Universiteit Twente
de ondernemende universiteit

ERNST & YOUNG

WERKWIJZE TER BEOORDELING VAN IT GOVERNANCE

OP BASIS VAN GEACCEPTEERDE METHODES OP HET TERREIN VAN IT GOVERNANCE

MASTER THESIS WILCO LEENSLAG UNIVERSITEIT TWENTE

MASTER THESIS WILCO LEENSLAG

Master of Science Business Information Technology
Universiteit Twente

WERKWIJZE TER BEOORDELING VAN IT GOVERNANCE

Afstudeerder

Naam:	Wilco Leenslag
Studentnummer:	s0076414
Opleiding:	Business Information Technology Universiteit Twente
Specialisatie:	ICT & Innovation

Opdrachtgever

Organisatie:	Ernst & Young EDP Audit
1ste begeleider:	drs. I.N. Kouters
2de begeleider:	O.E. Teule RE RA

Begeleiding

1ste begeleider:	Dr. Mr. Ir. Th.J.G. Thiadens Faculteit Bedrijf, Bestuur en Technologie
2de begeleider:	Dr. P.A.T. van Eck Faculteit Elektrotechniek, Wiskunde en Informatica

Afstudeerscriptie

Versie:	2.0
Datum:	23 augustus 2006

VOORWOORD

If I have seen a little further it is by standing on the shoulders of giants

(Isaac Newton 1676)

Voor u ligt het eindresultaat van mijn afstudeeropdracht aan de Universiteit Twente. Deze opdracht is uitgevoerd bij Ernst & Young EDP Audit te Apeldoorn. In de scriptie wordt een onderzoek beschreven om te komen tot een werkwijze waarmee de besturing (Governance) van de automatisering (IT) bij organisaties wordt beoordeeld. Het onderzoek staat in nauw verband met een aantal actuele inspanningen die bij verschillende organisaties gedaan (moeten) worden om meer grip te krijgen op de kwaliteit van IT Governance. Met dit onderzoek hoop ik een positieve bijdrage te leveren aan de academische en pragmatische wereld. Hierbij zijn nieuwe inzichten in en toepassingen van IT Governance speerpunten.

Met deze scriptie rond ik mijn studie MSc Business Information Technology (BIT) af. Als één van de weinigen die na zijn HBO-BI studie de MSc studie BIT aan de Universiteit Twente heeft gevolgd is het een traject geweest met pieken en dalen. Ik ben dan ook uitermate tevreden om met deze scriptie de studie af te ronden, waarmee ik probeer aan te tonen dat met inzet, doorzettingsvermogen en gedrevenheid veel bereikt kan worden.

Om te voorkomen dat het dankwoord een sentimenteel verhaal wordt ga ik niet elke persoon die mij heeft bijgestaan de afgelopen periode individueel langs. Ik vertrouw erop dat een ieder die zich betrokken heeft gevoeld weet in welke mate ik dat heb gewaardeerd. Er zijn natuurlijk wel een paar personen in het bijzonder die ik wil bedanken:

Mijn afstudeerbegeleiders, Ivo Kouters & Otto Teule, bij Ernst & Young EDP Audit wil ik bedanken voor de tijd die zij beschikbaar hebben gesteld gedurende mijn stage. Mijn begeleiders, Theo Thiadens & Pascal van Eck, van de Universiteit Twente wil ik bedanken voor hun academische kennis en toegewijde inzet. Uiteraard mag ik niet de collegaé bij Ernst & Young EDP Audit vergeten. Een goede sfeer draagt bij aan een leuke werkomgeving en daar hebben zij absoluut een positieve bijdrage aan geleverd. Ik wens iedereen veel succes in de toekomst. Onder het motto: *"In Nederland kun je nooit uitsluiten dat je elkaar niet meer tegen komt"* hoop ik iedereen in het vakgebied of daarbuiten nog met enige regelmaat te treffen.

Als laatste gaat een bijzonder dankwoord uit richting mijn ouders. Zij hebben mij tijdens de afgelopen maanden en tijdens de volledige studie op hun manier enorm gesteund.

Wilco Leenslag,

Neede, 23-8-2006

MANAGEMENTSAMENVATTING

IT Governance staat de laatste tijd volop in de belangstelling. Dit heeft echter nog niet geleid tot een hogere kwaliteit van besturing (Governance) van de automatisering (IT) bij organisaties. Het is wel de intentie van organisaties om dit te verbeteren. Om de kwaliteit van besturing van de automatisering bij organisaties te beoordelen is geen eenduidige en overdraagbare werkwijze beschreven bij Ernst & Young EDP Audit, maar deze is wel gewenst. Dit is aanleiding geweest voor het opzetten en uitvoeren van dit onderzoek. De doelstelling die hierbij is gehanteerd luidt:

Doelstelling:

Het doel van dit onderzoek is om een werkwijze te ontwikkelen waarmee de kwaliteit van besturing (Governance) van de automatisering (IT) bij organisaties wordt beoordeeld op basis van geaccepteerde methodes op het terrein van IT Governance.

Leenslag (2006)

Het doel van de werkwijze is tweeledig: (1) De werkwijze wordt gebruikt als overdraagbare methode bij Ernst & Young EDP Audit om auditors een handleiding te geven bij het beoordelen van de kwaliteit van besturing van de automatisering. (2) Daarnaast werkt het als communicatiemiddel richting organisaties om aan te geven hoe zij *in control* blijven van hun IT.

Om het onderzoeksgebied van IT Governance te verkennen is een literatuurstudie gedaan naar dit onderwerp. Hierbij is eerst gekeken naar de definitie van IT Governance waarbij de volgende definitie is gekozen:

Definitie IT Governance:

IT Governance is the responsibility of executives and the board of directors, and consists of the leadership, organisational structures and processes that ensure that the enterprise's IT sustains and extends the organisation's strategies and objectives.

IT Governance Institute (2006)

Naast de gekozen definitie zijn in de literatuur nog andere definities te vinden. Deze definities verschillen ten opzichte van elkaar maar hebben ook overeenkomsten. Veel gebruikte termen om IT Governance te beschrijven zijn: (1) structuren, (2) mechanismen en (3) processen. Deze termen representeren belangrijke concepten en hulpmiddelen van IT Governance. Deze zijn gebruikt bij het ontwikkelen van een eigen IT Governance benadering en werkwijze. Een ander begrip wat in de literatuur als essentieel wordt gezien voor effectieve IT Governance is *control.* Dit onderwerp is in dit onderzoek als kader gebruikt waar vanuit IT Governance benaderd wordt. De werkwijze om IT Governance te beoordelen is ontwikkeld om de mate van *control* te bepalen bij organisaties.

Om verschillende IT Governance benaderingen te bestuderen zijn drie dimensies geïdentificeerd die worden gebruikt als invalshoeken van IT Governance. Deze invalshoeken beschrijven de *wie, wat* en *hoe* van IT Governance en zijn gebruikt om een metamodel op te zetten. Met dit metamodel zijn een drietal IT Governance benaderingen bestudeerd: (1) De *research based* benadering van Weill et al. richt zich voornamelijk op de beslissingen die genomen moeten worden. In tegenstelling tot (2) de *practitioners based* benadering van de IT Governance Institute (ITGI) wordt niet gesproken over uit te voeren processen. (3) De *educated based* benadering bevat duidelijke *house-in-order* methodes. Daarnaast maakt deze benadering als enige een duidelijk onderscheid tussen de vraag- en aanbodorganisatie.

Gebruikmakend van de IT Governance benaderingen en de gekozen invalshoeken is een eigen IT Governance benadering met framework ontwikkeld. De toegevoegde waarde van de eigen benadering ten opzichte van bestaande benaderingen is dat expliciet onderscheid gemaakt wordt tussen de vraag- en aanbodorganisatie in combinatie met CoBiT processen. Sterke kant van de eigen IT Governance benadering is dat een aantal aandachtsgebieden methodisch ingevuld kunnen worden om IT gerelateerde onderwerpen te ondersteunen. Deze methodes zijn in drie categorieën gerubriceerd: (1) methodes die de vraag- en aanbodorganisatie ondersteunen, (2) methodes die specifieke IT aspecten ondersteunen, (3) methodes die prestaties beoordelen en evaluaties mogelijk maken.

De toepassing van methodes op het IT Governance framework heeft geresulteerd in het IT Governance werkmodel (Figuur 16). Dit werkmodel representeert op een concrete manier de eerder genoemde IT Governance concepten en hulpmiddelen. Het is een gestructureerd model dat gebruik maakt van mechanismen (methodes) om processen te beoordelen. De geselecteerde methodes hebben ten opzichte van CoBiT maar ook ten opzichte van elkaar een sterke samenhang. Middels dit model en de methodes is het mogelijk om de mate van *control* (kader onderzoek) te bepalen bij organisaties.

Vanuit de theorie is een werkwijze ontwikkeld die het mogelijk maakt om op een gestructureerde (aandacht voor aandachtsgebieden/processen, aspecten en perspectieven), overzichtelijke (selectie processen) en pragmatische (selectie van normen) manier de kwaliteit van IT Governance te beoordelen. Het resultaat is een IT Governance checklist met +/- 200 normen. Dit is een concrete vertaling van het IT Governance werkmodel. De checklist stelt EDP Auditors in staat om de kwaliteit van IT Governance bij organisaties te beoordelen. Organisaties kunnen de IT Governance checklist (en werkmodel) tevens gebruiken bij het inrichten van hun IT Governance structuur en bij het uitvoeren van self assessments. De werkwijze die is ontwikkeld voor dit onderzoek kan als volgt samenvattend weergegeven worden:

Werkwijze ter beoordeling van IT Governance:

Als werkwijze om de kwaliteit van
besturing (Governance) van de automatisering (IT) bij organisaties te bepalen
worden gekozen aspecten binnen de aandachtsgebieden voor een selectie van processen
beoordeeld vanuit verschillende perspectieven
gebruikmakend van een IT Governance checklist met normen.

Leenslag (2006)

In dit onderzoek is de toepasbaarheid van de werkwijze (werkmodel en IT Governance checklist) getoetst middels een drietal interviews. Hierbij is een oordeel over het IT Governance werkmodel en de IT Governance checklist gevraagd. Daarnaast is bij één van de organisaties de checklist (bijna) volledig toegepast. De resultaten van het praktijkonderzoek zijn gebruikt om de volledigheid en correctheid van de werkwijze te bepalen.

Het eindoordeel is dat de structuur en toepasbaarheid van het model en de checklist goed zijn bevonden. Het model is generiek opgezet om toepasbaar te zijn voor een breed assortiment van organisaties. Hiervoor kan het nodig zijn dat in enkele gevallen een klantspecifieke vertaalslag gemaakt moet worden om het model en de checklist aan te laten sluiten op rollen, verantwoordelijkheden en begrippen die gebruikt worden door de organisatie. Het is aan te bevelen om via een inleidend gesprek de structuur van de organisatie te matchen met de structuur van het IT Governance werkmodel en de checklist. Een tweede aanbeveling is om te kiezen voor een software tool om bij organisaties de +/- 200 normen te verwerken en te analyseren. Eenvoudige Microsoft Access en/of Microsoft Excel toepassingen zijn hiervoor afdoende. Aanvullend onderzoek is nodig naar de mogelijkheden van andere IT aspecten op het huidige model. Andere aspecten kunnen een positieve bijdrage leveren aan de beoordeling van de kwaliteit van IT Governance. Hierbij wordt geadviseerd om financieel management als eerste te bestuderen. Uit verschillende interviews blijkt dat de organisatietypologie invloed heeft bij de toepassing van de IT Governance checklist. Verder onderzoek is nodig naar het nut van de toepassing van organisatietypologieën op het ontworpen IT Governance model. Daarnaast is meer praktijkonderzoek aanbevolen naar de mogelijkheden/voordelen van de koppeling tussen de IT BSC en de traditionele bedrijfs-BSC van (IT) organisaties.

[blanco]

INHOUDSOPGAVE

LIJST VAN GEBRUIKTE FIGUREN

LIJST VAN GEBRUIKTE TABELLEN

HOOFDSTUK 1

INLEIDING

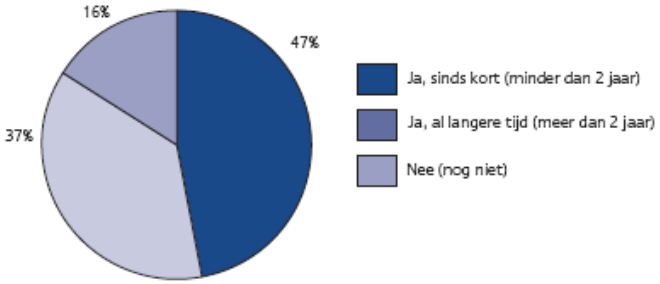
IT Governance is een onderdeel van Corporate Governance. Ernst & Young (2005) geeft aan dat Corporate Governance volop in de belangstelling staat. Hoewel Corporate Governance van alle tijden is, staat dit onderwerp met name de laatste vier jaren volop in de belangstelling. Eind jaren negentig bleek het noodzakelijk om de integriteit van het management van ondernemingen, de transparantie van het handelen en de balans tussen financiële doelstellingen en behoorlijk bestuur te verbeteren. In Nederland heeft dit gestalte gekregen in de Code Tabaksblat, die inmiddels een wettelijke verankering heeft gekregen. De besturing en beheersing van IT en daarmee samenhangende controlemaatregelen en –systemen wordt aangeduid als IT Governance [14].

In deze scriptie wordt een onderzoek beschreven naar een werkwijze ter beoordeling van de kwaliteit van besturing (Governance) van de automatisering (IT) bij organisaties gebaseerd op geaccepteerde methodes op het terrein van IT Governance.

In dit eerste hoofdstuk wordt in § 1.1 achtergrond informatie beschreven over het onderwerp van dit onderzoek. In § 1.2 wordt de organisatie beschreven waar deze opdracht is uitgevoerd. De laatste paragraaf behandelt de onderzoeksopzet.

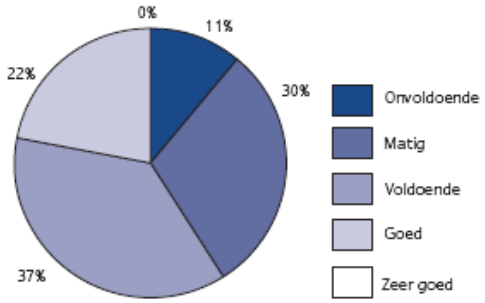
1.1 Achtergrond

IT Governance staat volop in de belangstelling binnen Nederlandse ondernemingen. In totaal stelt 84 procent van de organisaties dat het voor hen een issue is dat speelt. Voor veel bedrijven is die belangstelling van recente datum. Voor een minderheid van de bedrijven is het onderwerp al langere tijd actueel. De aandacht voor IT Governance is de afgelopen jaren dus flink toegenomen Figuur 1 [15].



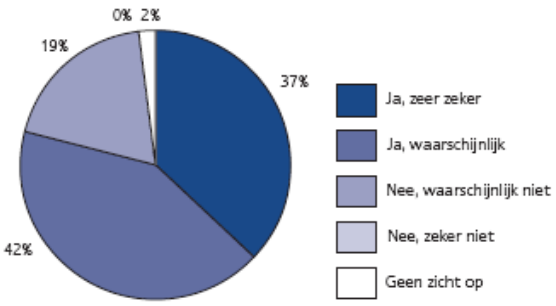
Figuur 1: IT Governance onderwerp binnen onderneming

De kwaliteit van IT Governance is in veel gevallen ontoereikend. Bij vier op de tien ondernemingen is deze onvoldoende of matig. Slechts 22 procent van de ondernemingen karakteriseert de kwaliteit van de *eigen* Governance als goed [15]. In een onderzoek van de ITGI (2006) blijkt dat organisaties in de financiële sector samen met de IT en *Telecom* sector beter presteren op het gebied van IT Governance dan andere type organisaties. Dit heeft te maken met de *strategic importance of IT* in deze sectoren [51] [31].



Figuur 2: Kwaliteit IT Governance

Dat het onderwerp IT Governance populair is blijkt wel als wordt gekeken naar de intentie om deze te verbeteren. Vier op de vijf ondernemingen heeft de intentie om op korte termijn de kwaliteit te verbeteren. Bijna iedere onderneming die zich realiseert dat de kwaliteit nu onvoldoende of matig is, wil snel actie ondernemen om deze te verhogen. Ook bedrijven waar de Governance nu op orde is, willen de kwaliteit nog verder verhogen om de grip op IT te verbeteren [15].



Figuur 3: Intentie verbetering kwaliteit IT Governance

Deze statistieken uit december 2003 geven goed de aanleiding en relevantie weer van dit onderzoek. Steeds meer organisaties zijn bezig met het onderwerp IT Governance en de kwaliteit hiervan. De beoordeling van deze kwaliteit wordt bij Ernst & Young door EDP Auditors gedaan. Het gebrek aan een beschreven werkwijze weerhoudt de overdraagbaarheid van de werkwijze en maakt communicatie over dit onderwerp met organisaties moeilijk.

Uit eigen onderzoek van Ernst & Young blijkt dat veel Nederlandse organisaties kiezen voor internationale standaarden en modellen zoals de Code voor Informatiebeveiliging (ISO 17799), CoBiT en ITIL. Maar liefst 44% van de Nederlandse respondenten maakt bijvoorbeeld gebruik van de Code voor Informatiebeveiliging, wereldwijd is dit 26%. Deze standaarden hebben zich in de praktijk bewezen en door toepassing van deze standaarden laat je als organisatie zien dat je op serieuze wijze omgaat met zaken als informatiebeveiliging en het beheer van je IT-organisatie [16]. Niet alleen voor organisaties (bij het inrichten van IT Governance) maar ook vanuit een audit perspectief wordt door verschillende auteurs het gebruik van methodes geadviseerd. Door het gebruik van methodes ontstaat een betere communicatie tussen partijen. Het gebruik van methodes bij SLM en Service Level Agreements kan leiden tot een beter inzicht in het managen van third-party services. Niet één methode dekt de volledige lading als het gaat om IT Governance. Een combinatie van methodes heeft de voorkeur. Bij het ontwikkelen van een werkwijze kan gebruik gemaakt worden van bestaande geaccepteerde methodes. Het wiel hoeft namelijk niet opnieuw uitgevonden te worden.

1.2 Organisatie Ernst & Young

1.2.1 Ernst & Young

Ernst & Young is de zakelijke aanduiding voor de samenwerkende maatschappen Ernst & Young Accountants en Ernst & Young Belastingadviseurs. Daarnaast maakt ook Ernst & Young Transaction Advisory Services BV deel uit van de organisatie. Juridische dienstverlening wordt verzorgd door de maatschap Holland Van Gijzen Advocaten en Notarissen, die een strategische alliantie heeft met Ernst & Young Belastingadviseurs.
Ernst & Young werkt voor ondernemingen, not-for-profitorganisaties, overheden, overheidsinstanties en particulieren. In zijn dienstverlening onderscheidt Ernst & Young twee segmenten: de beursgenoteerde en multinationaal opererende bedrijven en de grote, middelgrote en kleine nationale organisaties.
Ernst en Young opereert in Nederland vanuit 29 vestigingen. Ernst en Young Nederland maakt deel uit van de wereldwijde Ernst & Young-organisatie waarin ruim 140 landenfirma's en zo'n 106.000 medewerkers zijn samengebracht [33].

1.2.2 Ernst & Young EDP Audit

Ernst & Young EDP Audit is een gespecialiseerde adviesgroep van Ernst & Young Accountants, waarin onafhankelijke en deskundige EDP-auditors met verschillende achtergronden (informaticadeskundigen, technische specialisten en accountants) met elkaar samenwerken. Ernst & Young EDP Audit heeft vestigingen in Amsterdam, Apeldoorn, Den Haag, Eindhoven, Groningen, Rotterdam en Utrecht [22]. Dit onderzoek wordt uitgevoerd vanuit Apeldoorn.

In de dienstverlening aan beursgenoteerde ondernemingen moet duidelijk onderscheid worden gemaakt tussen de dienstverlening aan ondernemingen waar Ernst & Young de accountantscontrole uitvoert (controlerelaties) en ondernemingen waar dat niet het geval is (adviesrelaties) [33]. Bij Ernst & Young ziet men op dit moment groeimogelijkheden in adviesrelaties.

1.3 Onderzoeksopzet

1.3.1 Probleemstelling

Om de kwaliteit van besturing (Governance) van de automatisering (IT) bij hun klanten te kunnen beoordelen is geen formele werkwijze beschreven bij Ernst & Young EDP Audit. Methodes als CoBiT, ITIL en de Code voor Informatiebeveiliging worden wel gebruikt voor normenkaders bij de beoordeling van de kwaliteit van (delen van) IT Governance. Een beschreven overdraagbare werkwijze is op dit moment bij Ernst & Young EDP Audit niet beschikbaar maar wel gewenst, waarbij ook gebruik wordt gemaakt van andere methodes.

1.3.2 Doelstelling

Doelstelling:

Het doel van dit onderzoek is om een werkwijze te ontwikkelen waarmee de kwaliteit van besturing (Governance) van de automatisering (IT) bij organisaties wordt beoordeeld op basis van geaccepteerde methodes op het terrein van IT Governance.

Leenslag (2006)

Het doel van de werkwijze is tweeledig: De werkwijze wordt gebruikt als overdraagbare methode bij Ernst & Young EDP Audit om auditors een handleiding te geven bij het beoordelen van de kwaliteit IT Governance. Daarnaast werkt het als communicatiemiddel richting organisaties om aan te geven hoe zij *in control* blijven van hun IT processen.

1.3.3 Afbakening

In bovenstaande doelstelling wordt omschreven dat de werkwijze gebaseerd zal zijn op geaccepteerde methodes. Hieronder zal een korte beschrijving gegeven worden over de eigenschappen van methodes op het terrein van IT Governance ter afbakening van het onderzoek.

Methodes voor IT Governance worden beschreven als *frameworks*, *standards* en *best practices*. In de literatuur is de scheiding tussen deze termen niet altijd eenduidig. In dit onderzoek worden alle verschillende termen gezien als methodes voor IT Governance.

Een voordeel van standaarden is dat het wiel niet opnieuw uitgevonden hoeft te worden. Het is moeilijk voor individuele organisaties om een beter IT Management (of Governance) framework te bedenken dan bijvoorbeeld ITIL of CoBiT [45]. *Best practices* verminderen IT risico's zoals: *project failures*, *wasted investments*, *security breaches*, *system crashes* en *failures by service*

providers to understand and meet customer requirements [25]. Standaarden hebben invloed op de kwaliteit van de automatisering. Als een organisatie onderdelen van zijn IT gaat uitbesteden zal het gebruik van een standaard (als basis voor Service Level Agreements) leiden tot minder misverstanden en lagere kosten [45]. Uit gesprekken met de opdrachtgever is gebleken dat afspraken (bij klant organisaties) met een third-party vaak niet eenduidig zijn. Het ontbreken van een procesbeschrijving van Service Level Management (SLM) bij klant organisaties maakt een uitspraak over de kwaliteit van dit onderdeel zeer moeilijk. Door gebruik te maken van standaarden kan dit voorkomen worden. Ook auditors hebben een wezenlijk voordeel bij het gebruik van standaarden. Het gebruik van standaarden leidt tot lagere kosten voor zowel auditor als organisatie en het helpt beide partijen elkaar beter te begrijpen [45].

Er is niet één standaard die de volledige lading dekt als het gaat om IT Governance. Het advies is om meerdere te selecteren en te gebruiken. Voor het onderwerp security kan een combinatie van CoBiT, ISO 17799 en ITIL (security management) gebruikt worden [45]. Er zijn verschillende literatuurbronnen die het *mappen* van standaarden beschrijven [45] [26] [25] [56]. Hierbij wordt CoBiT als *overall control framework* gebruikt. Andere standaarden beschrijven specifieke IT aspecten [25]. Spafford beschrijft CoBiT, ISO 17799 en ITIL als de drie primaire IT standaarden. Hij noemt voordelen die ook door Oud [45] zijn genoemd. Een belangrijk voordeel dat door Spafford wordt genoemd is *auditable*. Zonder standaarden wordt het voor auditors moeilijker om de beheersing van IT in een organisatie te bepalen [58]. Spafford geeft voorkeur aan het gebruik van meerdere standaarden. Hierbij moet een aanpak gekozen worden die voorziet in de behoefte van een organisatie. Hij stelt een incrementele aanpak voor als het gaat om IT Governance verbetering. Selecteer eerst de gebieden die van groot belang zijn [58]. Wanneer de aandacht uitgaat naar IT security dan kan hiervoor ISO 17799 gebruikt worden. Wanneer Service Management belangrijk is kan ITIL gekozen worden [24]. Thiadens geeft het werken met methodes aan als een manier om in *control* te blijven van de ICT voorzieningen [61].

Om te voorkomen dat literatuuronderzoek naar methodes een eindeloze zoektocht wordt is een afbakening nodig. In gesprekken met de opdrachtgever zijn een aantal (CoBiT) processen aangegeven die belangrijk zijn voor dit onderzoek. Guldentops et al. hebben 15 van de 34 CoBiT processen geïdentificeerd als zeer belangrijk [18]. Aansluitend hierop hebben Van Grembergen et al. (2005) in opdracht van de IT Governance Institute een onderzoek gedaan naar de manier hoe *business goals* IT doelen aansturen in verschillende industrieën en hoe IT doelen worden ondersteund door IT processen. Voor dit onderzoek hebben Van Grembergen et al. (2005) acht verschillende industrieën geanalyseerd, namelijk:

- *Financial*
- *Health*
- *Government*
- *Retail*
- *Pharmaceutical*
- *Utilities*
- *IT Services and consulting*
- *Transportation*

Het onderzoek heeft de business goals van de verschillende sectoren in kaart gebracht en deze gekoppeld aan IT goals. Na analyse bleek dat meer dan 50% van alle goals generiek zijn. Voorbeelden hiervan zijn *IT disaster recovery and business continuity* en *standardizing IT systems*. De IT goals zijn daarna gekoppeld aan CoBiT processen. Deze generieke doelen sluiten goed aan bij de selectie CoBiT processen uit onderstaande tabel. In dit onderzoek zal aandacht besteed worden om methodes te vinden die toepasbaar zijn voor deze processen aangezien de werkwijze ook generiek moet zijn en toepasbaar moet worden voor alle type organisaties.

Ernst & Young EDP Audit	**Guldentops et al.**
	Define a strategic IT plan
	Determine technological direction
	Manage the IT investment
	Assess risk
Manage project	Manage projects
	Identify automated solutions
Acquire and maintain application software	Acquire and maintain application software
	Install and accredit systems
	Manage changes
	Define and manage service levels
Manage third-party services	
	Ensure continuous service
Ensure systems security	Ensure systems security
	Manage problems and incidents
	Manage data
	Monitor the process
Asses internal control adequacy	

Tabel 1: Selectie CoBiT processen

1.3.4 Onderzoeksvragen

In deze paragraaf worden een aantal onderzoeksvragen beschreven die zijn afgeleid van de doelstelling uit § 1.3.2. Deze worden beantwoord in de hoofdstukken van dit onderzoek.

1. Wat is IT Governance?

2. Welke invalshoeken zijn te onderscheiden voor IT Governance?

3. Wat zijn geaccepteerde methodes op het terrein van IT Governance?
   - Welke methodes zijn te vinden in de literatuur?
   - Waarin verschillende methodes van elkaar?
   - Welke overlap hebben de methodes?

- Welke deelgebieden worden ondersteund door de methodes?
- Welke methodes worden geselecteerd?

4. Welke koppeling tussen methodes is er mogelijk?
   - Op welke manier kunnen methodes aan elkaar gekoppeld worden?
   - Welke onderdelen van methodes kunnen gebruikt worden?
   - Geven de gevonden methodes voldoende dekking om een werkwijze te ontwikkelen?

5. Welke werkwijze kan met de gevonden methodes ontwikkeld worden?

6. Wat is het resultaat van de toepassing van de ontwikkelde werkwijze?
   - Wat is het oordeel van organisaties over de werkwijze?
   - Kan een beoordeling over de kwaliteit van IT Governance gemaakt worden?

1.3.5 Structuur

In deze paragraaf wordt de structuur beschreven van dit onderzoek. De structuur is ingedeeld in fases.

Werkwijze	**Resultaat**
Fase 0: Opzet	
Opzet scriptie inclusief inleiding, organisatiebeschrijving en onderzoeksopzet.	Hoofdstuk 1: Inleiding
Fase 1: IT Governance	
Bestuderen van literatuur (o.a. Weill, Ross, ITGI, ISACA, Thiadens, Starreveld, Applegate) over het onderwerp IT Governance.	Hoofdstuk 2: Definitie IT Governance Hoofdstuk 3: Invalshoeken IT Governance
Fase 2: Methodes IT Governance	
Zoeken en selecteren van methodes op het terrein van IT Governance.	Hoofdstuk 4: IT Governance methodes
Fase 3: Koppeling methodes	
Mapping & Aligning van methodes.	Hoofdstuk 5: Koppeling IT Governance methodes
Fase 4: Werkwijze	
Ontwikkelen van een werkwijze met behulp van de bevindingen van voorgaande fases.	Hoofdstuk 6: Werkwijze IT Governance beoordeling
Fase 5: Case study	
Interviews houden met om de compleetheid en toepasbaarheid te toetsen.	Hoofdstuk 7: Praktijkonderzoek
Fase 6: Conclusies & aanbevelingen	

Beschrijven van de conclusies van het onderzoek en de aanbevelingen.	Hoofdstuk 8: Conclusies & Aanbevelingen
Fase 7: Afronding	
Afmaken van het eindproduct: Scriptie	Samenvatting Reflectie Voorwoord

Tabel 2: Structuur

Dit hoofdstuk heeft de onderzoeksopzet behandeld voor deze scriptie. De volgende hoofdstukken zullen in het teken staan van de beantwoording van de onderzoeksvragen.

HOOFDSTUK 2

IT GOVERNANCE

IT Governance is a hot topic
though no one seems te be sure exactly what it is or how to explain it

(Broadbent 2003)

Met deze zeer treffende quote van Broadbent (2003) zal in dit hoofdstuk een poging gedaan worden om te beschrijven waar IT Governance over gaat. In het vorige hoofdstuk is aangegeven dat IT Governance en de kwaliteit hiervan bij veel organisaties hoog op de agenda staat. Om een werkwijze te ontwikkelen om de kwaliteit te beoordelen wordt in dit hoofdstuk het onderwerp IT Governance in meer detail verkend. De volgende onderzoeksvraag wordt behandeld:

Wat is IT Governance?

In de inleiding worden een aantal onderwerpen van IT Governance behandeld. In deze paragraaf wordt tevens beschreven waarom IT Governance belangrijk is. Dit is één van de dimensies van IT Governance. In het volgende hoofdstuk worden andere dimensies behandeld. In § 2.2 worden een aantal verschillende definities omschreven van IT Governance. Het hoofdstuk eindigt met een samenvatting over het onderwerp, waarbij een kader wordt geschept van IT Governance waar de werkwijze zich op zal richten.

2.1 Inleiding IT Governance

Zoals al eerder is beschreven is IT Governance een onderdeel van Corporate Governance [46]. NOREA, de beroepsorganisatie van IT-auditors, beschrijft dat de essentie van Corporate Governance het goed besturen van organisaties is en het aantoonbaar maken dat dit ook zo gebeurt. Hierbij gaat het om de wijze waarop de ondernemingsleiding bij de besturing van de organisatie rekening houdt met andere dan haar eigen belangen, zoals belangen van aandeelhouders, werknemers en de samenleving als geheel. Kort gezegd gaat het erom wat goed bestuur inhoudt, hoe daarop adequaat kan worden toegezien en hoe daarover verantwoording kan worden afgelegd aan de belanghebbenden ook wel *stakeholders* genoemd. De organisatieleiding moet in de meeste gevallen richting de belanghebbenden aantoonbaar kunnen maken dat zij de bedrijfsprocessen beheerst [44]. Het onderdeel IT Governance geeft aan hoe een organisatie de activiteiten bestuurt of beheerst die een verband hebben met informatie technology (IT) en het gebruik van IT [46].

Informatievoorziening ondersteunt een organisatie bij het realiseren van haar doelstellingen. De toepassing van informatietechnologie stelt een organisatie in staat producten efficiënter en effectiever te produceren, innovatiever te zijn en processen beter te beheersen. De IT-functie kan zich verheugen in een toenemende belangstelling van het management van een organisatie. De verwachtingen van een organisatie ten aanzien van de kwaliteit van informatievoorziening, functionaliteit, gebruikersgemak en snelheid van oplevering van nieuwe systemen zijn sterk toegenomen. Daarnaast vragen de snelheid van veranderingen op het gebied van informatie- en communicatietechnologie en de snelheid van veranderingen binnen organisaties om een adequate beheersing van de IT-risico's. De grote(re) afhankelijkheid van de informatiesystemen voor kritische bedrijfsprocessen vraagt om IT-beheerprocessen die nauwgezet zijn afgestemd op de organisatie [44].

De reden waarom IT Governance belangrijk is heeft te maken met het feit dat in het recente verleden grote IT investeringen zijn mislukt. Weill et al. (2004) noemen een aantal voorbeelden zoals slecht ontworpen of matig uitgevoerde *e*-business ondernemingen en nieuw ontwikkelde systemen die nooit effectief zijn gebruikt. Daartegenover zijn er organisaties die jaar na jaar bovengemiddeld scoren op verdiensten van hun IT investeringen. Deze succesvolle organisaties nemen niet alleen betere IT beslissingen maar ze nemen ze ook consequent. Deze organisaties hebben een betere IT Governance. Ze hebben mensen die betere IT gerelateerde beslissingen nemen dan hun concurrenten [75]. Hieruit blijkt al één van de redenen om IT Governance toe te passen, om gedegen IT beslissingen te nemen zodat organisaties een betere *value for IT* kunnen krijgen.

De ITGI (2003) geeft aan dat IT al enige tijd zeer belangrijk is voor het succes van organisaties. IT geeft een mogelijkheid om een concurrerend voordeel te behalen en biedt een middel voor het verhogen van de productiviteit. IT zal in de toekomst alleen nog maar belangrijker worden voor

het succes van organisaties [27]. Goed bestuur van IT is daarom belangrijk om de doelen van de organisatie mogelijk te maken.

Naast deze redenen geven Weill et al. (2004) nog aantal redenen waarom IT Governance zo belangrijk is. Grewal en Knutsson (2005) geven een overzicht van deze redenen [bijlage: I]. Gebruikmakend van deze twee bronnen zal hieronder een kort overzicht gegeven worden van de redenen:

- Good IT Governance pays off
- IT is expensive
- IT is pervasive
- New information technologies bombard enterprises with new business opportunities
- IT Governance is critical to organizational learning about IT value
- IT Value depends on more than good technology
- Senior management has limited bandwith
- Leading enterprises govern IT differently

Omdat er steeds meer geïnvesteerd wordt in IT is het nodig om een structuur te ontwikkelen die zorgt voor toegevoegde waarde van de investeringen voor organisaties. Met een succesvolle IT Governance kan een organisatie zich onderscheiden ten opzichte van concurrenten. Een IT Governance structuur moet zorgen voor een betere koppeling met de rest van de organisatie en met de strategie.

Uit deze inleiding valt gelijk op dat bij het begrip Governance, en in het bijzonder IT Governance, het onderwerp “besturen” wordt gebruikt om IT Governance te omschrijven. Deze en andere onderwerpen van IT Governance worden in dit hoofdstuk behandeld om een kader te scheppen voor het vervolg van dit onderzoek.

2.2 Definitie

Attempting to define IT Governance: wisdom or folly?

(Webb et al. 2006)

In de literatuur worden door verschillende auteurs en verschillende instanties definities gegeven voor IT Governance. Deze definities verschillen ten opzichte van elkaar maar hebben ook overeenkomsten. Het effect van verschillende definities is dat er verwarring ontstaat over het begrip IT Governance. Dit werd al even aangehaald in de quote van Broadbent (2003) aan het begin van dit hoofdstuk. Deze verwarring hindert de effectieve communicatie over het onderwerp zowel bij academici als bij pragmatici. Verschillende auteurs hebben hiervoor een studie gedaan naar de definitie van IT Governance [74] [36].

The IT Governance literature includes a range of definitions providing different perspectives on the concept of IT Governance [74].

Webb et al. (2006)

Structures of the IT function and mechanisms, *control frameworks* en *processes* zijn Engelse termen die veel worden gebruikt in de literatuur om IT Governance te beschrijven. Deze termen representeren belangrijke concepten en hulpmiddelen voor de toepassing, implementatie en ontwikkeling van IT Governance. Webb et al. (2006) geven aan dat deze termen *niet* IT Governance definiëren [74]. Echter zijn ze vaak *wel* terug te vinden in diverse definities. Wanneer de definities van IT Governance in de literatuur bestudeerd worden maken Jordan (2005) en Keyes-Pearce (2002) ook onderscheid in *structures (with and without (control) mechanisms)* en *processes* [36] [34]. Deze termen zullen in het vervolg van dit onderzoek worden aangeduid met structuren, mechanismen en processen. De volgende definities worden in dit hoofdstuk behandeld:

Definitie IT Governance (1):

Specifying the framework for decision rights and accountabilities to encourage desirable behavior in the use of IT [75].

Weill et al. (2002)

Het wenselijke gedrag van IT moet volgens Weill et al. (2002) consistent zijn met de missie, strategie, waarde en normen en cultuur van een organisatie. Deze samenhang tussen de *business organization* en *IT organization* is duidelijker terug te vinden in de definitie van Van Grembergen (2004) en in de definitie van de IT Governance Institute (ITGI).

Definitie IT Governance (2):

IT Governance is the organisational capacity exercised by the Board, executive management and IT management to control the formulation and implementation of IT strategy and in this way ensure the fusion of business and IT [69].

Van Grembergen et al. (2002)

In de definitie van Van Grembergen et al. (2002) wordt de samenhang aangegeven middels de *organisational capacity to control*. Payne (2003) en Rao (2003) in Ridley (2005) geven ook aan dat *control* een vereiste is voor effectieve IT Governance [39]. Omdat *control* een belangrijk onderdeel is in de definitie van Van Grembergen (2002) (en van IT Governance) wordt dit onderwerp verder uitgewerkt. Driessen et al. (2001) geven aan dat *control* (beheersingsmaatregelen) in feite een instrument is voor managers op alle lagen in de organisatie om er voor te zorgen dat de activiteiten leiden tot het gewenste resultaat (output) [11]. Een set van beheersingsmaatregelen is hetzelfde als een regelkring [12] in [11]. Een regelkring bestaat uit vijf stappen, te weten:

- Meten van de feitelijke situatie
- Vergelijken van de feitelijke situatie met de norm
- Signaleren van een eventuele afwijking
- Selecteren van een actie om de relevante afwijking op te heffen
- Uitvoeren van de geselecteerde actie

Deze omschrijving van *control* sluit goed aan bij de definitie die bij CoBiT wordt gebruikt [24]:

Definitie *control*:

Control is defined as the policies, procedures, practices and organisational structures designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented or detected and corrected.

CoBiT (2006)

Deze beschrijving van *control* sluit goed aan bij de definitie van IT Governance gegeven door de IT Governance Institute. Hierbij is de koppeling tussen de IT en de rest van de organisatie duidelijk terug te vinden.

Definitie IT Governance (3):

IT Governance is the responsibility of executives and the board of directors, and consists of the leadership, organisational structures and processes that ensure that the enterprise's IT sustains and extends the organisation's strategies and objectives [24].

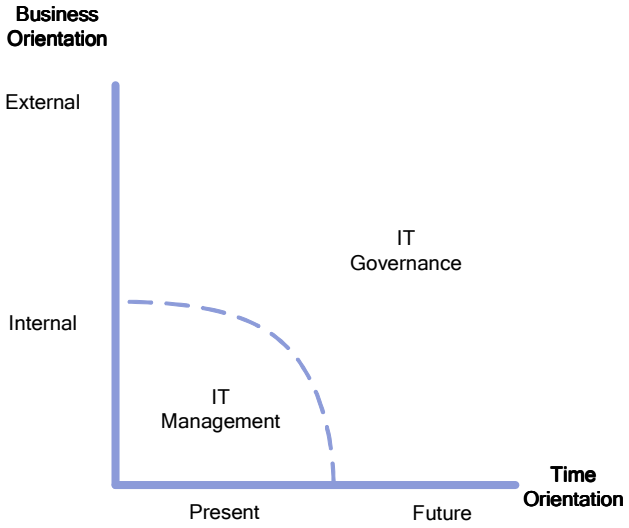
IT Governance Institute (2006)

IT Governance zorgt ervoor dat de IT uitgelijnd is met bedrijfsprocessen en dat deze op de juiste manier georganiseerd, bestuurd en beheerst is. IT Governance verschaft de structuur die een link legt tussen IT processen, IT resources en informatie met de organisatie strategie en doelen [4]. Dit wordt ook aangegeven door Van Grembergen (2002).

In de definitie van Van Grembergen (2002) wordt aangegeven dat IT Governance wordt uitgeoefend door onder andere IT Management. Sohal (2002) geeft aan dat IT Management en IT Governance verschillende functies zijn die elkaar aanvullen. Tevens geeft Sohal (2002) aan dat er weinig literatuur is die het onderscheid aantoont tussen deze twee functies. Vaak worden deze twee functies als synoniemen gezien [54]. De NOREA stelt dat IT Governance gaat over spelregels, vaststellen van het kader waarbinnen anderen opereren, beleid en aansturing. IT management is gericht op de uitvoering, besluitvorming en verantwoording van IT-activiteiten binnen de gestelde kaders. Procesmodellen als ITIL, Prince2 en CMM zijn beschikbaar om de organisatie van de IT-activiteiten en IT-processen te optimaliseren [44]. Dit is tevens terug te vinden in het onderscheid in de twee functies die Peterson (2003) aangeeft. Peterson probeert dit onderscheid aan te tonen op de volgende manier:

> **IT Management is focused on the internal effective supply of IT services and products and the management of present IT operations. IT Governance in turn is much broader, and concentrates on performing and transforming IT to meet present and future demands of the business (internal focus) and the business' customers (external focus) [49] (Figuur 4). This does not undermine the importance and complexity of IT management, …, but whereas elements of IT Management and the supply of (commodity) IT services and products can be commissioned to an external provider, IT Governance is organisation specific, and direction and control over IT can not be delegated to the market.**
>
> **Peterson (2003)**

Hierbij wordt het onderscheid aangegeven door middel van *supply* (IT Management) en *demand* (IT Governance). In dit onderzoek wordt deze mening niet gedeeld en omvat IT Governance zowel de *supply*- als de *demand side*. IT Governance en IT Management zijn in deze optiek elkaars verwante. Uit bovenstaande blijkt dat verschillende auteurs een onderscheid maken tussen begrippen als IT Governance en IT Management. In dit onderzoek wordt afgezien om scherp de verschillen tussen deze begrippen te definiëren. In dit onderzoek wordt onder IT Governance, (IT) sturing en IT Management hetzelfde verstaan.



