3.3

Waarde van ‘sturen op samenhang’ via recursiviteit en projectie

Roel Wagter, Dirk Witte en Leon van der Valk

Samenvatting

In deze bijdrage gaan wij in op de waarde van ‘sturen op samenhang’. We laten zien dat deze waarde zowel tot uitdrukking komt op het overkoepelende bedrijfsniveau, als op en tussen hiërarchisch lagere besturingsniveaus, als in allianties waar de enterprise deel van uitmaakt.

In onze visie leidt ‘sturen op samenhang’ in organisaties tot betere prestaties [9]. Wij zien enterprisearchitectuur (EA) als een instrument dat bij uitstek geschikt is om ‘sturen op samenhang’ inhoud te geven. Diverse onderzoeken hebben echter geleerd dat het in vele organisaties schort aan ‘sturen op samenhang’ [10, 15]. Dit betekent dat organisaties een enorme potentie onbenut laten. Wij zoeken hiervoor een uitweg door onszelf de vraag te stellen: hoe kan sturen op samenhang in organisaties, inclusief hun samenwerkingsverbanden, worden verbeterd? Hierbij denken wij aan vragen als: hoe kunnen onze nieuwste inzichten op het gebied van EA worden toegepast op meerdere niveaus binnen een organisatie om verticale samenhang te bevorderen? Maar ook: hoe te sturen op samenhang tussen een holding en daaronder sorterende divisies? En: hoe te sturen op samenhang in het geval van (out)sourcing c.q. de vorming van strategische allianties? En ook: hoe te sturen op horizontale (procesgerichte) samenwerking (tussen businessunits of op basis van ketenintegratie)?

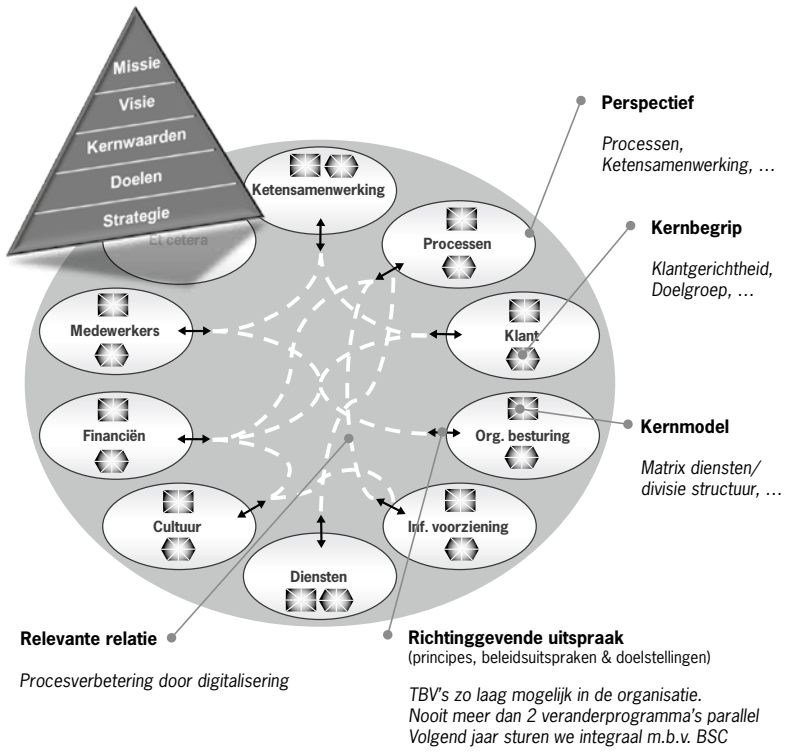
Wij hopen met deze bijdrage een aantal handvatten aan te reiken die leiden tot nieuwe inzichten en hopelijk vele zinvolle discussies. Dit om met elkaar ons mooie vakgebied weer een stukje verder te brengen.

Sturen op samenhang nader toegelicht

Onze visie op EA

4 Onze visie op EA [9] is ontwikkeld door een innovatieplatform van deelnemende partijen [16]. Aan dit platform nemen vele partijen deel uit de overheid, het bedrijfsleven en de wetenschap.

De kernboodschap van onze visie op EA luidt: 'Een betere samenhang leidt tot betere prestaties.' Dit inzicht heeft ertoe geleid om voor onze benadering van EA de subtitel 'sturen op samenhang' te introduceren. Met behulp van EA is een organisatie in staat de samenhang van de organisatie expliciet en daarmee bestuurbaar te maken. Het expliciet maken van de samenhang gebeurt door middel van het afleiden en definiëren van de elementen van samenhang die kenmerkend zijn voor een specifieke organisatie. Het 'sturen op samenhang' gebeurt door deze expliciet gemaakte samenhang toe te passen in het ontwikkelen van integrale oplossingsrichtingen en aanpakkeuzes voor belangrijke bedrijfsvraagstukken. EA onderkent twee onderling verbonden niveaus van samenhang: het niveau van zingeving en het niveau van vormgeving. Op het niveau van zingeving zijn de elementen van samenhang: missie, visie, kernwaarden, doelen en strategie [2, 6, 7, 8]. Op het niveau van vormgeving zijn de elementen van samenhang: perspectieven, kernbegrippen, richtinggevende uitspraken, kernmodellen en relevante relaties (zie figuur 1) [9, 11].



Figuur 1. Elementen van samenhang

Wij gaan ervan uit dat voornoemde elementen van samenhang op het niveau van zingeving bekende begrippen zijn. Hierna volgt een korte toelichting op de elementen van samenhang op het niveau van vormgeving:

- *Perspectief*
  Een invalshoek van waaruit men een organisatie wenst te beschouwen én waarop men wenst te sturen. Bijvoorbeeld: Processen, Medewerkers, Ketenintegratie, Marketing, Strategische alliantie.
- *Kernbegrip*
  Een invalshoek van waaruit men een perspectief wil beschouwen en waarop men wenst te sturen. Voorbeelden van kernbegrippen binnen een perspectief Financiën zijn: Financiering, Budgetting.
- *Kernmodel*
  Een representatie van een of meer perspectieven. Voorbeeld van een kernmodel is een representatie van het perspectief Processen door middel van bijvoorbeeld een value chain van Porter.
- *Richtinggevende uitspraak*
  Een binnen een organisatie uitgesproken en vastgelegd statement dat richting geeft aan gewenst gedrag. Voorbeeld: 'Met ingang van het volgende kwartaal gaan wij over tot klantgerichtheid.'
- *Relevante relatie*
  Een relatie waarmee het verband tussen twee perspectieven wordt beschreven. Voorbeeld van een verband tussen de perspectieven Acquisitie (van organisaties) en Kennis: 'Wij innoveren onze speerpunten van dienstverlening door het kopen van kennisconcepten.'

Aanpak om te komen tot elementen van samenhang

Nadat aan de elementen op het niveau van zingeving inhoud is gegeven door deze op te halen uit de organisatie, wordt uit het niveau van de zingeving de inhoud van de elementen op het niveau van vormgeving afgeleid, zoals richtinggevende uitspraken. Vervolgens worden deze aangevuld met richtinggevende kaders die alleen op het niveau van vormgeving spelen. Praktijkervaringen hebben ons geleerd dat bij de grotere organisaties (meer dan 1000 medewerkers) het aantal richtinggevende uitspraken ligt tussen de 150 en 250. Deze set van uitspraken wordt in nauwe samenwerking met belangrijke representanten van de organisatie getoetst op actualiteit en importantie in besluitvormingsprocessen. De richtinggevende uitspraken worden vervolgens gekoppeld aan de perspectieven waarop ze in hoofdzaak van toepassing zijn (zie figuur 1). Voor een toelichting op de overige elementen van samenhang verwijzen wij naar het boek *Sturen op samenhang op basis van GEA* [9].

