Referentie architectuur voor beveiliging

voor hooggerubriceerde omgevingen, uitgewerkt in een beveiligingsarchitectuur voor informatiestromen.

TU-Delft, Faculteit Techniek, Bestuur en Management
Afstudeerscriptie EPA, sectie ICT
M. van Oosten (1117297)
5-7-2012

Afstudeercommissie

Voorzitter	: Prof. dr. Y.H. Tan (TBM Hoofd sectie ICT)
Eerste begeleider	: Dr.ir. J. van den Berg (TBM sectie ICT)
Dagelijks begeleider	: Dr.ir. S. Daskapan (TBM sectie ICT)
Dagelijks begeleider	: Dr.ir. H.J. Honig (TBM sectie systeemkunde)
Extern begeleider	: Dr. L. Matthijssen

Afstudeerscriptie

TU Delft
Faculteit : Techniek, Bestuur en Management
Sectie : Informatie en Communicatie Technologie
Afstudeerrichting : Engineering and Policy Analysis
Studienummer : 1117297

Op 8 november 2011 heeft Mw Ir. M.H.P.C. Bos namens de examencommissie toestemming verleend om deze scriptie in het Nederlands te mogen schrijven.

M. van Oosten
Delft, 5 juli 2012

Managementsamenvatting

Ketensamenwerking binnen de Nederlandse veiligheidssector is sterk in ontwikkeling. Deze ontwikkeling wordt gedreven door de noodzaak om in een steeds eerder stadium in staat te zijn bedreigingen van de nationale Veiligheid te onderkennen. Deze ketensamenwerking moet mogelijk gemaakt worden binnen de informatievoorzieningen van rijksoverheidsorganisaties. De veiligheidssector heeft een aantal specifieke kenmerken die ketensamenwerking complex maakt. Vanwege de bedreigingen van Nationale Veiligheid en de bijzondere bevoegdheden die worden gebruikt in onderzoek naar deze dreigingen, is de rubricering van de informatie die wordt gedeeld hoog: Staatsgeheim. Wet- en regelgeving waar de ketenpartners zich aan moeten houden is sectoraal georganiseerd, soms verouderd en op enkele punten zelfs tegenstrijdig. Voor de inrichting van de informatiekoppelingen en de verwerking van deze informatie binnen de verschillende Rijksoverheidsorganisaties zijn aanpassingen nodig in de informatievoorziening omdat de natuurlijke ontwikkeling hiervan heeft plaatsgevonden op basis van beveiligingsconcepten die uitgingen van geslotenheid. Dit staat op gespannen voet met ketensamenwerking. Doel van het onderzoek is om een beveiligingsarchitectuur te ontwerpen waarmee in de Nederlandse veiligheidsketen veilig hooggerubriceerde informatie gedeeld kan worden om de Nationale Veiligheid zo goed mogelijk te waarborgen. Hiervoor is een beveiligingsarchitectuur nodig die sturend is voor de wijze waarop informatiekoppelingen ten behoeven van samenwerkingsverbanden tot stand worden gebracht. Ook is het belangrijk dat de strategie van beveiliging wordt herzien en dat de informatievoorzieningen die ketensamenwerking ondersteunen worden aangepast. Dit zorgt ervoor dat de beveiliging integraal gewaarborgd is, deze meetbaar wordt gemaakt, de samenhang goed bewaakt en dat beveiligingsoplossingen efficiënt en beheersbaar zijn.

De hoofdvraag is op de volgende manier uitgewerkt in onderzoeksvragen:

1. Aan welke randvoorwaarden en ontwerpeisen moet de beveiligingsarchitectuur voldoen?
2. Welke ontwerpeisen zijn van toepassing op architecturen en beveiligingsarchitecturen?
3. Uit welke elementen bestaat een beveiligingsarchitectuur?
4. Hoe ontstaat de beveiligingsarchitectuur voor informatiestromen?

Deze onderzoeksvragen zijn uitgewerkt door middel van literatuuronderzoek op het gebied van Enterprise Architecturen, beveiligingsarchitecturen en referentiearchitecturen en een ontwerpstudie, waarin is vastgelegd op welke wijze de beveiligingsarchitectuur precies tot stand is gekomen.

Het uiteindelijke product is een beveiligingsarchitectuur die is opgebouwd uit een referentiearchitectuur voor beveiliging en beveiligingsarchitecturen. De referentiearchitectuur voor beveiliging bevat gemeenschappelijke elementen voor beveiliging en een proces waarmee beveiligingsarchitecturen voor specifieke aspectgebieden van beveiliging kunnen worden geproduceerd. In de ontwerpstudie is het aspectgebied “informatiestromen” uitgewerkt naar een beveiligingsarchitectuur voor informatiestromen. Deze beveiligingsarchitectuur geeft het antwoord op de vraag hoe in een hooggerubriceerde omgeving ketensamenwerking mogelijk gemaakt kan worden.

Belangrijke conclusies uit dit onderzoek zijn dat beveiligingsarchitectuur voor informatiestromen beantwoordt aan de hoofdvraag, met enkele tekortkomingen die niet problematisch zijn. Op basis van de ervaringen die inmiddels zijn opgedaan, is toepassing van de beveiligingsarchitectuur voor informatiestromen in hooggerubriceerde omgevingen binnen andere delen van de rijksoverheid mogelijk, en wellicht zelfs in andere sectoren.

Inhoudsopgave

Lijst met afkortingen

A&K analyse: Afhankelijkheids- en Kwetsbaarheidsanalyse
ADM: Architecture Design Method
BBNP: Basis Beveiligingsniveau Nederlandse Politie
BCM: Business Continuity Management
Cert-CC: Cert Coordination Centre, Software Engineering Institute at Carnegie mellon University, Verenigde Staten
CISSP: Certified Information Systems Security Professional
CT-infobox: Contra-terrorsime Infobox
GAAOC: Generally Accepted Areas Of Concern
GBA: Wet Gemeentelijke Basis Administratie
KPI: Key Perfomance Indicator
MARIJ: Model Architectuur Rijksdienst
MIVD: Militaire Inlichtingen- en Veiligheidsdienst
NCC: Nationaal Crisis Centrum
NCTV: Nationaal Coördinator Terrorisme en Veiligheid
Nora: Nederlandse Overheid Referentie Architectuur
O-ISM3: The Open Group Information Security Management Maturity Model
PKI: Public Key Infrastructure
ROI: Return On Investment
TOGAF: The Open Group Architecture Framework
VIR: Voorschrift Informatiebeveiliging Rijksdienst
Vir-BI: Voorschrift Informatiebeveiliging Rijksoverheid - Bijzondere Informatie
VIR-GI: Voorschrift Informatiebeveiliging Rijksoverheid – Gerubriceerde Informatie
WIV: Wet op de Inlichtingen- en Veiligheidsdiensten
WJSG: Wet justitiële en strafvorderlijke gegevens
WOB: Wet Openbaarheid van Bestuur
WRR: Wetenschappelijke Raad voor Regeringsbeleid

Lijst met tabellen

Lijst met Figuren

1 Inleiding

Ketensamenwerking in de veiligheidssector van de Nederlandse Rijksoverheid wordt steeds meer gezien als belangrijk middel om eerder in staat te zijn bedreigingen van Nationale Veiligheid te onderkennen. Maatschappelijke- en technische ontwikkelingen op het gebied van radicalisering, terrorisme en de ontwikkeling van dreigingen die het Internet introduceert (Cyber) hebben ketensamenwerking op de politieke agenda geplaatst. Het idee achter verregaande ketensamenwerking is dat de actoren die uit zijn op aantasting van de Nationale Veiligheid altijd sporen nalaten. Door het aangaan van samenwerkingsverbanden kan informatie die bekend is binnen verschillende organisaties in de veiligheidsketen worden gecombineerd om zo het inzicht van de organisaties in de veiligheidsketen en daarmee de kans dat vroegtijdig kan worden ingegrepen, te vergroten. Meer dan eens is aangetoond dat bij toeval ontdekte relaties in informatie bij verschillende ketenparters in op zichzelf losstaande onderzoeken, ernstige gebeurtenissen hebben kunnen voorkomen (de Wijk, 2005).

Bij de realisatie van samenwerkingsverbanden is het noodzakelijk dat er technische koppelingen tot stand worden gebracht om het delen van de informatie praktisch gezien mogelijk maken. Ontwikkelen van relaties met ketenpartners betekent dat deze partijen tot op zekere hoogte toegelaten zullen moeten worden tot de eigen interne, hooggerubriceerde informatievoorziening. Van oudsher zijn de informatievoorzieningen tot stand gekomen op basis van de achterliggende beveiligingsconcepten in de huidige regelgeving: veelal opgebouwd als een gesloten geheel, gebaseerd op het slotgracht model: hoge buitenmuren en van binnen redelijk open. Grootschalig informatie delen met de buitenwereld past niet in dit plaatje. De beveiligingsstrategie waarop de informatiebeveiliging is gebaseerd zal moeten worden veranderd.

Ketensamenwerking introduceert een aantal additionele dilemma's als vanuit het informatie management-, juridisch-, organisatorisch en beveiligingsperspectief naar wordt gekeken (deze lijst is niet uitputtend):

- Wat betekent informatie delen tussen organisaties die van oudsher een zeer gesloten informatiehuishouding kennen? De organisaties zijn gewend om vooral op eigen kracht te voorzien in hun informatiebehoefte, samenwerking met ketenpartners is nooit een strategisch uitgangspunt geweest;
- De informatie waar het hier om gaat is meestal voorzien van een hoge rubricering[1] (Departementaal vertrouwelijk, Staatsgeheim Confidentieel, Staatsgeheim Geheim en Zeer geheim). Dit heeft vooral gevolgen voor de exclusiviteit van deze informatie: beveiligingskaders schrijven een strike Need-to-Know voor (zeer beperkte toegang tot de informatie) terwijl het samenwerken brede toegang impliceert (Need-to-Share);
- Hoe kun je informatie delen als technische koppelingen volgens de geldende beveiligingskaders niet toegestaan zijn? Beveiligingskaders hebben een respectabele leeftijd en zijn niet ingericht op het beantwoorden van de vragen die geïntroduceerd worden bij het aangaan van samenwerkingsverbanden;
- Hoe kun je informatie delen tussen organisaties die vanuit verschillende wettelijke kaders en beveiligingskaders opereren?
- Hoe kun je de informatieverwerking van gegevens die afkomstig zijn van ketenpartners en andere derde partijen veilig organiseren, waarbij de risico's die worden geïntroduceerd voor de eigen informatievoorziening beheersbaar blijven?

Het delen van informatie vermindert het risico op het missen van essentiële aanwijzingen. Aan de andere kant neemt hierdoor het risico juist toe voor:

- het weglekken van informatie omdat deze breder wordt gedeeld;
- mogelijke fouten door interpretatie van informatie buiten de context waarbinnen de informatie tot stand is gekomen.

[1] Dit is de terminologie die de rijksoverheid hanteert (vanuit het Voorschrift Informatiebeveiliging Rijksoverheid – Bijzondere Informatie); sommige organisaties (zoals Defensie of Politie) hanteren een aangepaste naamgeving, de beveiligingsniveaus zijn echter vergelijkbaar.

Voor de uitwerking van deze visie op informatiemanagement wordt gebruik gemaakt van architecturen. Onder de vlag van Enterprise Architectuur (EA) volgens the Open Group Architecture Framework (TOGAF) wordt, daar waar nodig, gebruik gemaakt van architectuur.

1.1 Doel van het onderzoek

Er is een aantal trends zichtbaar die een duidelijke koersverandering vereisen als het gaat om de wijze waarop de informatievoorziening en de bedrijfsprocessen beveiligd zullen moeten worden. De in de vorige paragraaf geschetste dilemma's zijn niet nieuw, maar de huidige omstandigheden vereisen dat deze onderwerpen opnieuw ter discussie worden gesteld. De belangrijkste aspecten die een rol spelen:

- De noodzaak om samenwerking te intensiveren omdat de maatschappij van ons vraagt in een steeds eerder stadium alert te zijn op bedreigingen van de nationale veiligheid;
- De geldende informatiebeveiligingswet- en regelgeving voor bijzondere informatie is gebaseerd op zeer principiële uitgangspunten die een obstakel vormen bij het inrichten van de noodzakelijke informatiekoppelingen. De regelgeving conflicteert met de taken en doelstellingen van de organisatie;
- De situatie op basis waarvan er nu met partijen informatie wordt uitgewisseld, leidt tot een divers spectrum aan communicatie oplossingen. Het beheer hiervan is arbeidsintensief en het is duur om informatie uitwisseling tot stand te brengen;
- Er is sprake van onnodige complexiteit in infrastructuuroplossingen die beveiligingsrisico's met zich mee brengt.

Er is een oplossing nodig waarbij de informatievoorziening beheersbaar, betaalbaar en veilig blijft. Dit leidt tot de volgende probleemstelling:

> *Hoe kan architectuur worden ingezet om mogelijk te maken dat organisaties hooggerubriceerde informatie kunnen delen met relevante partners binnen het Nederlandse Veiligheidsdomein en daarbuiten om de ketensamenwerking te bereiken die nodig is om de Nationale Veiligheid te waarborgen, zonder dat daarbij de beschikbaarheid, integriteit en exclusiviteit van de informatie in gevaar komt.*

In dit rapport wordt deze probleemstelling benaderd vanuit het perspectief van beveiliging.

Beveiliging wordt bij het ontwerpen van systemen gezien als een aandachtspunt en is veelal geen uitgangspunt. In de praktijk wordt de beveiliging in een relatief laat stadium in het systeemontwerp aangebracht. Helaas zijn de beveiligingseisen die van toepassing zijn op systemen waarin hooggerubriceerde informatie wordt verwerkt zodanig hoog dat structurele wijzigingen in het systeem, naar aanleiding van bijgestelde beveiligingseisen, dan onvermijdelijk zijn.

Bij het ontwerpen van systemen is de praktijksituatie dat slechts zeer beperkt wordt aangegeven op welke wijze specifieke beveiligingsoplossingen binnen systemen tot stand moeten komen. Er ontbreekt een architectuur.

Beveiliging wordt bij het ontwerpen van systemen meestal benaderd vanuit de historie. Open systemen en systeemkoppelingen met ketenpartners introduceren een heel nieuw spectrum aan dreigingen waarmee rekening gehouden moet worden in een systeemontwerp.

1.1.1 Oplossingsrichting

De oplossingsrichting voor de aangegeven beveiligingsproblemen wordt gezocht in een architectuur. Architectuur (Buffam, 2000, p. 14 e.v.) is een middel om een informatievoorziening te realiseren die:

- waarborgt dat strategische uitgangspunten worden nageleefd;
- de onderlinge samenhang tussen systemen of componenten daarvan vastlegt en waarborgt dat een ontwerp uitlegbaar is;
- zodanig flexibel is, dat snel ingespeeld kan worden op wijzigingen in strategische doelstellingen;
- complexiteit reduceert;
- tot kostenbeheersing leidt.

Vanwege de mogelijke voordelen van architectuur en de gehanteerde werkwijze voor ontwikkeling van de informatievoorziening binnen de rijksoverheid mag verwacht worden dat architectuur een veelbelovende oplossingsrichting biedt in de geschetste beveiligingsaanpak.

1.1.2 Onderzoeksvragen

De hoofdvraag luidt daarmee:

> *Ontwerp een beveiligingsarchitectuur voor een hooggerubriceerde informatievoorziening die het mogelijk maakt dat de organisatie kan voldoen aan de doelstellingen op het gebied van ketensamenwerking.*

Ketensamenwerking betekent voor de informatievoorziening het tot stand brengen van koppeling met derde partijen, het faciliteren van de verwerking van informatiestromen die de organisatie in en uitgaan en het vastleggen van deze informatie in een informatiesysteem zodat het ontsloten kan worden voor eindgebruikers.

Er zal onderzoek moeten worden verricht om vast te stellen wat de beveiligingsarchitectuur nu eigenlijk is en op welke wijze ketensamenwerking kan worden ondersteund. De scope en bedoelde omvang van dit onderzoek laat niet toe dat een volledig ingevulde beveiligingsarchitectuur wordt opgeleverd. Invulling van de beveiligingsarchitectuur vindt plaats voor zover dat voor de ondersteuning van informatie uitwisseling met ketenpartners noodzakelijk is.

De hoofdvraag is als volgt uitgewerkt in vier deelvragen:

1) Wat zijn de randvoorwaarden en ontwerpeisen waaraan de beveiligingsarchitectuur moet voldoen?
    a. Gezien de strategische context van de organisatie?
    b. Gezien de eisen die de organisatie stelt?

Deze vraag zal worden beantwoord in hoofdstuk 2.

2) Welke ontwerpeisen zijn van toepassing op architecturen en beveiligingsarchitecturen?

Deze vraag wordt beantwoord in hoofdstuk 3 door een theoretische analyse uit te voeren van relevante architectuurraamwerken, enterprise architecturen en beveiligingsarchitecturen.

3) Uit welke elementen bestaat een beveiligingsarchitectuur?

Deze vraag zal worden beantwoord in hoofdstuk 4 door op basis van de ontwerpeisen en randvoorwaarden bouwelementen te selecteren. Deze vormen samen een referentiearchitectuur[2] voor beveiliging (zie paragraaf 3.2). Deze referentiearchitectuur zal in hoofdstuk 5 worden toegepast op het aspectgebied informatiestromen:

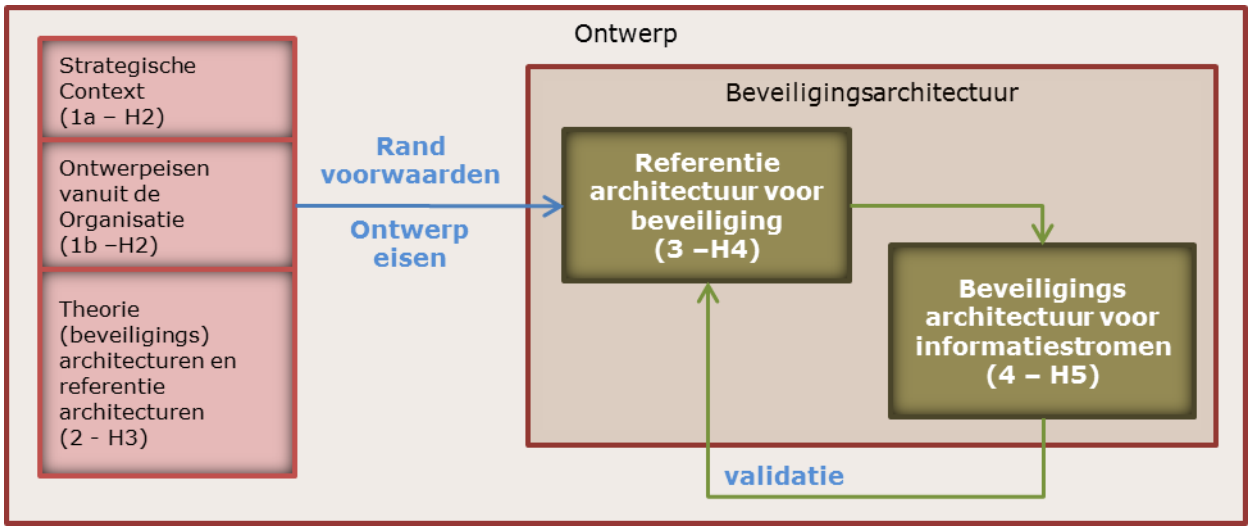
4) Hoe ontstaat de beveiligingsarchitectuur voor informatiestromen?

Dit is een uitgewerkt architectuurproduct dat voorschrijft hoe informatiekoppelingen gerealiseerd kunnen worden, waarmee de ketensamenwerking uiteindelijk wordt mogelijk gemaakt. Hiermee is de hoofdvraag beantwoord.

[2] Het uiteindelijke ontwerp is een referentiearchitectuur voor beveiliging.

1.2 Onderzoeksplan en methode

De wijze waarop de beveiligingsarchitectuur tot stand komt is zichtbaar gemaakt in het ontwerpmodel in Figuur 1. De nummering in de figuur verwijst naar de deelvragen uit paragraaf 1.1.2 en de hoofdstukken van dit document waarin de deelvragen zijn uitgewerkt.



Figuur 1: Ontwerpmodel

De bovenste twee rode blokken in het ontwerp hebben betrekking op hoofdstuk 2 waarin een ontwerponderzoek is uitgevoerd om de randvoorwaarden en ontwerpeisen uit organisaties in de Nederlandse veiligheidsketen te bepalen:

- De strategische context;
  Hier worden randvoorwaarden en ontwerpeisen in kaart gebracht, op basis van een analyse van het veiligheidsdomein, wetgeving en informatiebeveiligingsvraagstukken.
- Ontwerpeisen vanuit de Organisatie
  De organisatie zelf stelt eisen op het gebied van werkwijze, processen, te gebruiken externe standaarden, kaders en richtlijnen. Ook het beschrijven van de architectuur, de vorm waarin de architectuur wordt uitgewerkt en wijze waarop deze moet worden gerealiseerd, wordt bepaald door randvoorwaarden die de organisatie stelt.

Het onderste rode blok in het ontwerp heeft betrekking op hoofdstuk 3 waarin literatuuronderzoek heeft plaatsgevonden:

- Theorie van (beveiligings)architecturen en referentiearchitecturen:
  Deze informatie wordt gebruikt om te bepalen uit welke bouwelementen een beveiligingsarchitectuur moet bestaan en aan welke ontwerpeisen een goede beveiligingsarchitectuur moet voldoen. Door de theoretische analyse wordt voortgebouwd op bestaande theoretische kennis.

Informatiebeveiliging kent een aantal verschillende deelgebieden of aspecten zoals toegangscontrole, identity management, autorisatiebeheer, informatiestromen, etc. Uit de referentiearchitectuur voor beveiliging worden beveiligingsarchitecturen voor specifieke aspectgebieden afgeleid. Dit onderzoek is beperkt in scope tot het uitwerken van het aspectgebied informatiestromen met als product de beveiligingsarchitectuur voor informatiestromen.

De referentiearchitectuur voor beveiliging (zie Figuur 1) bevat:

- een proces waarin is vastgelegd hoe een beveiligingsarchitectuur voor een aspectgebied tot stand komt;
- elementen die nodig zijn om de beveiligingsarchitectuur voor een aspectgebied te produceren.

Het doel is om vanuit een referentiearchitectuur voor beveiliging een beveiligingsarchitectuur voor informatiestromen te genereren. Deze beveiligingsarchitectuur voor informatiestromen

dient als kader voor de realisatie van beveiligingsoplossingen voor het koppelen van informatievoorzieningen.

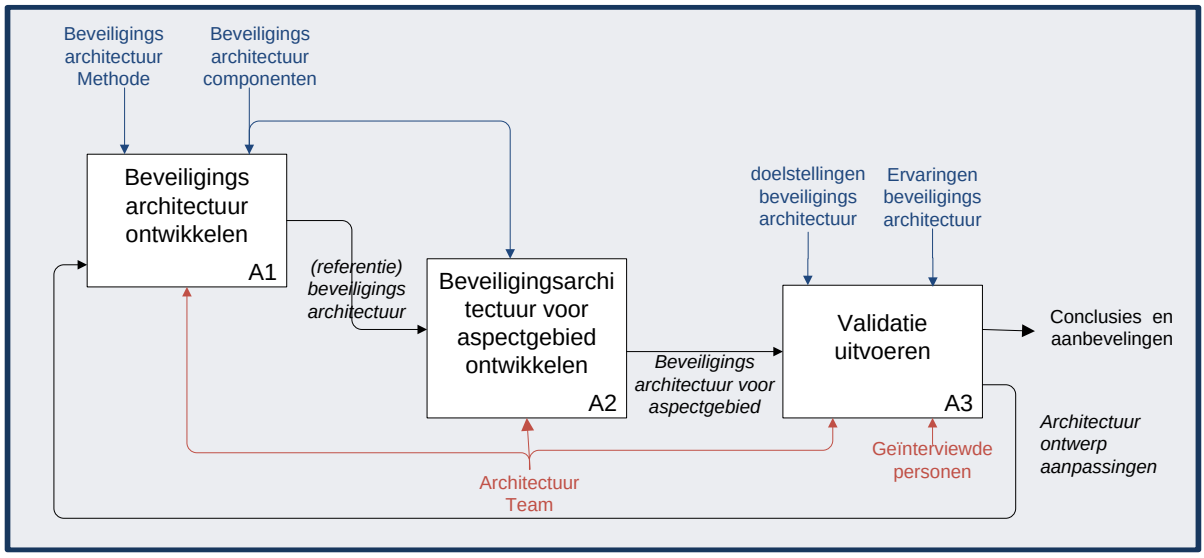
De relatie tussen de beveiligingsarchitectuur, referentie architectuur voor beveiliging en de beveiligingsarchitectuur voor informatiestromen is dat de beveiligingsarchitectuur bestaat uit een referentiearchitectuur voor beveiliging en de beveiligingsarchitectuur voor een aspectgebied.

In hoofdstuk 4 wordt een ontwerponderzoek uitgevoerd om op basis van de ontwerpeisen en randvoorwaarden de referentiearchitectuur voor beveiliging te ontwerpen.

In Hoofdstuk 5 wordt aangegeven hoe beveiligingsarchitectuur voor informatiestromen tot stand komt. Dit is voor wat betreft de specifieke eigenschappen van het aspect gebied informatiestromen een ontwerpstudie, het is ook een test van de in H4 ontworpen referentiearchitectuur van beveiliging.

1.2.1 Validatie

Validatie vindt plaatst door volledigheidscontrole van het ontwerp (1) en een analyse van het eindproduct (2). De volledigheidscontrole is een controle of in het ontwerp alle ontwerpeisen en randvoorwaarden zijn verwerkt. De validatie van het eindproduct is uitgewerkt in Figuur 5.



Figuur 2: Procesmodel ontwerp en validatie

De ontwerpmethode voor het ontwerp van de beveiligingsarchitectuur voor een aspectgebied wordt gevalideerd door analyse van het eindproduct: voldoet deze aan de gestelde doelstellingen? Praktijkervaringen met de beveiligingsarchitectuur voor informatiestromen kunnen gebruikt worden om conclusies te formuleren omdat ze iets zeggen over de inhoud en het proces dat is gebruikt om de beveiligingsarchitectuur voor een aspectgebied te produceren.

Door de gekozen opzet om vanuit een referentiearchitectuur een beveiligingsarchitectuur voor een aspectgebied te produceren en het feit dat in dit onderzoek slechts één enkel aspectgebied wordt uitgewerkt, is het niet mogelijk om te valideren in hoeverre de beveiligingsarchitecturen voor andere aspectgebieden juist zullen zijn. De beveiligingsarchitecturen voor informatiestromen kan wel worden gezien als een specifieke gevalstudie. Op basis daarvan kan uitspraak worden gedaan over andere beveiligingsarchitectuur voor aspectgebieden, voor zover de gebruikte objecten binnen de referentiearchitectuur van beveiliging voor meerdere gevallen van toepassing zijn. Het resultaat van de validatie wordt gebruikt om conclusies en aanbevelingen te formuleren.

1.2.2 Structuur van deze scriptie

De ontwerpstappen worden op de volgende wijze beschreven:

- Hoofdstuk 2 en 3 leveren de randvoorwaarden en ontwerpeisen;
- Hoofdstuk 4 beargumenteert de keuzes op basis waarvan de referentiearchitectuur voor beveiliging wordt ontworpen en vult de referentiearchitectuur voor beveiliging in.
- Hoofdstuk 5 beargumenteert de keuzes op basis waarvan de beveiligingsarchitectuur voor informatiestromen tot stand komt, de architectuur zelf is te vinden in bijlage C.
- Hoofdstuk 6 sluit af met conclusies en aanbevelingen.

De wetenschappelijke bijdrage van deze scriptie bestaat uit de methodieken om een referentie architectuur voor beveiliging te maken (het ontwerpproces van H4) en de methodiek om vanuit een bepaald aspectgebied van beveiliging een beveiligingsarchitectuur te produceren. De beveiligingsarchitectuur levert aanbevelingen voor het organiseren van informatiebeveiliging in de context van keteninformatisering. De bijdrage voor de organisatie bestaat uit de beveiligingsarchitectuur voor informatiestromen op basis waarvan beveiliging gerealiseerd kan worden die nodig is om ketensamenwerking op de juiste wijze te ondersteunen.

2 Beveiligingsprincipes

In dit hoofdstuk worden de volgende deelvragen beantwoord:

1) Wat zijn de randvoorwaarden en ontwerpeisen waaraan de beveiligingsarchitectuur moet voldoen?
   a. Gezien de strategische context van de organisatie?
   b. Gezien de eisen die de organisatie stelt?

De antwoorden op de deelvragen zijn geformuleerd in termen van beveiligingsprincipes en ontwerpeisen. Randvoorwaarden worden in architecturen vaak vertaald naar principes: dit zijn generieke regels en richtlijnen die niet erg aan verandering onderhevig zijn.

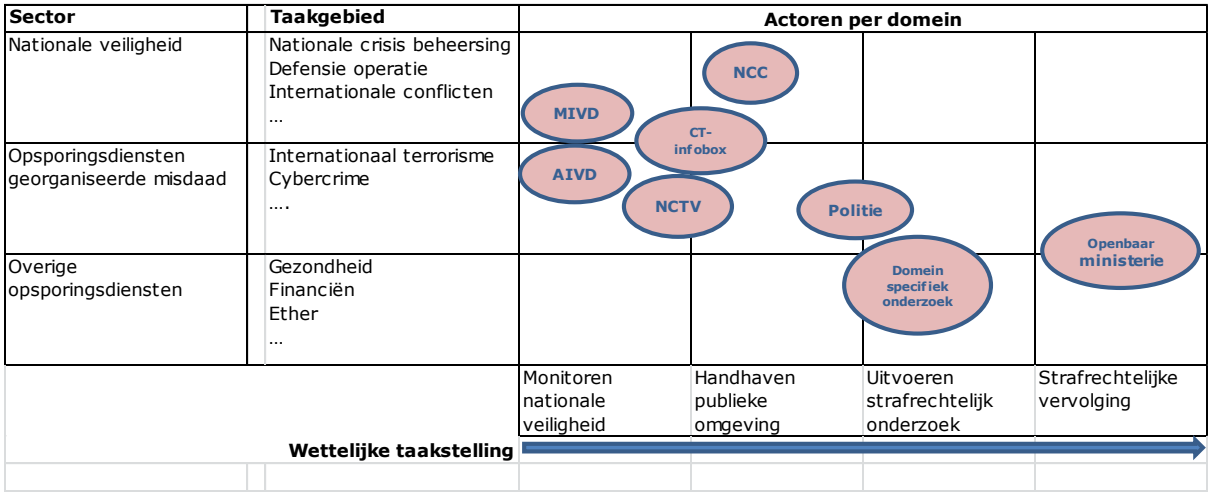
Paragraaf 2.1 beschrijft de strategische context van waaruit beveiligingsprincipes kunnen worden afgeleid. Paragraaf 0 beschrijft een aantal onderwerpen die te maken hebben met de verwerking van hooggerubriceerde informatie die zullen worden vertaald in beveiligingsprincipes. In paragraaf 2.3 wordt deelvraag 1b beantwoord, deze paragraaf beschrijft de ontwerpeisen die de organisatie stelt aan een beveiligingsarchitectuur. In paragraaf 2.4 is het antwoord op deelvraag 1a en deelvraag 1b samengevat in een overzicht van beveiligingsprincipes en ontwerpeisen.

2.1 Strategische context

Deze paragraaf beschrijft een aantal onderwerpen over de strategische context van samenwerking in de veiligheidsketen.

2.1.1 Plaats in het veiligheidsdomein

De omgeving waarbinnen keteninformatisering plaatsvindt betreft in eerste instantie partners in de veiligheidssector in Nederland. Zoals in de inleiding is beschreven, is er een tendens om de samenwerking tussen deze actoren te intensiveren met als doel te voorkomen dat relevante dreigingen van de Nationale Veiligheid niet tijdig worden onderkend. Het delen van informatie met ketenpartners is essentieel om aan de taakopdracht te kunnen voldoen. Meer dan eens is aangetoond dat bij toeval ontdekte relaties in informatie bij verschillende ketenparters in op zichzelf losstaande onderzoeken, ernstige gebeurtenissen hebben kunnen voorkomen (de Wijk, 2005).



Figuur 3: Veiligheidssector in Nederland (Ministerie van Binnelandse Zaken en Koninkrijksrelaties, 2010)

In Figuur 3 is de omgeving van de veiligheidssector geschetst. De figuur toont de meest belangrijke ketenpartners waarmee wordt samengewerkt. De horizontale as toont de juridische procesvolgorde, de verticale as geeft de taakverdeling in de veiligheidssector weer. Op deze twee assen zijn de relevante ketenpartners afgebeeld. De ketenpartners zijn: Nationaal Coördinator Terrorisme en Veiligheid (NCTV) Militaire Inlichtingen- en Veiligheidsdienst (MIVD), Nationaal Crisis Centrum (NCC), Contra-terrorsime Infobox (CT-infobox). Onder domein specifiek onderzoek vallen de FIOD, belastingdienst, agentschap Telecom (etherfrequenties), Inspectie voor de Gezondheidszorg en andere kleine opsporingsdiensten. (Veiligheidssector in Nederland, 2010).

Ontwikkelen van relaties met ketenpartners betekent dat deze partijen tot op zekere hoogte toegelaten zullen moeten worden tot de interne informatievoorziening. Van oudsher is de informatievoorziening een gesloten geheel, gebaseerd op het slotgracht model: hoge muren, van binnen redelijk open.

Voor de beveiliging betekent dit dat de beveiligingsstrategie zal moeten worden aangepast. In een omgeving waarin samenwerking essentieel wordt geacht is een gesloten benadering onhoudbaar.

P1 De strategie van beveiliging van de informatievoorziening moet zodanig worden aangepast dat veilige uitwisseling van informatie met ketenpartners mogelijk wordt gemaakt.

2.1.2 Wet- en regelgeving

De volgende wet- en regelgeving is vooral van toepassing op de informatiehuishouding:

- Wet op de Inlichtingen- en Veiligheidsdiensten (WIV);
- Communicatievoorschriften uit diverse sectorale wetgeving (Wet Gemeentelijke Basis Administratie (GBA), Wet justitiële en strafvorderlijke gegevens (WJSG), etc.);
- Archiefwet;
- Wet openbaarheid bestuur (WOB);
- Voorschrift Informatiebeveiliging Rijksdienst (VIR 92);
- VIR – Bijzondere Informatie (VIR-BI).

Nu volgt een korte toelichting van de effecten van de genoemde wet- en regelgeving bij de totstandkoming van samenwerkingsverbanden met ketenpartners.

<u>Informatiebasis</u>
Welke informatie precies gebruikt mag worden is voor een deel vastgelegd in de WIV. Om cruciale informatieleveranties uit andere (overheids)sectoren te verzekeren zijn in aparte sectorale wetgeving leverantieverplichtingen vastgelegd. Daar waar dit niet bij wet is geregeld ontstaan onduidelijke situaties waardoor informatiekoppelingen zeer moeizaam tot stand komen en niet zelden leiden tot zeer hoge kosten.

<u>Archiveren en openbaarmaken</u>
De problematiek van archivering, de lange termijn eisen van het de-rubriceren van informatie en de Wet Openbaarheid van Bestuur (WOB) leiden tot complexe afwegingen die vanuit een juridisch perspectief altijd controversieel zullen zijn. Voorbeeld hiervan is dat de-rubriceringsregels in wetgeving veroorzaken dat bepaalde informatie na verloop van tijd openbaar gemaakt zal moeten worden. De vraag is hoe je dat doet in omgevingen waarbij openbaarmaking nog steeds ernstige gevolgen kan hebben voor actoren die twintig jaar geleden een rol speelden in bepaalde kwesties van nationale veiligheid.

<u>Communicatie</u>
Communicatie van hooggerubriceerde informatie is bij wet aan zeer strenge richtlijnen gebonden (Ministerie van Veiligheid en Justitie, 2012). Om die reden staat het geldende

beveiligingskader (VIR-BI) informatiekoppelingen alleen in specifieke situaties en onder zeer strikte beveiligingsmaatregelen toe. Aan de andere kant is er de dagelijkse praktijk: er zijn veel verbindingen waarbij informatie met ketenpartners wordt uitgewisseld, waaronder staatsgeheime informatie. Het VIR-BI beschrijft beveiligingsmaatregelen teneinde de exclusiviteit van de informatie te kunnen waarborgen. De eisen zijn gedifferentieerd op basis van de rubricering van informatie en naar de deelgebieden fysieke beveiliging, transport van informatie, regels voor technische koppelingen en de beveiliging daarvan. De eisen zijn zodanig operationeel geformuleerd dat er weinig tot geen ruimte is om een goede beveiliging te kunnen realiseren.

