Architectuurdocumentatie Evaluatie

Security & Privacy

Aanzet tot een methode om architectuurdocumentatie te evalueren

Auteur: P.J. van Vlaanderen, B ICT

Plaats: Nijmegen
Datum: 06-07-2007

Versie: 1.1
Status: Definitieve versie

Begeleider: prof. dr. Daan Rijsenbrij
Referent: prof. dr. Erik Proper

Voorwoord

Voor u ligt het resultaat van een onderzoek uitgevoerd door Paul van Vlaanderen, student informatiekunde aan de Radboud Universiteit te Nijmegen. Het betreft een onderzoek welke als bijdrage dient aan een breder onderzoek naar de evaluatie van architecturen. Dit onderzoek heeft als resultaat de ADEM (ArchitectuurDocumentatie EvaluatieMethode[1]) opgeleverd. In dit voorwoord wil ik graag de personen bedanken die mij in de loop van het onderzoek bijgestaan hebben.

In de voorbereide fase van de ADEM hebben zes studenten van de Radboud Universiteit deelgenomen. Graag wil ik mijn medestudenten David Campbell, Guido Chorus, Yves Janse, Chris Nellen en Robin van 't Wout bedanken voor de prettige samenwerking en het mooie eindresultaat.

Om een beeld te krijgen van wat er van belang is als het gaat om architectuurevaluatie heb ik met mijn collega studenten interviews afgenomen met diverse experts op het gebied van architectuur en de evaluatie daarvan. De personen die hierbij betrokken waren vindt u in het voordwoord van de ADEM. Tijdens het ontwikkelen van de aspectscan security & privacy hebben diverse experts op dit vakgebied hun bijdrage geleverd. Ik wil in het bijzonder bedanken Wouter Teepe, Martijn Oostdijk, Bart Jacobs, Jurgen van der Vlught, Erno Duinhoven, Aaldert Hofman, Ben Elsinga, Ruben de Wolf en Alex de Jonge.

Als laatste wil ik mijn dankbaarheid uitspreken naar mijn begeleider prof. dr. Daan Rijsenbrij die met zijn kritische oplettende houding een positieve bijdrage aan de kwaliteit van dit werk heeft geleverd. Daarnaast heeft ook het inhoudelijke commentaar van referent prof. dr. Erik Proper er toe bijgedragen dat dit onderzoek goed verlopen is.

Paul van Vlaanderen

[1] Dit onderzoek is te vinden op www.digital-architecture.net/scripties

Inhoudsopgave

Inleiding

Dit document is het resultaat van een onderzoek binnen het vakgebied van de digitale architectuur met de nadruk op het aandachtsgebied security en privacy, zoals dit gedoceerd wordt aan de Radboud Universiteit te Nijmegen. Het totale onderzoek is door zes studenten uitgevoerd onder begeleiding van prof. dr. Daan Rijsenbrij en prof. dr. Erik Proper. Dit document beschrijft een concretisering van het eerder uitgevoerde werk.

Op individuele basis is deze aspectscan ontwikkeld en uitgevoerd naar voorbeeld van de structuur die in de ADEM is vastgelegd. Dit betekent dat er een norm is ontwikkeld om te bepalen welke elementen van belang zijn in architectuurdocumentatie binnen het vakgebied security & privacy. Deze norm is vastgelegd in een methode welke in dit document beschreven wordt. Ook wordt de in dit document voorgestelde methode getest door een bestaande architectuur te evalueren. Deze casus vindt u in Bijlage 1. Als architectuur is hier gekozen voor de Nederlandse Overheid Referentie Architectuur (NORA).

Om inzicht te krijgen in de persoonlijke visie van de auteur op architectuur en security & privacy is er voorafgaand aan het onderzoek een apart hoofdstuk toegevoegd.

Als eerste wordt een theoretisch kader geschetst waarbinnen het onderzoek plaats zal vinden. Aan de hand van dit kader wordt de relevantie van security & privacy in architectuurevaluatie aangetoond en wordt in het bijzonder verklaard hoe security een rol speelt in architectuurdocumentatie.

Vervolgens wordt het onderzoeksgebied afgebakend; wat wordt er precies geëvalueerd en wat is het precieze doel en de verwachte uitkomst van een evaluatie met deze aspectscan? In hoeverre zal de scan compleet zijn, is uitbreiding mogelijk en wat is de omvang van de evaluatie? Deze vragen zullen ondermeer in de scopebeschrijving beantwoord worden. In de ADEM zijn hier reeds enkele kaders voor gesteld, zie hoofdstuk 3 in de ADEM 'Richtlijnen voor de ADEM'.

Nadat het onderzoek is gepositioneerd en afgebakend binnen de theorie en de eisen die gesteld worden aan de evaluatiemethode helder zijn, kunnen de bevindingen worden gerapporteerd. Het raamwerk uit de ADEM (zie hoofdstuk 3.4 'Aspectfase' in de ADEM) zal worden gebruikt om ook de binnen security & privacy aanwezige elementen te kunnen onderscheiden. Naast het evalueren van aanwezigheid van deze elementen wordt ook beschreven hoe deze elementen ingevuld moeten worden binnen architectuurdocumentatie. Voor de invulling van deze elementen zijn indicatoren gegeven. Naast de indicatoren zal een evaluatie plaatsvinden op de inhoud van principes die van invloed kunnen zijn op de security en privacy van de architectuur. Deze principes worden gegroepeerd per security ele-

ment en zijn tevens geplaatst binnen het Enterpise Information Security Architecture raamwerk van Gartner [GART06a].

Het document wordt afgesloten met een reflectie over de bereikte resultaten. Hierbij gaat het ondermeer over toekomstig onderzoek, mogelijke verbeterpunten en een verantwoording over de haalbaarheid en validiteit van de methode.

Dit onderzoek staat volledig in verbinding met de ADEM en is ook niet los te zien van de ADEM. Een ieder die deze scriptie leest moet daarom eerst de ADEM hebben gelezen om de methodiek en de concepten die daar al geïntroduceerd zijn te kunnen begrijpen.

Zaken als doel, afbakening en verantwoording van deze scriptie zijn reeds behandeld in het voorafgaande onderzoek. Alleen waarneer er afwijkende zaken zijn worden deze genoemd in deze scriptie. De nadruk ligt op de scan en de uitvoering van deze scan. Een te grote contextbeschrijving zou hier afleiden van het werkelijke doel, het ontwikkelen van een aspectscan. Voor omliggende zaken en afbakening van het onderzoek wordt verwezen naar het scriptieonderzoek over de ADEM (zie hoofdstuk 2 in de ADEM 'Doel, afbakening en verantwoording'). Nieuwe bevindingen die zijn opgedaan om deze scan te kunnen ontwikkelen worden beschreven in de theoretische achtergrond en hoofdstuk 4 'Evaluatie van security & privacy binnen de architectuurwereld'.

Samenvatting

Deze scriptie bevat het individuele onderzoek uitgevoerd door Paul van Vlaanderen naar de evaluatie van security en privacy binnen architectuurdocumentatie. Dit onderzoek is onderdeel van de Architectuurdocumentatie Evaluatiemethode welke gezamenlijk met vijf medestudenten in opgezet(zie bijlage2). Deze scriptie bestaat uit acht hoofdstukken. De essentie van deze hoofdstukken wordt hier beschreven.

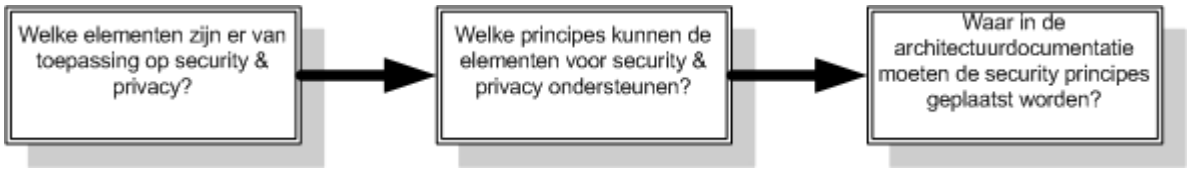
In hoofdstuk 1 worden de begrippen digitale architectuur en security & privacy uitgelegd zoals deze worden gezien door de auteur.

In hoofdstuk 2 wordt de theoretische achtergrond van dit onderzoek beschreven. Hierbij wordt vooral stilgestaan hoe security zich verenigt met architectuur. Security is veelal een apart hoofdstuk in architectuurdocumentatie en heeft weinig relatie met de rest van de architectuuraspecten. In dit onderzoek wordt uitgegaan van de ideale norm waarbij security & privacy een integraal onderdeel is van de architectuurdocumentatie. Hierbij past de opmerking van Aaldert Hofman, 'inbouwen in plaats van aanbouwen' wat betekent dat security een ingebouwd onderdeel moet zijn van de architectuur in plaats van een apart hoofdstuk voor specialisten[HOF04]. Verder wordt beschreven dat er op het gebied van security & privacy al diverse normen en best practises zijn en dat deze van toepassing zijn op dit onderzoek.

In hoofdstuk 3 worden doel, afbakening en verantwoording vastgelegd. De meeste van deze onderdelen zijn reeds beschreven in de ADEM en derhalve wordt hier minder aandacht aan besteed. Wat betreft security & privacy wordt beschreven waarom hier aandacht aan besteed moet worden in architectuurdocumentatie. Nieuwe ontwikkelingen in de markt zoals de hedendaagse netwerksamenleving maken het noodzakelijk dat security een essentieel onderdeel is van de bedrijfsvoering en derhalve ook geadresseerd moet worden in architectuurdocumentatie. Binnen architectuur zijn er diverse beschouwingniveaus te vinden. Op het hoogste niveau wordt de enterprise-architectuur beschreven. Dit onderzoek richt zich vooral op dit beschouwingniveau.

In hoofdstuk 4 wordt de evaluatie van security & privacy binnen de architectuurwereld besproken. Naar security & privacy is al veel onderzoek verricht. Er zijn veel normen waaraan organisaties zich kunnen conformeren. Voor privacy is zelfs wet en regelgeving geïntroduceerd. Organisaties kunnen zich laten toetsen aan deze normen en zich laten certificeren. Specifiek voor architectuurdocumentatie zijn er nog geen normen opgesteld.
Voor architectuur is wel onderzoek gedaan naar security principes. De uitkomsten van deze onderzoeken zijn meegenomen in dit onderzoek. Om security te kunnen integreren in de architectuurdocumentatie is de introductie van een raamwerk dat architectuur en security aan elkaar kan relateren noodzakelijk. Ten bate van de evaluatie van deze intergratie is er onderzoek gedaan naar diverse architectuurraamwerken.

In hoofdstuk 5 worden de resultaten van hoofdstuk 4 verwerkt tot een evaluatiemethode. De relaties tussen de onderwerpen uit hoofdstuk 4 worden beschreven. Binnen dit onderzoek zijn er drie belangrijke fasen onderkend. Deze fasen worden geïllustreerd in figuur 1.



Figuur 1: De belangrijkste fasen binnen het onderzoek naar de evaluatie van security & privacy

Fase 1 beschrijft de elementen die in de architectuurdocumentatie aanwezig moeten zijn. De elementen zijn gekozen op basis van huidige normen, best practises en NEN/ISO standaarden.

Fase 2 beschrijft de keuze voor security principes en hoe de aanwezigheid van principes gecontroleerd kan worden. Hierin is het van belang welke eisen er zijn aan principes. De eisen gelden niet alleen voor security principes maar ook voor andere architectuurprincipes. Voor de geïntroduceerde elementen zijn 50 principe-eisen gevormd die de elementen uit fase 1 moeten ondersteunen.

Fase 3 beschrijft de relatie tussen security & privacy met de rest van de architectuur. In deze fase wordt het EISA raamwerk van Gartner geïntroduceerd. Security is geen losstaande view op de architectuur zonder verdere relatie met de rest van de architectuur. Security moet een geheel vormen met alle andere aspecten die in architectuur belangrijk zijn en security moet verenigd zijn in het architectuurraamwerk. Wel heeft security zijn eigen modellen en requirements die vanuit een security viewpoint te bekijken zijn. Gartner zegt hier het volgende over in [Gart06a]

'An enterprise architecture (EA) framework should allow for security-related requirements and artifacts to be organized within primary EA viewpoints, but should also have these security elements abstracted to a security-only viewpoint. This allows different stakeholders to view these requirements and artifacts in ways that best help them do their jobs while ensuring that security requirements are built in to all aspects of solutions.'

In hoofdstuk 6 wordt de aspectscan beschreven. De aspectscan is het product van alle onderzochte onderdelen uit hoofdstuk 5. Als eerste worden 17 elementen geïntroduceerd. Per element wordt aangegeven wat het element inhoud, waarom het van belang is en hoe het gemeten kan worden. Voor elk element zijn diverse principe-eisen geformuleerd. Per element kan een conclusie gevormd worden. De principe-eisen worden gegroepeerd in het EISA architectuurraamwerk van Gartner.

Vervolgens worden in hoofdstuk 7 en 8 respectievelijk toekomstig onderzoek en een reflectie op het onderzoek beschreven.

De methode is getest in de praktijk door een bestaande architectuurdocumentatie te evalueren. Als onderzoeksobject is de Nederlandse Overheid Referentie Architectuur(NORA) gekozen. Het resultaat van deze evaluatie is te vinden in Bijlage 1.

1. Digitale architectuur, security & privacy

In de ADEM is geen persoonlijke visie op digitale architectuur gegeven. Iedereen kijkt anders tegen dit fenomeen aan en ook ik wil graag mijn persoonlijke mening hierop geven in dit hoofdstuk. Dit biedt de lezer inzicht in mijn ideeën en motivatie om dit onderzoek uit te voeren. Ik zal hier ook in het bijzonder aandacht besteden aan security & privacy.

Bij de afronding van dit onderzoek is het belang van een goede architectuur weer pijnlijk duidelijk geworden. De belastingdienst kampt al jaren met grote problemen met zijn informatiesystemen. De problemen bij de belastingdienst worden grootschalig uitgemeten in de media en dit is ook terecht. De samenleving is hier de dupe van. Ik zie architectuur als een middel om dit soort problemen te voorkomen. Architectuur moet zorgen voor overzicht en complexiteitsreductie. Het is een stuurmiddel voor de organisatie. Het is duidelijk dat de overheid dit overzicht al een tijdje geleden kwijt is geraakt. Met het programma e-overheid[2] heeft de overheid een nieuwe weg ingeslagen en worden architecturale zaken ondergebracht in een apart programma. Een van de belangrijkste deliverables hierin is de Nederlandse Overheid Referentie Architectuur(NORA)[3]. Dit programma is een van mijn drijfveren geweest om te participeren in dit onderzoek.

In het voorbereidende onderzoek is er reeds een definitie gegeven voor digitale architectuur. In dit onderzoek is de definitie van Daan Rijsenbrij geadopteerd. Rijsenbrij[RIJS05] ziet architectuur als

'Een coherente, consistente verzameling principes, verbijzonderd naar concerns, regels, richtlijnen en standaarden die beschrijft hoe een onderneming, de informatievoorziening, de applicaties en de infrastructuur zijn vormgegeven en zich voordoen in het gebruik.'

Ik ondersteun deze definitie in zijn geheel. Binnen de kaders van dit onderzoek is deze definitie ook zeer toepasbaar. Vaak wordt architectuur als alleen iets technisch gezien. Het is een zaak van de technische specialisten. Natuurlijk is het zo dat er bij architectuur een hoop techniek komt kijken maar dan vooral als achterliggende gedachte en om de ideeën van de architect te ondersteunen. Architectuur is in eerste instantie gebaseerd op de missie, visie en strategie van de onderneming. Deze onderneming wil graag zijn missie bewerkstelligen, het maken van winst, of een bepaalde groei doormaken. De architectuur ondersteunt deze missie en dit heeft weinig te maken met techniek maar met een overkoepelende visie op de toekomst. Architectuur kent verschillende werelden. Rijsenbrij omschrijft in zijn werk vier werelden namelijk de businesss-, informatie-, applicatie- en de infrastructuurwereld. Een

[2] http://www.e-overheid.nl/

[3] Te vinden op http://www.e-overheid.nl/atlas/referentiearchitectuur/

opdeling in werelden zal later in het onderzoek verder te spraken komen wanneer security aan architectuur gekoppeld wordt.

Het exact definiëren van architectuur en security & privacy ligt niet binnen de ambitie van dit onderzoek. Het gaat er juist om bestaande zaken te integreren in dit onderzoek en daaraan een evaluatie te koppelen. Het is echter wel belangrijk om de scope te bepalen wanneer we spreken over deze zaken. Dit onderzoek richt zich vooral op de security & privacy kwesties die bij architectuurbeschrijvingen van belang zijn. Dit gaat dus per definitie om informatie, systemen en andere digitale zaken. Architectuur is meer dan dat. Het gaat ook om beleving en sturing kunnen geven aan veranderingsprocessen.

Security eisen moeten worden geïntegreerd in de architectuur en het architectuurraamwerk. Hierbij moet security gezien worden vanuit de enterprise architecture viewpoints maar ook vanuit separate security viewpoints. Dit helpt de stakeholders om de security eisen vanuit een eigen viewpoint te bekijken terwijl de security eisen wel geïntegreerd zijn met de rest van de architectuur[GART06a]. Het introduceren van security geeft nieuwe kansen en bedreigingen voor de organisatie. De organisatie heeft de kans om zijn assets te beschermen. Bedreigingen komen uit alle hoeken. Security is er om met deze bedreigingen en risico's om te gaan. Er kunnen dreigingen zijn vanuit de mens(vooral intern), omgeving, technologie en natuur[OVER99]. Het onderkennen van kansen en bedreigingen is belangrijk voor een organisatie. Daarom wordt dit element ook in de ADEM geadresseerd. Vanuit deze kansen en bedreigingen ontstaan er concerns van de stakeholders van de organisatie. Architectuur en voornamelijk architectuurprincipes worden gevormd op basis van deze concerns.

Binnen de Radboud universiteit (in het bijzonder Bart Jacobs) wordt voor security vaak de definitie 'het reguleren van toegang tot assets' gebruikt. In de context van deze scriptie wordt deze definitie geadopteerd. Een asset is een waardevol onderdeel van de organisatie dat beschermd moet worden. Dit kan bij voorbeeld informatie of infrastructuur zijn. Onder het reguleren wordt de waarborging van de confidentialiteit, integriteit en beschikbaarheid verstaan. Wanneer we security willen evalueren moeten we de controlemechanismen en de assets van de organisatie evalueren.

Wanneer we de toegang tot assets reguleren moeten we dit in verschillende stadia doen. We noemen dit ook wel defence in depth. Dit zijn diverse fysieke, organisatorische en juridische schillen om een asset. De eerste schil kan bijvoorbeeld een firewall zijn. We praten dan over de schil preventie. Daarna krijgen we detectie, repressie, correctie en evaluatie. Deze indeling wordt gegeven door Snel [SNEL05] en wordt ook geadopteerd in de scriptie van Lucien Bongers[BON06]. Bij de evaluatie moet rekening gehouden worden met de diverse schillen om de assets.

Security & privacy wordt door velen als één onderwerp gezien. Ik heb er voor gekozen om deze entiteiten te scheiden. Ik heb dit vooral gedaan vanwege de recente ontwikkelingen in dit vakgebied. Sinds enkele jaren zijn we meer en meer bewust geworden van security én privacy. In Nederland zijn zelfs nieuwe wetten ingevoerd om onze privacy te beschermen[4]. Informatica is een vakgebied dat zich snel ontwikkelt en de wet en regelgeving moet dus bijblijven zodat er geen pijnlijke hiaten kunnen ontstaan.

In de huidige netwerksamenleving wordt steeds meer informatie gekoppeld. Een willekeurige zoekopdracht naar persoonsgegevens in Google levert vaak informatie op waarvan de auteur of eigenaar liever had gehad dat ze confidentieel gebleven was. Ook de overheid doet aan deze netwerksamenleving mee. Met de introductie van de Nederlandse Overheid Referentie Architectuur(NORA) worden ook de meeste overheidssystemen gekoppeld aan elkaar en de buitenwereld. Deze ontwikkelingen werpen bij mij grote vragen op en ik vind het dan ook onze taak en verantwoordelijkheid om hier onze deskundige mening op te geven[5]. Met dit onderzoek beoog ik weer een stap voorwaarts te zetten in de controle op het bedrijfsleven en de overheid op het naleven van verschillende privacy issues. Door security & privacy aspecten te evalueren moet het duidelijk worden hoe organisaties met hun informatie omgaan. Dit is in het belang van het bedrijfsleven en de samenleving in het algemeen.

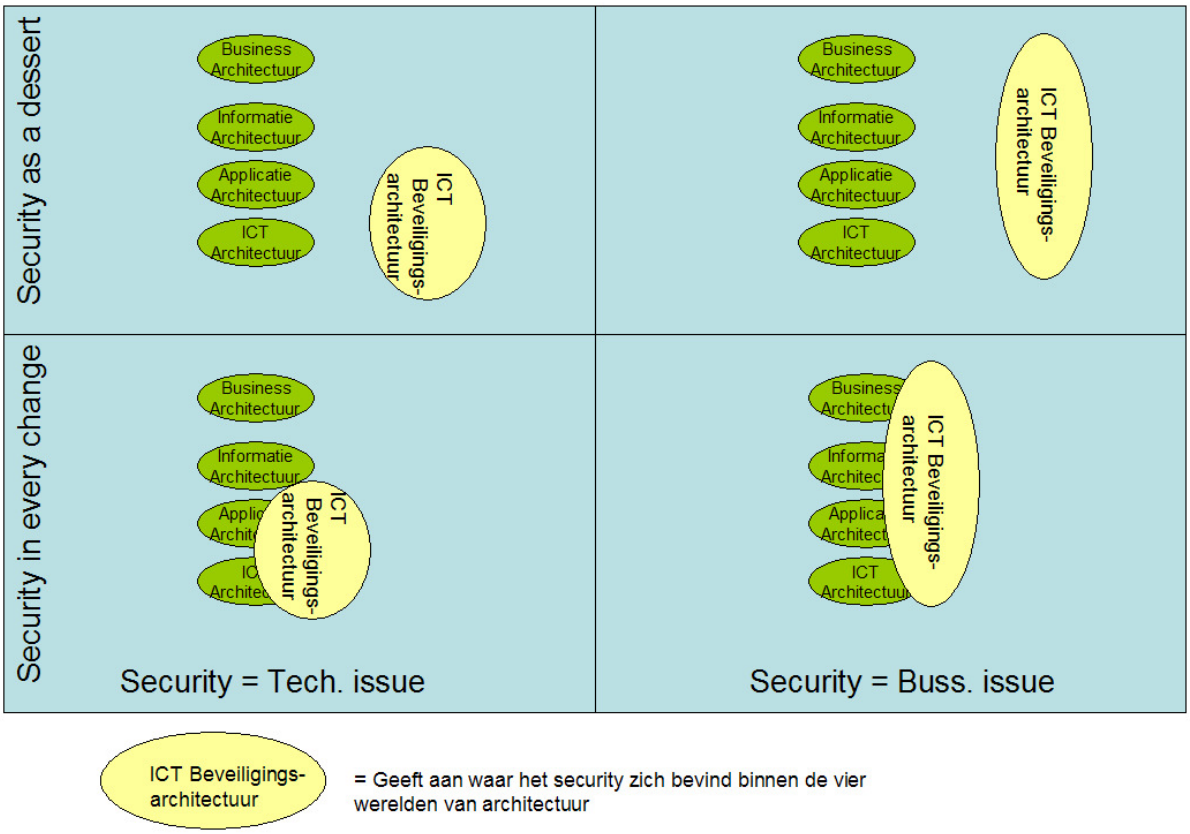
[4] Wet Bescherming Persoonsgegevens, zie http://www.cbpweb.nl/.

[5] Ik gebruik hier ' onze verantwoordelijkheid' omdat ik graag andere architecten en onderzoekers wil motiveren aan de discussie betreffende de digitale overheid deel te nemen.

2. Theoretische Achtergrond

In dit hoofdstuk wordt het theoretisch kader geschetst waarbinnen het onderzoek naar security & privacy binnen architectuurdocumentatie heeft plaatsgevonden. In de ADEM heeft u reeds de achtergrond kunnen lezen over de keuze om architectuurdocumentatie te evalueren(zie hoofdstuk 2.2. in de ADEM 'Waarom architectuurdocumentatie evalueren'). Binnen architectuur is security & privacy een belangrijk item waarin de publieke opinie een belangrijke rol speelt. De rol die security speelt in architectuurdocumentatie is echter niet bij iedereen geheel duidelijk. Veelal wordt securtiy als een losstaand probleem gezien wat resulteert in een niet geïntegreerde aanpak en losstaande oplossingen. Zo ook in architectuurdocumentatie is security vaak een apart hoofdstuk. De plaatsing van architectuur in de business wordt goed beschreven in werk van Aaldert Hofmann en Ben Elsinga [ELS03]. Hier worden twee termen geïntroduceerd, 'Security in every change' en 'security as a business issue'. 'Security in every change' geeft aan of security geïntegreerd is in de vier werelden van architectuur zoals deze zijn gedefinieerd in [IAF99] en [RIJS05] of dat security vooral een separaat hoofdstuk is. 'Security as a business issue' geeft aan of security een business issue is of dat het zich alleen beperkt tot louter infrastructuur en applicaties.

Deze twee termen kunnen in een matrix worden geplaatst. Bij de horizontale as wordt aangegeven of security ook doorkomt in de business of dat het alleen als een technisch fenomeen wordt gezien. Bij de verticale as wordt aangegeven of security wordt geïntegreerd met de rest van de organisatie of dat het een eiland is zonder relatie met zijn omgeving. Dit is geïllustreerd in Figuur 2.



Figuur 2: Plaatsing security in architectuurdocumentatie (Met dank aan Erno Duinhoven)

In de literatuur zijn er veel best practises, normen en standaarden te vinden over security en hoe deze toe te passen in een organisatorische context[ISO05a][BS99][ISA07]. Organisaties kunnen zich zelfs laten certificeren en audits laten uitvoeren door gespecialiseerde bureaus. Deze best practises, normen en standaarden worden echter niet concreet toegepast op architectuur en architectuurdocumentatie. Binnen dit onderzoek wordt bekeken hoe deze zaken verwerkt kunnen worden in architectuurdocumentatie. Wanneer er organisatiebeleid is op het gebied van security moet deze worden ondersteund door de architectuur. Het securitybeleid kan prima worden ondersteund door gebruik te maken van eerder genoemde best practises. Maar hoe zit dat dan met architectuur? Hoe wordt het securitybeleid toegepast in een werkbare en veilige architectuur? Dit zijn vragen die van belang zijn voor dit onderzoek. De antwoorden op deze vragen zijn bepalend voor de norm die gebruikt wordt voor de evaluatie.

We moeten bij security het wiel niet telkens opnieuw uitvinden. Het zou daarom niet verstandig zijn opnieuw te kijken naar welke aspecten belangrijk zijn binnen security en privacy. De eerder genoemde normen kunnen daarvoor gedeeltelijk gebruikt worden. Wat belangrijk is, is om de juiste elementen uit dit normenkader zo te herschrijven dat ze toepasbaar zijn op architectuurdocumentatie. De ADEM met zijn verdeling in elementen is hier uitermate geschikt voor. Als uitgangspunt worden enkele normen en best practises aangevuld met enkele eigen bevindingen gekozen om als referentiekader te dienen voor deze aspectscan.

3. Doel, Afbakening en Verantwoording

Architectuur in de Informatietechnologie is een relatief jong vakgebied. Het denken aan security en privacy in architecturen is nog veel jonger. In organisatorische context wordt al wel veel langer gedacht aan security. Sinds mensenheugenis bestaat er criminaliteit en diefstal. Bedrijven en individuen wapenen zich hier tegen. We beschermen onze eigendommen en proberen onze persoonlijke integriteit te waarborgen. Met de introductie van de informatietechnologie is hier een nieuwe kijk op gekomen. Systemen moeten beschermd worden voor aanvallen van buitenaf. Alleen het fysieke hek om het bedrijf werkt niet meer. De laatste jaren zijn we steeds meer een netwerkcommunity geworden en zijn systemen met elkaar gekoppeld. Organisaties worden zich meer en meer bewust van de rol van security en privacy. Architectuur moet hier dus op in spelen en mee gaan met deze ontwikkelingen.