Sturen op samenhang

Nadat alle elementen van samenhang zijn bepaald, wordt dit samenhangende stelsel gebruikt om integrale oplossingsrichtingen en aanpakkeuzes voor belangrijke bedrijfsvraagstukken te ontwikkelen [12, 14]. Hiertoe wordt een bedrijfsvraagstuk als het ware midden in de 'EA-vijver' geplonsd en worden twee analyses uitgevoerd. Wat is de impact van het vraagstuk op de perspectieven? En wat zijn de (on)mogelijkheden beredeneerd vanuit de perspectieven naar het vraagstuk toe, de oplossingsruimte? De synthese van

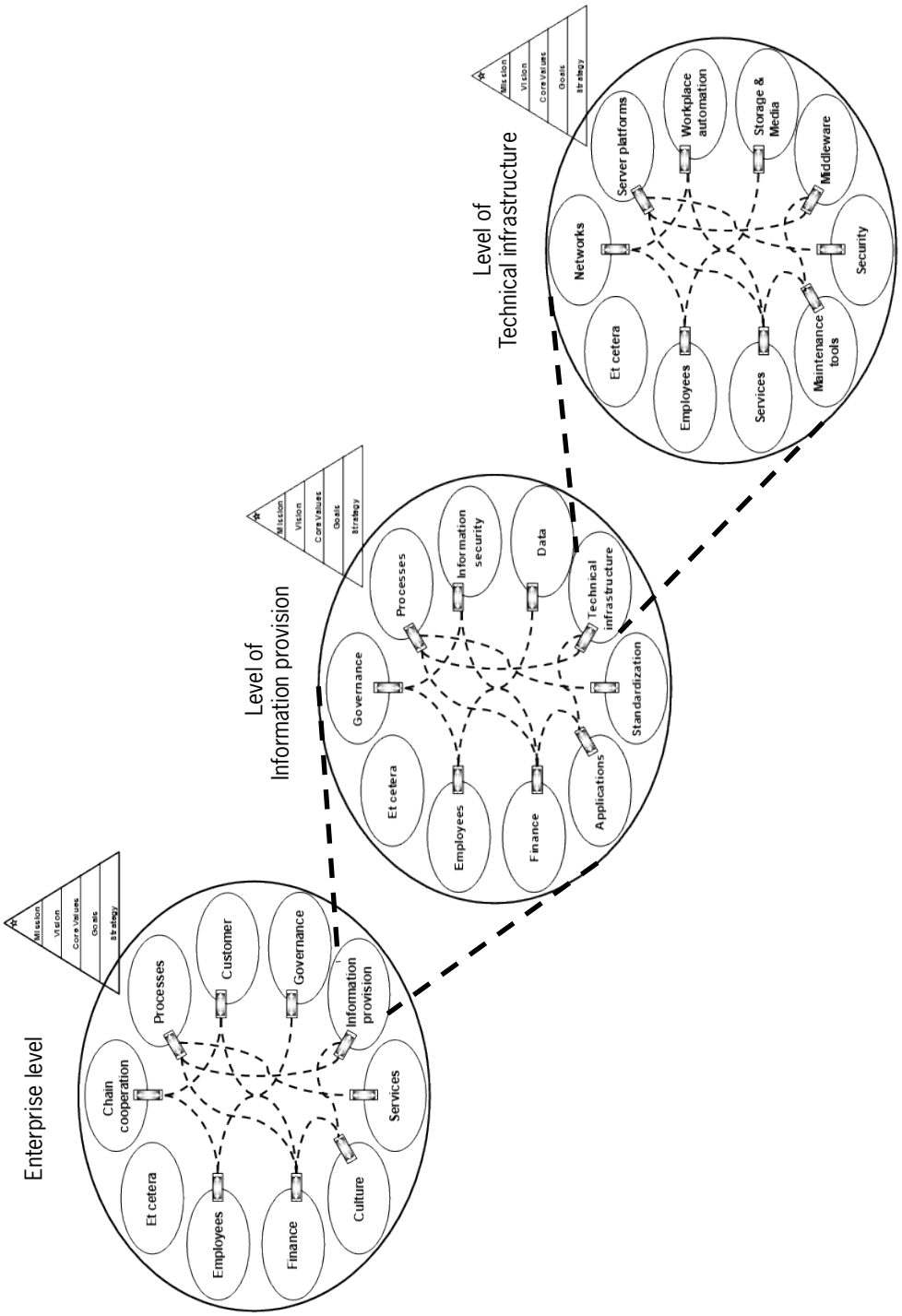
de uitkomsten van deze analyses levert de integrale oplossingsrichting en aanpakkeuze van het vraagstuk op. De impact vertaalt zich in aanpassingen op de richtinggevende kaders die op hun beurt weer tot wijzigingen in bedrijfsregels kunnen leiden, en de oplossingsruimte bestaat uit een verzameling veranderinitiatieven die nodig zijn om het vraagstuk integraal aan te pakken. Door het EA-stelsel continu actueel te houden en te gebruiken om integrale oplossingsrichtingen en aanpakkeuzes voor vraagstukken te ontwikkelen, wordt een permanente vorm van sturen op samenhang verkregen. De verkregen oplossingen zullen vanwege de gehanteerde integrale benadering namelijk een betere inpassing hebben in het grotere geheel. Het EA-concept is uitgewerkt in een stelsel van componenten waarmee sturen op samenhang als een bedrijfsfunctie is in te richten. Deze componenten zijn: EA-visie, EA-processen, EA-producten, EA-mensen, EA-middelen, EA-besturing en EA-methodologie [13].

6

Samenhang tussen meerdere niveaus door recursieve toepassing

De wijze waarop de elementen Perspectief en Kernbegrip zijn gedefinieerd, geeft EA een recursief karakter – vergelijkbaar met het 'Droste-effect' – waardoor hetzelfde besturingsmechanisme op verschillende abstractieniveaus kan worden toegepast. Als voorbeeld van verschillende niveaus hebben wij in figuur 2 het enterpriseniveau, het niveau van de informatievoorziening (IV) en het niveau van de technische infrastructuur (TI) recursief gekoppeld afgebeeld. Het recursief toepassen van sturen op samenhang is per definitie mogelijk voor elk perspectief. Om aan te geven hoe de recursieve werking voor de informatievoorziening toegepast kan worden, wordt ingezoomd op het perspectief IV op enterpriseniveau. Hierdoor verschijnt in figuur 2 de cirkel op het niveau van informatievoorziening (middelste cirkel) met als voorbeelden de perspectieven Processen, Informatiebeveiliging, Data, Technische infrastructuur (TI), Standaardisatie, Applicaties, enzovoort. Daarna zoomen we in op het perspectief TI van het niveau informatievoorziening, waardoor in figuur 2 de cirkel technische infrastructuur ontstaat (onderste cirkel) met perspectieven als Netwerken, Serverplatformen, Werkplekautomatisering, Opslag & Media, Middleware, Security, enzovoort.