In het recente verleden was dit slechts tot op zekere hoogte een probleem: technische koppelingen waren inefficiënt en duur, maar wel effectief. Organisaties die hooggerubriceerde informatie verwerkten konden op eigen wijze invulling geven aan de inrichting van hun informatie huishouding en toch voldoen aan het VIR-BI. Informatiekoppelingen bestonden vooral uit papieren documentstromen en fysiek transport van gegevensdragers omdat het inrichten van elektronische koppelingen leidt tot complexiteit en dure oplossingen.

Door de toenemende vraag naar digitale gegevensuitwisseling en de noodzaak om informatie breed in de organisatie te ontsluiten is deze werkwijze geen optie meer. Het handhaven van deze manier van werken leidt tot:

a) onveiligheid in werkprocessen omdat deze op een zodanige wijze zijn ingericht dat aan het VIR-BI wordt voldaan, de toegepaste "workarounds" leiden tot onveilige situaties;
b) zeer grote diversiteit in technische oplossingen met als gevolg hoge kosten, lange doorlooptijden en problemen met de beheersbaarheid.

De voorziene opvolger van het VIR-BI, het Voorschrift Informatiebeveiliging Rijksoverheid – Gerubriceerde Informatie (VIR-GI), gaat uit van een risicogebaseerde aanpak. Hierdoor worden risicogebaseerde afwegingen in specifieke situaties mogelijk gemaakt. Er is echter geen publicatiedatum bekend (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2010).

Voor de beveiliging van de informatievoorziening zijn de volgende constateringen van belang:

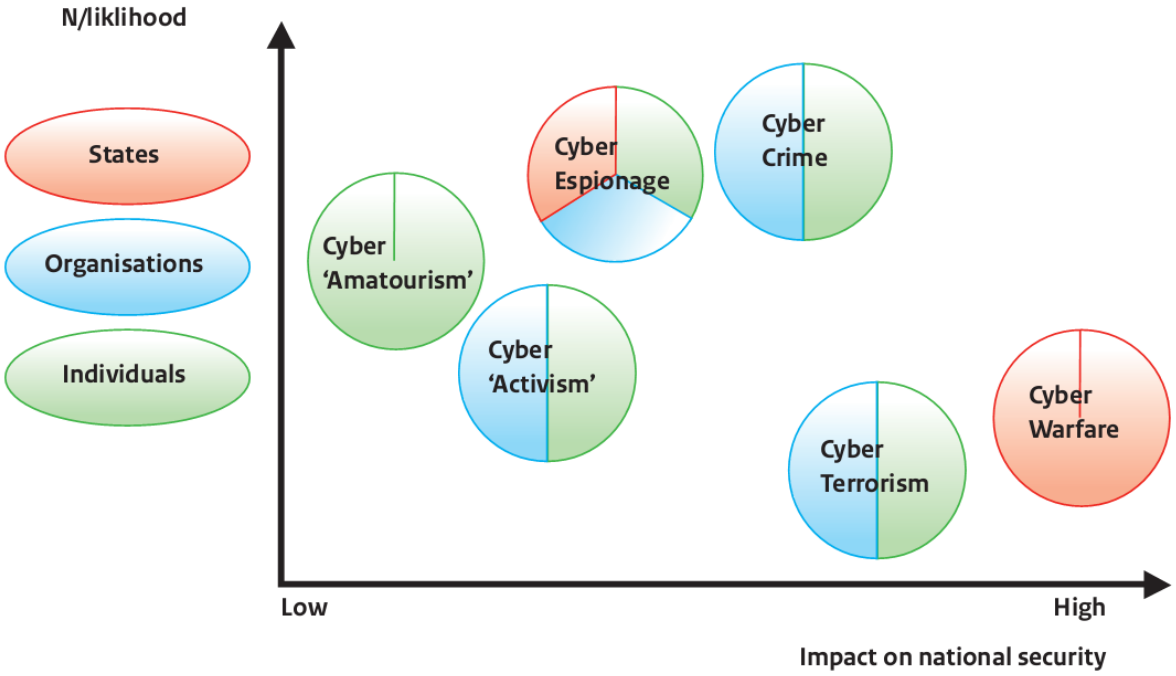
- *het maken van eigenstandige risico afwegingen in voorkomende gevallen noodzakelijk zal zijn omdat wet- en regelgeving blokkerend werkt;*
- *de bestaande communicatievoorschriften zijn gedateerd en vormen daarmee onvoldoende basis voor de beveiliging in samenwerkingsverbanden tussen ketenpartners. Hierin moet de beveiligingsarchitectuur voorzien;*
- *De genoemde wet-en regelgeving blijft wel randvoorwaardelijk.*

P2 De beveiliging van de informatievoorziening voorziet in het maken van eigenstandige risico afwegingen in situaties waar bestaande wet- en regelgeving tekort schiet.
P9 In lijn met de reeds bestaande beveiligingskaders, WIV, VIR, VIR-BI, WOB, Archiefwet en sectorale wetgeving (GBA, WJSG);

2.1.3 Kwetsbaarheid van informatievoorziening (exogeen)

De ontwikkelingen op het gebied van informatisering van de samenleving en de overheid zijn actuele onderwerpen die op dit moment op zowel op Europees- als landelijk niveau politieke aandacht krijgen. De Wetenschappelijke Raad voor Regeringsbeleid (WRR) heeft onderzocht wat deze ontwikkelingen betekenen voor de overheid als geheel en komt daarbij tot de conclusie dat bestuurlijke heroriëntatie noodzakelijk is omdat in het politiek bestuurlijke denken de nadruk ligt op losse technieken en individuele applicaties en niet op genetwerkte informatiestromen. Onder invloed van het uitwisselen van informatie in netwerken worden grenzen tussen organisaties en publieke- en private partijen diffuus. Naast de kansen die dit biedt, introduceert dit kwetsbaarheden waar aandacht voor nodig is (rapport iOverheid, 2011).

Een analyse van de kwetsbaarheden die er zijn op het gebied van Nationale Veiligheid brengt deze consequenties verder in beeld (Denktank nationale veiligheid, 2010, p. 29). Dit wordt toegelicht aan de hand van Figuur 4.



Figuur 4: Risico's in cyberspace (Bron: HCSS, ter voorbereiding van WCIT 2010 in amsterdam)

Figuur 4 (Rademaker & Frikling, 2010) schetst bedreigingen van de Nationale veiligheid naar soort actor in een grafiek met als verticale as de waarschijnlijkheid op een incident en als horizontale as de impact van een incident op de nationale veiligheid. Deze grafiek laat zien dat er aantoonbare incidenten zijn voor statelijke actoren, die direct grote consequenties hebben voor de Nationale veiligheid. Dit toont de relevantie van dit onderwerp voor de samenwerkingsverbanden in de veiligheidsketen. Dit geldt zowel in het kader van de bescherming van de Nationale veiligheid als vanuit een eigen verantwoordelijkheid ter verdediging van de eigen informatievoorziening.

Voor de beveiliging van de informatievoorziening betekent dit dat er terdege rekening gehouden dient te worden met toenemende dreigingen van buitenaf die ontstaan bij het koppelen met informatievoorzieningen van ketenpartners en derde partijen. Voor de risico's die dit introduceert is het dan wel belangrijk dat dit leidt tot een door de organisatie gevalideerd restrisico.

P3 Risico's die Informatiekoppelingen introduceren worden gereduceerd tot een acceptabel restrisico voor de organisatie.

2.2 Organisatorische context

Nu volgt de beschrijving van een aantal onderwerpen die van toepassing zijn binnen de organisaties in de veiligheidsketen.

2.2.1 Ondersteuning operationele doelen

De informatievoorziening moet voldoen aan hoge kwaliteitseisen, met name in tijden van crisis. Er worden zeer hoge eisen gesteld aan beschikbaarheid.

De technische infrastructuur moet ook mee kunnen met de nieuwste technische ontwikkelingen. Dit is noodzakelijk omdat uit onderzoek blijkt dat de kwaadwillenden steeds vaker beschikken over hoogwaardige technische kennis, geavanceerde technische middelen en de nodige financiële middelen. "Leading Edge" informatiesystemen vereisen veel technisch inhoudelijke kennis van medewerkers en worden veelal in eigen beheer ontwikkeld en gebouwd.

Dit levert voor informatiebeveiliging een aantal risico's op die op één of andere wijze beheerst zullen moeten worden dan wel bewust als risico geaccepteerd moeten worden. Het gaat om relatief jonge systemen die onder tijdsdruk en soms ook politieke druk ontwikkeld moeten worden. En het zijn vaak ook nog nieuwe technieken waarmee gewerkt wordt (non-proven technology). Deze risico's zijn hieraan verbonden:

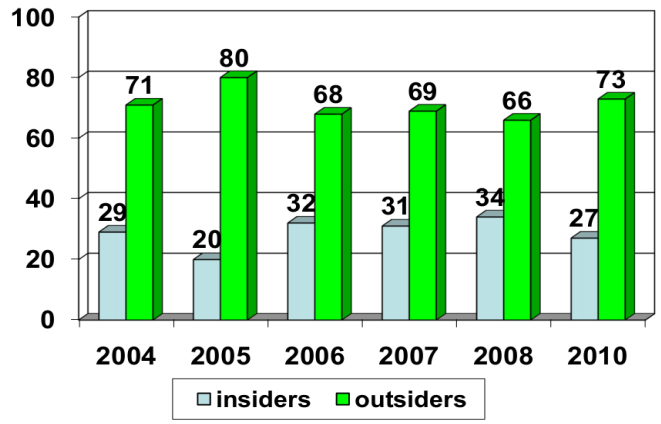
- er zijn systemen operationeel waarin kinderziekten en kwetsbaarheden zitten;
- functionaliteit gaat voor kwaliteit, veel beveiliging die in de standaard productieomgevingen als normaal wordt beschouwd, kan hier niet worden toegepast.

Deze risico's stellen speciale eisen aan de informatiebeveiliging. Beveiliging kan voor dit soort systemen niet altijd worden doorgevoerd tot op een niveau dat wordt verlangd van breed inzetbare systemen in hooggerubriceerde omgevingen.

P4 De beveiliging van noodzakelijke "Leading edge" technische voorzieningen ziet er anders uit dan voorzieningen die breed worden ingezet.

2.2.2 Kwetsbaarheid van informatievoorziening (endogeen)

De informatievoorziening is vooral kwetsbaar van binnenuit. Veel soorten malware vinden hun weg de organisatie in via social engineering van mensen. De aanval is vooral gericht op het plaatsen van software die de informatie doorstuurt. Naarmate het aantal informatiekoppelingen toeneemt, groeit het aanvalsvlak. Voorbeeld van een dreiging die zich recent voor heeft voorgedaan is Stuxnet, een zeer complexe, met een zeer specifiek doel voor ogen ontwikkelde malware (Symantec Security Response, 2011).



Figuur 5: Percentage insiders versus outsiders (U.S. Secret Service, Software Engeneering Institute CERT program at Carnegie Mellon University, jan 2011)

Een studie van het Cert Coordination Centre (Cert-CC) (zie Figuur 5) over een groot aantal gerapporteerde beveiligingsincidenten toont aan dat inbraak van buitenaf de grootste dreiging vormt, maar dat (voormalig) personeel en contractanten de op een na grootste dreiging vormen (Carnegie Mellon University, 2011).

Recente voorbeelden van dit soort incidenten die groot in het nieuws zijn geweest, zijn de vermeende activiteiten van Bradly Manning die leidden tot het ontstaan van WikiLeaks (Wikipedia, 2010). Een ander voorbeeld zijn een aantal veroordelingen voor schending van staatsgeheimen van medewerkers in overheidsdienst (wetboek-online). Ook voorbeelden over bedrijfsgeheimen die het Nederlandse bedrijfsleven kwijtraakt ondersteunen dit: zie recente publicaties over bedrijfsspionage waarbij Chinese medewerkers bedrijfsgeheimen ontvreemdden (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2010).

De informatievoorziening moet in staat zijn om informatie te verwerken die inherent malware bevat. Denk hierbij aan kopieën van gegevensdragers ten behoeve van forensisch onderzoek en internet gerelateerde gegevens of mogelijk andere informatie die op basis van bijzondere bevoegdheden is verkregen.

Voor de beveiliging van de informatievoorziening heeft dit de volgende consequenties:
- *Er zullen onderdelen van de infrastructuur blootgesteld worden aan malware. De infrastructuur dient voorzieningen te bevatten die de verwerking van gegevens die malware bevatten mogelijk maakt;*
- *Het risico op de aanwezigheid van malware binnen dat deel van de informatievoorziening waarin dat niet de bedoeling is, is niet nul: dit betekent dat veiligheidsmaatregelen noodzakelijk zijn om deze dreiging het hoofd te bieden;*
- *Het risico van dreiging vanuit interne medewerkers en contractanten wordt vooral ondervangen door screening. Analyse van deze categorie beveiligingsincidenten leert dat dit risico reducerend werkt maar dat deze maatregel op zich onvoldoende waarborg biedt voor het voorkomen van deze interne dreigingen.*

P5 De beveiliging van de informatievoorziening moet ingericht zijn op de verwerking van gegevens die malware bevatten.
P6 De beveiliging van de informatievoorziening is gericht op "Insider Threats" dreigingen.

2.2.3 Controle en verantwoording

In de WIV zijn de bijzondere bevoegdheden van de organisatie geregeld. Deze bevoegdheden zijn omkleed met strenge regels ten aanzien van controle en verantwoording. De beweging die plaatsvindt vanuit een gesloten naar meer open organisatie stelt speciale eisen aan controle en verantwoording. Als informatie breder beschikbaar is, zal deze informatie steeds vaker binnen een andere context worden beschouwd dan de context waarin de informatie tot stand kwam. Het is mogelijk dat daardoor meer fouten gemaakt worden. Daarom is het van belang dat volkomen duidelijk is waar informatie vandaan komt en hoe deze tot stand is gekomen.

Het omzeilen van fysieke koppelingen door mobiele gegevensdragers[3] maakt het moeilijker om verantwoording af te leggen over de wijze waarop de informatie precies tot stand is gekomen. Aan het gebruik van dergelijke gegevensdragers moeten in principe dezelfde eisen worden gesteld als aan andere typen koppelingen.

[3] Dit zijn bijvoorbeeld USB sticks, SDHC kaartjes of een DVD

Voor de informatiebeveiliging betekent dit dat de audit- en loggingsfaciliteiten ingericht moeten zijn teneinde de integriteit van de informatie te waarborgen en om vast te leggen hoe een bepaalde informatiepositie precies tot stand is gekomen.

P7 De totstandkoming van een informatiepositie moet verantwoord kunnen worden, ongeacht de wijze van koppelen.

2.2.4 Intern informatie delen

Er is binnen organisaties in de veiligheidsketen een discussie gaande over welke bedrijfsonderdelen toegang hebben tot welke informatie. Het breed delen van informatie over verschillende ketenpartners draagt bij aan de kans dat dreigingen op het gebied van Nationale Veiligheid tijdig kunnen worden onderkend. Voor de interne informatievoorziening is dit ook van toepassing. De van oudsher zeer gesloten cultuur leidt automatisch tot een bepaalde mate van verkokering van informatie. Het opheffen van deze verkokering biedt ook binnen organisaties een potentieel voordeel.

De mate waarin informatie wordt gedeeld wordt bepaald door drie assen: Need-to-Know (wat moet je weten om je werk te kunnen doen), Need-to-Share (wat moet je delen om je werk te kunnen doen) en de beveiligingscomponent die hierbij hoort: de Need-to-Protect (om welke afscherming vraagt de informatie op grond van de rubricering). De balans tussen deze aspecten is onderhevig aan verandering.

Voor informatiebeveiliging betekent dit dat de beveiliging in staat moet zijn de continue veranderingen belangen de driehoek Need-to-Know, Need-to-Share en Need-to-Protect te ondersteunen.

P8 Flexibiliteit is noodzakelijk in het omgaan met noodzakelijke aanpassingen in de relatie tussen Need-to-Know, Need-to-Share en Need-to-Protect.

2.3 Ontwerpeisen vanuit de organisatie

In overleg met de opdrachtgevers is een aantal specifieke ontwerpeisen vastgesteld waaraan de beveiligingsarchitectuur moet voldoen. Deze eisen zijn vastgesteld door middel van interviews met belanghebbenden: Beveiligingsambtenaar, Hoofd Informatiemanagement en de Enterprise architect. De onderstaande ontwerpeisen zijn een antwoord op deelvraag 1b, de volgorde waarin ze worden genoemd is willekeurig.

2.3.1 Aansluiten bij bestaande Enterprise Architectuur

De Enterprise Architectuur maakt gebruik van bestaande processen die zijn ingebed in de organisatie, zoals bijvoorbeeld een projectmanagementproces voor de ontwikkeling van nieuwe systemen. Beveiliging moet een integraal aandachtspunt zijn bij systeemontwikkeling. De beveiligingsarchitectuur kaders mogen uiteraard niet strijdig zijn met de Enterprise Architectuur kaders. Van belang is om gebruik te maken van de beveiliging-specifieke onderdelen die reeds ontwikkeld zijn binnen de Enterprise Architectuur en het vastleggen van de relaties met de Enterprise Architectuur.

O1 De relatie met de EA is aantoonbaar: de beveiligingsarchitectuur moet de relaties benoemen en vastleggen;
O2 Er wordt zoveel mogelijk gebruik gemaakt van reeds bestaande architectuurprocessen voor systeemontwikkeling en project management.

2.3.2 Gebruik van bestaande beveiligingsconcepten

Met bestaande beveiligingsconcepten is op zich niet heel veel mis. De samenhang tussen de bestaande beveiligingsconcepten is echter onvoldoende gewaarborgd. Het is van belang de samenhang op zijn minst is beschreven en vastgelegd. Eventuele problemen kunnen op deze manier worden gesignaleerd en verholpen.

O3 Bestaande architectuurproducten voor beveiliging worden ondersteund;
O4 De bestaande producten en de samenhang worden beschreven.

2.3.3 Aansluiting op extern beheerde- of de facto standaarden

De omgevingsdynamiek, complexiteit van de informatiehuishouding en de beperkte beschikbaarheid van architecten om onderdelen van de architectuur te maken en te onderhouden maakt het onmogelijk om eigen bedrijfsstandaarden voor toegepaste architectuur te ontwikkelen.

O5 Externe kaders en standaarden die gebruikt worden bij de ontwikkeling van aspect beveiligingsarchitecturen worden vastgelegd in de beveiligingsarchitectuur;
O6 Te leveren architectuurproducten zijn van een zodanig abstractie niveau dat de primaire afnemers van deze architectuur implementaties tot stand kunnen brengen;
O13 Het architectuurmodel moet door een klein team eenvoudig onderhouden kunnen worden.

2.3.4 Eisen op eigen wijze operationaliseren

Vanwege de aangegeven problemen met bestaande wet- en regelgeving op het gebied van staatsgeheimen is het noodzakelijk dat van de regels afgeweken kan worden, met inachtneming van de risico's die dit introduceert.

O7 De beveiligingsarchitectuur vervangt de afhankelijkheid van vastgelegde beveiligingsmaatregelen uit het Vir-BI door risicogebaseerde afwegingen te maken;
P10 Voor delen van informatiekoppelingen die buiten de eigen invloedssfeer liggen worden bestaande kaders per definitie wel toegepast;
P11 Voor delen van informatiekoppelingen die binnen de eigen invloedssfeer liggen worden bestaande kaders en regelgeving gerespecteerd, maar niet per definitie als leidend toegepast.

2.3.5 Kosten baten afwegingen

Mogelijkheden creëren om kosten/baten afwegingen te maken door maatregelen te relateren aan risico's en belangen. Belangrijk aandachtspunt is de hoge kosten voor het beheer van een hooggerubriceerde informatievoorziening. Het gaat dan om personeelskosten, meerdere fysieke omgevingen, de kosten van beveiligingsmaatregelen en het ontbreken van efficiency maatregelen die in andere informatie voorzieningen wel toegepast kunnen worden (zoals uitbesteden, het delen van infrastructuur).

O8 Risicogebaseerd denken introduceren;
O9 Beveiliging relateren aan bedrijfsdoelstellingen om kosten inzichtelijk te maken.

2.3.6 Beheer(s)baarheid

Beheersbare systemen zijn belangrijk vanwege de beperkte personeelscapaciteit. Beveiligingsrichtlijnen staan veelal niet toe dat de flexibiliteit die inhuur van personeel kan bieden wordt gebruikt. Het Vir-BI gaat volledig uit van exclusiviteitseisen. Dit heeft als gevolg dat de beschikbaarheid en integriteit niet als vanzelf worden meegewogen bij het ontwerpen van beveiligingsoplossingen.

P12 De architectuur beschouwt informatiebeveiliging integraal: beschikbaarheid, integriteit en exclusiviteit (Vertrouwelijkheid);
O10 De beveiligingsarchitecturen zijn zodanig generiek van aard dat er keuzes overblijven bij implementatie ten aanzien van toepassingen zodat op dat moment weloverwogen keuzes gemaakt worden ten aanzien van beheer.

2.3.7 Beveiligingsniveaus

Bij een volwassen beveiliging horen ook processen die het mogelijk maken om verantwoording af te leggen aan de organisatie over informatiebeveiliging.

O11 De stand van beveiliging van de informatievoorziening meetbaar maken.

2.3.8 Maatschappelijke veranderingen

Er is oog voor nieuwe dreigingen die voortvloeien uit maatschappelijke veranderingen die we nu doormaken op het gebied van netwerken (social media, cloud computing, etc.). "Klaar voor de toekomst" is een belangrijke wens. Gebruik van Social Media, Rijks Cloud strategie zijn ontwikkelingen die als driver fungeren voor veranderingen die momenteel in hoog tempo plaatsvinden.

O12 Kies voor architectuurcomponenten en kaders waaraan toekomstvisie ten grondslag ligt;

2.4 Samenvatting principes en ontwerpeisen uit de organisatie

Tabel 1 bevat een overzicht van de principes en ontwerpeisen die in dit hoofdstuk zijn benoemd, met een verwijzing naar de paragraaf waarin deze zijn toegelicht.

Code	par.	Type	tekst
P1	2.1.1	principe	De strategie van beveiliging van de informatievoorziening moet zodanig worden aangepast dat veilige uitwisseling van informatie met ketenpartners mogelijk wordt gemaakt.
P2	2.1.2	principe	De beveiliging van de informatievoorziening voorziet in het maken van eigenstandige risico afwegingen in situaties waar bestaande wet- en regelgeving tekort schiet.
P3	2.1.3	principe	Risico's die Informatiekoppelingen introduceren worden gereduceerd tot een acceptabel restrisico voor de organisatie.
P4	2.2.1	principe	De beveiliging van noodzakelijke "Leading edge" technische voorzieningen ziet er anders uit dan voorzieningen die breed worden ingezet.
P5	2.2.2	principe	De beveiliging van de informatievoorziening moet ingericht zijn op de verwerking van gegevens die malware bevatten.
P6	2.2.2	principe	De beveiliging van de informatievoorziening is gericht op "Insider Threats" dreigingen.
P7	2.2.3	principe	De totstandkoming van een informatiepositie moet verantwoord kunnen worden, ongeacht de wijze van koppelen.
P8	2.2.4	principe	Flexibiliteit is noodzakelijk in het omgaan met noodzakelijke aanpassingen in de relatie tussen Need-to-Know, Need-to-Share en Need-to-Protect.
P9	2.1.2	principe	De beveiligingsarchitectuur is in lijn met de reeds bestaande beveiligingskaders, WIV, VIR, VIR-BI, WOB, Archiefwet en sectorale wetgeving (GBA, WJSG).
O1	2.4.1	ontwerpeis	De relatie met de EA is aantoonbaar: de beveiligingsarchitectuur moet de relaties benoemen en vastleggen.
O2	2.4.1	ontwerpeis	Er wordt zoveel mogelijk gebruik gemaakt van reeds bestaande architectuurprocessen voor systeemontwikkeling en project management.
O3	2.4.2	ontwerpeis	Bestaande architectuurproducten voor beveiliging worden ondersteund.
O4	2.4.2	ontwerpeis	De bestaande producten en de samenhang worden beschreven.
O5	2.4.3	ontwerpeis	Externe kaders en standaarden die gebruikt worden bij de ontwikkeling van aspect beveiligingsarchitecturen worden vastgelegd in de beveiligingsarchitectuur.
O6	2.4.3	ontwerpeis	Te leveren architectuurproducten zijn van een zodanig abstractie niveau dat de primaire afnemers van deze architectuur implementaties tot stand kunnen brengen.
O7	2.4.4	ontwerpeis	De beveiligingsarchitectuur vervangt de afhankelijkheid van vastgelegde beveiligingsmaatregelen uit het Vir-BI door risicogebaseerde afwegingen te maken.
P10	2.4.4	principe	Voor delen van informatiekoppelingen die buiten de eigen invloedssfeer liggen worden bestaande kaders per definitie wel toegepast.
P11	2.4.4	principe	Voor delen van informatiekoppelingen die binnen de eigen invloedssfeer liggen worden bestaande kaders en regelgeving gerespecteerd, maar niet per definitie als leidend toegepast.
O8	2.4.5	ontwerpeis	Risico gebaseerd denken introduceren.
O9	2.4.5	ontwerpeis	Beveiliging relateren aan bedrijfsdoelstellingen om kosten inzichtelijk te maken.
P12	2.4.6	principe	De architectuur beschouwt informatiebeveiliging integraal: beschikbaarheid, integriteit en exclusiviteit (Vertrouwelijkheid).
O10	2.3.6	ontwerpeis	De beveiligingsarchitecturen zijn zodanig generiek van aard dat er keuzes overblijven bij implementatie ten aanzien van toepassingen zodat op dat moment weloverwogen keuzes gemaakt worden ten aanzien van beheer.
O11	2.4.7	ontwerpeis	De stand van beveiliging van de informatievoorziening meetbaar maken.
O12	2.4.8	ontwerpeis	Kies voor architectuurcomponenten en kaders waaraan toekomstvisie ten grondslag ligt.
O13	2.4.8	ontwerpeis	Het architectuurmodel moet door een klein team eenvoudig onderhouden kunnen worden.

Tabel 1: Randvoorwaarden en ontwerpeisen H2

3 Theoretisch kader

In dit hoofdstuk worden de volgende deelvraag beantwoord:

> 2) Welke ontwerpeisen zijn van toepassing op architecturen en beveiligingsarchitecturen?

Deze vraag wordt beantwoord door een analyse uit te voeren van relevante architectuurraamwerken, Enterprise Architecturen en beveiligingsarchitecturen met als doel vast te stellen wat de benodigde randvoorwaarden en ontwerpeisen precies zijn.

Om een uiteindelijk een beveiligingsarchitectuur te kunnen ontwikkelen worden een aantal stappen doorlopen:

1. Beschrijven van verschillende soorten architecturen;
2. Analyse van de verschillen tussen architecturen (criteriadefinitie);
3. Scoren van de verschillende architecturen op de gevonden selectiecriteria.

Paragraaf 3.1 definieert het begrip architectuur, in paragraaf 3.2 definieert het begrip referentiearchitectuur en in paragraaf 3.3 en 3.4 worden een aantal Enterprise Architecturen en beveiligingsarchitecturen beschreven (stap 1). Daarna worden in paragraaf 3.5 vergelijkingscriteria vastgesteld op basis waarvan de architecturen met elkaar kunnen worden vergeleken (stap 2 en 3).

3.1 Wat is Architectuur

Het is van belang om een eenduidig beeld vast te stellen van de betekenis van architectuur. Architectuur in de fysieke wereld is niet eenduidig gedefinieerd: het betekent "de wetenschap van het ontwerpen van gebouwen" of het product hiervan: "een blauwdruk of ontwerp van een gebouw", of het product hiervan: "een bouwobject". Tot slot kan ook nog een bepaalde bouwstijl zijn. (Lankhorst et al., 2005) (Buffam, 2000).

In lijn hiermee zijn vele definities van "digitale" architecturen te vinden. (Bongers, 2006) beschrijft dat sommige architecturen zich beperken tot een overzicht van technieken of een beschrijvend technisch ontwerp. IT architectuur is hier een goed voorbeeld van, het gaat bijvoorbeeld om een ontwerp van een netwerk of een deelsysteem van de informatievoorziening of de beveiliging van een internetkoppeling. Deze architecturen zijn niet opnieuw toepasbaar en onleesbaar voor niet ingewijden. In andere gevallen zijn architecturen van een zodanig hoog abstractie niveau dat de architectuur gaat lijken op een soort meta-structuur. De afstand tot de dagelijkse praktijk is groot. Het antwoord op de vraag "wat is architectuur?" in de digitale wereld is afhankelijk van het toepassingsgebied, het beoogde doel en de objecten die de architectuur wil beschrijven (Bongers, 2006).

Een veel gehanteerde definitie van architectuur is die uit de IEEE 1471-2000 (ISO/IEC, 2000):

> Architecture is the fundamental organization of a system embodied in its components, their relationships to each other, and to the environment, and the principle guiding its design and evolution.

Deze algemene definitie wordt vaak geïnterpreteerd of verbijzonderd naar verschillende toepassingsgebieden, zoals bijvoorbeeld Enterprise Architecturen.

3.2 Referentie architectuur

De term referentie architectuur is een multi-interpretabel begrip (Greefhorst, Grefen, Saaman, Bergman, & Beek, 2008). Zij constateren de volgende verschillen:

- De ene architectuur beschrijft allerlei ICT gerelateerde gebieden (business, informatie, applicatie, technologie), terwijl de andere in gaat op hele specifieke onderwerpen of aspectgebieden (bijvoorbeeld software);
- De ene architectuur heeft alleen hoog niveau- en technologieonafhankelijke modellen of principes, terwijl de ander technologie specifieke keuzen en heel gedetailleerde modellen biedt. Soms wordt ook verregaande ondersteuning geboden bij de vertaling van deze modellen naar oplossingen, bijvoorbeeld in de vorm van een code generator;
- De ene architectuur is vooral een lijst van principes, terwijl de ander eigenlijk geheel uit modellen bestaat. Anderen hanteren weer veel meer een vrije vorm.

(Greefhorst, Grefen, Saaman, Bergman, & Beek, 2008) concludeert uiteindelijk:

> Referentiearchitecturen zijn abstracte architecturen en zijn de basis voor meer specifieke architecturen.

In het kader van dit onderzoek is vooral van belang hoe deze definitie binnen de context van de Nederlandse Overheid wordt gezien. Binnen de Nederlandse Overheid zijn drie referentiearchitecturen beschikbaar: NORA (ketensamenwerking), MARIJ (rijksoverheid) en GEMMA (gemeenten). Deze referentiearchitecturen zijn sturend voor de ontwikkeling van Enterprise Architecturen van individuele overheidsorganisaties. In de context van de Nederlandse overheid heeft de term "referentiearchitectuur" de volgende kenmerken (Goutier & Lieshout, 2010):

- De referentiearchitectuur is hiërarchisch gezien een abstractieniveau hoger gepositioneerd dan de uitgewerkte architecturen die de overheidsorganisaties zelf onderhouden;
- De referentiearchitectuur bevat gedetailleerde modellen voor een specifiek aspectgebied of domein;
- Er vindt samenwerking tussen één of meerdere overheidsorganisaties plaats;
- De referentiearchitectuur is kaderstellend voor de Enterprise Architecturen van individuele overheidsorganen).

3.3 Enterprise Architectuur

Als architectuur wordt toegepast op het bedrijf als systeem[4] ontstaat Enterprise Achitecture (EA). Er zijn veel verschillende definities van enterprise architectuur. Verschillende Enterprise Architecturen hanteren de algemene definitie (zie paragraaf 3.1) die is verbijzonderd naar bedrijven en organisaties.

De enterprise architectuur definitie die in dit document gehanteerd wordt, is die van TOGAF (The Open Group Architecture Framework (TOGAF), 2009). Deze definitie is algemeen aanvaard en wordt in de praktijk binnen de rijksoverheid toegepast.

> Enterprise Architecture is
> 1. A formal description of a system, or a detailed plan of the system at component level, to guide its implementation (source: ISO/IEC 42010: 2007).
> 2. The structure of components, their inter-relationships, and the principles and guidelines governing their design and evolution over time.

[4] Systeem in de definitie vanuit de systeemtheorie (Alter, 1999): geheel van elementen waaruit een bedrijf of organisatie bestaat.

De volgende architecturen zijn geselecteerd uit een groot aantal anderen vanwege de relevantie voor dit onderzoek. De relevantie is per architectuur aangegeven.

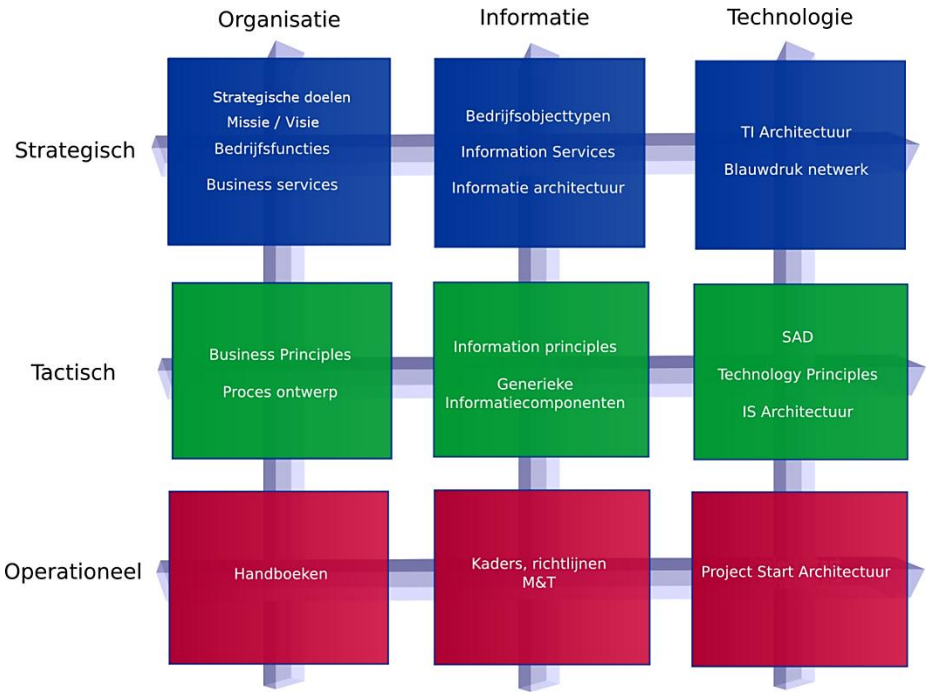
- Het PrimaVera model;
  Dit model wordt op verschillende plaatsen gebruikt binnen rijksoverheid als raamwerk voor de ontwikkeling van de informatievoorziening in brede zin;
- TOGAF;
  Dit is momenteel de toonaangevende Enterprise Architectuur. Ook wordt TOGAF toegepast in de dagelijkse praktijk van Enterprise Architectuur binnen diverse onderdelen van de rijksoverheid;
- NORA en MARIJ;
  Dit zijn twee referentiearchitecturen voor de overheid, opgezet vanuit de e-overheid visie, de "één loket" gedachte bij het leveren van diensten aan burgers en bedrijfsleven. Deze architectuurkaders zijn leidend voor overheidsorganisaties.

Nu volgt een korte beschrijving van deze architecturen.

3.3.1 Primavera

Het PrimaVera raamwerk (Maes, 2007) wordt binnen de rijksoverheid gebruikt als algemeen model voor de ontwikkeling van Informatiemanagement.

Zie
Figuur 6: de horizontale as bevat de elementen Organisatie, Informatie en Technologie, de verticale dimensie beschrijft de verschillende organisatieniveaus (strategisch, tactisch en operationeel).