Figuur 4: IT Management & IT Governance

2.3 Samenvatting IT Governance

Om antwoord te geven op de onderzoeksvraag: "*Wat is IT Governance?"* zijn verschillende definities bestudeerd. De conclusie hierbij is dat er relatief veel definities zijn van IT Governance. Een overzicht van verschillende definities wordt gegeven door Webb et al. (2006) en Keyes-Pearce (2002). Tijdens de verkenningsfase van dit onderzoek en bij het schrijven van dit hoofdstuk zijn veel van deze definities bestudeerd. De auteur van dit document is van mening dat de definities van de ITGI het beste aansluit bij de doelstelling van dit onderzoek. De reden hiervoor is dat in deze definitie een duidelijke koppeling wordt gelegd tussen de organisatie en IT. De verantwoordelijkheid ligt hierbij niet alleen bij de CIO of IT Manager maar ook bij het bestuur.

De gekozen definitie heeft een sterke koppeling met de definitie van *control* (beschreven door de ITGI) die op zijn beurt weer een sterke koppeling heeft met de definitie van *control* beschreven door Driessen et al. (2001). *Control* wordt als essentieel gezien voor effectieve IT Governance. Dit onderwerp wordt in dit onderzoek als kader gebruikt waar vanuit IT Governance wordt benaderd. De werkwijze om IT Governance te beoordelen wordt opgezet om de mate van *control* te bepalen bij organisaties.

Naast dit kader zijn in de literatuur een aantal termen gevonden die regelmatig gebruikt worden om IT Governance te omschrijven. Deze termen representeren belangrijke concepten en hulpmiddelen voor IT Governance. Deze concepten en hulpmiddelen zijn: structuur, mechanismen en processen. Deze worden in het onderzoek gebruikt om een IT Governance benadering en werkwijze op te zetten. Zowel de eigen benadering als de werkwijze moeten gestructureerd zijn waarbij mechanismen het mogelijk maken om de mate van *control* (kader) van IT processen te beoordelen.

HOOFDSTUK 3

INVALSHOEKEN IT GOVERNANCE

A good understanding of the business environment, risk appetite, business strategy, IT organization and knowledge of critical IT-related issues and change drivers for the use of IT is essential for a successful IT governance implementation.

Kordel (2004)

In het vorige hoofdstuk is uit de literatuur een definitie gekozen de gehanteerd wordt voor dit onderzoek. Daarnaast zijn verschillende concepten geïdentificeerd die worden gebruikt om een IT Governance benadering en werkwijze op te zetten. Hiervoor is het nodig om verschillende invalshoeken te bestuderen van IT Governance. In dit hoofdstuk wordt daarom ook de volgende onderzoeksvraag behandeld:

Welke invalshoeken zijn te onderscheiden voor IT Governance?

Om antwoord te kunnen geven op deze onderzoeksvraag worden verschillende invalshoeken van IT Governance gedefinieerd. Met het begrip invalshoek wordt bedoeld het punt van waaruit men een zaak of probleem benadert. In § 3.1 worden de invalshoeken van IT Governance beschreven. In § 3.2 t/m § 3.4 worden drie soorten IT Governance benaderingen onderscheiden. Deze drie benaderingen worden bestudeerd om te bekijken hoe ze de invalshoeken van IT Governance behandelen. In § 3.5 wordt een eigen IT Governance benadering opgezet die voor dit onderzoek wordt gebruikt.

3.1 Inleiding IT Governance invalshoeken

Aanvullend op de gekozen definitie van IT Governance uit het vorige hoofdstuk beschrijft de NOREA dat IT Governance gaat over het besturen, beheersen, uitvoeren, verantwoording afleggen over en het toezicht op de informatievoorziening binnen een organisatie [44]. De beschrijving van de NOREA over IT Governance sluit goed aan bij de algemene beschrijving van *in control* gegeven door Driessen et al. (2001):

Definitie *in control*:

De wijze van sturen, beheersen en toezicht houden, gericht op een effectieve en efficiënte realisatie van strategische en operationele doelstellingen alsmede het hierover op een open wijze communiceren en verantwoording afleggen ten behoeven van belanghebbenden [11].

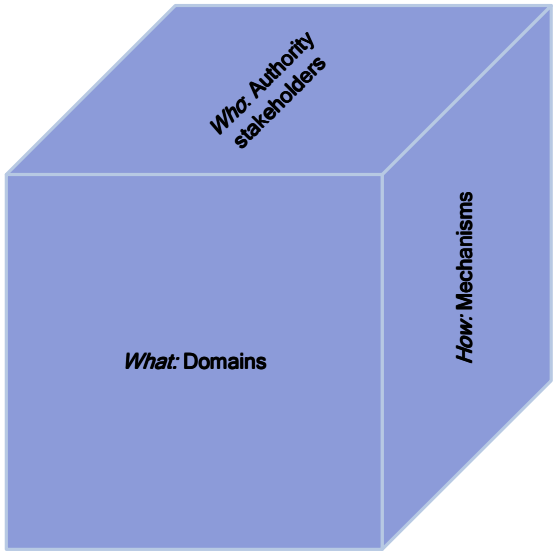
Driessen et al. (2001)

Broadbent (2003) identificeert drie dimensies voor IT Governance die aansluiten op de definities van IT Governance en worden gebruikt als invalshoeken. Deze drie componenten beschrijven de *what, who* en *how* van IT Governance. Deze dimensies van Broadbent (2003) zijn in de definitie van Driessen et al. (2001) over *in control* terug te vinden. De wijze van sturen, beheersen en toezicht houden beschrijft de *how*. Effectieve en efficiënte realisatie van strategische en operationele doelstellingen geeft de *what* aan. De belanghebbenden vertegenwoordigen de *who* dimensie.

Dalles (2002) breidt de dimensies van Broadbent uit door invulling te geven aan deze componenten. De *what* vertaalt zij naar de domeinen van IT, en beschrijft de *focus areas* van IT Governance. De *Who* geeft de *stakeholders* aan die verantwoordelijk zijn. De *how* geeft de structuur en processen aan [9]. Broadbent koppelt deze laatste aan *mechanisms*. Deze laatste drie begrippen werden eerder al in verschillende definities aangetroffen.

Deze drie invalshoeken van IT Governance worden gebruikt voor het metamodel (model van een model) om IT Governance benaderingen te structuren en te bestuderen voor dit onderzoek. Dit metamodel heeft de structuur zoals weergegeven in Figuur 5: IT Governance metamodel.

Met deze indeling voor IT Governance worden drie soorten IT Governance benaderingen bestudeerd. McLane (2003) heeft in zijn literatuurstudie onderscheid gemaakt in een *research based approach* en *standards based approach* (*practicitoners based approach*) [40]. Deze twee benaderingen worden ook door andere auteurs beschreven [17] [44] [69]. Het verschil tussen de twee benaderingen zal aangetoond worden middels de *what, who*, en *how* indeling. De *research based approach* is ontworpen door Weill et al. en de *practicitoners based approach* is gebaseerd op het werk van de ITGI en ISACA. Een derde benadering wordt beschreven door Thiadens, gebruikmakend van literatuur van onder andere Applegate en McFarlan en wordt in dit onderzoek gezien als de *educational approach*.



Figuur 5: IT Governance metamodel

3.2 Research based approach

De *research based approach* is gebaseerd op onderzoek van Weill et al. [6] [75] [78] [76]. Hiervoor zijn door Weill et al. grote organisaties over de hele wereld onderzocht in samenwerking met Gartner. Hierop gebaseerd hebben ze een IT Governance framework opgezet dat gebruikt kan worden om IT Governance te analyseren. Zij zien IT Governance als het specificeren van beslissingsrechten en verantwoordelijkheden voor belangrijke IT beslissingen. Organisaties die goed presteren hebben onderling en ten opzichte van andere organisaties verschillende IT Governance modellen:

> **Top performers design their IT Governance to reinforce their performance goals and link IT Governance to the governance of their other key enterprise assets.**
>
> **Weill et al. (2004)**

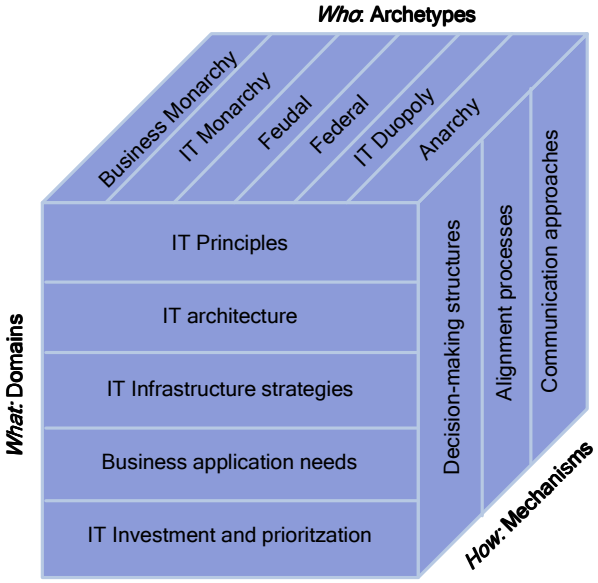
De conclusie die Weill et al. trekken uit hun onderzoek is dat niet één IT Governance model bestaat dat werkt voor elke organisatie. De koppeling met de rest van de organisatie is erg belangrijk bij IT Governance.

> **In our study of almost 300 enterprises around the world, we did not identify a single best formula for governing IT. However, one thing is clear: effective IT Governance doesn't happen by accident. Top performing enterprises carefully design governance. Managers throughout the enterprise make daily decisions putting that design into practice [77].**
>
> **Weill et al. (2004)**

De drie besproken componenten uit de vorige paragraaf worden op de volgende (samenvattende manier) door Broadbent (2003) beschreven:

> **First, five IT domains — IT principles or maxims, infrastructure strategies, architecture, business applications needs, IT investment and prioritisation — are areas where critical top-level decisions need to be made. Second, IT-governance styles define who provides input and who makes decisions in the IT domains. Third IT-governance mechanisms are techniques used to implement the IT-governance style [5].**
>
> **Broadbent (2003)**

In de bijlage [II] wordt een detailbeschrijving van deze drie dimensies beschreven. Wanneer de drie dimensies in het metamodel worden geplaatst ontstaat het onderstaande IT Governance model (Figuur 6: Research based IT Governance model). Dit model geeft de invalshoeken van IT Governance weer volgens de IT Governance benadering van Weill et al.

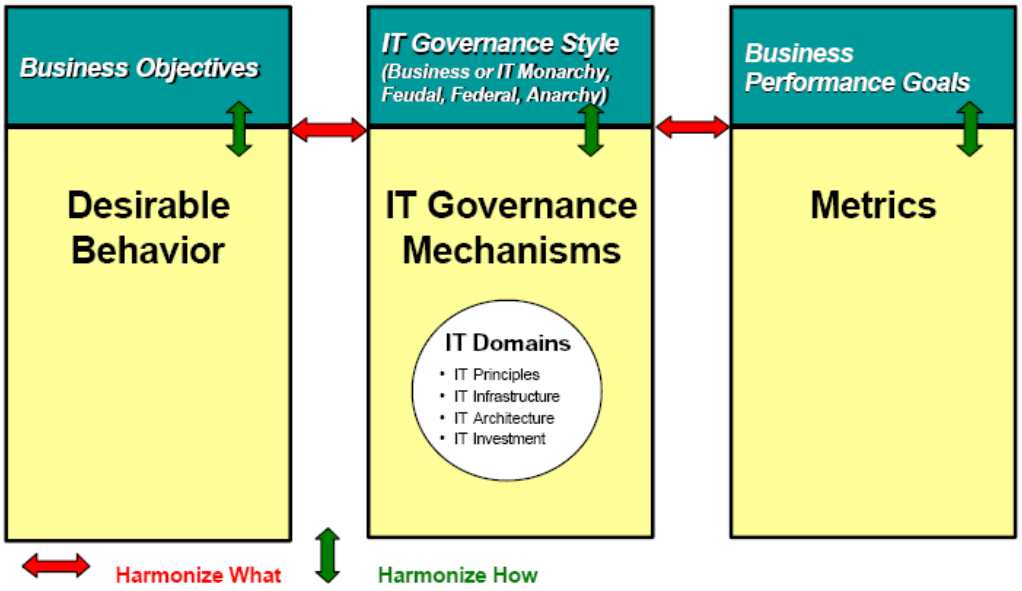


Figuur 6: Research based IT Governance model

Het onderzoek van Weill et al. heeft geleid tot de ontwikkeling van een IT Governance framework (Figuur 7: Research based IT Governance framework). De gedachtegang bij dit framework is:

Effective Governance requires the harmonization (i.e., the horizontal arrows) of business objectives, IT Governance style and business performance goals [75].

Weill et al. (2004)



Figuur 7: Research based IT Governance framework

Het framework van Weill et al. levert een manier op om IT Governance te analyseren. Het implementeren van IT Governance vereist een weloverwogen proces dat elk element van het framework specificeert en harmoniseert [78]. Om dit te bereiken worden er door Weill et al. een aantal stappen besproken. Deze stappen staan beschreven in de [bijlage: III].

Creating effective IT governance is critical if firms are to exploit information technology to achieve their business performance goals. Our framework provides a way to analyze IT governance combining IT domains, governance archetypes, mechanisms and metrics to encourage desirable behavior that supports the firms' performance objectives. Implementing effective IT governance requires a deliberate process, carefully specifying and harmonizing each of the elements in the framework. Each firm's governance structure will be unique to its objectives and performance goals.

Weill et al. (2004)

3.3 practicitoners based approach

Een pragmatische kijk op IT Governance is te vinden in een IT Governance framework gebaseerd op standaarden. Spafford (2003) geeft aan om standaarden te gebruiken als het gaat om IT Governance. Voordeel hierbij is dat gebruik wordt gemaakt van gecombineerde ervaringen van honderden organisaties en mensen [58]. Belangrijke instanties die deze benadering ondersteunen zijn de ITGI en de ISACA. Deze instanties hebben een belangrijke rol bij het ontwikkelen van een pragmatische op standaarden gebaseerd IT Governance framework.

Beschrijving ITGI:

The IT Governance Institute (ITGI) strives to assist enterprise leaders in their responsibility to make IT successful in supporting the enterprise's mission and goals. Its goals are to raise awareness and understanding among and provide guidance and tools to boards of directors, executive management and chief information officers (CIOs) such that they are able to ensure within their enterprises that IT meets and exceeds expectations, and its risks are mitigated [27].

ITGI (2003)

Beschrijving ISACA:

The Information Systems Audit and Control Association (ISACA®) is an international professional, technical and educational organisation dedicated to being a recognised global leader in IT governance, control and assurance. With members in more than 100 countries, ISACA is uniquely positioned to fulfill the role of a central harmonising source of IT control practice standards the world over. Its strategic alliances with other organisations in the financial, accounting, auditing and IT professions ensure an unparalleled level of integration and commitment by business process owners [27].

ITGI (2003)

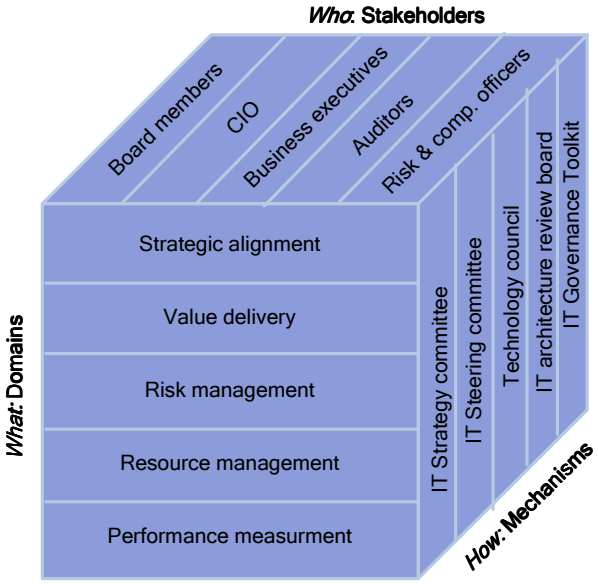
Een voordeel van standaarden is dat het wiel niet steeds opnieuw uitgevonden hoeft te worden. Standaarden hebben een positieve invloed op de kwaliteit van de automatisering, zoals ook al eerder werd omschreven.

Met dezelfde indeling als bij de *research based framework* (*what, who, how*) zal nu ook deze benadering van IT Governance bestudeerd worden. Het eerst component is *what*. Hiervoor heeft de ITGI ook een aantal domeinen (*focus areas*) opgezet na bestudering van marktanalyses van Gartner, Compass, Giga en CSC.

Fundamentally, IT governance is concerned about two things: IT's delivery of value to the business and mitigation of IT risks. The first is driven by strategic alignment of IT with the business. The second is driven by embedding accountability into the enterprise. Both need to be supported by adequate resources and measured to ensure that the results are obtained. This leads to the five main focus areas for IT governance.

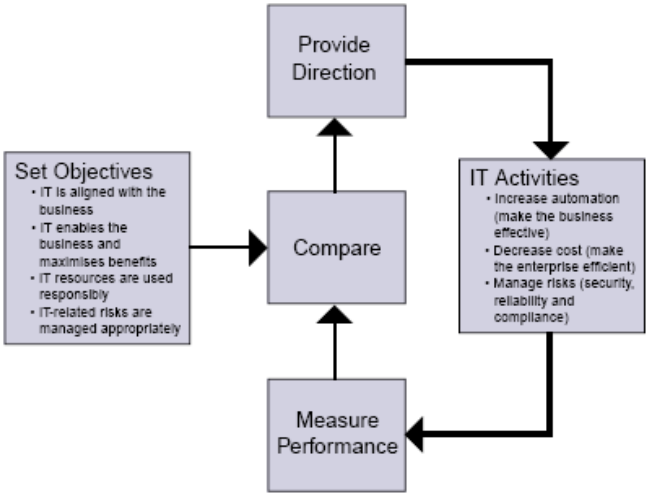
ITGI (2003)

Uit deze doelstelling zijn de vijf *focus areas* van IT Governance te onderscheiden. De andere twee dimensies (*who* en *how*) zijn af te leiden uit de *Board briefing on IT Governance* en staan beschreven met de *focus areas* in de [bijlage IV]. Wanneer deze dimensies toegepast worden op het eerder beschreven metamodel ontstaat het volgende IT Governance model.



Figuur 8: Practicitoners based IT Governance model

Er lijkt wat verwarring te ontstaan als bij de ITGI het IT Governance framework wordt gezocht. De zoektocht levert twee resultaten op. Het eerste is het IT Governance framework zoals weergeven in de *Board briefing on IT Governance*. Dit is een abstract framework:



Figuur 9: IT Governance framework

Het *tweede* IT Governance framework wat door de ITGI, ISACA en andere wordt aangedragen is CoBiT. Dit is een concreter framework dan het eerste.

COBIT (Control Objectives for Information and related Technology), issued by the IT Governance Institute, is increasingly accepted internationally as good practice for control over information, IT and related risks. Its guidance enables an enterprise to implement effective governance over the IT that is pervasive and intrinsic throughout the enterprise [27].

ITGI (2006)

De volgende aanname over deze twee IT Governance frameworks wordt hier gemaakt:

CoBiT wordt gezien als een instantie van het abstracte framework omschreven door de ITGI wat toepasbaar is in de praktijk.

Leenslag (2006)

In het CoBiT 4.0 document wordt CoBiT gezien als een control framework dat dient als *umbrella framework for IT governance* [24]. In tegenstelling tot het *research based framework* worden er bij CoBiT hele duidelijke processen onderscheiden. Dat maakt dit IT Governance framework concreet toepasbaar. In de *board briefing on IT Governance* worden net als in het Weill et al. framework een aantal stappen voorgesteld om IT Governance te implementeren [bijlage V].

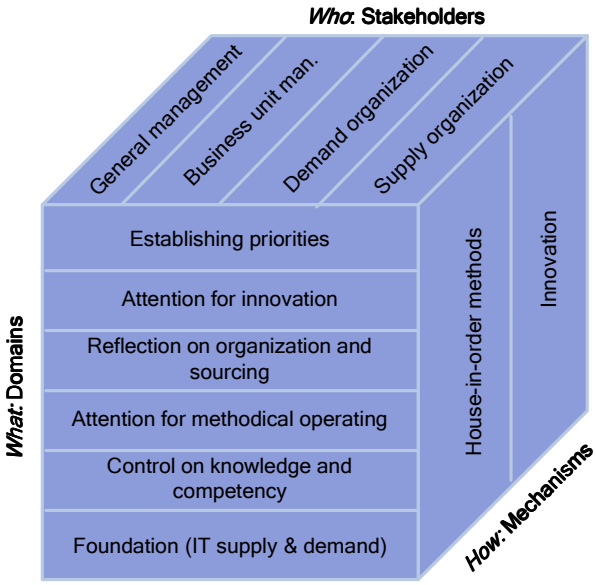
3.4 Educational based approach

Thiadens (2004) beschrijft dat we dagelijks te maken hebben met onderwerpen als IT alignment, verkorting van de doorlooptijd van idee naar implementatie, outsourcing, klantgerichtheid van ICT-afdelingen en kanteling van de ICT-organisatie. Dit zijn onderwerpen die direct te maken hebben met de sturing van ICT-voorzieningen door algemeen (*general*) en *business unit management* van een organisatie en de consequenties van de sturing op de ICT-organisatie zelf. Sturing (*Governance*) van ICT-voorzieningen is een onderwerp met diverse *stakeholders*. Er is een vraagorganisatie en een aanbodorganisatie [62].

Thiadens (2004) geeft aan dat er zes onderwerpen van sturing zijn. Dit is gebaseerd op het werk van Applegate (2003). Figuur 10: Educational based IT Governance model geeft in de *what* dimensie aan welke onderwerpen aandacht moeten krijgen bij sturing van ICT-voorzieningen.

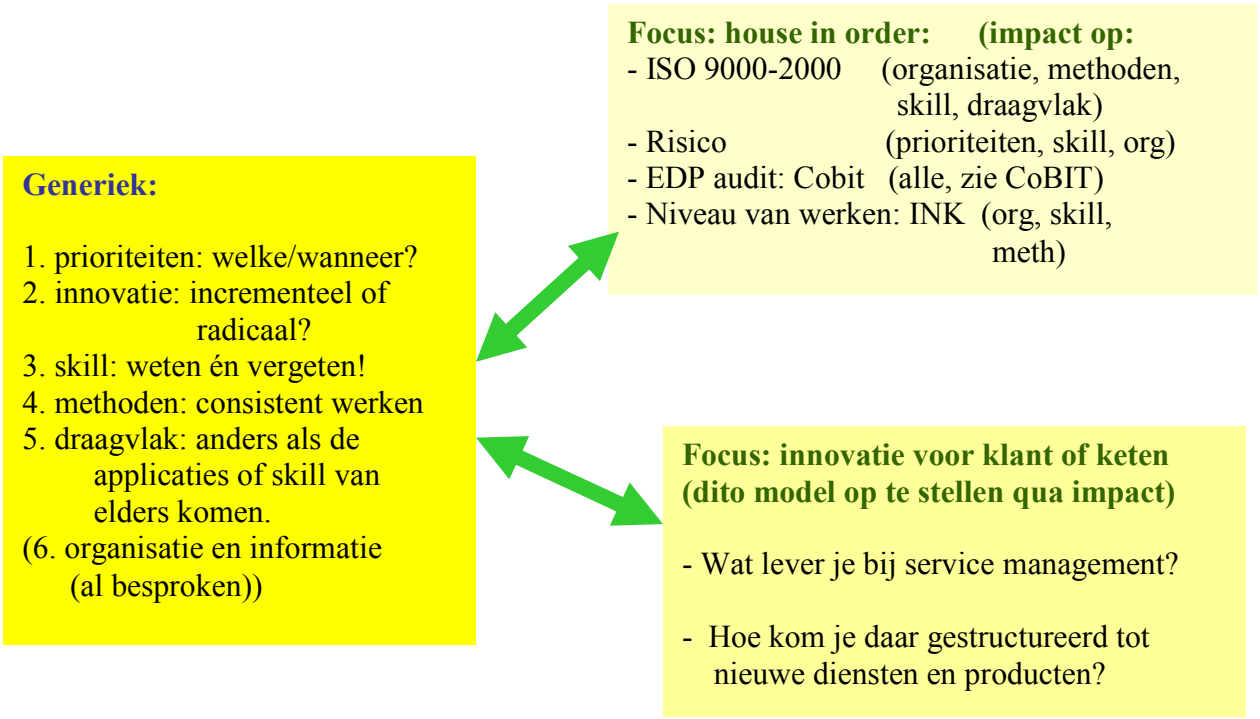
De *who* dimensie geeft *stakeholders* weer die door Thiadens (2004) worden onderscheiden. De sturing van algemeen management is erop gericht om te komen tot een zo optimaal mogelijke ondersteuning van de strategie van de organisatie door ICT op de korte, de middellange en de lange termijn. Business unit management stuurt direct vanuit de vraag naar ICT-voorzieningen. Het streeft een optimale ondersteuning van de bedrijfsprocessen na. De functioneel beheerorganisatie bundelt de vragen. Zij tracht zo optimaal mogelijk op de vraag van algemeen en business unit management in te springen en inzet van ICT-voorzieningen daarop te organiseren. In de gewenste ICT-voorzieningen wordt voorzien door de ICT-aanbodorganisaties (weergegeven door *supply organization*) [62].

Sturing van ICT-voorzieningen betekent onder meer sturing van processen in een ICT-organisatie. Methodes geven aan welke processen er kunnen worden ingericht. Met *house-in-order* worden methodes bedoeld om diensten en producten van een organisatie te verbeteren of zijn meer gericht op het stellen van normen aan producten en diensten. Thiadens (2004) beschrijft in zijn boek een verzameling van methodes [62]. Deze *house-in-order* methodes zijn de *mechanisms* en beschrijven de *how* dimensie.



Figuur 10: Educational based IT Governance model

Het framework wat hierbij hoort wordt weergegeven in
Figuur 11: educational IT Governance **framework**. Dit framework bestaat uit een deel van altijd aanwezige *controls* en een deel van specifieke sturing. Dit kan gericht zijn op house-in-order of op innovatie. Deze kan in het voordeel van de keten zijn, of in het voordeel van de klant.



Figuur 11: educational IT Governance framework

3.5 Eigen IT Governance approach

A major conclusion is that governing the enterprise's Information Technology is becoming more and more important in our knowledge-based and complex society. Key elements in IT Governance are the alignment of the business and IT that must lead to the achievement of business value through IT. These high level goals of IT Governance can be achieved by acknowledging IT Governance as a part of Corporate Governance and by setting up an IT Governance framework and its corresponding best practices. Such a framework and practices should be composed of a variety of structures, processes and relational mechanisms [69].

Van Grembergen (2004)

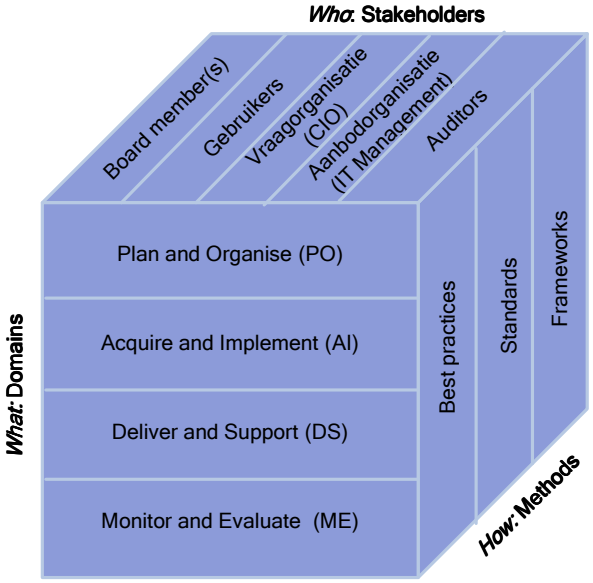
De volgende stap in het onderzoek, zoals ook Van Grembergen (2004) wordt aangegeven, is om een eigen IT Governance framework op te zetten en de daarbij horende *best practices* te zoeken.

Eerst wordt voor dit onderzoek een IT Governance model opgezet (Figuur 12: Wilco IT Governance model) waarvoor in het volgende hoofdstuk methodes (*best practices*, standaarden en *frameworks*) worden geselecteerd. Dit model is vanuit de literatuur opgezet en moet leiden tot een framework om aan de doelstelling van dit onderzoek te voldoen.

Voor dit "Wilco model" is gekozen om de aandachtsgebieden van CoBiT te gebruiken als domeinen. In het volgende hoofdstuk worden methodes gezocht die de aandachtsgebieden en processen concrete invulling geven. De *focus areas* zoals beschreven door de ITGI worden (niet verwonderlijk) goed ondersteund door de aandachtsgebieden (en processen) van CoBiT. De *focus areas* van Weill et al. zijn ook te relateren aan de aandachtsgebieden van CoBiT. De *focus areas* zoals beschreven door Thiadens zijn gedeeltelijk terug te vinden.

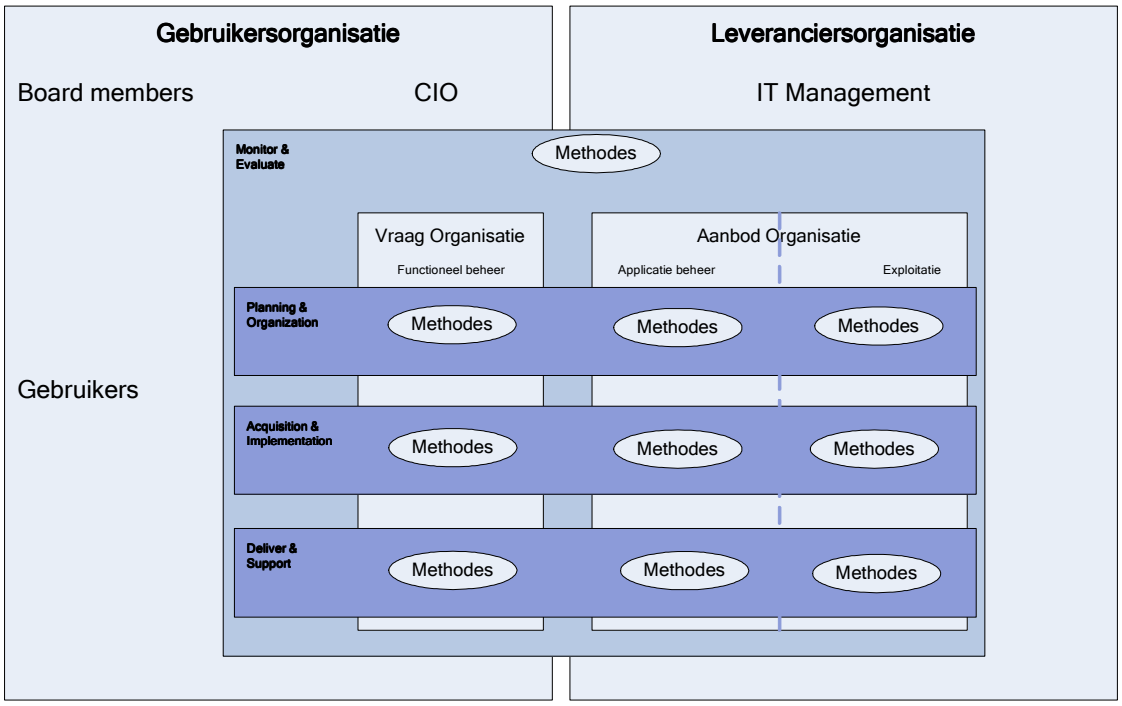
Met betrekking tot de stakeholders maakt de *educational approach* een duidelijk onderscheid in functioneel beheer (*demand*) en applicatiebeheer & technisch beheer (*supply*). Het onderscheid in deze typen beheer wordt door de ITGI niet expliciet gemaakt. In de praktijk zal door outsourcing het onderscheid juist wel expliciet zijn. Voor de eigen IT Governance benadering wordt gekozen om de vraag- en aanbodkant van een IT organisatie wel expliciet te maken. Bij het selecteren van methodes zal hier aandacht aan besteed worden.

Al meerdere keren is gemeld dat de verantwoordelijkheid van IT Governance bij het bestuur ligt. Dus het is belangrijk dat een lid (of meerdere leden) van het bestuur deelnemen aan een IT Governance initiatief. Thiadens maakt een onderscheid in de vraagkant van de organisatie en de aanbodkant van de organisatie. De CIO wordt in het onderstaande model gezien als de persoon om de vraagorganisatie op zich te nemen. De CIO van een organisatie zorgt voor de koppeling tussen de IT en de *business* [27]. De IT Manager vervult een belangrijke rol bij de aanbodorganisatie. In het IT Governance model heeft de EDP Auditor ook een rol.



Figuur 12: Wilco IT Governance model

Voor een groot gedeelte zijn de aandachtsgebieden van Weill et al. en ITGI terug te vinden in de domeinen van het Wilco IT Governance model. De stakeholders van de ITGI en Thiadens worden gebruikt. De benadering omschreven door Thiadens zal een grote invloed hebben op de invulling van de methodes voor dit IT Governance model. Het bijbehorende IT Governance framework wordt in Figuur 13: Wilco IT Governance framework weergegeven. Hiervoor worden in het volgende hoofdstuk methodes gezocht om het framework concrete invulling te geven.



Figuur 13: Wilco IT Governance framework

3.6 Samenvatting invalshoeken IT Governance

Om antwoord te geven op de tweede onderzoeksvraag: "*Welke invalshoeken zijn te onderscheiden voor IT Governance?"* is in dit hoofdstuk een metamodel ontworpen om verschillende invalshoeken van IT Governance te structureren en te bestuderen. Dit metamodel heeft geresulteerd in een vergelijking van verschillende IT Governance benaderingen uit de literatuur (Tabel 3: Overzicht IT Governance benaderingen).

De benadering van Weill et al. richt zich op beslissingen die genomen moeten worden. Zij beschrijven dat effectieve IT Governance de volgende vragen adresseert: "*what decisions must be made?*", "*who should make these decisions?*" en "*how will we make and monitor these decisions?*" [78]. Dit richt zich dus voornamelijk op de *stakeholders* en *committees* van IT Governance en is minder procesgericht. De *alignment processes* die beschreven worden bij de mechanismen (Tabel 3) zijn beperkt. De benadering van Weill et al. beschrijft in belangrijke mate de aandachtsgebieden waarover besluiten genomen dienen te worden zoals: de visie op en uitgangspunten voor het gebruik en toepassing van IT binnen de organisatie, de IT-infrastructuur, de IT-architectuur, business behoeften en IT-prioriteiten. Verder onderscheidt men de beslissingsnemers/besturingsmodellen variërend van centraal tot decentraal en de verschillende mechanismen als organisatievormen en hulpmiddelen om de besluitvorming voor de aandachtsgebieden gestalte te geven. In tegenstelling tot CoBiT wordt niet gesproken over uit te voeren processen [44]. Dit laatste maakt het IT Governance framework van de ITGI nou net zo interessant. De toepasbaarheid van de IT Governance benadering van Weill et al. is in de ogen van de auteur van deze scriptie beperkt in combinatie met de doelstelling uit hoofdstuk 1 en het kader waarvoor de werkwijze wordt opgezet. De *educational approach* geeft met zijn *house-in-order* mechanismen duidelijke methodes aan om diensten en producten van organisaties te verbeteren. De diensten en producten komen tot stand door het uitvoeren van processen.

	Weill et al.	**ITGI**	**Thiadens**	
What	• IT Principles • IT Architecture • IT Infrastructure strategies • Business application needs • IT investment and prioritization	• Strategic alignment • Value delivery • Risk management • Resource management • Performance management	• Establishing priorities • Attention for innovation • Reflection on organization and sourcing • Attention for methodical operating • Control on knowledge and competency • foundation	**Focus areas**
Who	• Business monarchy • IT monarchy • Feudal • Federal • IT duopoly	• Board members • CIO • Business executives • Auditors • Risk & compliance officers	• General management • Business unit management • Demand organization • Supply organization	**Stake-holders**

	• Anarchy			
How	• Decision making structures • Alignment processes • Communication approaches	• IT strategy committee • IT steering committee • Technology council • IT architecture review board • IT Governance toolkit	• House-in-order methods • innovation	**Mechanisms**

Tabel 3: Overzicht IT Governance benaderingen

Een IT Governance benadering (inclusief framework) moet alle invalshoeken goed bedienen. De benadering van Weill et al. valt hierbij in de ogen van de auteur van dit document af aangezien de invalshoeken alleen worden benaderd vanuit de beslissingsoptiek. Het CoBiT framework (met zijn processen) sluit beter aan bij de invalshoeken van IT Governance en is daardoor ook concreter toepasbaar. De mechanismen die door Thiadens worden beschreven sluiten goed aan bij het CoBiT framework. Tevens wordt door Thiadens een duidelijk onderscheid gemaakt tussen de *demand side* en *supply side*.

Gebruikmakend van de literatuur over IT Governance is een eigen IT Governance benadering met framework opgezet. Deze wordt gebruikt in het vervolg van dit onderzoek. Het framework steunt op het gebruik van geaccepteerde methodes. Deze methodes zullen in het volgende hoofdstuk geselecteerd worden. Dit framework is opgezet om aan de doelstelling van de opdrachtgever te voldoen. De eerder beschreven concepten en hulpmiddelen van IT Governance (structuur, mechanismen, processen) zijn te relateren aan het framework. Middels dit framework en (nader te specificeren) methodes moeten EDP Auditors in staat zijn om de kwaliteit van IT Governance bij organisatie te beoordelen, binnen het gestelde kader uit hoofdstuk 2. Om dit (abstracte) framework concreet toepasbaar te maken, tot een IT Governance werkmodel, worden in het volgende hoofdstuk methodes geselecteerd en toegepast.

HOOFDSTUK 4

IT GOVERNANCE METHODES

The good thing about standards is
that there are so many of them

(Oud 2005)

In het vorige hoofdstuk is middels een eigen IT Governance benadering een IT Governance framework opgezet die het mogelijk maakt om methodes toe te passen om een werkwijze te ontwikkelen waarmee de kwaliteit van IT Governance beoordeeld kan worden. Hiervoor wordt in dit hoofdstuk de volgende onderzoeksvraag behandeld:

Wat zijn geaccepteerde methodes op het terrein van IT Governance?

In § 4.1 wordt een inleiding gegeven over methodes. In § 4.2 worden methodes beschreven die in de literatuur geassocieerd worden met IT Governance. Deze methodes zijn toepasbaar om de aandachtsgebieden van het IT Governance framework uit het vorige hoofdstuk te ondersteunen. In § 4.3 wordt een samenvatting gegeven van dit hoofdstuk en wordt het IT Governance werkmodel voorgesteld dat het aanvangspunt is voor de werkwijze.

4.1 Inleiding methodes IT Governance

In hoofdstuk 1 is aangegeven dat methodes voor IT Governance worden beschreven als *frameworks, standards* en *best practices*. Daarnaast wordt in de literatuur ook het woord model soms genoemd. Voor dit onderzoek is gekozen om al deze beschrijvingen te zien als *methodes voor IT Governance*. Zoals in hoofdstuk 2 werd aangegeven en in dit hoofdstuk nog eens wordt aangehaald door Violino (2005): *Corporate and IT Governance is hot.* Dit is mede te danken aan de behoefte naar meer efficiëntere bestedingen en vernieuwde aandacht voor *security*, *reliability* en *risk management*. Cruciaal voor het succes van veel Governance inspanningen zijn de frameworks, modellen en standaarden die organisaties helpen om processen, *customer service*, kwaliteit en *control* te verbeteren. Daarnaast hebben ze een toegevoegde waarde om bedrijfsdoelen te halen [73].

Binnen het domein van inrichting en beheersing van bedrijfsprocessen in organisaties wordt in toenemende mate gebruik gemaakt van modellen. Het betreft veelal op *best practices* gerichte modellen. Auditors vervullen een belangrijke rol bij de bewaking van de kwaliteit van bedrijfsprocessen in organisaties. De auditor kan worden gezien als degene die in de managementcyclus van organisaties de evaluerende stap voor zijn rekening neemt. [64].

Een kritische kijk op het gebruik van modellen wordt gegeven door Van der Pijl et al. (2001). Zij weerleggen het nut van het gebruik van modellen niet maar geven wel duidelijk aan dat modellen zijn gebouwd als afbeelding van de werkelijkheid. Daarmee is nog niet gezegd dat de zaak kan worden omgekeerd en de werkelijkheid kan worden geconstrueerd naar het voorbeeld van een model [64]. Elk model heeft haar beperkingen. Zo is bijvoorbeeld CoBiT slechts een afspiegeling van de werkelijkheid. De kracht van de toepassing zit, naast de inherente kwaliteit van het model, ook in de kennis van de beperkingen van het model en zoals door Oud (2005) wordt aangegeven dekt niet één standaard de volledige lading [2] [45]. Om te voorkomen dat één model onvoldoende houvast geeft voor een audit worden voor dit onderzoek meerdere methodes gebruikt om aan de doelstelling te voldoen.

4.2 Selecteren van methodes

Er zijn door verschillende auteurs en instanties studies gedaan naar methodes op het terrein van IT Governance [38] [53] [52] [31] [21] [62] [67]. In deze paragraaf wordt een selectie gemaakt van methodes die gebruikt worden voor dit onderzoek.