Elk niveau heeft een eigen zingeving, als aangegeven in figuur 2, die in overeenstemming is met de zin- en vormgeving van de aanpalende niveaus. Toepassing van recursiviteit leidt zo tot een verticale cascade van expansies in vormgeving waarbij steeds de kernbegrippen van het eerst hoger gelegen niveau promoveren tot perspectieven op het daaronder liggend niveau. Het recursieve beginsel biedt zo handvatten om de relaties aan te geven tussen de drie niveaus van besturing zowel in opwaartse als neerwaartse richting. Vraagstukken die zich voordoen op strategisch, tactisch of operationeel niveau, kunnen leiden tot veranderingen in de samenhang op deze niveaus. Het inzicht in de recursieve relaties zoals hiervoor toegelicht, biedt de mogelijkheid om te sturen op samenhang op en tussen de verschillende niveaus.



Figuur 2. Samenhang tussen niveaus door recursieve toepassing

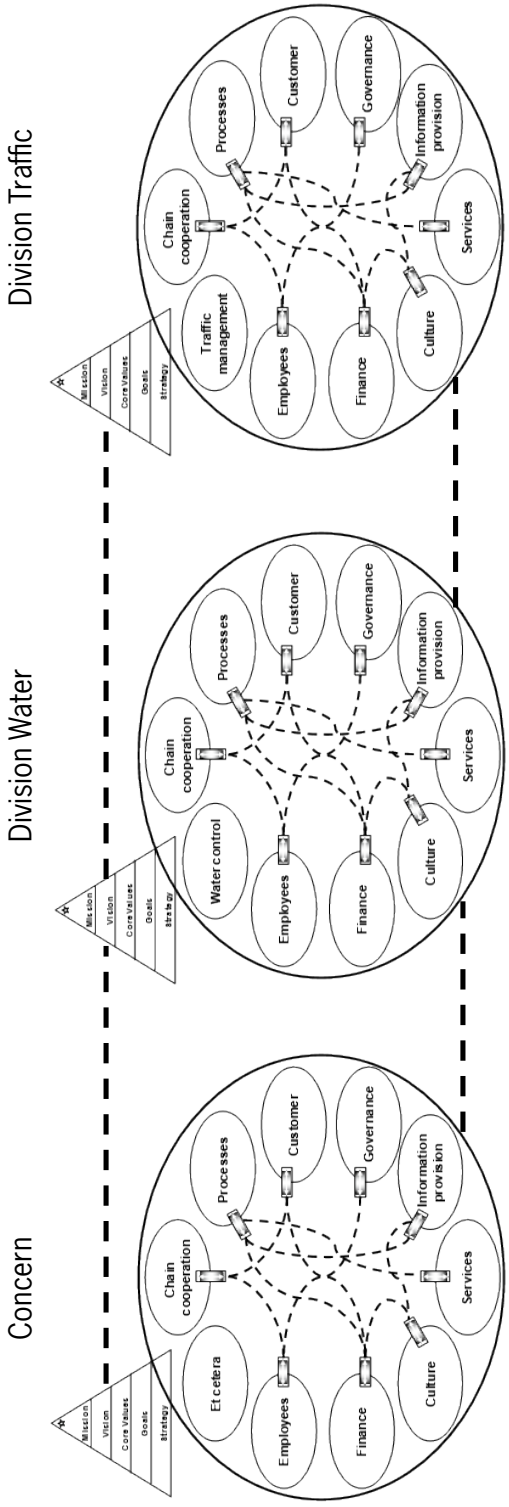
Specifieke technische infrastructuurvraagstukken worden opgelost op het niveau van technische infrastructuur (onderste cirkel) als uitvergroting van het perspectief TI op het niveau van informatievoorziening (middelste cirkel), dat op zijn beurt weer een uitvergroting is van het perspectief IV op het enterpriseniveau. De integrale oplossing van een TI-vraagstuk op het niveau van technische infrastructuur kan leiden tot een verstoring van de samenhang op het eerst hogere niveau doordat bijvoorbeeld veranderingen in de richtinggevende kaders van het perspectief TI invloed hebben op andere perspectieven op het niveau van informatievoorziening. Dit leidt tot een IV-vraagstuk waarvan de integrale oplossing zelfs kan doorwerken op het enterpriseniveau. De recursieve redeneertrant kan dus ook opwaarts worden toegepast, waardoor ook van technische infrastructuurvraagstukken op deze wijze inzichtelijk wordt gemaakt hoe deze strategische effecten kunnen veroorzaken!

Door sturen op samenhang simultaan op drie gekoppelde besturingsniveaus aan te brengen wordt bereikt dat, in dit specifieke voorbeeld, TI op natuurlijke wijze in de besluitvormingsprocessen is verankerd en daarmee de aandacht krijgt die het verdient en vereist. Tot slot kunnen technische infrastructuuraspecten gedistribueerd zijn over andere perspectieven, zoals Security als kernbegrip van het perspectief Informatiebeveiliging (IB) op het niveau van informatievoorziening. Het niveau TI (onderste cirkel) verschaft dan de richtinggevende kaders voor dit kernbegrip. Verder op in deze bijdrage hebben wij een deel van een casus van de recursieve toepassing van EA uitgewerkt voor het perspectief Informatiebeveiliging.

Samenhang tussen concernniveau en divisies door projectie

In het geval een organisatie meerdere divisies heeft, met een relatief lage mate van autonomie en een relatief hoge overeenkomst in operaties, is de toepassing van EA door middel van projectie zinvol. Als aan deze voorwaarden niet wordt voldaan, is het beter voor elke eenheid van de organisatie EA zelfstandig toe te passen.

In het eerste geval drukken we de relatie tussen concernniveau en divisies uit door middel van projectie (zie figuur 3). Door projectie erven de divisies alle leidende kaders van het concernniveau. Alleen de zaken die geen betekenis hebben voor de divisies, zoals corporate richtlijnen voor het verstrekken van beursinformatie, worden niet toegepast op divisieniveau. Elke divisie is in staat om specifieke elementen van de eigen samenhang toe te voegen op zowel het niveau van zingeving, zoals doelen, als op het niveau van vormgeving, zoals perspectieven, richtinggevende uitspraken, enzovoort. Als op divisieniveau een nieuwe richtinggevende uitspraak ontstaat met een generiek karakter, zal deze worden opgenomen op concernniveau en wordt hiermee geldig voor alle divisies. Op deze wijze kan door toepassing van projectie de relatie tussen eenheden van een vergelijkbaar niveau zichtbaar worden gemaakt en bestuurd.