Figuur 6: Primavera raamwerk (Maes, 2007)

Elk vlak kent zijn eigen informatie-gerelateerde onderwerpen, belanghebbenden en expertisegebieden. Het model is niet extensief uitgewerkt en beperkt zich tot enige duiding van de inhoud per vlak. Door op basis van de bedrijfscontext standaarden, processen en methodieken te selecteren en deze toe te passen komt een organisatie specifieke invulling van het informatiemanagement tot stand. Dit model is een middel om de bedrijfsdoelstellingen, bedrijfsprocessen en taakuitvoering van de organisatie te koppelen aan de Informatie en technologie die nodig is.

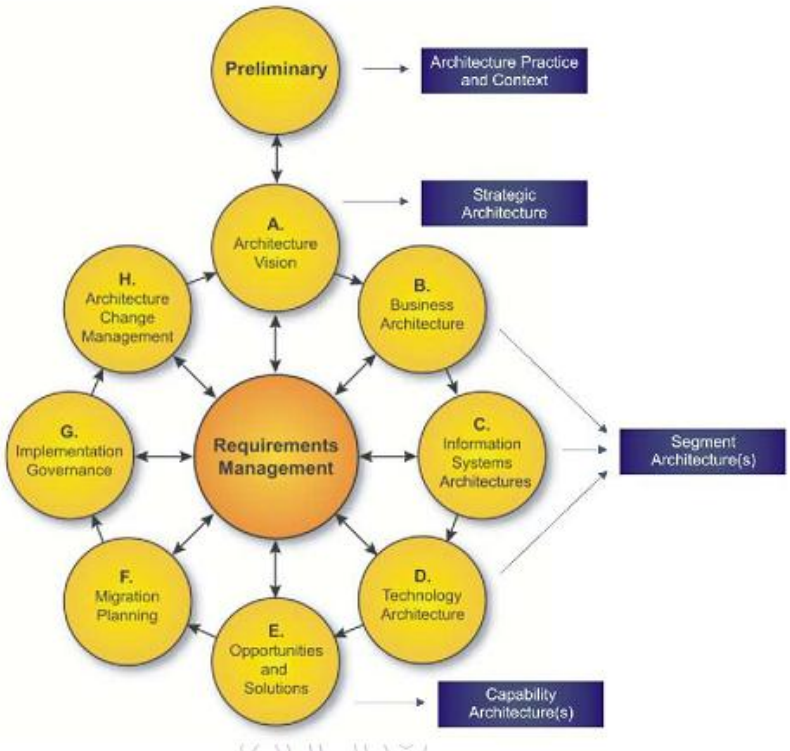
In een typische organisatie zijn, zonder de aanwezigheid van enterprise architectuur of een gecentraliseerde Informatie management afdeling, de vier hoekpunten van dit raamwerk op een of andere wijze ingevuld en in werking. Voor juiste positionering van informatie management en enterprise architectuur binnen de organisatie, zijn de bouwstenen die het kruis vormen de punten waarop normaliter organisatie en procesontwikkeling nodig is. Het gaat daarbij vooral het bereiken van de juiste interactie tussen de IT afdelingen en de rest van de organisatie (Informatie kolom) en de ontwikkeling van het tactisch niveau binnen de organisatie.

3.3.2 TOGAF

(The Open Group Architecture Framework (TOGAF), 2009) is een Enteprise Architectuur raamwerk. TOGAF is op dit moment de toonaangevende EA methode. Ook wordt TOGAF toegepast in de dagelijkse praktijk van Enterprise Architectuur binnen diverse onderdelen van de rijksoverheid. Dit maakt TOGAF een relevante kandidaat om hier verder toe te lichten.

TOGAF onderkent drie soorten architecturen: de strategische-, de segment- en de capability architectuur. TOGAF bevat ook een methodologie om een architectuur te maken: de Architecture Design Method (ADM). Dit is een proces of methode om de architectuur te ontwikkelen en beheren en bevat een beschrijving van elementen die nodig zijn in een architectuur.

TOGAF doet specifieke aanbevelingen hoe de TOGAF ADM kan worden gebruikt indien deze wordt toegepast op andere situaties dan de "Enterprise". TOGAF noemt zelf een aantal voordelen van deze constructie:
1) Het is een lichtgewicht oplossing;
2) Er is een sterke integratie tussen architecturen op verschillende niveaus in de organisatie;
3) Het werkt goed binnen één team.



Figuur 7: TOGAF ADM (The Open Group Architecture Framework (TOGAF), 2009)

Nadelen van deze oplossing die TOGAF noemt zijn:
1) De relatie tussen de verschillende soorten architecturen is niet per definitie geborgd;

2) Voordat de architectuurproducten toepasbaar zijn, moeten eerst de strategic-, segment- en capability architecturen worden ontwikkeld. Dit kan vertragend werken;
3) Het kan moeilijk worden om overzicht te houden over verschillende ontwerpactiviteiten die tegelijkertijd plaatsvinden.

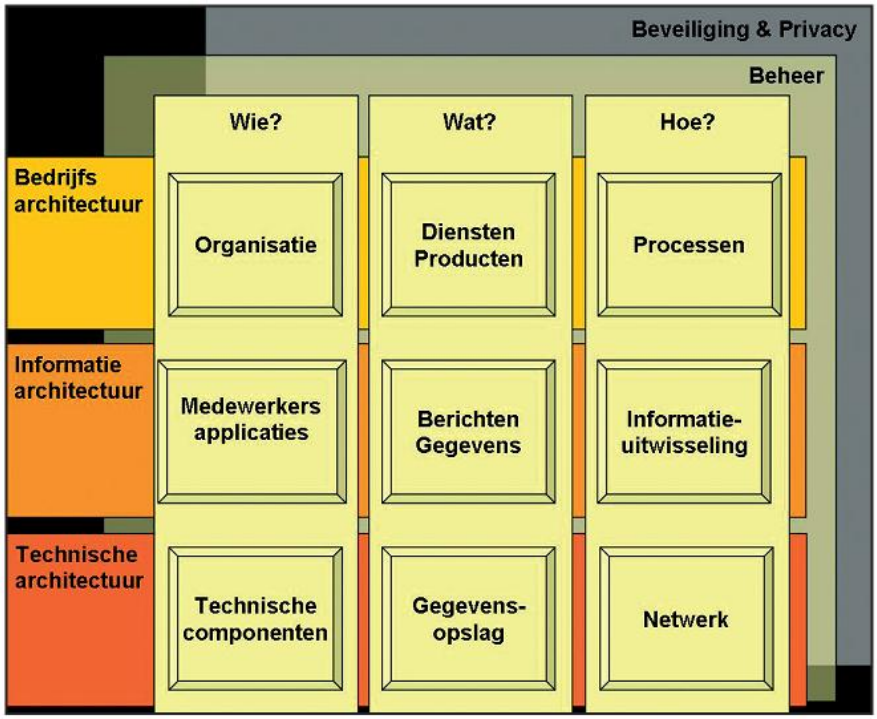
Ook geeft TOGAF advies op het gebied van beveiligingsarchitecturen. Dit is echter niet verder uitgewerkt dan een duiding van beveiligingsaspecten waarmee de architect rekening moet houden en een korte verbijzondering van de aandachtsgebieden van beveiliging. Deze aandachtsgebieden zijn opgenomen in de lijst met beveiligingsaspecten in bijlage B onder vermelding van generally accepted areas of concern for the security architect.

3.3.3 NORA

Nederlandse Overheid Referentie Architectuur (NORA) versie 3 (Goutier & Lieshout, 2010) is een referentiearchitectuur gemaakt voor overheidsorganisaties en heeft als doel om de uitwisseling van gegevens tussen overheden te standaardiseren. De NORA is een implementatie van de "Een loket naar de burger" gedachte van de overheid.

De NORA is kaderstellend voor alle overheidsorganisaties voor zover deze deelnemen in samenwerkingsverbanden binnen de overheid. De NORA beschrijft interoperabiliteit: het vermogen van overheidsorganisaties om effectief en efficiënt relaties aan te gaan en informatie te delen met elkaar en met burgers en bedrijven. NORA beziet al deze relaties in termen van diensten, als afgebakende prestaties van een persoon of organisatie (de dienstverlener), die voorzien in een behoefte van de omgeving (de afnemers). NORA stelt uitwisseling van producten en diensten centraal. Bij de NORA is een informatiebeveiligingskader geschreven.

De interessante onderdelen van de NORA zijn de kaderstellende principes. Dit zijn 10 leidende principes, geformuleerd in termen van algemene kwaliteitseisen en 40 daarvan afgeleide (geoperationaliseerde) principes.



Figuur 8: NORA raamwerk (Goutier & Lieshout, 2010)

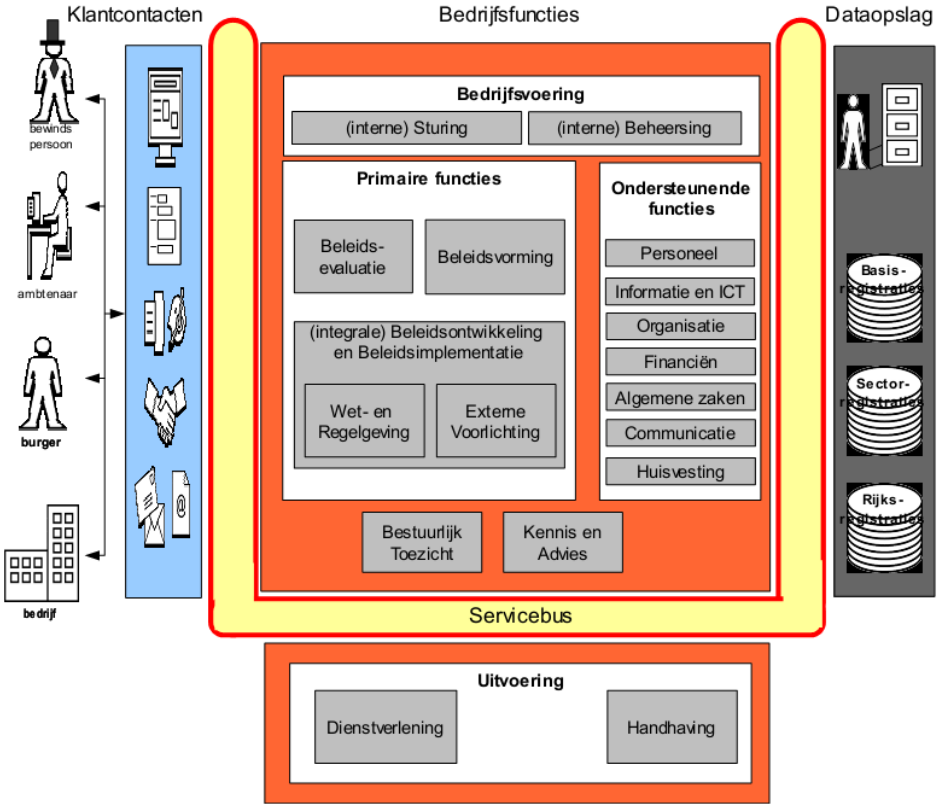
Binnen de NORA is ook een raamwerk aanwezig onder de naam "9-vlaks model" (zie Figuur 10), niet te verwarren met het Primavera model. Beide raamwerken hebben een dimensie

gemeen maar daarmee houdt de vergelijking zo goed als op. NORA beoogt voorschrijvend te zijn voor oplossingen op het gebied van ketensamenwerking, Primavera beoogt het informatiemanagement over een hele interne organisatie te structureren.

Typische operationele architectuurvragen zoals "Wanneer – Waarmee –Waar" worden in de NORA raamwerk buiten beschouwing gelaten vanuit de gedachte dat dit onderdeel moet zijn van de architectuur van een overheidsorgaan dat de referentiearchitectuur toepast op de eigen organisatie.

3.3.4 MARIJ

De Model Architectuur Rijksdienst (MARIJ) is een referentie architectuur (Logius, Kenniscentrum Architectuur, 2008). MARIJ 1.0 biedt een samenhangende architectuur voor de Rijksoverheid. Het is een houvast voor iedereen die vanuit "de concerngedachte" stappen wil zetten om de samenwerking tussen en binnen delen van de Rijksdienst te verbeteren. Dit is tevens de reden dat MARIJ relevant is voor dit onderzoek.



Figuur 9: MARIJ als basisarchitectuur voor een overheidsorganisatie (Logius, Kenniscentrum Architectuur, 2008)

MARIJ geeft verdere invulling aan het 9-vlaks model dat de NORA hanteert door vooral de "Hoe?" kolom nader uit te werken. Dit gebeurt door het invullen van een bedrijfsfunctiemodel en de verbijzondering van de NORA basisprincipes naar de Rijksoverheid als organisatie. MARIJ is veel rijker aan informatie dan de NORA en bevat een interessant beveiligingskatern, waarin ketensamenwerking is uitgewerkt in beveiligingsvoorschriften voor gegevenskoppelingen.

3.4 Beveiligingsarchitecturen

In deze paragraaf worden een aantal beveiligingsarchitecturen en standaarden beschreven.

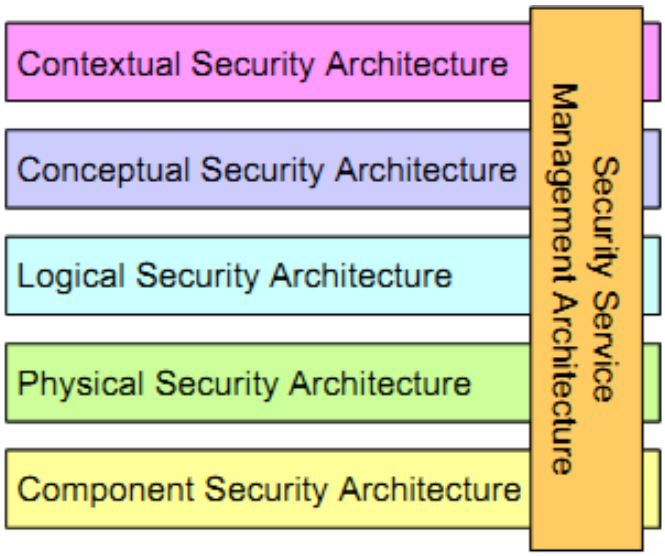
Er zijn slechts zeer weinig beveiligingsarchitecturen beschikbaar. Hiervoor zijn verschillende oorzaken aan te wijzen:

- In de literatuurstudie gevonden beveiligingsarchitecturen hebben hun naam gemeen, net als bij gewone architecturen blijkt na inhoudelijke analyse dat dit allerlei soorten documenten kunnen zijn (zie paragraaf 3.1), zoals technische documenten die implementaties van beveiligingsmaatregelen of security management processen beschrijven, of beleidsdocumenten en standaarden die onder de noemer beveiligingsarchitectuur zijn gepubliceerd. Publicatie van dit soort inhoudelijk gevoelige beveiligingsinformatie is niet waarschijnlijk.
- Ten tweede staat het vakgebied beveiligingsarchitectuur nog in de kinderschoenen, als dat wordt vergeleken met de het ontwikkelingsniveau van Enterprise Architecturen. De volgende voorbeelden illustreren de huidige dagelijkse praktijk: Master classes cursussen beveiligingsarchitectuur beperken zich tot het aangeven welke methodes, standaarden en best practices er zijn. De term "architectuur" veronderstelt structuur, samenhang op tactisch/strategisch niveau tussen strategische doelen, beveiligingsbeleid en de Enterprise Architectuur en dit zou moeten leiden tot overzicht, eenduidigheid en samenhang op operationeel niveau;

De enige echte beschikbare beveiligingsarchitectuur is SABSA. Deze wordt in de paragraaf 3.4.1 toegelicht. Voor het beoogde antwoord op de deelvraag is dit een te smalle basis om van uit te gaan in het ontwerp. Om die reden worden ook de ISO2700x standaard beschreven en het O-ISM3 raamwerk in respectievelijk paragraaf 3.4.2 en 3.4.3. Tot slot is een relevante externe beveiligingsarchitectuur voor hooggerubriceerde omgevingen beschreven in paragraaf 3.4.4.

3.4.1 Sabsa

Sabsa is het enige beschikbare model dat gezien kan worden als "Enterprise" Security Architecture" (Sherwood, Clark, & Lynas, SABSA Enterprise Security Architecture - A business driven approach, 2005). Sabsa definieert zichzelf als: "Model and methodology for developing risk-driven enterprise information security architectures and for delivering security infrastructure solutions that support critical business initiatives"



Figuur 10: SABSA model for Security Architecture (Sherwood, SABSA - Enterprise Security Architecture, 2009)

Het hart van SABSA is een ontwikkelproces dat beschrijft beveiligingsoplossingen kunnen worden gemaakt. Vanuit de SABSA visie is het cruciaal dat er gedacht wordt vanuit de bedrijfsvoering. Op deze wijze is beveiliging een "Business Enabler in plaats van een "Business Blocker".

Sabsa onderscheidt vijf views: Business, Architect, Designer, Builder en Tradesman (zie Figuur 12). Deze zijn zichtbaar gemaakt als de vijf gekleurde lagen. Dit zijn eigenlijk verschillende abstractieniveaus binnen de architectuur. De kolom "Security Service Management Architecture" zijn de processen gedefinieerd die nodig zijn om de uiteindelijk de beveiliging tot stand te brengen.

Figuur 11 laat de SABSA matrix zien: de abstractieniveaus zijn gekoppeld aan de contextvragen die afkomstig zijn uit een van de eerste Enterprise Architecturen: het Zachman framework (Zachman).

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
CONTEXTUAL ARCHITECURE	Business Decisions	Business Risk	Business Processes	Business Governance	Business Geography	Business Time Dependence
	Taxonomy of Business Assets, including Goals & Objectives	Opportunities & Threats Inventory	Inventory of Operational Processes	Organisational Structure & the Extended Enterprise	Inventory of Buildings, Sites, Territories, Jurisdictions, etc.	Time dependencies of business objectives
CONCEPTUAL ARCHITECTURE	Business Knowledge & Risk Strategy	Risk Management Objectives	Strategies for Process Assurance	Roles & Responsibilities	Domain Framework	Time Management Framework
	Business Attributes Profile	Enablement & Control Objectives; Policy Architecture	Process Mapping Framework; Architectural Strategies for ICT	Owners, Custodians and Users; Service Providers & Customers	Security Domain Concepts & Framework	Through-Life Risk Management Framework
LOGICAL ARCHITECTURE	Information Assets	Risk Management Policies	Process Maps & Services	Entity & Trust Framework	Domain Maps	Calendar & Timetable
	Inventory of Information Assets	Domain Policies	Information Flows; Functional Transformations; Service Oriented Architecture	Entity Schema; Trust Models; Privilege Profiles	Domain Definitions; Inter-domain associations & interactions	Start Times, Lifetimes & Deadlines
PHYSICAL ARCHITECTURE	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	ICT Infrastructure	Processing Schedule
	Data Dictionary & Data Inventory	Risk Management Rules & Procedures	Applications; Middleware; Systems; Security Mechanisms	User Interface to ICT Systems; Access Control Systems	Host Platforms, Layout & Networks	Timing & Sequencing of Processes and Sessions
COMPONENT ARCHITECTURE	ICT Components	Risk Management Tools & Standards	Process Tools & Standards	Personnel Man'ment Tools & Standards	Locator Tools & Standards	Step Timing & Sequencing Tools
	ICT Products, including Data Repositories and Processors	Risk Analysis Tools; Risk Registers; Risk Monitoring and Reporting Tools	Tools and Protocols for Process Delivery	Identities; Job Descriptions; Roles; Functions; Actions & Access Control Lists	Nodes, Addresses and other Locators	Time Schedules; Clocks, Timers & Interrupts
SERVICE MANAGEMENT ARCHITECTURE	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Management of Environment	Time & Performance Management
	Assurance of Operational Continuity & Excellence	Risk Assessment; Risk Monitoring & Reporting; Risk Treatment	Management & Support of Systems, Applications & Services	Account Provisioning; User Support Management	Management of Buildings, Sites, Platforms & Networks	Management of Calendar and Timetable

Figuur 11: SABSA Matrix (Sherwood, Clark, & Lynas, SABSA Enterprise Security Architecture - A business driven approach, 2005)

Het ontwikkelproces wordt de SABSA lifecycle genoemd. Dit is een variant van de kwaliteitscirkel van Deming (Deming, 1950) die in veel verschillende procesmodellen wordt gehanteerd.

SABSA bevat een methodologie om de (security) eisen en wensen (business requirements) in kaart te brengen. In essentie gaat beveiliging over kwaliteitsaspecten. SABSA gaat ervan uit dat goede beveiliging niet mogelijk is zonder eerst de business requirements goed in kaart te brengen. Alleen dan kan beveiliging ook een "business enabler" zijn.

3.4.2 ISO 2700X ISMS

De ISO27001 en ISO27002 internationale standaarden zijn een Information Security Management System. Het hart van dit model is een procesmodel waarbinnen de beveiliging

tot stand komt en gecontroleerd wordt verbeterd via een Plan-Do-Check-Act cyclus (Deming, 1950). De ISO standaard kent een bijbehorende Risico management methode (ISO 27005).

De ISO standaard gaat uit van Standaard best practices die "control objectives" op het gebied van informatiebeveiliging op procesniveau beschrijven (ISO27002). Ze beschrijven een beveiligingsdoelstelling die generiek wordt uitgewerkt. De "control objectives" zijn op een vrij hoog abstractieniveau geformuleerd met als gevolg dat ze prima generiek toepasbaar zijn. Hierdoor ontstaat echter ook een vrij grote natuurlijke afstand tussen de controle doelstellingen en de dagelijkse praktijk waarin beveiligingsmaatregelen worden geïmplementeerd. In kleine organisaties is de natuurlijke afstand geen belemmering. Juist in middelgrote en grotere organisaties is een juiste besturing van de operationele beveiliging noodzakelijk om de controledoelstellingen aangesloten te houden bij de dagelijkse praktijk.

De ISO standaard is belangrijk omdat dit een van de weinige Information Security Management Systems is waarvoor een organisatie gecertificeerd kan worden. Voor veel grote bedrijven is dit een vereiste op grond van internationale wet- en regelgeving.

3.4.3 O-ISM3

"The Open Group Information Security Management Maturity Model" O-ISM3 (Aceituno, Vincente; The Open Group, 2011) definieert beveiliging als resultante van een groot aantal mogelijke processen. De achterliggende gedachte is: hoe beter het proces, hoe beter de ROI van beveiliging om informatie te beschermen.

De uitgangspunten van het model (Narayaban, 2006):

- Het model gaat uit van "achievable security". Er is een proces dat beveiligingsdoelstellingen en de organisatie doelstellingen afstemt door het afspreken van targets. Deze targets worden in de processen meetbaar gemaakt;
- Security-in-context: "Secure" (beveiligd) betekent traditioneel niet-kwetsbaar, met andere woorden biedt weerstand tegen elke vorm van aanval, hier betekent "Secure" betrouwbaar, ondanks aanvallen, ongelukken en fouten;
- Wat traditioneel als een aantasting van beschikbaarheid, integriteit of exclusiviteit wordt gezien, betekent in het O-ISM3 model "het niet halen van organisatiedoelstellingen".

O-ISM3 onderkent vier modellen die gebruikt worden om de beveiliging vorm te geven:

1. ISM (Information Security Management) Process Model - het identificeren van hoofdprocessen;
2. Responsibilities Model – geeft een beeld van de organisatie vanuit gedelegeerde verantwoordelijkheden;
3. Security in Context Model – stemt bedrijfsdoelstellingen en beveiligingsdoelstellingen op elkaar af;
4. Information System Model – beschrijft en identificeert bedrijfskritische Informatie Systemen in de organisatie.

Verder bevat het O-ISM3 model sets van beveiligingsprocessen en onderscheidt daarin drie niveaus: strategisch, tactisch en operationeel. Ook worden aparte beveiligingsdomeinen in de organisatie onderscheiden: de vraag naar beveiliging is afhankelijk van de beveiligingsdoelstellingen die in bepaalde delen van de organisatie noodzakelijk zijn. Op deze wijze bepaalt de organisatie in welke situatie beveiligingsprocessen worden toegepast en in welke vorm.

3.4.4 Aanvulling op het BBNP

Er bestaat een beveiligingsarchitectuur voor hooggerubriceerde informatie van de Nederlandse politie (KLPD, 2006). Deze architectuur is bedoeld als een aanvulling op het BBNP waarin de specifieke beveiligingseisen voor hooggerubriceerde informatie zijn vastgelegd. De politie organisatie kent het Basis beveiligingsniveau Nederlandse Politie (BBNP). Het BBNP bestaat uit een pakket van beveiligingsmaatregelen op fysiek, logisch en

organisatorisch gebied. Het BBNP zelf is niet ingericht op beveiliging van hooggerubriceerde informatie.

De doelstellingen van de architectuur zijn:
- Aansluiten bij de bedrijfs- en procesarchitectuur
- Het vinden van de juiste balans tussen ”need-to-know” en “need-to-share”[5]

De opbouw van de beveiligingsarchitectuur is analoog aan de Informatie Architectuur Nederlandse Politie die ten tijde het schrijven van dit document actueel was. De informatiearchitectuur kent vijf niveaus: strategie en beleid, bedrijfsarchitectuur, informatieachitectuur, applicatiearchitectuur en Infrastructuurarchitectuur. De scope sluit het onderdeel “strategie en beleid” uit. Strategie en beleid wordt als randvoorwaardelijk beschouwd.

De architectuur is beschreven langs de vijf niveaus door middel van uitgewerkte principes, ontwerpregels en standaarden. Het principe is een (lange termijn) kernwaarde, de ontwerpregel is afgeleid van een principe en geeft sturing aan de invulling, net als de standaarden.

Daarnaast zijn beveiligingsfuncties benoemd waarlangs de beveiliging van de infrastructuur wordt uitgesplitst. Dit zijn aspectgebieden voor beveiliging die het indelen van uitvoeringsmaatregelen mogelijk maken naar beveiligingsgebied, bijvoorbeeld identificatie & authenticatie, transport & opslag inbraakpreventie & detectie. De infrastructuur architectuur wordt ingevuld door fysieke zonering te combineren met deze aspectgebieden en daarop (in principevorm) maatregelen en uitgangspunten voor de invulling van beveiliging te beschrijven.

3.4.5 Toekomstige ontwikkelingen

Op het gebied van beveiligingsarchitecturen is een belangrijke beweging gaande. O-ISM3 wordt op dit moment geïntegreerd in TOGAF. De integratie betekent dat het O-ISM3 raamwerk is vastgesteld als het Open Group raamwerk voor security management.

De tweede beweging die plaatsvindt is de integratie van SABSA in TOGAF. TOGAF integreert de in SABSA gehanteerde methodologie voor requirements management. Requirements management is een kernonderdeel van TOGAF, maar ook van oudsher bekend als een zwak punt in het TOGAF raamwerk. De wijze waarop SABSA omgaat met requirements management is een van de sterke punten van SABSA.

3.5 Het vergelijken van Architecturen

Er zijn in de literatuur over architecturen een aantal referenties te vinden die tot doel hebben architecturen te vergelijken. De criteria waarop de architecturen worden vergeleken en de vergelijkingen zelf, zullen in deze analyse gebruikt worden. De vergelijkingen zijn afkomstig van Sessions (Sessions, 2007), die raamwerken van Zachman, TOGAF, FEA en Gartner vergelijkt. Een andere bron die Enterprise Architecturen vergelijkt is (Stekkerman, 2004). Ook Gartner vergelijkt Enterprise Architecturen (Gartner, 2006). Tot slot is gebruikt gemaakt van een vergelijking van O-ISM3 (ISM3 Consortium, 2007) en ISO2700X (ISO/IEC, 2005). Dit zijn procesraamwerken op het gebied van Information Security Management.

3.5.1 Wijze van vergelijken

(Sessions, 2007) trekt in zijn vergelijking van vier architectuurraamwerken de volgende algemene conclusie: raamwerken vergelijken op inhoudelijke criteria blijkt problematisch. In de methodologie achter de raamwerken is weinig gemeenschappelijke basis te vinden. Ze hebben hetzelfde doel maar de wijze waarop de Enterprise Architectuur tot stand komt, het toepassingsgebied en het gehanteerde perspectief bij het kijken naar de organisatie zijn

[5] Het concept “Need to protect” wordt hier niet gehanteerd.

wezenlijk verschillend. De vergelijking van de Enterprise Architecturen vlg. (Sessions, 2007), (Stekkerman, 2004) kan alleen plaatsvinden op strategisch niveau, waarbij vooral de bruikbaarheid van de architectuur in een bedrijfscontext wordt getoetst (Gartner, 2006) onderschrijft deze conclusie. Bijlage A bevat de volledige lijst met criteria.

3.5.2 Vergelijkingscriteria

De criteria uit Bijlage A worden nu vertaald naar vergelijkingscriteria voor deze analyse. Dit wordt gedaan omdat er veel overeenkomstige criteria zijn, afkomstig uit verschillende bronnen. De vergelijkingscriteria zijn zodanig opgebouwd dat ze alle criteria uit de lijst in bijlage A omvatten. In de rest van deze paragraaf worden de vergelijkingscriteria kort beschreven:

- Per criterium is aangegeven uit welke bronnen het criterium afkomstig is;
- Om de criteria bruikbaar te maken als meetinstrument volgt daar waar nodig een korte afbakening van het criterium voor dit specifieke onderzoek;
- Uiteindelijk wordt een Key Perfomance Indicator (KPI) vastgesteld. De normering die is gebruikt, is afkomstig uit (Stekkerman, 2004), de normering van (Sessions, 2007) en (ISM3 Consortium, 2007) zijn hieraan aangepast.

Criterium 1 Compleetheid van scope;
Hoe ziet de scope van de architectuur of raamwerk eruit?
(Gartner, 2006), (ISM3 Consortium, 2007), (Sessions, 2007), (Stekkerman, 2004)
Scope van de architectuur is gedefinieerd als de compleetheid waarmee de organisatie wordt beschouwd: proces, organisatie, mensen, en informatie, interdependenties en externe relaties. (Gartner, 2006), (Sessions, 2007) en (Stekkerman, 2004) vinden een brede scope belangrijk omdat een architectuur niet in scope zou moeten worden beperkt. Er zou juist vanuit de bedrijfsstrategie geredeneerd moeten worden om mede de toekomst van het bedrijf te bepalen.

Voor dit onderzoek is deze brede scope ook van belang, omdat veiligheidsmaatregelen uiteindelijk in samenhang worden genomen op grensvlakken tussen verschillende bedrijfsobjecten en hun omgeving: proces, organisatie, mensen, informatie, interdependenties en externe relaties. Deze zijn allemaal relevant voor beveiliging.

Norm: (-- - N + ++) waarbij ++ de volledige dekkingsgraad over de organisatie is.

Criterium 2 Koppeling met strategische doelstellingen;
Mate waarin de architectuurmethode is gekoppeld aan bedrijfsdoelstellingen.
(Gartner, 2006), (ISM3 Consortium, 2007), (Sessions, 2007), (Stekkerman, 2004)
Alle schrijvers van de vergelijkingsdocumentatie geven aan dat het noodzakelijk is voor een architectuur om zijn toegevoegde waarde voor het bedrijf aan te tonen. Dat kan alleen door de architectuur te koppelen aan bedrijfsdoelstellingen: op deze manier kunnen ontplooide activiteiten en gebruik van middelen worden verantwoord.

Niet alleen de koppeling naar bedrijfsdoelstellingen is van belang, in een beveiligingsarchitectuur horen ook de (secundaire) doelstellingen op het gebied van beveiliging te worden opgenomen.

Norm (-- - N + ++) (niet – volledig)

Criterium 3 Organisatorische inbedding;
De mate waarin architectuur ondersteuning biedt aan de ontwikkeling binnen de rest van de organisatie (architectuur als cultuur).
(Gartner, 2006), (ISM3 Consortium, 2007), (Sessions, 2007), (Stekkerman, 2004)
Architectuur bedrijven is alleen zinvol als de ontwikkeling van de architectuur breed wordt ondersteund door alle geledingen binnen de organisatie. (Gartner, 2006), (Sessions, 2007) en (Stekkerman, 2004) geven aan dat de architectuur vooral de communicatie binnen de

organisatie moet bevorderen. Dit zorgt voor een gemeenschappelijke gedragen visie op basis waarvan beslissingen die veranderingen sturen kunnen worden genomen.

Norm (-- - N + ++) (niet – volledig)

Criterium 4 Besturingsmodel;
Bevat de architectuurmethode of raamwerk een effectief besturingsmodel voor architectuur? (Sessions, 2007)
Sessions ziet de governance van architectuur als een criterium vanwege het feit dat het ontbreken van een leidraad die de governance regelt, blokkerend werkt voor de implementatie van de architectuur in de organisatie.

Norm (ja/nee)

Criterium 5 Delegatie van taken;
Hoe goed ondersteunt een architectuur de distributie van verantwoordelijkheden en architectuurwerkzaamheden over de organisatie?
(ISM3 Consortium, 2007), (Sessions, 2007)
Verantwoordelijkheden delegeren is een belangrijk aspect voor (Sessions, 2007). Hij stelt dat de capaciteit van een architectuurteam in een organisatie beperkt is en dat het vaak noodzakelijk is om onderhoudstaken te delegeren naar andere delen van de organisatie. O-ISM3 signaleert een hetzelfde probleem vanuit een beveiligingsperspectief. De algemene praktijksituatie is dat er bedrijfsprocessen zijn waarvan beveiliging een belangrijk onderdeel uitmaakt, maar waar niet direct duidelijk is wie er nu verantwoordelijk is voor de beveiliging van het proces.

Norm (-- - N + ++) (niet – volledig)

Criterium 6 Eigen ontwikkeling en toekomstvastheid;
In hoeverre ondersteunt de architectuur of het raamwerk de eigen ontwikkeling en onderhoud en is deze toekomstvast.
(Gartner, 2006), (ISM3 Consortium, 2007), (Sessions, 2007), (Stekkerman, 2004)
Er zijn architecturen die erop gericht zijn om zichzelf continu te verbeteren. Er zijn ook architecturen die vooral gericht zijn op documenteren. Gartner en (Sessions, 2007) zien dit als aandachtspunt omdat van een Enterprise Architectuur verwacht mag worden dat er onderhoudsprocessen vastgelegd zijn. (Sessions, 2007) en O-ISM3 zien een risico in gebruik van methodieken en best-pratices die niet of slecht onderhouden worden, waardoor de architectuur niet met zijn tijd meegroeit.

Norm: (-- - N + ++) (niet ondersteund – volledig ondersteund)

Criterium 7 Architectuurproductondersteuning;
Biedt de architectuur of het raamwerk referentiemodellen, best practices en methodieken?
(ISM3 Consortium, 2007), (Sessions, 2007)
Naarmate een architectuur breder is gedocumenteerd zal er minder werk nodig zijn voor architecten om de architectuur te ontwerpen. Dit draagt bij aan een snelle realisatie van de architectuur.

Norm: (-- - N + ++) (niet ondersteund – volledig ondersteund)

Criterium 8 Volwassenheidsniveaus en toekomstdenken;
In hoeverre ondersteund de architectuur volwassenheidniveaus binnen verschillende delen van de organisatie?
(Gartner, 2006), (ISM3 Consortium, 2007), (Sessions, 2007), (Stekkerman, 2004)
(Sessions, 2007) benadert volwassenheidsniveaus vanuit een bedrijfsperspectief. Een Enterprise Architectuur moet verschillende niveaus van volwassenheid binnen de organisatie

onderkennen. Als dit niet gebeurd dan kan dat tot problemen leiden. O-ISM3 benadrukt dat het juiste beveiligingsniveau gekozen moet kunnen worden. Dit veronderstelt:

- dat in processen gemeten kan worden: zonder meetgegevens is het niet mogelijk om volwassenheidsniveaus dan wel beveiligingsniveaus te hanteren;
- dat wordt onderkend dat een huidige en een toekomstige situatie bestaat, ook wel plateau-denken genoemd (ISM3 Consortium, 2007) (Stekkerman, 2004);
- dat processen aanwezig zijn om organisatieveranderingen in goede banen te leiden en de flexibiliteit van de organisatie als geheel te bevorderen (Gartner, 2006) en (Stekkerman, 2007).

Norm (-- - N + ++) (niet – volledig)

Criterium 9 Aanwezigheid objecten catalogus;
Mate waarin de architectuur de productie van een architectuur objecten catalogus ondersteunt.
(Sessions, 2007)
Sessions benadrukt dat de aanwezigheid van een catalogus noodzakelijk is om hergebruik van componenten mogelijk te maken. Het doel hiervan is complexiteits- en kostenreductie door hergebruik.

