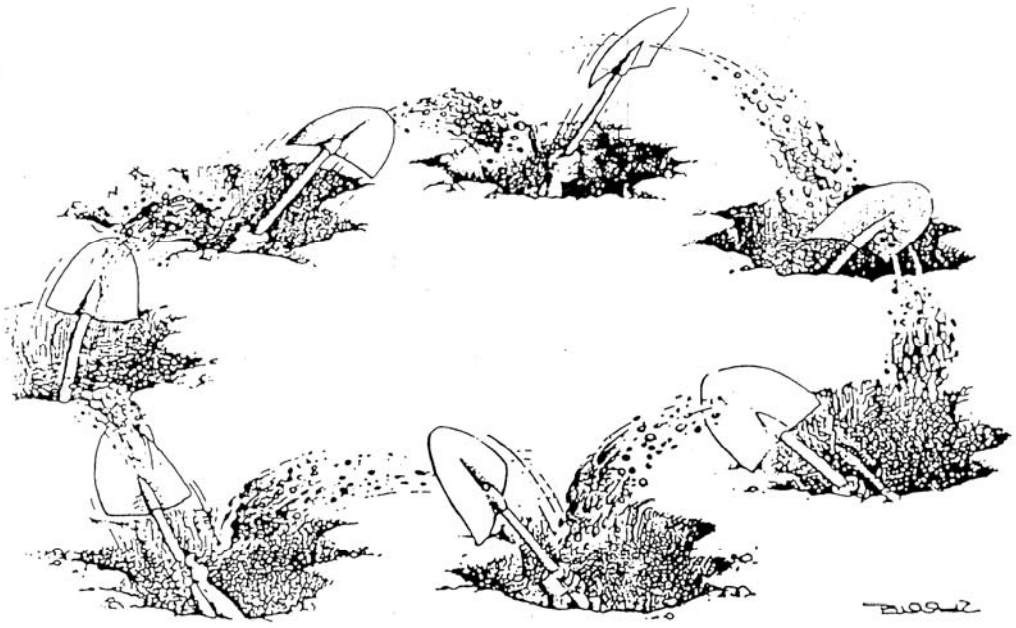
Naar Een Effectieve Werking

‘IT-auditing als kwaliteitsimpuls bij tendertrajecten’

Scriptie ter afronding van de post-graduate opleiding IT-audit aan de Vrije Universiteit te Amsterdam



H. (Henk) J. Huizer
H. (Henry) Westbroek

Amsterdam, 24 mei 2006
Vrije Universiteit Amsterdam
FEWEB, afdeling IT-audit

Voorwoord

IT-audit wordt steeds belangrijker. Of zeggen wij dat nu verkeerd. Is het niet de automatisering die steeds belangrijker wordt in onze maatschappij. Niet alleen voor bedrijven en het strategische nut ervan, maar ook in het dagelijks leven gaan de geautomatiseerde processen een steeds belangrijker rol spelen. Voorbeelden te over. Van onze bankrekeningen tot aan de persoonlijke gegevens in de gezondheidszorg.

Daar de automatisering dus steeds belangrijker wordt, neemt de complexiteit ervan rechtsevenredig toe. En daarmee ook de groeiende behoefte om de werking te garanderen.
Dit garanderen kan alleen door de automatisering te beheersen en daarop te controleren. En een van de exponenten in die controlefuncties is de IT-auditor. Maar door de toegenomen complexiteit is het voortdurend controleren van de gehele automatisering ondoenlijk geworden. De IT-auditor zal dan ook meer selectief ingezet moeten gaan worden. Deze scriptie en haar onderzoek willen aan die selectie een bijdrage leveren.

Deze scriptie is geschreven door twee personen. Althans, dat staat op het voorblad. Maar niets is minder waar. Zonder de hulp en welwillendheid van anderen hadden wij dit niet kunnen doen.

Wij bedanken onze scriptiebegeleiders dr. René Matthijsse, van Verdonck, Klooster & Associates, en drs. Ko van der Sande Re Ra, van de Auditdienst Financiën, voor hun positieve en kundige begeleiding bij het schrijven van onze scriptie. Daarnaast willen wij de medewerkers, met name Peter Bon, van de afdeling inkoopmanagement van de Belastingdienst/Centrum voor Informatie en Communicatietechnologie bedanken voor de gastvrijheid en mogelijkheden die wij hebben gekregen om ons onderzoek te kunnen uitvoeren.

Een studie van meer dan 2 jaar gaat aan je naasten nooit onopgemerkt voorbij. Toen wij hieraan begonnen en aan een collega vroegen of deze opleiding niets voor hem was, antwoordde hij: ‘na mijn laatste studie heb ik mijn gezin plechtig beloofd ze nooit meer met een andere studie te terroriseren’.
Een leuke opmerking en daarin een kern van waarheid.
Lieve familie, bedankt dat wij mochten studeren. Door jullie support werd het succesvol.

Resteert de vraag of je tijdens een studie alles leert en dat de koek daarna op is. Wij denken van niet! Tenslotte luidt een Twents spreekwoord: Je gaat slimmer naar huis dan dat je naar je werk komt.
(*Vrij vertaald vanuit een show van Herman Finkers: ‘Audit is mijn lust en mijn leven).*

Leeswijzer

Deze scriptie bevat een aantal hoofdstukken. Wij hebben geprobeerd de hoofdstukken elkaar zo logisch mogelijk te laten opvolgen.

In Hoofdstuk 1 hebben wij onder meer de inleiding, de hoofdvraag en onderzoeksvragen, hypothese, onderzoeksgebied en methode van onderzoek beschreven.

In Hoofdstuk 2 passeren een aantal basisbeginselen van IT-auditing de revue.

In Hoofdstuk 3 behandelen wij de theorie van het inkoopproces en aanbesteding.

In Hoofdstuk 4 is het veldonderzoek beschreven. Dit veldonderzoek is uitgevoerd voor een viertal geselecteerde tenders. Deze tenders zijn uitgeschreven door de Belasting/Centrum voor Informatie en Communicatietechnologie.

In Hoofdstuk 5 zijn de bevindingen uit de tenders geëvalueerd. Daarna zijn een aantal theoretische basisbeginselen van IT-auditing vergeleken met de praktijk. Tenslotte is hieruit een conclusie getrokken en zijn de onderzoeksvragen beantwoord.

In Hoofdstuk 6 is de hoofdvraag beantwoord en de gestelde hypothese getoetst.

Disclaimer

Ten behoeve van de scriptie is er onderzoek uitgevoerd naar een viertal aanbestedingen bij de rijksoverheid, te weten bij de Belastingdienst/Centrum voor Informatie en Communicatie Technologie. Uit deze aanbestedingen is een selectie gemaakt van voor het onderzoek van belang zijnde gegevens. Dit betekent dat niet alle beschikbare gegevens integraal zijn overgenomen uit de aanbestedingen naar de scriptie.

Derhalve kunnen de gegevens niet voor een ander doel dan het scriptie-onderzoek als opzichzelfstaand feitelijk materiaal gebruikt worden.

Daar verder alleen de IT-auditaspecten voor het scriptie-onderzoek van belang waren zijn de aanbiedende partijen geanonimiseerd. Iedere overeenkomst met bestaande zaken of personen berust derhalve op pure toevalligheid.

Overname en drukfouten blijven te allen tijde voorbehouden.

Inhoudsopgave

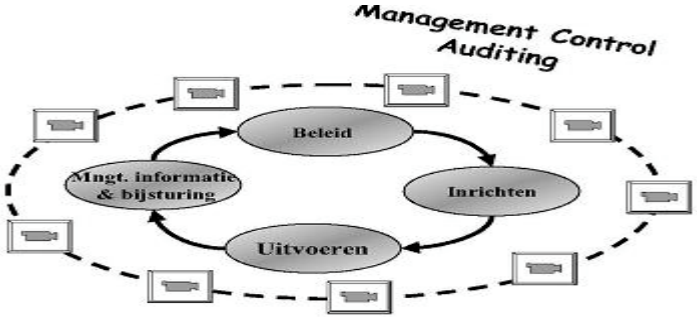
1 Inleiding

1.1 Algemeen

‘Entia non sunt multiplicanda praeter necessitatem’.

Voor het strategisch management staan de te behalen doelen centraal, en daarmee dus ook de risico’s die de realisatie van die doelen bedreigen alsmede de beheersmaatregelen hiervoor. Om een organisatie te beheersen wordt het principe van risicomanagement toegepast. Risicomanagement is het inventariseren van potentiële bedreigingen en risico’s. Vervolgens worden deze bedreigingen en risico’s geanalyseerd en de op te lopen schade gekwantificeerd. Daarna wordt vastgesteld welke risico’s men wenst te mitigeren en welke maatregelen men daarvoor wil treffen. Dat de uitkomsten van risicomanagement niet door iedereen begrepen worden, blijkt bijvoorbeeld uit een kamerbehandeling van de verantwoording van het Ministerie van Justitie. Het werkelijke aantal ontsnappingen uit de gevangenissen lag uiteindelijk lager dan vooraf verwacht en als een geaccepteerd risico in de begroting was aangegeven. Dit leverde de volgende vraag op: ‘waarom zijn er maar 15 ontsnappingen geweest, terwijl u dacht dat het er 20 zouden zijn’.

Bij risicomanagement vormt auditing een hulpmiddel om de zekerheid te verschaffen dat de juiste beheersmaatregelen bij de onderkende risico’s zijn getroffen of getroffen worden. IT-audit is daarbij ondersteunend voor het functioneren en in stand houden van het *internal control framework* van een bedrijf en IT-audit kan in voorkomende gevallen beschouwd worden als een managementinstrument. Het management maakt hierbij gebruik van het ‘plan-do-check-act’ principe.



(Bron: Presentatie 02, Auditing, Vu Amsterdam, 2004, ACS). Dit werkt als volgt: aanbevelingen leiden tot bijstelling van beleid, beleidsbijstellingen leiden tot bijstelling van organisatie en/of procedures. Deze cyclus ondersteunt het management bij het behalen van gestelde doelen in een controlerende - en/of monitoringsfunctie.

Bedrijven en overheden worden steeds afhankelijker van IT. Daarmee worden zij ook steeds kwetsbaarder indien er iets mis gaat met de verwerking, opslag en beschikbaarheid van de aanwezige data en ICT infrastructuur. Een raamwerk van technische, organisatorische en procedurele maatregelen moet de benodigde waarborgen scheppen om gevrijwaard te worden van “onheil”. En bij voorvallen moet men binnen een door de organisatie of de maatschappij aanvaardbare termijn de situatie weer meester zijn. IT-audit heeft ten opzichte van dit raamwerk een functie. Deze is tweeërlei. Enerzijds is het een specifieke ‘interne controle’ functie, zeg maar een controlerende - of monitoringsfunctie. De werkzaamheden van deze functies komen tot uitdrukking in het beheersingsraamwerk van een ICT-omgeving. Anderzijds heeft IT-audit ook een adviserende functie en kan er, vanuit het perspectief van beheersing van

de ICT-organisatie, behoefte zijn aan de adviesfunctie bij verwerven van ICT-producten. De inzet van IT-audit zal zich dan voornamelijk richten op het uitbrengen van advies over de impact van de verwerving van product X op de organisatie. De functie van interne controle is hier minder van toepassing daar het vaak om advisering ten opzicht van een aan te kopen product gaat en minder om de controle op aankoopproces zelf.

Voor het gebruik en inzet van IT-audit in het beheersingsraamwerk als instrument moeten er keuzes worden gemaakt. Om keuzes te kunnen maken moeten er nog wel een aantal vragen beantwoord worden. Een van die vragen is dat als IT-audit zijn plaats heeft in het beheersingsraamwerk, vastgesteld moet worden of er ook behoefte is aan IT-audit bij verwerving van ICT-producten. En zo ja, dan is er ook de vraag op welke wijze IT-audit daarbij ingezet kan of moet worden.

Vooral bij het beantwoorden van de laatste vraag kan er sprake zijn van een dilemma. Bij het aankopen van ICT-producten door middel van tendertrajecten kan er behoefte zijn aan de inzet van IT-audit. Een van de dilemma's is dat er sprake kan zijn van beperkte capaciteit van IT-audit. Een issue is dan: 'In welke tendertrajecten is IT-audit relevant en welke bijdrage wordt er verwacht'. Het dilemma dat IT-audit niet als effectief wordt gezien is een managementissue. De taken die auditmedewerkers uitvoeren dienen bij te dragen aan het behalen van de doelstellingen van een organisatie. Vanuit dat oogpunt bezien moeten door het management keuzes gemaakt worden over de inzet van IT-audit.

Maar naast de geschetste dilemma's is het vooral de vraag of gebruik van IT-audit in voortrajecten, zoals tenders, leidt tot een effectievere inzet van IT-auditcapaciteit. De vraagstelling die ontstaan is door een gebrek aan IT-auditcapaciteit en de bijbehorende dilemma's hebben geleidt tot het schrijven van deze scriptie.

1.2 De IT-auditor in het voortraject

Met de onderkenning dat IT en haar toepassingen een belangrijke schakel vormen in de bedrijfsvoering en de realisatie van de organisatiedoelstellingen mag de beheersing van IT zich verheugen in een warme belangstelling van IT-auditors. Andersom is ook waar. Door het toenemende belang van de IT en haar toepassingen voor de bedrijfsvoering is de behoefte aan beheersing van bedrijfskritische automatiseringsprocessen toegenomen. Uit deze toename is de behoefte ontstaan aan IT-auditors. Maar keerzijde van de medaille is dat omvang en complexiteit van de ICT omgeving een dusdanige omvang heeft gekregen dat het continu auditten van IT-processen niet meer doelmatig kan worden genoemd.

Op basis hiervan gaan er steeds meer geluiden op die de IT-auditor in het voortraject willen betrekken. Onder voortrajecten worden over het algemeen de processen bedoeld waar nieuwe automatiseringstoepassingen hun intrede doen in een bedrijf, bijvoorbeeld:
- Invoeringsprojecten nieuwe bedrijfsapplicaties.
- Dataconversies naar nieuwe databases.
- Due dilligence onderzoeken bij bedrijfsovernames.
- Beheersingsvraagstukken bij aanbestedingstrajecten.

Door, voorafgaand aan invoering in de feitelijke automatiseringsomgeving, IT-audit in te zetten kunnen latere complexe beheersingsvraagstukken opgelost worden. Immers, door in voortrajecten op deelgebieden beheersingsvraagstukken op te nemen wordt later onevenredige 'effort' in de beheersing voorkomen.

1.3 Onderzoeksgebied

Naar aanleiding van deze aaneenschakeling van argumenten en veronderstellingen, zou

de mening gepositioneerd kunnen worden dat IT-audit ingeschakeld moet worden bij voortrajecten van vernieuwingen in de automatiseringsomgeving. Afgaande op het voorgaande zou dat dan klakkeloos overgenomen kunnen worden. Maar klakkeloos IT-audit inzetten op basis van veronderstellingen leidt tot versnippering en niet tot doelmatigheid. Derhalve is het wenselijk dat veronderstellingen en argumentatie onderzocht worden op hun houdbaarheid. Dit heeft geleidt tot het onderzoeken van een deelgebied van de verzameling voortrajecten, te weten: IT-audit in relatie tot een tendertraject.

1.4 Probleemstelling

De onderzoeksvraag is gestoeld op een praktisch relevant probleem, te weten capaciteitsgebrek bij de Auditdienst Financiën. De Auditdienst Financiën voert audits uit in het kader van de controle op de jaarrekening van de Belastingdienst. In de loop der jaren is de omvang en complexiteit van de automatiseringsomgeving bij de Belastingdienst enorm toegenomen. Dit maakt het uitvoeren van audits op alle deelgebieden uitgebreid, tijdrovend en in principe ondoenlijk. Ook is de IT-auditcapaciteit daarvoor niet toereikend.

De beperking in IT-audit capaciteit en de keuzes die er gemaakt moeten worden hebben geleidt tot een onderzoeksvraag en daaruit gevolgde subvragen.

1.5 Hoofdvraag en onderzoeksvragen

Onze hoofdvraag luidt:

‘Is het inzetten van IT-audit in tendertrajecten wenselijk, bezien vanuit het perspectief van beheersing’.

