Evaluatie van Beveiliging en Privacy in Architectuurdocumentatie

MASTER THESIS INFORMATIEKUNDE

Begeleider: prof. dr. D.B.B. (Daan) Rijsenbrij

ing. Y.H.C. (Yves) Janse
Afstudeernummer 46 IK

Colofon

Naam:	ing. Y.H.C. (Yves) Janse
Studentnummer:	0515760
Afstudeernummer:	46 IK
Opleiding en Richting:	Informatiekunde en Digitale Architectuur
Plaats en Datum:	Nijmegen, juni 2007
Begeleider:	prof. dr. D.B.B. (Daan) Rijsenbrij
Referent:	prof. dr. H.A. (Erik) Proper
Faculteit:	Faculteit der Natuurwetenschappen, Wiskunde & Informatica
Instituut:	Nijmeegs Instituut voor Informatica en Informatiekunde Radboud Universiteit Nijmegen, Nederland
Versie en Status:	1.0 – Definitief

"Any real-world system is a complicated series of interconnections. Security must permeate the system: its components and connections."

Bruce Schneier [25]

Voorwoord

Deze afstudeerscriptie heb ik geschreven in het kader van mijn afstudeeronderzoek als student *Informatiekunde* aan het Nijmeegs Instituut voor Informatica en Informatiekunde van de Radboud Universiteit te Nijmegen voor het behalen van de titel Master of Science (*MSc*).

Ik wil graag van de gelegenheid gebruik maken om mijn begeleider prof. dr. Daan Rijsenbrij en referent prof. dr. Erik Proper te bedanken voor hun begeleiding en commentaar tijdens het project. Hiernaast wil ik ook mijn dank uitspreken aan de personen die voor mij tijd hebben vrijgemaakt om tijdens interviews en gesprekken mee te denken en inzicht en kennis te delen zonder welke deze scriptie niet mogelijk was geweest. Deze personen waren in willekeurige volgorde Bart Jacobs, Martijn Oostdijk en Wouter Teepe van de groep Security of Systems van de Radboud Universiteit Nijmegen; Aaldert Hofman en Ben Elsinga van Capgemini en Dries Bartelink, Andre van der Valk en Menno Gmelig Meijling van de Gemeente Amsterdam. Als laatste wil ik in het bijzonder Guido Chorus en Chris Nellen bedanken voor de goede samenwerking en de vele uren die we hebben gediscussieerd.

Nijmegen,
juni 2007

Yves Janse

Noot over terminologie

In deze scriptie zult U zowel Nederlandstalige als Engelstalige termen tegenkomen. Een deel van de vaktermen is van oorsprong Engelstalig en zal ook in die vorm gebruikt worden. Er is bewust gekozen om deze termen niet te vertalen in het Nederlands omdat het de ervaring van de schrijver is dat ook door Nederlandse professionals op het gebied van informatiebeveiliging tijdens interviews en in publicaties de Engelse termen gebruikt worden. Het is onwaarschijnlijk dat een geforceerde vertaling van deze begrippen de leesbaarheid en herkenning ten goede zal komen. Om verwarring te voorkomen is het gebruik van de termen zo consistent mogelijk gehouden en is er op pagina xiii een verklarende woordenlijst opgenomen die de meeste termen in beide talen beschrijft.

Inhoudsopgave

Lijst van Tabellen

Lijst van Afbeeldingen

Samenvatting

Deze scriptie behandelt het individuele derde onderdeel van het afstudeeronderzoek van Yves Janse naar de evaluatie van architectuurdocumentatie. De resultaten van de eerste twee onderdelen zijn opgenomen als aparte bijlagen bij deze scriptie.

Het individuele onderzoek bestond uit het ontwerpen van een aspectscan voor de evaluatie van het aspect Beveiliging en Privacy in architectuurdocumentatie. Deze aspectscan maakt deel uit van de aspectfase van de Architectuurdocumentatie Evaluatiemethode (ADEM) die in het eerste onderdeel van het afstudeeronderzoek is opgesteld. De scriptie is opgedeeld in vijf opeenvolgende delen:

In het deel *Beveiliging, Privacy en Architectuur* worden de belangrijkste begrippen en hun onderlinge samenhang geschetst. Tevens wordt de onderzoeksopzet van deze scriptie in hoofdlijnen beschreven en worden de onderzoeksdoelstelling en de onderzoeksvragen gedefinieerd.

De doelstelling voor het onderzoek dat beschreven is in deze scriptie is als volgt geformuleerd:

> Een invulling geven aan het aspect Beveiliging en Privacy in de vorm van een aspectscan ten behoeve van de Architectuurdocumentatie Evaluatiemethode en deze toetsen met de casus van het Handboek Architectuur van de Gemeente Amsterdam.

Deel II beschrijft het belangrijkste onderdeel van de scriptie: de aspectscan Beveiliging en Privacy. De aspectscan volgt de in de ADEM voorgeschreven indeling in twee deelscans: de voorbereidende aspectscan en de specifieke aspectscan. Beide deelscans worden in detail uitgewerkt in de hoofdstukken 4 en 5. Hoofdstuk 6 bevat een verzameling van bronnen van best practises met betrekking tot beveiliging en privacy. Deze fungeert als aanzet voor een best practises bibliotheek voor de aspectscan Beveiliging en Privacy.

Omdat de aspectscan Beveiliging en Privacy ook getoetst moet worden in de praktijk wordt er in deel III een case study uitgevoerd op basis van het Handboek Architectuur van de Gemeente Amsterdam. De voorbereidende aspectscan kon goed uitgevoerd worden maar de specifieke aspectscan niet. Dit komt doordat de Gemeente Amsterdam de beschrijving van het aspect beveiliging en privacy niet in de architectuurdocumentatie heeft opgenomen maar de losse organisatieonderdelen dit zelf beschrijven. Er worden een aantal aanbevelingen gedaan in hoofdstuk 9 voor de Gemeente Amsterdam op basis van de resultaten van de uitvoering van de case study.

In deel IV wordt er een persoonlijke reflectie gegeven op zowel de ontwikkelde aspectscan en de uitvoering ervan op het Handboek Architectuur, als op de eerder ontwikkelde ADEM. Als laatste worden er nog conclusies getrokken en aanbevelingen gedaan voor toekomstig onderzoek.

Deel V bevat de twee bijlagen *Architectuurdocumentatie Evaluatie: Aanzet tot een methode om architectuurdocumentatie te evalueren* (Bijlage A) en *Evaluatie Handboek Architectuur Amsterdam: Uitvoering van de Globale Fase* (Bijlage B).

Verklarende Woordenlijst

architectuur Architectuur is een verzameling van architectuurprincipes, verbijzonderd naar regels, richtlijnen en standaarden.

architectuurdocumentatie Een verzameling van geschreven documenten, afbeeldingen, schema's en overzichten die de architectuurprincipes, regels, richtlijnen en standaarden bevatten waaruit de architectuur is opgebouwd, aangevuld met de rationale van de architectuur die aantoont hoe de architectuur te herleiden is naar de bedrijfsdoelstellingen en wensen.

aspect Een aspect is een aandachtsgebied dat relevant is voor architectuurdocumentatie.

asset *bedrijfsmiddel, goed*. Een asset is een tastbaar of ontastbaar goed dat waarde heeft voor de organisatie en beveiligd dient te worden. Een voorbeeld hiervan is klantinformatie in een database.

attack *aanval*. Een aanval is een bewuste poging door een aanvaller om een asset negatief te beïnvloeden.

authentication *authentificatie, echtverklaring*. Met authentificatie wordt het bewijs gegeven dat iemand is wie hij zegt dat hij is, of dat een asset echt is.

authorization *autorisatie, bevoegdheid*. Met autorisatie wordt gecontroleerd of iemand bevoegd is om een bepaalde actie uit te voeren.

availability *beschikbaarheid*. De beschikbaarheid van een dienst of bedrijfsmiddel wanneer deze nodig is.

beveiliging *informatiebeveiliging*. Het voorkomen en herstellen van ongerechtigde of ongewenste vernieling, wijziging, ontsluiting of gebruik van informatie en informatiemiddelen, zei het per ongeluk of opzettelijk.

confidentiality *vertrouwelijkheid*. Vertrouwelijke informatie mag niet algemeen bekend worden gemaakt, zowel opzettelijk als per ongeluk.

controls *(beveiligings)maatregelen*. Maatregelen om beveiligingsaspecten zoals beschikbaarheid, vertrouwelijkheid en integriteit te kunnen waarborgen en beheersen.

identification *identificatie*. Identificatie is het kenbaar maken van de identiteit van een subject (een gebruiker of een proces).

onloochenbaarheid *non-repudiation*. Onloochenbaarheid is het achteraf niet kunnen ontkennen dat een transactie heeft plaatsgevonden.

privacy Het recht van individuen, groepen of organisaties om voor henzelf te bepalen wanneer, hoe en hoeveel informatie over hen aan anderen mag worden geopenbaard.

security patterns *beveiligingspatronen*. Standaard oplossingen voor veel voorkomende beveiligingsproblemen in een specifieke context.

veiligheid *safety*. Veiligheid[1] is de mate van afwezigheid van potentiële oorzaken van een gevaarlijke situatie of de mate van aanwezigheid van beschermde maatregelen tegen deze potentiële oorzaken.

[1] Bron: http://nl.wikipedia.org/wiki/Veiligheid

I

Beveiliging, Privacy en Architectuur

"Security should be business risk-driven. Security can be defined only relative to the value and risk propositions of the business."

John Sherwood (*SABSA®*, [28])

1

Inleiding

In deze scriptie staan de begrippen beveiliging, privacy en architectuur centraal. Dit hoofdstuk schetst het landschap waarin deze begrippen een rol spelen en beschrijft hun onderlinge samenhang. Tevens wordt het onderwerp van deze scriptie gepositioneerd in het voorafgaande onderzoek waarin de Architectuurdocumentatie Evaluatiemethode (ADEM) is voorgesteld.

1.1 Beveiliging en Privacy

Beveiliging is een breed begrip dat veel verschillende invullingen kent en een groot gebied beslaat. De *Van Dale Hedendaags Nederlands* definieert beveiligen als 'het onttrekken aan geweld, bedreiging, gevaar of schade'. In de vrije encyclopedie WIKIPEDIA is beveiliging gedefinieerd[1] als:

> 'Beveiliging is het treffen van maatregelen om een te beveiligen doel te beschermen tegen schadelijke invloeden. (...) Beveiliging is een manier om risico's te verminderen en beheersbaar te maken en de veiligheid te verhogen.'

Het is van belang het onderscheid op te merken tussen beveiliging en veiligheid, in het Engels respectievelijk *security* en *safety*, omdat deze begrippen soms door elkaar gebruikt worden. Veiligheid is gedefinieerd als:

> 'Veiligheid is de mate van afwezigheid van potentiële oorzaken van een gevaarlijke situatie of de mate van aanwezigheid van beschermde maatregelen tegen deze potentiële oorzaken.'

Er zijn veel soorten beveiliging die onder dezelfde noemer vallen, zo zijn er onder andere fysieke beveiliging, informatiebeveiliging, computerbeveiliging en netwerkbeveiliging. De definities van deze termen overlappen vaak en daarom wordt in deze scriptie bewust voor een algemene maar duidelijke en bruikbare definitie gekozen:

[1] Wikipedia Beveiliging: http://nl.wikipedia.org/wiki/Beveiliging

> 'Information Security is the prevention of, and recovery from, unauthorized or undesirable destruction, modification, disclosure, or use of information and information resources, whether accidental or intentional.' – (Thomas R. Peltier, [21])

In de meeste literatuur worden de beveiligingsdoelen van de CIA-triade gehanteerd, oftewel confidentiality, integrity en availability. In het Nederlands wordt hiervoor de afkorting BIV (weliswaar achterstevoren) gebruikt, voor beschikbaarheid, integriteit en vertrouwelijkheid. Lucien Bongers gebruikt deze BIV doelen in zijn scriptie [5] over beveiliging en enterprise architectuur, maar ik ben van mening dat deze drie doelen aangevuld moeten worden met twee andere doelen, namelijk: onloochenbaarheid (*non-repudiation*) en autorisatie (*authorization*). Onloochenbaarheid houdt in dat van een transactie achteraf niet ontkend kan worden dat deze heeft plaatsgevonden. Het begrip autorisatie bestaat uit drie opeenvolgende stappen: identificatie, authentificatie en autorisatie.

Het begrip *privacy* kent geen eenduidige Nederlandse vertaling en wordt veelal aangeduid met persoonlijke levenssfeer, privésfeer en beslotenheid. Het Engelse woordenboek *The Chambers Dictionary* definieert privacy als:

> 'privacy seclusion; (one's right to) freedom from intrusion by the public; avoidance of notice, publicity or display; secrecy, concealment; a private matter (*rare*).'

Eenvoudig gezegd is privacy het recht om met rust gelaten te worden en onbespied te blijven. Bart Jacobs schrijft [16]: 'Privacy beschrijft het 'recht' om informatie tot een bepaalde rol te beperken'. Wang, Lee en Wang [31] onderkennen vier kenmerken van privacy: eenzaamheid (solitude), intimiteit (intimacy), anonimiteit (anonymity) en terughoudendheid (reserve).

Deze scriptie hanteert de veelgebruikte [30] definitie van privacy geformuleerd door prof. Alan F. Westin van Columbia University:

> 'het recht van individuen, groepen of organisaties om voor henzelf te bepalen wanneer, hoe en hoeveel informatie over hen aan anderen mag worden geopenbaard.'

Bij privacy gaat het bij de genoemde informatie voornamelijk om persoonsgegevens. Deze zijn niet beperkt tot gegevens zoals naam, adres en geboortedatum maar ook klantprofielen, kredietinformatie, videobeelden en geluidsopnamen dienen beschermd te worden. Een lijst van namen enerzijds en een lijst van salarissen anderzijds zijn echter niet zomaar persoonsgevoelig. De *combinatie* van dergelijke gegevens maakt dat ze tot een persoon herleidbaar kunnen zijn. Met andere woorden: de context van de gegevens maakt het gevoelige gegevens.

Het wordt wel vaker beweerd dat beveiliging en privacy elkaars tegenpolen zijn en dit blijkt vaak ook zo te zijn. Het werkt in twee richtingen: beveiliging kan het waarborgen van privacy in gevaar brengen maar het kan tevens een goede bescherming van privacy mogelijk maken. Een kort voorbeeld is op zijn plaats. Er kan cameratoezicht in het publieke domein ingezet worden om criminaliteit terug te dringen terwijl hierdoor de privacy van de onschuldige voorbijganger geschonden zal worden. Aan de andere kant zorgen sterke encryptie-algoritmen zoals RSA[2] ervoor dat de vertrouwelijkheid van persoonsgegevens gegarandeerd kan worden.

[2]RSA is ten tijde van het schrijven van deze scriptie vooral veilig bij sleutellengten groter dan 1024 bits vanwege de snel toenemende rekenkracht van computers.

Er zal altijd een afweging gemaakt moeten worden in de vorm van een kosten-baten analyse tussen de resultaten van de beveiligingsmaatregelen enerzijds en de gevolgen voor de privacy anderzijds. Hierbij moet constant zorg gedragen worden voor de naleving van wet- en regelgeving. Een voorbeeld van beveiligingseisen die vanuit wetgeving opgelegd worden is artikel 13 van de Wbp [18]:

> 'De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand der techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.'

Ook internationale wet- en regelgeving heeft invloed op Nederlandse organisaties. Zo heeft het Europees Parlement in 2005 een voorstel aangenomen over dataretentie waarin staat dat alle internetproviders communicatiegegevens moeten opslaan voor een bepaalde tijd. Dit heeft zeer grote consequenties voor de manier waarop deze organisatie worden ingericht.

1.2 Bedreigingen voor Organisaties

Als gevolg van de sterke groei van het internet zijn bijna alle organisaties vertegenwoordigd op het internet met een website, gebruiken ze email, bieden ze diensten aan en gebruiken diensten van andere organisaties. Omdat het steeds makkelijker is geworden om informatie uit te wisselen en te delen is er een groeiende behoefte om deze informatie te beschermen. In principe zijn alle organisaties die verbonden zijn met het internet ontvankelijk voor aanvallen via dat medium, maar er zijn ook bedreigingen uit andere richtingen. Een organisatie kan ook aangevallen worden van binnenuit, door het eigen personeel of door bezoekers of inbrekers.

De doelen van een aantal veel voorkomende aanvallen genoemd in (Killmeyer, [29]) zijn:

- ◇ Het verstoren van communicatie.
- ◇ Het wijzigen of verwijderen van databases.
- ◇ Het verspreiden van misleidende propaganda.
- ◇ Het uitschakelijk van telefoonverbindingen.
- ◇ Het stelen van geld.
- ◇ Het installeren van virussen, Trojans, wormen en tijdbommen.
- ◇ Het verkrijgen van ongeauthoriseerde toegang tot gevoelige gegevens.
- ◇ Het verkopen van vertrouwelijke bedrijfsinformatie.
- ◇ Het illegaal kopieren van software.

Het is van groot belang dat elke organisatie de noodzaak inziet van het inventariseren van de daadwerkelijke bedreigingen. Door middel van beveiligingsarchitectuur krijgt de organisatie inzicht in de samenhang tussen enerzijds de bestaande beveiligingsmaatregelen en anderzijds

die maatregelen die genomen moeten worden. Architectuur vanuit het aspect Beveiliging en Privacy is hierbij een uitstekend middel om een goede balans te creëren tussen de daadwerkelijke risico's en de beveiligingsmaatregelen.

1.3 Architectuur en Architectuurdocumentatie

In het begin van het afstudeeronderzoek waarin de Architectuurdocumentatie Evaluatiemethode (ADEM, [9]) opgesteld werd is er door de zes schrijvers overeenstemming bereikt over de volgende definitie voor het begrip *architectuur*:

> 'Architectuur is een verzameling van architectuurprincipes, verbijzonderd naar regels, richtlijnen en standaarden.' (Rijsenbrij, [22])

Er is geen enkele reden om hier voor het vervolg van dit onderzoek vanaf te wijken en daarom hanteert deze scriptie dezelfde definitie. Rijsenbrij stelt dat architectuurprincipes prescriptieve richtinggevende uitspraken zijn die de ontwerpruimte voor de architectuurimplementatie inperken. Het verschil tussen regels en standaarden enerzijds en richtlijnen anderzijds is dat richtlijnen niet verplicht opgevolgd moeten worden in tegenstelling tot de regels en standaarden.

Volgens Rijsenbrij [22] is beveiliging een 'vast onderdeel van een geïntegreerde architectuurbenadering vormt', en 'alle vier werelden in samenhang beslaat'. Deze vier werelden zijn het bedrijfsgebeuren, informatieverkeer, applicatielandschap en de technische infrastructuur. Deze integrale, holistische aanpak wordt in de literatuur [17, 26, 28] dan ook steevast aangeraden.

De in paragraaf 1.2 genoemde balans komt ook naar voren in Rijsenbrij's beschrijving van wat beveiligingsarchitectuur moet inhouden:

> 'De beveiligingsarchitectuur beschrijft de manier waarop beveiliging wordt vormgegeven en beschouwt de beveiligingsmaatregelen van gebruiker tot dienst, een end-to-end beschouwing. Elke wereld heeft zijn eigen beveiligingsprincipes, die soms ook nog op gespannen voet staan met de principes uit die wereld zelf. Tussen de toegankelijkheid van een applicatie en de gegevensbeveiliging dient een balans te worden gevonden die past bij de onderhavige applicatie.' (Rijsenbrij, [22])

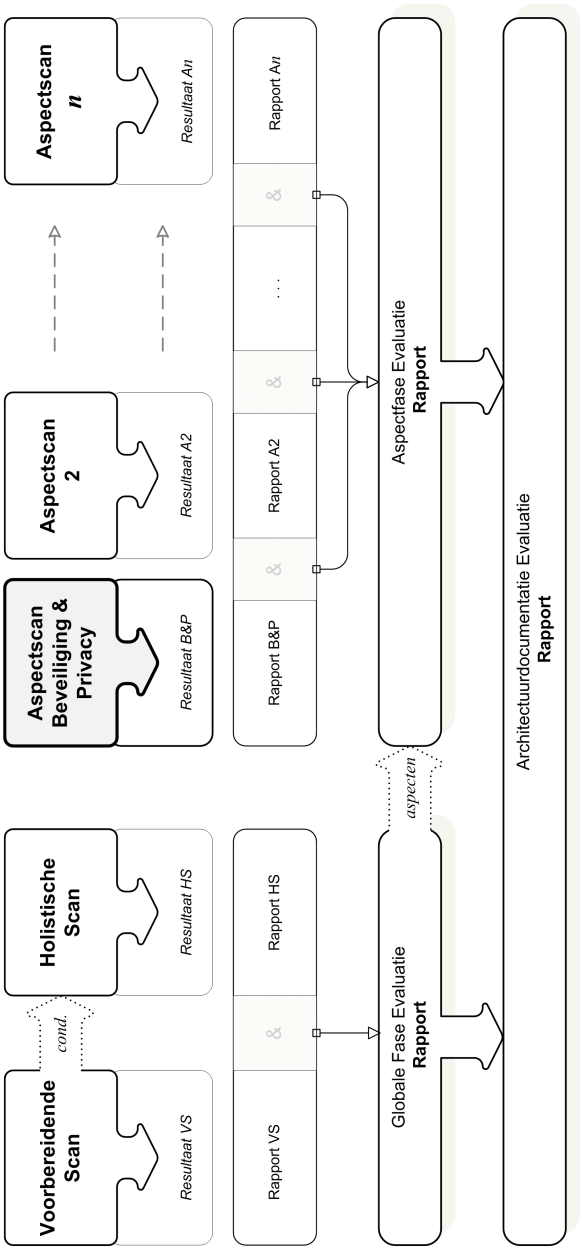
1.4 Positionering in de ADEM

De ADEM evalueert architectuurdocumentatie in twee fasen: de globale fase en de aspectfase. De structuur van de ADEM is schematisch weergegeven in afbeelding 1.1. Een eerste aanzet tot het ontwerpen van de globale fase is gerealiseerd in het eerste deelproject door zes afstudeerders.