In deze scriptie werd eerder het belang van de aspecten functioneel beheer (*demand side*) en applicatie- & technisch beheer (*supply side*) aangeven. Dit onderscheid wordt goed weergegeven door de *educational* IT Governance benadering uit het vorige hoofdstuk. Het onderscheid wordt door Meijer (2002) als volgt (samenvattend) weergegeven:

> **De objecten die worden beheerd, en daarmee de invalshoek waarmee naar de objecten wordt gekeken, verschillen. Een functioneel beheerder beheert functionaliteit en kijkt sterk vanuit een bedrijfsmatige bril; voor hem zijn de aansluiting naar het bedrijfsproces en kosten belangrijke issues. Applicatiebeheerders beheren toepassingen en kijken vooral naar de onderhoudbaarheid, geavanceerdheid of kwaliteit van de applicatie. Technisch beheerders beheren met name hardware en netwerken, en kijken naar beschikbaarheid en performance van de totale dienstverlening [42].**
>
> **ITGI (2004)**

Voorbeeld van de drie beheerorganisaties wordt door Meijer (2002) gegeven in Tabel 4:

Onderwerp	Functioneel beheer	Applicatiebeheer	Technisch beheer
Veelvoorkomende triggers voor het proces incident-management	Vragen/wensen/ klachten over: • gebruik van de applicatie; • functionaliteit	Meldingen over: • programmafout; • wijzigingsopdracht; • opdracht voor incidentele verwerking; • informatievraag	Meldingen over: • gebruikelijke output niet ontvangen • steeds trager wordende functies • job vastgelopen door ruimtegebrek (interne melding) • autorisatieprobleem
Voorbeeld servicecall	'ik heb extra output nodig' 'hoe voeg ik een nieuwe order toe'	'de uitkomst van de berekening klopt niet'	'de printer werkt niet' 'Word zit vast' (KA-omgeving)
Met wie contact hebben over de voortgang	Gebruikers	Functioneel Beheerders	Aanvragers (gebruikers, functioneel beheerders en/of applicatiebeheerders)
Activiteiten m.b.t. het aanvragen van niet-reguliere output	Functionaliteit bepalen	Query opstellen	Query draaien
Voorbeeld van de oorzaak van het niet goed kunnen werken door een gebruiker	Te weinig kennis van de applicatie, onduidelijke gebruikershandleiding	Programmafout	Netwerk- of serverstoring
Voorbeelden van configuratie managementobjecten	• handleidingen; • AO-procedures; • werkinstructies	• systeemdocumentatie; • programmasources (ook pakketten en onderhoudsversies) • datadefinities; • testbestanden/ scripts; • SLA, contracten	• servers; • pc's; • netwerkknooppunten; • systeemsoftware;

Tabel 4: Voorbeelden van onderscheid in beheer

Voor deze invalshoeken zijn methodes ontwikkeld, die meerdere IT processen ondersteunen. Daarnaast zijn er methodes die zich concentreren op bepaalde IT aspecten (bijvoorbeeld project management en beveiliging). Tijdens gesprekken met de opdrachtgever zijn een aantal aspecten en IT-processen aangegeven die belangrijk zijn om met methodes te ondersteunen. Bij het selecteren van methodes is hiermee rekening gehouden. Methodes die toepasbaar zijn voor bovenstaande aspecten richten zich met name op de inrichting van IT-processen. Tevens zijn er ook methodes die processen beoordelen, risico's identificeren en prestaties meten. Om het samen te vatten worden **meerdere** methodes geselecteerd die **relevante** aspecten van **IT gerelateerde** onderwerpen behandelen. Voor dit onderzoek zijn drie type methodes geïdentificeerd:

- Methodes die de vraag- en aanbodorganisatie ondersteunen (behandeld in § 4.2.1);
- Methodes die specifieke IT aspecten ondersteunen (behandeld in § 4.2.2);
- Methodes die gebruikt worden om de prestaties te beoordelen en om evaluaties mogelijk te maken (behandeld in § 4.2.3).

Een methode die tot op zekere hoogte alle bovenstaande onderwerpen behandeld is CoBiT. Onderdelen hiervan (aandachtsgebieden) zijn al gebruikt bij het IT Governance framework uit het vorige hoofdstuk.

CoBiT: control framework

CoBiT is een open standaard die de IT-activiteiten organiseert rond 34 IT-processen. Voor elk proces heeft CoBiT beheerdoelen en corresponderende management guidelines. In deze guidelines staan maturiteitsmodellen en hun corresponderende scorecards in de vorm van key-goal- en key-performance-indicatoren, wat handige instrumenten zijn in het governancetraject [67].

Van Grembergen (2004)

De reden om CoBiT te kiezen als *overall control framework* voor dit onderzoek is om zijn 34 processen. Deze zijn redelijk compleet voor de totale IT organisatie beschreven. Daarnaast wordt deze methode door Auditors veel gebruikt. Eerder is al aangegeven dat niet één standaard/methode de volledige lading dekt. Dit geldt ook voor CoBiT. Hoewel deze methode toepasbaar is voor IT Governance wordt helaas bij de omschrijving van de processen en bij de *control objectives* geen onderscheid gemaakt tussen de vraag- en aanbodorganisatie, een nadeel wat al eerder onderkend is. Bij CoBiT gaat het primair over de aanbodorganisatie en wordt de vraagorganisatie als een gegeven gezien. Dit wordt hieronder gedemonstreerd door een *control objective* van CoBiT voor het proces AI1 – Identify Automated Solutions:

AI1 - Identify Automated Solutions:

The need for a new application or function requires analysis before acquisition or creation to ensure that business requirements are satisfied in an effective and efficient approach…[] …steps enable organisations to minimise the cost to acquire and implement solutions whilst ensuring they enable the business to achieve its objectives.

ITGI (2006)

AI1.1 Definition and Maintenance of Business Functional and Technical Requirements:

Identify, prioritise, specify and agree business functional and technical requirements covering the full scope of all initiatives required to achieve the expected outcomes of the IT-enabled investment programme. Requirements take into account the business functional needs, the enterprise's technological direction, performance, cost….[]

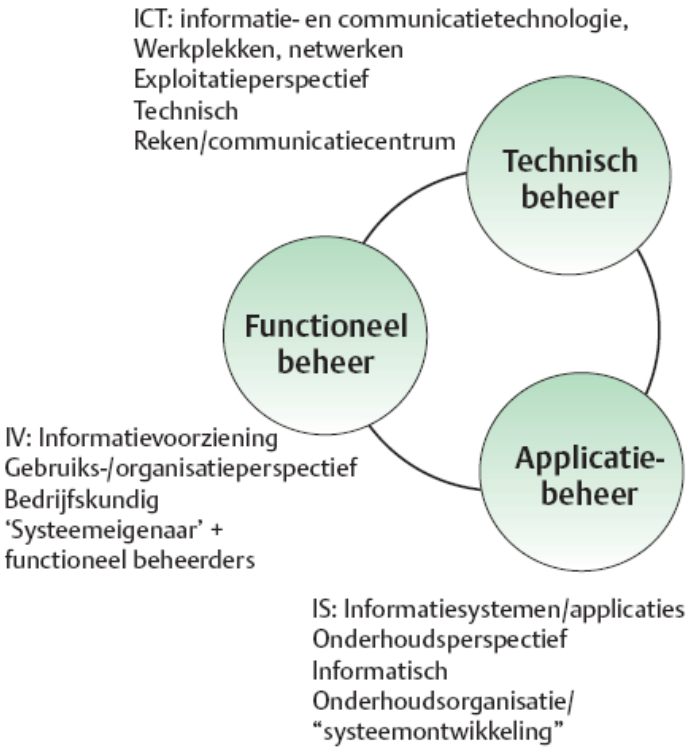
ITGI (2006)

In bovenstaand voorbeeld worden de *business requirements* als belangrijk onderdeel van het proces gezien. CoBiT erkent dus wel de rol van de vraagorganisatie (in dit onderzoek functioneel beheer genoemd). De ITGI geeft in hun *Board Briefing on IT Governance* en in CoBiT aan dat de CIO een brug moet slaan tussen IT en *the business*, en bedrijfsmanagers meer betrokken moeten zijn bij beslissingen betreffende IT. De vraagorganisatie levert een belangrijke bijdrage aan het correct uitvoeren van CoBiT processen. Veel van de CoBiT processen kunnen ook geïnitieerd worden vanuit de vraagorganisatie. Voorbeelden zijn wijzigingenbeheer, inkoop en SLM. De toegevoegde waarde van dit onderzoek ten opzichte van het huidige CoBiT model is dat expliciet onderscheid gemaakt wordt tussen de vraag- en aanbodorganisatie gebruikmakend van CoBiT processen. Concrete ondersteuning van deze processen voor beide type organisaties wordt geleverd door methodes voor de vraag- en aanbodorganisatie (§ 4.2.1).

4.2.1 Methodes voor de vraag- en aanbodorganisatie

Ter ondersteuning van de IT-processen zijn drie belangrijke methodes geselecteerd die op strategisch, tactisch en operationeel niveau de vraag- en aanbod processen beschrijven. Deze drie methodes ondersteunen het functioneel beheer, applicatiebeheer en technische beheer (exploitatie) [42]. Activiteiten die in alle drie domeinen spelen en waarbij goede samenwerking vereist is, zijn onder andere:

- Het dagelijks draaiend houden van informatiesystemen
- Servicecall-afhandeling
- Het doen van aanpassingen
- Aansturing van alle beheersactiviteiten aan de hand van afspraken en Service Level Agreements
- Strategievorming/strategic business ICT alignment



Figuur 14: Samenhang beheer

De volgende drie methodes worden hiervoor gebruikt:

BiSL: functioneel beheer

BiSL is bedoeld als een integraal procesframework voor functioneel beheer en informatiemanagement. BiSL wordt ondersteund door een groeiend aantal best practices. Zoals door Van Outvorst et al. (2005) wordt aangegeven vormt een aantal ontwikkelingen de oorzaak van de toegenomen aandacht voor functioneel beheer. Een belangrijke ontwikkeling is de toenemende professionalisering van ICT-leveranciers en ontwikkelingen op het terrein van outsourcing. Door deze toename van outsourcing is ook de vrijblijvendheid in de relatie tussen opdrachtgever en opdrachtnemer verdwenen. Hiervoor in de plaats zijn zakelijke afspraken en contracten gekomen. De structuur van BiSL onderkent processen op drie niveaus (uitvoerend, sturend en richtinggevend niveau) [71].

Van Outvorst et al. (2005)

ASL: applicatiebeheer

ASL is een leverancieronafhankelijke methode voor de uitvoering van applicatiebeheer. Populair gezegd: de 'Itil voor applicatiebeheer'. Naast een denkwijze en begrippenkader biedt ASL best practices voor de praktische invulling van de werkwijze en een procesmodel. Dit procesmodel (framework) is voor de operationele beheerprocessen en enkele sturende managementprocessen op ITIL gebaseerd. Daarnaast bevat het richtinggevende, beleidsmatige processen, waarin wordt aangegeven hoe een ict-leverancier met de klant kan meedenken over de toekomst van diens applicatieportfolio en een eigen dienstenstrategie kan bepalen [41].

Meijer (2003)

ITIL: exploitatie

De ITIL-methode onderkent een aantal processen op strategisch, tactisch en operationeel niveau [62]. Het biedt een raamwerk waarin de betreffende ICT-beheerprocessen in hun onderlinge samenhang zijn weergegeven. ITIL beschrijft de doelen, belangrijkste activiteiten, inputs en outputs van de verschillende processen [19]. Doelstellingen van bepaalde (CoBiT) IT-processen kunnen gerealiseerd worden met ITIL. Waar CoBiT zegt wat er moet gebeuren, zegt ITIL meer hoe het moet gebeuren [67]. In Nederland ziet men in ICT-organisaties vaak vooral toepassing van de service support en service delivery taken conform ITIL.

Thiadens (2004). Halfhide et al. (2003), Van Grembergen et al. (2004)

De beschreven methodes hebben raakvlakken met meerdere processen van de aandachtsgebieden zoals weergegeven in het IT Governance framework uit het vorige hoofdstuk. Deze methodes hebben ook een samenhang. Op de verschillende niveaus beschrijven ze vergelijkbare processen zoals processen voor Service Level Management, Change/Release Management en gebruikersondersteuning. Vanuit functioneel beheer worden bijvoorbeeld specificaties opgeleverd aan applicatiebeheer. Deze worden verder uitgewerkt wat zal leiden tot een wijziging in de applicatie. De acceptatietest vindt later weer bij functioneel beheer plaats.

4.2.2 Methodes voor specifieke IT-aspecten

De methodes uit de vorige subparagraaf zijn breed inzetbaar en komen in alle aandachtsgebieden van het IT Governance framework aan bod. Voor bepaalde IT onderwerpen worden in deze subparagraaf methodes beschreven die gebruikt worden voor specifieke IT aspecten.

ISO 17799: security / Code voor Informatiebeveiliging

Een standaard voor information security is de ISO 17799 of de Britse tegenhanger BS7799. deze standaard bevat een uitvoerige set van controls en best practices [38]. De standaard bestaat uit twee delen. Het ene deel is een managementraamwerk en geeft de door een organisatie te nemen maatregelen weer. Het tweede deel legt de eisen vast waarmee derde organisaties kunnen certificeren dat de processen in een organisatie of een gebruikte beveiligingsproduct voldoen aan een bepaalde norm [62]. In Nederland is deze standaard overgenomen in de Code voor Informatiebeveiliging.

Larsen et al. (2006), Thiadens (2004)

PRINCE2: project management

PRINCE2 biedt een raamwerk, waarin de projectmanagementprocessen in hun onderlinge samenhang zijn weergegeven. PRINCE2 beschrijft de doelen, belangrijkste activiteiten, inputs en outputs van de verschillende processen [19].

Halfhide (2003)

iSPL: inkoop ICT-producten en diensten

Het managen van acquisitie- en procurementtrajecten voor ICT-services (projecten en ongoing services). ISPL biedt een raamwerk voor acquisitie- en procurement-processen en een aantal best practices om deze processen uit te voeren. Doel is ervoor te zorgen dat alle relevante zaken tussen klant en leverancier worden besproken, zodat risico's worden beperkt. Kernpunten zijn het goed analyseren en beschrijven van de benodigde services, het inschatten van situatiefactoren en risico's en het daarvan afleiden van een strategie voor zowel de uitvoering van de services als de contractering. De best practices zijn vergaand uitgewerkt [19].

Halfhide (2003)

De verschillen tussen deze methodes zijn evident. Elke methode richt zich op een IT aspect. Dit wil nog niet zeggen dat deze methodes geen samenhang hebben. Methodes uit deze subparagraaf kunnen gecombineerd worden met elkaar en met methodes uit de voorgaande subparagraaf. Dit wordt in het volgende hoofdstuk in meer detail behandeld.

4.2.3 Methodes voor prestatie & evaluatie

Methodes uit de voorgaande subparagrafen worden gebruikt om een uitspraak te doen over de inrichting van IT-processen. De methodes die beschreven worden in deze subparagraaf worden gebruikt om processen te evalueren en/of om prestaties te bepalen.

CMM(i): *maturity*

Om te weten hoe ver men staat in het traject van IT Governance en strategische alignment, kan de organisatie gebruik maken van een maturiteitsmodel. Dit is een scoremethode die de organisatie in staat stelt om zichzelf te beoordelen op een schaal van "niet-bestaand" (score 0) tot "geoptimaliseerd" (score 5). Het verschil tussen waar men staat en wat men wil bereiken kan dan geanalyseerd worden en vertaald worden in concrete verbeteringsprojecten [67]. Het CMMi raamwerk steunt op het succes van Software CMM terwijl het een groter aanbod aan activiteiten en procesgebieden biedt en tevens in overeenstemming is met internationale standaarden [62]. Een van die standaarden is CoBiT. Gebaseerd op het CMM model heeft de ITGI een *maturity* assesment model gemaakt voor elk van de CoBiT processen. Hiermee kan de volwassenheid van elk van de 34 processen bepaald worden.

The assessment of process capability based on the COBIT maturity models is a key part of IT governance implementation. After identifying critical IT processes and controls, maturity modelling enables gaps in capability to be identified and demonstrated to management. Action plans can then be developed to bring these processes up to the desired capability target level [24].

Van Grembergen et al. (2004), Thiadens (2004)

Bij de beoordeling van IT processen kan de toewijzing van een *maturity* niveau arbitrair gebeuren door middel van het toekennen van de meest voor de hand liggende score. Dit is geen systematische aanpak en voor dit onderzoek wordt ook gekozen om een gestructureerde techniek te kiezen. In een artikel van Pederiva (2003) wordt een techniek voorgesteld om de CoBiT *maturity assessment* te gebruiken om de *maturity* van een proces te *berekenen* [48]. De opzet van

deze techniek is om beschrijvingen van verschillende *maturity* niveaus uit de CoBiT *maturity assessment* op te splitsen in unieke stellingen die individueel beoordeeld moeten worden.

> **To arrange the questionnaire, the *maturity* level descriptions of the COBIT *Maturity* Model were studied. It was concluded that the descriptions of the *maturity* levels could be viewed as sets of "atomic" statements. Each *maturity* level description is a statement that can be either true or false, or either partially true or partially false. The examination resulted in the realization that a compliance value could be computed for the *maturity* level by collecting and then combining a compliance value for each statement. Based on this concept, the *maturity* level descriptions were split into separate statements, and all statements in the *maturity* level descriptions were separate in the questionnaire [48].**
>
> **Pederiva (2003)**

Dit resulteert in een set stellingen waar een proces op beoordeeld wordt. Hierdoor is de Auditor in staat om veel gestructureerde het *maturity* niveau te bepalen. In de bijlage is een voorbeeld opgenomen van een berekening van de *maturity* voor een CoBiT proces.
De berekening hierbij werkt als volgt:

- Voor elke stelling wordt beoordeeld in welke mate een organisatie vindt (in overleg met een Auditor) dat het daaraan voldoet. Hieraan wordt vervolgens een waarde gekoppeld: (Not at all = 0, A little = .33, Quite a lot = .66, Completely = 1).
- De sommering van deze waardes per *maturity* level wordt gedeeld door het aantal stellingen.
- De score wordt vervolgens genormaliseerd en vermedigvuldigd met de sommering van de waardes per *maturity* level.

In dit voorbeeld wordt een *maturity* berekend voor DS2 – Manage Third-party Services. Het resultaat is een *maturity* van 3.05. Het uitgewerkte voorbeeld is triviaal maar bij het invullen moet men rekening houden dat (antwoorden voor) bepaalde stellingen tegenstrijdig kunnen zijn. De volgende twee stellingen kunnen niet beide ingevuld worden met antwoord *completely*:

- There are no formal policies and procedures regarding contracting with third parties?
- Well-documented procedures are in place to govern third-party services with clear processes for vetting and negotiating with vendors?

Er zijn meerdere methodes die zich bezig houden met *maturity* zoals het Nederlandse INK-managementmodel wat is afgeleid van de Europese versie, het EFQM Excellence Model. Beide methodes geven een handvat voor sturing van de organisatie door in korte tijd de uitgangspositie van een organisatie in kaart te brengen en daarop voortbouwend een actieplan voor de komende jaren te maken. Door het uitvoeren van een (self)-assessment wordt een beeld geschetst van het inzicht in de bedrijfsresultaten (financieel en niet financieel), de klant-, leveranciers-, medewerkers-, en maatschappelijke waardering. Verder wordt aangegeven in hoeverre leiderschap, beleid en strategie, management van medewerkers, middelen en processen zijn ingeregeld en waar de mogelijkheden voor verbetering liggen. Door regelmatig te meten kan de groei van de organisatie worden vastgesteld [43]. Omdat de ITGI voor CoBiT het CMM *maturity* model heeft gebruikt wordt in dit onderzoek ook gekozen voor deze methode. Het voorgestelde actieplan wat in het INK/EFQM model wordt voorgesteld wordt in dit onderzoek gestructureerd middels de IT BSC.

IT BSC: Performance measurement

De IT BSC is een effectief instrument om meer integratie tussen business en IT te bereiken (gebaseerd op de BSC van Kaplan en Norton). Het balanced-scorecardconcept kan een echt alignmentinstrument worden door een cascade van scorecards te implementeren. Om dit te bereiken moet een duidelijk relatie bestaan tussen de scorecard voor IT-operaties en die voor IT-ontwikkeling en IT-strategie. De scorecard voor IT-strategie kan dan op zijn beurt verbonden worden met de business balanced scorecard [67]. De cascade van scorecards kunnen gemapped worden op de domeinen die zijn gedefinieerd in het IT Governance model. Elke scorecard onderkent een aantal perspectieven, met de volgende high level targets:

Corporate contribution perspective:

providing insights into impacts made by the organization's entire portfolio of IT Investments to achieve the strategic needs of the enterprise as a whole, in contrast to specific individual customers within the enterprise

User/customer perspective:

providing insights in the quality (and cost) effectiveness of IT products and services to satisfy the needs of individual customers

Internal/ operational perspective:

evaluating the operational effectiveness and efficiency of the IT organization itself to fulfil or improve internal IT business performance that delivers IT products and services for individual customers and the enterprise

Future/Innovation & learning perspective:

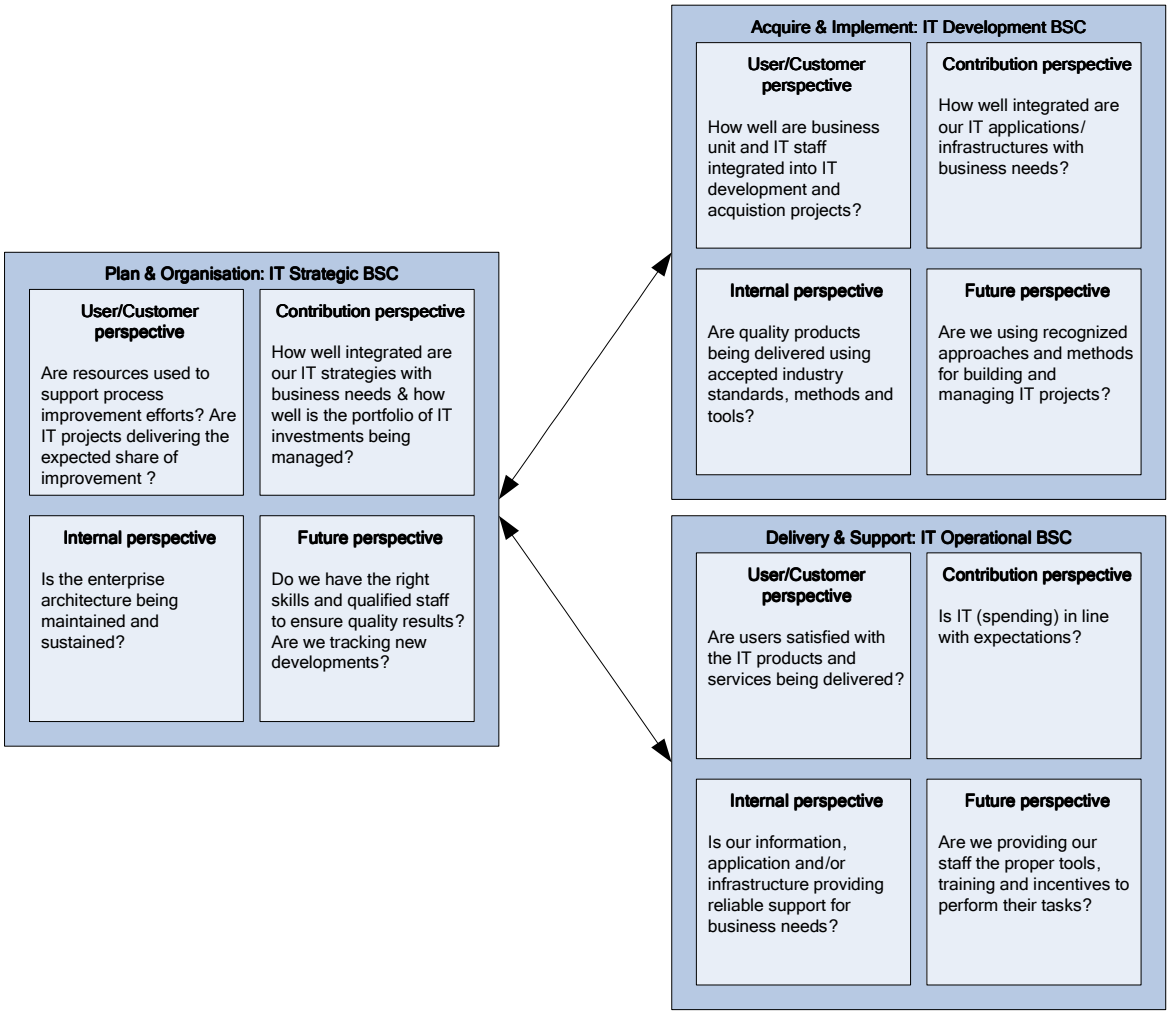
evaluating the organization's skill levels and capacity to consistently deliver quality results and accomplish ongoing IT innovation and learning as IT grows [63]

Van Grembergen (2004), GAO (1998)

A best practice is to use a balanced scorecard approach to IT performance measurement. The approach attempts to create a measurement balance across the overall performance management framework. A balanced approach to measuring the contribution of IT to mission outcomes and performance improvement recognizes the broad impact of IT's supporting role. By measuring IT performance across four goal areas that are critical to overall IT success, the scorecard forces managers to consider measurement within the context of the whole (IT) organization. This limits the possibility of overemphasizing one area of measurement at the expense of others. In addition, measuring IT performance from different perspectives helps strengthen the analysis of intangible and tangible benefits attributable to technology [63].

GAO (1998)

Gebruikmakend van de *executive guide on Measuring performance and demonstrating results of information technology investments* van de US General Accounting Office (GAO) wordt hieronder een voorbeeld gegeven van een IT BSC waarbij voor elk van de perspectieven *key objectives* zijn weergegeven die gemeenschappelijk zijn voor alle organisaties die de GAO heeft onderzocht [63].

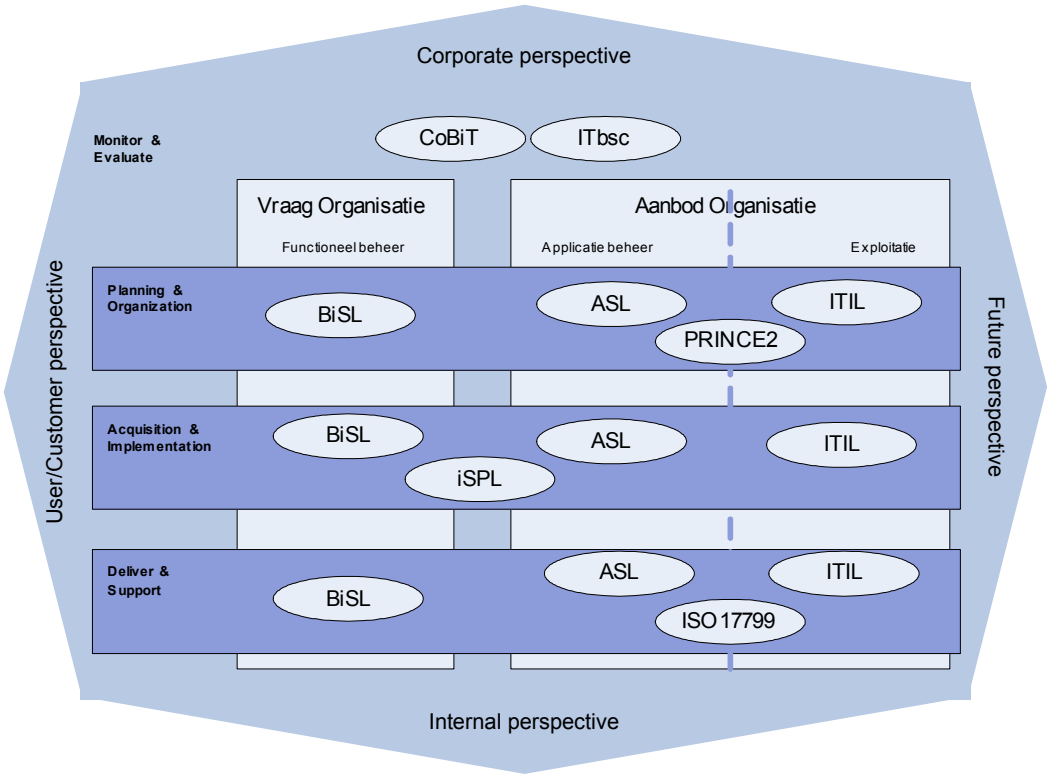


Figuur 15: IT BSC

4.3 Samenvatting methodes IT Governance

Om antwoord te geven op de onderzoeksvraag: *"Wat zijn geaccepteerde methodes op het terrein van IT Governance?"* zijn methodes geselecteerd die voor dit onderzoek gebruikt worden. Vanuit de literatuur is aangegeven dat elke methode zijn beperkingen heeft, daarom worden voor dit onderzoek meerdere methodes gebruikt om de kwaliteit van besturing van de automatisering van organisaties te beoordelen. Naast verschillen hebben de methodes ook een zekere samenhang. Zo zijn BiSL, ASL en ITIL te combineren. iSPL sluit aan bij ITIL (als het gaat om service organisaties) en PRINCE2 (als het gaat om project organisaties). Middels de combinatie CoBiT en CMM(i) is het mogelijk om de *maturity* te bepalen van de 34 processen die CoBiT beschrijft. De IT BSC wordt gebruikt om (CoBiT) aandachtsgebieden te beoordelen vanuit verschillende perspectieven.

Gebruikmakend van het eigen IT Governance framework uit het vorige hoofdstuk worden methodes uit dit hoofdstuk toegepast op dit framework. Hierbij zijn de volgende algemene beheer aspecten te onderscheiden: functioneel beheer, applicatiebeheer en technisch beheer (exploitatie). Specifieke methodes als iSPL, PRINCE2 en ISO17799 geven gedetailleerde beschrijvingen van bepaalde IT Governance aspecten (inkoop, projectmanagement en beveiliging). Daarnaast wordt CoBiT gebruikt om processen in aandachtsgebieden te identificeren die worden beoordeeld. Deze processen worden verder uitgewerkt door de methodes BiSL, ASL en ITIL. De combinatie van CoBiT en CMM(i) kan gebruikt worden om de *maturity* van processen te bepalen. De IT BSC is een instrument om de prestaties van aandachtsgebieden vanuit een viertal perspectieven te beoordelen. Dit heeft geresulteerd in het IT Governance werkmodel (Figuur 16). Dit werkmodel representeert op een concrete manier de eerder genoemde IT Governance concepten. Het is een gestructureerd model dat gebruik maakt van mechanismen (methodes) om processen te beoordelen. Middels dit model moet het mogelijk zijn om de mate van *control* te bepalen bij organisaties.



Figuur 16: IT Governance werkmodel

HOOFDSTUK 5

KOPPELING IT GOVERNANCE METHODES

De IT-auditor kan toegevoegde waarde leveren in
het efficiënt en effectief toepassen van bestaande frameworks
(zoals bijvoorbeeld CoBiT en ITIL) in IT Governance vraagstukken

(NOREA 2004)

In het vorige hoofdstuk zijn methodes toegepast op het IT Governance framework uit hoofdstuk 3. Deze *High-level* koppeling van methodes op de aandachtsgebieden van IT Governance is bedoeld als aanloop naar dit hoofdstuk waar in meer detail gekeken wordt naar de mogelijkheden van koppeling om de geselecteerde methodes, voor de werkwijze, efficiënt en effectief toe te passen. Hiervoor wordt in dit hoofdstuk de volgende onderzoeksvraag behandeld:

Welke koppeling tussen methodes is er mogelijk?

In § 5.1 wordt een inleiding gegeven over de manier van koppelen. Hierbij is gebruik gemaakt van een techniek die ook door de ITGI is gebruikt bij hun *mapping* documenten. In § 5.2 worden de resultaten beschreven van het koppelen van methodes. Hierbij is onderscheid gemaakt tussen de drie type methodes die zijn gedefinieerd in het vorige hoofdstuk. In § 5.3 wordt een samenvatting gegeven van dit hoofdstuk.

5.1 Inleiding koppeling methodes IT Governance

Eerder is al beschreven dat niet één standaard de volledige lading dekt als het gaat om IT Governance. Het advies is om meerdere te selecteren en te gebruiken. Dit is reeds in het vorige hoofdstuk gedaan. Om deze methodes te kunnen koppelen wordt CoBiT gebruikt als referentiemodel die 34 generieke IT processen beschrijft die toepasbaar zijn voor elke (grote) organisatie:

> **COBIT can be used at the highest level of IT governance, providing an overall control framework based on an IT process model that is intended by ITGI to generically suit every organisation. There is also a need for detailed, standardised practitioner processes. Specific practices and standards, such as ITIL and ISO 17799, cover specific areas and can be mapped to the COBIT framework, thus providing a hierarchy of guidance materials [25].**
>
> **ITGI (2005)**

In de afbakening van dit onderzoek is een selectie gemaakt van belangrijke IT processen. Bij de selectie van methodes is hiermee rekening gehouden. In dit hoofdstuk wordt een gedetailleerde koppeling beschreven tussen de methodes. Dit heeft als doel om de relaties van methodes ten opzichte van het referentiemodel (34 generieke IT processen) en de relatie ten opzichte van elkaar aan te tonen.

De ITGI heeft in het verleden meerdere keren methodes als ITIL, ISO17799 en andere gekoppeld aan CoBiT [25] [26] [29] [28]. Dit zijn gedetailleerde *mappings* waarbij CoBiT wordt gebruikt als referentiekader en wel op de volgende manier:

> **The mapping is performed in two layers. A high-level mapping compares the objectives stated by ISO/IEC17799:2000 with the high-level control objectives of COBIT. The detailed mapping was done as follows:**
>
> 1. **The original international standard ISO/IEC17799:2000 was split into small pieces of information. Those pieces of information are called "information requirements."**
> 2. **The information requirements were mapped to the COBIT control objectives as follows:**
>   - **2a A one-to-one mapping was done for information requirements that fit a single control objective.**
>   - **2b A one-to-n mapping was done for information requirements that fit more than one control objective.**
> 3. **The details described by the information requirements were compiled (from ISO/IEC17799:2000) and the result was sorted as defined by the COBIT Framework [26].**
>
> **ITGI (2000)**

Op één niveau hoger dan de *control objectives* (dus *high-level control objectives*) is deze manier van mapping ook uitgevoerd met de methodes uit het vorige hoofdstuk. In de volgende paragraaf worden de resultaten van deze koppeling beschreven. Deze manier van koppelen met CoBiT als referentiemodel creëert een overzicht met onder andere de volgende eigenschappen:

- Overzicht van de relatie en bijdrage van individuele methodes met generieke IT-processen.
- Overzicht van de onderlinge relaties van methodes, en de koppeling tussen vraag- en aanbodorganisaties.
- Overzicht van de mate waarin de ene methode voldoet aan de andere.

5.2 Koppeling methodes IT Governance

In het vorige hoofdstuk zijn drie type methodes beschreven:
- Methodes die vraag- en aanbodorganisatie ondersteunen (behandeld in § 4.2.1);
- Methodes die specifieke IT aspecten ondersteunen (behandeld in § 4.2.2);
- Methodes die gebruikt worden om de prestaties te beoordelen en om evaluaties mogelijk te maken (behandeld in § 4.2.3).

In subparagraaf 5.2.1 worden de resultaten beschreven van de koppeling van de drie primaire methodes (BiSL, ASL en ITIL) met CoBiT. Deze methodes hebben invloed op alle aandachtsgebieden. In subparagraaf 5.2.2 worden de specifieke methodes (iSPL, PRINCE2 en ISO17799) gekoppeld aan CoBiT en wordt hun relatie met de andere methodes beschreven. Deze methodes hebben invloed op bepaalde processen binnen de aandachtsgebieden. In de laatste subparagraaf wordt bekeken hoe de evaluatiemethodes toegepast kunnen worden.

5.2.1 Koppeling methodes vraag- en aanbodorganisatie

In de bijlage [VII, VIII, IX] worden overzichten weergegeven van de koppeling van de drie primaire IT Governance methodes (BiSL, ASL en ITIL) met CoBiT. Voor ITIL is hierbij gebruik gemaakt van het ITGI mapping document [25] [65] [66].

Zowel bij BiSL als bij ASL is een duidelijk verband te zien tussen de strategische processen die gekoppeld worden aan belangrijke *Plan & Organise* processen van CoBiT. De uitvoerende processen kunnen gekoppeld worden aan belangrijke *Acquire & Implement* en *Deliver & Support* processen De sturende processen werken voor een groot gedeelte op de grensvlakken tussen enerzijds *Plan & Organise* en anderzijds *Deliver & Support* en *Monitor & Evaluate*. Deze processen hebben een plannende, controlerende en evaluerende taak.

Uit de koppeling blijkt dat de beheermethodes (BiSL, ASL en ITIL) een brede dekking bieden voor het IT Governance framework. Tevens maken deze methodes onderscheid in de vraag- en aanbodkant. Daarnaast hebben deze drie beheermethodes ook een onderlinge koppeling. Processen van BiSL sluiten aan op processen van ASL en ITIL. Processen die bij BiSL een klant – leveranciers verhouding initiëren hebben aansluiting op vergelijkbare processen bij ASL en/of ITIL. Zo sluit Contract Management bij BiSL aan op Service Level Managment van ASL. De gebruikersondersteuning binnen BiSL heeft een relatie met de beheer processen van ASL en ITIL.

5.2.2 Koppeling methodes specifieke IT-aspecten

Naast de methodes uit de vorige subparagraaf zijn ook methodes geselecteerd die specifieke IT aspecten ondersteunen. De methodes PRINCE2 en iSPL richten zich op specifieke processen en hebben vooral koppeling met respectievelijk Project Management en Procure IT resources. De code voor informatiebeveiliging of ISO17799 heeft raakvlakken met meerdere processen waarbij processen in de *Deliver & Support* domein de meeste relaties kent.

De koppeling van de methodes iSPL en PRINCE2 met CoBiT is relatief eenvoudig. De onderlinge relaties en de relaties met methodes uit de vorige subparagraaf zijn uitvoeriger. Het ideaalbeeld van de ontwikkeling van de informatievoorziening voor een organisatie begint met het opstellen van een informatiestrategie. Daartoe wordt het bedrijfsbeleid vertaald in verbeterdomeinen en projecten, bijvoorbeeld kennismanagement, E-commerce en dergelijke [20]. De methodes uit de vorige subparagraaf geven op strategisch (en tactisch) niveau invulling hieraan. Het verbeterdomein wordt in een business case beschreven en aan de hand van de kosten en baten wordt afgewogen of het invoeren van het verbeteringsprogramma rendabel is. Voorts wordt vastgesteld op welke punten de ICT-organisatie moet worden verbeterd om de voorwaarden te scheppen om de benodigde ICT-systemen en projecten te kunnen implementeren en onderhouden. Methoden als ISPL, PRINCE2 en ITIL worden gebruikt om de ontwikkeling van de informatievoorziening te beheersen. ISPL gaat over de besturing van de acquisitie en geeft inzicht in de ‘wat’-vraag bij sourcingstrajecten. PRINCE2 vervult hierin nadrukkelijk de ‘hoe’-vraag. De projecten die ontstaan binnen het verbeterdomein, kunnen door de interne ICT-afdeling en de externe leverancier gemanaged worden met behulp van PRINCE2. Zij maken daarbij gebruik van documentatie die in het ISPL-traject is opgesteld, in het bijzonder de risicoanalyse [20].

Relatie iSPL met ITIL en ASL

ISPL is afgestemd met ITIL en omvat referenties naar relevante ITIL-processen en ITIL-handboeken [20]. Aangezien ASL als “*de ITIL van applicatiebeheer*” wordt gezien kan iSPL ook in combinatie met ASL functioneren.

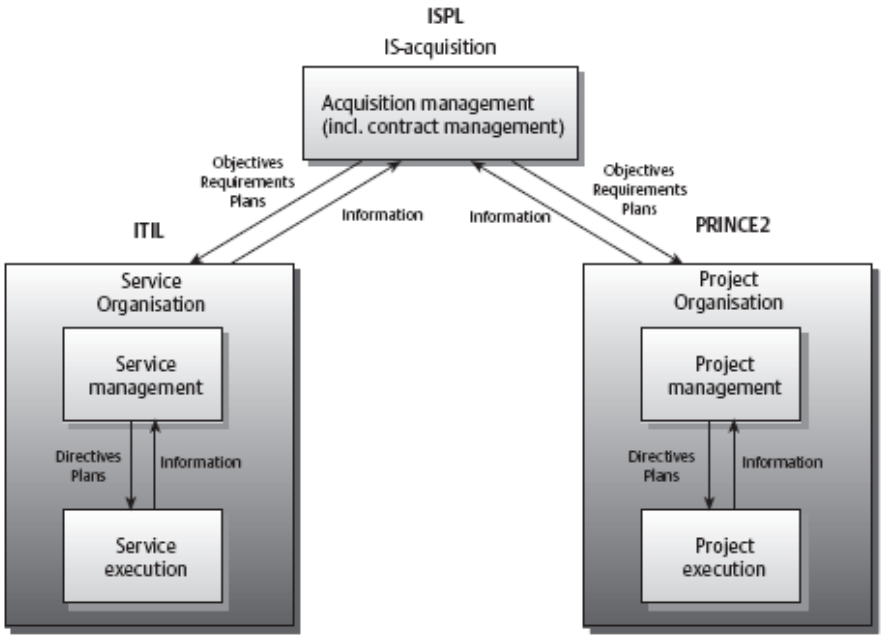
Voor de leverancier biedt de ISPL-beschrijving van Acquisitie Management een raamwerk voor het opleveren van de procesinrichting als onderdeel van een procurementtraject. Dit terwijl ITIL een handvat biedt voor de beschrijving van de deliverables. Heel nuttig in deze situatie is het onderscheid dat ISPL maakt tussen ‘target domain’ en ‘service domain’. De naamgeving kan verwarring geven, omdat ITIL met een service wat anders bedoelt dan ISPL. De leverancier is verantwoordelijk voor het ‘service domain’ en zal rekening moeten houden met het ‘target domain’ binnen de organisatie van de afnemer, zoals die in ISPL wordt gehanteerd op de aspecten processen, informatie, actoren en technologie [20].