Volgend op deze hoofdvraag kunnen er onderzoeksvragen geformuleerd worden:
1 Komen IT-auditaspecten tot uiting in een tendertraject.
2 Zijn IT-auditaspecten van invloed in een tendertraject.
3 Wat zijn de gevolgen voor de organisatie en beheersingsvraagstukken voor een automatiseringsomgeving als IT-auditaspecten niet erkend worden in tendertrajecten.
4 Is het inzetten van IT-audit in ieder willekeurig tendertraject noodzakelijk.

1.6 Hypothese

De hypothese die getoetst zal worden, luidt:

‘Kan, om IT-auditcapaciteit zo effectief mogelijk te benutten, een optimaal inschakelmoment bepaald worden voor tendertrajecten’.

1.7 Methode van onderzoek

De toegepaste methode van onderzoek is:
1 Formuleren van het onderzoeksgebied, hypothese en onderzoeksvragen.
2 Verzamelen, bestuderen en beschrijven van literatuur op het gebied van IT-audit principes en tendertrajecten.
3 Uitvoeren van veldonderzoek.
4 Evalueren van de bevindingen uit het veldonderzoek.
5 Het extraheren van conclusies uit bevindingen en de theorie.
6 Beantwoorden van de onderzoeksvragen en toetsen van de hypothese.

1.8 Samenvatting

In ons scriptieonderzoek willen we vaststellen of het voor de Auditdienst Financiën, vergelijkbaar met ieder andere interne auditdienst, effectief is om audits in te stellen in tendertrajecten en op welke momenten die audits dan het beste tot hun recht komen.

Wij proberen onze conclusies breder toepasbaar te maken dan alleen voor de Belastingdienst.

2 Principles of IT-Auditing

2.1 Algemeen

IT-auditors maken bij het uitvoeren van hun werkzaamheden gebruik van algemeen aanvaarde IT-auditwerkwijzen en algemeen aanvaarde IT-auditgrondslagen. In dit hoofdstuk zullen een aantal basisprincipes van IT-audit beschreven worden. Deze basisprincipes vormen de uitgangspunten voor de aanpak en methodiek van IT-audit. De volgende basisprincipes behoren tot het erfgoed van IT-audit;

- IT-auditgrondslagen;
  - Normenkader
  - Kwaliteitsaspecten
- Auditmethoden;
  - Wijze van onderzoek
  - Audittechniek
- Auditproducten;
  - Oordeel
  - Advies
  - Aanbevelingen
- Product-audit en proces-audit.
- Auditrisk.

2.2 IT-auditgrondslagen

2.2.1 Gebruik van normenkaders

De IT-auditor maakt voor zijn onderzoek gebruik van normenkaders. Deze normenkaders bevatten voor zijn onderzoek de meetpunten waartegen hij het object van onderzoek afzet. Bevindingen zijn de uitkomsten van dit proces. Naar aanleiding van bevindingen kunnen er conclusies getrokken worden. Interpretatie van geconstateerde verschillen kunnen leiden tot aanbevelingen en tot het treffen van maatregelen. Dit om de geconstateerde verschillen op te heffen, maar uitkomsten kunnen soms ook leiden tot een gewijzigd inzicht in de vastgestelde norm.

Normenkaders kunnen op diverse manieren ontstaan. Ze kunnen opgesteld worden aan de hand van een verstrekte opdracht. In zo'n geval komt het normenkader voort uit de opdracht. De opdrachtgever geeft in zijn opdracht een verwachting mee waaraan het te auditten object dient te voldoen. Deze normen kunnen bijvoorbeeld een afgeleide van het bedrijfsbeleid zijn. Het is de taak van de IT-auditor om de normen van de opdrachtgever vaktechnisch te toetsen. Aan de andere kant kan er aan de IT-auditor ook een opdracht verstrekt worden om een object te auditten aan de hand van normenkaders van derden. Voorbeelden hiervan zijn: wetgeving, voorschriften, 'best practices', algemeen aanvaarde verwachtingen (bijvoorbeeld een wasmachine, waarvan wordt verwacht dat deze wasgoed schoon wast). Het is dan de taak van de IT-auditor

om de verwachting van de opdrachtgever of opgelegde kaders van derden om te zetten in te hanteren normen (concretiseren). De IT-auditor stelt de normen vast, waaraan het te auditten object moet voldoen. Wel dient de IT-auditor het vastgestelde normenkader af te procederen met zijn opdrachtgever. Een norm dient altijd concreet en toetsbaar te zijn. (*Bron: Inleiding EDP-auditing van Jan van Praat en Hans Suerink, 5e druk 2004*).

2.2.2 Kwaliteitsaspecten

Kwaliteit laat zich definiëren als:
'Het geheel van vanzelfsprekende of vastgelegde behoeften waaraan een product of dienst moet voldoen'*. (Bron Inleiding EDP-audit, Jan van Praat, Hans Suerink, 5e druk, 2004).*

Kwaliteit heeft veel aspecten. De kwaliteitsaspecten voor IT-auditors zijn als volgt gedefinieerd:

- Effectiviteit: de mate waarin een object in overeenstemming is met de eisen en doelstellingen van de gebruikers en de mate waarin een object bijdraagt aan de organisatiedoelstellingen, zoals die in de informatiestrategie zijn vastgelegd.
- Efficiëntie: de verhouding tussen de gerealiseerde kosten en de begrote kosten van een object. De begrote kosten zijn daarbij de kosten die voorgenomen zijn voor het realiseren van het uit de organisatiedoelstellingen voortvloeiende gewenste prestatieniveau van het object.
- Exclusiviteit: de mate waarin uitsluitend geautoriseerde personen of apparatuur via geautoriseerde procedures en beperkt bevoegdheden gebruik maken van IT-processen.
- Integriteit: de mate waarin het object (gegevens en informatie-, technische- en processystemen) in overeenstemming is met de afgebeelde werkelijkheid.
- Controleerbaarheid: de mate waarin het mogelijk is kennis te verkrijgen over de structurering (documentatie) en werking van een object. Tevens omvat het kwaliteitsaspect controleerbaarheid de mate waarin het mogelijk is vast te stellen dat de informatieverwerking in overeenstemming met de eisen ten aanzien van de overige kwaliteitsaspecten is uitgevoerd.
- Continuïteit: de mate waarin een object continu beschikbaar is en de gegevensverwerking ongestoord voortgang kan hebben.
- Beheersbaarheid: de mate waarin het object kan worden aangestuurd en/of bijgestuurd, zodat het object bij voortduring aan de daaraan gestelde eisen voldoet of kan voldoen.

(Bron: NOREA Geschrift No. 1)

De IT-auditor voert zijn audit uit op basis van kwaliteitsaspecten en normenkaders. De IT-auditor vertaalt de vraag van zijn opdrachtgever naar kwaliteitsaspecten, het kwaliteitsniveau, waaraan het te auditten object dient te voldoen. In het kader daarvan zal hij dan normenkaders opstellen om de kwaliteit van het te auditten object te meten. Zo zal hij bij een opdracht, waarin gevraagd wordt te onderzoeken of gegevens alleen door toegestane functionarissen geraadpleegd kunnen worden, vertalen naar het kwaliteitsaspect 'Exclusiviteit'. Hij zal voor het te onderzoeken kwaliteitsniveau de deelaspecten identificatie, authenticatie en autorisatie gebruiken voor de toetsing van zijn normenkader. Een norm kan dan zijn: gegevens mogen alleen benaderd kunnen worden door daartoe aangewezen functionarissen.

De kwaliteitsaspecten Exclusiviteit, Integriteit, Controleerbaarheid en het deelaspect Beschikbaarheid worden in het Anglo-Amerikaans aangeduid als: C(onfidentiality), I(ntegrity), A(vailability) en A(uditebility). Voor het onderzoek, in het kader van deze scriptie, zijn deze kwaliteitsaspecten geclusterd in een gecombineerd aspect:

databenadering (CIAA). De overige kwaliteitsaspecten, Effectiviteit, Efficiency, Continuïteit en Beheersbaarheid zijn geclusterd als het gecombineerde aspect: beheersaspecten.

2.3 Auditmethoden

2.3.1 Wijze van onderzoek

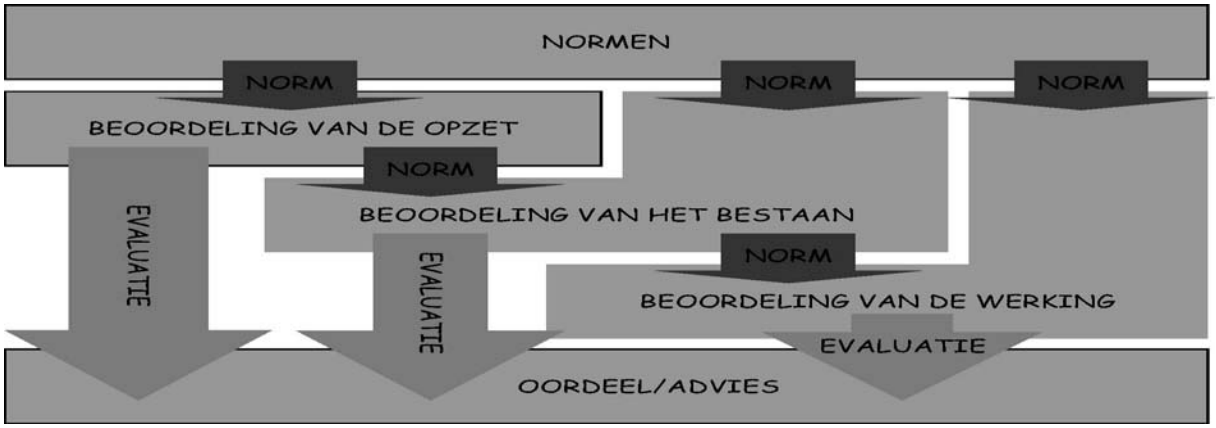
Na het verkrijgen van de opdracht zal de IT-auditor zijn auditplan opstellen. In het auditplan zal de IT-auditor een uitwerking geven van de opdracht waarin hij rekening houdt met diverse facetten zoals:

- Bedrijfsprocessen.
- Toegepaste informatietechnologie.
- Scope of reikwijdte van het onderzoek en kwaliteitsaspecten.
- Object van onderzoek.
- Auditrisk en materialiteit.
- Aard, omvang en tijdstip van de uit te voeren werkzaamheden.

(*Bron: NOREA Studierappport nr 2, 1997*).

In het kader van zijn onderzoek zal de IT-auditor zijn werkzaamheden zodanig inrichten dat voldoende bewijslast verkregen zal worden. Dit om zijn conclusies te onderbouwen, zijn oordeel en de daaruit eventueel voortvloeiende aanbevelingen te funderen. De bewijslast moet voldoende, betrouwbaar en relevant zijn.

De IT-auditor zal zijn onderzoek uitvoeren middels de methode van opzet, bestaan en werking.



In eerste aanleg zal de IT-auditor de opzet en inrichting van het te auditten object beoordelen. Komt de IT-auditor na deze beoordeling tot de conclusie dat het object in opzet voldoet aan de gestelde normen, dan zal hij het onderzoek voortzetten naar de periferique van het bestaan van het object. Dit mits zijn opdracht daartoe strekt. Komt de IT-auditor echter tot de slotsom dat het object in opzet reeds als onvoldoende gekwalificeerd moet worden, dan zal hij als zodanig het onderzoek beëindigen en navenant rapporteren en adviseren. Wordt, na beoordeling van het bestaan van het object, de conclusie getrokken dat het object als voldoende gekwalificeerd kan worden in zijn bestaan dan kan de IT-auditor nog de werking van het object beoordelen. Het beoordelen van de werking van een object is geen momentopname, maar een beoordeling van de wijze waarop een auditobject gedurende een bepaalde periode heeft gefunctioneerd (*Bron: Lesbrief 02, Auditing, VU Amsterdam, 2004*).

2.3.2 Audittechniek

Audittechnieken worden ingezet om audit evidence te verzamelen voor het auditonderzoek. In het auditonderzoek hebben de fasen opzet, bestaan en werking, elk hun geëigende audittechniek.

De audittechniek in de fase opzet kenmerkt zich vooral door toepassing van dossieronderzoek en het inwinnen van inlichtingen bij de gecontroleerde. Voor het dossieronderzoek wordt gebruik gemaakt van de audittechniek zoals het onderzoeken van documenten of bescheiden. Bij dit dossieronderzoek is het van belang dat deze documenten of bescheiden geverifieerd worden in de mate van betrouwbaarheid. De mate van betrouwbaarheid van de verkregen informatie is afhankelijk van de afstemming met andere interne en/of externe documenten. Van belang is daarbij de aard en de bron van de verkregen informatie, alsmede de effectiviteit van de interne controlemaatregelen waaraan deze bescheiden zijn onderworpen. Het inwinnen van inlichtingen bestaat uit de technieken van interview, enquête verhoor, etc.. Op basis van deze audit evidence zal de IT-auditor het object van onderzoek in opzet evalueren.

De audittechniek, in de fase bestaan, kenmerkt zich door toepassing van lijncontroles en eigen waarnemingen. De lijncontrole bestaat uit het verzamelen van bewijsstukken zoals facturen, notulen van vergaderingen, organisatieschema, parameterinstellingen, etc.. De uit te voeren lijncontroles kunnen zowel procesgericht als productgericht zijn. De eigen waarneming bestaat uit het optekenen van ingestelde parameters, oogtoezicht, uitvoeren van inventarisatie, cijferbeoordeling, etc.. Vanzelfsprekend geldt ook in deze fase dat de verzamelde bewijsstukken geverifieerd moeten worden naar de mate van betrouwbaarheid. De audittechniek 'eigen waarneming' dient uitermate zorgvuldig te worden gedocumenteerd, liefst onderbouwd met documentatie. Ook hier zal de IT-auditor op basis van de auditevidence het object van onderzoek in het bestaan ervan evalueren.

De audittechniek in de fase werking kenmerkt zich door toepassing van waarnemingen en het leggen van totaalverbanden over een periode. De waarnemingen kunnen verricht worden met behulp van bijvoorbeeld een steekproef op de uitkomsten van processen of het verzamelen van bescheiden over het functioneren van processen in een periode. Onder periodieke waarnemingen worden tevens eigen waarnemingen verstaan. De totaalverbanden over een periode kunnen bestaan uit een cijferbeoordeling maar ook het gebruik van een netwerk van controletotalen valt hieronder. Op basis van de verzamelde audit evidence zal de IT-auditor het object van onderzoek voor zijn werking beoordelen. (*Bron: Lesbrief 02, Auditing, VU Amsterdam, 2004*).

2.4 Auditproducten

2.4.1 Oordeel

Na het verzamelen van voldoende bewijsmateriaal zal de IT-auditor een onafhankelijk, onpartijdig en consistent oordeel vormen. Het oordeel zal altijd voor een deel subjectief zijn en onderhevig aan menselijke beperkingen. Het oordeel bevat alle materiele afwijkingen tussen de norm en de geconstateerde werkelijkheid.

In alle gevallen doet de IT-auditor geen uitspraak over toekomstige perioden, maar heeft zijn oordeel betrekking op de achterliggende beoordeelde periode, of over de situatie zoals hij die op enig moment heeft aangetroffen. De werkzaamheden van de IT-auditor zijn gericht op het verkrijgen van een redelijke mate van zekerheid betreffende het onderzochte object.

2.4.2 Aanbevelingen

Het rapport bevat als bijlage, de bevindingen, conclusies en aanbevelingen afgezet ten opzichte van de getoetste norm. Daarnaast kan er sprake zijn geweest van een adviserende opdracht, zonder oordeelsvorming, en hebben aanbevelingen de status van advisering.

Aanbevelingen komen voort uit de optiek om de gaten die zijn gesignaleerd tussen de norm en de geconstateerde werkelijkheid te dichten. Ze zijn erop gericht om de bedreigingen en de daaruit voortvloeiende risico's voor een organisatie te verminderen.