Deze globale fase bestaat uit twee scans, de voorbereidende scan en de holistische scan. Beide scans zijn getoetst tijdens een case study waarin de globale fase werd uitgevoerd op de NORA en het Handboek Architectuur van de Gemeente Amsterdam.

De aspectfase bestaat uit een verzameling van aspectscans die ieder een voor architectuur

relevant aandachtsgebied met grotere diepgang evalueren. In deze scriptie wordt een eerste aanzet gemaakt voor het opstellen van een aspectscan voor het aspect Beveiliging en Privacy.



Afbeelding 1.1: De Architectuurdocumentatie Evaluatiemethode (ADEM).

"If we knew what it was we were doing,
it wouldn't be called research, would it?"

ALBERT EINSTEIN

2

Onderzoeksopzet

In dit hoofdstuk is de opzet van het onderzoek in hoofdlijnen beschreven. Als eerste worden de drie onderdelen van de afstudeeropdracht uitgelicht en wordt deze scriptie in dat kader geplaatst. Hierna worden de probleemstelling en doelstelling van het onderzoek bepaald. In paragraaf 2.3 worden de onderzoeksvragen beschreven samen met de bijbehorende deelvragen. Hierop volgt de begripsbepaling en het definiëren van het kennisgebied. Het hoofdstuk eindigt met de keuze voor een onderzoeksstrategie en de op te leveren producten.

2.1 Driedelige Afstudeeropdracht

De afstudeeropdracht bestaat uit drie onderling verbonden onderdelen. Deze scriptie vormt het derde en laatste onderdeel van de opdracht; de twee voorafgaande onderdelen zijn opgenomen als bijlagen in deel V van deze scriptie.

Het eerste deel bestond uit het ontwikkelen van een methode voor het evalueren van de kwaliteit van architectuurdocumentatie. Dit is gedaan door de zes afstudeerders Guido Chorus, Chris Nellen, Robin van 't Wout, Paul van Vlaanderen, David Campbell en de schrijver van deze scriptie, Yves Janse. Het resultaat van dit onderzoek is de Architectuurdocumentatie Evaluatiemethode (ADEM, [9]) welke is opgenomen in de bijlagen. Voor dit onderdeel kwam een groot gedeelte van de kennis en informatie uit een reeks interviews met experts op het vakgebied van architectuur en uit een aantal interessante discussies gevoerd op het Landelijke Architectuur Congres 2006[1]. Daarnaast is er een uitgebreid literatuuronderzoek verricht naar het aspect beveiliging en privacy.

Om de ADEM te kunnen toetsen hebben de afstudeerders in twee groepen van drie personen de globale fase van de methode uitgevoerd op de Nederlandse Overheid Referentie Architectuur (NORA, [20]) en het Handboek Architectuur [3] van de Gemeente Amsterdam. Robin van 't Wout, Paul van Vlaanderen en David Campbell hebben de NORA geëvalueerd en Guido Chorus [7], Chris Nellen [19] en Yves Janse het Handboek Architectuur. Tijdens de evaluatie hebben wij een kritische houding aangenomen en over zowel de uitvoering als de resultaten gereflecteerd. Deze reflectie van de groep van 3 personen is opgenomen in de bijlagen; een korte persoonlijke reflectie op de ADEM is opgenomen in hoofdstuk 10.2 op pagina 71.

[1] LAC 2006 Website: http://www.lac2006.nl

De resultaten van de uitvoering van de globale fase op het Handboek Architectuur zijn teruggekoppeld met Andre van der Valk en Menno Gmelig Meijling van de Bestuursdienst Amsterdam. Een korte samenvatting van hun reactie hierop en hun interpretatie van de resultaten is opgenomen in de bijlagen.

Om naast de voorbereidende scan en de holistische scan van de globale fase ook de nodige diepgang te kunnen bereiken is er in de ADEM een aspectfase opgenomen. Elke van de zes afstudeerders ontwikkelde een aspectscan als individueel onderzoek. Robin van 't Wout en Guido Chorus evalueren het aspect Adaptiviteit, Chris Nellen en David Campbell evalueren ieder onafhankelijk het aspect Menselijke Maat en Paul van Vlaanderen en Yves Janse ontwikkelen ieder individueel een aspectscan voor het aspect Beveiliging en Privacy. Het resultaat van dit laatste ligt voor u in de vorm van deze scriptie.

2.2 Onderzoeksdoelstelling

De doelstelling voor het onderzoek dat beschreven is in deze scriptie is als volgt geformuleerd:

> Een invulling geven aan het aspect Beveiliging en Privacy in de vorm van een aspectscan ten behoeve van de Architectuurdocumentatie Evaluatiemethode en deze toetsen met de casus van het Handboek Architectuur van de Gemeente Amsterdam.

Het betreft hier een eerste invulling van het aspect Beveiliging en Privacy, welke later verbeterd en uitgebreid kan worden. Het is de bedoeling na een kritische reflectie op de aspectscan en de uitvoering daarvan enkele aanbevelingen te doen voor deze mogelijke verbeteringen.

2.3 Onderzoeksvragen

De hoofdvraag waarop deze scriptie antwoord tracht te geven is:

> Hoe kan architectuurdocumentatie geëvalueerd worden in het licht van het aspect Beveiliging en Privacy?

Om antwoord te kunnen geven op deze vraag zijn de volgende deelvragen geformuleerd:

1. Welke elementen moeten verplicht in de architectuurdocumentatie zijn opgenomen?
2. Welke elementen zijn gewenst en optioneel in de architectuurdocumentatie?
3. Hoe kunnen deze elementen gemeten worden en hoe kan hier een conclusie uit getrokken worden?
4. Welke specifieke evaluatiecriteria kunnen worden gedefinieerd voor het aspect Beveiliging en Privacy?
5. Hoe kunnen deze specifieke evaluatiecriteria gemeten worden en hoe kan hier een conclusie uit getrokken worden?

2.4 Begripsbepaling

Deze paragraaf definieerd de in de onderzoeksvragen gebruikte begrippen. De begrippen beveiliging, privacy en architectuurdocumentatie worden allemaal gedefinieerd in hoofdstuk 1 en zijn opgenomen in de verklarende woordenlijst op pagina xiii.

Elementen zijn stukken informatie in de vorm van tekst, modellen of afbeeldingen die een bepaald onderdeel van de architectuurdocumentatie beslaan dat relevant is voor de evaluatie. Een voorbeeld van een element is de verzameling van architectuurprincipes. De verschillende elementen kunnen geëvalueerd worden met de evaluatiecriteria van de aspectscan Beveiliging en Privacy.

2.5 Kennisgebied en Strategie

Het kennisgebied waarin dit onderzoek plaats vindt is het snijvlak tussen enerzijds architectuur en anderzijds beveiliging en privacy. De oorspronkelijke afstudeeropdracht begon met een sterke focus op architectuur waarin de architectuurdocumentatie evaluatiemethode is ontworpen. Toen later besloten werd om een aspectscan te ontwerpen in de methode kwam Beveiliging en Privacy als aspect naar boven. Toen het individuele onderzoek begon werd de focus verschoven naar het kennisgebied beveiliging en privacy terwijl de insteek van architectuurdocumentatie niet uit het oog verloren werd.

Voor het onderzoek voor deze scriptie zijn twee onderzoeksstrategiën gehanteerd: het literatuuronderzoek en de case study. Door middel van literatuuronderzoek (ook wel bureauonderzoek genoemd) wordt er een theorie ontwikkeld die tot een norm en evaluatiemethode leidt in de vorm van een aspectscan. Om deze aspectscan te valideren wordt een case study uitgevoerd op het Handboek Architectuur van de Gemeente Amsterdam.

Naast het bestuderen van literatuur zijn er een aantal interviews gehouden met experts in het vakgebied van beveiliging en privacy, en experts op het gebied van architectuur. Het onderzoek is cross-sectioneel omdat de stand van zaken met betrekking tot beveiliging en privacy zoals die zich op dit moment voordoet onderzocht wordt.

2.6 Produkten

De produkten die al zijn opgeleverd in de vorige twee delen van de afstudeeropdracht zijn opgenomen in de bijlagen. Dit zijn de volgende documenten:

- ◇ De Architectuurdocumentatie Evaluatiemethode (Bijlagen, [9]).
- ◇ De evaluatie van het Handboek Architectuur van de Gemeente Amsterdam: Uitvoering van de Globale Fase (Bijlagen, [8]).

In deze scriptie worden de volgende produkten opgeleverd als resultaat van het individuele onderzoek:

- ◇ De Aspectscan Beveiliging en Privacy (Deel II vanaf pagina 15).
- ◇ De case study op het Handboek Architectuur (Deel III vanaf pagina 49).

- ◇ Reflectie op de Aspectscan en de ADEM in het algemeen. (Deel IV vanaf pagina 67).

II

Aspectscan
Beveiliging en Privacy

"Any society that would give up a little liberty to gain a little security will deserve neither and lose both. "

Benjamin Franklin

3

Inleiding

De aspectscan Beveiliging en Privacy volgt de in de ADEM [9] voorgeschreven indeling in twee deelscans: de *voorbereidende* aspectscan en de *specifieke* aspectscan. Deze indeling is vastgesteld voor alle aspectscans om een goede aansluiting met de ADEM te kunnen garanderen. De invulling van deze twee deelscans is voor de aspectscans vrij te bepalen; hierin ligt de flexibiliteit van de methode. Het is de bedoeling dat na verloop van tijd de norm die in deze scans gebruikt is naar aanleiding van voortschrijdend inzicht aangepast en uitgebreid zal worden.

Het doel van de voorbereidende aspectscan is allereerst om te bepalen of de architectuurdocumentatie compleet genoeg is zodat deze geëvalueerd kan worden met deze aspectscan. Het heeft geen zin om een volledige aspectscan uit te voeren als in het begin al aangegeven kan worden dat een aantal essentiële elementen ontbreekt. Door bij de voorbereidende aspectscan te controleren of deze elementen aanwezig zijn kan er een *go/no-go* advies gegeven worden met betrekking tot het uitvoeren van de rest van de aspectscan.

Als tijdens het doorlezen van de architectuurdocumentatie blijkt dat er bepaalde elementen afwezig zijn dan kan de architect deze toevoegen of aanvullen. Later kan dan na een positieve uitkomst van de voorbereidende aspectscan de specifieke aspectscan uitgevoerd worden om beter inzicht te krijgen in de kwaliteit van de architectuurdocumentatie vanuit het oogpunt van het desbetreffende aspect. Het uitvoeren van de voorbereidende aspectscan kost weinig tijd en geld maar heeft een duidelijke toegevoegde waarde.

Het doel van de specifieke aspectscan is om de elementen uit de voorbereidende aspectscan inhoudelijk en in samenhang te evalueren. Waar het bij de voorbereidende aspectscan over aanwezigheid en volledigheid gaat, is het bij de specifieke aspectscan met name van belang *hoe* de elementen beschreven zijn in tegenstelling tot de vraag *of* ze beschreven zijn.

3.1 Eisen aan de Aspectscan

Om een goede aansluiting op de ADEM te kunnen garanderen zijn er een aantal regels gedefinieerd [9] die in acht genomen dienen te worden bij het opstellen van aspectscans. De aspectscan voor beveiliging en privacy is geen uitzondering en moet aan deze regels voldoen. Deze zes regels zijn als volgt:

Regel 1. Elke aspectscan moet betrekking hebben op een voor architectuur relevant aandachtsgebied.

Regel 2. Elke aspectscan moet zijn doel en relevantie (bestaansrecht) beschrijven en verantwoorden.

Regel 3. Elke aspectscan moet een voorbereidende aspectscan bevatten.

Regel 4. Elke aspectscan moet een deugdelijke meetmethode en methode om tot een oordeel te komen bevatten.

Regel 5. Elke aspectscan moet onafhankelijk uit te voeren zijn van andere aspectscans.

Regel 6. Elke aspectscan moet een bibliotheek met huidige best practises en standaarden met betrekking tot het aandachtsgebied van dit aspect bevatten, of een verwijzing naar een bestaande bibliotheek.

In de reflectie op de aspectscan Beveiliging en Privacy (Deel IV, hoofdstuk 10.1) wordt verantwoord hoe deze aspectscan aan bovenstaande regels voldoet.

3.2 Bijsluiter voor het gebruik

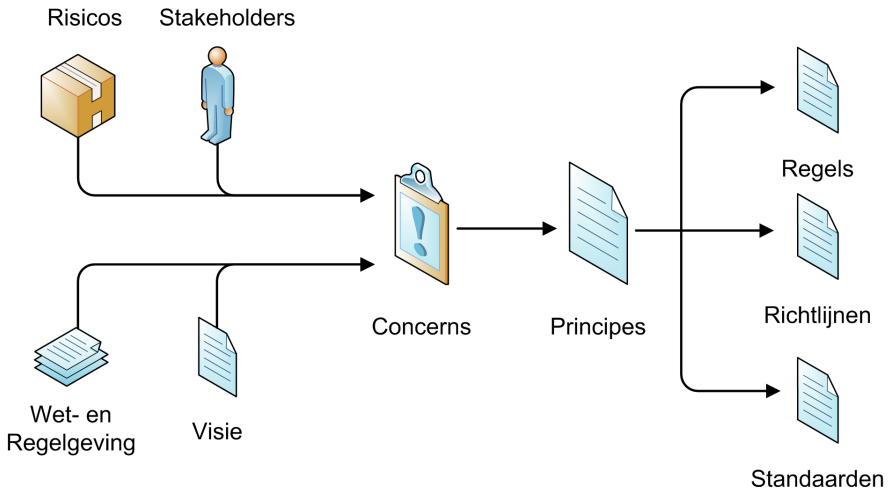
De aspectscan die hier in deel II van deze scriptie beschreven is, is niet meer en niet minder dan een eerste poging om het aspect Beveiliging en Privacy in architectuurdocumentatie te evalueren. Ten gevolge hiervan moet gezegd worden dat de resultaten van het uitvoeren van deze aspectscan gezien moeten worden met deze gedachte in het achterhoofd.

Het is de bedoeling dat in de toekomst verder onderzoek tot nieuwe ideëen en inzichten zal leiden. Architectuur als discipline staat nog in de kinderschoenen en het vakgebied beveiliging maakt een sterke groei door. Beveiliging zal steeds meer als een business issue gezien worden waardoor het vanuit architectuurperspectief veel aandacht zal krijgen. Er zullen meer raamwerken ontwikkeld worden en door de opkomst van de elektronische overheid komt er steeds meer bewustzijn voor het belang van bescherming van de privacy van burgers en ambtenaren. Al deze ontwikkelingen leiden tot voortschrijdend inzicht en zullen leiden tot verbeteringen in volgende versies van deze aspectscan.

Net zoals voor de ADEM is het doel van de aspectscan Beveiliging en Privacy het verschaffen van inzicht in de compleetheid en kwaliteit van de architectuurdocumentatie. Het is nadrukkelijk niet de bedoeling om een kwantitatief oordeel te geven in de vorm van een rapportcijfer op basis waarvan de architectuurdocumentatie van verschillende organisaties vergeleken kan worden.

3.3 Rationaliseringsketen voor Beveiliging en Privacy

De zogenaamde rationaliseringsketen is een centraal begrip in deze scriptie. Deze keten vormt de essentiële basis voor de architectuurdocumentatie. Het is geen geheel nieuw idee; zeven jaar geleden sprak men in de standaard IEEE 1471:2000 [14] ook al over het belang van de herleidbaarheid van concerns naar principes en vice versa. In afbeelding 3.1 is de rationaliseringsketen voor beveiliging en privacy weergegeven.



Afbeelding 3.1: Rationaliseringsketen voor Beveiliging en Privacy.

Er zijn twee belangrijke kenmerken van de rationaliseringsketen die uitgelegd dienen te worden. Allereerst is de keten verbonden en niet onderbroken; anderzijds kan de keten in twee richtingen worden doorlopen: van links naar rechts en vice versa.

Tijdens het architectuurontwikkelproces zal de architectuurdocumentatie meegroeien. In de rationaliseringsketen is dit weergegeven door de vier bronnen waaruit de concerns voorkomen, namelijk de stakeholders, risico's, wet- en regelgeving en de visie van de onderneming.

De stakeholders hebben verschillende belangen bij het voorbestaan van de onderneming en uiten deze in de vorm van concerns. Omdat deze belangen soms tegenstrijdig zijn is het aan te bevelen een prioritering aan te brengen in (groepen) stakeholders. Stakeholders kunnen voor het besluitvormingsproces grofweg ingedeeld worden in drie categorieën [22]: beslissende, beïnvloedende en overige stakeholders.

Naast de directe concerns van de stakeholders zijn er in het ecosysteem waarin de organisatie opereert altijd bedreigingen. Deze bedreigingen vormen risico's die het voortbestaan van de organisatie in gevaar kunnen brengen. In de theorie over risico management is het gebruikelijk een risico te definiëren als het product van de kosten van het verliezen van het bedreigde bedrijfsmiddel (of meerdere assets) en de kans dat dit ook daadwerkelijk gebeurt. Stel het kost een e-commerce organisatie per dag €10.000,- als hun website uit de lucht is, en de kans dat door een kwaadwillende de website aangevallen zal worden is misschien 1%. In het algemeen zou het dus niet verstandig zijn om beveiligingsmaatregelen te implementeren die meer kosten dan €100,- per dag. Uiteraard moet er ook nog rekening gehouden worden met andere dreigingen voor hetzelfde bedrijfsmiddel, en maatregelen die meerdere bedrijfsmiddellen beschermen. Deze risico's leveren beveiligingsvereisten op in de vorm van concerns.

De organisatie heeft altijd te maken met wet- en regelgeving in het ecosysteem waarin ze opereert. In Nederland kun je denken aan de Wet bescherming persoonsgegevens (Wbp, [18]) en de Nederlandse corporate governance code (Code Tabaksblat[1]). Vooral voor de overheid heeft de Wbp een grote impact op hoe de informatiehuishouding ingericht mag worden. In de Verenigde Staten is compliance met de Sarbanes-Oxley Act (SOX) verplicht. SOX is als

[1]Website: http://www.commissiecorporategovernance.nl/Definitieve%20code

wet aangenomen nadat de grote boekhoudingsschandalen van Enron en Worldcom aan het licht zijn gekomen. In Nederland zal naar verwachting vanaf 2007 langzaam Basel-II worden ingevoerd, ook bekend onder de naam New Capital Adequacy Framework.

Als vierde is de visie (en gedeeltelijk ook de missie) van de organisatie een bron van concerns voor de architectuur. In de visie is beschreven wat de organisatie over bijvoorbeeld 5 jaar bereikt wil hebben. Als een organisatie de overstap wil maken naar het internet, om bijvoorbeeld elektronische diensten aan te bieden, moet vanaf het begin al rekening gehouden worden met de toenemende behoefte aan beveiliging.

De concerns die uit deze vier bronnen voortkomen worden geadresseerd door principes te formuleren die richting geven aan oplossingen om de concerns op te lossen. Om deze architectuurprincipes concreet en tastbaar te maken worden ze verbijzonderd naar regels, richtlijnen en standaarden. In het vakgebied van beveiliging worden regels en richtlijnen vaak in de vorm van onder andere policies en procedures geformuleerd. De meeste organisaties hebben email of internet policies die door elke werknemer gelezen en ondertekend moet worden, waarin het acceptabel gebruik van de voorzieningen is beschreven. Daarnaast is het gebruikelijk dat er procedures zijn gedefinieerd voor het wijzigen van wachtwoorden, of het maken van backups van belangrijke data.

De rationaliseringsketen kan niet alleen van links naar rechts doorlopen worden, maar ook de tegenovergestelde richting is van groot belang: de herleidbaarheid (*traceability*) van elementen. Zo moeten alle principes teruggeleid kunnen worden naar de concerns die eraan ten grondslag liggen. Hetzelfde is ook van toepassing op de concerns, ze moeten kunnen worden herleid tot hun bron, zoals de stakeholder die het concern heeft.

Deze herleidbaarheid in twee richtingen toont het belang van de samenhang in architectuur. Als het niet mogelijk is om te verantwoorden waarom een principe er is, dan zijn oplossingen die op basis van dat principe geïmplementeerd worden misschien overbodig. Anderzijds wil je als organisatie kunnen controleren of de belangrijkste concerns zijn afgedekt. De rationaliseringsketen is een leidraad om deze verbondenheid te realiseren.

"I keep six honest serving men
(They taught me all I knew);
Their names are *What* and *Why* and *When*
And *How* and *Where* and *Who*. "

RUDYARD KIPLING

4

Voorbereidende Aspectscan

Dit hoofdstuk beschrijft de voorbereidende aspectscan, het eerste deel van de aspectscan Beveiliging en Privacy. Allereerst worden de te evalueren elementen geïdentificeerd en gegroepeerd in paragraaf 4.1 waarna de daadwerkelijke evaluatiecriteria gedefinieerd worden volgens een vast sjabloon. Het concluderen en rapporteren van de resultaten van de voorbereidende aspectscan wordt in paragraaf 4.3 behandeld.

4.1 Elementen voor Evaluatie

De elementen voor evaluatie in de voorbereidende aspectscan kunnen worden onderverdeeld in drie groepen: *vereiste*, *gewenste* en *optionele* elementen. De vereiste elementen vormen het absolute minimum wat aanwezig moet zijn in architectuurdocumentatie met betrekking tot beveiliging en privacy. Wanneer er tijdens het uitvoeren van de voorbereidende aspectscan blijkt dat er vereiste elementen afwezig zijn, zal dit direct een *no-go* advies ten gevolge hebben. Gewenste elementen dragen duidelijk bij aan de kwaliteit van de architectuur betreffende het aspect Beveiliging en Privacy, maar zouden eventueel afwezig kunnen zijn. Dit is vooral het geval bij organisaties die zich in een lager niveau van volwassenheid[1] bevinden.