Relatie iSPL met PRINCE2

PRINCE2 gaat ervan uit dat een project wordt uitgevoerd binnen de context van een contract. Het proces voor het voorbereiden en afsluiten van het contract is niet in de methode opgenomen. De activiteiten die in dit kader moeten worden uitgevoerd, kunnen worden gemanaged met behulp van PRINCE2. De target domain-beschrijving van ISPL dient te worden aangevuld en vormt dan

een prima kader voor de business cases van de PRINCE2-projecten. De situatie- en risicoanalyse van ISPL, uitmondend in een delivery strategy, is een effectieve aanvulling op PRINCE2. Het beslissingsproces van ISPL (Decision Points in combinatie met Specifying Deliverables) is een effectieve aanvulling op het productgericht plannen volgens PRINCE2 [20].

In onderstaand figuur is schematisch de relatie tussen iSPL, ITIL en PRINCE2 weergegeven. ASL kan op dezelfde manier een relatie hebben met iSPL. Tevens kan iSPL gekoppeld worden aan BiSL. Het proces Leveranciersmanagement van BiSL heeft een relatie hebben met iSPL als het gaat om het selecteren van leveranciers.



Figuur 17: Positionering methodes [20]

Beveiliging

Een methode die in het vorige hoofdstuk voor beveiliging is geselecteerd is de ISO17799 of de Nederlandse versie, code voor informatiebeveiliging. De ITGI heeft enkele documenten gepubliceerd waarin een zeer gedetailleerde mapping is beschreven van alle (sub)-paragrafen van de ISO17799 met de detail control objectives van CoBiT [25] [26]. Uit de detail *mapping* documenten van de ITGI blijkt dat onderstaande *high level mapping* mogelijk is:

Figure 8—High-level Mapping of ISO/IEC 17799:2000 With COBIT 4.0

COBIT 4.0 Processes and Domains	1	2	3	4	5	6	7	8	9	10	11	12	13
Plan and Organise	-	o	-	+	-	+	o	-	-	-			
Acquire and Implement	o	o	+	-	-	o	o						
Deliver and Support	-	o	o	o	+	-	o	-	-	o	+	+	o
Monitor and Evaluate	-	o	o	o									

(+) Good match (more than two objectives were mapped to a COBIT process)
(o) Partial match (one or two objectives were mapped)
(-) No or minor match (no objective was mapped)

Figuur 18: High level mapping of ISO17799 to CoBiT

Hieruit blijkt dat de volgende processen meerdere belangrijke relaties hebben:
- PO4: Define the IT processes, organisation and relationships
- PO6: Communicate management aims and direction
- DS2: Manage third-party services
- DS5: Ensure systems security
- DS11: Manage data
- DS12: Manage the physical environment

Andere processen die bij bestudering van de detail *mapping* als belangrijk worden beschouwd:
- PO7: Manage IT human resources
- PO8: Manage quality
- AI2: Acquire and maintain application software
- AI3: Acquire and maintain technology infrastructure
- AI6: Manage changes
- DS4: Ensure continuous service
- DS8 & DS10: Manage service desk, incidents and problems
- M2: Monitor and evaluate internal control

AI3 heeft *maar* twee objectives en DS13 heeft drie *objectives*. Deze staan dus verkeerd in bovenstaande *mapping*.

Dit zijn processen waarbij security (volgens ISO17799) een belangrijke rol speelt. Opvallend is dat ISO17799 nauwelijks aandacht besteed aan het (CoBiT) process *assess and manage IT risks*. Dit wordt door de ITGI gezien als een proces voor *security* [30]. Voor een detail *mapping* wordt verwezen naar de ITGI documentatie. Het is de mening van de auteur dat deze detail *mapping* te complex is voor een overzichtelijke en pragmatische werkwijze. (sub)-paragrafen van de ISO17799 verwijzen naar meerdere CoBiT processen en CoBiT processen kunnen meerdere (sub)-paragrafen bevatten van de ISO1779. Deze n:m relaties beperken de pragmatische toepassing van de ISO standaard in combinatie met CoBiT.

5.2.3 Koppeling methodes prestatie & evaluatie

In deze subparagraaf worden methodes besproken die geselecteerd zijn om de prestatie te bepalen en evaluatie uit te voeren. Deze methodes hebben niet zozeer een relatie met de CoBiT processen als het gaat om de inrichting van de IT processen, maar deze methodes zijn gekozen om processen en prestaties te beoordelen en te structureren. Hierbij beschrijft de IT BSC vier perspectieven die belangrijk zijn voor het succes van de IT organisatie. Een combinatie van CoBiT processen en CMM(i) wordt gebruikt om de *maturity* te bepalen van geselecteerde processen. In dit onderzoek wordt CMM(i) in combinatie met CoBiT gebruikt om de volwassenheid van processen te beoordelen. De techniek die hiervoor wordt gebruikt is beschreven in het vorige hoofdstuk en weergegeven in bijlage VI.

De IT BSC wordt in dit onderzoek gebruikt om bij de werkwijze het accent te leggen op vier belangrijke perspectieven. Daarnaast biedt de IT BSC mogelijkheden om doelen te definiëren en

hieraan *measurements* te koppelen. Het CoBiT proces waar deze methode aan gekoppeld kan worden is ME1 – *Monitor & evaluate* IT performance. De inhoud van deze methode omvat onderwerpen van alle geselecteerde IT processen van een organisatie. Daarom is het *Monitor & Evaluate* aandachtsgebied in het IT Governance framework uit het vorige hoofdstuk geplaatst om alle andere domeinen heen.

5.3 Samenvatting koppeling methodes IT Governance

Om antwoord te geven op de onderzoeksvraag: "*Welke koppeling tussen methodes is er mogelijk?*" zijn in dit hoofdstuk de geselecteerde methodes onderling met elkaar vergeleken en gekoppeld met CoBiT als generiek referentiekader.

Uit de koppeling blijkt dat de primaire methodes (BiSL, ASL en ITIL) vergelijkbare CoBiT processen ondersteunen en dat ze een afhankelijkheidsrelatie ten opzichte van elkaar hebben (vraag- aanbodorganisatie). Daar waar bepaalde processen bij BiSL ophouden gaan ze bij ASL of ITIL verder. Daarnaast blijkt dat specifieke methodes ook relaties hebben met elkaar en met de primaire methodes. De geselecteerde methodes hebben dus ten opzichte van CoBiT maar ook ten opzichte van elkaar een sterke samenhang.

In Tabel 6: Koppeling methodes wordt een overzicht gegeven in welke mate de methodes een relatie hebben met generieke CoBiT processen. Hieruit blijkt dat geselecteerde methodes op nagenoeg alle belangrijke IT Processen, zoals omschreven in § 1.3.3, een positieve bijdrage leveren. De *onderdelen* van methodes geven voldoende dekking voor belangrijke IT processen om een werkwijze op te zetten die de kwaliteit van de besturing van de automatisering kan beoordelen.

Rekening houdend met de selectie van CoBiT processen uit de afbakening van dit onderzoek en de ondersteuning van deze processen door methodes worden onderstaande processen als zeer belangrijk beschouwd:

PO1 Define a Strategic IT Plan	AI1: Identify Automated Solutions	DS1 Define and Manage Service Levels
PO2 Define the Information Architecture	AI2 Acquire and Maintain Application Software	DS2 Manage Third-party Services
PO3 Determine Technological Direction	AI5 Procure IT Resources	DS4 Ensure Continuous Service
PO4 Define the IT Processes, Organisation and Relationships	AI6 Manage Changes	DS5 Ensure Systems Security
PO6 Communicate Management Aims and Direction	AI7 Install and Accredit Solutions and Changes	DS11 Manage Data
PO10 Manage Projects		DS12 Manage the Physical Environment
ME1 Monitor and Evaluate IT Processes		

Tabel 5: Belangrijke generieke IT-processen

Doel van de werkwijze zal zijn om bovenstaande processen te ondersteunen. Middels deze koppeling en het resultaat van het volgende hoofdstuk wordt concrete invulling gegeven aan het IT Governance werkmodel uit hoofdstuk 3.

Proces	**FB**	**AB**	**TB**	**SEC**	**PM**	**INK**
CoBiT	BiSL	ASL	ITIL	iso17799	prince2	iSPL
PO1 Define a Strategic IT Plan	++	++	++	O	O	O
PO2 Define the Information Architecture	++	O	O	O	O	O
PO3 Determine Technological Direction	+	++	++	O	O	O
PO4 Define the IT Processes, Organisation and Relationships	++	++	++	++	O	O
PO5 Manage the IT Investment	+	+	+	O	O	O
PO6 Communicate Management Aims and Direction	++	+	++	++	O	O
PO7 Manage IT Human Resources	O	+	O	+	O	O
PO8 Manage Quality	+	+	O	+	+	O
PO9 Assess and Manage IT Risks	O	O	O	O	+	O
PO10 Manage Projects	O	O	O	O	++	+
AI1 Identify Automated Solutions	+	+	+	O	O	O
AI2 Acquire and Maintain Application Software	O	++	O	+	O	O
AI3 Acquire and Maintain Technology Infrastructure	O	O	+	+	O	O
AI4 Enable Operation and Use	+	O	+	O	O	O
AI5 Procure IT Resources	+	O	++	O	O	++
AI6 Manage Changes	+	++	++	+	O	O
AI7 Install and Accredit Solutions and Changes	++	++	++	O	O	O
DS1 Define and Manage Service Levels	++	+	++	O	O	+
DS2 Manage Third-party Services	++	O	+	++	O	O
DS3 Manage Performance and Capacity	+	+	+	O	O	O
DS4 Ensure Continuous Service	+	+	+	++	O	O
DS5 Ensure Systems Security	O	O	+	++	O	O
DS6 Identify and Allocate Costs	O	+	+	O	O	O
DS7 Educate and Train Users	+	O	O	O	O	O
DS8 Manage Service Desk and Incidents	+	+	+	+	O	O
DS9 Manage the Configuration	O	+	+	O	O	O
DS10 Manage Problems	O	O	+	+	O	O
DS11 Manage Data	+	O	O	++	O	O
DS12 Manage the Physical Environment	O	O	O	++	O	O
DS13 Manage Operations	O	O	O	+	O	O
ME1 Monitor and Evaluate IT Processes	++	++	+	O	O	O
ME2 Monitor and Evaluate Internal Control	O	O	O	+	O	O

ME3 Ensure Regulatory Compliance		O	O	O	O	O	O
ME4 Provide IT Governance		O	O	O	O	O	O
O	weinig tot geen relatie						
+	een relatie						
++	meerdere relaties						
FB:	Functioneel beheer						
AB:	Applicatiebeheer						
TB:	Technisch beheer (exploitatie)						
SEC:	Security						
PM:	Project Management						
INK:	Inkoop						

Tabel 6: Koppeling methodes

HOOFDSTUK 6

WERKWIJZE IT GOVERNANCE BEOORDELING

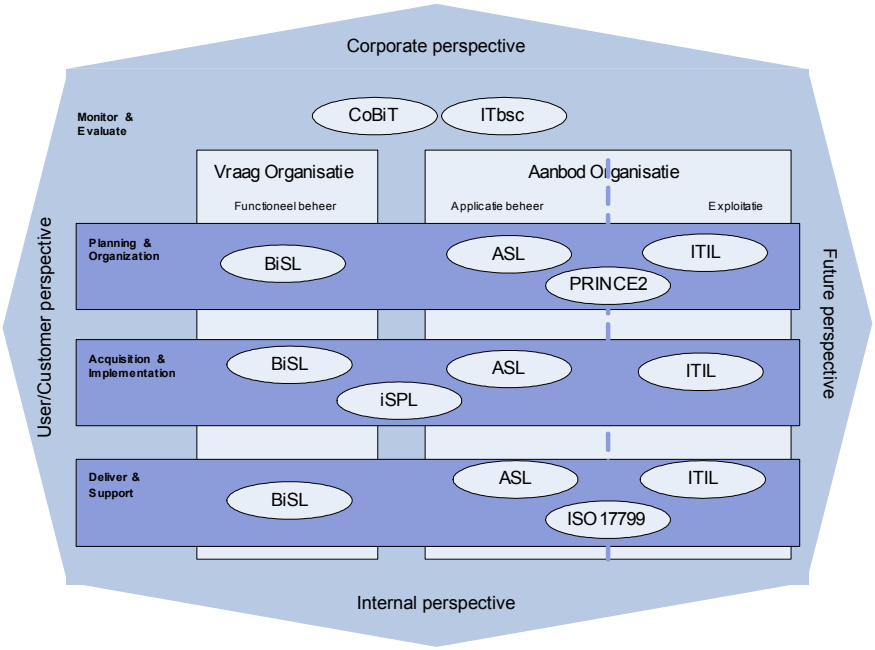
In dit hoofdstuk wordt de werkwijze voorgesteld die het mogelijk maakt om de kwaliteit van besturing van automatisering bij organisaties te beoordelen. Daarbij wordt de volgende onderzoeksvraag behandeld:

Welke werkwijze kan met de gevonden methodes ontwikkeld worden?

Om de onderzoeksvraag te beantwoorden worden een aantal onderwerpen behandeld. Het hoofdstuk begint in § 6.1 met een korte inleiding. In § 6.2 wordt de doelstelling van de werkwijze beschreven. Hierbij is het ontwikkelde IT Governance werkmodel, uit hoofdstuk 3, als uitgangspunt genomen. Het doel is om de werkwijze gestructureerd, overzichtelijk en pragmatisch toepasbaar te maken. § 6.3 beschrijft hoe het IT Governance werkmodel wordt toegepast gebruikmakend van de ontwikkelde IT Governance checklist. Dit is de aanpak (stijl) van de werkwijze.

6.1 Inleiding werkwijze IT Governance beoordeling

De voorgaande hoofdstukken liggen ten grondslag aan de beantwoording van de onderzoeksvraag. In hoofdstuk 3 is een eigen IT Governance benadering beschreven waarvoor een IT Governance framework is ontwikkeld. Het framework biedt de mogelijkheid om methodes te positioneren ten opzichte van elkaar. Een aantal methodes uit de literatuur zijn geselecteerd die bepaalde IT aspecten ondersteunen (hoofdstuk 4). Deze aspecten zijn functioneel beheer, applicatiebeheer, technisch beheer, projectmanagement, beveiliging en inkoop. Wanneer deze methodes worden geplaatst binnen het IT Governance framework ontstaat het IT Governance werkmodel:



Figuur 19: IT Governance werkmodel

Dit model is het aanvangspunt van de werkwijze en het aanvangspunt van dit hoofdstuk. In dit model zijn aandachtsgebieden, aspecten en perspectieven duidelijk te onderscheiden. Deze onderwerpen zijn belangrijk voor de toepassing van het werkmodel en worden uitvoerig behandeld in dit hoofdstuk.

6.2 Doelstelling werkwijze

Na bestudering van verschillende methodes uit hoofdstuk 4 en de toepassing hiervan (hoofdstuk 5) is een gesprek geweest met de opdrachtgever bij Ernst & Young EDP Audit om de pragmatische toepasbaarheid van het IT Governance framework, inclusief de geselecteerde methodes, te bespreken. Hieruit is gebleken dat een gestructureerde en overzichtelijke checklist met normen de oplossing moet bieden voor een uniforme en pragmatische wijze van werken (werkwijze) om de besturing van de automatisering te beoordelen bij organisaties. Deze doelstelling van de werkwijze wordt in deze paragraaf besproken. Uitgangspunt hierbij is het ontworpen IT Governance werkmodel uit hoofdstuk 4.

Structuur wordt geboden door de aandachtsgebieden en IT processen voor verschillende aspecten vanuit een aantal perspectieven te benaderen (IT Governance werkmodel). Overzicht wordt geboden door te kiezen voor een selectie van belangrijke IT processen die door de aspecten in ruime mate worden ondersteund (koppeling methodes met processen). Pragmatiek wordt geboden door te kiezen voor een checklist met nuttige en bruikbare normen om de kwaliteit van IT Governance te boordelen. In de volgende subparagrafen worden deze begrippen die de doelstelling van de werkwijze definiëren in meer detail behandeld.

6.2.1 Gestructureerde werkwijze

Wijze van opbouw van een samengesteld geheel

(Van Dale 2006)

De eigen IT Governance benadering uit hoofdstuk 3 biedt de mogelijkheid om aandachtsgebieden van IT Governance methodisch te benaderen. Dit is één van de sterke punten van deze IT Governance benadering. Binnen de aandachtsgebieden zijn een aantal aspecten geïdentificeerd die belangrijk zijn voor dit onderzoek. Voor deze aspecten zijn een aantal methodes geselecteerd die gebruikt worden om processen te beoordelen binnen de aandachtsgebieden. Hiervoor is in het vorige hoofdstuk een gedetailleerde koppeling gemaakt tussen methodes en IT processen. Om te voorkomen dat beoordelingen van de kwaliteit van IT Governance *maar* vanuit één oogpunt benaderd worden is gekozen om meerdere perspectieven te selecteren. De aandachtsgebieden, aspecten en perspectieven worden weergegeven in Tabel 7: Structuur werkwijze.

Aandachtsgebieden	**Aspecten**		**Perspectieven**
Planning & Organisation	Functioneel beheer	(FB)	Corporate contribution
Acquisition & Implementation	Applicatiebeheer	(AB)	Internal/operational
Deliver & Support	Technisch beheer	(TB)	User/customer
Monitor & Evaluate	Projectmanagement	(PM)	Future/innovation & learning
	Inkoop	(INK)	

	Beveiliging (SEC)	

Tabel 7: Structuur werkwijze

Aandachtsgebieden en IT processen:

Om de kwaliteit van IT Governance te beoordelen zijn aandachtsgebieden en generieke IT processen gebruikt van CoBiT. Deze methode wordt in de literatuur en in de praktijk regelmatig gebruikt als raamwerk om IT Governance initiatieven te structureren. De aandachtsgebieden en generieke IT processen zijn redelijk compleet beschreven en kunnen goed gebruikt worden voor een raamwerk die toepasbaar is voor veel (IT) organisaties. Daarnaast zijn de aandachtsgebieden en processen van CoBiT te gebruiken als communicatiemiddel richting organisaties. Het biedt namelijk de mogelijkheid om als uitgangspunt en referentiekader te gebruiken bij de beoordeling van de kwaliteit van IT Governance.

Aspecten en bijbehorende methodes:

Het tweede onderdeel wat voor structuur zorgt, zijn de gekozen aspecten. Aspecten beschrijven onderwerpen die worden beoordeeld. Deze hebben een aantal relaties met generieke IT processen uit de aandachtsgebieden. In dit onderzoek zijn een aantal aspecten besproken die als belangrijk worden beschouwd. Hiervoor zijn een aantal algemene IT beheer aspecten en een aantal specifieke IT aspecten omschreven. Deze zijn concreet ingevuld door methodes uit hoofdstuk 4. De relatie met IT processen is in hoofdstuk 5 beschreven.

Met deze structurering en de vorige kan een IT Governance initiatief vanuit twee kanten bekeken en beoordeeld worden. Aspecten kunnen invloed hebben op meerdere IT processen. Processen kunnen invloed hebben op één of meerdere aspecten. Eenvoudig gezegd beoordelen aspecten IT Governance op een verticale manier en processen beoordelen IT Governance op een horizontale manier, zoals ook weergegeven is in Tabel 6: Koppeling methodes op blz. 67.

Perspectieven en de IT BSC:

In voorgaande hoofdstukken zijn de perspectieven van de IT BSC al beschreven als methode om beoordelingen uit te voeren. Deze *best practices* aanpak wordt uitgebreid behandeld door verschillende instanties en auteurs waaronder Van Grembergen et al. Voor concrete toepassing van dit concept wordt in dit onderzoek gebruik gemaakt van het document wat is gepubliceerd door de United states General Accounting Office [63]. Hierin worden een aantal generieke *key objectives* beschreven die belangrijk bleken voor organisaties die zij hebben onderzocht. Deze *objectives* zijn weergegeven in de vorm van vragen en deze vragen worden in dit onderzoek gekoppeld aan de drie aandachtsgebieden zoals beschreven in het IT Governance framework en weergegeven in afbeelding Figuur 15: IT BSC uit hoofdstuk 4 (blz. 54). Doel van deze aanpak is om een gebalanceerde benadering te creëren waarbij alle perspectieven evenwichtig behandeld worden bij beoordelingen. Gebalanceerd betekent in deze context niet hetzelfde als gelijkheid. Dit wordt ook door de GOA (1998) aangegeven [63]. De toepassing van de *Balanced Scorecard* methode houdt in dat verschillende perspectieven in beschouwing worden genomen. Hierbij is de *IT-Business alignment* erg belangrijk zoals ook duidelijk wordt gemaakt in onderstaande quote:

Information technology (IT) products, services, and delivery processes are important resources for results-driven government programs and operations. IT also includes the organizational units and contractors primarily responsible for delivering IT. The operational customers relying on IT products and services and IT managers themselves, want to know "How are information technology products and services, including the information infrastructure, supporting the delivery and effectiveness of the enterprise's (agency) programs?" [63]

GOA (1998)

6.2.2 Overzichtelijke werkwijze

Gemakkelijk te overzien

(Van Dale 2006)

Omdat methodes elk op een eigen manier processen benaderen moet een uniforme aanpak zorgen voor een overzichtelijke werkwijze. De n:m relatie van (onderdelen van) aspecten en processen die werd aangetroffen bij de koppeling van ISO17799 met CoBiT (processen) resulteerde in een onoverzichtelijk en zeer complex toepasbare techniek om het beveiligingsaspect bij organisaties te beoordelen. Om het nadeel van onoverzichtelijkheid van koppeling tussen methodes en processen tegen te gaan is in de doelstelling opgenomen dat de werkwijze overzichtelijk moet zijn.

In hoofdstuk 5 zijn methodes die de aspecten ondersteunen gekoppeld aan IT processen. Dit heeft geresulteerd in een selectie IT processen die als belangrijk worden beschouwd om bepaalde aspecten te beoordelen. In dit onderzoek wordt deze selectie van processen gekozen om het overzicht te behouden. De werkwijze beoordeelt niet alle processen maar *slechts* een selectie van IT processen. Deze selectie heeft een vergaande relatie met methodes die belangrijke aspecten behandelen. De volgende IT processen van CoBiT zijn geselecteerd in hoofdstuk 5:

PO1 Define a Strategic IT Plan	AI1 Identify Automated Solutions	DS1 Define and Manage Service Levels
PO2 Define the Information Architecture	AI2 Acquire and Maintain Application Software	DS2 Manage Third-party Services
PO3 Determine Technological Direction	AI5 Procure IT Resources	DS4 Ensure Continuous Service
PO4 Define the IT Processes, Organisation and Relationships	AI6 Manage Changes	DS5 Ensure Systems Security
PO6 Communicate Management Aims and Direction	AI7 Install and Accredit Solutions and Changes	DS11 Manage Data
PO10 Manage Projects		DS12 Manage the Physical Environment
ME1 Monitor and Evaluate IT Processes		

Tabel 8: Overzicht van selectie IT processen

6.2.3 Pragmatische werkwijze

Op nut en bruikbaarheid gericht

Van Dale (2006)

Nu structuur en overzicht zijn gerealiseerd moet de werkwijze nog pragmatisch toepasbaar gemaakt worden om daadwerkelijk een beoordeling te kunnen uitvoeren. Hiervoor is gekozen om een IT Governance checklist op te zetten die in staat stelt om met normen IT processen op een evenwichtige manier te beoordelen.

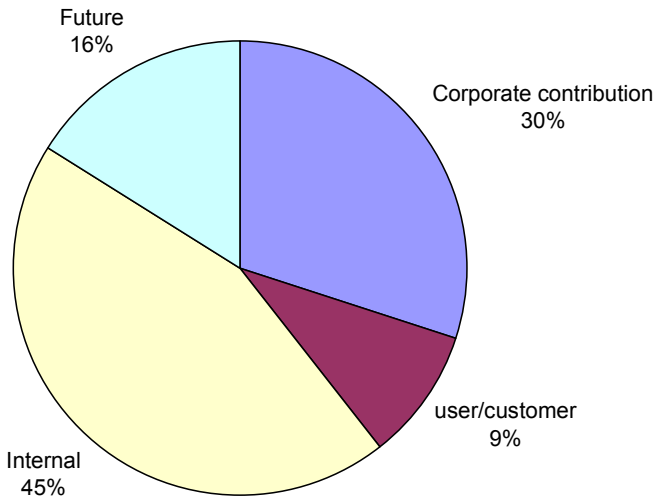
Om een checklist op te stellen is de literatuur van methodes geraadpleegd en zijn bestaande checklisten/vragenlijsten gebruikt die bij de methodes horen [65] [3] [66] [10] [32] [23] [72] [8]. Deze checklisten/vragenlijsten bleken te omvangrijk om zelfs maar een selectie van processen te ondersteunen, alleen de vragenlijst van de ISO17799 is al 65 pagina's lang. Een selectie is nodig om een geschikte IT Governance checklist te ontwikkelen zodat aan de doelstelling voldaan kan worden. Het nadeel bij het selecteren en beschrijven van uniforme normen gebruikmakend van methodes is dat:

- niet elke methode een bestaande checklist/vragenlijst heeft;
- niet alle checklisten/vragenlijsten dezelfde opbouw of indeling hebben (sommige zijn volgens een *maturity* model gestructureerd andere zijn in de vorm van vragen);
- methodes niet hetzelfde zijn (de ene methode is een best practices die processen beschrijft en de andere methodes is een standaard met *objectives*).

De verscheidenheid in methodes belemmert een systematische aanpak om normen te selecteren. De aanpak waarmee in dit onderzoek geschikte normen zijn geselecteerd kan omschreven worden als heuristisch. Hierbij is gezocht naar onderdelen die gebruikt konden worden om processen zo compleet en concreet mogelijk te beoordelen. Dit is niet volgens een formele strategie uitgevoerd maar volgens een intuïtieve strategie. De discussie kan ontstaan dat de selectie enigszins arbitrair is. Hierbij wordt de aantekening gemaakt dat op voorhand uitvoerig kennis is genomen van de methodes. Hierbij zijn globaal de volgende stappen uitgevoerd:

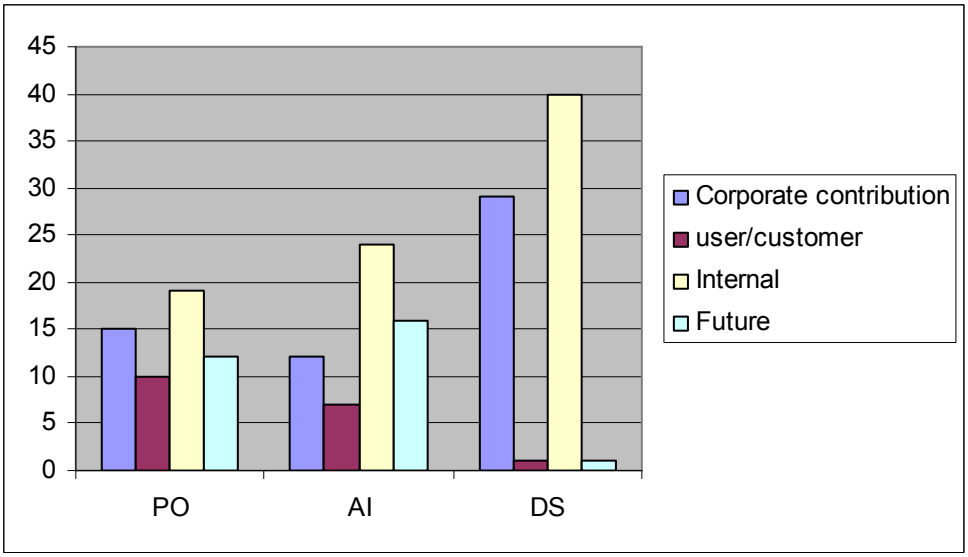
- Voor elke methode is bestudeerd hoe de onderdelen belangrijke IT processen ondersteunen;
- Uit deze onderdelen zijn belangrijke normen geëxtraheerd waarmee de essentie van het onderwerp wordt behandeld;
- Geprobeerd is om daar waar mogelijk alle perspectieven evenwichtig te behandelen.

Resultaat van de selectie is een checklist met normen die overzichtelijk is weergegeven per proces en verschillende aspecten behandelt vanuit een aantal perspectieven. Dit wordt weergegeven in onderstaande figuren. In Figuur 20: Verhouding perspectieven IT BSC is te zien dat bijna de helft van de normen wordt toegekend aan het *internal* perspectief. Het was te verwachten dat dit perspectief het grootste aandeel zou krijgen, aangezien traditioneel IT beoordelingen gerelateerd worden aan dit perspectief [63]. Een gedetailleerde verklaring wordt gegeven wanneer de resultaten bekeken worden vanuit de aandachtsgebieden.



Figuur 20: Verhouding perspectieven IT BSC

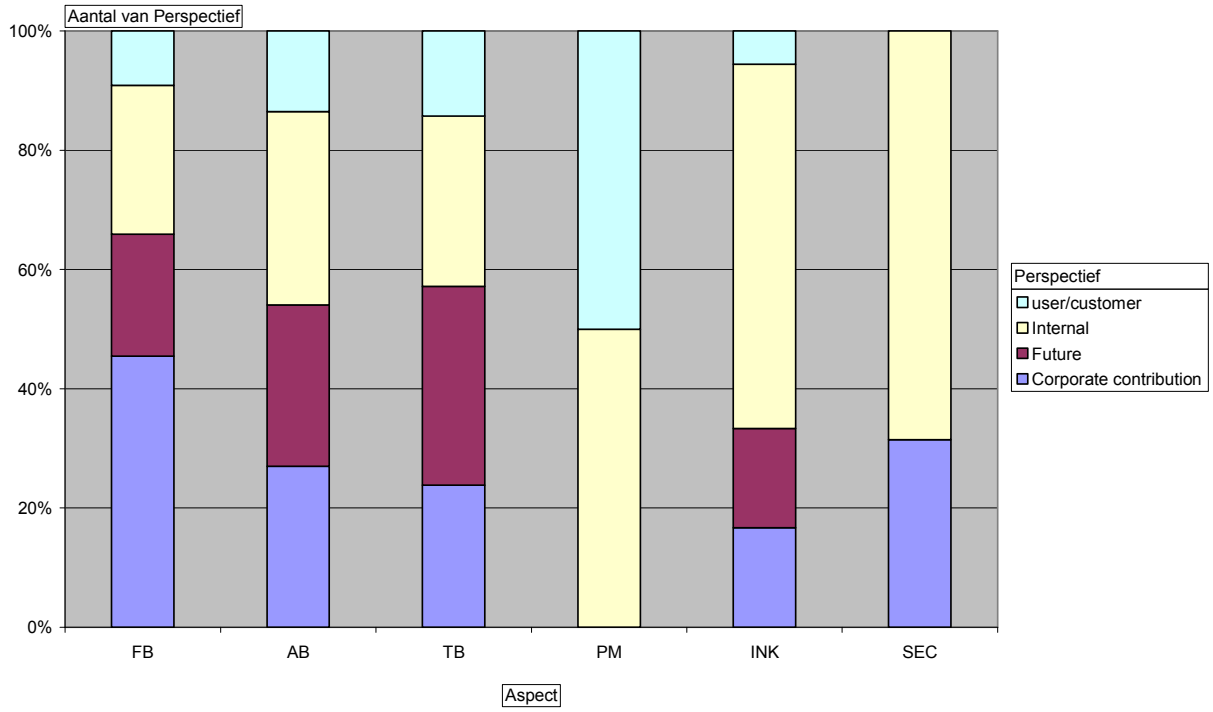
Wanneer gekeken wordt naar de verdeling van de vier perspectieven over de drie aandachtsgebieden, dan is te zien dat de verhouding in de aandachtsgebieden *Plan & Organise (PO)* en *Acquire & Implement (AI)* redelijk evenwichtig is, met een verhoogde aandacht voor het perspectief *internal*.



Figuur 21: Verhouding perspectieven t.o.v. aandachtsgebieden

Het *Deliver & Support (DS)* aandachtsgebied laat duidelijk zien dat de perspectieven *user/customer* en *future* weinig behandeld worden. Dat de individuele gebruikers weinig aandacht krijgen in dit aandachtsgebied was te verwachten en wordt verklaard door de processen die in dit

aandachtgebied uitgevoerd worden (SLM, Security Management, Continuïteitsmanagement). De gebruikers als geheel worden wel in dit aandachtsgebied behandeld door het *corporate* perspectief. Dit heeft te maken met de algehele belangen van gebruikers die tot uitdrukking komen bij het opzetten en bewaken/evalueren van SLA's en contracten. Bij de levering en ondersteuning wordt ook weinig aandacht gegeven aan innovatie. De focus ligt in dit aandachtsgebied op de uitvoering oftewel het *internal/operational* perspectief.



Figuur 22: Verhouding perspectieven t.o.v. aspecten

Opvallende zaken in Figuur 22: Verhouding perspectieven t.o.v. aspecten is het grote aandeel van het *user/customer* perspectief bij projectmanagement. Dit is te verklaren door de vergaande relatie met de opdrachtgever (klant) bij dit aspect. Daarnaast is het grote aandeel van *corporate contribution* bij het beveiligingsaspect (SEC) duidelijk te zien. De verklaring hiervoor is dat bij beveiliging meer vanuit het perspectief van de totale organisatie wordt gekeken i.p.v. individuele gebruikers.

6.3 Toepassing werkwijze

In de vorige paragraaf is de totstandkoming van de werkwijze beschreven om de kwaliteit van IT Governance te beoordelen. Dit heeft geresulteerd in een IT Governance checklist (Bijlage X). In hoofdstuk 2 is een definitie gekozen die aansluit bij de doelstelling van dit onderzoek. Deze definitie heeft een sterke koppeling met het begrip *control*. In ditzelfde hoofdstuk is geconcludeerd dat *control* wordt gebruikt als kader voor IT Governance. De werkwijze om IT Governance te beoordelen is opgezet om de mate van *control* te bepalen bij organisaties. Verschillende auteurs (uit hoofdstuk 2) geven aan dat *control* (beheersingsmaatregelen) een instrument is om te zorgen dat activiteiten leiden tot het gewenste resultaat. Een set van beheersingsmaatregelen is hetzelfde als een regelkring. Deze regelkring wordt als aanpak gebruikt om de werkwijze te positioneren. Een regelkring bestaat uit vijf stappen, te weten:

- Meten van de feitelijke situatie (observaties)
  - Bij organisaties worden observaties gedaan over de procesgang van IT gerelateerde aspecten (bijvoorbeeld functioneel beheer, beveiliging, etc.)
- Vergelijken van de feitelijke situatie met de norm (IT Governance checklist)
  - De observaties worden vergeleken met normen uit de IT Governance checklist. Elke norm krijgt een score toegewezen
- Signaleren van een eventuele afwijking (risico's)
  - Een analyse van de scores bepaalt risicoprocessen
  - Een analyse van de scores bepaalt risicoaspecten
  - Een analyse van de scores bepaalt afwijkingen voor bepaalde perspectieven.
- Selecteren van acties om afwijkingen op te heffen
  - Methodes uit het IT Governance werkmodel worden gebruikt om risico's op te heffen
- Uitvoeren van de geselecteerde acties

De focus van de werkwijze ligt op het tweede onderdeel (vergelijken van de feitelijke situatie met de norm). Een andere toepassing van de werkwijze is dat het de mogelijkheid biedt om verschillende analyses uit te voeren (dit wordt gedemonstreerd in het volgende hoofdstuk). De checklist beschrijft normen die binnen de aandachtsgebieden een selectie van processen beoordeeld. Met het toewijzen van een score voor elke norm kan een beoordeling gemaakt worden van de kwaliteit van IT Governance. Wanneer de IT Governance checklist volledig is ingevuld kan een uitspraak gedaan worden over de kwaliteit op verschillende manieren:

- Een uitspraak kan gedaan worden over de kwaliteit van processen binnen de aandachtsgebieden;
- Een uitspraak kan gedaan worden over de kwaliteit van verschillende aspecten (in combinatie met de processen);
- Een uitspraak kan gedaan worden over de verhouding van perspectieven. Waarbij beoordeeld wordt of de organisatie te weinig of teveel aandacht besteed aan één of meerdere perspectieven.

Onderstaand voorbeeld uit de IT Governance checklist laat zien dat in het aandachtsgebied *Plan & Organise* het proces *Define a Strategic IT Plan*, van het aspect functioneel beheer, vanuit het perspectief van *corporate contribution* wordt behandeld:

Plan & Organise (PO1): Define a Strategic IT Plan:

Aspect	Nummer	Item	perspectief
FB	3	Concrete plannen voor de lange termijn zijn opgesteld om verbeteringen aan te brengen in bedrijfsprocessen, organisatie, ondersteunende IV en de aansluiting daartussen	Corporate contribution

Wanneer slecht gescoord wordt op het perspectief *corporate contribution* in het *Plan & Organise* aandachtsgebied dan duidt dat o.a. op een matige integratie van IT strategieën met bedrijfsdoelen en matig beheer van de IS portfolio. Wanneer soortgelijke conclusies getrokken worden kan de volgende stap in de regelkring uitgevoerd worden: selecteren van acties om afwijkingen op te heffen. Dit valt echter buiten de scoop van dit onderzoek.

6.4 Samenvatting

Om antwoord te geven op de onderzoeksvraag: *"Welke werkwijze kan met de gevonden methodes ontwikkeld worden?"* is in dit hoofdstuk de werkwijze voorgesteld in de vorm van een IT Governance checklist. Deze werkwijze is vanuit de theorie opgezet waarbij gebruik is gemaakt van methodes.

Doelstelling bij het ontwikkelen van de werkwijze voor dit onderzoek is dat die gestructureerd, overzichtelijk en pragmatisch moet zijn:

- Structuur wordt geboden door aandachtsgebieden, aspecten en perspectieven;
- Het overzicht wordt geboden door onderdelen van methodes te koppelen aan een selectie van IT processen;
- De pragmatische kant van de werkwijze wordt geboden door de (IT Governance) checklist.

Het resultaat is een IT Governance checklist gebaseerd op het IT Governance model met +/- 200 normen die elk een score toegewezen krijgt bij de beoordeling van de processen. De IT Governance checklist (bijlage X) maakt het dus mogelijk om op een **gestructureerde** (aandacht voor aandachtsgebieden/processen, aspecten en perspectieven), **overzichtelijke** (selectie processen) en **pragmatische** (selectie van normen) manier de kwaliteit van IT Governance te beoordelen. Deze IT Governance checklist is een concrete vertaling van het IT Governance werkmodel die tevens aansluit bij de gedefinieerde doelstelling uit dit hoofdstuk. De checklist stelt EDP Auditors in staat om de kwaliteit van IT Governance bij organisaties te beoordelen. De werkwijze die is ontwikkeld voor dit onderzoek kan als volgt samenvattend weergegeven worden:

Werkwijze ter beoordeling van IT Governance:

Als werkwijze om de kwaliteit van
besturing (Governance) van de automatisering (IT) bij organisaties te bepalen
worden gekozen aspecten binnen de aandachtsgebieden voor een selectie van processen
beoordeeld vanuit verschillende perspectieven
gebruikmakend van een IT Governance checklist met normen.

Leenslag (2006)

HOOFDSTUK 7

PRAKTIJKONDERZOEK

In voorgaande hoofdstukken is de werkwijze ontwikkeld om de kwaliteit van besturing van automatisering te beoordelen bij organisaties. Deze werkwijze heeft als doelstelling om gestructureerd, overzichtelijk en pragmatisch te zijn. Het resultaat is een IT Governance checklist die het mogelijk maakt om een uitspraak te doen over de kwaliteit van IT Governance bij organisaties. In dit hoofdstuk wordt het praktijkonderzoek beschreven van de werkwijze. Daarbij wordt de volgende onderzoeksvraag behandeld:

Wat is het resultaat van de toepassing van de ontwikkelde werkwijze?

Om deze onderzoeksvraag te beantwoorden zijn drie interviews gehouden bij verschillende organisatie. In § 7.1 wordt een inleiding gegeven van dit hoofdstuk en wordt de opzet van het interview beschreven. § 7.2 beschrijft de resultaten van de interviews. Eén van de geïnterviewde organisaties heeft de IT Governance checklist ingevuld. Deze resultaten zijn verwerkt om een analyse over de kwaliteit van IT Governance mogelijk te maken. Dit wordt tevens in deze paragraaf behandeld. § 7.3 geeft een samenvatting van de resultaten van de interviews.

7.1 Inleiding praktijkonderzoek

In dit hoofdstuk wordt het praktijkonderzoek beschreven om de werkwijze toe te passen bij organisaties en om een oordeel te vragen over de werkwijze. Voor het praktijkonderzoek is gekozen voor *case studies* door middel van interviews. Hierbij zijn enkele organisaties geselecteerd en daarna benaderd om mee te werken aan het praktijkonderzoek. In dit hoofdstuk wordt respectievelijk een financiële dienstverlener, een uitgever van regionale dagbladen en het Kadaster behandeld.

De geïnterviewden zijn gevraagd om de IT Governance checklist toe te passen op hun eigen organisatie. Hierbij is een score gevraagd voor elke norm. Na toepassing van de checklist is in een diepte interview gevraagd om een oordeel te geven over de werkwijze om de besturing van automatisering te beoordelen. In de vragenlijst worden de volgende onderwerpen behandeld:

- Algemene onderwerpen:
  - Vragen over de organisatie en functionaris
- Algemene onderwerpen IT Governance:
  - Vragen om te onderzoeken in welke mate IT Governance wordt toegepast
- Onderwerpen IT Governance checklist:
  - Vragen om te beoordelen of de werkwijze de juiste structuur heeft. Vragen m.b.t. het overzicht van de werkwijze waarbij beoordeeld wordt of de checklist volledig genoeg is. En als laatste een beoordeling over de pragmatische toepasbaarheid.
- Eindoordeel:
  - Vragen waarbij de geïnterviewde een mening geeft over de IT Governance checklist in zijn geheel.