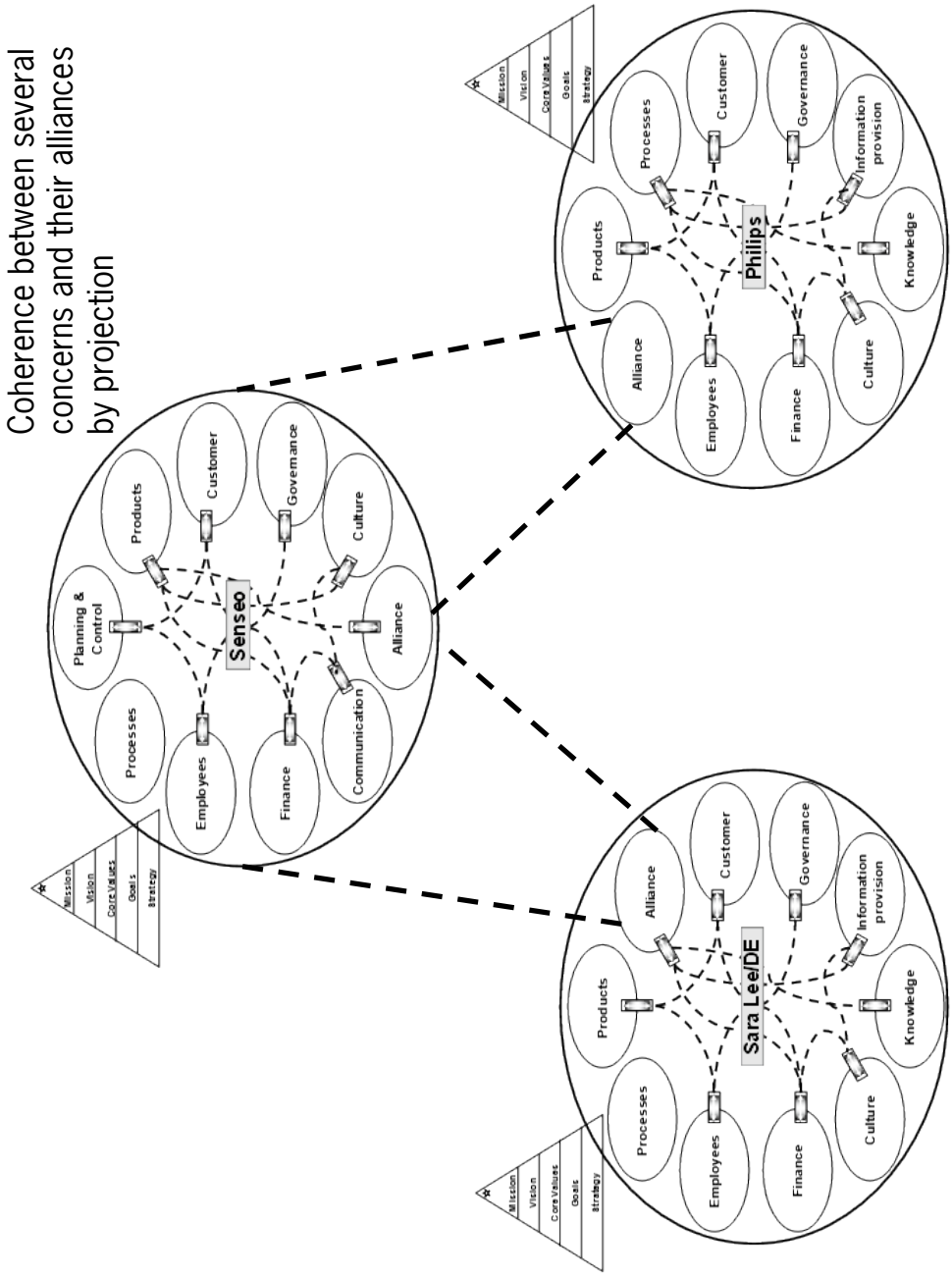


Figuur 3. Samenhang tussen concernniveau en divisies door projectie

Samenhang tussen meerdere organisaties en/of allianties door projectie

De relaties tussen verschillende organisaties en hun contractuele allianties kunnen ook worden uitgedrukt door middel van projectie. In figuur 4 hebben we als voorbeeld de bekende alliantie Senseo afgebeeld, een contractuele alliantie tussen Philips en Sara Lee/DE.

10



Figuur 4. Samenhang tussen twee organisaties die een alliantie vormen

Dit voorbeeld is ontleend aan het werk op het gebied van de alliantiebesturing van De Man [4]. De Man onderscheidt met betrekking tot de besturing van contractuele allianties dertien bouwstenen, alle geplaatst op een dichotomie formeel/informeel. Als het karakter van de alliantie een sterkere 'control'-benadering vergt, worden de elementen uitgedrukt op het corresponderende deel van de dichotomie, zoals de juridische vorm, financiële afspraken, scope en exclusiviteit, conflictoplossing procedures en gezagsverhouding/hiërarchie, meer dominant in de besturing van de alliantie. Als het karakter van de alliantie een relatief hoge 'trust'-benadering vergt, worden de elementen uitgedrukt op het corresponderende deel van de dichotomie, zoals normen/waarden, vertrouwen/commitment, cultuur, persoonlijke relaties, reputatie, leiderschap en communicatiestructuur, meer dominant in de besturing. De Man stelt dat in het geval van meer complexe organisaties zowel de formele als informele elementen goed moeten worden ontwikkeld.

In lijn met deze theorie nemen we zowel binnen het EA-stelsel van Philips als Sara Lee/DE deze dertien bouwstenen van de alliantiebesturing op als kernbegrippen binnen het perspectief Alliance. Alle effecten van de overeenkomsten (richtinggevende uitspraken) in verband met deze dertien kernbegrippen van het perspectief Alliance moeten worden geïmplementeerd zowel binnen Philips als Sara Lee/DE in termen van nieuwe of gewijzigde elementen van samenhang (perspectieven, kernbegrippen, richtinggevende uitspraken, kernmodellen en relevante relaties). Dit maakt duidelijk welke acties de twee organisaties in hun eigen organisatie moeten uitvoeren om klaar te zijn voor de feitelijke uitvoering van de voorgestelde alliantie. Zie de twee onderste cirkels in figuur 4. De bovenste cirkel van figuur 4 representeert de Senseo-alliantie. Alle effecten van de overeenkomsten met betrekking tot de genoemde dertien kernbegrippen komen samen en zijn in lijn met het niveau van zingeving van de alliantie Senseo. Uit dit Senseo-niveau van zingeving wordt het Senseo-niveau van vormgeving afgeleid in termen van perspectieven, enzovoort. Naast de gebruikelijke perspectieven als klant, medewerkers, enzovoort kunnen alle richtinggevende kaders van de dertien voornoemde bouwstenen van alliantiebesturing worden weergegeven op vormgevingsniveau in alle vormen van samenhangende elementen, afhankelijk van de aard en het belang. Op dit niveau komen alle afspraken, gemaakt in de vorm van samenhangende elementen van zowel Philips als Sara Lee/DE, bij elkaar. Zo worden binnen Senseo bij het perspectief Alliance de kernbegrippen Philips en Sara/DE opgenomen. Indien binnen Senseo van elke richtinggevende uitspraak de relatie wordt gedefinieerd met de kernbegrippen Philips en Sara Lee/DE van het perspectief Alliance, zijn als gevolg van een verandering in een richtinggevende uitspraak op Senseo-niveau snel de effecten voor respectievelijk Philips en Sara Lee/DE weer te geven.