Het doel van deze scan is niet alleen het evalueren van de security & privacy van architecturen maar kan ook als raamwerk dienen om van te voren na te denken over deze onderwerpen. In dit onderzoek is naar een paar best practises en normenkaders gekeken. Veel van deze best practises hebben onderling enige overlap en behandelen dezelfde elementen. Hierbij gaat het vaak over fysieke, organisatorische en juridische controlemechanismen om security & privacy te waarborgen. Een goede opdeling is te vinden in de code van informatiebeveiliging [ISO06a]die gebaseerd is op de British Standard BS 7799[BS99]. De elementen die hierin worden onderkend zullen de norm vormen voor deze security scan. De elementen moeten hiervoor worden omgeschreven naar werkbare indicatoren en security principes die toegepast kunnen worden op architectuurdocumentatie. Deze standaarden zijn wijd geaccepteerd en bieden dus een goed uitgangspunt voor dit onderzoek.

Zoals ook in de ADEM is architectuurdocumentatie het uitgangspunt voor deze scan. Zoals in de vorige paragraaf is aangeven zijn er vele gebieden waarop security invloed heeft en zijn er ook verschillende security maatregelen te bedenken om organisaties te beschermen. Veel security experts hebben vooral interesse in encryptie technologieën, complexe algoritmes en security protocollen. In architectuurdocumentatie speelt dit ook een rol echter wel op een ander niveau. Er wordt bijvoorbeeld een strategische keuze gemaakt tussen open of closed source[6][7]. Deze beslissingen hebben invloed op de technische maatregelen die in de organisatie worden ingevoerd. Binnen architectuur zijn er diverse beschouwingniveaus te vinden. Op het hoogste niveau bevindt zich de enterprise-architecture die binnen de fysieke architectuur het best is te vergelijken met een stadsarchitectuur. Strategische beslissingen die invloed hebben op de lagere beschouwingniveaus worden in de

[6] http://nl.wikipedia.org/wiki/Open_Source

[7] De visie van de Nederlandse Overheid op open source: http://www.egem.nl/kennisbank/informatievoorziening/open-standaarden-en-open-source-software

documentatie van de enterprise-architectuur vastgelegd. Binnen dit onderzoek wordt gekeken naar deze vorm van architectuur.

4. Evaluatie van security & privacy binnen de architectuurwereld

Elementen die van belang zijn voor security & privacy

In de ADEM is onderzoek verricht naar wat goede architectuur nu precies inhoud en hoe men dit moet meten. Wat goede security & privacy is en hoe men dit moet meten is al vastgelegd. Hier zijn best practises en normen voor waaraan organisaties zich kunnen toetsten. Er is ook veel wet en regelgeving voor security & privacy. Veel van deze normen en wetgevingen zijn afgeleid van elkaar. Voorbeelden hiervan zijn:

- De code voor informatiebeveiliging (NEN-ISO/IEC 17799:2005, gebaseerd op BS 7799) [ISO05a]
- British Standard 7799 [BS99]
- ISO/IEC 27001 (onderdeel code voor informatiebeveiliging, voorheen B7799-2)[ISO05b]
- NEN 7510 voor de zorgsector [NEN04]
- NEN-ISO/IEC 15816:2002 voor de telecommarkt [ISO02]
- Control Objectives for Information and related Technology (COBIT)[ISA07]
- Sarbanes-Oxley (Amerikaanse wetgeving)[8]
- WBP: Wet bescherming Persoonsgegevens (Nederlandse wetgeving)[WBP00]

Al deze documenten hebben betrekking op security & privacy. Voor dit onderzoek zijn de elementen die worden genoemd overgenomen als norm voor de scan. De elementen zijn zo herschreven dat ze toe te passen zijn op architectuurdocumentatie. Wet en regelgeving evenals best practises kunnen veranderen, de norm is daarom ook verdeeld in elementen. Elementen kunnen aangepast, verwijderd of toegevoegd worden. Om te evalueren hoe de elementen beschreven worden in de architectuurdocumentatie zijn indicatoren beschreven. In deze aspectscan wordt geen absoluut oordeel geveld over de inhoud van de elementen. In de ADEM kon een element als aanwezig, gedeeltelijk aanwezig of afwezig bestempeld worden. Binnen deze aspectscan zijn wel indicatoren onderkend maar er wordt geen waardeoordeel gegeven. Hoe binnen organisaties omgegaan wordt met security & privacy is erg afhankelijk van het ecosysteem van de organisatie. Het

[8] Volledige wettekst te vinden op http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h3763enr.tst.pdf

gaat er om dat de organisaties een weloverwogen beslissing maken over hoe zij willen omgaan met security & privacy. Door aan alle indicatoren te voldoen dwingt de organisatie beslissingen omtrent security & privacy te nemen.

Een traditionele benadering is het ommuren van persoonlijke eigendommen en systemen. Organisaties zijn echter afhankelijker van elkaar geworden en informatie moet snel en betrouwbaar geleverd worden. We koppelen daarom onze systemen. Dit wordt ook wel de hedendaagse netwerkmaatschappij genoemd. In verband met korte levertijden en kwaliteit van informatie worden de bestelsystemen van supermarkten gekoppeld aan de eigen voorraadadministratie en het leveringssysteem van de leverancier. Vervolgens wordt een connectie gemaakt met de distributeur zodat de vrachtwagens op tijd vertrekken. Een nieuwe benadering is dat we deze trend niet meer kunnen stoppen en maar mee moeten gaan hierin. Het Jericho forum[9] beschrijft de organisatie zonder muren en geeft aan dat we de autorisatie tot onze bronnen tot op het laatste moment moeten uitstellen. Jericho wil dit bewerkstelligen met integrale encryptie, protocollen en hardwareverbindingen die impliciet veilig zijn, federatief identiteitsmanagement, digital rights management en – vooral – sterke authenticatie op het niveau van individuele gegevenselementen. Duidelijk is dat architectuurdocumentatie deze uitdagingen moet adresseren en moet aangeven hoe ze met deze hedendaagse problematiek omgaat.

Tijdens een themamiddag over security en privacy binnen de overheid werd het begrip deperimetrisatie geïntroduceerd dat alles te maken heeft met 'gesloten systemen in een open omgeving'[10]. Dit was tevens de titel van de presentatie van Jurgen van der Vlugt. Een perimeter geeft een grens aan tussen twee systemen. De term deperimetrisatie geeft het verdwijnen van deze muren aan. Deze middag stond in het teken van de NORA en gaf aan dat ook de security experts het niet met elkaar eens zijn. Een levende discussie ontstond over deze begrippen en hoe bedrijven en overheid hier mee om zouden moeten gaan. In de aspectscan moeten dus eisen gesteld worden aan de relatie die de organisatie heeft met de buitenwereld

Binnen deze discussie bestaat er geen goed of fout. Er zijn verschillende benadering om security vraagstukken te beantwoorden. Wel is de organisatie gebonden aan wet en regelgeving. In Nederland is dit de wet bescherming persoonsgegevens. Er zijn genoeg accountancy bureaus die hier een audit op kunnen uitvoeren en derhalve is een goed of fout antwoord dus geen uitgangspunt van deze scan. Wat belangrijker is, is de maatschappelijke discussie en dat organisaties nadenken over security voordat ze acteren.

[9] http://www.opengroup.org/jericho/

[10] Een verslag van deze themamiddag is te vinden op http://www.pi4ib.nl/vak/20070418/verslag.html

De architectuurdocumentatie is voor security & privacy gebaseerd op het securitybeleid waarin de missie, visie en strategie van de onderneming worden vertolkt. Dit securitybeleid is voor elke organisatie anders. De elementen moeten dus vooral controleren of er beslissingen zijn genomen. Indicatoren geven bijvoorbeeld aan of er gekozen is voor open of closed source met een bijbehorende rationale. De indicatoren vertellen niet of deze beslissing juist is of niet. Wanneer een best practise aangeeft dat een bepaalde techniek gebruikt moet worden, wordt dit binnen de methode wel geadopteerd tot dat er een nieuwe best practise is.

Security & Privacy principes, hoe te evalueren

Er zijn verschillende onderzoeken naar security principes geweest[BLUM05][ELS03][GASSP][STONE]. Er zijn ook repositorys met security patterns[11]. In het onderzoek van Lucien Bongers worden vooral voorbeelden van security principes gegeven die als common sense voor architectuur gelden[BON06]. Deze principes zijn een goed uitgangspunt voor deze aspectscan. Het is echter niet zo dat deze lijst met principes compleet is. Er zullen altijd nieuwe principes ontstaan gebaseerd op nieuwe ideeën of een veranderende publieke opinie. Het is voor evaluatie doeleinden beter om de inhoud van deze principes te beschrijven en een raamwerk te bieden om ze te ordenen vanuit diverse security viewpoints. Een principe zal immers niet letterlijk overal hetzelfde verwoord zijn.

Principe eisen

Bij de evaluatie van de principes wordt er gekeken naar de inhoud van de principes en of ze de benoemde elementen voldoende ondersteunen. Per element zullen richtlijnen gegeven worden voor de invulling van de principes. Deze richtlijnen worden geformuleerd in principe-eisen. Deze eisen schrijven voor waar de principes aan moeten voldoen om het betreffende element voldoende te ondersteunen. Deze eisen worden gesteld aan security principes maar ook aan architectuurprincipes elders in de documentatie. Architectuurprincipes die buiten het hoofdstuk security vallen maar toch invloed uitoefenen op een bepaald security & privacy element moeten dus ook worden geëvalueerd.

De security principes zullen echter niet vaak letterlijk terugkomen in de architectuurdocumentatie. Daarom is het nodig om de evaluator een handvat te bieden waarmee hij de principes sneller kan vinden en identificeren. Architecturen zijn gebouwd op basis van een raamwerk. Dit raamwerk bestaat uit verschillende lagen. Om te bepalen waar in de architectuur deze principes geplaatst zijn of zouden moeten zijn worden de principes tevens geplaatst in een architectuur raamwerk. Bij de keuze van het raamwerk wordt er vooral gekeken naar het generieke karakter van het raamwerk en de relatie security ⇔ architectuur. De keuze van dit raamwerk wordt in de volgende paragraaf besproken.

[11] http://www.securitypatterns.org/patterns.html

Raamwerken voor security & privacy

Er zijn enkele methoden ontwikkeld die de plaatsing van security & privacy aangeven binnen de architectuurwereld [GART06a][HOF04][SHER05]. Enkele van deze methoden worden kort omschreven en er wordt bepaald hoe deze zijn toe te passen binnen de aspectscan security & privacy.

Gartner geeft verschillende mogelijkheden aan om security te integreren in een architectuurraamwerk[GART06a]. Een van deze aanpakken is gebaseerd op het definiëren van security als een aparte view. Dit betekent niet dat het los staat van de rest van de architectuur maar dat het een andere aanpak vergt met zijn eigen modellen en oplossingen. Deze aanpak is bij uitstek geschikt om de diverse principes te ordenen naar de verschillende architectuurlagen zoals deze ook te vinden zijn in het Rijsenbrij raamwerk[RIJS05]. Gartner geeft wel aan dat deze aanpak alleen toepasbaar is wanneer er ook aandacht wordt besteed aan security binnen het architectuurproces [GART06c]. Dit wordt vooral belangrijk gevonden voor bijvoorbeeld draagvlag en awareness binnen de gehele organisatie en niet alleen binnen de IT organisatie.

Het raamwerk dat Gartner introduceert heeft vier lagen die ieder diverse security requirements, modellen, raamwerken en principes bevatten. De architectuurlagen en de inhoud per laag worden in figuur 3 geïllustreerd.

Figuur 3: Architectuurlagen en de elementen die aanwezig zijn op het security gebied(bron [GART06a]

Figuur 3 illustreert welke elementen er op welk niveau in de organisatie aanwezig zijn. Binnen het raamwerk zijn er vier lagen te onderscheiden te weten:

- De businesslaag
- De conceptuele laag
- De logische laag
- De implementatie laag

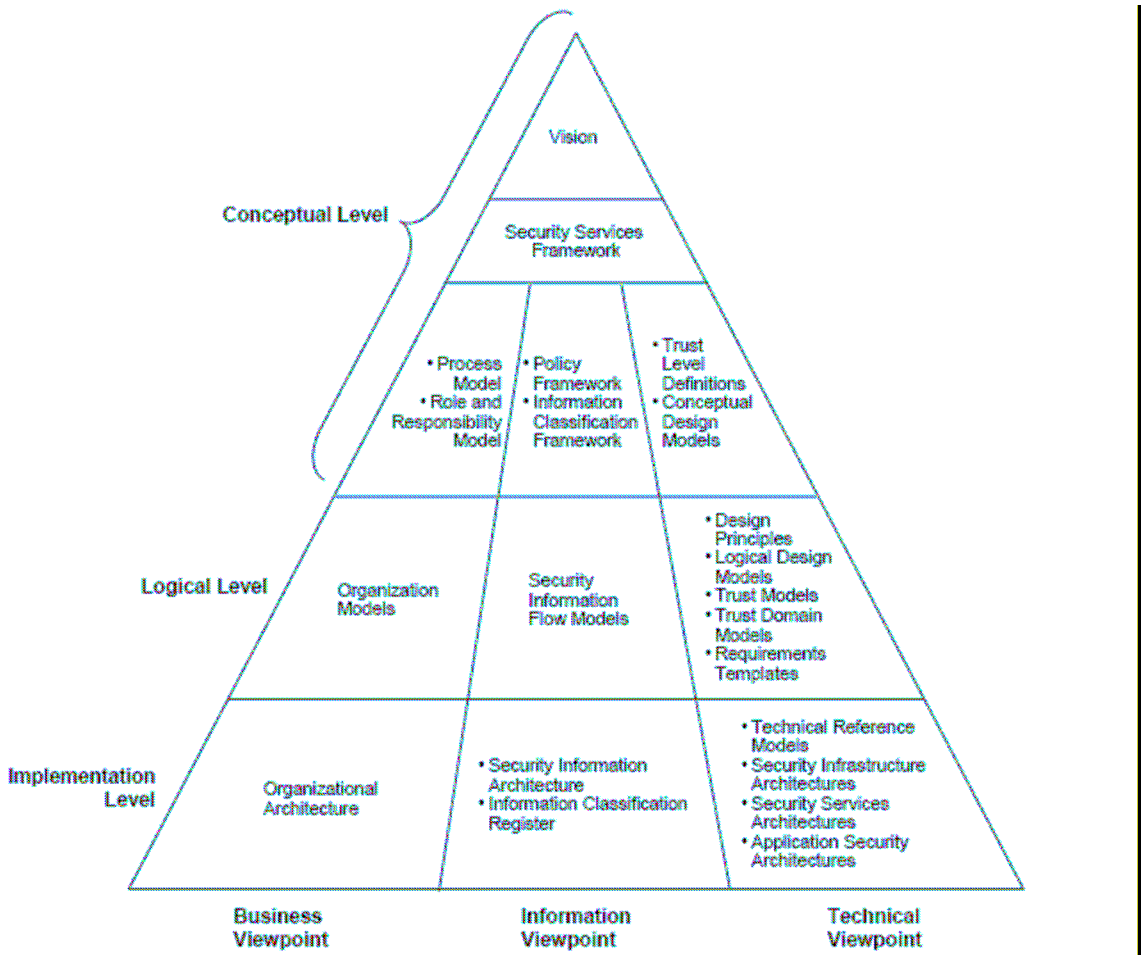
Deze lagen hebben betrekking op security en beschrijven op diverse abstractieniveaus welke onderdelen geadresseerd moeten zijn in de architectuurdocumentatie. De lagen worden hier kort beschreven.

We zien op de businesslaag vooral de visie van de organisatie terug. Wat zijn de algemene security & privacy doelstellingen van het bedrijf en hoe ziet het ecosysteem van de organisatie er uit. De omschrijving van dit ecosysteem is voor security doeleinden belangrijk. Het geeft de verwachtingen van klanten, leveranciers en partners aan die zij hebben bij de organisatie wanneer gesproken wordt over security & privacy. Bij een overheidsorganisatie hebben klanten een ander verwachtingspatroon dan bij de lokale koffieshop. In deze laag bevinden zich ook de compliancy vraagstukken. Wanneer de organisatie moet voldoen aan wet en regelgeving kan dit betekenen dat specifieke best practises en controls nodig zijn, bijvoorbeeld SOX of HIPAA(Health Insurance Portability and Accountability). Principes op dit gebied moeten dus hier geplaatst worden.

De conceptuele laag geeft een security gerelateerde visie met bijgehorende principes. De modellen zijn functioneel gericht op security. Een voorbeeld van deze functionele modellen is het risicomanagement model. In dit model worden alle functies benoemd die nodig zijn om risico's goed in kaart te kunnen brengen. In de logische laag wordt vooral de relatie met andere viewpoints op detail niveau onderkend. Security moet bijvoorbeeld geïntegreerd zijn met de menselijke maat. Alle oplossingen die in de implementatielaag worden omschreven moeten niet alleen veilig zijn maar ook werkbaar en ergonomisch verantwoord voor diegene die er mee moeten werken. Modellen uit andere viewpoints die op detailniveau een relatie hebben met security komen terug in de logische laag. De functies en services die kunnen worden toegepast worden omschreven in de implementatielaag. Het gaat hier over de technische security van applicaties en infrastructuur. Er worden bijvoorbeeld templates voor end to end solutions vastgelegd. Principes die te maken hebben met technieken moeten daarom in deze laag gevonden worden.

Gartner geeft vervolgens een raamwerk waarmee de verschillende architectuurelementen per viewpoint zijn te plaatsen binnen deze architectuurlagen. Hierbij is

rekening gehouden met drie viewpoints namelijk, een business, information en technical viewpoint. Alle modellen en architectuurprincipes die te invloed hebben op de security & privacy van een organisatie kunnen in dit raamwerk geplaatst worden. Het betreft dus ook de applicatie en infrastructuur architectuur van de organisatie. Deze informatie is vaak implementatie en context afhankelijk. Deze oplossingen zijn niet terug te vinden in enterprise architectuur of referentie architecturen maar eerder in afgeleide architecturen. De views die zijn gedefinieerd zijn belangrijk voor de diverse stakeholders. Binnen de security wereld zijn er mensen die zich bezig houden met organisatorische zaken zoals het securitybeleid en de inbedding van security in de organisatie. Daarnaast zijn er veel technische specialisten die alleen kijken naar encryptie en protocollen. Deze stakeholders hebben allemaal een andere kijk, een view, op het systeem. Het Enterprise Information Security Architecture raamwerk ondersteunt deze viewpoints, zie figuur 4.

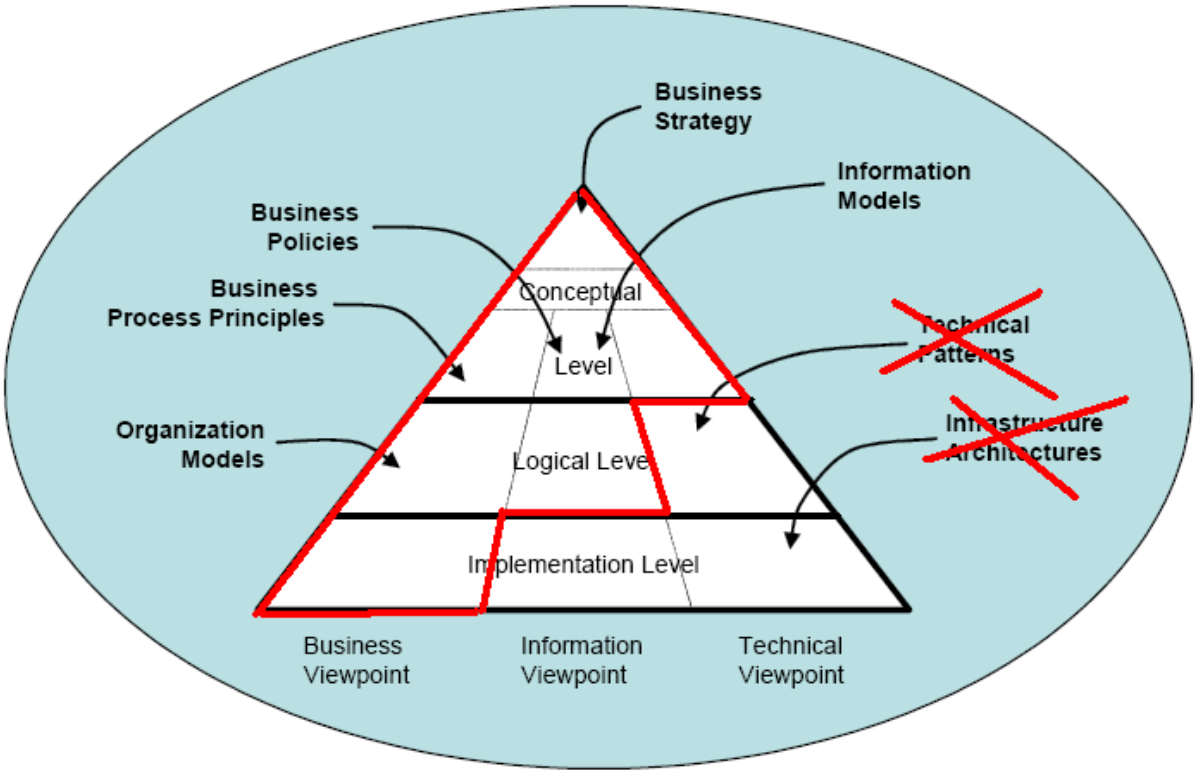


Figuur 4: Enterprise Information Security Architecture ingedeeld in architectuurlagen en viewpoints. [GART06c].

Hoe werkt dit model dan toegepast op EA architectuurdocumentatie? Deze vorm van architectuurdocumentatie is een high level overview op de architectuur en implementatiespecifieke details komen hier niet aan bod. Derhalve zijn een paar

vlakken van het oorspronkelijke raamwerk uitgesloten. De uitgesloten vakken bevatten implementatiespecifieke details en komen aan bod in overige documentatie zoals project start architecturen(PSA). De PSA is de vertaling van de algemene architectuurprincipes en -modellen naar projectspecifieke richtlijnen[12]. Op implementatie level komen nog wel business principes voor die op business niveau bepalen welke implementatiespecifieke details er gekozen mogen worden. Denk hierbij aan standaardisatie en compliancy vraagstukken.

In het EISA raamwerk wordt een verdeling gemaakt van elementen die wel en niet terug te vinden moeten zijn in de architectuurdocumentatie. Dit is geïllustreerd in figuur 5 waarbij de rode lijnen aangeven waar de afbakening zich bevind. Met pijlen is aangegeven welke informatie en principes in de architectuurlagen en viewpoints te vinden zijn.



Figuur 5: EISA toegepast op EA architectuurdocumentatie.

Het gebruik van elementen, security principes, en de ordening van principes in een raamwerk zijn in dit hoofdstuk besproken. Het ESIA raamwerk geeft na aanpassing een goede verdeling om security principes te plaatsen in de architectuurdocumentatie. Zo ontstaat er een raamwerk met drie verschillende viewpoints op drie verschillende architectuurlagen waarbij expliciet is aangegeven welke viewpoints aanwezig zijn in EA architectuurdocumentatie. Verderop in dit document zullen

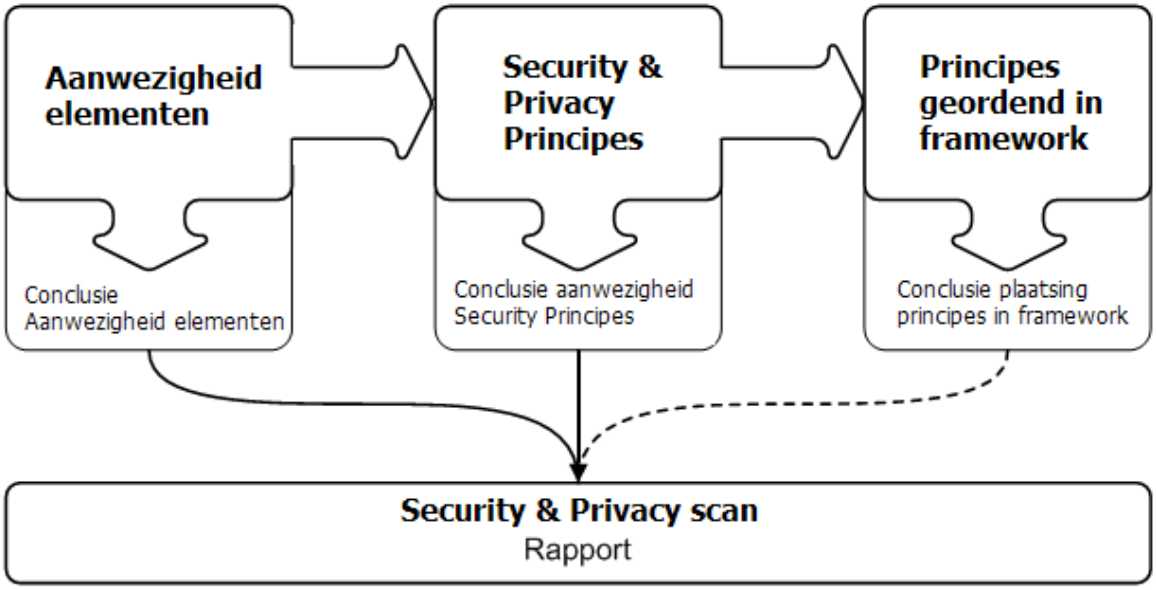
[12] http://www.dya.info/Home/dya/technieken/project_start_architectuur.jsp

eisen ontworpen worden voor security principes. Deze principe-eisen zullen per architectuurlaag en viewpoint verdeeld worden.

In het volgende hoofdstuk wordt de relatie tussen de elementen, de principes en het raamwerk beschreven en er zal een vast evaluatieproces geïntroduceerd worden.

5. Toepassing op de aspectscan

Er zijn in deze aspestscan drie belangrijke fasen. Fase één behandelt het controleren en evalueren van elementen op basis van huidige best practises en standaarden. Het controleren van de inhoud van principes die in relatie staan met de onderwerpen uit het desbetreffende element wordt in fase twee behandeld. De principes zijn daarom gesorteerd per element. Fase drie is optioneel en is eigenlijk meer een hulpmiddel voor zowel de organisatie om haar principes te classificeren als voor de evaluator om de principes terug te vinden. Het proces is schematisch weergegeven in figuur 6. De fasen worden hieronder kort omschreven.



Figuur 6: De aspectscan schematisch weergegeven.

Fase 1: Aanwezigheid elementen

In de eerste fase worden architectuurelementen onderzocht. Zijn ze aanwezig en wat is de inhoud ervan? Dit is niet alleen het controleren op syntactische aanwezigheid maar ook een meer diepgaande analyse op de inhoud van het element. De elementen zijn gebaseerd op diverse best practises en standaarden. Deze best practises geven concrete controlemechanisme aan om deze elementen af te dekken. Niet al deze controlemechanismen zijn toe te passen op architectuurdocumentatie en daarom is er een abstractie gemaakt van welke controlemechanismen er aanwezig moeten zijn in de architectuurdocumentatie. Controles op het gebied van fysieke beveiliging en camerabewaking in de gebouwen wordt niet meegenomen in de scan. Hooguit moeten de risico's hieromtrent kort aangestipt worden. Dit zijn zaken die omschreven moeten zijn in security policies en beleid van de organisatie. Een voorbeeld van een aanwezig element is de omschrijving van de organisa-

tiedoelstellingen betreffende security en privacy. Een indicator hierbij is dat in ieder geval een onderscheid moet zijn gemaakt in organisatorische categorieën zoals de naleving van wet en regelgeving of de effectiviteit van bedrijfsprocessen. Een best practise op dit gebied is COSO[13] die diverse categorieën voor organisatiedoelstellingen introduceert.

De volgende tabel geeft een generiek beeld van hoe de elementen worden weergegeven in deze methode. Deze weergave helpt de evaluator bij het evalueren van een element. Wanneer eventueel elementen worden toegevoegd aan deze methode, zullen ze op dezelfde manier moeten worden weergegeven.