Voor aanvang van het interview is de vragenlijst en IT Governance checklist verstuurd naar de geïnterviewde. De vragenlijst voor de interviews is opgenomen in bijlage XII. Er is gekozen om de IT Governance checklist in de bijlage weg te laten uit de vragenlijst. Uiteraard is de checklist wel verstuurd met de vragenlijst naar de geïnterviewde. In de volgende paragraaf worden de resultaten van de interviews beschreven. In de laatste paragraaf volgt een samenvatting en een conclusie met betrekking tot de uitkomsten van de interviews.

7.2 Resultaten onderzochte cases

7.2.1 Case: Financiële dienstverlener

Organisatie:
Bij een grote financiële dienstverlener is gesproken met de staffunctionaris Corporate IT Staff department verantwoordelijk voor IT Performance and Investment Management. De geïnterviewde is tevens een expert op het gebied van IT Governance en wordt door de auteur van dit onderzoek gezien als waardevolle persoon om een oordeel te geven over het IT Governance model en de checklist. De organisatie van de geïnterviewde is in meer dan 50 landen actief met een uitgebreid productassortiment op het gebied van bankieren, verzekeren en vermogensbeheer. De totale organisatie kent 114.000 medewerkers waarvan 14.000 behoren tot de IT organisatie. Het budget van de IT organisatie bedraagt 2.5 miljard euro. Er kan dus gesproken worden van een zeer grote (IT intensieve) organisatie.

IT Governance:
IT Governance wordt expliciet toegepast bij deze organisatie. De IT Governance benadering van de financiële dienstverlener heeft betrekking op organisatie en besluitvorming. Er is een Operation & Informations Services Leadership Council met IT Managers van de verschillende lines of business en een Operations & Informations Services Board met board members. IT Governance wordt door de financiële dienstverlener beschouwd als het geheel van processen en structuren waarbij IT ondersteuning geeft aan de te behalen business doelstellingen en dat de besluitvorming over processen, IT architecturen en IT infrastructuren zoveel mogelijk op die niveaus worden gelegd waarop zinvolle besluitvorming over deze onderwerpen kan plaatsvinden. Op centraal niveau betekent dit besluitvorming over bijvoorbeeld gemeenschappelijk gebruik van infrastructuur, of applicaties. Op decentraal niveau betreft het meer de Line of Business specifieke IT applicaties en infrastructuur, etc. In de organisatie worden bestaande methodes gebruikt, zoals PRINCE, CMM, CMMi, Six Sigma en ISO17799.

IT Governance checklist:
Bij de beoordeling van de structurering van de checklist en het werkmodel kwam de vraag van de geïnterviewde naar voren wat de selectiecriteria zijn geweest voor de gekozen CoBiT processen. Aangezien de geïnterviewde geen aanvullende informatie heeft ontvangen over de selectie van processen is dit een logische observatie. Processen als PO9 – Manage Risks en PO5 – Manage IT Investments zijn volgens de geïnterviewde belangrijke processen die in de checklist niet voorkomen.

Met betrekking tot de perspectieven refereerde de geïnterviewde naar de toepassing van Business Goals zoals beschreven in CoBiT 4.0. Deze Business Goals zijn gestructureerd volgens het BSC principe en zijn door de ITGI gekoppeld aan IT Goals welke vervolgens weer zijn gerelateerd aan

CoBiT 4.0 processen. De koppeling van deze Goals en de IT BSC is niet duidelijk terug te vinden in het model.

Eindoordeel:
De IT Governance checklist was in de ogen van de geïnterviewde niet op strategisch niveau toepasbaar bij de financiële dienstverlener. Hiervoor waren de geselecteerde normen te concreet en gedetailleerd. De normen zijn wel geschikt om op tactisch/operationeel niveau een oordeel te geven en wordt op dat niveau als redelijk compleet beschouwd.

Het is de mening van de geïnterviewde dat het ontwikkelde IT Governance model en checklist op decentraal niveau bij de Line of Business goed kunnen functioneren. Voor een grote financiële dienstverlener met meerdere Line of Business is het niet direct mogelijk om de vragenlijst in zijn algemeenheid te beantwoorden op centraal niveau.

Een aanvullend onderwerp kwam aan bod tijdens het interview. Het is belangrijk om het kader te bepalen waarbinnen het ontwikkelde model valt. Aangezien IT Governance een vrij omvangrijk onderwerp is wordt met de titel <Beoordeling IT Governance> gesuggereerd dat de complete IT Governance beoordeeld wordt. Bij bestudering van het model en de checklist blijkt dat het om een beperkt gedeelte gaat van IT Governance. De positionering van dit model in het grotere IT Governance concept is volgens de geïnterviewde erg belangrijk waarbij duidelijk moet blijken wie de doelgroep is. Dit is bij aanvang van het interview niet goed aangegeven.

Samenvatting:
- Oordeel checklist is goed
- Voor zeer grote organisatie alleen toepasbaar op tactisch en operationeel niveau i.v.m. detail
- Positie van ontworpen IT Governance model in de totale IT Governance structuur
- Duidelijkheid creëren over beoogde doelgroep

7.2.2 Case: Uitgever

Organisatie:
Bij een grote uitgever is gesproken met de internal auditor / security officer. De organisatie is de grootste uitgever van regionale dagbladen en huis-aan-huiskranten in Nederland en een belangrijke speler in West-Europa op het gebied van direct marketing. Daarnaast ontwikkelt en exploiteert de organisatie internetproducten en -diensten, geeft special-interesttijdschriften uit en levert grafische producten en diensten. De organisatie telt meer dan 5000 medewerkers. Hiervan hebben meer dan 150 een IT functie. De omzet van de totale organisatie is 665 miljoen euro. Het IT budget bedraagt 30 miljoen euro.

IT Governance:
IT Governance wordt expliciet toegepast in de organisatie. IT Governance heeft vooral betrekking op de aansluiting van IT op de business organisatie en het afleggen van verantwoording. Bekende methodes als ITIL en ISO17799 (Code voor Informatiebeveiliging) worden gebruikt. Andere methodes van het IT Governance werkmodel worden niet toegepast in de organisatie.

IT Governance checklist:
Over de structurering was de geïnterviewde tevreden, hij herkende de COSO en CoBiT structuur terug in het model. Dit was een interessante observatie aangezien de geïnterviewde bij aanvang van het gesprek geen volledige kennis had van de opdracht en de totstandkoming van het model. De geïnterviewde kon de onderdelen van de structuur uitstekend positioneren. In de visie van de geïnterviewde zijn geen essentiële aandachtsgebieden, processen, aspecten en perspectieven weggelaten.

De gesproken functionaris is naast internal auditor ook security officer waardoor tijdens het gesprek veel aandacht uitging naar het beveiligingsaspect (SEC). De geïnterviewde is tevreden met de geselecteerde normen (gebaseerd op ISO17799) en de resultaten geven een goed inzicht in de kwaliteit van dit aspect voor de organisatie. De normen voor het beveiligingsaspect worden nuttig en bruikbaar bevonden.

De koppeling met perspectieven kwam bij enkele normen (van het beveiligingsaspect) ter discussie, hier wordt na de interviews door de auteur nog eens extra kritisch naar gekeken. Mogelijke discrepanties zijn opgetreden i.v.m. het verplaatsen van bepaalde normen naar andere aandachtsgebieden.

De geïnterviewde is van mening dat de normen erg formeel omschreven zijn. De geïnterviewde geeft zelf aan dat dit komt door de theoretische achtergrond van de normen. Het wordt niet aanbevolen om de theorie ter discussie te stellen en de normen minder formeel te maken.

Eindoordeel:
Een conclusie die werd gedaan was dat het model en de checklist een hoog strategisch gehalte hebben. Het is echter wel nodig om met de checklist verder de organisatie (op tactisch en operationeel niveau) in te gaan om alle normen te beoordelen. De organisatie werkt namelijk met divisies en veel normen zijn toepasbaar voor meerdere divisies. De checklist moet meerdere keren ingevuld worden. In de ontwikkelde IT Governance benadering is niet expliciet rekening gehouden met organisatie typologieën, zoals centrale, decentrale en hybride organisaties.

Het eindoordeel was dat IT Governance checklist een goed hulpmiddel is om *awareness* over IT onderwerpen en de kwaliteit hiervan te creëren.

Samenvatting:
- Oordeel totale checklist is goed waarbij het beveiligingsaspect in detail is behandeld tijdens het interview
- Formeel beschreven normen
- Strategisch gehalte waarbij rekening gehouden moet worden met divisies
- Toewijzing van perspectieven aan normen in enkele gevallen discutabel

7.2.3 Case: Kadaster

Organisatie:
Bij het Kadaster is gesproken met de manager afdeling Beleid en Advies. Het Kadaster registreert gegevens over registergoederen in Nederland, houdt deze bij in openbare registers en in de kadastrale registratie (die omvat de administratief juridische gegevens en de kadastrale kaart), het Kadaster levert tegen betaling gegevens uit de openbare registers (de akten) en de kadastrale registratie. Onder registergoed worden onroerende zaken (zoals percelen, appartementsrechten en leidingnetwerken) en roerende zaken (zoals schepen en luchtvaartuigen) beschouwd. De organisatie is opgericht in 1832. Om alle taken beter uit te kunnen voeren, is de organisatie sinds 1994 een zogeheten 'Zelfstandig Bestuursorgaan' (ZBO). Dit betekent dat de organisatie een publiekrechtelijke rechtspersoon is, die als organisatie zijn taken zelfstandig uitvoert, daarbij verantwoording afleggend aan de minister van VROM. De taken en organisatorische aspecten van het Kadaster worden beschreven in de Kadasterwet en in de organisatiewet Kadaster.
De organisatie biedt werk aan 2.200 mensen en heeft een omzet van 210 miljoen euro. Het budget voor IT heeft een omvang van 54 miljoen euro. Tijdens het interview werd duidelijk dat het Kadaster gezien kan worden als een innovatieve organisatie. Dit blijkt ook wel aan het budget wat de IT organisatie te besteden heeft. De projectportefeuille is gevuld met zaken als het stelsel van basisregistraties, vernieuwing van systemen, realisatie van systemen in het kader van de wet kenbaarheid publiekrechtelijke beperkingen, vernieuwing in de informatieontsluiting, ontwikkeling nieuwe producten *en* een aantal punten ter verbetering van de efficiency voor de klant en de interne efficiency.

IT Governance:
Bij het Kadaster vindt voortdurend overleg plaats tussen beleidsmedewerkers van de kant van de "business" en van de kant van "IT". Het business- en IT-belang worden samengebracht en ontwikkelingen worden ingezet. Van de kant van de business worden de Kadasterambities en strategische doelstellingen uitgewerkt, van de kant van de IT worden alternatieve oplossingen uitgewerkt, hierbij wordt gewerkt op basis van architecturen om ontwikkelingen te analyseren, af te bakenen en te plaatsen temidden van andere ontwikkelingen. Onderdeel van de business alignment is het gezamenlijk (business en IT) bepalen van de prioriteit van nieuwe ontwikkelingen, hierbij speelt het business en het IT-belang mee. Eenvierde van de totale kosten van het Kadaster zijn IT-gerelateerd. De rol die IT bij het Kadaster speelt is zonder meer die van business enabler. Deze rol wordt breed binnen de organisatie gedragen en bevorderd door het lid van de raad van bestuur die IT in zijn portefeuille heeft. Deze rol is vergelijkbaar met die van CIO. Bij het Kadaster wordt expliciet IT Governance toegepast door:

- business alignment waarbij de business aangeeft *wat* er moet gebeuren en de IT organisatie aangeeft *hoe* dit moet gebeuren;
- Projectmatige realisaties van nieuwe ontwikkelingen waarbij de business case en prioriteit van belang zijn;
- Werken op basis van architecturen;

- Bedrijfbrede IT-planning van IT-ontwikkelingen die gevraagd worden door het bedrijf en IT-ontwikkelingen die gevraagd worden door de IT-functie.

De geïnterviewde geeft aan dat zij veelvuldig gebruik maken van bronnen als Gartner als het gaat om IT Governance. Het Kadaster streeft naar een optimale inzet van IT-middelen, resources en budget. Dit wordt gedaan door ontwikkelingen en exploitatie van systemen aan te laten sluiten op de eigen bedrijfsdoelstellingen en op de bedrijfsprocessen van klanten. Het Kadaster heeft de ambitie om deze systemen op een betaalbare, beheersbare en beheerbare wijze te realiseren. Zij laat haar IT-performance daarom op gezette tijden extern toetsen om de prestaties waar nodig te verbeteren. De organisatie maakt gebruik van verschillende methodes. De (traditionele) balanced scorecard wordt gebruikt door de IT organisatie. De organisatie is ISO-gecertificeerd tegen o.a. ISO 9001 en de Code voor Informatiebeveiliging.

IT Governance checklist:
De structuur van het IT Governance werkmodel en de IT Governance checklist is niet één-op-één te vergelijken met de structuur van IT Governance zoals die gehanteerd wordt bij het Kadaster. Dit gaf enkele problemen bij het invullen van de checklist. Voor de geïnterviewde is niet eenduidig hoe de rol van functioneel beheer zich verhoudt t.o.v. de organisatie. Bij het Kadaster wordt wel gebruik gemaakt van de naam functioneel beheer, maar in een andere betekenis dan in het gehanteerde model. Wel zijn in de organisatie anders genoemde rollen te identificeren die verantwoordelijk zijn voor dit aspect. Als een vertaalslag gemaakt wordt dan is de CIO verantwoordelijk voor de normen die bedoeld zijn voor het functioneel beheer aspect. De service organisatie van het Kadaster is verantwoordelijk voor applicatie- en technisch beheer.

Met betrekking tot de perspectieven wordt het belangrijk bevonden dat onderscheiden wordt dat lijnmanagement (gebruikersorganisatie) voldoende betrokken is bij IT Governance vraagstukken. Dit is voor deze case erg belangrijk aangezien het Kadaster werkt met business units. De business units zijn in wezen de klanten van de IT organisatie.

Er ontbreken volgens de geïnterviewde geen essentiële aandachtsgebieden, aspecten en perspectieven. Wel wordt het belangrijk bevonden dat duidelijk wordt gemaakt waar verantwoordelijkheden van processen liggen. Dit wordt door het (generieke) IT Governance model niet altijd even duidelijk gemaakt.
Een aspect wat door de geïnterviewde als aanvulling wordt gezien is het financiële aspect. Aspecten rond Investeringen, budgetten, etc. worden niet concreet genoeg terug gevonden in de IT Governance checklist.

De IT Governance checklist is tijdens de toepassing als nuttig en bruikbaar bevonden waarbij de aantekening wordt gemaakt dat enige *tuning* van rollen, verantwoordelijkheden en begrippen nodig is voor deze case situatie.

Eindoordeel:
De structuur van het model t.o.v. het Kadaster verschilt op een aantal punten. Bij het Kadaster was het niet mogelijk om de volledige IT Governance checklist door de functionaris in te laten

vullen. Andere medewerkers zijn hiervoor nodig. Deze waren helaas niet aanwezig. Echter is een aanzienlijk gedeelte ingevuld door de geïnterviewde.

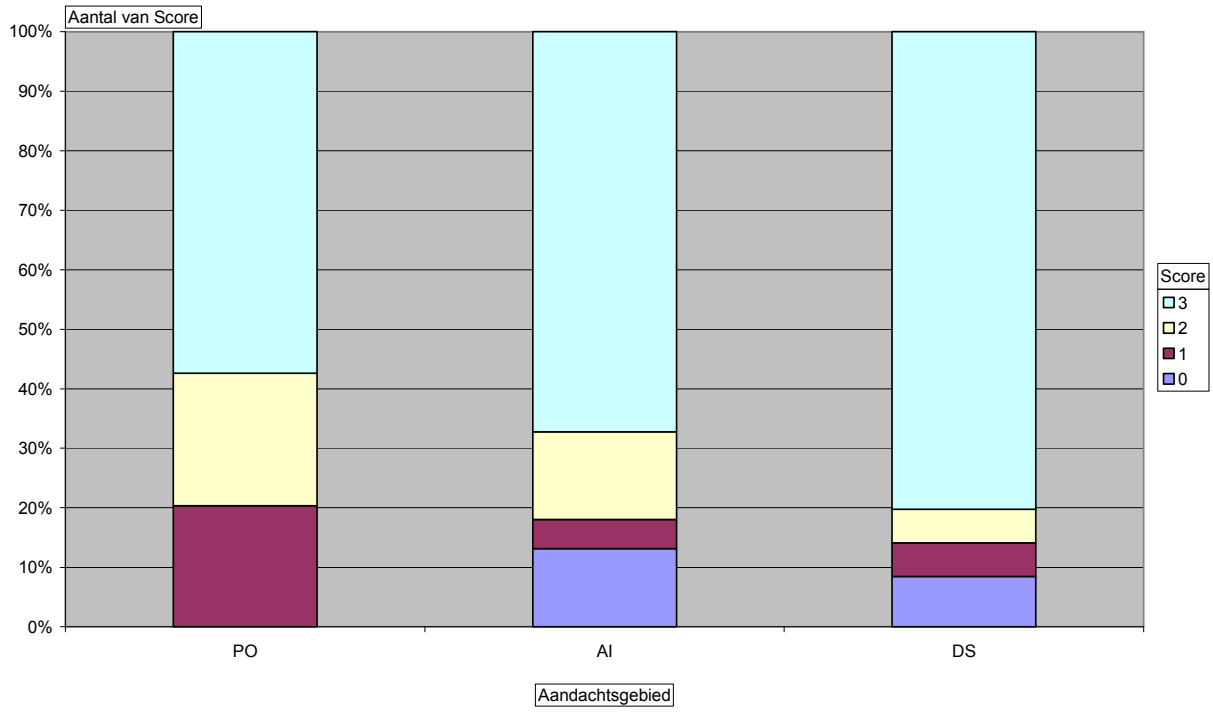
Samenvatting oordeel:

- Oordeel inhoud checklist: goed
- Aansluiting van business en ICT niet altijd duidelijk
- Structuur model niet één-op-één toepasbaar op structuur organisatie
- Tuning van verantwoordelijkheden, rollen en begrippen

Analyse resultaten IT Governance checklist:

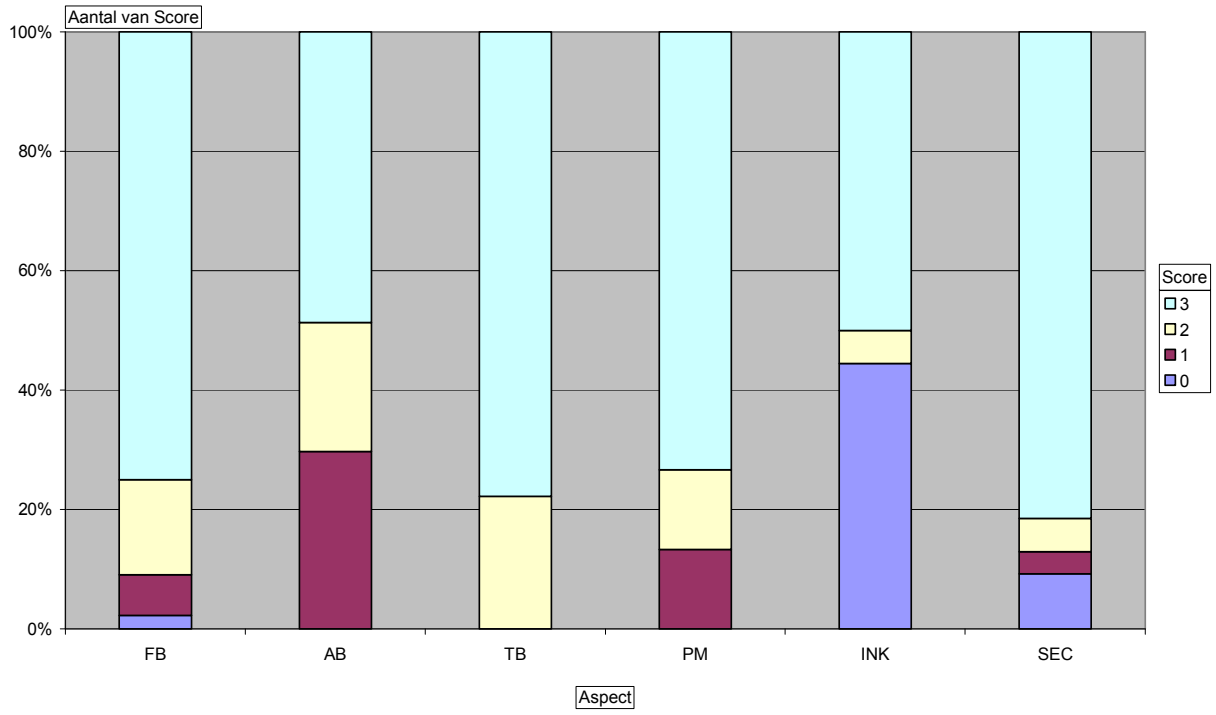
De geïnterviewde is in staat geweest vrij compleet de IT Governance checklist in te vullen. Voor bijna alle processen zijn scores aan de normen gegeven. Een aantal normen kon niet ingevuld worden. Deze normen zijn met een 0 (niet van toepassing) ingevuld. Dit is met name terug te zien bij het aspect Inkoop. Uit de score voor de totale checklist is op te maken dat het Kadaster veel normen met een 3 beoordeeld. Dit houdt in dat de norm gehaald wordt en dat het Kadaster in hoge mate *in control* is.

Uit de score per aandachtsgebied (Figuur 23) is op te maken dat het *Plan & Organise (PO)* aandachtsgebied het minste scoort van alle aandachtsgebieden. Als gekeken wordt naar de resultaten van alle aandachtsgebieden met score 3 en 2, waarbij 2 aangeeft dat verbeteringen relatief eenvoudig zijn, dan verschillen de aandachtsgebieden ten op zichte van elkaar niet veel.



Figuur 23: Score per aandachtsgebied

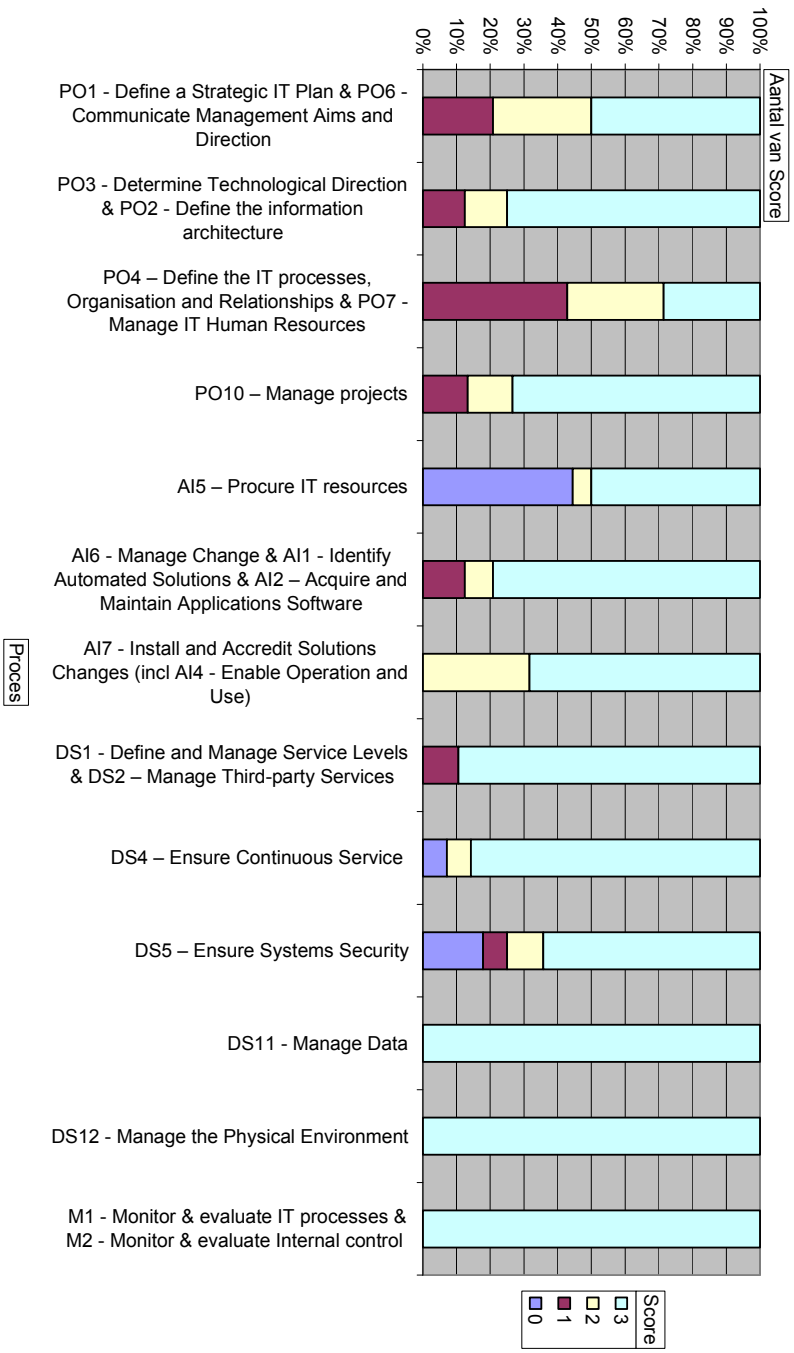
De score per aspect (Figuur 24) laat duidelijk zien dat applicatiebeheer minder goed scoort dan alle andere aspecten, die rond de 80% zitten (met uitzondering van het aspect Inkoop). Ook hier geldt dat een groot gedeelte van de normen met een 3 beoordeeld is wat aangeeft dat de kwaliteit van IT Governance hoog is.



Figuur 24: Score per aspect

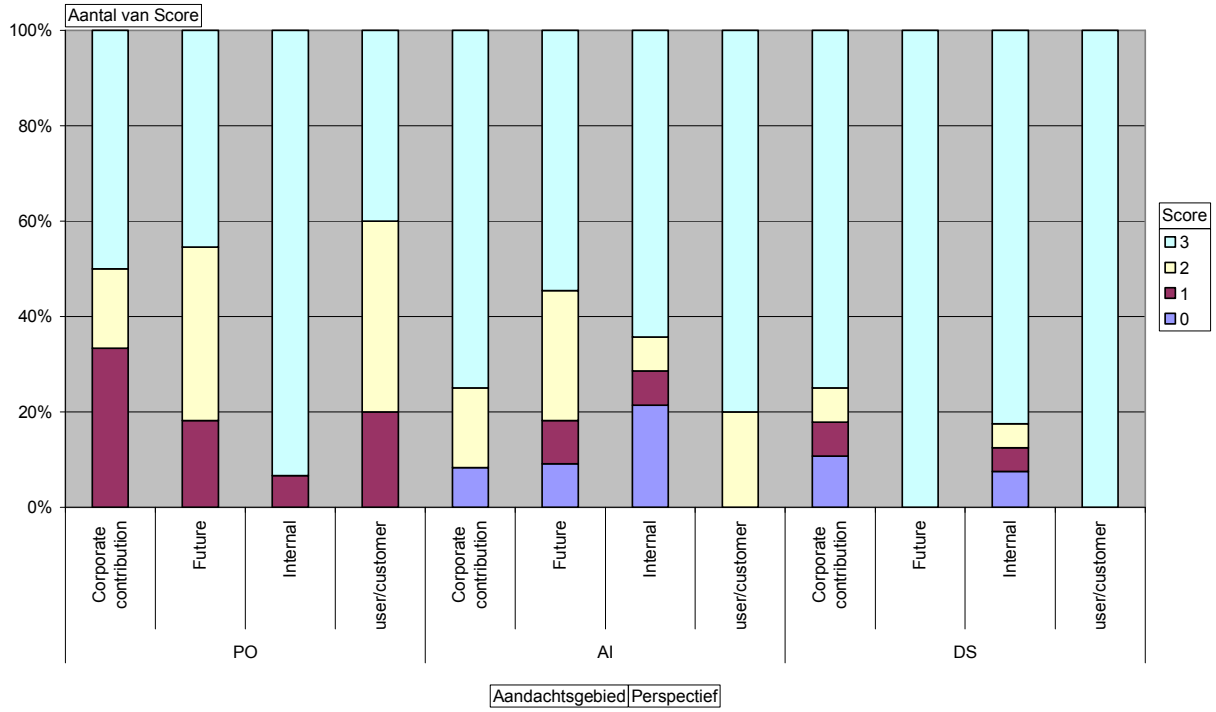
De volgende opvallende observaties worden gedaan wanneer de score per proces (Figuur 25) bestudeerd wordt:

- Architectuur en het volgen van nieuwe ontwikkelingen op gebied van IT scoort zeer hoog;
- Organisatie omtrent IT Governance scoort laag;
- Onderwerpen als onderhoud en vernieuwing (*change & release management*) scoren uitstekend;



Figuur 25: Score per proces

Bij de scores per aandachtsgebied en perspectief (Figuur 26) zijn ook een aantal interessante observaties te maken:
In het aandachtsgebied *Plan & Organise* scoren de perspectieven *corporate contribution*, *future* en *user/customer* veel lager dan *internal/operational*. Bij verdere bestudering van dit effect blijkt dat met name de aanbodorganisatie "verantwoordelijk" is voor de lage scores. Operationeel dragen ze afdoende hun steentje bij maar als het gaat over onderwerpen die betrekking hebben op de andere perspectieven laten ze het enigszins liggen.



Figuur 26: score per aandachtsgebied en perspectief

Het tweede wat opvalt in Figuur 26 is de hoge score van het perspectief *corporate contribution* en *user/customer* in het aandachtsgebied *Acquire & Implement (AI)*. Dit toont o.a. aan dat de integratie van applicaties/infrastructuren met behoeften vanuit de gebruikersorganisatie hoog is. Tevens worden gebruikers voldoende betrokken als het gaat om onderwerpen als bijvoorbeeld wijzigingsbeheer.

7.3 Samenvatting praktijkonderzoek

Om antwoord te geven op de laatste onderzoeksvraag: *"Wat is het resultaat van de toepassing van de ontwikkelde werkwijze?"* zijn in dit hoofdstuk de resultaten van een drietal interviews beschreven waarbij een oordeel over het IT Governance werkmodel en de IT Governance checklist is gevraagd. Daarnaast is bij één van de organisaties de checklist (bijna) volledig toegepast om een analyse van de kwaliteit van IT Governance te maken. Het doel van de interviews is om de structuur, volledigheid en toepassing van de IT Governance checklist en het model te laten beoordelen. Geïnterviewden zijn gevraagd om missende onderdelen of onjuistheden aan het licht te brengen. In deze paragraaf wordt een samenvatting gegeven.

IT Governance

Bij de geïnterviewde organisaties wordt expliciet IT Governance toegepast. Hierbij valt op dat twee van de drie organisaties een IT Governance benadering hebben die het beste geassocieerd kan worden met die van Weill et al. (*research approach* uit hoofdstuk 3.2). Zoals werd verwacht worden een aantal bekende methodes uit het model toegepast in de organisaties.

Oordeel checklist

Door meerdere organisaties wordt de IT Governance checklist als concreet en gedetailleerd beschouwd. Hiermee wordt bedoeld dat de normen zeer uitvoerig beschreven zijn. De normen hebben ook een formele uitstraling wat te maken heeft met de theoretische achtergrond. De IT Governance checklist is tijdens de toepassing als nuttig en bruikbaar bevonden waarbij de aantekening wordt gemaakt dat enige *tuning* van rollen, verantwoordelijkheden en begrippen nodig is voor bepaalde case situaties. Het IT Governance werkmodel en de checklist zijn generiek opgezet zodat deze voor alle grote organisatie gebruikt kan worden. Het effect dat het model niet te allen tijde past bij de structuur van de organisatie zal vaker voorkomen. Het model moet in enkele gevallen klantspecifiek gemaakt worden om verantwoordelijkheden en begrippen aan te laten sluiten op praktijksituaties van organisaties.

Omdat een selectie is gemaakt van belangrijke CoBiT processen om bepaalde aspecten te ondersteunen zal altijd de discussie bestaan dat het model niet volledig is. De vraag welke selectiecriteria gehanteerd zijn heeft hiermee ook te maken. Bepaalde processen worden niet *weggelaten* omdat ze onbelangrijk zijn bevonden voor de beoordeling van IT Governance maar omdat de gekozen aspecten (functioneel beheer, applicatiebeheer, technisch beheer, projectmanagement, beveiliging en inkoop) een vergaande relatie hebben met bepaalde processen en een beperkte relatie hebben met de overgebleven processen. De reden dat bijvoorbeeld PO9 – *Manage Risk* niet expliciet is opgenomen heeft te maken met het feit dat processen als *procure resources, manage change* en *manage project* al risico management onderwerpen behandelen. Bij meerdere interviews kwam naar voren dat het financiële aspect een aanvulling kan zijn op het model. Onderwerpen over investeringen, budgetten, etc. worden niet concreet genoeg terug gevonden in de IT Governance checklist. De ontwikkelde IT Governance benadering en het IT

Governance werkmodel laten het toe om, middels methodes, andere aspecten toe te voegen om op deze manier de IT Governance checklist completer te maken.

Tijdens de ontwikkeling van de IT Governance checklist is als doelstelling gehanteerd om middels de IT BSC methode een gebalanceerde verhouding van normen te krijgen. De business goals zoals beschreven in CoBiT 4.0 zijn gestructureerd volgens de BSC methode en kunnen gebruikt worden in combinatie met de cascade IT BSC principe zoals beschreven in de scriptie. Deze koppelt de traditionele BSC met de IT BSC. De algemene Business Goals zijn een manier om bedrijfsdoelen te koppelen aan IT processen. Het voordeel van het ontwikkelde IT Governance model en checklist is dat deze gestructureerd zijn volgens de (IT) BSC principes. Koppeling met de CoBiT 4.0 Business Goals en de Business BSC behoeft dan ook geen probleem te zijn. Uiteraard kan de IT Governance checklist ook gekoppeld worden aan een eigen bedrijfs-BSC. Hierbij wordt door één van de geïnterviewde geadviseerd om de gebruikersorganisatie voldoende te betrekken bij IT Governance vraagstukken. De perspectieven *user/**customer*** en, in zekere mate, *corporate contribution* zijn hiervoor bedoeld. Zoals weergegeven in hoofdstuk 6 hebben deze twee perspectieven een substantieel aandeel in het IT Governance model. Verder onderzoek moet uitmaken wat de toegevoegde waarde hiervan is voor de BSC van de IT organisatie. Dit valt buiten de scope van deze interviews.

Met betrekking tot de toewijzing van perspectieven aan normen kwam bij één van de interviews naar voren dat enkele niet correct bleken te zijn. Hiervoor is na de interviews nog eens heel kritisch gekeken naar de toewijzing van perspectieven aan normen. Enkele wijzigingen zijn doorgevoerd en verwerkt in de scriptie. In het *Plan & Organise* aandachtsgebied zijn enkele aanpassingen gedaan waarbij met name wijzigingen zijn aangebracht tussen *user/customer* & *corporate* en *user/customer* & *internal*. In het aandachtsgebied *Acquire & Implement* zijn met name enkele *internal* perspectieven veranderd in *future/innovation & learning*. Deze leggen meer nadruk op de aanpak/procedures van processen. In het aandachtsgebied *Deliver & support* zijn een aantal aanpassingen gedaan op de perspectieven *internal* en *corporate contribution*. Procentueel is niet veel veranderd m.b.t. de verhouding van perspectieven in de aandachtsgebieden. De verhouding van de perspectieven zoals die na de wijziging is wordt weergegeven in de diagrammen uit hoofdstuk 6. De wijzigingen aan de normen en de redenen zijn opgenomen in bijlage XI. In bijlage X is de IT Governance checklist weergegeven zoals die moet zijn na de wijzigingen.

Eindoordeel interviews

Het eindoordeel is dat de structuur en toepasbaarheid van het model en de checklist goed zijn bevonden. Het model is generiek opgezet om toepasbaar te zijn voor een breed assortiment organisaties. Het kan nodig zijn dat in enkele gevallen een klantspecifieke vertaalslag gemaakt moet worden om het model en de checklist aan te sluiten op rollen, verantwoordelijkheden en begrippen die gebruikt worden door de organisatie. Wanneer de IT Governance checklist toegepast wordt op een case is het aan te raden om in een inleidend gesprek de structuur van de organisatie te matchen met de structuur van het IT Governance werkmodel en de checklist.

Een ander eindoordeel van het model en de checklist is dat door de gebruiker aangegeven moet worden wat de positie van het model ten opzichte van IT Governance in het geheel is. De normen in de checklist worden als gedetailleerd omschreven. Echter wanneer dit model *zomaar* bij een organisatie wordt toegepast is niet direct duidelijk wat het precieze kader is t.o.v. IT Governance en wie de beoogde doelgroep is. Zoals eerder beschreven in de scriptie zorgt IT Governance ervoor dat de IT uitgelijnd is met bedrijfsprocessen en dat deze op de juiste manier georganiseerd, bestuurd en beheerst is. IT Governance verschaft structuur die een link legt tussen IT processen, IT resources en informatie met de organisatiestrategie en doelen. Verschillende auteurs geven aan dat *control* een vereiste is voor effectieve IT Governance. Vanuit dit oogpunt wordt het ontwikkelde IT Governance werkmodel benaderd en dit is tevens zijn kader. Middels de toepassing van de IT Governance checklist bij het Kadaster is geprobeerd aan te tonen in welke mate *control* wordt uitgevoerd. De doelgroep van de ontwikkelde werkwijze zijn IT specialisten en verantwoordelijken van IT in organisaties.

Het proces om alle +/- 200 normen te beoordelen is omvangrijker dan in eerste instantie werd aangenomen. Verantwoordelijken hebben niet altijd volledige beschikking over de benodigde informatie om een uitspraak te doen. De lijst is te uitgebreid en gedetailleerd om *maar* door één functionaris in een grote organisatie in te laten vullen. Andere functionarissen zijn nodig om bepaalde aspecten te beoordelen. Het is niet verwonderlijk dat een persoon die verantwoordelijk is voor functioneel beheer niet (alle) normen van applicatiebeheer kan beoordelen. Dus om bepaalde processen volledig te beoordelen kan het nodig zijn om meerdere personen te interviewen. Hier ligt natuurlijk de rol van de EDP Auditor om organisaties te assisteren in het verkrijgen van de informatie om op deze manier de kwaliteit van IT Governance te beoordelen.

Het niveau (strategisch, tactisch of operationeel) waarop de checklist toepasbaar is lijkt te verschillen. Voor hele grote organisatie, zoals de financiële dienstverlener, speelt de IT Governance checklist op een tactisch/operationeel niveau en zijn andere vraagstukken van IT Governance aan de orde op strategisch niveau. Bij de andere twee organisaties is de checklist wel op strategisch niveau toepasbaar.

Bij twee van de drie interviews kwam naar voren dat de lijst, op bepaalde onderdelen, per divisie ingevuld moet worden. In de IT Governance benadering kan de centrale, decentrale en hybride organisatie typologieën meegenomen worden om te verduidelijken welk onderdelen van de checklist door welke eenheid van de organisatie ingevuld moet worden. Het effect van onderscheid in typologieën is dat bij een decentrale typologie bepaalde normen meerdere keren worden beoordeeld. Door deze extra dimensie aan de IT Governance benadering toe te voegen wordt het model formeler en mogelijkerwijs minder pragmatisch. Aanvullend onderzoek is nodig naar het nut van de toevoeging van deze dimensie aan de IT Governance benadering en het effect op de complexiteit van het IT Governance model en IT Governance checklist.

HOOFDSTUK 8

CONCLUSIES & AANBEVELINGEN

In dit hoofdstuk worden de conclusies & aanbevelingen beschreven van de scriptie. De doelstelling zoals omschreven in hoofdstuk 1 heeft geresulteerd in een aantal onderzoeksvragen. Deze zijn in voorgaande hoofdstukken behandeld. De conclusies uit de theorie en empirie worden in dit hoofdstuk behandeld.

Dit hoofdstuk begint in § 8.1 met een korte inleiding. In § 8.2 worden de conclusies gepresenteerd uit de theorie. In § 8.3 worden de conclusies over de toepassing van de werkwijze op organisaties besproken. De resultaten van de theorie en de praktijk leveren een aantal aanbevelingen. Deze zijn van belang bij de toepassing van de werkwijze en voor verder onderzoek op dit gebied.

8.1 Inleiding conclusies & aanbevelingen

Statistieken hebben aangetoond dat IT Governance momenteel volop in de belangstelling staat binnen Nederlandse ondernemingen. Helaas is de kwaliteit van IT Governance in veel gevallen nog ontoereikend. Beoordelingen over de kwaliteit van besturing (Governance) van de automatisering (IT) bij organisaties wordt bij Ernst & Young door EDP Auditors uitgevoerd. Hiervoor is geen beschreven werkwijze beschikbaar. Methodes zoals CoBiT, ITIL en de Code voor informatiebeveiliging worden wel als normenkaders gebruikt bij beoordelingen. Het gebrek aan een eenduidige werkwijze weerhoudt de overdraagbaarheid van de werkwijze en maakt communicatie over dit onderwerp met organisaties moeilijk. Daarnaast kunnen andere methodes ook gebruikt worden bij de beoordeling van IT Governance bij organisaties. Dit is de aanleiding geweest van dit onderzoek. Hierbij is de volgende doelstelling gehanteerd:

Doelstelling:

Het doel van dit onderzoek is om een werkwijze te ontwikkelen waarmee de kwaliteit van besturing (Governance) van de automatisering (IT) bij organisaties wordt beoordeeld op basis van geaccepteerde methodes op het terrein van IT Governance.

Leenslag (2006)

Het doel van de werkwijze is tweeledig: (1) De werkwijze wordt gebruikt als overdraagbare methode bij Ernst & Young EDP Audit om auditors een handleiding te geven bij het bepalen van de kwaliteit van IT Governance. (2) Daarnaast werkt het als communicatiemiddel richting organisaties om aan te geven hoe zij *in control* blijven van hun IT processen. Om deze doelstelling te realiseren zijn in dit onderzoek een aantal onderzoeksvragen behandeld (Tabel 9: Onderzoeksvragen). Deze onderzoeksvragen zijn in voorgaande hoofdstukken uitvoerig behandeld. De conclusies worden in de volgende paragrafen beschreven.

