het functioneren van de organisatie. Dit past in de visie voor het toepassen van een raamwerk met modulair opgezette normenkaders.

[12] Rob Fijneman, Edo Roos Lindgreen, Piet Veltman; Grondslagen IT-auditing, 2005-2008. SDU uitgevers Den Haag

De risico's die samenhangen met de general controls hebben betrekking op:

- continuïteit;
- beveiliging;
- capaciteits- en performance management;
- change management.

Continuïteit

Het continuïteitsrisico geeft aan in hoeverre een organisatie afhankelijk is van informatietechnologie. Een indicator voor deze afhankelijkheid is de tijd die een organisatie kan blijven functioneren zonder gebruik te maken van haar informatietechnologie. In de laatste jaren is de afhankelijkheid van informatietechnologie sterk toegenomen. Continuïteit is daardoor een belangrijk aspect voor het beoordelen van de risico's.

Beveiliging

Beveiligingsrisico geeft aan in hoeverre er inbreuk kan plaatsvinden op de integriteit, vertrouwelijkheid en beschikbaarheid van informatie. Beveiliging valt uiteen in een tweetal aandachtsgebieden, te weten logische en fysieke toegangsbeveiliging. De logische toegangsbeveiliging ziet toe op het verkrijgen toegang tot het systeem en niveaus van toegang tot gebruik van gegevens. Fysieke toegangsbeveiliging ziet toe op fysieke toegang tot ruimtes waar it-componenten staan.

Capaciteit en performance management

Capaciteits- en performancerisico geeft aan in hoeverre het elektronisch documentbeheersysteem voldoet aan haar efficiency- en effectiviteitseisen. Dit heeft met name betrekking op het kwaliteitsaspect beschikbaarheid.

Change management

Risico's met betrekking tot changemanagement hebben betrekking op het niet gewenst functioneren van informatiesystemen als gevolg van wijzigingen in de programmatuur. Een organisatie en haar omgeving zijn voortdurend onderhevig aan veranderingen. De veranderingen kunnen zowel door interne als externe impulsen worden opgeroepen. Een externe factor is niet alleen technologie, maar bijvoorbeeld ook wet- en regelgeving, een veranderende markt en economische ontwikkelingen, zorgen ervoor dat de bedrijfsprocessen aangepast moeten worden. De aanpassingen kunnen een impact hebben op de informatietechnologie, hetgeen gedegen gemanaged moet worden.

4 Raamwerk

4.1 Inleiding

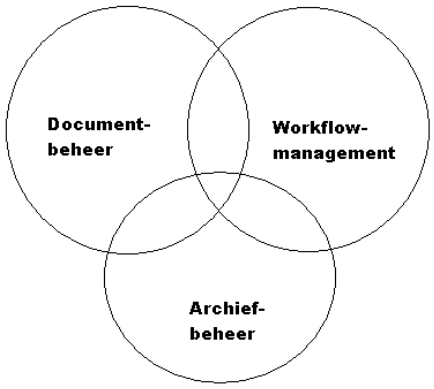
Wij hanteren de stelling dat het weinig zinvol is om een uitgebreid raamwerk te definiëren voor de informatievoorziening als geheel in een organisatie. Immers de beleidsmatige aspecten zijn universeel en kunnen separaat aan de hand van een algemeen raamwerk worden beoordeeld. De proces en organisatorische aspecten kunnen afzonderlijk in een stelsel van opgedeelde normenkaders worden beoordeeld, waarbij een specifiek normenkader is toegespitst op het deel van de organisatie of een proces. Daarbij geldt dat bepaalde organisatorische aspecten sterk verweven zijn met technische oplossingen. Wij veronderstellen dat op dat gebied nog een behoorlijke efficiency-slag gemaakt kan worden, door universele normenkaders in modulaire vorm te definiëren.

Gedurende de literatuurstudie hebben wij vastgesteld dat er algemene normenkaders zijn voor beperkte toepassingsgebieden en dus maar een beperkte bruikbaarheid hebben. Dit zou betekenen dat bestaande best-practices en normenkaders deels uit elkaar getrokken zouden kunnen worden en in logische modules worden opgedeeld. Dit is wellicht een uitdaging voor een volgend scriptieonderwerp.

4.2 Modulaire opzet raamwerk

Wij hebben voor de audit van een elektronisch documentbeheersysteem een raamwerk gedefinieerd, conform de in paragraaf 1.2.3. beschreven onderzoeks-methode.

Bij het inventariseren van de te treffen beheersmaatregelen hebben wij gebruik gemaakt van beschikbare normenkaders, die van toepassing zijn voor informatie- en archiefbeheer. In deze normenkaders ligt de nadruk op record management. Er bestaan zeker raakvlakken tussen archief- en documentbeheer.



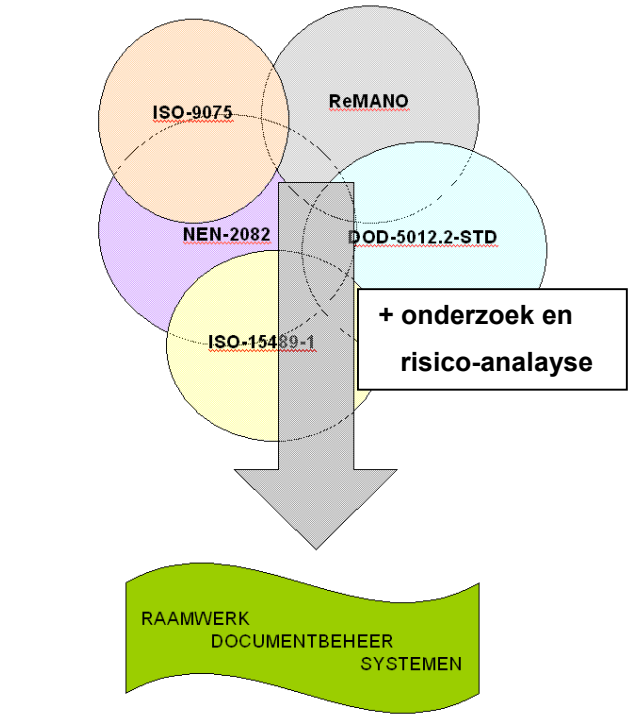
Figuur 6: *Overlap documentbeheer, workflowmanagement en archiefbeheer*