We lichten deze waarde met een kort voorbeeld toe. Binnen het perspectief Financiën van Philips is als gevolg van afspraken over de verdeling van de winst de richtinggevende uitspraak opgenomen: de Senseo-alliantie betaalt maandelijks x% van de winst op coffeepads aan Philips. Binnen het perspectief van Financiën van Sara Lee/DE is in dit geval de richtinggevende uitspraak opgenomen: de Senseo-alliantie betaalt maandelijks aan Sara Lee/DE y% van de winst op coffeepads. Betreffende deze winstverdeling bevindt zich in het perspectief Financiën van de alliantie Senseo de richtinggevende uitspraak: de winst op coffeepads zal maandelijks worden betaald in verhouding tot x% en y% respectievelijk aan Philips en Sara Lee/DE. Toen na verloop van tijd duidelijk werd dat het patent op de Senseo-coffeepads niet langer houdbaar bleek, was het voor alle stakeholders (onder andere vertegenwoordigers van de Senseo-perspectieven) meteen duidelijk dat deze situatie niet alleen financiële gevolgen had voor Sara Lee/DE, maar ook van invloed

was op de financiële positie van Philips. Ook zou deze nieuwe situatie de aanleiding kunnen zijn om de verhouding van de winstverdeling van coffeepads te veranderen. Door sturen op samenhang op allianties toe te passen kunnen relaties tussen verschillende organisaties zichtbaar en bestuurbaar worden gemaakt en dit leidt tot een hogere kwaliteit in de besluitvorming.

Recursieve toepassing van EA uitgewerkt voor het perspectief Informatiebeveiliging

In deze paragraaf laten wij zien hoe de recursieve eigenschap van EA kan worden toegepast aan de hand van een casus op het gebied van informatiebeveiliging.

Informatiebeveiliging vanuit een historisch perspectief

De wens voor stringentere antwoorden op beveiligingsvraagstukken is mede ingegeven door veranderende wetgeving, de beschikbaarheid van nieuwe technologie en een agressieve hackersgemeenschap. Daarnaast ervaren de auteurs bij het uitvoeren van risicoanalyses en het bepalen van mitigerende beveiligingsmaatregelen dat er op directieniveau niet altijd oog is voor beveiliging. Beveiliging wordt vooral beschouwd als een technische aangelegenheid, te regelen door de automatiseringsafdeling. De ervaring leert dat bij de uitvoering van projecten beveiliging vaak een sluitpost is en naderhand alsnog dient te worden gerealiseerd. De gevolgen daarvan zijn dat in de ontwerpfasen van applicaties beveiligingseisen onvoldoende worden meegenomen waardoor deze systemen niet optimaal beveiligd zijn tegen bedreigingen. En dit kan leiden tot beveiligingsincidenten resulterend in imagoschade, verlies van bedrijfsgegevens en daarmee gepaard gaande hoge herstel- en faalkosten.

In een recent verschenen rapport, opgesteld door het CyLab van de Carnegie Mellon University, wordt aangegeven dat veel topmanagers van bedrijven geen verband zien tussen ICT-risico's en de bedrijfsrisico's van hun onderneming. Zij blijken geen zicht te hebben op de rol van computersystemen en informatie als het gaat om het lopen van allerlei bedrijfsrisico's [5]. Hoewel dit een Amerikaanse studie is, nemen wij aan dat deze situatie zich ook dichter bij huis voordoet, waarbij managers onvoldoende besef hebben van de gevaren waaraan hun organisatie blootstaat als gevolg van gebrekkige informatiebeveiliging. Kennelijk heeft informatiebeveiliging niet de prioriteit die het verdient. In deze paragraaf geven wij een voorbeeld hoe deze prioriteit geregeld kan worden. We laten zien hoe een strategiewijziging op enterpriseniveau via het domein Informatievoorziening (IV) ingrijpt op het IB-domein.

Ondanks een gebrek aan noodzaak- en urgentiebeleving bij het hoger management is het vakgebied volop in beweging. Zo bestaan er diverse raamwerken op het gebied van beveiliging met als voorbeeld Zachman, SABSA, Cobit en het beveiligingskatern van NORA 2.0. Al deze raamwerken hebben als gemeenschappelijk kenmerk dat zij structuur bieden voor beveiligingsinfrastructuren vanuit een organisatorische, functionele en technologische invalshoek. Wat deze operationele structuren niet invullen, is de relatie met het strategische niveau van de organisatie. Wij tonen aan hoe met behulp van het EA-model deze relatie gelegd kan worden.

Visie op informatiebeveiliging

In onze visie is informatiebeveiliging (IB) een invalshoek van besturing binnen het verantwoordelijkheidsgebied van de CIO waarvan de richtinggevende kaders direct afleidbaar zijn van de zingeving (missie, visie, kernwaarden, doelen, strategie) van de organisatie. Door IB op deze wijze te positioneren worden in het oplossen van strategische vraagstukken 'automatisch' de impact en oplossingsruimte vanuit IB meegenomen. Hierdoor worden direct in het eerste ontwikkelstadium van een oplossingsrichting de (on)mogelijkheden van IB en het effect daarvan op alle andere invalshoeken van besturing verdisconteerd. Toepassing van het stuurinstrument EA zal op deze wijze een significante bijdrage leveren aan het oplossen van beveiligingsvraagstukken.

Samenhang tussen meerdere niveaus door recursieve toepassing

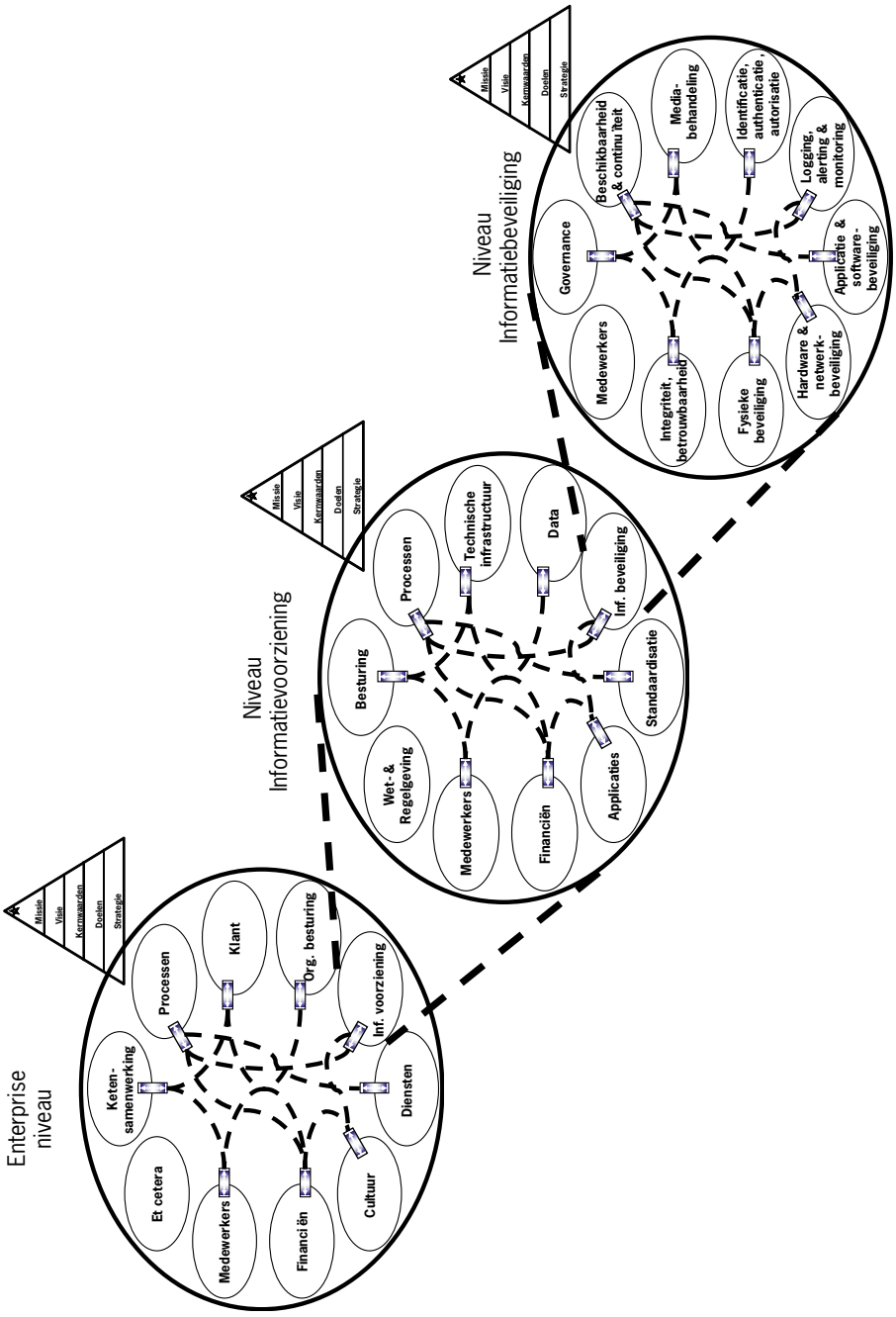
Als voorbeeld van verschillende niveaus hebben wij in figuur 5 het enterpriseniveau, het niveau van de informatievoorziening (IV) en het niveau van informatiebeveiliging (IB) afgebeeld. Het recursief toepassen van GEA is per definitie mogelijk voor elk perspectief.