Norm (-- - N + ++) (niet – volledig)

Criterium 10 Vendor Lock-in;
De hoeveelheid informatie die vrij of tegen geringe kosten beschikbaar is over raamwerken of architecturen.
(ISM3 Consortium, 2007), (Sessions, 2007)
Er zijn rijke architecturen waarvan de inhoud tegen substantiële bedragen onder licentie beschikbaar wordt gesteld. Gebruik hiervan leidt mogelijk tot een vendor lock-in: zolang de architectuur wordt gebruikt ben je gehouden aan licenties en bijbehorende methodieken. Het leidt waarschijnlijk wel tot snelle implementatie met bijbehorend resultaat. Er zijn ook goede architecturen die tegen geringe kosten gebruikt kunnen worden. Daarbij wordt veelal gebruik gemaakt van standaarden en best practices. (Sessions, 2007) en O-ISM3 zien vendor-lock in als een bedreiging.

Norm (-- - N + ++) (hoog – laag)

Criterium 11 Implementatietijd;
De tijd die het kost voordat een architectuurmethode toegevoegde waarde gaat opleveren voor de organisatie.
(Sessions, 2007)

Norm (-- - N + ++) (1 jaar – 5 jaar)

Criterium 12 Certificering;
In hoeverre levert de architectuur of het raamwerk een bijdrage aan het vertrouwen dat de organisatie geniet van het management en/of externe partijen?
(ISM3 Consortium, 2007)
Certificering en gebruik van bepaalde standaarden is vooral belangrijk vanuit compliancy omdat dit een bepaalde zekerheid geeft over de manier van werken en zelfs in normatieve zin iets zegt over de staat van beveiliging.

Norm (-- - N + ++) (niet – volledig)

Criterium 13 Architectuur succesfactoren;
Is controleerbaar wanneer een architectuur of raamwerk aan de verwachtingen voldoet?
(ISM3 Consortium, 2007), (Stekkerman, 2004)

Volgens (Stekkerman, 2004) is Gartner erg gericht op de bruikbaarheid van een architectuur. Je kunt alleen vaststellen of de architectuur werkt als je vooraf definieert wat je met de architectuur wil bereiken. O-ISM3 ziet dat ook: vooraf ambitieniveaus en verwachtingen vaststellen zodat achteraf aantoonbaar is of de architectuur voldoet of niet.

Norm: (ja – nee)

Criterium 14 Aandacht voor beveiliging
Besteed een architectuur aandacht aan beveiliging?
(The Open Group Architecture Framework (TOGAF), 2009), (ISO/IEC, 2005).
Er zijn verschillende manieren waarop beveiliging opgenomen kan zijn in de architectuur. Hierbij is van belang of er aandacht voor is, of daarbij het strategisch niveau wordt belicht (vanuit de visie dat een holistische benadering van beveiliging noodzakelijk is), of de architectuur of het raamwerk beveiligingsaspecten definieert.

Norm (-- - N + ++) (niet – volledig)

3.5.3 Samenvatting Criteria

De in de vorige paragraaf beschreven criteria zijn in Tabel 2 samengevat.

#	Criterium	defintie
1	Compleetheid van scope	De mate waarin de architectuur toestaat objecten wel of niet te classificeren
2	Koppeling met strategische doelstellingen	Mate waarin de architectuurmethode zijn eigen toegevoegde waarde voor de organisatie zichtbaar maakt
3	Organisatorische inbedding	De mate waarin architectuur binnen de rest van de organisatie is doorgedrongen en wordt gebruikt (architectuur als cultuur)
4	Besturingsmodel	Bevat de architectuurmethode of raamwerk een effectief besturingsmodel voor architectuur
5	Delegatie van taken	De mate waarin verspeiding van de werkzaamheden over de organisatie om een architectuur te beheren wordt ondersteund.
6	Eigen ontwikkeling en toekomstvastheid	Hoe goed is de procesondersteuning voor het creeren en onderhouden voor de EA
7	Architectuur productondersteuning	Hoe goed ondersteunt de methode de bouw van relevante referentie modellen
8	Volwassenheidsniveau en toekomstdenken	In hoeverre ondersteund de architectuur volwassenheidniveaus binnen verschillende delen van de organisatie
9	Ondersteuning van een objecten catalogus	Mate waarin de architectuur ondersteund in het maken van een architectuur objecten catalogus met als doel hergebruik van componenten.
10	Vendor lock-in	De mate van vendor lock-in die plaatsvindt als wordt gekozen voor een specifieke architectuur methode
11	Implementatietijd	De tijd die het kost voordat een architectuurmethode toegevoegde waarde gaat opleveren voor de organisatie
12	Certificering	Certificering van de organisatie kan een bijdrage leveren aan het vertrouwen dat de organisatie geniet van management en/of externe partijen
13	Architectuur succesfactoren	Is controleerbaar wanneer een architectuur of raamwerk aan de verwachtingen voldoet
14	Aandacht voor beveiliging	De mate waarin beveiliging is vertegenwoordigd in het raamwerk of de architectuur

Tabel 2: Selectiecriteria architecturen H3

Om deze criteria toe te kunnen passen op architectuurraamwerken is een multicriteriatabel opgezet (zie Tabel 3). De verticale as bevat de criteria, op de horizontale as zijn alle architecturen en raamwerken opgenomen die in dit hoofdstuk aan de orde zijn geweest. In de tabel is vervolgens ingevuld hoe een bepaald raamwerk scoort op het aangegeven criterium. De scores zijn op drie manieren tot stand gekomen:

- Rode scores zijn afkomstig uit vergelijkingsdocumentatie van Sessions (Sessions, 2007);
- Groene scores zijn afkomstig uit vergelijkingsdocumentatie van O-ISM3 (ISM3 Consortium, 2007);
- Blauwe scores zijn toegekend door een expert panel. Vijf personen hebben de architectuurbeschrijvingen geanalyseerd. Vervolgens is de gemiddelde de score bepaald door de volgende rekenmethode toe te passen:
    - -- = -2
    - - = -1
    - N = 0
    - + = 1
    - ++ = 2

  Waarna het rekenkundig gemiddelde is bepaald en terugvertaald volgens dezelfde tabel naar de normering die in de criteria gebruikt zijn.
- De volgende documenten zijn als referentie gebruikt: (Stekkerman, 2004) (The Open Group Architecture Framework (TOGAF), 2009) (Gartner Defines the Term "Enterprise Architecture", 2006) (ISO/IEC 27001:2005 - Information technology -- Security techniques -- Information security management systems -- Requirements, 2005) (Zachman) (PrimaVera - An Integrative Perspective on Information Management, 2007) (MARIJ, 2008) (Nora 3.0 - prinipes voor samenwerking en dienstverlening, 2010) (SABSA - Enterprise Security Architecture, 2009).

		TOGAF	Zachman	FEA	EISA Framework (Gartner)	NORA	MARIJ	Primavera	beveiligings arch politie	SABSA	O-ISM3	ISO 2700x
1	Compleetheid van scope	O	++	O	-	+	O	--	O	+	O	-
2	Koppeling met strategische doelstellingen	O	--	-	++	++	+	O	+	++	++	--
3	Organisatorische inbedding	O	--	O	++	--	-	+	--	-	++	--
4	Besturingsmodel	+	--	+	+	--		O	--	++	+	O
5	Delegatie van taken	O	--	++	+	-	-	-	--	O	++	--
6	Proces voor eigen ontwikkeling	++	-	-	+	-	+	-	--	-	++	O
7	Architectuur productondersteuning	+	--	++	--	+	-	--	--	++	+	+
8	Volwassenheidsniveau en toekomstdenken	-	--	+	O	-	-	-	--	+	++	-
9	Ondersteuning van een objectencatalogus	O	--	++	+	+	O	--	+	++	+	O
10	Vendor lock-in (-- = hoog)	++	-	O	--	--	--	++	--	-	++	+
11	Implementatietijd	+	--	--	++	+	-	+	++	--	O	O
12	Certificering	++	--	-	O	-	--	--	--	-	++	++
13	Architectuur succesfactoren	ja	nee	nee	ja	nee	nee	nee	nee	ja	ja	nee
14	Aandacht voor beveiliging	+	--	-	-	+	+	--	+	++	++	O
	Bron	Sessions	Sessions	Sessions	Sessions	zelf	zelf	zelf	zelf	zelf	ISM3	ISM3

Tabel 3: Criteria en architecturen

Deze multicriteriatabel zal gebruikt worden voor de onderbouwing van de selectie van onderdelen van de beveiligingsarchitectuur mogelijk te maken. Dit is verder uitgewerkt in hoofdstuk 4.

4 Ontwerp beveiligingsarchitectuur

Dit hoofdstuk bevat het ontwerp voor een beveiligingsarchitectuur. De volgende deelvraag wordt in dit hoofdstuk uitgewerkt:

> 3) Uit welke elementen bestaat een beveiligingsarchitectuur?

Het ontwerpproces is opgebouwd uit twee stappen. De eerste stap omvat de selectie van het raamwerk. Een raamwerk is eigenlijk een keuze voor een basisarchitectuurmodel waar de rest van de architectuurcomponenten aan gekoppeld worden. De tweede stap is de invulling van de architectuurcomponenten waaruit de beveiligingsarchitectuur zal bestaan.

Voor de keuzes die gemaakt moeten worden bij het ontwerp van een beveiligingsarchitectuur zijn een aantal randvoorwaarden en ontwerpeisen beschikbaar:

1. De principes die voortvloeien uit de strategische- en organisatorische context (zie paragraaf 2.4);
2. De principes ontwerpeisen vanuit die door de organisatie zijn meegegeven (zie paragraaf 2.4);
3. De selectiecriteria voor architecturen (zie paragraaf 3.5.3).

De ontwerpkeuzes zullen op basis van deze gegevens worden gemaakt.

In paragraaf 4.1 wordt de keuze van het raamwerk toegelicht (stap 1). In paragraaf 4.2 wordt bepaald welke bouwelementen noodzakelijk zijn voor een beveiligingsarchitectuur. Paragraaf 4.3 vult de bouwelementen in (stap 2) en paragraaf 4.4 reflecteert op de verschillen tussen architecturen en referentiearchitecturen. Daarna wordt in paragraaf 4.5 wordt het ontwerp samengevat. In paragraaf 4.6 wordt getoetst op volledigheid door te controleren of alle randvoorwaarden en ontwerpeisen zijn gebruikt bij het de keuzes voor bouwelementen.

4.1 Keuze raamwerk

De selectiecriteria voor architecturen zijn opgenomen in een multicriteriatabel. Om uiteindelijk het raamwerk te kiezen is het noodzakelijk om aan te geven welke raamwerken in aanmerking komen voor de keuze van het raamwerk. Ook wordt bepaald welke selectiecriteria leidend zijn voor de keuze van het raamwerk door te kijken wat de randvoorwaarden en ontwerpeisen hierover zeggen.

Principe 12 en de ontwerpeisen O9 t/m O13 zijn op de volgende manier van toepassing op criteria in de multicriteriatabel:

- Principe P12 schrijft voor dat de beveiligingsarchitectuur integraal moet wordt beschouwd. Criterium 1 (compleetheid van scope) beschrijft dit ook;
- Ontwerpeis O9 beschrijft de noodzakelijke koppeling met strategische doelstellingen, net als Criterium 2;
- Ontwerpeisen O10 en O13 stellen eisen aan de wijze waarop de besturing van de architectuur wordt geregeld in de organisatie, dat is in lijn met criteria 4 en 5. Ontwerpeis O12 gaat over toekomstperspectief, dit correspondeert met criterium 6;
- Volgens ontwerpeis O11 moet beveiliging meetbaar gemaakt worden. Dat kan alleen als er sprake is van denken in volwassenheidsniveaus in combinatie met toekomstdenken. Dit is in lijn met de inhoud van criterium 8.

In Tabel 4 is dit zichtbaar gemaakt door betreffende criteria groen te arceren.

#	Criterium	TOGAF	Zachman	FEA	EISA Framework (Gartner)	NORA	MARIJ	Primavera	beveiligingsarchitectuur politie	SABSA	O-ISM3	ISO 2700X
1	Compleetheid van scope	O	++	O	-	+	O	--	O	+	O	-
2	Koppeling met strategische doelstellingen	O	--	-	++	++	+	O	+	++	++	--
3	Organisatorische inbedding	O	--	O	++	--	-	+	--	-	++	--
4	Besturingsmodel	+	--	+	+	--		O	--	++	+	O
5	Delegatie van taken	O	--	++	+	-	-	-	--	O	++	--
6	Proces voor eigen ontwikkeling	++	-	-	+	-	+	-	--	-	++	O
7	Architectuur productondersteuning	+	--	++	--	+	-	--	--	++	+	+
8	Volwassenheidsniveau en toekomstdenken	-	--	+	O	-	-	-	--	+	++	-
9	Ondersteuning van een objectencatalogus	O	--	++	+	+	O	--	+	++	+	O
10	Vendor lock-in (-- = hoog)	++	-	O	--	--	--	++	--	-	++	+
11	Implementatietijd	+	--	--	++	+	-	+	++	--	O	O
12	Certificering	++	--	-	O	-	--	--	--	-	++	++
13	Architectuur succesfactoren	ja	nee	nee	ja	nee	nee	nee	nee	ja	ja	nee
14	Aandacht voor beveiliging	+	--	-	-	+	+	--	+	++	++	O
	Bron	Sessions	Sessions	Sessions	Sessions	zelf	zelf	zelf	zelf	zelf	O-ISM3	O-ISM3

Tabel 4: Kader keuze raamwerk

Architecturen, raamwerken of standaarden die geen bruikbaar raamwerk bevatten kunnen niet als architectuurraamwerk gebruikt worden. Dit geldt voor de beveiligingsarchitectuur politie, O-ISM3 en ISO2700x.

Architecturen en raamwerken die andere dimensies hanteren dan die nu in de Enterprise Architectuur worden gebruikt, voldoen in principe niet aan ontwerpeisen O1 t/m O4. Deze ontwerpeisen schrijven voor hoe de koppeling tussen de beveiligingsarchitectuur en de Enterprise Architectuur eruit moet zien. Zachman, SABSA, FEA en EISA gebruiken allemaal andere dimensies in hun hoofdraamwerk.

Hierdoor blijven alleen Primavera, TOGAF, NORA en MARIJ over als mogelijke kandidaten. In Tabel 4 is te zien dat TOGAF en Primavera het best scoren op de relevante criteria (groen gearceerde rijen), van de mogelijke raamwerken (groen gekleurde raamwerken).

Het Primavera 9-vlaks model wordt vooral gehanteerd om bedrijfsbrede informatie gerelateerde kwesties op managementniveau bespreekbaar te maken. In eerste instantie was het doel van dit model om "Informatie Management in brede zin" te ontwikkelen binnen de organisatie. Pas in een later stadium, bij het invullen van het raamwerk, ontstond vraag naar Enterprise Architectuur en zijn producten. Daarin voorziet Primavera niet. TOGAF speelt vooral een rol op het niveau van de architectuurprocessen: ontwikkeling van de architectuur en zijn producten en in de koppeling met de rest van de organisatie (bijvoorbeeld via project portfolio management, plannen van vernieuwingstrajecten, technologiekeuze, rationalisatie systeemlandschap, etc.).

Het gekozen raamwerk bestaat uit een combinatie Primavera en TOGAF.

Door de Primavera/TOGAF combinatie als raamwerk te gebruiken, wordt het beste voldaan aan de eisen en randvoorwaarden: er is een aantoonbare relatie met de Enterprise Architectuur, er wordt zoveel mogelijk gebruik gemaakt van bestaande architectuurprocessen, bestaande architectuurproducten voor beveiliging worden ondersteund en in samenhang beschreven. Bij het ontwikkelen van de beveiligingsarchitectuur levert dit een besparing vanwege mogelijk hergebruik van architectuuronderdelen.

TOGAF en Primavera vormen samen geen beveiligingsarchitectuur. Het is daarom noodzakelijk om te analyseren welke andere bouwelementen nodig zijn om uiteindelijk een beveiligingsarchitectuur te realiseren.

4.2 Tekortkomingen Primavera/Togaf

Met het gekozen raamwerk in het achterhoofd rijst de vraag in hoeverre TOGAF toepasbaar is als beveiligingsarchitectuur. De vraag is nu: welke basiselementen uit een beveiligingsarchitectuur ontbreken in Primavera/TOGAF?

Stekkerman beschrijft een groot aantal architecturen langs lijnen, die gezien kunnen worden als noodzakelijke elementen in een architectuur (S), (Stekkerman, 2004). Daarnaast zijn nog een aantal gemeenschappelijke beveiligingscomponenten te onderscheiden die aanwezig zijn in SABSA en de andere beveiligingsraamwerken uit paragraaf 3.4 (B):

Raamwerk	S	Architectuur bevat een raamwerk in de vorm van een structuurbeschrijving waarin enerzijds een decompositie van de organisatie is gemaakt en waarin anderzijds abstractieniveaus zijn te onderscheiden die zo gekozen worden dat de juiste onderwerpen en relaties benoemd kunnen worden;
Procesmodel	S	De architectuur bevat een procesmodel waarin wordt vastgelegd hoe de architectuur ingrijpt op de organisatie en de bedrijfsprocessen.
Veiligheids-aspectgebieden	B	De beveiligingsarchitectuur kent veiligheidsaspectgebieden;
Metamodel	S	De architectuur bevat een metamodel waarin is vastgelegd welke objecten in de architectuur zijn opgenomen;
Principes	S	De architectuur bevat principes;
Viewpoints	S	De architectuur kan verschillende viewpoints bevatten. Viewpoints zijn is een middel om het perspectief op een onderwerp van specifieke belanghebbenden vast te leggen;
Beveiligings-Processen	B	De beveiligingsarchitectuur bevat besturingsprocessen voor beveiliging;
Risicoanalyse	B	De beveiligingsarchitectuur is risico gebaseerd.
Visie	S	De architectuur bevat een visie die uitlegt wat het doel en de scope is van de architectuur;

Bovenstaand overzicht geeft aan welke noodzakelijke onderdelen een beveiligingsarchitectuur moet bevatten. Nu dit bekend is, kan bepaald worden op welke wijze deze elementen moeten worden ingevuld.

4.3 Selectie van bouwelementen

Bij de selectie van bouwelementen gelden de volgende uitgangspunten:

1) TOGAF/Primavera zijn primaire leverancier van bouwelementen;
2) Indien TOGAF/Primavera niet kan voorzien in een bouwelement, zal deze uit een andere architectuur, raamwerk of standaard moeten worden geselecteerd. Hiervoor kan het overzicht in Tabel 4 worden gebruikt. Dat Sabsa als raamwerk ongeschikt is, wil niet zeggen dat bepaalde goed uitgewerkte onderdelen van deze beveiligingsarchitectuur niet gebruikt zou kunnen worden. Dit geldt in principe voor alle architecturen in Tabel 4;
3) Het overzicht met randvoorwaarden en ontwerpeisen en de architectuurbeschrijvingen uit H3 worden gebruikt om de keuze te onderbouwen.

De multicriteriatabel (zie Tabel 4) die gebruikt wordt voor de selectie van bouwelementen, bevat vergelijkingscriteria die zijn geaggregeerd. Bij de selectie van sommige bouwelementen is het noodzakelijk om te kijken naar de sub-criteria waaruit een criterium bestaat, omdat het sub-criterium op zichzelf relevant is voor het bouwonderdeel. Een totaaloverzicht waarin zichtbaar is op welke wijze een criterium is opgebouwd staat vermeld in bijlage A.

In de volgende paragrafen worden gemaakte keuzes onderbouwd door te bepalen in hoeverre de combinatie TOGAF/Primavera voorziet in het bouwelement, of te kijken welke elementen beschikbaar zijn. Daarna wordt de keuze beargumenteerd en vastgesteld.

4.3.1 Procesmodel Architectuur

Voor het procesmodel zijn een aantal kandidaten beschikbaar (Tabel 4, criterium 6): TOGAF, O-ISMS3, SABSA, EISA, NORA, MARIJ en IOS2700X. Procesmodellen voor de beveiligingsraamwerken (SABSA, ISO2700X en O-ISMS3) zijn alleen relevant voor beveiligingsprocessen (zie 4.3.6), daarom vallen deze af als kandidaat voor het architectuurprocesmodel. In eerste instantie wordt gekeken naar TOGAF.

Het procesmodel van TOGAF is de ADM (zie voor een inhoudelijke toelichting paragraaf 3.3.2). De ADM heeft een aantal eigenschappen die dit procesmodel geschikt maken om toe te passen binnen de beveiligingsarchitectuur:

1) De TOGAF ADM kent drie abstractieniveaus: strategische-, segment- en capability architectuur. Deze architecturen kunnen onafhankelijk van elkaar onderhouden worden. De ontwerpeisen zijn duidelijk over het gewenste abstractieniveau: zodanig uitgewerkt dat implementatie specialisten de architectuur kunnen toepassen. In de beveiligingsarchitectuur is een algemeen (strategisch) deel voorzien en aparte beveiligingsarchitecturen voor de aspectgebieden. De drie verschillende niveaus in de TOGAF ADM (strategisch-, segment- en capability architectuur) en passen goed bij de niveaus in de beveiligingsarchitectuur (strategisch en beveiligingsaspectgebieden en technische realisatie). Dit vult ontwerpeisen O6, O10 en O13 in;
2) De TOGAF ADM wordt reeds toegepast binnen de Enterprise Architectuur. Dit betekent dat bestaande processen moeten worden aangepast en uitgebreid, daarmee wordt voorkomen dat een hele set nieuwe processen ontworpen en gerealiseerd moet worden. Op deze wijze wordt invulling gegeven aan ontwerpeis O2;
3) De TOGAF ADM kan zich aanpassen aan specifieke situaties (zoals een beveiligingsarchitectuur) op basis van aangepaste stappen van de TOGAF ADM zie (The Open Group Architecture Framework (TOGAF), 2009) hoofdstuk 20.4.

> Het gekozen Procesmodel is de TOGAF ADM.

4.3.2 Veiligheidsaspecten

Alle raamwerken die de ISO 2700X standaard als uitgangspunt nemen, benoemen aspectgebieden van beveiliging langs proceslijnen. The Open Group (TOGAF) hanteert veiligheidsaspecten in termen van kwaliteitskenmerken aan een informatie systeem (The Open Group Security Forum, 2007). Sabsa benoemt beveiligingsdiensten. Het niveau logical security architecture past het best bij het abstractieniveau waarop deze beveiligingsarchitectuur wordt ontwikkeld. Deze security services zijn zeer compleet uitgewerkt.

Mogelijke aspectgebieden zijn benoemd in bijlage B. Dit is een bonte verzameling woorden die zich niet eenvoudig laat categoriseren. Vanuit het perspectief van het raamwerk waaruit ze afkomstig zijn, zijn ze logische gekozen. Wat ze allemaal gemeen hebben, met uitzondering van Sabsa, is dat een zorgvuldige definitie van de scope van het aspectgebied ontbreekt. Aspectgebieden zijn daarom niet zomaar bruikbaar om op te nemen in de beveiligingsarchitectuur. Nu wordt eerst de selectiemethode voor aspectgebieden uitgelegd.

Eerst wordt gekeken naar de relatie tussen het Primavera raamwerk en aspectgebieden. Daarna wordt beschreven welke ontwerpeisen en randvoorwaarden van toepassing zijn op de keuze van aspectgebieden. Met deze informatie kan worden vastgesteld of een aspectgebied in aanmerking komt om opgenomen te worden in de beveiligingsarchitectuur.

In de beveiligingsarchitectuur fungeren de aspectgebieden als input om een beveiligingsarchitectuur te produceren. Daarmee worden aspectgebieden in het strategisch deel van de beveiligingsarchitectuur geplaatst. Op dit niveau kunnen aspectgebieden gezien worden als een “derde dimensie” in het tweedimensionale Primavera raamwerk (zie

Figuur 6). Een aspectgebied moet dan wel passen op de dimensies van het Primavera raamwerk. Een aspectgebied dat slechts in één blok van de drie bij drie matrix uit het Primavera raamwerk wordt uitgewerkt, is een slecht gekozen aspectgebied. Dit beveiligingsonderwerp zal op andere wijze moeten worden uitgewerkt en opgenomen in de beveiligingsarchitectuur.

Drie randvoorwaarden en ontwerpeisen zijn van toepassing op aspectgebieden:

- Ontwerpcriterium O13 stelt dat de architectuur te onderhouden moet zijn door een klein team. Dit betekent dat er slechts beperkte capaciteit ter beschikking staat om beveiligingsarchitectuur voor aspectgebieden te produceren. De selectie van aspectgebieden zou moeten plaatsvinden op basis van de vraag naar beveiligingsarchitectuur producten. Dit zijn bijvoorbeeld regelmatig terugkerende beveiligingsvragen, of situaties die vragen om kaderstellende afspraken.
- Volgens ontwerpcriterium O1 moet de scope van de architectuur compleet zijn. Voor de keuze van aspectgebieden betekent dit dat alle aspecten samen een zo compleet mogelijk beeld zullen moeten vormen van de informatiebeveiliging. In combinatie met ontwerpcriterium O13 betekent dit dat de set aspectgebieden nooit dekkend kan zijn voor alle onderdelen van beveiliging, het is echter wel van belang dat een aspectgebied zelf zo volledig mogelijk wordt uitgewerkt.
- Het abstractieniveau van het aspect: een te laag abstractieniveau leidt tot versnippering binnen de beveiligingsarchitectuur. Voor de onderlinge samenhang is dit een bedreiging (Principe P6), net als voor het abstractieniveau van de te leveren architectuurproducten (ontwerpeis O6);

Samengevat zijn dit de criteria op basis waarvan selectie van een aspectgebied kan plaatsvinden:

1) Het aspectgebied raakt een goot deel van de organisatie en is van toepassing op meerdere niveaus (strategisch – tactisch – operationeel);
2) Er ligt een concrete beveiligingsvraag die de ontwikkeling van een beveiligingsarchitectuur voor een aspectgebied verantwoordt;
3) De beveiligingsarchitectuur voor het aspectgebied moet zelf compleet zijn, compleetheid van scope is niet van toepassing op de set aspectgebieden.
4) Het abstractieniveau van het aspectgebied levert generieke beveiligingsoplossingen op en zijn met de beveiligingsarchitectuur voor het aspect in de hand te realiseren.

In Bijlage B is een lijst met mogelijke beveiligingsaspecten opgenomen. De vraag “hoe worden aspectgebieden vastgesteld” kan het best worden beantwoord door de bovengenoemde criteria 1 t/m 4 toe te passen op de lijst net aspectgebieden. In bijlage B zijn de aspectgebieden daarom voorzien van een inschatting op basis van deze criteria. Op deze wijze wordt duidelijk welke aspectgebieden passen in het ontwerp van de beveiligingsarchitectuur en welke niet.

De volgende aspectgebieden zijn relevant bevonden:

> De aspectgebieden zijn: Toegang en autorisatie, Business Continuity Management, PKI, Controle en Logging, Informatiestromen.

4.3.3 Visie

Een architectuur visie bevat de scope van de architectuur, doelstellingen, beschrijft de omgeving en procesmodellen, actoren, hun rollen en verantwoordelijkheden, principes, ontwerpeisen en een architectuurmodel dat het resultaat is van het in verband brengen van ontwerpeisen en architectuurcomponenten.

Op zich zijn veel van deze elementen op organisatieniveau terug te vinden in de Enterprise Architectuur. De visie voor de beveiligingsarchitectuur moet vastleggen welke deel van deze

informatie voor beveiliging relevant is. Een ander deel van de visie is afkomstig uit het informatiebeveiligingsbeleid van de organisatie. Daar zijn typische elementen van informatiebeveiliging als de organisatie van beveiliging, het beveiligingsproces en de rollen en verantwoordelijkheden vastgelegd. Het laatste deel van de visie is afkomstig uit de context beschrijving van hoofdstuk 2: voor de dillema's en beveiligingsprincipes die een rol spelen op het niveau van de organisatie zijn richtinggevende uitspraken nodig.

> De visie wordt samengesteld uit beveiligingsrelevante elementen uit de Enterprise Architectuur, het informatiebeveiligingsbeleid en contextbeschrijvingen van de (deel)architecturen in de beveiligingsarchitecturen.

De elementen zijn benoemd, aanwezig, maar een integrale beschrijving ontbreekt. Opname in de beveiligingsarchitectuur van deze visie is geen onderdeel van de opdracht omdat de visie invullen een project op zich is.

4.3.4 Principes

Binnen de beveiligingsarchitectuur bestaan principes op twee niveaus:

1) Strategische principes – deze zijn gerelateerd aan bedrijfsdoelstellingen en afgeleid uit de strategische context van de organisatie en de beveiligingsrelevante principes uit de Enterprise Architectuur;
2) Specifieke beveiligingsprincipes - Dit zijn geoperationaliseerde principes voor de specifieke context van een beveiligingsaspect. Deze principes zijn mogelijk afkomstig uit documentatie over het beveiligingsaspect of uit architectuurkaders. Een voorbeeld hiervan is de NORA waarin principes geformuleerd zijn die van toepassing zijn op informatiekoppelingen.

Voor de beveiligingsarchitectuur zijn in H2 een aantal principes gevonden die moeten worden opgenomen in de beveiligingsarchitectuur. Tabel 5 bevat het overzicht van deze principes. De letter S geeft aan dat het gaat om een Strategisch principe, D heeft betrekking op een principes die specifiek zijn voor een aspectgebied.

Code		tekst
P1	S	De strategie van beveiliging van de informatievoorziening moet zodanig worden aangepast dat veilige uitwisseling van informatie met ketenpartners mogelijk wordt.
P2	S	Informatiekoppelingen en de kwetsbaarheden die daarmee geïntroduceerd worden, leiden tot een acceptabel restrisico voor de organisatie.
P3	S	De beveiliging van de informatievoorziening voorziet in het maken van eigenstandige risico afwegingen in situaties waar bestaande wet- en regelgeving tekort schiet.
P4	S	De beveiliging van noodzakelijke "Leading edge" technische voorzieningen ziet er anders uit dan voorzieningen die breed worden ingezet.
P5	S	De beveiliging van de informatievoorziening moet ingericht zijn op de verwerking van gegevens die malware bevatten.
P6	S	De beveiliging van de informatievoorziening is gericht op "Insider Threats" dreigingen.
P7	S	De totstandkoming van een informatiepositie moet verantwoord kunnen worden, ongeacht de wijze van koppelen.
P8	S	Flexibiliteit in het omgaan met noodzakelijke aanpassingen in de relatie tussen Need-to-Know, Need-to-Share en Need-to-Protect.

P9	S	In lijn met de reeds bestaande beveiligingskaders, WIV, VIR, VIR-BI, WOB, Archiefwet en sectorale wetgeving (GBA, WJSG).
P10	D	Voor delen van informatiekoppelingen die buiten de eigen invloedssfeer liggen worden bestaande kaders per definitie wel toegepast.
P11	D	Voor delen van informatiekoppelingen die binnen de eigen invloedssfeer liggen worden bestaande kaders en regelgeving gerespecteerd, maar niet per definitie als leidend toegepast.
P12	S	De architectuur beschouwt informatiebeveiliging integraal: beschikbaarheid, integriteit en exclusiviteit (Vertrouwelijkheid).

Tabel 5: Principes beveiligingsarchitectuur

De principes voor de beveiligingsarchitectuur voor informatiestromen zijn verder uitgewerkt in paragraaf 5.3.

> Principes zullen worden uitgewerkt volgens de "TOGAF" methode, die in de Enterprise Architectuur ook wordt toegepast.

4.3.5 Viewpoints

"Viewpoints" zijn zienswijzen op een view (situatie) voor specifieke actoren. TOGAF kent deze architectuurelementen. Welke viewpoints worden gemaakt en voor wie, wordt bepaald door de uitkomst van stakeholder analyses en door het uit te werken aspectgebied. Er zijn geen ontwerpeisen die iets zeggen over viewpoints. Op dit punt is dus sprake van volledige ontwerpvrijheid.

> Viewpoints zullen worden uitgewerkt volgens de "TOGAF" methode, die in de Enterprise Architectuur ook wordt toegepast.

4.3.6 Security management processen

SABSA, ISO2700X en O-ISMS3 zijn onderdelen die Security management procesdefinities bevatten. Security Management is binnen deze raamwerken een uitvoerend proces op tactisch niveau. De theoretische analyse (zie paragraaf 3.4) laat zien dat security management processen altijd worden toegepast, de verschillen zitten vooral in de diepgang waarmee processen zijn uitgewerkt, de wijze van uitvoering en welke delen van de beveiliging gezien worden als onderdeel van het procesraamwerk. TOGAF kent geen security management processen, deze zullen dus op een andere wijze moeten worden ingevuld.

Een aantal randvoorwaarden en ontwerpeisen zijn van toepassing bij de selectie van de security management processen:

- Meetbaarheid van de realisatie van beveiligingsdoelstellingen en van de stand van de beveiliging van de informatievoorziening (O9, O11); De enige manier om meetbaarheid te realiseren is door dit op te nemen als criterium voor de tactische security management processen. Meetbaarheid komt ook terug in selectiecriterium 8 (volwassenheidsniveaus en toekomstdenken) en criterium 13 (succescriteria);
- Informatiebeveiliging integraal beschouwen (P12); Criterium 1, compleetheid van scope is ook van toepassing; Er moet dus gezocht worden naar een zo compleet mogelijk procesraamwerk.

Bij het opstellen van de criteria op basis waarvan de vergelijkingen plaatsvinden, is gebruik gemaakt van sub-criteria die afkomstig zijn uit de specifieke beveiligingsraamwerken (zie

bijlage A). De volgende sub-criteria zijn relevant: 16, 22 en 37. Deze sub-criteria vallen onder de volgende criteria in de multicriteriatabel:
- Criterium 2: Worden bedrijfsdoelstellingen en beveiliging gekoppeld?
- Criterium 5: Hoe goed wordt de distributie van verantwoordelijkheden over de organisatie ondersteund?
- Criterium 6: Toekomstvastheid van de methode.

Analyse van de multicriteriatabel (zie Tabel 3) voor de criteria 1, 2, 5, 6, 8 en 13 laat zien dat O-ISM3 het optimale procesmodel biedt.

> O-ISM3 is het procesmodel voor het security management.

4.3.7 Risicoanalyse methode

Ontwerpeisen O7 en O8 beschrijven de noodzaak van een risicoanalyse methode. TOGAF maakt slecht zeer beperkt gebruik van risico management. In de informatiebeveiliging wordt bijna elke beslissing bepaald door een risicoafweging.

Sabsa ziet risico management als de enige juiste oplossing om ervoor te zorgen dat beveiligings- en organisatie eisen en wensen goed op elkaar worden afgestemd. ISO27005 bevat een risico analyse methode op basis van categorieën Beschikbaarheid, Integriteit en Exclusiviteit en beveiligingsniveaus die toe te passen maatregelen in deze drie categorieën plaatsen. Ook bevat de ISO27005 een uitgebreid beeld van dreigingen die relevant zijn voor informatiebeveiliging. Het VIR (een vroege voorloper van de ISO2700X) kent de A&K analyse (Ministerie van Economische Zaken, 1996) waarin voor een informatiesysteem op basis van dreigingen en maatregelen wordt bepaald wat de restrisico's zijn. Het VIR-BI bevat een risicoanalyse op hoog niveau van waaruit operationele (zeer gedetailleerde) maatregelen zijn geformuleerd.

Een relevant verschil voor de risicoanalyse tussen de SABSA de ISO2700X is dat SABSA de risico analyse ziet als stuurmiddel voor de kostenbeheersing van beveiliging (de organisatie krijgt de beveiliging naar de investering die ze daarvoor wenst te doen) terwijl de ISO standaard de risico analyse gebruikt om normatief aan te geven wat voor soort maatregelen getroffen moeten worden.

In een hooggerubriceerde omgeving is een risicoanalyse op een gedetailleerd niveau noodzakelijk. De reden hiervoor is dat "grofstoffelijke dreigingen" (uit bijvoorbeeld beveiligingsbeleid, VIR-BI of ISO27005) te algemeen zijn om rechtstreeks te kunnen worden toegepast binnen een beveiligingsarchitectuur voor een aspectgebied. De gevolgen van te algemeen geformuleerde maatregelen zijn:
- Er blijft te veel ontwerpvrijheid over waardoor sturing op hergebruik van beveiligingsoplossingen moeilijk wordt;
- Er blijven restrisico's bestaan die in een hooggerubriceerde omgeving niet acceptabel zijn.