Hier staat de naam van het element.	
Wat is het?	Hier wordt beschreven waar het element over gaat.
Waarom is het belangrijk?	Hier wordt beschreven waarom het belangrijk is dat het element geëvalueerd wordt.
Hoe te meten?	Hier wordt precies beschreven hoe de evaluator tot een beoordeling komt met betrekking tot een criterium. Er wordt beschreven welke indicatoren een element heeft.
Eisen principes	Hier staat beschreven waar de principes aan moeten voldoen die dit element moeten afdekken. Het is hierbij vooral van belang om de aanwezigheid van de principes en de rationale hiervan te achterhalen. Dit beslaat fase 2 van de methode en kan dus apart uitgevoerd worden van de eerste drie onderwerpen (wat, waarom, hoe) binnen het element. De principes staan namelijk vaak niet gegroepeerd per element. Om de principes terug te vinden kan het raamwerk uit stap 3 worden gebruikt. Elk principe heeft een nummer dat vooraf gegaan wordt door de code PE (principe-eis).

Fase 2: Security & privacy principes

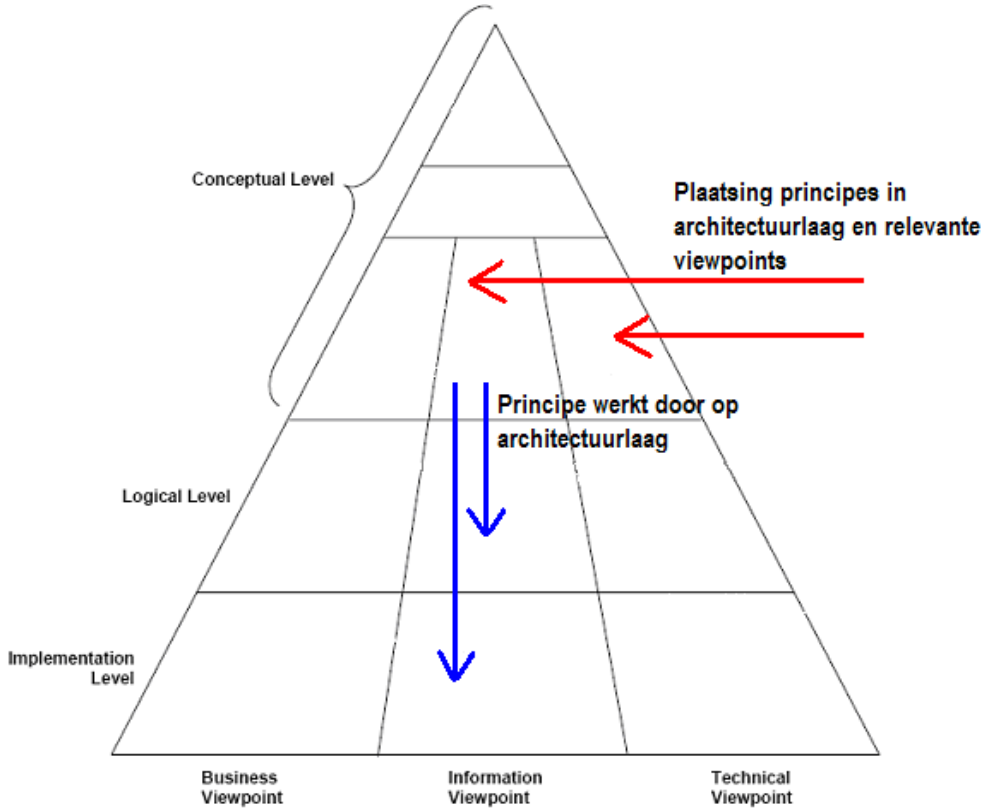
Security is een aparte view en daarbij horen aparte principes. Dit betekent echter niet dat andere principes, die ogenschijnlijk niets te maken hebben met security, niet worden bekeken. In tegendeel, architectuurprincipes op het hoogste niveau werken altijd door op alle lagen van de architectuur en zo ook op de security. Security moet als enabler van de business omgaan met de organisatieoverstijgende principes. Dit impliceert dat de werking van deze principes ook gecontroleerd moet

[13] http://www.coso.org/

worden. Door gebruik te maken van huidige best practises is deze scan up to date en houdt zij rekening met alle aandachtsgebieden binnen de security wereld. Deze aandachtsgebieden zijn verdeeld over de aanwezige elementen. De principes moeten deze aandachtsgebieden bewaken. De ADEM geeft globale richtlijnen voor de principes. Zo moet er in ieder geval een rationale van het principe gegeven worden. Deze controle heeft al plaatsgevonden in de voorbereidende scan van de ADEM en zal derhalve niet nogmaals worden gecontroleerd. In de aspectscan worden aanvullende eisen benoemd voor principes die van belang zijn in een bepaald element. Sommige eisen aan principes zijn voor meerdere elementen van belang. Deze principe-eisen worden dan ook herhaald in de elementen waarvoor ze van toepassing zijn. In totaal zijn er 50 principe-eisen gedefinieerd.

Fase 3: Principes geordend in EISA raamwerk

Architectuur is vaak gebaseerd op een raamwerk. Vandaar dat de toepassing en benoeming van een architectuurraamwerk ook in de ADEM als een van de vereiste elementen is benoemd. Principes zijn meestal verdeeld over de architectuurlagen van een dergelijk raamwerk. Bij security principes is dit ook het geval. Voorheen waren deze raamwerken niet met elkaar verbonden maar met de introductie van het eerder benoemde Enterprise Information Security Architecture is een aanzet gemaakt om te komen tot een geïntegreerde security aanpak. Per principe wordt aangegeven waar dit principe voorkomt. In figuur 7 is dit weergegeven met rode pijlen. Een principe kan maar op één architectuurlaag voorkomen maar kan wel doorwerken op de andere architectuurlagen. Een principe kan vanuit verschillende viewpoints bekeken worden en kan dus op dezelfde laag vaker voorkomen. De plaatsing van principes in het EISA raamwerk wordt geïllustreerd in figuur 7.



Figuur 7: Plaatsing principes binnen het EISA raamwerk

De invulling van dit raamwerk heeft een paar doelstellingen:

- Het raamwerk geeft diverse security views voor security experts. Experts met een technische achtergrond kunnen bijvoorbeeld de principes evalueren die alleen in het viewpoint 'technical' voorkomen.
- De invulling van het raamwerk helpt de evaluator de principes in de architectuurdocumentatie te adresseren. Wanneer de architectuurdocumentatie is opgebouwd uit verschillende architectuurlagen zouden de principes in de benoemde architectuurlagen moeten voorkomen.
- Wanneer de principes voor de evaluatie nog niet geordend zijn kan dit na afloop van de evaluatie gedaan worden met behulp van het ingevulde raamwerk.
- Het ordenen van de security principes met behulp van het EISA raamwerk zorgt voor een geïntegreerde architectuuraanpak[GART06a]. De principes staan niet meer als een los hoofdstuk gegroepeerd maar het is duidelijk op welke architectuurlagen zij invloed hebben.
- De security principes kunnen ook vanuit een business viewpoint bekeken worden. Managers krijgen zo een betere indruk wat de consequentie is van de voorgestelde security principes op de benoemde architectuurlagen.

Eisen aan de aspectscan

De aspectscan moet volgens de richtlijnen van de ADEM flexibel zijn en daarmee moet het mogelijk zijn de norm te veranderen. De voorgestelde methode met de verdeling in drie fasen zal gehandhaafd blijven. De norm die op de huidige best practises is gebaseerd is echter flexibel en zal dus over de jaren heen evolueren. De ADEM geeft ook als richtlijn dat een voorbereidende aspectscan aanwezig moet zijn. Tijdens de loop van dit onderzoek is voortschrijdend inzicht ontstaan betreffende deze eis. Nadat een evaluatie met de ADEM heeft plaatsgevonden heeft de evaluator een prima zicht op de kwaliteit en inhoud van de architectuurdocumentatie. Het is daarom onnodig om hier uitgebreid bij stil te staan als men een aspectscan gaat uitvoeren. De evaluator heeft tijdens het uitvoeren van de ADEM ook reeds inzicht gekregen in de onderwerpen die in de aspectscan worden geëvalueerd en kan daarom zelf de beslissing nemen of een bepaald aspect wel of niet uitgevoerd kan worden. Binnen de opgeleverde aspectscan zijn dan ook geen eisen vooraf opgenomen. Het zou ook zeer kwalijk zijn dit te doen voor een aspectscan die security & privacy evalueert. Over ieder onderdeel uit de architectuurdocumentatie valt namelijk wat te zeggen op het gebied van security & privacy. Het is daarbij geheel onbelangrijk of er wel of niet een hoofdstuk security is opgenomen in de documentatie. Niet evalueren zou betekenen dat wij als auteurs van de ADEM security zien als een losstaand probleem wat niets te maken heeft met de rest van de architectuur. Principes die niet in het hoofdstuk security voorkomen zouden dan geen invloed hebben op security & privacy? Het is daarom altijd zinvol om deze aspectscan te doorlopen. Het kunnen doorlopen van de voorbereidende scan is hiermee de preconditie van de aspectscan security & privacy geworden.

Wat levert de evaluatie op?

Zoals al eerder beschreven is, levert de methode geen ja/nee antwoord op de vraag 'is dit een secure architecture?'. De scan geeft inzicht en antwoord op de vraag of er aan alle zaken is gedacht die komen kijken bij security & privacy. De elementen en de evaluatie van de principes geven inzicht in hoe de organisatie omgaat met architectuur.

Het rapport van de aspectscan security & privacy bevat de conclusies over elk element en een lijst met principes die dit element beïnvloeden. Tevens dient voor elk element en principe te worden genoteerd waar het element en principe is gevonden en waarom er een bepaalde conclusie is getrokken, zodat de architect van de architectuurdocumentatie eventueel verbeteringen kan aanbrengen. De volgende tabel dient de evaluator per element in te vullen.

Elementnaam	
Meting	Per evaluatiecriterium dient de evaluator hier aan te geven waar hij de beschrijving van het element gevonden heeft in de architectuurdocu-

	mentatie. Daarnaast dient de evaluator een kleine samenvatting te geven van het gevonden evaluatiecriterium. Wanneer een evaluatiecriterium niet aanwezig is of beoordeeld kan worden, dient dit hier ook aangeven te worden.
Welke principes?	In fase twee wordt een evaluatie gedaan naar de aanwezigheid van principes die invloed hebben op de security & privacy. Hier geeft de evaluator aan welke principes gevonden zijn. Hoe deze principes invloed hebben op het element wordt omschreven in de conclusie.
Conclusie	De evaluator schrijft hier op waarom een bepaalde conclusie getrokken is. Deze conclusie is mede gebaseerd op architectuurprincipes die het element beïnvloeden. Niet alleen de principes hebben invloed op deze conclusie maar ook overige onderdelen die beschreven zijn in de architectuurdocumentatie zoals modellen en achtergrondbeschrijvingen.
Aanbeveling	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.

6. De Aspectscan Security & Privacy

Fasering

Zoals eerder besproken zijn er drie fasen te onderkennen binnen de aspectscan security & privacy. Deze fasen zijn besproken in hoofdstuk 'toepassing op de aspectscan'. Dit is geïllustreerd in figuur 6 op pagina 23. Fase één en twee zijn verplicht en moeten altijd uitgevoerd worden. Fase drie helpt de evaluator bij het vinden van de architectuurprincipes. Het is essentieel voor architectuurdocumentatie dat architectuurprincipes correct geordend zijn in een raamwerk. Dit is in het belang om goede viewpoints te creëren voor de stakeholders van het domein dat de architectuur beslaat. De evaluator maakt een model waarin de principes binnen de architectuurdocumentatie overzichtelijk worden gegroepeerd. De lezer van het evaluatierapport heeft hiermee inzicht in op welke architectuurlagen de genoemde principes betrekking hebben. Bij het verbeteren van de architectuurdocumentatie kan hier rekening mee gehouden worden.

Globale Fase

Fase 1+2: Aanwezigheid van elementen & principes

In Tabel 1 wordt een lijst gegeven met alle elementen die worden geëvalueerd tijdens de aspectscan. Fase 2 wordt in deze tabellen meegenomen in de vorm van principe-eisen. In deze tabel wordt dit aangeduid met de kolom Eisen voor principes. Binnen deze kolom heeft iedere principe-eis een uniek opvolgend nummer.

Aanwezigheid van elementen	

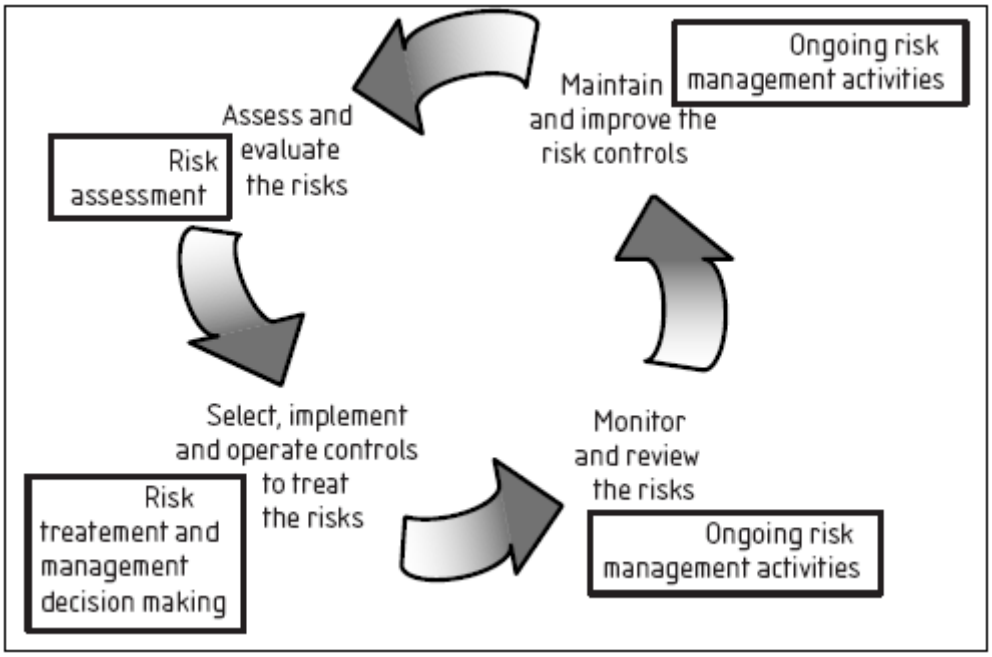
Elementen	- Organisatiedoelstellingen met betrekking tot Security & Privacy
	- Risicomanagement
	  - Risicomanagement: Identificatie en evaluatie van risico's
	  - Risicomanagement: Behandeling van risico's
	  - Risicomanagement: Monitoring en evaluatie van risico's
	  - Risicomanagement: Evaluatie en aanpassing van controlemechanismen
	- Toepassing van SOA en bijbehorende security issues
	- Beveiligingsbeleid
	- Beveiligingsorganisatie
	- Classificatie en beheer van bedrijfsmiddelen
	- Beveiligingseisen ten aanzien van personeel
	- Toegangsbeveiliging
	- Ontwikkeling en onderhoud van systemen
	- Incidentmanagement

	- Continuïteitsmanagement - Naleving - Compliant aan WBP

Tabel 1: Elementen aanwezig in de aspectscan.

Organisatiedoelstellingen met betrekking tot Security & Privacy	
Wat is het?	Elke organisatie heeft eigen doelstellingen. Deze doelstellingen staan vaak beschreven in de missie, visie en strategie van de onderneming. Ten aanzien van security en privacy moeten er ook doelstellingen geformuleerd zijn. Om deze organisatiedoelstellingen helder te formuleren kan gebruik gemaakt worden van COSO. COSO is een managementmodel dat een referentiekader biedt voor de interne controle en het beheersingssysteem van organisaties. Het is een bekend systeem bij auditors. COSO identificeert de relaties tussen de ondernemingsrisico's en het interne beheersingsysteem. COSO is gebaseerd op het verkrijgen van een redelijke mate van zekerheid (door het interne beheerssysteem) omtrent het bereiken van doelstellingen in verschillende categorieën.
Waarom is het belangrijk?	Doelstellingen op het gebied van security kunnen op verschillende gebieden liggen. Organisaties moeten bijvoorbeeld compliant zijn aan wet en regelgeving. De organisatie moet kunnen aangeven op welke wijze zij willen omgaan met security & privacy vraagstukken, zowel voor haar interne stakeholders als voor de betrokkenen uit het ecosysteem. Om de doelstellingen helder te omschrijven en van elkaar te scheiden is het belangrijk een methode hiervoor te gebruiken.
Hoe te meten?	- Er wordt een methode gebruikt voor het duidelijk omschrijven van de organisatiedoelstellingen betreffende security & privacy. - Er wordt een onderscheid gemaakt in diverse categorieën doelstellingen Een voorstel dat COSO hiervoor biedt is een opdeling in de volgende vier categorieën: - bereiken van de strategische doelstellingen (Strategic) - effectiviteit en efficiëntie van bedrijfprocessen (Operations) - betrouwbaarheid van de financiële informatieverzorging (Reporting) - Naleving van relevante wet- en regelgeving (Compliance)
Eisen voor principes	• PE1: Er zijn principes die de organisatiedoelstellingen behartigen van beleid tot en met controle.

Tabel 2: Organisatiedoelstellingen met betrekking tot security & privacy.

Risicomanagement	
Wat is het?	Het hanteren van een proces dat zorgt voor de continuering van het adresseren van risico's, het beheersen van risico's, reviewen en weer opnieuw adresseren van security risico's [BS99]. Figuur 8 illustreert dit proces.  Figuur 8: Risicomanagement proces [BS99] Het beschrijven van dit proces is één van de belangrijkste elementen op het gebied van security & privacy. Om voldoende aandacht te besteden aan elk proces worden de processen opgedeeld in vier subelementen. o Risicomanagement: Identificatie en evaluatie van risico's o risicomanagement: Behandeling van risico's o Risicomanagement: Monitoring en evaluatie van risico's o Risicomanagement: Evaluatie en aanpassing van controlemechanismen Deze gelaagdheid moet ook terugkomen in de architectuurdocumentatie. Risicobeheersende maatregelen moeten worden ondersteund door business principles of requirements.
Waarom is het belangrijk?	Het is belangrijk om risico's altijd in kaart te brengen. Risico's veranderen over de tijd. Er komen nieuwe risico's bij en oude risico's zijn in de toekomst wellicht minder van belang. Het zorgt voor awareness bij het vormen van security requirements en de noodzaak om controle mechanismen en poli-

	cies te implementeren.
Hoe te meten?	- Risico bepaling vindt plaats. Subprocessen in de risicobepaling worden beschreven. Deze subprocessen worden omschreven in het element Risicomanagement: Identificatie en evaluatie van risico's. - Controlemechanismen voor de risico's worden geselecteerd geïmplementeerd en uitgevoerd om bedreigingen en risico's te behandelen. Dit element wordt verder omschreven in het element Risicomanagement: Behandeling van risico's. - Risico's en controlemechanismen worden gemonitoord en geavaleerd. Dit element wordt omschreven in het element Risicomanagement: Monitoring van risico's en controlemechanismen. - Controlemechanismen worden geavaleerd en verbeterd. Dit element wordt omschreven in het element Risicomanagement: Evaluatie en aanpassing van controlemechanismen. - Er wordt een baseline security gegeven.
Eisen voor principes	• PE2 Op bedrijfsniveau worden principes geformuleerd die aangeven hoe de organisatie wenst om te gaan met risicomanagement. • PE3 De principes zijn gebaseerd op de requirements van de organisatie aangaande risicobeheersing. • PE4 Principe dat vastlegt dat security een integraal onderdeel is van de bedrijfsvoering.

Tabel 3: Risicomanagement.

Risicomanagement: Identificatie en evaluatie van risico's.	
Wat is het?	Identificatie en evaluatie van risico's tegen een vooraf bepaalde norm. Welke risico's zijn van belang en hebben invloed op de dagelijkse bedrijfsvoering. Noodzakelijk voor het identificeren van risico's is het bepalen van criteria voor risicoacceptatie. Welke risico's worden onder welke omstandigheden geaccepteerd. Hiervoor is het nodig te bepalen welk mate van risico geaccepteerd wordt. Dit is nodig om een juiste proportionaliteit van de risicobeheersing te bepalen. Bij de bepaling van de grote van het risico zijn twee zaken van belang. De waarschijnlijkheid van het risico en de impact die het risico heeft op de organisatie. De waarschijnlijkheid van een ontploffing van een kernreactor in de buurt van de organisatie is klein, de impact is echter zeer groot. De organisatie moet afwegen welke risico's geaccepteerd kunnen worden en welke risico's teruggedrongen moeten worden. Een juiste proportionaliteit van de risicobeheersing betekent dat de maatregelen die genomen worden in relatie staan tot de waarschijnlijkheid en de impact van het risico.

Waarom is het belangrijk?	De eerste stap in het risicomanagement proces is het identificeren van risico's. Een goede identificatie van risico's is noodzakelijk voor een goede bedrijfsvoering. Er moet bepaald worden welke assets van de organisatie belangrijk zijn om te beschermen en waar tegen ze beschermd moeten worden.
Hoe te meten?	• Risico bepaling vind plaats. Subprocessen in de risico bepaling worden beschreven. Subprocessen zijn: - Assets worden geïdentificeerd . - Business requirements die relevant zijn voor de assets worden geidentificeerd. - Er vindt een waardebepaling plaats van de assets met inachtneming van de business requirements voor de assets. Hierbij wordt rekening gehouden met de gewenste confidentialiteit, integriteit en beschikbaarheid van de asset. - Bedreigingen voor de asset worden vastgesteld. - De waarschijnlijkheid van de bedreigingen wordt vastgesteld. - Evaluatie van de risico's vindt plaats .
Eisen voor principes	• PE5 Risico's gerelateerd aan contact met externe partijen worden geïdentificeerd in de principes. • PE6 Fysieke en logische grenzen zijn vastgesteld in het security beleid. • PE7 Er zijn principes voor de identificatie van de relevante bedrijfsprocessen en het vastleggen van kritische niveaus van verstoring van die bedrijfsprocessen. • PE8 Principes die duidelijk maken wat de implicaties van de security maatregelen zijn (organisatorisch, technisch, menselijk). • PE9 Is er consistenties in de principes i.v.m. security (afstemming stakeholders, prioritering).

Tabel 4: Risicomanagement: Identificatie en evaluatie van risico's.

Risicomanagement: Behandeling van risico's	
Wat is het?	De tweede stap in het risicomanagement proces is het behandelen van de risico's door het implementeren van controlemechanismen. Dit is typisch gebaseerd op een concern van een stakeholder. Concerns van stakeholders komen voort uit bedreigingen en kansen. De stakeholder wenst dat het risico wordt behandeld om zodoende zijn concern af te dekken. De behandeling van de risico's geschiedt door het uitkie-

	zen en implementeren van geschikte maatregelen.
Waarom is het belangrijk?	Er zijn verschillende risico's die de dagelijkse bedrijfsvoering kunnen ondermijnen. Het is evident dat de organisatie deze risico's moet beheersen om zodoende deze bedrijfsvoering te beschermen. Bij de behandeling van risico's moet worden bepaald wat er beschermd moet worden in relatie tot de asset: de confidentialiteit, integriteit of de beschikbaarheid. Voor het bepalen van de juiste proportionaliteit moet worden bepaald hoe vaak het risico zich voordoet en wat de kosten en impact hiervan zijn op de organisatie.
Hoe te meten?	- Er moet worden bepaald hoe de organisatie met het risico wil omgaan. Hierbij zijn verschillende opties mogelijk. Het accepteren van het risico tot een bepaalde norm, het reduceren van het risico, het verplaatsen van het risico (bijvoorbeeld verzekeren) en het vermijden van het risico. - Controls voor de risico's worden geïmplementeerd. Deze controls zijn beschreven in de principes. Bij het selecteren van de controls wordt rekening gehouden met het gebruiksgemak van het controlemechanisme, betrouwbaarheid, herhaalbaarheid, sterkte en type control (preventie, detectie, recovery, correctie, monitoring of voorlichting (awareness) .
Eisen voor principes	• PE10 Principes hebben een juiste proportionaliteit. Ze staan in verhouding tot het concern. • PE11 Principes worden opgebouwd in verschillende fysieke en logische lagen (security in depth). • PE12 Principes staan niet op zichzelf maar hebben een onderlinge relatie. • PE13 Van elk principe dat een security maatregel voorstelt is duidelijk op welk gebied de maatregel wordt genomen (fysiek, organisatorisch, technisch of juridisch). • PE14 Bij de invoering van een principe zijn de kosten van de middelen niet hoger dan de mogelijke schade. • PE15 Principes houden rekening met single point of failures.

Tabel 5: Risicomanagement: Behandeling van risico's.

Risicomanagement: Monitoring van risico's en controlemechanismen	
Wat is het?	Nadat risico's zijn geïdentificeerd en controls zijn gekozen om deze risico's te beheersen zijn geïmplementeerd, worden de risico's gemonitoord.

Waarom is het belangrijk?	Monitoring van security controls vindt plaats om te controleren of de controls nog steeds correct en effectief functioneren. Monitoring van risico's vindt plaats om te controleren of risico's en toegewezen geïmplementeerde controls door verandering in het ecosysteem niet ineffectief zijn geworden. (BS ISO/IEC 27001:2005).
Hoe te meten?	- Activiteiten ten bate van de monitoring vinden op reguliere basis. - Logfiles worden gecontoleerd. - Controls, policies en procedures worden up to date gehouden met nieuwe versies.
Eisen voor principes	• PE16 Principes die monitoring en logging afdwingen.

Tabel 6 Risicomanagement: Monitoring van risico's en controlemechanismen.

Risicomanagement: Evaluatie en aanpassing van controlemechanismen	
Wat is het?	Het aanpassen van controlemechanismen wanneer deze ineffectief blijken te zijn.
Waarom is het belangrijk?	Wanneer controlemechanismen blijken inadequaat te werken moeten deze aangepast worden. Het telkens doorlopen van het risicomanagement proces zorgt ervoor dat risico's over de tijd geïdentificeerd zijn en dat maatregelen genomen worden.
Hoe te meten?	- Problemen in de controlemechanismen worden verbonden aan een oorzaak. - Er vindt controle plaats op het daadwerkelijk implementeren van de controlemechanismen. - Er worden preventieve maatregelen genomen zodat het problemen zich niet nogmaals voordoen. - Er wordt feedback gegeven op problemen met controlemechanismen. - Controlemechanismen worden aangepast wanneer nodig.
Eisen voor principes	• PE17 Principes die afdwingen dat van informatie periodiek (routinematig) het niveau, sensitiviteit en kritiekheid wordt bekeken en opgeslagen. • PE18 Principes die aangeven hoe er wordt geleerd van fouten.

Tabel 7: Risicomanagement: Evaluatie en aanpassing van controlemechanismen.

Toepassing van SOA en bijbehorende security issues	
Wat is het?	Dit element is alleen van toepassing wanneer er gebruik gemaakt wordt van een service georiënteerde architectuur. Het toepassen van SOA is een huidige best practise en wordt in veel architecturen toegepast. SOA brengt security issues met zich mee die gerelateerd kunnen worden aan deze aanpak.
Waarom is het belangrijk?	Bij het adopteren van een service georiënteerde aanpak komen nieuwe security vraagstukken naar boven. Zo moeten organisaties vaak veel transparanter worden omdat services diverse onderdelen van de organisatie moeten aanspreken. Dit is op zich geen extra risico maar vraagt wel om een security aanpak die meer geavanceerd is dan bij een traditionele architectuur. Zonder een SOA voert een medewerker zijn taken vaak uit binnen zijn eigen domein. Bij een SOA kan een bepaalde service over meerdere domeinen lopen. Bij het aanroepen van de service moet de aanroeper geautoriseerd worden om meerdere domeinen van de organisatie te kunnen aanspreken[GART06d]. De aanroeper is zelf geautoriseerd om de service aan te roepen. Binnen de service zijn echter weer autorisaties die te toegang tot een aangrenzende service reguleren. Bij het uitvoeren van een service worden verschillende entiteiten aan elkaar gekoppeld. Voor het uitgeven van een lening worden bijvoorbeeld kredietcontroles uitgevoerd en het betalingsgedrag gecontroleerd. De koppeling met andere services of diensten mag pas plaatsvinden wanneer de service wordt aangeroepen.
Hoe te meten?	- Er wordt beschreven welke authenticatie en authorisatie checks er zijn uitgevoerd alvorens een service wordt gestart. - Is beschreven welke andere services of entiteiten door de service worden aangeroepen. - Componenten mogen niet aan elkaar gekoppeld worden tot dat zij worden aangeroepen, daarom moeten de componenten afzonderlijk worden ontworpen zonder een affiniteit met een bepaalde afnemer of context.
Eisen aan principes	• PE19 Principes die vastleggen dat er gewerkt wordt met uniforme entiteiten (voor onweerlegbaarheid). • PE20 Principes die de herleidbaarheid van transacties afdwingen. • PE21 Security eisen afgedwongen in principes zijn door de gehele keten even sterk. De ketting is zo sterk als de zwakste schakel.