Bij de voorbereidende scan in de globale fase van de ADEM zijn er verschillende optionele elementen onderkend die op aanwezigheid getoetst worden. Bij deze eerste aanzet tot een aspectscan Beveiliging en Privacy zijn er geen elementen die als optioneel gezien worden. Bijna alle elementen zijn vereist en de gewenste elementen zijn ook van groot belang voor een integrale behandeling van de beveiliging. Het feit dat er zoveel vereiste elementen zijn kan verklaard worden door het belang van de rationaliseringsketen voor beveiliging en privacy, zoals beschreven in paragraaf 3.3 in de inleiding van deel II. Het oude gezegde 'de keten is zo sterk als de zwakste schakel' gaat hier ook op; de schakels van de keten zijn de elementen in de rationaliseringsketen.

De elementen die in deze voorbereidende aspectscan geëvalueerd worden zijn weergegeven in tabel 4.1 hieronder. Deze elementen komen uit verschillende bronnen zoals literatuur over beveiliging, privacy en architectuur, maar ook voor een deel uit interviews met experts op

[1] Voor een indeling in volwassenheid van onder andere beveiligingsarchitectuur in organisaties zie bijvoorbeeld het veel toegepaste CobiT™ Capability Maturity Model (CMM).

deze gebieden. Omdat in de literatuur vaak gemengde begrippen gebruikt worden zijn in de tabel zowel de Nederlandse als Engelse namen vermeld. Bij de definities van de elementen worden de bronnen vermeld wanneer dit van toepassing is.

Vereist	Engels: ◇ **Security Aspect** ◇ Stakeholders ◇ Concerns ◇ Risks ◇ Security Principles ◇ Security Baseline ◇ Asset Classification ◇ Controls ◇ Roles and Responsibilities	Nederlands: 1. **Beveiligingsaspect** 2. Belanghebbenden 3. Belangen 4. Risico's 5. Beveiligingsprincipes 6. Uitgangssituatie Beveiliging 7. Bedrijfsmiddelenclassificatie 8. Maatregelen 9. Rollen en Verantwoordelijkheden
Gewenst	Engels: ◇ Policies ◇ Procedures ◇ Security Services Models ◇ Security Process Models	Nederlands: 10. Gedragslijnen 11. Procedures 12. Beveiligingsdienstenmodel 13. Beveiligingsprocesmodel
Optioneel	–	-

Tabel 4.1: Elementen voor het aspect Beveiliging en Privacy.

De aanwezigheid en compleetheid van deze elementen wordt gemeten door middel van evaluatiecriteria. Deze evaluatiecriteria worden in paragraaf 4.2 gedefinieerd volgens een vast sjabloon. Er zijn twee schalen van conclusies mogelijk bij deze evaluatiecritera. Dit zijn enerzijds de waarden {*Aanwezig*, *Afwezig*} voor de criteria waarbij het element niet gedeeltelijk aanwezig kan zijn, en anderzijds {*Compleet*, *Incompleet*, *Afwezig*} wanneer dit onderscheid wel gemaakt kan worden.

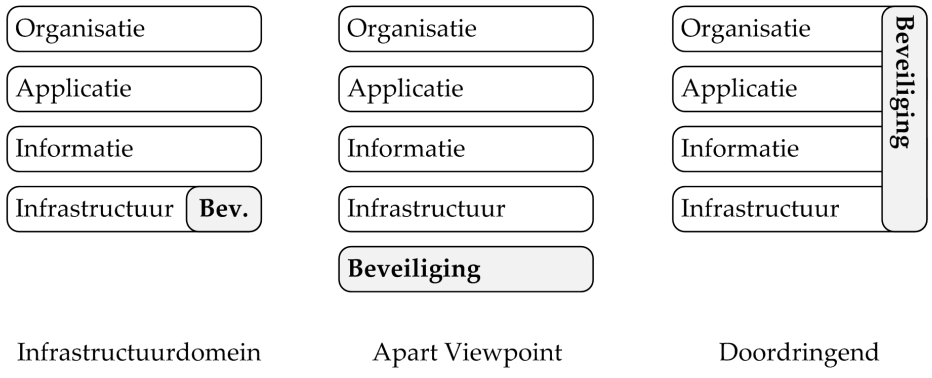
4.2 Definitie van de Evaluatiecriteria

In deze paragraaf worden op de volgende bladzijden de evaluatiecriteria voor de voorbereidende aspectscan gedefinieerd. Per evaluatiecriterium wordt er een definitie van het begrip gegeven, tevens wordt de relevantie aangetoond evenals de meetmethode en worden regels om tot een bepaalde conclusie te komen beschreven.

De evaluatiecriteria zijn in tabelvorm opgenomen zodat ze gemakkelijk bruikbaar zijn als referentie tijdens het uitvoeren van de evaluatie. Elk criterium heeft een nummer en een uniek onderschrift zodat er naar verwezen kan worden vanuit de rapportage van de resultaten.

1. Beveiligingsaspect	Vereist
Wat is het?	Het aspect Beveiliging en Privacy vertegenwoordigt in de vorm van een domein in de technische infrastructuur, een apart viewpoint of als een doordringend integraal aspect in alle lagen van de architectuurdocumentatie. Deze drie vormen zijn door Gartner [17] geïdentificeerd en schematisch weergegeven in afbeelding 4.1.
Waarom is het van belang?	Het is vanzelfsprekend dat als het aspect Beveiliging en Privacy niet vertegenwoordigd is in de architectuurdocumentatie, het uitvoeren van deze aspectscan geen zin heeft.
Hoe te meten?	Lees de architectuurdocumentatie door en zoek naar de beschrijving van beveiliging en privacy in één van de drie genoemde vormen. Hoewel de doordringende vorm beter is dan de infrastructuurdomein-vorm maakt dit evaluatiecriterium hiertussen geen onderscheid. Het is voor dit evaluatiecriterium van belang dat er aandacht is voor beveiliging en privacy in de architectuurdocumentatie, zodat deze geëvalueerd kan worden.
Hoe een conclusie te trekken?	Als één van de 3 benaderingswijzen gebruikt wordt: **Aanwezig** In alle andere gevallen: **Afwezig**

Tabel 4.2: Evaluatiecriterium 1: Beveiligingsaspect.



Afbeelding 4.1: Drie verschillende benaderingswijzen van het aspect Beveiliging.

2. Stakeholders	Vereist
Wat is het?	Stakeholders zijn personen, groepen en organisaties die belang hebben bij de architectuur en het voortbestaan van de organisatie. Er zijn drie categorieën stakeholders voor het besluitvormingsproces: beslissende, beïnvloedende en overige stakeholders (Rijsenbrij, [22]). Voorbeelden van belangrijke stakeholders met een belang bij beveiliging en privacy zijn de managers, gebruikers en beheerders.
Waarom is het van belang?	De stakeholders moeten beschreven zijn omdat ze een van de belangrijkste startpunten zijn van de rationaliseringsketen (zie paragraaf 3.3 en afbeelding 3.1). Een architectuur die geen rekening houdt met de belangen van de juiste stakeholders zal niet succesvol zijn. De architectuur zal dan een minder sterk draagvlak hebben, met alle gevolgen van dien.
Hoe te meten?	Lees de architectuurdocumentatie door en zoek naar een lijst of opsomming van de stakeholders met een belang bij beveiliging en privacy, die de organisatie belangrijk vindt.
Hoe een conclusie te trekken?	Als de stakeholders beschreven zijn: **Aanwezig** In alle andere gevallen: **Afwezig**

Tabel 4.3: Evaluatiecriterium 2: Stakeholders.

3. Concerns	Vereist
Wat is het?	Concerns (belangen) zijn de bestaansreden van de architectuurprincipes. Het zijn problemen of zorgen die bij het hogere management en bij de andere stakeholders leven, op het gebied waar architectuur een uitkomst moet bieden.
Waarom is het van belang?	Vanuit de concerns worden de architectuurprincipes opgesteld, en dus ook de beveiligingsprincipes. Er zijn drie bronnen: stakeholders hebben concerns, maar ook vanuit wet- en regelgeving, risico's binnen en buiten de organisatie en de bedrijfsvisie komen concerns naar voren (zie paragraaf 3.3 en afbeelding 3.1). Vanwege de focus op beveiliging en privacy worden de risico's als een apart element gezien in deze voorbereidende aspectscan. Als er geen concerns worden beschreven weet de organisatie niet of er (en zo ja, welke) oplossingen moeten komen en kan de architect niet de juiste principes formuleren om hier richting aan te geven.
Hoe te meten?	Lees de architectuurdocumentatie door en zoek naar een overzicht van concerns met betrekking tot stakeholders, wet- en regelgeving en concerns die voortkomen uit de visie. Het is niet voldoende om de visie zelf op te nemen, er moeten daadwerkelijk concerns geformuleerd worden.
Hoe een conclusie te trekken?	Als er concerns zijn opgenomen uit alle drie bovenstaande bronnen: **Compleet** Als er alleen stakeholder concerns zijn opgenomen: **Incompleet** In alle andere gevallen: **Afwezig**

Tabel 4.4: Evaluatiecriterium 3: Concerns.

4. Risico's	Vereist
Wat is het?	Een risico is iets wat met een bepaalde waarschijnlijkheid kan gebeuren en een impact heeft op het bereiken van doelstellingen. De grootte van het risico is de kans dat een bedreiging realiteit wordt, vermenigvuldigd met de schade die geleden wordt in dat geval. De schade is bijvoorbeeld de vervangingswaarde van het bedreigde bedrijfsmiddel.
Waarom is het van belang?	Het is van essentieel belang om te weten welke bedreigingen er zijn zodat de organisatie de risico's kan managen. Wanneer een organisatie niet weet welke risico's er zijn, kan ze zich niet efficiënt beveiligen omdat er geen inzicht is in de beveiligingsmaatregelen die getroffen moeten worden. Goed gedefinieerde risico's maken een balans tussen investering en bescherming mogelijk.
Hoe te meten?	Lees de architectuurdocumentatie door en zoek naar een lijst of opsomming van risico's. Dit kan een enkele lijst zijn met alle risico's, of een lijst van risico's per architectuurlaag of view.
Hoe een conclusie te trekken?	Als er risico's zijn opgenomen: **Aanwezig** In alle andere gevallen: **Afwezig**

Tabel 4.5: Evaluatiecriterium 4: Risico's.

5. Beveiligingsprincipes	Vereist
Wat is het?	Beveiligingsprincipes zijn architectuurprincipes die betrekking hebben op beveiliging en privacy. In een artikel over beveiligingsprincipes [13] definiëren Hofman en Elsinga beveiligingsprincipes als een 'hoog-niveau model om de manier waarop de organisatie over beveiliging denkt uit te drukken". Beveiligingsprincipes zijn er op verschillende niveaus: mindset principes op strategisch niveau, architectuurprincipes op tactisch niveau en execution principes op operationeel niveau.
Waarom is het van belang?	Door beveiligingsprincipes te formuleren toont de organisatie aan dat ze beveiliging en privacy serieus neemt en het niet als een louter technische zaak ziet, maar ook als een business issue. Principes zijn voor een architectuur onmisbaar en geven richting aan de veranderingen in de organisatie en scheppen een kader voor de beveiliging van te ontwerpen applicaties en processen. Zonder beveiligingsprincipes is er geen inperking van deze ontwerpruimte en blijft beveiliging een ondergeschoven kindje.
Hoe te meten?	Lees de architectuurdocumentatie door en zoek naar een lijst of opsomming van beveiligingsprincipes. Dit kan een enkele lijst zijn met alle principes, of een lijst van principes per architectuurlaag of view.
Hoe een conclusie te trekken?	Als er beveiligingsprincipes zijn opgenomen: **Aanwezig** In alle andere gevallen: **Afwezig**

Tabel 4.6: Evaluatiecriterium 5: Beveiligingsprincipes.

6. Uitgangssituatie Beveiliging	Vereist
Wat is het?	De uitgangssituatie van de beveiliging is vaak het resultaat van de initiële risico assessment. Het doel van een dergelijke *baseline* opstellen is niet alleen het ontdekken van zwakheden en risico's, maar ook het identificeren van sterke punten en bestaande beveiligingsmaatregelen.
Waarom is het van belang?	Architectuurdocumentatie beschrijft doorgaans een toekomstige *to-be* situatie, maar de uitgangssituatie is een duidelijke *as-is* situatie. Het is niet voldoende eenmalig de beveiliging te testen en dan aan te nemen dat het veilig blijft. Omdat aanvallers veranderen en andere middelen en motieven kunnen krijgen is het van belang om periodieke risico assessments uit te voeren. De uitgangssituatie van de beveiliging is onmisbaar om de effectiviteit van beveiligingsmaatregelen over een periode achteraf te kunnen meten [29]. Ook kan er door deze te combineren met een bedrijfsmiddelenclassificatie bepaald worden welke beveiligingsmaatregelen nodig zijn om de gewenste niveaus van beveiliging te garanderen.
Hoe te meten?	Lees de architectuurdocumentatie door en zoek naar een beschrijving van de uitgangssituatie van de beveiliging.
Hoe een conclusie te trekken?	Als er een uitgangssituatie is opgenomen: **Aanwezig** In alle andere gevallen: **Afwezig**

Tabel 4.7: Evaluatiecriterium 6: Uitgangssituatie Beveiliging.

7. Bedrijfsmiddelenclassificatie	Vereist
Wat is het?	Een bedrijfsmiddel (asset) is een tastbaar of ontastbaar goed dat waarde heeft voor de organisatie en beveiligd dient te worden. Een voorbeeld hiervan is klantinformatie in een database. Bedrijfsmiddelen maken de bedrijfsvoering mogelijk en zijn van belang voor het voortbestaan van de organisatie. Bedrijfsmiddelen kunnen in grofweg vier categoriëen [27] ingedeeld worden: informatie, software, fysieke bedrijfsmiddelen en diensten (services). In een bedrijfsmiddelenclassificatie wordt ook onder andere het eigenaarschap van bedrijfsmiddelen vastgelegd en authentificatie en authorisatie.
Waarom is het van belang?	Als de organisatie niet weet wat haar bedrijfsmiddelen zijn en wat de waarde daarvan is, kan ze niet bepalen welke beveiligingseisen hieraan verbonden zijn.
Hoe te meten?	Lees de architectuurdocumentatie door en zoek naar een bedrijfsmiddelenclassificatie.
Hoe een conclusie te trekken?	Als er een bedrijfsmiddelenclassificatie is opgenomen met alle vier categoriëen bedrijfsmiddelen: **Compleet** Als niet alle categoriëen zijn opgenomen, maar er wel een bedrijfsmiddelenclassificatie gemaakt is: **Incompleet** In alle andere gevallen: **Afwezig**

Tabel 4.8: Evaluatiecriterium 7: Bedrijfsmiddelenclassificatie.

8. Beveiligingsmaatregelen	Vereist
Wat is het?	Beveiligingsmaatregelen (controls) zijn maatregelen om beveiligingsdoelen zoals beschikbaarheid, vertrouwelijkheid, integriteit, onloochenbaarheid en autorisatie te kunnen waarborgen en beheersen. Killmeyer [29] onderkent drie groepen maatregelen: fysieke controls (zoals backups, kluizen, bewakers en biometrische beveiliging), administratieve controls (beveiligingsbewustzijn, policies en procedures, audits en noodplannen) en technische controls (encryptie, wachtwoorden, antivirus, firewalls). In deze groepen maakt Killmeyer een onderscheid tussen preventieve en detectieve maatregelen, maar in de praktijk worden daar vaak nog reactieve en repressieve maatregelen aan toegevoegd. Fysieke beveiligingsmaatregelen zijn wel belangrijk voor een goede beveiliging, maar horen niet in detail thuis in de architectuurdocumentatie. Ze perken vooral de fysieke ontwerpruimte in, en hebben slechts een beperkte invloed op de digitale ontwerpruimte. Om deze reden worden ze niet meegenomen in de conclusie van dit evaluatiecriterium.
Waarom is het van belang?	Als de organisatie geen beveiligingsmaatregelen implementeert dan is ze kwetsbaar voor alle risico's die zich voor kunnen doen. Dit bedreigt de organisatie in haar voortbestaan en kan tot gezichtsverlies leiden. Door een inventarisatie te maken van de huidige en toekomstige beveiligingsmaatregelen kan er op basis van de baseline in combinatie met de bedrijfsmiddelenclassificatie gekeken worden of de maatregelen afdoende de beveiligingsdoelen bereiken.
Hoe te meten?	Lees de architectuurdocumentatie door en zoek naar een overzicht van beveiligingsmaatregelen. Dit kan een enkele centrale lijst zijn, maar is bij voorkeur een lijst per laag in de architectuurdocumentatie.
Hoe een conclusie te trekken?	Als er technische en administratieve beveiligingsmaatregelen worden genoemd: **Compleet** Als er alleen administratieve beveiligingsmaatregelen worden genoemd, maar geen technische maatregelen: **Incompleet** In alle andere gevallen: **Afwezig**

Tabel 4.9: Evaluatiecriterium 8: Beveiligingsmaatregelen.

9. Rollen en Verantwoordelijkheden	Vereist
Wat is het?	Rollen en verantwoordelijkheden zijn twee dingen die veel met elkaar te maken hebben. Rollen zijn de verschillende functies die actoren in een organisatie uitvoeren. Een enkele persoon kan verschillende rollen vervullen, bijvoorbeeld die van werknemer bij een bank en als klant bij dezelfde bank. Voor deze verschillende rollen gelden verschillende regels en toegangsrechten. Een rol is vaak gekoppeld aan het uitvoeren van bepaalde samenhangende activiteiten in een proces. Op dit niveau gaat het echter om een abstracte representatie van strategisch functies zoals governance, leiderschap, advies en ontwerp, in tegenstelling tot een gedetailleerd functioneel model (Gartner, [26]). Het Genootschap van Informatie Beveiligers (GvIB, [12]) schrijft over verantwoordelijkheden het volgende: 'Informatiebeveiliging is een integraal aspect van ieders functie, zodat uiteindelijk ook iedereen naar rato verantwoordelijk is voor de informatiebeveiligingsaspecten die aan zijn functie of verantwoordelijkheidsgebied worden toegewezen.' Voorbeelden van taken die bij de primaire verantwoordelijkheden horen zijn het geven van opdracht tot het treffen van beveiligingsmaatregelen, zorgdragen voor het onderhouden en aanpassen van deze maatregelen, en het instellen van interne controle op het naleven van de maatregelen.
Waarom is het van belang?	Het is van belang om de beveiligingsverantwoordelijkheden voor alle individuën in de organisatie vast te leggen en van even groot belang om deze duidelijk te communiceren om bewustzijn te creëren op alle niveaus, van de boardroom tot de werknemers. Alleen wanneer de verantwoordelijkheden bekend zijn kan er op een juiste manier budget en tijd toegewezen worden om het voor de verantwoordelijke partijen mogelijk te maken om hun taken te doen zoals die van hun verwacht worden. Wanneer er niemand expliciet verantwoordelijk is voor de beveiliging van een artefact kan het voorkomen dat mensen zich achter elkaar verschuilen, of aannemen dat 'iemand anders het wel zal doen'. De bevoegdheden moeten in balans zijn met de verantwoordelijkheden.
Hoe te meten?	Lees de architectuurdocumentatie door en zoek naar een overzicht van rollen en verantwoordelijkheden met betrekking tot beveiliging en privacy.
Hoe een conclusie te trekken?	Als zowel overzichten van de rollen als de verantwoordelijkheden zijn opgenomen: **Aanwezig** In alle andere gevallen: **Afwezig**

Tabel 4.10: Evaluatiecriterium 9: Rollen en Verantwoordelijkheden.

10. Gedragslijnen	Gewenst
Wat is het?	Gedragslijnen (*policies*) dienen om alle werknemers op de hoogte te stellen van hoe ze zich moeten gedragen met betrekking tot een bepaald onderwerp, hoe de boardroom over dat onderwerp denkt en welke specifieke maatregelen en sancties de organisatie bereid is te nemen met betrekking tot de naleving (Killmeyer, [29]). Een voorbeeld van een gedragslijn is een e-mail policy waarin regels voor het veilig gebruik van email zijn vastgelegd, zoals het gebruik van encryptie en digitale handtekeningen.
Waarom is het van belang?	Gedragslijnen dienen vooral om bewustzijn te creëren en om duidelijk te stellen dat de organisatie beveiliging serieus neemt en draagvlak heeft in de boardroom. Gedragslijnen maken delen van de beveiligingsprincipes inzichtelijk voor alle niveaus, het management en de werknemers op de werkvloer.
Hoe te meten?	Lees de architectuurdocumentatie door en zoek naar een beschrijving van of een verwijzing naar een aantal gedragslijnen (minimaal 2) op het gebied van beveiliging en privacy. De tekst van de gedragslijnen hoeft niet zelf volledig in de architectuurdocumentatie te zijn opgenomen, een verwijzing met korte samenvatting volstaat in dit geval.
Hoe een conclusie te trekken?	Als er twee of meer gedragslijnen zijn opgenomen: **Compleet** Als er verwijzingen zijn, zonder samenvatting: **Incompleet** In alle andere gevallen: **Afwezig**

Tabel 4.11: Evaluatiecriterium 10: Gedragslijnen.