2.5 Product-audit en proces-audit

2.5.1 Definitie en onderscheid

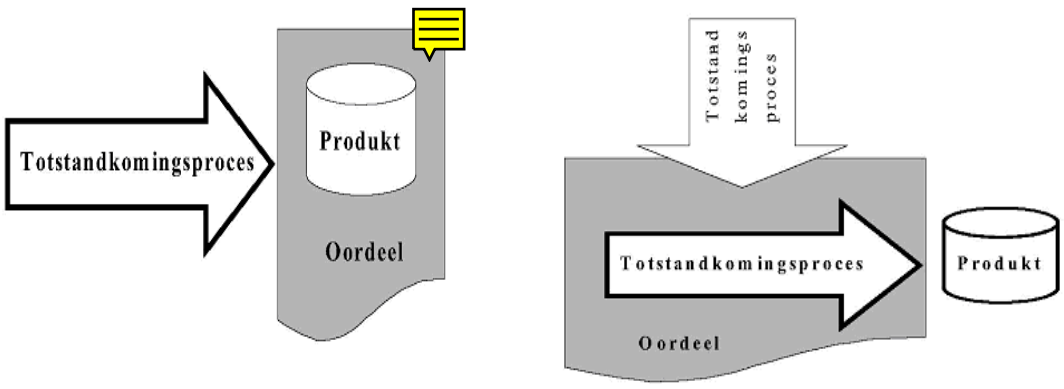
Zoals vooraf al gesteld is, is een goede definitie van het auditobject van groot belang. Immers, naar aanleiding van het vastgestelde auditobject (deel van de scope) vindt de acceptatie van de opdracht plaats, wordt het plan van aanpak opgesteld en de audit uitgevoerd. Waarna een oordeel wordt gegeven over het desbetreffende auditobject. Desondanks blijft een goede afbakening van het auditobject in de praktijk vaak achterwege. Een veel voorkomend onderscheid dat niet wordt gemaakt, is de afbakening tussen een product als auditobject en een proces als auditobject. Bij dit laatste is de audit gericht op de voorafgaande totstandkoming van een product, het proces. Tussen deze twee auditobjecten, een product of een (totstandkomings)proces, bestaan wezenlijke verschillen.

In veel gevallen is het de opdrachtgever te doen om een oordeel te verkrijgen over een product. Voorbeelden hiervan zijn: de controle van de jaarrekening en de beoordeling van een technisch ontwerp. Soms vraagt de opdrachtgever om een oordeel over een (totstandkomings)proces. Voorbeelden hiervan zijn: de audit op een tendertraject en de audit op een systeemontwikkelingsproces. Hierbij moet worden opgemerkt dat daarbij doorgaans geen oordeel wordt gegeven over de uitvoerders van het proces, maar over de opzet en inrichting van het proces (dit laatste is strikt genomen op zichzelf weer een product).

2.5.2 Product versus proces

Producten en processen kunnen nauw met elkaar samenhangen en dit kan voor onduidelijkheid zorgen. Want, een product kan immers het resultaat van een proces zijn.

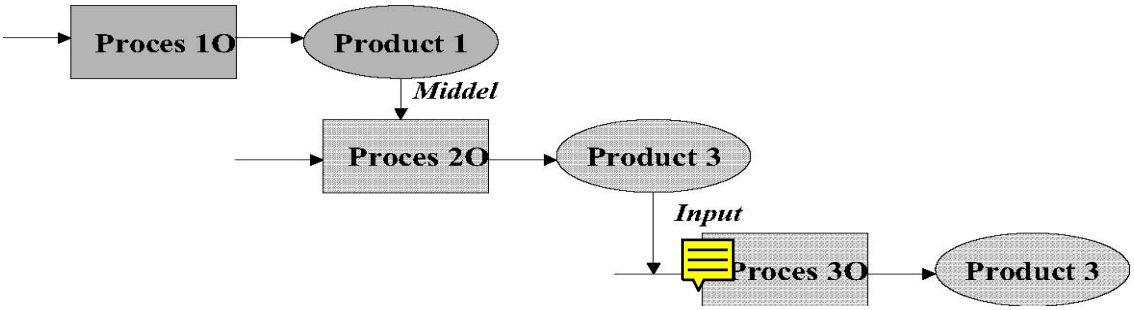
Product audit **Proces audit**



In het vakgebied van IT-auditing worden vier componenten onderscheiden:
- Product;

- Proces;
- Structuur;
- Middelen.

Doorgaans wordt de structuur, welke bestaat uit functies, afdelingen, personen, en middelen, beschouwd als onderdeel van het proces. Bij een proces-audit worden deze componenten dan ook meestal meegenomen. Hierbij moet worden opgemerkt, dat ten aanzien van de structuur, dit specifiek is voor een organisatieonderzoek en alleen in voorkomende gevallen bij een proces-audit wordt meegenomen. De samenhang tussen processen en producten kan als volgt worden weergegeven:



De kwaliteit van product 1 O is afhankelijk van proces 1 en daarmee van de kwaliteit van proces 1. De kwaliteit van product 2 is afhankelijk van de kwaliteit van proces 2 O. De kwaliteit van proces 2 O is mede afhankelijk van de kwaliteit van product 1 en dus indirect ook van de kwaliteit van proces 1. Enzovoort.

Wordt aan een IT-auditor gevraagd om een oordeel te geven over een specifiek product, dan is het mogelijk het daaraan voorgaande proces mede te onderzoeken. Expres wordt hier het woord ‘mede’ gebruikt omdat in die gevallen het alleen beoordelen van het (totstandkomings)proces onvoldoende zou zijn. Dit wordt veroorzaakt door de wetenschap dat een goed proces niet automatisch leidt tot een goed product als gevolg van de regel: garbage in, garbage out.

Daarnaast is het van belang zich te realiseren dat de inhoudelijke betekenis van een kwaliteitsaspect afhankelijk is van het auditobject waartegen het wordt afgezet. Een voorbeeld daarvan is het kwaliteitsaspect continuïteit. Het is goed mogelijk de continuïteit van een proces te beoordelen, maar dit laat zich niet vertalen naar een product. Bij een product spreken we van beschikbaarheid. Derhalve kan een audit naar de waarborgen van de beschikbaarheid van een product, bijvoorbeeld uitgaande facturen, een bredere scope hebben dan een audit van alleen een geautomatiseerd factureringsproces. Immers, discontinuïteit van het proces behoeft niet te impliceren dat de facturen niet meer beschikbaar komen. Er kan dan sprake zijn van alternatieve processen, bijvoorbeeld handmatig opstellen van facturen.

Het is belangrijk dat de IT-auditor dit onderscheid maakt voorafgaand aan de uitvoering van de audit. (*Bron: Lesbrief 02, Auditing, VU Amsterdam, 2004*).

2.6 Auditrisk

Door middel van het geven van een oordeel, waarin de materiële afwijkingen tussen norm en werkelijkheid worden meegenomen, geeft de IT-auditor invulling aan de doelstelling van de audit. Deze doelstelling is de opdrachtgever een redelijke mate van zekerheid te geven. Bij het hanteren van het begrip ‘een redelijke mate van zekerheid’ bouwt de IT-auditor een zekere tolerantie in. Ofwel, er zal altijd sprake zijn van enige mate van onzekerheid.

Tolerantie heeft met risicoanalyse te maken. Hierbij is er een onderscheid tussen de begrippen risico en analyse. Er is sprake van een risico wanneer de kans dat een voorval optreedt groter is dan nul. Het begrip analyse hangt samen met een systematische en gestructureerde aanpak van risico's. Van een dergelijke aanpak is sprake wanneer risico's worden onderkend, geïnventariseerd en geëvalueerd en op basis daarvan conclusies getrokken kunnen worden.

De definitie van risicoanalyse luidt dan ook:
'Risicoanalyse is het op systematische wijze onderkennen en inventariseren van mogelijk optredende ongewenste gebeurtenissen en evalueren van maatregelen tegen het geschieden van gebeurtenissen en schadebeperking, zodat hieruit onderbouwde conclusies getrokken kunnen worden'.
Het is mogenlijk alle aspecten van risicoanalyse in een model samen te voegen. In dit model kunnen dan drie vormen van risico's onderscheiden worden;
- het inherente risico
- het beheersingsrisico
- het ontdekkingsrisico

Deze risico's tezamen vormen de auditrisk.

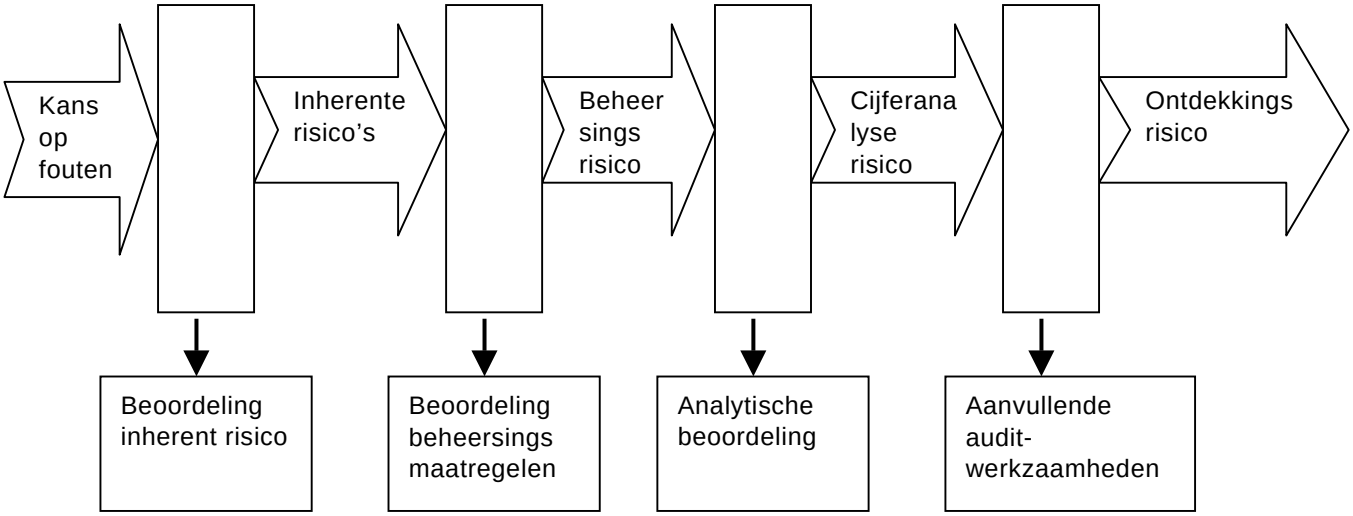
<u>Inherent risico</u>
Het inherente risico heeft betrekking op de mate waarin een onderzoeksobject gevoelig is voor storingen. Dit zijn de risico's die direct samenhangen met het gebruik van een bepaald object.
Om het inherente risico tot een acceptabel niveau terug te brengen zal men maatregelen moeten nemen. Het gaat hier om beheersingsmaatregelen. Maar hoewel men een groot scala aan maatregelen kan nemen, blijft er altijd het risico bestaan dat er iets fout gaat. Met andere woorden, in het verlengde van de beheersingsmaatregelen ligt een beheersingsrisico.

<u>Beheersingsrisico</u>
Het beheersingsrisico is het risico dat optreedt en de schade die men kan oplopen indien de beheersingsmaatregelen, getroffen om het inherente risico af te dekken, niet of onvoldoende functioneren.
De grootte van het beheersingsrisico is afhankelijk van een tweetal factoren:
1 De structuur van de beheersingsmaatregelen; men heeft meerdere mogelijkheden c.q. de keuze tussen een combinatie van beheersingsmaatregelen;
2 De werking van de beheersingsmaatregelen; ook al heeft men een bepaald uitgangspunt bij het instellen van beheersingsmaatregelen, uiteindelijk kunnen de ingestelde maatregelen wel eens niet zo werken als men in eerste aanleg bedoeld heeft.

Een organisatie kan de IT-auditor vragen een onderzoek te doen naar de kwaliteit van de beheersingsmaatregelen. Echter, tijdens zo'n onderzoek bestaat de kans dat de auditor bepaalde risico's niet ontdekt, het ontdekkingsrisico.

Ontdekkingsrisico
De kans dat fouten door onderzoek van de IT-auditor niet ontdekt worden.

Uit het voorgaande blijkt dat er een relatie is tussen de verschillende risico's enerzijds en auditwerkzaamheden anderzijds en leiden tot de Auditrisk. (*Bron: Inleiding EDP-auditing van Jan van Praat en Hans Suerink, 5e druk 2004).*



3 Tendertrajecten: Quest ce que c'est?

3.1 Inleiding

Aangezien aanbesteding niet meer is dan een bijzondere vorm van inkoop verdiepen we ons eerst in het logisch model zoals beschreven door Starreveld cs.. Vervolgens bezien we een theoretische beschrijving van een tendertraject. Tenslotte besteden we enige aandacht aan de regelgeving omtrent aanbestedingen.

3.2 Conceptueel inkoopmodel van Starreveld

3.2.1 Introductie

Starreveld beschrijft uitgebreid de controletechnische functiescheiding die in een organisatie aanwezig moet zijn. Deze controletechnische functiescheiding werkt namelijk ondersteunend aan de betrouwbaarheid van de bestuurlijke informatievoorziening. De controletechnische functiescheiding is daarmee een noodzakelijk gevolg van het delegeren van taken binnen de organisatie. De controletechnische functiescheiding volgens Starreveld maakt onderscheid in de functies:
- Beschikken.
- Bewaren.
- Registreren.
- Uitvoeren.
- Controleren.

Voorbeelden hiervan zijn:
- De Inkoopfunctie is een beschikkende functie (mutaties in goederenvoorraad, genieten van diensten van derden, mutatie in financiële verhoudingen).
- De bestelafdeling is een uitvoerende functie.

Tezamen hebben zij als doel: verwerven van goederen en diensten op de voor het

bedrijf meest doelmatige wijze.

3.2.2 Functie en activiteiten van de inkoopafdeling

Delegatie van de inkoopfunctie gaat gepaard met het stellen van algemene regels ten aanzien van goederen die mogen worden aangekocht, functionarissen op wier verzoek orders mogen worden geplaatst, limieten waarboven machtiging moet worden verleend en procedures voor het aanvragen van offertes of het plaatsen van bestellingen.

Voor menig bedrijf is er aanleiding tot een zelfstandige functionalisatie van de inkoop, waarmee bedoeld is, dat de inkoop niet onder één van de overige functies wordt weggestopt. Bij een toenemende omvang van de organisatie, een hoge graad van verantwoordingsbehoefte of bij een markt waar specialistische kennis nodig is, zal een dergelijke zelfstandigheid van een inkoopafdeling vaker voorkomen. Specialistische kennis kan een product betreffen, maar ook de kaders, bijvoorbeeld het Europese aanbestedingsrecht of de ICT.

Uit het oogpunt van interne controle verdient het in het algemeen de aanbeveling de inkoopfunctie niet op te dragen aan functionarissen die belast zijn met:
- De ontvangst, de bewaring, het verbruik of de verkoop van de in te kopen goederen.
- De fiattering of de effectuering van betalingen aan leveranciers.
- De verzorging van de administratie aan de hand waarvan controle wordt uitgeoefend op het inkopen zelf, op de juiste en volledige verantwoording van alle uit de inkopen voortvloeiende activiteiten, alsmede op de aanwezigheid van alle per saldo uit die activiteiten voortvloeiende bezittingen en schulden.
- De uitvoering van één of meer van de in het vorige punt genoemde controles.

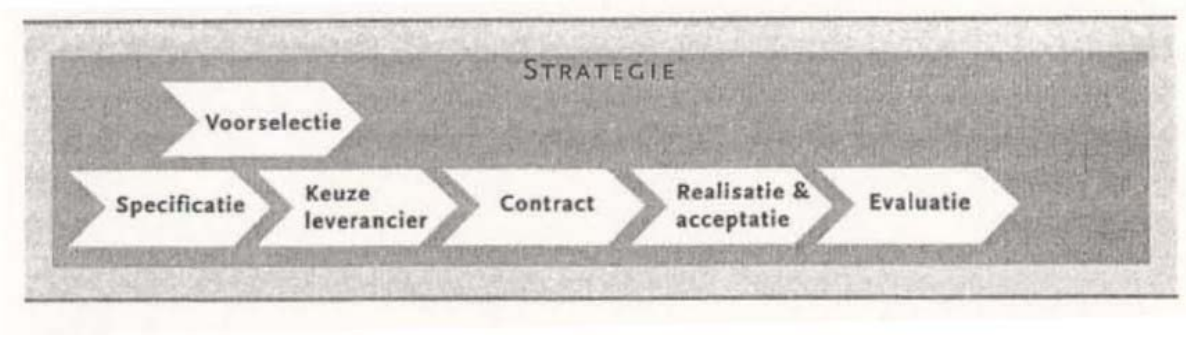
Met deze uitgangspunten als basis geeft Starreveld de volgende onderverdeling van de inkoopfunctie:
1. Het initiatief tot inkoop.
2. Het aanvragen van offertes.
3. De inkoopbeslissing.
4. Het plaatsen van een bestelling.
5. De ontvangst van de goederen.
6. Eventuele retourzendingen.
7. De controle op de levering van diensten.
8. De ontvangst en controle van facturen.
9. De berekening van bijkomende kosten.
10. De behandeling van betalingskortingen.