De wijze van werken op basis van de ISO2700X en het VIR is binnen gewone (niet hooggerubriceerde) omgevingen binnen veel organisaties dagelijkse praktijk. Deze werkwijze leidt echter niet tot het gewenste beveiligingsniveau voor hooggerubriceerde beveiligingstoepassingen.

Door de risicoanalyse onderdeel te maken van de beveiligingsarchitectuur voor een aspectgebied, ontstaat een situatie waarmee specialisten die beveiligingstoepassingen realiseren in staat worden gesteld te controleren of de getroffen beveiligingsmaatregelen leiden tot acceptabel rest-risico voor de organisatie.

De elementen die de beveiligingsarchitectuur moet bevatten zijn:

1) De risicoanalyse methode
2) Een set algemene dreigen op de organisatie

De risico analyse methode en de lijst met algemene dreigingen op de organisatie is meestal in het beveiligingsbeleid van de betreffende organisatie of onderdeel daarvan vastgelegd. Beide elementen zijn inhoudelijk geen onderdeel van de opdracht, ze worden dan ook benoemd maar niet verder uitgewerkt.

De elementen die de beveiligingsarchitectuur voor het aspectgebied moet bevatten zijn:

1 De dreigingsanalyse uit het Informatiebeveiligingsbeleid. Deze is geformuleerd op een hoog abstractieniveau en geeft aan welke dreigingen voor de organisatie relevant zijn;
2 Een op het aspectgebied gerichte dreigingsanalyse. Deze is noodzakelijk om dat dreigingen geoperationaliseerd moeten worden naar het aspect dat de architectuur beschrijft. Alleen dan worden de juiste beveiligingsmaatregelen getroffen;
3 Een procesbeschrijving die laat zien op welke wijze de risicoanalyse moet worden toegepast.

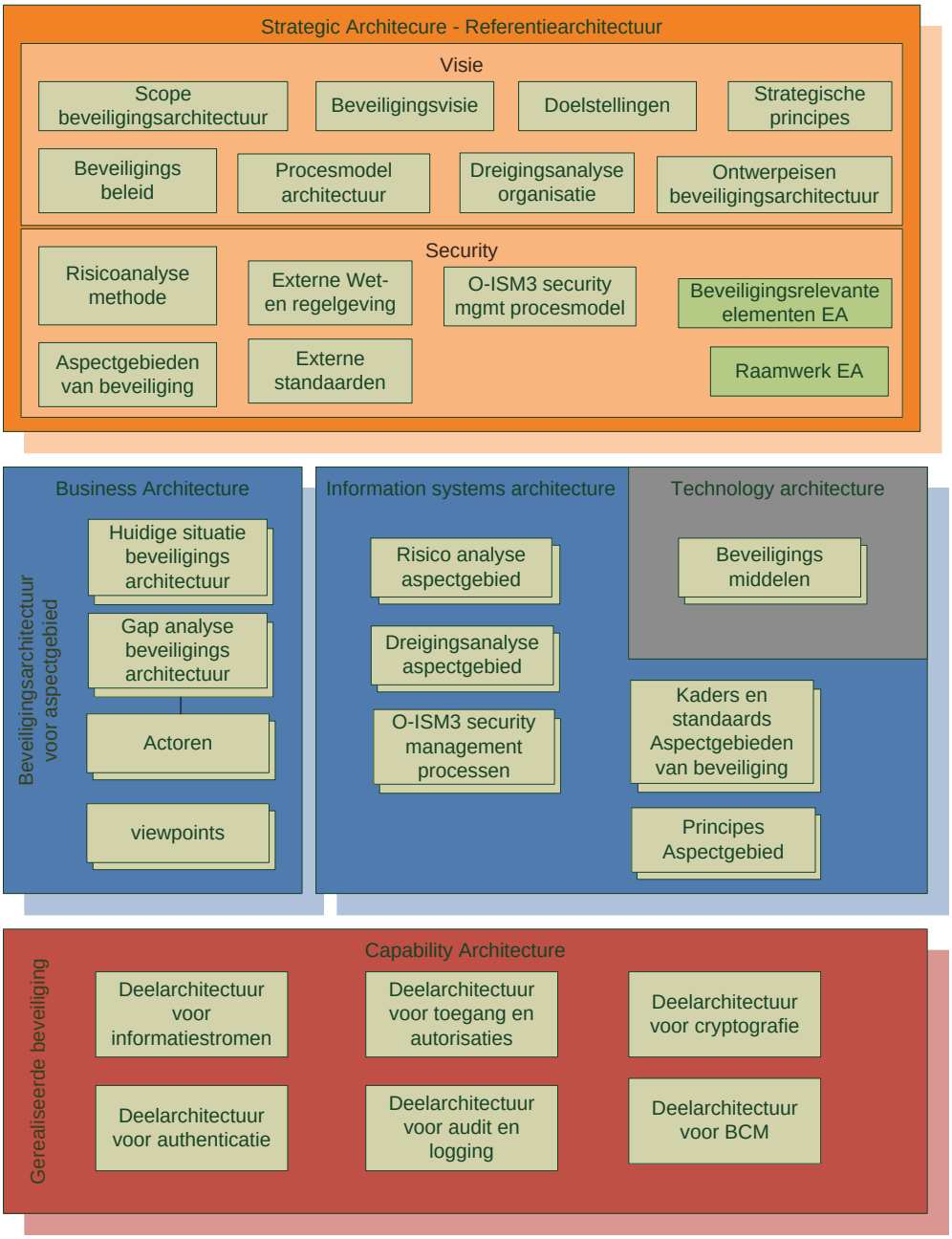
4.3.8 Content metamodel

Een content metamodel is een middel dat wordt gebruikt om de bouwstenen van de architectuur te definiëren en vast te leggen. Dit model is een belangrijk middel, waarin de relatie tussen de beveiligingsarchitectuur en de Enterprise Architectuur vormgegeven kan worden. Er zijn geen ontwerpeisen die iets zeggen over het content metamodel. Dit betekent volledige ontwerpvrijheid. TOGAF bevat een beschrijving voor het content metamodel die gebaseerd is op gebruik van de TOGAF ADM. Het ligt daarom voor de hand om het Content Meta Model in te vullen volgens de geldende TOGAF standaard.

Het gekozen Content Meta Model is het TOGAF model.

Ontwerpeis O5 schrijft voor dat in de beveiligingsarchitectuur de externe kaders en standaarden die worden gebruikt bij de uitwerking van aspectgebieden moeten worden opgenomen. Dit element is daarom toegevoegd aan het model.

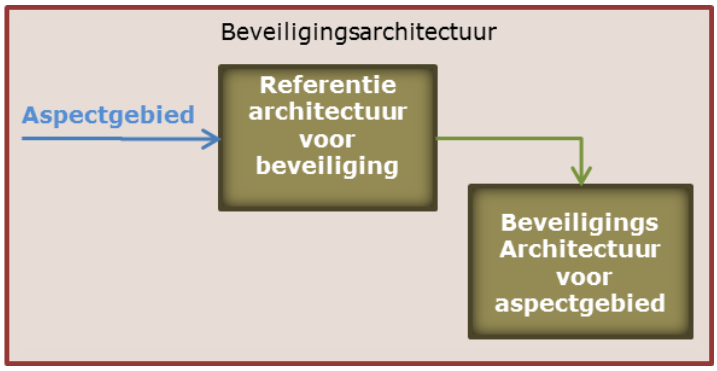
In Figuur 12 is het content meta model gevisualiseerd.



Figuur 12: Content meta model beveiligingsarchitectuur

4.4 Architectuur of referentiearchitectuur?

Het ontworpen product (beveiligingsarchitectuur) bestaat nu uit twee delen die een duidelijke hiërarchische relatie hebben (zie Figuur 13). Als de beveiligingsarchitectuur wordt beschouwd in het licht van de definitie van een referentiearchitectuur (zie paragraaf 3.2) wordt duidelijk dat de beveiligingsarchitectuur het geheel is van één referentiearchitectuur en verschillende beveiligingsarchitecturen voor aspectgebieden. Het is valide om te constateren dat vanaf dit punt in het ontwerp de "beveiligingsarchitectuur" de "referentiearchitectuur voor beveiliging is geworden:



Figuur 13: Ontwerp beveiligingsarchitectuur

4.5 Samenvatting en reflectie

Het product dat is ontworpen is de referentiearchitectuur voor beveiliging, bestaande uit een raamwerk, een procesmodel en architectuurelementen. De enige beschikbare beveiligingsarchitectuur (SABSA) blijkt, op basis van afwijkende dimensies in het hoofdraamwerk ten opzichte van de Enterprise Architectuur, niet geschikt te zijn om toe te passen. Daarom is een eigen beveiligingsarchitectuur samengesteld door te kijken welke noodzakelijke elementen de beveiligingsarchitectuur zou moeten bevatten. Daarna heeft selectie van deze elementen plaatsgevonden. De selectie van deze componenten leverde een aantal belangrijke vragen op waarop het antwoord in eerste instantie moeilijk was te vinden:

> Hoe selecteer je een raamwerk voor een beveiligingsarchitectuur?

Organisatorische randvoorwaarden zoals beschikbare mankracht, middelen en de scope bepalen het antwoord op de vraag wat is haalbaar? Hergebruik van bestaande Enterprise Architectuur componenten zijn vervolgens bepalend voor de keuze: kies voor een raamwerk basisarchitectuur die al wordt gebruikt in de organisatie.

> Hoe selecteer je een architectuur procesmodel?

TOGAF kent als één van de weinige architecturen een generiek procesmodel dat zich laat aanpassen aan specifieke –niet Enterprise Architectuur- vraagstukken (zoals veiligheidsaspecten) en het model kent verschillende abstractieniveaus. Afhankelijk van beoogd doel en scope van de (aspect)architectuur is dit model in aangepaste vorm zeer geschikt om toe te passen.

> Op welke wijze worden beveiligingsaspecten geselecteerd?

Beveiligingsaspecten kunnen gezien worden als derde dimensie aan het architectuur raamwerk. Een aspect gebied uitwerken tot een beveiligingsarchitectuur heeft alleen zin als de beveiligingsarchitectuur van toepassing is op meerdere onderdelen van het (tweedimensionale) architectuur raamwerk. Als dit uitgangspunt gehanteerd wordt als selectiecriterium, wordt duidelijk welke aspectgebieden relevant zijn.

De drie antwoorden op vragen zijn een bijproduct van dit ontwerpproces, omdat uit de literatuurstudie is gebleken dat het antwoord op deze vragen niet is terug te vinden.

4.6 Volledigheidscontrole randvoorwaarden en ontwerpeisen

In paragraaf 4.2 en 4.3 zijn de relevante onderdelen van de beveiligingsarchitectuur uitgewerkt, op basis van de ontwerpeisen, randvoorwaarden en selectiecriteria die in hoofdstuk 2 en 3 tot stand zijn gekomen. Of alle ontwerpeisen en randvoorwaarden zijn toegepast in het ontwerp is in Tabel 6 zichtbaar gemaakt in de kolom "verwerkt". Hier is aangegeven in welke paragraaf van hoofdstuk 4 de randvoorwaarde of ontwerpeis is gebruikt voor de onderbouwing van de gemaakte keuze.

Code	Type	tekst	Verwerkt:
P1	principe	De strategie van beveiliging van de informatievoorziening moet zodanig worden aangepast dat veilige uitwisseling van informatie met ketenpartners mogelijk wordt.	4.3.5
P2	principe	De beveiliging van de informatievoorziening voorziet in het maken van eigenstandige risico afwegingen in situaties waar bestaande wet- en regelgeving tekort schiet.	4.3.5
P3	principe	De beveiligingsarchitectuur komt tegemoet aan de groeiende vraag naar informatiekoppelingen en borgt dat de kwetsbaarheden die daarmee geïntroduceerd worden, leiden tot een acceptabel restrisico voor de organisatie.	4.3.5
P4	principe	De beveiliging van noodzakelijke "Leading edge" technische voorzieningen ziet er anders uit dan voorzieningen die breed worden ingezet en hoge beschikbaarheidseisen kennen.	4.3.5
P5	principe	De beveiliging van de informatievoorziening moet ingericht zijn op de verwerking van gegevens die malware bevatten.	4.3.5
P6	principe	De beveiligingsarchitectuur bevat een set coherente maatregelen om "Insider Threats" dreigingen te mitigeren.	4.3.5
P7	principe	De totstandkoming van een informatiepositie moet verantwoord kunnen worden, ongeacht de wijze van koppelen.	4.3.5
P8	principe	Flexibiliteit is noodzakelijk in het omgaan met noodzakelijke aanpassingen in de relatie tussen Need-to-Know, Need-to-Share en Need-to-Protect.	4.3.5
P9	principe	De beveiligingsarchitectuur is in lijn met de reeds bestaande beveiligingskaders, WIV, VIR, VIR-BI, WOB, Archiefwet en sectorale wetgeving (GBA, WJSG).	4.3.5
O1	ontwerpeis	De relatie met de EA is aantoonbaar: de beveiligingsarchitectuur moet de relaties benoemen en vastleggen.	4.1, 4.3.2
O2	ontwerpeis	Er wordt zoveel mogelijk gebruik gemaakt van reeds bestaande architectuurprocessen voor systeemontwikkeling en project management.	4.1, 4.3.1
O3	ontwerpeis	Bestaande architectuurproducten voor beveiliging worden ondersteund.	4.1
O4	ontwerpeis	De bestaande producten en de samenhang worden beschreven.	4.1
O5	ontwerpeis	Externe kaders en standaarden die gebruikt worden bij de ontwikkeling van aspect beveiligingsarchitecturen worden vastgelegd in de beveiligingsarchitectuur.	4.3.3
O6	ontwerpeis	Te leveren architectuurproducten zijn van een zodanig abstractie niveau dat de primaire afnemers van deze architectuur implementaties tot stand kunnen brengen.	4.3.1, 4.3.2
O7	ontwerpeis	De beveiligingsarchitectuur vervangt de afhankelijkheid van vastgelegde beveiligingsmaatregelen uit het Vir-BI door risicogebaseerde afwegingen te maken.	4.3.8
P10	principe	Voor delen van informatiekoppelingen die buiten de eigen invloedssfeer liggen worden bestaande kaders per definitie wel toegepast.	4.3.5

P11	principe	Voor delen van informatiekoppelingen die binnen de eigen invloedssfeer liggen worden bestaande kaders en regelgeving gerespecteerd, maar niet per definitie als leidend toegepast.	4.3.5
O8	ontwerpeis	Risico gebaseerd denken introduceren.	4.3.8
O9	ontwerpeis	Beveiliging relateren aan bedrijfsdoelstellingen om kosten inzichtelijk te maken.	4.1, 4.3.7
P12	principe	De architectuur beschouwt informatiebeveiliging integraal: beschikbaarheid, integriteit en exclusiviteit (Vertrouwelijkheid).	4.3.5, 4.3.7
O10	ontwerpeis	De beveiligingsarchitecturen zijn zodanig generiek van aard dat er keuzes overblijven bij implementatie ten aanzien van toepassingen zodat op dat moment weloverwogen keuzes gemaakt worden ten aanzien van beheer.	4.1, 4.3.1
O11	ontwerpeis	De stand van beveiliging van de informatievoorziening meetbaar maken.	4.1, 4.3.7
O12	ontwerpeis	Kies voor architectuurcomponenten en kaders waaraan toekomstvisie ten grondslag ligt.	4.1
O13	ontwerpeis	Het architectuurmodel moet door een klein team eenvoudig onderhouden kunnen worden.	4.1, 4.3.1, 4.3.2

Tabel 6: Overzicht volledigheidscontrole randvoorwaarden en ontwerpeisen

Het ontwerp is opgebouwd en alle randvoorwaarden en ontwerpeisen zijn toegepast.

5 Beveiligingsarchitectuur voor Informatiestromen

Dit hoofdstuk geeft antwoord op beschrijft hoe de beveiligingsarchitectuur voor informatiestromen tot stand komt.

4) Hoe ontstaat de beveiligingsarchitectuur voor informatiestromen?

In dit hoofdstuk wordt beschreven hoe de bouwelementen uit paragraaf 4.3 verder zijn uitgewerkt in een beveiligingsarchitectuur voor informatiestromen. Paragraaf 5.1 bevat een korte toelichting op de beveiligingsarchitectuur van informatiestromen. Deze toelichting is noodzakelijk voor een juist begrip van de rest van dit hoofdstuk. De uitgewerkte beveiligingsarchitectuur is voor het beantwoorden van deelvraag 4 van ondergeschikt belang en is opgenomen in bijlage D.

Een aantal bouwelementen uit paragraaf 4.3 zijn reeds beschreven en ingevuld in hoofdstuk 4 omdat ze onderdeel uitmaken van de referentiearchitectuur voor beveiliging. Volgens het ontwerpproces worden deze elementen meegenomen in de beveiligingsarchitectuur voor informatiestromen. Na een korte inleiding in paragraaf 5.1 wordt in paragraaf 5.2 tot en met 5.6 beschreven hoe de bouwelementen voor de beveiligingsarchitectuur voor informatiestromen zijn ingevuld. Tenslotte volgt een samenvatting van de bevindingen uit dit hoofdstuk in paragraaf 5.7. Paragraaf 5.8 beschrijft de validatie van het ontwerp van de beveiligingsarchitectuur als geheel.

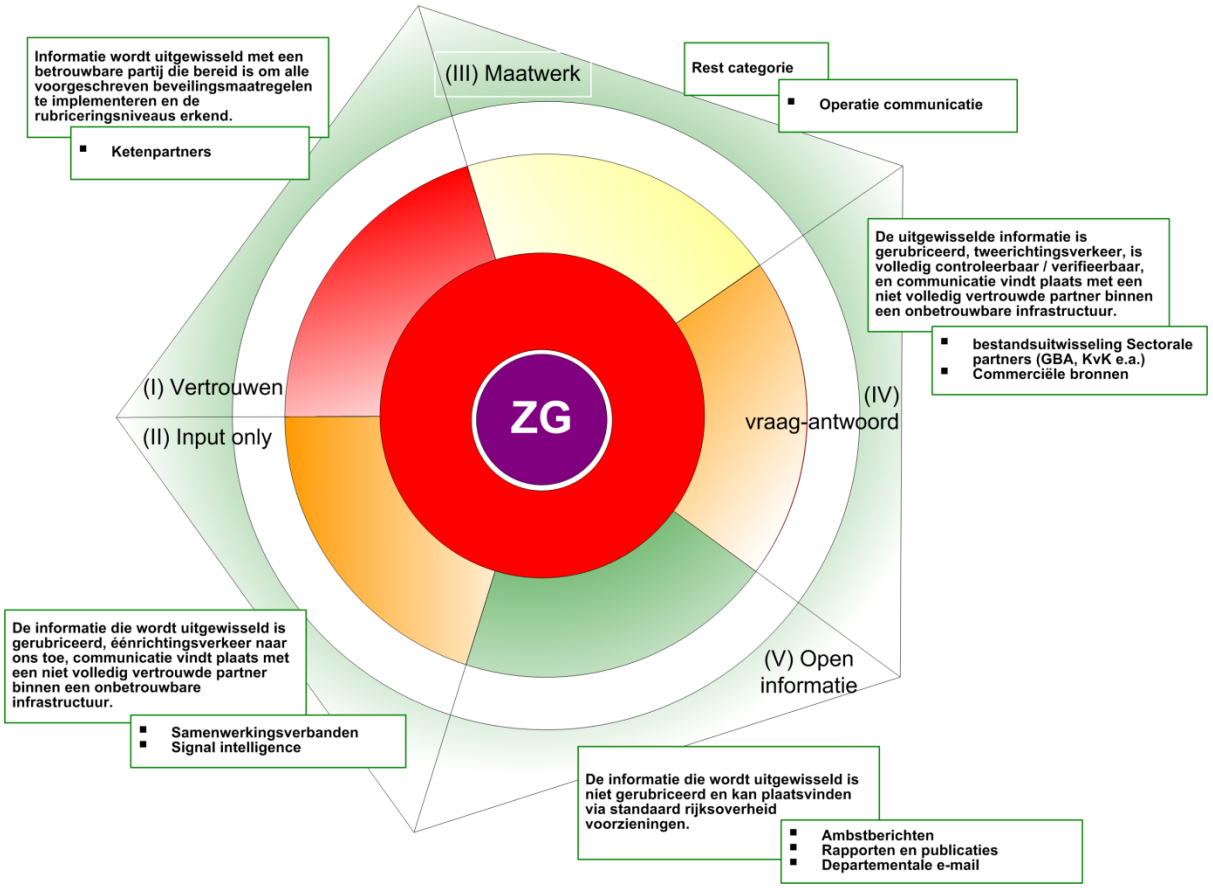
5.1 Inleiding beveiligingsarchitectuur voor informatiestromen

Doel van de beveiligingsarchitectuur voor informatiestromen is om standaard, meetbare oplossingen te bieden voor het delen van informatie met derde partijen en dit te standaardiseren in direct toepasbare operationele oplossingen.

Meetbaarheid wordt in de ontwerpeisen als een belangrijk gegeven gezien. Om die reden is de doelstelling geoperationaliseerd in een aantal meetbare subdoelstellingen zodat de effectiviteit van de beveiligingsarchitectuur meetbaar wordt (zie Tabel 7).

	Subdoelstelling	KPI
DO1	Verlagen van de drempel om informatiekoppelingen tot stand te brengen;	Vergelijk de doorlooptijd van de realisatie van een aansluiting.
DO2	Reductie van niet noodzakelijke menselijke interventie in informatiestromen;	Tel het aantal werkprocessen die gebruik maken van gegevensdragers.
DO3	Verbetering van verantwoording van de herkomst van informatie;	Geef aan bij welk deel van de informatiestromen er sprake is van een volledige en juiste borging van verantwoording van de informatiestroom.
DO4	Eenduidigheid in technische oplossingen;	Leg vast welke informatiestromen aan de beveiligingsarchitectuur voor informatiestromen voldoen.
DO5	Aantoonbare kostenbesparingen in aanleg en exploitatie van koppelingen;	Kwantificeer de kosten van het beheer en implementatie per informatiestroom en vergelijk dit met implementaties volgens de nieuwe architectuur.
DO6	Reductie van het niet noodzakelijk gebruik van informatiedragers in informatiestromen;	Controleer de hoeveelheid uitstaande autorisaties die betrekking hebben op werkprocessen. Tel het aantal gegevensdragers dat wordt uitgegeven.
DO7	Maak gebruik een beperkt aantal aansluitcategorieën;	Beperkt aantal aansluitcategorieën (<8);
DO8	Maatwerk blijft altijd een optie vanwege de aard van het werk. Dit maakt dat een deel van de informatiestromen niet kan worden ondergebracht in een aansluitcategorie;	80% van de informatiestromen moet ondergebracht kunnen worden in een aansluitcategorie, 20% mag maatwerk zijn;

Tabel 7: Subdoelstellingen architectuur voor informatiestromen



Figuur 14: Aansluitcategorieën beveiligingsarchitectuur voor informatiestromen

De beveiligingsarchitectuur voor informatiestromen is uitgewerkt door informatiestromen te clusteren in aansluitcategorieën. De gedachte hierbij is dat informatiestromen met een soortgelijk risicoprofiel zoveel mogelijk worden aangesloten in generieke aansluitcategorieën. Dit is afgebeeld in Figuur 14. De ringen stellen voor: wit = koppelingslaag met de buitenwereld, eerste gekleurde ring is de verwerkingslaag van de informatiestroom, de rode ring is de hooggerubriceerde informatievoorziening, de binnenring is informatievoorziening voor Zeer Geheim gerubriceerde informatie en kent geen koppelingen. De verschillende categorieën zijn "Input Only", "Vertrouwen", "Maatwerk", "vraag-antwoord" en "Open informatie". De categorieën zijn ontstaan door factoren aan de informatiestromen te identificeren die relevant zijn voor de inrichting van beveiliging, bijvoorbeeld de rubricering van de getransporteerde informatie en de fysieke beveiliging van de locatie waarmee gekoppeld wordt. Een volledig overzicht van deze factoren is opgenomen in Tabel 10 in paragraaf 5.6.

De aansluitcategorieën zijn verder uitgewerkt door invulling van de architectuur bouwelementen zoals beschreven in de rest van dit hoofdstuk.

5.2 Procesmodel Architectuur

De TOGAF ADM methode is opgenomen in de referentiearchitectuur voor beveiliging. Deze methode wordt gebruikt om de beveiligingsarchitectuur voor informatiestromen te produceren. In het ontwerp is beargumenteerd dat deze beveiligingsarchitectuur in TOGAF ADM termen een "segment architectuur" is. Volgens de TOGAF ADM wordt een segment architectuur geproduceerd door drie stadia te doorlopen: Business Architecture, Information Systems Architecture en Technology Architecture. De producten en activiteiten die deze drie

stadia moeten opleveren, worden geciteerd, daarna wordt per stadium aangegeven op welke wijze de producten en activiteiten zijn terug te vinden in de beveiligingsarchitectuur voor informatiestromen.

De Business Architecture fase bevat de volgende producten en activiteiten:
1. Een beschrijving van de huidige situatie van het aspectgebied;
2. Een beschrijving van het aspectgebied, op basis van organisatie doelstellingen en strategische principes;
3. Een analyse van het verschil tussen beide beschrijvingen (gap analyse);
4. Selecteren van relevante viewpoints met als doel de belangen van relevante stakeholders duidelijk te kunnen maken;
5. Selecteren van te gebruiken middelen die gebruikt worden in combinatie met de aangegeven viewpoints.

De punten 1 en 2 zijn uitgewerkt in de context beschrijvingen in hoofdstuk 2 en in paragraaf 5.1. Een gedetailleerde beschrijving van de beveiligingsarchitectuur voor informatiestromen is opgenomen in de inleiding van bijlage C. Punt 3 is uitgewerkt in bijlage C door de verschillen met de huidige situatie te benoemen. Punt 4 en 5 (viewpoints) zijn uitgewerkt in een overzicht van informatiestromen en de beveiligingsrelevante factoren aan de informatiestroom. Alle door de TOGAF-ADM aangegeven punten voor de Business Architecture fase zijn hiermee doorlopen.

De Information Systems Architecture fase bevat de volgende activiteit:
6. Het ontwerpen van de onderliggende gegevens- en applicatie componenten ter ondersteuning van de Business Architectuur.

De applicatiecomponenten bestaan uit de verschillende aansluitsegmenten met bijbehorende uitgangspunten en principes. Deze zijn opgenomen in bijlage C, in de paragraaf die de uitwerking van de aansluitcategorieën bevat.

De Technology Architecture fase levert de volgende producten:
7. De relatie tussen applicatie componenten en technologie componenten (hardware en software);
8. De planning van de technische realisatie;
9. Het maken van huidige en toekomstige views van de technologie componenten.

Punt 7 en 9 zijn voor zover nodig voor deze beveiligingsarchitectuur ingevuld door in de views van de verschillende aansluitcategorieën aan te geven welke beveiligingscomponenten absoluut noodzakelijk zijn. Deze stappen zijn echter niet compleet: per aansluitcategorie zijn additionele beveiligingscomponenten noodzakelijk. Het is een bewuste keuze om de verdere uitwerking hiervan over te laten aan specialisten die de oplossingen realiseren. De reden hiervoor is dat dat op het abstractieniveau waarop de infrastructuurcomponenten in de architectuur zijn beschreven, het detailniveau waaruit de koppelingen bestaan onvoldoende zichtbaar is. Voor het bepalen van de restrisico's die de koppeling introduceert, is dit niveau van detail is wel noodzakelijk.

Punt 8, planning van de realisatie is niet opgenomen in de beveiligingsarchitectuur voor informatiestromen omdat het veel meer voor de hand ligt om de verdere uitwerking van punt 7 en 9 (de infrastructuurcomponenten) en punt 8 (de planning) over te laten aan implementatiespecialisten. Dit punt valt daarom buiten de afbakening van de beveiligingsarchitectuur voor informatiestromen.

5.3 Principes

De principes die zijn opgenomen in de beveiligingsarchitectuur voor informatiestromen zijn strategische principes voor de organisatie die betrekking hebben op informatiestromen en principes afkomstig uit externe kaders die relevant zijn (zoals de NORA en MARIJ). Verder zijn er aanvullende, meer uitgewerkte principes geformuleerd die sturend zijn voor de wijze waarop de verschillende aansluitcategorieën moeten worden ingericht. Tabel 8 bevat een

aantal voorbeelden van dit soort principes, op het gebied van infrastructuur.

Code	Principe	Statement
INFSTR.1	Eén huishouding van informatie	Alle informatie gebruikt bij de primaire processen dient eenvoudig op generieke wijze beschikbaar te zijn.
INFSTR.2	Mate van vertrouwen is bepalend voor maatregelen	Juridische afhankelijkheden, werkafspraken in de partner waarmee informatie wordt uitgewisseld is medebepalend voor de genomen beveiligingsmaatregelen.
INFSTR.3	Geautomatiseerde stromen lopen van buiten naar binnen	Voor een informatiestroom die van buiten naar binnen loopt, gelden minder beperkingen dan voor informatie die van binnen naar buiten loopt.
INFSTR.4	Informatie wordt in het hooggerubriceerde netwerk gearchiveerd	Archieven moeten integraal doorzoekbaar zijn. Dat lukt niet als informatie zich in geïsoleerde netwerksegmenten of informatiedomeinen bevindt.
INFSTR.5	Bij internationale uitwisseling is er ruimte voor maatwerk	Bij internationale uitwisseling kunnen maatregelen die gewenst zijn door de partner prevaleren boven de eigen architectuurprincipes. Voorbeeld: NATO of EU richtlijnen.

Tabel 8: Voorbeeldprincipes architectuur voor informatiestromen

Een overzicht van alle principes voor de beveiligingsarchitectuur voor informatiestromen is opgenomen in bijlage C en bijlage D.

5.4 Viewpoints

Viewpoints zijn gezichtspunten van specifieke belanghebbenden op een aspect van een architectuur. Het doel hiervan is om duidelijk te kunnen maken wat een architectuur of component daarvan betekent voor de belangen van de actor. Het produceren van viewpoints kost veel tijd. Het vereist een netwerkanalyse en een inventarisatie van de belangen en dilemma's die samenhangen met de architectuur.

Er zijn twee verschillende viewpoints uitgewerkt binnen de beveiligingsarchitectuur voor informatiestromen:

1. De categorie indeling waarin voor het management van de organisatie en niet-technische medewerkers duidelijk wordt gemaakt welke categorieën er zijn en welke type informatiestromen zij bevatten (zie Figuur 14, blz. 46);
2. Een algemeen model van een informatiestroom, die duidelijk maakt voor relatiebeheerders, gegevensbeheerders en implementatiespecialisten hoe de factoren op basis waarvan de categorie indeling wordt bepaald, samenhangen met de informatiestroom (zie bijlage C, risicoanalyse).

5.5 Security management processen

De relevante security management processen worden geselecteerd uit het O-ISM3 raamwerk. Dit raamwerk bevat een groot aantal voorgedefinieerde security management processen die, afhankelijk van de situatie, kunnen worden toegepast. Behalve een procesbeschrijving en een definitie van inputs en outputs levert O-ISM3 ook KPI's waarmee processen meetbaar kunnen worden gemaakt. Voor de beveiligingsarchitectuur voor aspectgebieden zijn vooral operationele processen relevant. Tabel 9 bevat een overzicht van processen die raken aan de beveiligingsarchitectuur voor informatiestromen. De processen in het O-ISM3 raamwerk zijn hiërarchisch opgebouwd langs niveaus strategisch (S), tactisch (T) en operationeel (O). Dit is zichtbaar gemaakt door gebruik van de letters T (tactisch) en O (operationeel) in het O-ISM3-ID.

Proces	O-ISM3 ID

Define Security Targets & Security Objectives	TSP-14
Inventory management	OSP-3
IS change control	OSP-4
Managed domain hardening	OSP-7
Segmentation and Filtering management	OSP-16
Malware protection management	OSP-17
Access Control	OSP-11
Phisical Environment Protection	OSP-14
Alerts monitoring	OSP-22
Handling of (near)incidents	OSP-24

Tabel 9: O-ISM3 processen voor de architectuur van informatiestromen

De in Tabel 9 opgenomen processen zijn op één na allemaal operationele security management processen. Deze zijn vooral gericht op de controle en uitvoering van security in de ICT infrastructuur. Er is geen specifiek proces in het O-ISM3 raamwerk dat iets zegt over informatiestromen zelf. Dit betekent dat er niet zonder meer meetinformatie beschikbaar komt over de informatiestromen uit de O-ISM3 processen.

Een informatiestroom raakt aan een aantal infrastructuur componenten, bijvoorbeeld een firewall, een server waar gegevens worden opgeslagen, een intern netwerk dat zorg draagt voor gegevenstransport en een informatiesysteem waarin de informatie wordt verwerkt. Meten aan de informatiestroom kan alleen door metingen aan een aantal specifieke infrastructuur componenten. Rapporteren vanuit het perspectief van een aansluitcategorie vereist daarom de vastlegging welke infrastructuurcomponenten er in specifieke aansluitcategorieën worden toegepast. Door deze set componenten als een filter te gebruiken over de reeds bestaande rapportages in de operationele omgeving, kunnen meetgegevens over de categorieën beschikbaar worden gemaakt.

Behalve de in paragraaf 5.1 aangegeven meetcriteria aan de architectuur zijn er verder geen randvoorwaarden of ontwerpeisen die aangeven welke rapportagebehoefte er precies is, er zijn geen operationele security management processen die direct relateren aan informatiestromen en er is beschreven hoe de meetinformatie beschikbaar gemaakt zou kunnen worden. Daarom worden de KPI's niet verder uitgewerkt.

5.6 Risicoanalyse

De beveiligingsarchitectuur voor informatiestromen bevat een abstracte risico analyse methode die zodanig is uitgewerkt dat bij het technisch ontwerp van een categorie een concrete risico analyse kan worden uitgevoerd. De risico analyse is uitgewerkt vanuit een algemeen model van een informatiestroom (afkomstig uit de NORA) en bevat een overzicht van dreigingen op informatiestromen. Dit overzicht is opgenomen in bijlage E. De risicoanalyse methode, met als input de dreigingen en het technisch ontwerp van een aansluitcategorie zijn de elementen die nodig zijn om de restrisico's voor een aansluitcategorie te bepalen.

Een informatiestroom kent beveiligingsrelevante factoren. Deze zijn geïnventariseerd en opgenomen in Tabel 10. Deze factoren kunnen worden gebruikt om – daar waar nodig - in het technisch ontwerp van een categorie nog onderscheid aan te kunnen brengen tussen groepen informatiestromen. Voor het indelen in aansluit categorieën is binnen de Beveiligingsarchitectuur voor Informatiestromen gebruik gemaakt van de meest relevante factoren (nummer 1 t/m 5). Meer factoren konden niet rechtstreeks gebruikt worden om de aansluitcategorieën vast te stellen omdat dit leidt tot een te grote hoeveelheid aansluitcategorieën. Dit betekent dat in het technisch ontwerp van de uiteindelijke aansluitcategorieën rekening gehouden zal moeten worden met de factoren 6 tot en met 10.