	• PE22 Principes die de authenticiteit van entiteiten door de gehele keten van services waarborgt.

Tabel 8: Toepassing van SOA en bijbehorende security issues.

Beveiligingsbeleid	
Wat is het?	In het beveiligingsbeleid wordt omschreven hoe men de bedrijfsbelangen nastreeft. Deze belangen worden gecontroleerd en aangestuurd vanuit het management. Het beleid beschrijft dus de strategie die gevoerd wordt aangaande security en privacy.
Waarom is het belangrijk?	Het beleid dat gevoerd wordt aangaande security en privacy moet bekend gemaakt worden. De architectuur moet hier namelijk op gebaseerd worden. Zonder een goede omschrijving zijn de security controls die geïmplementeerd worden niet gebaseerd op de wensen en eisen van de organisatie. De omschrijving van het beveiligingsbeleid is essentieel om security controls te kunnen implementeren die de bedrijfsbelangen ondersteunen.
Hoe te meten?	- In de architectuurdocumentatie is het beveiligingsbeleid opgenomen. - Security & privacy elementen zijn afgestemd op dit beleid.
Eisen voor principes	• PE23 Principes zijn afgestemd op het beveiligingsbeleid.

Tabel 9 Beveiligingsbeleid.

Beveiligingsorganisatie	
Wat is het?	De inrichting van de organisatie die er voor moet zorgen dat het beveiligingsbeleid wordt ondersteund. Dit door het inrichten van de organisatie met beveiligingsfuncties, taken en verantwoordelijkheden, coördinatie, samenhang, rapportagelijnen en autorisatieprocessen. Afspraken over samenwerking met derden worden expliciet gemaakt.
Waarom is het belangrijk?	In de architectuurdocumentatie moet vastgelegd worden wie waar verantwoordelijk voor is. De verantwoordelijke staat garant voor een correcte uitvoering van de security maatregelen die benoemd zijn.
Hoe te meten?	Het vastleggen van verantwoordelijkheden en de coördinatie tussen de verantwoordelijken met invulling van duidelijke rapportagelijnen. Activiteiten zijn onder andere: het organiseren van de implementatie van het

	security & privacy beleid, het toezicht houden op veranderende risico's, het opstellen van de uitwijkplannen, het reageren op eventuele incidenten en het organiseren van externe onafhankelijke beoordeling van de beveiliging. - De verantwoordelijkheden zijn vastgelegd (dit kan op dienstenniveau zijn maar ook op dataniveau of assets). - Het tijdelijke karakter van risico's en wensen en eisen aangaande security wordt onderkend. - Er wordt een security officer aangesteld. - Rapportagelijnen zijn vastgelegd. - Uitwijkplannen zijn vastgelegd. - Incidentmanagement, implementatiebeleid en andere aan security gerelateerde activiteiten zijn door de organisatie in kaart gebracht. - Voor elke dienst wordt een verantwoordelijke persoon aangesteld.
Eisen aan principes	• PE24 Voor elk principe wordt de eigenaar vastgelegd. • PE25 Voor elke asset wordt een asseteigenaar aangesteld. • PE26 Principes die vastleggen wie er controle uitoefent op het naleven van organisatiedoelstellingen en geformuleerde principes.

Tabel 10: Beveiligingsorganisatie.

Classificatie en beheer van bedrijfsmiddelen	
Wat is het?	Weten wat je in huis hebt door inzicht in de aanwezige bedrijfsmiddelen en hun verantwoordelijke 'eigenaar'. Gebruik van classificatieschema's voor informatie en systemen koppelt het belang van informatie en andere middelen aan specifieke beveiligingsmaatregelen.
Waarom is het belangrijk?	Beschreven moet worden waarom bepaalde assets belangrijk zijn om ze zodoende goed te kunnen beveiligen.
Hoe te meten?	- Belangrijke assets voor de organisatie worden onderkend en ge classificeert. - Van elk asset is duidelijk waar het tegen beschermd moet worden. - Voor elk asset is beschreven wat de eisen zijn aangaande confidentialiteit, integriteit en beschikbaarheid.

Eisen aan principes	• PE27 Principes die het veiligheidsniveau van de asset vaststellen. • PE28 Principes die de beschikbaarheid van assets moeten waarborgen. • PE29 Principes die de confidentialiteit van assets moeten waarborgen. • PE30 Principes die de integriteit van assets moeten waarborgen.

Tabel 11: Classificatie en beheer van bedrijfsmiddelen.

Beveiligingseisen ten aanzien van personeel	
Wat is het?	Niet alleen van buitenaf zijn er gevaren die de dagelijkse bedrijfsvoering kunnen ondermijnen. Vooral vanuit de interne organisatie zijn er bedreigingen, bijvoorbeeld van het eigen personeel. Dit is niet iets typisch wat in architectuurdocumentatie wordt beschreven maar moet toch in enige mate worden geadresseerd. Hierbij kan gedacht worden aan het verdelen van autorisaties. Wie is er verantwoordelijk voor dit beleid. Social engineering is tegenwoordig een veelgebruikt middel om toegang te krijgen tot bedrijfsgevoelige informatie. Wanneer architectuur vooral een technische aangelegenheid is worden deze bedreigingen vergeten. Mochten er zich problemen voordoen (bijvoorbeeld een mislukte autorisatie) moet het personeel weten hoe te handelen.
Waarom is het belangrijk?	Succesvolle informatiebeveiliging begint bij betrouwbaar, zorgvuldig en goed opgeleid personeel. Daarvoor is nodig: training, security awareness, veilig gedrag op de werkvloer, aannamebeleid en functioneringsbeoordeling. Personeel moet weten hoe te reageren op beveiligingsincidenten.
Hoe te meten?	- Er wordt onderkend dat niet alleen technische issues relevant zijn in het beveiligingsbeleid. - Personeel weet waar men security incidenten kan rapporteren. - Er is een CERT team geïnstalleerd. - Er wordt vastgelegd hoe gecontroleerd wordt op het handelen van eigen werknemers (met in achtneming van WBP) - Toekenning van verantwoordelijkheden worden duidelijk gedefinieerd, ondersteund en erkend.
Eisen aan principes	• PE31 Principes die het melden van een incident verplichten. • PE32 Principes die aangeven hoe wordt omgegaan met de persoonlijke levenssfeer van het eigen personeel bij eventuele controles.

Tabel 12 Beveiligingseisen ten aanzien van personeel.

Toegangsbeveiliging	
Wat is het?	De toegang tot informatie en IT-middelen wordt op bedrijfsmatige overwegingen gebaseerd. Dit vraagt om een autorisatieproces voor toegang tot informatie en IT-middelen. De uitgegeven autorisaties worden procesmatig onderhouden, bewaakt en eventueel weer ingetrokken.
Waarom is het belangrijk?	Toegangsbeveiliging is één van de eerste stappen om informatie confidentieel, integer en beschikbaar te houden. Het moet duidelijk zijn wie, wanneer en waarom toegang mag hebben tot bepaalde assets die geadresseerd zijn. Vanwege functie promotie, degradatie, wisseling en uittreding kunnen autorisaties veranderen. Het proces van uitgeven en intrekken van autorisaties moet op een geordende manier verlopen, dit kan middels een geautomatiseerd autorisatieproces. Voor het uitgeven van rechten aan functies(rollen) is een best practise beschikbaar, namelijk Role Based Access Control. Er zijn extra aandachtspunten bij het verdelen van rechten. Hoe is de afstemming tussen verantwoordelijkheden en bevoegdheden? De mate van verschil in directe afstemming hiertussen bepaalt de flexibiliteit van de organisatie. Idealiter zou deze afstemming 100% zijn, iedereen mag alleen doen wat hij moet doen. De klant is hier echter niet altijd mee gebaard. Iedereen kent het gevoel van het kastje naar de muur gestuurd te worden door een callcenter agent met het antwoord "dat mag ik niet regelen, daarvoor moet u een andere afdeling hebben". Vanuit security oogpunt wordt er uitgegaan van een één op één afstemming van verantwoordelijkheden en bevoegdheden echter moet dit wel in het oogpunt van de klant worden opgesteld.
Hoe te meten?	- Autorisaties worden goedgekeurd door een vooraf geïdentificeerde hiërarchie van functies. - Autorisaties worden regelmatig gecontroleerd op hun rechtsgeldigheid. - Niet geslaagde autorisaties worden gelogd. - Er is transparantie in autorisatieniveaus. Het is duidelijk wie wat wel en niet mag. - Identity management wordt beschreven. - Toekenning van verantwoordelijkheden worden duidelijk gedefinieerd, ondersteund en erkend. - Er wordt gebruik gemaakt van single sign on (huidige best practise op dit gebied)

Eisen aan principes	• PE33 Er wordt gebruik gemaakt van RBAC wanneer rechten aan rollen gekoppeld worden. • PE34 Rechten worden uitgedeeld op basis van 'need to know'. • PE35 Principes die vastleggen dat er gewerkt wordt met uniforme entiteiten (voor onweerlegbaarheid). • PE36 Principes die vastleggen hoe de authenticiteit vastgelegd wordt van entiteiten. • PE37 Principes die vastleggen hoe autorisaties worden verleend aan de hand van een bekende authenticiteit. • PE38 Authenticatie en authorisatie van gebruikers en processen om toegangscontrole te waarborgen wordt zowel binnen als buiten de domeinen toegepast. • PE49 Principes die de mate van toegang tot assets (high confidential, staatsgeheim) bepalen. • PE40 Principe dat vertelt of en hoe wordt omgegaan met single sign on.

Tabel 13: Toegangsbeveiliging.

Ontwikkeling en onderhoud van systemen	
Wat is het?	Architectuurdocumentatie geeft onder andere een handleiding over hoe systemen er uit gaan zien op basis van de geschetste architectuur. De architectuur heeft een grote invloed op de te ontwikkelen systemen. In dit element wordt vooral beschreven wat de impact is van security gerelateerde principes op de ontwikkeling van toekomstige systemen.
Waarom is het belangrijk?	Aandacht voor de nodige beveiligingsfunctionaliteit en veilige ontwikkel- en onderhoudsmethoden leiden tot veilige systemen, die ook veilig blijven (change management). Een huidige ontwikkeling is dat systemen mobiel moeten zijn. Werknemers willen overal en op elk tijdstip toegang tot bedrijfsinformatie. Systemen worden toegankelijk gemaakt via het internet of informatie wordt op laptops of usb sticks mee naar huis genomen. Binnen de architectuurdocumentatie moet beschreven zijn hoe de organisatie omgaat met mobility issues. Aan het openstellen van systemen zitten namelijk grote risico's. Het openstellen van informatiesystemen biedt extra mogelijkheden om in te breken maar het alternatief (niets doen) leidt tot een ongeleid projectiel (usb sticks in het nieuws). De architectuurdocumentatie moet beschrijven hoe de organisatie hier mee om

	wilt gaan.
Hoe te meten?	- De potentiële impact op de gedeelde infrastructuur, internet, publiekelijk verbonden netwerken en andere verbonden systemen bij de implementatie van netwerk security maatregelen is bekend. - Security wordt ook gewaarborgd bij het buiten werking stellen of verwijderen van een systeem. - Voor alle principes, requirements en voorstellen is duidelijk hoe deze invloed uitoefenen op ontwikkeling van informatiesystemen.
Eisen aan principes	• PE41 Principes die te maken hebben met de bereikbaarheid van systemen houden rekening met mobiliteit en de gevaren hiervan.

Tabel 14: Ontwikkeling en onderhoud van systemen.

Incidentmanagement	
Wat is het?	Het vastleggen van incidenten die plaatsvinden.
Waarom is het belangrijk?	Hoe veilig systemen ook gebouwd worden er zullen altijd incidenten plaats blijven vinden. Wanneer er aanval zou plaatsvinden die mislukt, is het belangrijk dit op te merken zodat controlemechanismen hierop aangescherpt kunnen worden.
Hoe te meten?	- Audit mechanism zijn aanwezig om niet-geautoriseerd gebruik te detecteren en incidentonderzoek te ondersteunen. - De relatie tussen incidenten wordt vastgelegd.
Eisen aan principes	• PE42 Er zijn principes die de detectie van serieuze afwijkingen van de normale bedrijfsvoering afdwingen. • PE43 Voor de principes is vastgelegd hoe incidenten worden vastgelegd en gerapporteerd.

Tabel 15: Incidentmanagement.

Continuïteitsmanagement	
Wat is het?	Het waarborgen van de continuïteit van de dagelijkse bedrijfsvoering. Wanneer er onverhoopt incidenten plaatsvinden die deze bedrijfsvoering in gevaar brengen zorgt een goed management er voor dat de

	dagelijkse gang van zaken doorgang kan vinden.
Waarom is het belangrijk?	Een calamiteit hoeft nog geen ramp te worden indien vooraf is nagedacht over de eisen aan continuïteit en er een proces is voor continuïteitsborging inclusief calamiteitenopvang, rampenplannen en (geoefende) uitwijk.
Hoe te meten?	- Er is een calamiteitenplan vastgelegd of er wordt een calamiteitenplan verplicht gesteld. - Kritieke processen voor de organisatie worden benoemd. - Uitwijkmogelijkheden worden geboden.
Eisen aan principes	• PE44 Bij uitval van systeemonderdelen is er een uitwijkmogelijkheid. Principes leggen vast welke uitwijkmogelijkheden er zijn (bijvoorbeeld verschillende authenticatiemogelijkheden) • PE45 Principes die vastleggen hoe wordt omgegaan met rampen en ernstige verstoringen.

Tabel 16 Continuïteitsmanagement.

Naleving	
Wat is het?	Door middel van auditing en andere vormen van toezicht wordt inzicht verkregen in het halen van de security & privacy doelstellingen uit het beleid en de realisatie van de afspraken. Ook is er aandacht voor de naleving van wettelijke en contractuele voorschriften, beveiligingscontrole op IT systemen, IT-audit en interne controle.
Waarom is het belangrijk?	Er moet op regelmatige basis gecontroleerd worden of de doelstellingen van de organisaties wel gehaald worden.
Hoe te meten?	- Er worden IT audits georganiseerd - Er vindt interne controle plaats op mensen, middelen en systemen.
Eisen aan principes	• PE46 Principe dat vastlegt dat security incidenten worden gesignaleerd, vastgelegd, verwerkt en gerapporteerd. (het principe moet ook verwoorden wat een incident is, bij een keten dus ook weer de verantwoordelijke aanwijzen.)

Tabel 17: Naleving.

Compliant aan WBP	
Wat is het?	WBP staat voor wet bescherming persoonsgegevens en is een Nederlandse wet die de privacy van burgers moet beschermen.
Waarom is het belangrijk?	Bijna elke Nederlandse onderneming moet voldoen aan deze wet en daarom is het verplicht in elke architectuurdocumentatie te identificeren hoe de onderneming deze wet nastreeft. Een aantal organisaties hoeft niet te voldoen aan deze wetgeving. Denk hierbij aan bijvoorbeeld de algemene inlichtingen en veiligheidsdienst (AIVD). Dit aspect is daarom alleen van toepassing op organisaties die zich aan deze wet en regelgeving dienen te houden.
Hoe te meten?	- De onderneming heeft in kaart gebracht op welke plaatsen zij welke persoonsgegevens voor welk doel verwerkt en heeft dit op de juiste plaatsen geregistreerd. - De onderneming ziet er op toe dat er een expliciete en rechtmatige grondslag bestaat voor alle persoonsgegevens die zij (verzamelt en) verwerkt. - De onderneming draagt zorg dat zij niet meer persoonsgegevens verwerkt dan zij voor de (onderkende en rechtmatig geachte) doelen nodig heeft. - De onderneming heeft deze persoonsgegevens adequaat beveiligd. - De onderneming biedt de noodzakelijke voorzieningen voor inzage en eventuele correctie van de persoonsgegevens die zij verwerkt. - De onderneming houdt nauwgezet bij aan welke derden zij de persoonsgegevens eventueel verstrekt. - De onderneming legt over de gehele beheersing van persoonsgegevens verantwoording af.
Eisen aan principes	• PE47 Principes die te maken hebben met de opslag van persoonlijke gegevens voldoen aan bovenstaande indicatoren. • PE48 Principe dat waarborgt of de organisatie voldoet aan nationale wet en regelgeving. (in nl is dit dus de WBP) • PE49 Principe dat vastlegt aan wie informatie wordt verschaft betreffende gegevens van een individu of organisatie. • PE50 Principes die vastleggen welke technologieën gebruikt worden om privacy te waarborgen (Best practise: PET)

Tabel 18 Compliant aan WBP.

Fase 3: Principe-eisen vastgelegd in het EISA raamwerk

Voor alle principe eisen is vastgelegd in welke architectuurlaag deze principes voorkomen. Naast de plaatsing van principe eisen in de architectuurlagen wordt ook vastgelegd welke security views er gevormd kunnen worden. Van elk principe wordt vastgelegd welke views er van toepassing kunnen zijn op de principe eis. In hoofdstuk 5, paragraaf 'fase3: principes geordend in EISA raamwerk' zijn deze views onderkend. De plaatsing van de principes en de gekozen viewpoints zijn vastgelegd in tabel 19.

PE	Principe-eisen aspectscan security & privacy	Arch. laag			View-points			Werkt door op		
		Conceptual	Logical	Implementation	Business	Information	Technical	Logical	Implementation	Werkt niet door
1	Er zijn principes die de organisatiedoelstellingen behartigen van beleid tot en met controle.	x			x	x	x	x	x	
2	Op bedrijfsniveau worden principes geformuleerd die aangeven hoe de organisatie wenst om te gaan met risicomanagement.	x			x	x				x
3	De principes zijn gebaseerd op requirements van de organisatie aangaande risicobeheersing.		x		x	x			x	
4	Principe dat vastlegt dat security een integraal onderdeel is van de bedrijfsvoering.	x			x					x
5	Risico's gerelateerd aan contact met externe partijen worden geïdentificeerd in de principes.	x			x	x				x
6	Fysieke en logische grenzen zijn vastgesteld in het security beleid.		x			x			x	
7	Er zijn principes voor de identificatie van de relevante bedrijfsprocessen en het vastleggen van kritische niveaus van verstoring van die bedrijfsprocessen.	x			x	x				x
8	Principes die duidelijk maken wat de implicaties van de security maatregelen zijn (organisatorisch, technisch, menselijk).			x	x	x	x			x
9	Is er consistenties in de principes i.v.m. security (afstemming stakeholders, prioritering).	x			x	x				x
10	Principes hebben een juiste proportionaliteit. Ze staan in verhouding tot het concern.		x		x		x			x
11	Principes worden opgebouwd in verschillende fysieke en logische			x			x			x

	lagen (security in depth).										
		Conceptual	Logical	Implementation	Business	Information	Technical	Logical	Implementation	Werkt niet door	
12	Principes staan niet op zichzelf maar hebben een onderlinge relatie.		x			x				x	
13	Van elk principe dat een securitymaatregel voorstelt is duidelijk op welk gebied de maatregel wordt genomen (fysiek, organisatorisch, technisch of juridisch).		x		x	x	x			x	
14	Bij de invoering van een principe zijn de kosten van de middelen niet hoger dan de mogelijke schade.	x			x			x	x		
15	Principes houden rekening met single point of failures			x			x			x	
16	Principes die monitoring en logging afdwingen.			x		x	x			x	
17	Principes die afdwingen dat van informatie periodiek (routinematig) het niveau, sensitiviteit en kritiekheid wordt bekeken en opgeslagen.		x		x	x			x		
18	Principes die aangeven hoe er wordt geleerd van fouten.	x			x					x	
19	Principes die vastleggen dat er gewerkt wordt met uniforme entiteiten (voor onweerlegbaarheid).		x			x	x		x		
20	Principes die de herleidbaarheid van transacties afdwingen.		x			x	x		x		
21	Security eisen afgedwongen in principes zijn door de gehele keten even sterk. De ketting is zo sterk als de zwakste schakel.	x			x	x	x	x	x		
22	Principes die de authenticiteit van entiteiten door de gehele keten van services waarborgt.		x			x	x		x		
23	Principes zijn afgestemd op het beveiligingsbeleid.	x			x					x	
24	Voor elk principe wordt de eigenaar vastgelegd.		x		x	x				x	
25	Voor elke asset wordt een asseteigenaar aangesteld.		x		x	x				x	
26	Principes die vastleggen wie er controle uitoefent op het naleven van organisatiedoelstellingen en geformuleerde principes.	x			x	x				x	
27	Principes die vastleggen dat er gewerkt wordt met uniforme entiteiten (voor onweerlegbaarheid).		x			x	x		x		
28	Principes die het veiligheidsniveau van de asset vaststellen.		x		x	x				x	

		Conceptual	Logical	Implementation	Business	Information	Technical	Logical	Implementation	Werkt niet door
29	Principes die de beschikbaarheid van assets moeten waarborgen.		x		x	x				x
30	Principes die de confidentialiteit van assets moeten waarborgen.		x		x	x				x
31	Principes die de integriteit van assets moeten waarborgen.		x		x	x				x
32	Principes die het melden van een incident verplichten.	x			x	x		x		
33	Principes die aangeven hoe wordt omgegaan met de persoonlijke levenssfeer van het eigen personeel bij eventuele controles.	x			x	x				x
34	Er wordt gebruik gemaakt van RBAC wanneer rechten aan rollen gekoppeld worden.			x			x			x
35	Rechten worden uitgedeeld op basis van 'need to know'.	x				x		x	x	
36	Principes die vastleggen hoe de authenticiteit vastgelegd wordt van entiteiten.		x			x	x		x	
37	Principes die vastleggen hoe autorisaties worden verleend aan de hand van een bekende authenticiteit.		x			x	x		x	
38	Authenticatie en authorisatie van gebruikers en processen om toegangscontrole te waarborgen wordt zowel binnen als buiten de domeinen toegepast.	x			x	x	x	x	x	
39	Principes die de mate van toegang tot assets (high confidential, staatsgeheim) bepalen.	x			x	x				x
40	Principe dat vertelt of en hoe wordt omgegaan met single sign on.			x			x			x
41	Principes die te maken hebben met de bereikbaarheid van systemen houden rekening met mobiliteit en de gevaren hiervan.	x			x		x		x	
42	Er zijn principes die de detectie van serieuze afwijkingen van de normale bedrijfsvoering afdwingen.	x			x		x			x
43	Voor de principes is vastgelegd hoe incidenten worden vastgelegd en gerapporteerd.		x			x				x
44	Bij uitval van systeemonderdelen is er een uitwijkmogelijkheid. Principe legt vast welke uitwijkmogelijkheden er zijn (bijvoorbeeld verschillende authenticatiemogelijkheden).	x					x	x	x	
45	Principes die vastleggen hoe wordt omgegaan met rampen en ernsti-	x			x	x	x			x

	ge verstoringen.										
		Conceptual	Logical	Implementation	Business	Information	Technical	Logical	Implementation	Werkt niet door	
46	Principe dat vastlegt dat security incidenten worden gesignaleerd, vastgelegd, verwerkt en gerapporteerd. (het principe moet ook verwoorden wat een incident is, bij een keten dus ook weer de verantwoordelijke aanwijzen.)	x				x				x	
47	Principes die te maken hebben met de opslag van persoonlijke gegevens voldoen aan indicatoren van het element WBP.	x				x	x	x	x		
48	Principe dat waarborgt of de organisatie voldoet aan nationale wet en regelgeving. (in nl is dit dus de WBP)	x			x	x	x	x	x		
49	Principe dat vastlegt aan wie informatie wordt verschaft betreffende gegevens van een individu of organisatie.		x			x				x	
50	Principes die vastleggen welke technologieën gebruikt worden om privacy te waarborgen. (Best practise: PET)			x			x			x	

Tabel 19: Plaatsing Principe-eisen in EISA raamwerk.

5. Validiteit en toegevoegde waarde van de methode

Voor dit onderdeel wordt verwezen naar de ADEM waarin de schaalbaarheid wordt uitgelegd. De flexibiliteit van de norm is een belangrijk punt voor de aspectscan. Deze flexibiliteit is er, de norm kan aangepast worden aan voortschrijdend inzicht en nieuwe ontwikkeling in de markt. De aspectscan voldoet ook aan de eisen die er gesteld zijn in de ADEM en daarmee is de validiteit van de methode gewaarborgd.

Wat betreft security & privacy is er gekozen om geen stelling in te nemen bij de keuze voor technieken. Het gaat vooral om de onderbouwde keuze. Architectuurprincipes moeten beschrijven dat de architect aan bepaalde security & privacy elementen gedacht heeft tijdens het opstellen van de architectuur. In het geval dat er een best practise bestaat waarin een bepaalde techniek als expliciet beter wordt beschouwd dan een andere techniek is dit meegenomen in dit onderzoek. In de meeste gevallen is dit echter niet expliciet beschreven. Een 512bits sleutel is 'veiliger' dan een 64 bits sleutel. Een kortere sleutellengte is echter in sommige situaties wenselijk. Waar een organisatie aangeeft dat zij met encryptie willen werken om hun uiterst confidentiële informatie of bijvoorbeeld klantgegevens veilig te stellen is dit wel een probleem.

7. Toekomstig onderzoek

Digitale architectuur is een groeiend vakgebied en zal continu blijven veranderen om aan de wensen van de huidige markt te kunnen blijven voldoen. Het service georiënteerd denken is hier een voorbeeld van. Deze vorm van architectuur wordt pas sinds enkele jaren toegepast in het bedrijfsleven. De wetenschap moet hierop in spelen. In deze aspectscan is hier rekening mee gehouden. Momenteel is SOA een best practise en wordt door veel organisaties toegepast. Dit element is daarom opgenomen in de norm van de aspectscan. Toekomstig onderzoek moet uitwijzen of deze normen veranderen. Daarbij is het niet de vraag of de norm zal veranderen maar wanneer. Daarom worden experts uitgedaagd deze norm te blijven verbeteren zodat deze aspectscan up to date blijft en toegepast kan blijven worden op de architectuurdocumentatie van de toekomst.

De subtitel van deze scriptie luidt 'Aanzet tot een methode om architectuurdocumentatie te evalueren'. De titel geeft hiermee aan dat het werk nog niet compleet is. Het kunnen evalueren van architectuurdocumentatie is erg complex en daarbinnen kan aan het evalueren van security & privacy al een heel afstudeeronderzoek worden besteed. Met deze aspectscan is een aanzet gemaakt waarin de meeste beste practises en officiële normen zijn verwerkt. Het kan echter zijn dat deze lijst niet geheel compleet is en dat een bedrijf zelf specifieke wensen heeft aangaande security & privacy. De scan is zo opgezet dat deze op veel branches van toepassing is. Aangaande compliancy zijn er voor speciale branches zoals de zorg aparte normen opgesteld. Het is dus mogelijk dat er een aparte versie van deze aspectscan ontwikkeld wordt die speciaal toepasbaar is voor de zorgsector.

8. Reflectie

Deze reflectie behandelt mijn persoonlijke visie op het werk dat geleverd is tijdens het voorafgaande onderzoek en het werk dat geleverd is voor deze aspectscan. Als eerste wordt op het proces en de leermomenten gereflecteerd om vervolgens het product zelf nader te beschouwen. De ambitie voor dit onderzoek werd al meteen bij de opdrachtomschrijving duidelijk. Toen ik met dit onderzoek begon wist ik dat het een hoop werk zou gaan worden. Het zou echter ook veel mogelijkheden bieden. Het onderzoek dat uitgevoerd is wordt door de universiteit ondersteund en er zijn plannen om dit werk voort te zetten. Het onderzoek behelst vraagstukken die voor de maatschappij belangrijk zijn. Een zekere mate van interesse uit de publieke opinie en het bedrijfsleven kan dus verwacht worden. Ik heb de mogelijkheid gehad om met veel autoriteiten op dit vakgebied te spreken. Dit was een hele ervaring en ik heb daar dan ook zeer veel van geleerd.