11. Procedures	Gewenst
Wat is het?	Procedures zijn plannen of processen die specifiek beschrijven hoe een bepaalde actie uitgevoerd moet worden. Ze maken het mogelijk kennis over te dragen tussen mensen die hetzelfde werk doen, of tijdelijk voor iemand anders invallen (Killmeyer, [29]). Procedures ontstaan uit het herkennen en toepassen van best practises in het dagelijkse werk. Policies geven richting aan de ontwikkeling van procedures.
Waarom is het van belang?	Procedures beschrijven de uit te voeren stappen op een dusdanig laag niveau dat een werknemer geen extra uitleg nodig heeft. De beveiligingsprincipes worden verbijzonderd naar regels, richtlijnen en standaarden. Deze regels en richtlijnen zijn terug te vinden in de procedures. Als er duidelijke procedures zijn kan wanneer dit nodig is (bijvoorbeeld bij ziekte van een werknemer) iemand anders het werk overnemen.
Hoe te meten?	Lees de architectuurdocumentatie door en zoek naar een beschrijving van of een verwijzing naar een aantal procedures (minimaal 2) op het gebied van beveiliging en privacy. De tekst van de procedures hoeft niet zelf volledig in de architectuurdocumentatie te zijn opgenomen, een verwijzing met korte samenvatting volstaat in dit geval.
Hoe een conclusie te trekken?	Als er twee of meer procedures zijn opgenomen: **Compleet** Als er verwijzingen zijn, zonder samenvatting: **Incompleet** In alle andere gevallen: **Afwezig**

Tabel 4.12: Evaluatiecriterium 11: Procedures.

12. Beveiligingsdienstenmodel	Gewenst
Wat is het?	Gartner definieert in het Enterprise Information Security Architecture raamwerk (EISA, [26]) een dienstenmodel (*security services model*) als een belangrijke input voor andere delen van de EISA. Een dienstenmodel is een raamwerk dat het portfolio van beveiligingsdiensten identificeert en positioneert. Gartner noemt identificatie, authenticatie, toegangscontrole, inbraak detectie en encryptie als voorbeelden van beveiligingsdiensten.
Waarom is het van belang?	De organisatie moet de beveiligingsdiensten op conceptueel niveau definiëren zodat ze aansluiten bij de andere diensten in de organisatie. Dit is vooral van belang bij organisaties die hun adaptiviteit proberen te verhogen door het service oriented paradigma te gebruiken.
Hoe te meten?	Lees de architectuurdocumentatie door en zoek naar een beveiligingsdienstenmodel.
Hoe een conclusie te trekken?	Als er een beveiligingsdienstenmodel is opgenomen: **Aanwezig** In alle andere gevallen: **Afwezig**

Tabel 4.13: Evaluatiecriterium 12: Beveiligingsdienstenmodel.

13. Beveiligingsprocesmodel	Gewenst
Wat is het?	Gartner definieert in het Enterprise Information Security Architecture raamwerk (EISA, [26]) een procesmodel (*security process model*) als een verzameling van beschrijvingen van processen die in de organisatie geïmplementeerd moeten worden. Met name de processen die de relaties tussen het beveiligingsteam aangeven (strategische processen zoals policy management en bewustzijnscampagnes) en processen voor het implementeren en handhaven van beveiligingsmaatregelen (identititeits en access management IAM, risicomanagement).
Waarom is het van belang?	Processen faciliteren schaalbaarheid, verklaarbaarheid (accountability) en meetbaarheid, maar nog specifieker vanuit het oogpunt van beveiliging faciliteert het gebruik van processen ook auditability. Deze attributen zijn allemaal van belang voor een goede beveiligingsarchitectuur (Gartner, [26]), en auditability is vaak wettelijk verplicht (SOX, Basel-II).
Hoe te meten?	Lees de architectuurdocumentatie door en zoek naar een beveiligingsprocesmodel.
Hoe een conclusie te trekken?	Als er een beveiligingsprocesmodel is opgenomen: **Aanwezig** In alle andere gevallen: **Afwezig**

Tabel 4.14: Evaluatiecriterium 13: Beveiligingsprocesmodel.

4.3 Concluderen en Rapporteren

Het rapport van de voorbereidende scan wijkt wat betreft structuur niet af van de structuur van de voorbereidende scan uit de globale fase van de ADEM. Ook bij de voorbereidende aspectscan bevat het rapport een overzicht van de conclusies over elk evaluatiecriterium van de elementen.

4.3.1 Uitvoering

Tijdens het uitvoeren van de voorbereidende aspectscan vult de evaluator per evaluatiecriterium een tabel in met een aantal vaste onderdelen. In tabel 4.15 zijn deze onderdelen weergegeven. De meting wordt beschreven met een verwijzing naar de locatie in de architectuurdocumentatie waar de meting is verricht. Zo kan iemand die het rapport leest gemakkelijk opzoeken waarom een bepaalde conclusie getrokken is.

n. Evaluatiecriterium	Vereist/Gewenst/Optioneel
Meting en Locatie:	De evaluator geeft aan waar hij de beschrijving van het element gevonden heeft in de architectuurdocumentatie. Daarnaast dient de evaluator een korte samenvatting te geven van het gevonden element. Wanneer een element niet aanwezig was of beoordeeld kon worden, dient dit hier ook aangeven te worden.
Conclusie en Rationale:	De evaluator geeft een verantwoording voor de getrokken conclusie.
Aanbevelingen:	Hier dient de evaluator op te schrijven wat eventueel verbeterd kan worden aan de architectuurdocumentatie met betrekking tot het element. Tevens heeft de evaluator hier de ruimte om op- en aanmerkingen te geven.

Tabel 4.15: Template voor rapportage van evaluatiecriteria.

Door de conclusie te verantwoorden is het voor de lezer van het rapport inzichtelijk waarom deze bepaalde conclusie is getrokken. De aanbevelingen geven direct een leidraad voor het verbeteren van de architectuurdocumentatie.

Deze tabellen worden allemaal opgenomen als bijlage in het uiteindelijke rapport. Het rapport zelf bestaat uit een management samenvatting van de meest belangrijke resultaten en het onderbouwde *go/no-go* advies voor het uitvoeren van de specifieke aspectscan.

4.3.2 Regels

Wanneer er voor één of meerdere vereiste elementen de conclusie *Afwezig* is getrokken, mogen de gewenste elementen niet meer geëvalueerd worden. Dit komt omdat dan het advies voor het uitvoeren van de specifieke aspectscan al duidelijk negatief is en de gewenste elementen hier niets meer aan kunnen veranderen. In deze situatie mag de specifieke aspectscan niet uitgevoerd worden en stopt de uitvoering.

De specifieke aspectscan is zo ontworpen dat van elementen die in de voorbereidende aspects-

can vereist zijn wordt aangenomen dat ze aanwezig zijn in de architectuurdocumentatie. De voorbereidende aspectscan werkt dus als een soort kwalificatie-ronde.

"Complexiteit is de vijand van beveiliging. Architectuur heeft als doel het reduceren van complexiteit."

John Sherwood (*SABSA®*, [28])

5

Specifieke Aspectscan

Dit hoofdstuk beschrijft de specifieke aspectscan, de tweede en laatste deelscan van de aspectscan Beveiliging en Privacy. Allereerst worden de verschillende te evalueren aandachtsgebieden geïdentificeerd in paragraaf 5.1 waarna de daadwerkelijke evaluatiecriteria gedefinieerd worden volgens een vast sjabloon zoals in hoofdstuk 4 bij de voorbereidende aspectscan. Het concluderen en rapporteren van de resultaten van de specifieke aspectscan wordt in paragraaf 5.4 behandeld.

Het doel van de specifieke aspectscan is om de elementen uit de voorbereidende aspectscan inhoudelijk en in samenhang te evalueren. Waar het bij de voorbereidende aspectscan over aanwezigheid en volledigheid gaat, is het bij de specifieke aspectscan met name van belang *hoe* de elementen beschreven zijn in tegenstelling tot de vraag *of* ze beschreven zijn.

5.1 Aandachtsgebieden voor Beveiliging en Privacy

De specifieke aspectscan wordt alleen uitgevoerd als de voorbereidende aspectscan succesvol is doorlopen zonder de afwezigheid van verplichte elementen.

De elementen uit tabel 4.1 worden voor de specifieke aspectscan niet op aanwezigheid maar op inhoudelijke kwaliteit en onderlinge samenhang geëvalueerd. In totaal zijn er 15 evaluatiecriteria gedefinieerd die zijn gegroepeerd in 9 aandachtsgebieden geïllustreerd in afbeelding 5.1. In toekomstige versies van deze aspectscan zullen mogelijk sommige evaluatiecriteria verdwijnen of aangevuld worden, en zullen er nieuwe toegevoegd worden. Deze flexibele norm zal na verloop van tijd steeds beter aansluiten bij de op dat moment actuele theoriën, raamwerken en best practises. Om dit te faciliteren kunnen er naar keuze aandachtsgebieden toegevoegd worden.

De elementen die in de voorbereidende aspectscan aangemerkt zijn als *Afwezig* kunnen niet verder geëvalueerd worden en vormen daarom geen onderdeel van de specifieke aspectscan. Elementen die in de voorbereidende aspectscan aangemerkt zijn als *Compleet* of *Incompleet*, zijn die elementen waarover wel een uitspraak gedaan wordt.

Afbeelding 5.1: Negen aandachtsgebieden voor evaluatiecriteria in de specifieke aspectscan.

5.2 Definitie van de Evaluatiecriteria

In deze paragraaf worden op de volgende bladzijden de evaluatiecriteria voor de specifieke aspectscan gedefinieerd. Per evaluatiecriterium wordt er een definitie van het begrip gegeven, wordt de relevantie aangetoond en de meetmethode beschreven en als laatste worden de regels om tot een bepaalde conclusie te komen beschreven.

De evaluatiecriteria zijn ook in dit hoofdstuk consistent in tabelvorm opgenomen zodat ze gemakkelijk bruikbaar zijn tijdens het uitvoeren van de evaluatie. Elk criterium heeft een nummer en een uniek onderschrift zodat er naar verwezen kan worden vanuit de rapportage van de resultaten.

In de ADEM is er ook nog per evaluatie een apart item 'Verantwoording van de manier van beoordelen' opgenomen, maar omdat dit in de praktijk vaak redundant of overbodig was (zie reflectie hoofdstuk 10.2) is er voor gekozen om in deze aspectscan de verantwoording samen te voegen met de beschrijving van de relevantie in het onderdeel 'Waarom is het belangrijk?'.

In tegenstelling tot de mogelijke waarden voor de conclusies van de verschillende evaluatiecriteria uit de voorbereidende aspectscan gebruiken de evaluatiecriteria uit de specifieke aspectscan de schaal {*Voldaan*, *Gedeeltelijk Voldaan*, *Niet Voldaan*} of {*Voldaan*, *Niet Voldaan*} om aan te geven in hoeverre de architectuurdocumentatie voldoet aan het evaluatiecriterium.

14. Behoefte aan Beveiliging	Beveiligingsbehoefte
Wat is het?	De behoefte aan beveiliging is een omschrijving van de mate waarin de organisatie behoefte heeft aan beveiliging zodat op basis van deze informatie een trade-off gemaakt kan worden.
Waarom is het van belang?	Niet alle organisaties hebben dezelfde behoefte aan beveiliging. Zo is het mogelijk om een snackbar te beveiligen als Fort Knox, maar dan zullen de klanten wegblijven en de snackbar failliet gaan. Het draait allemaal om de trade-off (Schneier, [24]) van de kosten en de baten van de beveiliging. Meer beveiliging betekent niet automatisch betere beveiliging. De behoefte aan beveiliging is onder andere afhankelijk van de business van de organisatie en het ecosysteem waar ze in opereert.
Hoe te meten?	Lees de architectuurdocumentatie door en zoek naar de beschrijving en verantwoording van de behoefte aan beveiliging.
Hoe een conclusie te trekken?	Als de behoefte aan beveiliging is beschreven: **Voldaan** In alle andere gevallen: **Niet Voldaan**

Tabel 5.1: Evaluatiecriterium 14: Behoefte aan Beveiliging.

15. Prioritering van Stakeholders	Stakeholders
Wat is het?	De prioritering van stakeholders is een lijst van stakeholders geordend op prioriteit en eventueel ingedeeld in de drie categorieën stakeholders voor het besluitvormingsproces: beslissende, beïnvloedende en overige stakeholders (Rijsenbrij, [22]).
Waarom is het van belang?	Er zijn altijd meerdere stakeholders, en stakeholders kunnen tegenstrijdige belangen (concerns) bij beveiliging en privacy hebben. Wanneer dit ontdekt wordt is het van belang een prioritering in stakeholders te hebben welke als uitgangspunt genomen kan worden om een discussie te starten om het conflict op te lossen. Hierbij wordt aangenomen dat de conflicterende concerns te herleiden zijn tot de stakeholders. Deze prioritering mag echter niet gebruikt worden om zomaar alle concerns van stakeholders met een lagere prioriteit van tafel te schuiven; er moet gestreefd worden naar een optimale samenhang met oog voor de belangen van alle stakeholders.
Hoe te meten?	Lees de architectuurdocumentatie door en controleer of de stakeholders met een belang bij beveiliging en privacy zijn geordend op prioriteit.
Hoe een conclusie te trekken?	Als de stakeholders geprioriteerd zijn: **Voldaan** In alle andere gevallen: **Niet Voldaan**

Tabel 5.2: Evaluatiecriterium 15: Prioritering van Stakeholders.

16. Dekking van Beveiligingsprincipes	Beveiligingsprincipes
Wat is het?	De dekking van beveiligingsprincipes geeft aan of er beveiligingsprincipes zijn op alle lagen van het architectuurraamwerk.
Waarom is het van belang?	Beveiliging is een business issue, het is niet alleen maar een technische zaak ([24, 28, 29]). Het is niet voldoende om een paar firewalls te installeren en alle email te versleutelen. De echte dreigingen komen vaak van binnen de organisatie, van (voormalig) personeel of social engineers, zowel opzettelijk als onbedoeld. Social Engineering is een techniek waarbij een computerkraker een aanval op computersystemen tracht te ondernemen door zichzelf voor te doen als iemand anders. Kenmerkend hierbij is dat er geen aanval is op de technische infrastructuur. Dit doet de aanvaller met het doel om via de aangenomen, vertrouwenwekkende, rol informatie te verkrijgen die op een andere manier niet of met aanzienlijk meer inspanning of hogere kosten te krijgen is. (Wikipedia) Er moet aandacht zijn voor beveiliging en privacy op alle lagen, van de organisatielaag tot en met de technische infrastructuur want beveiliging is een ketting. Een ketting is zo sterk als de zwakste schakel, en die zwakste schakel is vaak de mens. Als er geen bewustzijn is over beveiliging in de organisatie dan plakken werknemers Post-It's met hun wachtwoord op de monitor, of geven ze hun wachtwoord door over de telefoon aan iemand die zich voordoet als systeembeheerder.
Hoe te meten?	Lees de architectuurdocumentatie door en controleer of er op elke laag van het architectuurraamwerk specifieke beveiligingsprincipes zijn gedefinieerd. Als de beveiligingsprincipes niet zijn verdeeld over de lagen, controleer of voor zowel *people*, *process* en *technology* op operationeel, tactisch en strategisch niveau principes zijn beschreven (Connor et al, [10]).
Hoe een conclusie te trekken?	Als op alle bovenstaande lagen en niveau's beveiligingsprincipes zijn beschreven: **Voldaan** In alle andere gevallen: **Niet Voldaan**

Tabel 5.3: Evaluatiecriterium 16: Dekking van Beveiligingsprincipes.

17. Beveiligingsprincipes voor alle Doelen	Beveiligingsprincipes
Wat is het?	Dit evaluatiecriterium toetst of alle beveiligingsdoelen vertegenwoordigd zijn in de beveiligingsprincipes. De beveiligingsdoelen zijn beschikbaarheid, integriteit, vertrouwelijkheid, onloochenbaarheid en authorisatie.
Waarom is het van belang?	Goede beveiligingarchitectuur besteedt aandacht aan alle beveiligingsdoelen. De behoefte aan beveiligingsmaatregelen verschilt per bedrijfsmiddel, maar uiteindelijk moet de organisatie als geheel alle beveilingsdoelen bereiken. Door principes te formuleren die deze beveiligingsdoelen vertegenwoordigen kan de organisatie ervoor zorgen dat er ook regels, richtlijnen en standaarden worden opgesteld om deze doelen te bereiken.
Hoe te meten?	Lees de architectuurdocumentatie door en controleer of alle beveiligingsdoelen vertegenwoordigd zijn in de beveiligingsprincipes.
Hoe een conclusie te trekken?	Als alle vijf beveiligingsdoelen vertegenwoordigd zijn in de beveiligingsprincipes: **Voldaan** In alle andere gevallen: **Niet Voldaan**

Tabel 5.4: Evaluatiecriterium 17. Beveiligingsprincipes voor alle Doelen.

18. Ordening van Beveiligingsprincipes	Beveiligingsprincipes
Wat is het?	Dit evaluatiecriterium toetst of de beveiligingsprincipes zijn geordend volgens een ordeningsraamwerk zoals GAISP [15] of de indeling van Elsinga en Hofman [13]. Elsinga en Hofman ordenen beveiligingsprincipes in drie groepen: *mindset*principes op strategisch niveau; *architectuur*principes op tactisch niveau en *uitvoerings*principes op operationeel niveau voor respectievelijk hoe de organisatie denkt over beveiliging, hoe ze zich wil verdedigen en hoe die verdediging opgezet moet worden. Tevens zijn er in de Generally Accepted Information Security Principles (GAISP, [15]) 9 *pervasive* principes gedefinieerd met 14 *broad functional* principes die daarvan afgeleid zijn. Deze broad functional principes worden weer gedetailleerd in *detailled* principes.
Waarom is het van belang?	Met betrekking tot beveiliging gebruiken architecten vaker bestaande algemeen geaccepteerde principes. Om het kiezen van de meest toepasselijke beveiligingsprincipes te ondersteunen is het zinvol de principes te ordenen middels een raamwerk.
Hoe te meten?	Lees de architectuurdocumentatie door en controleer of de beveiligingsprincipes zijn geordend volgens een van de bovenstaande indelingen of een andere vergelijkbare indeling.
Hoe een conclusie te trekken?	Als alle beveiligingsprincipes geordend zijn: **Voldaan** In alle andere gevallen: **Niet Voldaan**

Tabel 5.5: Evaluatiecriterium 18. Ordening van Beveiligingsprincipes.

19. Prioritering van Beveiligingsprincipes	Beveiligingsprincipes
Wat is het?	De prioritering van beveiligingsprincipes is een lijst van beveiligingsprincipes geordend op prioriteit.
Waarom is het van belang?	Beveiligingsprincipes hebben vaker een zekere mate van overlapping. Het is dus goed mogelijk dat beveiligingsprincipes tegenstrijdigheden bevatten. Wanneer dit ontdekt wordt is het van belang een prioritering in beveiligingsprincipes te hebben welke als uitgangspunt genomen kan worden om een discussie te starten om het conflict op te lossen. Dit geldt voor beveiligingsprincipes onderling, maar ook voor conflicten tussen beveiligingsprincipes en de overige architectuurprincipes. Daarom moeten alle principes geprioriteerd worden, echter is dat geen onderdeel van deze aspectscan maar hoort het in de holistische scan van de ADEM.
Hoe te meten?	Lees de architectuurdocumentatie door en controleer of de beveiligingsprincipes zijn geprioriteerd.
Hoe een conclusie te trekken?	Als alle de beveiligingsprincipes geprioriteerd zijn: **Voldaan** In alle andere gevallen: **Niet Voldaan**

Tabel 5.6: Evaluatiecriterium 19. Prioritering van Beveiligingsprincipes.

20. Herleidbaarheid van Beveiligingsprincipes	Beveiligingsprincipes
Wat is het?	Herleidbaarheid van beveiligingsprincipes houdt in dat alle beveiligingsprincipes te herleiden zijn tot hun bron. Deze bronnen kunnen risico's zijn, stakeholder concerns, wet- en regelgeving of de bedrijfsvisie (zie rationaliseringsketen, pagina 16). Voor elk beveiligingsprincipe dient de bron vermeld te worden.
Waarom is het van belang?	Als beveiligingsprincipes herleidbaar zijn tot hun bronnen is het bestaansrecht van de principes duidelijker te verantwoorden. In de andere richting kan als een bron van concerns verandert beter gezien worden welke impact dit heeft op de bestaande principes.
Hoe te meten?	Lees de architectuurdocumentatie door en controleer of alle beveiligingsprincipes herleidbaar zijn tot minimaal één van de bovenstaande bronnen.
Hoe een conclusie te trekken?	Als alle beveiligingsprincipes herleidbaar zijn: **Voldaan** In alle andere gevallen: **Niet Voldaan**

Tabel 5.7: Evaluatiecriterium 20. Herleidbaarheid van Beveiligingsprincipes.

21. Dekking van Beveiligingsmaatregelen	Beveiligingsmaatregelen
Wat is het?	Het is gebruikelijk om beveiligingsmaatregelen in te delen in de drie groepen: administratieve, technische en fysieke maatregelen (Killmeyer, [29]). Administratieve maatregelen zijn bijvoorbeeld het scheiden van functies en het handhaven van gedragslijnen. Technische maatregelen zijn zaken zoals encryptie en antivirusproducten. Fysieke beveiligingsmaatregelen zijn wel belangrijk voor een goede beveiliging, maar horen niet thuis in de architectuurdocumentatie. Het gaat hier meestal om dingen zoals hekken, sloten en waakhonden. Naast de indeling in groepen is er ook een gebruikelijke indeling in soorten maatregelen. Oorspronkelijk werden maatregelen ingedeeld in preventieve en detectieve maatregelen [29]. Later kwamen daar reactieve maatregelen bij om zo snel mogelijk weer te herstellen en repressieve maatregelen om een aanval te kunnen onderdrukken. Met de opkomst van governance en auditing zijn hier maatregelen aan toegevoegd die het mogelijk maken de aanval en reactie te evalueren om hier van te leren.
Waarom is het van belang?	Een aantal jaren geleden werd beveiliging nog altijd gezien als een technisch probleem met een technische oplossing. Dit beeld is nu veranderd, beveiliging is een business issue. Er moeten dus ook administratieve maatregelen komen want als je een server perfect technisch beveiligd, maar het wachtwoord staat op een sticker onder het toetsenbord, dan is het hele systeem lek. Het is van belang om te controleren of er aandacht is geweest voor alle belangrijke groepen en soorten beveiligingsmaatregelen zodat er geen zwakke schakels in de beveiliging zitten.
Hoe te meten?	Lees de architectuurdocumentatie door en controleer of er zowel administratieve als technische beveiligingsmaatregelen zijn geformuleerd. Controleer tevens of er zowel preventieve, detectieve, reactieve, onderdrukkende en evaluatieve (nabeschouwende) beveiligingsmaatregelen worden beschreven.
Hoe een conclusie te trekken?	Als er zowel administratieve als technische maatregelen zijn in alle vijf soorten: **Voldaan** Als er zowel administratieve als technische maatregelen zijn in de soorten preventief, detectief en reactief: **Gedeeltelijk Voldaan** In alle andere gevallen: **Niet Voldaan**

Tabel 5.8: Evaluatiecriterium 21. Dekking van Beveiligingsmaatregelen.