	Eigenschap	Omschrijving
1	Controleerbaarheid	**De mate waarin de organisatie de mogelijkheid heeft de omgeving bij de derde partij te controleren of daar invloed op uit te oefenen;**
2	Vertrouwen Externe partij	**Vertrouwen in de "mens" aan de andere kant van de informatiestroom/Bron/verbinding is bepalend voor het vertrouwen dat wij stellen in de informatie die binnen komt;**
3	Rubricering	**Inschatting van de schade die de Staat der Nederlanden of andere actoren wordt berokkend als de informatie openbaar wordt;**
4	Inhoud informatie is verifieerbaar	**Informatie juiste en tijdig? Bevat het mogelijk virussen of andere ongewenste artefacten? Zijn er afspraken met de leverende partij op dit gebied?**
5	Gerichte zoekvraag aan de buitenwereld	**Is een specifieke zoekvraag ook een vraag in een systeem buiten de deur**
6	Gebruik van draadloos of publiek domein	**Het type netwerk dat wordt gebruikt om de koppeling tot stand te brengen.**
7	Verrijking van gegevens	**Menselijke handelingen en/of geautomatiseerde verwerking van gegevens voordat er sprake is van geduide informatie**
8	Geografische locatie	**De fysieke locatie van het eindpunt van de koppeling**
9	Mate van isolatie van de bron	**Er is een belang bij om de informatie afkomstig van bepaalde partijen strikt gescheiden te houden van elkaar.**
10	Import en/of Export van informatie	**(Menselijke) Interventiedreiging Controleerbaarheid (weten wat de I/O is);**

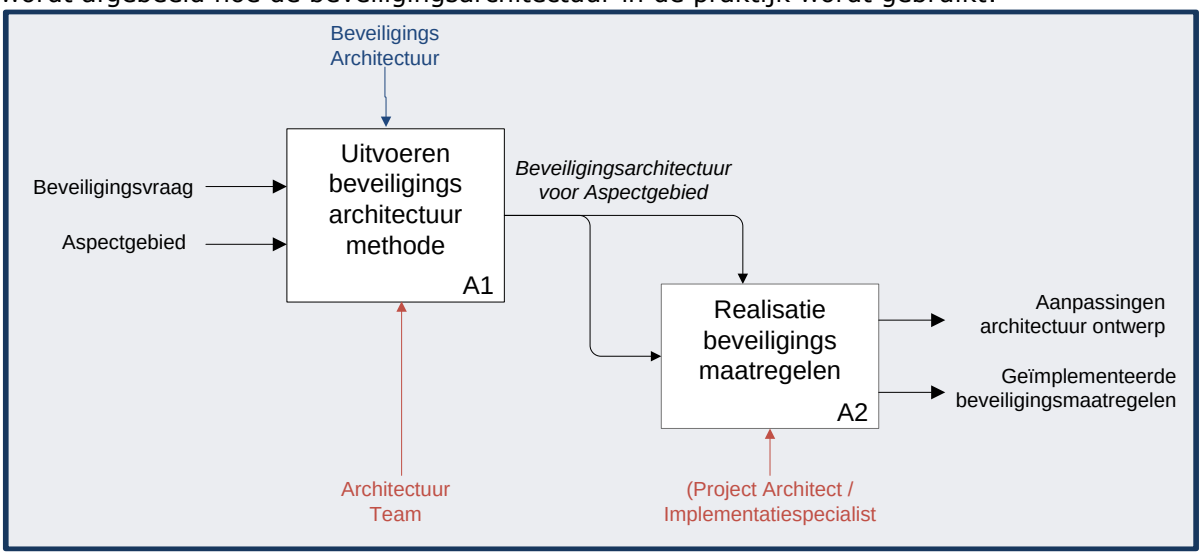
Tabel 10: Lijst relevante beveiligingseigenschappen informatie

De eigenschappen vloeien voort uit maatregelen die in veel gevallen niet rechtstreeks zijn af te leiden uit beschikbare dreigingsscenario's, zoals de ISO 27005 en dreigingsanalyses op beleidsniveau. Deze eigenschappen horen echter wel onderdeel te zijn van de selectie van beveiligingsmaatregelen voor het koppelen van hooggerubriceerde informatiestromen.

5.7 Samenvatting en reflectie

In dit hoofdstuk is aangegeven hoe de verschillende elementen van de Beveiligingsarchitectuur voor Informatiestromen zijn ingevuld. Dit is het laatste deel van de ontwerpfase. De uitgewerkte Beveiligingsarchitectuur voor Informatiestromen is opgenomen in bijlage C.

Het uiteindelijke product van H4 en H5 samen is een beveiligingsarchitectuur. In Figuur 15 wordt afgebeeld hoe de beveiligingsarchitectuur in de praktijk wordt gebruikt:



Figuur 15: Beveiligingsarchitectuur in de uitvoeringspraktijk

Op basis van beveiligingsvragen die voortvloeien uit systeemwijzigingen, wordt stap A1 uitgevoerd. Daaruit volgt een beveiligingsarchitectuur voor het aspectgebied. Deze architectuur is kaderstellend voor de wijze waarop beveiligingsmaatregelen worden geïmplementeerd. Ook levert de beveiligingsarchitectuur voor het aspectgebied input in de vorm van voorgeschreven maatregelen. De output bestaat uit geïmplementeerde beveiligingsmaatregelen en ervaringsinformatie die gebruikt kan worden voor de verdere ontwikkeling van de beveiligingsarchitectuur.

De hoofdvraag van dit onderzoek luidde:

> *Ontwerp een beveiligingsarchitectuur voor een hooggerubriceerde informatievoorziening die het mogelijk maakt dat de organisatie kan voldoen aan de doelstellingen op het gebied van informatie uitwisseling en ketensamenwerking.*

De kernwoorden in deze vraag zijn *beveiligingsarchitectuur, hooggerubriceerde informatievoorziening, informatie uitwisseling en ketensamenwerking*. Op basis van deze kernwoorden is de volgende samenvatting van dit ontwerp samengesteld:

In dit ontwerp is de hoofdvraag ingevuld door randvoorwaarden, ontwerpeisen en selectiecriteria voor de te ontwerpen beveiligingsarchitectuur te destilleren uit de theorie voor (beveiligings)architecturen, de context waarin ketensamenwerking plaatsvindt en specifieke eisen die door de organisatie aan de beveiligingsarchitectuur gesteld worden.

Daarnaast is voor het onderwerp ketensamenwerking en informatie uitwisseling een beveiligingsarchitectuur voor informatiestromen ontworpen. In het totale onderzoek is rekening gehouden met de rubricering van de omgeving. Dit is vooral tot uiting gekomen in de wijze waarop beveiligingsaspecten worden uitgewerkt in de architectuur, de benodigde diepgang van de uitwerking van technische beveiligingsoplossingen en een aangepaste manier van het maken van een risico analyse. Dit alles binnen de grenzen van de mogelijkheden van de organisatie in termen van middelen: “just enough” beveiligingsarchitectuur.

5.8 Validatie

In dit onderzoek is gebruik gemaakt van een aantal onderzoeksmethoden waarvan het gebruik verantwoord moet worden. In paragraaf 1.2.1 is tijdens de ontwerpfase van dit onderzoek reeds aangegeven op welke wijze het eindproduct gevalideerd kan worden. Dit zijn: de volledigheidscontrole van het ontwerp en de validatie aan de hand van analyse van het eindproduct. Daarnaast is in H3 een multicriteria analyse toegevoegd, gebruik daarvan wordt verantwoord onder het kopje criteria.

Volledigheidscontrole ontwerp

De volgende inputs zijn gebruikt bij het ontwerp:

1. principes (randvoorwaarden);
2. ontwerpeisen uit de organisatie;

Paragraaf 4.6 bevat een de verantwoording van het gebruik van inputs 1 en 2 in het ontwerp. Er is gekeken of alle randvoorwaarden en ontwerpeisen zijn gebruikt bij de onderbouwing van ontwerpkeuzes. Hiermee is gevalideerd dat in het eindproduct alle randvoorwaarden en ontwerpeisen zijn opgenomen.

In het ontwerp voor de beveiligingsarchitectuur voor informatiestromen (H5) zijn bijna alle elementen aanwezig die volgens het ontwerp van de referentiearchitectuur voor beveiliging (H4) aanwezig zouden moeten zijn. Niet alle elementen zijn volledig uitgewerkt. Dit zijn:

1. Detailuitwerking van koppeling tussen applicatiecomponenten en technologiecomponenten;

2. Maken van huidige en toekomstige views van de technologiecomponenten;
3. Planning en realisatie van de beveiligingsarchitectuur voor informatiestromen;
4. Meetbaarheid van de informatiebeveiliging voor aansluitcategorieën;
5. Afgeronde risicoanalyse.

Deze elementen worden voor de beveiligingsarchitectuur voor informatiestromen gezien als onderdeel van realisatiefase. Hiermee is gevalideerd dat het ontwerp van de beveiligingsarchitectuur voor informatiestromen compleet is volgens het ontwerp van de referentiearchitectuur voor beveiliging.

Criteria

Bij het opstellen van de selectiecriteria voor architecturen (zie paragraaf 3.5.2) zijn uit verschillende bronnen afkomstige criteria samengevoegd. Dit is reproduceerbaar gemaakt doordat het samenvoegen van criteria plaatsvindt op basis van een onderbouwde redenering (zie bijlage A).

Bij het toekennen van scores die selectie mogelijk maken is zoveel als mogelijk gebruik gemaakt van literatuurverwijzingen. De zogenaamde "blauwe" scores zijn tot stand gekomen door een expert panel van vijf personen voor elk criterium de score te laten bepalen en hier het rekenkundig gemiddelde van te nemen (zie paragraaf 3.5.3).

De validatie van het eindproduct (zie ook 1.2.1):

Inmiddels wordt de beveiligingsarchitectuur voor informatiestromen daadwerkelijk toegepast. Juist door de toepassing in de praktijk, wordt duidelijk of de architectuur ook werkt.

Onderstaande bevindingen laten zien op welke wijze de beveiligingsarchitectuur voor informatiestromen voldoet aan de subdoelstellingen uit paragraaf 5.1:

- De doorlooptijd van het realiseren van verbindingen is nog steeds hoog. Dit wordt vooral veroorzaakt omdat er afspraken gemaakt moeten worden met derde partijen. Dit is vaak onderdeel van een juridisch-politiek belangenspel en onderhandelingen waardoor besluitvorming zeer traag verloopt. De technische doorlooptijd is verkort van enkele maanden naar enkele weken. Dit relateert aan subdoelstelling DO1;
- Koppelingen worden nu per definitie volledig geautomatiseerd aangelegd, er is sprake van reductie van autorisaties voor het gebruik van gegevensdragers. Dit draagt positief bij aan subdoelstelling DO2, DO3 en DO6;
- Er zijn intussen diverse beveiligingscomponenten aanwezig die kunnen worden gebruikt, ook is duidelijk welke beveiligingscomponenten nog ontwikkeld moeten worden. Dit toont aan dat voldaan wordt aan subdoelstelling DO4;
- De beveiligingsarchitectuur voor informatiestromen bevat momenteel 5 categorieën, daarmee wordt voldaan aan subdoelstelling DO7;
- De laatste stand is dat 90% van de koppelingen is ondergebracht in een aansluitcategorie. Daarmee wordt voldaan aan subdoelstelling DO8.

Alleen voor subdoelstelling DO5 (aantoonbare kostenbesparingen in aanleg en exploitatie van koppelingen) zijn nog onvoldoende meetgegevens beschikbaar. Dit wordt veroorzaakt door het feit dat het aantal koppelingen dat per jaar gerealiseerd wordt laag ligt (minder dan vijf).

De validatie van de beveiligingsarchitectuur voor informatiestromen valideert ook tot op zekere hoogte de referentiearchitectuur voor beveiliging. Door de gekozen opzet om vanuit een referentiearchitectuur een beveiligingsarchitectuur voor een aspectgebied te produceren en het feit dat in dit onderzoek slechts een aspectgebied is uitgewerkt, is het niet mogelijk om te valideren in hoeverre de beveiligingsarchitecturen voor andere aspectgebieden juist zullen zijn. De beveiligingsarchitectuur voor informatiestromen kan wel worden gezien als een specifieke gevalstudie. Op basis daarvan kan uitspraak worden gedaan over andere beveiligingsarchitectuur voor aspectgebieden, voor zover de gebruikte objecten binnen de referentiearchitectuur van beveiliging voor meerdere gevallen van toepassing zijn.

6 Onderzoeksresultaten

In dit hoofdstuk worden conclusies geformuleerd op basis van bevindingen in dit onderzoek. Daarnaast worden aan de hand van de ervaringen die zijn opgedaan met de beveiligingsarchitectuur voor informatiestromen een aantal verbeterpunten geformuleerd. Tot slot wordt in paragraaf 6.3 gereflecteerd op dit onderzoek.

6.1 Bevindingen

Gedurende dit onderzoek zijn een aantal bevindingen en ervaringen opgedaan. In deze paragraaf zijn ze bijeengebracht. Ze worden gebruikt als onderbouwing van de conclusies en aanbevelingen in paragraaf 6.2.

Er zijn geen direct toepasbare modellen en methoden om een beveiligingsarchitectuur te ontwerpen.

Zowel in het Enterprise Architectuur domein als in het beveiligingsdomein is een uitgebreide zoektocht noodzakelijk geweest. De ontwikkelsnelheid in het vakgebied van beveiliging leidt ertoe dat je als beveiligingsarchitect eigenlijk altijd achter de feiten aan loopt. Het ontwikkelen van toepasbare modellen en methoden kost veel tijd, die is vaak niet voor handen. In het vakgebied van Enterprise Architectuur wordt dit inmiddels erkend, het vakgebied beveiligingsarchitectuur heeft op dit gebied nog een ontwikkeling door te maken.

Beveiligingsarchitectuur is een proces.

De beschikbare technieken om gebruik dan wel misbruik te maken van ICT middelen worden steeds geavanceerder. Dat gaat net even iets sneller dan de de technologische ontwikkeling van ICT middelen zelf. Dit leidt tot een zeer snel bewegende context. Dit betekent voor de beveiligingsarchitectuur dat er flexibiliteit moet worden ingebouwd en dat het onderhoud arbeidsintensief is.

Factoren die de complexiteit vergroten.

Het ontwerpen van beveiligingsarchitectuur voor aspectgebieden van beveiliging introduceert op tactisch niveau (logisch architectuurniveau) een extra dimensie. Daarmee wordt de hoeveelheid werk om de beveiligingsarchitectuur te beschrijven en te onderhouden verveelvoudigd voor elk aspect. Om dit beheersbaar te houden is het noodzakelijk om gebruik te maken van reeds beschikbare componenten in de Enterprise Architectuur. Alleen door “just enough” beveiligingsarchitectuur toe te passen is een beveiligingsarchitectuur te onderhouden.

Het kiezen van de juiste afbakening van architectuurelementen, het niveau van detail en het vinden van de methode om de juiste keuzes te kunnen maken maakt beveiligingsarchitectuur complex.

Op het gebied van beveiliging hangt alles samen: fysieke beveiliging, beveiliging van bedrijfsprocessen en logische beveiliging komt allemaal terug in een beveiligingsarchitectuur. In de beveiligingsarchitectuur is vooral gekeken hoe informatiebeveiligingstechnische randvoorwaarden moeten worden ingericht. Beveiligingsfuncties die elders geregeld zijn, zoals bijvoorbeeld de organisatie van beveiliging in het beveiligingsbeleid en de fysieke beveiliging zouden onderdeel kunnen zijn van de architectuur.

Wet- en regelgeving, beleidsvorming en besluitvorming.

De mogelijkheden die er zijn om de informatievoorziening te beveiligen zijn groot. Er is echter een aanpassingsprobleem ontstaan tussen werkpraktijk en regelgeving omdat de vernieuwing van regelgeving en de bijbehorende politieke besluitvorming zeer traag verloopt. Vanwege de inhoudelijke complexiteit van de informatievoorziening wordt de reikwijdte van besluiten over wet- en regelgeving serieus onderschat door bestuurders. De combinatie van het grote belang dat gemoeid is met hooggerubriceerde informatie en de complexe afwegingen die meespelen als het gaat om gebruik van bijzondere bevoegdheden is het

basisrecept voor een politieke deadlock situatie. We zullen moeten leven met het feit dat deze problematiek niet op korte termijn zal worden opgelost.

Ontwerpproces en praktijk

Terugkijkend naar de wijze waarop het ontwerp van de beveiligingsarchitectuur voor informatiestromen tot stand is gekomen blijkt dat het gevolgde proces in werkelijkheid een stuk grilliger verloopt dan dat dit ontwerpdocument doet vermoeden. Op zich is dat niet erg: de praktijk is nu eenmaal weerbarstig. De procesvolgorde zoals de TOGAF ADM deze beschrijft is echter wel in grote lijnen gevolgd. De TOGAF ADM ondersteunt deze bevindingen: TOGAF onderkent dat dit soort ontwerpprocessen meestal niet volgens een vast patroon verlopen.

Beveiligingsarchitectuur voor informatiestromen

De eerste conclusie over de beveiligingsarchitectuur voor informatiestromen is dat deze brengt wat was beoogd. Op sommige onderdelen is de beveiligingsarchitectuur voor informatiestromen onvolledig, maar dit is niet problematisch. Dit is bij een dergelijke ontwerpstudie ook te verwachten, de essentie is dat hiervan geleerd kan worden en dat aanpassingen kunnen worden doorgevoerd via het onderhoudsproces aan de architectuur. De volgende bevindingen zijn niet genoemd in paragraaf 5.7, maar zijn wel relevant voor de conclusies en aanbevelingen:

- De architectuur voor informatiestromen schept duidelijkheid bij systeemimplementaties. Er is sprake van vastgestelde (generieke) beveiligingsfunctionaliteiten die worden ontwikkeld en hergebruikt. Functioneel- en technisch beheerders zien kansen ontstaan omdat de architectuur praktische oplossingen biedt voor belemmerende problematiek van externe koppelingen. Dit leidt tot eenheid in beveiliging en tot effectiviteit in bedrijfsprocessen.

- In het verleden kon de discussie bij het koppelen van externe gegevensbronnen makkelijk ontaarden in gebruik van beveiligingsargumenten die plaats-, tijd- en persoonsgebonden leken te zijn. Een belangenspel zonder dat het belang van de organisatie als geheel daar een stem in had. De geaccordeerde beveiligingsarchitectuur voor informatiestromen zorgt ervoor dat de discussies nu gaan over de zaken die er toe doen: dreigingen, risico's en kansen voor de organisatie.

- De architectuur voor informatiestromen wordt gehanteerd als kader bij advisering over informatiebeveiligingsvraagstukken. De architectuur is niet alleen kaderstellend op het gebied van koppelingen (het externe deel), maar ook intern als het gaat over de wijze waarop informatie moet vastgelegd en worden ontsloten voor eindgebruikers.

- De informatiestromen architectuur kent ook beperkingen. Bij vragen over de beveiliging van externe koppelingen speelt gegevensmanagement altijd een rol omdat het uiteindelijk altijd gaat om het ontsluiten van informatie aan eindgebruikers. Benodigde functionaliteit (bijvoorbeeld integraal zoeken over meerdere bronnen) is leidend voor de wijze waarop de informatie intern wordt opgeslagen en ontsloten. Dit is nu geen expliciet onderdeel van de beveiligingsarchitectuur voor informatiestromen, dat zou het wel moeten zijn.

6.2 Conclusies en Aanbevelingen

De conclusies en aanbevelingen zijn geformuleerd vanuit verschillende gezichtspunten: Beveiligingsarchitectuur voor informatiestromen, Beveiligingsarchitectuur, Organisatie en Ketensamenwerking in het veiligheidsdomein.

Beveiligingsarchitectuur voor informatiestromen

De volgende conclusies en aanbevelingen zijn onderbouwd in paragraaf 5.7.

a. De beveiligingsarchitectuur voor informatiestromen beantwoordt aan de hoofdvraag die in dit ontwerpdocument is gesteld.

b. De beveiligingsarchitectuur voor informatiestromen houdt onvoldoende rekening met organisatiedoelstellingen op het gebied van gegevensmanagement. Het uitwerken van gegevensmanagement in het kader van informatiestromen zal de beveiligingsarchitectuur verbeteren.

Beveiligingsarchitectuur

c. De referentiearchitectuur voor beveiliging uitvoeren betekent een omslag in het denken over beveiliging, vanuit een controle en audit perspectief (prescriptief in een aanbodstructuur) naar mogelijkheden scheppen vanuit beveiliging voor de organisatie (adaptief in een vraagstructuur).

d. Deze scriptie beperkt zich tot een referentiearchitectuur voor beveiliging en een beveiligingsarchitectuur voor informatiestromen. Bij het tot stand brengen van ketensamenwerking komt veel meer kijken: Bestuurlijke en juridische aspecten zoals de omgang met informatie die de organisatie ontvangt of verstrekt en de context waarin die informatie verwerkt mag worden zijn onderdeel van de problematiek die een beveiligingsarchitectuur probeert te ondervangen, maar zijn geen onderdeel geweest van dit onderzoek.

e. De architectuur is niet volledig. De koppeling met informatiebeveiligingsbeleid, koppeling met andere beveiligingsfuncties zoals fysieke beveiliging, personele beveiliging en procesbeveiliging zijn slechts beperkt aanwezig. Het opnemen van deze elementen kan een goede aanvulling zijn voor de beveiligingsarchitectuur.

Organisatie

f. De beveiligingsarchitectuur is een adequaat middel gebleken om informatie gerelateerde vraagstukken en beveiligingsproblematiek met elkaar in verband te brengen. Ze is sturend voor veranderingen binnen de informatievoorziening.

Ketensamenwerking in NL veiligheidsketen

g. De bestaande wetten en kaders zijn onvoldoende toegerust om op de juiste wijze sturend te zijn om doelstellingen op het gebied van ketensamenwerking te realiseren.

h. De beveiligingsarchitectuur voor informatiestromen is toepasbaar binnen de veiligheidsketen. Toepassing van de beveiligingsarchitectuur voor informatiestromen in hooggerubriceerde omgevingen binnen andere delen van de rijksoverheid is mogelijk, en wellicht ook in andere sectoren waar gewerkt wordt met hooggerubriceerde informatie.

6.3 Reflectie

Beveiligingsarchitectuur is complex. Daarnaast is beveiliging een vakgebied waarin ontwikkelingen zeer snel gaan. Terwijl het ontwerp van de beveiligingsarchitectuur tot stand kwam, was een duidelijke trend zichtbaar: ingehaald worden door de werkelijkheid. Dit geldt bijvoorbeeld voor de adoptie van het O-ISM3 security management proces raamwerk in TOGAF, de ontwikkeling van een nieuwe versie van het VIR-BI en de centralisatie van de informatievoorziening van de rijksoverheid die momenteel plaatsvinden in het kader van de (e)i-overheid. Hierdoor is integrale samenwerking van rijksdiensten van "een onderwerp voor de nabije toekomst" in hoog tempo werkelijkheid geworden in de dagelijkse praktijk.

Het bleek niet eenvoudig om een dergelijk complex onderwerp gestructureerd op papier te krijgen Dat heeft geleid tot een aanzienlijke investering in tijd en het herschrijven van deze scriptie. Tijdrovend, maar leerzaam. Na een aantal jaren werken in een ambtelijke organisatie is het goed om te ontdekken dat de scherpte die nodig is voor het schrijven van een technische scriptie nog aanwezig is.

Afstuderen als deeltijd student met een baan en een druk gezin is geen eenvoudige opgave gebleken. De bijna duizend uur toewijding die noodzakelijk is om tot een goed afstudeerverslag te komen is alleen op te brengen als alles klopt: werksituatie, privésituatie en voldoende ruimte voor ontspanning.

7 Bibliografie

Aceituno, Vincente; The Open Group. (2011). *Open Group - Information Security Management Maturity Model.* ISBN 1-931624-86-0: The Open Group.

Alter, S. (1999). *Information systems - A management perspective.* San Fransisco; ISBN 2-201-52108-3: Addison Wesley Longman, Inc.

Bongers, L. (2006). *Security binnen de Enterprise Architectuur.* Opgeroepen: jan 2009, van NICIS Master Thesis Lab - Archive 2005-2008 computing and information sciences: http://www.cs.ru.nl/mtl/scripties/2006/LucienBongersScriptie.pdf

Buffam, W. (2000). *E-Business and IS Solutions - an architectural approach to business problems and opportunities.* ISBN 0-201-70847-7: Addison-Wesley.

Carnegie Mellon University. (2011). *Cyber security watch survey.* Opgeroepen: jan 2012, van http://www.cert.org/archive/pdf/CyberSecuritySurvey2011Data.pdf

de Wijk, R. (2005). *Supermacht Europa.* Alphen a/d Rijn; ISBN 9053304630: Haasbeek.

Deming, W. (1950, 12 01). *Kwaliteitscirkel van Deming*. Opgeroepen: mrt 2012, van Wikipedia: http://nl.wikipedia.org/wiki/Kwaliteitscirkel_van_Deming

Denktank nationale veiligheid. (2010, 10 02). *ICT-kwetsbaarheid en Nationale Veiligheid.* Opgeroepen: mrt 2011, van http://www.hcss.nl/nl/download/1610/file/HCSS ICT-kwetsbaarheid en Nationale Veiligheid.pdf

Gartner. (2006). *Gartner Defines the Term "Enterprise Architecture".* Stanford USA; G00141795: Gartner.

Goutier, H., & Lieshout, J. v. (2010). *Nora 3.0 - prinipes voor samenwerking en dienstverlening.* Opgeroepen: apr 2011, van http://www.infopuntveiligheid.nl/Infopuntdocumenten/NORA%203_0%202010-2.pdf

Greefhorst, D., Grefen, P., Saaman, E., Bergman, P., & Beek, W. v. (2008). *Referentie-architectuur.* Opgeroepen: jul 2011, van http://www.archixl.nl/files/lac2008_referentiearchitectuur.pdf

ISM3 Consortium. (2007). *ISM-3 compared to ISO27001.* Madrid. Opgeroepen: jun 2009

ISO/IEC. (2000). Recommended practice for Architectural Description of Software-Intensive Systems. Joint Technical Committee 1 of the International Organization for Standardization and the International Electrotechnical Commission.

ISO/IEC. (2005). ISO/IEC 27001:2005 - Information technology -- Security techniques -- Information security management systems -- Requirements. ISO/IEC.

Lankhorst et al., M. (2005). *Enterprise Architecture at Work, ISBN 9783642013096.* Heidelberg: Spinger Science+Business Media.

Logius, Kenniscentrum Architectuur. (2008, 7 1). *MARIJ.* Opgeroepen: jan 2009, van E-Overheid: http://www.e-overheid.nl/atlas/referentiearchitectuur/marij/marij.html

Maes, R. (2007). *PrimaVera - An Integrative Perspective on Information Management.* Opgeroepen: okt 2010, van http://primavera.fee.uva.nl/PDFdocs/2007-09.pdf

Ministerie van Algemene Zaken. (2002, december). *Art. 6 Wet: de Inlichtingen- en Veiligheidsdiensten*. Opgeroepen: dec 2011, van overheid.nl: http://wetten.overheid.nl/BWBR0013409

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. (2010, 5 18). Jaarverslag 2010 Ministerie van BZK. Den Haag.

Ministerie van Economische Zaken. (1996). *A&K analyse*. Opgeroepen: jan 2012, van http://rm-inv.enisa.europa.eu/methods_tools/m_dutch_ak_analysis.html

Ministerie van Veiligheid en Justitie. (2012, 01 01). *Art. 98 Wetboek van Strafrecht*. Opgeroepen: jun 2011, van Overheid.nl: http://wetten.overheid.nl/BWBR0001854/TweedeBoek705742/TitelI/Artikel98

Narayaban. (2006). *Think Beyond "Controls": A "process" based approach for Information Security Management using ISM3*. Opgeroepen: apr 2011, van www.anupnarayanan.org/ismsusingism3.pdf

Rademaker, M., & Frikling, E. (2010). ICT kwetsbaarheid - de invulling van de Nationale Cyberstrategie. *Magazine nationale veiligheid en crisisbeheersing*, pagina 37.

Sessions, R. (2007). *Comparison of the Top Four Enterprise Architecture Methodologies.* Opgeroepen: apr 2011, van objectwatch.com: http://www.objectwatch.com/white_papers.htm#4EA

Sherwood, J. (2009). *SABSA - Enterprise Security Architecture.* Opgeroepen: mrt 2011, van Sabsa institute: http://www.sabsa-institute.org/whitepaperrequest.aspx?pub=Enterprise+Security+Architecture

Sherwood, J., Clark, A., & Lynas, D. (2005). *SABSA Enterprise Security Architecture - A business driven approach.* San Fransisco: CMP Books - ISBN 978-1-57820-318-5.

Stekkerman, J. (2004). *How to survive in the jungle of architecture frameworks.* Trafford Publishing - ISBN 978-1-41201-607-0.

Symantec Security Response. (2011). *W32.Stuxnet Dossier v1.4.* Opgeroepen: jun 2011, van http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

The Open Group Architecture Framework (TOGAF). (2009, 01 01). *TOGAF™ version 9, Enterprise Edition.* Opgeroepen: jan 2009, van The Open Group, making standards work: http://www.opengroup.org/togaf/

The Open Group Security Forum. (2007, 10). *Information Security Strategy (A framework for Information-Centric Security Governance.* Retrieved jun 2008, from www.opengroup.org: http://www.opengroup.org/pubs/catalog/w075.htm

U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Deloitte. (2011, januari). *2011 CyberSecurityWatch Servey.* Opgeroepen: dec 2011, van http://www.cert.org/archive/pdf/CyberSecuritySurvey2011.pdf

wetboek-online. (sd). *Wetboek van Strafrecht*. Opgeroepen: okt 2011, van http://www.wetboek-online.nl/wet/Sr/98.html

Wetenschappelijke Raad voor Regeringsbeleid. (2011, 03 01). *rapport iOverheid.* Opgeroepen: mrt 2011, van WRR: http://www.wrr.nl/content.jsp?objectid=5656

Wikipedia. (2010). *Bradly Manning*. Opgeroepen: jul 2011, van Wikipedia.org: http://en.wikipedia.org/wiki/Bradley_Manning

Zachman. (sd). *Zachman Framework*. Opgeroepen: mrt 2012, van Wikipedia: http://en.wikipedia.org/wiki/Zachman_Framework

A. Bijlage vergelijkingscriteria paragraaf 3.5.2

De criteria van (Sessions, 2007), Gartner, (Stekkerman, 2004) en O-ISM3 zijn opgenomen in deze bijlage. De eerste kolom bevat het volgnummer waarop het criterium is gevonden in de brongegevens. De tweede kolom is het volgnummer van criteria die als relevant worden beschouwd. In de referentie kolom is voor gelijksoortige criteria dit volgnummer opgenomen. De derde kolom bevat het volgnummer van het criterium in de verklarende tekst in paragraaf 3.5.2.
Een aantal elementen uit de lijst zijn eigenlijk succesfactoren van een architectuur. Deze kunnen in sommige gevallen worden vertaald naar een criterium, maar vaker zijn het randvoorwaarden die nodig zijn om een architectuur te laten functioneren in de organisatie. Dit geldt in voor elke architectuur en daarom zijn ze ook niet bruikbaar als criterium om architecturen te vergelijken. In de tabel staan ze gemarkeerd met de letter F (feature). Tenslotte zijn een aantal elementen gemarkeerd met de letter X, niet opgenomen in de onderstaande lijst met criteria om verschillende redenen. Deze staan vermeld in de kolom "rationale".

#	Analyse	Criterium in tekst	Omschrijving		bron	Criteriatabel	definitie	Ref #	Rationale
1	1	1	Taxonomy Completeness	Criterium	Sessions	Compleetheid van scope	De mate waarin de architectuur toestaat objecten wel of niet te classificeren.	1	
2	2	6	Process Completeness (build/maintance)	Criterium	Sessions	Proces voor eigen ontwikkeling	Hoe goed is de procesondersteuning voor het creëren en onderhouden voor de EA.	6	
3	3	7	Reference-model guidance	Criterium	Sessions	Architectuur productondersteuning	Hoe goed ondersteunt de methode de bouw van relevante referentie modellen.	7	
4	4	3	Practice guidance	Criterium	Sessions	Organisatorische inbedding	De mate waarin architectuur binnen de rest van de organisatie is doorgedrongen en wordt gebruikt (architectuur als cultuur).	3	
5	5	8	Maturity Model	Criterium	Sessions	Volwassenheidsniveau en toekomstdenken	In hoeverre ondersteund de architectuur volwassenheidniveaus binnen verschillende delen van de organisatie.	8	
6	6	2	Business Focus	Criterium	Sessions	Koppeling met strategische doelstellingen	Mate waarin de architectuurmethode zijn eigen toegevoegde waarde voor de organisatie zichtbaar maakt.	2	
7	7	4	Governance guidance	Criterium	Sessions	Besturingsmodel	Bevat de architectuurmethode of raamwerk een effectief besturingsmodel voor architectuur.	4	
8	8	5	Partitioning guidance	Criterium	Sessions	Delegatie van taken	De mate waarin verspreiding van de werkzaamheden over de organisatie om een architectuur te beheren wordt ondersteund.	5	
9	9	9	Prescriptive catalog	Criterium	Sessions	Ondersteuning van een objectencatalogus	Mate waarin de architectuur ondersteund in het maken van een architectuur objecten catalogus met als doel hergebruik van componenten.	9	

10	10	10	Vendor Neutrality	Criterium	Sessions	Vendor lock-in	De mate van vendor lock-in die plaatsvindt als wordt gekozen voor een specifieke architectuur methode.	10	
11			Information availability	Criterium	Sessions		De hoeveelheid informatie die vrij of tegen geringe kosten beschikbaar is over een methode.	10	
12	11	11	Time to Value	Criterium	Sessions	Implementatietijd	De tijd die het kost voordat een architectuurmethode toegevoegde waarde gaat opleveren voor de organisatie.	11	
13			Maturity level	Criterium	O-ISM3		Het raamwerk bevat volwassenheidsniveaus.	8	
14			Certification Value protection	Criterium	O-ISM3		De mate waarin de architectuur ruimte laat voor interpretatie door auditors bij certificering.	F	
15			Organizational Model	Criterium	O-ISM3		De compleetheid/granulariteit waarmee de architectuur de organisatie beschouwd.	1	
16			Link between business goals and Information security	Criterium	O-ISM3		Worden bedrijfsdoelstellingen en beveiliging gekoppeld.	2	
17			Goal	Criterium	O-ISM3		Absolute security versus achievable security.	X	Is onderdeel van beveiligingsdoelstelling en is daarom geen criterium
18			Inputs	Criterium	O-ISM3		Processen kennen afhankelijkheden door outputs als inputs voor andere processen te definiëren.	X	Is noodzakelijk onderdeel van 20
19			ouputs	Criterium	O-ISM3		gedefinieerde proces outputs maken metingen mogelijk.	X	Is noodzakelijk onderdeel van 20
20			Metrics	Criterium	O-ISM3		Het raamwerk moet meetbaarheid ondersteunen zodat een continu proces van verbetering mogelijk wordt.	8	
21	13	12	Accreditable	Criterium	O-ISM3	Certificering	Certificering van de organisatie kan een bijdrage leveren aan het vertrouwen dat de organisatie geniet van management en/of externe partijen.	12	
22			Distribution of responsibilities	Criterium	O-ISM3		Hoe goed ondersteund een architectuur de distributie van verantwoordelijkheden over de organisatie.	5	
23			References	Criterium	O-ISM3		De mate waarin best practices voor de architectuur methode beschikbaar zijn.	7	
24			Cost	Criterium	O-ISM3		Keuze vrijheid ten aanzien van kosten door volwassenheidsniveaus.	8	
25			Implementation Guidance	Criterium	O-ISM3		De mate waarin het raamwerk een leidraad is voor organisatorische aspecten.	7	
26			Security Proces Selection	Criterium	O-ISM3		Op basis van security doelstellingen (O-ISM3) versus external controls (ISO).	F	Gaat over selectie van security processen (inhoud)
27	14	13	Success criteria	Criterium	O-ISM3	Architectuur succesfactoren	Is controleerbaar wanneer een architectuur of raamwerk aan de verwachtingen voldoet.	13	