Om aan te geven hoe de recursieve werking voor het IB-domein toegepast kan worden, wordt ingezoomd op het perspectief IV op enterpriseniveau. Hierdoor verschijnt in figuur 5 de GEA-cirkel op het niveau van informatievoorziening (middelste cirkel) met als voorbeelden de perspectieven Processen, Besturing, Medewerkers, Wet- en Regelgeving, Data, Financiën, Applicaties, Technische infrastructuur, Informatiebeveiliging en Standaardisatie.

Daarna zoomen we in op het perspectief IB van het niveau informatievoorziening, waardoor in figuur 5 de GEA-cirkel informatiebeveiliging ontstaat (onderste cirkel) met perspectieven als Governance, Beschikbaarheid & continuïteit, Mediabehandeling, Identificatie, Authenticatie & autorisatie, Logging, Alerting & monitoring, Applicatie & softwarebeveiliging, Hardware & netwerkbeveiliging, Fysieke beveiliging, Integriteit & betrouwbaarheid en Medewerkers.

Specifieke beveiligingsvraagstukken worden opgelost op het niveau van informatiebeveiliging (onderste cirkel) als uitvergroting van het perspectief IB op het niveau van informatievoorziening (middelste cirkel), dat op zijn beurt weer een uitvergroting is van het perspectief IV op het enterpriseniveau. De integrale oplossing van een IB-vraagstuk op het niveau van informatiebeveiliging kan leiden tot een verstoring van de samenhang op het eerst hogere niveau doordat bijvoorbeeld veranderingen in de richtinggevende kaders van het perspectief IB invloed hebben op andere perspectieven op het niveau van informatievoorziening. Dit leidt tot een IV-vraagstuk waarvan de integrale oplossing zelfs kan doorwerken op het enterpriseniveau. De recursieve redeneertrant kan dus ook opwaarts worden toegepast, waardoor ook beveiligingsvraagstukken op deze wijze strategische effecten kunnen veroorzaken!

Door sturen op samenhang simultaan op drie gekoppelde besturingsniveaus aan te brengen wordt bereikt dat IB op natuurlijke wijze in de besluitvormingsprocessen is verankerd en daarmee de aandacht krijgt die het verdient en vereist. Tot slot kunnen beveiligingsaspecten gedistribueerd zijn over andere perspectieven, zoals Beveiliging als kernbegrip van het perspectief Technische infrastructuur (TI) op het niveau van informatievoorziening. Het niveau IB (onderste cirkel) verschaft dan de richtinggevende kaders voor dit kernbegrip.



Figuur 5. Samenhang informatiebeveiliging/enterprise via recursiviteit

Voorbeeld van EA-elementen in het IB-domein Overheid

De inspanningen in de laatste jaren door de overheid om te komen tot gemeenschappelijke normenkaders voor informatiebeveiliging hebben geleid tot de definitie van een integrale

visie op het gebied van informatiebeveiliging. Daarmee komt één overheidbreed kader tot stand dat bestaande departementale kaders vervangt. Immers, het hanteren van zo veel verschillende normenkaders is verwarrend en belemmert een beheerste beveiliging en het implementeren en beheren van de normen. Deze integrale visie is verwoord in de nieuwe Baseline Informatiebeveiliging Rijksdienst (BIR) [1] die zich op het moment van schrijven in een goedkeuringstraject bevindt om als integrale overheidsbaseline te worden vastgesteld.

De auteurs zijn werkzaam als consultant en hebben ruime ervaring bij diverse departementen binnen de Nederlandse overheid. Zij hebben daarom de BIR als uitgangspunt genomen en deze met EA instrumenteel stuurbaar gemaakt. In overheidsomgevingen wordt de BIR beschouwd als de leidraad bij het inrichten van departementale beveiligingsmaatregelen.

In de zingeving op het niveau van informatiebeveiliging is de doelstelling van de BIR een bijdrage te leveren aan een veilige overheid. Voorbeelden van richtinggevende uitspraken uit de BIR zijn:

- Risicomanagement is het uitgangspunt voor informatiebeveiliging.
- Methoden voor classificatie van informatie en de effectiviteit van beveiligingsmaatregelen dienen regelmatig te worden getoetst.
- Medewerkers dienen verantwoord en bewust gedrag te vertonen ten aanzien van het werken met overheidsinformatie.

De BIR is gebaseerd op een aantal wetten, normen en standaarden (zie figuur 6). Als uitgangspunt voor het EA Securitymodel is de BIR genomen en daarmee impliciet genoemde wetten, normen en standaarden.

Figuur 6. Basis voor BIR

Bij het uitwerken van de perspectieven en kernbegrippen in de vormgeving op het niveau van informatiebeveiliging is de groepering van de BIR aangehouden. Deze groepering sluit goed aan op de invalshoeken waarbij in de praktijk op informatiebeveiliging wordt gestuurd. Voor een nadere toelichting op deze groepering verwijzen wij naar de BIR [1].

In tabel 1 zijn deze perspectieven en hun definities verwoord.