Onderzoeksvragen	Hoofdstuk
Wat is IT Governance?	Hoofdstuk 2: IT Governance
Welke invalshoeken zijn te onderscheiden voor IT Governance?	Hoofdstuk 3: Invalshoeken IT Governance
Wat zijn geaccepteerde methodes op het terrein van IT Governance?	Hoofdstuk 4: IT Governance methodes
Welke koppeling tussen methodes is er mogelijk?	Hoofdstuk 5: Koppeling IT Governance methodes
Welke werkwijze kan met de gevonden methodes ontwikkeld worden?	Hoofdstuk 6: Werkwijze IT Governance beoordeling
Wat is het resultaat van de toepassing van de ontwikkelde werkwijze?	Hoofdstuk 7: Praktijkonderzoek

Tabel 9: Onderzoeksvragen

8.2 Conclusies vanuit het theoretische kader

IT Governance:

De vele definities uit de literatuur over IT Governance tonen aan dat niet duidelijk is hoe men IT Governance moet omschrijven. Veel van de definities verschillen van elkaar maar tonen ook enig overlap. In dit onderzoek zijn verschillende definities bestudeerd en zijn overeenkomsten gebruikt om uiteindelijk tot de conclusie te komen dat de definitie van de ITGI het beste past bij de doelstelling van dit onderzoek. IT Governance zorgt ervoor dat de IT uitgelijnd is met bedrijfsprocessen en dat deze op de juiste manier georganiseerd, bestuurd en beheerst is. Een belangrijk onderwerp bij IT Governance die in meerdere definities gebruikt wordt is *control*. Dit is een vereiste voor effectieve IT Governance. Dit is tevens het kader geweest van IT Governance voor dit onderzoek die aansluit bij de doelstelling. Belangrijke termen bij IT Governance zijn: *structures*, *mechanisms* en *processes*. Deze onderwerpen zijn voor het onderzoek gebruikt bij het ontwikkelen van een eigen IT Governance benadering en werkwijze.

Met betrekking tot de discussie wat de verschillen zijn tussen IT Governance en IT Management is geconcludeerd dat voor dit onderzoek geen expliciet onderscheid is gemaakt tussen de twee begrippen. Onder IT Governance, IT sturing en IT Management wordt hetzelfde verstaan.

Invalshoeken en benaderingen van IT Governance:

Vanuit de literatuur zijn verschillende IT Governance benaderingen geïdentificeerd. Om deze benaderingen te bestuderen en onderling te vergelijken is vanuit de theorie een metamodel ontworpen om deze benaderingen op een uniforme wijze te structureren. Dit metamodel maakt gebruik van drie dimensies: de wie, wat en hoe van IT Governance. De drie IT Governance benaderingen die zijn bestudeerd zijn: *research based approach*, *practicitoners based approach, educational based approach*. Het is gebleken dat alle benaderingen hun voor- en nadelen hebben. Na bestudering is een eigen IT Governance benadering ontwikkeld die aan de doelstelling van de opdracht en het (gekozen) kader voldoet. Hierbij is gebruik gemaakt van sterke eigenschappen van bestaande IT Governance benaderingen. Het eigen IT Governance framework geeft aandacht aan: (1) de vraag- en aanbodorganisatie, (2) aandachtsgebieden van IT Governance en (3) biedt de mogelijkheid om methodes toe te passen. Met dit IT Governance framework is het mogelijk om voor een aantal aspecten, binnen de aandachtsgebieden, de kwaliteit van IT Governance te beoordelen.

Methodes:

Om het abstracte IT Governance framework concreet te maken zijn verschillende methodes uit de literatuur geselecteerd. Deze methodes hebben unieke eigenschappen maar globaal zijn ze op de volgende manier onder te verdelen: (1) methodes die de vraag- en aanbodkant ondersteunen, (2) methodes die specifieke IT aspecten ondersteunen en (3) methodes om evaluaties mogelijk te maken. De volgende methodes zijn uiteindelijk gebruikt voor dit onderzoek: CoBiT, BiSL, ASL, ITIL, PRINCE2, iSPL, ISO 17799 en IT BSC. Deze verzameling is niet compleet om alle aspecten van IT af te dekken. Een selectie is nodig geweest om binnen de kaders van dit

onderzoek te blijven. Positionering van deze methodes heeft geresulteerd in een concreet toepasbaar IT Governance werkmodel (Figuur 16). Tijdens de literatuurstudie is ook CMM(i) als methode bestudeerd om de *maturity* van processen te beoordelen. De beschreven systematische techniek om de processen te scoren is gebaseerd op literatuur en bestaat uit een vragenlijst per CoBiT proces. Tijdens de ontwikkeling van de werkwijze is deze methode niet gebruikt. Dit zou de werkwijze te omslachtig maken. Daarnaast is de toegevoegde waarde hiervan *slechts* een score van 0 tot en met 5. Tijdens het ontwikkelen van de werkwijze is gekozen voor een checklist met normen die met scores beoordeeld worden. Er is gekozen om naast de checklist niet nog een vragenlijst te gebruiken om de *maturity* te beoordelen. Echter staat het werkmodel toe om met de beschreven techniek uit hoofdstuk 4 de *maturity* van geselecteerde processen te beoordelen. Dit brengt wel meer werk met zich mee, en meer vragen die door de organisatie beantwoord moet worden. De kans dat een organisatie op niveau 2 (*Controls are in place but are not documented*) of niveau 3 (*Controls are in place and are adequately documented*) zit is relatief hoog. De normen uit de IT Governance checklist zijn concreter en gedetailleerder om beoordelingen (en analyses) mogelijk te maken.

Koppeling methodes:

Eerder genoemde methodes zijn gekoppeld aan generieke IT processen waarbij CoBiT als referentiemodel is gebruikt. Het resultaat hiervan is: (1) een overzicht van de relaties en bijdrage van individuele methodes met generieke IT-processen, (2) een overzicht van de onderlinge relaties van de methodes (en de koppeling tussen de vraag- en aanbodorganisaties) en (3) een overzicht van de mate waarin de ene methode voldoet aan de andere. De conclusie die hieruit wordt getrokken is dat een selectie van CoBiT processen goed worden ondersteund door de gekozen methodes. Deze processen zijn dan ook gekozen om de kwaliteit van IT Governance te beoordelen. De koppeling maakt het mogelijk om IT Governance bij organisaties verticaal en horizontaal te beoordelen. Verticaal betekent dat IT Governance vanuit het oogpunt van IT aspecten wordt behandeld en horizontaal betekent dat IT Governance vanuit het oogpunt van processen wordt behandeld. Dit wordt duidelijk weergegeven in Tabel 6: Koppeling methodes. Om een uitspraak te doen over de (horizontale) processen is het nodig om de (verticale) aspecten te beoordelen.

Werkwijze:

Het ontwikkelde werkmodel is de basis van de werkwijze. Deze stelt in staat om op een gestructureerde, overzichtelijke en pragmatische manier de kwaliteit van IT Governance bij organisaties te beoordelen. De structuur omvat: (1) de aandachtsgebieden, (2) de aspecten en (3) perspectieven waarop beoordeeld wordt. De selectie van IT processen die een vergaande relatie hebben met onderdelen uit de methodes zorgen voor een overzichtelijke werkwijze waarbij alleen processen worden beoordeeld die belangrijk zijn (voor de gekozen aspecten). Nut en bruikbaarheid van de werkwijze worden gerealiseerd door een checklist met normen. Deze normen zijn gebaseerd op de onderdelen van de verschillende methodes. Dit heeft geresulteerd in een IT Governance checklist die +/- 200 normen bevat. Aan deze normen wordt een score toegewezen waarnaar een uitspraak gedaan kan worden over: (1) de kwaliteit van processen, (2) aspecten en (3) over de verhouding van de perspectieven. Deze werkwijze om de kwaliteit van IT

Governance bij organisaties te beoordelen is opgenomen in bijlage X. Hiermee wordt, vanuit de literatuur, voldaan aan de doelstelling van de opdracht:

Werkwijze ter beoordeling van IT Governance:

Als werkwijze om de kwaliteit van
besturing (Governance) van de automatisering (IT) bij organisaties te bepalen
worden gekozen aspecten binnen de aandachtsgebieden voor een selectie van processen
beoordeeld vanuit verschillende perspectieven
gebruikmakend van een IT Governance checklist met normen.

Leenslag (2006)

8.3 Conclusies vanuit het empirische kader

Normen voor belangrijke processen om de aspecten te ondersteunen zijn verwerkt in een IT Governance checklist. De beoordeling van deze checklist en de toepassing ervan is middels een drietal interviews uitgevoerd. De resultaten van het praktijkonderzoek zijn gebruikt om de volledigheid en correctheid van de werkwijze te bepalen.

Uit de literatuur bleek al dat IT Governance volop in de belangstelling staat bij organisaties. Dit werd nog eens bevestigd tijdens het praktijkonderzoek. Bij alle organisaties waar een interview is gehouden wordt expliciet IT Governance toegepast.

Met betrekking tot de volledigheid van de werkwijze kwam naar voren dat een aspect toegevoegd kan worden, namelijk het financieel management. Dit is in de context van IT Governance een hele logische aanvulling op het huidige model. De normen zijn als zeer correct beoordeeld door de verschillende organisaties. De normen worden als nuttig en bruikbaar gezien. De huidige aspecten zijn in voldoende detail uitgewerkt om een beoordeling mogelijk te maken over de kwaliteit van IT Governance. Bij één van de interviews kwam naar voren dat enkele normen in een bepaald aspect mogelijke aanpassingen nodig hadden met betrekking tot de toewijzing van het perspectief aan de norm. Hiervoor zijn na de interviews een aantal wijzigingen doorgevoerd aan de IT Governance checklist. Deze wijzigingen zijn opgenomen in bijlage XI. De IT Governance checklist na de wijzigingen is weergegeven in bijlage X, en dit is dus ook het eindproduct. Middels bijlage XI is het mogelijk om de huidige IT Governance checklist te reconstrueren naar de checklist voor de interviews. Deze is niet seperaat opgenomen in de bijlage van de scriptie om verwarring te voorkomen.

De mate waarin een organisatie *in control* is van hun IT Governance is aangetoond middels de toepassing van de checklist op één van de organisaties. Hieruit blijkt dat de kwaliteit redelijk hoog is. Helaas zijn van de overige twee organisaties geen analyses mogelijk omdat deze de lijst niet volledig konden invullen. De reden hiervoor was dat de persoon in kwestie niet de beschikking had over de volledige informatie om alle normen te beoordelen. Om de lijst in zijn geheel toe te passen is het nodig om met meer personen te spreken. Wat wel bleek uit deze twee interviews is dat, officieus, één van de twee organisaties hoog zou scoren en de ander betrekkelijk laag.

Aangezien de normen uit de IT Governance checklist vanuit de literatuur zijn opgezet hebben ze een formeel en generiek karakter. Uit de interviews blijkt dat niet te allen tijde de structuur en begrippen van de checklist aansluiten bij de organisatie. Het is dus in enkele gevallen nodig om de lijst klantspecifiek te maken. Dit werd door één van de geïnterviewde genoemd als het *tunen* van de IT Governance checklist.

Afhankelijk van de organisatietypologie kan het voorkomen dat de IT Governance checklist meerdere keren bij één organisatie ingevuld dient te worden, bijvoorbeeld bij divisies of *business*

units. Daarnaast komt het voor dat de IT Governance checklist (met al zijn IT aspecten) niet door één functionaris volledig ingevuld kan worden.

Uit bovenstaande conclusies blijkt dat het belangrijk is om voor aanvang van de beoordeling eerst een *assessment* te maken van het type organisatie en de rollen, verantwoordelijkheden en begrippen. Deze moeten dan vergeleken worden met het model en de checklist om te zorgen voor een optimale aansluiting met de organisatie.

8.4 Aanbevelingen

Deze paragraaf beschrijft een aantal aanbevelingen die voor dit onderzoek van belang zijn. Deze zijn in te delen in twee categorieën. De eerste categorie betreft aanbevelingen over de toepassing van de werkwijze in praktijksituaties. De tweede categorie betreft aanbevelingen voor verder onderzoek.

8.4.1 Aanbevelingen over toepassing werkwijze:

De eerste aanbeveling heeft betrekking op toepassing van de werkwijze. Uit het praktijkonderzoek blijkt dat er behoefte is naar de ontstaansgeschiedenis van het model en de IT Governance checklist. Daarnaast is de structuur van het model niet altijd één-op-één toepasbaar op de organisatie. Eerder is al vermeld dat het model klantspecifiek gemaakt moet worden om rollen, verantwoordelijkheden en begrippen aan te laten sluiten op de organisatie. De aanbeveling is dan ook om bij de beoordeling van de kwaliteit van IT Governance een inleidende sessie te houden met verantwoordelijken in de organisatie om het model klantspecifiek toepasbaar te maken. Dit verduidelijkt de communicatie met de klant en voegt waarde toe aan het model en de IT Governance checklist. Een aantekening die hierbij gemaakt moet worden, en die ook bij één van de interviews naar voren kwam, is dat het niet aan te raden is om *zomaar* normen om te schrijven en wellicht daarmee de context te veranderen. Hiermee wordt namelijk de correctheid vanuit de theorie aangetast. Zorgvuldig omgaan met wijzigingen aan de normen wordt aanbevolen.

Een tweede aanbeveling is om te kiezen voor een (eenvoudige) tooling om bij organisaties de +/- 200 normen te verwerken en te analyseren. In de scriptie is al een toepassing van deze tooling gedemonstreerd bij de analyse van de resultaten van het Kadaster. Eenvoudige Access en/of Excel toepassingen kunnen afdoende zijn om personen optimaal te ondersteunen in hun beoordeling van de kwaliteit van IT Governance.

8.4.2 Aanbevelingen voor verder onderzoek:

Voor dit onderzoek zijn drie algemene IT beheer aspecten en drie specifieke IT aspecten gekozen om op te nemen in een IT Governance werkmodel. Andere aspecten kunnen een positieve bijdrage leveren aan de beoordeling van de kwaliteit van IT Governance. Aanvullend onderzoek is nodig naar de mogelijkheden van andere IT aspecten op het huidige model. Hierbij wordt geadviseerd om financieel management als eerste te bestuderen. Dit aspect kwam bij enkele interviews naar voren als gewenste aanvulling op het huidige model.

Uit verschillende interviews blijkt dat de organisatietypologie invloed heeft op de uitvoering van de IT Governance checklist. Met name voor organisaties die met divisies werken is het

interessant hoe de structuur van het model past op hun organisatie. Verder onderzoek is nodig naar het nut van de toepassing van organisatietypologieën op het ontworpen IT Governance model, zoals organisaties met divisies of machinebureaucratie. Daarnaast moet bestudeerd worden wat voor gevolgen dit heeft voor de IT Governance checklist. Met name praktijkonderzoek, voorafgaande aan een korte literatuurstudie, is hiervoor geschikt.

In het IT Governance model en in de checklist zijn heel expliciet de perspectieven van de IT BSC gebruikt. Tijdens de interviews kwam naar voren dat (IT) organisaties ook gebruik maken van de traditionele BSC aanpak. Praktijkonderzoek is nodig naar de mogelijkheden/voordelen van de koppeling tussen de IT BSC en de traditionele bedrijfs-BSC van (IT) organisaties. Hierbij is het tevens interessant om *measurements* mee te nemen in de algehele beschouwing. Hiermee kunnen organisaties concrete waardes toewijzen en benchmarken om de kwaliteit van IT Governance te meten.

REFLECTIE

Dit hoofdstuk staat in het teken van een eigen beschouwing over het verloop van dit onderzoek. De opdracht zoals die beschreven staat in de onderzoeksopzet is tot stand gekomen in overleg met de opdrachtgever, Ernst & Young EDP Audit. De probleemstelling is ontstaan vanuit een praktische behoefte binnen de organisatie. Bij aanvang van het onderzoek was de auteur relatief onbekend met de concepten IT Governance en sommige methodes zoals CoBiT. Het algehele onderwerp (IT Governance) en de insteek van de opdracht (beoordeling kwaliteit) is gedurende de gehele opdracht als uitermate boeiend ervaren.

Daar waar sommige studenten afstuderen op één methode zoals CoBiT, BiSL of ITIL dan wel een IT onderwerp als applicatiebeheer of *outsourcing* worden in dit onderzoek meerdere methodes en IT aspecten toegepast en gecombineerd. Dit heeft de complexiteit van de opdracht vergroot. Dit risico is vanaf het begin bekend geweest maar wellicht toch onderschat. Wat wel als pluspunt wordt beschouwd is het verkregen brede inzicht in een groot assortiment van methodes en IT aspecten, evenals de toepassing hiervan.

Bij aanvang van de opdracht is gekozen om de doorlooptijd met één maand te verkorten om te voorkomen dat belangrijke onderdelen (zoals interviews) midden in de zomervakantie (eind juli, augustus) uitgevoerd moesten worden. Dit resulteerde in strakke tussentijdse deadlines welke niet altijd gehaald zijn. Het is in de ogen van de auteur met name in het begin tegen gevallen om het juiste ritme te vinden wat een langzame start tot gevolg heeft gehad. Deze *achterstand* is later niet meer goed gemaakt waardoor de doelstelling van het afronden van de scriptie in 6 maanden niet is gehaald. Met behulp van de zeer correcte inzet van de begeleiders heeft het schrijven van de scriptie *slechts* enkele weken vertraging opgelopen.

Wat als zeer prettig werd beschouwd is dat regelmatig afspraken zijn geweest met de begeleiders. Zowel de docenten van de Universiteit Twente als de begeleiders bij Ernst & Young EDP Audit zijn druk bezette personen, echter hebben ze te allen tijde ruimte gemaakt om de opdracht en de auteur te ondersteunen. De vaktechnische inzicht en goede academische begeleiding tezamen met een kritische kijk en praktische ervaring van de heren begeleiders hebben een positieve bijdrage geleverd aan de totstandkoming van deze scriptie.

ADRESGEGEVENS

Afstudeerder:
Wilco Leenslag
Fazantweg 14
7161 HR Neede
S-nummer: 0076414
Tel: 06 28 25 93 64
Email: w.leenslag@student.utwente.nl

Begeleiding Ernst & Young EDP Audit:
1ste begeleider
drs. I.N. (Ivo) Kouters
Senior Manager
Ernst & Young EDP Audit
Boogschutterstraat 1 a
7324 AE Apeldoorn
Postbus 652
7300 AR Apeldoorn
Tel: 055 529 13 21 / 06 21 25 15 65
Email: ivo.kouters@nl.ey.com

2de begeleider
O.E. (Otto) Teule
Senior Manager EDP-Audit
Ernst & Young EDP Audit
Boogschutterstraat 1 a
7324 AE Apeldoorn
Postbus 652
7300 AR Apeldoorn
Tel: 055 529 13 14 / 06 21 25 25 34
Email: otto.teule@nl.ey.com

Begeleiding Universiteit Twente:
1ste begeleider
Dr. Mr. Ir. Th.J.G. Thiadens
Kaaplaan 4
3941 RL Doorn
Tel: 0343 420 860 / 06 44 90 28 85
Email: thiadens@ict-management.com

2de begeleider
Dr. P.A.T. van Eck
Zilverling 3051
Drienerlolaan 5
7522 NB Enschede
Postbus 217
7500 AE Enschede
Tel: 053 489 46 48 / 06 51 22 97 11
Email: vaneck@cs.utwente.nl

REFERENTIES

[1] Applegate, L.M., Austin R.D., McFarlan F.W.; Corporate information strategy and management; McGrawhill Higher Education; ISBN: 0-07-245665-5; 2003

[2] Barlage R., Steenvoorden L.; Bruikbaarheid van CoBiT in een IT-audit; de EDP-auditor; nummer 2; 2000

[3] Blok E. E.; Organiseren van functioneel beheer; Afstudeeropdracht Open Universiteit Nederland Management Informatie en Technologie (MIT); 2005

[4] Brand K, Boonen H; IT governance □ase don CobiT; Van Haren Publishing; Zaltbommel; 2004; ISBN: 90 77212 19 1; page 16-18

[5] Broadbent M.; A Clear and present Objective; CIO; St Leonards, Mei 2003;

[6] Broadbent, M.; The Right Combination; CIO; St Leonards, April 2003; p. 13

[7] Cameron A.; ITIL and beyond; PinkRoccade; 2002

[8] Central Computers & Telecommunications Agency; Managing Successful projects with PRINCE2 ;1999

[9] Dallas, S.; Six IT Governance rules to boost IT and user credibility; Oct 31, 2002; Gartner; url (20-02-2006): http://facweb.cs.depaul.edu/nsutcliffe/483readings/3-6-ITGoveranceRulesToBoostITnUserCredibility.htm

[10] Deurloo K., Van der Pols R., Sieders R.; ASL Zelfevaluatie; Stichting ASL Foundation; Ten Hagen & Stam Uitgevers

[11] Driessen A.J.G., Kamstra R, Molenkamp A.; In control statements. Tijdschrift Controlling. Pp 55 (2001)

[12] Driessen A.J.G., Van der Kerk J.W., Molenkamp A.; Operational auditing, een managementkundige benadering; Kluwer, 1997

[13] Dubie D.; Better management through best practices; Network World; 2006

[14] Eye on ICT digitale nieuwsbrief, jaargang 2, nummer 1 februari 2005, http://www.ey.nl/download/publicatie/Nieuwsbrief__Eye_on_ICT_feb2005.pdf

[15] Gianotten J.; Governance van IT en outsourcing; Kennisplatform Topmanagement & IT; 2004; ISBN 90-74712-37-1

[16] Global Information Security Survey 2005; Ernst & Young; url (31-01-2006): http://www.ey.nl/download/overig/EDP/GISS_2005_Dutch_management_summary.pdf

[17] Grewal P., Knutsson F.; IT Governance in a global logistics company; Master Thesis in Informatics; Göteborg University, Department of Informatics; Sweden 2005

[18] Guldentops E., Van Grembergen cW., De Haes S.; Control and Governance *Maturity* Survey: Establishing a Reference Benchmark and a Self-assessment Tool; Information Systems Control Journal, Volume 6, 2002

[19] Halfhide O., Hendriks L., Mast G., Mosterman A., Teeuwen J.; Procurement, projecten en processen in de praktijk; IT Beheer Jaarboek; 2003

[20] Halfhide O., Hendriks L., Mast G., Mosterman A., Teeuwen J.; Procurement, projecten en processen in de praktijk; de samenhang tussen iSPL, PRINCE2 en ITIL; IT Beheer Jaarboek 2003

[21] Heschl J.; CoBiT in Relation to Other International Standards; Information Systems Control Journal; Volume 4; 2004

[22] http://www.ey.nl/download/publicatie/Uw_ICT_onder_controle.pdf

[23] ISO; Information technology - Code of practice for information security management, ISO/IEC 17799:2000; ISBN 0 580 36958 7; 2001

[24] ITGI ; CobiT4.0 beschikbaar op: www.itgi.org

[25] ITGI, Aligning CoBiT, ITIL and ISO 17799 for business benefit

[26] ITGI, CoBiT Mapping – Mapping of ISO/IEC 17799:2000 With CoBiT, www.isaca.org/cobit

[27] ITGI; Board briefing on IT Governance; 2003

[28] ITGI; COBIT Mapping: Overview of International IT Guidance, 2nd Edition; 2006; ISBN 1-933284-31-5

[29] ITGI; CoBiT Mapping; overview of international IT Guidance; 2004

[30] ITGI; Information Security Governance 2nd edition; 2006

[31] ITGI; IT Governance Global Status Report – 2006; ISBN: 1-933284-32-3

[32] ITSMF; Checklist ITIL; www.itsmf.com/news/news.asp?NewsID=71; 2006

[33] Jaarverslag 2004/2005, Ernst & Young

[34] Jordan, E., Musson, D; Corporate Governance and IT Governance: Exploring the Board's Perspective; (December 2, 2004). Available at SSRN: http://ssrn.com/abstract=787346

[35] Keijl S.; SAS70 en SysTrust; Internationale standaarden voor third party assurance bij IT-serviceorganisaties; de EDP-Auditor; nummer 3; 2002

[36] Keyes-Pearce S.V.; Rethinking the importance of IT Governance in the e-world; 6th pacific asia conference on information systems; 2002

[37] Kordel L.; IT Governance Hands-on: Using CoBiT to implement IT Governance; Information Systems Control Journal; Volume 2; 2004

[38] Larsen M.H., Pedersen M.K.; Andersen K.V.; IT Governance: Reviewing 17 IT Governance Tools and Analysing the case off Novozymes A/s; Proceedings of the 39th Hawaii International Conference on System Sciences; 2006

[39] Liu, Q. and Ridley, G.; IT Control in the Australian Public Sector: An international comparison; 13th European Conference of Information Systems; Germany; May, 2005.

[40] McLane G.; IT Governance and its Impact on IT Management: a literature review; University of technology sydney ; 2003; url (16-02-2006): http://itmp.uts.edu.au/about/Project_A_Glen_McLane.pdf

[41] Meijer M.; ASL grote stap naar INK-niveau III; Informatie; 2003

[42] Meijer M.; Effectief IT-beheer: samenwerken waar nodig, zelfstandig opereren waar mogelijk;

IT Beheer jaarboek; 2002

[43] Meijer M.; Relatie tussen ASL en het INK-managementmodel; 2002; www.aslfoundation.org

[44] Norea; IT Governance, een verkenning; 2004; te downloaden van www.norea.nl

[45] Oud E. J.; The value to IT of using international standards; Information Systems Control Journal, Volume 5, 2005

[46] Parkes H.; IT Governance and outsourcing; Information Systems Control Journal; Volume 5; 2004

[47] Patel, N.V.; An emerging stategy for e-business IT Governance; in W. Van Grembergen; Strategies for Information Technology Governance; Hershey; Pa; Idea Group Publishing; 2003

[48] Pederiva A.; The COBIT *Maturity* Model in a Vendor Evaluation Case; Information Systems Control Journal, Volume 3, 2003

[49] Peterson, R. R.; Information strategies and tactics for Information Technology governance; 2003; In W. Van Grembergen (Ed.), Strategies for Information Technology Governance. Hershey, PA: Idea Group Publishing.

[50] Ribbers, P.M.A. Peterson, R.R. Parker, M.M.; Designing information technology governance processes: diagnosing contemporary practices and competing theories; Proceedings of the 35th Annual Hawaii International Conference on System Sciences; 2002

[51] Ridley G.; Young J; Carroll P.; COBIT and Its Utilization: A Framework from the Literature; Proceedings of the 37th Annual Hawaii International Conference on System Sciences; 2004

[52] Sallé M.; IT Service Management and IT Governance: Review, Comparative Analysis and their Impact on Utility Computing; Trusted Systems Laboratory; 2004

[53] Sjong R. L.; Frameworks Boost Business Efficiency; www.cica.an/archief_newsletters/Frameworks.doc; 2005

[54] Sohal A.; Fitzpatrick P.; IT governance and management in large Australian organisations; International Journal of Production Economics; Volume 75, Issues 1-2, 10 January 2002, Pages 97-112

[55] Solms von B.; Information security governance: CoBiT or ISO 17799 or both?; Computers & Security; Elsevier; Volume 24, 2005

[56] Solms von B.; Information security governance: CoBiT or ISO 17799 or both?; Computers & Security; Elsevier; Volume 24, 2005

[57] Spafford G.; Control Framework Misconceptions; IT management; 2004; url (30-01-2006): http://itmanagement.earthweb.com/netsys/article.php/3439901

[58] Spafford G.; The benefits of standard IT Governance; IT Management: Network & Systems Management; 2003; url (27-01-2006): itmanagement.earthweb.com/netsys/article.php/2195051

[59] Starre D., B. de Jong, IT governance and management, Nolan Nortan Institute, The Netherlands, 1998.

[60] Starreveld, R.W., van Leeuwen, O.C. van Nimwegen, H.; Bestuurlijke informatieverzorging Deel 1: Algemene grondslagen; vijfde editie Stenfert Kroese Groningen/Houten, 2002

[61] Thiadens, T, Manage IT, Springer Dordrecht, 2005, ISBN: 1-4020-3639-6

[62] Thiadens, T, Sturing en organisatie van ICT-voorzieningen, Van Haren, 2004, ISBN; 90 77212 25 6

[63] United States General Accounting Office; Measuring performance and demonstraating results of information technology investments; 1998

[64] Van der Pijl G.J., Nuijten A.L.P.; Het gebruik van beheersmodellen; MAB; november; 2001

[65] Van der Pols R., Donatz R., Van outvorst F.; BiSL: een framework voor functioneel beheer en informatiemanagement; Van Haren; 2005; ISBN: 90 77212 40 X

[66] Van der Pols R.; ASL: een framework voor applicatiebeheer; Ten Hagen Stam 2001; ISBN: 90 440 0266 X

[67] Van Grembergen W., De Haes S.; Een raamwerk voor de besturing van IT; Informatie; 2004

[68] Van Grembergen W., de Haes Steven, Moons J.; Linking business goals to IT goals and COBIT processes; Information systems control journal; 2005; p. 18-22

[69] Van Grembergen, W., De Haes, S., Guldentops, E.: Structures, Processes and Relational Mechanisms for IT Governance, in Grembergen (Ed), Strategies for Information Technology Governance, Idea Group Publishing, 2004

[70] Van Grembergen; The balanced scorecard and IT Governance; Information Systems Journal; Volume 2; 2000

[71] Van Outvorst F., Donatz R., Van der Pols R.; Introductie BiSL: Een framework voor functioneel beheer en informatiemanagement; IT Service Management; 2005

[72] Verhoef D., Kemmerling G., Van der Meulen E., Schutte H.; IT Services Procurement, een introductie op basis van ISPL; Van Haren publishing; ISBN: 90-77212-34-5; 2004

[73] Violino B.; Frameworks boost business efficiency; Compliancepipeline.com ; 2005

[74] Webb P., Pollard C., Ridley G.; Attempting to define IT Governance: Wisdom or Folly?; Proceedings of the 39th Hawaii International Conference on System Sciences; 2006

[75] Weill and R. Woodham, Don't Just Lead, Govern: Implementing Effective IT Governance, MIT CISR WP No. 326, MIT Sloan School of Management (April 2002).

[76] Weill P., Ross J. W.: IT governance : how top performers manage IT decision rights for superior results; Boston: Harvard Business School Press; 2004; ISBN 1-59139-253-5

[77] Weill P., Ross J.W.; IT Governance on one page; MIT CISR WP No. 349, MIT Sloan School of Management (November 2004).

[78] Weill, Don't Just Lead, Govern: How top-performing firms Govern IT, MIT CISR WP No. 341, MIT Sloan School of Management (March 2004).

[79] CIOportal; Redactie Financieel-management.nl; 2006; http://www.cioportal.nl/index.php?p=artikel&id=1494

BIJLAGE

I. Overzicht redenen IT Governance

Good IT Governance pays off:

A study Weill et al. did showed that firms that were successful in their IT Governance had more than 20% higher Return On Assets (ROA) than similar firms with the same strategy but with ineffective IT Governance. IT Governance was not the only factor that affected the result but good government often comes with good management [17].

IT is expensive:

The average enterprise's IT investment is now greater than 4.2 percent of annual revenues and still rising. As IT has become more important and pervasive, senior management teams are increasingly challenged to manage and control IT to ensure that value is created. To address this issue, many enterprises are creating or refining IT Governance structures to better focus IT spending on strategic priorities [76].

IT is pervasive:

In many enterprises, centrally managed IT is no longer possible or desirable. There was a time when requests for IT spending came only from the IT group. Now IT spending originates all over the enterprise. Well-designed IT Governance arrangements distribute IT decision making to those responsible for outcomes [76].

New information technologies bombard enterprises with new business opportunities:

Development of new information technologies is being made rapidly today and this creates new business opportunities and threats. If companies should be able to respond fast enough to changes they need a flexible infrastructure. This infrastructure has to be cost effective, meet the business needs today, and be flexible in order to be able to support future business needs [17].

IT Governance is critical to organizational learning about IT value:

It is often difficult to evaluate value received from IT investments and especially to evaluate them in advance. IT Governance plays an important role when it comes to organisational learning about value received from an IT investment. With an effective IT Governance, mechanisms can be created and through them potential value can be debated within the organization [17].

IT value depends on more than good technology:

Many IT projects have failed during recent years. One reason that many IT projects fail is that organisations fail to adopt new processes that support the implementation of new technologies. It is important to have the right people involved when making IT decisions and senior mangers should not just abdicate to IT executives [17].

Senior management has limited bandwidth:

Senior management does not have the bandwidth to consider all the requests for IT investments that occur in a large enterprise left alone to get involved in the many other IT-related decisions [78]. Senior management should not get involved in to many IT decisions but decisions taken should be in line with the direction that the senior management is trying to take the organization [17].
Carefully designed IT Governance provides a clear, transparent IT decision-making process that leads to consistent behavior linked back to the senior management vision while empowering everyone's creativity [78].

Leading enterprises govern IT differently:

IT Governance is performed differently in different leading enterprises. It is common that different leading enterprises' IT Governance makes the tension, between IT decisions such as standardisation versus innovation, transparent [17].

II. IT Governance componenten Weill et al.

In onderstaande tabellen staan de drie componenten beschreven volgens het onderzoek van Weill et al. In Tabel 10: IT decisions Domains worden de domeinen beschreven die antwoord moeten geven op de *what* vraag van IT Governance.

Domains	Description
IT principles	High level statements about how IT is used in the business
IT architecture	An integrated set of technical choices to guide the organization in satisfying business needs. The architecture is a set of policies and rules for the use of IT and plots a migration path to the way business will be done (includes data, technology, and applications)
IT infrastructure strategies	Strategies for the base foundation of budgeted-for IT capability (both technical and human), shared throughout the firm as reliable services, and centrally coordinated (e.g., network, help desk, shared data)
Business application needs	Specifying the business need for purchased or internally developed IT applications
IT investment and prioritisation	Decisions about how much and where to invest in IT including project approvals and justification techniques

Tabel 10: IT decisions Domains

In Tabel 11: IT Governance Archetypes worden de verschillende type groepen beschreven die een beslissing over IT Governance nemen, die toepasbaar zijn op de *decisions domains*.

Type	Description
Business monarchy	A group of, or individual, business executives (i.e., CxOs). Includes committees comprised of senior business executives (may include CIO). Excludes IT executives acting independently.
IT monarchy	Individuals or groups of IT executives
Feudal	Business unit leaders, key process owners or their delegates
Federal	C level executives and at least one other business group (e.g., CxO and BU leaders) –IT executives may be an additional participant. Equivalent to a country and its states working together.
IT Duopoly	IT executives and one other group (e.g., CxO or BU leaders)
Anarchy	Each individual user

Tabel 11: IT Governance Archetypes

Type	Description
Decision-making structures	Organizational units and roles responsible for making IT decisions, such as committees, executive teams, and business/IT relationship managers.
Alignment processes	Formal processes for ensuring that daily behaviors are consistent with IT policies and provide input back to decisions. These include IT investment proposal and evaluation processes, architecture exception processes, service-level agreements, chargeback and metrics.
Communication approaches	Announcements, advocates, channels, and education efforts that disseminate IT Governance principles and policies and outcomes of IT decisionmaking processes.

Tabel 12: IT Governance mechanismen type

De *how* wordt door Weill et al. gestructureerd door *IT-Governance mechanisms*. Zij beschrijven deze mechanismen als:

> **The vehicles used to implement a particular governance archetype including: organizational structures, procedures, committees and policies.**
>
> **Weill et al. (2004)**

Deze kunnen specifiek voor één domein zijn of van meerdere domeinen. Er zijn drie soorten IT Governance mechanismen. In Tabel 13: Governance mechanisms worden de verschillende mechanismen beschreven die volgens Weill et al. een hoge impact hebben en uitdagend zijn om te implementeren [76].

Mechanisms	Objectives
Executive and senior management committee	Holistic view of business, including IT
Architecture committee	Identify strategic technologies and standards
Process teams with IT membership	Take process view using IT (and other assets) effectively
Capital investment approval and budgets	Consider IT as another business investment
Service-level agreements	Specify and measure IT service
Chargeback	Recoup IT costs from business
Formal tracking of business value of IT	Measure IT investments and contribution to business value often using balanced scorecard

Tabel 13: Governance mechanisms

III. Stappenplan IT Governance Weill et al.

Step 1:

Map the "as is" IT governance onto a diagram like Figuur 27: Uitwerking huidige situatie. What governance mechanisms are used? Are the mechanisms working together to encourage desirable behaviors in the firm?

Domain / Archetype	IT Principles		IT Infrastructure Strategies		IT Architecture		IT Investment	
	Input	Decision	Input	Decision	Input	Decision	Input	Decision
Business Monarchy		• ITEC						• ITEC • CIO
IT Monarchy				• CIO • IT Leadership	•IT Leadership •Arch Office	• CIO • IT Leadership		
Feudal								
Federal	• ITEC • CIO • IT Leadership • IT Org		• IT Leadership • ITEC Arch Office				• CIO • Budgets • SLA • Activity Tracking • IT Leadership	
Anarchy								

Typical Firm

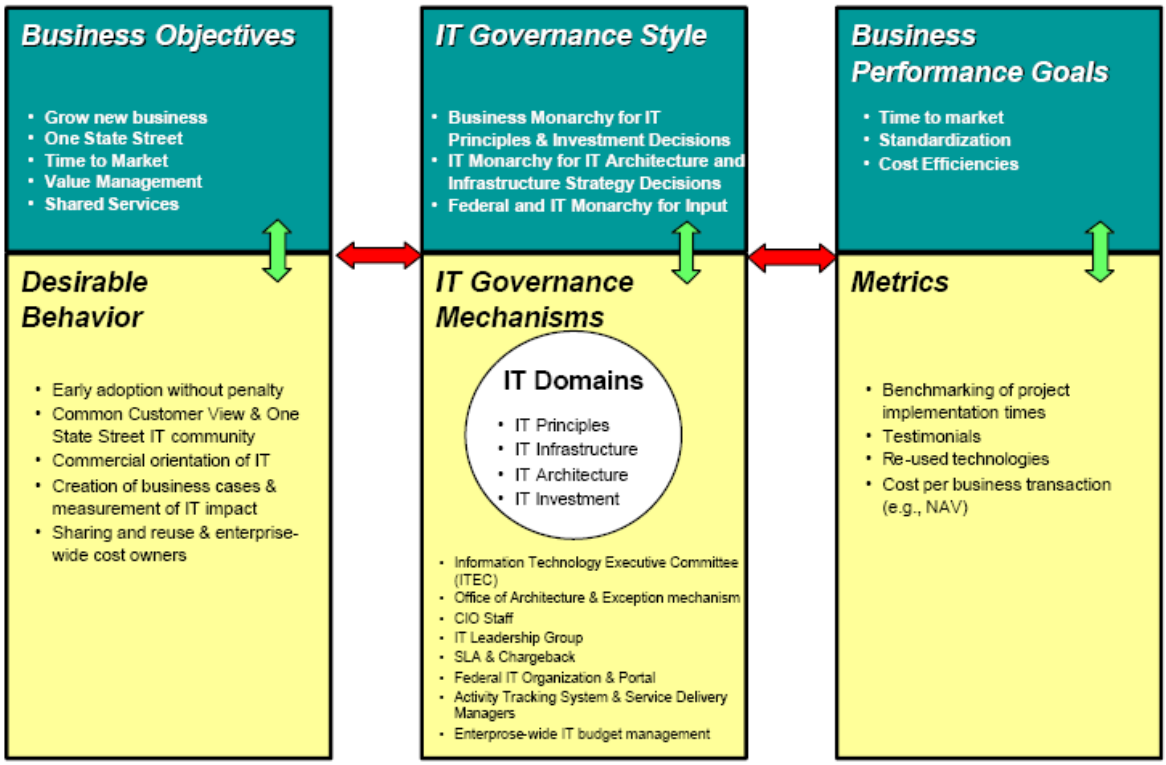
ITEC	Information Technology Executive Committee
Arch Office	Office of Architecture
CIO	CIO Staff
IT Leadership	IT Leadership Group

SLA	Service Delivery Agreements and Chargeback
IT ORG	Federated IT Organization
Activity Tracking	Activity Tracking System
Budgets	Enterprise-Wide IT Budget Management

Figuur 27: Uitwerking huidige situatie

Step 2:

Identify the business objectives for the firm and the associated desirable behaviors by completing the left hand box of a diagram like the one in Figuur 28: Uitwerking IT Governance framework.



Figuur 28: Uitwerking IT Governance framework

Step 3:

Consider the way the typical firm governs IT and how the top performers on each financial metric are different. Consider the mechanisms typically used and their characteristics.

Step 4:

Redesign the firm's IT governance by completing the middle box of Figuur 28: Uitwerking IT Governance framework for the firm. Create a "to be" version of Figuur 27: Uitwerking huidige situatie for the firm identifying which mechanisms will be used for each IT domain.

Step 5:

Identify the performance goals, metrics and accountabilities required for the new governance models by completing the right-hand box onFiguur 28: Uitwerking IT Governance framework.

Step 6:

Plan the move from the “as is” to the “to be” governance mechanism recognizing the major organizational and cultural changes involved.