Het was een hele ervaring om met zes studenten een onderzoek uit te voeren. Bij mij weten is dit uniek binnen de universiteit. Dit betekende ook dat wij niet terug konden vallen op ervaringen van anderen. De combinatie die wij zijn aangegaan was nieuw en hoe hiermee om te gaan hebben wij aan den lijve moeten ondervinden. Vooral binnen de architectuurwereld zijn personen eigengereid. Wij als mogelijk toekomstige architecten hebben ook bepaalde karaktertrekjes waarmee binnen een groep moeilijk om te springen is. Het is ons toch gelukt om een bepaalde groepscohesie te kunnen vormen, al hoewel niet iedereen het daar volledig mee eens zal zijn. Bij het werken in een groep waarin iedereen een erg expliciete mening heeft is het moeilijk compromissen te sluiten. Dit resulteerde dan ook vaak in hevige discussies. Ik ben echter van mening dat deze discussies de kwaliteit van het werk alleen maar positief beïnvloed hebben. Ideeën die er waren over het werk moesten eerst binnen de groep besproken worden. Over elk idee en concept in de ADEM heeft dus eerst een interne controleslag plaatsgevonden.

Het product dat wij gezamenlijk hebben bewerkstelligd mag er best zijn. Natuurlijk zijn er aanvullingen te bedenken en is de methode aan te scherpen. De fundamentele ideeën achter het evaluatieproces staan echter als een huis. Er is op een wetenschappelijke wijze gekeken naar digitale architectuur als geheel. Binnen de architectuur zijn verschillende stromingen onderkend. Zo is er het architectuurproces, de architectuurdocumentatie en zijn er architectuurimplementaties. Binnen dit onderzoek is er voor gekozen de architectuurdocumentatie te evalueren. Architectuurdocumentatie is zonder andere resources te evalueren. De evaluator hoeft daarbij geen interviews af te leggen om bepaalde beslissingen te achterhalen. Bij de bepaling van de norm is er niet alleen gekeken naar de praktijk maar vooral ook naar wetenschappelijke contributies in het vakgebied. Uit diverse papers is een norm opgesteld waar in de theorie een bepaalde mate van consensus over is bereikt. Zo spreken de meeste papers over de aanwezigheid van stakeholders en architectuurprincipes[GART06][IEEE1471][RIJS05].

Belangrijke items in architectuur zijn het proces, de documentatie en de implementatie. Volgens sommige praktijkmensen kan dit niet gescheiden worden maar wij hebben bewezen dat dit zeker wel mogelijk is. In de diverse gesprekken met deskundigen hebben wij een soort common sense weten te abstraheren over de inhoud van architectuurdocumentatie. Dit heeft geleid in de benoeming van de elementen. Een goede verdeling die in de praktijd vaak toegepast wordt is een verdeling in verplichte, gewenste en optionele elementen. Over de inhoud van de indicatoren kan gespeculeerd worden. Dit is echter zeker niet het belangrijkste issue binnen het onderzoek. Indicatoren kunnen gewijzigd worden, de methode staat. Dit zelfde geldt voor de aspectscan.

Het is niet gemakkelijk om security en privacy te evalueren. Er is veel kennis en kunde op dit vakgebied maar een structuur ontbreekt. Er zijn technische maatregelen maar ook organisatorische maatregelen. Wat goede en slechte maatregelen zijn is ook onduidelijk. Een security control kan in de ene organisatie wel goed werken en in een andere organisatie met een andere context desastreus zijn. Om dit te bepalen moet de context van de organisatie meegenomen worden. In architectuurdocumentatie ontbreekt vaak een goede contextomschrijving. Wat wel geëvalueerd kan worden is of men over de security controls heeft nagedacht. Als regel in de ADEM is opgenomen dat een architectuur principe een rationale moet hebben. De rationale vertelt iets over de totstandkoming van het principe. De doelstelling is daarom ook om met deze scan inzicht te geven. De organisatie moet zelf zijn eigen oplossing bedenken. Een evaluator kan aangeven waar hiaten zitten en waar conflicterende principes voor problemen kunnen zorgen.

Over zowel de ADEM en de aspectscan ben ik erg tevreden. Het heeft een hoop werk gekost en de ideeën er achter zijn vaak besproken en overdacht. De processen van de voorbereidende scan, de holistische scan en de aspectfasen vullen elkaar goed aan en zorgen voor een totale dekking. Terugkijkend op het onderzoek is er veel tijd verloren gegaan aan oplossingen die niet bleken te werken. Daar is echter lering uit getrokken en er is een oplossing gevonden waar mee gewerkt kan worden. De methode is getest in de praktijk en wij hebben met het evalueren van de NORA geen moeite gehad met het uitvoeren van de concepten in de ADEM. Ook de aspectscan is goed te doen. Dit blijkt uit de vele bevindingen die naar boven zijn gekomen waar het ICTU mee aan de slag kan. Ook geven de resultaten van het onderzoek nieuwe input voor discussies die geleid kunnen worden door expertverenigingen zoals het GvIB14 en PI15.

[14] http://www.gvib.nl/ Op deze pagina is een speciale discussie betreffende security & privacy in de NORA.

[15] http://www.platforminformatiebeveiliging.nl/index.php

Literatuurlijst

[BLUM05] Blum, D. Security and Risk Management Strategies Reference Architecture Principles, Burton Group, januari 2005

[BON06] Bongers, L. Security binnen enterprise architectuur. Scriptie, februari 2006 . www.cs.ru.nl/onderwijs/afstudereninfo/scripties/2006/LucienBongersScriptie.pdf

[BS99] BS 7799-1:1999 Information security management, Code of practice for information security management, British Standards, 1999

[ELS03] Elsinga, B. Hofman, A. Security Principles, pattern paper ingestuurd voor EuroPlop 2003

[GART06] Lapkin, A. *Gartner Defines the Term 'Enterprise Architecture'*. Gartner. ID Number: G00128285, 2006

[GART06a] Kreizman, G. Robertson, B. Integrating Security Into the Enterprise Architecture Framework. Gartner. ID Number: G00137069, 2006

[GART06b] Scholtz, T. Structure and Content of an Enterprise Information. Gartner. ID Number: G00136867, 2006

[GART06c] Kreizman, G. Robertson, B. Integrating Security Into the Enterprise Architecture Process. Gartner. ID Number: G00137028, 2006

[GART06d] MacDonald, N. Achieving Agility: Building Blocks for a Policy-Driven, Agile Security Services Infrastructure. ID Number: G00137977, 2006

[GASSP] International Information Security Foundation, GASSP (Generally Accepted System Security Principles), juni 1999

[HOF04] Hofman, A. Inbouwen in plaats van aanbouwen, Artikel in het tijdschrift 'Informatiebeveiliging', mei 2004

[IAF99] Goedvolk, H. Rijsenbrij D.B.B. (1999) . White Paper Integrated Architecture Framework, version 1.0.

[IEEE1741] *Recommended Practice for Architectural Description of Software Intensive Systems*, Technical Report IEEE P1471-2000, The Architecture Working Group of the Software Engineering Committee, Standards Department, IEEE, Piscataway, New Jersey, USA, September 2000

[ISA07] ISACA, COBIT Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition, 2007

[ISO91] ISO/IEC IS 9126, Information Technology—Software Product Evaluation: Quality Characteristics and Guidelines for Their Use, Geneva, ISO, 1991

[ISO02] NEN-ISO/IEC 15816:2002 en Information technology - Security techniques - Security information objects for access control, Geneva, 2002

[ISO05a] ISO/IEC 17799:2005. Information Technology-Security Techniques-Code of Practice for Information Security Management. International Standards Organization, Geneva, 2005

[ISO05b] ISO/IEC 27001:2005. Information Technology-Security Techniques-Code of Practice for Information Security Management systems- Requirments. International Standards Organization, Geneva, 2005

[NEN04] Normcommissie 303 001, NEN 7510 Informatiebeveiliging in de zorg – Algemeen, april 2004

[OVER99] Overbeek, P. Sipman, W. Informatiebeveiliging, 2e druk, Tu-tein Nolthenius, september 1999

[RIJS05] Rijsenbrij, D.D.B. (2005). Architectuur *in de digitale wereld, Syllabus: Inleiding in de Digitale Architectuur*. http://www.digital-architecture.net/collegedictaat.htm

[SHER05] Sherwood, J. Clark, A. Lynas, D. Enterprise Security Architecture: A Business-Driven Approach. CMP Books, Computer Security Institute, San Francisco, 2005. ISBN 1-57820-318-X.

[SNEL05] Snel, B. Informatie Beveiliging Opzet & Bewustzijn, Siemens whitepaper, juni 2005

[STONE] Stoneburner, G. Hayden, C. Feringa, A. Engineering Principles for Information Technology Security (A Baseline for Achieving Security), NIST Special Publication 800-27 Rev A.

[WBP00] Nederlandse Overheid. Wet bescherming persoonsgegevens. 's-Gravenhage, 6 juli 2000

Woordenlijst

Architectuur
Een consistente, coherente verzameling van architectuurprincipes, verbijzonderd naar regels, richtlijnen en standaarden [RIJS05].

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. De architectuurdocumentatie moet compleet genoeg zijn om een implementatie te kunnen uitvoeren gebaseerd op de beschreven informatie.

Architectuurimplementatie
De verzameling van artefacten en hun samenhang die gebaseerd zijn op de architectuurdocumentatie. Architectuur wordt moet uiteindelijk gebouwd kunnen worden op basis ban de architectuurdocumentatie.

Architectuurrationale
De beslissingen en gedachtegangen die de afleiding vanuit onder andere stakeholder concerns, missie, visie en strategie en bedrijfsdoelstellingen naar de opgestelde architectuur verantwoorden. De rationale is opgenomen in de architectuurdocumentatie.

Architectuurontwikkeling
De combinatie van het architectuurontwikkelproces en de architectuurontwikkeldocumentatie.

Architectuurontwikkelproces
Het gevolgde proces voor het ontwikkelen van een architectuur, ook bekend als *architecting*.

Architectuurontwikkeldocumentatie
De documenten die het verslag bevatten van het architectuurontwikkelproces, zoals notulen en prototypen.

Architectuurprincipes
Richtinggevende uitspraken die de essentie van de architectuur vormen en die de ontwerpruimte voor de architectuurimplementatie inperken. Deze principes moeten eenduidig en ondubbelzinnig geformuleerd zijn zodat ze ieder minimaal een specifiek stakeholder concern bedienen.

Architectuurgedachtegoed
De verzameling van alle gemeenschappelijke ideeën, gedachtegangen en theorieën op het gebied van architectuur. Vaak worden deze zaken gevat in een architectuurraamwerk.

Aspect
Een bepaald aandachtsgebied binnen de architectuurdocumentatie dat relevant of interessant is voor een organisatie.

Aspectscan
De evaluatie van een aspect middels een vooraf gedefinieerde norm.

Asset
Een tastbaar of ontastbaar goed waar de organisatie waarde aan hecht. Dit kunnen zowel diensten, informatie, mensen en producten zijn.

Authenticatie
Middels authenticatie wordt bewezen wie of wat iemand is. Dit kan typisch op drie manieren bewezen worden. Iets tonen wat je hebt(pas), iets dat je weet(pin), of iets dat je bent(biometrie)

Evaluatieraamwerk
Een raamwerk dat ontwikkeld is om de kwaliteit van architecturen te kunnen bepalen aan de hand van een vooraf opgestelde norm.

Documentatie
Een verzameling van geschreven documenten, afbeeldingen, schema's en overzichten over een bepaald onderwerp.

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.

Proces
Een verzameling van taken, uitgevoerd in een specifieke volgorde om een specifiek doel te bereiken.

Referentiearchitectuur
Abstracte architecturen die gebruikt worden als referentie door organisaties die een op maat gesneden architectuur willen ontwikkelen voor een specifieke organisatie of afdeling.

Bijlage 1: Uitvoering aspectscan

Architectuurdocumentatie Evaluatie

Evaluatierapport aspectscan

Security & Privacy

Onderzoeksobject

Nederlandse Overheid Referentie Architectuur (NORA v1)

Auteur: P.J. van Vlaanderen, B ICT

Plaats: Nijmegen
Datum: 05-07-2007

Versie: 1.0
Status: Definitieve versie

Begeleider: prof. dr. Daan Rijsenbrij
Referent: prof. dr. Erik Proper

Inhoudsopgave

Samenvatting van het onderzoeksobject

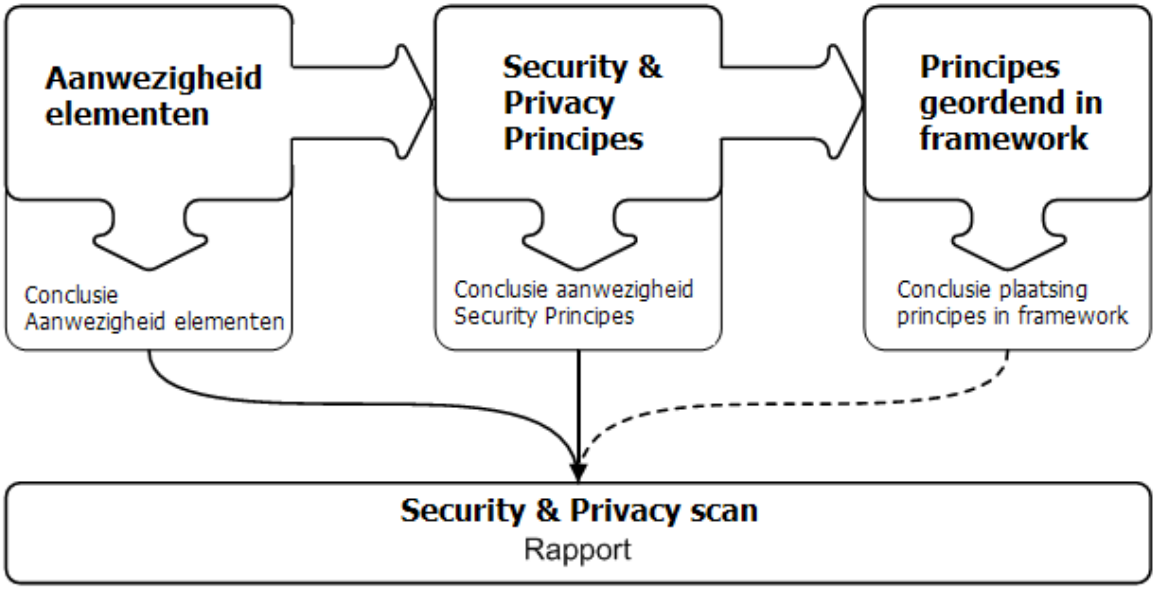
Om alle elementen en begrippen uit deze evaluatie te begrijpen moet eerst de samenvatting van het onderzoeksobject de NORA gelezen worden. Een uittreksel van de belangrijkste zaken in het onderzoeksobject 'NORA' is te vinden op http://www.digital-architecture.net/scripties.htm .

De evaluatie

Dit rapport bevat de resultaten van de evaluatie met de aspectscan security & privacy en is een integraal onderdeel van de resultaten die eerder zijn gevormd met de uitvoering van de ADEM. De resultaten die zijn opgedaan met de uitvoering van de globale fase van de ADEM zijn te vinden op:

http://www.digital-architecture.net/scripties/evaluatiegroep/NORA.pdf

De evaluatie van de aspecten security & privacy zal volgens de volgende drie fasen uitgevoerd worden:



figuur 1: Fasen in de aspectscan security & privacy

Deze fasen zijn uitgebreid beschreven in de aspectfase security & privacy. In fase 1 zullen de elementen tegen een vooraf gedefinieerde norm geëvalueerd worden. In fase 2 worden de principes die invloed hebben op de benoemde elementen getoetst aan de principe-eisen die zijn opgesteld in de aspectscan. In fase 3 worden

de gevonden architectuurprincipes geplaatst in het EISA raamwerk. Alle gevonden principes worden ook gerelateerd aan de principe-eisen.

Doelstelling evaluatie

De evaluatie van de NORA in het kader van security & privacy heeft twee belangrijke doelstellingen. De eerste doelstelling is het testen van de methode in de praktijk. Door het uitvoeren van deze evaluatie wordt inzicht verkregen in de toepasbaarheid en bruikbaarheid van de methode. Resultaten die verkregen zijn in deze evaluatie helpen bij het verder uitbreiden en evolueren van de aspectscan security & privacy.

De tweede doelstelling is inzicht geven in de kwaliteit van de architectuurdocumentatie van de NORA op aspect security & privacy. In dit onderzoek wordt niet getracht een waardeoordeel te geven over de architectuurdocumentatie. De resultaten moeten vooral inzicht verschaffen in hoe de Nederlandse Overheid omgaat met security & privacy. De conclusies die getrokken worden kunnen de auteurs van de documentatie helpen deze te verbeteren. De NORA gaat veel invloed hebben op de communicatie tussen overheidsinstanties onderling en tussen overheid en burgers. Het is dus van groot belang dat er een goed inzicht ontstaat op het gebied van security & privacy. De resultaten van dit onderzoek kunnen inhoud geven aan al bestaande discussies over de NORA.

Fase 1: Geëvalueerde elementen

Sjabloon voor conclusies

Elementnaam	
Meting	Per evaluatiecriterium dient de evaluator hier aan te geven waar hij de beschrijving van het element gevonden heeft in de architectuurdocumentatie. Daarnaast dient de evaluator een kleine samenvatting te geven van het gevonden evaluatiecriterum. Wanneer een evaluatiecriterium niet aanwezig is of beoordeeld kan worden, dient dit hier ook aangeven te worden.
Welke principes?	In fase twee wordt er een evaluatie gedaan naar de aanwezigheid van principes die invloed hebben op de security & privacy. Hier geeft de evaluator aan welke principes er gevonden zijn en hoe deze invloed hebben op het element.
Conclusie	De evaluator schrijft hier op waarom een bepaalde Conclusie getrokken is.

Aanbeveling	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 1: sjabloon om conclusies te presenteren

Aanwezigheid elementen en principes

Organisatiedoelstellingen met betrekking tot Security & Privacy	
Meting	Er zijn diverse organisatiedoelstellingen benoemd in paragraaf 3.3. NORA wilt zich conformeren aan het european interoperability framework. Dit framework stelt dat organisaties compliant moeten zijn aan nationale wet en regelgeving. De NORA zegt hier het volgende over op pagina 45. *'De verlening van overheidsdiensten dient in lijn te zijn met de nationale wetgeving terzake. Voor de individuele gebruikers betekent dit dat functies die gerelateerd zijn aan beveiliging (identificatie, autorisatie, onweerlegbaarheid en vertrouwelijkheid) volledig transparant zijn, weinig inspanning kosten en voldoen aan de gestelde normen. Belangrijke normatieve kaders in dit verband zijn de internationaal geaccepteerde British Standard, in Nederland vertaalt naar de Code voor Informatiebeveiliging.'* De code voor informatiebeveiliging is een goed middel om te komen tot een goede informatiebeveiliging die aansluit bij bijvoorbeeld de wet bescherming persoonsgegevens. De NORA geeft hiermee dus aan deze wetgeving te respecteren en te willen voldoen hieraan. In hoofdstuk 9 'security en privacy' worden nog nadere doelstellingen genoemd die betrekking hebben op security & privacy. *'Vertrekpunt voor de nadere invulling van beveiliging en privacy is dat de individuele organisaties hun zaken al op orde hebben. Ze beheersen hun informatiebeveiliging en privacy goed en reageren slagvaardig en voorspelbaar op verstoringen in hun bedrijfsvoering.'* De NORA gaat er hier van uit dat er een soort baseline security is alvorens organisaties de NORA adopteren als referentiearchitectuur voor eigen architecturen. De doelstellingen hiervoor zijn ondergebracht in een aantal categorieën, namelijk: • De organisatie beheerst haar informatiebeveiliging. • De organisatie beheerst haar bescherming van persoonsgegevens ter bescherming van de persoonlijke levenssfeer van de betrokkenen. • De organisatie beheerst de continuïteit van haar belangrijkste bedrijfsprocessen. Deze peilers vormen de daadwerkelijke baseline. De volgende peilers zijn gevormd om de communicatie tussen organisaties onderling te waarborgen. • De samenwerkende partijen richten gezamenlijk de governan-

	ce in voor hun informatiebeveiliging, privacy en continuïteit van de belangrijkste processen in de bedrijfsvoering. • Alle organisaties in de e-overheid dragen bij en maken gebruik van een te ontwikkelen gemeenschappelijk normenkader. • E-overheidsorganisaties zorgen voor een uniforme en betrouwbare wijze waarmee burgers en bedrijven zaken met haar kunnen doen. • Informatiebeveiliging, privacy en continuïteit van bedrijfsprocessen vormen een integraal onderdeel van een service of dienst. Op pagina 135 wordt er verwezen naar de COSO. Het COSO rapport stelt dat informatiebeveiliging een intergraal onderdeel vormt van de bedrijfsvoering. Op dit gedeelte adopteert de NORA het COSO rapport.
Welke principes?	Er zijn geen principes gevonden die expliciet betrekking hebben op de organisatiedoelstellingen.
Conclusie	De baseline security die wordt verondersteld aanwezig te zijn bij organisaties die de NORA willen adopteren als referentiearchitectuur is niet verder geconcretiseerd dan het benoemen van enkele abstracte peilers die voor meerdere interpretaties vatbaar zijn.
Aanbeveling	Dat de NORA een soort drempel legt voor organisaties die mee willen doen met de NORA is zeker verstandig. Echter roept dit een vraag op 'is de NORA er niet om juist te komen tot een betrouwbare en veilige e-overheid?'. In de NORA staan allerlei middelen om de onderlinge overheidsorganisaties te beveiligen maar veel van deze eisen zijn dus al een baseline om daadwerkelijk mee te mogen gaan doen. Ook is er verder geen controle of deze maatstaaf daadwerkelijk gehaald wordt mocht een organisatie zich willen aansluiten bij de NORA. Men zou er aan kunnen denken een soort van commissie in het leven te roepen die deze grenzen bewaakt.

Tabel 19: Organisatiedoelstellingen met betrekking tot security & privacy.

Risicomanagement	
Meting	In paragraaf 2.8 pagina 34 worden enkele risico's benoemd voor beveiliging & privacy in het algemeen. 'Communiceren via moderne technologie brengt de nodige nieuwe risico met zich mee. Gegevens kunnen verloren raken, systemen kunnen dienst weigeren, kabels kunnen door graafma-

	chines doorgetrokken worden, etc. Tegenover dit soort continuïteitsrisico moeten de nodige maatregelen gezet worden. Zo ook als het gaat om de bescherming van de persoonlijke levenssfeer. Gegevens mogen alleen gebruikt worden door bevoegde functionarissen en moeten niet wederrechtelijk door criminelen afgetapt kunnen worden. Dus bij het ontwerpen van de elektronische overheid moeten maatregelen in het kader van beveiliging en privacy van meet af aan meegenomen worden.' *Er worden eisen benoemd voor informatieraadpleging. Er wordt onderkend dat er continuïteitsrisico's zijn en dat hier maatregelen voor getroffen moeten worden. Persoonlijke levenssfeer wordt ook benoemd. Er zijn hierbij dus concerns onderkend die te maken hebben met privacy. De eisen zijn echter niet gegroepeerd en staan totaal niet met elkaar in relatie.* Risicomanagement wordt tevens als aandachtspunt bij de inrichting van de governance binnen de overheid onderkend. Zie pagina 39.
Welke principes?	Principe 9.3.1 Informatiebeveiliging is een integraal aspect van de bedrijfsvoering (corporate governance) Principe 5.1.1.2. Overheidsorganisaties werken systematisch aan kwaliteitsverbetering
Conclusie	Principe 5.1.1.2. beschrijft dat er gewerkt moet worden via een kwaliteitsmanagementsysteem. Onderdeel van een dergelijk systeem kan volgens de NORA een plan, do, check, act cirkel van Deming bevatten[16]. Een dergelijk kwaliteitsmanagementsysteem wordt niet verder omschreven. Risicomangement vindt ook plaats via een managementsysteem. De NORA beschrijft dus dat er gebruik gemaakt moet worden van een dergelijk systeem. De NORA specificeert het management van kwaliteit niet verder naar bijvoorbeeld concrete elementen als risicomanagement. Principe 9.3.1. staat bijna letterlijk bij de eisen aan principes. Hier is dus perfect aan voldaan. De rationale die bij de eis gegeven is beschrijft tevens een managementcyclus om een adequate bedrijfsvoering te onderhouden. Hierbij wordt risicobeoordeling en het selecteren van controls ook beschreven. *Informatiebeveiliging (IB) vormt een integraal onderdeel van bedrijfsvoering. De gebruikelijke management cycli (Plan Do Check Act) zijn daarbij te onderkennen. Een adequate bedrijfsvoering richt zich op een*

[16] http://www.balancedscorecard.org/bkgd/pdca.html

	vijftal elementen en de daarbij te onderkenen aandachtspunten: • *Omgevingsfactoren zoals integriteit, ethiek, competenties, inrichting van controleactiviteiten, aard van de managementstijl, organisatie- en verantwoordelijkheidsstructuur en HR beleid en procedures;* • *Risicobeoordeling ten aanzien van organisatiedoelstellingen;* • *Uitvoering door middel van het selecteren van keycontrols, documenteren van processen, identificeren van risico's in processen, documenteren controlemaatregelen en selecteren van key-controls, vaststellen toereikendheid en werking van maatregelen;* • *Verzamelen, vastleggen en verwerken van informatie en een effectieve communicatie;* • *Monitoring van het proces, de evaluatie en de rapportage over tekortkomingen en de wijze waarop deze worden ondervangen.* De onderdelen uit dit proces komen overeen met de onderdelen die in de aspectscan onderkend zijn. Ze zijn echter niet toegespitst op risicobeoordeling. De NORA wordt zelf wel weer als risicomodel gebruikt zoals blijkt uit doelstellingen van de NORA beschreven in paragraaf 1.4 *'Instrument voor risicobeheersing* *Het gebruik van de NORA kan leiden tot het vroegtijdig onderkennen van conflicterende ontwikkelingen binnen de e-overheid, zodat een tijdige bijsturing door de beleidsverantwoordelijken mogelijk wordt. Risico's worden hierdoor verkleind.'*
Aanbeveling	Risicomanagement wordt als een onderdeel gezien van kwaliteitsmanagement. Binnen kwaliteitsmanagement voorziet een risicomanagement in het continu verbeteren en evalueren van risico's. Het is aan te bevelen om risico's continu te blijven identificeren en evalueren. Voor de het opstellen van security & privacy principes is het identificeren van risico's het begin stadium van de rationaliseringsketen. Deze rationaliseringsketen doorloopt de volgende stadia: Identificeren van bedreigingen (risico's) en kansen > concerns > stakeholders > architectuurprincipe. Om een goed beleid te voeren aangaande risicomanagement is het aan re raden hier een vast proces voor in te richten. De overheid kan dit natuurlijk niet voor al haar instanties doen, maar kan het wel voorschrijven en richtlijnen meegeven. Risico's die alle overheidsorganisaties aangaan (die bijv. te maken hebben met de infrastructuur) moeten in

	de referentiearchitectuur worden geadresseerd.

Tabel 20: Risicomanagement.