Perspectief	Definitie
Integriteit & betrouwbaarheid	Integriteit & betrouwbaarheid betreft de te verwerken informatie; deze dient juist en correct te zijn wanneer deze onderdeel is van een operationeel proces en mag als onderdeel van communicatie en bij opslag niet onderweg ongewenst gemanipuleerd of gewijzigd worden.
Identificatie, authenticatie & autorisatie	Het onweerlegbaar vaststellen van de juiste identiteit van de gebruiker, dit toetsen aan de rechten en verantwoordelijkheden die zijn vastgelegd en deze gebruiker toegang verlenen tot de informatie waarvoor bevoegdheid is verleend.
Fysieke beveiliging	Het voorkomen van onbevoegde fysieke toegang tot, schade aan of verstoring van het terrein en de informatie van de organisatie. Werknemers, ingehuurd personeel en externe gebruikers zijn gewezen op hun verantwoordelijkheden, begrijpen deze en zijn geschikt en toegerust voor de rollen die zij krijgen toegekend.
Hardware- & netwerkbeveiliging	Het beveiligen van de systemen en infrastructuur waar gebruik van wordt gemaakt bij het verwerken en versturen van informatie.
Applicatie- & softwarebeveiliging	Het beveiligen van de applicaties en operationele softwareplatformen die worden ingezet bij het verwerken van informatie.
Logging, monitoring & alerting	Logging is het vastleggen van alle activiteiten van applicaties, software, hardware en netwerkcomponenten om in het kader van monitoring tijdig incidenten te kunnen detecteren en tijdig actie te kunnen ondernemen (alerting). Als de detectie pas in een laat stadium plaatsvindt, kan met behulp van de logging worden achterhaald welke gebeurtenissen eraan voorafgingen.
Behandeling van media	Het bereiken en handhaven van een adequate bescherming van bedrijfsmiddelen van de organisatie. Deze dienen een eigenaar te hebben, te zijn gerubriceerd en geïnventariseerd waarbij er regels voor documentatie, verwerking en opslag worden nageleefd.
Beschikbaarheid & continuïteitsvoorzieningen	Het tegengaan van onderbreking van de bedrijfsactiviteiten en bescherming van kritische bedrijfsprocessen tegen de gevolgen van omvangrijke storingen in informatiesystemen of rampen en om tijdig herstel te bewerkstelligen.
Security governance	De besturing van het IB-domein. In de BIR is een hoofdstuk opgenomen met betrekking tot de controleerbaarheid met een verwijzing naar de VIR. Door het uitvoeren van een intern onderzoek en het afgeven van een control statement wordt aangegeven in welke mate wordt voldaan aan het gestelde beveiligingsniveau. Dit statement wordt vermeld in de rapportage over de bedrijfsvoering.

Tabel 1. Perspectieven Informatiebeveiliging en definities conform BIR

In onze EA-theorie zijn kernbegrippen een nadere uitwerking van de perspectieven. Het zijn de relevante onderdelen waar het om draait binnen een perspectief, de invalshoeken van waaruit men het perspectief wenst te besturen.

Samenhang binnen IB-domein en met tactisch en strategisch niveau

Na in eerdere paragrafen het IB-domein te hebben toegelicht, geven wij nu aan de hand van een voorbeeld aan hoe via recursiviteit de samenhang tussen de perspectieven binnen het IB-domein en de verschillende niveaus van zin- en vormgeving in de praktijk werkt.

Een organisatie besluit met ingang van 2014 'Het Nieuwe Werken' te omarmen en medewerkers toe te staan gebruik te maken van privéapparatuur voor het werken met bedrijfsinformatie (doel in de zingeving op enterpriseniveau). Dit wordt ook wel het Bring-Your-Own-Device-concept (BYOD) genoemd. Dit doel leidt in de vormgeving op enterpriseniveau tot een aantal nieuwe richtinggevende uitspraken (RGU's) voor een aantal perspectieven in figuur 7. Zie bijvoorbeeld bij het perspectief Informatievoorziening de nieuwe RGU 'Alle primaire bedrijfssystemen dienen plaats- en tijdsonafhankelijk werken van medewerkers te faciliteren' en bij het perspectief Medewerkers de nieuwe RGU 'Medewerkers die het BYOD-concept willen gebruiken, dienen aan additionele IB-maatregelen te voldoen.'

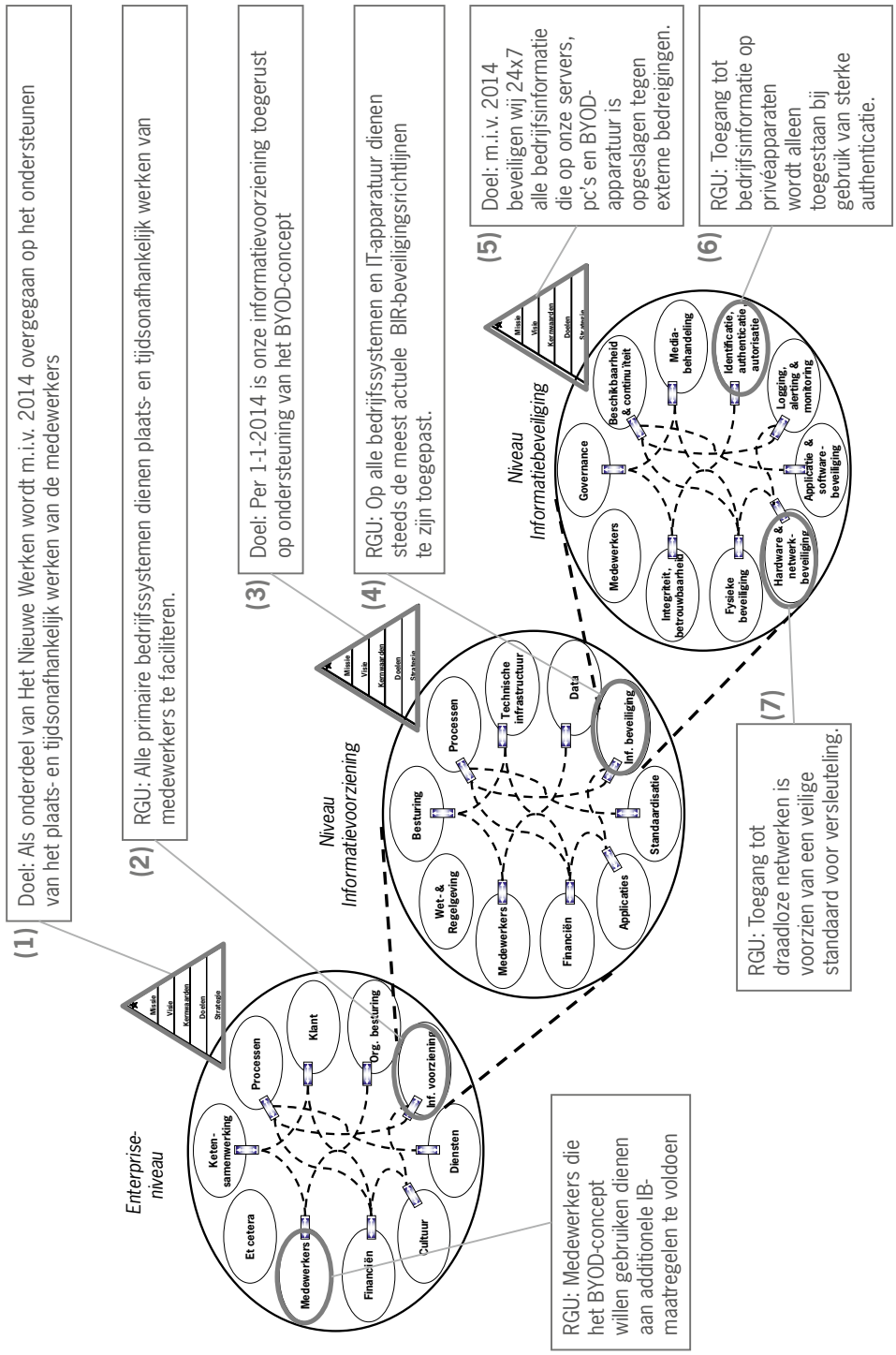
Dit heeft ook gevolgen in de zin- en vormgeving op het niveau van informatievoorziening. Op dit niveau leidt dit tot het volgende doel: 'Per 1-1-2014 is onze informatievoorziening toegerust op ondersteuning van het BYOD-concept.' Dit doel resulteert in een aantal nieuwe RGU's voor een aantal perspectieven. Bijvoorbeeld de RGU 'Op alle bedrijfssystemen en IT-apparatuur dienen steeds de meest actuele BIR-beveiligingsrichtlijnen te zijn toegepast' voor het perspectief Informatiebeveiliging.