Binnen deze onderscheidingen is ook weer functiescheiding te onderkennen. Als voorbeeld kan gelden de controlerende functie op de afgeleverde goederen, maar ook het ontvangen van goederen en de ontvangst en controle van facturen. Door het inkoopproces op deze wijze in te delen ontstaan belangentegenstellingen en controlemomenten. Dit veranderd niet na intrede van ICT en/of bij een verantwoorde invoering van ERP. Het logisch model van Starreveld is universeel.

Voor ons onderzoek zijn uitsluitend de eerste drie stappen van belang. (*Bron: Hoofdstuk 1.2, Starreveld, Van Leeuwen en Van Nimwegen, Bestuurlijke Informatie Verzorging Deel 1: Algemene Grondslag, 5^{e} druk, 2002*).

3.3 Aanbesteding van ICT-projecten

De strategie van aanbesteden ziet er als volgt uit:



3.3.1 Voorselectie van aanbieders

A-priori is het uitgangspunt dat de beslissing tot aanbesteding is genomen (hetzij op wettelijke dan wel alleen op zakelijke gronden) en dat het programma van eisen opgesteld is. In een eerste ronde van aanbesteding, waarbij alleen de hoofdzaken worden bekend gemaakt, kan een voorselectie van aanbieders worden gemaakt. Met deze aanbieders wil de aanbesteder verder. De details van het programma van eisen worden aan hen bekend gemaakt, eventueel in een vertrouwelijk overleg met elk van de geselecteerde aanbieders. De eerste fase is de openbare aanbesteding geweest, in de tweede fase gaan partijen onderhands verder. Dit betekent bepaalt niet dat geen verantwoording verschuldigd is. Integendeel, beslissingen moeten ook in deze fase voldoen aan wettelijke eisen van transparantie, objectiviteit en non-discriminatie.

3.3.2 Specificatie

Het programma van eisen, ofwel bestek, vormt de specificatie waaraan de aan te kopen applicatie moet voldoen. Deze eisen liggen op functioneel gebied, op technische gebied, kunnen juridisch van aard zijn, een financiële achtergrond hebben, enzovoort. In dit stadium moeten dus ook de eisen voor informatiebeveiliging bekend zijn. Deze dienen afgeleid te worden van het normenkader van de organisatie die de opdracht tot aankoop verleent. In dit stadium is het van groot belang dat de organisatie zodanig is dat inderdaad gebruik gemaakt wordt van de richtlijnen, procedures en normen die de organisatie heeft vastgesteld. Die hebben uiteindelijk immers tot doel dat het aan te kopen product gaat meewerken om de business goals te bereiken op de wijze die de organisatie wenst. Voor deze scriptie zijn met name de informatiebeveiliging, welke het aspect databenadering (de aspecten C.I.A.A.) raakt en de beheersaspecten van belang.

3.3.3 Keuze leverancier

Aan de hand van de vergelijking van de offertes wordt een keuze gedaan voor de leverancier waar de aanbesteder mee in zee wil gaan. Voorwaarde is dat de offertes onderling vergelijkbaar zijn

3.3.4 Contract

Het contract is de schakel tussen het aanbestedingstraject en het aangaan van de verbintenis tot aankoop. In het contract zal verwezen worden naar de specificaties zoals in de aanbesteding vastgelegd. Het contract is cruciaal als het gaat om de vaststelling dat partijen aan hun verplichtingen hebben voldaan.

3.3.5 Realisatie en acceptatie

Op enig moment zal de opdrachtgever vast moeten stellen of datgene wat is verworven

overeenkomstig het afgesloten contract is. Indien niet is geleverd overeenkomstig het afgesloten contract, kan dit leiden tot ontbinding van de afgesloten overeenkomst. Eventueel kunnen er maatregelen worden getroffen om te waarborgen dat het product alsnog aan de wensen voldoet.

3.3.6 Evaluatie

De evaluatie heeft tot doel vast te stellen of de gevolgde procedures hebben geleid tot de aankoop van een goed product. Wat voor verschillen bestaan tussen de aangetroffen werkelijkheid en de vooraf in het normenkader geformuleerde wensen. En wat voor conclusies kunnen hieruit worden getrokken. Deze ervaringen kunnen leiden tot aanpassing van procedures, richtlijnen of normenstelsels. De aanpassingen volgen het 'plan, do, check and act' principe. Dit geldt zeker als blijkt, uit de realisatie- en acceptatiefase, dat aanvullende maatregelen getroffen moesten worden omdat het aangekochte product bijvoorbeeld niet voldoet aan de eisen van informatiebeveiliging die de organisatie stelt. In de evaluatiefase zal dan, naast het vaststellen van de afwijkingen, eveneens vastgesteld moeten worden hoe het zover heeft kunnen komen.

Voor ons onderzoek zijn uitsluitend de eerste drie onderwerpen van belang. (*Bron voor hoofdstuk 3.3: Aanbesteding van ICT projecten,Jacques van Berkel e.a., Stichting Het Expertise Centrum, 1e druk, 2003)*

3.4 Aanbesteding en recht.

3.4.1 Algemeen

Het uitschrijven van een tender door overheden en overheidslichamen is onderworpen aan aanbestedingsvoorschriften. Deze aanbestedingsvoorschriften zijn vastgelegd in:
- Besluit aanbestedingsregels voor overheidsopdrachten.
- Besluit aanbesteding speciale sectoren.

Deze besluiten zijn geldig vanaf 1 december 2005. Ze zijn gebaseerd op Europese richtlijnen. In behandeling is nog de Raamwet aanbesteden, die naar verwachting in 2007 in werking zal treden. (*Bron: Computable, VU Business Publications, 3 februari 2006)*

3.4.2 Wetswijzigingen

In de oude situatie werd onderscheid gemaakt tussen:
1. Openbare aanbestedingen.
2. Niet openbare aanbestedingen.
3. Onderhandelingsprocedure met voorafgaande bekendmaking.
4. Onderhandelingsprocedure zonder voorafgaande bekendmaking.
5. Prijsvraag.

Ten opzichte van de oude situatie zijn er drie opmerkelijke nieuwe vormen:
6. De concurrentiegerichte dialoog, die het de aanbesteder mogelijk maakt wel aan te besteden, maar zonder gedetailleerde specificaties. Deze worden in een vertrouwelijke dialoog met voorgeselecteerde gegadigden besproken.
7. De gunning door middel van een dynamische aankoopsysteem, waarbij de IT als drager van het aanbestedingstraject fungeert.
8. Raamovereenkomsten waarbinnen partijen voor een periode de randvoorwaarden vastleggen.

Het doel van het aanbestedingsrecht is het bieden van gelijke kansen. Daartoe wordt in

de rechtsregels een drietal beginselen uitgewerkt:
1. transparantie
2. objectiviteit
3. non-discriminatie

(B*ron: IT-Recht, Quick Reference voor IT-auditors, juni 2005, NOREA/Kluwer)*.

In een recente procedure heeft de voorzieningenrechter als volgt beslist: “Het toekennen van wegingsfactoren achteraf aan de ruwe scores, door – naar valt aan te nemen – de leidinggevenden van de betrokken afdelingen, zet de deur open voor de mogelijkheid van manipulatie achteraf. Een dergelijke beoordelingsmethodiek voldoet niet aan de eisen van objectiviteit en toetsbaarheid achteraf”. (*Bron: Computable, VNU Business Publications, 3 februari 2006)*.

3.4.3 Algemene rechtsregels

Naast het aanbestedingsrecht is het Burgerlijk Wetboek van toepassing, met de daarop gebaseerde rechtsverhouding die gegrond is op de goede trouw. Dit geldt ook voor het als precontractuele fase te kenschetsen aanbestedingstraject. Een en ander betekent dat partijen zich op de weg naar het contract ook moeten laten leiden door de gerechtvaardigde belangen van de tegenpartij. Voorts dat een overeenkomst vernietigd kan worden als (bijvoorbeeld) sprake is van een wilsgebrek of van misbruik van omstandigheden.
(*Bron: recht en computer, 5^{e} druk, Prof. Mr H. Franken e.a., Kluwer, 2004*)

3.4.4 Conclusie

De aanbesteder moet zich bewegen binnen de wettelijke kaders van het specifieke aanbestedingsrecht en het algemene verbintenissenrecht. Bij een aanbesteding heeft de aanbesteder verschillende mogelijkheden t.a.v. de keuze van de vorm van het aanbestedingstraject. De aanbesteder moet duidelijk zijn in de eisen die aan het te verwerven product worden gesteld. Dit betekent dat een helder normenkader beschikbaar moet zijn als grondslag voor de eisen waaraan het te verwerven object moet voldoen.

4 Veldonderzoek tendertrajecten

4.1 Algemeen

In dit hoofdstuk worden de werkwijze van B/CICT en een viertal tendertrajecten, naar aanleiding van het uitgevoerde veldonderzoek, beschreven. Het veldonderzoek is uitgevoerd bij de Belastingdienst Centrum voor Informatie en Communicatietechnologie (hierna te noemen: B/CICT), afdeling inkoopmanagement.

Binnen de populatie van afgesloten tendertrajecten heeft een selectie plaatsgevonden van geschikte tendertrajecten. De selectie heeft plaatsgevonden aan de hand van een aantal criteria. Deze zijn:
1 De verwerving middels een tender moet betrekking hebben op een applicatie.
2 De applicatie dient raakvlakken te hebben met databenadering en beheersaspecten als beveiliging van resources, bedrijfscontinuïteit van de automatiseringsomgeving, etc
3 De tendertrajecten die geselecteerd worden dienen zo divers mogelijk te zijn.

Naar aanleiding van deze selectiecriteria zijn een viertal tenders geselecteerd. Deze vier tenders zijn op dezelfde wijze ge-reviewed. Dat wil zeggen dat alle vier de tenders zijn

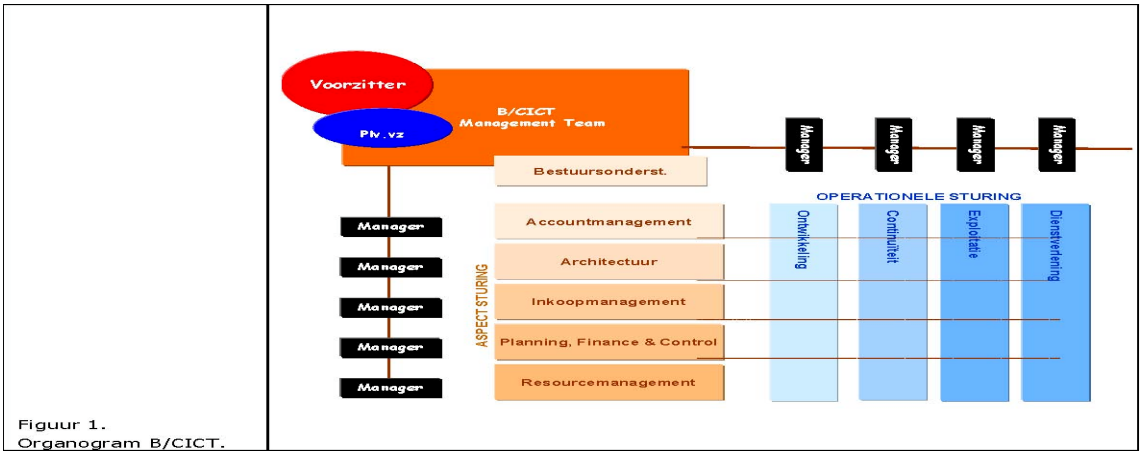
ge-reviewed op dezelfde onderdelen en volgens dezelfde methode:
1 Een opgesteld bestek of programma van eisen.
2 Response in de vorm van ontvangen offertes.
3 Een beoordelings- of wegingsmodel.
4 Gunningsadvies.
Deze onderdelen zijn ge-reviewed op de aanwezigheid van IT-auditaspecten en op de wijze waarop zij in de genoemde onderdelen voorkomen.

Onder de noemer Organisatie B/CICT zal de organisatie en inrichting van het inkoopproces beschreven worden. Daarna zullen de geselecteerde tenders beschreven worden.

4.2 Organisatie B/CICT

4.2.1 Processen

Het B/CICT ontwerpt, bouwt, verwerft en onderhoudt binnen de Belastingdienst applicaties en technische infrastructuur in samenwerking met de opdrachtgevers en gebruikers. Ook beheert het B/CICT het landelijke computernetwerk en de elektronische communicatiefaciliteiten. (zie Figuur 1, Organogram B/CICT).



Figuur 1.
Organogram B/CICT.

Een van de sectoren is Inkoopmanagement en deze is onderverdeeld in de volgende deelprocessen:
1. Tactische inkoop (Europese aanbestedingen).
2. Operationele inkoop (orders en controles).
3. Leveranciersmanagement (relatieonderhoud).
4. Logistiek (ICT-hardware en voorraad).
5. Juridische zaken (ICT en arbeidszaken).

Het onderdeel tactische inkoop is vervolgens onderverdeeld in de procesonderdelen:
1. Inkoop
- Specificeren: Het samenstellen van eenduidige specificaties om de leveranciers een passende offerte uit te laten brengen.
- Selecteren: Het toetsen van de offertes van de leveranciers op basis van het beoordelingsmodel en de offerteaanvraag. Op basis hiervan wordt een gunningsadvies opgemaakt, waarin een leverancier als beste wordt geselecteerd. Het gunningsadvies is input voor het proces contracteren.
- Contracteren: Het afsluiten van het contract met de geselecteerde leverancier en het communiceren over het contract met het B/CICT.
2. Contractmanagement:

Geeft sturing aan het vastleggen, monitoring op het nakomen en anticiperen op de uitputting en expiratie van contracten. Het proces geeft advies over de inhoud en wijze van opstellen van contracten en leverancierperformance. Voor het zekerstellen van een ongestoorde levering is adequaat contractmanagement van essentieel belang.

Voor ons onderzoek valt het contractmanagement buiten de scope.

Voor elk deelproces is een UBGI tabel van toepassing. UBGI is het ingerichte model voor de controletechnische functiescheiding in het inkoopproces en is als statement opgebouwd uit de volgende componenten:

- Uitvoeren.
- Beoordelen.
- Goedkeuren.
- Informeren.

In de tabel is aangegeven welke functionaris of welk instituut verantwoordelijk is voor een bepaalde (deel)processtap, wie goedkeuring moet geven, wie beoordeelt en wie moet worden geïnformeerd

Aan de afdeling inkoopmanagement is een medewerker ‘quality assurance’ toegevoegd. Deze medewerker wordt, hiërarchisch gezien, direct aangestuurd door het management van B/CICT. De QA-medewerker rapporteert rechtstreeks aan het management. Deze QA-medewerker beoordeelt alleen het inkoopproces. Inhoudelijk heeft hij geen bemoeienis met dit inkoopproces. Hij verifieert alleen de verplicht te nemen stappen in dat proces. Wij hebben een tweetal rapportages inhoudelijk doorgenomen. Hierbij zijn ten opzichte van het inkoopproces bij B/CICT geen noemenswaardige afwijkingen bevonden. Uit de rapportages blijkt dat men het opvolgen van adviezen van het vorig onderzoek reviewt. Op deze wijze geeft men vorm aan het principe van de verbetercyclus; ‘plan-do-check-act'. (Bron: procesbeschrijvingen en tenders B/CICT)

<u>Inrichting tendertrajecten B/CICT, afdeling inkoopmanagement</u>

De tendertrajecten worden opgestart en uitgevoerd ter verwerving van een object.
Bij de start hiervan wordt een verzoek tot opdrachtaanvaarding opgesteld, gericht aan inkoopmanagement en afkomstig van bijvoorbeeld de sector Ontwikkeling van B/CICT.
Naar aanleiding van de aanvaarding van de opdracht wordt er een projectteam geformeerd, dat het tendertraject zal uitvoeren. Bij grote projecten wordt er tevens een kernteam geformeerd. Het projectteam legt verantwoording af aan het management van B/CICT.

Het projectteam formuleert een inkoopplan welke het management van inkoopmanagement goedkeurt. In dit inkoopplan wordt de wijze van inkoop vastgelegd. Hiervan zijn te noemen; de te verwerven faciliteit of faciliteiten, de bepaling of de tender openbaar dient te worden aanbesteed in het kader van de aanbestedingsregels, het eventueel opsplitsen in percelen van de aanbesteding, de tijdsplanning, het determineren van de mijlpalen in het project, de wijze van voortgangsrapportage, de organisatie van het projectteam met autorisatiematrix en het projectbudget.