22. Impact van Beveiligingsmaatregelen	Beveiligingsmaatregelen
Wat is het?	De impact van beveiligingsmaatregelen geeft aan op welk gebied de beveiligingsmaatregelen invloed hebben, en in welke mate.
Waarom is het van belang?	Het is belangrijk te weten wat de impact is van de beveiligingsmaatregelen omdat deze consequenties kunnen hebben voor andere maatregelen. Ook kan een beveiligingsmaatregel die het ene bedrijfsmiddel beschermt een zwakheid introduceren in een ander bedrijfsmiddel. Door beveiligingsmaatregelen te implementeren wordt doorgaans de complexiteit verhoogd, je voegt immers componenten toe aan een systeem. Complexiteit is echter de vijand van beveiliging, dus de beveiligingsmaatregelen moeten met zorg gekozen worden en met aandacht voor de impact en consequenties van de implementatie.
Hoe te meten?	Lees de architectuurdocumentatie door en controleer of bij alle beveiligingsmaatregelen de impact is beschreven.
Hoe een conclusie te trekken?	Als voor alle beveiligingsmaatregelen de impact is beschreven: **Voldaan** In alle andere gevallen: **Niet Voldaan**

Tabel 5.9: Evaluatiecriterium 22. Impact van Beveiligingsmaatregelen.

23. Theoretische effectiviteit van Beveiligingsmaatregelen ★	Beveiligingsmaatregelen
Wat is het?	De effectiviteit van de beveiligingsmaatregelen geeft aan of de beschreven beveiligingsmaatregelen het gewenste niveau van de bedrijfsdoelen garanderen zoals gedefinieerd in de bedrijfsmiddelenclassificatie, uitgaande van de gedefinieerde baseline. Een simpel voorbeeld is: de huidige baseline voor de klantendatabase geeft aan dat de vertrouwelijkheid van de gegevens 'Laag' is. Als oplossing wordt de beveiligingsmaatregel 'encryptie van de gegevens' aangedragen. Het gewenste niveau van vertrouwelijkheid voor het bedrijfsmiddel klantendatabase is 'Hoog'. Kan de encryptie dit theoretisch gezien waarmaken?
Waarom is het van belang?	Dit evaluatiecriterium geeft inzicht in de theoretische effectiviteit van de gekozen oplossingen. Omdat de architectuurdocumentatie een toekomstig gewenste situatie beschrijft is het nog niet mogelijk om in de praktijk de effectiviteit van de beveiligingsmaatregelen te meten, omdat ze nog niet geïmplementeerd zijn.
Hoe te meten?	Dit is een evaluatiecriterium dat door een expert op het gebied van beveiliging uitgevoerd moet worden. Het resultaat hiervan wordt opgenomen in de conclusie van dit evaluatiecriterium.
Hoe een conclusie te trekken?	Indien de expert van mening is dat de beschreven beveiligingsmaatregelen adequaat zijn: **Voldaan** In alle andere gevallen: **Niet Voldaan**

Tabel 5.10: Evaluatiecriterium 23. Theoretische effectiviteit van Beveiligingsmaatregelen.

24. Beschrijving van Risico's	Risico Management
Wat is het?	Dit evaluatiecriterium toetst de beschrijving van de risico's. Van belang is zijn de volledigheid van de risico's, de vraag of de risico's specifiek genoeg zijn, en dat risico's worden beschreven op het niveau waarop ze gemanaged worden. Onder volledigheid van de beschrijving wordt verstaan dat voor alle risico's de volgende zaken worden beschreven: ◇ De kans op of waarschijnlijkheid van het voorkomen van het risico. ◇ De impact of consequenties als het risico zich manifesteert. Dit is meestal uitgedrukt in kosten of schade. ◇ De eigenaar en eindverantwoordelijke voor het risico. Er moet altijd iemand eigenaar en verantwoordelijke zijn voor een risico. Dit hoeft niet dezelfde persoon te zijn. ◇ De betreffende bedrijfsmiddelen die bedreigd worden. ◇ De prioriteit: risico's met een hoge kans en een hoge impact dienen zo snel mogelijk gemanaged te worden. ◇ De risico management strategie die genomen wordt met betrekking tot dit risico. Er zijn vier mogelijke manieren om een risico te managen: *Acceptance*, *Avoidance*, *Mitigation* en *Transference*. Risico's met een verwaarloosbare of acceptabele kans en impact kunnen geaccepteerd worden. Mitigation houdt in het matigen van het risico door beveiligingsmaatregelen. Bij transference verplaats je het risico door bijvoorbeeld een verzekering af te sluiten of beveiliging voor dat risico te outsourcen. Avoidance is geen acceptabele strategie omdat dan eigenlijk alleen geprobeerd wordt het risico uit de weg te gaan, terwijl er geen beveiligingsmaatregelen worden genomen. (Killmeyer, [29]).
Waarom is het van belang?	Risico's moeten altijd specifiek zijn, tegen algemene risico's kan een organisatie zich niet goed beveiligen. Door de bovenstaande zaken te beschrijven worden de risico's specifieker en begrijpelijker voor alle stakeholders. Daarnaast dient het invullen van een vaste lijst in de beschrijving ook als leidraad bij de discussie over het analyseren van de risico's.
Hoe te meten?	Lees de architectuurdocumentatie door en controleer of alle genoemde zaken per risico worden beschreven en of de risico's worden beschreven op het juiste niveau. Een risico over een technische aanval op een encryptie-algoritme hoort bijvoorbeeld op de operationele niveaus.
Hoe een conclusie te trekken?	Als alle zaken per risico zijn beschreven: **Voldaan** In alle andere gevallen: **Niet Voldaan**

Tabel 5.11: Evaluatiecriterium 24. Beschrijving van Risico's.

25. Dekking van Risico's	Risico Management
Wat is het?	De dekking van risico's geeft aan of er risico's van alle 4 domeinen geïdentificeerd door Sherwood (SABSA®, [28]) zijn beschreven in de architectuurdocumentatie: ◇ People – Opzettelijke menselijke fouten en nalatigheid van het personeel. ◇ Processes – Fouten in bestaande procedures. ◇ Systems – Slecht ontworpen systemen, systemuitval. ◇ External – Kwaadwillende derden, natuurrampen, nalatigheid van derden.
Waarom is het van belang?	Het is van belang om aandacht te hebben voor alle domeinen waaruit risico's kunnen ontstaan zodat er geen risico's over het hoofd gezien worden. Tegen onbekende risico's kun je geen beveiligingsmaatregelen nemen, dus loop je het risico dat er zwakke schakels in de beveiliging zitten.
Hoe te meten?	Lees de architectuurdocumentatie door en controleer of er risico's van alle 4 bovenstaande domeinen zijn beschreven.
Hoe een conclusie te trekken?	Als alle vier domeinen worden vertegenwoordigd: **Voldaan** In alle andere gevallen: **Niet Voldaan**

Tabel 5.12: Evaluatiecriterium 25. Dekking van Risico's.

26. Bescherming van Persoonsgegevens	Privacy
Wat is het?	Dit evaluatiecriterium evalueert of de organisatie de intentie uitdraagt om de bescherming van persoonsgegevens te garanderen.
Waarom is het van belang?	Voor de meeste Nederlandse informatieverwerkende organisaties is de Wet bescherming persoonsgegevens (Wbp, [18]) van toepassing. Deze wet vervangt de Wet persoonsregistraties (WPR). Naleving van toepasselijke wetten is verplicht voor alle organisaties.
Hoe te meten?	Lees de architectuurdocumentatie door en controleer of de Wbp van toepassing is op de organisatie (of een van de organisatieonderdelen) door de test uit te voeren uit de handleiding van de Wbp [23]. Indien de wet van toepassing is, lees de architectuurdocumentatie door en zoek naar een verantwoording van de risicoklasse waarin de organisatie zich bevindt volgens de wet en welke artikelen uit de wet gevolgen hebben voor de de architectuur en via die weg de inrichting van de informatievoorziening. Des te hoger de risicoklasse, des te meer beveiligingseisen de Wbp stelt.
Hoe een conclusie te trekken?	Als de Wbp van toepassing is en dit verwoord is tezamen met de verantwoording van de risicoklasse en een opsomming van de wetsartikelen: **Voldaan** In alle andere gevallen: **Niet Voldaan**

Tabel 5.13: Evaluatiecriterium 26. Bescherming van Persoonsgegevens.

27. Bad Practises in Beveiligingsprincipes	Bad Practises
Wat is het?	Elsinga en Hofman hebben in het artikel *Security Principles* [13] een opsomming gemaakt van 20 beveiligingsprincipes op strategisch en operationeel niveau die als bad practise gezien worden.
Waarom is het van belang?	Hoewel er situaties zijn waarin sommige van de genoemde 'slechte' beveiligingsprincipes goed kunnen werken is het toch van belang om wanneer deze principes ontdekt worden in de architectuurdocumentatie hieraan extra aandacht te besteden. De architect dient dan in discussie te gaan met de boardroom en de verschillende stakeholders om samen vast te stellen of de betreffende beveiligingsprincipes wel juist zijn voor de organisatie. Daarnaast dienen ze ook als een soort van checklist voor de mindset over beveiliging in de organisatie.
Hoe te meten?	Lees de architectuurdocumentatie door en controleer of de beveiligingsprincipes overeenkomen met bad practise beveiligingsprincipes van Elsinga en Hofman.
Hoe een conclusie te trekken?	Als er geen principes zijn die overeenkomen: **Voldaan** Als alle principes zijn die wel overeenkomen een goede onderbouwing hebben: **Gedeeltelijk Voldaan** In alle andere gevallen: **Niet Voldaan**

Tabel 5.14: Evaluatiecriterium 27. Bad practises in Beveiligingsprincipes.

28. Raamwerken voor Beveiligingsarchitectuur	Raamwerken en Standaarden
Wat is het?	Er zijn een aantal raamwerken voor het ontwikkelen van een (enterprise) architectuur voor beveiliging gedefinieerd. Dit zijn onder andere het *Enterprise Information Security Architecture* raamwerk (EISA, [26]) en het *Sherwood Applied Business Security Architecture* raamwerk (SABSA®, [28]). Vooral SABSA® is sterk gebaseerd op best practises en biedt veel praktische hulpmiddelen om een holistische aanpak van beveiligingsarchitectuur te ondersteunen.
Waarom is het van belang?	Het gebruik van raamwerken biedt veel voordelen voor de architect. Raamwerken zijn meestal gebaseerd op best practises en proven technology. Een architectuurontwikkelproces dat ondersteund wordt door een raamwerk is daardoor herhaalbaar en beter te plannen. Daarnaast biedt een raamwerk een vaste structuur die de architectuurdocumentatie meer inzichtelijk en beter communiceerbaar maakt.
Hoe te meten?	Lees de architectuurdocumentatie door en controleer of er een bestaand raamwerk gebruikt wordt voor het ontwikkelen van de beveiligingsarchitectuur.
Hoe een conclusie te trekken?	Als er een bestaand raamwerk gebruikt wordt: **Voldaan** In alle andere gevallen: **Niet Voldaan**

Tabel 5.15: Evaluatiecriterium 28. Raamwerken voor Beveiligingsarchitectuur.

5.3 Niet uitgewerkte Evaluatiecriteria

Door een gebrek aan tijd zijn helaas niet alle tijdens het onderzoek geïdentificeerde evaluatiecriteria uitgewerkt in deze specifieke aspectscan. Deze paragraaf geeft kort weer welke evaluatiecriteria nog uitgewerkt zouden moeten worden in een volgende versie van de aspectscan.

5.3.1 Aandachtsgebied Bedrijfsmiddelenclassificatie

Een bedrijfsmiddelenclassificatie (*asset classification*) is een overzicht van alle tastbare en ontastbare bedrijfsmiddelen die waarde hebben voor de organisatie. In dit overzicht wordt onder andere aangegeven welke business waarde elk bedrijfsmiddel heeft, waar het zich bevindt, wie de eigenaar en de eindverantwoordelijke zijn en welke niveaus van beschikbaarheid, integriteit, vertrouwelijkheid, onloochenbaarheid en authentificatie gewenst zijn.

Deze niveaus bestaan uit waarden die in classificatieschemas zijn opgesteld. Een gebruikelijk classificatieschema voor vertrouwelijkheid is van laag naar hoog: {*publiek*, *privé*, *vertrouwelijk*, *staatsgeheim*}. Tijdens gesprekken met beveiligingsexperts werd ook consequent gesteld dat de beveiliging begint met het opstellen van een bedrijfsmiddelclassificatie.

De volgende evaluatiecriteria zijn niet gedefinieerd in deze versie van de aspectscan:

- ◇ Zijn de vier soort bedrijfsmiddelen[1] vertegenwoordigd?
- ◇ Is er voor alle bedrijfsmiddelen minimaal één persoon als eigenaar gedefinieerd?
- ◇ Is er voor alle bedrijfsmiddelen minimaal één persoon als eindverantwoordelijke?
- ◇ Zijn voor alle beveiligingsdoelen classificatieschemas gedefinieerd?
- ◇ Zijn voor alle bedrijfsmiddelen de beveiligingsdoelen geclassificeerd?
- ◇ Is voor alle bedrijfsmiddelen de businessvalue gedefinieerd?
- ◇ Is voor alle bedrijfsmiddelen de lokatie gedefinieerd?
- ◇ Zijn voor alle bedrijfsmiddelen de toegangsrechten gedefinieerd?

5.3.2 Aandachtsgebied Privacy

Op het gebied van privacy en de Wet bescherming persoonsgegevens (Wbp, [18]) is het volgende evaluatiecriterium niet gedefinieerd in deze versie van de aspectscan:

- ◇ Worden er oplossingen aangedragen die de persoonlijke levenssfeer van de werknemers, klanten of burgers kunnen aantasten?

5.3.3 Menselijke Maat en Beveiliging

Er is een interessante overlap tussen het aspect Beveiliging en Privacy en het aspect Menselijke Maat. Het is vaak het geval dat het gebruiksgemak het moet afleggen tegen de beveiligingsmaatregelen, zoals gebruikers die voor elk systeem waar ze mee werken een ander lang en complex wachtwoord moeten onthouden.

[1] Information assets, software assets, physical assets en services. (Identifying and Classifying Assets, [27])

Anderzijds kan ook de beveiliging wijken voor het gebruiksgemak: een systeembeheerder die niet voor alle servers het wachtwoord wil onthouden stelt misschien overal hetzelfde wachtwoord in. Er is behoefte aan een goede balans tussen deze twee aspecten met zo weinig mogelijk compromissen aan beide kanten.

Het volgende evaluatiecriterium is niet gedefinieerd in deze versie van de aspectscan:

- ◇ Wordt er bij de beschrijving van de beveiligingsarchitectuur voldoende rekening gehouden met de menselijke maat, in zowel principes, regels, richtlijnen en standaarden?

5.3.4 Creatieve Risico Analyse

Een alternatieve methode om de dekking enc ompleetheid van de risico analyse te kunnen meten kwam naar voren tijdens een interview met Ben Elsinga en Aaldert Hofman van Capgemini.

De creatieve risico analyse houdt in dat de evaluator de architectuurdocumentatie in zijn geheel doorleest en zichzelf gedurende het lezen continue onder andere de volgende vragen stelt:

- ◇ Wat kan er hiermee fout gaan?
- ◇ Wat gebeurt er als dit fout gaat?
- ◇ Hoe kan dit kapot / uitgeschakeld / verstoord worden?

Deze vragen dienen gesteld te worden bij alle voorgestelde oplossingen in de architectuurdocumentatie. Wanneer deze vragen na het doorlezen van de architectuurdocumentatie nog niet (voldoende) beantwoord zijn is het mogelijk dat de oorspronkelijke risico analyse incompleet is en onvolledig is uitgevoerd. Voor het meten van dit evaluatiecriterium is een expert op het gebied van beveiliging nodig die voldoende ervaring heeft om potentiële risico's te identificeren.

5.4 Concluderen en Rapporteren

De specifieke aspectscan wordt alleen uitgevoerd bij een duidelijk *go*-advies vanuit het rapport van de voorbereidende aspectscan. Als aan deze voorwaarde is voldaan dan is de methode van concluderen en rapporten voor de specifieke aspectscan hetzelfde als voor de voorbereidende aspectscan. Deze methode is beschreven in paragraaf 4.3 op pagina 29.

De evaluator vult voor de specifieke aspectscan hetzelfde template in als voor de voorbereidende aspectscan, dat in tabel 4.15 is opgenomen. Eveneens bestaat het rapport van de specifieke aspectscan uit een samenvatting van de gevonden resultaten en een overzicht van de belangrijkste aanbevelingen.

"In theory there is no difference between theory and practice. In practice there is."

YOGI BERRA

6

Best Practises in Beveiliging en Privacy

Dit hoofdstuk bevat een verzameling van bronnen van best practises met betrekking tot beveiliging en privacy. Deze fungeert als aanzet voor een best practises bibliotheek voor de aspectscan Beveiliging en Privacy.

6.1 Standards of Good Practise for Information Security

Er is een uitgebreid 247 pagina's tellend handboek [11] opgesteld door het Information Security Forum (ISF). Dit handboek is gevuld met best practises van de leden van het ISF en wordt elke twee jaar herzien en gepubliceerd in een nieuwe versie. Dit handboek deelt best practises op in vijf categorieën: Computer Installations, Networks, Critical Business Applications, Systems Development en Security Management.

Computer Installations en *Networks* vormen de onderliggende infrastructuur waar de *Critical Business Applications* op draaien. *Systems Development* gaat over de ontwikkeling van nieuwe applicaties en *Security Management* adresseert sturing en beheersing op hoog niveau.

6.2 Standaarden en Normen

Het vakgebied beveiliging en privacy heeft alles behalve een gebrek aan internationale en nationale normen en standaarden. Een aantal van deze normen en standaarden worden hier genoemd.

De ISO 27000-series van standaarden wordt op dit moment gepland en zal een reeks standaarden bevatten over management van informatiebeveiliging in dezelfde vorm als de veelgebruikte ISO 9000-series over kwaliteitsaspecten. ISO/IEC 17799:2005 is de meest recente versie van de ISO standaard '*Information technology - Security techniques - Code of practice for information security management*' en zal later opgenomen worden in de 27000-series.

Naast de ISO standaarden is er het IT governance raamwerk CobiT van ISACA en het IT

Governance Instituut. De CobiT is op dit moment bij versie 4.1 en wordt wereldwijd veel gebruikt. In Nederland wordt vooral de Code voor Informatiebeveiliging (CvIB) veel toegepast door organisaties.

Een wat oudere norm die nog geregeld wordt gebruikt is de ITSEC: *Information Technology Security Evaluation Criteria*. Deze norm is 1990 gepubliceerd door een samenwerkingsverband tussen Frankrijk, Duitsland, Nederland en het Verenigde Koninkrijk.

III

Casus Amsterdam
Handboek Architectuur

7

Inleiding en Aanpak

In deel II van deze scriptie werd een aanzet gemaakt tot een aspectscan voor het evalueren van het aspect Beveiliging en Privacy in architectuurdocumentatie. Deze aspectscan maakt deel uit van de aspectfase van de Architectuurdocumentatie Evaluatiemethode (ADEM, [9]).

Dit deel van de scriptie beschrijft de toetsing van de ontwikkelde aspectscan. De aspectscan voor Beveiliging en Privacy bestaat uit 2 deelscans: de voorbereidende aspectscan en de specifieke aspectscan. De voorbereidende aspectscan is een soort kwalificatie voor de specifieke aspectscan. De specifieke aspectscan wordt alleen uitgevoerd bij een duidelijk *go*-advies vanuit de voorbereidende aspectscan. Aanvankelelijk worden beide deelscans door middel van een case study getoetst.

De Gemeente Amsterdam heeft haar architectuur gedocumenteerd in het Handboek Architectuur [3]. Dit handboek is publiekelijk beschikbaar gesteld via de website[1] van de gemeente en een van de opstellers van het handboek, Dries Bartelink, heeft toestemming verleend om deze architectuurdocumentatie als casus materiaal te gebruiken.

Voor de uitvoering van de case study wordt gebruik gemaakt van versie 0.1 van 23 augustus 2006. Dit is dezelfde versie als voor de uitvoering van de globale fase van de ADEM is gebruikt.

7.1 Doel

Het primaire doel van het uitvoeren van de aspectscan Beveiliging en Privacy op het Handboek Architectuur in de context van deze case study is niet het evalueren van de kwaliteit van de architectuurdocumentatie maar het toetsen van de aanzet tot een dergelijke aspectscan die in deze scriptie is gemaakt.

Door de aspectscan in de praktijk toe te passen op de architectuurdocumentatie kunnen de bruikbaarheid en toepasbaarheid getoetst worden. Indien de evaluatie goed verloopt, levert het voor de Gemeente Amsterdam een aantal eerste inzichten op over het aspect Beveiliging en Privacy in haar architectuurdocumentatie en eventueel een aantal bruikbare aanbevelingen.

[1] Handboek Architectuur: http://www.ict.amsterdam.nl/documents/HandboekArchitectuur.pdf

7.2 Uitzondering op de Regel

De methode stelt als regel dat wanneer er één of meerdere vereiste elementen als *Afwezig* of *Incompleet* wordt beoordeeld de gewenste elementen niet meer geëvalueerd mogen worden. In hoofdstuk 9 zal blijken dat dit voor het Handboek Architectuur het geval is. Om de voorbereidende aspectscan toch nog verder te kunnen toetsen wordt deze regel niet gehanteerd in deze casus.