Risicomanagement: Identificatie en evaluatie van risico's.	
Meting	Pagina 135 paragraaf 9.3 'Een organisatie stelt op basis van een expliciete (en dus vastgelegde) risicoafweging de betrouwbaarheidseisen voor haar informatiesystemen vast' In de rationale van principe 9.3.1. wordt een risicoafweging verplicht gesteld. *'Op het tactische niveau worden beslissingen genomen die het stelsel van IB maatregelen beïnvloeden. Voor elk informatiesysteem wordt (door de verantwoordelijke lijnmanager) een expliciete risicoafweging gemaakt en op basis hiervan worden de betrouwbaarheidseisen vastgesteld.'* Er worden nog meer additionele eisen gesteld aan de risicoafweging in principe 9.3.1. *'Op de verschillende onderkende niveaus zijn er verbindingen met de ketenafspraken te onderkennen: In de risicoanalyse wordt de ketenbrede risicoperceptie als uitgangspunt gehanteerd, dit heeft dus voorrang boven de (perceptie van) risico's van de eigen organisatie.* *De organisatie conformeert zich in de normen (beleid, interne audit dienst), beveiligingsdoelstellingen alsmede concrete maatregelen (beveiligingsplannen, keuze van groepen samenhangende maatregelen) aan de ketenbrede afspraken. Waar de uitwerking op basis van de ketenbrede afspraken leidt tot problemen in de uitwerking in de organisatie, wordt dit geëscaleerd naar leiding van de eigen organisatie alsmede naar de ketenpartners.'*
Welke principes?	Gevonden principes: *Principe 9.8.5. 'Middels (publiekelijke) voorlichting worden ook klanten van de diensten bewust gemaakt van de risico's en de noodzaak van beveiligingsmaatregelen.'* *Principe 9.8.6. 'Let op de beveiliging, privacybescherming en continuïteit van de bedrijfsvoering bij ingekochte diensten'*
Conclusie	Het is zeer verstandig dat de overheid werkt aan publieksvoorlichting. Aan diensten gebonden veiligheidsrisico's worden bekend gemaakt en concrete beveiligmaatregelen worden voorgesteld. De processen die een goede risico-identificatie waarborgen worden

	gedelegeerd aan de onderlinge overheidsinstanties. Hierbij wordt expliciet aangegeven hoe omgegaan moet worden met risico's die organisatieoverstijgend zijn. Bij het inkopen bij derden moet worden gelet op beveiliging en privacy. Aan deze principe eis wordt dus voldaan. Dit wordt verder niet geconcretiseerd.
Aanbeveling	Veel van de subprocessen die horen bij de identificatie van risico's worden niet genoemd. Waarschijnlijk komt dit doordat dit proces is uitbesteed aan de onderlinge overheidsinstanties. Het wordt aanbevolen om dit proces ook te voeren op referentieniveau. Er zijn veel risico's die voor alle overheidsorganisaties gelden. Deze kunnen dus alvast geïdentificeerd worden en concrete beveiligingsmaatregelen kunnen voorgeschreven worden. Een belangrijk punt is het bepalen van de waarschijnlijkheid en impact van het risico. Deze punten zijn erg belangrijk om proportionele beveiligingsmaatregelen te bepalen. Principe 9.3.1 gaat uit van risicoperceptie of te wel risicowaarneming. Het principe lijkt te beschrijven dat uitgegaan wordt van waarneming in plaats van vooraf alle mogelijke risico's te identificeren. Risico's moeten altijd geïdentificeerd worden. Risico's die voor een bepaalde organisatie niet van belang zijn of de impact is te verwaarlozen kunnen dan geaccepteerd worden.

Tabel 21: Risicomanagement: Identificatie en evaluatie van risico's.

Risicomanagement: Behandeling van risico's	
Meting	Pagina 135, paragraaf 9.3 'Die normen zijn uitgewerkt tot op het niveau van concrete maatregelen (organisatorisch, procedureel, technisch et cetera)' Op pagina 136 wordt beschreven wat er na het identificeren van een risico gebeurt. *'Deze betrouwbaarheidseisen worden vervolgens uitgewerkt tot het niveau van maatregelen, waarbij zoveel mogelijk voortgebouwd wordt op de gemeenschappelijke normen en maatregelen / voorzieningen. De maatregelen zijn veelal vastgelegd in een beveiligingsplan. De getroffen maatregelen worden in de organisatie geïmplementeerd en vervolgens in beheer genomen. Wijzigingen van het stelsel van maatregelen zijn onderhevig aan een proces van changemanagement.'*
Welke principes?	Gevonden principes: *Principe 9.8.3. Ketenorganisaties specificeren maatregelen (op het*

	gebied van informatiebeveiliging, privacy en continuïteit) van bedrijfsvoering voor specifieke diensten en services op basis van de met die diensten en services samenhangende risico's. *Algemene controlemechanismen die worden voorgesteld in principes* *Principe 9.7.1. Gebruik elektronische handtekeningen bij hoge eisen aan de onweerlegbaarheid van een bericht of transactie.* *Principe 9.7.2 Tenminste bij transacties die een verplichting vormen voor een burger of bedrijf/instelling, zal de e-overheidsorganisatie kwijting geven van het afgerond hebben van een transactie / wezenlijke processtap.* *Principe 9.7.3 E-overheidsorganisaties spreken standaarden af voor beveiligde onderlinge communicatie op in ieder geval berichtenniveau.* *Principe 9.7.4. E-overheidsorganisaties beveiligen de toegang tot hun diensten middels generieke authenticatie diensten op basis van DigiD en/of PKIoverheid.*
Conclusie	Het belangrijkste principe is principe 9.8.3. Dit principe verplicht dat maatregelen worden gebaseerd op bestaande risico's. Principe 9.8.3. waarborgt dat er ook op het gebied van services specifieke maatregelen worden genomen om risico's af te dekken. Maatregelen worden genomen op het gebied van informatiebeveiliging, privacy en continuïteit. Hierbij wordt ook onderscheid gemaakt in organisatorische en technische maatregelen. Principe 9.7.1 is een controlemechanisme om onweerlegbaarheid te waarborgen. Principe 9.7.3 verplicht organisaties controlemechanismen in te voeren die de beveiliging van de communicatie moet waarborgen. In de toelichting van dit principe worden een aantal controlemechanismen als standaard aangegeven. Deze standaarden betreffen smartcards, PKIoverheid, SSL en certificaten voor veilige communicatie.
Aanbeveling	Bij het principe 9.7.3. ontbreekt een deel van de zin. Het principe is dus niet compleet. Er moeten standaarden worden bepaald voor berichtenniveaus en nog niets anders. Dit 'iets anders' wordt niet meer verder omschreven. Dit moet natuurlijk verbeterd worden omdat anders de afspraken niet als gewenst verlopen. Of de principes de juiste proportionaliteit hebben is niet te zeggen. De risico's waarop ze gebaseerd zijn ontbreken namelijk. Om de juiste proportionaliteit te kunnen bepalen moet elk principe waarbij een beveiligingsmaatregel getroffen wordt gekoppeld zijn aan een concern en een risico. Vooral bij de 20 hoofdprincipes uit de NORA is dit van onmiskenbaar belang! De architectuur van een hele samenleving (in

	relatie tot overheidszaken) wordt gebaseerd op deze 20 principes. Het is dus van groot belang dat er inzicht ontstaat in de risico's die deze principes moeten afdekken.

Tabel 22: Risicomanagement: Behandeling van risico's.

Risicomanagement: Monitoring van risico's en controlemechanismen	
Meting	Paragraaf 9.3 op pagina 135 beschrijft enkele aspecten die voor dit element van belang zijn - Voor het behalen van de beveiligingsnormen i.c. het uitvoeren van maatregelen zijn verantwoordelijken benoemd. - Er is een systematiek om te meten of deze normen worden gehaald.
Welke principes?	*Principe 9.6.4. Op basis van monitoring geeft elke ketenorganisatie zekerheid over de naleving van de ketenafspraken.* *Principe 6.1.1.7 Voor het ondersteunen van de controlefunctie van een organisatie kan gebruik gemaakt worden van een management informatie systeem*
Conclusie	Er worden in de verschillende delen van de architectuurdocumentatie controlemechanismen geïntroduceerd. De meeste controles hebben te maken met de controle op de bedrijfscontinuïteit. Deze controles hebben wel een relatie met de monitoring van algemene beveiligingsmaatregelen. Wanneer er een verstoring is in een bevredigingsmaatregel die leidt tot een verstoring in de bedrijfscontinuïteit zal deze verstoring geïdentificeerde worden. Het is dan echter al wel te laat. Bij voorkeur vindt er een goede controle plaats op de beveiligingsmaatregelen. Fouten in de beveiligingsmaatregelen kunnen dan verholpen worden voor er problemen ontstaan.
Aanbeveling	Er wordt niet omgeschreven dat policies en procedures up to date gehouden moeten worden, dit is wel aan te raden. De meeste contoles die benoemd zijn hebben te maken met de controle op de algemene continuïteit van de organisatie en niet met de controle op nieuwe risico's. Het is belangrijk om nieuwe risico's te blijven identificeren en de juiste maatregelen hierop te nemen. Nu lijkt het er op dat er eerst een incident moet plaatsvinden alvorens het nieuwe risico geïdentificeerd wordt.

Tabel 23: Risicomanagement: Monitoring van risico's en controlemechanismen.

Risicomanagement: Evaluatie en aanpassing van controlemechanismen	
Meting	Paragraaf 9.3 op pagina 135 beschrijft een aspect dat voor dit element van belang is: 'De risico-afwegingen en de passendheid van maatregelen wordt periodiek, alsmede naar aanleiding van incidenten geëvalueerd.'.
Welke principes?	Principe 6. *Om een vlotte dienstverlening mogelijk te maken leggen organisaties in het publieke domein routinematig uit te voeren controles binnen het primaire dienstverleningsproces. De noodzakelijke controles worden zo uitgevoerd dat een snelle en soepele dienstverlening plaatsvindt. Meer specifieke controles vinden in beginsel via afzonderlijke processen, parallel of achteraf plaats (eerst mensen, dan regels)* *Principe 9.8.1. Om een service en de onderliggende informatie aantoonbaar goed te beveiligen en in de tijd ook beveiligd te houden moet elke organisatie een beveiligingscyclus voor de service inrichten.*
Conclusie	Er vinden controles plaats op de processen die te maken hebben met de primaire dienstverlening. Deze controles moeten derhalve ook uitgevoerd worden op de veiligheid van de dienstverlening. Waar er zich problemen voordoen kunnen deze aangepast worden. De controlemechanismen ondersteunen de betrouwbaarheid en beschikbaarheid van de dienstverlening. Deze controlemechanismen worden besproken in hoofdstuk 9 security & privacy.
Aanbeveling	Dit element wordt alleen op hoofdzaken beschreven terwijl het een belangrijke plek in neemt in de cyclus van risicomanagement. Het is aan te bevelen alle subprocessen uit de methode expliciet te benoemen. Subprocessen die nu niet benoemd zijn: - Problemen in de controlemechanismen worden verbonden aan een oorzaak. - Er vindt controle plaats op het daadwerkelijk implementeren van de controlemechanismen. - Er worden preventieve maatregelen genomen zodat het problemen zich niet nogmaals voordoen. - Er wordt feedback gegeven op problemen met controlemechanismen.

Tabel 24: Risicomanagement: Evaluatie en aanpassing van controlemechanismen.

Toepassing van SOA en bijbehorende security issues	
Meting	Soa wordt toegepast in de NORA onder de naam SGA. Er zijn dus specifieke beveiligingseisen die geïmplementeerd zouden moeten zijn. Deze SGA wordt op pagina 57 geïntroduceerd. Er worden hier geen expliciete eisen gesteld voor beveiliging en privacy. Aan alle meetvoorwaarden wordt voldaan in de principes en de rationale hiervan.
Welke principes?	*Principe 9.6.1. Convergentie van informatiebeveiliging, privacy en continuïteit van de bedrijfsvoering tussen (in ketens of netwerken) samenwerkende organisaties moet het gevaar van 'de zwakste schakel' voorkomen.* *Principe 9.8.1. Om een service en de onderliggende informatie aantoonbaar goed te beveiligen en in de tijd ook beveiligd te houden moet elke organisatie een beveiligingscyclus voor de service inrichten.* *Principe 9.8.4. De service voldoet aan wet- en regelgeving en contractuele verplichtingen.* *Principe 5.2.1.2. Tot de kwaliteitsindicatoren van een (combinatie)dienst behoren ten minste: juistheid, volledigheid, doorlooptijd, rechtmatigheid en de informatiebeveiliging, privacybescherming en continuïteit* *Principe 5.3.1. Services triggeren elkaar en kunnen daardoor processen verbinden*
Conclusie	De eisen die genoemd worden in principe 5.2.1.2. zijn vastgelegd in regelgeving en uitvoeringsbesluiten. Per (combinatie)dienst worden deze kwaliteitsindicatoren vastgelegd; bij voorkeur op een voor burgers en bedrijven toegankelijke manier (transparante overheid). In het bijzonder is deze transparantie van belang waar het de privacyaspecten van een dienst betreft. De NORA onderkent dat kwaliteitsindicatoren niet alleen over de gehele dienst moeten worden vastgelegd maar per element van een dienst. Dit is een goede zaak, zonder deze toevoeging zouden de kwaliteitseisen te abstract zijn beschreven. Verdere conclusies: - Er wordt een beveiligingscyclus ingericht voor de service - Een veel voorkomend probleem, een zwakke schakel in de ketting van services wordt in ieder geval benoemd. De oplossing is convergentie. Hier moeten nog wel indicatoren voor gegeven worden. - Bij de vorming van diensten moeten beveiligingseisen en privacy worden meegenomen. Hoe dit ingevuld moet worden wordt aan de afzonderlijke overheidsinstantie over gelaten. Dit brengt echter weer risico's naar voren die te maken hebben met zwak-

	ke schakels. - Principe 5.3.1. lijkt de eis betreffende koppeling van services (Componenten mogen niet aan elkaar gekoppeld worden tot dat zij worden aangeroepen) af te dekken. De rationale van dit principe biedt hier echter geen duidelijk over.
Aanbeveling	Geen aanbevelingen.

Tabel 25: Toepassing van SOA en bijbehorende security issues.

Beveiligingsbeleid	
Meting	Aan geen van de indicatoren is voldaan. Er is geen beveiligingsbeleid opgenomen in de NORA.
Welke principes?	Geen principes gevonden.
Conclusie	Het beveiligingsbeleid is niet opgenomen in de architectuurdocumentatie. Er zijn enkel een aantal losse eisen aangaande dit beleid geformuleerd. Meestal worden deze punten kort benoemd als een principe hierop gebaseerd is.
Aanbeveling	Het verdient aanbeveling om het beveiligingsbeleid bij te sluiten bij de architectuurdocumentatie of te verwijzen naar beleid dat openbaar is gemaakt.

Tabel 26 Beveiligingsbeleid.

Beveiligingsorganisatie	
Meting	Op pagina 130 paragraaf 8.3 worden de beheerstaken van de ketenverantwoordelijke vastgelegd. De partij die verantwoordelijkheid draagt voor het leveren van een dienst aan burgers of bedrijven heeft een belangrijke rol in het afstemmen van de dienstenniveaus in de totale keten. Dit betekent dat deze organisatie, naast het transparant beschikbaar stellen van haar eigen diensten, contact onderhoudt met alle andere ketenpartijen en regie voert. De ketenverantwoordelijke draagt hierbij zorg voor de afstemming van alle aspecten van de dienstverlening die organisatieoverstijgend zijn. Dit betreft onder andere:

	· Afstemming van gebruikte standaards en afspraken door de keten heen, bijvoorbeeld templates van XML berichten ; *· Het coördineren van het doorvoeren van wijzigingen en onderhoud die (tijdelijk) impact hebben op het functioneren van de dienst;* *· Het bijhouden van een ketenreleaseplanning;* *· Het coördineren van de oplossing van incidenten die betrekking hebben op meerdere ketenpartners;* *· Het verzamelen van wensen en klachten van de afnemers van de dienst en het bemiddelen in de realisatie van nieuwe functionaliteiten binnen de gehele keten;* *· Het verzorgen van rapportage over de dienstverlening over de keten heen. Hierin moet onderscheid worden gemaakt naar rapportage op strategisch, tactisch en operationeel gebied of aan de klanten van de dienst.* Hiermee zijn verantwoordelijkheden die te maken hebben met ketenintergratie vastgelegd. Het inrichten van het beheer is volgens het subsidiariteitsbeginsel[17] dat wordt toegepast in de NORA een zaak van de organisatie zelf. Hierbij dient de organisatie er wel voor te zorgen dat het beheer op een dusdanige manier is ingericht, zodat de externe diensten en bijbehorende dienstenniveaus met betrouwbaarheid kunnen worden geleverd. De NORA stelt ook voor dat er een security officer wordt aangesteld (pagina 137, rationale principe 9.3.3.). Er wordt echter niet ingegaan op de daadwerkelijke plaatsing van de security officer in de organisatie. Het is dus niet duidelijk wat de precieze functie van deze security officer is en welke incidenten er aan hem gemeld moeten worden.
Welke principes?	Principe17. Organisaties in het publieke domein organiseren zich als een onderdeel van een integraal opererende en als eenheid optredende overheid, die in haar handelen naar burgers, bedrijven en maatschappelijke instellingen consistent en betrouwbaar is. *Principe 9.3.2 De leiding van organisaties is verantwoordelijk voor een toereikende organisatie van informatiebeveiliging.*

[17] Het Subsidiariteitsbeginsel betekent dat het accent ligt op het formuleren van voorstellen die betrekking hebben op samenwerking, de koppelvlakken tussen organisaties en dan uitsluitend waar dat nodig is. Wat binnen een overheidsorgaan geregeld kan worden, wordt daar geregeld. Pas als dat onvoldoende mogelijkheden oplevert voor soepele samenwerking ten behoeve van de dienstverlening, worden afspraken gemaakt op het niveau van een sector, een ander niveau (in de Nederlandse situatie vaak het daarbovenliggende niveau) of binnen een andere groepering (meestal een grotere deelverzameling). Indien ook dat onvoldoende blijkt te zijn, worden afspraken gemaakt voor de gehele overheid

	Principe 9.6.2. Samenwerkende partijen leggen verantwoording af waarin zij de relatie leggen tussen de door hen getroffen maatregelen en de gemaakte keten / netwerkafspraken. *Principe 9.7.6. Elektronische diensten worden verleend op basis van een bekende identiteit, waar het gaat om persoonlijke gegevens en transacties.* *Principe 9.7.7. De handelingen van overheidsmedewerkers (al dan niet in het kader van een aan een burger of bedrijf te leveren dienst) zijn tot op de persoon herleidbaar.*
Conclusie	Principe 9.3.2 behandelt de verantwoordelijkheden wat betreft de organisatiedoelstellingen die te maken hebben informatiebeveiliging. De eisen die gesteld worden aan de beveiligingsorganisatie worden gehaald.
Aanbeveling	Het subsidiariteitsbeginsel zorgt ervoor dat organisaties zelf hun beheer in kunnen regelen als er geen overkoepelende afspraken gemaakt moeten worden. Bij een grote onderneming als de overheid kan niet alles centraal aangestuurd worden en moeten dit soort zaken ook gedelegeerd worden. De principes in de NORA moeten wel opgevolgd worden wanneer een organisatie zijn architectuur baseert op de referentiearchitectuur 'NORA'. Zodoende is de bewegingsvrijheid wel ingeperkt van de organisatie en heeft de Overheid wel invloed op beslissingen die lager in de keten genomen worden. Een voorbeeld hiervan is de baseline security die door de NORA voorgeschreven wordt. De NORA kan dit niet anders regelen. Hier schuilen echter wel gevaren in. Omdat de onderlinge overheidsorganisaties niet verplicht zijn om de diverse eisen aangaande security & privacy te handhaven bestaat het gevaar van de zwakste schakel. Betrouwbaarheidseisen voor externe dienstverlening zouden verplicht moeten worden.

Tabel 27: Beveiligingsorganisatie.

Classificatie en beheer van bedrijfsmiddelen	
Meting	Op pagina 150 worden de betrouwbaarheidseisen van services gedefinieerd in termen van de beschikbaarheid, integriteit en vertrouwelijkheid.
Welke principes?	Gevonden principes: *Principe 9.7.1: 'Gebruik elektronische handtekeningen bij hoge eisen aan de onweerlegbaarheid van een bericht of transactie.'*

	Principe 9.8.2: ' De beschikbaarheid van de service is door de eigenaar gedefinieerd en geborgd.' *Principe 6.2.2: 'Elk gegeven kent een eigenaar en een beheerder.'* *Principe 6.2.2.3: 'De eigenaar van een gegeven is verantwoordelijk voor de kwaliteit (actualiteit, betrouwbaarheid) van een gegeven.'* *Principe 6.2.6.2: 'Een gemeenschappelijk gegeven kent slechts één beheerder.'* *Principe 7.2.1.3: ' Databasegegevens zijn herleidbaar tot de bron.'*
Conclusie	Principes die het veiligheidsniveau van de assets moeten bepalen ontbreken. Alle andere eisen zijn afgedekt.
Aanbeveling	De indruk wordt gewekt dat het eigenaarschap van de data die verwerkt wordt van de burger, niet bij de burger ligt. De overheid beslist immers aan wie zij de data verstrekt en wat ze er verder mee doet. Dit gebeurt wel met in achtneming van de wettelijke eisen. De burger heeft inzage recht en recht op wijziging. Hoe dit vormgegeven wordt, is niet bekend. Het lijkt een onmogelijke opgave om van alle data die verwerkt wordt een inzichtelijk rapport te krijgen.

Tabel 28: Classificatie en beheer van bedrijfsmiddelen.

Beveiligingseisen ten aanzien van personeel	
Meting	Er zijn geen duidelijke eisen ten aanzien van het personeel gevonden.
Welke principes?	Principe 9.4.6. Bij controle op werknemers wordt het privacybelang van de werknemers door de werkgever in acht genomen. Er zijn verder geen principes opgesteld die de beveiligingeisen ten aanzien van het personeel afdekken.
Conclusie	Er zijn in de overige elementen verschillende verantwoordelijkheden benoemd aangaande dit element. Op pagina 30 wordt wel gesproken over een CERT team. Er wordt echter nergens anders gesproken over de installatie van dit CERT team.
Aanbeveling	Beveiligingseisen ten aanzien van het personeel moeten worden opgenomen in de architectuurdocumentatie of er moet hiernaar verwezen worden.

Tabel 29 Beveiligingseisen ten aanzien van personeel.

Toegangsbeveiliging

Meting	Waar de eisen erg hoog zijn voor de toegangsbeveiliging en een sterke authenticatie wenselijk is, wordt een combinatie met PKIoverheid voorgesteld. PKI staat voor public key infrastructure. PKIoverheid is een infrastructuur die voorziet in één betrouwbaarheidsniveau voor de elektronische communicatie en transacties van en met de overheid, gebaseerd op Europese standaarden en de Wet elektronische handtekeningen. Hiermee kunnen gebruikers (burgers en bedrijven, maar ook overheidsorganisaties) volgens de NORA er op vertrouwen dat zij op een veilige, betrouwbare en rechtmatige wijze informatie via het internet kunnen uitwisselen met de overheid[18]. Voor offline dienstverlening is DigiD inherent minder geschikt. Onder offline dienstverlening wordt dienstverlening verstaan die niet plaatsvindt via het internet. Hier wordt aanbevolen gebruik te maken van de op PKI gebaseerde elektronische handtekeningen. De NORA geeft aan dat door haar klanten de gelegenheid te geven hun vertegenwoordigingsrelaties in de elektronische diensten te modelleren, de elektronische diensten van de e-overheidsorganisatie beter op de praktijk aansluiten. Zo wordt ook oneigenlijke doorgifte van persoonlijke authenticatiemiddelen (zoals verstrekt door DigiD) tegengegaan. Vertegenwoordigingsrelaties worden op pagina 148 als volgt omschreven 'Bij zowel de burger en bij bedrijven/instellingen kan er sprake zijn van vertegenwoordigingsrelaties. Specifiek bij bedrijven/instellingen is er, zeker voor online dienstverlening, rekening te houden met de interne differentiatie van rollen en rechten'. Een mogelijke invulling is dat met behulp van deze dienst: · organisaties hun eigen rollen en bijbehorende autorisaties kunnen modelleren; · autorisaties op bestaande rollen tussen verschillende organisaties kunnen worden ingericht; · rollen en autorisaties voor aan burgers en bedrijven gerichte elektronische diensten kunnen worden gemodelleerd en vastgelegd, inclusief een verbinding met DigiD voor authenticatie. Er is geen hiërarchie omschreven voor het uitdelen van de authorisatie Er is geen controle op de rechtsgeldigheid van autorisaties en niet geslaagde autorisaties worden niet gelogd.
Welke principes?	Gevonden principes:

[18] https://www.pkioverheid.nl/

	Principe 5.2.1.14: *'Burgers krijgen door middel van het burgerservicenummer een digitale, unieke identiteit. Dit BSN dient maximaal door overheidsorganisaties te worden toegepast.'* Principe 5.2.1.15: *'Bedrijven en instellingen krijgen door middel van het bedrijven en instellingennummer een digitale, unieke identiteit. Dit BIN dient via tussenkomst van DigiD maximaal door overheidsorganisaties te worden toegepast bij de inrichting van hun communicatie met individuele bedrijven en instellingen.'* *Principe 9.7.4: 'E-overheidsorganisaties beveiligen de toegang tot hun diensten middels generieke authenticatie diensten op basis van DigiD en/of PKIoverheid.'*
Conclusie	DigId heeft als betrouwbaarheidsniveau 'basis'. Waar er een hogere vorm van betrouwbaarheid wenselijk is kan authenticatie plaatsvinden op basis van een elektronische identiteitskaart (eNIK) of via sms berichten per mobiele telefoon. Er zijn dus verschillende manieren van authenticatie met diverse betrouwbaarheidsniveaus. De meeste eisen aan de principes worden meegenomen bij het opstellen van principes die te maken hebben met authenticatie en autorisatie. De eis '*Rechten worden uitgedeeld op basis van 'need to know'* ' wordt niet expliciet beschreven. Hier wordt echter wel rekening mee gehouden van rechtswegen omdat men wil voldoen aan de WBP welke afdwingt dat organisaties alleen gegevens mogen inzien wanneer daar ook een aanleiding voor is. Role based access control wordt niet toegepast.
Aanbeveling	De NORA geeft de organisaties handvatten om te zorgen dat er geen oneigenlijke doorgifte van authenticatiemiddelen zoals DigID plaatsvindt. Hier blijkt wel weer dat niet alleen technische middelen het succes van een architectuur waarborgen. Wij herinneren ons allemaal het incident dat in 2007 plaatsvond. De belastingdienst adviseerde burgers de DIgID code van de buurman te gebruiken wanneer zij zelf nog niet de beschikking hadden over DigId. Dit was echter duidelijk niet de bedoeling van DigID en had dus ook niet zo verkondigd mogen worden. Door een verkeerde uitspraak van een individu of enkele overheidsorganisatie kan het hele beveiligingssysteem omver geworpen worden. Een set aan instructies over hoe om te gaan met deze authenticatiemiddelen zou bijgesloten moeten worden in de gedragsregels van overheidsfunctionarissen. Als er een hoge mate van betrouwbaarheid wordt verwacht kan er gebruik gemaakt worden van 'veiligere' systemen dan DigId. Echter moet de burger dan wel de beschikking hebben over een mobiele telefoon of een elektronische identiteitskaart. Niet iedereen heeft de beschikking over een mobiele telefoon en dit zou derhalve niet verplicht mogen worden. De uitwerking van authenticatie middels een elektronische identiteitskaart zou een hogere prioriteit moeten genie-

	ten. De authenticatie via het internet wordt volop besproken in de NORA. Authenticatiemiddelen via telefoon of loket worden echter nauwelijks genoemd en uitgewerkt. Via het loket zou men gebruik kunnen maken van de eNIk(zie pag.32) echter is deze kaart nog niet in gebruik. Authenticatiemiddelen voor het contactcentrum van de overheid worden niet besproken. Een andere discussie die voortvloeit uit de implementatie van de NORA is het verminderen van contactpunten die niet via het internet geïnitieerd worden. De overheid geeft geen keiharde garanties hiervoor.

Tabel 30: Toegangsbeveiliging.