Na vaststelling van het bestek volgt publicatie in het kader van de openbare aanbesteding. Bij grote projecten wordt het eigenlijke bestek voorafgegaan door de publicatie waarin een Request for Information wordt gevraagd. Het Request for Information wordt gebruikt voor projecten waarbij gebruik wordt gemaakt van bijvoorbeeld nieuwe technologische ontwikkelingen, die nog enige mate van onzekerheden met zich meedragen. Het is daarbij de bedoeling dat de aanbieders zelf concepten schetsen ter invulling van de klantwens. Reacties van gegadigden zijn geadministreerd en op verzoek is het bestek verzonden aan deze gegadigden. Ook

eventuele afmeldingen van mededingers zijn geadministreerd.

Het projectteam is eveneens verantwoordelijk voor de beoordelingsprocedure en het wegingsmodel. De wegingsfactoren worden door het projectteam vastgesteld, ter goedkeuring voorgelegd en opgenomen in het bestek. De offertes worden door verschillende projectleden beoordeeld en afwijkende scores geëvalueerd. Op de weging van de verschillende offertes volgt het gunningsadvies. De gunning is voorbehouden aan het management van B/CICT. Dit geldt ook voor de ondertekening van de contracten.

4.3 Tender 1: Antivirus

4.3.1 Algemeen

Doel van de aanbesteding is het selecteren van één of meer leveranciers die in staat zijn antivirussoftware, ondersteuning bij de implementatie, support en software update's te leveren.

Virussen kunnen op diverse manieren binnen de Belastingdienst Technische Infrastructuur (TIS) terechtkomen. Daarnaast is het noodzakelijk dat implementatie en configuratie van het antivirus product met single point of administration kan plaatsvinden. Hierdoor kan op een snelle wijze adequaat worden gereageerd, en initiatieven worden genomen, bij het ontstaan van besmettingen. Een single point of administration geeft ook inzage in de betrouwbaarheid van koppelpunten.

Virusbesmettingen kunnen plaatsvinden op de diverse platformen. Aangezien binnen de Belastingdienst TIS diverse platformen voorkomen, is het van belang dat deze worden ondersteund door het antivirus product.

De Belastingdienst TIS en daarbij gebruikte Platformen worden hieronder genoemd:
- Novell/Windows 2000 lokale fileservers
- GCOS – Unix/HVX/GCOS
- Unix (AIX en HP/UX)
- OS/390 MVS/RACF
- WindowsNT cliënt (vaste werkplek)
- WindowsNT cliënt (portables)
- WindowsNT servers
- Mail-server (Domino)
- WindowsNT TSE-Citrix

Databases:
- sybase
- DB2
- Oracle

Netwerk:
Het TCP/IP netwerk is verdeeld in verschillende compartimenten welke gescheiden zijn door routers en firewalls. De aangeboden oplossing dient een minimale impact te hebben op de instellingen van deze routers en firewalls.

Het tendertraject heeft gelopen van september 2001 tot de ondertekening van het contract in juni 2002.

4.3.2 Bestek

Het bestek bestaat uit de volgende onderdelen:
- Leeswijzer
- Hoofdstuk 1 Algemeen
- Hoofdstuk 2 De aanbestedingsprocedure
- Hoofdstuk 3 Algemene eisen aan de offerte
- Hoofdstuk 4 Functionele en technische specificaties
- Hoofdstuk 5 Financiën
- Hoofdstuk 6 Juridische kaders van de opdracht
- Hoofdstuk 7 ` Bijlage

In hoofdstuk 2 worden de meer formele eisen gesteld waaraan de leveranciers moeten voldoen om mee te kunnen dingen naar de opdracht. Deze eisen zijn:
- Inschrijvers dienen te voldoen aan eisen die hun financiële en economische draagkracht aantonen.
- Daarnaast dienen zij hun technische bekwaamheid aan te tonen met behulp van een bedrijfsbeschrijving en met referenties. Aanbieders die hier niet in slagen kunnen niet voor gunning in aanmerking komen.

Tenslotte worden de aan de testfase gestelde eisen toegelicht.

In hoofdstuk 3 worden de begrippen toegelicht, waarvan voor het onderzoek de eisen, wensen en vragen het belangrijkste zijn. Eisen, wensen en vragen zijn uniek geïdentificeerd en worden als volgt onderscheiden:
- Aan een eis moet worden voldaan. Indien niet rechtstreeks aan de eis kan worden voldaan, moet de leverancier beschrijven op welke indirecte wijze toch aan de eis kan worden voldaan.
- Wanneer een leverancier de in een wens omschreven functionaliteiten niet biedt, zal deze als minder functioneel beoordeeld worden in vergelijking met een concurrerende leverancier, die wel de gevraagde functionaliteit biedt. De offerte zal niet worden uitgesloten van de gunning als aan één of meerdere wensen niet tegemoet kan worden gekomen.
- Een vraag wordt gesteld als het nodig is om aanvullend inzicht te krijgen met betrekking tot een criterium. Het antwoord op de vraag kan dan zodoende invloed hebben op de waardering van een positief oordeel en uiteindelijk in de aanbeveling tot gunning (t.a.v. aspecten als correctheid, compleetheid, inhoud van het antwoord).

In hoofdstuk 4 van het bestek vinden we de IT-auditaspecten terug en is een lijst met gunningscriteria opgenomen. Hiervan zijn te noemen:
- Scandiepte/bereik
- Beveiligingsmaatregelen – preventief
- Beveiligingsmaatregelen – detectief
- Beveiligingsmaatregelen – correctief
- Beveiligingsmaatregelen – repressief
- Distributie – vanuit leverancier naar de Belastingdienst
- Distributie binnen de Belastingdienst
- Services
- Testfase

Hoewel files inhoudelijk op de aanwezig van virussen worden gescand, kan er geen data inzichtelijk worden gemaakt. Derhalve zien we alleen de beheersaspecten tevoorschijn komen.

De tender is opgesplitst in 5 percelen, te weten:
- Perceel A: Mail-server laag (Domino op AIX)

- Perceel B: File-server laag (Novell)
- Perceel C: File-server laag (Windows 2000)
- Perceel D: cliënt laag (vaste werkplekken, portables, beheerwerkplekken)
- Perceel E: Windows NT TSE-Citrix

Gunning vindt plaats aan de inschrijver met de economisch meest voordelige aanbieding. Daarbij worden de volgende gunningscriteria gehanteerd, in volgorde van afnemend belang:
- Financiële aspecten.
- Functionele specificaties.
- Beheer en Exploitatie.
- Technische Specificaties.
- Conformiteit met bijgevoegde overeenkomsten.

Tijdens de testfase wordt de geselecteerde inschrijver geacht de goede werking van de door hem aangeboden software, aan te tonen en eventueel voorkomende problemen op te sporen en waar nodig van een passende structurele oplossing te voorzien.

Ook de financiële aspecten worden in hoofdstuk 5 verder uitgewerkt, zowel algemeen als per perceel.

4.3.3 Beoordelingsprocedure en Wegingsmodel

Als eerste wordt beoordeeld of de financiële en economische draagkracht van de inschrijvers voldoende is. Het resultaat is dat slechts 5 inschrijvers hieraan voldoen en geaccepteerd worden als aanbieder.

Vervolgens wordt beoordeeld of elk van de leveranciers kan voldoen (ja/nee) aan de eisen zoals opgenomen in de functionele - en technische specificaties. Dit leidt er toe dat 1 inschrijver alsnog afvalt daar deze niet kon voldoen aan de algemene eisen. Verder valt nog 1 inschrijver af voor 1 perceel omdat deze niet kan voldoen aan de specifieke eisen voor dat perceel.

Vervolgens worden de wensen en vragen uit de specificatie beoordeeld. Daarbij worden de volgende gunningscriteria voor de percelen gehanteerd:

	Criteria	Weging
G1	Financiële aspecten	35
G2	Functionele specificaties	25
G3	Beheer en Exploitatie	22,5
G4	Technische specificaties	12,5
G5	Conformiteit met bijgevoegde overeenkomst	5

Prijs (G1) en kwaliteit (G2, G3. G4 en G5) krijgen vervolgens een weging van respectievelijk 0,4 en 0,6. Deze laatste weging leidt tot de definitieve score die bepalend is voor de beste prijs-kwaliteitverhouding en daarmee voor de keuze van de contractpartner.

4.3.4 Gunningsadvies

De conclusie van het projectteam is dat één inschrijver op het gebied kwaliteit op alle percelen het beste scoort (waarbij alle percelen even zwaar meewegen), maar op prijs maar matig scoort als de percelen afzonderlijk worden afgenomen. Echter, als alle percelen aan deze inschrijver worden gegund, scoort deze ook op prijs het beste. Dat

wordt veroorzaakt door een korting die wordt toegekend indien alle 5 percelen aan de aanbieder worden gegund. Aan deze aanbieder is de aanbesteding uiteindelijk gegund.

4.4 Tender 2: Plug and Play Authorisatietooling en Externe Media Encryptie

4.4.1 Algemeen

Aanleiding voor de tender is dat de werkplekken binnen de Belastingdienst gebruik maken van Windows XP. Deze kent een open karakter en is gericht op connectivity met een breed scala aan devices. Vanuit beveiligingsperspectief acht de Belastingdienst het niet wenselijk dat deze connectivity vrij door alle medewerkers gebruikt kan worden. Daarnaast acht de Belastingdienst het noodzakelijk dat de vertrouwelijkheid van elektronische informatie, die in de buitenwereld terecht kan komen, gewaarborgd kan worden.

Het doel van de aanbesteding is het selecteren van een in de markt gangbaar product voor Plug and Play Authorisatietooling (hierna te noemen: PnP AT) en Externe Media Encryptie (hierna te noemen: EME). De aan te besteden faciliteit is bestemd voor de gehele Belastingdienst en voor alle gebruikers. EME alleen voor geautoriseerde gebruikers, welke een subset zal zijn van de eerste verzameling.

De aanbesteding wordt gedaan voor twee percelen, te weten;
- perceel 1 PnP AT
- perceel 2 EME

Het is de mededingers vrij om voor een perceel een aanbieding af te geven, dan wel voor de twee separate percelen of een gecombineerde aanbieding af te geven.

Naar aanleiding van de publicatie van de aanbesteding is er een pre-bidmeeting georganiseerd. Het inkoopproject heeft gelopen van januari 2005 tot en met juli 2005 en is beëindigd door middel van overdracht aan de afdeling contractbeheer en een dechargeverklaring aan inkoopmanagement.

4.4.2 Bestek

Het bestek is opgesteld aan de hand van eisen en wensen. De eisen, waaraan het te verwerven product moet voldoen, zijn in het bestek aangegeven met een (e) achter het betreffende onderdeel. Deze zijn geformuleerd aan de hand van door de organisatie geformuleerd beleid, gebruikerswensen en technische architectuur. Voldoet het aangeboden product niet aan een van eisen, dan wordt de aanbieder in principe uitgesloten van de verdere procedure.
De wensen, in het bestek met een (v) aangegeven achter het betreffende onderdeel, zijn zaken waarop de aanbieder de punten kan verkrijgen in het kader van de gunning.

Het bestek van de percelen PnP AT en EME bestaat uit de volgende onderdelen:
- Leeswijzer
- Hoofdstuk 1 Algemeen
- Hoofdstuk 2 Procedure
- Hoofdstuk 3 Algemene eisen aan de offerte
- Hoofdstuk 4 Functionaliteit
- Hoofdstuk 5 Technische specificaties
- Hoofdstuk 6 Beheer&Exploitatie
- Hoofdstuk 7 ` Financiën
- Hoofdstuk 8 Juridische voorwaarden
- Hoofdstuk 9 Bijlagen

In Hoofdstuk 2 Procedure staan de selectiecriteria en gunningscriteria beschreven.
In het bestek worden de volgende selectiecriteria voor aanbieders aangelegd:
1. Financiële en economische draagkracht. Deze verder in detail uitgewerkte eisen hebben tot doel te komen tot selectie van solide leveranciers.
2. Technische bekwaamheid. De aanbieder wordt in de gelegenheid gesteld zijn technisch kunnen, met referenties en certificaten aan te tonen.

Tijdens de testfase wordt de geselecteerde inschrijver(s) geacht de goede werking van de door hem aangeboden software, aan te tonen en eventueel voorkomende problemen op te sporen en waar nodig van een passende structurele oplossing te voorzien.

In de hoofdstukken 4 Functionaliteit, Hoofdstuk 5 Technische specificaties en Hoofdstuk 6, Beheer&Exploitatie, vinden we de IT-auditaspecten terug.

Van Hoofdstuk 4 Functionaliteit zijn hiervan te noemen;
- Identificatie en Authenticatie
- Autorisatie
- Accounting en Auditing
- Versleuteling

Van Hoofdstuk 5 Technische specificaties zijn hiervan te noemen;
- Inpassing in IT-architectuur
- Platform en Active Directory

Van Hoofdstuk 6 Beheer&Exploitatie zijn hiervan te noemen;
- Acceptatie
- ITIL beheersprocessen als configuratie- en changemanagement

Ten opzichte van de IT-auditaspecten kan er zowel sprake zijn van een eis als van een vraag.

Gunning vindt plaats aan de inschrijver met de economisch meest voordelige aanbieding.

4.4.3 Beoordelingprocedure en Wegingsmodel

Als eerste wordt beoordeeld of de financiële en economische draagkracht van de inschrijvers voldoende is. Het resultaat is dat van slechts 5 inschrijvers de aanbiedingen worden geaccepteerd.

Vervolgens worden de wensen en vragen uit de specificatie beoordeeld. Daarbij wordt de volgende weging van de gunningscriteria voor de percelen gehanteerd:

Gunningscriteria	**Gewicht**	**Bestekvragen**
Product functionaliteit	35%	Hoofdstuk 4
Inpasbaarheid infrastructuur	30%	Hoofdstuk 5
Beheer&Exploitatie	20%	Hoofdstuk 6
Commercieel/Juridisch	15%	Overige hoofdstukken

Voor de geoffreerde prijs wordt de volgende weging toegepast. De goedkoopste aanbieder ontvangt voor het element prijs (in het bestek Total Cost of Ownership, TCO, genoemd) 100% van de te behalen score. Daarna zijn er twee mogelijkheden.
1 Het prijsverschil tussen de laagste en hoogste aanbieder bedraagt minder dan of is gelijk aan 50 procent. In deze situatie krijgt de goedkoopste aanbieder 100

punten. Bij de andere aanbieders wordt per procent afwijking ten opzichte van het goedkoopste bod 2 punten in mindering gebracht.

2 Het prijsverschil tussen de hoogste en laagste aanbieder bedraagt meer dan 50%. In deze situatie krijgt de goedkoopste aanbieder 100 punten en de duurste aanbieder 0 punten. Bij alle andere (tussenliggende) aanbieders wordt per procent afwijking ten opzichte van het goedkoopste aanbod een X-aantal punten in mindering gebracht, waarbij X wordt bepaald op basis van het verschil tussen het hoogste en laagste aanbod.

Binnen de aanbesteding is er sprake van twee percelen. De mogelijkheid bestaat derhalve dat de uitkomst van de weging een tweetal producten oplevert die van verschillende leveranciers afkomstig kunnen zijn. Dit kan problemen opleveren indien achteraf blijkt dat deze twee producten niet kunnen samenwerken. Derhalve is het wenselijk om in de beoordeling een bonus toe te kennen aan combinaties van percelen die van dezelfde leverancier afkomen. Nog wenselijker is het als de twee percelen in een productsuite worden aangeboden. Daarom wordt de volgende constructie toegepast:

- In eerste instantie worden beide producten afzonderlijk beoordeeld;
- Vervolgens worden alle denkbare combinaties van de producten uit beide percelen gevormd;
- Combinaties bestaande uit producten van een aanbieder krijgen een bonus van 15 procent boven op de samengestelde (vermenigvuldigde) score;
- Combinaties bestaande uit producten afkomstig uit een en dezelfde productsuite krijgen en bonus van 30 procent boven op de samengestelde (vermenigvuldigde) score.

De offertes worden, na te zijn beoordeeld op de formele eisen, gewogen. Iedere offerte wordt door meerdere leden van het projectteam beoordeeld. Indien er afwijkingen zijn in de scores voor dezelfde vragen, worden deze afwijkingen besproken. Op deze wijze ontstaat er een gewogen gemiddelde.