De normenkaders hebben daarom zeker een toegevoegde waarde voor het inventariseren van risico's en de te treffen beheersmaatregelen. Normenkaders voor archiefbeheer:

- In de internationale norm voor informatie- en archiefbeheer (NEN-ISO 15489-1) staan beleidsmatige en organisatorische kaders en randvoorwaarden waaraan een archiefsysteem zou moeten voldoen. Veel van deze voorwaarden zijn van toepassing op een elektronisch documentbeheersysteem.
- Het Amerikaanse ministerie van Defensie, US Department of Defense (DoD), heeft een standaard gepubliceerd voor de minimale functionele eisen voor elektronisch archiefbeheer, DoD 5015.2.
- In Nederland zijn software specificaties voor Records Management Applicaties voor de Nederlandse Overheid (ReMANO) ontwikkeld. Bij de ontwikkeling van ReMANO is mede rekening gehouden met Nederlandse wet en regelgeving op het gebied van archiefbeheer. In juni 2008 is ReMANO vervangen en is NEN 2082 de geldende norm.

Om de volledigheid van de door ons onderkende risico's te valideren hebben wij deze risico's laten beoordelen door deskundigen op het gebied van informatiemanagement en documentbeheer.

Zoals reeds eerder vermeld is dit raamwerk opgezet vanuit principle-based gedachte. In de kolom "Bron(nen)" van het raamwerk wordt verwezen naar een bestaand normenkader, waarin eventueel handvatten te vinden zijn voor verdere uitdieping.



Figuur 7: *Raamwerk op basis van diverse normenkaders*

Wij hebben onderkend dat strakke kaders beperkingen opleggen, en dat men bij het hanteren van normen die te “eng” zijn geformuleerd, onherroepelijk te maken krijgt met enorme hoeveelheden gedetailleerde regels en handvatten, gebaseerd op rule-based uitgangspunten. Dit belemmert een organisatie, ze wordt in een te strak harnas gedwongen. Voor de auditor is het mogelijk een probleem om assurance te geven, indien er op basis van rule based uitgangspunten bepaalde zaken niet conform de norm zijn uitgevoerd.

Afwijkingen van de gestelde norm kunnen wellicht onvoldoende zijn voor het geven van asscurance op rule based basis. Bij het hanteren van principle based uitgangspunten kan de auditor echter op basis van zijn expertise, de kennis van het klant en het object, toch voldoende assurance geven op basis van een professionele afweging.

Wij propageren om een kader te maken waarin de technologie, maar ook de wet- en regelgeving met “open vizier” worden benaderd. Een voorbeeld ter toelichting:

- Technologisch: In het kader van beveiligde toegang kan men een gedetailleerde regel benoemen, die encryptietechnologie voorschrijft, bijvoorbeeld de lengte van de sleutel en encryptietechnologie PGP. Een dergelijke technische regel verandert onherroepelijk in de tijd. De voorkeur verdient een regel te definiëren die stelt dat de data versleuteld dienen te worden opgeslagen met afdoende beveiliging.
- Regelgeving: een soortgelijke stelling geldt voor regelgeving en wetten. Deze zijn veranderlijk en normen dienen daarom onafhankelijk daarvan te worden opgesteld, zodat de duurzaamheid en bruikbaarheid van een normenkader verantwoord kunnen worden opgesteld.

Daarbij gaan wij er tevens vanuit dat in het informatiebeleid (en/of beveiligingsbeleid) van de organisatie is opgenomen dat technologische ontwikkelingen met regelmaat worden getoetst aan de stand van zaken binnen de organisatie.

4.3 Raamwerk toetsingsnormen Elektronisch Documentbeheersysteem

In het raamwerk zijn de toetsingsnormen opgenomen die gebruikt kunnen worden voor het beoordelen van de aanschaf, implementatie en werking van een elektronisch documentbeheersysteem. Het uitfaseren laten wij in het kader van het onderzoek buiten beschouwing.

De commissie Normen en Standaarden van de NOREA heeft de volgende vereisten met betrekking tot normen vastgesteld:

- objectief (normen zijn vrij van persoonlijke beïnvloeding);
- eenduiding (normen zijn concreet);
- relevant (normen zijn bepaalde audit-opdrachten).

Uitgangspunt is dat de normen geldig zijn voor ieder elektronisch documentbeheersysteem.

Het raamwerk bestaat uit een tabel van normen, welke zo compact mogelijk zijn geformuleerd. De indeling is gebaseerd op de centrale vraagstelling van het onderzoek. Bij een audit op een systeem zal doorgaans vanuit een bepaalde invalshoek worden getoetst. Het voegt weinig toe om een audit op de gehele levenscyclus van het systeem uit te voeren.

Risico	Voor-waarde	Norm	Bron(nen)
ALG	BELEID	De noodzakelijke “general controls” zijn randvoorwaardelijk aanwezig.	---
BEL-01	BELEID	De organisatie heeft voorafgaand aan het besluit om een elektronisch documentbeheersysteem in gebruik te nemen, de hiermee te realiseren doelstellingen vastgesteld.	ISO 15489-1:2001 8.4.a
BEL-01	BELEID	De organisatie beschikt over een door het verantwoordelijk management goedgekeurd plan van aanpak, alvorens het besluit te nemen om een elektronisch documentbeheersysteem in gebruik te nemen.	---
BEL-02	BELEID	De organisatie heeft alle van belang zijnde functionarissen geraadpleegd voorafgaand aan het besluit om een elektronisch documentbeheersysteem in gebruik te nemen.	ISO 15489-1:2001 8.4.b
BEL-02 BEL-03	BELEID	De organisatie heeft alle bedrijfsprocessen en transacties geïnventariseerd en gedocumenteerd, voorafgaand aan het besluit om een elektronisch documentbeheersysteem in gebruik te nemen.[13]	ISO 15489-1:2001 8.4.b
BEL-03	BELEID-TECHN	De gekozen applicatie ondersteunt de validatie van de registratiegegevens, volgens de door de organisatie opgestelde regels voor termijnen, formaten etc..	DoD 5015.2-STD (2002) C4.1.1. C2.2.3.4. C2.2.3.10 en C2.2.3.11.
BEL-04	BELEID	De organisatie heeft rekening gehouden met de door het verantwoordelijk management goedgekeurde kosten-batenanalyse.	---

[13] *Toelichting:* De applicatie dient te voorzien in de mogelijkheid om de workflows te definiëren. Dit in termen van behandelstappen, behandelstatus, prioritering obv gedefinieerde voorwaarden en gebruikers, rollen, en profielen.