28			Outsourcing	Criterium	O-ISM3		ondersteund meetbaarheid zodat KPI kunnen worden gedefinieerd (SLA).	X	Bij outsourcing is meetbaarheid van belang, onderdeel van 20
29			Capability	Criterium	O-ISM3		Hoe eenduidig definieert de architectuur de doelstellingen van een volwassenheidsniveau.	8	
30			Paradigm	Criterium	O-ISM3		Hoe goed integreren processen in reeds bestaande methoden waarop bedrijfsprocessen zijn gebaseerd, zoals COBIT, ITIL, ISO9001.	3	
31			Process improvement cycle	Criterium	O-ISM3		De mate waarin processen zijn gericht op verbetering en het niveau waarop dit plaatsvindt (strategisch, tactisch, operationeel).	8	
32			Approach	Criterium	O-ISM3		Top down (O-ISM3) versus bottom up (ISO2700X): ISO uses assets, O-ISM3 business goals.	X	Is onderdeel van beveiligingsdoelstelling en is daarom geen criterium
33			Information system model	Criterium	O-ISM3		Perspectief waarmee een informatiesysteem wordt bekeken.	X	Gaat over beveiligingsperspectief (inhoud)
34			Scope	Criterium	O-ISM3		Keuzevrijheid in scope voor beveiliging ten aanzien van kritische systemen.	1	
35			License	Criterium	O-ISM3		De hoeveelheid informatie die vrij of tegen geringe kosten beschikbaar is van een raamwerk, is het een standaard.	10	
36			Issuer	Criterium	O-ISM3		O-ISM3 of ISO?	X	Niet relevant als criterium
37			Timeline maintenance cycle	Criterium	O-ISM3		In hoeverre blijft de architectuur up-to-date met best practices en technologische ontwikkelingen.	6	
38			EA is the process	Criterium	Gartner		Enterprise architectuur is geen bibliotheek met dingen maar een proces.	6	
39			translates business vision and strategy	Criterium	Gartner		Strategie, bedrijfsdoelstellingen zijn leidend anders bestaat het risico dat de EA een doel op zich wordt.	2	
40			supports change	Criterium	Gartner		EA bestaat omdat het noodzakelijk is om organisatieveranderingen te ondersteunen.	8	
41			Enables communication, creates and improves key principles and models	Criterium	Gartner		Output is proces, informatie en technologieveranderingen, op basis van principes die beslissingen ondersteunen en modellen die de resultaten hiervan aantonen.	3	
42			Discribes future state of the enterprise and enbles its evolution	Criterium	Gartner		EA geeft richting aan het projectportfolio en draagt vernieuwende initiatieven aan die ervoor zorgen dat de toekomstvisie wordt gerealiseerd.	8	

43			The scope of EA includes people, proces, information and technology, their interrelationships and external connections	Criterium	Gartner		De scope van de EA gaat veel verder dan technologie. Bedrijfsprocessen, technologie, organisatie en informatie kennen onderlinge afhankelijkheden en externe relaties die ook beschouwd moeten worden.	1	
44			Holistic solutions that address business challenges and support the governance needed to implement them	Criterium	Gartner		Architecten zijn betrokken bij besturing en strategische planningsprocessen die noodzakelijke vernieuwingen ondersteunen.	1	
45			Holistic in Scope	approach	Stekkerman		Een architectuur moet breder zijn dan zijn scope.	1	
46			Collaboration based	approach	Stekkerman		De hele organisatie moet vertegenwoordigd zijn bij het ontwikkelen van de architectuur.	3	
47			Alignment driven	approach	Stekkerman		Architectuur ontwikkeling moet worden getoetst aan de business en IT strategie.	2	
48			Value Driven	approach	Stekkerman		Architectuur bevat een mechanisme dat ervoor zorgt dat de waarde van de architectuur zichtbaar wordt.	2	
49			Dynamic Environments	approach	Stekkerman		De architectuur is bestand tegen een dynamische omgeving door verandering op verschillende gebieden te faciliteren.	8	
50			Normative results	approach	Stekkerman		Oplossingen die de architectuur biedt moeten valideerbaar en meetbaar zijn en moeten dicht bij de werkelijkheid staan (real-world solutions).	13	
51			Non-prescriptive	approach	Stekkerman		Een implemetatie aanpak valt buiten de scope van de architectuur.	1	
52			include common vision	Succesfactor	Stekkerman		Zorg dat de business en IT een gemeenschappelijke visie hanteren.	6	
53			drive continuous business IT alignment	Succesfactor	Stekkerman		Zorg dat er een proces is dat zorg draagt voor de Business - IT alignment.	3	
54			Future state aware	Succesfactor	Stekkerman		Zorg dat er een toekomstvisie ligt waar naartoe gewerkt kan worden.	8	
55			Agility by lowering complexity barrier	Succesfactor	Stekkerman		Zorg dat er complexiteitsreductie kan plaatsvinden.	F	
56			Flexibility in linking wih external partners	Succesfactor	Stekkerman		Zorg dat de organisatie flexibel wordt voor de keuze voor een externe partner.	F	
57			Pro active organisation that drives innovation	Succesfactor	Stekkerman		Een architectuur kan alleen werken als de organisatie voldoende proactief is (procesvolwassenheid).	F	
58			Reduce risk	Succesfactor	Stekkerman		Zorg dat risico's die de organisatie loopt worden gereduceerd.	F	

59			Business unit IT functions should cooperate	Succesfactor	Stekkerman		Een architectuur werkt alleen als IT business units samenwerken.	F	
60			Progressive technology refinement program	Succesfactor	Stekkerman		Zorg dat nieuwe technologieen bewust worden gekozen.	F	
61			Unify business processes acros the enterprise	Succesfactor	Stekkerman		Zorg dat soortgelijke processen zoveel mogelijk worden verenigd.	F	
62			Unify information silos across the enterprise	Succesfactor	Stekkerman		Voorkom verkokering van Informatie, dit stoort innovatie en hergebruik van infomatie.	F	
63			Eliminate duplicate and overlapping technologies	Succesfactor	Stekkerman		Elimineer dubbele of overlappende technologiën	F	
64			Reuse technology and business application	Succesfactor	Stekkerman		Stimuleer hergebruik van technologie en toepassingen.	F	

B. Bijlage lijst met mogelijke beveiligingsaspecten

De gebruikt afkortingen in deze bijlage: Generally Accepted Areas Of Concern (GAAOC), Certified Information Systems Security Professional (CISSP), Public Key Infrastructure (PKI), Business Continuity Management (BCM)

De lijst in Tabel 11 bevat mogelijke beveiligingsaspecten. De in paragraaf 4.3.2 benoemde criteria voor aspecten zijn ingevuld. Hierbij is de volgende normering gebruikt:

- Criterium 1: 1 = beslaat 1-3 vlakken, 2 = beslaat 4-6 vlakken, 3 = beslaat 7-9 vlakken van het Primavera model.
- Criterium 3: is een volledige beveiligingsarchitectuur te maken op dit aspect? 1 =ja, o =nee
- Criterium 4: is dit aspect direct gerelateerd aan de inhoud van beveiligingsmaatregelen?

Criterium 2 (is er een beveiligingsvraag) is niet opgenomen omdat dit niet als selectie criterium voor mogelijke beveiligingsaspecten gebruikt kan worden.

Bron	Aspect	1	3	4
Sabsa security services	Access Control	3	1	1
CISSP domain	Access Control	3	1	1
Nora 3 beveiligingskader	alarmering	1	1	0
Sabsa security services	Application server security services	1	1	0
TOGAF GAAOC	Asset protection	2	0	1
TOGAF GAAOC	assurance	3	0	1
TOGAF GAAOC	audit	3	1	1
Nora 3 beveiligingskader	authenticatie	1	1	1
TOGAF GAAOC	authentication	1	1	1
Sabsa security services	Authentication services	1	1	1
TOGAF GAAOC	authorization	3	1	1
Sabsa security services	Authorization services	3	1	1
Nora 3 beveiligingskader	autorisatie	3	1	1
TOGAF GAAOC	availability	3	0	1
ISO 2700x	BCM	3	1	1
CISSP domain	Business Continuity and Disaster recovery	3	1	1
Sabsa security services	Certificate services	2	1	1
Sabsa security services	Client-server interaction	1	0	0
ISO 2700x	Compliance	3	0	1
Nora 3 beveiligingskader	continuiteisvoorzieningen	3	1	1
Nora 3 beveiligingskader	Controle	3	1	1
CISSP domain	Cryptograpy	2	1	1
Sabsa security services	Data management security services	1	1	1
Nora 3 beveiligingskader (hoe)	deponeren broncode	1	1	1
Sabsa security services	Directory services	1	1	0
Nora 3 beveiligingskader	filtering	3	1	0
ISO 2700x	Fysieke beveiliging	2	0	1
Nora 3 beveiligingskader	geprogrammeerde controles	1	0	0
Nora 3 beveiligingskader	identificatie	1	1	1
Politie	identificatie&authenticatie	1	1	1
Politie	inbraakpreventie en detectie	1	1	1

ISO 2700x	Incident management	1	0	1
ISO 2700x	Informatie assets	3	0	1
ISO 2700x	Informatie beleid	3	0	1
ISO 2700x	Informatie beveiliging infrastructuur	1	0	1
ISO 2700x	Informatiebeveiliging in systeemontwikkeling	1	1	1
CISSP domain	Information security governance	2	0	1
Sabsa security services	Intusion detection services	1	0	0
CISSP domain	Legal, regulations, compliance	3	0	1
Sabsa security services	Middleware security services	1	0	0
Sabsa security services	Network security services	1	0	0
Nora 3 beveiligingskader	onweerlegbaarheid	1	0	1
ISO 2700x	Personele beveiliging	1	0	1
CISSP domain	Physical security	1	1	1
Sabsa security services	Platform security services	1	0	0
Nora 3 beveiligingskader	rapportering	1	1	0
Sabsa security services	Registration services	2	1	1
TOGAF GAAOC	Risk management	3	0	1
CISSP domain	Risk management	3	0	1
TOGAF GAAOC	Security Administration	2	0	0
CISSP domain	Security Architecture and Design	3	0	1
CISSP domain	Security Operations	2	0	1
Sabsa security services	Services management	1	0	0
CISSP domain	Software development	1	1	1
CISSP domain	Telecommunications and Network	1	1	1
Sabsa security services	Time services	1	0	0
ISO 2700x	Toegang van buitenaf	1	1	1
ISO 2700x	Toegangscontrole	1	1	1
Politie	transport en opslag	1	1	1
Sabsa security services	User client services	1	0	0
Nora 3 beveiligingskader	vastleggen gebeurtenissen	1	1	1
Nora 3 beveiligingskader	zonering	3	1	1

Tabel 11: Overzicht mogelijke aspectgebieden

Tabel 12 bevat het overzicht als gefilterd wordt op Criterium 1 > 1, Criterium 3 en 4 allebei 1. Analyse van deze tabel levert de volgende mogelijke aspectgebieden (in deze opsomming zijn gelijksoortige aspecten slecht eenmaal vermeld): Access Control, Audit, Authorization, BCM, Certificate services, Controle, Cryptograpy, Informatiebeveiliging in systeemontwikkeling, Registration Services, Zonering.

Deze termen worden vervolgens vertaald en samengevoegd naar de volgende aspecten voor de beveiligingsarchitectuur: toegang en autorisatie, Business Continuity Management, PKI, Controle en Logging, informatiestromen.
De verklaring voor deze lijst:

1) Vanwege de relatie tussen toegangscontrole en autorisatie ligt het voor de hand deze samen te nemen;
2) Certificate services, Cryptograpy en Registration services zijn allemaal onderdeel van PKI;
3) Zonering heeft alles te maken met informatiedomeinen en is opgenomen in de informatiestromen architectuur.

4) Audit is een perspectief voor auditors (de controlerende instantie op informatiebeveiliging). In de praktijk is vastlegging van wat er gebeurd in de informatievoorziening het aspect waar het om gaat: logging.

Bron	Aspect	1	3	4
Sabsa security services	Access Control	3	1	1
CISSP domain	Access Control	3	1	1
TOGAF GAAOC	audit	3	1	1
TOGAF GAAOC	authorization	3	1	1
Sabsa security services	Authorization services	3	1	1
Nora 3 beveiligingskader	autorisatie	3	1	1
ISO 2700x	BCM	3	1	1
CISSP domain	Business Continuity and Disaster recovery	3	1	1
Sabsa security services	Certificate services	2	1	1
Nora 3 beveiligingskader	continuiteisvoorzieningen	3	1	1
Nora 3 beveiligingskader	Controle	3	1	1
CISSP domain	Cryptograpy	2	1	1
Sabsa security services	Registration services	2	1	1
Nora 3 beveiligingskader	zonering	3	1	1

Tabel 12: Gefilterde mogelijke aspectgebieden

C. Bijlage Architectuur voor Informatiestromen

Inleiding

Volgens het vigerend rijksbeleid voor het omgaan met gerubriceerde informatie - het VIR-BI - is het koppelen van informatiedomeinen met een belangrijk deel van de informatie niet zonder meer toegestaan. Dit treft vooral de Stg. Confidentieel en hoger gerubriceerde informatie. Door de steeds veranderende omgeving, de snelle technologische ontwikkelingen van de laatste jaren en de verregaande samenwerking met ketenpartners is er een duidelijke noodzaak ontstaan om steeds meer informatie te kunnen opnemen in de informatiehuishouding.

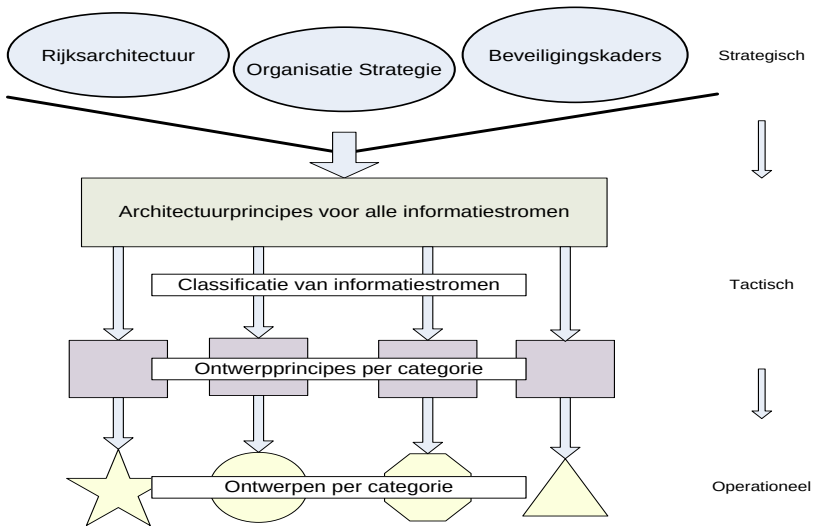
Het ontbreken van duidelijke richtlijnen over *hoe* er informatie gedeeld kan worden heeft geleid tot een praktijksituatie met diverse verschillende oplossingen. De gevolgen hiervan zijn:

1. Er worden te hoge kosten gemaakt voor het beheer van diverse oplossingen. Hetzelfde type probleem wordt met verschillende technologische oplossingen opgelost.
2. De drempel om te komen tot het delen van informatie is hoog. Voordat met partners kan worden overgegaan tot het delen van informatie vergt nu elke keer een lang proces van afstemming en ontwerp.
3. De informatiebeveiliging over onze informatie is zeer lastig te waarborgen. De complexiteit van het stelsel van oplossingen is niet goed te overzien, de verantwoording van de herkomst van informatie staat ter discussie en er zijn geen duidelijke kaders om implementatie ontwerpen te toetsen.

Doel van de architectuur op informatiestromen is standaard, toetsbare oplossingen te bieden voor het delen van informatie met anderen en dit te standaardiseren in direct toepasbare operationele oplossingen. Deze architectuur gaat ervan uit dat er geen onderscheid gemaakt wordt tussen data en (geduide) informatie. In sommige context is dit zinvol; hier gaan we er van uit dat inkomende en uitgaande data altijd geduide informatie kan bevatten en dus ook als zodanig behandeld dient te worden.

Opzet

De opzet wordt toegelicht in Figuur 16. De doelen en bepalingen uit de rijksarchitectuur, het strategisch kader van de organisatie en het informatiebeveiligingsbeleid dienen als basis voor de paragraaf “externe kaders”. Daarna worden in de paragraaf “Pincipes” de algemene principes afgeleid voor het delen van informatie binnen de organisatie. Deze principes zijn geldig voor alle uitwisseling van informatie, ongeacht de indeling van de informatiestroom in aansluitcategorieën. Hieruit volgt in de paragraaf “classificatie van informatiestromen” de indeling in aansluitcategorieën.



Figuur 16 :Opzet van de architectuur voor Informatiestromen

Daarna worden mogelijke ontwerpen van oplossingen die bij de verschillendeaansluitcategorieën horen beschreven. Tot slot wordt de risicoanalyse voor externe verbindingen beschreven.

Externe kaders

Rijsarchitectuur

De rijksoverheid stelt centraal kaders voor dienstverlening van overheidsonderdelen met burgers, bedrijven en andere overheidsonderdelen op. De basisprincipes van dit kader gaan voor een groot deel over het delen van diensten en informatie en zijn dus naast noodzakelijk tevens nuttig als uitgangspunt voor architectuurvorming binnen de organisatie.

Belangrijkste principes voor de overheid op het gebied van informatie uitwisseling en ketensamenwerking zijn gebundeld in een zogenaamde Referentiearchitectuur, de NORA (Nederlands Overheid Referentiearchitectuur). De basisprincipes uit de NORA 3 die van toepassing zijn op het uitwisselen van informatie zijn:

Burgers, bedrijven en overheidsorganisaties

- kunnen diensten eenvoudig vinden.
- ervaren uniformiteit in de dienstverlening door het gebruik van standaardoplossingen.
- hebben inzage in voor hen relevante informatie
- krijgen gerelateerde diensten gebundeld aangeboden.
- kunnen erop vertrouwen dat informatie niet wordt misbruikt.

Deze principes zijn niet direct toetsbaar maar bedoeld als uitgangspunt voor verder uitgewerkte architectuurprincipes. Als zodanig zullen ze in deze architectuur ook gehanteerd worden. Daarnaast bevat NORA 3.0 een aantal concreet uitgewerkte principes die hier van belang zijn, voornamelijk als uitwerking van het laatste basisprincipe:

- **AP37** Informatiebeveiliging door zonering en filtering: De betrokken faciliteiten zijn met behulp van filters gescheiden in zones.
- **AP38** Controle op volledigheid, juistheid en tijdigheid: De betrokken systemen controleren (informatieobjecten) op juistheid, volledigheid en tijdigheid.
- **AP39** Uitwisseling van berichten is onweerlegbaar.

Strategisch kader organisatie

Het delen van informatie is uiteindelijk slechts één van de middelen om organisatiedoelen te bereiken. Bij het inrichten hiervan is het belangrijk om organisatie doelen te beschouwen. Deze zijn relevant:

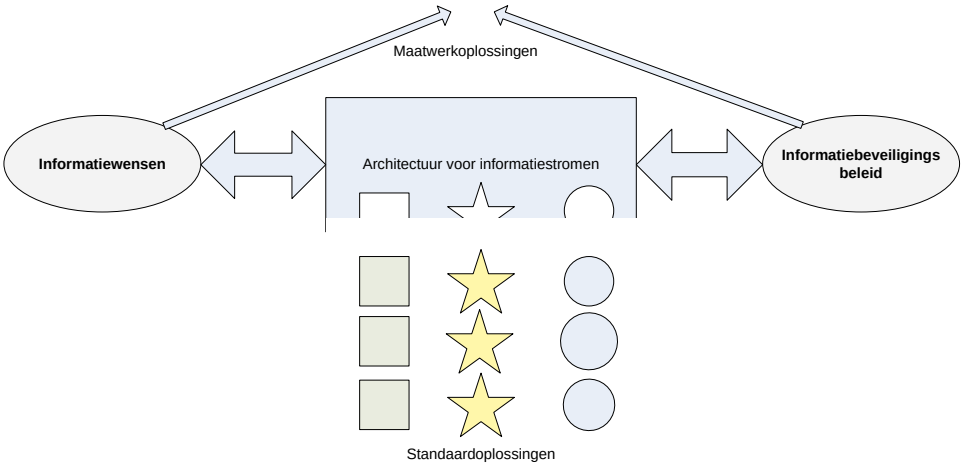
- Wij werken samen met ketenpartners.
- Wij maken de toegevoegde waarde van de organisatie intern én extern zichtbaar.

Deze doelen zijn bewust vanuit een ambitieniveau geformuleerd en kennen een zekere spanning met het exclusiviteitsbeginsel uit het VIR-(BI) over het gescheiden houden van gerubriceerde informatie.

Beveiligingskaders

Deze architectuur geeft hanteerbare kaders voor het delen van informatie en een motivatie van de keuze van de kaders. Voor het veilig toepassen van de architectuurprincipes is uiteraard meer nodig. De bij deze architectuur horende risicoanalyse beschrijft de risico's die optreden bij het delen van informatie en een geeft een beeld van de restrisico's bij toepassing van de hier gehanteerde principes.

Als deze architectuur gebruikt wordt bij realisatie van informatiekoppelingen kan de risicoanalyse worden gebruikt om te kijken of de ontworpen beveiligingsmaatregelen de risico's in voldoende mate afdekken.



Figuur 17: Werken onder architectuur voor Informatiestromen

In het informatiebeveiligingsbeleid staan een groot aantal relevante bepalingen. Hier lichten we een aantal bepalingen uit het plan ter illustratie van het niveau en type beschrijving van de maatregelen:

- Voor de verwerking van Stg. ZEER GEHEIM is koppeling met netwerken niet toegestaan. Draadloze netwerken mogen niet gekoppeld worden aan interne netwerken waarop bijzondere informatie verwerkt wordt. Interne netwerken met een rubricering Stg. GEHEIM worden niet direct of indirect gekoppeld aan externe verbindingen.
- Bij koppeling met informatiesystemen of informatievoorzieningen die niet onder het beheer van de eigen organisatie staan (externe verbinding) dient de betrouwbaarheid van de eigen systemen en voorzieningen niet te worden aangetast. Verbindingen dienen geverifieerd en bekrachtigd te worden middels authenticatie van apparatuur en gebruikers.
- Externe verbindingen die gebruikt worden voor de uitwisseling van bijzondere informatie, dienen te worden beveiligd met een vercijfermechanisme dat door het NBV (Nationaal Bureau Verbindingsbeveiliging) is goedgekeurd voor de betreffende rubricering. Voor een afdoende beveiliging dient naast de gebruikte ICT-apparatuur ook de fysieke locatie waar deze apparatuur gebruikt wordt, beveiligd te zijn.

Voor gerubriceerde informatie geldt verder volgens artikel 12 uit het VIR:

- Bijzondere informatie wordt zodanig beveiligd dat alleen personen die daartoe zijn gerechtigd bijzondere informatie kunnen behandelen of inzien voor zover dit noodzakelijk is voor een goede uitoefening van hun taak en dat inbreuken op de beveiliging worden gedetecteerd en gedegen onderzoek naar (mogelijke) inbreuken mogelijk is.

Principes

Deze principes zijn geformuleerd op basis van de relevante principes uit de NORA 3.0, het beveiligingsbeleid en de organisatiestrategie. De principes zijn in volledig uitgeschreven vorm te bekijken in bijlage D.

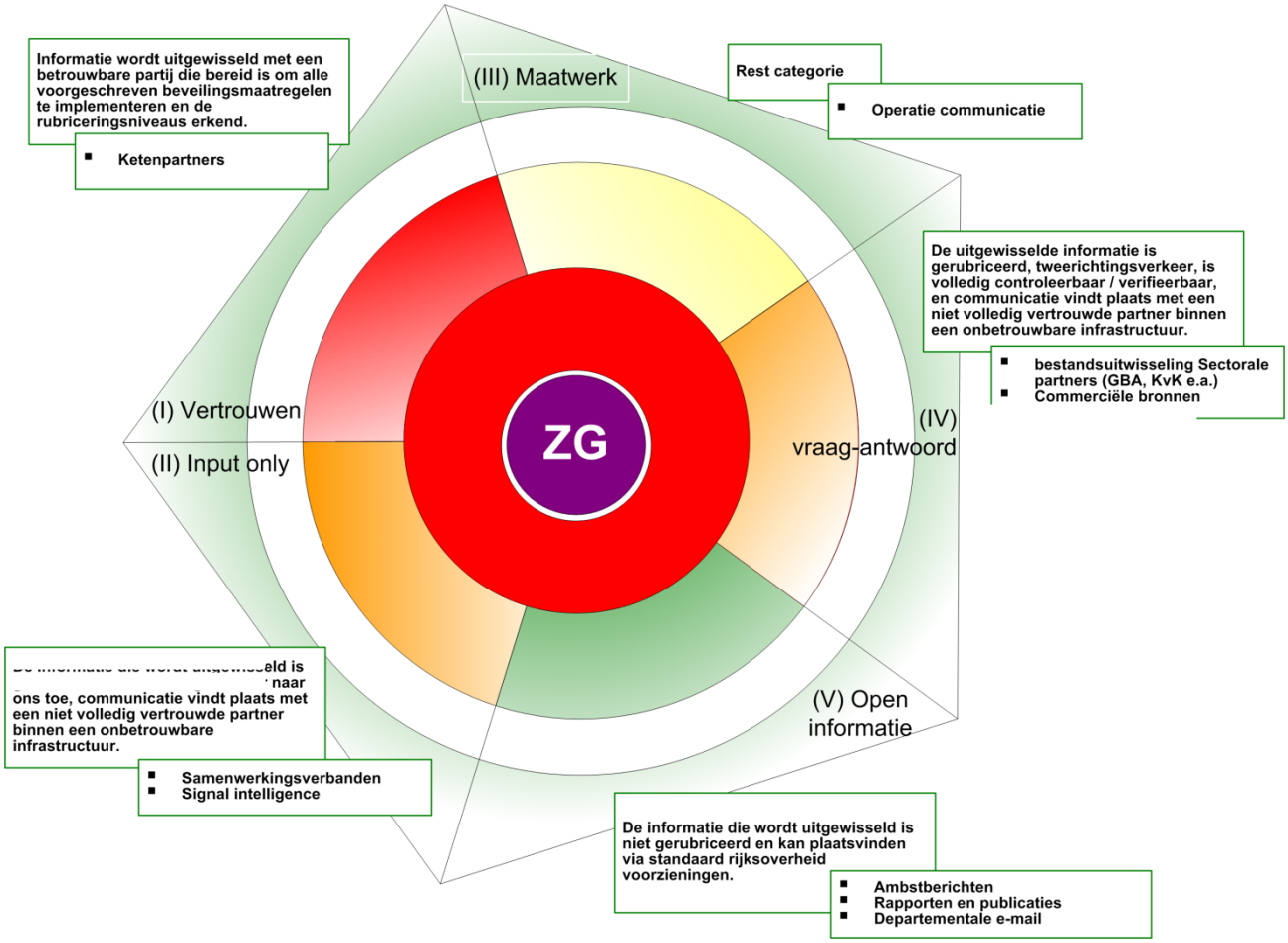
Code	Principe	Statement
INFSTR.1	Eén huishouding van informatie	Alle informatie gebruikt bij de primaire processen dient op gemakkelijk op generieke wijze beschikbaar te zijn.
INFSTR.2	Mate van vertrouwen is bepalend voor maatregelen	De mate van vertrouwen in de partner waarmee informatie wordt uitgewisseld is medebepalend voor de genomen beveiligingsmaatregelen.
INFSTR.3	Geautomatiseerde stromen lopen van buiten naar binnen	Voor geautomatiseerde stromen die van buiten naar binnen lopen gelden minder beperkingen dan voor informatie die van binnen naar buiten loopt.
INFSTR.4	Informatie wordt in het hooggerubriceerde netwerk gearchiveerd	Archieven moeten integraal doorzoekbaar zijn. Dat lukt niet als informatie zich in geïsoleerde netwerksegmenten of informatiedomeinen bevindt.
INFSTR.5	Bij internationale uitwisseling is er ruimte voor maatwerk	Bij internationale uitwisseling kunnen maatregelen die gewenst zijn door de partner prevaleren boven de eigen

		architectuurprincipes. Voorbeeld: NATO of EU richtlijnen.
INFSTR.6	Eigen infrastructuur in door derden gecontroleerde fysieke omgeving op basis van bestaande kaders.	Er worden alleen door het NBV goedgekeurde middelen ingezet, of een door het NBV geëvalueerde op infrastructuur die niet onder onze eigen invloedssfeer ligt.
INFSTR.6	Eigen infrastructuur in door eigen organisatie gecontroleerde fysieke omgeving worden kaders niet per definitie als leidend toegepast.	In deze situatie is het toegestaan op basis van de deugdelijke risico analyse niet goedgekeurde middelen in te zetten.

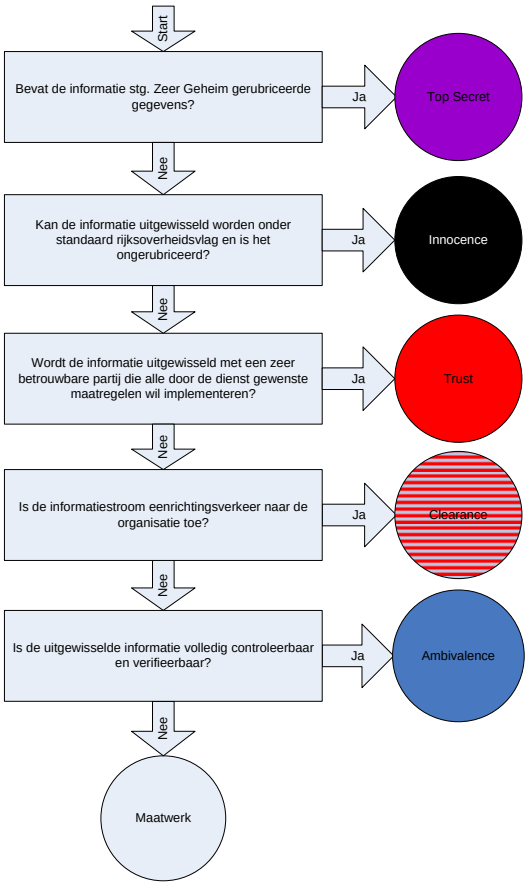
Classificatie van informatiestromen

Deze paragraaf beschrijft de principes die onderscheid aanbrengen tussen de diverse informatiestromen.

Bij de principes wordt per geclassificeerde categorie onder Rationale wel een korte toelichting van de betreffende categorie gegeven. Onder implicaties wordt de link naar de operationele systemen zoals de huidige netwerken gelegd. Figuur 18 bevat een schematische voorstelling van deze indeling, waarbij de categorieën worden benoemd, de scheidingscriteria worden aangegeven en enkele voorbeelden van informatiestromen worden gegeven.



Figuur 18: Basismodel architectuur voor Informatiestromen



Figuur 19: Beslisboom voor categorisering van informatiestromen

Om de keuze voor aansluitcategorieën van informatie-uitwisseling te vereenvoudigen is het schema in Figuur 19 opgesteld. Om de beslisboom te vereenvoudigen is soms een versimpeling van de onderliggende architectuurprincipes toegepast.

Ontwerpbeslissingen per categorie

Onderstaand overzicht bevat de ontwerpeisen (in de vorm van principes) voor de verschillende categorieën.

Code	Principe	Statement
ZG.1	Er is geen informatiestroom van of naar categorie ZG	Er is geen geautomatiseerde informatiestroom voor stg. Zeer Geheime informatie.
ZG.2	Zeer geheime informatie wordt fysiek gescheiden	
Open Info.1	Verkeer vanaf internet naar de organisatie is niet als zodanig herkenbaar	Het ontwerp voor het “Open Informatie”-domein is zodanig opgezet dat niet rechtstreeks te herleiden is waar dit verkeer van afkomstig is.
Vertrouwen.1	Communicatie met de vertrouwde partij is geïsoleerd	Communicatie met de vertrouwde partij dient te geïsoleerd te worden van communicatie met andere partijen.
Vertrouwen.2	Het niveau van fysieke beveilig dient gelijkwaardig te zijn aan dat van de benodigde informatiebeveiliging	
Input Only.1	Technisch afdwingen van éénrichtingsverkeer	In de categorie “Input only” wordt d.m.v. een diode altijd technisch afgedwongen dat informatie alleen richting de eigen infrastructuur gaat.
Input Only.2	Vastgestelde	Per informatiestroom in de categorie “Vraag-Antwoord”

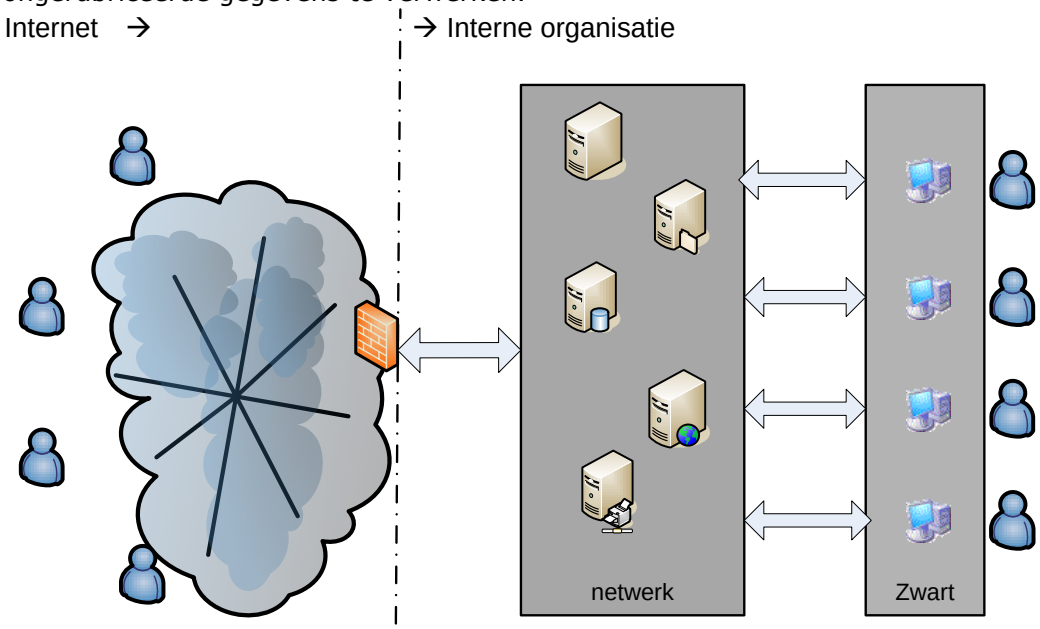
	cleaningsmaatregelen met risico-analyse	dienen vastgestelde cleaningsmaatregelen te worden ingezet en het gebruik hiervan dient te worden voorzien van een risicoanalyse voor de betreffende informatiestroom.
Vraag-Antw.1	Vastgestelde controlemaatregelen met risico-analyse	Per informatiestroom in de categorie “Vraag-Antwoord” dienen vastgestelde controlemaatregelen te worden ingezet en het gebruik hiervan te worden voorzien van een risicoanalyse voor de betreffende informatiestroom.
Vraag-Antw.2	Bevraging kan binnen en buiten plaatsvinden	Voor informatiestromen in de categorie “Vraag-Antwoord” kan de betreffende bron zowel binnen als buiten de organisatie staan.
Vraag-Antw.3	Logging van zoekvragen en antwoorden	Informatiestromen in de categorie “Vraag-Antwoord” bevatten zoekvragen en antwoorden waarvan een audittrail dient te worden vastgelegd.

De ontwerpen die nu volgen zijn van een logisch niveau. Ze zijn bedoeld om als basis te dienen voor een uitgewerkt technisch ontwerp. Vooral de noodzakelijke componenten en hun onderling relaties worden hier aangegeven.

Uitwerking van de aansluitcategorieën

Open informatie

Dit betreft de zwarte netwerkinfrastructuur. Er zijn richtlijnen over het gebruik van dit domein en er is een aparte infrastructuur voor het gebruik van ongerubriceerde data. Er dienen controles te worden ingericht of deze infrastructuur daadwerkelijk alleen gebruikt wordt om met ongerubriceerde gegevens te verwerken.



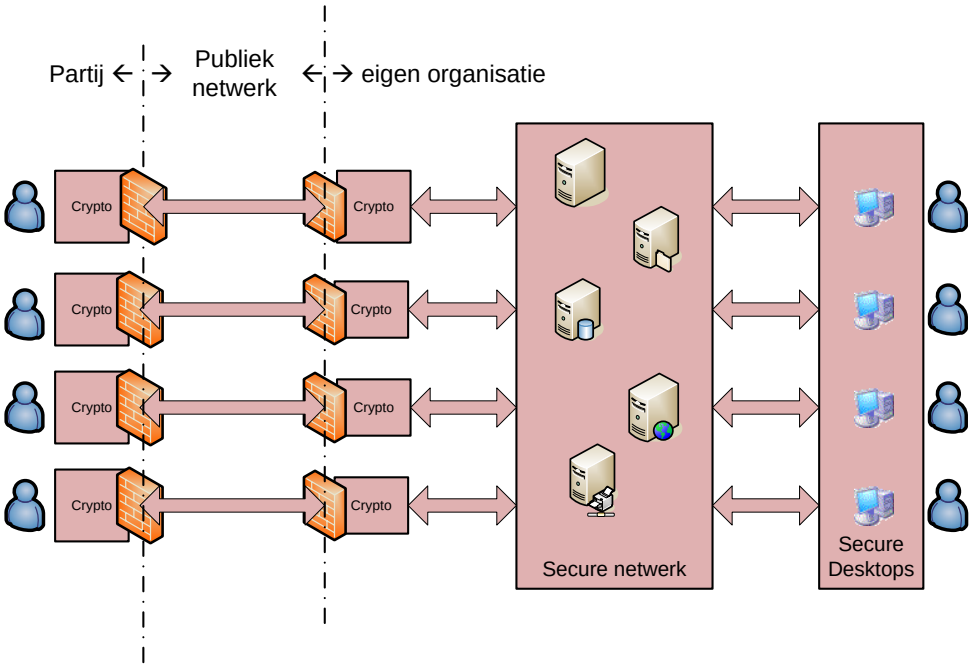
Figuur 20: Ontwerp voor informatiestromen uit de categorie Open Informatie

Vertrouwen

In het ontwerp voor de informatie uit de categorie “Vertrouwen” is het van belang dat samen met de partner een manier wordt gevonden om samen op veilige wijze hooggerubriceerde informatie uit te wisselen.