4.4.4 Gunningsadvies

De offertes zijn door verschillende leden van het projectteam beoordeeld. Uit de aanbiedingen blijkt dat de meeste aanbieders voor beide percelen gecombineerde aanbiedingen hebben uitgebracht. Eén aanbieder heeft dat niet gedaan. Daarop is door de projectgroep besloten om de twee percelen samen te voegen en de gecombineerde aanbieding te beoordelen.

Het beoordelen van de selectie- en gunningseisen heeft een afvaller opgeleverd. Deze afvaller voldeed niet aan een aantal gunningseisen, waardoor deze partij werd uitgesloten van de gunning. Verder zijn er nog twee partijen geweest waarvan er een, voor wat betreft de aanbieding, niet voldeed aan de vormvereisten en één partij niet aan de eis voor encryptie van een floppy kon voldoen. Men heeft besloten om toch alle offertes toch te beoordelen.

Voor de financiële beoordeling (criterium prijs) is een rekenmodel gebruikt. Verder is iedere vraag gekoppeld aan een subcriterium welke deel uitmaakt van een hoofd- c.q. gunningscriterium. In de onderstaande tabel zijn de (nominale) scores per subcriterium opgenomen waarbij de toegepaste kleuren de volgende betekenis hebben:

Groen: betreffende partij heeft op dit criterium de beste score.
Geel: betreffende partij heeft op dit criterium een gemiddelde score (tussen beste en slechtste).
Rood: betreffende partij heeft op dit criterium de slechtste score.

Subcriterium		Partij 1	Partij 2	Partij 3	Partij 4	Partij 5
A1	Productontwikkeling	72,50	74,17	75,00	79,17	56,67
A2	Beheerbaarheid	66,59	65,34	65,66	74,25	66,25
A3	Support	76,25	50,75	61,25	71,25	66,25
A4	Opleidingen	80,00	83,00	87,50	77,50	87,50
A5	Documentatie	74,06	74,06	74,06	73,13	65,00
B1	Gebruikersvriendelijkheid	63,33	63,33	63,33	79,17	70,00
B2	Versleuteling	36,00	36,00	36,00	81,00	84,60
B3	Performance	48,75	48,75	48,75	52,50	45,00
B4	Rapportage, Alerting en Logging	40,00	40,00	40,00	55,00	30,00
B5	Dekkingsgraad apparatuur	56,67	60,33	56,67	54,17	54,17
B6	Toekomstige ontwikkelingen	47,50	47,50	47,50	59,50	56,25
B7	Accounting	36,67	36,67	36,67	56,67	56,67
B8	Autorisatieniveau's	51,79	51,79	51,79	77,86	66,43
B9	Sleutelbeheer	60,00	60,00	60,00	50,00	40,00
B10	Primaire functionaliteit	90,83	90,83	90,83	86,67	86,67
C1	Schaalbaarheid	84,00	84,00	73,13	73,25	66,75
C2	Compatibiliteit	83,33	83,33	83,33	74,50	71,00
C3	Installeerbaarheid	36,50	36,50	36,50	30,00	36,50
C5	Integratie AD	56,50	56,50	56,50	47,00	40,00
C6	Productarchitectuur	75,00	75,00	68,50	50,00	43,50
D1	Prijs	89,94	100,00	93,64	0,00	2,66
D2	Juridische voorwaarden	50,00	60,00	100,00	80,00	20,00
Aantal keer de beste		9	10	8	8	4
Aantal keer gemiddeld		8	6	9	10	5
Aantal keer slechtste		5	6	5	4	13

Deze uitkomsten hebben middels een verwerking in DSS (wegingsapplicatie) tot de volgende uitslag geleid:

Partij 2	21,9%
Partij 3	21,7%
Partij 1	21,5%
Partij 4	18,4%
Partij 5	16,5%

4.5 Tender 3: DBMS-tooling

4.5.1 Algemeen

Ten behoeve van het mainframe DBMS-tooling heeft het B/CICT op dit moment een contract met een drietal leveranciers. De aanleiding tot het uitvoeren van deze aanbesteding was het aflopen van deze contracten
Onder DBMS-tooling wordt verstaan software die in hoofdzaak is ontwikkeld ter ondersteuning van het beheer van databasemanagementsystemen, en met name de mainframe-DBMS'en, DB2 en IMS.

In het licht van de centralisatie van beheertaken wordt gezocht naar één leverancier die in staat is om tooling te leveren, inclusief onderhoud, ondersteuning en aanverwante dienstverlening. In het bestek wordt aangegeven hoe beleid en architectuur van ICT en applicaties er uit zien. Samengevat betekent dit dat B/CICT zich sterk maakt voor een effectieve en efficiënte gegevensverwerking die zoveel mogelijk centraal wordt uitgevoerd en met de nieuwste maar betrouwbare technologieën is opgebouwd. Het mainframe is daarbij de basis voor massale gegevensverwerking.

In een projectteam, bestaande uit een tenderkernteam (inkoper, jurist en adviseur information economics), aangevuld met technische expertise (productbeheerder, architect, DBA en programmaleider inkoop), zijn de eisen en wensen vastgesteld.

In de beheerinfrastructuur, waarin de tools worden ingezet, wordt onderscheid gemaakt in:
1. Beheerstoepassingen, de servicemanagementtools die procestaken ondersteunen.
2. Generieke exploitatiehulpmiddelen, in gebruik bij de technisch specialisten.
3. Event console, de ontkoppellaag tussen de beheertoepassingen en de generieke exploitatiehulpmiddelen.
4. Rapportagetools voor onder andere serviceniveaurapportage.

Vervolgens wordt een toelichting gegeven op functionaliteit, beheer en financiën. De toelichting wordt aangevuld met eisen en vragen.

De periode van het tendertraject heeft van januari 2005 tot eind juli 2005 gelopen en is beëindigd met de ondertekening van het contract en het verlenen van decharge aan inkoopmanagement.

4.5.2 Bestek

Het bestek bestaat uit de volgende onderdelen:
- Leeswijzer
- Hoofdstuk 1 Algemeen
- Hoofdstuk 2 Procedure
- Hoofdstuk 3 Algemene eisen aan de offerte
- Hoofdstuk 4 De tool
- Hoofdstuk 5 Financiën
- Hoofdstuk 6 Juridische voorwaarden
- Hoofdstuk 7 ` Planning
- Hoofdstuk 8 Bijlagen

In hoofdstuk 2 worden de begrippen toegelicht waarvan voor het onderzoek de eisen, wensen en vragen de belangrijkste zijn. Eisen en vragen zijn uniek geïdentificeerd en worden als volgt onderscheiden:
- Aan een eis moet worden voldaan.
- Met vragen wordt beoogd uw aanbieding af te kunnen zetten tegen concurrerende aanbiedingen. Indien u de vraag niet beantwoordt, scoort u laag in de beoordeling.

Eveneens in hoofdstuk 2 worden de meer formele eisen gesteld waaraan de leveranciers moeten voldoen om mee te kunnen dingen naar de opdracht. Deze eisen zijn:
- Invullen en ondertekenen van de verklaring “Bevordering Integriteits Beoordelingen door het Openbaar Bestuur".
- Conformiteit aan de Business Etiquette van de Belastingdienst.
- Inschrijvers dienen te voldoen aan eisen die hun financiële en economische

draagkracht aantonen.
- Daarnaast dienen zij hun technische bekwaamheid aan te tonen met referenties. Aanbieders die hier niet in slagen kunnen niet voor gunning in aanmerking komen.

Vervolgens, als de aanbieder aan al deze eisen heeft voldaan, komt de beoordelingsfase, waarin het doel is te komen tot selectie van de aanbieder met de economisch meest voordelige aanbieding. Daarbij wordt gebruik gemaakt van toekenning van punten aan de beantwoording van de vragen en een weging van de geoffreerde prijs. De uitkomst van de weging is een rangorde van leveranciers.

Ten slotte worden de eisen, gesteld aan de testfase, toegelicht.

In hoofdstuk 4 van het bestek is een lijst gunningscriteria opgenomen. Tevens zien we hierin de IT-auditaspecten naar voren komen. Per item is aangegeven of sprake is van een eis dan wel van een vraag. Aan een eis moet volledig en zonder voorbehoud worden voldaan. Wordt geen antwoord gegeven of een voorbehoud gemaakt, dan is de score nee, en kan de inschrijver dus niet voor gunning in aanmerking komen. De lijst is onder te verdelen in:
1. Beleid en architectuur
2. Functionaliteit
3. Beheer
- installatie
- beveiliging
- storingen
- service en ondersteuning
- capacity & performance
4. documentatie en opleiding

De IT-auditaspecten zitten met name in de onderdelen 2 en 3:
- back-up en recovery
- installeerbaarheid op de configuratie
- beïnvloeding van andere software
- beveiligbaar via RACF
- application controls
- herstelbaarheid
- beveiliging, registraties, autorisatie, logging

In hoofdstuk 5 worden eisen en vragen verwoord met betrekking tot:
1. financiën
2. software licenties
3. maintenance & support
4. dienstverlening

Ook hoofdstuk 6 bevat nog eisen en wensen, en dan op het vlak van de juridica.

Gunning vindt plaats aan de inschrijver met de economisch meest voordelige aanbieding.

4.5.3 Beoordelingsprocedure en Wegingsmodel

Als eerste wordt beoordeeld of de financiële en economische draagkracht van de inschrijvers voldoende is. Vervolgens wordt bezien of elk van de leveranciers kan voldoen (ja/nee) aan de eisen uit de functionele en technische specificaties. Vervolgens worden de wensen en vragen uit de specificatie beoordeeld. Daarbij worden de

volgende weging van de gunningscriteria voor de percelen gehanteerd:

Functionaliteit	42%
Prijs	35%
Beheer	18%
Juridische voorwaarden	5 %

De waardering vindt plaats door leden van een team, eerst elk afzonderlijk en vervolgens door het team, waarbij significante verschillen besproken worden. De uiteindelijke score wordt ingevoerd in DSS, een wegingsapplicatie.

Met betrekking tot het aspect prijsaanbieding wordt aldus gehandeld:
- De voordeligste aanbieding scoort 30 punten.
- Iedere procentuele afwijking ten opzichte van deze aanbieding leidt tot een aftrek van 1/33 van 30 punten.
- Een afwijking van 33% leidt zodoende tot 0 punten.

4.5.4 Gunning

Uiteindelijk zijn er drie aanbieders die doorstromen naar deze fase.
De scores die zij behalen zijn:

	Maximum	A	B	C
Functionaliteit en beheer	60	35,99	53,92	43,41
Juridische voorwaarden	5	3,55	3,85	2,25
Prijsgerelateerde vragen	5	0,90	0,25	1,25
Prijsaanbieding	30	30	0,00	0,00
Totaal	100	70,44	58,02	46,91
Ranking		1	2	3

Uit deze tabel blijkt dat de winnaar het minst scoort (van de drie) op functionaliteit en beheer en door het onderdeel prijsaanbieding als eerste eindigt. Zelfs al zouden beide andere aanbieders op prijs 0 punten hebben gescoord, maar op de overige aspecten het maximale (70 punten) zouden zij het afgelegd hebben tegen de winnaar.
Leverancier A heeft voldaan aan alle eisen, een voldoende gescoord op functionaliteit en een scherpe prijs geboden. De aanbieding van A heeft hiermee de beste totaalscore gerealiseerd. Het advies is dan ook om de opdracht voorwaardelijk aan A te gunnen. Het voorbehoud bestaat uit het met goed resultaat afronden van de testfase en het succesvol afsluiten van de benodigde overeenkomsten.

4.6 Tender 4: Mobiel werken

4.6.1 Algemeen

Het doel is om op termijn de gehele Belastingdienst te kunnen voorzien van mobiele oplossingen. Daarom wordt er gezocht naar een leverancier, die de rol van ‘Partner Mobiele Diensten’ voor het realiseren van mobiele oplossingen moet gaan vervullen. De partij aan wie gegund wordt, zal samen met B/CICT, de komende jaren mobiele oplossingen voor de Belastingdienst ontwerpen, bouwen, implementeren en beheren. Per klantvraag zal de partner een opdracht krijgen om een bijdrage te leveren in het tot

stand komen van de mobiele oplossingen. In elke fase blijft B/CICT eindverantwoordelijke.

De specificaties worden Belastingdienstbreed opgesteld, maar blijven gericht op het bereiken van 1e, 2e, en 3e plateaus. Na selectie van een partner worden, na een gezamenlijk ontwerptraject, de eerste bestellingen voor het ontwikkelen van mobiele applicaties bij de geselecteerde partij geplaatst. De Belastingdienst wil grip houden op alle aspecten van de te ontwikkelen oplossingen. De geselecteerde partij mag geen applicaties ontwikkelen met behulp van niet-marktconforme exotische technologie met als gevolg dat in de toekomst expertise schaars is en de exotische apparaten niet meer ondersteund kunnen worden. Daarom zal, voorafgaand aan iedere nieuwe klantvraag een product/proces- en architectuurfase uitgevoerd worden. De partner draagt hieraan bij, maar B/CICT is de beslissende partij.

Naar aanleiding van de publicatie van de aanbesteding is er een pe-bidmeeting georganiseerd. In de publicatie is er een Request for Information gevraagd. Dit in tegenstelling tot de meeste aanbestedingen waarin een Request for Proposal wordt gevraagd. Daar het hier gaat om oplossingen welke niet standaard zijn, zowel voor de mobiliteit als voor de apparatuur als voor de applicaties, wordt de markt eerst gevraagd een visie weer te geven en aan te geven welke technologie er voorradig is en op welke wijze men mobiele oplossingen wil toepassen. In het Request for Information wordt tevens duidelijk gevraagd cases te beschrijven van projecten welke de aanbieder al heeft uitgevoerd, zijn rol hierin en de mobiele oplossingen welke men ontwikkeld en toegepast heeft.

Het inkoopproject heeft gelopen van april 2005 tot en met oktober 2005 en is beëindigd door middel van overdracht aan de afdeling contractbeheer en een dechargeverklaring aan inkoopmanagement.

4.6.2 Bestek

Het bestek is opgesteld aan de hand van eisen en wensen. De eisen waaraan het te verwerven product in het bestek moet voldoen, in het bestek aangegeven met een (e) achter het betreffende onderdeel, zijn geformuleerd aan de hand van door de organisatie geformuleerd beleid en technische architectuur. Voldoet het aangeboden product niet aan een van eisen, dan wordt de aanbieder uitgesloten van de verdere procedure.
De wensen, in het bestek met een (v) aangegeven achter het betreffende onderdeel, zijn zaken waarop de aanbieder de punten kan verkrijgen in het kader van de gunning.

Het bestek bestaat uit de volgende onderdelen:
- Leeswijzer
- Hoofdstuk 1 Algemeen
- Hoofdstuk 2 Procedure
- Hoofdstuk 3 Algemene eisen aan de offerte
- Hoofdstuk 4 Visie op mobiel werken Belastingdienst
- Hoofdstuk 5 Functionele specificaties
- Hoofdstuk 6 Technische specificatie
- Hoofdstuk 7 ` Beheer&Exploitatie
- Hoofdstuk 8 Financiën
- Hoofdstuk 9 Juridische voorwaarden
- Hoofdstuk 10 Bijlagen

In Hoofdstuk 2 Procedure staan de selectiecriteria en gunningscriteria beschreven.
In het bestek worden de volgende selectiecriteria voor aanbieders aangelegd:

1 Financiële en economische draagkracht. Deze verder in detail uitgewerkte eisen hebben tot doel te komen tot selectie van solide leveranciers.
2 Technische bekwaamheid. De aanbieder wordt in de gelegenheid gesteld zijn technisch kunnen, met referenties en certificaten aan te tonen.

In dit tendertraject is er geen sprake van een testfase.