BEL-05	BELEID	De organisatie heeft de keuze voor een leverancier van een elektronisch documentbeheersysteem bepaald op basis van een vooraf door het verantwoordelijk management goedgekeurde voorwaarden.	---
BEL-06	BELEID-TECHN	De organisatie heeft bij de keuze voor een elektronisch documentbeheersysteem rekening gehouden met de facto en de jure standaarden.[14]	ISO 9075 en ISO 15489-1:2001 8.4.b
BEL-06	BELEID	De organisatie heeft bij de keuze voor een elektronisch documentbeheersysteem rekening gehouden met aanwezige architectuur.[15]	ISO 15489-1:2001 8.4.d
BEL-07	BELEID	De gekozen applicatie is zodanig toegankelijk dat de werkwijze helder is voor de gebruikers.	---
BEL-07	BELEID	Gebruikers zijn voldoende toegerust om hun taken en verantwoordelijkheden te kunnen uitvoeren.[16]	---
BEL-08	BELEID	De organisatie heeft bij de keuze voor een applicatie rekening gehouden met de uitvoering van het noodzakelijke onderhoud na aanschaf van de applicatie.	---
BEL-09	BELEID	De organisatie heeft bij de keuze voor een applicatie rekening gehouden met eisen op het gebied van wet- en regelgeving.	ISO 15489-1:2001 6.2
IMP-01	ORG	De implementatie van de applicatie is uitgevoerd met behulp van projectplanning, en op de situatie afgestemde methoden met de bedoeling om de werking te integreren met bedrijfsprocessen en verwante systemen.	ISO 15489-1:2001 8.4.g
IMP-01	BELEID	Het verantwoordelijk management van de organisatie heeft verantwoordelijkheden en bevoegdheden met betrekking tot informatie- en documentmanagement vastgesteld en toegewezen, en bekend gemaakt aan de gehele organisatie.[17]	ISO 15489-1:2001 6.3
IMP-01	ORG-TECHN	De applicatie waarborgt dat toegangsbeperkingen tot systeemfuncties zijn opgezet overeenkomstig de rol van gebruikers.	DoD 5015.2-STD (2002)
IMP-02	ORG-TECHN	De applicatie verleent toegangsrechten aan gebruikers overeenkomstig met de beveiligingsniveaus en informatiebehoefte op basis van “need-to-know”.	DoD 5015.2-STD (2002) C2.2.7

[14] *Toelichting:* De technische standaarden hebben betrekking op:
- hardware omgeving (server platforms werkstations);
- operating system omgevingen (bv. Microsoft Windows NT4, 98,2000 – MacOS, Unix);
- industriestandaarden voor gebruikersinterface (Microsoft Windows, Macintosh, X-windows, intranet browser);
- relationele databases;
- netwerk protocollen en operating systems (TCP/IP, Ethernet types, Novell, Microsoft Windows NT servers;
- Codering op verschillende niveaus (ASCII, Unicode16, NEN-ISO/IEC 8859-11:2002 en Adobe Pdf, XML vergezeld van een stylesheet (XML, CSS) of andere gelijkwaardige toepassingsspecificaties;
- applicatie programma interface en ontwikkelinstrumenten (COM, DCOM, COBRA);
- coderingen voor landcodes, munteenheden en talen.

[15] *Toelichting:* Het systeem moet dusdanig zijn opgezet, dat het past binnen de gedefinieerde architectuur van de organisatie en de eisen die daaraan zijn gesteld in termen van beheer (onderhoud etc.), zodat de continuïteit en beschikbaarheid van het systeem als geheel is gewaarborgd.

[16] *Toelichting:* Gebruikers moeten over de juiste opleiding en vaardigheden beschikken, en bekend te zijn met de werkinstructies en processen die zij uitvoeren.

[17] *Toelichting:* Er is duidelijkheid wie waar verantwoordelijk voor is.

IMP-02	TECHN	De applicatie moet invoer van verplichte registratiegegevens afdwingen.	---
IMP-03	ORG-TECHN	De applicatie voorziet in het overbrengen van bestanddelen en/of documenten naar een andere (interne of externe) applicatie, waarbij de integriteit is gewaarborgd.	---
IMP-04	BELEID	Gebruikers zijn toegerust om hun taken en verantwoordelijkheden te kunnen uitvoeren[18].	---
IMP-05 IMP-06	BELEID	De implementatie, gebruikertest, gebruikersacceptatie en het onderhoud van de applicatie vinden plaats in gescheiden omgevingen[19].	---
PROD-01 PROD-03	TECHN	De applicatie waarschuwt bij poging een incompleet of inconsistent document op te nemen, of maakt dat onmogelijk. Hetzelfde geldt voor een ondersteund formaat.	DoD 5015.2-STD (1997) DoD 5015.2-STD (2002) C2.1.1. en C.2.2.5.3
PROD-02	TECHN	De applicatie waarschuwt als een document niet in het systeem is opgenomen.	---
PROD-04 PROD-06	TECHN	De applicatie biedt de mogelijkheid om documenten op basis van meta-kenmerken te vinden en te raadplegen (unieke identificatie).	DoD 5015.2-STD (2002) C2.2.6.8.1 C2.2.6.8.2 C3.2.9 en C3.2.10.
PROD-05 PROD-08 PROD-09	TECHN	De applicatie presenteert en legt de voortgang van een procesgang vast, zodat gebruikers de behandelstatus van een document of dossier kunnen bepalen.	---
PROD-07	TECHN	De applicatie voorkomt dat de inhoud van een definitieve versie van een digitaal document door gebruikers en/of geautoriseerde gebruikers wordt gemuteerd.	DoD 5015.2-STD (2002) C2.2.3.8
PROD-07	TECHN	De applicatie biedt de gebruikers de mogelijkheid bieden tot het raadplegen en bewerken van de laatste versie dan wel raadpleging van een van de voorgaande versies moet, indien van een document meerdere versies bestaan[20].	DoD 5015.2-STD (2002) C2.2.3.20
PROD-07	TECHN	De applicatie beschikt over de mogelijkheid aan documenten beveiligingsniveaus toe te kennen. De applicatie en ontzegt een gebruiker de toegang tot documenten als daaraan een hoger beveiligingsniveau is toegekend dan de leesrechten van de gebruiker.	DoD 5015.2-STD (2002) C2.2.7 - C4
PROD-07	TECHN	De applicatie waarborgt dat vooraf gespecificeerde registratiegegevens van een document, alleen kunnen worden gemuteerd door de applicatiebeheerder, of een daarvoor door deze daartoe geautoriseerde gebruiker.	DoD 5015.2-STD (2002) C2.2.1.1
PROD-07	TECHN	De applicatie garandeert dat de authenticiteit van een document gewaardborgd blijft.[21]	---