In het volgende hoofdstuk wordt er een korte samenvatting gegeven van het Handboek Architectuur in het licht van het aspect Beveiliging en Privacy. Het doel van deze samenvatting is om snel in grote lijnen aan te geven wat er met betrekking tot beveiliging en privacy beschreven is in de architectuurdocumentatie.

Hoofdstuk 9 beschrijft de rapportage van de resultaten van de uitvoering van de aspectscan en vat de aanbevelingen samen. Tevens zijn in dit hoofdstuk de gedetailleerde metingen opgenomen in de vorm van het template dat hiervoor gedefinieerd is in tabel 4.15.

8

Beveiliging in het Handboek Architectuur

Dit hoofdstuk bestaat uit een korte samenvatting van het Handboek Architectuur [3] van de Gemeente Amsterdam in het licht van het aspect Beveiliging en Privacy. Deze samenvatting geeft een overzicht van de onderdelen in de architectuurdocumentatie waar beveiliging en privacy aan de orde komen. Het is in dit hoofdstuk niet de bedoeling om een volledige samenvatting te geven voor het hele document; een samenvatting die het gehele Handboek Architectuur beslaat is opgenomen als hoofdstuk in de bijlage '*Evaluatie Handboek Architectuur Amsterdam: Uitvoering van de Globale Fase*' [8].

De versie van het Handboek Architectuur die in deze scriptie geëvalueerd wordt is versie 0.1 van 23 augustus 2006. Er is een nieuwe versie in de maak maar die was ten tijde van het onderzoek voor deze scriptie nog niet publiekelijk beschikbaar. Tevens is bij het toetsen van de globale fase van de ADEM dezelfde versie van het handboek gebruikt.

Opgemerkt moet worden dat de Adviesgroep Architectuur zich ervan bewust is dat het aspect beveiliging en privacy in het Handboek Architectuur nog erg in de kinderschoenen staat. Dit wordt duidelijk door de verscheidene voetnoten en opmerkingen in de tekst zoals bij elke paragraaf over beveiliging in de vijf lagen: 'Verdere uitwerking vindt nog plaats i.s.m. het Platform Informatiebeveiliging' en de opmerking 'In volgende versies van de architectuur dient dit onderdeel nog verder verdiept te worden'. Vooral bij de bovenste lagen is er bijna geen beschrijving van het aspect beveiliging en privacy.

Het doel van deze versie van het Handboek Architectuur is dan ook: 'het faciliteren en stimuleren van samenwerking door het bieden van inzicht en overzicht, en het aanreiken van richtlijnen en standaarden die primair zijn gericht op (de ontwikkeling van) gemeenschappelijke voorzieningen voor de gemeente Amsterdam en het programma Basisregistraties en ICT-voorzieningen in het bijzonder' (PAGINA 2-3, [3]).

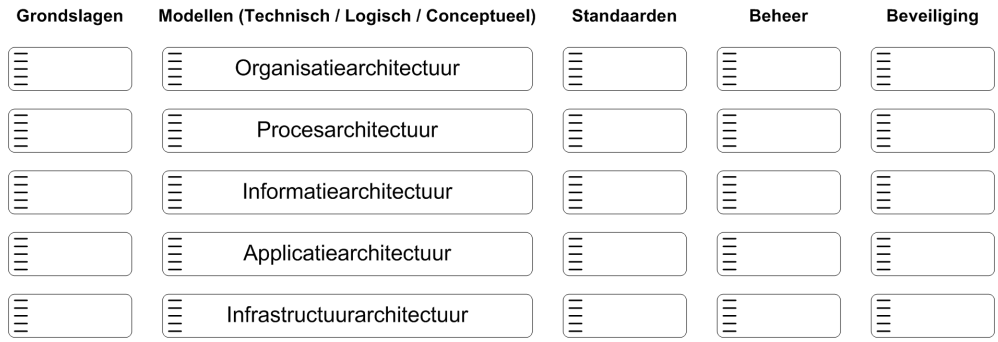
8.1 Terminologie

Voor de duidelijkheid is het goed te vermelden dat men in het Handboek Architectuur spreekt over grondslagen in plaats van architectuurprincipes. Daarnaast gebruikt de Adviesgroep Architectuur de term bedrijfsobject voor bedrijfsmiddelen en zijn richtlijnen een bijzondere vorm van standaarden. De betekenis van de term richtlijn is echter hetzelfde als in deze scriptie.

In deze scriptie wordt *Beveiliging en Privacy* (met hoofdletters) gebruikt als naam voor het aspect. Privacy wordt dus expliciet genoemd naast beveiliging omdat het speciale aandacht verdiend. Het Handboek Architectuur spreekt voornamelijk over beveiliging, maar het is duidelijk dat privacy hieronder valt.

8.2 Het Amsterdams Architectuurraamwerk

De Gemeente Amsterdam gebruikt een model met vijf lagen als architectuurraamwerk. Dit raamwerk deelt een architectuur inhoudelijk op in vijf (horizontale) lagen en vijf (verticale) kolommen (zie afbeelding 8.1).



Afbeelding 8.1: Het Amsterdamse architectuurraamwerk.

Beveiliging wordt onderkend als een belangrijk aspect dat vaak een ondergeschoven kindje is. Om zelf niet in deze valkuil te vallen is beveiliging opgenomen als apart viewpoint op alle lagen van het architectuurraamwerk. Dit houdt in dat elke laag in een apart hoofdstuk beschreven is, en dat voor alle lagen een paragraaf aan beveiliging is gewijd. Op PAGINA 1-2 wordt aangegeven dat het Handboek 'concrete afspraken over beveiliging' bevat.

8.3 Gemeentelijke Informatiebeveiligingsnorm

Op pagina 2-8 van het Handboek Architectuur wordt beschreven wat dit viewpoint op beveiliging inhoudt:

Het beleid voor informatiebeveiliging binnen de gemeente is vastgelegd in de Gemeentelijke InformatiebeveiligingsNorm (GIBN). De GIBN is een samenhangend geheel van maatregelen van procedurele, organisatorische, fysieke, technische en juridische aard.

Het raakt aan:

- ◇ algemeen beveiligingsbeleid (bijv. deuren, kluizen, toegangscontrole)
- ◇ personeelsbeleid (bijv. screening, opleiding en functietypering)
- ◇ organisatiebeleid (bijv. functiescheiding)
- ◇ informatiebeleid (bijv. standaardisering en 'proven technology')
- ◇ privacybeleid (bijv. correct gebruik van persoonsgegevens)
- ◇ juridisch beleid (bijv. afbreukrisico's bij privacyschendingen, clausulering in overeenkomsten met derden, Third Party Mededelingen)

Het doel van de GIBN is het behoud van:

- ◇ continuïteit en beschikbaarheid (voorkomen van uitval van systemen),
- ◇ integriteit en betrouwbaarheid (gegevens zijn juist, actueel en volledig)
- ◇ exclusiviteit en vertrouwelijkheid (onbevoegden kunnen geen kennis nemen van informatie die een organisatie onder zich heeft)

Per laag is aangegeven welke paragrafen uit de GIBN van toepassing zijn. Zonodig zijn ook aanvullende richtlijnen of uitgangspunten opgenomen. In volgende versies van de architectuur dient dit onderdeel nog verder verdiept te worden.

De Gemeentelijke InformatiebeveiligingsNorm (GIBN, versie 2.0 april 2005) zelf maakt echter geen onderdeel uit van de architectuurdocumentatie en is ook geen bijlage, het is een apart document en zal daarom niet geëvalueerd worden. Wel worden er in BIJLAGE 3 een paar hoofdlijnen uit de GIBN genoemd.

Op alle lagen van het architectuurraamwerk wordt in de paragraaf over beveiliging een opsomming gemaakt van de paragrafen uit de GIBN die van toepassing zijn en wordt de titel van die paragraaf genoemd. De daadwerkelijke invulling daarvan is de verantwoordelijkheid van de losse organisatieonderdelen. Naast de opsomming van paragrafen is er op sommige lagen een korte aanvulling op de GIBN opgenomen, maar deze onderdelen zijn hoofdzakelijk placeholders en zullen in samenwerken met het Platform Informatiebeveiliging in latere versies uitgewerkt worden.

8.4 Beveiligingsprincipes

Het Handboek Architectuur beschrijft architectuurprincipes per laag van het model, maar bevat geen specifieke opsomming van beveiligingsprincipes. Wel zijn er twee principes die im-

pact hebben op de inrichting van beveiliging in de Gemeente Amsterdam op de verschillende lagen: grondslag 0.1 over privacy en grondslag 3.4 over informatiebeveiliging.

Grondslag 0.1 De gemeente Amsterdam ontsluit publieke informatie, maakt zichtbaar wat zij doet, welke besluiten ze neemt, welke gegevens zij heeft en gebruikt en hoe zij werkt.

Grondslag 3.4 De gemeente Amsterdam garandeert de vertrouwelijkheid van gegevens, betrouwbaar (digitaal) contact en zorgvuldige (elektronische) archivering.

Verder zijn er nog twee principes die raakvlakken hebben met het aspect, zijnde grondslag 0.2 over naleving van wet- en regelgeving en grondslag 3.2 over de inrichting van de informatiehuishouding.

Grondslag 0.2 De gemeente Amsterdam voert haar taken uit volgens de wet en volgt bestaande en aangekondigde wet- en regelgeving.

Grondslag 3.2 Gegevens worden éénmalig opgeslagen en meervoudig gebruikt.

Grondslag 0.2 geeft aan dat de Gemeente Amsterdam zich aan de Wet bescherming persoonsgegevens gaat houden en daardoor de privacy van de burger gaat beschermen, maar ook de aangekondigde wet op dataretentie zal naleven. De keuze voor het eenmalig opslaan van alle gegevens op een centrale plaats is vanuit beveiligingsoogpunt van belang, omdat deze centrale plaats dan een populair doelwit zal worden. Dit wordt in vakjargon een *single point of failure* genoemd. En als laatste zijn er drie grondslagen uit de applicatielaag (4.2 en 4.3) en infrastructuurlaag (5.1) genoemd die handelen over standaardisering. Dit heeft ook invloed op de beveiliging. Het is meestal veiliger om open standaarden te gebruiken voor bijvoorbeeld authentificatie en authorisatie protocollen.

Grondslag 4.2 Applicaties zijn gebaseerd op open standaarden en platform onafhankelijk.

Grondslag 4.3 De gemeente Amsterdam maakt maximaal gebruik van standaard componenten.

Grondslag 5.1 De infrastructuur is schaalbaar, betrouwbaar en gebaseerd op open standaarden.

Wat betreft de betrouwbaarheid in grondslag 5.1 wordt op PAGINA 1-1 geschreven dat de diensten van de Gemeente Amsterdam voor de burger 24/7 beschikbaar moeten zijn. Om dit te kunnen realiseren moet de infrastructuur betrouwbaar zijn.

In een voetnoot op PAGINA 3-1 staat dat 'in de Nederlandse Overheid Referentie Architectuur (NORA, [20]) heel veel grondslagen staan. Veel van deze grondslagen zouden ook van toepassing kunnen worden verklaard op deze architectuur'. De NORA bevat inderdaad een verzameling van dertig beveiligingsprincipes maar de Adviesgroep Architectuur heeft er voor gekozen om het in ieder geval in deze versie bij een kleine verzameling principes te houden.

9

Resultaten en Aanbevelingen

In dit hoofdstuk worden de resultaten van de uitvoering van de aspectscan Beveiliging en Privacy gerapporteerd en worden er aanbevelingen gedaan naar de Adviesgroep Architectuur van de Gemeente Amsterdam op basis van de norm die in de aspectscan is vastgelegd.

9.1 Resultaten van de Voorbereidende Aspectscan

In de voorbereidende aspectscan worden eerst de negen vereiste elementen met evaluatiecriteria getoetst op aanwezigheid en compleetheid. Van deze negen mogen er geen als *Afwezig* of *Incompleet* worden geconcludeerd. Indien er wel evaluatiecriteria zijn die deze conclusie hebben, worden de gewenste elementen niet meer geëvalueerd en zal dit tot een bindend *no-go*-advies leiden met betrekking tot het uitvoeren van de specifieke aspectscan.

Alleen indien alle vereiste elementen *Aanwezig* zijn komen de vier gewenste elementen aan bod. Wanneer er van deze vier elementen één of meerdere *Afwezig* of *Incompleet* zijn heeft dit geen gevolgen voor het advies. Wel hebben deze gewenste elementen een toegevoegde waarde die in de bijbehorende evaluatiecriteria aangetoond wordt. Het is dan ook in het algemeen aan te raden dat wanneer een organisatie de vereiste elementen op orde heeft, ze aandacht besteed aan het eventueel uitwerken van de gewenste elementen om de kwaliteit van de architectuurdocumentatie te verhogen.

De conclusies van de negen vereiste en vier gewenste elementen zijn in tabel 9.1 op pagina 56 in het Rapport Voorbereidende Aspectscan samengevoegd.

Uit het rapport blijkt dat vijf van de negen vereiste elementen *Afwezig* zijn. Daarnaastzijn twee van de negen vereiste elementen *Incompleet*. Alleen de elementen 1. (Beveiligingsaspect) en 5. (Beveiligingsprincipes) zijn aanwezig, met als gevolg dat volgens de hierboven beschreven regels het advies voor het uitvoeren van de specifieke aspectscan duidelijk negatief is.

Als de regels van de aspectscan strikt gevolgd worden stopt de hele evaluatie hier. Zoals aangegeven in paragraaf 7.2 wordt er in deze casus een uitzondering op deze regel gemaakt en werd de gehele voorbereidende scan uitgevoerd. Hierna blijkt dat ook de vier gewenste elementen allemaal *Afwezig* zijn.

Rapport Voorbereidende Aspectscan voor Beveiliging en Privacy Handboek Architectuur Amsterdam	
Vereiste Elementen	
1. Beveiligingsaspect	**Aanwezig**
2. Stakeholders	*Afwezig*
3. Concerns	*Afwezig*
4. Risico's	*Afwezig*
5. Beveiligingsprincipes	**Aanwezig**
6. Uitgangssituatie Beveiliging	*Afwezig*
7. Bedrijfsmiddelenclassificatie	Incompleet
8. Beveiligingsmaatregelen	Incompleet
9. Rollen en Verantwoordelijkheden	*Afwezig*
Gewenste Elementen	
10. Gedragslijnen	*Afwezig*
11. Procedures	*Afwezig*
12. Beveiligingsdienstenmodel	*Afwezig*
13. Beveiligingsprocesmodel	*Afwezig*
	Advies: **No-Go**

Tabel 9.1: Rapport Voorbereidende Aspectscan voor Beveiliging en Privacy.

9.1.1 Metingen, Conclusies en Aanbevelingen

De uitvoering van de geëvalueerde elementen uit de voorbereidende scan is op de volgende pagina's beschreven volgens het template uit tabel 4.15 op pagina 29. In deze tabellen wordt voor alle elementen de meting en de locatie van de meting in de architectuurdocumentatie vastgelegd, evenals de getrokken conclusie en eventuele aanbevelingen voor verbetering of uitbreiding van de beschrijving van het element.

Om verwarring te voorkomen worden verwijzingen naar pagina's, tabellen en hoofdstukken in het Handboek Architectuur anders weergegeven dan de verwijzingen naar delen van deze scriptie. Bijvoorbeeld PAGINA 3-1 in het Handboek Architectuur en pagina 42 in de scriptie.

1. Beveiligingsaspect	Vereist
Meting en Locatie:	Op PAGINA 2-5 wordt het Amsterdamse architectuurraamwerk weergegeven in TABEL 2-1. Het aspect Beveiliging en Privacy is vertegenwoordigd als doordringend integraal aspect op alle lagen van het architectuurraamwerk.
Conclusie en Rationale:	De beste van de drie vertegenwoordigingsvormen wordt gebruikt, dus is de conclusie: **Aanwezig**.
Aanbevelingen:	Geen, dit element is in orde.

Tabel 9.2: Uitvoering evaluatiecriterium 1: Beveiligingsaspect.

2. Stakeholders	Vereist
Meting en Locatie:	Er is geen expliciet overzicht of lijst van stakeholders die belang hebben bij beveiliging en privacy. Wel wordt er in GRONDSLAG 2.1 gesproken over 'burgers, bedrijven en overige belanghebbenden' maar is er nergens een expliciete vermelding van de wie relevante stakeholders zijn.
Conclusie en Rationale:	De stakeholders zijn niet expliciet beschreven, dus is de conclusie: **Afwezig**.
Aanbevelingen:	Voer een krachtenveld analyse uit en maak een overzicht van van de belangrijkste (groepen van) stakeholders en hun concerns op hoog niveau. Prioriteer de stakeholders en orden ze in beslissende, beïnvloedende en overige stakeholders.

Tabel 9.3: Uitvoering evaluatiecriterium 2: Stakeholders.

3. Concerns	Vereist
Meting en Locatie:	Er wordt geen expliciet overzicht gegeven van stakeholder concerns. Wel wordt er op PAGINA 6-3 aangegeven dat er 'rond het delen van persoonsgegevens extra aandacht nodig is voor privacybescherming' en op PAGINA 6-19 wordt de naleving van de Wet bescherming persoonsgegevens genoemd. Grondslag 0.2 geeft aan dat de Gemeente Amsterdam alle van toepassing zijnde wet- en regelgeving naleeft en in BIJLAGE 3 wordt er een opsomming gemaakt van een negental wetten nageleefd moeten worden. De visie wordt beschreven op PAGINA 1-1 maar er worden hieruit geen expliciete concerns geformuleerd.
Conclusie en Rationale:	Er zijn geen stakeholder concerns of concerns vanuit de visie. Er is een opsomming van de van toepassing zijnde wet- en regelgeving maar hieruit zijn geen expliciete concerns geformuleerd. De conclusie is dus: **Afwezig**.
Aanbevelingen:	Maak een duidelijk expliciet overzicht van de stakeholder concerns in combinatie met de aanbevelingen van evaluatiecriterium 2 in tabel 9.3. Leid concerns af uit de visie en de geldende wet- en regelgeving en beschrijf deze op een vindbare plaats in het begin van de architectuurdocumentatie. In het verdere document kan er dan naar deze concerns verwezen worden zodat de herleidbaarheid van principes en de verbijzondering daarvan mogelijk is.

Tabel 9.4: Uitvoering evaluatiecriterium 3: Concerns.

4. Risico's	Vereist
Meting en Locatie:	Er worden geen risico's gedefinieerd. In BIJLAGE 3 wordt in de uitgangspunten van de Gemeentelijke Informatiebeveiligingsnorm (GIBN, [2]) gesteld dat: 'Ieder organisatieonderdeel is op deze wijze verplicht expliciet een gemotiveerde uitspraak te doen over het gewenste beveiligingsniveau en zelf maatregelen te selecteren op basis van classificatie en risicoanalyse.'
Conclusie en Rationale:	Er is geen overzicht van risico's, dus is de conclusie: **Afwezig**.
Aanbevelingen:	Omdat Amsterdam een concern is van 14 stadsdelen, de centrale stad en ongeveer 46 diensten en bedrijven is het begrijpelijk dat er op concernniveau geen overzicht van alle specifieke risico's is opgenomen. Echter wordt er wel een infrastructuur beschreven die door al deze organisatieonderdelen gedeeld en gebruikt gaat worden. Mijn aanbeveling is dan ook om juist de risico's die samenhangen met deze gedeelde gemeenschappelijke infrastructuur op zowel strategisch, tactisch en operationeel niveau te definiëren in de architectuurdocumentatie als aanvulling op de losse invullingen per organisatieonderdeel.

Tabel 9.5: Uitvoering evaluatiecriterium 4: Risico's.

5. Beveiligingsprincipes	Vereist
Meting en Locatie:	Er zijn twee beveiligingsprincipes geformuleerd, GRONDSLAG 0.1 over privacy en GRONDSLAG 3.4 over informatiebeveiliging, op respectievelijk PAGINA 3-1 EN 3-2. Deze principes worden aangeduid als 'algemene grondslag' en als grondslag voor de informatielaag. Verder zijn er nog twee principes die raakvlakken hebben met het aspect, zijnde GRONDSLAG 0.2 over naleving van wet- en regelgeving waaronder de Wet bescherming persoonsgegevens en GRONDSLAG 3.2 over de inrichting van de informatiehuishouding.
Conclusie en Rationale:	Er zijn twee beveiligingsprincipes opgenomen, dus is de conclusie: **Aanwezig**.
Aanbevelingen:	Formuleer meer beveiligingsprincipes op elke laag van het architectuurraamwerk, zowel op strategisch, tactisch en operationeel niveau. Gebruik hiervoor eventueel de methode van Elsinga en Hofman [13] voor het selecteren van beveiligingsprincipes.

Tabel 9.6: Uitvoering evaluatiecriterium 5: Beveiligingsprincipes.

6. Uitgangssituatie Beveiliging	Vereist
Meting en Locatie:	Er is geen uitgangssituatie van de beveiliging beschreven in de architectuurdocumentatie. Dit is volgens de GIBN de taak van de losse organisatieonderdelen.
Conclusie en Rationale:	Er is geen uitgangssituatie opgenomen, dus is de conclusie: **Afwezig**.
Aanbevelingen:	Beschrijf de uitgangssituatie van de beveiliging van de bedrijfsmiddelen die door de organisatieonderdelen gedeeld worden. Dit zijn vooral bedrijfsmiddelen die deel uit maken van de gedeelde infrastructuur zoals de basisregistraties en kernadministraties.

Tabel 9.7: Uitvoering evaluatiecriterium 6: Uitgangssituatie Beveiliging.