In hoofdstuk 4 beschrijft de Belastingdienst haar visie op 'Mobiel Werken'. Hoewel dit redelijk globaal is neergezet geeft het wel een indicatie van de diverse soorten mobiele functionaliteit die de Belastingdienst in de nabije en verdere toekomst wil hebben alsmede de richting die de Belastingdienst op wil gaan. De visie is voor de totale functionaliteit van de Belastingdienst, die er verwacht wordt, voor de komende jaren op mobiel gebied uitgewerkt. De functionaliteit is beschreven op basis van use-cases en beschrijven vanuit het gezichtspunt van een actor de functionaliteit van een systeem. Er is in de functionaliteit een ordening gemaakt in de use-cases en verdeeld over drie logische systemen, te weten:

- *Mobiel datasysteem*
  Systeem dat de mobiele ambtenaar 'in het veld' door middel van ICT ondersteunt, d.w.z. voorziet van informatie afkomstig uit andere systemen, gegevenstransacties in andere systemen kan laten uitvoeren, datacommunicatie met andere partijen of systemen mogelijk maakt en overige (standalone) functies biedt zoals tekstverwerken en route plannen.
- *Plaatsbepalingssysteem*
  Systeem de geografische positie van een mobiele ambtenaar kan bepalen en gegevens hierover beschikbaar kan stellen aan o.a. het mobieldatasysteem (t.b.v. route plannen en navigeren) en het regie- en begeleidingssysteem.
- *Regie- en begeleidingssysteem*
  Systeem dat door de ambtenaren op kantoor gebruikt wordt voor het aansturen en begeleiden van de mobiele ambtenaren.

Deze verdeling in logische systemen behoeft niet te leiden tot een identieke verdeling in fysieke systemen.
Het mobiele datasysteem heeft een drietal componenten, te weten:

- Mobiele informatiefunctie voor informatie op te halen uit andere systemen
- Mobiele interactiefunctie voor het uitwisselen van informatie met andere systemen
- Mobiele transactiefunctie voor het uitvoeren van datatransacties in en met andere informatiesystemen

In de hoofdstukken 5 Functionele specificaties, Hoofdstuk 6 Technische specificaties en Hoofdstuk 7 Beheer&Exploitatie, vinden we de IT-auditaspecten terug.

Van Hoofdstuk 5 Functionele specificaties zijn hiervan o.m. te noemen:

- Uitwisselen van gegevens : hierbij zijn vooral de IT-auditaspecten vertrouwelijkheid en exclusiviteit van belang.
- Identificatie, Authenticatie en Autorisatie: in het kader van mobiele datasystemen is het van belang dat de juiste personen toegang verkrijgen tot de data.
- Beschikbaarheid: in het kader van beschikbaarheid netwerk en doorkoppeling naar datasystemen.
- Performance: in het kader van transport van data en de performance van het landelijk dekkend netwerk.
- Logging en Auditing.

Voor dit hoofdstuk heeft de Belastingdienst verzocht om de gestelde vragen beschrijvend te beantwoorden in een zogenoemde 'use-case'. De aanbieder dient behalve een te schetsen oplossing, mede concrete voorbeelden te beschrijven ten einde duidelijkheid te verschaffen over de mogelijkheden, maar ook onmogelijkheden, van de

techniek. Voor dit hoofdstuk wordt het logische model gevraagd.

Van Hoofdstuk 6 Technische specificaties zijn hiervan te noemen:
- IT-architectuur
- E-fundament
- Externe netwerken
- Beveiliging van data, w.o.
    - Identificatie en Authenticatie
    - Autorisatie
    - Vertrouwelijkheid
    - Integriteit
    - Controleerbaarheid
    - Beveiligingsaudit

In dit hoofdstuk worden de technische of fysieke oplossingen gevraagd.

Van Hoofdstuk 7 Beheer&Exploitatie zijn hiervan te noemen:
- Beheersprocessen als configuratie- en changemanagement.

In dit hoofdstuk wordt de aanbieder gevraagd de voorgenomen inrichting van de processen te beschrijven alsmede aan te geven op welke wijze de medewerkers van B/CICT participeren in het beheer. Daarnaast wordt gevraagd de voorgenomen transitie van het beheer van aanbieder naar B/CICT aan te geven.

Ten opzichte van de IT-auditaspecten kan er zowel sprake zijn van een eis als van een vraag. Bij deze tender zijn de IT-auditaspecten ten opzichte van de beveiliging van data en van het netwerk als eis geformuleerd in het bestek in de hoofdstukken 5 en 6. Deze gespecificeerde eisen zijn terug te vinden in Hoofdstuk 5 en Hoofdstuk 6 en dienen technisch te worden afgedwongen c.q. opgelost.

Gunning vindt plaats aan de inschrijver met de economisch meest voordelige aanbieding.

4.6.3 Beoordelingsprocedure en Wegingsmodel

Als eerste wordt beoordeeld of de offerte van elk van de inschrijvers voldoet aan de formele vereisten. Het resultaat is dat van de acht aanbieders er twee aanbieders afvallen.

Vervolgens wordt bezien of elk van de leveranciers kan voldoen (ja/nee) aan de eisen uit de functionele en technische specificaties. Dit heeft er toe geleid dat de zes overgebleven aanbiedingen, na een eerste toets op de formele vereisten, individueel zijn beoordeeld door leden van de projectgroep. Hierbij hebben alle aanbieders voldaan aan de in het bestek geformuleerde eisen. Vervolgens zijn de beschrijvingen van voorgestelde oplossingen in de use-cases beoordeeld en gewogen.

Daarbij wordt de volgende weging van de gunningscriteria gehanteerd:

Gunningscriteria	**Gewicht**
Kwaliteit en levertijd	45%
Prijs	20%
Referentieprojecten	15%
Projectbeheersing	15%
Juridisch	5%

De combinatie kwaliteit en levertijd kent een verhouding van 2:1 met voor kwaliteit maximaal 35 punten en voor levertijd maximaal 10 punten.

Voor deze aanbesteding zijn er subgunningscriteria gedefinieerd, te weten;

Gunningscriterium	Subcriteria	Gewicht
Kwaliteit	Functionaliteit en kwaliteit plateau 1	25,0
	Functionaliteit Toekomst	10,0
Levertijd	Levertijd	10,0
Prijs	Prijsmodel	19,9
	Bankgarantie	0,1
Referenties	Referentie 1	5,0
	Referentie 2	5,0
	Referentie 3	5,0
Projectbeheersing	Vragen	15,0
Juridische voorwaarden	De mate waarin inschrijver integraal akkoord gaat met de voorgelegde overeenkomst(en)	5,0
Totaal		100,0

De offertes worden, na te zijn beoordeeld op de formele eisen, gewogen. Iedere offerte wordt door meerdere leden van het projectteam beoordeeld. In dit tendertraject worden de offertes door verschillende gespecialiseerde afdelingen beoordeeld. Indien er afwijkingen zijn in de scores voor dezelfde vragen, worden deze afwijkingen besproken. Op deze wijze ontstaat er een ‘gewogen’ gemiddelde.

4.6.4 Gunningsadvies

Voorafgaand aan het gunningsadvies worden de aanbiedingen beoordeeld. Gezien de omvang van de aanbesteding en aanbiedingen heeft men besloten de scores te verwerken in een MS-Excel spreadsheet en de totaal scores per onderdeel onder te brengen in de wegingsapplicatie DSS. Verder is gebleken dat de aanbiedingen onderling sterk verschilden in uitvoering betreffende de aangeboden kwaliteit. Onder kwaliteit dient in dit verband te worden verstaan; technologische infrastructuur, apparatuur en applicaties en beheersorganisatie. Men heeft, om de aanbiedingen naast elkaar te kunnen leggen, aanbieders verzocht voorgeschreven aannames door te configureren en door te berekenen in de uitgebrachte aanbieding. Op deze wijze werd het mogelijk de aanbiedingen uniform te beoordelen op de meest relevant geachte aspecten.

Dit heeft geleid tot de volgende onderstaande resultaten.

Kwaliteit en Levertijd	Partij 1	Partij 2	Partij 3	Partij 4	Partij 5	Partij 6
	17,14	12,86	45,00	0	32,14	10,71
Referenties						
	3,75	0	15,00	0	8,75	0
Prijs						
	13,17	13,87	20,00	13,17	1,21	0
Juridische voorwaarden						
	4,47	0	3,42	3,16	5,00	2,37
Project beheersing						
	5,92	11,84	7,89	0	15,00	3,55
Totaal score						
	44,45	38,57	91,31	16,33	62,10	16,63

De opdracht is gegund aan partij 3. De conclusie van het projectteam in het

gunningsadvies was: ‘deze partij biedt een oplossing voor de gewenste functionaliteit die qua kwaliteit (techniek) uitstekend bij de Belastingdienst past. Dit wordt ook bevestigd door het Telematica Instituut die als onafhankelijke partij ondersteuning tijdens het gehele proces heeft geboden’.

5 Evaluatie, conclusie uit veldonderzoek en theorie, en beantwoording onderzoeksvragen

5.1 Algemeen

Dit hoofdstuk is opgezet volgens het stramien:
1. Korte samenvatting van de onderzochte tenders.
2. Evaluatie van het veldonderzoek.
3. Evaluatie van IT-auditaspecten: van theorie naar praktijk.
4. Conclusie met betrekking tot IT-auditaspecten in tendertrajecten.
5. Beantwoording van de onderzoeksvragen.

5.2 Korte samenvatting van de onderzochte tenders

5.2.1 Selectie

Wij hebben, in het kader van dit onderzoek, een viertal tenders onderzocht. Daarbij is naar voren gekomen, dat bij geen van deze tenders van IT-audit gebruik is gemaakt. Bij de selectie van de te onderzoeken tenders hebben wij de volgende criteria gebruikt:

1 De tender moet betrekking hebben op de verwerving van een applicatie.
2 De applicatie dient raakvlakken te hebben met databenadering en/of beheersaspecten, zoals beveiliging van resources, bedrijfscontinuïteit van de automatiseringsomgeving, etc..
3 De tendertrajecten die geselecteerd worden dienen zo divers mogelijk te zijn.

Wij hebben het onderzoek uitgevoerd door middel van een dossierreview, waarbij de nadruk lag op:
- Het bestek.
- De beoordelingsprocedure en wegingsmodel.
- Het gunningsadvies.

Deze onderdelen zijn ge-reviewed op de aanwezigheid en behandeling van IT-auditasepecten.

5.2.2 De vier onderzochte tenders

<u>Antivirus</u>
Het doel van de aanbesteding is het selecteren van één of meer leveranciers die in staat zijn antivirussoftware, ondersteuning bij implementatie, support en software update's te leveren.

Het gunningsadvies kenmerkt zich door de conclusie dat de aanbieder die het beste scoort, dat zowel doet voor de kwaliteit als voor de prijs. Kwaliteit wordt hier dan gebruikt als containerbegrip voor de onderdelen functionele specificaties, beheer en exploitatie, technische specificaties en conformiteit met de standaard overeenkomst.

<u>PnP AT en EME</u>
Het doel van de aanbesteding is het selecteren van een in de markt gangbaar product voor Plug en Play Authorisatietooling en Externe Media Encryptie.

De aanbesteding was aanvankelijk in twee delen gesplitst, maar de voorkeur ging uit naar een leverancier die een gecombineerde aanbieding zou doen. Aangezien de meeste aanbieders een gecombineerde aanbieding deden, is besloten die te beoordelen.

Ook hier blijkt uit het gunningsadvies dat de aanbieder die qua prijs het beste scoorde ook bij de beoordeling van de overige specificaties zeer hoog scoorde.

DBMS-tooling
Het doel van de aanbesteding is het verwerven van software ter ondersteuning van het beheer van databasemanagementsystemen (DB2 en IMS).

Uit het gunningsadvies blijkt dat de partij die als beste scoort, deze positie te danken heeft aan de voordelige prijs. Daarmee heeft hij een dusdanige score opgebouwd, dat de andere partijen dit met hun hogere scores op het gebied van functionaliteit en beheer niet meer kunnen verbeteren.

Mobiel werken
Het doel is om op termijn de gehele Belastingdienst te kunnen voorzien van mobiele oplossingen. De partij aan wie gegund wordt zal samen met B/CICT de komende jaren mobiele oplossingen voor de Belastingdienst ontwerpen, bouwen, implementeren en beheren. Eerst voor een beperkte groep van enkele honderden gebruikers, daarna meer uitgebreid.

Deze aanbesteding kenmerkt zich door een hoge mate van onzekerheid. Of misschien is het beter om te zeggen dat de tender in dit geval niet meer dan een schets bevat, waarbij aan “de markt” wordt gevraagd aan te geven met welk concept de betreffende partij aan de schets denkt te kunnen voldoen.

In deze tender is niet alleen sprake van verwerving van software, maar ook van hardware en infrastructuur. Dit alles met bijbehorende beveiliging.

5.3 Evaluatie van het veldonderzoek

In deze paragraaf evalueren wij de bevindingen uit het veldonderzoek.

5.3.1 Evaluatie van de review van het tenderproces

De evaluatie brengt ons tot de volgende bevindingen:
1. De afdeling inkoopmanagement werkt zeer procesmatig, volgens de hoofdlijnen van het theoretische inkoopmodel, zoals door Starreveld beschreven.
2. In de procesmatige werkwijze van de afdeling inkoopmanagement wordt aanbestedingsrecht toegepast.
3. In het tenderproces is controletechnische functiescheiding ingebouwd.
4. Het vaststellen van het eisen- en wensenpakket geschiedt op basis van interne normen en gebruikerswensen.
5. Zodra er veel onzekerheden zijn in een aanbestedingstraject, wordt er gebruik gemaakt van het instrument Request for Information.
6. Zodra eisen en wensen vaststaan en de weging heeft plaatsgevonden, wordt het resultaat een keuze voor de economisch meest gunstige aanbieding.
7. In de aanbestedingsprocedure is een testfase wel voorgeschreven, maar deze komt pas nadat de geselecteerde aanbieder gecontracteerd is.

Uit de review is het ons aannemenlijk gebleken dat het tenderproces van voldoende

kwaliteit is. (Wij bedoelen hiermee, dat wij niet een vaktechnisch verantwoorde audit op het tenderproces hebben uitgevoerd, dat zou de grenzen van het onderzoeksobject overschrijden. Op basis van onze indruk, en niet meer dan dat, steunen wij op het proces). Daarnaast merken wij op dat IT-auditaspecten alleen voorkomen in de producten die het tenderproces genereert, zoals het bestek, wegingsmodel en gunningsadvies. Daarom beschouwen wij een IT-audit naar het *proces* 'tendertraject' als ondoelmatig. De IT-audit zal zich als zodanig op de producten bestek, wegingsmodel en gunningsadvies, die in het tendertraject tot stand komen, dienen te richten.

5.3.2 Evaluatie van de aanwezigheid van IT-auditaspecten

De IT-auditaspecten, zoals beschreven in de kwaliteitsaspecten van hoofdstuk 2, en verder samengevat in de clusters databenadering en beheersaspecten, vinden in de aanbesteding hun plaats in diverse onderdelen. Ten behoeve van de evaluatie van de aanwezigheid van IT-auditaspecten in de onderzochte tendertrajecten is het volgende overzicht gemaakt:

Cluster/Tender	Antivirus	PnP AT	DBMS tooling	Mobiel werken
Databenadering		**X**	**X**	**X**
Beheersaspecten	**X**	**X**	**X**	**X**

Uit bovenstaande tabel blijkt dat er in de tender Anti-Virus geen aspecten van databenadering worden geraakt. De IT-audit beheersaspecten komen in alle onderzochte tenders voor.

5.3.3 Evaluatie van het gewicht van IT-auditaspecten

Wij hebben bevonden dat IT-auditaspecten niet alleen voorkomen in de eisen waaraan leveranciers moeten voldoen. Ook in de wensen/vragen zijn IT-auditaspecten te onderkennen. Het verschil tussen het gewicht van een eis en van een wens/vraag is:

- Aan een eis moet altijd worden voldaan. Wordt daaraan niet voldaan, dan kan de aanbieder niet voor de opdracht in aanmerking komen.
- Aan een vraag of wens behoeft niet of niet volledig te worden voldaan, maar het gevolg daarvan is dat voor dat item geen of minder punten verkregen wordt. Toch kan de aanbieder de opdracht krijgen, als hij in totaliteit de meeste punten scoort. In feite is de afweging: wie voldoet tegen de laagste prijs het beste aan de wensen/vragen?

Verder hebben wij bevonden dat, afhankelijk van het te verwerven object, de hoeveelheid eisen, maar ook wensen/vragen, variëert per tendertraject.

Evaluerend kunnen wij stellen dat het gewicht van een eis groter is dan dat van een wens/vraag en dat het gewicht van IT-auditaspecten, de combinatie van eisen en wensen, tevens varieert per tendertraject.