[18] *Toelichting:* Gebruikersmoeten over de juiste opleiding en vaardigheden beschikken, en bekend te zijn met de werkinstructies en processen die zij uitvoeren.

[19] *Toelichting:* conform OTAP-principes.

[20] *Toelichting:* Alle versies van een documenten worden of:
- als één document vastgelegd;
- vernietigd, nadat één versie van het stuk als document is vastgelegd; of
- als afzonderlijke documenten vastgelegd.

[21] *Toelichting:* Dit kan bijvoorbeeld plaatsvinden door een elektronische handtekening.

PROD-08 PROD-09 PROD-11	TECHN	De applicatie bericht een gebruiker als een document ter kennisneming of ter behandeling in diens werkvoorraad is opgenomen.	---
PROD-09	TECHN	De applicatie bewaakt en signaleert reactie- en behandeltermijnen.	---
PROD-09	TECHN	De applicatie beschikt over een workflowfaciliteit[22].	---
PROD-10	TECHN	De applicatie legt essentiële informatie (metadata) van een document vast.[23]	DoD 5015.2-STD (2002) C2.2.3.2 - C2.2.3.17 C2.2.2.4.2
PROD-10 PROD-12	TECHN	De applicatie voorkomt dat een document, na opname, wordt gewist of verplaatst, met uitzondering van de applicatiebeheerder.	DoD 5015.2-STD (2002) C2.2.2.4
CONT-01 CONT-02	TECHN	De applicatie legt iedere actie inzake een verandering aan een document en/of parameterinstellingen vast in een niet muteerbare audit-trail[24].	DoD 5015.2-STD (2002) C2.2.8.1
CONT-01	TECHN	De applicatie behoudt registratiegegevens van bestanddelen en documenten die vernietigd, overgebracht of geëxporteerd zijn.	DoD 5015.2-STD (2002) C2.2.6.5.5
CONT-01 CONT-02	TECHN	De applicatie ondersteunt de registratie van digitale documenten door registratiegegevens en/of audittrail gegevens toe te voegen voor in beginsel elk type document.	DoD 5015.2-STD (2002) C2.2.8.1-C3.2.7
CONT-01	TECHN	De applicatie legt essentiële informatie vast tijdens het uitvoeren van wissen of verplaatsen door een applicatiebeheerder.[25]	DoD 5015.2-STD (2002) C2.2.2.4

[22] *Toelichting:* Dit ter ondersteuning van het toekennen van bewaartermijnen , beoordelingen en het overbrengings-, export- of vernietigingsproces. Dit valt te realiseren door het vastleggen van:
- voortgang of status van een beoordeling, zoals 'in afwachting van' of 'in behandeling', inclusief gegevens over de geautoriseerde gebruiker die het proces uitvoert en de datum;
- gegevens over bestanddelen of documenten die wachten op;
- overbrenging, export of vernietiging als gevolg van een beoordelingsbeslissing;
- voortgang van het overbrengings-, export en/of vernietigingsproces.

[23] *Toelichting:* Het betreft de volgende essentiële elementen:
- de inhoud en integriteit van het digitale document inzake vorm, structuur en (optioneel) gedrag (bijvoorbeeld, alle componenten van een emailbericht met attachment(s), of van een web pagina met hyperlinks);
- gegevens over het digitale document (bijvoorbeeld de naam);
- de datum van creatie en andere gegevens over de elementen van het document;
- gegevens over de context waarin het digitale document is ontstaan en afgekondigd, bijvoorbeeld de werkprocessen, de oorspronkelijke eigenaar(s) en de auteur(s);
- gegevens over de applicatie (inclusief de versie daarvan) die het document heeft gegenereerd.

[24] *Toelichting:* Hierbij vindt de volgende registratie en opslag van gegevens plaats:
- door de organisatie gespecificeerde handelingen uitgevoerd met betrekking tot documenten;
- de gebruiker die de handeling uit voert;
- de datum en tijd van de uitvoering van de handeling.

[25] *Toelichting:* Het betreft de volgende essentiele elementen:
- de handeling vastgelegd in de audittrail;
- de gehele inhoud van een bestanddeel gewist of verplaatst;
- er voor zorg gedragen dat geen documenten worden gewist die ook deel uitmaken van een andere rubriek en/of bestanddeel;
- er voor zorg gedragen dat uitdrukkelijk toestemming wordt gevraagd om de betreffende handeling uit te voeren, indien een koppeling of link aanwezig is vanuit een ander bestanddeel of een andere registratie.
- er voor zorg gedragen dat de volledigheid, integriteit en duurzaamheid van de registratiegegevens en eventuele andere metadata wordt gehandhaafd.