7. Bedrijfsmiddelenclassificatie	Vereist
Meting en Locatie:	Er is geen bedrijfsmiddelenclassificatie opgenomen in de architectuurdocumentatie. Ook dit is volgens de GIBN de taak van de losse organisatieonderdelen. Wel is er in HOOFDSTUK 8 (de infrastructuurlaag) een gedetailleerde beschrijving van de E-Net infrastructuur opgenomen met een indeling in drie beveiligingsdomeinen met een classificatie in verschillende niveaus van beveiliging. Ook zijn er voor E-Net beschrijvingen van identificatie, authentificatie en authorisatie opgenomen maar niet van andere bedrijfsmiddelen dan die van E-Net.
Conclusie en Rationale:	Er is geen complete bedrijfsmiddelenclassificatie maar er is wel een aanzet tot een soortgelijke beschrijving voor de E-Net infrastructuur. De conclusie is daarom: **Incompleet**.
Aanbevelingen:	E-Net is de gedeelde infrastructuur van de Gemeente Amsterdam waarop alle organisatieonderdelen worden aangesloten. Het is aan te bevelen om een duidelijke expliciete classificatie van de bedrijfsmiddelen van E-Net op te stellen, maar ook van alle andere gedeelde bedrijfsmiddelen, en deze in de architectuurdocumentatie op te nemen.

Tabel 9.8: Uitvoering evaluatiecriterium 7: Bedrijfsmiddelenclassificatie.

8. Beveiligingsmaatregelen	Vereist
Meting en Locatie:	Er is geen expliciet overzicht van de beveiligingsmaatregelen. Ook dit is volgens de GIBN de taak van de losse organisatieonderdelen. Wel staan er her en der in de tekst wat maatregelen genoemd, maar niet volgens een vaste structuur.
Conclusie en Rationale:	Er is geen overzicht van beveiligingsmaatregelen met alle 3 groepen maatregelen, maar er zijn wel soms losse technische beveiligingsmaatregelen genoemd en enkele administratieve maatregelen. De conclusie is dus: **Incompleet**.
Aanbevelingen:	Orden alle beveiligingsmaatregelen in een helder gestructureerd overzicht.

Tabel 9.9: Uitvoering evaluatiecriterium 8: Beveiligingsmaatregelen.

9. Rollen en Verantwoordelijkheden	Vereist
Meting en Locatie:	Op PAGINA 2-7 wordt beschreven dat de eigenaren van de modellen en standaarden verantwoordelijk zijn voor het beheer daarvan. Dit is echter niet specifiek voor beveiliging en gaat vooral over functioneel beheer. Op PAGINA 4-32 staat in de tabel 'Relevante paragrafen GIBN' bij paragraaf 3.2 dat de toewijzing van de verantwoordelijkheid voor informatie gedefinieerd moet worden per organisatieonderdeel. In BIJLAGE 3 wordt deze stelling nogmaals herhaald.
Conclusie en Rationale:	Er worden geen rollen beschreven maar er zijn wel enkele uitingen over verantwoordelijkheid, maar er is geen duidelijk overzicht. Er is wel merkbaar aandacht voor het belang van toewijzing van verantwoordelijkheden, maar deze toewijzing wordt niet in de architectuurdocumentatie opgenomen. De conclusie is dus: **Afwezig**.
Aanbevelingen:	Definieer een aantal rollen voor de concern organisatie op abstract niveau en wijs verantwoordelijkheden toe. Voorbeelden van deze rollen zijn de Chief Information Security Officer (CISO) en de functioneel applicatiebeheerder. Neem dit als een duidelijk overzicht op in de architectuurdocumentatie.

Tabel 9.10: Uitvoering evaluatiecriterium 9: Rollen en Verantwoordelijkheden.

10. Gedragslijnen	Gewenst
Meting en Locatie:	Er worden geen gedragslijnen genoemd in de architectuurdocumentatie. Ook dit is volgens de GIBN de taak van de losse organisatieonderdelen.
Conclusie en Rationale:	Er zijn geen gedragslijnen opgenomen en er zijn geen verwijzingen naar gedragslijnen in andere documenten. De conclusie is dus : **Afwezig**.
Aanbevelingen:	Verwijs eventueel naar een aantal gedragslijnen die gelden voor de gemeenschappelijke gebieden tussen de losse organisatieonderdelen.

Tabel 9.11: Uitvoering evaluatiecriterium 10: Gedragslijnen.

11. Procedures	Gewenst
Meting en Locatie:	Er worden geen procedures genoemd in de architectuurdocumentatie. Ook dit is volgens de GIBN de taak van de losse organisatieonderdelen.
Conclusie en Rationale:	Er zijn geen procedures opgenomen en er zijn geen verwijzingen naar procedures in andere documenten. De conclusie is dus : **Afwezig**.
Aanbevelingen:	Verwijs eventueel naar een aantal procedures die gelden voor de gemeenschappelijke gebieden tussen de losse organisatieonderdelen.

Tabel 9.12: Uitvoering evaluatiecriterium 11: Procedures.

12. Beveiligingsdienstenmodel	Gewenst
Meting en Locatie:	Er wordt geen beveiligingsdienstenmodel genoemd in de architectuurdocumentatie. Tevens is er in de hoofdlijnen van de GIBN in BIJLAGE 3 geen sprake van het opstellen van een beveiligingsdienstenmodel.
Conclusie en Rationale:	Er is geen beveiligingsdienstenmodel opgenomen, dus de conclusie is: **Afwezig**.
Aanbevelingen:	Geen.

Tabel 9.13: Uitvoering evaluatiecriterium 12: Beveiligingsdienstenmodel.

13. Beveiligingsprocesmodel	Gewenst
Meting en Locatie:	Er wordt geen beveiligingsprocesmodel genoemd in de architectuurdocumentatie. Tevens is er in de hoofdlijnen van de GIBN in BIJLAGE 3 geen sprake van het opstellen van een beveiligingsprocesmodel.
Conclusie en Rationale:	Er is geen beveiligingsprocesmodel opgenomen, dus de conclusie is: **Afwezig**.
Aanbevelingen:	Geen.

Tabel 9.14: Uitvoering evaluatiecriterium 13: Beveiligingsprocesmodel.

9.2 Resultaten van de Specifieke Aspectscan

De specifieke aspectscan is niet uitgevoerd omdat uit het rapport van de voorbereidende aspectscan bleek dat 11 van de 13 vereiste en gewenste elementen afwezig of incompleet waren. Het heeft geen zin om een uitzondering te maken op de regel die stelt dat de specifieke aspectscan alleen bij een *go*-advies uitgevoerd mag worden, omdat de uitvoering dan niet representatief genoeg is zodat er iets gezegd kan worden over de bruikbaarheid van de specifieke aspectscan.

Het doel van de case study was het toetsen van de bruikbaarheid van de aspectscan Beveiliging en Privacy, maar vanwege de specifieke situatie van de Gemeente Amsterdam leent het Handboek Architectuur zich niet voor evaluatie met deze aspectscan. Evaluatie van het Handboek Architectuur door middel van andere aspectscans is waarschijnlijk goed mogelijk, zoals de aspectscan Adaptiviteit.

In de reflectie op de voorbereidende aspectscan in paragraaf 10.1 worden de redenen voor het niet uitvoeren van de specifieke aspectscan nogmaals toegelicht.

9.3 Aanbevelingen van de Voorbereidende Aspectscan

Hier volgt een overzicht van de aanbevelingen die tijdens de uitvoering van de voorbereidende aspectscan op het Handboek Architectuur aangedragen werden:

Stakeholders Voer een krachtenveld analyse uit en maak een overzicht van van de belangrijkste (groepen van) *stakeholders* en hun concerns op hoog niveau. Prioriteer de stakeholders en orden ze in beslissende, beïnvloedende en overige stakeholders.

Concerns Maak tevens een duidelijk expliciet overzicht van de *stakeholder concerns*. Leid concerns af uit de *visie* en de geldende *wet- en regelgeving* en beschrijf deze op een vindbare plaats in het begin van de architectuurdocumentatie. In het verdere document kan er dan naar deze concerns verwezen worden zodat de herleidbaarheid van principes naar concerns mogelijk is.

Risico's Definieer juist de *risico's* die samenhangen met deze gedeelde gemeenschappelijke infrastructuur op zowel strategisch, tactisch en operationeel niveau als aanvulling op de losse invullingen per organisatieonderdeel.

Beveiligingsprincipes Formuleer meer beveiligingsprincipes op elke laag van het architectuurraamwerk, zowel op strategisch, tactisch en operationeel niveau. Gebruik hiervoor eventueel de methode van Elsinga en Hofman [13] voor het selecteren van beveiligingsprincipes.

Baseline Beveiliging Maak een *baseline* voor de beveiliging van de bedrijfsmiddelen die door de organisatieonderdelen gedeeld worden. Dit zijn vooral bedrijfsmiddelen die deel uit maken van de gedeelde infrastructuur zoals de basisregistraties en kernadministraties.

Bedrijfsmiddelenclassificatie Stel een duidelijke expliciete *bedrijfsmiddelenclassificatie* op van E-Net, maar ook van alle andere gedeelde bedrijfsmiddelen, en neem deze op in de architectuurdocumentatie. Beperk dit niet tot alleen de infrastructuurlaag.

Beveiligingsmaatregelen Orden alle *beveiligingsmaatregelen* in een helder gestructureerd overzicht.

Rollen en Verantwoordelijkheden Definieer een aantal rollen voor de concern organisatie op abstract niveau en wijs verantwoordelijkheden toe. Neem dit als een duidelijk overzicht op in de architectuurdocumentatie.

Wat opvalt tijdens de evaluatie is dat op basis van de Gemeentelijke Informatiebeveiligingsnorm (GIBN) telkens de verantwoordelijkheid voor het uitwerken naar de losse organisatieonderdelen wordt overgedragen waarna de beveiliging als aspect grotendeels uit de architectuurdocumentatie verdwijnt.

Zoals al eerder is aangegeven kan dit verklaard worden door het feit dat de Gemeente Amsterdam zo'n grote organisatie is die uit 14 stadsdelen, de centrale stad en ongeveer 46 diensten en bedrijven bestaat. Dit neemt echter niet weg dat juist architectuur een middel is om samenhang tussen deze organisatieonderdelen te realiseren. Deze samenhang komt voor een groot deel tot uiting in de samenwerking van de verschillende organisatieonderdelen.

Technisch gezien is E-Net de gedeelde infrastructuur die deze samenwerking moet gaan ondersteunen. Maar ook op organisatorisch en administratief is er sturing nodig op het gebied van informatiebeveiliging. De belangrijkste aanbeveling voor de Gemeente Amsterdam is dan ook:

> Richt de beveiligingsarchitectuur voor de Gemeente Amsterdam juist op de overkoepelende gemeenschappelijke gebieden waarin alle organisatieonderdelen samenwerken op strategisch, tactisch en operationeel niveau.

Naast de elementen die in deze aspectscan geëvalueerd worden is er nog één algemeen aandachtspunt dat van belang is voor de Gemeente Amsterdam. Dat is het punt dat het erg lastig is om zaken te vinden in het Handboek Architectuur. Nu is dit pas de eerste versie van een document waar nog veel aan geschaafd kan worden, maar de informatie die erin staat zou beter tot zijn recht komen als het wat vindbaarder zou zijn. Er wordt dan ook aanbevolen om meer overzichten, opsommingen en structuren te gebruiken ter verduidelijking van de vele verschillende stukken tekst.

IV

Reflectie

10

Persoonlijke Reflectie

In dit hoofdstuk reflecteer ik op de in deze scriptie ontwikkelde aspectscan en de uitvoering daarvan op het Handboek Architectuur van de Gemeente Amsterdam. Hierna volgt een persoonlijke reflectie op de Architectuurdocumentatie Evaluatiemethode (ADEM) welke het resultaat was van het onderzoek van een groep van zes afstudeerders.

10.1 Reflectie op de Aspectscan

10.1.1 Eisen voor de Aspectscan

In de ADEM zijn er zes eisen opgesteld waar elke aspectscan aan moet voldoen om aansluiting op de methode te kunnen garanderen. Deze eisen zijn in paragraaf 3.1 op pagina 15 gedefinieerd. In deze paragraaf wordt verantwoord dat de aspectscan aan al deze eisen voldoet.

Regel 1. *Elke aspectscan moet betrekking hebben op een voor architectuur relevant aandachtsgebied.*
Het vakgebied Beveiliging en Privacy is voor architectuur relevant omdat het ook nu nog vaak gezien wordt als een puur technische zaak, niet als een verantwoordelijkheid voor het management waarvoor op hoog niveau zowel administratieve als technische maatregelen moeten worden genomen om de risico's te kunnen beheersen.

Door het definieren van de rationaliseringsketen voor beveiliging en privacy in paragraaf 3.3 is inzichtelijk gemaakt hoe beveiliging en architectuur samenhangen.

Regel 2. *Elke aspectscan moet zijn doel en relevantie (bestaansrecht) beschrijven en verantwoorden.*
De doelen van de voorbereidende en specifieke aspectscans evenals de relevantie worden beschreven in hoofdstuk 3.

Regel 3. *Elke aspectscan moet een voorbereidende aspectscan bevatten.*
De aspectscan Beveiliging en Privacy bevat een voorbereidende aspectscan die is gedefinieerd in hoofdstuk 4 op pagina 19.

Regel 4. *Elke aspectscan moet een deugdelijke meetmethode en methode om tot een oordeel te komen bevatten.*

De meetmethode en methode om tot een oordeel te komen zijn beschreven in de paragrafen 4.3 en 5.4 voor respectievelijk de voorbereidende aspectscan en de specifieke aspectscan. Daarnaast is de meetmethode per evaluatiecriterium beschreven in de 28 tabellen in deze twee hoofdstukken.

Regel 5. *Elke aspectscan moet onafhankelijk uit te voeren zijn van andere aspectscans.*
De aspectscan Beveiliging en Privacy is onafhankelijk van andere aspectscans. De enige input is de architectuurdocumentatie, conform de regels van de ADEM.

Regel 6. *Elke aspectscan moet een bibliotheek met huidige best practises en standaarden met betrekking tot het aandachtsgebied van dit aspect bevatten, of een verwijzing naar een bestaande bibliotheek.*
Voor de aspectscan Beveiliging en Privacy is er in hoofdstuk 6 een eerste aanzet gemaakt tot een best practises bibliotheek. In de toekomst zal deze verder aangevuld en verfijnd worden.

10.1.2 Reflectie op de Uitvoering

Zoals in het rapport van de voorbereidende aspectscan in tabel 9.1 en in de tabellen 9.2 tot en met 9.14 bij de meting en aanbevelingen vaak naar voren komt, is het overgrote merendeel (85%) van de elementen afwezig of incompleet. Dit geeft een vertekend beeld van de kwaliteit van de beveiliging en privacy in de Gemeente Amsterdam.

De reden dat in de voorbereidende aspectscan zoveel elementen afwezig zijn is niet dat de Gemeente Amsterdam haar beveiliging niet op orde zou hebben. In tegendeel, informatiebeveiliging wordt juist serieus en professioneel aangepakt binnen de gemeente. Dit valse beeld komt voornamelijk doordat de gemeente heeft besloten de informatiebeveiliging losstaand van de architectuurdocumentatie in de Gemeentelijke Informatiebeveiligingsnorm (GIBN, [2]) te documenteren:

De GIBN is een norm die is vastgesteld om informatiebeveiliging gemeentebreed te kunnen garanderen en bestaat uit minimum betrouwbaarheidseisen. Deze hebben betrekking op onder andere:

- ◇ Beveiligingsbeleid;
- ◇ De organisatie rondom informatiebeveiliging;
- ◇ Personeelsbeleid;
- ◇ Logische en fysieke toegangsbeveiliging;
- ◇ Continuïteitsmanagement.

Het is de bedoeling dat de GIBN-maatregelen zo snel mogelijk door alle gemeentelijke diensten, bedrijven en stadsdelen worden toegepast. Het jaar 2002 gold als overgangsjaar, in 2003 moesten alle gemeentelijke onderdelen aan de nieuwe norm voldoen. Met de norm is één duidelijke richtlijn gekomen voor informatiebeveiliging waar alle diensten en stadsdelen aan moeten voldoen. Bron: Website Amsterdam[1]

Op 5 april 2005 is er een vernieuwde versie 2.0 van de GIBN uitgegeven. Voor deze nieuwe herziene versie werd gebruik gemaakt van de internationale standaard voor informatiebeveiliging NEN-ISO/IEC 17799:2002, later vervangen door [1]. Toen in augustus 2006 de eerste

[1] Website: http://www.ict.amsterdam.nl/live/index.jsp?nav=213&loc=492&det=40493

versie van het Handboek Architectuur publiekelijk werd gemaakt bestond de GIBN al vijf jaar.

De Gemeente Amsterdam is een concern van 14 stadsdelen, de centrale stad en ongeveer 46 diensten en bedrijven. De keuze om informatiebeveiliging per organisatieonderdeel te implementeren is begrijpelijk. Om deze reden is het ook begrijpelijk dat er geen specifieke beveiligingsmaatregelen, bedrijfsmiddelenclassificatie, risicoanalyse en dergelijke elementen zijn opgenomen in de architectuurdocumentatie.

Omdat de case study het Handboek Architectuur als onderzoeksobject gebruikt is en er volgens de ADEM geen informatie die buiten de architectuurdocumentatie valt mag worden meegenomen in de evaluatie, scoort het handboek bijzonder slecht in de voorbereidende aspectscan van het aspect Beveiliging en Privacy.

De specifieke aspectscan heb ik helaas niet kunnen uitvoeren op de casus van de Gemeente Amsterdam omdat bijna alle te evalueren elementen afwezig waren in de architectuurdocumentatie. Om deze reden kan ik ook niet reflecteren op de uitvoering van de specifieke aspectscan.

Hieruit kan worden geconcludeerd dat het Handboek Architectuur geen goede keuze is geweest voor het toetsen van de aspectscan in deze casus. Voor de aspectscan Beveiliging en Privacy is het Handboek Architectuur niet representatief genoeg voor een architectuurdocumentatie waarin beveiliging een aspect is. Het was beter geweest om de architectuurdocumentatie van een kleinere organisatie te nemen om de aspectscan te kunnen uitvoeren. Ik wil dan ook aanraden om de aspectscan te toetsen op de architectuur voor een organisatie die wel zelf verantwoordelijk is voor haar inrichting van de beveiliging, zoals bijvoorbeeld de Belastingsdienst, Rijkswaterstaat, de Informatie Beheer Groep of een grote bank.

10.1.3 Reflectie op de Aspectscan

Het was bijzonder moeilijk om een duidelijke lijn te trekken tussen elementen van het aspect Beveiliging en Privacy die enerzijds thuishoren in de architectuurdocumentatie en anderzijds aanwezig zijn in losse beveiligingsbeleidstukken, strategische IT-plannen en dergelijke. Dit heeft te maken met de verbondenheid van de elementen; wanneer je één van de elementen vereist in de architectuurdocumentatie volgen er direct een aantal andere elementen die nauw verbonden zijn met elkaar.

Tijdens het literatuuronderzoek heb ik vele boeken gelezen over beveiliging en privacy, maar praktisch alle boeken gaan over de implementatie van beveiliging op basis van internationale normen en standaarden zoals ISO 17799:2005 en de Code voor Informatiebeveiliging [4]. Security werd overal gezien als een enorme checklist die je kunt aflopen waarna je veilig zou zijn en de architectuurbenadering kwam nergens aan de orde. Sterker nog, op bijna alle plaatsen waar over Security Architecture gesproken werd betrof het eigenlijk engineering. Een voorbeeld hiervan is de Common Data Security Architecture (CDSA) van de OpenGroup, wat een cryptografisch raamwerk is voor het ontwikkelen van software. Daarnaast is er het boek *Designing Security Architecture Solutions* door Jay Ramachandran, waarin beveiligingsarchitectuur beschreven wordt als een fase in het software ontwikkelproces.

Slechts twee bronnen benaderden beveiliging vanuit een daadwerkelijk architectuurperspectief. Dit waren EISA: *Enterprise Information Security Architecture* van Gartner en SABSA®: *Sher-*

wood Applied Business Security Architecture van Sherwood et al. Uit deze twee bronnen, maar ook internationale standaarden, interviews met security professionals en verschillende artikelen heb ik de evaluatiecriteria gedestilleerd op basis waarvan in de voorbereidende en specifieke aspectscans geëvalueerd kan worden.

Omdat de elementen die ik tijdens het literatuuronderzoek heb geïdentificeerd zo sterk samenhangen, werd het al snel een grote verzameling aan evaluatiecriteria. Omdat er voor de deelopdracht die in deze scriptie beschreven wordt niet de volledige 18 EC aan tijdsbesteding vrij zijn maar slechts ongeveer 30% daarvan, zijn er een aantal niet uitgewerkte evaluatiecriteria genoemd die in de specifieke aspectscan hadden moeten zitten. Deze zijn opgenomen in paragraaf 5.3 op pagina 42.

Tijdens het literatuuronderzoek en het ontwerpen van de aspectscan had ik vaak de neiging om de diepte in te gaan, omdat beveiliging mij sterk interesseert. Het nadeel hiervan is dat juist door die diepgang de focus op de architectuurdocumentatie iets naar de achtergrond verschuift. Deze afstudeeropdracht is in essentie een opdracht op het vakgebied van architectuur, niet van beveiliging. Door tijdig bij te sturen is deze diepgang dan ook tot een niveau beperkt gebleven waarop het goed past bij het evalueren van architectuurdocumentatie.

Wat betreft de voorbereidende aspectscan ben ik tevreden over de te evalueren elementen. Ik ben van mening dat deze elementen samen de basis leggen voor een gedegen beschrijving van het aspect Beveiliging en Privacy in architectuurdocumentatie. Het blijkt daarentegen wel moeilijk te zijn om aandacht voor een bepaald aspect ook daadwerkelijk goed meetbaar te maken.

Er bestaan verschillende raamwerken voor het opstellen van een beveiligingsarchitectuur die soms in detail aangeven wat er exact allemaal ontwikkeld moet worden. Dit zijn bijvoorbeeld het EISA raamwerk van Gartner en SABSA® van Sherwood et al. Ik heb er echter voor gekozen om de aspectscan onafhankelijk te houden. In plaats van gewoon één raamwerk of methode te kiezen en die te volgen heb ik geprobeerd het beste uit beide raamwerken te combineren en aan te vullen met theorieën en ideeën van experts uit het vakgebied.