Ontwikkeling en onderhoud van systemen	
Meting	De NORA beoogt een koppeling van overheidssystemen onderling. Daarnaast worden de overheidssystemen gekoppeld aan publieke netwerken zoals het internet. Via het internet kan de burger de overheid benaderen en diensten afnemen. De impact van deze keuze is groot en daarom moet onderkend worden hoe dit effect heeft op de security maatregelen in de NORA. De NORA wil gebruik maken van publieke netwerken om gegevens te transporteren. De NORA zegt hier het volgend over op pagina 126. 'Deze paragraaf (7.3 netwerkonderhoud) behandelt de fysieke verbindingen waarmee data van verschillende applicaties, die op gescheiden locaties kunnen staan, getransporteerd worden. Nederland ligt vol koper en glasvezel en loopt daarmee internationaal voorop. De kunst is om dit kostbare netwerk efficiënt te gebruiken en de betrouwbaarheid ervan op een hoog niveau te brengen en houden.' *In pararaaf 2.8 worden enkele uitgangspunten genoemd die betrekking hebben op security & privacy.* • Het merendeel van de diensten van organisaties in het publieke domein moet via het internet verleend kunnen worden. Dit kanaal leent zich voor een uitstekende dienstverlening aan burgers en bedrijven. Tot 24 uur per dag en 7 dagen per week. • Bereikbaar vanaf elke denkbare locatie (tijd- en plaatsonafhankelijkheid). Gegevens die al binnen de overheid bekend zijn, moeten niet opnieuw aan burgers en bedrijven worden gevraagd (éénmalige gegevensaanlevering;

	meervoudig gebruik). De NORA moedigt het gebruik van open standaarden aan. De NORA ziet het gebruik van open source als volwaardig alternatief voor closed source. Security wordt ook gewaarborgd bij buiten werking stellen of verwijderen van een systeem.
Welke principes?	Principe 7.3.1. '*Communicatie tussen overheidsorganisaties verloopt via of besloten, separate netwerken of door middel van een virtual private network verbinding via netwerken van particuliere bedrijven.'* Principe 7.3.2. '*Communicatie e-overheid en burgers/bedrijven via beveiligde internetverbinding of VPN'* Principe 7.3.3. '*Het interne netwerk van overheidsorganisaties is via één redundant en veilig uitgevoerde koppeling aangesloten op het publieke netwerk'* Principe 1. '*Diensten via internet: organisaties in het publieke domein verlenen hun diensten aan burgers, bedrijven en maatschappelijke instellingen via het internet (elektronisch loket) en stimuleren het gebruik van dit kanaal.'* Principe 2. '*De bestaande kanalen zoals post, telefoon en balie blijven beschikbaar, zodat burgers, bedrijven en maatschappelijke instellingen gebruik kunnen maken van het kanaal van hun keuze.'* Principe 8. '*Eenmaal uitvragen van gegevens, meermalen gebruiken; de organisaties in het publieke domein zullen burgers en bedrijven niet opnieuw om gegevens vragen die bij de overheid al bekend zijn.'* *Principe 16. 'Organisaties in het publieke domein attenderen burgers en bedrijven op voor hen relevante diensten (pro-actieve dienstverlening), maar bieden ruimte voor eigen regie en verantwoordelijkheid door burgers en bedrijven op de feitelijke afname van diensten (zelfwerkzaamheid). Daarbij verstrekken organisaties begrijpelijke informatie, bijvoorkeur geïndividualiseerd, over rechten, plichten en mogelijkheden voor burgers en bedrijven.'* *Principe 18. 'Organisaties in het publieke domein gebruiken gegevens die accuraat, actueel en volgens wettelijke normen beveiligd zijn en delen die gegevens met andere organisaties in het publieke domein.'* *Principe 6.1.1.9 'Ontwikkelstraten maken gebruik van internationale open standaards tav frameworks voor toolsets en methoden en technieken voor software ontwikkeling.'* *Principe 6.2.1.2. 'Gegevensverzamelingen die eigendom zijn van een overheidsorganisatie worden – met in achtneming van nadere wettelijke regels - ter beschikking gesteld aan de gehele overheid.'*

Conclusie	Communicatie tussen overheidsorganisatie vind grotendeels over het internet of andere openbare netwerken plaats. Het is daarom belangrijk dat de NORA hier aandacht aan besteedt in de architectuurdocumentatie. De NORA hanteert enkele principes die de veiligheid bij deze communicatie moeten waarborgen. Principe 7.3.1 en principe 7.3.2 lijken elkaar tegen te spreken. De overheid wil communiceren via eigen beheerde netwerken maar er vindt ook communicatie plaats via het internet. Principe 1 en 2 hebben veel invloed op de ontwikkeling van systemen voor de overheid. Systemen moeten bijvoorbeeld webbased worden geprogrammeerd. Dit brengt veel beveiligingsrisico's met zich mee. Het is een goed streven van de overheid om hun diensten via het internet aan te bieden. Authenticatie van de burger geschiedt middels DigID. Het is echter nog niet mogelijk om autorisatie voor overheidsdiensten te koppelen aan een burger die geauthenticeerd is. Het is niet duidelijk welke autorisaties de burger heeft. Welke zaken kan hij wel regelen met DigID en welke niet. Bevoegdheden van een burger zijn niet gekoppeld aan de DigID. Het is de evaluator niet geheel duidelijk hoe deze dienstverlening via het internet dan zal plaatsvinden. Er wordt aangedragen dat de systemen gebaseerd op de NORA wanneer nodig 24 uur per dag en op elke plaats beschikbaar moeten zijn. Dit zou via het internet geregeld kunnen worden. DigId is het authenticatiemiddel voor de overheid. Bij uitval van dit middel wordt er momenteel geen uitkijkmogelijk geboden. Dit duidt op een single point of failure.
Aanbeveling	De NORA onderkent dat naarmate de getransporteerde data privacygevoeliger is of de aard van de verleende dienst meer een rechtsgeldig karakter draagt, er ten minste via een HTTPS protocol gewerkt moeten worden. Dit is een goed uitgangspunt maar het zou verstandig zijn om hier te bepalen dat alle data waarbij persoonsgegevens van burgers betrokken zijn via een veilig protocol moet lopen. Het is niet aan de overheid om te bepalen wat er wel of niet privacy gevoelig is. Het is aan de burger of het bedrijfsleven om te bepalen wat privacy gevoelige gegevens zijn. De burger zou daarom altijd de mogelijkheid geboden moeten worden om via een veilig protocol te werken. Een stap in de goede richting is om over te gaan naar de meest nieuwe protocollen zoals Ipv6. Bij de verantwoording van principe 7.3.3. wordt het gebruik van firewalls aangeraden. Daarbij wordt ook gedacht aan het dubbel uitvoeren van een dergelijke gateway om een single point of failure te voorkomen. Het dubbel uitvoeren van hardware is één, echter wanneer eenzelfde fouten in de firewall blijken te zitten is er nog steeds een single point of

	failure. Principe 2 geeft aan dat er meerdere kanalen gehandhaafd blijven voor de dienstverlening. De NORA is echter vooral geschreven voor elektronische dienstverlening en er wordt weinig geschreven over de gevaren van dienstverlening via het internet. Uit de praktijd blijkt dat het noemen van een geboortedatum en naam al voldoende autorisatie biedt om een dienst te kunnen afnemen. Wanneer diensten via internet goed beveiligd zijn maar via andere kanalen betrekkelijk weinig beveiliging bieden heeft de beveiliging van de elektronische dienstverlening weinig zin. Er zouden meer afspraken gemaakt moeten worden voor de andere overheidskanalen. Hierbij is het natuurlijk wel een noodzaak dat andere overheidskanalen open blijven. Het principe heeft dus zeker bestaansrecht. Principe 16 heeft veel invloed op de privacy van de burger. De overheid wil de burger pro-actief bedienen. Dit betekent dat gegevens geraadpleegd worden zonder dat deze geraadpleegd moeten worden op verzoek van deze burger. Dit principe kan dus op veel weerstand rekenen en de overheid zou er goed aan doen om dit principe verder uit te leggen. Welke diensten worden er wel niet pro-actief aangeboden. Dit principe is tevens hetzelfde als principe 5.2.1.13 dat ook gebaseerd is op principe 16. Dit principe wijst dus naar zichzelf. Tijd en locatie eisen brengen grote risico's met zich mee. De NORA adresseert maar enkele risico's die hiermee gepaard gaan. Het is aan te raden hier meer aandacht aan te besteden. Het lekken van informatie via mobiele gegevensdragers is al te veel in het nieuws geweest. Wanneer overheidsfunctionarissen meer en meer informatie digitaal tot hun beschikking hebben wordt het risico op uitlekken van gegevens alleen maar groter. Principe 16 wordt expliciet in deze tabel opgenomen omdat dit principe invloed heeft op de bouw van toekomstige informatiesystemen in het kader van de NORA. Bij de ontwikkeling van systemen moet rekening gehouden worden met zogenaamde 'mobility issues'. In een gesprek met Alex de Jonge van het ministerie van buitenlandse zaken werd een hoop duidelijkheid geschept op dit vlak. Dit ministerie houdt expliciet rekening met deze issues. Het ministerie kiest er voor om zijn systemen toegankelijk te maken voor haar medewerkers via veilige VPN verbindingen. Zo wordt ontmoedigd om gevoelige informatie mee te nemen op onveilige gegevensdragers. Het zou naar mijn mening verstandig zijn USB sticks in zijn geheel te verbieden binnen de overheid. Dit valt echter buiten de scope van dit onderzoek maar de NORA dient wel rekening te houden met deze zaken. Diverse spellingsfouten in de principes maken de principes moeilijk leesbaar. Principes 7.3.1 en 7.3.2 zouden beter geformuleerd kunnen worden.

Tabel 31: Ontwikkeling en onderhoud van systemen.

Incidentmanagement	
Meting	Paragraaf 9.3 op pagina 135 beschrijft een aspect dat voor dit element van belang is: *'Er is een proces om incidenten af te handelen en zo goed mogelijk te beheersen.'*. Ook wordt de plaats waar incidentmanagement plaatsvindt onderkend. Pagina 135 *'op het operationele niveau worden maatregelen tot uitvoer gebracht en wordt de goede werking van die maatregelen beoordeeld. Op dit niveau vindt ook incidentmanagement plaats.'*
Welke principes?	*Principe 7. Organisaties in het publieke domein kennen een transparante en toegankelijke klachten en bezwarenprocedure.* *Principe 9.3.3. Security incidenten worden gesignaleerd, vastgelegd en gerapporteerd. Beveiligingsrelevante afwijkingen bij de uitvoering van processen worden aangemerkt als security incidenten.* *Principe 9.6.4. Op basis van monitoring geeft elke ketenorganisatie zekerheid over de naleving van de ketenafspraken.*
Conclusie	Wanneer er klachten (incidenten) zijn, kunnen deze gemeld worden door de burger. Dit wordt afgedekt middels principe 7. In de rationale van 9.6.4 wordt beschreven dat er managementsrapportages gemaakt moeten worden bij het voorkomen van incidenten. In de rationale van principe 9.3.3. richt de organisatie een mechanisme in om incidenten vast te leggen en door beoordeling hieruit lering te trekking. Afwijkingen in bijzonder beveiligingskritische processen worden met voorrang geanalyseerd en bij het oordeel dat het een security incident betreft ook aan de security officer gerapporteerd. Het bovenstaande principe impliceert dus ook dat er een security officer aangesteld moet worden.
Aanbeveling	Audit mechanisme om niet-geautoriseerd gebruik te detecteren en incident onderzoek te ondersteunen, zijn niet aanwezig. De implementatie van een dergelijk mechanisme kan het identificeren van incidenten ondersteunen. Het wordt dan ook aanbevolen een dergelijk mechanisme te implementeren.

Tabel 32: Incidentmanagement.

Continuïteitsmanagement	
Meting	Er worden uitwijkmogelijkheden geboden doordat de burger meerdere contactkanalen kan benaderen. Bij het uitvallen van loketten kan er

	gekozen worden om via het internet contact te zoeken. Er is geen uitwijkmogelijkheid gevonden wanneer authorisatie middels DigId niet goed verloopt. Op pagina 137 worden de verantwoordelijkheden betreffende continuiteitsmanagement vastgelegd. *'De leiding van een organisatie benoemt de verantwoordelijken, rollen en bijbehorende taken specifiek voor het proces van continuïteitsmanagement. Tevens richt de leiding, in geval en voor zover de risicoafwegingen daar aanleiding toe vormen, een crisisorganisatie in die verantwoordelijk is voor de voorbereiding op, de tests van en de respons op een continuïteitsbedreigende crisis inclusief de communicatie naar medewerkers en het mediabeleid. '*
Welke principes?	Principe 9.5.1. Organisaties richten een proces in voor de waarborging van de continuïteit van de diensten en services die via hun bedrijfsprocessen worden geleverd.
Conclusie	Continuïteitsmanagement is aanwezig binnen de NORA
Aanbeveling	Continuïteitsmanagement is aanwezig echter zijn er wel enkele single point of failures bekend in de NORA. Deze continuïteitsrisico's zouden al direct benoemd moeten worden.

Tabel 33 Continuïteitsmanagement.

Naleving	
Meting	De indicatoren die in de meting zijn onderkend worden binnen dit element alleen afgedekt door principes.
Welke principes?	Principe 12. Organisaties in het publieke domein geven burgers, bedrijven en maatschappelijke instellingen inzicht in de status van voor hen lopende dienstverleningsprocessen(transparante, traceerbare dienstverleningsprocessen) Principe 15. Organisaties in het publieke domein maken zichtbaar wat zij doen, welke besluiten zij nemen, welke gegevens zij hebben en gebruiken en wat hun werkwijze is. (controleerbaar) Principe 9.3.4. Samenwerkende organisaties organiseren de vastlegging van relevante gebeurtenissen (event logging, audit logging) met een organisatieoverschrijdend karakter op een inhoudelijk samenhangende wijze. Principe 9.6.3. Toezicht wordt uitgeoefend met behulp van audits

	door een onafhankelijke deskundige. De relevante auditresultaten worden beschikbaar gesteld aan de partners in de samenwerking.
Conclusie	Principes 12 en 15 geven de burger de mogelijkheid de overheid te controleren. De overheid conformeert zich ook aan de WBP. De WBP geeft daarnaast bijvoorbeeld ook de mogelijkheid om een WOB[19] verzoek in te dienen. Hiermee heeft de burger de mogelijk om inzicht te krijgen in de opslag van gegevens van de burger. De burger kan zo controleren of de regels worden nageleefd. Er kunnen audits worden uitgevoerd door onafhankelijke derden. Aan deze eis is dus voldaan. De NORA zoekt ook actief naar organisaties en expertgroepen die een mening willen geven over het document. De eisen die door de burger en het bedrijfsleven worden gesteld kunnen daarmee gecontroleerd worden.
Aanbeveling	Geen aanbevelingen.

Tabel 34: Naleving.

Compliant aan WBP	
Meting	In paragraaf E4 op pagina 45 gaat de NORA in op privacy en de WBP 'Elektronische dienstverlening moet de vertrouwelijkheid van persoonlijke data garanderen, inclusief maatregelen die het mogelijk maken om aan te geven of data voor andere doeleinden mogen worden gebruikt dan waarvoor zij zijn verstrekt. In Nederland gaat het hierbij met name om het respecteren van de Wet Bescherming Persoonsgegevens (WBP).'

[19] Een Wob-verzoek is een verzoek om overheidsinformatie. Elk verzoek om informatie is een Wob-verzoek. Zo'n verzoek moet worden ingediend bij het bestuursorgaan dat beschikt over het document. De Wob valt onder de verantwoordelijkheid van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK). Voor meer informatie zie de website van BZK:

http://www.minbzk.nl/grondwet_en/openbaarheid/veelgestelde_vragen

Welke principes?	Principe 9.4.1. Organisaties waarborgen de persoonlijke levenssfeer (privacy)van natuurlijke personen door te voldoen aan de eisen uit de Wet Bescherming Persoonsgegevens en onderliggende richtlijnen zoals door het College Bescherming Persoonsgegevens uitgegeven. Principe 9.4.2. Overheidsorganisaties betrachten maximale transparantie voor de betrokkenen wat betreft de op hen betrekking hebbende verwerkingen van persoonsgegevens en verstrekkingen aan derden van die persoonsgegevens. Zij streven daarom naar inzage langs elektronische weg voor de betrokkenen. Principe 9.4.3. In de keten samenwerkende organisaties toetsen de toereikendheid van de waarborgen voor de persoonlijke levenssfeer (privacy) van natuurlijke personen Principe 9.4.4. Overheidsorganisaties operationaliseren de wettelijke eisen aangaande privacy via een managementcyclus van beleid tot en met controle Principe 9.4.5 Overheidsorganisaties streven naar zelfregulering op het gebied van bescherming persoonsgegevens. Principe 9.4.6. Bij controle op werknemers wordt het privacybelang van de werknemers door de werkgever in acht genomen. Principe 9.4.7. Privacy wordt zoveel mogelijk in het ontwerp van geautomatiseerde systemen geborgd middels Privacy Enhancing Technologies. Principe 9.4.8. Met behulp van encryptie worden bijzonder gevoelige gegevens (in het bijzonder persoonsgegevens of geheime gegevens) onleesbaar gemaakt voor ongeautoriseerde kennisname.
Conclusie	De overheid moet in deze context compliant zijn aan zijn eigen wet en regelgeving. Het mag verondersteld worden dat dit daarom ook goed geregeld is. De NORA slaagt hier redelijk goed in. De principes die genoemd worden zijn bijna afdoende om onderlinge organisaties te sturen naar een architectuur die voldoet aan de eisen genoemd in WBP.

Aanbeveling	Principe 9.4.2 wordt gekenmerkt als de facto principe[20]. Dit principe is gebaseerd op wet en regelgeving omdat in de WBP vermeld wordt dat de gegevensverwerkende organisatie verplicht is om duidelijk inzicht te geven waar er gegevens van de betrokkenen worden vastgelegd. De status van dit principe moet dus verhoogd worden naar 'de jure'. De NORA gaat op twee punten in de WBP verdacht weinig in. Het lijkt er sterk op dat dit met opzet niet gebeurd zodat de overheid middelen ter beschikking heeft om burgers te kunnen controleren. In de media hebben we allemaal kunnen vernemen dat de overheid van plan is vergaande maatregelen te nemen op het gebied van logging van internetverkeer. Dit moet gebeuren in het kader van terrorismebestrijding. Waarschijnlijk is het zo dat deze systemen die dit moeten gaan reguleren niet onder de NORA gaan vallen. echter geeft het wel de doelstellingen van de overheid aan. Opslag van internetverkeer vindt plaats bij de provider, derhalve zullen deze systemen niet onder de NORA vallen. De overheid wil op enige wijze controle houden op de burger en heeft daarbij gegevens nodig die zij niet in eerste instantie nodig heeft voor interne processen of dienstverlening. De twee punten die niet genoemd worden in de principes zijn de volgende: - De onderneming ziet er op toe dat er een expliciete en rechtmatige grondslag bestaat voor alle persoonsgegevens die zij (verzamelt en) verwerkt. - De onderneming draagt zorg dat zij niet meer persoonsgegevens verwerkt dan zij voor de (onderkende en rechtmatig geachte) doelen nodig heeft. Vanwege het natuurlijke en wellicht gegronde wantrouwen dat de burger heeft betreffende de vastlegging van zijn persoonsgegevens lijkt het verstandig om te beschrijven hoe er aan deze punten voldaan gaat worden. Vanwege de eis op onloochenbaarheid van transacties moeten overheidsfunctionarissen ook uniek geïdentificeerd worden. Momenteel zijn er plannen om dit via hun eigen BSN te doen. Hierdoor komt er een directe koppeling tussen het doen en laten van het individu als hij werkzaam is als ambtenaar en privé-handelingen van het individu. Wanneer een overheidsfunctionaris bijvoorbeeld voor zijn functie bevoegd is om kinderporno op het web op te speuren worden deze handelingen ook aan hem als individu gekoppeld. Er zal een strikte scheiding van rollen geïmplementeerd moeten worden.

[20] De status van principes is verdeeld in verschillende categorieën. De uitleg van deze categorieën vind u in het rapport 'evaluatie NORA met de ADEM' te vinden op www.digital-architecture.net/scripties

Tabel 35 Compliant aan WBP.

Fase 2: Relatie principe-eisen en gevonden principes

In de aspectfase zijn 50 principe-eisen benoemd. Per element wordt er bekeken of er aan deze principe-eisen is voldaan. Het is niet altijd direct duidelijk welke principes uit de NORA gerelateerd kunnen worden aan de principe-eisen. Soms lijkt de omschrijving van het principe niet op de principe-eis maar wordt de relatie in de rationale van het principe duidelijk. De omschrijving van deze rationale wordt dan gegeven in de conclusie. Dit hoofdstuk geeft de relatie weer tussen de principe-eisen en de gevonden principes in de NORA. Niet alle principes die in de elementen genoemd zijn komen in deze tabel terug. Diverse principes waren niet direct te koppelen aan de principe-eisen maar hadden wel invloed op het betreffende element. Deze relatie is dan beschreven in de conclusie van het element. Voor de gevonden principes die wel direct aan principe-eis te relateren waren is een aparte tabel opgesteld welke hieronder getoond wordt.

PE	Principe-eisen aspectscan security & privacy	Wordt teruggevonden in principes in de NORA:
1	Er zijn principes die de organisatiedoelstellingen behartigen van beleid tot en met controle.	Principe 9.4.4. Overheidsorganisaties operationaliseren de wettelijke eisen aangaande privacy via een managementcyclus van beleid tot en met controle.
2	Op bedrijfsniveau worden prinicipes geformuleerd die aangeven hoe de organisatie wenst om te gaan met risicomanagement.	Principe 5.1.1.2. Overheidsorganisaties werken systematisch aan kwaliteitsverbetering.
		Er worden nog meer additionele eisen gesteld aan de risicoafweging in principe 9.3.1.
3	De principes zijn gebaseerd op requirements van de organisatie aangaande risicobeheersing.	Is niet teruggevonden.
4	Principe dat vastlegt dat security een integraal onderdeel is van de bedrijfsvoering.	Principe 9.3.1 Informatiebeveiliging is een integraal aspect van de bedrijfsvoering (corporate governance).

5	Risico's gerelateerd aan contact met externe partijen worden geïdentificeerd in de principes.	Principe 9.8.5. Middels (publiekelijke) voorlichting worden ook klanten van de diensten bewust gemaakt van de risico's en de noodzaak van beveiligingsmaatregelen.
		Principe 9.8.6. Let op de beveiliging, privacybescherming en continuïteit van de bedrijfsvoering bij ingekochte diensten.
6	Fysieke en logische grenzen zijn vastgesteld in het security beleid.	Is niet teruggevonden.
7	Er zijn principes voor de identificatie van de relevante bedrijfsprocessen en het vastleggen van kritische niveaus van verstoring van die bedrijfsprocessen.	Principe 9.8.3. Ketenorganisaties specificeren maatregelen (op het gebied van informatiebeveiliging, privacy en continuïteit) van bedrijfsvoering voor specifieke diensten en services op basis van de met die diensten en services samenhangende risico's.
8	Principes die duidelijk maken wat de implicaties van de security maatregelen zijn (organisatorisch, technisch, menselijk).	Bij de meeste principes is het duidelijk waar zij invloed op hebben. Echter is dit niet overal uitgewerkt.
9	Is er consistenties in de principes i.v.m. security (afstemming stakeholders, prioritering).	Voor elk principe is een status vastgelegd. Deze statussen zijn te vinden in de NORA en geven aan of het principe bijvoorbeeld gebaseerd is op wet en regelgeving en derhalve verplicht wordt gesteld.
10	Principes hebben een juiste proportionaliteit. Ze staan in verhouding tot het concern.	Bij het evalueren van de NORA zijn er veel principes gevonden die niet in verhouding staan met de concerns. Dit zijn vooral principes die een grote invloed hebben op het handelen van de burger. Dit is omschreven in de conclusie.
11	Principes worden opgebouwd in verschillende fysieke en logische lagen (security in depth).	Is niet teruggevonden.
12	Principes staan niet op zichzelf maar hebben een onderlinge relatie.	Elk principe is gerelateerd aan een van de hoofdprincipes van de NORA. Principes zijn gegroepeerd en hebben daarmee een onderlinge relatie.

13	Van elk principe dat een securitymaatregel voorstelt is duidelijk op welk gebied de maatregel wordt genomen (fysiek, organisatorisch, technisch of juridisch).	De inhoud van het principe maakt meestal duidelijk op welk gebied maatregelen genomen worden. De status van de principe vertelt ook of deze op wettelijke gronden genomen wordt of niet.
14	Bij de invoering van een principe zijn de kosten van de middelen niet hoger dan de mogelijke schade.	In de NORA is hier geen aandacht aan besteed.
15	Principes houden rekening met single point of failures	In de NORA is hier niet of nauwelijks aandacht aan besteed.
16	Principes die monitoring en logging afdwingen.	Principe 9.6.4. Op basis van monitoring geeft elke ketenorganisatie zekerheid over de naleving van de ketenafspraken.
17	Principes die afdwingen dat van informatie periodiek (routinematig) het niveau, sensitiviteit en kritiekheid wordt bekeken en opgeslagen.	Principe 6.1.1.7 Voor het ondersteunen van de controlefunctie van een organisatie kan gebruik gemaakt worden van een management informatie systeem.
		Principe 9.8.1. Om een service en de onderliggende informatie aantoonbaar goed te beveiligen en in de tijd ook beveiligd te houden moet elke organisatie een beveiligingscyclus voor de service inrichten.
		Principe 6. Om een vlotte dienstverlening mogelijk te maken leggen organisaties in het publieke domein routinematig uit te voeren controles binnen het primaire dienstverleningsproces. De noodzakelijke controles worden zo uitgevoerd dat een snelle en soepele dienstverlening plaatsvindt. Meer specifieke controles vinden in beginsel via afzonderlijke processen, parallel of achteraf plaats (eerst mensen, dan regels).
		Principe 9.8.1. Om een service en de onderliggende informatie aantoonbaar goed te beveiligen en in de tijd ook beveiligd te houden moet elke organisatie een beveiligingscyclus voor de service inrichten.
18	Principes die aangeven hoe er wordt geleerd van fouten.	Is niet teruggevonden.

19	Principes die vastleggen dat er gewerkt wordt met uniforme entiteiten (voor onweerlegbaarheid).	Zie PE 27.
20	Principes die de herleidbaarheid van transacties afdwingen.	Principe 5.3.1. Services triggeren elkaar en kunnen daardoor processen verbinden.
		Principe 9.7.1. Gebruik elektronische handtekeningen bij hoge eisen aan de onweerlegbaarheid van een bericht of transactie.
		Principe 9.7.7. De handelingen van overheidsmedewerkers (al dan niet in het kader van een aan een burger of bedrijf te leveren dienst) zijn tot op de persoon herleidbaar.
21	Security eisen afgedwongen in principes zijn door de gehele keten even sterk. De ketting is zo sterk als de zwakste schakel.	Principe 9.6.1. Convergentie van informatiebeveiliging, privacy en continuïteit van de bedrijfsvoering tussen (in ketens of netwerken) samenwerkende organisaties moet het gevaar van 'de zwakste schakel' voorkomen.
22	Principes die de authenticiteit van entiteiten door de gehele keten van services waarborgt.	Principe 9.7.4. E-overheidsorganisaties beveiligen de toegang tot hun diensten middels generieke authenticatie diensten op basis van DigiD en/of PKIoverheid.
		Principe 9.7.2 Tenminste bij transacties die een verplichting vormen voor een burger of bedrijf/instelling, zal de e-overheidsorganisatie kwijting geven van het afgerond hebben van een transactie / wezenlijke processtap.
		Principe 9.8.4. De service voldoet aan wet- en regelgeving en contractuele verplichtingen.
		Principe 9.7.6. Elektronische diensten worden verleend op basis van een bekende identiteit, waar het gaat om persoonlijke gegevens en transacties.