CONT-03	TECHN	De applicatie beschikt over een automatische back-up- en herstelfunctie of heeft toegang tot een gerelateerde automatische back-up en herstelfunctie. De integriteit van de gegevens gedurende en na deze rollback zijn gewaarborgd.	DoD 5015.2-STD (2002) C2.2.9.3 C2.2.9.3.1 C2.2.9.3.2 C2.2.9.4.
CONT-04	BELEID-TECHN	De applicatie wordt volgens vooraf gedefinieerde eisen onderhouden[26].	---

Naast dit raamwerk geld voor informatiesystemen in het algemeen dat er een set van universele normen geldt:

- Van de gehele ISO 9075 Information technology – database languages – SQL worden door het Nederlands Normalisatie Instituut alleen de volgende normen ondersteund: NEN-ISO/IEC 9075:2000/C1:2001en, NEN-ISO/IEC 9075-1:2000en, NEN-ISO/IEC 9075-1-2-5:2000/A1:2001en, NEN-ISO/IEC 9075-10:2000en, NEN-ISO/IEC 9075-2:2000en, NEN-ISO/IEC 9075-3:2000en, NENISO/IEC 9075-4:2000en, NEN-ISO/IEC 9075-5:2000en, NEN-ISO/IEC 9075-9:2001en.
- NEN-ISO 8601:1994 en Data-elementen en uitwisselingsformats; Gegevensuitwisseling; Weergave van datum en tijd.
- NEN-EN-ISO 3166-1:1997 en Codes voor de weergave van landnamen en hun onderverdelingen; Deel 1: Landencodes.
- NEN-ISO 639:1989 nl Code voor namen van talen.
- NEN-EN-ISO 4217:2001 codes voor de weergave van valuta's.

[26] *Toelichting:* Hierbij vat te denken aan releases, updates en patches.

4.3.1 Raamwerk Elektronisch Documentbeheersysteem schematisch

Het beschreven raamwerk bestaat uit een tabel van normen, welke door ons zo compact mogelijk zijn geformuleerd. Deze indeling is gebaseerd op de centrale vraagstelling van het onderzoek. In hoordstuk 1 hebben wij de lifecycle van een elektronisch documentbeheersysteem beschreven, waarbij wij de fasen Selectie, Implementatie, Productie en Onderhoud/Beheer onderkennen.

Een audit op een systeem zal doorgaans vanuit een bepaalde invalshoek worden getoetst; het voegt weinig toe om een audit op de levenscyclus van het systeem uit te voeren. Om die reden hebben wij de risico's in een onderstaande matrix opgenomen, zodat op een overzichtelijke manier de normen gekozen kunnen worden ten behoeve van een specifieke audit.

	Selectie	Implementatie	Productie	Onderhoud
Beleid	BEL-01, BEL-02, BEL-03, BEL-04, BEL-05, BEL-07, BEL-09	IMP-01, IMP-02, IMP-04, IMP-05, IMP-06		CONT-04
Organisatie	BEL-01, BEL-02, BEL-03, BEL-04, BEL-05, BEL-07, BEL-09		PROD-05, PROD-07, PROD-08, PROD-09, PROD-11, PROD-12	CONT-01, CONT-03
Technisch	BEL-06, BEL-08	IMP-02, IMP-03	PROD-01, PROD-02, PROD-03, PROD-04, PROD-06, PROD-10	CONT-02

Tabel 5: *Matrix risico's*

5 Toets externe deskundigen

5.1 Toetsing Argitek

Wij hebben prof. dr. ir. Wouter Keller en drs. Michael Roovers van M&I Argitek (e-business architects) bereid gevonden om hun deskundige mening over onze bevindingen te laten schijnen. Arigitek is een bedrijf dat organisaties begeleid bij het implementeren van zogenaamde zaak-systemen[27], welke in grote mate dossier- en archief zijn georiënteerd. Zij hebben omvangrijke ervaring op dit gebied en waren zeer geïnteresseerd in een normenkader dat het onderzoeksgebied afdekte.

5.1.1 Bevindingen

Wouter Keller adviseerde ons om het normenkader zo compact mogelijk te houden. “Beperk het bij voorkeur tot maximaal 30 normen”. Daarnaast heeft hij ons geadviseerd om de formulering van de normen stelliger en algemener te houden. Dit heeft naar onze mening geleid tot een robuuster normenkader, waarbij de bronvermelding beter tot zijn recht komt. In eerste instantie hadden wij een directe relatie met de bron door de norm direct daaraan te ontlenen. Door de norm meer “principle-based” te herformuleren voldoen wij in sterkere mate aan onze doelstelling “principle-based”. Verdieping is eventueel te vinden in de gerelateerde bron.

Michael Roovers heeft met name integrale aanbevelingen gedaan op de consistentie van de tekst, en inhoudelijke verbeteringen geadviseerd. Deze aanbevelingen hebben de tekst structureel sterker gemaakt en beter in samenhang gebracht.

5.2 Toetsing HEC

Namens het Het Expertise Centrum (HEC) hebben wij een gesprek gevoerd met Boudien Glashouwer RE RI CISA en ir. Auke Bloembergen over de bevindingen van ons onderzoek. Het Expertise Centrum levert consultants voor ICT en bestuur in de publieke sector. Boudien Glashouwer is in de praktijk veel werkzaam op het gebied van digitalisering en duurzame archivering. Denk daarbij aan het digitaliseren van processen bij een ministerie of gemeente of de ontwikkeling van een digitaal depot. Auke Bloembergen is van oorsprong Civiel Ingenieur, maar is de automatisering ingerold en bezit veel kennis op het gebied informatiemanagement, systeemontwikkeling en –beheer.

[27] Zaakgericht werken: koude en warme digitale dossiers, W.J. Keller (Argitek)

5.2.1 Bevindingen

Boudien Glashouder benadrukte dat wij er ons bewust van moeten zijn dat een audit altijd start met “Understanding the bussiness”. Het in kaart brengen van de doelstellingen en de kritische succesfactoren van een organisatie is van essentieel belang om een normenkader effectief te kunnen toepassen. Een audit mag niet resulteren in het afvinken van normen zonder deze in context met de activiteiten van een organisatie plaatsen.