5.3.4 Evaluatie van de invloed van IT-auditaspecten

Wij hebben bevonden dat een eis ondergraven kan worden door een aanvullende wens/vraag. Dit ondergraaft de formele betekenis van een eis. Een voorbeeld hiervan is (bron tender PnP AT EME):

- Eis; het product moet bijvoorkeur beveiligd kunnen worden met RACF.
- Wens/vraag; geef aan op welke wijze het product beveiligd kan worden.

Deze situatie is verscheidene malen aangetroffen in de onderzochte tenders. Dit heeft tot gevolg dat het totaal van de IT-auditaspecten van weinig invloed wordt in tendertrajecten, mede door het uitgangspunt 'economisch meest gunstige aanbieding',

5.4 Evaluatie van IT-auditaspecten: van theorie naar praktijk

De theorie spreekt van;
- Adviesfunctie.
- Attestfunctie.
- Opdrachtgever.
- Scope van het onderzoek.
- Object van onderzoek.
- Normenkaders.
- Kwaliteitsaspecten.
- Opzet, bestaan en werking.
- Product- of procesaudit.
- Auditrisk, etc..

Wij hebben bevonden dat het voor een effectieve inzet van IT-audit relevant is om eerst te beoordelen wat men met de tender beoogt te verwerven. Wij concluderen vervolgens dat bij gebruik van IT-audit inzet in tendertrajecten, IT-audit moet beginnen met het beoordelen van het te verwerven product op zijn invloed op de organisatie en de, bij dit product behorende, complexiteit en onzekerheid. Naar aanleiding daarvan dient te worden vastgesteld welke kwaliteitsaspecten het te verwerven product verondersteld wordt te gaan raken. Op basis van deze afweging dient de benodigde inzet van IT-audit en de auditrisk te worden bepaald. Vervolgens kan gebruik worden gemaakt van IT-auditmethoden en IT-audittechnieken.

Wij zijn van mening dat, indien IT-audit inzet relevant wordt geacht, er sprake moet zijn van een adviserende functie.

5.5 Beantwoording van de onderzoeksvragen

Komen IT auditaspecten tot uiting in een tendertraject

De IT-auditaspecten kunnen voor komen in een tendertraject, maar niet altijd en niet allemaal. Een voorbeeld hiervan is de tender Anti-Virus waar het clusteraspect databenadering niet aanwezig is (zie par. 5.3.2). IT-auditaspecten bevinden zich in het kielzog van het te verwerven product. Geconcludeerd kan worden dat door het inkoopproces en het gebruik van de interne normenkaders, die de inkooporganisatie gebruikt voor het opstellen van het inkoopplan en bestek, de inherent aanwezige IT-auditaspecten tot uiting komen.

5.5.1 Zijn IT-auditfactoren van invloed in een tendertraject

De geselecteerde tenders raken allen op enigerlei wijze het aspect databenadering en/of beheersaspecten. Uit het veldonderzoek kan de conclusie getrokken worden dat IT-auditaspecten niet van doorslaggevende betekenis zijn geweest. De invloed ervan heeft niet verder gestrekt dan het minimum beheersingsniveau, zoals dat is gedefinieerd in de interne normen van de organisatie. De invloed van IT-auditaspecten, die het minimum beheersingsniveau overstijgen, wordt vaak ondergesneeuwd door het principe van de gunning: ‘economisch meest gunstige aanbieding’.

5.5.2 Wat zijn de gevolgen voor de organisatie en de beheersingsvraagstukken voor de automatiseringsomgeving indien IT-auditaspecten niet erkend worden in een tendertraject

Zoals reeds eerder vermeld wordt bij het samenstellen van het eisen- en wensenpakket geen IT-audit geconsulteerd. De IT-auditaspecten die wel erkend worden, en als eis

en/of wens/vraag worden opgenomen in het bestek, zijn afgeleid van de vastgestelde interne normen. Dit heeft enerzijds tot gevolg dat, in de na het sluiten van het contract volgende testfase, of anders bij de implementatie dan wel in de beheerfase, manco's naar boven kunnen komen. Wij doelen dan op manco's op het gebied van databenadering en beheeraspecten. De risico's en bedreigingen die daar weer het gevolg van kunnen zijn en de dan te nemen mitigerende maatregelen kunnen van een organisatie een grote inspanning vragen. Het valt niet uit te sluiten dat deze inspanning de dan opgedane winst van het tendertraject (economisch meest gunstige aanbiedingen), weer te niet doet of zelfs kan overstijgen.

5.5.3 Is het inzetten van IT-audit in ieder willekeurig tendertraject noodzakelijk

Naar aanleiding van de beantwoording van de drie hier voor staande onderzoeksvragen kunnen we concluderen dat het inzetten van IT-audit noodzakelijk is, maar niet in ieder willekeurig tendertraject. Deze noodzaak komt naar voren uit het van onvoldoende invloed zijn van IT-auditaspecten en het gevolg hiervan , te weten; onvoldoende toevoeging van kwaliteit. Dit kan zich dan weer vertalen naar problemen in de beheerfase, onvoldoende beheersniveau van de (automatiserings)organisatie en het extra inzetten van resources om dit op te lossen.

5.6 Conclusie relevantie IT-auditaspecten in tendertrajecten

In tendertrajecten voor de aankoop van ICT-producten, en met name voor applicaties, kunnen IT-auditaspecten aanwezig zijn. Uit de evaluatie en de beantwoording van de onderzoeksvragen kunnen wij de volgende conclusies trekken:

- Er is verschil te ontdekken in gewicht en invloed van IT-auditaspecten per tender.
- Bovendien vallen verschillen te constateren in de complexiteit van IT-auditaspecten in de onderzochte tenders.
- Het te verwerven product kan daarnaast onzekerheden met zich meebrengen. Deze onzekerheden blijken weer een relatie te hebben met de producten die zogenaamd 'Off the Shelf' komen en 'proven technology' hebben, en producten waar een zeker maatwerk uit voort komt.
- Daarnaast blijkt dat producten, waarin het maatwerk toeneemt en daarbij ook de onzekerheden, een groter risicoprofiel verkrijgen, en navenant meer impact in de (automatiserings)organisatie hebben.
- Naarmate ze meer impact hebben moet de (automatiserings)organisatie meer 'effort' leveren om de risico's middels beheersingsmaatregelen af te dekken.

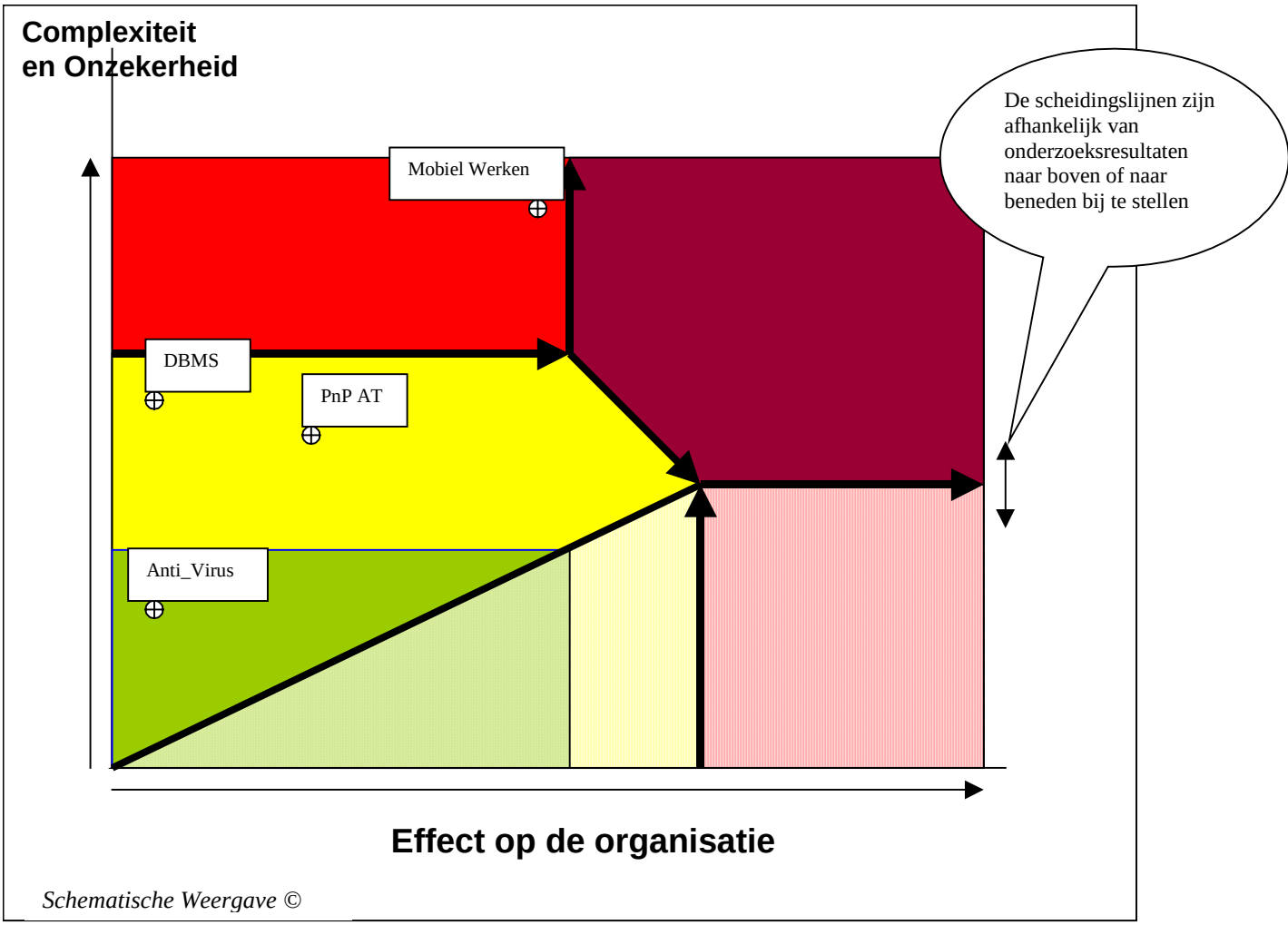
Indien sprake is van de aanschaf van standaardproducten met een beperkte complexiteit en onzekerheid in IT-auditaspecten, en een beperking in het effect op de organisatie, dan kan er worden gesteund op het functioneren van de organisatie en is inzet van IT-audit niet nodig. In de situatie dat sprake is van een toenemende complexiteit en onzekerheid alsmede een toename van het effect op de organisatie, zoals bijvoorbeeld bij de tender Mobiel werken het geval is, dan zou IT-audit zelfs op meer plaatsen in het traject ingezet moeten worden.

De conclusies kunnen verwerkt worden in een schematische weergave. Op de verticale-as kunnen dan de begrippen 'complexiteit en onzekerheid' geplaatst worden en op de horizontale-as 'effect op de organisatie'. Voor de tenders van het veldonderzoek kan dan in deze grafiek kan een plaats worden aangegeven voor tendertrajecten die geen IT-audit inzet nodig hebben, tendertrajecten waarvoor een beperkte inzet van IT-audit verlangd wordt en tendertrajecten waarvoor volledige IT-audit advisering noodzakelijk wordt geacht. De door ons dik getekende lijnen hebben de volgende betekenis:

- Tussen geel en lichtrood; overgang naar volledige trajectadvisering, veroorzaakt door grotere complexiteit en onzekerheid en/of toename van het effect op de organisatie.

- De lijn die het donker rode vlak begrenst; het donker rode gebied kenmerkt een grote mate van complexiteit en onzekerheid, in combinatie met bijna maximale effecten op de organisatie. In dat donkerrode gebied heeft de organisatie een vergrote kans op een zogenaamde ‘bleeder’.
- De schuine lijn tot donkerrood, daarna afbuigend; het rood gearceerde gebied kenmerkt zich door minimale complexiteit en onzekerheid, in combinatie met bijna maximale effecten op de organisatie. In dit gearceerde gebied dient de organisatie zich af te vragen of er niet geautomatiseerd wordt om te automatiseren.

In een schematische weergave zou er dit dan als volgt zichtbaar kunnen worden gemaakt.



Geen IT-auditing noodzakelijk

IT-auditing beperkt noodzakelijk

IT-auditing noodzakelijk

IT-auditing noodzakelijk, gevarengebied voor de organisatie

Geen IT-auditing noodzakelijk

IT-auditing beperkt noodzakelijk

IT-auditing noodzakelijk, kosten-baten analyse

6 Epiloog

6.1 Beantwoording van de hoofdvraag

De hoofdvraag (uit Hoofdstuk 1), luidt: “Is het inzetten van IT-audit in tendertrajecten wenselijk, bezien vanuit het perspectief van beheersing?”.

Op deze vraag kan, gezien de beantwoording van de onderzoeksvragen, geen eenduidig ‘ja’ geantwoord worden. Voor de beantwoording van de hoofdvraag komt het er op neer dat indien een bepaalde complexiteit en onzekerheid in IT-auditaspecten van toepassing is, het inzetten van IT-audit wenselijk wordt. Neemt daarnaast ook nog eens het effect op de organisatie toe, dan wordt de wenselijkheid nog groter. Het wenselijke eraan is tweeledig.

Een is dat inzetten van IT-audit het omvangrijk auditten in de beheerfase kan beperken waardoor een grotere effectiviteit van de IT-auditcapaciteit valt te behalen. Al was het alleen maar omdat tegenwoordig omvangrijk auditten, vanwege de toegenomen complexiteit van automatiseringsomgevingen, als ondoenlijk wordt beschouwd. Zeker als daarbij ook de beperkte beschikbare IT-auditcapaciteit in ogenschouw wordt genomen.

Twee is dat, vanwege de afwisseling in tendertrajecten en de te verwerven objecten, de ‘plan-do-check-act’ cyclus niet goed functioneert. Er valt geen uniform en gedetailleerd normenkader te ontwikkelen dat geldt voor alle tendertrajecten vanwege de grote variatie. Zou dat wel gebeuren, dan zou dat normenkader een te strak keurslijf vormen en zijn doel voorbij schieten, zeg maar ondoelmatig worden, en de inkooporganisatie eerder frustreren. Derhalve is het hanteren van een minimum voor het beheersniveau, middels de interne normenkaders, een vrij realistische opvatting en komt het de effectiviteit van een inkooporganisatie ten goede. Bij het raken van IT-auditaspecten en een toename van onzekerheden zal de IT-auditor een waardevolle aanvulling in het inkoopproces blijken te zijn en zijn rendement voor de latere beheerfase vermeerderen. ‘The best of two worlds’, willen we stellen.

6.2 Toetsing van de hypothese

‘Kan, om IT-auditcapaciteit zo effectief mogelijk te benutten, een optimaal inschakelmoment bepaald worden voor tendertrajecten’.

Het antwoord hierop is: ‘ja’, mits sprake is van een beperking van de complexiteit in IT-auditaspecten en onzekerheden, die het te verwerven object met zich meebrengt. Dan kan volstaan worden met een eenmalig inschakelmoment. Vanwege de rechtsregels inzake openbare aanbestedingen ligt dat inschakelmoment in de bestekfase. Het formuleren van de juiste objecteisen in deze fase zorgt voor een grotere effectiviteit van IT-audit inzet en verhoogd de kwaliteit van het product.

6.3 Toekomstvisie

In het inkoopproces waar de tenders worden uitgevoerd, moet ruimte geschapen worden om IT-audit in te zetten. IT-audit zou door de inkooporganisatie op de hoogte moeten worden gesteld van de op handen zijnde aanbestedingen en vervolgens kan IT-audit vaststellen welke aanbestedingen in aanmerking komen voor begeleiding/advisering. Het ontwikkelde model van paragraaf 5.5 kan hiervoor een hulpmiddel zijn.

6.4 Persoonlijke reflectie

Wij hadden niet gedacht dat we tijdens dit onderzoek zo weinig IT-audit inzet zouden signaleren. Daartegenover staat dat ons onderzoek ons in aanraking heeft gebracht met aspecten van IT-audit die het gehele vakgebied bestrijken. Dit zijn twee constateringen die haaks op elkaar staan. Wij hebben getracht in ons onderzoek en met onze conclusie een brug te slaan zonder te verzanden in uitgebreide regels of selectiecriteria. Wij zijn wij van mening dat het opstellen van meer regels, of het uitgebreid opsommen van selectiecriteria, niet bijdraagt aan de verwezenlijking van het doel: betere beheersing van IT en effectievere inzet IT-audit. Wij sluiten deze scriptie dan ook af met de opmerking waarmee wij begonnen zijn:

'Men moet de dingen niet ingewikkelder maken dan nodig is'.
(bron: William Occam, filosoof, 1285-1349)