Domains	Description
Strategic alignment	focus on aligning with the business and collaborative solutions
Value delivery	concentrating on optimising expenses and proving the value of IT
Risk management	addressing the safeguarding of IT assets, disaster recovery and continuity of operations
Resource management	optimising knowledge and IT infrastructure Furthermore, none of these factors can be managed appropriately without
Performance measurement	tracking project delivery and monitoring IT services

Tabel 14: IT Governance domains

Gebruikmakend van de *Board briefing on IT Governance* en van een artikel van Kordel (2004) worden de volgende stakeholders onderscheiden die de *who* aangeven [27] [37]:

- Board members
- CIO
- Business executives
- Auditors
- Risk and compliance officers

Voor de *how* worden een aantal elementen genoemd. Vergelijkbaar als bij de research based framework van Weill et al. wordt in de *Board briefing on IT Governance* door de ITGI een overzicht gegeven van de rollen en verantwoordelijkheden in de vorm van comités. De volgende groepen zijn te onderscheiden:

- IT Strategy committee
- IT steering committee
- Technology council
- IT architecture review board

De *Board briefing on IT Governance* beschrijft ook een *toolkit* als hulpmiddel ter ondersteuning van IT Governance. Deze bestaat uit de volgende elementen:

Elements	Description
Activities	comprise actions that should be carried out to exercise the IT governance responsibilities and the subjects comprise those items that typically get onto an IT governance agenda objectives, opportunities, risks, key processes and core competencies).
Outcome measures	relate directly to the subjects of IT governance, such as the

	alignment of business and IT objectives, cost-efficiencies realised by IT, capabilities and competencies generated and risks and opportunities addressed.
Best practices	comprise examples of how the activities are being performed by those who have established leadership in governance of technology. These practices have been classified to reflect the IT governance area(s) to which they provide the greatest contribution: value delivery, strategic alignment, resource management, risk management and/or performance.
Critical success factors	are conditions, competencies and attitudes that are critical to being successful in the best practices.
Performance drivers	drivers provide indicators on how IT governance is achieving, as opposed to the outcome measures that measure what is being achieved. They often relate to the critical success factors.

Tabel 15: IT Governance elements

V. Stappenplan IT Governance ITGI

Step 1: Set up a Governance organizational framework

Set up a governance organisational framework that will take IT Governance forward and own it as an initiative, with clear responsibilities and objectives and participation from all interested parties.

Step 2: Align IT strategy with business goals

What are the current business concerns and issues where IT has a significant influence, e.g., cost reduction, competitive advantage and/or merger/acquisition? Obtain a good understanding of the business environment, risk appetite and business strategy as they relate to IT. Identify the top IT issues on management's agenda.

Step 3: Understand/define the risks

Given top management's business concerns, what are the risk indicators relating to IT's ability to deliver against these concerns? Consider:

- ***Previous history and patterns of performance***
- ***Current IT organisational factors***
- ***Complexity and size/scope of the existing or planned IT environment***
- ***Inherent vulnerability of the current and planned IT environment***
- ***Nature of the IT initiatives being considered, e.g., new systems projects, outsourcing considerations, architectural changes***

Step 4: Define target areas

Identify the process areas in IT that are critical to managing these risk areas. Use the CoBiT process framework as a guide.

Step 5: Analyse current capability and identify gaps

Perform a *maturity* capability assessment to find out where improvements are needed most. Use CoBiT's management guidelines as a guide.

Step 6: Develop improvement strategies

Decide which are the highest priority projects that will help improve the management and governance of these significant areas. This decision should be based on most potential benefit and ease of implementation, and a focus on important IT processes and core competencies. Define specific IT governance projects as the first step in the IT governance continuous improvement initiative.

Step 7: Measure results

Establish a balanced scorecard mechanism for measuring current performance. Monitor the results of new improvements considering, as a minimum, the following key considerations:

- ***Will the organisational structures support strategy implementation?***
- ***Are responsibilities for risk management embedded in the organisation?***
- ***Do infrastructures exist that will facilitate and support the creation and sharing of vital business information?***
- ***Have strategies and goals been communicated effectively to everyone who needs to know within the organisation?***

Step 8: Repeat steps 2-7 on a regular basis.

VI. CoBiT Maturity Model

DS2 - Manage Third-party Services	not at all	a little	quite a lot	completely		
0 Non-existent when						
Responsibilities and accountabilities about relationships are not defined.	x				0	
There are no formal policies and procedures regarding contracting with third parties.	x				0	
Third-party services are neither approved nor reviewed by management.	x				0	
There are no measurement activities and no reporting by third parties.	x				0	
In the absence of a contractual obligation for reporting, senior management is not aware of the quality of the service delivered.	x				0	
						0
1 Initial/Ad Hoc when						
Management is aware of the need to have documented policies and procedures for third-party management, including having signed contracts.	x				0	
There are no standard terms of agreement with service providers.	x				0	
Measurement of the services provided is informal and reactive.		x			0,33	
Practices are dependent on the experience of the individual and the supplier (e.g., on demand).	x				0	
						0,33
2 Repeatable but Intuitive when						
The process for overseeing third-party service providers, associated risks and the delivery of services is informal.		x			0,33	
A signed, *pro forma* contract is used with standard vendor terms and conditions (e.g., the description of services to be provided).	x				0	
Reports on the services provided are available, but do not support business objectives.	x				0	
						0,33
3 Defined Process when						
Well-documented procedures are in place to govern third-party services with clear processes for vetting and negotiating with vendors.			x		0,66	
When an agreement for the provision of services is made, the relationship with the third party is purely a contractual one.	x				0	
The nature of the services to be provided is detailed in the contract and includes legal, operational and control requirements.			x		0,66	
The responsibility for oversight of third-party services is assigned.				x	1	
Contractual terms are based on standardised templates.				x	1	
The business risk associated with the third-party services is assessed		x			0,33	

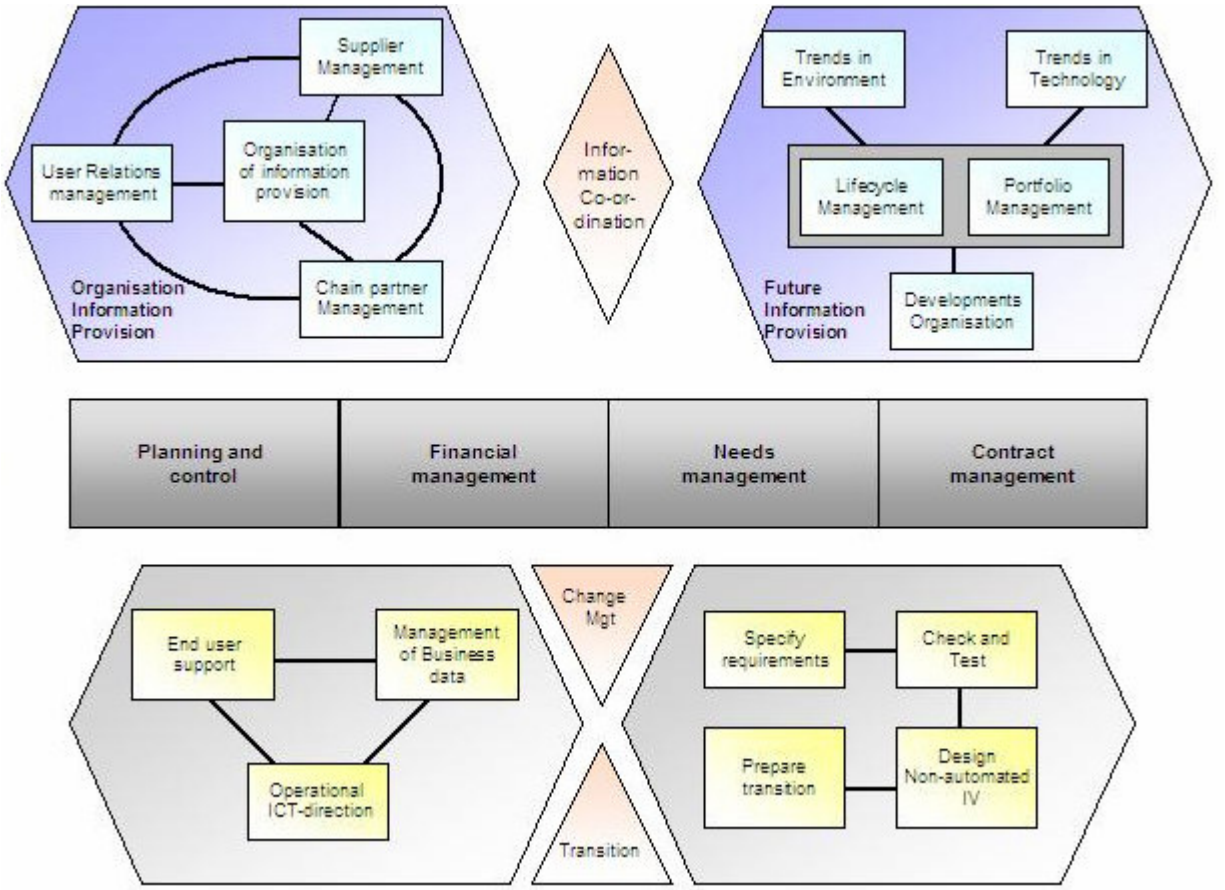
and reported.				
				3,65
4 Managed and Measurable when				
Formal and standardised criteria are established for defining the terms of engagement, including scope of work, services/deliverables to be provided, assumptions, schedule, costs, billing arrangements and responsibilities. Responsibilities for contract and vendor management are assigned.		x	0,66	
Vendor qualifications, risks and capabilities are verified on a continual basis.		x	0,33	
Service requirements are defined and linked to business objectives.	x		0	
A process exists to review service performance against contractual terms, providing input to assess current and future third-party services.	x		0	
Transfer pricing models are used in the procurement process.	x		0	
All parties involved are aware of service, cost and milestone expectations.		x	0,66	
KPIs and KGIs for the oversight of service providers have been agreed.	x		0	
				1,65
5 Optimised when				
Contracts signed with third parties are reviewed periodically at predefined intervals.		x	0,33	
The responsibility for managing suppliers and the quality of the services provided is assigned.	x		0	
Evidence of contract compliance to operational, legal and control provisions is monitored and corrective action is enforced. The third party is subject to independent periodic review, and feedback on performance is provided and used to improve service delivery.	x		0	
Measurements vary in response to changing business conditions.	x		0	
Measures support early detection of potential problems with third-party services.	x		0	
Comprehensive, defined reporting of service level achievement is linked to the third-party compensation.	x		0	
Management adjusts the process of third-party service acquisition and monitoring based on the outcome of KPIs and KGIs.	x		0	
				0,33

Tabel 16: CoBiT *Maturity* Model

Maturity level	Sommering (A)	Aantal stellingen (B)	(A/B)	Normalisatie [(A/B)/som(A)]	Bijdrage (Norm**maturity* level)
0	0	5	0,00	0,00	0,000
1	0,3	4	0,08	0,08	0,076
2	0,3	3	0,11	0,10	0,203
3	3,7	6	0,61	0,56	1,684
4	1,7	7	0,24	0,22	0,870
5	0,3	7	0,05	0,04	0,218
			1,08	1,00	**3,05**

Tabel 17: Uitwerking CoBiT *Maturity* Model

VII. Koppeling BiSL – CoBiT



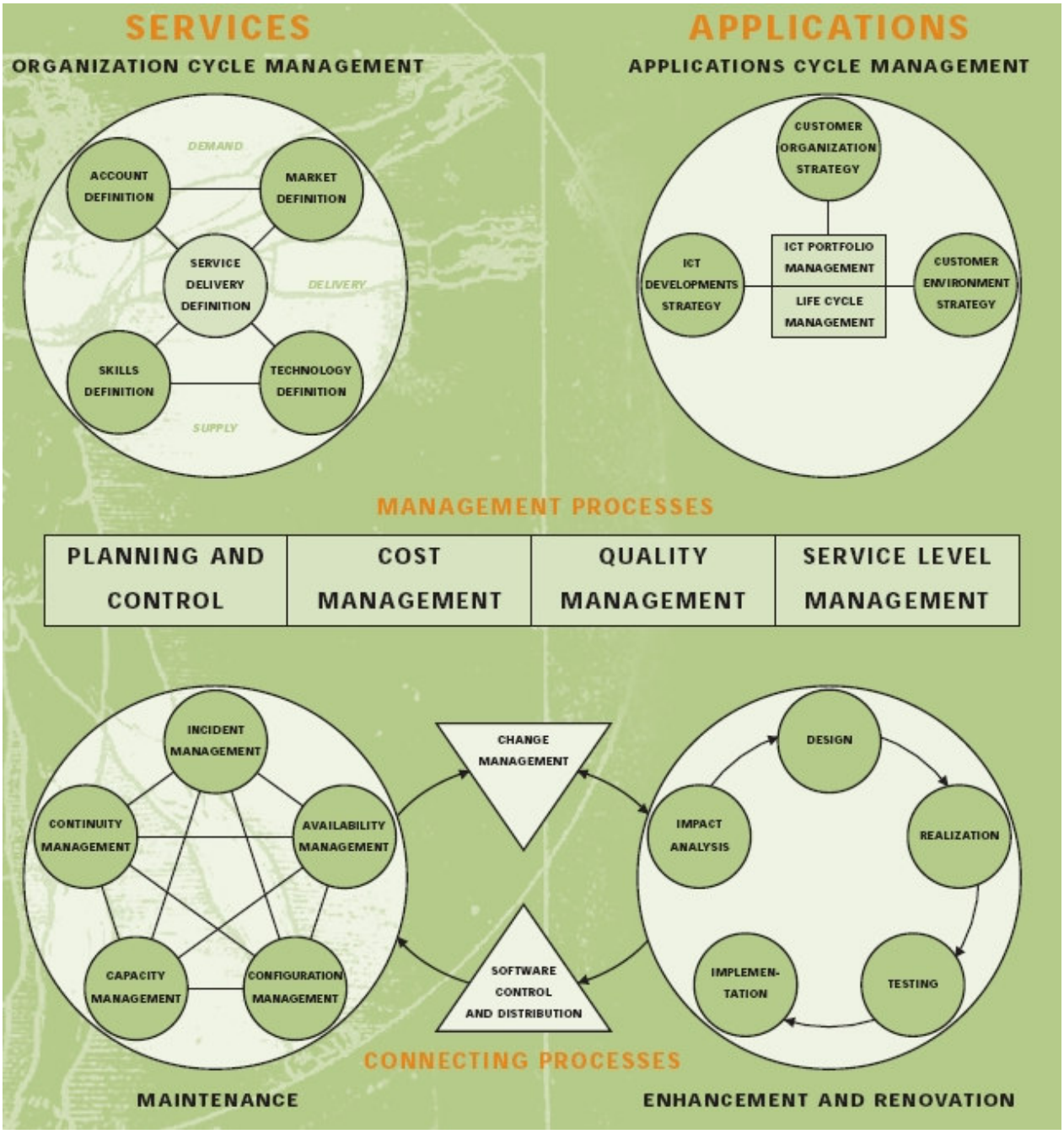
Figuur 29: BiSL Framework

BiSL proces	CoBiT proces
Opstellen informatie strategie	
Bepalen keten ontwikkeling	PO1
Bepalen bedrijfsproces ontwikkelingen	PO1
Bepalen technologie ontwikkelingen	PO3
Informatie lifecycle management	PO1
Informatie portfolio management	PO1/PO2
Opstellen IV-organisatie strategie	
Leveranciersmanagement	PO1//AI5/DS2
Ketenpartners management	PO4
Relatie management gebruikersorganisatie	PO4
Strategie inrichting IV-functie	PO4/PO6

Informatiecoördinatie	PO1/PO4
Planning en control	PO1/PO4/ME1
Financieel management	PO1/PO5/ME1
Behoefte management	PO1/PO4/PO6/ME1
Contract management	DS1/DS2
Gebruikersbeheer	
Gebruikersondersteuning	DS7/DS8
Beheer bedrijfsinformatie	PO2/DS11
Operationele ICT aansturing	DS1/DS3/DS4
Wijzigingenbeheer	AI6
Transitie	AI7
Functionaliteitenbeheer	
Specificeren	AI1
Vormgeven niet-geautomatiseerde informatievoorziening	AI4
Voorbereiden transitie	AI7
Toetsen en testen	AI7

Tabel 18: Koppeling BiSL - CoBiT

VIII. Koppeling ASL – CoBiT



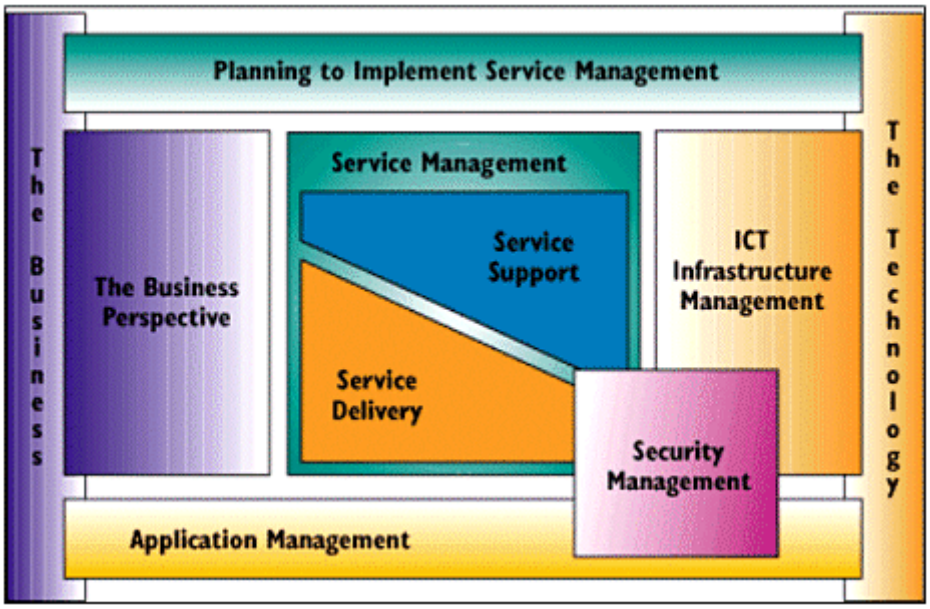
Figuur 30: ASL Framework

ASL proces	CoBiT proces
Applicatie-invalshoek	

Customer environment strategy	PO1
Customer organization strategy	PO1
ICT development strategy	PO3
Life-cycle management	PO1
ICT-portfolio management	PO1/PO6
Services-invalshoek	
Market definition	PO1
Account definition	PO4
Skills definition	PO7
Technology definition	PO3
Service definition	PO1
Planning en control	PO1//ME1
Kosten management	PO1/PO5/DS6/ME1
Kwaliteits management	PO4/PO8/ME1
Service Level Management	DS1/ME1
Beheer	
Incidentenbeheer	DS8
Configuratiebeheer	DS9
Beschikbaarheidsbeheer	DS3
Capaciteitsbeheer	DS3
Continuïteitsbeheer	DS4
Wijzigingenbeheer	AI6
Onderhoud en vernieuwing	
Impactanalyse	AI6
Ontwerp	AI2
Realisatie	AI2
Testen	AI7
Implementatie	AI7
Programmabeheer en distributie	AI7

Tabel 19:Koppeling ASL - CoBiT

IX. Koppeling ITIL – CoBiT



Figuur 31: ITIL Framework

ITIL proces	CoBiT proces
Business Perspective	
Understand business context	PO6
Develop business relationships and establish communications plan	PO6
Establish service portfolio	DS1
Analyse business requirements and ascertain future business direction	PO1
Develop IS strategy	PO1
Review business and IS strategic alignment	PO1
Develop service plans	AI1
Formalise supplier relationships	DS2
Manage service provision	AI5
Manage contracts	AI5
Establish service reporting policy	PO4
Manage performance and realise business benefits	M1
ICT infrastructure management (strategy)	
Maintain ICT business plans	PO1
Review current position and determine ICT strategies	PO3
Establish ICT standards and policies	PO3
Maintain ICT architectural blueprints	PO3

Design and implement technical migration plans	PO3
Review programme againts strategy and business plans	PO4
Undertake ICT research studies and evaluations	PO3
ICT infrastructure management (maintenance/innovation)	
Develop and ratify ICT solutions	AI all
Define appropriate working environments	AI7
Test ICT solutions	AI7
Build appropriate roll-out strategy	AI7
Roll-out ICT solutions	AI7
Undertake post-project evaluation and reviews	AI7
Build appropriate working environments	AI7
Service Level Management	DS1
Financial Management for IT Services	PO5/DS6
Capacity management	DS3
IT Service continuity Management	DS4
Availability Management	DS3/DS4
Service desk	DS8
Incident Management	DS8
Problem Management	DS10
Configuration Management	DS9
Change Management	AI6
Release Management	AI7

Tabel 20: Koppeling ITIL - CoBiT

Note that for the purposes of this mapping the primar y control objective(s) in COBIT has been identified although there may be other objectives in COBIT that can be related. In most cases one objective has been selected, but in some cases more have been chosen where they are considered helpful [25].

X. IT Governance Checklist

Gebruikte afkortingen:

Functioneel Beheer (FB), Applicatiebeheer (AB), Technisch Beheer (TB), Security (SEC), Inkoop (INK), Project Management (PM)

Score	Kwalificatie	Omschrijving
0	n.v.t.	De norm is niet van toepassing op de organisatie
1	Onvoldoende	De norm wordt niet gehaald, verbeteringen zijn relatief omvangrijk
2	Matig	De norm wordt niet gehaald, verbeteringen zijn relatief eenvoudig
3	Voldoende	De norm wordt gehaald

PO1 - Define a Strategic IT Plan & PO6 - Communicate Management Aims and Direction

Aspect		Business-IT alignment	Perspectief	Score
FB	1	Periodiek wordt geëvalueerd of het beleid t.a.v. Informatie Voorzieningen (IV) doeltreffend is waarbij de aanwezige Informatie Portfolio de organisatie in staat moet stellen te concurreren met andere organisaties	Corporate contribution	
FB	2	Periodiek wordt onderzocht of de huidige IV nog aansluit bij de behoeften vanuit de organisatie en op eventuele discrepanties worden verbeteracties uitgezet en bewaakt	Corporate contribution	
FB	3	Concrete plannen voor de lange termijn zijn opgesteld om verbeteringen aan te brengen in bedrijfsprocessen, organisatie, ondersteunende IV en de aansluiting daartussen	User/customer	
FB	4	Vastgesteld is welke expertise, informatiesystemen en infrastructuren in brede zin nodig zijn om de business te kunnen ondersteunen. Deze behoeften zijn concreet genoeg om het aanschaf- en/of ontwikkelproces aan te sturen	Future	
AB	1	Op basis van onderzoek naar ontwikkelingen binnen klantorganisaties en in de omgeving van klantorganisaties worden voorstellen gedaan om te komen tot betere integratie van bedrijfsprocessen en applicaties	Corporate contribution	
AB	2	Applicaties worden periodiek geëvalueerd op toekomstvastheid, hierbij wordt rekening gehouden met de kwaliteit van bestaande programmatuur, gedrag in exploitatie en de concrete aansluiting bij bedrijfsprocessen en gebruikers. Verbeteringen aan het systeem worden aangegeven (vernieuwingsscenario's)	Corporate contribution	
TB	1	Door technisch beheer wordt marktonderzoek gedaan naar ontwikkelingen (producten en dienstverlening) in de branche, dit leidt tot inzicht in IT-partijen die werkzaam zijn in de branche (mogelijke concurrenten)	Future	

Aspect		Strategisch plan	Perspectief	Score
FB	5	In het strategisch plan wordt een toekomstbepaling beschreven van de gewenste IV, waarbij rekening wordt gehouden met de levenscyclus van systemen	Corporate contribution	
FB	6	Er is een risico analyse uitgevoerd om de onderwerpen te bepalen voor het strategisch plan	Internal	
FB	7	Het gewenste beeld van de levenscyclus met daarin de toekomstvastheid, onderhoudbaarheid en kwaliteit van geautomatiseerde IV (applicaties en infrastructuur) ter ondersteuning van bedrijfsprocessen wordt vastgelegd	Corporate contribution	

FB	9	Strategische plannen zijn mede gebaseerd op nieuwe mogelijkheden en trends in IT om concurrentievoordelen te behalen	Future
FB	8	Activiteiten uit het strategisch plan dekken geïdentificeerde risico's af	Internal
AB	3	Applicatiebeheer heeft een visie en concrete doelstellingen voor toekomstige diensten beschreven (strategisch plan) waarin o.a. omvang, sterkten en zwakten onderkend zijn van diensten	Corporate contribution

Aspect		Tactisch plan	Perspectief	Score
FB	10	In de portfolioplanning zijn alle veranderingen op het gebied van IV opgenomen inclusief daarbij behorende oplossingen	Corporate contribution	
FB	11	In het ICT jaarplan zijn belangrijke werkzaamheden van functioneel beheer voor het komende jaar ingepland. Dit plan wordt beoordeeld op haalbaarheid	Internal	
FB	12	Samenhang tussen verschillende plannen (portfolioplannen en de plannen van functioneel beheer zelf) t.a.v. de IV wordt bewaakt en begeleid	Corporate contribution	
FB	13	Er is gepland welke kosten en baten samenhangen met beheer, onderhoud en exploitatie en deze kosten worden bewaakt. Eventuele afwijkingen leiden tot bijstelling van processen	Corporate contribution	
FB	14	Het beleid over te gebruiken methodes, werkwijze, standaarden en hulpmiddelen wordt periodiek geëvalueerd en aangepast aan ervaringen, ontwikkelingen en behoeften	Future	
AB	4	De visie van applicatiebeheer is vertaald naar concrete projecten/acties waarin duidelijk staat beschreven welke veranderingen aan de dienstverlening nodig zijn en welke activiteiten daarvoor ondernomen moeten worden	User/customer	
AB	5	Een applicatieportfolio bevat beschrijvingen van alle belangrijke systemen en wordt geregeld bijgewerkt. Hierdoor bestaat inzicht in omvang/complexiteit, belang, kwaliteit en continuïteit van de applicaties	Corporate contribution	
AB	6	Analyses op applicatieportfolio leiden structureel tot projecten/acties, bijstellen van projecten/acties of afstoten van applicaties	Corporate contribution	
AB	7	Werkzaamheden en projecten binnen de applicatiebeheerorganisatie worden opgenomen in een jaarplan. Dit plan wordt beoordeeld op haalbaarheid en realiseerbaarheid en bij uitvoering wordt deze bewaakt	Internal	
TB	2	In tactische plannen worden onderwerpen beschreven over de benodigde capaciteit van netwerk, servers en desktop apparatuur en de aansluiting van deze hardware en infrastructuur op de doelstellingen en behoeften van de gebruikersorganisatie. Hiervoor worden periodiek analyses uitgevoerd	Corporate contribution	
TB	3	In tactische plannen worden voorstellen gedaan om de onderhoudbaarheid en beschikbaarheid van IT te verbeteren. Trendanalyses en onderzoek naar IT storingen vormen input voor dit plan	Corporate contribution	

PO3 - Determine Technological Direction & PO2 - Define the information architecture

Aspect		Informatie architectuur	Perspectief	Score
FB	15	In de informatiearchitectuur komt tot uitdrukking hoe middelen van IV op het hoogste niveau samenhangen en hoe deze nader zijn onderverdeeld	Internal	

FB	16	Er is sprake van een gedetailleerd en actueel bedrijfsbreed informatiemodel ten behoeve van het beheer van bedrijfsinformatie	Internal

Aspect		Ontwikkelingen	Perspectief	Score
FB	17	Informatie over ontwikkelingen op technologiegebied (applicaties en infrastructuur) wordt ingewonnen bij ICT-dienstverleners. Deze informatie wordt gebruikt om bedrijfsprocessen beter te ondersteunen	Future	
AB	8	Nieuwe technologische ontwikkelingen op het gebied van bijvoorbeeld compilers en ontwikkelomgevingen worden door applicatiebeheer i.s.m. technisch beheer onderzocht om te zorgen voor een optimale aansluiting van applicaties en infrastructuur	Future	
AB	9	Er bestaan standaardwerkwijzen om nieuwe technologie te implementeren in de ontwikkelomgeving. Hierop wordt getoetst	Internal	
AB	10	Na implementatie van nieuwe technologie wordt het invoeringstraject geëvalueerd en worden werkwijze en toetsingscriteria daar waar nodig aangepast	Internal	
AB	11	Applicatiebeheer adviseert gebruikers pro-actief over mogelijkheden van toepassing van nieuwe technologieën	User/customer	
TB	4	Nieuwe technologische ontwikkelingen op het gebied van ICT infrastructuur worden onderzocht waarbij capaciteit en aansluiting op behoeften van gebruikers en applicaties, zoals in tactische plannen beschreven staat, leidraad zijn	Future	

PO4 – Define the IT processes, Organisation and Relationships & PO7 - Manage IT Human Resources

Aspect			Perspectief	Score
FB	18	Taken, verantwoordelijkheden en rollen zijn onderkend en beschreven	Internal	
FB	19	De werkwijze wordt periodiek geëvalueerd en bijgesteld om aansluiting met de gebruikersorganisatie te optimaliseren	Corporate contribution	
FB	20	Functioneel beheer coördineert activiteiten, belangen en verantwoordelijkheden met diverse partijen (ICT-dienstverleners, gebruikersorganisaties en functioneel beheer zelf)	Internal	
AB TB	12 5	Applicatiebeheer en/of technisch beheer definieren op basis van het beleid duidelijke en meetbare doelstellingen ten aanzien van kennismanagement	Internal	
AB TB	13 6	Applicatiebeheer en/of technisch beheer hebben kwalitatief en kwantitatief zicht op de expertises/skills die nodig zijn om de gewenste dienstverlening, zoals aangegeven in het strategisch plan, te realiseren	Future	
AB TB	14 7	Pro-actief en vooruitlopend op vragen vanuit de markt wordt geïnvesteerd in vergroting van kennis en ervaring zoals beschreven in skills-beleid en uitgewerkt in profielen, opleidingsplannen en kennismanagement	Future	
TB	8	Het personeel dat verantwoordelijk is voor technisch beheer is naar behoren getraind en maakt gebruik van geaccepteerde standaarden en tooling wat dient om kwaliteit van geleverde dienstverlening te waarborgen en/of te verhogen	Future	

PO10 – Manage projects

Aspect	Organisatie en aanpak	Perspectief	Score

PM	1	Er is een geaccepteerde projectmanagement methode die zorgt dat projecten op een gecontroleerde manier een set aan activiteiten uitvoert die leiden tot het gewenste eindresultaat (levering van producten)	Internal
PM	2	De business case beschrijft het “waarom” van het project. Hierin wordt vastgelegd wat de reden is voor het project, de benefits, kosten-baten schatting, risicoafweging	User/customer
PM	3	Er is een duidelijke scheiding tussen projectorganisatie en beheerorganisatie	Internal
PM	4	De projectorganisatie heeft een projectmanager, heeft voldoende gebruikers betrokken en heeft de rollen en activiteiten van (beheer) leveranciers eenduidig gedefinieerd	User/customer
PM	5	Voor alle betrokkenen is duidelijk en beschreven waarom het project nodig is, wat de verwachte uitkomst is, hoe deze uitkomst wordt bereikt en wat de verantwoordelijkheden en taken van iedereen zijn	User/customer

Aspect		**Planning en voortgang**	**Perspectief**	**Score**
PM	6	Het projectplan voldoet aan de vereisten en standaarden van de gekozen projectmanagement methode en beschrijft het “wat”, “hoe”, “wanneer” en “wie” van een project	Internal	
PM	7	Het projectplan bevat minimaal de volgende onderdelen: op te leveren producten, activiteiten om tot die producten te komen, activiteiten om kwaliteit te valideren van producten, benodigde resources en tijd voor alle activiteiten, mijlpalen, beslispunten en interne & externe afhankelijkheden	Internal	
PM	8	Bedrijfs- en projectrisico’s zijn geïdentificeerd en geanalyseerd (impact), maatregelen om risico’s te beperken zijn in het projectplan opgenomen en worden continue bewaakt en periodiek geëvalueerd.	Internal	
PM	9	De gebruikersorganisatie heeft kwaliteitsverwachtingen m.b.t. producten eenduidig gedefinieerd	User/customer	
PM	10	Het kwaliteitsplan beschrijft duidelijk hoe het project tegemoet komt aan de kwaliteitseisen van de opdrachtgever	Internal	
PM	11	In het kwaliteitsplan staat beschreven wat het beleid t.a.v. kwaliteit is, welke technieken & procedures worden toepast, wie verantwoordelijk is en wat de gedefinieerde kwaliteitscriteria zijn. Hierover wordt periodiek gerapporteerd	Internal	
PM	12	Periodieke evaluaties/reviews van de voortgang van het project (en projectplan) worden vergeleken met de business case om te beoordelen of het project de business case nog voldoende ondersteunt	user/customer	
PM	13	Het resultaat van periodieke evaluaties is dat op elk willekeurig moment bekend is wat de status is van producten (en de onderlinge relaties) die worden geleverd en wie ermee bezig zijn	Internal	
PM	14	Er is een onafhankelijke Quality Assurance rol binnen projecten, waardoor wordt toegezien op de beheerste uitvoering van projecten, de onderlinge samenhang en op de kwaliteit van de door deze projecten opgeleverde producten	user/customer	
PM	15	De structuur voor Quality Assurance is zodanig dat vastgesteld kan worden of de resultaten van projecten van het vereiste niveau zijn, mijlpalen in de planning worden gehaald en kosten binnen het budget blijven	user/customer	

AI6 - Manage Change & AI1 - Identify Automated Solutions & AI2 – Acquire and Maintain Applications Software

Aspect	**Wijzigingsverzoeken**	**Perspectief**	**Score**

FB	21	Voor alle nieuwe functionele eisen wordt een gestructureerd (standaard) wijzigingsverzoek opgesteld. Hierbij wordt geborgd dat beheerprocessen (zoals continuity, availability, security) worden meegenomen bij het specificeren, ontwerpen, realiseren, etc van wijzigingen	Future
FB	22	Heldere afspraken zijn gemaakt over formele goedkeuring van wijzigingsverzoeken Strategische en tactische plannen zijn een kader voor goedkeuring	Corporate contribution
AB	15	De procedure voor het indienen, beslissen over en afvoeren van wijzigingsverzoeken is beschreven en wordt bewaakt door applicatiebeheer o.a. ten behoeve van terugkoppeling naar de gebruikersorganisatie	Future
AB	16	Er is een expliciet besluit genomen over wel of niet releasematig werken m.b.t. wijzigingsverzoeken. Releasematig werken houdt in dat een verzameling gegroepeerde wijzigingen gelijktijdig en in gezamelijkheid worden aangebracht	Corporate contribution
AB	17	Verschillende wijzigingsvoorstellen worden onderling gerelateerd. Bij inplanning van deze wijzigingen in een release worden deze relaties, naast prioriteit, ook meegenomen	Corporate contribution
TB	9	Voor wijzigingen aan de technische infrastructuur bestaat een procedure voor goedkeuren, verifiëren en inplannen van verzoeken, waarbij altijd bedrijfs- en technische impact van wijzigingen worden beoordeeld	Future

Aspect		**Opstellen specificaties**	**Perspectief**	**Score**
FB	23	Een standaard (template) is beschikbaar voor het opstellen van specificaties waarin helder is beschreven waaraan aandacht wordt besteed. Bijvoorbeeld functionele specificaties en eisen, interfaces, performance, beschikbaarheid, betrouwbaarheid, etc	Internal	
FB	24	Er wordt geborgd, dat alle relevante partijen betrokken zijn bij het opstellen van specificaties bij onderhoud en vernieuwing van de IV waarbij een duidelijke weging van verschillende belangen plaatsvindt	User/customer	
FB	25	Expliciete aandacht wordt besteed aan koppelingen, relaties en afhankelijkheden met andere systemen	Corporate contribution	
FB	26	Heldere afspraken zijn gemaakt met ICT-dienstverleners over het aanleveren van specificaties	User/customer	

Aspect		**Impact-analyse**	**Perspectief**	**Score**
AB	18	Door applicatiebeheer is beschreven/vastgelegd waar aandacht aan besteed wordt in een impact-analyse. Een standaard is aanwezig voor een impact-analyserapport	Future	
AB	19	In een impact-analyse wordt expliciet aandacht besteed aan onderhoudbaarheid, beheersbaarheid en exploiteerbaarheid van applicaties en de effecten voor het bedrijfsproces van de klant	Internal	
TB	10	In de impact-analyse voor wijzigingen aan infrastructuur (routers, switches, etc) of hardware systemen (servers, etc) wordt aandacht besteed aan effecten als beschikbaarheid, capaciteit en onderhoudbaarheid, etc.	Internal	

Aspect		**Ontwerp**	**Perspectief**	**Score**
AB	20	Het functioneel ontwerp beschrijft de functionaliteit en gegevensstructuur tot op detailniveau en sluit aan op bedrijfsprocessen en doelstellingen van de gebruikersorganisatie	Corporate contribution	

AB	21	Ontwerpen zijn consistent, volledig en eenduidig in interpretatie en zijn daardoor voor klanten bruikbaar om te accorderen en om te gebruiken voor acceptatietesten	Internal
FB	27	Toetsing van het door de ICT-dienstverleners opgestelde ontwerp vindt plaatst aan de hand van de door functioneel beheer opgestelde specificaties	Corporate contribution
SEC	1	Tijdens het ontwerpen van nieuwe systemen of releases van bestaande systemen is een analyse gemaakt van beveiligingseisen, hierbij is naast de geautomatiseerde maatregelen ook aandacht besteed aan handmatige maatregelen (procedures)	Internal
SEC	2	Bij analyse van beveiliginseisen is aandacht besteed aan o.a. logische toegangsbeveiliging, gegevensencryptie, back-up, voorkomen van ongeautoriseerde wijzigingen en de impact op de werking van de beveiliging van bestaande systemen	Internal

Aspect		**Realisatie**	**Perspectief**	**Score**
AB	22	De realisatie van programmatuur is beschreven in technische ontwerpen en wordt toegelicht door verklarend commentaar in de code	Future	
AB	23	Er zijn afspraken over de wijze waarop geprogrammeerd (platform, object oriented, etc) wordt Nakoming van deze afspraken wordt getoetst	Future	

Aspect		**Evaluatie**	**Perspectief**	**Score**
FB	28	Periodiek wordt getoetst of zowel opdrachtverstrekking als oplevering van ICT-dienstverleners efficiënt en effectief verloopt	Future	
AB	24	Stelselmatig wordt gerapporteerd over de voortgang van wijzigingen en rapportages worden met de opdrachtgever besproken	User/customer	
TB	11	De status van wijzigingen wordt continue bijgehouden ten behoeve van terugkoppeling aan de opdrachtgever en voor procesevaluatie	User/customer	
TB	12	Bij evaluatie van wijzigingen wordt nagegaan of bedrijfsbehoeften volledig zijn vervuld. Indien dit niet het geval is wordt geanalyseerd wat de redenen hiervoor waren	Corporate contribution	

AI7 - Install and Accredit Solutions Changes (incl AI4 - Enable Operation and Use)

Aspect		**Testen**	**Perspectief**	**Score**
AB	25	Testaanpak en methodes zijn beschreven waarbij onderscheid gemaakt wordt tussen functionele testen en technische testen (bijvoorbeeld unit testing)	Future	
AB	26	Door applicatiebeheer wordt uitvoerig getest op de afgesproken specificaties van functioneel beheer waardoor in acceptatietesten, door gebruikers, zelden fouten in applicaties worden ontdekt	Internal	
AB	27	Er worden registraties bijgehouden van testen, fouten, oorzaken, verbeteracties, resultaten en hertesten	Future	
FB	29	Door functioneel beheer is beschreven hoe acceptatietesten worden uitgevoerd, hierover zijn afspraken met gebruikers gemaakt	Future	

FB	30	In acceptatietesten stelt men vast of de (vernieuwde) werkwijze aansluit op het gewijzigde systeem	Corporate contribution

Aspect		Implementatie	Perspectief	Score
AB	28	Applicatiebeheer draagt zorg dat gebruikers voorafgaand aan inproductiename de impact van releases op hun werk en consequenties voor het bedrijfsproces kennen	User/customer	
AB	29	Voltooiing van releases kent een formele decharge van de opdrachtgever, deze toetst en neemt verantwoordelijkheid over, werkwijze en criteria zijn hiervoor vastgelegd	User/customer	
AB	30	Voor applicatieobjecten zijn verschillende stadia (zoals archief, ontwikkel, test en productie) onderkend waarbij afspraken over overzetting van applicatieobjecten van het ene naar het andere stadium leidt tot eenduidigheid welke objecten gebruikt zijn bij welke release (dit ten behoeve van bijvoorbeeld rollback acties)	Internal	
AB	31	Een eenduidige vorm van uitlevering van applicatieobjecten naar exploitatieomgevingen heeft als doel dat er geen implementaties worden gedaan zonder dat vooraf expliciet bekend is bij technisch beheer wat de consequenties zijn voor exploitaite	Internal	
AB	32	Procedures en afspraken voor opslag en distributie van applicatieobjecten worden regelmatig (pro-actief) geëvalueerd en zo nodig bijgesteld	Future	
TB	13	Procedures voor installatie van nieuwe hardware leiden tot correct geassembleerde en geteste versies tijdens implementatie	Future	
TB	14	Voor elke wijziging aan hardware of infrastructuur worden implementatieplannen, back-out & roll-back plannen, testplannen, acceptatie criteria en testresultaten opgeleverd ter evaluatie	Internal	
TB	15	Ten behoeve van de installatie van nieuwe hardware (componenten) zijn voldoende resources beschikbaar gesteld voor het assembleren, testen en implementeren	Internal	
FB	31	Het transitieplan beschrijft alle te verrichten activiteiten en middels een draaiboek worden deze in een dusdanige volgorde gezet dat een overzichtelijke, geplande en beheerste uitvoering van het transitietraject wordt gerealiseerd	Internal	
FB	32	Verantwoordelijkheid voor het vrijgeven van gewijzigde systemen voor gebruik en beheer is duidelijk belegd	User/customer	
FB	33	Periodiek wordt beoordeeld of uitgevoerde wijzigingen hebben geleid tot foutsituaties of andere onvolkomenheden. Beoordelingen leiden tot verbetering van het proces	Future	

Aspect		Gebruik	Perspectief	Score
FB	34	Werkwijzen worden vroegtijdig aangepast en hierbij wordt de gehele AO (handleidingen, procesbeschrijvingen, procesmodel, werkinstructies, formulieren e.d.) in beschouwing genomen	Corporate contribution	
FB	35	Voor de beschrijving van handleidingen en werkinstructies zijn standaarden/templates	Internal	
FB	36	Werkinstructies/handleidingen en procedures worden gecontroleerd op werkbaarheid, dit in nauwe samenwerking met de gebruikersorganisatie	Future	