Het is bij aanvang van een audit van belang of een organisatie zelf een risico-analyse heeft uitgevoerd. De nadruk dient hierbij te liggen op het totstandkomingsproces, zijn bijvoorbeeld alle belanghebbenden bij de risico-analyse betrokken. Het in kaart brengen van de wijze waarop een organisatie een risico-analyse heeft uitgevoerd is van belang in welke mate een auditor kan steunen op deze analyse. Dit verhoogt de effectiviteit en efficiency van een audit.

De nadruk is ons gesprek lag met name op het gebied van recordmanagement. In onze opinie vinden zowel Boudien Glashouwer als Auke Bloembergen het jammer dat wij de “koude” documenten buiten ons ondergebied hebben gelaten.

5.3 Toetsing Van Bussel Document Services

Dr. Geert Jan van Bussel is oprichter van Van Bussel Document Services, een consultancy bureau op het vlak van document-, record management en content auditing. In 2009 is Geert-Jan van Bussel gepromoveerd met een proefschrift over verantwoording in en door organisaties en de relatie daarvan met de archivering van informatie.

Geert-Jan van Bussel was betrokken bij het samenstellen van het ReMANO 2004 en heeft namens de Stichting Certificatie ReMANO als ReMANO-Auditor opgetreden. Hij treedt nu op als auditor voor de NEN-ISO-normen NEN 2082 en NEN-ISO 15489. Hij is als docent verbonden aan de Hogeschool van Amsterdam en de Universiteit van Amsterdam.

5.3.1 Bevindingen

Geert Jan van Bussel benadrukte een aantal zaken waarmee een auditor rekening moet houden bij de uitvoering van een audit van een elektronisch documentbeheersysteem. In de praktijk onderkent Geert-Jan van Bussel dat organisaties onvoldoende beseffen dat geautomatiseerde informatievoorziening leidend is geworden. Organisaties zijn afhankelijk van documenten in geautomatiseerde omgevingen. Tijdens processen worden aan documenten data toegevoegd. Deze data moeten tevens als documenten worden beschouwd. Dit zijn bijvoorbeeld records met een status van een document.

Daarnaast maakte Geert-Jan van Bussel een belangrijk onderscheid tussen de technische en de organisatorische beheersmaatregelen. De technische maatregelen zijn volgens hem ondergeschikt omdat ze deze maatregelen ondersteunend zijn aan de gekozen organisatorische maatregelen. De gekozen technische oplossing door de softwarefabrikant is niet meer te beïnvloeden. Daarnaast geldt nog dat een technische oplossing in feite alleen beoordeeld kan worden door een toetsing van de broncode.

Geert-Jan van Bussel stelt dat het van belang is om een auditor voorafgaand aan de implementie van een elektronisch documentbeheersysteem te betrekken. Hierdoor kan worden gewaarborgd dat voldoende rekening wordt gehouden met de beleidsmatige aspecten van de organisatie.

5.4 Toetsing IT-Auditor Belastingdienst

Fred de Grunt RA is een ervaren IT-auditor bij de Belastingdienst. Fred de Grunt is werkzaam in het segment Zeer Grote Ondernemingen en heeft veel ervaring met vraagstukken op het gebied van bewaarplicht. Fred de Grunt is lid van het landelijk kennisnetwerk EDP-auditing van de Belastingdienst, en is lid van de commissie die zich bezig houdt met pakketonderzoeken.

5.4.1 Bevindingen

Met Fred de Grunt hebben wij in een sessie uitgebreid gediscussieerd over de normen die wij in het definitieve concept van ons raamwerk hadden opgenomen. Het resultaat van deze sessies is dat wij het aantal normen hebben gereduceerd van 59 in de conceptfase naar 41. Een aantal normen zijn “scherper” geformuleerd. De vermindering van het aantal normen sluit aan bij de wens van Wouter Keller om het het raamwerk zo compact mogelijk te houden.

Fred de Grunt heeft tevens de consistentie in de tekst beoordeeld en volledigheid van de risico’s geverifieerd. Dit heeft een positieve bijdrage geleverd aan de kwaliteit van het raamwerk en de scriptie als geheel.

6 Samenvatting en conclusie

Deze scriptie is geschreven in het kader van de postgraduate IT-audit opleiding aan de Vrije Universiteit van Amsterdam. De doelgroep van de scriptie zijn IT-auditors, maar vanzelfsprekend kunnen ook andere belanghebbenden en/of geïnteresseerden gebruik maken van deze scriptie.

Het onderzoeksobject van deze scriptie is een elektronisch documentbeheersysteem. Om te komen tot een raamwerk voor een audit op een elektronisch documentbeheersysteem hebben wij een aantal deelvragen beantwoord.

De eerste twee deelvragen, “Welke beleidsmatige, organisatorische en technische voorwaarden spelen een rol bij het inrichten en beheren van een elektronisch documentbeheersysteem” en “Welke risicogebieden kunnen worden onderscheiden bij elektronische documentsystemen en op welke wijze kunnen adequate beheersmaatregelen worden genomen”, hebben een directe relatie met een audit. Deze vragen bepalen de scope en brengen de risico’s in beeld. De derde en laatste deelvraag, “Welke elementen en kenmerken bevat een IT-audit control- framework voor elektronische documentsystemen”, is bedoeld om de bevindingen in balans te brengen met de taak van een auditor; een oordeel geven.