De voornoemde wijzigingen in doelen leiden op het niveau van informatiebeveiliging tot het formuleren van het doel 'Met ingang van 2014 beveiligen wij 24×7 alle bedrijfsinformatie die op onze servers, pc's en BYOD-apparatuur is opgeslagen, tegen externe bedreigingen.' Dit heeft in de vormgeving op dit niveau een aantal RGU's voor een aantal perspectieven tot gevolg. Bijvoorbeeld de RGU 'Toegang tot bedrijfsinformatie op een privéapparaat wordt alleen toegestaan bij gebruik van sterke authenticatie' voor het perspectief Identificatie, authenticatie & autorisatie en 'Toegang tot draadloze netwerken is voorzien van een veilige standaard voor versleuteling' bij het perspectief Hardware- & netwerkbeveiliging.

Dit voorbeeld betreft een fragment uit de GEA-analyse en laat zien hoe een voornemen op strategisch niveau zich uiteindelijk via het besturingsniveau informatievoorziening manifesteert in veranderingen op het niveau van informatiebeveiliging. We laten hier ter illustratie slechts een enkelvoudig, neerwaarts causaal patroon van veranderende kaderstellingen zien. In werkelijkheid zullen neerwaartse en opwaartse patronen naast elkaar lopen waardoor de drie besturingsniveaus onderling stabiliseren, een vereiste om te komen tot performante bedrijfsomstandigheden!

Conclusie en aanbevelingen

In dit artikel hebben wij laten zien hoe de waarde van het stuurinstrument EA zowel tot uitdrukking komt op het overkoepelende bedrijfsniveau als op en tussen hiërarchisch lagere besturingsniveaus, als in allianties waar de enterprise deel van uitmaakt. We hebben voorbeelden gegeven hoe de domeinen Technische infrastructuur en Informatiebeveiliging



Figuur 7. Samenhang binnen het IB-domein en met het tactisch en strategisch niveau

integraal meegenomen kunnen worden in het oplossend vermogen van organisaties. Deze werkwijze maakt het mogelijk om vraagstukken op deze gebieden en nadelige effecten daarvan preventief aan te pakken door zowel op alle niveaus te kunnen sturen op samenhang alsook tussen die niveaus. Mede ontstaat hierdoor de mogelijkheid om de sturing van bijvoorbeeld het TI-domein te koppelen aan de andere besturingscycli van de organisatie en de TI-aspecten direct van invloed te doen zijn bij het ontwikkelen van integrale oplossingen voor vraagstukken die spelen op enterpriseniveau. Ook hebben wij een aanzet gegeven om de samenhang tussen organisaties inzichtelijk en daarmee bestuurbaar te maken.

EA is een open model dat uitnodigt om toegepast en verder ontwikkeld te worden. De auteurs nodigen vakgenoten uit tot het toepassen van EA en dit te verfijnen op basis van hun praktijkervaringen. Wij danken Rob Stovers en Rutger Goedendorp van Ordina en Willem Krijgsman van Spax Solutions B.V. voor hun reviewinspanningen.

Literatuur

1. Ministerie van Binnenlandse Zaken en Koninkrijkrelaties (2012). Baseline Informatiebeveiliging Rijksdienst (BIR) Tactisch Normenkader (TNK), versie 0.99g, 11 januari 2012.
2. Collins, J. en j. Porras (1996). 'Building Your Company's Vision', *Harvard Business Review*.
3. De Algemene Rekenkamer (2008). *Lessen uit ICT-projecten bij de overheid, Deel B*.
4. De Man, A.P. (2006). *Alliantiebesturing: samenwerking als precisie-instrument*, Stichting Management Studies, Van Gorkum.
5. Westby, J.R. (2012). *Governance of Enterprise Security: CyLab 2012 Report, How Board & Senior Executives Are Managing Cyber Risks*, Carnegie Mellon University, Forbes, 16 mei 2012.
6. Kaplan, R.S., D.P. Norton en E.A. Barrows (2008). 'Developing the Strategy: Vision, Value Gaps, and Analysis', Harvard Business School Publishing Corporation.
7. Senge, P.M. (1990). *The Fifth Discipline*, New York: Currency, ISBN 0-385-51725-4.
8. Thenmozhi, M., *Module 9 – Strategic Management*, Lecture Notes, Department of Management Studies, IIT Madras 26.
9. Wagter, R. (2009). *Sturen op samenhang op basis van GEA – Permanent en event driven*. Zaltbommel: Van Haren Publishing.
10. Wagter, R., H.A. Proper en D. Witte (2011). 'Enterprise Coherence Assessment', *Proceedings of the 2rd Working Conference on Practice-driven Research on Enterprise Transformation*, PRET 2011, Luxemburg-Kirchberg; Berlijn: Springer, september 2011, pp. 28-52.
11. Wagter, R., H.A. Proper en D. Witte (2012). *A Practice-Based Framework for Enterprise Coherence*, volume 0120 of the Lecture Notes in Business Information Processing series, PRET 2012, Gdansk; Berlijn/Heidelberg: Springer-Verlag.
12. Wagter, R., H.A. Proper en D. Witte, (2012). 'Enterprise Coherence in the Dutch Ministry of Social Affairs and Employment', *Proceedings of the 7th International Workshop on Business/IT-Alignment and Interoperability* (BUSITAL2012), Berlijn: Springer.
13. Wagter, R., H.A. Proper en D. Witte (2012). 'Enterprise Architecture: a strategic specialism', *Proceedings of 2012 IEEE 14th International Conference on Commerce and Enterprise Computing* (CEC 2012), Hangzhou, China, september 2012, pp. 1-8.

14. Wagter, R., H.A. Proper en D. Witte (2012). 'Enterprise Architecture: On the Use of GEA at the Dutch Ministry of Social Affairs and Employment', *Proceedings of 2012 IEEE 14th International Conference on Commerce and Enterprise Computing* (CEC 2012), Hangzhou, China, september 2012, pp. 115-119.

15. Wagter, R., H.A. Proper en D. Witte (2012). 'The Extended Enterprise Coherence-governance Assessment', *Proceedings of the 7th workshop on Trends in Enterprise Architecture Research* (TEAR 2012), Berlijn: Springer.

16. www.groeiplatformgea.nl.

Over de auteurs

Roel Wagter is partner bij Ordina.
E-mail: roel.wagter@ordina.nl

Dirk Witte is principal consultant bij Logica Business Consulting.
E-mail: dirk.witte@logica.com

Leon van der Valk is security consultant bij Security & Risk Management Ordina.
E-mail: leon.van.der.valk@ordina.nl