De daadwerkelijke informatiestroom kan over een publiek netwerk plaatsvinden. In dat geval dient goedgekeurde cryptografie ingezet te worden.

Er zijn twee belangrijke pijlers in dit ontwerp. Ten eerste dienen de informatiestromen tussen de verschillende partners geïsoleerd blijven. Ten tweede dient de fysieke beveiliging van de locatie te voldoen aan de eisen die het Vir-bi aan het werken met de informatie van die rubricering stelt.

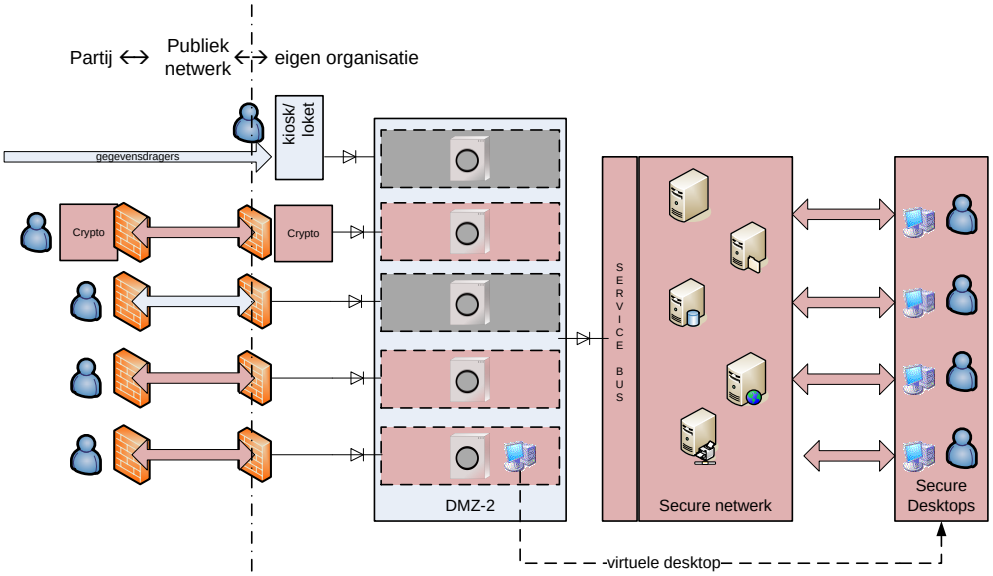


Figuur 21: Ontwerp voor informatiestromen uit de categorie Vertrouwen

Input Only

In dit informatiedomein kan zowel gerubriceerde als ongerubriceerde informatie verwerkt worden. Per informatiestroom kan in dit domein virtuele (stippellijn in het ontwerp) "hardware" draaien die de cleaning uitvoert. Hierbij valt te denken aan virusscanners en convertors.

Daarnaast is het mogelijk, maar niet verplicht, via een virtuele desktop (zichtbaar gemaakt op het rode desktop netwerk) handmatig informatie te filteren. De service bus routeert informatie tussen de losse netwerksegmenten in "schoon netwerk" en de applicaties op het rode netwerk, maar alleen als de informatie eenrichtingsverkeer is, door een diode afgedwongen.

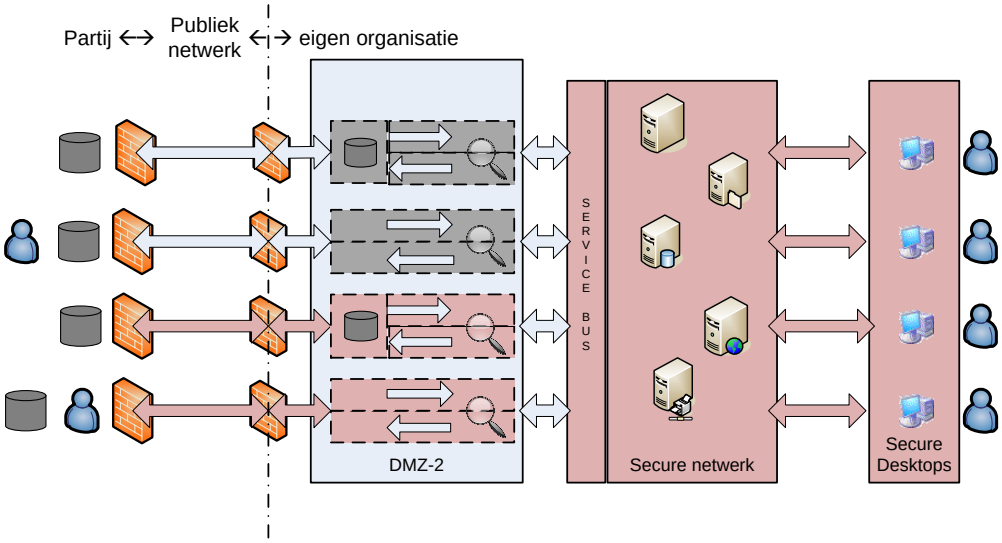


Figuur 22: Ontwerp voor informatiestromen uit de categorie Input Only

Tot slot is in dit ontwerp te zien dat er voor het importeren van losse media een apart loket wordt opgezet dat aansluit op één specifieke wasstraat en waarna de informatie het gewone proces doorloopt.

vraag-antwoord

Het ontwerp van de categorie "vraag-antwoord" toont veel gelijkenissen met het ontwerp voor "Input Only". Waar er voor de laatste een speciaal informatiedomein "schoon netwerk" ingezet is, kent deze categorie een Demilitarized zone (dmz). Het verschil is de 2-weg communicatie die hier mogelijk is.



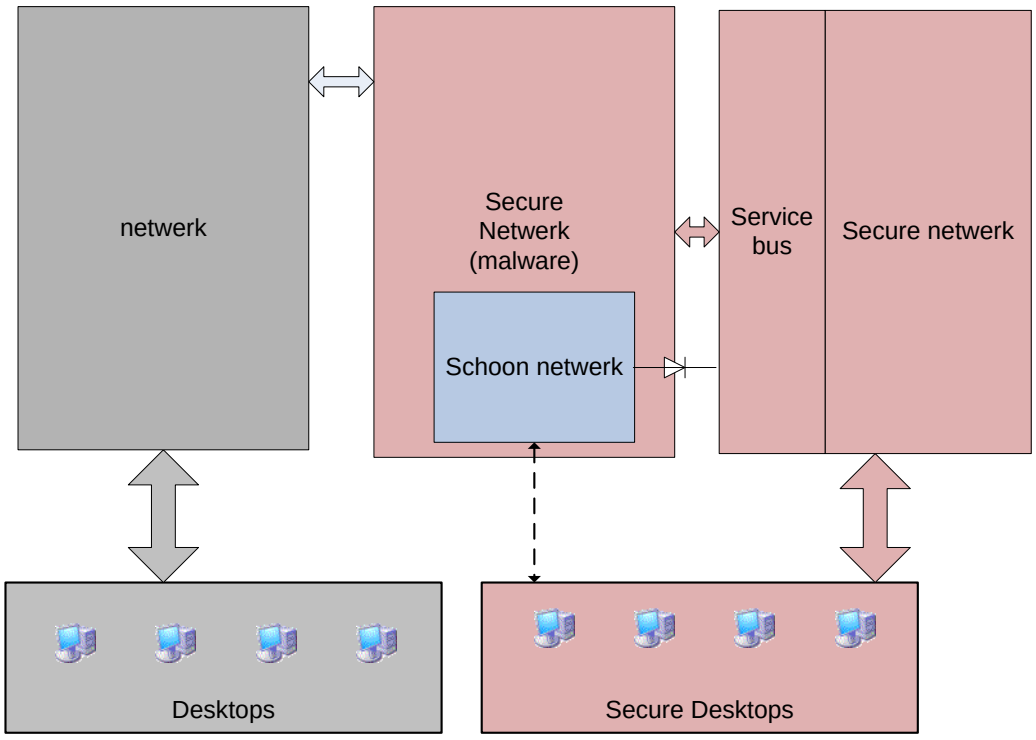
Figuur 23: Ontwerp voor informatiestromen uit de categorie Vraag-Antwoord

Maatwerk

Alle informatiestromen die niet binnen een van bovengenoemde categorieën vallen hebben specifieke maatregelen nodig. Er is naar gestreefd om een dusdanige verdeling van categorieën te maken dat zo min mogelijk bestaande informatiestromen een maatwerkoplossing nodig hebben. Veel van de koppelingen die direct ondersteunen aan operationele werkzaamheden vallen in deze categorie.

Samenhang tussen informatiedomeinen

De vorige paragrafen bevatten een aantal nieuwe informatiedomeinen. De koppelingen tussen deze informatiedomeinen zijn zelf ook weer informatiestromen. Dit is weergegeven in het onderstaande ontwerp. In dit ontwerp zijn virtuele desktops opgenomen met een gestippelde lijn. Het middelste secure netwerk kan malware bevatten (vuile data).



Figuur 24: Samenhang tussen de informatie categorieën

Processen en meetbaarheid

Alle overige meetgegevens zullen afkomstig moeten zijn van indirecte security management processen die worden gebruikt bij de implementatie van deze architectuur. Het gaat dan om de volgende processen:

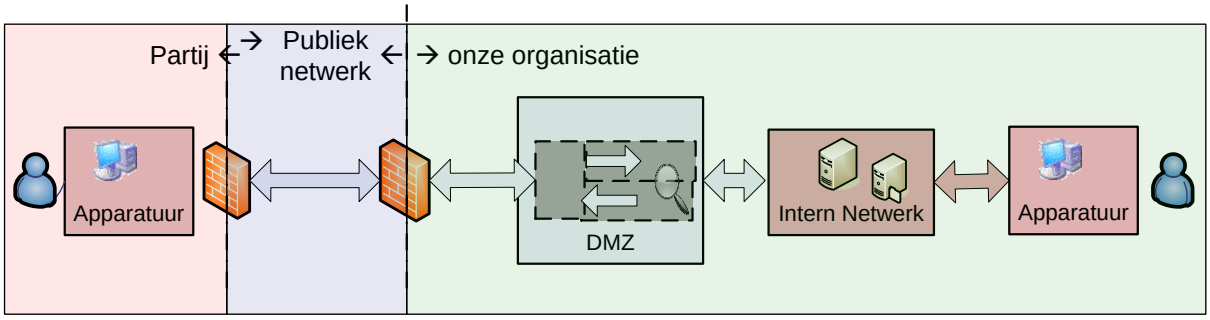
Process	ID
Define Security Targets & Security Objectives	TSP-14
Inventory management	OSP-3
IS change control	OSP-4
Managed domain hardening	OSP-7
Segmentation and Filtering management	OSP-16
Malware protection management	OSP-17
Access Control	OSP-11
Phisical Environment Protection	OSP-14
Alerts monitoring	OSP-22
Handling of (near)incidents	OSP-24

Risicoanalyse

Model van een informatiestroom

De informatie waar het hier over gaat bevindt zich niet per definitie binnen grenzen die wij zelf controleren. De scope is het *domein* waarbinnen deze informatie zich beweegt. Dat is dus niet alleen het interne netwerk waarop de informatie zich bevindt of de geografische grenzen die we stellen aan locaties. Het is inclusief het punt waar de informatie de communicatie infrastructuur betreedt (het endpoint). Voorbeeld hiervan is een crypto telefoon.

Om de beveiligingsaspecten te verduidelijken is een model (een –voor dit doel- vereenvoudigde afspiegeling van de werkelijkheid) gemaakt[6]. Hieronder volgt een korte beschrijving van dit model, waarna een toelichting wordt gegeven op de beveiligingsrelevante kenmerken die hierop van toepassing zijn.



Figuur 25: Algemeen model van een informatiekoppeling

Partij
De partij is de actor waarmee informatie wordt uitgewisseld. Hiervoor zijn meestal afspraken in een bepaalde vorm gemaakt. Er is zeer veel diversiteit in oplossingen, dit varieert van convenanten met vaste lijnverbindingen tot incidentele (ad-hoc) afspraken voor levering van informatie op losse gegevensdragers.

Er is apparatuur die wordt gebruikt voor gegevensopslag en communicatie van deze informatie. De infrastructuur hiervoor bevindt zich in een bepaalde context. Geografische locatie, staat van fysieke beveiliging van de locatie, de mate waarin wij zelf in staat zijn deze te beïnvloeden of te controleren, de beveiliging van de apparatuur, de mate waarin wij in staat zijn de beveiliging van de apparatuur te beïnvloeden of te controleren zijn voorbeelden beveiligingsaspecten waarmee rekening gehouden moet worden.

Publiek netwerk
Het type netwerk dat wordt gebruikt om een koppeling met een actor tot stand te brengen: een gegevensdrager (CD), een plain old telephone system (POTS) verbinding (deze heeft als kenmerk dat er alleen een verbinding aanwezig is als er gecommuniceerd wordt), een speciale point to point verbinding (vaste lijn), gedeelde netwerk infrastructuur (netwerk provider) of open netwerken (Internet).

Eigen Infrastructuur
De informatie die binnenkomt wordt opgevangen in een DMZ (demilitarized zone). Beveiligingsaspecten die relevant zijn voor de beveiliging van de DMZ zijn de wijze van aanleveren, de vraag of de informatie voorbewerkt moet worden om opgenomen te kunnen worden in de informatievoorziening en enkele specifieke kwaliteitskenmerken aan de informatie zoals de mogelijke aanwezigheid van malware en de integriteit van de gegevens.

In de DMZ vindt soms opslag van de data plaats, kan geautomatiseerde- of handmatige verrijking plaatsvinden, wordt informatie geschoond zodat de integriteit van de gegevens voldoende gewaarborgd is en vindt bij voorkeur geautomatiseerd transport plaats naar het informatiesysteem op het interne netwerk.

[6] Dit model wordt ook gehanteerd binnen de NORA

Beveiligingsrelevante factoren aan informatie

De informatiestromen zijn geïnventariseerd. Hierop is een analyse uitgevoerd waarin is bepaald welke kenmerken aan de informatie en zijn omgeving relevant zijn om rekening mee te houden. Een aantal van deze eigenschappen worden gebruikt in de beveiligingsarchitectuur voor informatiestromen om te kunnen bepalen in welke categorie een informatiebron valt. De overige factoren zijn natuurlijk ook relevant (er gaat een bepaalde dreiging vanuit) en moeten daarom worden toegepast in de technische ontwerpen voor de categorieën. De volgende lijst met eigenschappen is relevant bevonden:

	Eigenschap	Omschrijving
1	Controleerbaarheid	De mate waarin wijzelf de mogelijkheid hebben de omgeving bij de derde partij te controleren of daar invloed op uit te oefenen.
2	Vertrouwen Externe partij	Vertrouwen in de "Mens" aan de andere kant van de informatiestroom/Bron/verbinding is bepalend voor het vertrouwen dat wij stellen in de informatie die binnen komt.
3	Rubricering	Inschatting van de schade aan de Staat der Nederlanden
4	Inhoud informatie is verifieerbaar	Informatie juiste en tijdig? Bevat het mogelijk virussen of andere ongewenste artefacten? Zijn er afspraken met de leverende partij op dit gebied?
5	Gerichte zoekvraag aan de buitenwereld	Is een specifieke zoekvraag ook een vraag in een systeem buiten de deur
6	Gebruik van draadloos of publiek domein	Het type netwerk dat wordt gebruikt om de koppeling tot stand te brengen.
7	Verrijking van gegevens	Menselijke handelingen en/of geautomatiseerde verwerking van gegevens voordat er sprake is van geduide informatie
8	Geografische locatie	De fysieke locatie van het eindpunt van de koppeling
9	Mate van isolatie van de bron	Er is een belang bij om de informatie afkomstig van bepaalde partijen strikt gescheiden te houden van elkaar.
10	Import en/of Export van informatie	(Menselijke) Interventiedreiging Controleerbaarheid (weten wat de I/O is);

In de architectuur voor informatiestromen zijn de primaire kenmerken (1 t/m 5) bepalend voor de categorie indeling. De overige kenmerken moeten worden gebruikt bij het opzetten van de architectuurkaders die de technische inrichting van de categorieën bepalen.

Dreigingsbeeld voor informatiestromen

De aansluitcategorieën zijn:

Open Informatie.....: ◇
Vertrouwen.....: ◇
Input Only .....: ◇
Vraag-Antwoord .....: ◇
Maatwerk.....: ◇

Op basis van de dreigingen met bijbehorende beschrijvingen en de architectuurbeschrijving van de aansluitcategorieën is een risico inschatting gemaakt. Het gaat hierbij om een inschatting van het risico van een dreiging *zonder* dat er beveiligingsmaatregelen genomen zijn.

Dreiging	inschatting			
	Hoog	Gemiddeld	laag	Zeer laag
Afluisteren van binnenuit		◇ ◇	◇ ◇	◇
Afluisteren van buitenaf d.m.v. doorbreken van encryptie				◇ ◇ ◇ ◇ ◇
Afluisteren van buitenaf d.m.v. grootschalig onderscheppen		◇ ◇ ◇ ◇ ◇		
Afluisteren van buitenaf d.m.v. ICT-sniffing		◇	◇ ◇ ◇	◇
Afluisteren van buitenaf d.m.v. onderscheppen van berichtenverkeer			◇ ◇ ◇ ◇ ◇	
Afluisteren van buitenaf d.m.v. opvangen/meelezen van straling		◇ ◇ ◇ ◇ ◇		
Chantage	◇ ◇ ◇ ◇			◇

Compromitteren informatie, bewust	◇◇◇◇◇			
Compromitteren informatie, onbewust	◇◇◇◇◇			
Corruptie		◇◇◇◇◇		
Diefstal	◇◇	◇	◇◇	
Hacking gericht	◇◇◇◇			◇
Hacking ongericht	◇	◇◇◇	◇	
Misbruik van bedrijfsmiddelen		◇◇◇◇		◇
Ongeautoriseerde toegang tot systemen	◇◇◇◇◇			
Onopzettelijk verstoren van processen	◇◇	◇◇◇		
Opzettelijk verstoren van processen	◇◇◇◇◇			
Sabotage				◇◇◇◇◇

Figuur 26: Dreigingsbeeld voor Informatiestromen

Dit zijn de globale risico's waartegen de informatiestromen moeten worden beveiligd. Met behulp van de dreigingsmatrix in bijlage F (deze bevat een meer expliciet gemaakte lijst van dreigingen) kan duidelijk worden of de in het technisch ontwerp genomen maatregelen de dreigingen afdekken. Zo worden uiteindelijk restrisico's van de oplossing benoemd.

D. Bijlage Principes per aansluitcategorie informatiestromen

INFSTR.5	**Categorie ZG**
Statement	Alle Stg. Zeer Geheime en gelijkwaardig gerubriceerde informatie valt onder het architectuurbeleid van ZG
Rationale	Stg. Zeer Geheime informatie is informatie die de staat zeer ernstige schade toebrengt bij uitlekken. Als zodanig is er een zwaar palet aan maatregelen opgelegd voor het verwerken van dergelijke informatie. Het delen van stg. Zeer Geheime informatie met internationale mogendheden geeft daarnaast nog een grote set aan externe regelgeving waaraan voldaan dient te worden. Deze hoge mate van exclusiviteit zorgt er voor dat er een eigen regime en dus categorie moet gelden voor dit type informatie.
Implicaties	Geautomatiseerde koppeling van lager gerubriceerde informatie met deze categorie zou betekenen dat een veel grotere set aan informatie (bijvoorbeeld stg. Zeer Geheim en stg. Geheim) dezelfde ZG-maatregelen moeten worden toegepast. Door de hoge kosten verbonden aan omgaan met deze informatie, kan voor deze categorie dus **niet** voldaan worden aan *INFSTR.1: Eén huishouding van informatie*.

INFSTR.6	**Categorie Open informatie**
Statement	Alle uitwisseling van ongerubriceerde gegevens, waarbij geen informatie wordt weggegeven valt onder het architectuurbeleid van "Open informatie".
Rationale	Goede informatiebeveiliging is kostbaar en geheimhouding vergt goede afstemming met de partijen waar informatie mee wordt uitgewisseld. Het ligt dus voor de hand met open vizier en rijksbrede oplossingen naar buiten te treden als dit kan. Deze categorie is hier voor bedoeld. Naast het bieden van bv. standaard internetmogelijkheden voor medewerkers kunnen via deze categorie open bronnen worden geraadpleegd. Uiteraard alleen indien dit niet gebeurt door het uitvragen van gerubriceerde gegevens of andere karakteriseringen van de informatievoorziening weggegeven.
Implicaties	Er moet onderscheid gemaakt worden tussen operationeel en niet-operationeel gebruik van bronnen. In sommige gevallen is een individuele bevraging van een bron niet direct herleidbaar tot de organisatie, maar een hele set aan bevragingen wel. Indien bijvoorbeeld één medewerker om 17:00 de neerslagkaart opvraagt leidt dit niet tot verdenking, als honderden dit doen wel. Regelgeving is dus noodzakelijk omdat menselijk handelen op detailniveau het verschil kan maken.

INFSTR.6	**Categorie Vertrouwen**
Statement	Alle gerubriceerde informatie uitgewisseld met een betrouwbare partner, die bereid is beveiligingsmaatregelen volledig te implementeren valt onder het architectuurbeleid van "Vertrouwen".
Rationale	Er is een goede ketensamenwerking tussen de partners in de veiligheidsketen. Een groot deel van de beveiligingsnormen die de rijksoverheid hanteert worden erkend en gehanteerd door deze partijen. Dit maakt uitwisseling van gegevens met deze partijen eenvoudiger dan met bijvoorbeeld commerciële partijen. Indien er informatie moet worden uitgewisseld met een externe locatie en deze locatie voldoet aan alle maatregelen waaraan gebouwen

	voldoen én de koppeling gebruikt encryptie apparatuur, goedgekeurd tot het rubriceringsniveau van de uitgewisselde informatie, is er geen reden om deze partner niet direct te koppelen.
Implicaties	Een implicatie van het koppelen van andere locaties met het eigen netwerk is dat het eigen netwerk groter en meer complex wordt. Dit betekent dat op het interne netwerk een zwaarder beveiligingsniveau noodzakelijk is. Zo moet er bijvoorbeeld meer worden geïnvesteerd in defense in depth, zowel op technologisch vlak als in de bijbehorende security management-processen.

INFSTR.5	**Categorie Input Only**
Statement	Alle niet verifieerbare informatie met/of zonder rubricering die richting de organisatie komt valt onder het architectuurbeleid van "Input Only".
Rationale	Het restrisico is het op enigerlei wijze besmetten en/of vernietigen van informatie door de binnengehaalde data. Denk hierbij aan malware en/of onjuiste of te grote hoeveelheden data (Denial of Service attack). Er zijn veel technische middelen op de markt om dit risico te verkleinen. Daarnaast kan het handmatig selecteren van de gewenste gegevens uit de gehele set het risico verkleinen.
Implicaties	Er dient een zone te komen die robuust is tegen het mogelijk optreden van de bovengenoemde risico's zonder dat het primaire informatiedomein wordt aangetast.

INFSTR.5	**Categorie vraag-antwoord**
Statement	Alle gerubriceerde informatie die volledig verifieerbaar en controleerbaar naar binnen komt op basis van een vraag die buiten de eigen infrastructuur wordt gesteld, valt onder het architectuurbeleid van "vraag-antwoord".
Rationale	In de vraag-antwoord categorie zit een vorm van tweeslachtigheid. Aan de ene kant wil men graag informatie uitwisselen, aan de andere kant is er óf geen volledige vertrouwen in de andere partij óf moet informatie worden weggegeven om relevante informatie terug te krijgen. Een duidelijk voorbeeld bij deze categorie betreft het extern stellen van een zoekvraag op een extern beschikbare bron (dus op de locatie van de andere partij). Aangezien het uitwisselen van gerubriceerde gegevens niet zonder meer past binnen de geldende beveiligingskaders is het tweerichtingsverkeer van informatie hier beperkt tot stromen waarvan de verifieerbaarheid van de informatie hoog is. Onder de verifieerbaarheid wordt verstaan: tot op het laagste niveau is controleerbaar welke informatie er wordt uitgewisseld.
Implicaties	Omdat onder deze categorie een groot en divers gezelschap van partijen en informatietypes valt zal er minder kunnen worden teruggevallen op standaardoplossingen. De ontwerpbeslissingen bij deze categorie zullen dus vooral beveiligingsvoorwaarden bevatten. Alle informatie van een technisch ongestructureerd karakter, zoals willekeurige documenten of media-fragmenten vallen niet in deze categorie. Er dient een zone te komen die optreden van de bovengenoemde risico's minimaliseert zonder dat het primaire informatiedomein wordt aangetast

ZG.1	**Er is geen informatiestroom van of naar categorie "Top Secret"**
Statement	Er is geen geautomatiseerde informatiestroom voor stg. Zeer Geheime informatie.

Rationale	Alle informatie die zich bevindt in een Zeer Geheim compartiment is daar geproduceerd en blijft daar gestationeerd.
Implicaties	Ø

ZG.2	**ZG informatie wordt fysiek gescheiden**
Statement	ZG informatie wordt altijd gescheiden van andere informatie door geheel fysieke scheiding.
Rationale	Dit vloeit voor uit het Vir-bi. Hierin staat dat stg. Zeer Geheime informatie geen netwerk koppeling mag hebben.
Implicaties	Ø

Open info.1	**Verkeer vanaf internet naar organisaties is niet als zodanig herkenbaar**
Statement	Het ontwerp voor het "Open informatie"-domein is zodanig opgezet dat niet rechtstreeks te herleiden is waar dit verkeer van afkomstig is.
Rationale	Opereren op internet brengt risico's met zich mee op het gebied van weggeven van modus operandi. Dergelijke oplossingen vallen onder de maatwerkcategorie. In een groot deel van de processen die internet raken kan echter eenvoudiger worden voorzien, nl. onder alias.
Implicaties	Er dient een maatwerkoplossing te zijn voor het opereren op internet.

Vertrouwen.1	**Communicatie met de vertrouwde partij is geïsoleerd**
Statement	Communicatie met de vertrouwde partij dient te geïsoleerd te worden van communicatie met andere partijen.
Rationale	Het vertrouwen dat partijen in elkaar uitspreken gaat niet verder dan die onderlinge relatie. In het ontwerp van de communicatie met andere partijen betekent dit dat isolatie onderling vorm gegeven zal moeten worden. .
Implicaties	Tot het moment dat de informatiestroom op het rode netwerk komt, dient de informatiestroom gescheiden te worden van informatiestroom met anderen.

Vertrouwen.2	**Het niveau van fysieke beveilig dient gelijkwaardig te zijn aan dat van de benodigde informatiebeveiliging**
Statement	Het niveau van fysieke beveilig dient gelijkwaardig te zijn aan dat van de benodigde informatiebeveiliging.
Rationale	Het Vir-Bi gaat vooral uit van beveiligingsmaatregelen op basis van de rubcricering van de gegevens. Dit wordt zowel in fysieke zin als in logische (informatiebeveiligings-)zin uitgelegd. Door dit als architectuurprincipe mee te nemen, worden maatregelen vereenvoudigd. Het doortrekken van het gewenste beveiligingsniveau naar de partij waar informatie mee wordt uitgewisseld biedt tevens voordeel voor het uitwisselen van informatie in twee richtingen. Het is gemakkelijk interne informatie, zoals zoekvragen, naar een andere partij te sturen als het niveau van de beveiliging gewaarborgd is. Dit geldt zowel voor fysieke-, technische- procedurele als organisatorische maatregelen.
Implicaties	Een deel van het beheer van het uitwisselingsysteem, ook bij de partner, zal voor onze rekening komen om één niveau van beveiliging te waarborgen.

Input Only.1	**Technisch afdwingen van éénrichtingsverkeer**
Statement	In de categorie "Input Only" wordt d.m.v. een diode altijd technisch afgedwongen dat informatie alleen richting de organisatie gaat.
Rationale	Het intern ontsluiten van willekeurige data is tegelijkertijd nuttig en risicovol. Risico's zoals malware kunnen voor een deel ondervangen worden door geforceerd eenrichtingsverkeer af te dwingen.

Implicaties	Informatie in deze categorie kan alleen gebruikt worden om te zoeken wanneer deze informatie intern beschikbaar is gemaakt.

Input Only.2	**Vastgestelde cleaningsmaatregelen met risico-analyse**
Statement	Per informatiestroom in de categorie "Input Only" dienen vastgestelde cleaningsmaatregelen te worden ingezet en het gebruik hiervan dient te worden voorzien van een risicoanalyse voor de betreffende informatiestroom.
Rationale	Er zijn diverse mogelijkheden om virussen, trojans en kwaadwillende scripts te verminderen, maar deze zijn uiteenlopend van aard. Een juiste mix van maatregelen vraagt om een specifieke afweging. In deze categorie bevinden zich informatiestromen bestaande uit een grote bulk van ongestructureerde gegevens. Een van de mogelijke maatregelen is het handmatig filteren van deze stromen en enkel de van belang zijnde elementen door te sluizen naar het primaire informatiedomein.
Implicaties	Er is een verbinding noodzakelijk van een desktop naar het domein waarin de informatie opgeschoond wordt om handmatig te kunnen filteren.

vraag-antw.1	**Vastgestelde controlemaatregelen met risico-analyse**
Statement	Per informatiestroom in de categorie "vraag-antwoord" dienen vastgestelde controlemaatregelen te worden ingezet en het gebruik hiervan dient te worden voorzien van een risicoanalyse voor de betreffende informatiestroom.
Rationale	Er zijn diverse mogelijkheden om te controleren dat bepaalde informatie die wordt uitgewisseld ook de bedoelde informatie is. Er is een breed scala aan mogelijkheden om dit af te dwingen, elk met een eigen risicoprofiel.
Implicaties	Geen.

vraag-antw.2	**Bevraging kan binnen en buiten plaatsvinden**
Statement	Voor informatiestromen in de categorie "vraag-antwoord" kan de betreffende bron zowel binnen als buiten de organisatie staan.
Rationale	Bij het uitwisselen van informatie spelen vaak uiteenlopende belangen. Het is niet altijd mogelijk om een externe databron waar informatie uit gehaald moet worden binnen te plaatsten. De categorie "vraag-antwoord" is bij uitstek de categorie waar informatiestromen worden geplaatst waar naar de belangen van beide partijen gekeken wordt.
Implicaties	Informatiestromen uit deze categorie vergen uitgebreide afspraken, bijvoorbeeld in de vorm van een convenant, met de andere partij.

vraag-antw E.3	**Logging van zoekvragen en antwoorden**
Statement	Informatiestromen in de categorie "vraag-antwoord" bevatten zoekvragen en antwoorden waarvan een audittrail dient te worden vastgelegd.
Rationale	Informatiestromen die via de categorie "vraag-antwoord" worden ontsloten leveren een reeds geduid antwoord op een vraag. Eventuele verwerkingen op deze geduide informatie dient geautomatiseerd plaats te vinden, zonder interventie van eindgebruikers zodat een audittrail ontstaat.
Implicaties	Alleen geautomatiseerde verwerking van reeds geduide gegevens en ontsluiting hiervan op het Rode netwerk.

E. Bijlage dreigingscenario's

Dreiging	Exclusiviteit	Integriteit	Beschikbaarheid
afluisteren	Plaatsen van afluisterapparatuur t.b.v. meeluisteren door derden		
afluisteren	Kopieren van informatiedragers		
afluisteren	Gebruik maken van bestaande tekortkomingen in het systeem (zowel hard als software)		
afluisteren	Installeren van software t.b.v. het meeluisteren door derden		
afluisteren	Kraken encryptie: - Brute force - Gebruik van back doors - Plaatsen van back doors - Diefstal van sleutels		
afluisteren	Opstellen luisterstations en filtering, maar dan op een (grotere) schaalgrootte en het bereik van het afluisterdomein (publiek netwerk of KPN-wolk, point to point)		
afluisteren	Plaatsen van afluisterapparatuur t.b.v. meeluisteren door derden		
afluisteren	Opgraven van kabels in de omgeving van het object		
afluisteren	Tempestdreigingen		
data leakage	Transport van gegevens naar buiten niet regulier traceerbare activiteit (b.v. fysieke gegevens dragers)		
data leakage	Transport van gegevens naar buiten regulier traceerbaar		
data leakage	Diefstal van Hardware (b.v. netwerkapparatuur, Sinabox, servers, etc)		Diefstal van Hardware
hacking	Niet op elkaar afgestemde beveiligingsmaatregelen		
hacking	Gebruik maken van bestaande tekortkomingen in het systeem (zowel hard als software)	Het ongeautoriseerd aanpassen van gegevens	Door het moedwillig vernietigen van gegevens en eventueel de hardware en software
misbruik van bedrijfsmiddelen	Gebruik van informatie voor eigen doeleinden (bijbehorende maatregel is b.v. logging of toegangscontrole		Verstoren van de bedrijfsprocessen door intern misbruik
ongeautoriseerde toegang tot systemen	Gebruik maken van bestaande tekortkomingen in het systeem (zowel hard als software)		
ongeautoriseerde toegang tot systemen	Niet correct op elkaar afgestemde beveiligingsmaatregelen		
verstoren processen	Verstoren van processen of systemen	Fouten in de data of de samenhang tussen gegevens	
sabotage	Destructie van hardware		
Fysieke schade			Schade door - brand (vuur) - Waterschade - Schade door vervuiling - Schade door grote ongevallen (b.v. er valt een Boeing op je dak) - Vernietiging van apparatuur of media - stof, corrosie of bevriezing

Natuurrampen			Schade door: - Klimaatverschijnselen (b.v. periode van droogte, - periode van koude, periode van hitte) - Aardbevingen - Vulkaanuitbarstingen - Weerkundige verschijnselen (b.v. bliksem, hagel) - Overstromingen
Verstoringen als gevolg van straling			- Elektromagnetische straling - Warmte/hitte-straling - Elektromagnetische impulsen
Uitval van essentiële verzieningen			- Uitvallen van de luchtbehandeling of watervoorziening - Uitvallen van de stroomvoorziening - Uitvallen van telecommunicatieapparatuur
Compromitteren van informatie	- Onderscheppen van compromitterende interferende signalen (overspraak tussen verbindingen, b.v. overspraak tussen het rode en het zwarte netwerk) - Op afstand vergaren van informatie (bespieden) - Afluisteren - Diefstal van media (informatiedragers) of documenten Diefstal van apparatuur - Terugwinning van informatie vanaf afgedankte of weer bruikbaar gemaakte media - Onthulling of openbaarmaking van informatie - Data van onbetrouwbare bronnen		- Knoeien met hardware - Knoeien met software
Technisch falen	- Overbelasting van het informatiesysteem - Software storing	Software storing	- Uitval van apparatuur - Storing in apparatuur - Overbelasting van het informatiesysteem - Software storing - Nalatigheid in het onderhoud (of niet uitvoeren - D8 van onderhoud) van informatiesystemen
Onbevoegde en ongeoorloofde handelingen	- Onbevoegd gebruik van apparatuur - Frauduleus kopiëren van software - gebruik van nagemaakte/vervalste of gekopieerde software	Beschadiging van data	
Verstoren van processen (functies)	Misbruik van rechten	Fouten tijdens het gebruik Vervalsen van rechten Stilleggen van handelingen Gebrek aan beschikbaar personeel	Stilleggen van handelingen Gebrek aan beschikbaar personeel