In de literatuur blijkt hoe beleid, organisatie en techniek een onlosmakelijk geheel vormen om systemen op een juiste manier in een organisatie te implementeren en te laten functioneren. Dit beeld wordt aangevuld met implementatietrajecten die deskundigen hebben beschreven, waarbij organisaties vaak in de valkuil vallen door onvoldoende beleidsmatig te werk te gaan. Hierdoor wordt een systeem geïmplementeerd, waarbij onvoldoende wordt rekening gehouden met continue ontwikkelingen in de omgeving. Met name flexibiliteit op aanpassingen van omgevingsvariabelen zoals wettelijke aspecten, organisatieveranderingen en daarmee gepaarde procesaanpassingen blijken moeilijk realiseerbaar. Een belangrijke nevenconclusie die we daarmee willen trekken is:

De beginfase van de lifecycle van een elektronisch documentbeheersysteem is bepalend. Wanneer er tijdens het keuzeproces onvoldoende rekening wordt gehouden met bestaande bedrijfsdoelstellingen, bedrijfsprocessen, gebruikers en technische infrastructuur is de implementatie van een elektronisch documentbeheersysteem gedoemd te mislukken.

De organisatorische en technische voorwaarden zijn het meest concreet beschreven in de literatuur. Deze zullen in de praktijk het best worden uitgewerkt. De risico’s die wij onderkennen op beleidsmatig gebied zijn daardoor het belangrijkst. Vanuit de auditpraktijk is een onderzoek voornamelijk gericht op het functioneren in de actualiteit, waarbij de aandacht voornamelijk uitgaat naar risico’s op het gebied van productiefase van het systeem. De analyserende vraag omtrent de risicogebieden en de beheersmaatregelen hebben wij daarom expliciet gericht op de afzonderlijke fasen Beleid, Implementatie, Productie en Controle.

Op deze wijze hebben wij risico's en maatregelen inzichtelijk gemaakt naar de verschillende fasen van de lifecycle van een elektronisch documentbeheersysteem. Als nevenproduct levert dat een matrix op, dat een hulpmiddel is voor de auditor bij een specifieke audit.

Als samenvattende conclusie stellen wij dat we een compact raamwerk hebben gecreëerd uitgaande van de antwoorden op de deelvragen, daarmee antwoord gevend op de centrale onderzoeksvraag:

Welke beleidsmatige en organisatorische maatregelen spelen een rol bij de inrichting van een elektronisch documentbeheersysteem om te waarborgen, dat documenten gedurende de gehele levensduur in oorspronkelijke en onveranderde vorm beschikbaar zijn, en welke technische aspecten ondersteunen deze maatregelen?

Bij het formuleren van deze onderzoeksvraag hebben wij ons gerealiseerd dat het voor een scriptie-onderwerp breed geformuleerde vraag is. Met dat in gedachte stond het ons voor ogen om de onderzoeksvraag te beantwoorden in de vorm van een algemeen raamwerk, op een redelijk abstract niveau. Het formuleren van de normen in het raamwerk is gebaseerd op de 'principle-based' gedachte.

De ruime onderzoeksvraag heeft als voordeel dat de toepasbaarheid van het raamwerk breed is, maar vraagt van de auditor daarentegen wel een keuze te maken welke diepgang hij wil hanteren. Het raamwerk verwijst naar onderliggende gepubliceerde en breed geaccepteerde normenkaders die gebruikt kunnen worden om verder invulling te geven bij de uitvoering van een audit. Dit heeft het voordeel dat de IT-auditor weloverwogen kan kiezen waar hij de accenten wil en/of moet leggen, op basis van zijn 'professional judgement'.

Het raamwerk is geverifieerd door externe deskundigen. Deze deskundigen beschikken over een schat aan ervaring op het gebied van het implementeren en het auditen van een elektronisch documentbeheersysteem. Door deze verificatie is de kwaliteit van het raamwerk naar onze mening gewaarborgd.

7 Reflectie

Tijdens onze werkzaamheden bij de Belastingdienst zijn wij de afgelopen tijd in toenemende mate geconfronteerd met “elektronische documenten”. Tot voor de scriptie was dit een redelijk onbekend terrein, waarbij wij in beperkte mate bekend waren met de risico’s die samenhangen met elektronisch documentbeheer. Tijdens het literatuuronderzoek, en gesprekken met deskundigen hebben wij hierover veel kennis verkregen. Hierdoor hebben wij ervaren dat de bij aanvang geformuleerde onderzoeksvraag breed is, waardoor het raamwerk algemeen is gebleven. Een uitdaging om in een vervolgonderzoek een deelaspect uit de lifecycle diepgaand te onderzoeken. Het door ons geformuleerde brede raamwerk heeft als voordeel dat het toepasbaar is op de totale lifecycle van een elektronisch documentbeheersysteem. Door modulaire opbouw is het mogelijk om in een specifieke situatie slechts een gedeelte uit het raamwerk te gebruiken.

Na het definiëren van onze centrale vraagstelling hebben wij, op basis van onze theoretische bagage en discussies met deskundigen, een antwoord gegeven op deze vraagstelling in de vorm van een raamwerk. Het samenstellen van het raamwerk levert een bijdrage aan de kwaliteit van onze toekomstige werkzaamheden. De vele gesprekken met begeleiders en deskundigen leidden meerdere malen tot nieuwe inzichten. De afwegingen die wij daarbij hebben moeten maken wat wel of niet mee te nemen in onze scriptie, hebben bijgedragen aan de ontwikkeling van ons “professional judgement”. De toegenomen kennis is meteen gebleken bij een specifiek pakketonderzoek, waarbij we een door collegae opgesteld raamwerk kritisch hebben kunnen beoordelen en de nodige verbeteringen hebben kunnen voorstellen.

Het schrijven van deze scriptie was uitdagend, stimulerend en prettig. Het volgen van de ontwikkelingen op het gebied elektronisch documentbeheer zal in ieder geval een uitdaging blijven. Organisaties zullen in toenemende mate afhankelijk zijn van geautomatiseerde informatiesystemen en de bewustwording daarvan lijkt achter te blijven. Een blijvende “zorg” voor de it-auditor.

8 Literatuurlijst

Richtlijnen:

- Department of Defense (US) 5015.2, Design criteria for electronic records manangement software applications;
- NEN-ISO 15489-1, Informatie en archiefmanagement - Deel 1: Algemeen;
- NEN-ISO 15489-2, Archiefbeheer - Deel 2: Richtlijnen;
- NEN-ISO 23081-1, Informatiebeheer (deel 1: processen);
- NEN-ISO 23081-2, Information and documentation – (deel 2: implementation);
- NEN-ISO-2082, Eisen voor functionaliteit van informatie- en archiefmanagement in programmatuur;
- REMANO, Softwarespecificaties voor Records Management Applicaties voor de Nederlandse overheid (2004); Drs. G.J van Bussel MBA, P.J. Horsman MSc., Drs. H. Waalwijk.