Voor de dertien verschillende evaluatiecriteria uit de voorbereidende aspectscan is de beschrijving in het onderdeel 'Hoe te meten?' vaak hetzelfde. Zo begint dit onderdeel tekens met 'Lees de architectuurdocumentatie door en zoek naar…' gevolgd door de naam van het desbetreffende element. Dit veronderstelt dat de evaluator in staat is om zelf deze elementen te herkennen in de architectuurdocumentatie. Enerzijds is het mogelijk om de elementen meer uitgebreid en expliciet te beschrijven waardoor ze makkelijker te herkennen zijn, maar anderzijds wil je generiek blijven en niet vastzitten aan bijvoorbeeld één bepaalde representatievorm van een specifiek raamwerk.

Naast de toetsing op aanwezigheid en compleetheid in de voorbereidende aspectscan wordt er door middel van vijftien evaluatiecriteria uit de specifieke aspectscan een inhoudelijke evaluatie uitgevoerd. Toch zou ik naast deze vijftien en de verschillende niet uitgewerkte criteria uit paragraaf 5.3 nog een aantal evaluatiecriteria willen definieren die meer de samenhang tussen het aspect Beveiliging en Privacy en andere aspecten onder de loep nemen. Zo is het interessant om te kunnen evalueren of er voldoende aandacht is geweest voor de Menselijke Maat bij de keuze voor de genomen beveiligingsmaatregelen.

Tijdens de terugkoppeling van de resultaten van de uitvoering van de globale fase op het Handboek Architectuur van de Gemeente Amsterdam kwam naar voren dat er een verschil

van mening is tussen de auteurs van het handboek en de afstudeerders. Als afstudeerders en ontwerpers van de ADEM streven we naar het expliciet maken van de verschillende elementen van de architectuurdocumentatie terwijl de Gemeente Amsterdam er bewust ervoor kiest om veel elementen impliciet te houden. Zoals Andre van der Valk (Hoofd Informatiebeleid Directie Concern Organisatie Amsterdam) tijdens de terugkoppeling zei: "Bedenk dat we eigenlijk de architectuur van 15 verschillende gemeenten en zo'n 40 tal gemeentelijke dienst-takken beschrijven. Zouden we dit voor een partij hebben moeten doen, dan zou het handboek wellicht veel concreter en dunner zijn".

Het is bijzonder moeilijk om een verzameling van elementen te identificeren die verplicht opgenomen moeten worden in de architectuurdocumentatie van alle organisaties, zowel groot als klein. Dit is een moeilijke opdracht voor architectuurdocumentatie in het algemeen, maar voor de evaluatie van het aspect Beveiliging en Privacy in het bijzonder. Architecturen zijn maatwerk voor een organisatie maar hebben toch een aantal gemeenschappelijke karakteristieken. Het zijn juist deze gemeenschappelijke elementen van het aspect Beveiliging en Privacy die geëvalueerd moeten worden.

10.2 Reflectie op de ADEM

In deze paragraaf wordt gereflecteerd op de ADEM in het algemeen. De ADEM is het product van het eerste deelproject, uitgevoerd door zes afstudeerders.

10.2.1 De Globale Fase

Wat betreft de ADEM in het algemeen is er een zeer uitgebreide reflectie geschreven door Guido Chorus, Chris Nellen en mijzelf in de bijlage '*Evaluatie Handboek Architectuur Amsterdam: Uitvoering van de Globale Fase*' [8]. In dit document wordt een groot aantal kanttekeningen geplaatst bij met name de holistische scan.

In deze paragraaf van de scriptie zal ik die niet allemaal herhalen, maar een paar hoofdpunten kort toelichten. Wanneer u geïnteresseerd bent in een meer volledige en diepgaande reflectie op de ADEM nodig ik u uit om de bijlage te lezen.

De voorbereidende aspectscan werd op twee hoofdpunten nabeschouwd. Enerzijds was er de reflectie op de methode, anderzijds werd er gereflecteerd op de norm.

Bij het uitvoeren van de voorbereidende scan op de architectuurdocumentatie van de gemeente Amsterdam zijn er met betrekking tot de methode geen kritiekpunten gevonden. Wat betreft de norm waren er een aantal opmerkingen gemaakt over de volgorde van de elementen in de evaluatie en het concept van herleidbaarheid. De belangrijkste opmerking was dat bij sommige elementen de meting niet voldoende concreet is beschreven; de criteria zijn niet specifiek genoeg om altijd te kunnen bepalen of een element impliciet of expliciet aanwezig is.

Na het uitvoeren van de voorbereidende scan hadden de evaluators een goed gevoel over de kwaliteit van de architectuurdocumentatie maar in het rapport van de voorbereidende scan komt dit echter niet naar voren. Er zijn heel wat zaken incompleet of zelfs afwezig beoordeeld. Dit komt hoofdzakelijk door de insteek van de Gemeente Amsterdam om niet een uiteindelijke kant en klare architectuur op te leveren. Ze bevinden zich nog in een verkennende fase. De ADEM houdt geen rekening met het feit dat de architectuurdocumentatie een tussen-versie

kan zijn en evalueert deze telkens alsof het volledig en compleet is. Een architectuur is echter nooit helemaal af en kan door veranderingen in bijvoorbeeld strategie, technische mogelijkheden, concurrentiepositie en wetgeving aangepast moeten worden.

Bij de holistische scan werden heel wat meer kanttekeningen geplaatst. De holistische scan in de huidige vorm voldoet niet aan alle opgestelde eisen en bevat naast oppervlakkige fouten ook ernstige inhoudelijke fouten. De holistische scan vormt een belangrijk onderdeel van de ADEM, omdat deze de architectuurdocumentatie inhoudelijk evalueert zonder naar een specifiek aspect te kijken. De holistische scan zal danig moeten worden bijgesteld naar aanleiding van het inzicht dat wij verworven hebben door het gebruik van dit instrument op de architectuur van de gemeente Amsterdam.

Binnen de huidige holistische scan is het holistische karakter verkeerd opgevat en daardoor verkeerd geïmplementeerd. De kwaliteitsattributen bieden geen holistische kijk op de architectuurdocumentatie, maar hebben alleen betrekking op een dieper inhoudelijk niveau. Deze scan zou moeten gaan over de samenhang tussen de verschillende elementen in de architectuur, zonder te kijken naar de afzonderlijke elementen in diepgang. Om dit holistische gedeelte te evalueren zou de rationaliseringsketen in de architectuurdocumentatie moeten worden geëvalueerd.

De aanbevelingen voor het toekomstige werk met betrekking tot de ADEM zijn in het kort:

1. De rationaliseringsketen moet gezien worden als het belangrijkste uitgangspunt van de holistische scan. Er moeten duidelijke en uitvoerbare handvatten opgesteld worden om de correctheid van de gebruikte rationaliseringsketen te evalueren.
2. De architectuurprincipes moeten losstaand geëvalueerd worden, bijvoorbeeld zoals beschreven in (Buitenhuis, [6]).
3. De documentatie waarin de architectuur is beschreven dient te worden geëvalueerd aan de hand van kwaliteitsattributen. Er moeten daarvoor duidelijke en uitvoerbare handvatten gemaakt worden, en de toepasbaarheid van de kwaliteitsattributen moet worden bewezen.
4. Kwaliteitsattributen als middel lijken bruikbaar te zijn voor een diepgaande evaluatie met betrekking tot de beschreven architectuur in de architectuurdocumentatie, mits de toepasbaarheid wordt aangetoond en er duidelijk uitvoerbare handvatten worden gegeven.

10.2.2 Toegevoegde Waarde van de ADEM

Ik heb mijn twijfels bij de toegevoegde waarde van het evalueren van de architectuurdocumentatie terwijl er juist veel vraag is naar wetenschappelijke evaluatiemethode voor het architectuurontwikkelproces. Bijna iedereen die we op het LAC 2006 hebben gesproken vond het opmerkelijk dat we niet naar het proces keken maar juist naar de documentatie. Ook Ben Elsinga en Aaldert Hofman van Capgemini lieten doorschemeren dat ze hun twijfels hebben bij het nut van de methode en ook Andre van der Valk en Menno Gmelig Meijling van de Gemeente Amsterdam zagen niet echt een toegevoegde waarde in de methode. Maar aan de andere kant wordt er wel een NK ICT Architectuur georganiseerd waarbij verschillende architectuurbeschrijvingen geëvalueerd worden.

De consensus lijkt te zijn dat het evalueren van de architectuurdocumentatie van onderge-

schikt belang is ten opzichte van het architectuurontwikkelproces. Toch hebben we met de ADEM een nuttige bijdrage geleverd aan het architectuurgedachtengoed. Naar mate de methode meer volwassen wordt zal de toegevoegde waarde stijgen.

Ik ben van mening dat we door de vereiste en gewenste elementen in architectuurdocumentatie te identificeren een goede basis hebben gelegd. Deze elementen kunnen gebruikt worden in een evaluatie zoals in de ADEM, maar door ze anders op te schrijven kan er een raamwerk opgezet worden dat als leidraad gebruikt kan worden voor het opstellen van een complete en kwalitatief goede architectuurdocumentatie. Daarnaast ben ik van mening dat een goede architectuurdocumentatie zeker bijdraagt aan de kwaliteit van de architectuur. Een begrijpelijk en inhoudelijk document helpt het draagvlak te vergroten binnen de organisatie en minimaliseert de kans op verkeerde interpretaties die leiden tot mogelijk foute implementaties.

Naast het evalueren van architectuurdocumentatie is een gedegen evaluatie op het totstandkomingsproces ook erg belangrijk. Zo kan er tijdens het proces bijgestuurd worden in tegenstelling tot achteraf constateren dat er een aantal zaken nog de nodige aandacht verdienen. De beste aanpak is het goed managen van het architectuurontwikkelproces en het periodiek uitvoeren van de globale fase van de ADEM om te zien of de ontwikkeling nog op het juiste spoor zit. Een daadwerkelijke

11

Conclusies en Aanbevelingen

In deze scriptie werd de aspectscan Beveiliging en Privacy gepresenteerd. De eerste deel scan, de voorbereidende aspectscan, werd uitgevoerd op het Handboek Architectuur van de Gemeente Amsterdam om zodoende in de praktijk te kunnen toetsen of deze uitvoerbaar is.

Doordat 85% van de te evalueren elementen afwezig of incompleet was in de voorbereidende aspectscan is het niet mogelijk geweest om de specifieke aspectscan uit te voeren. Dit moet nog een keer gebeuren op de architectuurdocumentatie van een onderneming die beveiliging als aspect meer uitgebreid in de architectuurdocumentatie beschrijft. Daarnaast is het aan te bevelen om ook de aspectscan in zijn geheel nogmaals op een aantal andere architecturen toe te passen; één uitvoering is erg weinig om een goed beeld te krijgen van de bruikbaarheid van de aspectscan.

Daarnaast is er gereflecteerd op de uitvoering van deze case study en op de aspectscan in het algemeen in deel IV van deze scriptie. De voorbereidende aspectscan blijkt goed bruikbaar te zijn, ondanks de resultaten voor het Handboek Architectuur van de Gemeente Amsterdam. Deze resultaten gaven een vals beeld van de kwaliteit van de architectuurdocumentatie met betrekking tot het aspect Beveiliging en Privacy. Dit kwam niet door de aspectscan zelf maar doordat de gemeente heeft besloten de informatiebeveiliging losstaand van de architectuurdocumentatie in de Gemeentelijke Informatiebeveiligingsnorm (GIBN, [2]) te documenteren waardoor het aspect grotendeels uit de architectuurdocumentatie verdwijnt.

Hoewel ik tevreden ben met de in een relatief korte tijd opgeleverde aspectscan wil ik nog een tweetal aanbevelingen maken naast het verbeteren, bijschaven en uitbreiden van de aspectscan: Allereerst zou er een aspectscan moeten worden ontwikkeld die Menselijke Maat en Beveiliging en Privacy in samenhang evalueert. Chris Nellen ontwikkelt op dit moment een aspectscan voor het aspect Menselijke Maat in architectuurdocumentatie en Bart Jacobs heeft een boek geschreven 'Menselijke Maat in de ICT' (Jacobs, [16]) waarin hij een aantal belangrijke privacy concerns over de elektronische overheid aanstipt.

Ten tweede is het aan te bevelen om meer onderzoek te verrichten naar het opstellen van een raamwerk voor het eenduidig vastleggen van het beveiligingsbeleid op strategisch niveau in architectuurdocumentatie. De nadruk ligt nog steeds te sterk op naleving van internationale normen die op basis van een checklist van meer dan 700 vragen [4] de implementatie van de beveiliging controleert. De raamwerken SABSA®en EISA kunnen hiervoor als eerste uitgangspunt dienen.

11.0.3 Onderzoeksdoel en Onderzoeksvragen

Het onderzoeksdoel was in hoofdstuk 2 op pagina 2 gedefinieerd als:

> Een invulling geven aan het aspect Beveiliging en Privacy in de vorm van een aspectscan ten behoeve van de Architectuurdocumentatie Evaluatiemethode en deze toetsen met de casus van het Handboek Architectuur van de Gemeente Amsterdam.

Dit doel is in deze scriptie bereikt. De hoofdstukken 3, 4, 5 en 6 in deel II van deze scriptie beschrijven de aspectscan Beveiliging en Privacy die invulling geeft aan het genoemde aspect.

De uitvoering van de aspectscan als toetsing in de vorm van een case study is gedeeltelijk gelukt. De voorbereidende aspectscan kon goed worden uitgevoerd maar voor de uitvoering van de specifieke aspectscan was onmogelijk omdat 85% van de te evalueren elementen niet aanwezig was in de architectuurdocumentatie.

De vijf deelvragen die in paragraaf 2.3 geformuleerd werden worden in deze scriptie beantwoord. De verplichte, gewenste en optionele elementen worden in hoofdstuk 4.1 geïdentificeerd. De methoden voor het meten en het trekken van conclusies worden per evaluatiecriterium beschreven. In totaal zijn er 13 evaluatiecriteria voor de voorbereidende aspectscan en 15 evaluatiecriteria voor de specifieke aspectscan gedefinieerd.

Bibliografie

[1] ISO/IEC 17799:2005. *Information Technology-Security Techniques-Code of Practice for Information Security Management*. International Standards Organization, Geneva, 2005.

[2] Gemeente Amsterdam. *Gemeentelijke Informatiebeveiligingsnorm (GIBN) 2005*. College van Burgemeester en Wethouders, Directie Concernorganisatie en Bestuursdienst, 5 April 2005. Versie 2.0 - Nr. DCO2005/3195.

[3] Adviesgroep Architectuur. *Handboek Architectuur: De samenhang in de organisatie en informatievoorziening van de gemeente Amsterdam*. Amsterdam, 23 Augustus 2006. Versie 0.1.

[4] Joop Bautz, Jan Boogers, Sjaak Boone, Marja van der Burg, Walter van de Garde, Ben Verbeek, and Kees van der Zwan. *Checklist Informatiebeveiliging*. tenHagenStam, 2000. ISBN 90-267-2912-X.

[5] Lucien Bongers. *Security binnen Enterprise Architectuur*. Master's thesis, Radboud Universiteit Nijmegen, Nederland, Februari 2006.

[6] Pieter Buitenhuis. *Fundamenten van het principe: Op weg naar een prescriptieve architectuurmodelleertaal*. Master's thesis, Radboud Universiteit Nijmegen, Nederland, Maart 2007.

[7] G.J.N.M. (Guido) Chorus. *Adaptiviteit in Architectuur: Aanzet tot een evaluatiemethode en resultaten van een evaluatie*. Master's thesis, Radboud Universiteit Nijmegen, Nederland, Juni 2007.

[8] G.J.N.M. (Guido) Chorus, Y.H.C. (Yves) Janse, and C.J.P. (Chris) Nellen. *Evaluatie Handboek Architectuur Amsterdam: Uitvoering van de Globale Fase*. Radboud Universiteit Nijmegen, Nederland, April 2007.

[9] G.J.N.M. (Guido) Chorus, Y.H.C. (Yves) Janse, C.J.P. (Chris) Nellen, D.S (David) Campbell, P.J. (Paul) van Vlaanderen, and R.P. (Robin) van 't Wout. *Architectuurdocumentatie Evaluatie: Aanzet tot een methode om architectuurdocumentatie te evalueren*. Radboud Universiteit Nijmegen, Nederland, April 2007.

[10] Bill Conner, Tom Noonan, and Robert W. Holleyman, II. *Information Security Governance: Toward a Framework for Action*. *Business Software Alliance*, 2004.

[11] Information Security Forum. *The Standard of Good Practice for Information Security*. Southwark Towers, 32 London Bridge Street, London, SE1 9SY, United Kingdom., January 2005. Version 4.1.

[12] GvIB. *Functies in de informatiebeveiliging: een visiedocument*. Genootschap van Informatie Beveiligers en het Platform Informatiebeveiliging, 2006. ISBN: 90-78786-01-9.

[13] Aaldert Hofman and Ben Elsinga. *Security Principles*. *Technology Services, Capgemini Nederland B.V.*, 2003.

[14] IEEE Std 1471-2000. *IEEE Recommended Practise for Architectural Description of Software-Intensive Systems*. IEEE Computer Society, 2000.

[15] Information Systems Security Association. *Generally Accepted Information Security Principles*. Version 3.0, Augustus 2003.

[16] Bart Jacobs. *De Menselijke Maat in ICT*. Januari 2007. ISBN: 978-90-9021619-5; Creative Commons, Naamsvermelding-NietCommercieel-GeenAfgeleideWerken.

[17] Gregg Kreizman and Bruce Robertson. *Integrating Security into the Enterprise Architecture Framework*. Published 25 January 2006. Gartner Research, ID Number: G00137069.

[18] Nederlandse Overheid. *Wet bescherming persoonsgegevens*. 's-Gravenhage, 6 juli 2000.

[19] C.J.P. (Chris) Nellen. *Architectuur en de belevingswereld: een aanzet tot het evalueren van menselijke maat in architectuur*. Master's thesis, Radboud Universiteit Nijmegen, Nederland, Juni 2007.

[20] Nederlandse Overheid. *Nederlandse Overheid Referentie Architectuur (NORA)*. Amsterdam, September 2006. Versie 0.1 - http://www.e-overheid.nl/atlas/referentiearchitectuur/.

[21] Thomas R. Peltier. *Information Security Policies and Procedures: A Practitioner's Reference, Second Edition*. Auerbach Publishers Inc., 2004. ISBN: 0-849-319-587.

[22] Daan Rijsenbrij. *Architectuur in de digitale wereld. Syllabus: Inleiding in de Digitale Architectuur.* 2005. http://www.digital-architecture.net/collegedictaat.htm.

[23] Mr. L.B. Sauerwein and Mr. J.J. Linnemann. *Wet bescherming persoonsgegevens: Handleiding voor verwerkers van persoonsgegevens*. April 2002. Ministerie van Justitie, Den Haag, Nederland.

[24] Bruce Schneier. *Beyond Fear - Thinking Sensibly about Security in an Uncertain World*. Copernicus Books, 37 East 7th Street, New York, NY 10003, 2003. ISBN 0-387-02620-7.

[25] Bruce Schneier. *Secrets & Lies - Digital Security in a Networked World*. Wiley Computer Publishing, 10475 Crosspoint Blvd, Indianapolis, IN 46256, 2004. ISBN 0-471-45380-3.

[26] Tom Scholtz. *Structure and Content of an Enterprise Information Security Architecture*. Published 23 January 2006. Gartner Research, ID Number: G00136867.

[27] Security Watch. Identifying and classifying assets. *Network Magazine India*, September 2002.

[28] John Sherwood, Andrew Clark, and David Lynas. *Enterprise Security Architecture: A Business-Driven Approach*. CMP Books, Computer Security Institute, San Francisco, 2005. ISBN 1-57820-318-X.

[29] Jan Killmeyer Tudor. *Information Security Architecture*. Auerbach Publishers Inc., 2006. ISBN 0-8493-1549-2.

[30] R.D. van Bruggen, H.A.A. van Dun, and E. de Lange. *Juridische Aspecten van de Informatievoorziening*. Academic Service, 2003. ISBN: 90-395-1887-4.

[31] Huaiqing Wang, Matthew K. O. Lee, and Chen Wang. *Consumer privacy concerns about Internet marketing*. *Commun. ACM*, 41(3):63–70, 1998.

V

Bijlagen

Bijlage A:

Architectuurdocumentatie Evaluatie

Aanzet tot een methode om architectuurdocumentatie te evalueren

TE VERKRIJGEN VIA:
http://www.digital-architecture.net/scripties.htm

Auteurs:	ing. D.S. (David) Campbell ing. Y.H.C. (Yves) Janse P.J. (Paul) van Vlaanderen, BICT	ing. G.J.N.M. (Guido) Chorus ing. C.J.P. (Chris) Nellen ing. R.P. (Robin) van 't Wout
Plaats:	Nijmegen	
Datum:	15-06-2007	
Versie:	1.5	
Status:	Uiteindelijke versie.	
Begeleider:	prof. dr. D.D.B. (Daan) Rijsenbrij	
Referent:	prof. dr. H.A. (Erik) Proper	

Bijlage B:

Evaluatie Handboek Architectuur Amsterdam

Uitvoering van de Globale Fase

TE VERKRIJGEN VIA:
http://www.digital-architecture.net/scripties.htm

Auteurs:	ing. G.J.N.M. (Guido) Chorus ing. Y.H.C. (Yves) Janse ing. C.J.P. (Chris) Nellen
Plaats:	Nijmegen
Datum:	18-06-2007
Versie:	1.0
Status:	Definitieve versie
Begeleider:	prof. dr. D.B.B. (Daan) Rijsenbrij
Referent:	prof. dr. H.A. (Erik) Proper