23	Principes zijn afgestemd op het beveiligingsbeleid.	Er is geen beveiligingsbeleid gevonden. Het is dus niet duidelijk of principes hierop afgestemd zijn. Wel zijn er diverse eisen aan de beveiliging genoemd. De principes binnen het element beveiligingsorganisatie voldoen aan de eisen die er gesteld zijn aan beveiliging.
24	Voor elk principe wordt de eigenaar vastgelegd.	Principe 9.3.2 De leiding van organisaties is verantwoordelijk voor een toereikende organisatie van informatiebeveiliging.
		Principe 9.6.2. Samenwerkende partijen leggen verantwoording af waarin zij de relatie leggen tussen de door hen getroffen maatregelen en de gemaakte keten / netwerkafspraken.
25	Voor elke asset wordt een asseteigenaar aangesteld.	Principe 6.2.2.2. Elk gegeven kent een eigenaar en een beheerder.
		Principe 6.2.6.2. Een gemeenschappelijk gegeven kent slechts één beheerder.
26	Principes die vastleggen wie er controle uitoefent op het naleven van organisatiedoelstellingen en geformuleerde principes.	Principe 9.3.2 De leiding van organisaties is verantwoordelijk voor een toereikende organisatie van informatiebeveiliging.
27	Principes die vastleggen dat er gewerkt wordt met uniforme entiteiten (voor onweerlegbaarheid).	Principe 9.7.1. Gebruik elektronische handtekeningen bij hoge eisen aan de onweerlegbaarheid van een bericht of transactie.
		Principe 7.2.1.3. Databasegegevens zijn herleidbaar tot de bron.
		Principe 9.7.2 Tenminste bij transacties die een verplichting vormen voor een burger of bedrijf/instelling, zal de e-overheidsorganisatie kwijting geven van het afgerond hebben van een transactie / wezenlijke processtap.
28	Principes die het veiligheidsniveau van de asset vaststellen.	Principe 6.2.2.3. De eigenaar van een gegeven is verantwoordelijk voor de kwaliteit (actualiteit, betrouwbaarheid) van een gegeven.
29	Principes die de beschikbaarheid van assets moeten waarbor-	Principe 9.8.2. De beschikbaarheid van de service is door de eigenaar gedefinieerd

	gen.	en geborgd.
30	Principes die de confidentialiteit van assets moeten waarborgen.	Is niet teruggevonden.
31	Principes die de integriteit van assets moeten waarborgen.	Is niet teruggevonden.
32	Principes die het melden van een incident verplichten.	Is niet teruggevonden.
33	Principes die aangeven hoe wordt omgegaan met de persoonlijke levenssfeer van het eigen personeel bij eventuele controles.	Principe 9.7.7. De handelingen van overheidsmedewerkers (al dan niet in het kader van een aan een burger of bedrijf te leveren dienst) zijn tot op de persoon herleidbaar.
		Principe 9.4.6. Bij controle op werknemers wordt het privacybelang van de werknemers door de werkgever in acht genomen.
		Principe 9.4.1. Organisaties waarborgen de persoonlijke levenssfeer (privacy)van natuurlijke personen door te voldoen aan de eisen uit de Wet Bescherming Persoonsgegevens en onderliggende richtlijnen zoals door het College Bescherming Persoonsgegevens uitgegeven.
34	Er wordt gebruik gemaakt van RBAC wanneer rechten aan rollen gekoppeld worden.	Is niet teruggevonden.
35	Rechten worden uitgedeeld op basis van 'need to know'.	Is niet teruggevonden.
36	Principes die vastleggen hoe de authenticiteit vastgelegd wordt van entiteiten.	Principe 5.2.1.14: Burgers krijgen door middel van het burgerservicenummer een digitale, unieke identiteit. Dit BSN dient maximaal door overheidsorganisaties te worden toegepast.

		Principe 5.2.1.15: Bedrijven en instellingen krijgen door middel van het bedrijven en instellingennummer een digitale, unieke identiteit. Dit BIN dient via tussenkomst van DigiD maximaal door overheidsorganisaties te worden toegepast bij de inrichting van hun communicatie met individuele bedrijven en instellingen.
37	Principes die vastleggen hoe autorisaties worden verleend aan de hand van een bekende authenticiteit.	Principe 9.7.6. Elektronische diensten worden verleend op basis van een bekende identiteit, waar het gaat om persoonlijke gegevens en transacties.
		Principe 9.7.4: E-overheidsorganisaties beveiligen de toegang tot hun diensten middels generieke authenticatie diensten op basis van DigiD en/of PKIoverheid
38	Authenticatie en authorisatie van gebruikers en processen om toegangscontrole te waarborgen wordt zowel binnen als buiten de domeinen toegepast.	Authenticatie binnen het domein vindt plaats via DigID. Buiten het domein, aan de balie, wordt de identificatiekaart eNik gebruikt.
39	Principes die de mate van toegang tot assets (high confidential, staatsgeheim) bepalen.	Is niet teruggevonden.
40	Principe dat vertelt of en hoe wordt omgegaan met single sign on.	Is niet teruggevonden.
41	Principes die te maken hebben met de bereikbaarheid van systemen houden rekening met mobiliteit en de gevaren hiervan.	Principe 7.3.1. 'Communicatie tussen overheidsorganisaties verloopt via of besloten, separate netwerken of door middel van een virtual private network verbinding via netwerken van particuliere bedrijven.
		Principe 7.3.2. 'Communicatie e-overheid en burgers/bedrijven vindt plaats via beveiligde internetverbinding of VPN'.
		Principe 7.3.3. 'Het interne netwerk van overheidsorganisaties is via één redundant en veilig uitgevoerde koppeling aangesloten op het publieke netwerk'

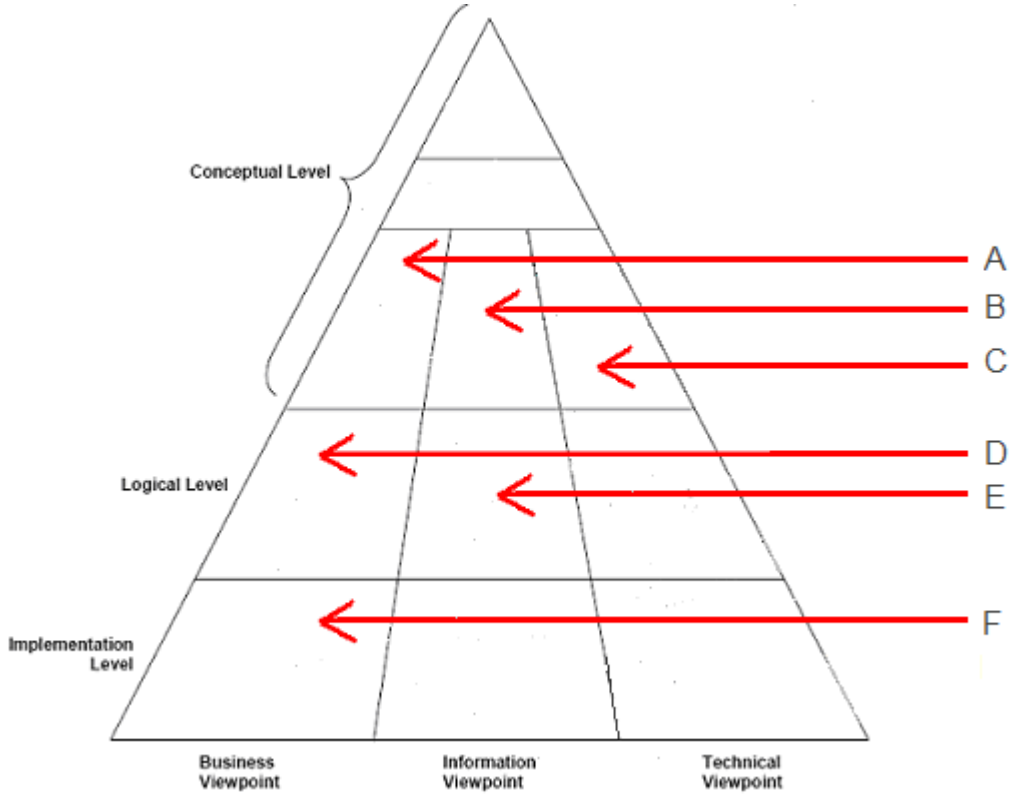
		Principe 1. Diensten via internet: organisaties in het publieke domein verlenen hun diensten aan burgers, bedrijven en maatschappelijke instellingen via het internet (elektronisch loket) en stimuleren het gebruik van dit kanaal.
		Principe 2. De bestaande kanalen zoals post, telefoon en balie blijven beschikbaar, zodat burgers, bedrijven en maatschappelijke instellingen gebruik kunnen maken van het kanaal van hun keuze.
42	Er zijn principes die de detectie van serieuze afwijkingen van de normale bedrijfsvoering afdwingen.	Principe 9.3.3. Security incidenten worden gesignaleerd, vastgelegd en gerapporteerd. Beveiligingsrelevante afwijkingen bij de uitvoering van processen worden aangemerkt als security incidenten.
43	Voor de principes is vastgelegd hoe incidenten worden vastgelegd en gerapporteerd.	Principe 7. Organisaties in het publieke domein kennen een transparante en toegankelijke klachten en bezwarenprocedure.
44	Bij uitval van systeemonderdelen is er een uitwijkmogelijkheid. Principe legt vast welke uitwijkmogelijkheden er zijn (bijvoorbeeld verschillende authenticatiemogelijkheden).	Principe 9.5.1. Organisaties richten een proces in voor de waarborging van de continuïteit van de diensten en services die via hun bedrijfsprocessen worden geleverd.
45	Principes die vastleggen hoe wordt omgegaan met rampen en ernstige verstoringen.	Is niet teruggevonden.
46	Principe dat vastlegt dat security incidenten worden gesignaleerd, vastgelegd, verwerkt en gerapporteerd. (het principe moet ook verwoorden wat een incident is, bij een keten dus ook weer de verantwoordelijke aanwijzen.)	Principe 9.6.4. Op basis van monitoring geeft elke ketenorganisatie zekerheid over de naleving van de ketenafspraken.
		Principe 9.3.3. Security incidenten worden gesignaleerd, vastgelegd en gerapporteerd. Beveiligingsrelevante afwijkingen bij de uitvoering van processen worden aangemerkt als security incidenten.

47	Prinicpes die te maken hebben met de opslag van persoonlijke gegevens voldoen aan indicatoren van het element WBP.	Principe 12. Organisaties in het publieke domein geven burgers, bedrijven en maatschappelijke instellingen inzicht in de status van voor hen lopende dienstverlenings-processen(transparante, traceerbare dienstverleningsprocessen).
48	Principe dat waarborgt of de organisatie voldoet aan nationale wet en regelgeving. (in nl is dit dus de wpb)	Principe 9.4.1. Organisaties waarborgen de persoonlijke levenssfeer (privacy)van natuurlijke personen door te voldoen aan de eisen uit de Wet Bescherming Persoonsgegevens en onderliggende richtlijnen zoals door het College Bescherming Persoonsgegevens uitgegeven.
49	Principe dat vastlegt aan wie informatie wordt verschaft betreffende gegevens van een individu of organisatie.	Principe 6.2.1.2. Gegevensverzamelingen die eigendom zijn van een overheidsorganisatie worden – met in achtneming van nadere wettelijke regels - ter beschikking gesteld aan de gehele overheid.
		Principe 15. Organisaties in het publieke domein maken zichtbaar wat zij doen, welke besluiten zij nemen, welke gegevens zij hebben en gebruiken en wat hun werkwijze is. (controleerbaar)
50	Principes die vastleggen welke technologieën gebruikt worden om privacy te waarborgen. (Best practise: PET)	Principe 9.4.7. Privacy wordt zoveel mogelijk in het ontwerp van geautomatiseerde systemen geborgd middels Privacy Enhancing Technologies.

Tabel 18: Relatie tussen principe-eisen en gevonden principes in de NORA.

Fase 3: Verdeling van principes in het EISA raamwerk

De plaatsing van de principes is geïllustreerd in figuur 2. Elk vak binnen het raamwerk heeft een unieke identificatie in de vorm van een letter. Deze letters worden gebruikt bij de bepaling waar de principes uit de NORA geplaatst moeten worden in het EISA raamwerk. Een principe kan vanuit verschillende viewpoints bekeken worden maar bevindt zich maar in één architectuurdimensie. Het principe kan wel naar beneden doorwerken en zo invloed hebben op lagere dimensies.



Figuur 2: Plaatsing van principes in het EISA raamwerk.

Legenda:

Plaats principe	Architectuurdimensie	Viewpoint
A	Conceptueel	Business
B	Conceptueel	Information
C	Conceptueel	Technical
D	Logisch	Business
E	Logisch	Information
F	Conceptueel	Business

Tabel 19: Legenda

Principes geplaatst in EISA raamwerk

Voor de hoofdprincipes uit de NORA is aangeven in welke architectuurlaag ze geplaatst moeten worden en tot welke laag de principes doorwerken. Tevens is voor elk principe bepaald welke views er mogelijk zijn.

NR	Hoofdprincipes uit de NORA	Plaatsing	Werkt door op
P1	Diensten via internet: organisaties in het publieke domein verlenen hun diensten aan burgers, bedrijven en maatschappelijke instellingen via het internet (elektronisch loket) en stimuleren het gebruik van dit kanaal.	A, B, C	Logical, Implementation
P2	De bestaande kanalen zoals post, telefoon en balie blijven beschikbaar, zodat burgers, bedrijven en maatschappelijke instellingen gebruik kunnen maken van het kanaal van hun keuze.	A, B, C	Logical, Implementation
P3	Organisaties in het publieke domein geven een helder, vindbaar beeld van de diensten en producten die burgers, bedrijven en maatschappelijke organisaties van hen kunnen afnemen. Daartoe zijn hun elektronische loketten benaderbaar via landelijke ingangen zoals de website www.overheid.nl (één loketgedachte, no wrong door).	D, E	Implementation
P4	Organisaties in het publieke domein bieden hun diensten (producten) bij voorkeur aan in voor de klant logische bundels per (soort) gebeurtenis aan de kant van de klant (geboorte, huwelijk, starten bedrijf) en werken daartoe samen met andere organisaties in het publieke domein (one-stop-shopping).	E	Implementation
P5	Burgers, bedrijven en maatschappelijke instellingen beschikken over één identiteit die bruikbaar is voor alle contacten met organisaties in het publieke domein en die afhankelijk van de soort dienstverlening ook nodig is en gevraagd moet worden. Dit ongeacht de keuze voor een kanaal. Een en ander komt neer op één administratieve identiteit (één identificatienummer). Deze administratieve identiteit dient afgebeeld te worden op een (ook digitaal toepasbaar) identiteitsbewijs.	F	Werkt niet verder door.
P6	Om een vlotte dienstverlening mogelijk te maken leggen organisaties in het publieke domein routinematig uit te voeren controles binnen het primaire dienstverleningsproces. De noodzakelijke controles worden zo uitgevoerd dat een snelle en soepele dienstverlening plaatsvindt. Meer specifieke controles vinden in beginsel via afzonderlijke processen, parallel of achteraf plaats (eerst mensen, dan regels).	F	Werkt niet verder door.
P7	Organisaties in het publieke domein kennen een transparante en toegankelijke klachten- en bezwarenprocedure.	A,B	Implementation
Administratieve lastenverlichting			
P8	Eenmaal opvragen van gegevens, meermalen gebruiken; de organisaties in het publieke domein zullen burgers en bedrijven niet opnieuw om gegevens vragen die bij de overheid al bekend zijn.	F	Werkt niet verder door.
P9	Organisaties in het publieke domein streven naar zo laag mogelijke administratieve lasten en een zo laag mogelijke regellast voor burgers, bedrijven en maatschappelijke organisaties.	A, B	Werkt niet verder door.

P10	Organisaties in het publieke domein zorgen voor een eenvoudige regelgeving, in omvang beperkt, onderling consistent en goed controleerbaar en handhaafbaar.	A	Logical
Transparantie			
P11	Organisaties in het publieke domein geven aan op welke momenten welke stadia in het dienstverleningsproces doorlopen dienen te zijn en streven daarbij naar zo kort mogelijke doorlooptijden.	A	Logical
P12	Organisaties in het publieke domein geven burgers, bedrijven en maatschappelijke instellingen inzicht in de status van voor hen lopende dienstverleningsprocessen (transparante, traceerbare dienstverleningsprocessen)	D	Werkt niet verder door.
P13	Organisaties in het publieke domein zorgen dat zij naar burgers, bedrijven en maatschappelijke instellingen periodiek verantwoording afleggen over de kwaliteit van de gerealiseerde dienstverlening	A, C	Werkt niet verder door.
P14	Organisaties in het publieke domein ontsluiten algemene overheidsinformatie, waaronder wet- en regelgeving.	A	Logical, Implementation
P15	Organisaties in het publieke domein maken zichtbaar wat zij doen, welke besluiten zij nemen, welke gegevens zij hebben en gebruiken en wat hun werkwijze is.	A,B,C	Logical
Pro-actieve dienstverlening			
P16	Organisaties in het publieke domein attenderen burgers en bedrijven op voor hen relevante diensten (pro-actieve dienstverlening), maar bieden ruimte voor eigen regie en verantwoordelijkheid door burgers en bedrijven op de feitelijke afname van diensten (zelfwerkzaamheid). Daarbij verstrekken organisaties begrijpelijke informatie, bij voorkeur geïndividualiseerd, over rechten, plichten en mogelijkheden voor burgers en bedrijven.	D,E,	Implementation
Integrale en betrouwbare overheid			
P17	Organisaties in het publieke domein organiseren zich als een onderdeel van een integraal opererende en als eenheid optredende overheid, die in haar handelen naar burgers, bedrijven en maatschappelijke instellingen consistent en betrouwbaar is.	A,B,C	Logical, Implementation
P18	Organisaties in het publieke domein gebruiken gegevens die accuraat, actueel en volgens wettelijke normen beveiligd zijn en delen die gegevens met andere organisaties in het publieke domein.	A,B,C	Logical, Implementation
Verbeteren doelmatigheid overheid			
P19	Gebruik waar mogelijk generieke componenten. Organisaties in het publieke domein streven er naar om beschikbare gemeenschappelijke voorzieningen te gebruiken, als deze op de punten functionaliteit, beveiliging en kosten gelijkwaardig zijn aan individuele voorzieningen.	F	Werkt niet verder door.
P20	Standaardiseer waar mogelijk koppelvlakken en hiermee samenhangende componenten. Organisaties in het publiek domein streven er naar hun koppelvlakken en hiermee samenhangende componenten te standaardiseren, waardoor het eenvoudiger wordt om in ketens samen te werken en gebruik te maken van generieke voorzieningen.	F	Werkt niet verder door.

Tabel 20: Hoofdprincipes NORA geplaatst in het EISA raamwerk

Conclusies

In dit hoofdstuk worden de belangrijkste bevindingen van de evaluatie met de aspectscan gedocumenteerd. Niet alle conclusies die naar boven zijn gekomen kunnen verwerkt worden in de huidige vorm van de aspectscan. Tijdens alle interviews en bijeenkomsten is er een breed beeld ontstaan over wat er speelt op het gebied van security en privacy binnen de NORA. Deze zaken liggen vaak op het gebied van maatschappelijke discussies. Hoe ver moet de overheid gaan in de dienstverlening naar de burger? Hoe ver kan de overheid gaan bij de controle op persoonsgegevens en het handelen van de burger? Door de ICTU wordt op diverse seminars naar mijn mening terecht aangegeven dat deze discussie buiten hun scope valt. Dit zijn breed maatschappelijke discussies en wet en regelgeving beïnvloeden de mogelijkheden die de architecten hebben wanneer zij de NORA vormgeven. In dit onderzoek wordt wel getracht inhoud te geven aan deze discussie en derhalve wordt aan deze onderwerpen in dit document aandacht besteed.

Doelstellingen van de NORA

De doelstellingen in de NORA om de burger tot dienst te zijn, zijn wellicht te ver doorgeschoten. Het lijkt een mooi uitgangspunt om burgers pro-actief te benaderen wanneer zij in aanmerking komen voor subsidies of belastingteruggave echter breekt dit ook in op de privacy van burgers. Veel burgers zijn niet gediend van een dergelijke bemoeizucht van de overheid. Zij willen niet pro-actief benaderd worden. Daarentegen moeten security experts ook toegeven dat er veel burgers zijn die dit wel appreciëren. Een goede balans moet daarom gevonden worden. Daarnaast moet de burger de mogelijkheid krijgen om zichzelf uit te sluiten van deze pro-actieve diensten. Deze mogelijkheid wordt momenteel nog niet geboden. De illustratie hieronder geeft dit beeld weer.

Infrastructuur

De infrastructuur die de NORA biedt geeft de mogelijkheid om diverse overheidssystemen aan elkaar te koppelen. Dit gebeurt ook op grote schaal. In de NORA worden alleen doelstellingen genoemd die te maken hebben met de dienstverlening aan de burger. We moeten echter niet vergeten dat deze koppelingen er ook zijn

om de burger te controleren. Dit kan misschien wel niet de doelstelling van de NORA zijn, echter maakt de overheid er wel gretig gebruik van. Systemen van de sociale dienst worden gekoppeld aan het RDW om te controleren of personen die een uitkering hebben niet in een dure luxe auto rijden. Wellicht moeten we als belastingbetaler blij zijn met deze controle echter moeten wij als burgers wel onze grenzen bewaken. De overheid zou in eerste instantie uit moeten gaan van een goede vertrouwensband met de burger. In het publiek strafrecht worden wij pas als verdachte gezien wanneer hier aanleiding toe is. Bij het vooraf en periodiek controleren van gegevens kunnen wij al eerder als verdachte worden aangemerkt zonder dat hier wellicht aanmerking toe is. Daarnaast moeten we ook kijken naar de toekomst. We hebben nu een overheid die als 'betrouwbaar' gezien kan worden. Er zijn echter tijden geweest dat er geen betrouwbare overheid was. In de tweede wereld oorlog heeft de Duitse bezetter gebruik gemaakt van gemeentelijke administraties bij de opsporing van Joden. Wanneer er in de toekomst nog eens een overheid plaatsneemt die het minder voor heeft met zijn burgers is er een infrastructuur gelegd waarmee ongekende mogelijkheden zijn. Dit doemscenario moet ons niet meteen laten terugdeinzen om nieuwe systemen en infrastructuren te ontwikkelen echter moeten wij wel goed nadenken voor dat we handelen.

Profiling

Met de koppeling van systemen zijn er ook meer mogelijkheden om profielen te maken van burgers. Welke informatie vragen zij op en welke bezwaren worden er ingediend. Alle interacties die de burger met de overheid heeft kunnen in principe opgeslagen worden als de overheid een legitiem doel kan vinden om deze data op te slaan. Met het bijhouden van aanvragen voor diensten ontstaat er dus een soort profiel van de burger. De angst voor het ontstaan van een 'bad' profile kan de burger belemmeren in zijn persoonlijke doen en laten. Bij het opslaan van gegevens wordt er vaak luchtig gereageerd en dat is onterecht. We moeten ons hierbij van bewustzijn dat alle gegevens die er opgeslagen worden wellicht later van groter belang kunnen worden. Momenteel is het geen probleem om de meisjesnaam van de moeder van een individu op te slaan. Maar wat als deze informatie straks een authenticatiemiddel wordt om toegang te krijgen tot informatie. Het noemen van een geboortedatum en adres is vaak al voldoende om toegang te krijgen tot persoonlijke gegevens van een individu. De overheid geeft op de website waar de e-overheid geëtaleerd wordt al een slecht voorbeeld. De volgende disclaimer geeft aan wat de overheid doet met gegevens die worden achtergelaten op de website.

'Doel en verwerking van (persoons)gegevens

Met het registreren van gegevens van bezoekers van de website(s) beoogt Kenniscentrum de effectiviteit van haar website(s) te verbeteren. Gegevens met betrekking tot datum, tijd en duur van uw bezoek aan de website(s) verwerkt Kenniscentrum voor het vastleggen van voorkeuren van alle betrokkenen. Deze gegevens worden ***niet*** *na de sessie verwijderd.*

Voor het gebruik van deze adressen geldt, dat alleen de gegevens gebruikt worden die de bezoeker zelf actief achtergelaten heeft en dat adressen niet aan derden ter beschikking worden gesteld of gebruikt voor andere doeleinden dan waarvoor de bezoeker ze heeft achtergelaten. Bovendien wordt de adressenlijst slechts gebruikt

door Kenniscentrum. Ook verzamelt Kenniscentrum geen adressen middels op deze site aangeboden bestelformulieren of andere vormen van elektronische feedback.'

Bron: http://www.e-overheid.nl/privacy/

Het is een prima initiatief om in ieder geval te verkondigen wat de website doet met gegevens die ingevuld worden maar hier blijkt al uit dat gegevens worden opgeslagen zonder dat de burger hier invloed op heeft. Ik kan er voor kiezen om de website niet te gebruiken, echter als ik informatie nodig heb word ik gedwongen om informatie af te staan.

De architectuurdocumentatie

De architectuurdocumentatie over de NORA is hoofdzakelijk volgens het boekje. Zowel in de voorbereidende scan, de holistische scan en deze aspectfase komen de meeste eisen die gesteld worden terug in de NORA. Er is duidelijk nagedacht over de inhoud van het document, hiervoor de complimenten. Vanwege het abstracte karakter van de NORA zijn er echter wel veel interpretatiemogelijkheden. De elementen zijn weinig concreet en overheidsinstanties kunnen dus hun eigen interpretatie geven aan security en privacy vraagstukken. Of een architectuur die gebaseerd is op de referentiearchitectuur de NORA echt veilig is kan niet gezegd worden.

Reflectie op de belangrijkste principes

Het principe eenmalige gegevensverstrekking moet er voor zorgen dat de burger maar een keer zijn gegevens hoeft te verstrekken aan de overheid. De overheid is er zelf verantwoordelijk voor dat de gegevens die verstrekt zijn bij de onderlinge instanties terecht komt. Dit principe heeft veel invloed op de kwaliteit van de informatie. Wanneer de informatie correct verstrekt wordt hebben alle overheidsorganisaties hier profijt van. Wanneer er echter een fout in de data sluipt wordt deze fout door de gehele keten getransporteerd. Het ligt in de lijn der verwachtingen dat er veel kopieën zullen komen van databases. Afzonderlijke overheidsorganisaties hebben veel legacy systemen die niet aangesloten kunnen worden op de standaard basisregistraties. Om toch gebruik te kunnen maken van deze data worden kopieën opgeslagen. Het kan dus erg moeilijk worden om een fout ongedaan te maken.

Het principe

'Burgers, bedrijven en maatschappelijke instellingen beschikken over één identiteit die bruikbaar is voor alle contacten met organisaties in het publieke domein en die afhankelijk van de soort dienstverlening ook nodig is en gevraagd moet worden. Dit ongeacht de keuze voor een kanaal. Een en ander komt neer op één administratieve identiteit (één identificatienummer). Deze administratieve identiteit dient afgebeeld te worden op een (ook digitaal toepasbaar) identiteitsbewijs'

heeft veel invloed op de relatie tussen de burger en de overheid. Elke burger krijgt één identiteit en de overheid correspondeert dus altijd met de burger via deze ene bekende identiteit. Veel burgers voelen er weinig voor om bij elke overheid instantie

met dezelfde entiteit te communiceren. Ik wil mijn gegevens ook niet aan alle overheidsinstanties geven. Deze entiteiten zijn momenteel nog niet met elkaar verenigd, echter in de toekomstige situatie bestaat deze rollenscheiding niet meer. Veel van deze concerns worden ook door experts benoemd. Zo geeft ook Prof. Bart Jabobs invulling aan deze discussie in zijn boek de menselijke maat in ICT[21].

Mandaat

Een veel gehoorde klacht over de NORA is het gebrek aan mandaat. Dit heeft betrekking op de gehele overheid dus ook als het gaat over beveiliging. De diverse overheidsinstanties hebben veel vrijheden. Het is moeilijk om iemand bij de overheid aan te wijzen die verantwoordelijk is voor het correct functioneren van de e-overheid. De lead-architect van de NORA, Guido Bayens, geeft aan dat het niet opleggen van de architectuur er juist voor zorgt dat veel overheidsorganisaties zich willen aansluiten bij de NORA. Gedeeltelijk heeft de architect het hier bij het goede eind. Er zijn binnen de overheid al vaker programma's uitgerold die een e-overheid wilden bewerkstelligen. Het lijkt echter niet onverstandig iemand hier toch als verantwoordelijke voor aan te wijzen. De bouwers van de NORA kunnen immers niet als verantwoordelijke worden aangewezen. Een goed initiatief dat wordt geopperd op het via nova forum[22] is het aanstellen van een rijksbouwmeester. Ik daag de lezer van mijn scriptie uit om aan deze discussie een bijdrage te leveren.

[21] Jacobs, B. De Menselijke Maat in ICT. Januari 2007. ISBN: 978-90-9021619-5

[22] De discussie is te vinden op http://www.via-nova-architectura.org/special-features/moet-er-een-digitale-rijksbouwmeester-k-2.html

Bijlage 2: De ADEM

Architectuurdocumentatie Evaluatie

Aanzet tot een methode om architectuurdocumentatie te evalueren

Te vinden op

www.digital-architecture.net/scripties

Auteur:	Ing. D.S. (David) Campbell Ing. Y.H.C. (Yves) Janse P.J. van Vlaanderen, B ICT	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:	Definitieve versie	
Begeleider:	prof. dr. Daan Rijsenbrij	
Referent:	prof. dr. Erik Proper	

Bijlage 3: Evaluatie van de ADEM met de NORA

Evaluatie Nederlandse Overheid Referentie Architectuur

Uitvoering van de Globale Fase

Te vinden op

www.digital-architecture.net/scripties

Auteur:	Ing. D.S. (David) Campbell Ing. R.P. (Robin) van 't Wout P.J. van Vlaanderen, B ICT
Plaats:	Nijmegen
Datum:	25-06-2007
Versie:	1.0
Status:	Definitieve versie
Begeleider:	prof. dr. Daan Rijsenbrij
Referent:	prof. dr. Erik Proper