Regelgeving-overheid

- Archiefregeling 2010: Staatscourant nr. 70, 6 januari 2010;
- Bewaren en bewijzen: ISBN 978-90-76957-21-0 ECP.NL, maart 2007,
- Compliance en IT Beheer 2006: Impact van wet- en regelgeving op het beheer van de informatievoorziening, ISBN 90-52610492-X,
- Voorschrift Informatiebeveiliging Rijksoverheid – Bijzondere Informatie (VIRBI).

Literatuur

- BCT, Documentmanagementonderzoek. Cantab Marketing Services BV , september 2005;
- Cobit-ISO-15489 - Alignement , november 2009;
- De moderne informatiehuishouding van de digitale overheid, Albert G. Arnold, Boudien Glashouwer, juni 2005;
- Digitaal documentbeheer: orde in de digitale chaos, dr J.J.M. Uijlenbroek, consultant Het Expertise Centrum, oktober 1998;
- Digitale documenten en processen, Wouter J. Keller, 2008;
- Grondslag IT-auditing, Rob Fijneman, Edo Roos Lindgreen, Piet Veltman, sept 2008;
- Informatiebeveiliging onder controle, Paul Overbeek, Edo Roos Lindgreen, Marcel Spruit, druk: juni 2007;
- Inleiding EDP-auditing, J.C. van Praat, J.M. Suerink, druk: aug 2008;
- Op zoek naar de herinnering …. Verantwoordingssystemen, content-intensieve organisaties en performance, G.J van Bussel, F.F.M. Ector, druk: 2009;
- Rapport Digitaal archiefbeheer in de praktijk, Filip Boudrez, Hannelore Dekeyzer, juli 2004;
- Zaakgericht werken: koude en warme digitale dossiers. F.J. Kuiper, T.G.J. Koster, A.J. Damstra, W.J. Keller, druk: 2008.

Bijlage 1: Begrippen

Tijdens het onderzoek bleek dat een aantal begrippen met betrekking tot ons onderzoek op diverse wijze worden uitgelegd, in verschillende bronnen. Vanwege deze problematiek, welke wij niet kunnen oplossen, geven wij hieronder een verdergaande beschrijving van begrippen in de totale context, en begrippen die in de tekst nog niet zijn gedefinieerd.

Archiefdocument

Een document dat in het verleden is ontvangen of gemaakt, en wordt gebruikt bij de uitvoering van processen, taken en activiteiten.

Audit-trail

Een audit-trail registreert handelingen automatisch en slaat deze registraties zonder manuele tussenkomst op. Een audit-trail mag op geen enkele wijze worden aangepast of verwijderd door ongeacht welke gebruiker. De applicatie moet (pogingen tot) inbreuken op de toegangscontrole in de audit-trail vastleggen.

Digitaal document

Een document in digitale vorm. Een digitaal document kan digitaal zijn ontstaan, maar ook een oorspronkelijk papieren document betreffen dat is gedigitaliseerd, bijvoorbeeld door scanning en eventueel voorzien van *optical character recognition*.

Digitalisering

Het converteren van papieren documenten naar digitale documenten, doorgaans door middel van scanning. In het algemeen de ontwikkeling binnen organisaties waarbij een toenemend deel van de documentaire activiteiten in digitale vorm plaats vinden.

Document

Zie paragraaf 1.2.1.3.

Documentaire informatievoorziening (DIV)

Het beheren, archiveren, registreren en beschikbaar stellen van documenten binnen een organisatie. Deze werkzaamheden worden uitgevoerd zowel voor interne als externe klanten. Dit geldt voor digitale en papieren documenten. Dit is een wat oudere term, maar kan als overkoepelend begrip worden beschouwd als men deze vertaald naar de hedendaagse tijd en de beperking “papieren” weghaalt. Onder de paraplu van DIV kunnen dan ECM en DMS worden gepositioneerd.

Documentbeheer

Het beheer van documenten tijdens het bedrijfsproces.

Documentmanagementsysteem (DMS)

Synoniem voor Documentbeheersysteem. Een DMS speelt in een organisatie vaak een belangrijke rol als facilitator van bepaalde processen binnen een organisatie[28] .

Document registratiesysteem

Software, specifiek ter ondersteuning van het vastleggen van (archivistische) metadata van (archief)documenten

Dossier

Logisch geheel van documenten die betrekking hebben op een zaak of een object.

Enterprise Contect Management

Zie paragraaf 1.2.1.

Informatiemanagement

Informatiemanagement is een vakgebied binnen het management. Het houdt zich bezig met het leiden en sturen van de wijze waarop organisaties in hun informatiebehoefte kunnen voorzien.

Workflowmanagement

Beheer en sturing van processen. Workflowmanagement gaat vaak “hand in hand” met een DMS, omdat veel processen met behulp van een documentstroom worden ondersteunt en uitgevoerd. Middels workflowmanagement kunnen documentstromen binnen processen worden gestructureerd en beheerst.

[28] Zaakgericht werken: koude en warme digitale dossiers (blz 13), W.J. Keller (Argitek)

Bijlage 2: Lijst met belangrijkste afkortingen:

AO/IC	Administratie Organisatie / Interne Controle
COBIT	Control Objectives for Information and related Technology
DoD	US Department of Defense
ECM	Enterprise Content Management
EDP	Electronic Data Processing
HEC	Het Expertise Centrum
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
IT	InformatieTechnologie
ITGI	IT Governance Institute
NEN	NEderlandse Norm
NIVRA	Nederlands Instituut Van Registeraccountants
NOREA	Nederlandse Orde van EDP-Auditors
ReMANO	Records Management Applicaties voor de Nederlandse Overheid
SaaS	Software as a Service

Bijlage 3: Gebruikte figuren en tabellen