AI5 – Procure IT resources

Aspect		Acquisitie strategie	Perspectief	Score
INK	1	Acquisities van ICT systemen en services worden uitgevoerd door een beschreven proces met de volgende of vergelijkbare (sub)-processen: acquisitie-initiatie, procurements en acquisitie-voltooiing (ter controle en evaluatie) gebruikmakend van op best practices gebaseerde templates	Future	
INK	2	Tijdens acquisities worden zowel bij klant als leverancier rollen toegewezen en beschreven, deze geven aan waar verantwoordelijkheden en bevoegdheden binnen een acquisitie liggen en welke kennis en vaardigheden nodig zijn	user/customer	
INK	3	Tijdens de acquisitie-initiatie worden bedrijfsbehoeften en eisen aan services en/of systemen vastgelegd (acquisitiedoel) in een servicebeschrijving en/of systeembeschrijving	Corporate contribution	
INK	4	De definitie van het doeldomein geeft de reikwijdte van het systeem of service aan en dient te voorkomen dat o.a. interfaces met andere systemen niet worden herkend, niet alle betrokken actoren worden herkend, kosten en baten verkeerd worden ingeschat en niet alle relevante risico's worden geïdentificeerd	Corporate contribution	
INK	5	De acquisitiestrategie wordt bepaald aan de hand van een overzicht van mogelijke scenario's en analyse van de situatiefactoren en risico's	Corporate contribution	
INK	6	Het resultaat van de acquisitiestrategie is een acquisitieplan waarin staat welke beslissingen op welke momenten genomen moeten worden	Internal	

Aspect		Procurement technieken	Perspectief	Score
INK	7	Elke procurement heeft een leveringsplan wat klantorganisaties en leveranciers samen opzetten. Dit proces omvat activiteiten die te maken hebben met tendering, contractmonitoring en contractvoltooiing.	Internal	
INK	8	Bij het opzetten van een leveringsplan wordt per procurement gebruik gemaakt van de volgende of vergelijkbare technieken: situatie- en risicoanalyse, leveringsstrategie, planning beslispunten (wie wat levert gedurende de uitvoering van het contract) en eisen die aan deliverables worden gesteld	Future	
INK	9	De situatie- en risicoanalyse leiden tot een gedegen inzicht in complexiteit en onzekerheid in het doeldomein (klantorganisatie) en servicedomein (leveranciersorganisatie)	Internal	
INK	10	De leveringsstrategie beschrijft eenduidige maatregelen om risico's te beperken en een analyse van de impact van gekozen maatregelen	Internal	
INK	11	In de planning van beslispunten komt de leveringstrategie tot uiting, hierbij liggen de te nemen beslissingen bij procurements o.a. op het vlak van: systeem- en service-eisen (doel), tijdsplanning, kosten en baten, type leverancier, dienstverleningsniveau, betrokkenen, voornaamste deliverables, etc.	Internal	

Aspect		Procurement proces & deliverables	Perspectief	Score
INK	12	Tijdens de tendering fase van procurements worden tendering-deliverables opgeleverd. Dit zijn de offerteaanvraag, offerte, leverancierse valuatieverslag en contract	Internal	
INK	13	Door de gebruikersorganisatie wordt per procurement een offerteaanvraag opgesteld. Deze aanvraag is in overeenstemming met het acquisitiedoel en het acquisitieplan en vormt voldoende basis voor leveranciers om een offerte uit te brengen	Internal	
INK	14	Door de gebruikersorganisatie worden offertes en ICT-leveranciers beoordeeld op begrip van probleemsituatie, geboden oplossing, leveringsplan, projectplan, tarieven, etc en op basis hiervan wordt een leverancier geselecteerd	Future	

INK	15	De gebruikersorganisatie levert serviceplannen om eisen te stellen aan de serviceorganisatie. Dit is een specificatie van service levels, deliverables, tijdslijnen, resources, etc en heeft een duidelijke relatie met SLM	Internal
INK	16	Tijdens contractmonitoring van procurements wordt de levering van services en deliverables gecontroleerd aan de hand van eisen die zijn gesteld, deze hebben betrekking op operationele items als deliverables, dit kunnen o.a. hardwarecomponenten, software of gebruiker- en beheerderhandleidingen zijn	Internal
INK	17	Voor operationele deliverables (hardware, software, handleidingen, etc) wordt vastgelegd in welke kwaliteitsfase deze zich bevinden (welke kwaliteitsprocedures zijn doorlopen). Deze deliverables dragen bij aan het correct functioneren van het doeldomein	Internal
INK	18	De leverancier levert servicerapportages om de klant grip te geven op inhoud en kwaliteit van geleverde en de te leveren services, hierin wordt de status van de service beschreven	Internal

DS1 - Define and Manage Service Levels & DS2 – Manage Third-party Services

Aspect		Opstellen SLA	Perspectief	Score
FB	37	SLA's zijn gezamenlijk door gebruikersorganisatie en ICT-dienstverleners opgesteld. Gemaakte service afspraken geven een reëel inzicht in eisen vanuit de gebruikersorganisatie	Corporate contribution	
FB	38	In SLA's zijn eenduidige afspraken beschreven over het niveau en kwaliteit van de dienstverlening en de te leveren prestaties en verantwoordelijkheden. Deze afspraken zijn concreet en meetbaar	Corporate contribution	
AB	33	Dienstverlening, te leveren prestaties en verantwoordelijkheden zijn duidelijk omschreven in SLA's waarin gedetailleerde afspraken over het niveau en de kwaliteit van de dienstverlening vertaald zijn naar eenheden die door applicatiebeheer meetbaar zijn	Internal	
TB	16	Het management heeft procedures voor het opstellen en beoordelen van SLA's, waarbij duidelijk is hoe onderwerpen als service hours, beschikbaarheid, betrouwbaarheid, ondersteuning, reactietijd en wijzigingsbeheer gemeten worden	Corporate contribution	
TB	17	Voor alle aangeboden diensten is een dienstencatalogus opgesteld die een actueel beeld geeft van het dienstenaanbod	Internal	
SEC	3	Risico's van toegang door derden tot apparatuur of programmatuur zijn geanalyseerd waarbij rekening is gehouden met de wijze waarop toegang wordt verkregen en waarde van informatie	Internal	
SEC	4	Beveiligingsmaatregelen zijn genomen om risico's van toegang door derden tot een aanvaardbaar niveau te brengen	Internal	
SEC	5	De beveiligingseisen bij uitbesteding zijn vastgelegd in een contract dat bekrachtigd is door alle betrokken partijen	Corporate contribution	
SEC	6	De beveiligingseisen in het contract omvat minimaal: • verantwoordelijkheden van alle partijen; • hoe wordt voldaan aan wettelijke vereisten zoals de wetgeving ter bescherming van privacy; • welke kwaliteitsnormen worden gehanteerd; • welke maatregelen zijn genomen voor fysieke en logische toegangsbeveiliging; • en hoe de gewenste beveiliging van middelen wordt gehandhaafd en getest.	Internal	

Aspect	Bewaken & evalueren service levels	Perspectief	Score

FB	39	Evaluaties van ICT-dienstverleners resulteren in een dienstverlening die in lijn is met strategische plannen van functioneel beheer	Corporate contribution
FB	40	Door ICT-dienstverleners uitgevoerde opdrachten worden bewaakt, gecontroleerd, geëvalueerd en desgewenst bijgesteld	Corporate contribution
FB	41	ICT-dienstverleners leveren periodiek rapportages die de beheersing en verbetering van hun processen aantonen, bijvoorbeeld een TPM of SAS70	Corporate contribution
FB	42	Periodiek wordt de dienstverlening besproken met proceseigenaren en met ICT-dienstverleners en wordt de geleverde dienstverlening aangepast aan behoeften. Hierbij wordt rekening gehouden met nieuwe ontwikkelingen aan de gebruikerskant en dienstverlening	Corporate contribution
SEC	9	Kwaliteitseisen betreffende te leveren producten/diensten en inspectie daarop zijn contractueel met ICT- leveranciers vastgelegd	Corporate contribution
SEC	10	Escrow-regelingen zijn getroffen voor het geval de externe partij wordt overgenomen of failliet gaat	Corporate contribution
AB	34	Applicatiebeheer bewaakt of gemaakte afspraken gerealiseerd zijn. Een evaluatie moet duidelijkheid scheppen waarom afspraken niet gerealiseerd zijn	Corporate contribution
TB	18	Alle diensten die in SLA's beschreven staan worden gemeten en vergeleken met afgesproken dienstenniveaus. Hierover worden periodiek service rapporten geleverd zodat klanten duidelijke informatie geboden wordt over kwaliteit van geleverde dienstverleningen	Corporate contribution
TB	19	Periodiek worden, voor het management, rapportages opgeleverd waarin aangeboden diensten vergeleken worden met behaalde prestaties, trends in Service Level Breaches, aantal verzoeken van nieuwe of aangepaste diensten, etc. en wordt het dienstenaanbod adequaat aangepast	Corporate contribution
TB	20	Periodiek wordt gemeten op klanttevredenheid en wordt in overleg met gebruikersorganisaties beoordeeld of de aangeboden dienstverlening aansluit bij behoeften	user/customer

DS4 – Ensure Continuous Service

Aspect		**Continuïteitsplan**	**Perspectief**	**Score**
FB	43	Door functioneel beheer wordt continuïteitsmanagement aangestuurd in samenwerking met de gebruikersorganisatie en afgestemd met ICT-dienstverleners	Internal	
SEC	11	Een strategie is vastgelegd voor continuïteitsmanagement. Deze strategie sluit aan op strategische IV doelen/beleid	Corporate contribution	
SEC	12	Risico's die onderbreking van bedrijfsprocessen kunnen veroorzaken en de gevolgen van deze risico's zijn vastgesteld. Hierbij valt te denken aan (zware) storingen aan apparatuur, wateroverlast en brand	Internal	
SEC	13	Ter ondersteuning van de strategie voor continuïteitsmanagement is een proces van continuïteitsplanning ingericht en deze omvat minimaal: • specificeren van kritische bedrijfsprocessen, de daarbij behorende ondersteunende applicaties en de daartoe benodigde centrale en decentrale organisatorische en technische automatiseringsinfrastructuren; • toewijzen van continueringprioriteiten aan bedrijfsprocessen/applicaties in termen van maximaal toegestane uitvalsduur; • inventariseren van continuïteitsbedreigingen, de gevolgen hiervan voor de kritische bedrijfsprocessen/applicaties en in te zetten interne dan wel externe	Internal	

		continuïteitsvoorzieningen; • vastleggen van verantwoordelijkheden met betrekking tot de in te zetten continuïteitsvoorzieningen, waarbij te denken valt aan escalatieprocedures, beslissingsstructuren, crisismanagement, coördinatie bij het operationaliseren van de continuïteitsvoorzieningen; • procedures voor het testen en bijwerken van continuïteitsplannen.	
SEC	14	Het proces van continuïteitsplanning omvat het specificeren van kritische processen, daarbij behorende ondersteunende applicaties en daartoe benodigde centrale en decentrale organisatorische- en technische automatiseringsinfrastructuren	Internal
SEC	15	Continuïteitsplanning omvat de toewijzing van continueringsprioriteiten aan bedrijfsprocessen/applicaties in termen van maximaal toegestane uitvalsduur	Internal
SEC	16	Continuïteitsplanning omvat een inventarisatie van continuïteitsbedreigingen, gevolgen hiervan voor kritische bedrijfsprocessen/applicaties en in te zetten interne dan wel externe voorzieningen	Internal
SEC	17	Continuïteitsplanning omvat vastlegging van verantwoordelijkheden met betrekking tot in te zetten voorzieningen, waarbij te denken valt aan escalatieprocedures, beslissingsstructuren, crisismanagement, coördinatie bij het operationaliseren van continuïteitsvoorzieningen	Internal
SEC	18	Continuïteitsplanning omvat procedures voor testen (testactiviteiten) en bijwerken van continuïteitsplannen	Internal
SEC	19	Een modelstructuur voor een continuïteitsplan omvat minimaal condities om het plan te activeren, procedures voor noodsituaties, uitwijkprocedures, terugkeerprocedures, onderhoudsplanning, bewustwording- en opleidingsactiviteiten en een beschrijving van verantwoordelijkheden van alle betrokkenen	Internal
TB	21	In geval van calamiteiten bij technisch beheer staat beschreven wat de reactietijden moeten zijn, hoe een damage assessment uitgevoerd moet worden en hoe mens en middelen in veiligheid gebracht worden, etc	Internal
FB	44	Het calamiteitenplan wordt periodiek getest door of in opdracht van functioneel beheer en wordt eventueel bijgesteld. Hierbij wordt rekening gehouden met ontwikkelingen en verandering in de organisatie, bedrijfsproces en IT	Corporate contribution
AB	35	De toekomstvastheid van gebruikte hulpmiddelen (bijvoorbeeld compilers) is bekend waardoor duidelijkheid geschept wordt wat de kans en risico is dat hulpmiddelen niet meer ondersteund worden (in de nabije toekomst)	Future
AB	36	Uitwijk voor alle belangrijke objecten (inclusief data, documentatie) wordt door applicatiebeheer getest	Corporate contribution

DS5 – Ensure Systems Security

Aspect		Beleid	Perspectief	Score
SEC	20	Het bestuur heeft een projectorganisatie ingesteld om het beveiligingsbeleid te ontwerpen en te implementeren	Internal	
SEC	21	Na het ontwerp van het beleidsdocument wordt deze door het bestuur geaccordeerd	Corporate Contribution	
SEC	22	Na accorderen van het beleidsdocument toont het bestuur door middel van security awareness-programma's zich zichtbaar betrokken om doelstellingen, principes en maatregelen van informatiebeveiliging bij managers en medewerkers onder de aandacht te brengen	Corporate Contribution	

SEC	23	Het beleid voor informatiebeveiliging kent een eigenaar die verantwoordelijk is voor implementatie, handhaving en evaluaties van het beveilingsbeleid in diverse organisatorische eenheden	Internal
SEC	24	Het beleidsdocument voor informatiebeveiliging geeft aan in hoeverre belangrijke bedrijfsprocessen afhankelijk zijn van informatiesystemen (applicaties en netwerken)	Corporate Contribution
SEC	25	Ten behoeve van het beleidsdocument wordt een overzicht vervaardigd van de classificatie van bedrijfsmiddelen	Internal
SEC	26	Bij inventarisatie van bedrijfsmiddelen wordt onderscheid gemaakt naar informatie, programmatuur, apparatuur, dienstverlening en eigenaren van bedrijfsmiddelen	Internal
SEC	27	Door middel van risico-inventarisatie wordt in het beleidsdocument vastgesteld wat bedreigingen zijn voor belangrijke bedrijfsprocessen en bedrijfsmiddelen en welke maatregelen worden getroffen	Internal
SEC	28	Het beleidsdocument besteedt aandacht aan het voldoen aan wettelijke en contractuele verplichtingen, eisen voor scholing van beveilgingsfunctionarissen en eisen voor continuïteit van bedrijfsprocessen	Internal
SEC	29	Bestaan en werking van het informatiebeveilingsbeleid (en maatregelen) worden beoordeeld door onafhankelijke functionarissen, waarbij gecontroleerd wordt of de beveiligingsnormen en procedures worden nageleefd	Corporate contribution
SEC	30	In het beveiligingsbeleid staan richtlijnen voor toewijzing van functies en verantwoordelijkheden m.b.t. beveiliging, zoals het verlenen van toegangsrechten voor informatiesystemen en het verlenen van toegang tot fysieke ruimtes	Internal
SEC	31	Er is een formele procedure voor toekennen, registreren en rapporteren van toegangsrechten ten aanzien van IT-voorzieningen waarin o.a. wordt geregeld dat wijzigingen van toegangsrechten worden teruggekoppeld naar de eigenaar van de IT-voorziening	Internal
SEC	32	Maatregelen zijn getroffen die voorzien dat niet alle bevoegdheden bij het uitvoeren van specifieke werkzaamheden in één hand terechtkomen, deze functiescheiding is formeel in functiebeschrijvingen, onder de noemer beveiligingseisen, personeel vastgelegd	Internal
SEC	33	Toegangsrechten en user-id's worden bij vertrek of functiewijziging van functionarissen tijdig verwijderd of gewijzigd	Internal

Aspect		**Applicatie- en systeembeveiliging**	**Perspectief**	**Score**
SEC	34	Door applicatiebeheer wordt in combinatie met klanten, betreffende toegang tot gegevens, een bevoegdhedenmatrix opgesteld waarbij het mogelijk is om toegangsrechten te differentiëren naar lezen, schrijven, wijzigen, uitvoeren, etc	Internal	
AB	37	Autorisaties worden periodiek bekeken op actualiteit in overleg met gebruikersorganisaties en worden op tijd ingetrokken	Internal	
SEC	35	Het interne netwerk is beveiligd tegen ongeautoriseerde toegang vanuit externe verbindingen/netwerken door middel van firewalls, secure gateways, etc	Internal	
SEC	36	Omvangrijke netwerken worden gesplitst in afzonderlijke logische netwerkdomeinen (segmentering), ondersteund met firewalls ter afscherming van de afzonderlijke domeinen	Internal	
SEC	37	Bekend (en beschreven) is welke gevolgen het gebruik van externe-services (inbelfunctie, vpn, webservices, etc) heeft voor de vertrouwelijkheid, integriteit en beschikbaarheid van getransporteerde data en van data die zich bevindt op aangesloten systemen	Internal	

SEC	38	Op periodieke basis worden penetratietesten uitgevoerd ten einde kwetsbaarheden in de beveiliging te detecteren. Hierbij wordt gebruik gemaakt van onafhankelijke experts	Internal
SEC	39	Analyse van systeemgebruik geeft volledig inzicht in bedreigingen voor het systeem en in welke situaties deze zich kunnen voordoen	Internal
SEC	40	Voor analyses van systeemgebruik zijn procedures opgesteld ten einde vast te stellen dat gebruikers uitsluitend handelingen verrichten waarvoor zij zijn geautoriseerd	Internal
SEC	41	Resultaten van analyses van systeemgebruik worden regelmatig beoordeeld, hierbij wordt rekening gehouden met risico's als afhankelijkheid van applicaties, gevoeligheid van informatie en de mate waarin het systeem verbonden is met andere (publiek toegankelijke) netwerken	Corporate contribution

Aspect		**Bewaking en evaluatie**	**Perspectief**	**Score**
SEC	42	Door functioneel beheer wordt namens het management van gebruikersorganisaties frequent gecontroleerd dat de beveiliging door gebruikers wordt gewaarborgd conform geldende beveiligingsnormen	Corporate contribution	
SEC	43	Door functioneel beheer wordt namens het management van de gebruikersorganisatie frequent gecontroleerd dat de beveiliging door ICT-leveranciers wordt gewaarborgd conform geldende beveiligingsnormen	Corporate contribution	
SEC	44	Door applicatiebeheer wordt frequent gecontroleerd dat beveiliging van applicaties zodanig werkt, dat beveiligingsrisico's binnen aanvaardbare grenzen zijn en blijven	Corporate contribution	
SEC	45	Door technisch beheer wordt frequent gecontroleerd dat de beveiliging voor computer- en netwerksystemen zodanig werkt, dat beveiligingsrisico's voor netwerk en infrastructuur binnen aanvaardbare grenzen zijn en blijven	Corporate contribution	
SEC	46	Controles worden periodiek uitgevoerd op het gebied van: beveiligingsovertredingen, wijzigingen in logische toegangsbeveiliging, wijzigingen in beveiligings- en/of controlekritische besturingsparameters, wijzigingen in kritische systeemsoftware-libraries, etc	Corporate contribution	

DS11 - Manage Data

Aspect		**Back-up**	**Perspectief**	**Score**
SEC	47	Frequent wordt een back-up gemaakt van alle belangrijke gegevens zoals databestanden en programmatuur, autorisatie en logbestanden en de volledige schijveninhoud. Hierdoor is het mogelijk verloren gegane gegevens te reconstureren	Internal	
SEC	48	Back-ups die minimaal nodig zijn om systemen te herstellen worden opgeslagen op een locatie die zich op zodanige afstand bevindt dat geen schade kan worden aangericht als zich een calamiteit voordoet op de hoofdlocatie	Internal	
SEC	49	Back-ups en restore procedures worden regelmatig getest, zodat het zeker is dat deze betrouwbaar zijn en in geval van nood kunnen worden gebruikt	Corporate contribution	

DS12 - Manage the Physical Environment

Aspect		**Pysieke beveiliging**	**Perspectief**	**Score**
SEC	53	Fysiek te beveiligen ruimtes in het gebouw zijn duidelijk gedefinieerd waarbij de mate van beveiliging in overeenstemming is met de waarde van bedrijfsmiddelen of diensten die worden beveiligd	Internal	
SEC	54	In het gebouw worden ruimtes onderscheiden door zones, zoals: publieksruimten, algemene kantooruimten, netwerkruimten, technische ruimte voor energievoorziening, centrale computerruimten, etc	Internal	

SEC	55	Ruimtes zijn doelmatig van elkaar gescheiden en afgesloten voor onbevoegde medewerkers en bezoekers die niet de juiste identificatie kunnen tonen	Internal	
SEC	56	Beveligingssystemen voor fysiek te beveiligen ruimtes in een gebouw worden regelmatig gestest	Corporate contribution	

Aspect		**Stroomvoorziening**	**Perspectief**	**Score**
SEC	57	Apparatuur is beveiligd tegen stroomstoringen en andere elektrische storingen, zoals blikseminslag of statische elektriciteit	Internal	
SEC	58	Reservevoedingseenheden zijn aanwezig en kennen voldoende vermogen om apparatuur gedurende een vooraf bepaalde tijdsduur te voorzien van elektriciteit	Internal	
SEC	59	Reservevoedingseenheden (en aangesloten generatoren) worden regelmatig gestest in overeenstemming met voorschriften van fabrikanten	Corporate contribution	

M1 - Monitor & evaluate IT processes & M2 - Monitor & evaluate internal control

Aspect		**Aanpak**	**Perspectief**	**Score**
ALL	1	Ten behoeve van besturing van IT (IT Governance) wordt door het management een controle framework en aanpak opgesteld die de scope, methodologie en te volgen processen beschrijft	Corporate contribution	
ALL	2	Het management, in overleg met de gebruikersorganisatie, heeft een gebalanceerde set van prestatie *objectives* gedefinieerd die o.a. het volgende omvatten: bijdrage van IT aan de business (niet alleen financieel), beoordeling van belangrijke IT processen incl. ontwikkeling en dienstenlevering, toekomstgerichte activiteiten zoals opkomende nieuwe technologieën en personele vaardigheden	Internal	

Aspect		**Beoordeling**	**Perspectief**	**Score**
ALL	3	Periodiek worden prestaties van de volledige IT organisatie beoordeeld ten opzichte van gedefineerde doelstellingen. Analyse van tekortkomingen leidt tot verbeteracties	Internal	
ALL	4	Periodiek wordt de effectiviteit van interne controlemaatregelen beoordeeld waarbij o.a. de volgende onderwerpen worden behandeld: naleving van beleid en standaarden, informatiebeveiliging, SLA's	Internal	
ALL	5	Periodiek wordt door een externe partij controlemaatregelen beoordeeld op compleetheid en effectiviteit	Corporate contribution	

XI. Wijzigingen IT Governance Checklist

Checkitem	Oud perspectief	Nieuw perspectief	Reden van wijziging
Plan & Organise			
AB 2	User/customer	Corporate contribution	Aansluiting op de totale gebruikersorganisatie en doelen van de organisatie
FB 7	Internal	Corporate contribution	Portfolio planning net als FB 5
FB 11	User/customer	Internal	Het plan is bedoeld voor intern gebruik om IT Beheer voor de organisatie zo goed mogelijk uit te voeren en legt niet het accent op *process improvement*
AB 7	User/customer	Internal	Plan voor intern gebruik waarbij wordt bewaakt of het voldoet aan de standaard
TB 3	Future/innovation & learning	Corporate contribution	Verbeteren van IT diensten ten behoeve van gebruikersorganisaties
FB 20	User/customer	Internal	Breder dan alleen gebruikersorganisaties. Bedoeld om efficiënt IT beheer mogelijk te maken
PM 5	Internal	User/customer	Draagt in belangrijke mate bij aan de vraag: "leveren projecten de verwachte resultaten"
PM 7	User/customer	Internal	Standaard onderdelen van een projectplan
PM 10	User/customer	Internal	Beoordeeld dat een onderdeel (kwaliteitsplan) van een IT project voldoet aan standaarden (kwaliteitseisen)
Acquire & Implement			
AB 15	Internal	Future/innovation & learning	Richt zich meer op de procedure/aanpak dan op producten
AB 16	Internal	Corporate contribution	Software releases gaat over integratie van wijzigingen
TB 9	Internal	Future/innovation & learning	Richt zich meer op de procedure/aanpak dan op producten
FB 23	Future/innovation & learning	Internal	Een standaard wordt gebruikt om te zorgen voor een kwalitatief hoog product
FB 26	Internal	User/customer	Beoordeeld hoe de vraag- en aanbodorganisatie samenwerken (integratie)
AB 18	Internal	Future/innovation & learning	Richt zich meer op de procedure/aanpak dan op producten
TB 10	Corporate contribution	Internal	Heeft betrekking op de kwaliteit van de impact-analyse
AB 21	User/customer	Internal	Heeft meer betrekking op de kwaliteit van ontwerpen dan op de integratie tussen gebruikersorganisatie en applicatiebeheer
AB 23	Internal	Future/innovation & learning	Richt zich meer op de procedure/aanpak dan op producten
TB 12	User/customer	Corporate contribution	Heeft te maken met de integratie van gewijzigde systemen met bedrijfsbehoeften
FB 29	Internal	Future/innovation & learning	Richt zich meer op de procedure/aanpak dan op producten
TB 13	Internal	Future/innovation &	Richt zich meer op de procedure/aanpak dan op producten

		learning	
INK 6	Corporate contribution	Internal	Beoordeelt een op te leveren product
Deliver & Support			
FB 39	Internal	Corporate contribution	De prestaties van leveranciers worden beoordeeld en vergeleken met plannen/verwachtingen van functioneel beheer
FB 41	Internal	Corporate contribution	Verwachtingen worden vergeleken met wat werkelijk geleverd is
AB 34	Internal	Corporate contribution	Verwachtingen (afspraken) worden vergeleken met wat werkelijk geleverd is
TB 19	Internal	Corporate contribution	Verwachtingen (aangeboden diensten) worden vergeleken met behaalde prestaties
SEC 12	Corporate contribution	Internal	Geen verwachtingen die hieraan ten grondslag liggen
SEC 20	User/customer	Internal	Klanttevredenheid is hier niet aan de orde
SEC 22	Internal	Corporate contribution	Verwachtingen (doelstellingen, principes en maatregelen) worden onder de aandacht gebracht
SEC 34	Corporate contribution	Internal	Geen verwachtingen die hieraan ten grondslag liggen
SEC 49	Internal	Corporate contribution	Om te beoordelen of back-up en restore procedures nog aan de verwachtingen voldoen wordt regelmatig getest
SEC 53	Corporate contribution	Internal	Beveiliging is in overeenstemming met *business needs*
SEC 57	Corporate contribution	Internal	Geen verwachtingen die hieraan ten grondslag liggen

XII. Interview:

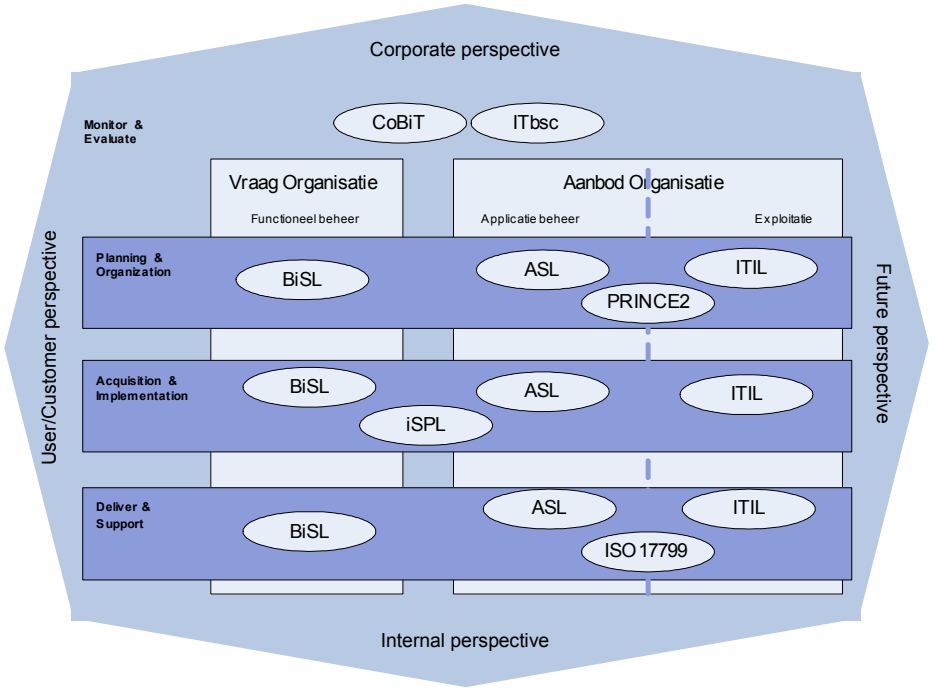
WERKWIJZE TER BEOORDELING IT GOVERNANCE

1.1 Inleiding onderwerp:

IT Governance staat de laatste tijd volop in de belangstelling. Echter heeft dit nog niet altijd geleid tot een hogere kwaliteit van besturing (Governance) van de automatisering (IT) bij organisaties. Het is wel de intentie van organisaties om dit te verbeteren. Door Wilco Leenslag is in het kader van zijn afstuderen aan de Universiteit Twente een werkwijze ontwikkeld met als doel om de kwaliteit van besturing van automatisering op een gestructureerde, overzichtelijke en pragmatische manier te beoordelen gebruikmakend van geaccepteerde methodes (standaarden, best practices, etc).

1.2 IT Governance werkmodel:

Om de werkwijze ***structuur*** te geven is een IT Governance framework ontwikkeld die het mogelijk maakt om verschillende methodes te positioneren ten opzichte van elkaar. De volgende methodes zijn hiervoor geselecteerd: BiSL, ASL, ITIL, PRINCE2, iSPL, ISO17799, CoBiT en ITbsc. In de bijlage van dit document staat een korte omschrijving van de methodes. Wanneer deze methodes worden geplaatst binnen het IT Governance framework ontstaat het volgende model:



Figuur 32: IT Governance werkmodel

De gekozen methodes behandelen verschillende aspecten in een viertal aandachtsgebieden die vanuit een aantal perspectieven benaderd worden. Voor de werkwijze worden de volgende aandachtsgebieden, aspecten en perspectieven onderscheiden:

aandachtsgebieden	**aspecten**		**perspectieven**
Planning & Organisation	Functioneel beheer	(FB)	Corporate contribution
Acquisition & Implementation	Applicatiebeheer	(AB)	Internal/operational
Deliver & Support	Technisch beheer	(TB)	User/customer
Monitor & Evaluate	Projectmanagement	(PM)	Future/innovation & learning
	Inkoop	(INK)	
	Beveiliging	(SEC)	

Tabel 21: Structuur werkwijze

De verschillende methodes zijn gekoppeld aan generieke IT processen (CoBiT) binnen de aandachtsgebieden. Een ***overzichtelijke*** selectie is gemaakt van IT processen die als belangrijk worden beschouwd bij de beoordeling van IT Governance. De volgende IT processen van CoBiT zijn geselecteerd:

PO1 Define a Strategic IT Plan	AI1: Identify Automated Solutions	DS1 Define and Manage Service Levels
PO2 Define the Information Architecture	AI2 Acquire and Maintain Application Software	DS2 Manage Third-party Services
PO3 Determine Technological Direction	AI5 Procure IT Resources	DS4 Ensure Continuous Service
PO4 Define the IT Processes, Organisation and Relationships	AI6 Manage Changes	DS5 Ensure Systems Security
PO6 Communicate Management Aims and Direction	AI7 Install and Accredit Solutions and Changes	DS11 Manage Data
PO10 Manage Projects		DS12 Manage the Physical Environment
ME1 Monitor and Evaluate IT Processes		

Tabel 22: Overzicht van selectie IT processen

De onderdelen van methodes die bovenstaande IT processen ondersteunen zijn vervolgens gebruikt om een IT Governance checklist op te zetten met normen met als doel een ***pragmatische*** werkwijze te realiseren teneinde de kwaliteit van IT Governance te beoordelen. Deze checklist wordt weergegeven op blz 8.

2.1 Inleiding interview:

Het interview bestaat uit twee gedeeltes:

- Het eerste gedeelte bestaat uit het toepassen van de IT Governance checklist (blz. 8) op de organisatie. Hier wordt gevraagd om de beschreven normen elk een score toe te kennen, zoals beschreven in de IT Governance checklist.
- Het tweede gedeelte bestaat uit een vragenlijst (blz. 4). In deze vragenlijst wordt de mening gevraagd over de toepasbaarheid van de IT Governance checklist.

Het is aan te raden om de IT Governance checklist voor aanvang van het interview in te vullen.

2.2 Opbouw vragenlijst:

De vragenlijst voor het interview is als volgt opgebouwd:

1. Algemene onderwerpen om een profiel van de geïnterviewde en organisatie te schetsen.
2. Algemene onderwerpen IT Governance die de toepassing van IT Governance bij de organisatie vast stelt.
3. Onderwerpen over de IT Governance checklist waarbij een oordeel gevraagd wordt over de toepasbaarheid van de lijst.
4. Eindoordeel met vragen over de IT Governance checklist in zijn geheel.

3.1 **Vragenlijst toepassing en beoordeling IT Governance checklist**

1. Algemene onderwerpen:

1.1	Naam organisatie:
1.2	Naam functionaris:
1.3	Functie:
1.4	Grootte van organisatie in aantal medewerkers:
1.5	Grootte van IT organisatie in aantal medewerkers:
1.6	Grootte van organisatie in euro's omzet:
1.7	Grootte van budget IT organisatie:

2. Algemene onderwerpen IT Governance:

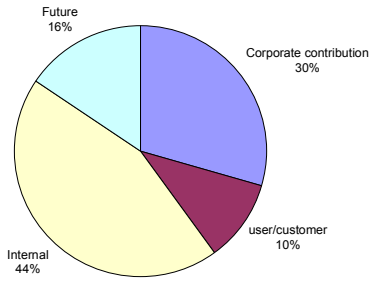
2.1	Is IT Governance *expliciet* toegepast in uw organisatie? Ja: ☐ Nee: ☐
2.2	Op welke (expliciete dan wel impliciete) manier is IT Governance toegepast in uw organisatie?
2.3	Maakt u gebruik van bestaande methodes, best-practices en standaarden om de kwaliteit van besturing van de automatisering te bevorderen (zo ja, welke)?

3. Onderwerpen IT Governance Checklist:

Oordeel structurering checklist:

3.1 Zijn er belangrijke **aandachtsgebieden** en/of IT processen die volgens u ontbreken in de checklist?
3.2 Zijn er belangrijke **aspecten** die volgens u ontbreken in de checklist?
3.3 Zijn er volgens u andere **perspectieven** te onderkennen, die belangrijk zijn bij beoordeling van IT Governance?

Oordeel volledigheid checklist:

3.4	Worden de gekozen **aandachtsgebieden** *en* geselecteerde **IT processen** volgens u gedetailleerd genoeg behandeld?
3.5	Worden de gekozen **aspecten** volgens u door de normen voldoende uitgewerkt?
3.6	Worden alle **perspectieven** volgens u evenwichtig behandeld? Waarbij de verhouding van de checklist als volgt is: 

Oordeel pragmatische toepasbaarheid:

3.7	Is de **checklist** in voldoende mate op nut en bruikbaarheid gericht om de kwaliteit van IT Governance te beoordelen?

4. Eindoordeel:

4.1	Is de IT Governance checklist een goed hulpmiddel om sterke en zwakke punten van IT Governance aan het licht te brengen?
4.2	Bevat de IT Governance Checklist in de ogen van de geïnterviewde onjuistheden?
4.3	Hebt u nog aanvullende opmerkingen dan wel aanbevelingen over het IT Governance werkmodel en de IT Governance checklist?

Bedankt voor uw medewerking

4.1 **IT Governance checklist**

Weggelaten uit deze bijlage.

Bijlage: Beschrijving geselecteerde methodes:

BiSL: functioneel beheer

BiSL is bedoeld als een integraal procesframework voor functioneel beheer en informatiemanagement. BiSL wordt ondersteund door een groeiend aantal best practices. Zoals door Van Outvorst et al. (2005) wordt aangegeven vormt een aantal ontwikkelingen de oorzaak van de toegenomen aandacht voor functioneel beheer. Een belangrijke ontwikkeling is de toenemende professionalisering van ICT-leveranciers en ontwikkelingen op het terrein van outsourcing. Door deze toename van outsourcing is ook de vrijblijvendheid in de relatie tussen opdrachtgever en opdrachtnemer verdwenen. Hiervoor in de plaats zijn zakelijke afspraken en contracten gekomen. De structuur van BiSL onderkent processen op drie niveaus (uitvoerend, sturend en richtinggevend niveau).

Van Outvorst et al. (2005)

ASL: applicatiebeheer

ASL is een leverancieronafhankelijke methode voor de uitvoering van applicatiebeheer. Populair gezegd: de 'Itil voor applicatiebeheer'. Naast een denkwijze en begrippenkader biedt ASL best practices voor de praktische invulling van de werkwijze en een procesmodel. Dit procesmodel is voor de operationele beheerprocessen en enkele sturende managementprocessen op ITIL gebaseerd. Daarnaast bevat het richtinggevende, beleidsmatige processen, waarin wordt aangegeven hoe een ict-leverancier met de klant kan meedenken over de toekomst van diens applicatieportfolio en een eigen dienstenstrategie kan bepalen.

Meijer (2003)

ITIL: exploitatie

De ITIL-methode onderkent een aantal processen op strategisch, tactisch en operationeel niveau. Het biedt een raamwerk waarin de betreffende ICT-beheerprocessen in hun onderlinge samenhang zijn weergegeven. ITIL beschrijft de doelen, belangrijkste activiteiten, inputs en outputs van de verschillende processen. Doelstellingen van bepaalde (CoBiT) IT-processen kunnen gerealiseerd worden met ITIL. Waar CoBiT zegt wat er moet gebeuren, zegt ITIL meer hoe het moet gebeuren. In Nederland ziet men in ICT-organisaties vaak vooral toepassing van de service support en service delivery taken conform ITIL.

Thiadens (2004). Halfhide et al. (2003), Van Grembergen et al. (2004)

PRINCE2: project management

PRINCE2 biedt een raamwerk, waarin de projectmanagementprocessen in hun onderlinge samenhang zijn weergegeven. PRINCE2 beschrijft de doelen, belangrijkste activiteiten, inputs en outputs van de verschillende processen.

Halfhide (2003)

iSPL: inkoop ICT-producten en diensten

Het managen van acquisitie- en procurementtrajecten voor ICT-services (projecten en ongoing services). ISPL biedt een raamwerk voor acquisitie- en procurement-processen en een aantal best practices om deze processen uit te voeren. Doel is ervoor te zorgen dat alle relevante zaken tussen klant en leverancier worden besproken, zodat risico's worden beperkt.

Kernpunten zijn het goed analyseren en beschrijven van de benodigde services, het inschatten van situatiefactoren en risico's en het daarvan afleiden van een strategie voor zowel de uitvoering van de services als de contractering. De best practices zijn vergaand uitgewerkt.

Halfhide (2003)

ISO 17799: security / Code voor Informatiebeveiliging

Een standaard voor information security is de ISO 17799 of de Britse tegenhanger BS7799. deze standaard bevat een uitvoerige set van controls en best practices. De standaard bestaat uit twee delen. Het ene deel is een managementraamwerk en geeft de door een organisatie te nemen maatregelen weer. Het tweede deel legt de eisen vast waarmee derde organisaties kunnen certificeren dat de processen in een organisatie of een gebruikte beveiligingsproduct voldoen aan een bepaalde norm. In Nederland is deze standaard overgenomen in de Code voor Informatiebeveiliging.

Larsen et al. (2006), Thiadens (2004)

CoBiT: control framework

CoBiT is een open standaard die de IT-activiteiten organiseert rond 34 IT-processen. Voor elk proces heeft CoBiT beheerdoelen en corresponderende management guidelines. In deze guidelines staan maturiteitsmodellen en hun corresponderende scorecards in de vorm van key-goal- en key-performance-indicatoren, wat handige insturment zijn in het governancetraject.

Van Grembergen (2004)

IT BSC: Performance measurement

De IT BSC is een effectief instrument om meer integratie tussen business en IT te bereiken (gebaseerd op de BSC van Kaplan en Norton). Het balanced-scorecardconcept kan een echt alignmentinstrument worden door een cascade van scorecards te implementeren. Om dit te bereiken moet een duidelijk relatie bestaan tussen de scorecard voor IT-operaties en die voor IT-ontwikkeling en IT-strategie. De scorecard voor IT-strategie kan dan op zijn beurt verbonden worden met de business balanced scorecard. De cascade van scorecards kunnen gemapped worden op de domeinen die zijn gedefinieerd in het IT Governance model. Elke scorecard onderkent een aantal perspectieven, met de volgende *high level targets*:

Corporate contribution perspective:

providing insights into impacts made by the organization's entire portfolio of IT Investments to achieve the strategic needs of the enterprise as a whole, in contrast to specific individual customers within the enterprise

User/customer perspective:

providing insights in the quality (and cost) effectiveness of IT products and services to satisfy the needs of individual customers

Internal/ operational perspective:

evaluating the operational effectiveness and efficiency of the IT organization itself to fulfil or improve internal IT business performance that delivers IT products and services for individual customers and the enterprise

Future/Innovation & learning perspective:

evaluating the organization's skill levels and capacity to consistently deliver quality results and accomplish ongoing IT innovation and learning as IT grows

Van Grembergen (2004), GAO (1998)

[blanco]

Universiteit Twente
de ondernemende universiteit

ERNST & YOUNG